nouvelle édition avec l'ajout de plus de 160 pages
métrologie quantique, inventaire des laboratoires français, glossaire, bibliographie, etc.

Comprendre l'informatique quantique

septembre 2019

Olivier Ezratty

A propos de l'auteur

Olivier Ezratty — olivier (at) oezratty.net , www.oezratty.net , @olivez

consultant et auteur — +33 6 67 37 92 41

Olivier Ezratty conseille les entreprises dans l'élaboration de leurs business plans, stratégies produits et marketing, avec une focalisation sur les innovations technologiques du numérique : objets connectés, santé et intelligence artificielle. Il leur apporte une triple expertise : technologique, marketing et management ainsi que la connaissance des écosystèmes dans les industries numériques.

Il a réalisé depuis 2005 des missions diverses d'accompagnement stratégique et de conférences ou formations dans différents secteurs tels que le secteur **médias/télécoms** (Orange, Bouygues Télécom, TDF, Médiamétrie, BVA), la **finance et l'assurance** (BPCE, BNP, Caisse des Dépôts, Crédit Agricole, Crédit Mutuel-CIC, Generali, MAIF, Société Générale) ainsi que dans l'**industrie et les services** (Schneider, Camfil, Vinci, NTN-STR, Econocom, GrtGaz, SNCF, …). Ces missions toujours très courtes couvrent des conférences, séminaires et formations ainsi que l'assistance à la définition de stratégies produit et d'innovation ouverte.

Ses contributions s'appuient sur un fort investissement dans l'écosystème de l'innovation et sous différentes casquettes, notamment dans l'univers des startups :

- Expert auprès de **Wilco** – ex Scientipôle Initiative – depuis 2007, dans l'accélérateur santé depuis 2016.
- Formateur sur l'intelligence artificielle auprès de **Capgemini Institut**.
- Membre depuis fin 2015 du Comité Scientifique de l'**ARCEP**.
- Membre du jury de divers **concours entrepreneuriaux** comme le Grand Prix de l'Innovation de la Ville de Paris ou la Startup Academy, mentor dans de nombreux **Startups Weekends**.

Il intervient comme conférencier dans divers établissements d'enseignement supérieur tels que HEC, Neoma Rouen, SciencePo, CentraleSupelec, l'Epita, l'Epitech ou Les Gobelins, sur le marketing de l'innovation dans les industries numériques, sur l'entrepreneuriat et le product management, en français comme en anglais selon les besoins. Il est aussi formateur sur l'intelligence artificielle et sur l'informatique quantique pour **Cap Gemini Institut** depuis fin 2017.

Olivier Ezratty est l'auteur du **Rapport du CES de Las Vegas**, publié à la fin janvier de chaque année depuis 2006, et du **Guide des Startups** qui est devenu une référence en France avec plus de 400 000 téléchargements à date, mis à jour tous les ans (23e édition et 13e année en 2019), ainsi que de l'ebook **Les usages de l'intelligence artificielle** en octobre 2017 et novembre 2018, puis **Comprendre l'informatique quantique** en septembre et novembre 2018, puis septembre 2019. Le tout étant publié sur le blog « Opinions Libres » (www.oezratty.net) qui traite de l'innovation technologique vue sous les angles scientifiques, technologiques, entrepreneuriaux et des politiques publiques de l'innovation. Comme photographe, il est aussi le co-initiateur en 2012 de « Quelques Femmes du Numérique ! » (http://www.qfdn.net), devenu une association en 2016, et qui vise à augmenter la place des femmes dans les métiers du numérique, en sensibilisant les jeunes à ces métiers.

Et avant tout cela ? Olivier Ezratty débute en 1985 chez **Sogitec**, une filiale du groupe Dassault, où il est successivement Ingénieur Logiciel, puis Responsable du Service Etudes dans la Division Communication. Il initialise des développements sous Windows 1.0 dans le domaine de l'informatique éditoriale ainsi que sur SGML, l'ancêtre de HTML et XML. Entrant chez **Microsoft France** en 1990, il y acquiert une expérience dans de nombreux domaines du mix marketing : produits, canaux, marchés et communication. Il lance la première version de Visual Basic en 1991 ainsi que Windows NT en 1993. En 1998, il devient Directeur Marketing et Communication de Microsoft France et en 2001, de la Division Développeurs dont il assure la création en France pour y lancer notamment la plateforme .NET et promouvoir la plate-forme de l'éditeur auprès des développeurs, dans l'enseignement supérieur et la recherche ainsi qu'auprès des startups.

Olivier Ezratty est ingénieur de l'école **Centrale Paris** (1985) dénommée CentraleSupelec depuis 2015.

 ISSN 2680-0527

Illustration de couverture : création personnelle associant une sphère de Bloch décrivant un qubit et le symbole de la paix.

Table des matières

Pourquoi

Cela fait déjà plusieurs années que l'informatique quantique m'intrigue. J'ai commencé à l'évoquer aux fins fonds de la rubrique des composants électroniques du **Rapport du CES de Las Vegas** à partir de l'édition 2015 tout en admettant, à l'époque, n'y rien comprendre et en mettant sérieusement en doute la compréhension du sujet par les médias relayant diverses annonces sur le sujet.

Je m'étais donné alors comme objectif de comprendre les enjeux scientifiques, technologiques et économiques de cette branche passionnante de l'informatique avec une échéance précise : ma conférence traditionnelle du Web2Day à Nantes en juin. En juin 2017 était planifiée la conférence **Le quantique, c'est fantastique** que j'ai eu le plaisir de délivrer en plénière avec **Fanny Bouton** le 14 juin 2018 (vidéo). Le Web2day un lieu unique d'expérimentation de nouveaux contenus et formats[1].

J'ai publié pendant l'été 2018 une série de 18 articles sur l'informatique quantique, transformée en ebook fin septembre 2018 puis mis à jour en novembre 2018. Cette version de septembre 2019 est une nouvelle mise à jour, bien plus importante, de cet ebook qui s'épaissit dans plusieurs directions, avec une enrichissement de la partie historique et sur le panorama des grands scientifiques du secteur (dont un plus grand nombre de femmes), des explications techniques plus complètes, une actualisation de l'ensemble du contenu au gré de la riche actualité, la documentation d'un grand nombre de concepts que j'ai pu découvrir ces derniers mois comme le measurement based quantum computing, un point sur la prise en main du sujet par l'exécutif et le législatif en France mais aussi aux USA, une partie entière sur la métrologie, une liste à jour des startups du secteur, un inventaire des laboratoires de recherche quantiques en France une bibliographie et un glossaire complet du sujet.

L'ouvrage tire aussi profit des nombreuses occasions qui m'ont été données de faire découvrir l'informatique quantique dans le milieu professionnel : à la Société Générale, à la BNP, à l'ARCEP, au Cigref[2], au Club Ivy de dirigeants du numérique, dans une formation d'une journée organisée par l'association *Quelques Femmes du Numérique !* chez Roland Berger et avec Axelle Lemaire, auprès de la Commission Européenne et de ses entités en charge de la cybersécurité et auprès de l'European Union Institute for Security Studies et du Council of Foreign Relations (USA). En septembre 2019, Fanny et moi testions aussi une formule originale : expliquer l'informatique quantique en deux heures à un public de jeunes filles de 15 à 18 ans, en compagnie de l'une d'entre elles, Tara Mestman, organisée par l'association « Quelques Femmes du Numérique ! » et Magic Makers, qui forme les jeunes à la programmation. La mixité se prépare très en amont !

---

[1] J'avais eu l'occasion d'y défricher d'autres sujets associant les sciences, l'innovation et l'entrepreneuriat : le merveilleux monde des semiconducteurs (2014), les promesses du séquençage de l'ADN (2015), la biologie de la prise de parole en public, en duo avec Annabelle Roberts (2016) puis l'astronomie et l'entrepreneuriat (2017). En juin 2019, toujours avec Fanny Bouton, nous nous attaquions au sujet des transports du futur.

[2] Le Cigref a lancé en 2018 un groupe de travail sur l'informatique quantique, piloté par Frédéric Lau.

Un sujet complexe mais vulgarisable

Après avoir balayé de nombreux pans de la science et des deep techs, je peux résolument positionner l'informatique quantique, et la mécanique quantique qui la sous-tend, au top du top de cette échelle de la complexité.

On pourrait juste ajouter un niveau 10 pour un cas particulier de l'informatique quantique, le quantique topologique, que nous aurons l'occasion d'essayer d'expliquer. La cryptographie post-quantique qui est traitée dans cet ouvrage est aussi positionnée entre les niveaux 9 et 10.

Pour ne prendre qu'un exemple, vous pourriez bien tourner en rond longtemps pour piger cette perle, la définition de l'intrication d'une particule qui vaut son pesant d'imbitabilité[3] !

Tout ça pour dire que deux particules intriquées portent les mêmes valeurs quantiques au lieu d'en porter chacune une, individuelle et différente ! Nous décoderons cela dans cet ebook, expliquant cette notion de produit tensoriel et de factorisation.

"deux particules sont dites dans un état intriqué lorsque l'état des deux particules n'est pas factorisable en un produit tensoriel de deux états à une particule."

source : Wikipedia, "Inégalités de Bell"

Cela traduit la difficulté qu'ont de nombreux physiciens de la mécanique quantique à traduire ce qu'ils font en langage naturel ainsi que le lien ténu entre la mécanique quantique et de nombreux concepts mathématiques qui peuvent facilement nous échapper.

Au passage, je précise que cet ouvrage reste du domaine de la vulgarisation et n'a pas la prétention de la parfaite exactitude scientifique, même si de nombreuses parties ont été relues et corrigées par quelques chercheurs spécialistes du domaine.

Comme l'indiquait il y plusieurs décennies **Richard Feynman**, lorsque l'on étudie la mécanique quantique, si l'on croit que l'on a tout compris, c'est que l'on n'a pas tout compris et que l'on se raconte des histoires. **Alain Aspect** le confirme, exprimant toujours des doutes sur sa compréhension de l'intrication quantique dont il a pourtant prouvé l'existence avec des photons dans la fameuse expérience de 1982.

[3] Elle est extraite de la page Wikipedia sur les inégalités de Bell.

La mécanique quantique est le règne physique et métaphorique du “peut-être”, “ou pas” et du “en même temps”[4], d’une approche probabiliste du monde qui a de ce point de vue quelques vagues points communs avec l’approche connectionniste de l’intelligence artificielle.

Il faut l’admettre avec humilité, la pédagogie de l’informatique quantique est un art nouveau et difficile. La méthode “*au ralenti*”, avec de l’écrit complète bien les conférences qui vont toujours trop vite pour nos cerveaux embrumés par un trop grand nombre de nouveaux concepts.

Cet ouvrage se positionne de manière intermédiaire : plus technique que la moyenne de la couverture média de l’informatique quantique, mais bien moins que la littérature scientifique qui est complètement inabordable pour les non-spécialistes.

Le sujet est passionnant car il couvre une large panoplie de sciences et technologies. C’est le paradis de l’ingénieur généraliste et des geeks curieux ! En plus de la mécanique quantique, on y trouve donc de l’informatique, de la cryogénie, de la thermodynamique, des matériaux nouveaux, des semiconducteurs, des radiofréquences, de photonique, des mathématiques, de la programmation et de la géopolitique.

Nouvelle vague pour le numérique

Pourquoi l’informatique quantique devient-elle est un sujet important ? D’abord, parce qu’elle commence à faire parler d’elle, au travers de la communication de grands acteurs du numérique comme IBM, Google, Intel ou Microsoft, avec des annonces impressionnantes qu’il faut cependant prendre avec des pincettes, beaucoup de recul et décoder, si ce n’est “débullshitiser”.

Mais surtout, parce qu’elle pourrait impacter sérieusement de nombreux champs scientifiques puis certains usages du numérique. Elle permettra théoriquement de résoudre des classes de problèmes tellement complexes que les ordinateurs traditionnels, même les supercalculateurs géants, ne pourront jamais traiter.

La préparation de la conférence de Web2day de juin 2018 avait pris du temps, presque un an au compteur ! Une conférence de presse du **CEA** sur l’informatique quantique avait lieu à Paris le même jour pour présenter la publication d’un numéro spécial de Clefs, leur magazine, entièrement dédié aux applications du quantique et qui est d’excellente facture pour développer votre culture scientifique générale sur le quantique[5]. Le journal **La Tribune** publiait le même jour un dossier de quatre pages de mon cru sur l'informatique quantique[6].

---

[4] Qui fait évidemment penser à l’expression macronienne « *en même temps* ». Et l’on commence à parler de « politique quantique », qui n’est que métaphorique, bien entendu. Elle est élaborée par le Président Arménien Armen Sarkissian cité dans Quantum politics and a world turned upside down, et dans le Financial Times dans Quantum politics and a world turned upside down, septembre 2018. Mais à vrai dire, ce qui est ici quantique relèverait plutôt de la théorie du chaos. Le quantique a sa part de chaos, certainement, mais pas que cela.

[5] Lien de téléchargement de ce numéro de Clef. Et conférence du 29 juin 2018 organisée à l’école Polytechnique avec notamment Daniel Estève, Etienne Klein et Christian Gamrat (1h26m).

[6] Voir Le quantique, la prochaine révolution de l'informatique ?, juillet 2018.

Une session sur le quantique avait aussi lieu sur **VivaTech** fin mai 2018 à Paris avec Bo Ewald, président de ce même D-Wave. Et **IBM** présentait les entrailles de son dernier ordinateur quantique sur son stand !

Lors de la préparation de cette conférence du Web2day, Fanny Bouton et moi-même avons eu la chance de pouvoir rencontrer des français et étrangers qui comptent dans le quantique : **Alain Aspect**, le vénérable vérificateur de l'intrication quantique en 1982, **Philippe Duluc** et **Cyril Allouche**, qui pilotent la recherche dans l'informatique quantique chez Atos, **Daniel Estève**, le grand spécialiste des qubits supraconducteurs au CEA à Saclay, **Pat Gumann**, un chercheur des laboratoires d'IBM à Yorktown aux USA, aussi spécialisé dans les qubits supraconducteurs ainsi que **Doug Carmean**, un chercheur de Microsoft qui nous a évidemment parlé des fermions de Majorana qui sont l'équivalent quantique de "en attendant Godot". Nous avons aussi rencontré **Maud Vinet** du CEA-Leti à Grenoble qui pilote les recherches sur les qubits à base de composants CMOS ainsi que **Tristan Meunier** du CNRS Institut Néel. Depuis, s'y sont ajoutés **Philippe Grangier** (CNRS), **Alexia Auffèves** (CNRS, spécialiste de la thermodynamique quantique), les équipes de métrologie quantique de **Thales TRT** et plein d'autres encore.

L'autre raison de cet intérêt soudain pour l'informatique quantique est que nous sommes encore aux débuts d'une longue histoire qui va voir la science et l'industrie se sédimenter, avec la création de nouveaux leaders, et le développement d'un écosystème d'acteurs. Le tout dans un domaine où subsiste une énorme incertitude scientifique et technologique. Il est très difficile d'évaluer la faisabilité de la création d'ordinateurs quantiques opérationnels. Les chercheurs que nous avons rencontrés ont parfois calmé nos ardeurs. Pour eux, il faudra patienter encore quelques décennies avant d'en voir la couleur ! L'ennemi : le bruit ! Ce bruit qui génère des erreurs dans l'évolution des qubits pendant les calculs quantiques et qui est à la fois difficile à éviter et à corriger.

C'est une étude de cas vivante des plus intéressantes. Les phases d'incertitudes sont les périodes pendant lesquelles certaines formes de leadership se construisent. La France va une fois encore se poser la question de son leadership supposé ou mérité sur le sujet. Sur un sujet encore jeune, sommes-nous prêts à relever le défi ? A investir ? Où faut-il le faire ? Que faudrait-il faire pour y arriver ? Ce sont des questions lancinantes qui ont eu leur lot de réponses sur l'intelligence artificielle, avec plus ou moins de bonheur comme nous avons pu le constater avec le Rapport de la Mission Villani publié en mars 2018[7]. En prenant un nouveau sujet plus en amont, nous avons peut-être des chances de mieux nous en sortir. C'est en amont des grandes vagues que les positions se prennent. D'où l'intérêt de la mission parlementaire pilotée par la députée Paula Forteza et lancée en avril 2019.

[7] J'avais décortiqué le rapport Villani dans Ce que révèle le Rapport Villani en mars 2018.

Sommaire et résumé

Cet ebook est un gros pavé. Cela ne vous surprendra pas. J'essaye d'y couvrir tous les recoins du sujet à 360°. Son cœur en est le calcul quantique mais j'y traite des autres applications numériques du quantique comme la cryptographie quantique et post-quantique ainsi que la métrologie quantique.

Voici les grandes parties et leur résumé associé :

Pourquoi l'informatique quantique ?

- L'informatique quantique sert à dépasser les limites des processeurs traditionnels pour des applications spécifiques d'optimisation et de simulation dont la complexité croit de manière exponentielle avec la taille du problème.
- Pourquoi les technologies CMOS classiques sont-elles insuffisantes pour atteindre cet objectif ?

Les scientifiques de la mécanique et de l'informatique quantique

- C'est le "*hall of fame*" du sujet où je mettrais en évidence les efforts de dizaines de scientifiques de renom qui ont découvert puis fait progresser la mécanique quantique, puis l'informatique quantique. Cela brossera une chronologie du domaine, une histoire des idées et rendra aux Césars du quantique ce qui leur revient.

Les basiques de la mécanique quantique

- Quels sont les fondements de la mécanique quantique qui servent à créer des ordinateurs quantiques ? L'intrication, la superposition, la dualité ondes-particules et l'incertitude de la mesure. Cela ne sera pas un cours de mécanique complet, mais juste les bases permettant de comprendre la suite.
- Nous y couvrirons aussi la supraconductivité et la superfluidité qui sont très utilisées dans les ordinateurs quantiques.

Les qubits

- Les ordinateurs quantiques exploitent au niveau le plus bas des qubits, des entités qui ont deux états simultanés (par superposition) et peuvent se combiner via des portes quantiques (et produire de l'intrication). Dans les ordinateurs quantiques, l'information ne bouge pas et reste dans des qubits. Les portes quantiques agissent de manière programmatique sur ces qubits. En fin de calcul, on évalue la valeur des qubits qui n'ont pas bougé physiquement pour lire le résultat.
- Il existe de nombreuses méthodes de création de qubits issues d'entreprises privées (Google, IBM, Intel, Microsoft), de startups (D-Wave, Rigetti) et de laboratoires (dont le CEA). Ils sont à base de supraconducteurs à effet Josephson, d'ions piégés, de phase de photons, de spins d'électrons, de fermions de Majorana ou de cavités dans des diamants dopés à l'azote. Quels sont les avantages et inconvénients de ces voies techniques très différentes ?

- Ces différentes approches sont nécessaires. Il est possible que seule l'une d'entre elle porte ses fruits. On ne sait pas prédire laquelle à ce stade.

L'ordinateur quantique

- Nous verrons dans le détail comment est organisé un ordinateur quantique avec ses qubits, ses registres, ses portes et ses outils de mesure.
- Le fonctionnement des ordinateurs quantiques à grande échelle n'est pas encore possible ni assuré mais les progrès sont cependant rapides et suivent pour l'instant l'équivalent de la loi de Moore.
- La majeure partie des ordinateurs quantiques actuels doivent être réfrigérés à 10-20 mK, proche du zéro absolu, ce qui n'est pas évident sur de gros volumes. Certains laboratoires travaillent sur des qubits fonctionnant à température ambiante.
- Nous décrirons ce problème du bruit qui affecte les qubits et comment il peut être évité ou donner lieu à des corrections, que l'on appelle les QEC (Quantum Error Corrections).
- La communauté scientifique n'est pas en phase sur l'éventualité de créer des ordinateurs quantiques avec un grand nombre de qubits. Certains pensent que c'est impossible, d'autres que cela prendra plusieurs décennies, et quelques-uns, que l'on y arrivera dans moins de 10 ans.
- Avec les techniques actuelles, un ordinateur quantique tient dans quelques mètres-cubes et consomme environ 15 KW, ce qui est très raisonnable compte-tenu de la puissance de calcul fournie. C'est un outil destiné aux centres de calcul, exploitable à distance dans le cloud.

Algorithmes et applications quantiques

- Les ordinateurs quantiques exploitent des algorithmes quantiques qui servent à résoudre des problèmes de calculs complexes bien plus rapidement qu'avec des supercalculateurs. Ces algorithmes sont très différents de ceux de l'informatique traditionnelle. De tels algorithmes quantiques sont régulièrement inventés depuis le début des années 1990 après ceux de Deutsch-Jozsa, Grover et Shor. Mais il n'y en a pas tant que cela.
- Les grandes applications de l'informatique quantique portent sur la simulation de physique des matériaux, en biologie moléculaire, des optimisations complexes et aussi pour l'entraînement de réseaux de neurones ainsi que pour le machine learning.
- La suprématie quantique qualifie une situation future où des ordinateurs quantiques permettront de réaliser des calculs inaccessibles aux supercalculateurs actuels et pour certaines applications et algorithmes spécifiques. Elle n'arrivera donc pas d'un seul coup et sera progressive, application par application et ordinateur quantique par ordinateur quantique.

- Nous évoquerons aussi les questions des théories de la complexité des problèmes et les limitations des ordinateurs quantiques.
- Nous examinerons l'offre d'outils de développement en distinguant ceux qui sont issus de laboratoires de recherche de ceux qui proviennent de sociétés privées.
- Nous ferons un tour des applications potentielles de l'informatique quantique dans différents secteurs d'activité comme les transports, la santé, l'énergie, la finance et le marketing.

Panorama des acteurs

- Nous ferons le tour des principaux acteurs industriels de l'informatique quantique, par type de qubits avec notamment D-Wave, IBM, Google, Rigetti, IonQ, Intel, Microsoft, Nokia et QDTI. Avec leurs technologies, le point où ils en sont et leurs premières études de cas lorsqu'elles existent.
- Ces acteurs se préparent déjà en créant des outils de développement adaptés à l'exploitation de l'informatique quantique avant même que l'on soit assuré du caractère opérationnel des ordinateurs quantiques. C'est un beau cas d'école de l'innovation où nombre d'acteurs publics et privés avancent de concert dans un environnement très incertain.

Les startups de l'informatique quantique

- De nombreuses startups, surtout anglo-saxonnes, prennent déjà leur position sur un marché qui est à peine existant. Notamment, dans la partie logicielle et au-dessus des seuls ordinateurs quantiques disponibles, ceux de D-Wave.
- C'est une étude de cas "in vivo" d'écosystème en cours de constitution, très en avance de phase par rapport à l'émergence du marché correspondant.

La cryptographie quantique et la cryptographie post-quantique

- C'est le marché le plus mûr de l'informatique quantique. Il est la conséquence directe des menaces que font peser à long terme les ordinateurs quantiques sur la cryptographie à clés publiques.
- Le marché comprend deux composantes : la cryptographie quantique qui permet de transporter des clés de sécurité sans qu'elles soient violables pendant leur transport, et la cryptographie post-quantique qui permet de se prémunir des capacités de déchiffrement que l'algorithme de Shor donnera aux possesseurs d'ordinateurs quantiques.
- De manière plus large, la cryptographie quantique fait partie du domaine plus large des télécommunications quantiques, utilisable notamment pour relier des ordinateurs quantiques entre eux.

Métrologie quantique

- Quelles sont les applications quantiques dans les outils de mesure de précision : du temps, des fréquences de la lumière, de la gravité et du magnétisme ? Cette partie est un ajout de l'édition de septembre 2019.

Stratégies industrielles

- Les pays les plus actifs dans l'informatique quantique sont les USA, la Chine, le Canada, UK, l'Australie, l'Autriche, la Suisse, les Pays-Bas et l'Australie. A part le cas particulier d'Atos que nous décrirons, la France semble peu active du point de vue industriel et devra rapidement rattraper le coup. Sa recherche est cependant au niveau du côté des couches physiques, notamment dans les qubits à supraconducteurs.

Fumisteries quantiques

- Un petit détour par la médecine quantique avec quelques-uns de ses fondamentaux scientifiques qui méritent le détour à bas niveau puis les approche à haut niveau qui relèvent dans l'ensemble de la charlatanerie.
- D'autres fumisteries quantiques diverses détectées dans l'industrie comme le management quantique et le marketing quantique.

Société

- Quels sont les questions éthiques et philosophiques soulevées par l'informatique quantique ?
- Les biais et l'explicabilité des algorithmes à l'heure de l'informatique quantique, les grandes différences avec ces mêmes questions lorsqu'elles sont appliquées au deep learning.
- Le jargon du quantique et ses dérives. La volonté de puissance sur les données, la nature et la compréhension du monde.
- Les enjeux en termes de formation.
- Le marketing de l'offre et ses exagérations.

Entreprises

- Proposition d'une simple démarche pour aborder la thématique de l'informatique quantique dans l'entreprise.

Ecosystème français

- Comment est structuré l'écosystème quantique en France ? Quelle stratégie pour la France et les entreprises françaises dans ce monde scientifique encore très incertain ? Peut-on créer une stratégie européenne ?
- Tour d'horizon de l'écosystème quantique français dans la recherche, les startups, les investisseurs, les entreprises utilisatrices, les conférences et les associations.

Glossaire

- Un glossaire introduit dans la version de 2019 qui décrit les termes techniques employés dans l'ebook. Un bon moyen de vérifier ses connaissances sur le sujet. Ne serait-ce que pour l'auteur !

Pourquoi l'informatique quantique ?

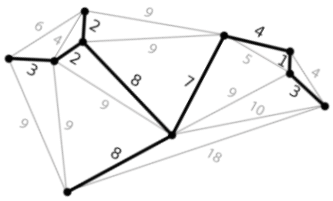
L'une des motivations de l'informatique quantique est de pouvoir résoudre des problèmes que les ordinateurs traditionnels ne savent pas et ne sauront peut-être jamais traiter. Il s'agit des problèmes de nature exponentielle, dont la complexité augmente exponentiellement avec la quantité des données à traiter.

Le schéma *ci-dessous* présente quelques exemples de problèmes complexes de nature exponentielle.

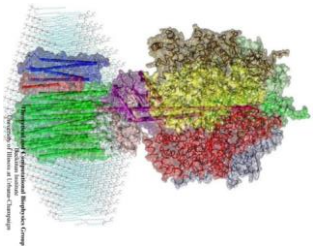
Cela commence avec divers problèmes d'optimisation comme celui du parcours du livreur ou de véhicules autonomes dans le trafic. Lorsque la combinatoire à optimiser est très grande, les algorithmes classiques trouvent leurs limites sur les ordinateurs traditionnels.

Cela se complique avec l'optimisation du trafic de parcs de véhicules autonomes de villes intelligentes du futur. Aujourd'hui, on optimise son trajet avec Google Maps ou Waze en s'appuyant sur l'état du trafic. Celui-ci est variable et la durée du trajet finale n'est pas toujours optimale et ne correspond pas forcément à la durée prévue.

C'est un système hautement indéterministe. Avec une flotte intégralement autonome, on devrait pouvoir théoriquement optimiser le trajet individuel de chaque véhicule en fonction de leur lieu de départ et de destination. Les algorithmes classiques pourraient fonctionner avec une quantité limitée de véhicules mais au-delà de quelques milliers, les capacités de calcul traditionnelles seraient largement saturées. Le quantique arriverait alors à la rescousse !

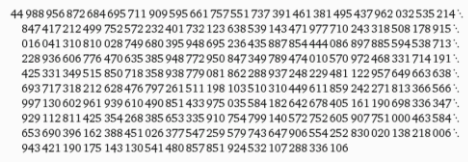


optimisations combinatoires
trajets, placements, cartes, finance



simulations moléculaires
matériaux et biologie

intelligence artificielle
machine learning et deep learning



factorisation
de très grands nombres entiers

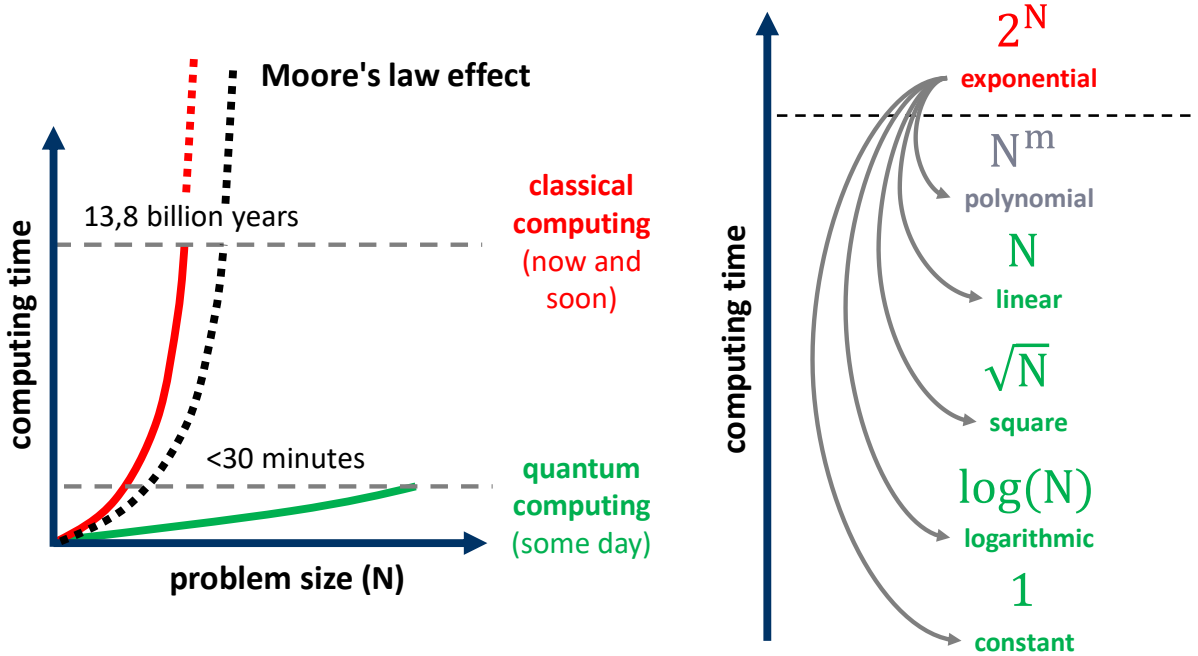
L'entraînement de réseaux de neurones est un second domaine d'application. Il est aujourd'hui à la portée des ordinateurs classiques, équipés de GPU comme ceux de Nvidia ou les processeurs neuromorphiques qui mettent en œuvre dans le silicium des portes logiques dont l'organisation est très proche de la logique des réseaux de neurones.

Mais aujourd'hui, la puissance de calcul disponible rend difficile l'entraînement de réseaux de grande taille. Pour ne prendre que l'exemple des réseaux convolutifs de reconnaissance d'images, ceux-ci ont une résolution d'image en entrée généralement limitée à 227x227 pixels.

En troisième lieu intervient la simulation du fonctionnement de la matière au niveau atomique. Elle est régie par les règles de la mécanique quantique qui dépendent d'équations connues mais dont la combinatoire est un problème d'optimisation complexe à résoudre, particulièrement pour comprendre l'interaction de nombreux atomes dans des molécules ou des structures cristallines complexes. Cela concerne aussi bien la simulation chimique que celle du vivant. L'informatique quantique pourrait ainsi servir à simuler le quantique du monde réel dans l'infiniment petit. Rassurez-vous, cela n'ira pas au point de simuler un être vivant en entier. Cela sera déjà une prouesse fantastique que de le faire un niveau du repliement d'une seule protéine sur elle-même !

Enfin, nous pouvons citer la factorisation de nombres entier qui intéresse notamment la NSA et les services de renseignement pour casser les codes de sécurité sur Internet de type RSA qui reposent sur l'envoi de clés publiques. Nous aurons l'occasion de creuser cela en détails.

D'autres applications pourront émerger pour différents marchés comme la finance ou l'assurance. Nombre d'applications métiers sont concernées par les problèmes d'optimisation complexes et restent à inventer, notamment à destination du grand public.



Pour mieux comprendre l'intérêt de l'informatique quantique, voici une mise en abyme du temps de calcul comparé de problèmes très complexes.

Dans les cas extrêmes, les temps de calcul sur ordinateurs classiques, même avec les plus puissants des supercalculateurs du moment, dépasseraient l'âge de l'Univers, soit 13,85 milliards d'années sachant que la Terre restera encore vivable dans le meilleur des cas pendant seulement 2 milliards d'années, modulo les effets à court terme – à l'échelle cosmique - du réchauffement planétaire.

Comparativement, des ordinateurs quantiques pourraient en théorie résoudre ces mêmes problèmes dans un temps raisonnable à l'échelle d'une vie humaine, en heures, journées, semaines ou mois. Je raisonne au conditionnel car on n'est pas vraiment sûr d'y arriver.

Le principe du calcul quantique est de modifier l'échelle de temps de résolution d'un problème. Il permet en théorie pour un problème donné de modifier l'ordre de grandeur de son temps de résolution. Dans l'échelle *ci-dessus à droite*, on voit de tels ordres de grandeur. Les problèmes exponentiels sont dits « intractables » car leur temps de calcul évolue dans des proportions folles avec leur taille.

Les autres temps de calcul, polynomiaux, linéaires, racinaires ou logarithmiques, évoluent beaucoup moins vite avec N. En théorie, le quantique permet de passer d'un niveau de cette échelle à un niveau plus bas. Il est utile lorsque N est grand.

Les barrières technologiques si ce n'est scientifiques à franchir sont cependant encore immenses avant d'y parvenir.

L'informatique quantique n'est pas juste là pour aller plus vite que l'informatique traditionnelle dans son champ opératoire actuel. Elle sert à résoudre des problèmes inaccessibles aux ordinateurs classiques, même en s'appuyant sur un éventuel mouvement perpétuel de la loi de Moore, qui, on le sait, n'est pas du tout assuré.

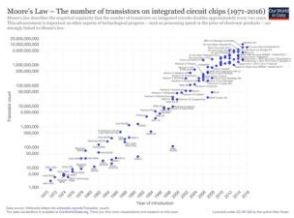
On pourrait ainsi affirmer que le potentiel de disruption de l'informatique quantique est "multi-mooresque".

dessin de François Cointe, publié avec son autorisation, source : https://www.lemagit.fr/dessin/Google-presente-son-ordinateur-quantique

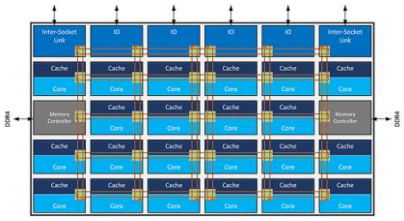
Comment augmente-t-on actuellement la puissance des ordinateurs classique ? On s'appuie sur quelques techniques connues, certaines n'ayant pas encore été explorées à fond. Nous avons l'augmentation de la densité des processeurs en transistors qui permet d'aligner plus de fonctions dans un processeur mais sans forcément en augmentant sa rapidité.

Nous créons des architectures multicœurs qui permettent de paralléliser les traitements pour peu que les logiciels associés le permettent.

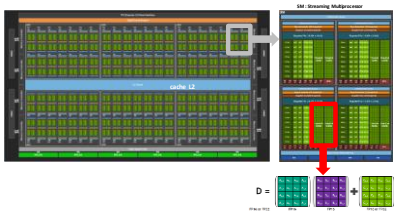
L'accélération de traitements peut provenir de processeurs utilisant des tenseurs (multiplicateurs de matrices) ou des processeurs neuromorphiques (imitant le fonctionnement des neurones biologiques, avec une mémoire intégrée comme avec les memristors). Le tout étant intéressant pour l'entraînement et l'inférence des réseaux de neurones du deep learning utilisés notamment dans la reconnaissance d'images et celle du langage.



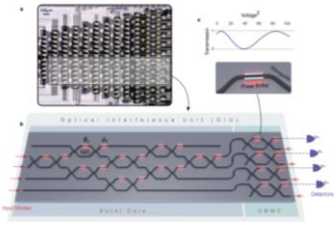
densité transistors



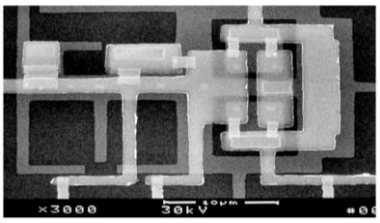
multicoeurs



neuromorphique et memristors



optronique

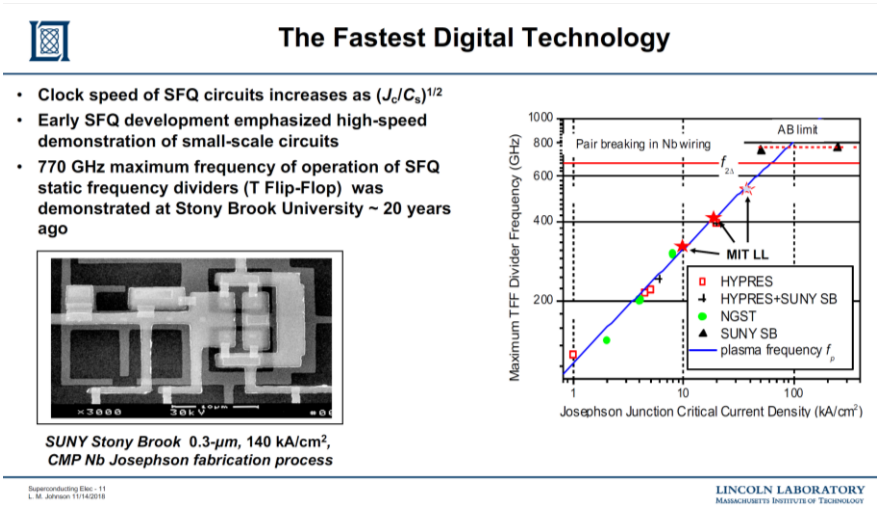


transistors supraconducteurs

Nous pouvons passer par l'optronique en remplaçant les électrons par des photons pour faire circuler l'information. Cela permettrait en théorie de créer des processeurs allant 20 à 25 fois plus vite que les processeurs CMOS actuels et d'atteindre 100 GHz. Mais ces processeurs sont difficiles à mettre au point et à intégrer, il est presque impossible de créer des équivalents des transistors avec des photons et les matériaux utilisés étant différents de ceux des processeurs CMOS. On passerait ainsi du silicium au cadmium, à l'indium, au gallium et autres métaux plutôt rares.

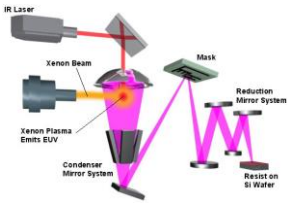
Une autre piste consisterait à créer des transistors fonctionnant à des températures supraconductrices, de l'ordre de 4K.

Des composants utilisant des transistors à effet Jospheson fonctionnant à 770 GHz ont même été expérimentés à la fin des années 1990 !



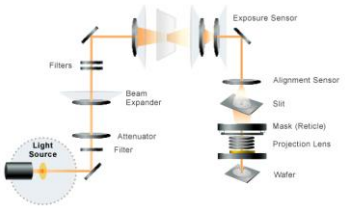
Ces composants pourraient équiper des supercalculateurs moins voraces en énergie[8]. Pour aller de l'avant, il faut trouver le moyen de développer des technologies clés et de contourner des limitations physiques connues.

La barrière de la chaleur limite l'augmentation de la vitesse d'horloge des processeurs. Elle plafonne de manière courante à 4 GHz dans les processeurs Intel du marché et peut monter à 6 GHz avec des refroidissements de compétition[9].

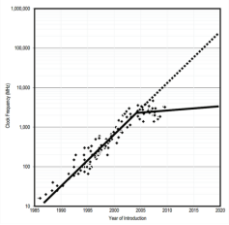


Extreme Ultra Violet (EUV)
difficile à mettre au point <= 10 nm

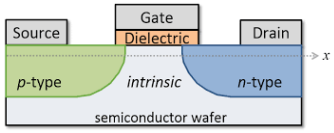
limites techniques du CMOS



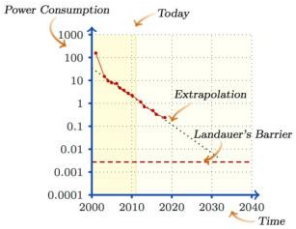
taille maximale des réticules
limite haute de la taille des chipsets



barrière de la chaleur
limite la fréquence des processeurs



effets quantiques indésirables vers 5 nm
diélectrique
= 6 atomes d'épaisseur



barrière de Landauer
limite basse de consommation

Pour créer des transistors avec une intégration en-dessous de 10 nm, il faut faire appel à des systèmes de gravure utilisant l'extrême ultra-violet. En effet, leur résolution dépend de la longueur d'onde de la lumière utilisée pour projeter un masque sur une résine photosensible.

Pour diminuer la taille des transistors, il faut augmenter cette fréquence pour diminuer la longueur d'onde, et donc passer de l'ultra-violet actuel à l'extrême ultra-violet.

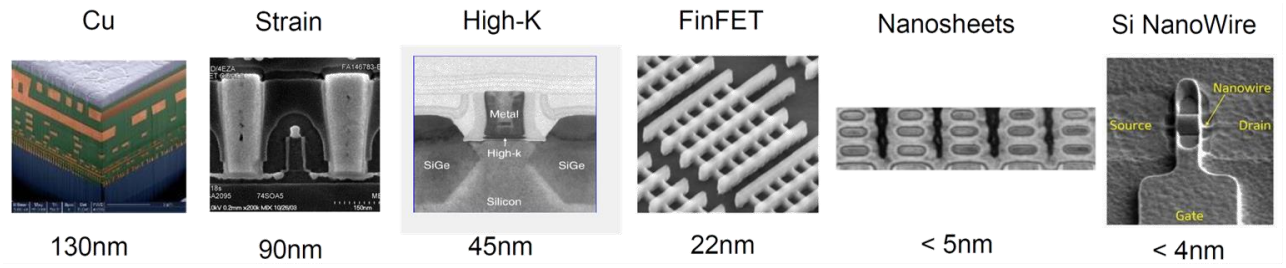
Cela fait presque 10 ans que ces machines de gravure EUV sont mises au point, et de manière très laborieuse. Qui plus est, lorsque l'on miniaturise les transistors en deçà de 5 nm, on voit apparaître des effets quantiques indésirables. Ce qui n'empêche toutefois pas les roadmaps de Samsung et TSMC de prévoir d'atteindre les 3 nm d'ici 2025, grâce notamment à la technique des nanowires et des nanosheets[10].

---

[8] Voir cette très intéressante présentation sur les composants supraconducteurs : Superconducting Microelectronics for Next-Generation Computing de Leonard Johnson, novembre 2018 (27 slides). Le gain en consommation d'énergie serait compris entre 10 et 1000. Le niveau d'intégration est pour l'instant faible, de l'ordre de 200 nm à comparer à 7 nm pour les processeurs les plus denses en CMOS. Mais il progresse régulièrement. Il existe même des pistes pour combiner transistors supraconucteurs, optoélectronique t réseaux de neurones. Voir Superconducting Optoelectronic Loop Neurons de Amir Jafari-Salim, 2018 (48 pages).

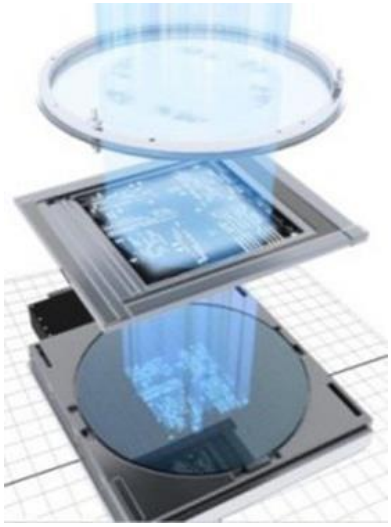
[9] Voir à ce sujet Minimum Energy of Computing, Fundamental Considerations par Victor Zhirnov, Ralph Cavin et Luca Gammaitoni, 2014 (40 pages) qui compare au passage l'efficacité énergétique du vivant et de l'électronique.

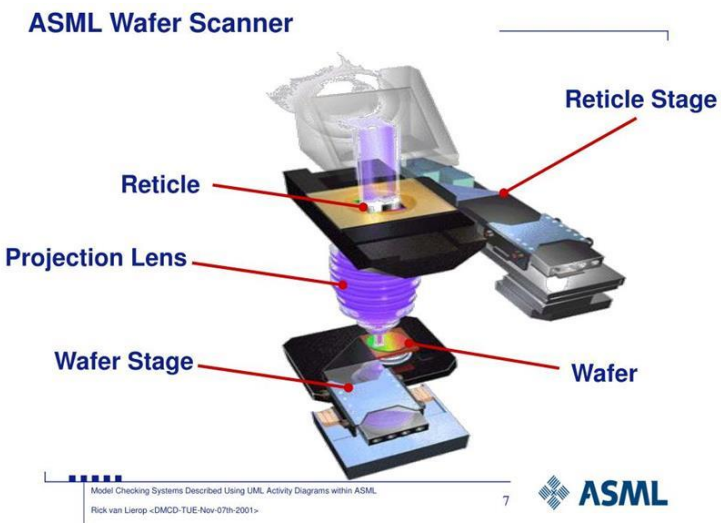
[10] Voir Beyond CMOS, Superconductors, Spintronics, and More than Moore Enablers de Jamil Kawa, Synopsys, mars 2019 (43 slides), une bonne presentation qui décrit les différentes pistes d'amélioration de la puissance des composants dont les Cold CMOS, les semiconducteurs fonctionnant à une température voisine de l'azote liquide (-70°C) dans compter les transistors supraconducteurs à effet Josephson. Le schéma de la page suivante en est issu.



Deux autres limites sont à prendre en compte comme la barrière de **Rolf Landauer** (chercheur chez IBM, en 1961) qui indique le minimum d'énergie nécessaire pour modifier une information. C'est une barrière théorique contestée par certains physiciens.

Enfin, il existe une limite de taille des réticules, ces systèmes optiques de gravure de processeurs dont la taille est physiquement limitée. Les illustrations ci-dessous issues d'ASML, le leader mondial de la lithogravure de semiconducteurs, permettent de comprendre cela.





Le plus gros processeur actuel, le **Nvidia** V100 avec ses 21 milliards de transistors, atteint déjà cette limite de taille. Son successeur doublera probablement son nombre de transistors grâce au passage à une intégration en 7 nm, qui n'est pas encore annoncée mais ne saurait trop tarder.

L'informatique quantique permettra de passer outre les diverses limitations des processeurs CMOS actuels pour certaines tâches. Elle ne les remplacera toutefois pas du tout pour les tâches actuellement accomplies par les ordinateurs et mobiles actuels.

Comme ses usages ne seront pas les mêmes, il est difficile d'anticiper le paysage informatique qui germera. Les prévisions de Ray Kurzweil sur la singularité qui s'appuient fortement sur la prolongation ad-vitam de la loi de Moore mériteront en tout cas d'être révisées !

Scientifiques

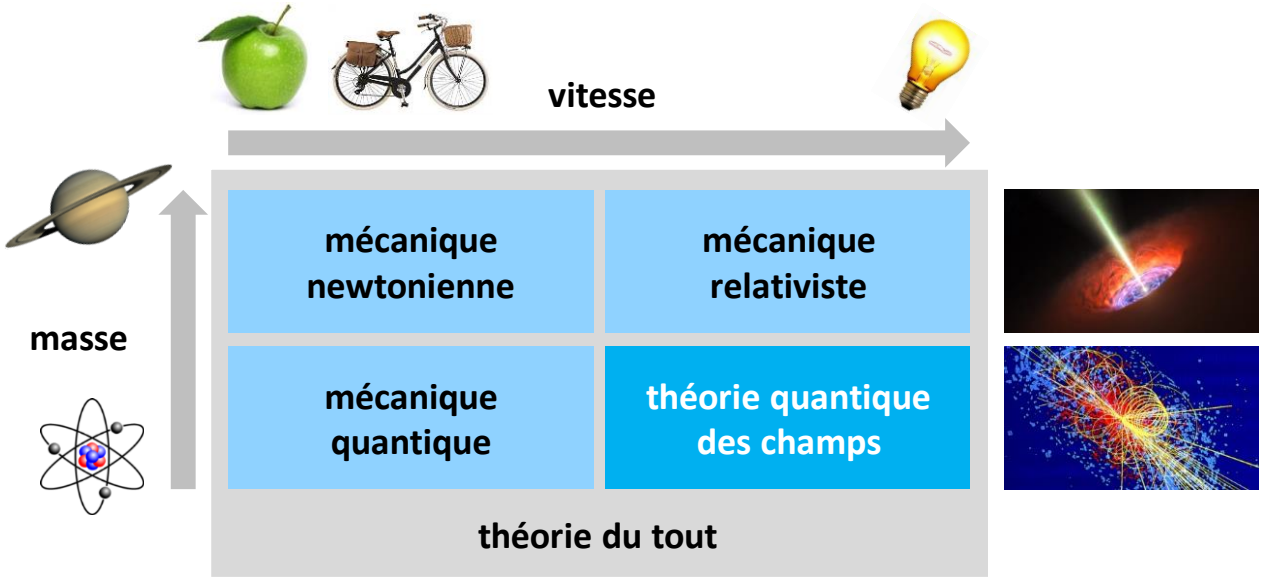
Après avoir posé le décor et le sommaire de cet ebook sur l'informatique quantique, nous allons faire un petit retour en arrière pour découvrir la riche histoire de cette discipline.

Chaque épopée scientifique et technologique est avant tout une grande Histoire humaine. Celles de la mécanique quantique et de l'informatique quantique n'y échappent pas. Je vais ici rendre hommage aux scientifiques qui ont rendu tout cela possible et continuent encore de plancher dessus pour ceux qui sont encore de ce monde.

La physique ou mécanique quantique s'intéresse à l'infiniment petit et à ses différences par rapport à la mécanique classique, souvent dite newtonienne, qui régit de manière prédictible le fonctionnement des objets de taille raisonnable, au-delà de quelques microns jusqu'à la taille des planètes et des étoiles. La mécanique quantique s'intéresse particulièrement aux interactions entre la lumière et la matière.

La mécanique classique est régie par les lois de Newton avec les équations du mouvement de la matière, par les lois de Maxwell qui décrivent les champs électromagnétiques et les forces associées et par la physique statistique qui comprend la thermodynamique, et décrit les milieux continus comme les gaz et les fluides.

Dans l'infiniment grand, on fait appel à la théorie de la relativité et à son lien avec la gravitation qui explique la courbure de l'espace-temps. Elle est indispensable pour interpréter les phénomènes extrêmes que sont les trous noirs ou les étoiles à neutrons. Elle permet d'interpréter l'Histoire de l'Univers, mais pas entièrement.



S'y ajoute enfin la théorie quantique des champs qui décrit les phénomènes qui se produisent avec les particules élémentaires circulant à très haute vitesse, comme celles que l'on observe dans les accélérateurs de particule avec les quarks ou les bosons de Higgs[11].

Le physicien Richard Feynman est l'un des pères de l'électrodynamique quantique qui est un sous-ensemble de la théorie quantique des champs.

La physique n'est toujours pas complète ni totalement unifiée. Certains phénomènes physiques observables lui résistent encore. On ne sait pas expliquer précisément l'origine précise de la gravitation et on cherche toujours la matière et l'énergie noires qui expliqueraient la cohésion des galaxies. L'Homme aimerait bien tout savoir et tout expliquer mais il est fort probable que cette quête sera toujours en devenir, ne serait-ce que sur la forme qu'avait l'Univers avant le big bang.

La théorie du tout recherchée par nombre de physicien serait un formalisme permettant d'unifier l'ensemble des théories de la physique et en particulier la théorie de la relativité et la mécanique quantique et leurs formalismes mathématiques différents. C'est un champ très sérieux, mais en devenir, de la physique[12].

Vous pouvez passer cette partie et aller directement à la suivante si l'Histoire des sciences ne vous intéresse pas. Cette partie sert surtout de référence pour bien mémoriser qui est qui dans l'Histoire de la mécanique et de l'informatique quantiques.

Scientifiques de la mécanique quantique

Un topo sur l'informatique quantique démarre immanquablement par un "101" de la mécanique quantique. Il requiert de couvrir quelques basiques, même s'ils sont parfois abstraits. Mon objectif sera de raccommoder les morceaux avec le fonctionnement pratique des ordinateurs quantiques. Comprendre la mécanique et l'informatique quantique relève de l'assemblage d'un vaste puzzle. On ajoute les pièces une par une. Le puzzle n'est jamais complet. Au bout d'un certain temps, on y voit une image qui permet d'avoir une vue d'ensemble sans forcément que le puzzle soit terminé. C'est ce qui vous arrivera probablement au terme de la lecture de ces articles.

La physique quantique est une science qui a pris forme aux débuts du XXe siècle. Malgré ses enrichissements constants, elle a fait preuve d'une étonnante solidité pour résister à l'épreuve du temps. Comme presque toutes les sciences, elle résulte des travaux de très nombreux scientifiques et chercheurs et d'allers et retours entre expérimentation, construction de théories descriptives et explicatives et de modèles mathématiques. La mécanique quantique reste cependant incomplète car elle n'explique pas au plus bas niveau ce qu'elle modélise mathématiquement, comme l'intrication.

---

[11] Voir ce cours de vulgarisation sur les particulers élémentaires, quark dans les neutrons et protons, Les particules élémentaires par Guillaume Lumin et Franck Stevens, 2012.

[12] Le physicien américano-japonais Michio Kaku estime que cette théorie du tout sera finalisée d'ici 2100. Voir Michio Kaku thinks we'll prove the theory of everything by 2100, avril 2019. On ne sera probablement pas là pour le verifier à ce moment-là ! Ce Michio Kaku n'est pas un marginal. Il est à l'origine de la théorie des cordes. Il définit très bien l'articulation entre les différentes branches de la physique et cette théorie du tout dans A theory of everything?.

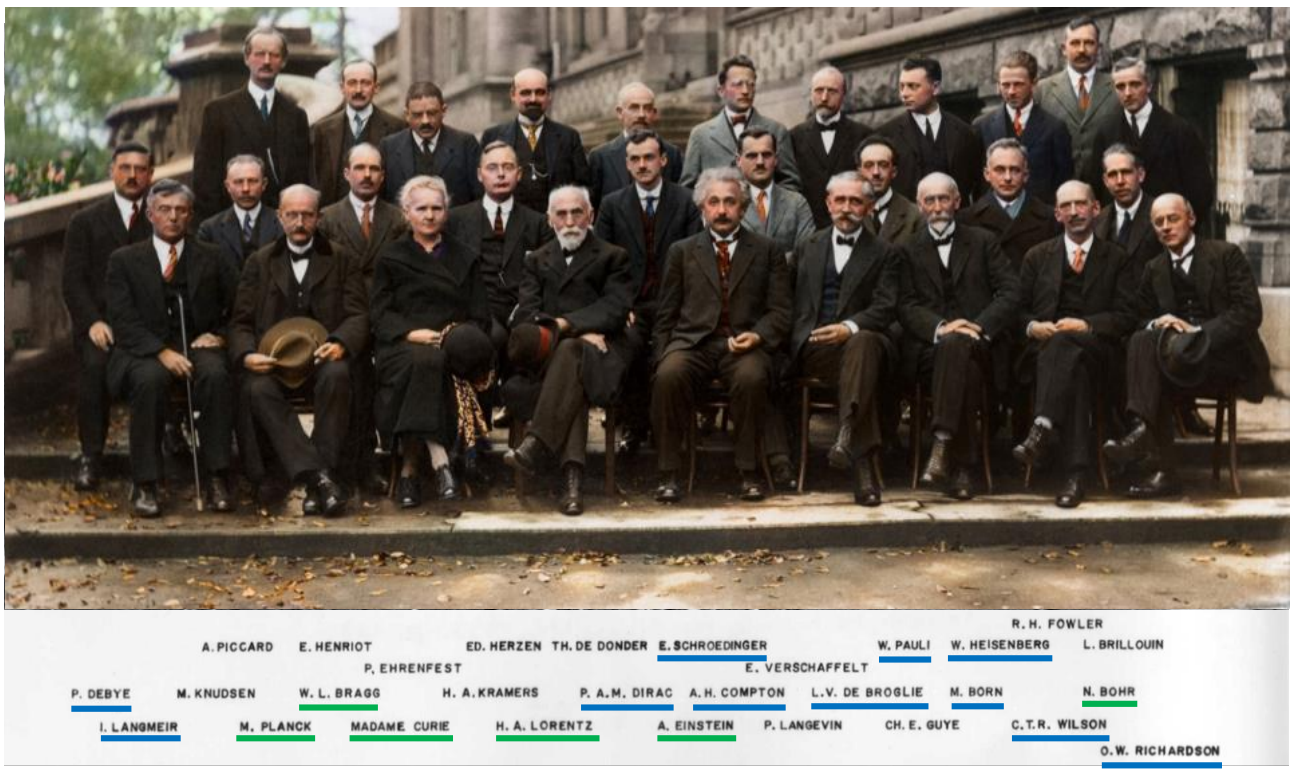
L'histoire des idées de la mécanique quantique est une aventure humaine qui a rassemblé des talents immenses qui se sont confrontés, qui ont fait évoluer pas à pas leur compréhension de l'infiniment petit. Régulièrement, de nouvelles générations de scientifiques ont remis en question l'état des lieux de leurs prédécesseurs. Dans la mécanique quantique comme dans une bonne part de l'histoire de la physique, cette compréhension a associé des physiciens et des mathématiciens. Les physiciens ont mené de nombreuses expériences pour identifier des paradoxes, des inconnues, bâtir des théories puis les vérifier par l'expérience, parfois avec plusieurs décennies de latence.

Les mathématiciens ont bâti des modèles de représentation des données, comme les matrices et l'algèbre linéaire, qui jouent un très grand rôle dans la mécanique quantique pour décrire les états des quantums et leur évolution dans l'espace et dans le temps. Cette algèbre linéaire est au cœur du fonctionnement des qubits des ordinateurs quantiques. Très souvent, les représentations mathématiques de la physique quantique dépassent les interprétations physiques.

Nombre de ces scientifiques ont laissé une trace mémorable connue des connaisseurs voire même du grand public avec le célébrissime chat de Schrödinger et le principe d'indétermination d'Heisenberg. Comme souvent, d'autres contributeurs moins connus ont aussi apporté leur pierre à l'édifice et il faut aussi leur rendre hommage.

Vous n'y trouverez pas d'inventeur à la Roland Moreno ou d'entrepreneurs sauce Steve Jobs ou Elon Musk, même si les fondateurs de startups telles que le Canadien D-Wave font partie des pionniers entrepreneurs de ce secteur d'activité naissant.

Ce côté collectif de la mécanique quantique est incarné par l'épisode mythique du cinquième **Congrès de Physique Solvay de 1927**, tenu à l'hôtel Métropole de Bruxelle. La photo associée qui immortalise l'épisode a été coloriée après coup.



Ce congrès rassemblait les plus grands mathématiciens et physiciens de l'époque dont presque tous les pères de la mécanique quantique avec Bohr, Schrödinger, Born, de Broglie, Heisenberg, Planck, Dirac et Einstein. 17 des 29 participants ont obtenu un Prix Nobel, dont 6 en étaient déjà détenteurs au moment de la réunion (noms soulignés en vert). C'était probablement l'un des plus gros concentrés de jus de cervelle au mètre carré de l'histoire de l'humanité !

Les congrès Solvay ont lieu tous les 3 à 4 ans. Ils sont thématisés. Celui de 1927 portait sur les électrons et les photons, qui sont au cœur de la mécanique quantique. Un congrès sur deux portait sur la mécanique quantique, le dernier du genre ayant eu lieu en 2011. La dernière édition, la 27ème, a eu lieu en 2017.

Voici donc quelques-uns de ces protagonistes et leurs grandes contributions associées avec au passage, des indications de qui a influencé qui, les contributions étant généralement organisées par ordre chronologique.

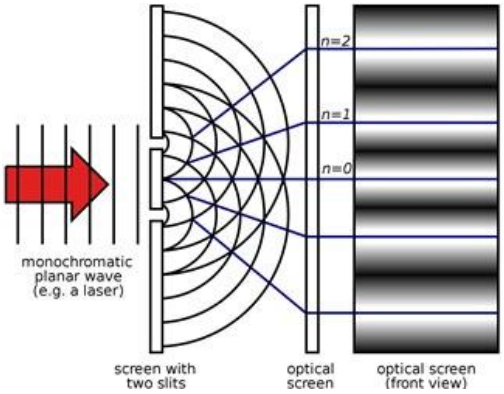
Précurseurs

Nous commençons avec les physiciens et mathématiciens qui ont posé des bases scientifiques qui ont permis à leurs successeurs du XXe siècle de formaliser les bases de la physique quantique. Notez que je n'indique pas toujours la source des schémas. Ils font partie d'explications scientifiques courantes qui font maintenant partie du domaine public.

C'est parti pour ce tour historique !

Thomas Young (1773-1829, Anglais) détermine la nature ondulatoire de la lumière. Il la prouve avec l'expérience des doubles fentes dites de Young vers 1806, illustrée *ci-dessous*. Elle génère des interférences qui créent une illumination alternant lumière et absence de lumière liée à la nature ondulatoire de la lumière.

Ce grand spécialiste de l'optique a aussi travaillé sur les principes de la réfraction et de la vision trichromatique. Thomas Young était aussi égyptologue et avait étudié la fameuse pierre de Rosette. Son expérience a été ensuite rééditée avec des électrons, en 1927, avec un résultat voisin, illustrant la dualité onde-particule de l'électron, résultat des travaux du Français Louis de Broglie en 1924.



William Rowan Hamilton (1805-1865, Irlandais) est un mathématicien et astronome. Vers 1827, il invente de nouvelles formulations mathématiques des lois de la physique qui intègrent l'électromagnétisme. En mécanique quantique, on parle souvent d'Hamiltonien ou de fonction hamiltonienne.

Il s'agit d'équations servant à décrire l'énergie totale et potentielle d'un système de particules élémentaires (détails). L'équation de Schrödinger créée en 1926 décrit l'évolution dans le temps d'un hamiltonien. Ce concept est notamment utilisé dans les ordinateurs quantiques à recuit quantique de D-Wave que nous aurons l'occasion de décrire dans le détail dans cet ebook.

Niels Henrik Abel (1802-1829, Norvégien) est un mathématicien à l'origine de ce que l'on appelle les groupes abéliens. Ses travaux portent sur la semi-convergence des séries numériques, des suites et séries de fonctions, les critères de convergence d'intégrale généralisée, sur la notion d'intégrale elliptique et sur la résolution d'équations algébriques.

Il est mort à 26 ans de la tuberculose ! C'est bien dommage pour un tel génie ! Avec Hamilton et Hermite, c'est l'un des fournisseurs des fondements mathématiques utilisés dans la mécanique quantique. L'appellation "abéliens" et "non abéliens" est associée aux anyons, les quasi-particules qui sont la base de l'informatique quantique topologique. Pourquoi ces concepts de mécanique quantiques inventés bien avant sa mort font-ils référence à ce mathématicien ? Notamment parce que la distinction entre abéliens et non abéliens est lié à leur représentation mathématique commutative (= "abélien", quand A*B = B*A) ou non commutative ("non abélien", lorsque A*B n'est pas égal à B*A) ! Les opérations non commutatives les plus courantes sont les multiplications de matrices. Ainsi la multiplication d'une matrice (p x q) x (q x p) donnera une matrice (p x p) alors que dans l'autre sens, (q x p) x (p x q) générera une matrice (q x q), q et p étant ici des nombres de lignes et/ou colonnes.

La non commutativité est souvent rencontrée dans le calcul quantique. Ainsi, l'ordre dans lequel on mesure l'état des qubits influe sur les résultats. C'est même une technique à part entière qui est exploitée dans le Measurement Based Quantum Computing (MBQC) que nous aurons l'occasion de décrire.

Charles Hermite (1822-1901, Français) est un mathématicien très prolixe, qui a fait avancer la théorie des nombres, les formes quadratiques, la théorie des invariants, les polynômes orthogonaux, les fonctions elliptiques et l'algèbre. Ses principaux travaux sont concentrés sur la période 1848-1860.

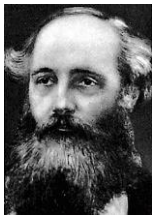
On lui doit la notion d'hermitiens, une notation mathématique utilisée en mécanique quantique et l'explication va s'arrêter là car après, c'est bien trop compliqué. Les matrices hermitiennes sont des matrices composées de nombres réels dans la diagonale et pouvant être complexes dans le reste, et qui sont égales à leur transconjuguée. A savoir, leur transposée dont on a inversé la valeur des nombres complexes (i devient -i).

Voir l'exemple *ci-contre*. Les matrices décrivant les opérations des portes quantiques dans les ordinateurs quantiques sont des matrices hermitiennes.

$$A = \begin{pmatrix} 3 & i & -5i \\ -i & -2 & 5 \\ 5i & 5 & 10 \end{pmatrix}$$ est une matrice hermitienne :

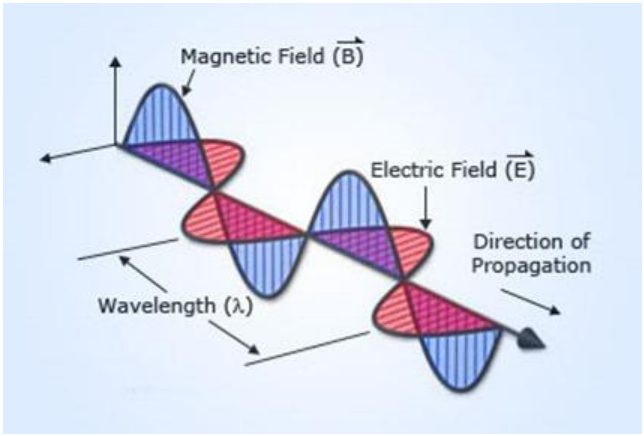
$$\overline{A} = \begin{pmatrix} 3 & -i & 5i \\ i & -2 & 5 \\ -5i & 5 & 10 \end{pmatrix} \text{ et } (\overline{A})^T = \begin{pmatrix} 3 & i & -5i \\ -i & -2 & 5 \\ 5i & 5 & 10 \end{pmatrix} = A$$

Elles ne changent pas la longueur des vecteurs qui sont transformés par ces matrices.



James Clerck Maxwell (1831-1879, Ecossais) est le créateur en 1865 de la théorie des champs électromagnétiques, associant un champ électrique et un champ magnétique orthogonaux comme dans le schéma *ci-dessous*, se déplaçant à la vitesse de la lumière. Cette théorie explique les interactions entre lumière et lumière comme la réflexion, la diffraction, la réfraction et les phénomènes d'interférences.

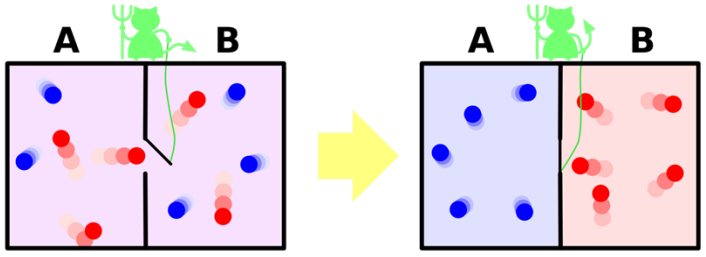
On lui doit la création de pistes de création de la photographie en couleur s'appuyant sur les trois couleurs primaires de la vision humaine. Sa description des ondes électromagnétiques va avoir un impact phénoménal dans les télécommunications électromagnétiques et dans l'optronique. Cela servira de fondements à la mécanique quantique élaborée par Max Planck en 1900.



Il est aussi à l'origine de la loi statistique de distribution des gaz Maxwell–Boltzmann.

Il est aussi le concepteur en 1867 de l'expérience de pensée dite du « **démon de Maxwell** » qui rendrait possible la réversibilité de processus d'échanges thermodynamiques et invaliderait le second principe de la thermodynamique[13]. Elle repose sur deux boîtes contenant deux gaz différents ou un gaz à deux températures différentes séparées par un trou et une obturation contrôlée par un « démon ». Lorque l'on ouvre la porte, les gaz se mélangent.

Une fois mélangé (*à gauche dans le schéma ci-contre provenant de Wikipedia*), le démon contrôlerait celles des molécules pouvant aller d'une boîte à l'autre, tirant parti de l'énergie cinétique naturelle des gaz.



Cela permettrait en théorie et au bout d'un certain temps de revenir à l'équilibre antérieur dans une situation de non équilibre (*à droite*).

Il a fallut attendre plusieurs décennies pour trouver la faille, notamment via Léo Szilard en 1929 et Léon Brillouin en 1948. Au départ, l'explication était que le démon a besoin de dépenser de l'énergie pour obtenir de l'information sur l'état des molécules de gaz pour les trier. Il y a donc consommation d'énergie pour modifier l'équilibre stable obtenu pour mélanger les gaz. L'explication « à jour » est quelque peu différente. Le coût énergétique provient de la remise à zéro de la mémoire du démon, qui consiste ultimement en un seul bit d'information[14].

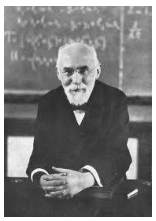
Tout ceci a eu des retombées sur la notion de valeur énergétique de l'information et conduit, bien plus tard, à la création du champ de la thermodynamique de l'information, c'est-à-dire de l'étude des empreintes énergétiques et entropiques de l'information, notamment en calcul quantique. Ce champ a ensuite été investi par Rolf Landauer, connu pour son étude de la génération de chaleur des circuits de gestion de l'information irréversibles et par Charles Bennett et Gilles Brassard, les coinventeurs du protocole BB84 dont nous reparlerons.

Ludwig Boltzmann (1844-1906, Autrichien) est un physicien, père de la physique statistique, défenseur de l'existence des atomes et créateur d'équations décrivant la dynamique des fluides et des gaz en 1872. Il est aussi à l'origine du second principe de la thermodynamique. Dépressif, il est mort en se suicidant !

---

[13] Voir l'explication du démon de Maxwell dans Démon de Maxwell, FuturaScience.

[14] Voici l'explication détaillée par Alexia Auffèves (CNRS) : on peut comprendre l'opération de reset d'un bit de mémoire en considérant un moteur de Carnot ultime, constitué d'une seule particule qui peut se trouver à gauche ou à droite d'un certain volume thermostaté. Gauche = 0, Droite = 1. Il y a deux opérations possibles : la compression. La particule se trouve initialement à gauche ou à droite du volume qui la contient (on ne sait pas) et on comprime ledit volume pour qu'à la fin elle se trouve nécessairement à gauche. C'est une opération d'initialisation où le bit est remis dans l'état 0. Comme pour toute compression, il faut payer, ici dans ce cas ultime, le travail à dépenser est kT log 2. C'est le fameux travail de Landauer, qui pose une borne énergétique à toutes les opérations logiquement irréversibles. La seconde opération est la détente. Au début, on sait que la particule se trouve à gauche ou à droite. On positionne une paroi, une poulie avec une masse au bout et on laisse la détente s'opérer tout en extrayant un travail élémentaire équivalent à kT log 2. C'est une machine de Szilard. Ces deux manipulations ont été réalisées expérimentalement en 2011. Elles montrent l'empreinte énergétique de l'information et constituent la solution ultime au paradoxe du démon de Maxwell.



Henri Poincaré (1854-1912, Français) est un mathématicien et physicien, précurseur de la théorie de la relativité et des ondes gravitationnelles. On lui doit une fonction probabiliste qui porte son nom et qui est l'équivalent en optique de la représentation de Bloch que nous verrons plus tard qui décrit mathématiquement l'état des qubits.

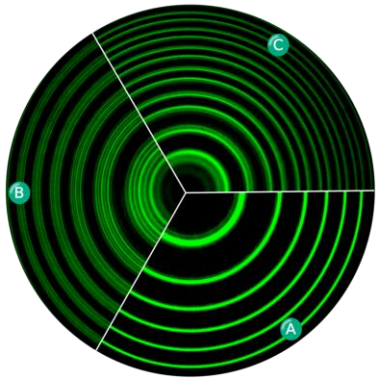
Il est aussi l'auteur de la conjecture qui porte son nom et qui a été démontrée en 2003 par le Russe Grigori Perlman. Elle est relative à l'existence de sphères dans des espaces quadri-dimentionnels. C'était un cousin germain de Raymond Poincaré, président de la République Française pendant la première guerre mondiale.

David Hilbert (1862-1943, Allemand) est un mathématicien prolifique à qui l'on doit à la fin du 19e siècle les fondamentaux mathématiques de la mécanique quantique, et notamment ses espaces dits de Hilbert utilisant des vecteurs permettant de mesurer des longueurs, des angles et de définir des orthogonalités.

On les utilise pour représenter l'état des qubits avec des vecteurs ou nombres complexes. Ses travaux n'avaient cependant rien à voir à l'origine avec la mécanique quantique qui n'était alors pas encore formulée.

Pieter Zeeman (1865-1943, Hollandais) est un physicien, prix Nobel de physique en 1902 avec Hendrik Lorentz pour la découverte de l'effet qui porte son nom entre 1896 et 1897. L'effet Zeeman se manifeste lorsqu'une source de lumière traverse un champ électromagnétique et voit ses raies spectrales séparées en plusieurs raies. L'effet s'observe par une spectroscopie qui décompose les rayons lumineux avec un prisme.

Les raies spectrales se décomposent en un nombre pair (effet Zeeman normal) ou impair de raies (effet anormal). La décomposition dépend de l'intensité du champ magnétique traversé.

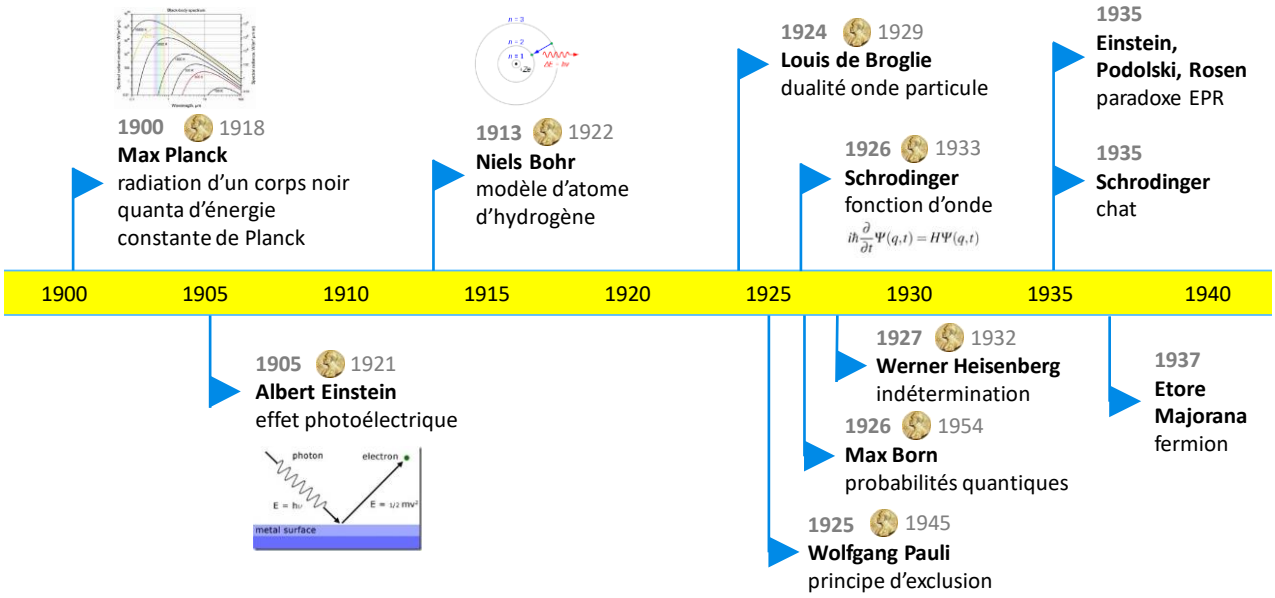


Elle s'accompagne d'une polarisation de la lumière générée dont la nature et l'intensité dépendent de l'orientation du champ magnétique relativement au faisceau de lumière comme le montre l'illustration Wikipedia *ci-contre*. En astronomie, la mesure de l'effet Zeeman permet d'en déduire les champs magnétiques intenses dans les étoiles ainsi que dans la Voie Lactée. Elle est aussi exploitée dans les spectroscopies de résonance magnétique (nucléaire et électronique) dans les scanners IRM.

Fondateurs

La mécanique quantique a vu le jour avec Max Planck, puis a pris forme sur trois décennies et demies, en gros jusqu'en 1935 avec les contributions successives d'Einstein, Bohr, De Broglie, Born, Schrödinger et Heisenberg pour ne prendre que les plus connues.

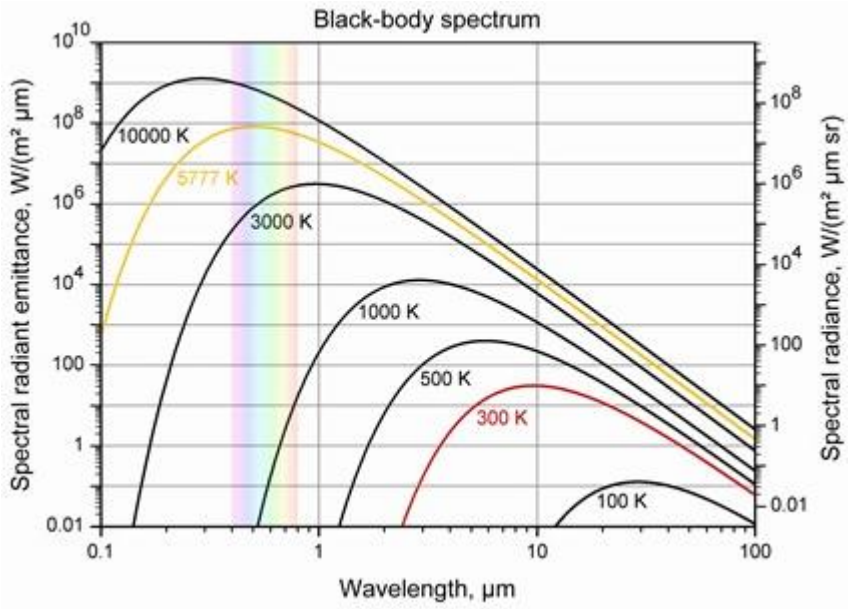
Voici donc un tour des grands physiciens et mathématiciens qui ont établi les bases de la physique quantique. Ce sont tous des européens qui vont pour une bonne part s'expatrier aux USA avant la seconde guerre mondiale[15].



Max Planck (1858-1947, Allemand) est un physicien, initialement spécialisé dans la thermodynamique. En 1900, il imagine la théorie des quantas, émettant l'hypothèse que le rayonnement de la matière n'est pas continu mais varie par seuils, par paliers d'une certaine quantité d'énergie, d'où le terme de "quanta" et de "physique quantique".

Sa théorie lui permet d'expliquer pour la première fois l'énigmatique rayonnement du corps noir, un corps qui absorbe tout rayonnement magnétique incident.

Les exemples de corps noir sont une cavité fermée comme un four, un métal chauffé qui devient rouge, orangé, puis blanc en fonction de la température, ou une étoile comme le Soleil. Le spectre d'ondes électromagnétiques émis par un corps noir dépend uniquement de sa température selon le schéma *ci-contre* et pas du tout de sa matière.



[15] Le déroulé de cette histoire est bien raconté, formules mathématiques à l'appui par Didier Robert de l'Université de Nantes dans Des mathématiques dans la mécanique quantiques, 2014 (86 slides).

Plus la température est élevée, plus le spectre électromagnétique émis par le corps noir glisse vers les fréquences élevées, donc vers le violet et l'ultra-violet avec le niveau de la température.

Max Planck élabore une formule décrivant le spectre électromagnétique du corps noir qui est rapidement vérifiées par l'expérience. Il devient prix Nobel de physique en 1918. Max Planck est ainsi l'un des premiers à formuler les bases de la mécanique quantique[16].

On lui doit également la constante qui porte son nom et qui est exploitée dans son explication du rayonnement d'un corps noir. Cette constante fut ensuite utilisée dans l'équation selon laquelle l'énergie du changement d'état d'un atome égale la fréquence du rayonnement multipliée par la constante de Planck.

Lorsqu'un électron change d'orbite dans un atome d'hydrogène, cela émet ou absorbe une onde électromagnétique dont l'énergie est égale à la constante de Planck multipliée par la fréquence lumineuse émise. Bien qu'Albert Einstein, Niels Bohr et d'autres réalisèrent quelques années plus tard des vérifications physiques de la théorique quantique, Planck exprima jusqu'à sa mort des doutes sur les principes de la mécanique quantique !

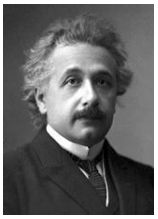
Planck est aussi à l'origine de deux constantes : le temps ou bien durée de Planck qui est $t_P=10^{-44}$s et la longueur de Planck qui est $l_P=1{,}616255*10^{-35}$m. Elles sont reliées entre elles par les équations *ci-dessous*. Le temps de Planck est celui qui serait nécessaire à un photon pour parcourir la distance de Planck.

En gros, ce sont les dimensions de l'infiniment petit en-dessous desquelles toute observation est impossible avec les connaissances actuelles de la physique. l_P étant tellement petit, un photon pour l'observer aurait une énergie tellement élevée qu'il créeait un trou noir autour de lui et serait donc inobservable !

$$t_\mathrm{P} = \sqrt{\frac{hG}{2\pi c^5}} = \sqrt{\frac{\hbar G}{c^5}} = \frac{\ell_\mathrm{P}}{c}$$

$$\ell_P = \sqrt{\frac{\hbar G}{c^3}}$$

$\hbar$ est la constante de Planck réduite ;
G est la constante gravitationnelle ;
c est la vitesse de la lumière dans le vide ;
ℓ_P est la longueur de Planck.

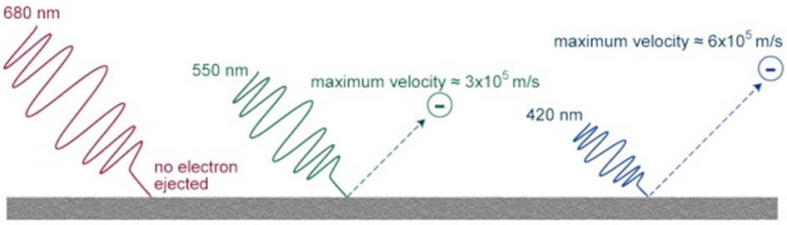


Albert Einstein (1879-1955, Allemand puis Américain) est un physicien que l'on ne présente plus, prix Nobel en 1921 pour son interprétation de l'effet photoélectrique en 1905, qui est devenue l'un des fondements de la mécanique quantique après Planck et avant De Broglie, Heisenberg et Schrödinger.

[16] Etienne Klein raconte bien le cheminement intellectuel de Max Planck dans la vidéo "La naissance de la physique quantique" (2016).

Dans On a Heuristic Viewpoint Concerning the Production and Transformation of Light, il détermine que les quantas de Planck sont des photons, des quantités discrètes d'énergie lumineuse, dont l'énergie est égale à la fréquence électromagnétique des ondes transportées multipliée par la constante de Planck.

L'effet photoélectrique est aussi à l'origine du solaire photovoltaïque et des principes de la photosynthèse dans les plantes, qui permet la production de glucose.



Il correspond à la capacité d'un photon à déloger un électron d'une orbite généralement intérieure d'un atome et de créer du courant électrique[17].

L'interprétation d'Einstein s'appuyait sur les travaux antérieurs de **Heinrich Hertz** (1857-1894, Allemand) qui découvrit en 1887 que la lumière peut arracher un électron à du métal et de **Philipp Lenard** (1862-1947, Allemand) qui étudia en 1902 l'effet photoélectrique et détermina qu'il ne se déclenche qu'à partir d'une certaine fréquence de la lumière projetée. Ce dernier obtint le prix Nobel de physique en 1905. Devenu fervent Nazi et opposé à Einstein par rivalité scientifique puis par antisémitisme virulent, il est passé dans les oubliettes de l'Histoire.

Bien entendu, Einstein est aussi à l'origine de la théorie de la relativité restreinte et générale qui couvre l'infiniment grand alors que la mécanique quantique touche l'infiniment petit. Aussi curieux que cela puisse paraître, Einstein n'a jamais obtenu le prix Nobel pour ses travaux sur la relativité malgré son impact considérable sur la physique et l'astronomie.

En 1925, Einstein prédit un comportement particulier de la matière, le condensat de Bose-Einstein qui se manifeste lorsque l'on refroidit des gaz à très basse température. Les atomes se trouvent alors dans un état quantique d'énergie minimale présentant des propriétés physiques particulières. C'est le cas de l'hélium superfluide, découvert en 1938, et qui, à très basse température, n'a plus de viscosité, à savoir qu'il peut se déplacer sans dissiper d'énergie.

Bose est le nom du chercheur indien **Satyendranath Bose** (1894-1974) avec qui Einstein avait travaillé pendant les années 1920 et à qui l'ont doit les "bosons", qui vérifient les caractéristiques des condensats de Bose-Einstein.

[17] Les couches d'électrons des atomes sont numérotés 1 à N, leur nombre quantique. On démarre aussi la numérotation par K (première couche proche du noyau avec un maximum de 2 électrons) puis L (8 électrons au maximum), M (avec un maximum de 18 électrons mais en pratique 8), etc. L'effet photoélectrique concerne essentiellement les couches K et L. L'électron éjecté est ensuite remplacé par un électron d'orbite extérieure, ce qui génère un nouveau photon, dans les rayons X ou en fluorescence, selon l'énergie du photon incident. Cela émet alors un photon de rayon X du fait du différentiel d'énergie entre couches électroniques ou bien un électron dit « Auger » du nom de Pierre Auger. Ce phénomène a été découvert autour de 1923 par ce dernier et par Lise Meitner. Une autre variante de l'effet photoélectrique est l'effet Compton, lorsque l'énergie élevée d'un photon incident dans les rayons gamma va dégager un électron de la couche de valence et générer un autre photon. Enfin, lorsque l'énergie du photon incident est encore plus élevée, l'interaction a lieu au niveau du noyau de l'atome visé et génère un électron et un positron.

Cela comprend les particules élémentaires sans masse telles que les photons mais aussi certains atomes comme le deutérium ou l'Helium 4 ainsi que certaines quasi-particules comme les paires d'électrons supraconducteurs que sont les paires de Cooper.

Einstein est aussi à l'origine de l'expérience de pensée dite du **paradoxe EPR**, ou Einstein Podolski Rosen, en 1935 portant sur la non localité des quantums et sur l'incomplétude de la mécanique quantique de l'époque[18].

Le débat portait sur le fait que la mécanique quantique ne semblait pas décrire complètement le monde physique, la fonction d'onde de Schrödinger étant insuffisante pour décrire la réalité physique des quantums.

Einstein proposait l'introduction de variables cachées locales expliquant le phénomène de l'intrication quantique.

Il pensait qu'une réalité physique devait exister indépendamment des observations, que le hasard pur n'existait pas et que Dieu ne jouait pas aux dés.


The New York Times.

NEW YORK, SATURDAY, MAY 4, 1935. TWO CENTS

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

La réflexion a été poursuivie dans les années 1960 par l'Américain John Stewart Bell avec ses "inégalités". L'expérience d'Alain Aspect en 1982 a démontré qu'il n'y avait pas de variables cachées et donc, a pu, de ce fait invalider l'hypothèse des variables cachées d'Einstein. Chapeau bas !

Comble de l'Histoire, Einstein n'a pas réussi avant sa mort à parfaire sa théorie de la relativité générale qui était aussi incomplète que ne l'était pour lui la mécanique quantique. Il voulait notamment réconcilier la mécanique quantique et la gravité.

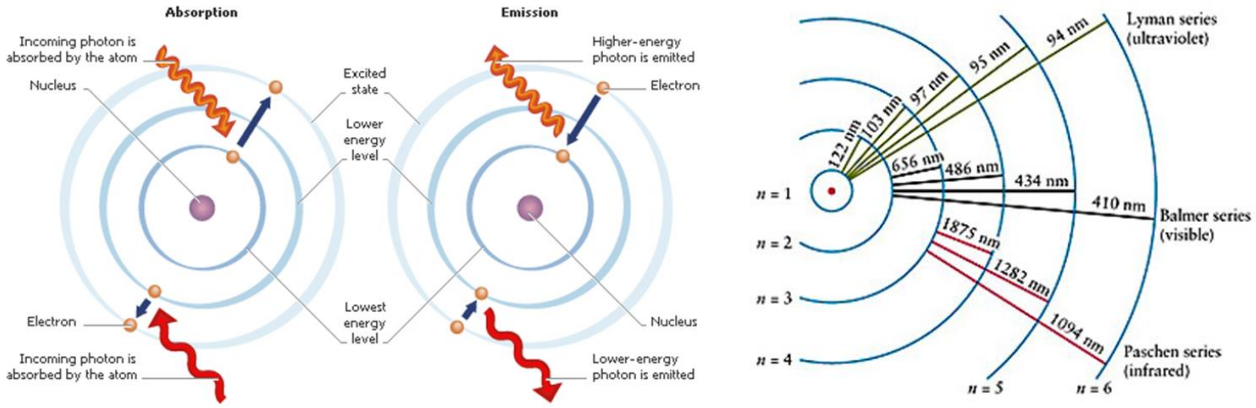
Attention cependant aux images d'Epinal ! Il se dit et s'écrit bien trop souvent qu'Einstein était « contre » la mécanique quantique ou n'y croyait pas. Ce n'est pas tout à fait cela puisqu'il en était à l'origine avec Max Planck. Il la trouvait en fait incomplète pour expliquer l'intrication ! Cette incomplétude subsiste plus de 80 ans après, car on n'explique toujours pas l'intrication. On se contente de la décrire.

Niels Bohr (1885-1962, Danois) est un physicien, prix Nobel en 1922, à l'origine de la création en 1913 d'un modèle descriptif de l'atome d'hydrogène avec son noyau fait d'un proton et un électron tournant autour du noyau sur des orbites précises correspondant à un niveau d'énergie cinétique des électrons multiple de h/2π, h étant la constante de Planck et n = 1, 2, 3, etc.

[18] Voir Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, 1935.

Ce modèle permettait d'expliquer les raies spectrales observées dans l'analyse de l'énergie de l'hydrogène dans les expériences de **Johann Balmer** (1825-1898) de 1885, de **Theodore Lyman** (1874-1954) de 1906 et de **Friedrich Paschen** (1865-1947) en 1908.

Niels Bohr s'appuie principalement sur les travaux de l'Anglais **Ernest Rutherford** (1871-1937) qui découvrit en 1911 la structure des atomes avec leur noyau chargé positivement, grâce à ses protons, et leurs électrons tournant autour du noyau.



Les électrons avaient été découverts par l'Anglais **Joseph John Thomson** (1856-1940) en 1897, ce qui lui permit d'obtenir le Prix Nobel de Physique en 1906.

Ernest Rutherford avait imaginé l'existence des neutrons qui ne fut vérifiée expérimentalement qu'en 1932 par l'Anglais **James Chadwick** (1891-1974). **Marie Curie** (1867-1934) avait bien découvert le polonium et le radium en 1898 et certains effets de la radioactivité mais pas celle des neutrons.

Selon Bohr, les électrons émettent ou absorbent un photon lorsqu'ils changent d'orbite. Il est donc aussi l'un des fondateurs de la mécanique quantique, complétant les travaux de Planck et Einstein. Il a longtemps débattu sur le sujet, notamment avec Albert Einstein à partir du Congrès de Solvay de 1927.

Par la suite, les travaux de Louis de Broglie sur la dualité ondes-particules démontraient que les orbites des électrons étaient un multiple entier de leur longueur d'onde associée.

Avec Werner Heisenberg, Pascual Jordan et Max Born, Niels Bohr est à l'origine de l'interprétation dite de **Copenhague** de la physique quantique qui s'appuie sur trois principes clés[19] :

- La description d'une onde-particule est réalisée par sa fonction d'onde, et aucune autre information "cachée" ne peut servir à décrire son état.

[19] Voir aussi Seven ways to skin Schrödinger's cat de Richard Webb, 2016 qui décrit les différentes écoles de pensée de la physique quantique. Voir aussi les autres interprétations de la physique quantique dans The Biggest Myth In Quantum Physics Starts With A Bang d'Ethan Siegel, dans Forbes, 2018, d'où est issu le schéma *ci-dessus*.

- Lorsqu'une mesure de l'état d'un quantum est réalisée, sa fonction d'onde composite de plusieurs états est réduite à la fonction d'onde de l'un des états possibles du quantum. C'est l'effondrement de la fonction d'onde.
- Lorsque deux propriétés sont reliées par une relation d'incertitude, on ne peut pas mesurer les deux propriétés avec une précision supérieure à ce que permet la relation d'incertitude (principe d'Heisenberg). Qui plus est, lorsque l'on mesure la position d'une particule, on affecte son mouvement, et réciproquement.

Interpretation	Author(s)	Deterministic?	Wavefunction real?	Unique history?	Hidden variables?	Collapsing wavefunctions?	Observer role?	Local?	Counterfactual definiteness?	Universal wavefunction exists?
Ensemble interpretation	Max Born, 1926	Agnostic	No	Yes	Agnostic	No	No	No	No	No
Copenhagen interpretation	Niels Bohr, Werner Heisenberg, 1927	No	No[1]	Yes	No	Yes[2]	Causal	No	No	No
de Broglie–Bohm theory	Louis de Broglie, 1927, David Bohm, 1952	Yes	Yes[3]	Yes[4]	Yes	Phenomenological	No	No[15]	Yes	Yes
Quantum logic	Garrett Birkhoff, 1936	Agnostic	Agnostic	Yes[5]	No	No	Interpretational[6]	Agnostic	No	No
Time-symmetric theories	Satosi Watanabe, 1955	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes
Many-worlds interpretation	Hugh Everett, 1957	Yes	Yes	No	No	No	No	Yes	Ill-posed	Yes
Consciousness causes collapse	Eugene Wigner, 1961	No	Yes	Yes	No	Yes	Causal	No	No	Yes
Stochastic interpretation	Edward Nelson, 1966	No	No	Yes	Yes[14]	No	No	No	Yes[14]	No
Many-minds interpretation	H. Dieter Zeh, 1970	Yes	Yes	No	No	No	Interpretational[7]	Yes	Ill-posed	Yes
Consistent histories	Robert B. Griffiths, 1984	No	No	No	No	No	No	Yes	No	Yes
Transactional interpretation	John G. Cramer, 1986	No	Yes	Yes	No	Yes[8]	No	No[12]	Yes	No
Objective collapse theories	Ghirardi–Rimini–Weber, 1986, Penrose interpretation, 1989	No	Yes	Yes	No	Yes	No	No	No	No
Relational interpretation	Carlo Rovelli, 1994	Agnostic	No	Agnostic[9]	No	Yes[10]	Intrinsic[11]	Yes[53]	No	No
QBism	Christopher Fuchs, Ruediger Schack, 2010	No	No[16]	Agnostic[17]	No	Yes[18]	Intrinsic[19]	Yes	No	No

A noter que le fils de Niels Bohr, Aage Niels Bohr, fut prix Nobel de physique en 1975 pour ses travaux portant sur la structure du noyau des atomes[20] !

Emmy Noether (1882-1935, Allemande) est la créatrice du theorème qui porte son nom en 1915 à l'Université de Göttingen en Allemagne[21]. A l'origine du champ de l'algèbre abstraite, c'est le fondateur de la mécanique Lagrangienne, précurseur de la théorie d'Hamilton. A cette époque, elle ne pouvait pas enseigner à l'Université car ce rôle était interdit aux femmes.

Son théorème n'a été publié qu'en 1918 et ne pu officiellement enseigner qu'à partir de 1919. Elle ne reçut ainsi un salaire de l'Université qu'à partir de 1923. Son théorème, difficile à vulgariser, relie les príncipes de conservation et les symétries. C'est l'un des fondements de la physique des particules.

$$\frac{d}{dt}\left(\sum_a \frac{\delta L}{\delta \frac{dq_a}{dt}} \delta q_a\right) = 0$$

Ses travaux ont notamment aidé Albert Einstein à peaufiner les bases de la théorie de la relativité générale qu'il avait élaborée en 1915[22]. Ce dernier l'admirait particulièrement. De confession juive comme lui, elle dû s'expatrier aux USA en 1933 où elle ne vécu que deux ans. Elle est décédée relativement jeune, à 53 ans.

[20] Voir Quantum Model of the Atom de Helen Klus, 2017.

[21] Voir In her short life, mathematician Emmy Noether changed the face of physics Noether linked two important concepts in physics: conservation laws and symmetries, par Emily Conover, 2018.

[22] Voir Women in Science: How Emmy Noether rescued relativity, par Robert Lea, février 2019.

Jacques Salomon Hadamard (1865-1963, Français) est un mathématicien qui a donné son nom à la porte de Hadamard utilisée dans les ordinateurs et algorithmes quantiques. Il avait notamment travaillé sur les nombres complexes, la géométrie différentielle et les équations aux dérivées partielles, en particulier pendant les années 1920.

On lui doit notamment les transformées qui portent son nom, des opérations matricielles carrées de 2 puissance n valeurs complexes ou entières de côté. Elles s'apparentent à des transformées de Fourrier discrètes. La porte de Hadamard utilisée en calcul quantique sert à crée une superposition de 0 et de 1 avec une transformée de Hadamard H1. Nous la verrons plus tard lorsque nous décrirons l'architecture d'un ordinateur quantique à portes universelles.

$$H_0 = 1$$

$$H_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

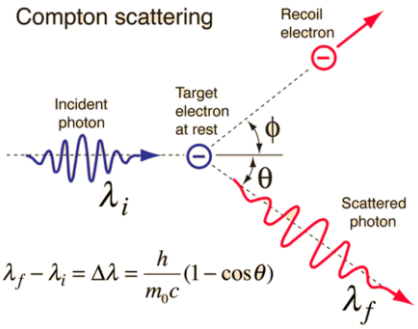
$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_3 = \frac{1}{2^{3/2}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Arthur Holly Compton (1892-1962, Américain) est un physicien prix Nobel de physique de 1927 pour la découverte en 1922 de l'effet qui porte son nom et qui démontre l'aspect corpusculaire des photons, dans une expérience faisant interagir un photon avec un électron libre autour d'un atome, validant les théories de Planck et Einstein.

L'effet Compton est une variante de l'effet photoélectrique qui s'applique à la réception d'un photon de rayon X ou Gamma qui a une énergie supérieure à celle de l'électron éjecté. L'effet est utilisé dans les radios à rayons X.

Le photon X est ralenti et dévié avec une énergie inférieure et devient un photon diffusé. On appelle aussi cela un choc élastique. Les rayons X sont émis lors de transitions électroniques entre les couches atomiques K, L et M (les premières autour du noyau de l'atome). Les angles d'émission de l'électron éjecté et du photon réémis dépendent du niveau d'énergie du photon incident.

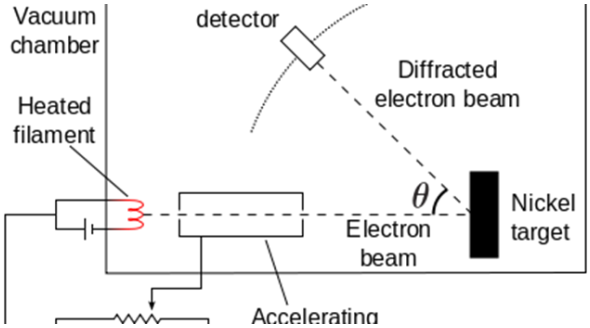


Louis de Broglie (1892-1987, Français) est un mathématicien et physicien à qui l'on doit, en 1924, l'extension du dualisme ondes corpuscules aux électrons, atomes, protons et neutrons en plus du photon. Cela lui valut le prix Nobel de physique en 1929. C'est le principal contributeur Français à la mécanique quantique d'entre deux-guerres.

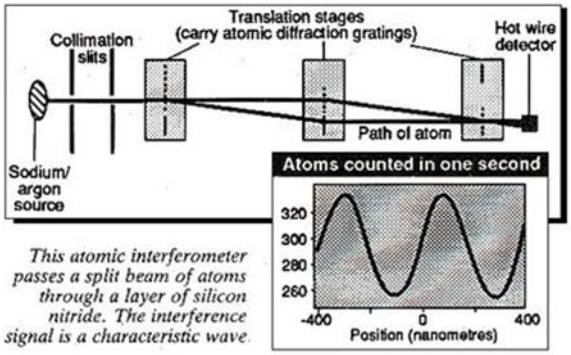
Selon ce principe, les particules élémentaires peuvent présenter des propriétés de corpuscule (avec une position, une trajectoire et éventuellement une masse) et d'ondes (délocalisée, se diffuse dans toutes les directions, génère des interférences) selon les circonstances.

C'est le cas des électrons qui ont une masse et peuvent interférer les uns avec les autres, des atomes ainsi que des photons. Louis de Broglie exprimait cette dualité avec une équation : $\lambda p=h$, où λ est une longueur d'onde, p une quantité de mouvement et h est la constante de Planck.

La dualité ondes-particules fut confirmée en 1927 pour ce qui concerne les électrons, par les équipes de l'Ecossais **George Paget Thomson** (1892-1975) de l'Université d'Aberdeen et de **Clinton Davisson** (1881-1958) et **Lester Germer** (1896-1971) des Bell Labs aux USA (*ci-contre*), qui ont partagé en 1937 un prix Nobel de physique pour ces expériences.

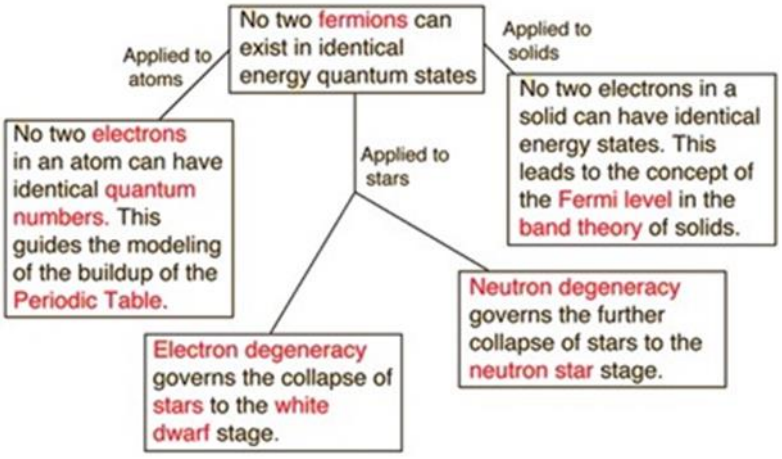


La confirmation de la dualité onde-particule a été ensuite vérifiée pour les neutrons en 1988, par Roland Gähler et Anton Zeilinger (source) et pour des atomes en 1991 par Olivier Carnal et Jürgen Mlynek (source du schéma *ci-contre*) ! Elle est même vérifiable avec des molécules de plusieurs atomes.



Wolfgang Pauli (1900-1958, Autrichien) est à l'origine du principe d'exclusion qui porte son nom élaboré en 1925 et selon lequel deux électrons ne peuvent pas avoir le même état quantique dans un atome, de la découverte du spin de noyau et d'électron et enfin, de la découverte du neutrino.

Il obtient le prix Nobel de physique en 1945. Le spin d'électron est décrit comme un sens de polarisation magnétique ou comme une rotation angulaire de l'électron dans un sens ou l'autre, mais ce n'est qu'une image et pas une représentation physique. Ce spin est utilisé dans des qubits dits CMOS dont nous reparlerons.



Erwin Schrödinger (1887-1961, Allemand) est un physicien, prix Nobel en 1933 pour sa fonction d'ondes, élaborée en 1926, ou équation de Schrödinger (*ci-dessous*), qui décrit l'évolution dans le temps et l'espace de l'état ondulatoire d'un quantum, à savoir les probabilités de trouver le quantum à un endroit donné et moment donné.

Il existe en fait deux principales équations de Schrödinger avec la plus simple, celle qui est dite indépendante du temps.

$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

Ψ(r,t) : fonction d'onde.
δ : dérivée première.
i : nombre complexe imaginaire dont le carré égal -1.
ħ : constante de Planck (h) divisée par 2π.

Et celle qui est dépendante du temps, avec un hamitonien H décomposé.

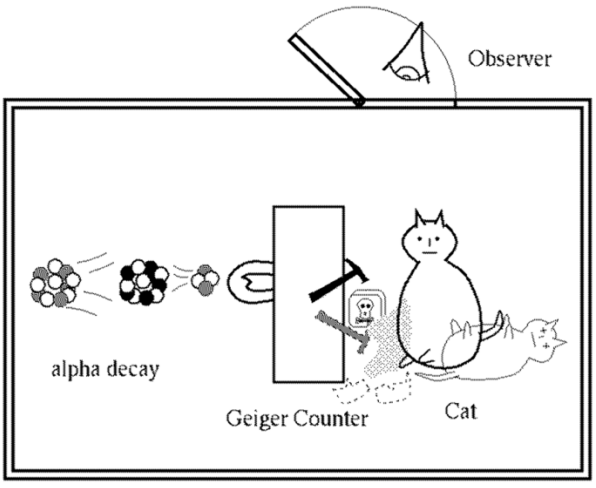
$$i\hbar\frac{\partial}{\partial t}\Psi(\vec{r},t) = \left[\frac{-\hbar^2}{2m}\nabla^2 + V(\vec{r},t)\right]\Psi(\vec{r},t)$$

m : masse de la particule.
V : énergie de la particule.
∇^2 : Laplacien qui décrit le mouvement de la particule dans l'espace.

Je vous passe les détails sur l'explication de cette équation différentielle ! Comment cette équation est-elle validée ? Elle l'est principalement de manière expérimentale[23]. Elle ne dérive pas d'autres lois de la physique. Le défi de cet ebook qui n'a pas la prétention d'être un livre de mécanique quantique est de vous faire comprendre les grands principes de l'informatique quantique sans avoir à vous plonger dans les arcanes et le formalisme mathématiques de la mécanique quantique.

On doit aussi à Erwin Schrödinger sa fameuse expérience de pensée quelque peu alambiquée visant à expliquer la notion d'états superposés avec son chat à la fois vivant et mort dans une boite.

On y a placé une fiole de poison dont l'ouverture est provoquée par la désintégration d'un atome radioactif de radium via un compteur Geiger détectant cette radiation ionisante. La radiation est faite de particules alpha, comprenant deux protons et deux neutrons. C'est l'équivalent d'un atome d'hélium 4 sans ses électrons. Comme le radium a une chance sur deux de se désintégrer après sa demi-vie, le chat a une chance sur deux d'être vivant et mort, tant que l'on n'ouvre pas la boîte.



[23] Voir la vidéo Quantique - D'où vient l'équation de Schrödinger?, de Benoît Hébert, professeur de physique en classes préparatoires. La démonstration n'est pas abordable au commun des mortels !

Lorsqu'on l'ouvre, il est vivant ou mort. Tant que la porte n'est pas ouverte, il est à la fois vivant et mort. Bon bon. Sauf que le chat peut mourir juste après l'ouverture de la boite si l'atome de radium se désintègre à ce moment là ! Et une fois que le chat est mort, il ne peut plus être vivant. Je me demande si Schrödinger n'a pas mélangé simultanéité et causalité dans son expérience de pensée qui parait bien trop compliquée !

Il a aussi négligé le fait qu'une fois que le chat est mort, il ne peut pas revivre. Sa superposition entre vivant et mort est donc impossible car la mort n'est pas réversible contrairement à la modification de l'état d'un quantum.

De plus, la notion de demi-vie d'un atome radio-actif ne relève pas de la superposition des états de quantas. Un atome radioactif est soit en un état désintégré, avec une certaine probabilité que cela intervienne liée à sa demi-vie, soit en état normal. La désintégration qui relève de la fission n'est pas un processus réversible ! Il n'y a donc pas de superposition quantique des états de l'atome de radium entre état d'origine et état désintégré ! Un atome de radium donné n'est jamais à la fois en état normal et en état désintégré. Si c'était le cas, le chat serait d'ailleurs presque immédiatement mort !

Pour que l'expérience du chat soit véritablement quantique, il faudrait éventuellement qu'elle s'appuie sur un atome de radium qui traverse un miroir semi-réfléchissant avec une chance sur deux de le traverser dans un cadre quantique[24], auquel cas on se rapprocherait d'une interprétation quantique.

Tout ça pour remettre en question l'interprétation de Copenhague de Niels Bohr et de ses compères ! En fait, il voulait mettre en évidence le fait que la superposition ne s'appliquait qu'à l'infiniment petit et pas aux objets macroscopiques. L'Histoire n'a retenu que le principe de superposition et pas cette différence entre le microscopique et le macroscopique.

Mais je ne vais pas me permettre de remettre en question un tel génie ! Oublions tout de même le chat et retenons la fonction d'onde de Schrödinger et la notion de superposition des états qui n'a de sens qu'à l'échelle microscopique ! Dans sa vie privée, Schrödinger était un grand coureur de jupons. Il était même capable de mener plusieurs liaisons en même temps, appliquant à sa vie privée le principe de la superposition quantique.

Max Born (1892-1970, Allemand) est un physicien et mathématicien à l'origine de la représentation mathématique des quantums sous forme matricielle. C'est à lui que l'on doit en 1926 l'explication statistique de la probabilité de trouver un électron dans un état énergétique donné à partir de sa fonction d'onde, élaborée par Schrödinger la même année.

On retrouve ce principe dans la sphère de Bloch, où la somme du carré des fonctions d'onde des niveaux des différents états d'un quantum est égale à 1. Sachant qu'alpha et beta sont en fait des nombres complexes.

[24] L'interprétation sur la désintégration se trouve dans la fiche Wikipedia du chat de Schrödinger, et celle du miroir dans Quantum Enigma de Bruce Rosenblum, Fred Kuttner.

Ce ne sont pas des nombres entiers ou flottants. Werner Heisenberg était son assistant ! Max Born a obtenu le prix Nobel de physique en 1954.

Werner Heisenberg (1901-1976, Allemand) est un physicien, prix Nobel en 1932 à qui l'on doit en 1927 le fameux principe d'incertitude, ou plutôt d'indétermination, selon lequel on ne peut pas mesurer avec précision à la fois la position et la vitesse d'une particule élémentaire.

Cette incertitude a été ensuite formulée mathématiquement en 1928 par Earle Hesse Kennard dans l'équation *ci-contre*, où le produit de l'écart type de la position et la vitesse est supérieur à la moitié de la constante de Planck.

$$\Delta\chi\Delta\rho \geq \frac{\hbar}{2}$$

Pour certains, ce principe d'incertitude serait une interprétation simplificatrice appliquée à une compréhension corpusculaire de la matière. Il mène à se poser la question de la position et de la vitesse d'un électron, alors qu'il n'aurait pas de position précise. Il n'y a pas là d'incertitude qui traduirait une méconnaissance de notre part. Nous tentons d'appliquer à l'électron des concepts de mécanique classique qui ne lui sont pas applicables. Ou tout du moins, qui ne sont pas observables de près.

En pratique, les particules quantiques ne sont pas des particules physiques classiques et on ne peut donc pas en mesurer aussi bien la vitesse que la position. On ne peut les décrire que par leur fonction d'onde (de Schrödinger). Plus généralement, Heisenberg énonce le principe selon lequel dans l'infiniment petit, la mesure influe sur la grandeur à mesurer. Le schéma *ci-contre*[25] illustre le phénomène avec recul.

Si vous éclairez un insecte avec la lumière du soleil et une loupe, vous risquez de le faire brûler ! C'est le même problème avec des différents systèmes d'imagerie médicale, comme ceux qui sont à base de rayons X.

On doit aussi à Heisenberg la formulation matricielle et en algèbre linéaire de la mécanique quantique. Elle conduit à représenter l'état d'un système quantique sous forme de vecteurs qui permettent au passage de représenter mathématiquement la superposition des états quantiques.

James Chardwick (1891-1974) est un physicien anglais à qui l'on doit la découverte des neutrons. Cette découverte est tardive par rapport à la mécanique quantique et à la découverte des électrons. La physique nucléaire a en effet progressé parallèlement à la physique quantique qui avait surtout trait aux interactions entre électrons et photons. Avant la découverte des neutrons, les scientifiques pensaient que le noyau des atomes comprenait des protons et des électrons.

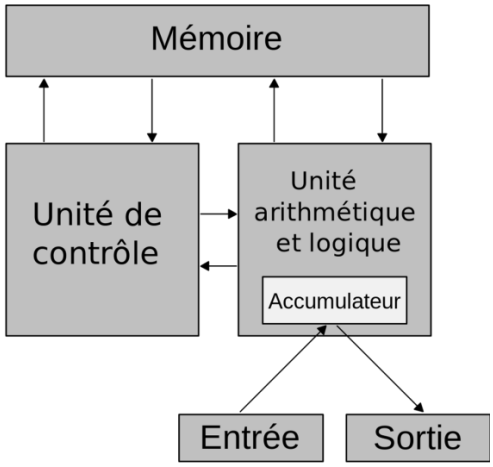
[25] Source de l'image : It's only when you look at an ant through a magnifying glass on a sunny day that you realise how often they burst into flames.

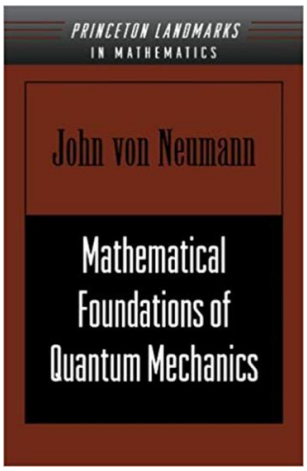
Pascual Jordan (1902-1980, Allemand) est un physicien qui a collaboré avec avec Max Born et Werner Heisenberg et à contribué à poser les fondements mathématiques de la mécanique quantique, notamment au niveau du calcul matriciel. Comme Philipp Lenard, il a été quelque peu oublié, en particulier, du fait de son adhésion au Parti Nazi pendant les années 1930.

John Von Neumann (1903-1957, Hongrois puis Américain) était un polymath, surtout mathématicien, qui a participé à la création des fondements mathématiques de la mécanique quantique, notamment dans "Mathematical Foundations of Quantum Mechanics" publié en 1932. Il a aussi participé au projet Manhattan aux USA. C'est le créateur de la notion de matrice de densité.

On lui doit aussi les concepts de base des ordinateurs.

Les ordinateurs d'aujourd'hui utilisent ainsi une archirecture de Von Neumann avec mémoire, unité de contrôle, unité de calcul, entrées et sorties.



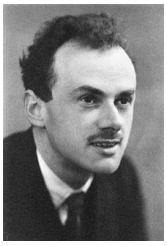


Boris Podolsky (1896-1966, Russe puis Américain) a conçu le paradoxe EPR avec Albert Einstein et Nathan Rosen en 1935 sur l'intrication quantique et les questions de non localité des propriétés des quantums intriqués. C'était un spécialiste de l'électrodynamique qui porte sur l'analyse des champs électriques et électromagnétiques.

Eyant émigré aux USA, selon les archives russes, il aurait été un espion du KGB après-guerre et aurait renseigné l'URSS sur les programmes atomiques américains.

Nathan Rosen (1909-1995, Américain puis Israélien) est le troisième larron du paradoxe EPR qui faisait partie de l'interprétation ou école de Copenhague, expliquant la logique probabiliste de la mécanique quantique par les interactions entre quantums et outils de mesure. Selon cette interprétation, il n'est pas nécessaire de trouver des variables cachées pour expliquer le fonctionnement de quantums intriqués.

Emigrant en Israël en 1953, il y fonde l'institut de physique de l'Université Technion à Haïfa. Il a aussi travaillé sur les trous noirs.



Paul Dirac (1902-1984, Anglais) est un mathématicien et physicien. On lui doit l'équation sur le spin des électrons en 1928. Il prévoit l'existence de l'antimatière avec celle des positrons, en 1932, les homologues des électrons avec une charge positive au lieu d'être négative. Il introduit aussi en 1939 la notation bra-ket dit de Dirac, qui définit les états de quantum, en <phi|psy> en algèbre linéaire.

Il obtient le Prix Nobel de Physique en 1933, donc à 31 ans. Les prix Nobel des débuts du 20eme siècle pouvaient être attribués à de jeunes scientifiques, ce qui semble passé de mode depuis !

The Dirac equation in the form originally proposed by Dirac is:

$$\left(\beta mc^2 + \sum_{k=1}^{3} \alpha_k p_k c\right) \psi(\mathbf{x},t) = i\hbar \frac{\partial \psi(\mathbf{x},t)}{\partial t}$$

Le plus jeune prix Nobel de Physique fut Lawrence Bragg, qui l'obtint à 25 ans en 1915 pour sa découverte de la réfraction des rayons X réalisée à l'âge de 22 ans.

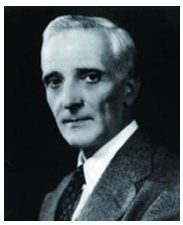
Ettore Majorana (1906-circa 1938, Italien) a imaginé l'existence d'un fermion en 1937 en s'appuyant sur les équations de Dirac, une particule qui serait sa propre antiparticule. Son existence aurait été découverte en 2012 et vérifiée en 2016, même si c'est contesté par de nombreux physiciens.

Ces fermions de Majorana doivent permettre de concevoir des ordinateurs quantiques universels dits topologiques, la voie choisie par Microsoft après les travaux de Freedman et Kitaev à la fin des années 1990. Voir à ce sujet cette intéressante conférence d'Etienne Klein en 2016 sur l'œuvre d'Ettore Majorana. Ce dernier se serait suicidé après une dépression, et d'après Etienne Klein, ayant eu du mal à supporter la pression de son génie ! Mais sa disparition reste énigmatique car on n'a jamais retrouvé trace de son corps !

Alonzo Church (1903-1995, Américain) est un mathématicien à qui l'on doit des travaux dont sont dérivés la thèse dite de Church-Turing selon lequel n'importe quel calcul automatique peut-être réalisé avec une machine de Turing. La thèse de Church-Turing étendue édicte que le temps de calcul d'un problème est équivalent au pire à un polynôme fonction de la taille du problème.

Elle est d'ailleurs non démontrable. Elle est à l'origine de la création du lambda calculus en 1936.

Et les autres, connus, inconnus ou moins célèbres du congrès de Solvay de 1927 ? Nombre d'entre eux n'étaient pas des contributeurs de la mécanique quantique. Il y avait par exemple **Émile Henriot** et **Marie Curie** qui étaient focalisés sur la radioactivité, **Paul Langevin** (avec qui Marie Curie avait eu une liaison en 1910, après la mort accidentelle de son mari Pierre Curie en 1906), ainsi qu'un bon nombre de chimistes. Deux noms méritent cependant d'être cités qui avaient un lien avec la physique quantique.



Léon Brillouin (1889-1969, Franco-Américain) qui est moins connu en France du fait de son expatriation aux USA pendant la seconde guerre mondiale. Il a contribué aux avancées de la mécanique quantique entre les deux guerres mondiales. Il a notamment rapproché la mécanique quantique de la cristallographie.

Il a surtout découvert les phénomènes de diffraction des ondes traversant les cristaux ("Brillouin scattering").

Et puis, enfin, **Hendrik Anthony Kramers** (1894-1952, Hollandais) qui a assisté Niels Bohr dans la création de la théorie des quanta et de la mécanique quantique.

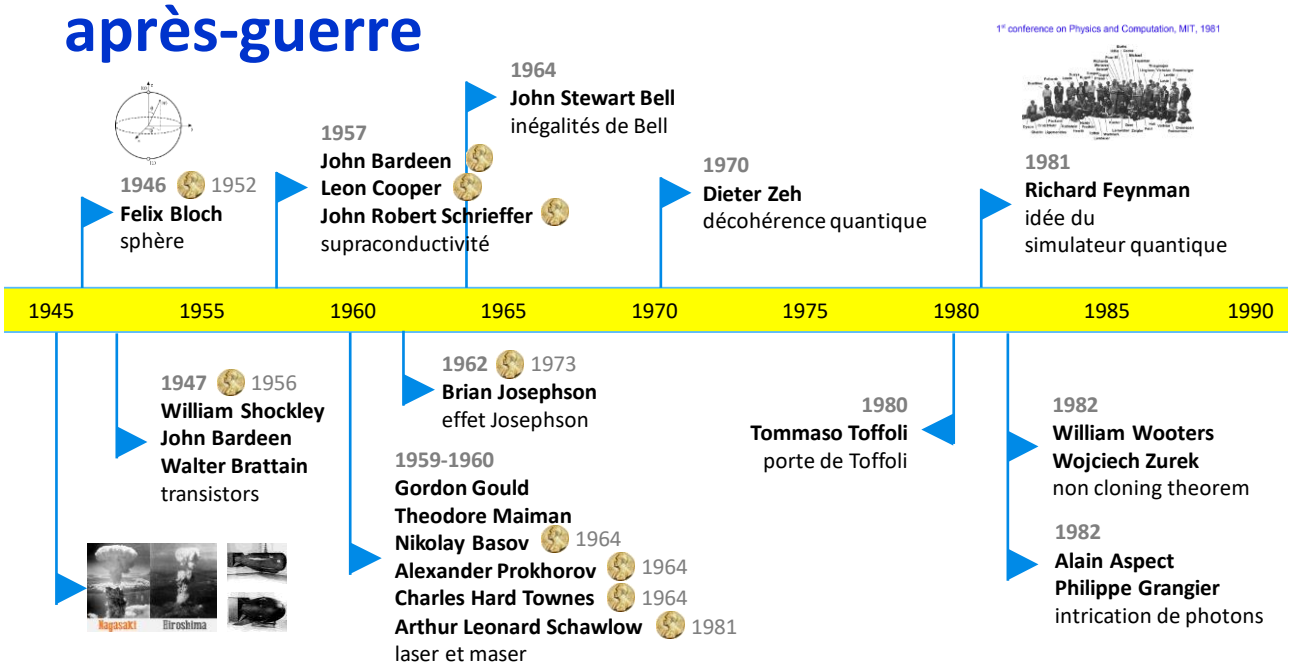
Après-guerre

La mécanique quantique a connu un calme relatif entre les années 1935 et 1960. Les physiciens étaient alors surtout occupés par l'arme et l'énergie nucléaires. Cela a conduit à délaisser quelque peu la mécanique quantique, ou tout du moins à l'utiliser surtout dans le cas de la physique nucléaire, même si son apport était tout relatif dans ce cas.

On peut citer deux branches importantes issues de la mécanique quantique : l'invention des **transistors** en 1947 par William Shockley, John Bardeen et Walter Brattain puis celle des **lasers** et des masers entre 1959 et 1960 par Gordon Gould, Theorodre Maiman, Nikolay Basov, Alexander Prokhorov, Charles Hard Townes et Arthur Leonard Schawlow, une partie d'entre eux seulement ayant reçu le prix Nobel associé à ces découvertes.

La période des trentre glorieuses est dominée dans la physique quantique par les travaux de John Stewart Bell en 1964 et par leur vérification par l'expérience d'Alain Aspect en 1982. Nous avons aussi une date clé avec 1981 qui marque les débuts symboliques de l'informatique quantique, imaginée par Richard Feynman.

L'appellation de seconde révolution quantique couvre les avancées à partir des années 1990, où l'on a commencé à contrôler les propriétés quantiques de quantums individuels, au niveau de photons (polarisation, …), d'électrons (spin) et d'atomes ou d'ions ce qui a notamment permis l'émergence de la cryptographie et des télécommunications quantiques, en plus des prémisses du calcul quantique.



Chien Shiung Wu (1912-1997, Chinoise puis Américaine) est une scientifique qui a surtout contribué aux développements de la physique nucléaire et au projet Manhattan aux USA. Elle a aussi contribué à la physique quantique en conduisant la première expérience relative à la synchronisation de paires de photons en 1947[26], bien avant l'expérience d'Alain Aspect et Philippe Grangier en 1982.

Cette expérience était différente et s'appuyait sur la mesure de la corrélation angulaire de photons dans les rayons gamma (très haute fréquence et énergie) générés par la rencontré d'électron et de positron.

Felix Bloch (1905-1983, Suisse puis Américain) est un physicien à qui l'on doit notamment la représentation physique de l'état d'un qubit dans une sphère qui porte son nom, la sphère de Bloch, élaborée en 1946. Il fut prix Nobel de physique en 1952 pour ses travaux sur la résonance magnétique nucléaire. Il fut aussi le premier directeur du laboratoire de physique des particules international CERN en 1954.

[2626] Voir notamment The Angular Correlation of Scattered Annihilation Radiation, Wu et Shaknov, 1949.

Hugh Everett (1930-1982, Américain) est un physicien à qui l'on doit la formulation des états relatifs et d'une fonction d'onde globale intégrant les observations, les observateurs et les outils d'observation des phénomènes quantiques, et à l'hypothèse des multiverses expliquant l'intrication quantique et la non localité.

John Stewart Bell (1928-1990, Irlandais) a relancé la recherche en mécanique quantique dans les années 1960 sur la notion d'intrication. On lui doit les "inégalités de Bell" qui mettent en avant les paradoxes soulevés par l'intrication quantique. Le théorème de Bell de 1964 indique qu'aucune théorie de variable cachée - imaginée par Einstein en 1935 - ne peut reproduire les phénomènes de la mécanique quantique[27].

Il invalide donc l'hypothèse d'existence de variables cachées expliquant l'intrication quantique. Les inégalités de Bell ont été violées par les expériences du Français Alain Aspect en 1982 puis 1998, démontrant l'inexistence de ces variables cachées. Mais avant cette expérience, les inégalités de Bell ont été démontrées théoriquement par John Clauser, Michael Horne, Abner Shimony et Richard Holt en 1969 dans ce que l'on appelle les inégalités CHSH[28].

Alain Aspect (1947, Français) invalide donc le paradoxe EPR et les inégalités de Bell en 1982 dans une expérience menée au laboratoire de SupOptique du bâtiment 503 de la faculté d'Orsay, puis confirmée dans d'autres expériences en 1998. Elle valide l'intrication de photons distants ayant interagi par le passé et le principe de la non localité des propriétés quantiques[29].

Il explique cela très bien dans diverses conférences dont celle-ci. J'ai pu le rencontrer en mai 2018 avec Fanny Bouton à l'école Supoptique de Palaiseau près de Paris. Il continue de diffuser la bonne parole sur ses expériences, notamment dans des MOOC réalisés pour l'école Polytechnique où il continue d'enseigner. Il fait partie du conseil scientifique d'Atos et accompagne la startup Pasqal. On le présente souvent comme un futur prix Nobel de physique. Mais ce sésame pourrait lui échapper dans la mesure où son travail relevait d'une approche expérimentale plus que théorique, cette dernière revenant plutôt à John-Steward Bell.

Philippe Grangier (1957, Français) est un ancien thésard d'Alain Aspect avec qui il avait travaillé sur l'expérience de ce dernier en 1982 avec Gérard Roger et Jean Dalibard. C'est l'un des spécialistes mondiaux de la cryptographie quantique, notamment de la CV-QKD. Il est à l'origine de la startup associée, Sequrnet, créée en 2008 et fermée en 2017.

---

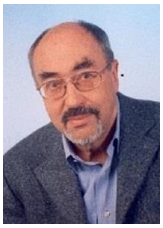
[27] Voir cette explication du théorème de Bell dans un document de Tim Maudlin à l'occasion des 50 ans du théorème : What Bell Did, 2014 (28 pages).

[28] Voir Proposed experiment to test local hidden-variable theories, 1969 (5 pages).

[29] L'expérience a été depuis multipliée à l'envie. En 2017, des chercheurs de Varsovie arrivaient ainsi à intriquer un photon avec des milliards d'atomes de rubidium. Voir Quantum entanglement between a single photon and a trillion of atoms, 2017.

John Wheeler (1911-2008, Américain) supervisa la thèse de Hugh Everett et un spécialiste de la gravitation quantique. Il a surtout travaillé dans le domaine de la physique nucléaire et notamment sur la matière nucléaire à très haute densité que l'on trouve dans les étoiles à neutrons. A noter qu'il a eu comme élève et thésard un certain Richard Feynman.

Bruce DeWitt (1922-2004, Américain) était un contributeur du rapprochement de la théorie de la relativité et de la mécanique quantique, notamment autour de la gravitation quantique. Il a aussi un lien avec les travaux de Hugh Everett sur les multiverses.



Dieter Zeh (1932-2018, Allemand) est le découvreur du phénomène de la décohérence quantique en 1970, c'est-à-dire, la fin du phénomène de superposition d'états de quantum, lorsque les particules sont perturbées par leur environnement et que la phase est modifiée. La notion de décohérence est clé dans la conception d'ordinateurs quantiques.

L'objectif recherché étant de retarder autant que possible ce phénomène qui résulte de l'interaction entre les quantums et leur environnement[30].

Wojciech Zurek (1951, Polonais) qui est un physicien spécialiste de la décohérence quantique qui a contribué aux fondements de la physique quantique appliquée aux calculateurs quantiques. On lui doit le théorème du non clonage qui veut qu'il soit impossible de cloner un qubit à l'identique sans que les qubits résultants soient ensuite intriqués.

Anton Zeilinger (1945, Autrichien) est un physicien prolifique qui a notamment fait avancer le champ de la téléportation quantique dans les années 2000. En 1991, il valide la dualité onde-particule des neutrons. Il a été aussi le premier à réaliser la téléportation d'un qubit. C'est un spécialiste de l'intrication quantique, ayant prouvé qu'il était possible d'intriquer plus de deux quantums ou qubits.

Il a créé des fondements théoriques et expérimentaux de la cryptographie quantique. On lui doit aussi avec deux collègues la notion d'état superposé GHZ (Greenberger-Horne-Zeilinger) qui permet de démontrer l'inexistence de variables cachées dans l'intrication quantique d'au moins trois particules et avec un nombre fini de mesures. La notion date de 1989 et sa validation expérimentale de 1999.

Serge Haroche (1944, Français), prix Nobel de physique en 2012, a créé des qubits avec des atomes couplés à des cavités supraconductrices contenant quelques photons. On compte **Jean-Michel Raymond**[31] et **Michel Brune** parmi ses collaborateurs. Serge Haroche a été le premier à mesurer le phénomène de décohérence de quantums (perte de superposition) dans une expérience en 1996.

---

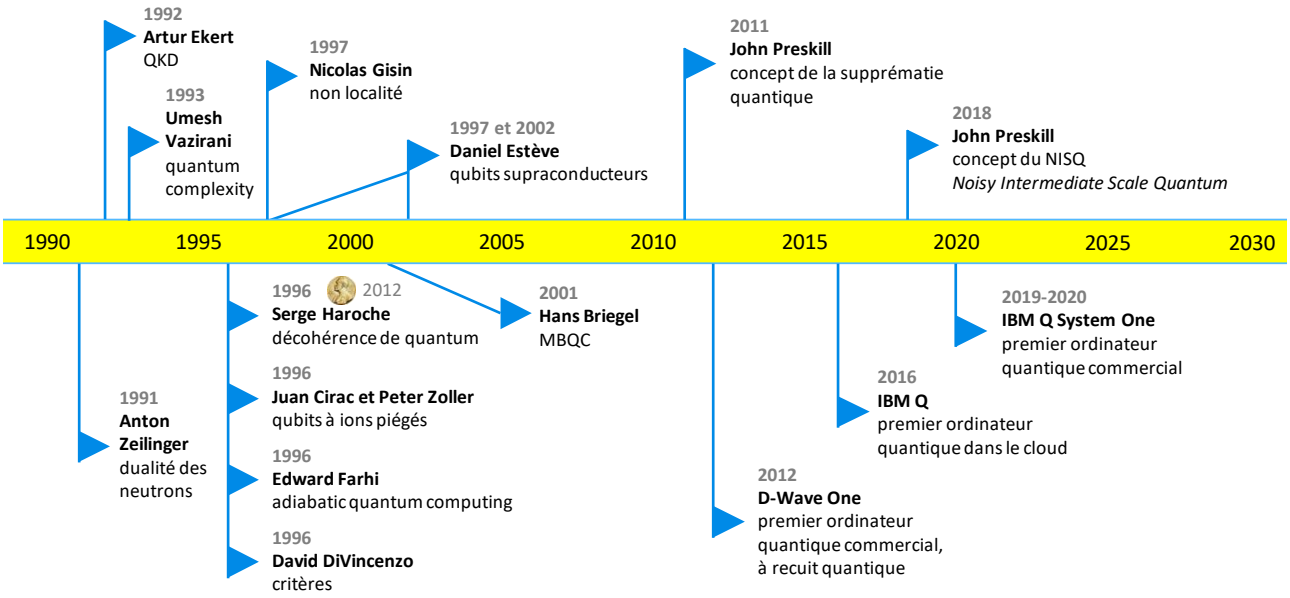
[30] Dieter Zeh est notamment l'auteur de On the Interpretation of Measurement in Quantum Theory en 1970 (8 pages).

[31] Voir son intéressante conférence Informatique quantique ou comment utiliser l'étrangeté du monde microscopique, Jean-Michel Raymond, 2015 (1h36mn). Voir aussi le support de présentation (56 slides).

Cette expérience a été menée à l'ENS avec des atomes de rubidium. Serge Haroche fait partie du conseil scientifique d'Atos où il fait partie des scientifiques les plus réservés sur le devenir de l'informatique quantique.

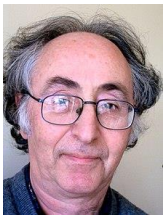
Physiciens de l'informatique quantique

Je complète cette histoire par un tour d'horizon des physiciens de l'informatique quantique, qui sont souvent des spécialistes de l'optique ou de la matière condensée, comme les supraconducteurs, servant à créer des qubits.



Richard Feynman (1918-1988, Américain) théorise la possibilité de créer des ordinateurs quantiques dans Simulating Physics with Computers publié en 1981, capables de simuler des phénomènes quantiques pour résoudre des problèmes de simulation du fonctionnement de la matière[32]. Il est aussi à l'origine de la découverte de l'hélium superfluide, sans trop de rapport avec l'informatique quantique.

Enfin, il est surtout connu du grand public scientifique pour son grand talent de vulgarisateur.



Brian Josephson (1940, Anglais) est un physicien de l'Université de Cambridge, prix Nobel de physique en 1973 à 33 ans, ce qui est très rare, pour sa prédiction de l'effet qui porte son nom en 1962 alors qu'il n'avait donc que 22 ans. L'effet Josephson décrit le passage de courant par effet tunnel dans un circuit supraconducteur.

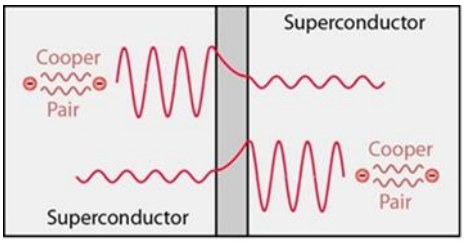
Le courant traverse une fine barrière isolante de quelques nanomètres d'épaisseur. En-dessous d'une certaine tension, le courant se met à osciller.

[32] Voir également Quantum Mechanical Computers, également de Richard Feyman, publié en 1985 (10 pages). Il y décrit comment un ordinateur quantique pourrait réaliser des opérations mathématiques similaires à celles des ordinateurs traditionnels. Il conclue en disant que l'on pourrait créer des ordinateurs où un bit tiendrait dans un seul atome ce qui donnerait encore du mou à la loi de Moore !

Il est généré par les électrons organisés en paires de Cooper du nom de Leon Cooper qui les a découverts en 1952. Ces électrons en paires sont de spins opposés (polarité magnétique) et se constituent du fait du rapprochement des ions métalliques à leur passage.

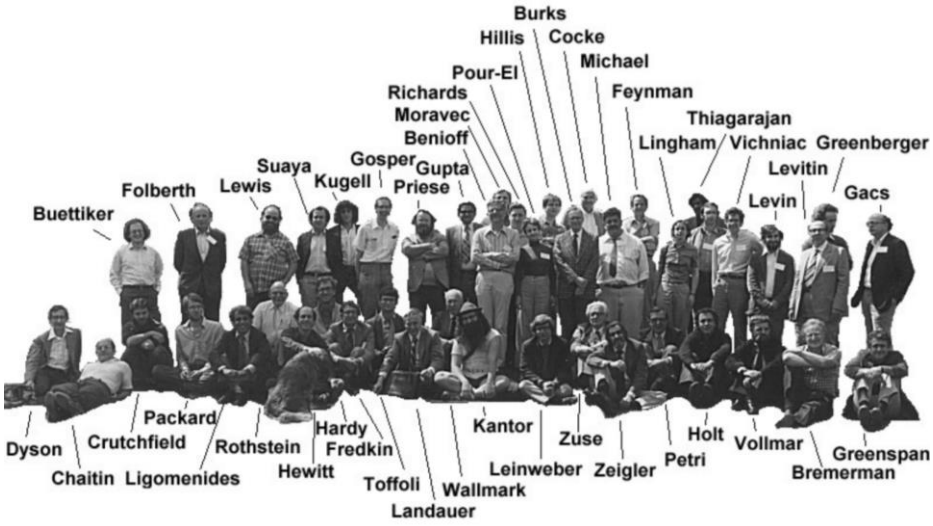
Le système se comporte comme une résistance associée à une inductance en boucle, l'oscillation étant contrôlable par un champ magnétique et pouvant se faire avec deux états énergétiques distincts. La supraconductivité a été découverte pour sa part en 1911 par le Hollandais Heike Kamerlingh Onnes.

C'est la base des qubits supraconducteurs et de leurs portes quantiques ! Le physicien Serge Haroche explique l'effet Josephson dans cette vidéo de son cours du Collège de France de 2011. A noter que Brian Josephson s'intéresse depuis sa découverte à la méditation transcendantale.



Yuri Manin (1937, Russe et Allemand) est un mathématicien qui, avec Paul Benioff et Richard Feynmann, fait partie des premiers à avoir proposé l'idée de créer des ordinateurs quantiques, et en 1980 dans son livre "Computable and Uncomputable".

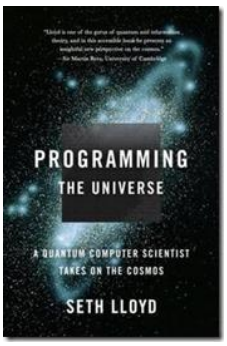
Ils participaient à la conférence "Physics & Computation" du MIT en 1981 qui rassemblait un bon nombre de noms connus de l'informatique quantique comme Tommaso Toffoli et Edward Fredkin (*ci-contre, source*).



Tommaso Toffoli (1943, Italien puis Américain) est un ingénieur connu pour la création, au début des années 1980, de la porte quantique à son nom, une porte conditionnelle à trois entrées qui est très utilisée en programmation quantique. Il est enseignant à l'Université de Boston depuis 1995.

Edward Fredkin (1934, Américain) est professeur de Carnegie Mellon. On lui doit la porte quantique d'interversion à deux entrées (SWAP). Il est aussi le concepteur de la notion d'ordinateur réversible. C'est un inventeur prolixe, à l'origine des transpondeurs d'identification de véhicules et de la géonavigation automobile.

C'est enfin un promoteur de la notion de "philosophie digitale" qui réduit le monde et son fonctionnement à un programme géant quantique, une théorie qu'il partage avec **Seth Lloyd** (1960, Américain) auteur de "Programming the Universe". Cette idée a été remise au goût du jour par Elon Musk qui pense que l'Univers est un programme gigantesque et que nous vivons dans une simulation. Le respect « automatique » de lois physiques élémentaires est-il un « programme » ? Epineuse question sémantique !

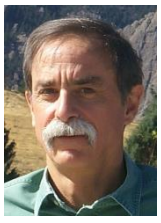


Wolfgang Paul (1913-1993, Allemagne), prix Nobel de physique en 1989 est un physicien qui conceptualise les ions piégés dans les années 1950. Les physiciens **Juan Cirac** (1965, Espagnol) et **Peter Zoller** (1952, Autriche) théorisent, conçoivent et testent les premiers qubits à ions piégés en 1996 à partir des travaux de Wolfgang Paul.

Claude Cohen-Tannoudji (1933, Français) est notamment ancien élève de Normale Sup où il a suivi les enseignements des mathématiciens Henri Cartan et Laurent Schwartz et du physicien Alfred Kastler. Il devient Prix Nobel de Physique en 1997 en même temps que Steven Chu, qui fut plus tard Ministre de l'Energie de la première présidence de Barack Obama.

Il doit son prix Nobel à ses travaux sur le refroidissement d'atomes par laser qui permis d'atteindre des températures extrêmement basses, inférieures au milli-Kelvin (voir sa lecture). A noter qu'Alain Aspect a un temps travaillé dans son équipe.

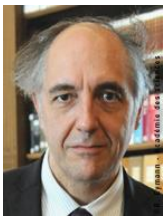
Rainer Blatt (1952, Autrichien et Allemand) de l'Université d'Innsbruck est un spécialiste, entre autres choses, des qubits réalisés avec des ions piégés. Il est le premier à avoir pu intriquer l'état quantique de deux ions piégés. C'est un peu l'analogue autrichien d'Alain Aspect pour la France.



David Wineland (1944, Américain) est un physicien du NIST connu pour ses avancées dans le domaine des ions piégés et leur refroidissement par laser en 1978. Il a aussi créé la première porte quantique unitaire à base d'un seul atome en 1995. Il a obtenu le Prix Nobel de physique en 2012 conjointement avec le Français Serge Haroche.

Edward Fahri (1952, Américain) est un physicien ayant travaillé dans de nombreux domaines, notamment dans la physique des particules à haute énergie, en particulier au LHC du CERN à Genève. Il est surtout le créateur d'algorithmes adaptés aux ordinateurs quantiques adiabatiques.

Ce sont les algorithmes utilisés dans les ordinateurs quantiques de D-Wave qui permettent de faire converger un système complexe de qubits vers une solution de problèmes d'optimisation, une méthode que l'on appelle le recuit quantique ("quantum annealing").



Daniel Estève (1954, Français) est un physicien spécialiste de l'informatique quantique, responsable du laboratoire Quantronique du CEA à Saclay, lancé en 1984. Il planche en particulier sur les qubits supraconducteurs à effet tunnel exploitant une jonction Josephson de type transmon.

Il a créé un premier qubit opérationnel en 1997, le quantronium, suivi d'un autre prototype en 2002. On peut considérer qu'il est l'un des grands pionniers de cette branche. Daniel Estève fait partie du conseil scientifique d'Atos. Je l'ai rencontré début juin avec Fanny Bouton et il nous a brossé un beau tableau de l'histoire des qubits supraconducteurs.

Michel Devoret (1953, Français) est un ingénieur télécom devenu physicien, cofondateur du laboratoire Quantronique avec Daniel Estève au CEA de Saclay entre 1985 et 1995, qui est un des pionniers mondiaux des qubits supraconducteurs à base d'effet Josephson. Il est depuis 2002 professeur à l'Université de Yale aux USA. Il est cofondateur de la startup américaine QCI.

Il a aussi travaillé avec John Martinis, alors à l'Université de Santa Barbara, pour faire un inventaire en 2004 des bases de la création de qubits supraconducteurs[33].

Artur Ekert (1961, Polonais et Anglais) est un physicien en mécanique quantique connu pour être l'un des créateurs du champ de la cryptographie quantique. Petite anecdote : il avait rencontré Alain Aspect en 1992 pour lui parler de cette inspiration après avoir découvert les expériences de ce dernier.

C'est un bel exemple d'inventions par étapes, un chercheur en inspirant un autre ! Il fait aussi partie du conseil scientifique d'Atos.

Nicolas Gisin (1952, Suisse) est un physicien spécialiste de la communication quantique. Il a démontré la non localité quantique avec une expérience en 1997 sur une distance de 10 km, étendant la performance réalisée en laboratoire par Alain Aspect en 1982. Comme Philippe Grangier, c'est un spécialiste de la cryptographie quantique.

Il est notamment le cofondateur de IDQ en 2001, une startup suisse spécialisée dans la génération de nombres véritablement aléatoires à partir de photons traversant un miroir dichroïque.

[33] Dans Implementing Qubits with Superconducting Integrated Circuits (41 pages)

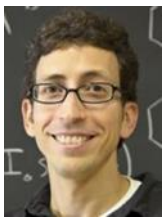
David DiVicenzo (1959, Américain) était un chercheur chez IBM et il est à l'origine des critères qui portent son nom et qui définissent les besoins minimums d'un ordinateur quantique à portes universelles. Il est maintenant chercheur et professeur à l'Université d'Aix la Chapelle en Allemagne.

Lieven Vandersypen (1972, Belge) est un scientifique de l'Université TU Delft aux Pays-Bas et de sa spin-off QuTech. C'est un pionnier des qubits à base de spins d'électrons. A ce titre, il travaille notamment avec Intel qui teste chez QuTech ses chipsets de qubits CMOS et dans laquelle Intel a investi $50M.

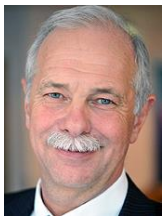
John Preskill (1953, Américain) est professeur à Caltech. C'est le créateur de la notion de suprématie quantique en 2011 et du NISQ en 2018, les Noisy Intermediate-Scale Quantum, la dénomination des calculateurs quantiques actuels et à venir dans un futur proche, qui sont de taille intermédiaire et sujets à un bruit quantique qui en limite les capacités.

C'est aussi un très bon vulgarisateur[34].

John Martinis (1958, Américain), est un physicien de l'UCSB et Google. Il dirige les efforts dans l'informatique quantique de ce dernier autour des qubits supraconducteurs. Il a fait sa thèse dans le laboratoire Quantronics de Daniel Estève au CEA à Saclay, donc également dans les qubits supraconducteurs.



Jason Alicea (Américain) est un professeur de physique théorique de l'IQIM, Institute for Quantum Information and Matter, de l'Université Caltech en Californie. C'est un spécialiste de l'informatique quantique topologique, un concept utilisé par Microsoft et Nokia, ce dernier via les Bell Labs aux USA. Cf ses publications dans Arxiv.



Jürgen Mlynek (1951, Allemand) est un physicien spécialiste de l'optronique et de l'interférométrie. Il est le coordinateur de l'European Flagship project sur le quantique. On lui doit comme, évoqué au sujet de Louis De Broglie, l'expérience validant la dualité ondes-particules des atomes réalisée en 1991.

Marie-Anne Bouchiat (1934, Française) est une spécialiste de la physique des atomes de rubidium et notamment de leur contrôle par pompage optique. Ce sont les fondements de la création d'ordinateurs quantiques à base d'atomes froids. Sa fille Hélène Bouchiat est également physicienne, spécialiste en nanosciences !

[34] Voir sa présentation qui fait un tour d'horizon de l'état de l'art de l'informatique quantique Quantum Computing for Business, JohnPreskill, décembre 2017 (41 slides).

Elisabeth Giacobino (1946, Française) est une spécialiste de la physique des lasers, de l'optique non-linéaire, de l'optique quantique et de la superfluidit, en liaison notamment avec le contrôle des atomes froids. Elle officiait au CNRS au sein du laboratoire Kastler-Brossel. Elle fait partie du comité scientifique de sélection des projets du flagship quantique européen.

Jean Dalibard (1958, Français) est un physicien chercheur à l'ENS et enseignant à Polytechnique ainsi qu'au Collège de France. C'est un spécialiste de l'optique quantique et des interactions entre les photons et la matière[35]. Il avait participé avec Philippe Grangier au montage de l'expérience d'Alain Aspect en 1982.

Jacqueline Bloch (1967, Française) est une ingénieure-chercheuse qui travaille sur le couplage entre lumière et matière à l'aide de semi-conducteurs. Directrice de Recherche au sein du Centre de Nanosciences et de Nanotechnologies (C2N) du CNRS, elle travaille sur les polaritons, des quasi-particules qui associent des photons et des dipôles magnétiques à base d'arséniure de gallium.

Ceux-ci ont des applications potentielles dans la création de simulateurs quantiques à base de réseaux de polaritons (source).

Jean-Michel Gérard (1962, Français) est un physicien du laboratoire IRIG du CEA à Grenoble et directeur du service PHELIQS (PHotonique, ELectronique et Ingénierie QuantiqueS) qui associe l'Université de Grenoble et le CEA (c'est une UMR : Unité Mixte de Recherche). Il travaille notamment sur la création de sources de photons uniques.

Maud Vinet (1975, Française) dirige un laboratoire du CEA-Leti de Grenoble qui planche sur les nanotechnologies CMOS à l'origine de nombreux progrès comme le SOI utilisé par SOITEC et le FD-SOI de STMicroelectronics, deux technologies qui réduisent la consommation électrique et améliorent la performance des chipsets en CMOS, notamment dans la mobilité.

Son laboratoire est focalisé sur l'ingénierie de la création de qubits à base de composants CMOS. Nous décrirons ses travaux plus en détail plus loin dans cet ebook. Maud Vinet coordonne les efforts de la filière de recherche Grenobloise qui intègre plusieurs laboratoires dont le Leti, l'IRIG (aussi du CEA) et l'Institut Néel du CNRS.

[35] Voir notamment sa leçon sur les atomes froids au Collège de France qui décrit bien comment on refroidit des atomes à très basses températures avec des lasers.

Alexia Auffèves (1976, Française) est une spécialiste de la thermodynamique quantique, basée à l'institut Néel de Grenoble. Elle étudie notamment les notions d'échelle de temps, d'irréversibilité et leurs liens avec la mesure et la décohérence des qubits. Elle développe aussi une ontologie de la mécanique quantique avec Philippe Grangier et la philosophe Naila Farouki[36].

Elle contribue activement aux efforts coordonnés des laboratoires de Grenoble pour la création d'ordinateurs quantiques autour de la notion de quantum engineering ainsi qu'à la vulgarisation grand public de la mécanique quantique[37].

Pascale Senellart (1972, Française) est une physicienne du CNRS, dont elle est médaille d'argent 2014, au laboratoire C2N à Palaiseau, qui travaille également sur les sources de photons. Elle est aussi cofondatrice de la startup Quandela qui est spécialisée dans les composants à base de quantum dots semiconducteurs pour l'émission ou la manipulation de photons.

Ceux-ci peuvent servir à différents usages comme la création d'ordinateurs quantiques à base de photons ou à des systèmes de communication quantique.

Eleni Diamanti (1975, Grecque) est une grande spécialiste de la cryptographie et de la communication quantique. Elle est enseignante-chercheuse au LIP6 (CNRS). Je l'avais croisée lors de L'Echappée Volée en juillet 2018 où elle réalisait la performance d'expliquer l'informatique quantique en 8 minutes (vidéo).

Elham Kashefi (1973, Iran) est une spécialiste des protocoles de communication quantiques ainsi que du « blind quantum computing », que nous aurons l'occasion d'expliquer. Elle est aussi co-fondatrice de la startup de télécommunications quantiques sécurisées VeriQloud. Elle gère des recherches à cheval entre Edimbourg et Paris au LIP6 (Jussieu).

Avec son équipe, elle est à l'origine de la création d'un site sur le zoo des protocoles de communication quantique[38].

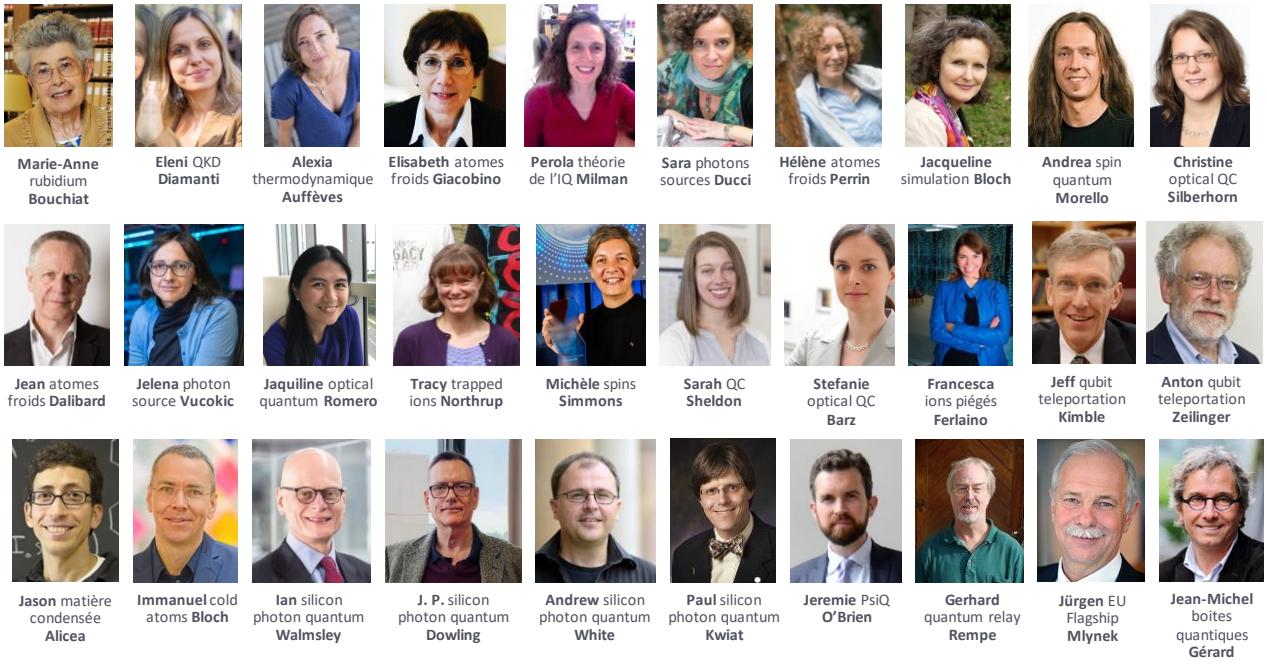
Hélène Perrin (c. 1975, Française) est une spécialiste des atomes froids, oeuvrant au Laboratoire de Physique des Lasers (LPL) de Paris 13. Elle pilote avec Pascal Simon le projet Quantum Simulation SIM, un simulateur quantique à base d'atomes froids, l'une des branches de l'informatique quantique parallèlement avec celle des ordinateurs quantiques à portes universelles.

---

[36] Voir Contexts, Systems and Modalities: a new ontology for quantum mechanics par Alexia Auffèves et Philippe Grangier, 2015 (9 pages).

[37] Voir Donner du sens à la mécanique quantique par Sylvain Guilbaud, une interview dans le journal du CNRS avec Alexia Auffèves et Philippe Grangier, 2016.

[38] Voir https://wiki.veriqloud.fr/index.php?title=Protocol_Library.



Michelle Simmons (1967, Anglo-Australienne) est une physicienne de l'Université de Nouvelle Galle en Australie (UNSW), spécialisée dans la branche de l'informatique quantique qui s'appuie sur le contrôle de spins d'électrons dans du silicium. Elle est la cofondatrice de la startup Silicon Quantum Computing (Australie, $66M).

C'est une spinoff de son université et de son laboratoire Centre of Excellence for Quantum Computation and Communication Technology (CQC2T).

Christine Silberhorn (1974, Allemande) est une chercheuse spécialisée dans l'informatique quantique à base de photon. Officiant dans l'Université de Paderborn située entre Dortmund et Hanovre. Elle planche notamment sur les mémoires quantiques optiques.

Stephanie Wehner (1977, Allemande) est une physicienne spécialisée dans le développement de protocoles de communication quantique, basée à l'université de Delft aux Pays-Bas. Elle coordonne la « Quantum Internet Alliance", l'un des projets du Flasgship Quantique européen qui ambitionne de déployer un réseau Internet protégé par clés quantiques (QKD) en mode réseau maillé.

Perola Milman (c. 1975, Française) est une spécialiste de la théorie de l'informatique quantique et notamment des photons et ions piégés. Elle a en particulier démontré la capacité d'intrication de molécules. Elle est enseignante-chercheuse du Laboratoire Matériaux et Phénomènes Quantiques de l'Université Paris Diderot.

Sara Ducci (1971, Française) est une autre enseignante-chercheuse du même Laboratoire Matériaux et Phénomènes Quantiques et elle est spécialisée dans les sources de photons, notamment à base de semiconducteurs. Elle s'intéresse aussi à la caractérisation (mesure de l'état…) et à la manipulation des photons.

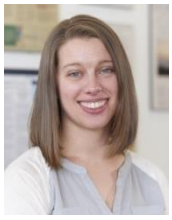
Jacquiline Romero (c. 1985, Philippines) est une spécialiste de l'optique quantique et de l'intrication qui fait de la recherche en Australie dans l'Université de Queensland. Elle travaille notamment sur les architectures neuromorporphiques optiques.

Jelena Vucokic (c. 1980, Serbe) est enseignante chercheuse à Stanford, spécialisée en photonique quantique. Elle dirige le Nanoscale and Quantum Photonics Lab. Elle contribue aux développements en photonique qui serviront au développement d'ordinateurs quantiques optiques.

Francesca Ferlaino (1977, Italienne) et une chercheuse typiquement européenne, étant passée par plusieurs laboratoires de plusieurs pays. Elle est directrice de recherche à l'IQOQI d'Innsbruck en Autriche. C'est une spécialiste des ions piégés.

Tracy Northrup (c. 1975, Autriche) est une chercheuse spécialisée dans les ions piégés, l'une des grandes branches du calcul. Elle travaille à l'Université d'Innsbrück qui en l'une des plus actives dans le domaine.

Anne Matsuura (c. 1970, Japonaise-Américaine) est une physicienne qui dirige le laboratoire de recherche quantique des Intel Labs. Elle pilote les efforts de l'Américain dans la création d'ordinateurs quantiques supraconducteurs et CMOS/spin d'électrons, avec une vision d'ensemble de l'architecture matérielle.



Sarah Sheldon (c. 1987, Américaine) fait partie depuis 2013 des équipes d'IBM qui planchent sur l'informatique quantique. Elle est notamment active dans le domaine des codes de correction d'erreurs et la qualité des qubits supraconducteurs.

Stefanie Barz (c. 1980, Allemande) est enseignante en optique quantique à l'Université de Stuttgart. Elle s'intéresse notamment à la cryptographie et aux télécommunications quantiques. Elle pilote le projet SiSiQ finance dans le cadre du Flagship européen.

Alexei Grinbaum (1978, Franco-Russe) est un chercheur du CEA-Saclay dans le laboratoire LARSIM. Il planche sur les fondations de l'informatique quantique et sur la philosophie de la physique quantique. Il est notamment l'auteur de l'ouvrage « Les robots et le mal » publié en 2018.

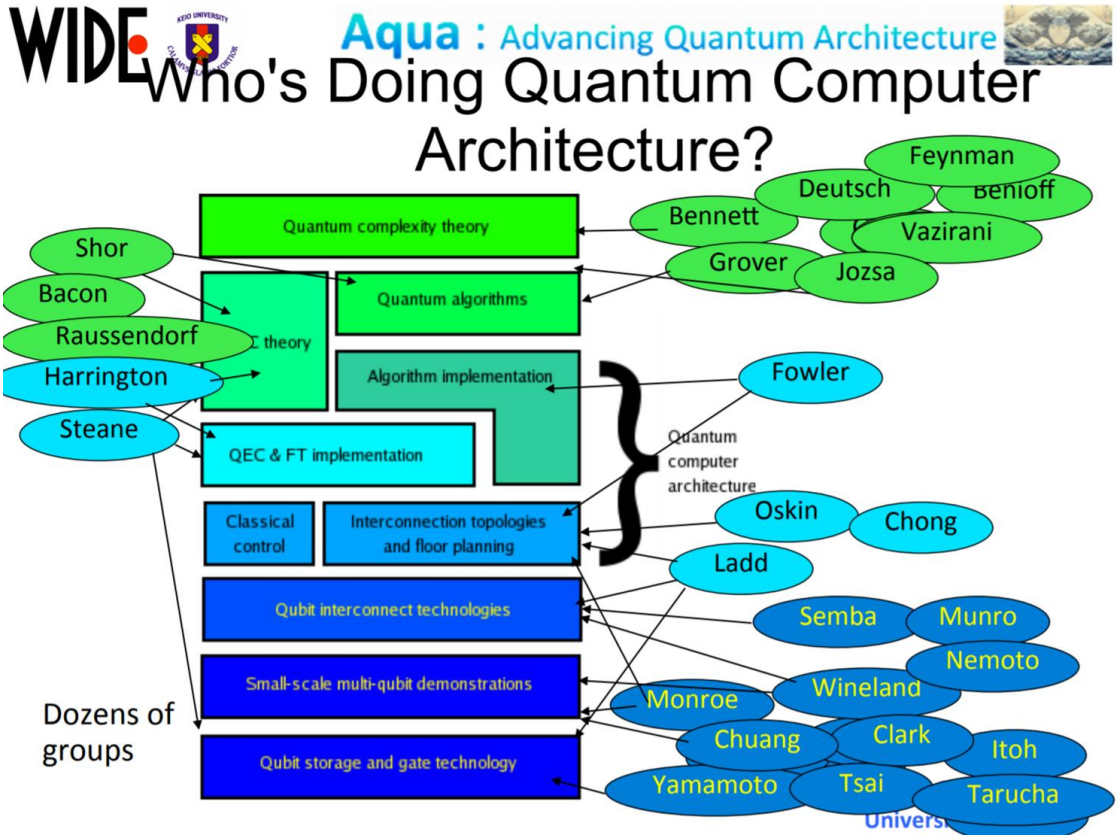
Frédéric Grosshans (Français) est un chercheur du CNRS (LAC Université Paris-Sud) spécialisé dans la QKD, les répéteurs et les réseaux quantiques. Voir cette liste de chercheurs du PCQC (Paris Center for Quantum Computing) qui comprend d'autres chercheurs de laboratoires français.

Cet inventaire de scientifiques, *ci-dessus* comme *ci-dessous* n'est pas bâti sur des critères rigoureux et quantifiés. Ce sont des personnalités que j'ai découvertes au fil de l'eau dans mes recherches d'information sur le sujet. Il résulte aussi, parfois, de rencontres, notamment pour ce qui est des scientifiques français.

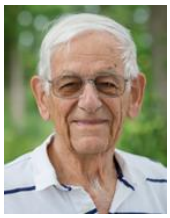
Créateurs d'algorithmes quantiques

Terminons ce long "hall of fame" avec quelques-uns des principaux contributeurs à la création d'algorithmes quantiques, une discipline relativement nouvelle qui a vu le jour au début des années 1990.

Autre manière de voir les choses, extraite de la présentation Quantum Computer Architecture Rod Van Meter, 2011 (89 slides). Histoire de n'oublier personne ! Avec en vert, les spécialistes des algorithmes quantiques, en bleu clair, ceux des codes de correction d'erreurs, et en bleu foncé, ceux des couches physiques des qubits.



Alexander Holevo (1943, Russe) est un mathématicien russe spécialiste de l'information quantique et à qui l'on doit le théorème qui porte son nom selon lequel on ne peut pas récupérer plus de N bits d'un registre de N qubits[39]. Il a aussi développé les bases mathématiques de la communication quantique.



Paul Benioff (1930, Américain) est un physicien pionnier de l'informatique quantique théorique. A noter qu'il est passé quelques temps par le CNRS en France entre 1979 et 1982, à l'Université de Marseille-Luminy.

Umesh Virkumar Vazirani (1945, Indien) est enseignant à Berkeley. C'est l'un des fondateurs du calcul quantique, avec son papier coécrit en 1993 avec son étudiant Ethan Bernstein, Quantum Complexity Theory, pas facile à piger pour le profane. Il est aussi le créateur de l'algorithme de la transformée de Fourier quantique utilisé par Peter Shor pour son fameux algorithme de factorisation de nombres entiers.

[39] Ce théorème valide indirectement le fait qu'il est difficile de faire du « big data » avec un ordinateur quantique au sens du stockage et de l'analyse de gros volumes d'information. Par contre, l'algorithme de Grover permet de retrouver rapidement une aiguille dans une botte de foin, nous le verrons plus loin.

Peter Shor (1959, Américain) est le père de l'algorithme du même nom qui permet la factorisation d'entiers en nombres premiers, à base de transformées de Fourier quantiques. Il est aussi à l'origine d'un algorithme de correction d'erreurs à 9 qubits pour les ordinateurs quantiques. Il enseigne les mathématiques appliquées au MIT depuis 2003.

On lui doit indirectement tout le mouvement de la cryptographie post-quantique qui vise à créer des systèmes de cryptographie résistant au cassage de clés publiques via son algorithme… avec des calculateurs quantiques qui n'existent pas encore. Peter Shor a créé son fameux algorithme de factorisation alors qu'il travaillait aux Bell Labs.

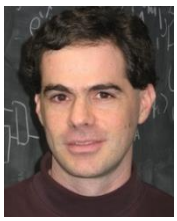
David Deutsch (1953, Israélien et Anglais) est un physicien du laboratoire d'informatique quantique de l'Université d'Oxford au Royaume-Uni. Il est l'auteur d'un algorithme de recherche qui porte son nom, avec deux variantes, une première en 1985 et une seconde en 1992 co-créée avec Rochard Jozsa.

L'algorithme est très performant mais n'a pas de véritable utilisation pratique.

Michael Freedman (1951, Américain) est un mathématicien Médaille Fields en 1986 qui dirige le laboratoire Microsoft Station Q à Santa Barbara en Californie. Il est l'un des pères de l'informatique quantique topologique avec Alexei Kitaev.

Alexei Kitaev (1963, Russe et Américain) est avec Michael Freedman l'un des pères du concept d'ordinateur quantique topologique en 1997, utilisé par Microsoft. Il était chercheur chez Microsoft Research au début des années 2000 et est maintenant à l'Université de Caltech.

Aram Harrow (Américain) est un spécialiste prolifique des algorithmes quantiques. Il enseigne au MIT. Il est l'auteur d'un algorithme de résolution d'équations linéaires avec Avinatan Hassidim et Seth Lloyd. Voir Quantum algorithm for linear systems of equations, 2009 (24 pages).



Daniel Gottesman (1970, Américain) est un physicien du Perimeter Institute de Waterloo au Canada. Il a fait sa thèse à Caltech sous la supervision de John Preskill. Il est connu pour ses travaux sur les codes de correction d'erreurs quantiques (QEC) et est coauteur du théorème de Gottesman–Knill.

Ce théorème prouve que l'intrication quantique n'est pas suffisante pour générer une meilleure performance des algorithmes quantiques exécutés sur ordinateurs quantiques par rapport à des algorithmes optimisés pour ordinateurs traditionnels. Heureusement, il y a aussi la superposition des états des qubits !

Gil Kalai (1955, Israélien) est un professeur de mathématiques de l'Université Hébraïque de Jérusalem et à Yale. Il est l'inventeur de nombreux algorithmes. Son ambition est de démontrer mathématiquement qu'il sera impossible aux ordinateurs quantiques universels de monter en puissance.

En cause, leur taux d'erreurs, même avec des codes de correction d'erreurs et la notion de qubits logiques qui assemblent des qubits physiques.

Scott Aaronson (1981, Américain) enseigne les sciences de l'information à l'Université d'Austin au Texas. C'est un grand spécialiste des algorithmes quantiques et des théories de la complexité. Il est notamment à l'origine d'un algorithme quantique d'échantillonnage de bosons ("boson sampling").

Les bosons sont les particules de spin entier comme les photons alors que les particules comme les électrons, les neutrons et les protons sont des fermions, avec un spin 1/2. Les bosons peuvent fonctionner en meute, comme les photons dans un laser, tandis que les fermions ne peuvent cohabiter au même endroit dans le même état.

Andrew Steane (1965, Anglais) est un professeur de physique de l'Université d'Oxford. Il est à l'origine de codes de correction d'erreurs quantiques qui portent son nom et qu'il a conçus en 1996.

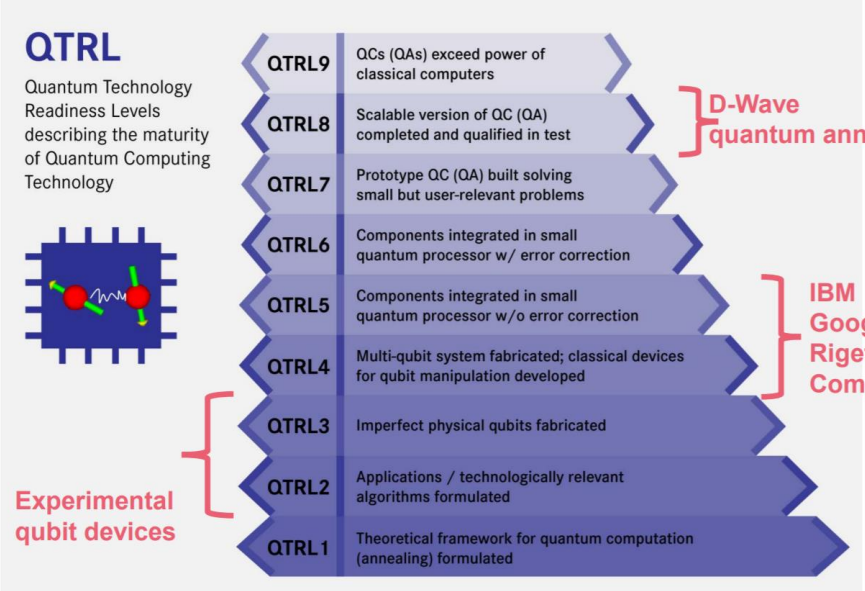
Alan Aspuru-Guzik (circa-1978, Américain) est un directeur de recherche de l'Université de Toronto, anciennement à Harvard, qui a notamment créé divers algorithmes de chimie quantique, un sujet que j'aborderais dans la partie consacrée aux algorithmes quantiques.

Mazyar Mirrahimi (circa 1980, Iranien) est un mathématicien qui a trempé dans la physique quantique. Il est actuellement directeur du laboratoire Quantic de l'Inria qui est spécialisé dans les codes de correction d'erreurs et les algorithmes quantiques entre autres sujets.

Shi Yaoyun (1976, Chinois) est professeur à l'Université du Michigan et aussi dirigeant du laboratoire quantique d'Alibaba. Il est à l'origine de divers records de simulation quantique sur des clusters de serveurs.

Kristel Michielsen (cica-1969, Belge) est une physicienne œuvrant à l'université d'Aix la Chapelle en Allemagne. Elle a contribué à de nombreux travaux en informatique quantique aussi bien côté physique que côté algorithmes. Elle est à l'origine de la création de l'échelle QTRL, pour Quantum Technology Readiness Level.

Celle-ci définit le niveau de maturité des technologies d'ordinateurs quantiques sur 9 niveaux (*ci-dessous*).



Dave Wecker (Américain) est un architecte en informatique quantique chez Microsoft. Il travaille notamment sur la conception d'algorithmes quantiques. On lui doit notamment la notion de "magic states", une technique de gestion de codes de corrections d'erreurs s'appuyant sur des états spécifiques descriptibles par leur position dans la sphère de Bloch (que nous verrons dans la partie sur les qubits)[40].

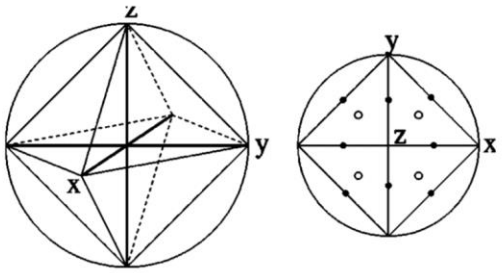


FIG. 1. Left: the Bloch sphere and the octahedron O. Right: the octahedron O projected on the $x-y$ plane. The magic states correspond to the intersections of the symmetry axes of O with the Bloch sphere. The empty and filled circles represent T-type and H-type magic states, respectively.

[40] Les Magic states sont décrits dans Universal quantum computation with ideal Clifford gates and noisy ancillas, 2005 (14 pages) de Sergey Bravyi et Alexei Kitaev.

John Watrous (Canadien) est un chercheur de l'Université de Waterloo au Canada spécialisé dans les algorithmes quantiques et les théories de la complexité. Il a déjà collaboré avec Scott Aaronson. Il est l'auteur du volumineux The Theory of Quantum Information, 2018 (598 pages).

Ryan Babbush (circa-1989, Américain) est un chercheur de Google spécialisé dans la création d'algorithmes de simulation de phénomènes physiques quantiques impossibles à simuler sur supercalculateurs. Il vise à créer des solutions commerciales de chimie quantique.

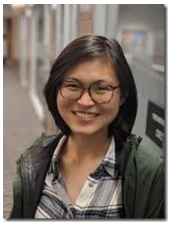
Matthias Troyer (1968, Autrichien) est professeur de physique computationnelle à l'ETH Zurich. Il a rejoint Microsoft Research à Redmond début 2017. Il est l'un des créateurs du langage Q# de programmation d'ordinateur quantique topologique. Il s'intéresse notamment à la simulation chimique avec des ordinateurs quantiques.

Iordanis Kerenidis (c. 1980, Grec) est un chercheur du laboratoire IRIF (Institut de Recherche en Informatique Fondamentale) du CNRS, spécialisé en cryptographie et communication quantique et dans les théories de la complexité quantique. Il est l'un des membres de la mission parlementaire sur le quantique pilotée par la députée Paula Forteza depuis avril 2019. Il fait aussi partie de l'équipe fondatrice de la startup américaine QCWare.

Benoît Valiron (1980**,** France) est un chercheur du laboratoire LIRI du CNRS et l'un des rares enseignants des algorithmes et de la programmation quantiques. Il officie à CentraleSupelec. Ce spécialiste de la programmation quantique est le co-auteur du langage Quipper alors qu'il était à University de Pennsylvanie.

Bettina Heim (c. 1980) est une dévelopeuse de Microsoft spécialisée en logiciels quantiques. Elle est responsable du développement du compilateur du langage de programmation quantique Q# dont Microsoft fait la promotion depuis 2017 et qui fait partie de leur Quantum Development Kit, pour l'instant tournant sur émulateurs quantiques sur processeurs traditionnels.

Christian Calude (1952, Roumain/Néo-Zélandais) et **Elena Calude** (Roumaine/Néo-Zélandaise) sont un couple de chercheurs de l'Institute of Information Sciences, de l'Université d'Albany à Auckland en Nouvelle Zélande. Ils sont spécialistes de l'algorithmie quantique, des algorithmes quantiques hybrides et des théories de la complexité.



Ewin Tang (2000, Américaine) a publié en juillet 2018 un papier démontrant un algorithme de recommandation classique aussi performant qu'un algorithme conçu pour les ordinateurs quantiques de D-Wave et conçu notamment par Iordanis Kerenidis en France[41]. Elle avait 18 ans à l'époque. Donc, à surveiller de près !

Sophia Economou (c. 1980, Gréco-Américaine) est une physicienne, professeure associée du Département de Physique du Virginia Tech College of Science. Elle travaillait auparavant à l'US Naval Research Laboratory. C'est une spécialiste du contrôle de spins de quantum dots semiconducteurs et de leurs interfaces spin-photons. Elle est aussi créatrice d'algorithmes avancés de simulation moléculaire sur ordinateurs quantiques.

Philippe Duluc (1961, Français) est CTO en charge du big data et de la cybersécurité chez Atos. Il pilote les efforts du groupe Atos dans l'informatique quantique. C'est un ingénieur de l'armement, issu donc de l'Ecole Polytechnique et de l'ENSTA. Il était initialement spécialisé dans la cybersécurité.

Cyril Allouche (Français), dirige les efforts de R&D en informatique quantique chez Atos depuis leurs débuts en 2015. Il est l'un des rares français dans les équipes européennes du Flagship Quantique de l'Union Européenne. Philippe Duluc et Cyril Allouche sont les "implémenteurs" de la vision quantique de Thierry Breton, le CEO d'Atos.

C'est l'un des rares industriels français du numérique à faire le pari de l'informatique quantique. Si ce n'est le seul !

Ça en fait du monde ! Nous croiserons une bonne part de ces personnages lors des parties suivantes de cet ebook au gré des thèmes abordés. Et des contributeurs plus jeunes, parfois de moins de 40 ans, s'ajouteront plus tard à cette liste pour faire avancer la discipline de l'informatique quantique qui ne fait que commencer à poindre du nez !

[41] Voir A quantum-inspired classical algorithm for recommendation systems, Ewin Tang, juillet 2018 (32 pages) et Major Quantum Computing Advance Made Obsolete by Teenager par Kevin Harnett, juillet 2018.

Basiques

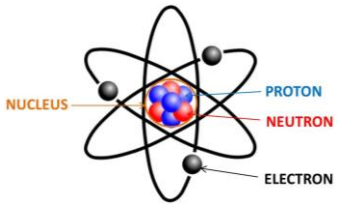
Après avoir fait le tour des plus grands contributeurs de la mécanique et de l'informatique quantique, passons aux grands fondamentaux de la physique quantique qui nous permettront de comprendre la suite et notamment le fonctionnement des qubits et de leurs diverses techniques de mise en œuvre.

Plusieurs années d'études sont nécessaires pour comprendre les arcanes de la mécanique quantique et ceux qui sont passés par là sont toujours dans l'interrogation à son sujet. Mais on peut se contenter de quelques basiques ici présents pour se préparer à comprendre le fonctionnement des calculateurs quantiques.

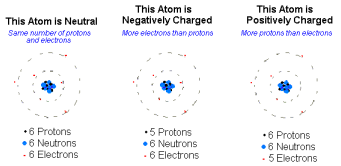
La mécanique quantique est apparue il y a un peu plus d'un siècle pour expliquer le fonctionnement et la dynamique des particules élémentaires. Les principales particules élémentaires à qui s'appliquent les principes de la mécanique quantique sont les **photons** et les **électrons**, mais cela concerne aussi les **atomes** soit neutres soit ionisés[42]. Les effets quantiques les plus connus se manifestent sur la phase des photons ainsi que sur les niveaux d'énergie ou les spins d'électrons, ces derniers étant liés en approximation à leur orientation magnétique.

la physique quantique s'intéresse aux particules de l'échelle atomique et sub-atomique

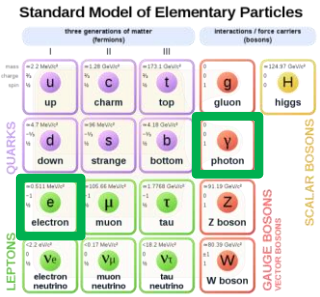
à cette échelle, la matière a des comportements qui ne correspondent pas aux observations « macro »

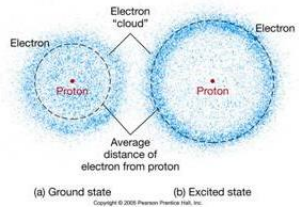


atomes

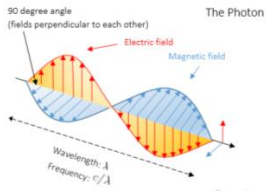


ions





électrons



photons

Le point essentiel est de bien appréhender la notion de **superposition d'états** qui est à la base du fonctionnement des qubits et de l'énorme capacité de traitement des calculateurs quantiques.

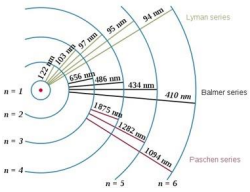
L'**intrication** vient juste après et permet d'expliquer comment fonctionnent les portes quantiques dans les calculateurs quantiques, que nous verrons dans la partie dédiée au fonctionnement de ces derniers.

[42] Pour mémoire, voici la dimension des particules élémentaires : 10^{-10} pour un atome, 10^{-15} pour le diamètre d'un noyau d'atome d'hydrogène, donc d'un proton unique et 10^{-18} pour celui d'un électron.

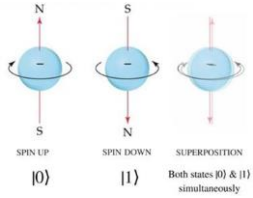
Tous les qubits connus d'ordinateurs quantiques s'appuient sur l'une de ces deux particules. A part le cas des qubits réalisés à base de photons, tous les autres sont à base de différents comportements quantiques d'électrons. C'est le cas des qubits à base de supraconducteurs à effet Josephson qui exploitent des effets très particuliers que nous expliquerons plus tard, reposant sur le comportement des électrons de matériaux supraconducteurs.

Les ions piégés, les cavités de diamants, les qubits CMOS et même les qubits à base d'anyons et des hypothétiques fermions de Majorana exploitent eux-aussi les effets quantiques des électrons.

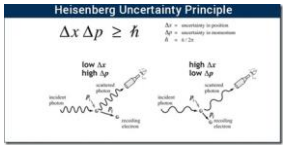
Des phénomènes quantiques peuvent se manifester avec d'autres particules élémentaires comme les atomes, les neutrons et les protons mais ce ne sont pas à ce jour des pistes explorées par les chercheurs dans le contexte du calcul quantique.



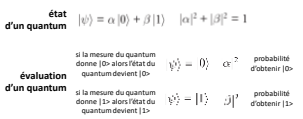
quantification



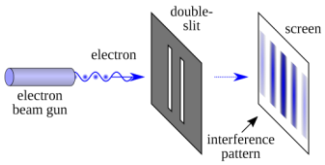
superposition d'états



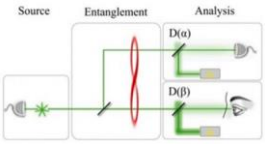
indétermination



réduction d'états

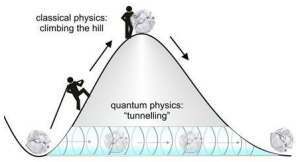


dualité onde-particule



intrication

non clonage

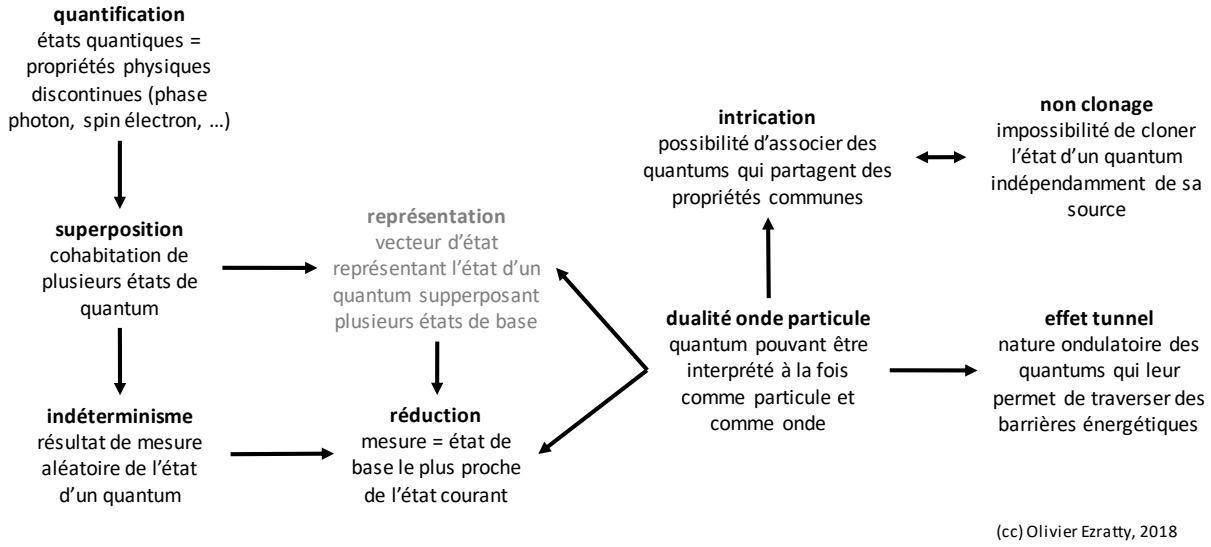


effet tunnel

Voici un petit schéma de mon cru qui connecte entre eux les principes de base de la physique quantique que nous allons explorer. Il fournit quelques relations de causalité entre ces différents principes. Ainsi, c'est la quantification des propriétés d'un quantum qui aboutit à leur superposition. Cette dernière entraine l'indéterminisme de la mesure de l'état d'un quantum et la notion de réduction.

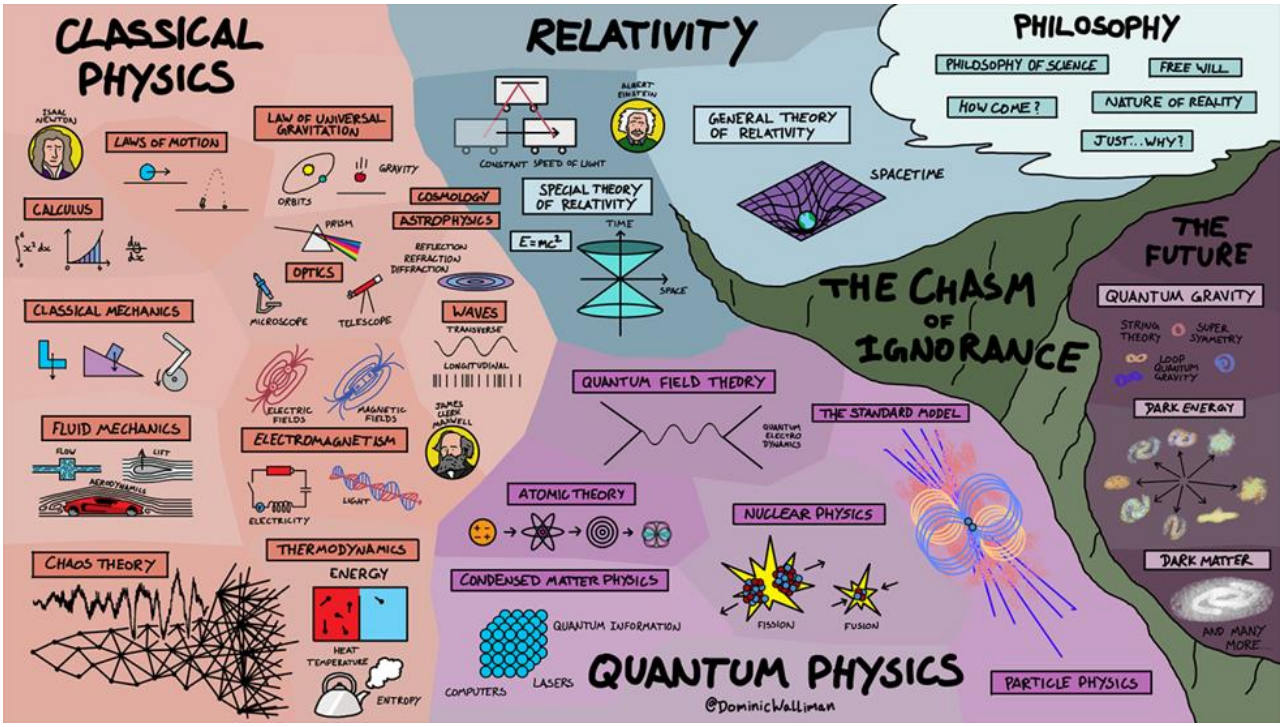
L'ensemble est représenté mathématiquement par un vecteur d'état qui contient deux nombres complexes, pour ce qui est des quantums à deux états possibles. Les propriétés mathématiques des vecteurs d'état s'expliquent par la dualité onde-particule des quantums et la possibilité d'additionner les ondes liées aux différents états des quantums. La dualité onde-particule est liée à la notion d'intrication qui elle-même explique le théorème de non clonage ainsi que l'effet tunnel. C'est peut-être approximatif mais permet de se faire une idée de l'architecture d'ensemble.

liaisons entre concepts de la physique quantique



J'ai ajouté deux champs à ce panorama, celui des supraconducteurs et de la superfluidité qui sont utilisés à différents endroits dans les ordinateurs quantiques (qubits supraconducteurs et connectique, réfrigération à dillution).

En parcourant de nombreux ouvrages sur la physique quantique et l'informatique quantique, j'ai pu constater que la pédagogie y était des plus variée. Le formalisme mathématique y prend rapidement le dessus de la description physique des phénomènes quantiques. Il est tellement prédominant qu'il ne correspond pas forcément à la réalité physique des quantums. Il est généralement très mal expliqué comme nous le verrons dans la partie suivante pour ce qui est du modèle de représentation de la sphère de Bloch.



source : https://dominicwalliman.com/post/153828312160/here-is-the-map-of-physics-as-an-image

Je vais toutefois essayer de vous épargner cela dans ce qui suit à la fois parce que c'est un véritable tonneau des Danaïdes et parce que cela perdrait une grande majorité de lecteurs. Et même avec ces précautions, rien ne dit que tous vont suivre. Dans la physique quantique, il faut avoir systématiquement l'humilité de reconnaître que l'on ne sera pas forcément compris et/ou que l'on s'est mal expliqué !

Voyons donc cela dans le détail !

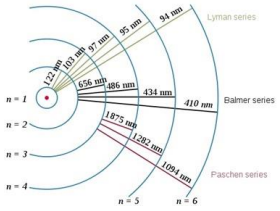
Quantification

En physique quantique, les quantums correspondent à des propriétés physiques de particules élémentaires matérielles ou immatérielles qui sont discontinues et non continues. Cela peut correspondre à des états énergétiques, des polarisations pour les photons, ou des orientations magnétiques pour les électrons.

Les orbites des électrons autour de noyaux d'atomes sont définies de manière discrète comme nous l'avons vu dans la partie précédente sur l'atome d'hydrogène avec les travaux de Max Planck en 1900, Albert Einstein en 1905 et Niels Bohr en 1913.

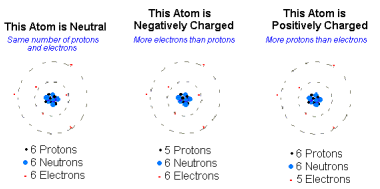
propriétés discontinues de la matière à l'échelle nanoscopique

notamment au niveau des états énergétiques



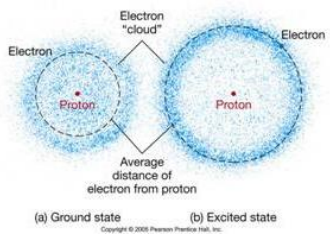
atomes

états énergétiques



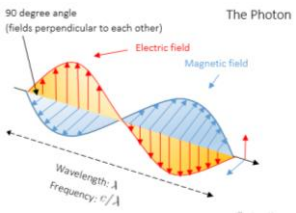
ions

niveaux d'excitation



électrons

spin magnétique (up, down)
caractéristiques de courants supraconducteurs



photons

polarisation (H, V),
fréquence, phase

concept : Ludwig Boltzmann, 1877
découverte : Max Planck, 1900

Il existe aussi une correspondance entre l'énergie des photons et les transitions énergétiques discontinues des électrons en orbite autour des atomes. Dans le calcul quantique, ce principe est utilisé un peu partout, surtout pour distinguer deux états clairement séparés dans les qubits.

Les qubits utilisés dans les calculateurs quantiques doivent s'appuyer sur des quantums qui n'ont que deux états possibles qui peuvent être à la fois initialisés, modifiés et ensuite mesurés. Même les qubits supraconducteurs s'appuient sur deux niveaux d'énergie clairement distincts du courant oscillant qui traverse leur isolant à effet Josephson.

Superposition

La superposition a un lien direct avec la quantification qui porte sur les différents états des particules élémentaires.

Les particules quantiques peuvent avoir plusieurs états simultanément, comme le sens de magnétisation du spin d'électron qui est orienté vers le haut ou vers le bas – cf schéma *ci-dessous* –, la polarisation linéaire des photons, qui est horizontale ou verticale après passage au travers de filtres polarisants, ou la fréquence ou l'énergie d'un courant oscillant dans un qubit supraconducteur.

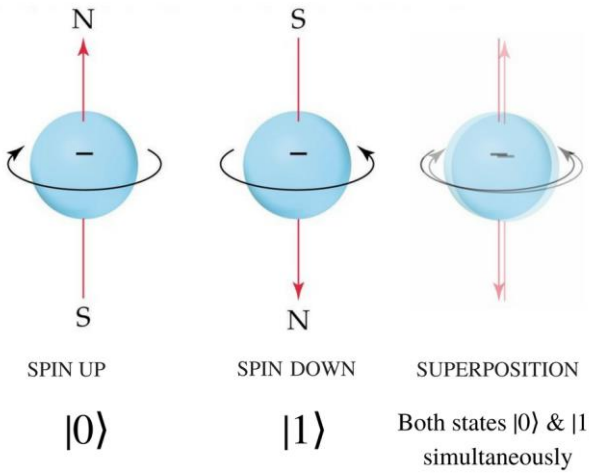
Le principe de la superposition veut qu'une particule élémentaire puisse être simultanément dans plusieurs de ces états quantiques. Dans une interprétation de physique classique, cela serait explicable par une fréquence très élevée des modifications d'états de ces particules. Elle est peut-être inexacte pour les spécialistes mais c'est un moyen intuitif de se représenter ce principe de la superposition.

les différents états
d'un quantum sont superposés

interprétation inexacte :
la matière « vibre » à haute fréquence
entre ces différents états

interprétation plus exacte :
superposition d'ondes

concept : Paul Dirac



En calcul quantique, ce principe est utilisé dans les qubits, leur permettant d'avoir en même temps la valeur 0 et 1 au lieu d'avoir seulement l'une des deux valeurs comme avec les bits traditionnels. C'est cela qui permet aux calculateurs quantiques de paralléliser les calculs à un niveau inégalé comparativement aux meilleurs supercalculateurs classiques. S'il n'y a qu'un élément de mécanique quantique à retenir pour comprendre les ordinateurs quantiques, c'est bien celui-ci !

Dualité ondes particules

Les particules élémentaires ont des comportements qui relèvent à la fois des particules avec une masse, une énergie et un mouvement et comme des ondes avec une fréquence et une longueur d'onde, et des effets d'interférences et le fait qu'elles peuvent s'additionner pour donner d'autres ondes. Un peu comme les couleurs (photons) et les sons (ondes acoustiques) se mélangent.

Diverses expériences comme celle des doubles fentes de Young montrent que les électrons qui sont des particules matérielles avec une masse se comportent à la fois comme des particules et comme des ondes, générant des interférences. Les équations de Planck, Einstein et Bohr donnent la correspondance entre photons et états énergétiques d'atomes liés à la position orbitale des électrons.

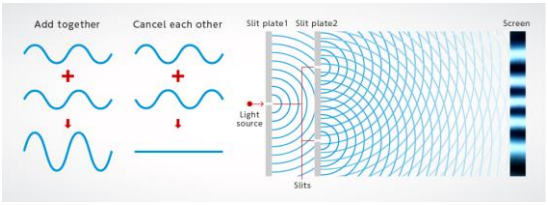
une particule physique comme un électron ou un atome peut se comporter à la fois comme de la matière (avec une masse)
ou une onde (avec des interférences)

c'est vérifié dans l'expérience des fentes de Young avec un faisceau d'électrons

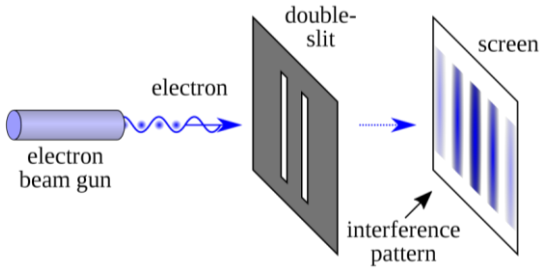
mais aussi avec des atomes et même des molécules de grande taille

concept : Louis de Broglie, 1924.

validation : George Paget Thomson, Clinton Davisson et Lester Germer, 1927.



phénomène d'annulation d'ondes avec des photons



même phénomène observé avec des électrons

La dualité ondes/particules est utilisée dans nombre d'ordinateurs quantiques pour faire interagir des qubits physiques comme des ions piégés avec de l'énergie sous forme de photons émis par des lasers. Les qubits peuvent aussi interférer les uns avec les autres en reproduisant une partie de ce mécanisme d'interférence ondulatoire.

Cette dualité ondes-particules explique aussi pourquoi le formalisme mathématique de la physique quantique s'appuie sur des vecteurs qui peuvent s'additionner comme des ondes.

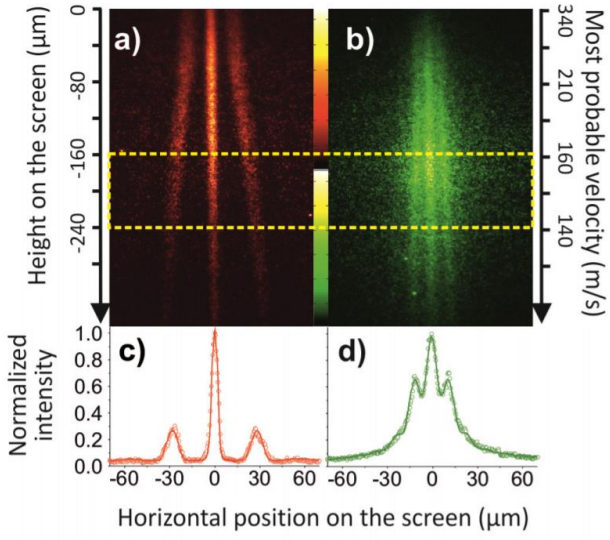
On comprend donc que les électrons ont cette capacité à se comporter comme des particules et comme des ondes.

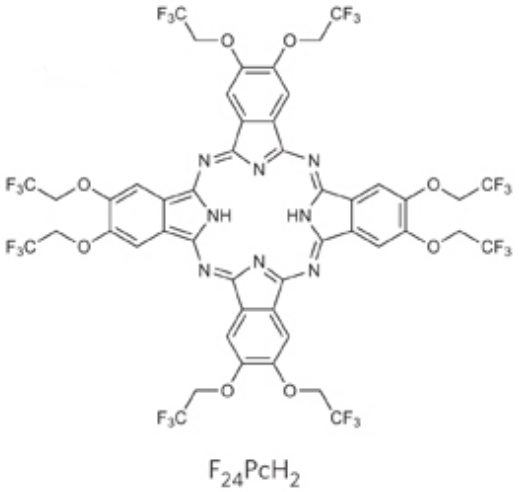
La dualité onde-particule a été vérifiée avec des atomes en 1991 dans des expériences d'interférométrie comprenant des lasers et des optiques classiques.

L'expérience des fentes de Young a même été réalisée en Autriche en 2012 sur des molécules de 58 et 114 atomes, cette dernière dénommée $F_{24}PcH_2$ faites de fluor, carbone, oxygène, hydrogène et azote[43]. Voir l'illustration *ci-dessous* avec la forme de la molécule.

Mais qu'en est-il des photons ? Ils peuvent se comporter dans certaines conditions comme des particules. Lorsqu'ils atteignent un atome, ils peuvent ainsi lui transmettre un mouvement cinétique.

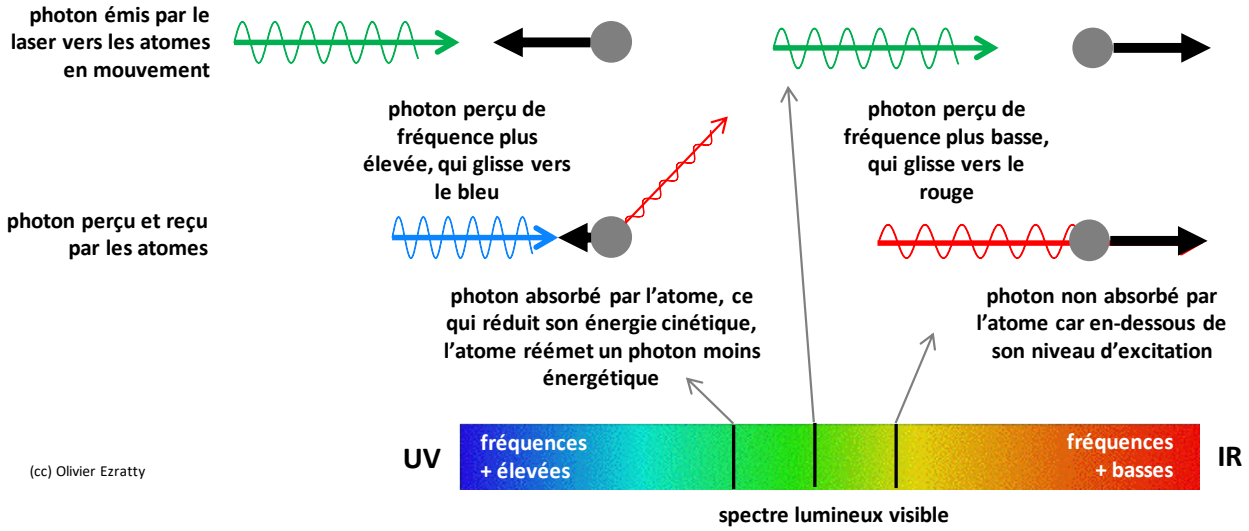
[43] Voir Real-time single-molecule imaging of quantum interference par Thomas Juffmann & Al, 2012 (16 pages). Voir également la vidéo de l'expérience. Highly Fluorinated Model Compounds for Matter-Wave Interferometry de Jens Tüxen, 2012 (242 pges) décrit pour sa part le dispositif expérimental de vérification de la dualité onde-matière de grandes molécules.





C'est ce qui permet de générer un phénomène physique un peu contre-intuitif : le refroidissement d'atomes avec des lasers. La température est liée au mouvement des atomes dans leur milieu gazeux, liquide ou solide. Baisser la température revient à ralentir le mouvement des atomes.

On utilise l'effet Doppler pour ce faire. On éclaire les atomes en mouvement avec un laser dont la fréquence est positionnée juste en-dessous du niveau d'aborption d'énergie des atomes en question.



Ceux des atomes qui se déplacent vers la lumière vont absorber les photons, car la fréquence apparente des photons est plus élevée et génère une énergie légèrement supérieure au niveau d'absorbtion. Cela réduit l'énergie cinétique des atomes en question. Ceux qui se déplacent dans l'autre direction ne les absorberont pas car la fréquence apparente du photon incident est trop faible pour changer l'état énergétique des atomes. Grâce au mouvement aléatoire des atomes dans toutes les directions, au bout d'un certain temps, la température d'ensemble baisse. Magique !

Ces techniques sont utilisées pour refroidir des atomes à des températures voisines du zéro absolu[44]. Elles sont notamment employées pour préparer des « atomes froids » utilisés dans certains types d'ordinateurs quantiques.

Réduction

La réduction explique dans le détail la nature de l'indéterminisme de la mesure de l'état des quantums.

Lorsque l'on mesure un état d'un quantum, celui-ci est affecté par la mesure. La mesure change l'état du quantum. Celui-ci se rabat en quelque sorte sur l'état de base le plus proche de son état avant la mesure et que l'on appelle un "observable".

L'état "pur" avant la mesure est une combinaison d'états de base du quantum. Par exemple, une combinaison de polarisation verticale et horizontale pour un photon.

On appelle aussi cela "*l'écrasement de la fonction d'onde de Schrödinger*" (ou « effondrement »). Pourquoi donc ? Parce que qu'un quantum multi-états superpose plusieurs états distincts qui sont représentés chacun par une fonction d'onde. L'état composite de deux fonctions d'ondes est aussi une fonction d'onde. Lorsque l'on mesure l'état d'un tel quantum, c'est l'état de base le plus proche des états superposés qui est détecté. Cet état mesuré devient l'état du quantum qui vient d'être mesuré. Etat qui est associé à une fonction d'onde, celle qui est obtenue par écrasement ! Vous suivez ? Non ? C'est normal, ne vous inquiétez pas.

Prenons l'exemple d'un photon de polarité intermédiaire entre la polarité horizontale ou verticale, ou de polarisation circulaire. Il va devenir un photon polarisé horizontalement ou verticalement après sa mesure de polarité.

La notion de réduction est une application pratique du fameux principe d'Heisenberg selon lequel la mesure de l'état d'un quantum influe sur la grandeur à mesurer dans l'infiniment petit, alors que ce n'est pas le cas dans la mécanique newtonienne classique.

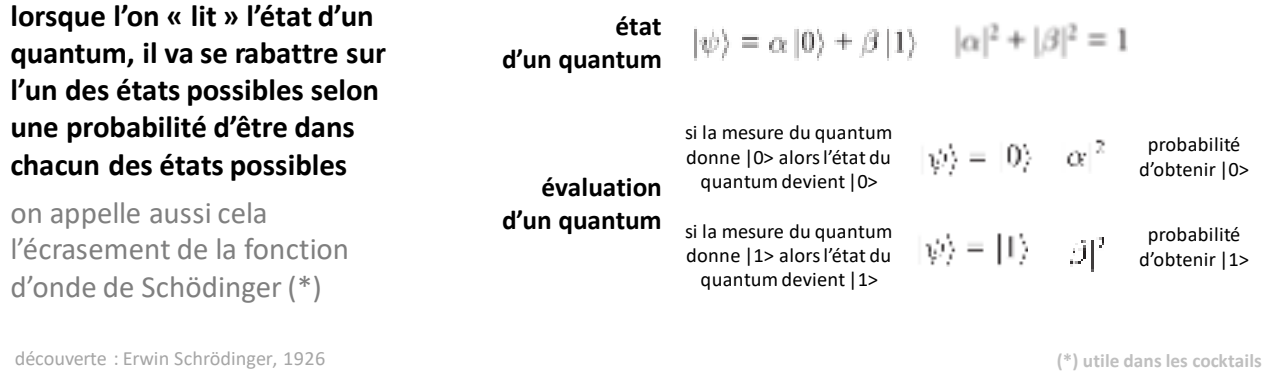
Le principe d'indétermination d'Heisenberg dit précisément que l'on ne peut pas mesurer à la fois la position et la vitesse d'une particule élémentaire. Intuitivement, cela se comprend : en mécanique newtonienne, l'outil de mesure est en général plus petit que la grandeur à mesurer, comme pour évaluer la vitesse des astres et des planètes.

Dans l'infiniment petit, l'outil de mesure est habituellement bien plus grand que la grandeur physique à mesurer. D'où la perturbation sur la grandeur à mesurer !

Pour les puristes, la notion de vitesse et de position des particules n'a pas de sens, pour ce qui est par exemple d'un électron. Sa caractérisation passe par sa nature ondulatoire et par sa description via la fonction d'onde de Schrödinger.

[44] Source de l'illustration : https://sites.ualberta.ca/~ljleblan/background/laser-cooling.html.

En informatique quantique, ce principe de réduction est en œuvre lors de la mesure de l'état d'un qubit, qui modifie sa valeur en la rabattant à 0 ou 1. Le 0 et le 1 mesuré est, en gros, la valeur la plus proche de son état quantique du moment qui est une combinaison de 0 et de 1.



C'est illustré dans le schéma *ci-dessus*. Nous reviendrons sur la signification de α et β dans la partie suivante sur les qubits, ces deux variables étant en fait des nombres complexes.

La subtile information contenue dans un qubit qui est représentée par un nombre complexe ou un vecteur à deux dimensions est réduite à 0 ou 1 au moment de sa mesure. Mathématiquement, on a donc bien une réduction d'une information riche comportant l'équivalent de deux nombres flottants à un simple bit !

Cette réduction intervient au dernier moment après les calculs. Pendant ces derniers, les qubits sont modifiés par des portes quantiques qui conservent la richesse de leur information et la combinatoire de leurs valeurs liée à la superposition.

Indétermination

Le principe de l'indétermination d'Heisenberg veut que l'on ne peut pas mesurer avec précision à la fois la position et la vitesse d'une particule élémentaire ou deux grandeurs complémentaires. Au même titre, on ne peut pas observer en même temps une particule élémentaire dans son état particule et dans son état ondulatoire, un principe édicté par Niels Bohr ver 1928.

Il intervient lors de la mesure de l'état d'un quantum. Le résultat est en partie aléatoire. La mesure de la polarisation d'un photon va donner des résultats différents d'un coup à l'autre dans une proportion de phases qui dépend de son état quantique. Si les photons évalués ont suivi un processus de transformation identique, en réalisant un grand nombre de mesures, on va obtenir une proportion donnée de phases horizontales et verticales.

Si la mesure donne un résultat aléatoire, la proportion des états évalués ne l'est pas pour autant. Réalisée plusieurs fois, elle va converger tangentiellement vers une proportion qui dépend des conditions de préparation d'un quantum. Si on prend l'exemple de photons polarisés à 45°, leur mesure de polarisation verticale et horizontale va converger vers une proportion de 50%/50%.

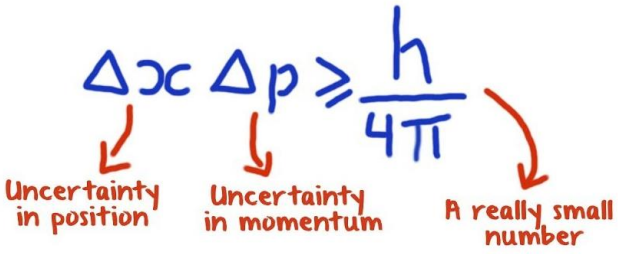
à l'échelle nanoscopique, on ne peut pas mesurer à la fois la vitesse et la position d'une particule

version dérivée : à l'échelle nanoscopique, l'outil de mesure influe sur la grandeur à mesurer

…

ça marche aussi dans les sondages !

découverte : Werner Heisenberg, 1926



Si les photons mesurés sont polarisés à seulement 5°, la proportion de photons évalués comme étant polarisés verticalement (0°) sera plus grande que celle de deux qui sont polarisés horizontalement.

En informatique quantique, ce principe est utilisé lorsque l'on mesure le résultat d'un calcul en évaluant l'état des qubits de l'ordinateur quantique. Dans les ordinateurs à recuit quantique de D-Wave, on va généralement réaliser cette mesure plusieurs fois pour obtenir une moyenne de 0 et de 1, en exécutant à chaque fois une réinitialisation complète du système et un calcul complet.

La recherche de 0 ou de 1 déterministes ou de proportion probabiliste de 0 et 1 donnant une moyenne va dépendre des algorithmes utilisés. C'est un peu l'analogue en informatique traditionnelle de calculs générant un résultat booléen (0 ou 1) ou un nombre flottant (ici, compris entre 0 et 1).

Intrication

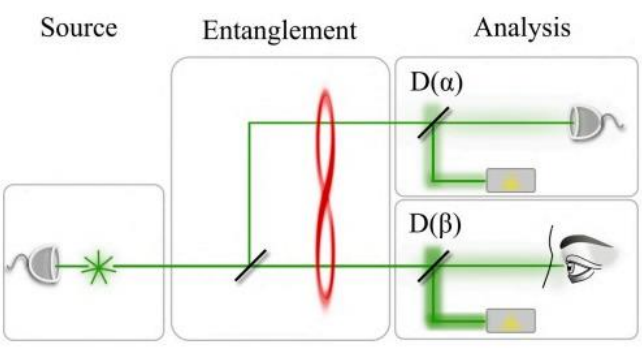
Des quantums peuvent être intriqués, à savoir qu'ils peuvent avoir la même fonction d'onde ou représentation quantique alors qu'ils sont distants. Donc, être dans un état quantique similaire, sans être pour autant strictement identique, ne serait-ce qu'au niveau de leur localisation spatiale. C'est le principe de la non localité des propriétés quantiques de quantums intriqués qui perturbait Einstein en 1935. L'intrication est dénommée "entanglement" en anglais.

deux particules peuvent être dépendantes l'une de l'autre et à distance, si on modifie l'état de l'une, cela modifiera instantanément l'état de l'autre, et plus vite que la lumière

vérifié sur des photons en 1982 par l'expérience d'Alain Aspect et Philippe Grangier

mais on ne peut pas l'utiliser pour transmettre une information plus vite que la lumière !

vérification : Alain Aspect et Philippe Grangier, 1982



Ainsi, avec une paire de quantums intriqués, une mesure effectuée sur un quantum aura instantanément un effet sur l'autre quantum, sans attendre un délai de transmission d'information à la vitesse de la lumière entre les deux quantums. C'est le principe de la "non localité" des propriétés quantiques.

Les particules intriquées ne sont pas liées par hasard. Elles ont généralement un passé commun. Par exemple, deux photons intriqués sont le résultat du passage d'un seul photon dans un miroir dichroïque qui les sépare en deux photons de polarisations orthogonales. L'action sur l'un des deux photons a un impact sur l'autre photon comme l'a démontré Alain Aspect dans sa fameuse expérience réalisée en 1982. Une expérience de 2019 menée à l'Université de Glasgow a même permis de photographier une représentation de l'état de photons intriqués[45].

En informatique quantique, ce principe est utilisé dans les portes quantiques à deux ou trois qubits, pour les relier entre eux. Une fois intriqués, les qubits ont le même état quantique indissociable. Cette intrication est associée à une impossibilité de dissocier les quantums ainsi intriqués.

Dans la science à la frontière de la science-fiction, certains imaginent exploiter l'intrication quantique pour analyser l'état de l'intérieur d'un trou noir[46] !

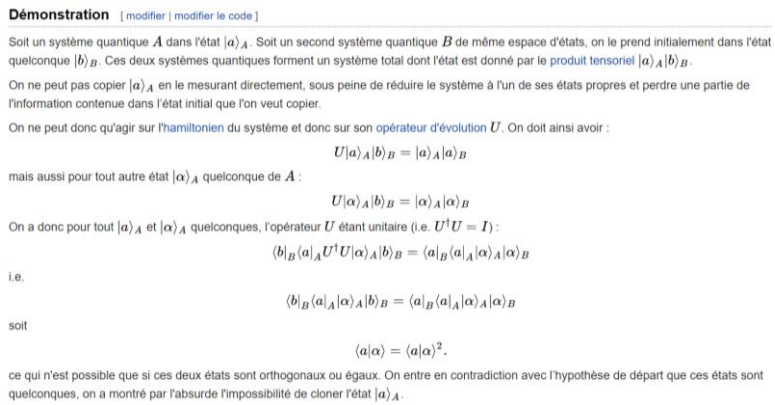
Non clonage

Le théorème d'impossibilité du clonage quantique a été énoncé en 1982 dans un article publié dans Nature par William Wootters, Wojciech Hubert Zurek et Dennis Dieks. L'article n'est toujours pas disponible en open source sur un site tel qu'Arxiv, s'auto-appliquant le principe du non clonage ! Mais une version résumée est consultable ici (*ci-dessous*).

l'état d'un quantum
ne peut pas être dupliqué
à l'identique
dans un autre quantum

c'est démontrable
mathématiquement par l'absurde

découverte : James Park en 1970
puis William Wooters et Wojciech Zurek en 1982.



Démonstration [modifier | modifier le code]

Soit un système quantique A dans l'état $|a\rangle_A$. Soit un second système quantique B de même espace d'états, on le prend initialement dans l'état quelconque $|b\rangle_B$. Ces deux systèmes quantiques forment un système total dont l'état est donné par le produit tensoriel $|a\rangle_A|b\rangle_B$.

On ne peut pas copier $|a\rangle_A$ en le mesurant directement, sous peine de réduire le système à l'un de ses états propres et perdre une partie de l'information contenue dans l'état initial que l'on veut copier.

On ne peut donc qu'agir sur l'hamiltonien du système et donc sur son opérateur d'évolution U. On doit ainsi avoir :

$$U|a\rangle_A|b\rangle_B = |a\rangle_A|a\rangle_B$$

mais aussi pour tout autre état $|\alpha\rangle_A$ quelconque de A :

$$U|\alpha\rangle_A|b\rangle_B = |\alpha\rangle_A|\alpha\rangle_B$$

On a donc pour tout $|a\rangle_A$ et $|\alpha\rangle_A$ quelconques, l'opérateur U étant unitaire (i.e. $U^\dagger U = I$) :

$$\langle b|_B\langle a|_A U^\dagger U|\alpha\rangle_A|b\rangle_B = \langle a|_B\langle a|_A|\alpha\rangle_A|\alpha\rangle_B$$

i.e.

$$\langle b|_B\langle a|_A|\alpha\rangle_A|b\rangle_B = \langle a|_B\langle a|_A|\alpha\rangle_A|\alpha\rangle_B$$

soit

$$\langle a|\alpha\rangle = \langle a|\alpha\rangle^2.$$

ce qui n'est possible que si ces deux états sont orthogonaux ou égaux. On entre en contradiction avec l'hypothèse de départ que ces états sont quelconques, on a montré par l'absurde l'impossibilité de cloner l'état $|a\rangle_A$.

Il interdit la copie à l'identique de l'état d'un quantum. Le théorème se démontre mathématiquement en six lignes (*ci-dessus*) même si chaque mot de la démonstration nécessite quelques recherches préalables pour être compris ! Je la refais page 94.

Il a comme conséquence qu'il est impossible de copier l'état d'un qubits pour l'exploiter indépendamment de son original.

---

[45] Voir Scientists unveil the first-ever image of quantum entanglement, juillet 2019… par le chercheur français Paul-Antoine Moreau.

[46] Voir Can entangled qubits be used to probe black holes?, de Robert Sanders, 2019.

Dans les ordinateurs quantiques, on peut bien dupliquer des qubits via des portes quantiques et l'intrication, mais les qubits résultants sont intriqués et donc en quelque sorte synchronisés. La lecture de la copie détruit l'original par projection de l'état des deux qubits sur le 0 ou le 1 le plus proche de leur état initial.

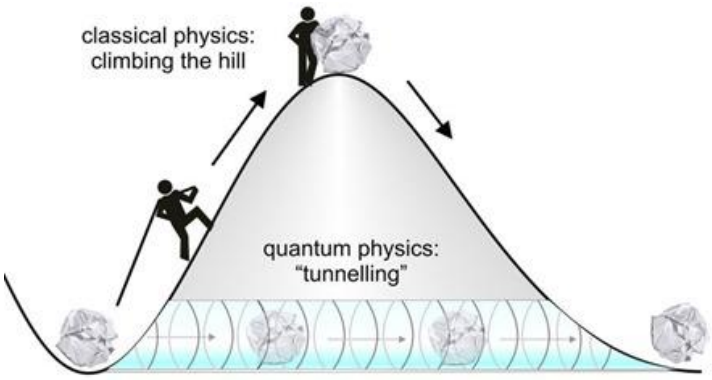
Cela a un impact direct sur la conception d'algorithmes quantiques et notamment sur les codes de correction d'erreurs des ordinateurs quantiques. Heureusement, ces codes de correction d'erreurs ne nécessitent pas de lire le contenu des qubits clonés et échappent donc aux foudres du théorème de non-clonage.

Effet tunnel

La double nature corpusculaire et ondulatoire de la matière lui permet de traverser des obstacles. Ces obstacles peuvent être des "murs énergétiques". Le phénomène a été découvert en 1927 par le physician allemande Friedrich Hund (1896-1997).

la double nature corpusculaire et ondulatoire de la matière lui permet de traverser des obstacles. Ces obstacles peuvent être des "murs énergétiques".

le principe est utilisé dans les ordinateurs « à recuit quantique » de D-Wave pour trouver le minimum énergétique d'un système complexe (dit « hamiltonien »)



Ce phénomène est utilisé dans les ordinateurs à recruit quantique de D:Wave qui permettent de faire converger un système multi-qubits ("hamiltonien") vers un minimum énergétique correspondant à la résolution d'un problème de combinatoire complexe ou de recherche de minimum énergétique comme en chimie ou en biologie moléculaire.

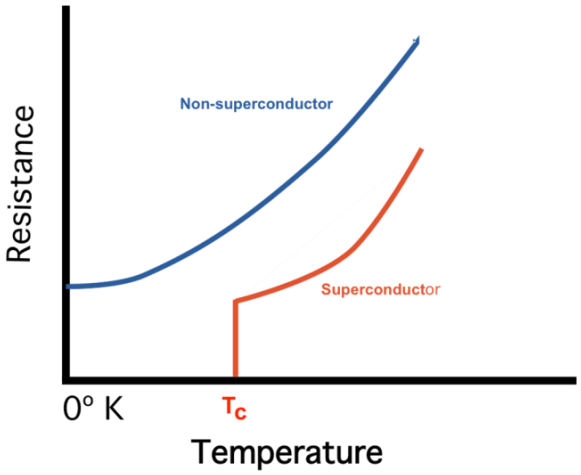
Supraconductivité

Le phénomène de la supraconductivité a été découvert expérimentalement en 1911 avec du mercure à 4,2K par Heike Kamerlingh Onnes, Cornelis Dorsman, Gerrit Jan Flim et Gilles Holst à l'Université de Leiden aux Pays-Bas. Notons le faux ami en anglais : la supraconductivité devient *superconductivity*.

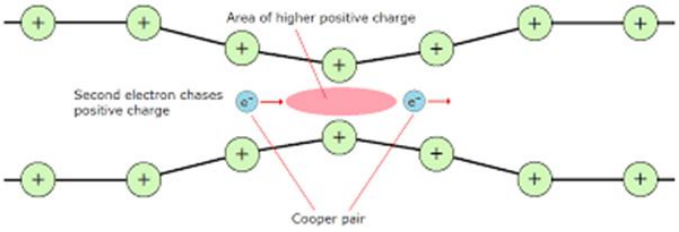
Son interprétation n'a été formulée qu'en 1957 par John Bardeen[47], Leon Neil Cooper et John Robert Schrieffer de l'Université de l'Illinois, qui ont bâti ce que l'on appelle la théorie BCS[48].

[47] John Bardeen est détenteur de deux prix Nobel de physique, l'un en 1956 pour l'invention du transistor avec h William Shockley et Walter Brattain et l'autre pour l'interprétation de la supraconductivité en 1972 avec Leon Neil Cooper et John Robert Schrieffer. Cooper a cocréé la théorie BCS à 27 ans et a obtenu le prix Nobel correspondant à 42 ans. Né en 1930, il est toujours de ce monde.

La supraconductivité se manifeste lorsque l'on baisse la température de certains matériaux. A partir d'un certain niveau, ils n'opposent plus de résistance au courant électrique. Dans la conductivité habituelle, les électrons se balladent d'atomes en atomes et, ce faisant, transforment une partie de leur énergie cinétique en chaleur, liée au mouvement des atomes. En supraconductivité, les électrons s'arrangent en paires, dites de Cooper, qui circulent entre les atomes et sans friction.

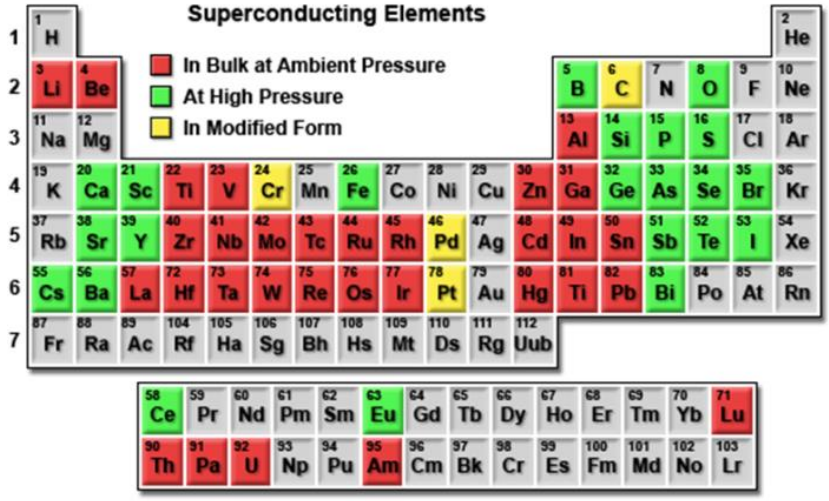


La structure des atomes du métal conducteur est aussi modifiée. Il se produit des ondulations des atomes qui suivent et accompagnent le mouvement des paires de Cooper. On appelle cela des phonons[49].



Les paires de Cooper sont des électrons de spins opposés. C'est notamment là que la mécanique quantique intervient pour expliquer la supraconductivité. Le fonctionnement des électrons dans ces paires est formalisé par leur fonction d'onde. Tout le formalisme mathématique associé est celui de la mécanique quantique. Heike Kamerlingh Onnes a aussi découvert qu'un champ magnétique dont le niveau dépend de la température pouvait faire disparaître l'effet supraconducteur.

Une cinquantaine d'éléments sont supraconducteurs à basse température mais le seuil de la supraconductivité en température et pression est très variable. La supraconductivité est aussi possible avec des matériaux composites comme des alliages de germanium, de titane et de niobium ou à base de cuivre (les cuprates).



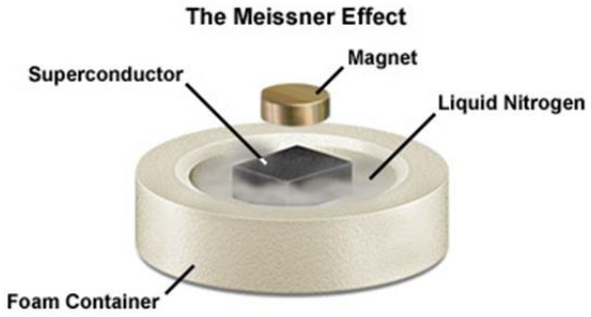
[48] Une timeline précise de la découverte du principe de la supraconductivité est fournie dans la présentation 50 Years of BCS Theory "A Family Tree" Ancestors BCS Descendants, de Douglas James Scalapino, John Rowell et Gordon Baym, 2007 (52 slides). Voir aussi l'excellent ouvrage The rise of superconductors de P.J. Ford et G.A. Saunders 2005 (224 pages) qui raconte bien l'histoire de la découverte puis de l'interprétation de la supraconductivité.

[49] Source de l'illustration : Superconducting properties of ZrNi2-xTMxGa (TM = Cu, Co) and ZrNi2AlxGa1-x Heusler Compounds (77 pages). Lien supprimé car site générant une détection dans l'antivirus Avast.

C'est notamment le cas de l'aluminium et du mercure. Dans la pratique, un alliage de niobium et de titane est le plus souvent utilisé[50]. On le retrouvera plus loin dans les câbles supraconducteurs de lecture de l'état de qubits supraconducteurs à effet Josephson.

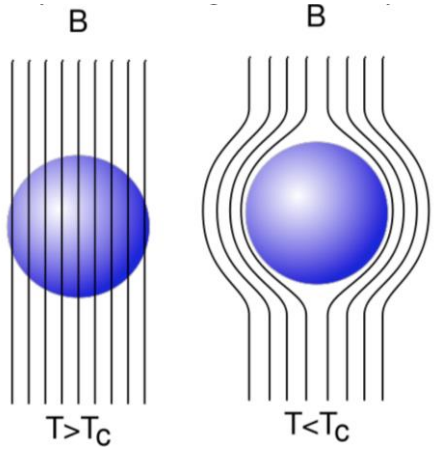
L'effet supraconducteur est maximum pour les atomes qui ont un grand nombre d'électrons de valence, à savoir dans la dernière couche orbitale et de nombre quantique le plus élevé.

La supaconductivité explique des phénomènes inattendus comme la lévitation d'aimant au-dessus de supraconducteurs plongés dans le l'azote liquide.

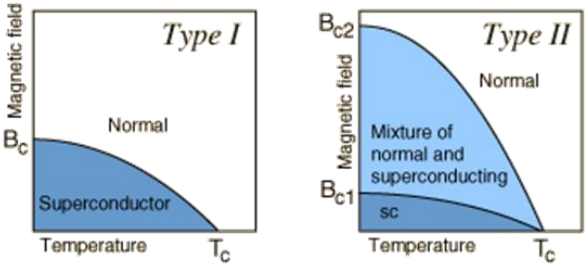


Des céramiques supraconductrices, découvertes à partir de 1986 peuvent être utilisées dans cette expérience saisissante[51].

Le champs magnétique est alors expulsé de l'intérieur du matériau supraconducteur. C'est l'effet Meissner, découvert en 1933 par Walther Meissner, qui ne s'applique qu'à certains supraconducteurs dits de type I. Il explique la répulsion démontrée dans de nombreuses expériences. Le type II qui ne génère pas ce phénomène comprend les alliages de niobium titane qui sont fréquemment utilisés avec un ratio 1 pour 1 de chaque dans l'alliage.



Dans les supraconducteurs de type II, il existe une phase intermédiaire entre la phase métallique classique et la phase supraconductrice qui laisse passer le champs magnétique partiellement[52].



Le Graal de la supraconductivité serait de l'obtenir à température ambiante, permettant par exemple de réduire les pertes en ligne du transport de l'électricité.

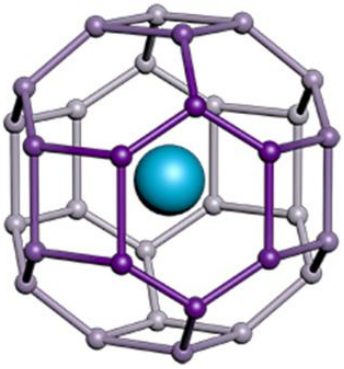
---

[50] Voir Superconductivity 101. Les propriétés supraconductrices de l'alliage niobium-titane ont été découvertes en 1962. Celui-ci est très utilisé dans le refroidissement des scanners IRM mais aussi dans de nombreux instruments scientifiques, notamment dans le réacteur expérimental de fusion nucléaire ITER de Caradache.

[51] Les céramiques supraconductrices à haute température ont été découvertes en 1986 par Georg Bednorz et Alex Müller, combinant du lanthanium, du barium du cuivre et de l'oxygène, et supraconductrices à 30K, un record pour l'époque. Cela leur a valu le Prix Nobel en 1987, un délai très rapide après leur découverte.

[52] Source de l'illustration.

Les scientifiques ont commencé à découvrir des alliages métalliques supraconducteurs au-dessus de 77K à la fin des années 1980, soit la température de l'azote liquide. La plupart sont des cuprates (à base de cuivre). Un record a été obtenu en 2019 avec une molécule associant du lanthanium et de l'hydrogène et à 17°C, donc une température ambiante. Dans ce dernier cas, cela ne fonctionne toutefois qu'à une pression énorme de 170 gigapascals, soit 1,7 millions de fois la pression atmosphérique qui est de 101 325 pascals[53][54].



Ce n'est donc pas très pratique ! D'où les projets d'utilisation de simulateurs ou ordinateurs quantiques pour faire jouer les équations de la supraconductivité et identifier des matériaux qui seraient supraconducteurs à température ambiante ou presque ambiante.

La supraconductivité est couramment utilisée dans les **scanners IRM**[55]. Ceux-ci exploitent des aimants géants supraconducteurs qui sont redroidis à l'hélium liquide. Les scanners sont enrobés d'une protection pour contenir le magnétisme à l'intérieur du scanner. Le câblage de bobines y est réalisé en niobium-titane et est intégré dans une matrice de cuivre. C'est le même alliage que celui des fils supraconducteurs qui servent à lire l'état des qubits supraconducteurs.

source de l'illustration à droite : Helium Reclaim in Magnetic Resonance Imagers de Dan Hazen, MKS Instruments (5 pages).

On retrouve la supraconductivité dans un nouveau train à grande vitesse maglev **Chuo Shinkansen** expérimenté au Japon depuis 2013 et dont la vitesse commerciale doit atteindre 505 km/h.

---

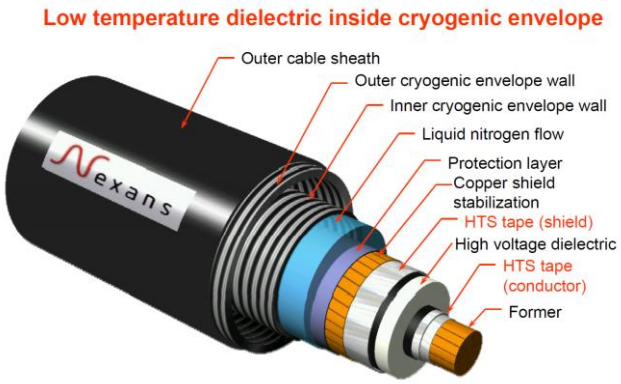
[53] Voir "Superhydride" shows superconductivity at record-warm temperature, mai 2019.

[54] Un record de pression a été obtenu avec un alliage de niobium-titane, avec 261,7 GPa. A cette pression, la température limite de la supraconductivité est passée de 10K à 19,1K. Voir Record-High Superconductivity in Niobium-Titanium Alloy de Jing Guo & Al, 2016 (14 pages).

[55] Imagerie à résonance magnétique nucléaire.

Il utilise une suspension magnétique qui exploite la supraconductivité. Cela entraîne des infrastructures hors de prix. La consommation électrique au passager/kilomètre est du triple des Shinkansen traditionnels mais compétitive face aux avions. La démonstration est intéressante mais ce genre de moyen de transport n'a pas forcément vocation à se répandre. Une ligne Tokyo-Nagoya de 286 km doit ouvrir en 2027.

Des câbles supraconducteurs ont été lancés pour transmettre de l'électricité sans perte d'énergie et avec une plus grande capacité permettant de répondre à la demande qui est en augmentation constante. Ils sont notamment proposés par le fabricant français de câbles Nexans qui en a installé un à Long Island.



Leur câble sous-terrain de 600 m est en opération depuis 2008. Il permet d'alimenter 300 000 foyers en électricité[56]. Mais c'est complexe à mettre en œuvre. Le projet a couté en tout $46,9M.

Pour ce qui concerne les ordinateurs quantiques, la supraconductivité est utilisée en particulier dans les qubits supraconducteurs qui utilisent l'effet Josephson qui nous avons déjà décrit dans une partie précédente.

La supraconductivité pourrait aussi servir à créer des processeurs CMOS fonctionnant à basse température et capables d'opérer jusqu'à 100 GHz, doit vingt-cinq fois plus rapidement que les processeurs serveurs actuels (3 à 4 GHz maximum chez AMD et Intel)[57]. Une équipe du MIT communiquait en juillet 2019 sur une proposition de technique de création de neurones artificielles à impulsion (spiking neurons) avec des circuits supraconducteurs à effet Josephson exploitant des nanofils[58]. Reste à créer un prototype pour tester tout cela ! Ces différentes recherches menées depuis deux décennies ne semblent pas avoir encore abouti commercialement.

Enfin, une quantité impressionnante d'aimants supraconducteurs à haute puissance sont utilisés dans les accélérateurs de particules comme le **LHC** du CERN à Genève. Il y en a sur plus de 21 km de long ! La supraconductivité permet de créer un courant de 11 850 ampères générant un puissant champ magnétique de 8,33 tesla qui créé une force centripète maintenant les particules accélérées dans le grand cercle de l'accélérateur. Ces aimants sont refroidis par 10 000 tonnes d'hélium 4 superfluide à 1,9K. Leurs câbles sont constitués de filaments de niobium-titane entourés de cuivre. Le tout consomme 40MW. C'est le frigo le plus grand et le plus puissant du monde !

---

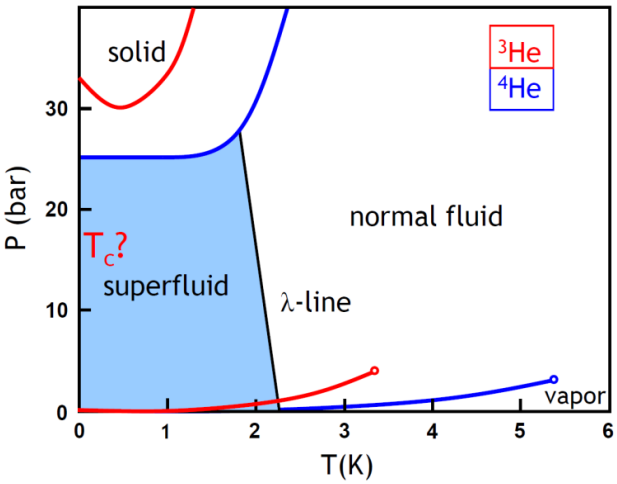
[56] Source de l'information : Long Island HTS Power Cable, Department of Energy, 2008 (2 pages). En plus de Nexans, le système de cryogénie a été fourni par Air Liquide.

[57] Voir Superconductor ICs: the 100-GHz second generation par Darren Brock, Elie Track et John Rowell d'Hypress, 2000 (7 pages).

[58] Voir A Power Efficient Artificial Neuron Using Superconducting Nanowires par Emily Toomey, Ken Segall et Karl Berggren, 2019 (17 pages).

Superfluidité

Un dernier phénomène qui relève de la mécanique quantique reste à décrire, celui de la superfluidité. Il se manifeste avec l'hélium superfluide qui, à pression ambiante, ne gèle jamais, aussi basse soit la température.

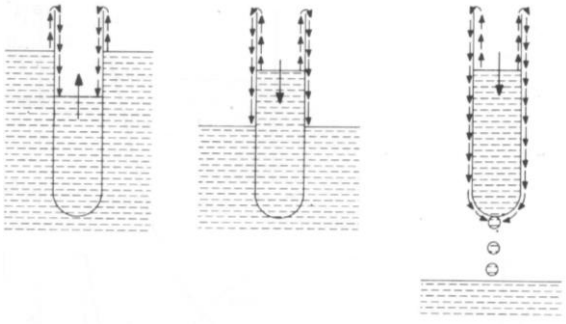


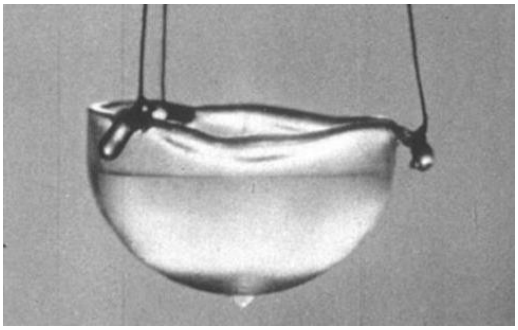
Lorsque l'on en verse dans un vase, il a tendance à remonter par capillarité sur le bord du vase et à s'écouler à l'extérieur de celui-ci. Il peut même traverser des capillaires très fins[59].

Ce sont des propriétés physiques très utiles pour la réfrigération cryogénique, en particulier pour descendre à des températures inférieures à 1K.

L'hélium a été liquéfié pour la première fois en 1908 et à 4,2K par Heike Kamerlingh Onnes, le découvreur de la supraconductivité en 1911. Sa superfluidité a été mise en evidence indépendamment en 1938 par Piotr Kapitsa (URSS) et Joan F. Allen et Don Misener (USA)[60].

Il existe deux isotopes de l'hélium : l'hélium 3 avec un seul neutron, le moins courant, et l'hélium 4 avec deux neutrons, le plus abondant. Ce dernier est un boson, de spin entier, ce qui lui donne des propriétés différentes de l'hélium 3 qui est un fermion avec un spin demi-entier. A basse température, l'hélium 3 se comporte comme des condensats de Bose-Einstein, qui sont des gaz et pas des liquides.





Il devient superfluide à plus basse température que l'hélium 4, soit 1 mK en l'absence d'un champ magnétique (cf le diagramme *ci-dessus*), vs 2,17K pour l'hélium 4. Sa superfluidité n'a été découverte qu'en 1973.

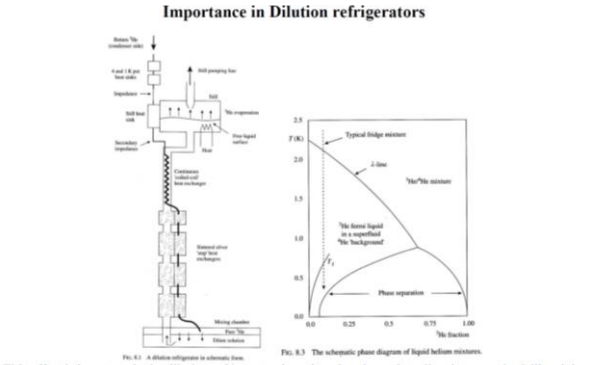
Ce sont les différentes propriétés de l'hélium 3 et 4 qui servent à faire fonctionner les systèmes de cryogénie à dillusion qui équipent nombre d'ordinateurs quantiques dont la température opérationnelle est située entre 10mK et 20mK.

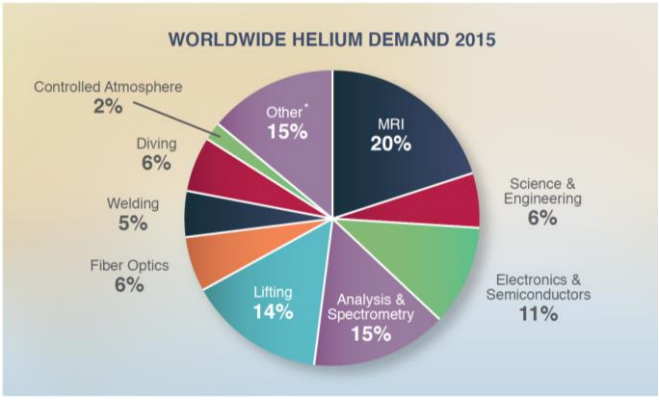
---

[59] Source du schéma : Helium 4 (14 slides).

[60] Voir Viscosity of Liquid Helium below the λ-Point, P. Kapitsa, Nature 74, 141 (1938) et Flow of liquid helium II, Joan F. Allen, Don Misener, 1938 (pages). Pyotr Kapitsa a obtenu le prix Nobel en 1978 pour ses travaux dans le domaine des basses températures.

La demande industrielle d'hélium est répartie dans de nombreux secteurs d'activité. Le premier est l'imagerie médicale. Le second correspond aux industries micro-électroniques dont font partie celles de l'informatique quantique.





source du schéma à droite : Intelligas Consulting.

Applications du quantique

Cet ebook est très focalisé sur les calculateurs quantiques mais ce n'est pas la seule application nouvelle de la mécanique quantique.

On compte au moins quatre autres grands domaines dans ce vaste secteur :

- La **cryptographie quantique** qui est un moyen de diffusion de clés quantiques inviolables grâce au principe de l'intrication entre photons, et qui repose soit sur des communications par fibre optique, soit en liaison spatiale avec des satellites comme le font les Chinois avec le satellite Micius depuis 2017. Nous traitons du sujet dans une partie dédiée à partir de la page 339. Il faut la distinguer de la **cryptographie post-quantique** qui est destinée à remplacer les solutions actuelles de cryptographie pour les rendre résistantes aux attaques réalisées avec l'algorithme de Shor tournant dans des ordinateurs quantiques. Nous nous y intéresserons à partir de la page 348.
- Les **télécommunications quantiques** qui permettent, grâce à l'intrication quantique de photons ayant un passé commun, de communiquer à distance et instantanément l'état de quantums. C'est un cas plus général que la cryptographie quantique qui en est un cas particulier. C'est un domaine en devenir car pour l'instant, on peut certes envoyer une information très rapidement, mais pas l'exploiter directement. En particulier, l'information a beau être transmise instantanément, donc plus vite que la lumière, on ne peut pas pour autant exploiter cette bizarrerie dans la transmissions d'informations classiques[61].

[61] Mais… « *Les états intriqués ne peuvent pas être utilisés pour communiquer d'un point à un autre de l'espace-temps plus vite que la lumière. En effet, les états de ces deux particules sont seulement coordonnés et ne permettent pas de transmettre une information : le résultat de la mesure relatif à la première particule est toujours aléatoire. Ceci est valable dans le cas des états intriqués comme dans le cas des états non-intriqués. La modification de l'état de l'autre particule, pour instantanée qu'elle soit, conduit à un résultat tout aussi aléatoire. Les corrélations entre les deux mesures ne pourront être détectées qu'une fois les résultats comparés, ce qui implique nécessairement un échange d'information classique, respectueux de la relativité. La mécanique quantique respecte ainsi le principe de causalité* ». Source : https://fr.wikipedia.org/wiki/Intrication_quantique.

Cela peut cependant servir pour distribuer des traitements quantiques sur plusieurs processeurs quantiques et notamment pour le « blind computing » que nous évoquons aussi à différents endroits dans cet ebook.

- La **métrologie quantique**, qui permet de mesurer des ordres de grandeur de l'infiniment petit avec une très grande précision. C'est un vaste domaine scientifique qui fait l'objet de nombreux travaux de recherche et à la commercialisation de solutions industrielles. Cela comprend les horloges atomiques ultra précises à atomes[62] ou ions froids comme celles de SCPTime qui fonctionne au césium, les accéléromètres et gyromètres à atomes froids qui utilisent de l'interférométrie atomique, les gravimètres qui en sont une variante pour mesurer la gravité avec précision, que fabrique notamment le Français Muquans qui est basé à Bordeaux[63] ou les magnétomètres à base de cavités de diamants comme ceux de Thales. Ce sont des marchés de taille modeste. Une nouvelle rubrique de cet ebook est consacrée à la métrologie à partir de la page 368.

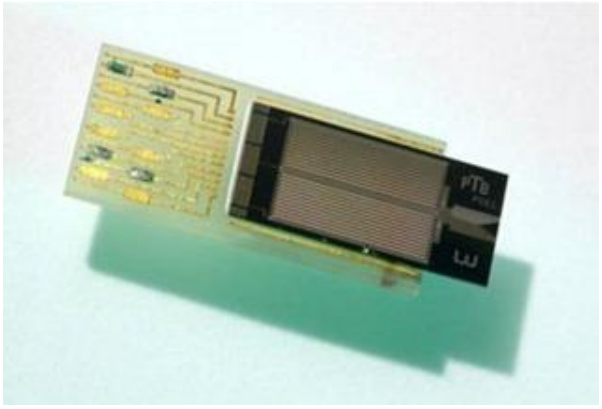


Table 1. Quantum Metrology and Sensing Technologies

Technology	Technological Readiness[a]	Potential Market
Measurement		
Atomic clocks	Commercial	$50–$500 million
Meters for voltage, current, and resistance	Commercial	—
Sensors		
Gravimeters and other atomic interferometers	Commercial	< $50 million
Quantum inertial motion units	Medium-term	$50–$500 million
Atomic magnetometers	Commercial	$50–$500 million
Magnetoencephalography	Commercial	$50–$500 million
Quantum electron microscopes	Medium-term	$50–$500 million
Quantum-assisted nuclear spin imaging	Long-term	< $50 million
Signal measurement	Medium-term	—

Sources: European Commission (2017) United States Air Force Scientific Advisory Board 2015; interviews.

- L'**imagerie médicale quantique** qui exploite diverses techniques dont les quantum dots, que l'on trouve aussi dans les écrans LCD pour améliorer leur colorimétrie. L'imagerie quantique peut aussi prendre des chemins de traverse au propre et au figuré pour voir au travers des obstacles [64]! On peut cependant considérer que l'imagerie médicale quantique est un sous-domaine de la métrologie quantique.

---

[62] Voir par exemple ces travaux du NIST sur une horloge atomique à base de rubidium, l'élément le plus fréquemment utilisé dans les horloges atomiques. NIST Team Demonstrates Heart Of Next-Generation Chip-Scale Atomic Clock, mai 2019.

[63] La startup **Muquans** employait 29 personnes en mai 2019 et qui faisait 2,9M€ en 2018. Ils développent un gravimètre quantique qui sert par exemple à la détection de cavités pour le BTP, la prospection pétrolière et la surveillance de volcans comme pour l'Etna en Italie. Le produit s'appelle **Absolute Quantum Gravimeter**. Le système exploite des atomes froids (rubidium) éclairés et refroidis à 1 µK par laser dans 6 directions et piégés magnétiquement sous vide. Le système mesure avec une grande précision la chute gravitationnelle du nuage d'atome. Un système à base de fluorescence et de laser mesure la vitesse de la chute et le fait dans la durée pour évaluer sa variation temporelle. Ils participent aux projets du flasgship européen **Quantum Internet Alliance** pour créer un matériel d'extension de la portée des systèmes de QKD et **Pasquans** dans la simulation quantique à atomes froids. La société a été crée en 2011.

[64] Voir Quantum camera snaps objects it cannot 'see', par Belle Dume, mai 2018. C'est une variante de Diffraction Free Light Source for Ghost Imaging of Objects Viewed Through Obscuring Media par Ronald Meyers, 2010 (22 pages). Yanhua Shih (Université de Maryland) US Army Research Laboratory, travaille depuis 2005 sur le sujet. Quantum Imaging de Yanhua Shih, 2007 (25 pages). Quantum Imaging – UMBC (47 slides).

Qubits

On peut comprendre le fonctionnement d'un ordinateur quantique sans trop se plonger dans la mécanique quantique au-delà de la compréhension de ses mécanismes de base, vus dans dans la partie précédente, et surtout celui de l'intrication. Par contre, il faut se plonger un peu dans quelques éléments de mathématiques, d'algèbre linéaire et de trigonométrie, ce que nous allons commencer à faire ici.

Le premier élément de base d'un ordinateur quantique est l'inévitable qubit. Vous avez certainement déjà entendu parler de cet objet mystérieux capable d'être simultanément dans la valeur 0 et 1. Les explications courantes s'arrêtent le plus souvent là et vous tombez immédiatement dans l'expectative, vous demandant comment cela peut ensuite bien fonctionner.

Nous allons donc commencer ici par expliquer le fonctionnement logique, mathématique et matériel de ces qubits[65]. Dans la partie suivante de cette série d'articles, nous irons plus loin en décrivant tour à tour les registres, les portes, l'organisation et l'architecture complète d'un ordinateur quantique en nous appuyant sur l'exemple courant des ordinateurs quantiques à qubits supraconducteurs. A chaque fois, lorsque nécessaire, nous ferons le parallèle avec les ordinateurs traditionnels.

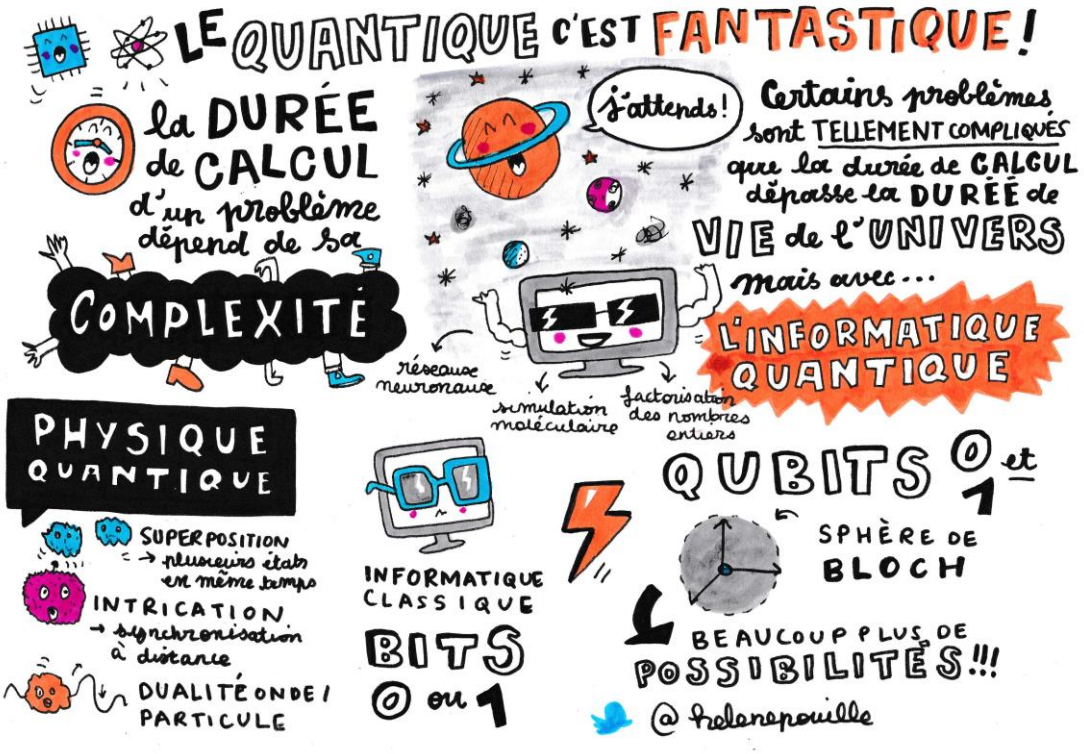


Illustration de la conférence "Le quantique, c'est fantastique" du 14 juin 2018 à Nantes au Web2day par Hélène Pouille, voir son site et la vidéo de la conférence.

[65] L'appellation qubit, fusion de quantique et bit, est apparue en 1995 dans Quantum coding de Benjamin Schumacher, avril 1995 (34 pages).

Pour pouvoir suivre cette partie, il faut connaître quelques basiques mathématiques : la trigonométrie, les vecteurs et matrices et avoir déjà entendu parler des nombres complexes.

Principe des qubits

Les qubits sont les éléments de manipulation de base de l'information dans les ordinateurs quantiques. Ils s'opposent aux bits de l'informatique traditionnelle. Avec eux, on passe d'un monde déterministe à un monde probabiliste.

Dans l'informatique traditionnelle, les bits correspondent à des charges électriques circulantes qui traduisent le passage d'un courant électrique ou son absence. Un bit est de valeur 1 si le courant passe soit de 0 si le courant ne passe pas. La lecture d'un bit donne 1 ou 0. Elle est déterministe, à savoir que si l'on répète l'opération de lecture plusieurs fois, ou l'opération de lecture après une réédition du calcul, on obtiendra normalement le même résultat.

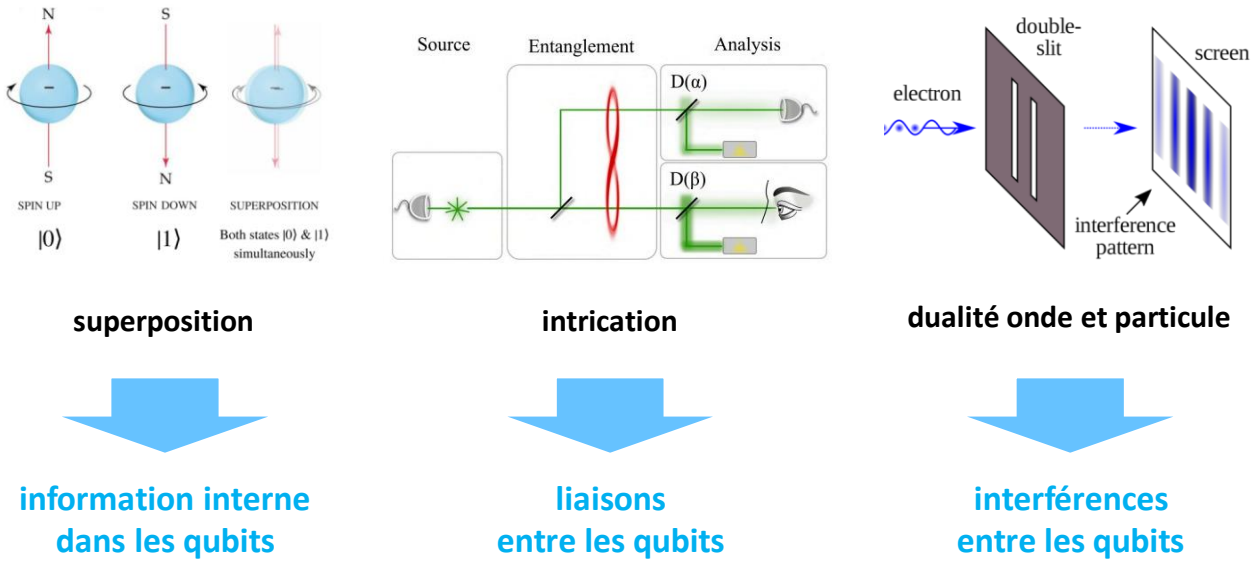
C'est vrai aussi bien pour le stockage de l'information que pour son transport et pour les traitements dans des processeurs. Ceci est valable modulo les erreurs qui peuvent intervenir dans le parcours. Celles-ci interviennent le plus souvent au niveau de la mémoire et sont corrigées via des systèmes… de correction d'erreurs utilisant de la redondance.

	bits : 0 ou 1	**qubits : 0 et 1**
états	deux états possibles exclusifs	deux états possibles simultanés
initialisation	0 ou 1	0
représentation interne	0 ou 1	vecteur à deux dimensions
dimensionnalité interne	1 binary digit	un flottant et un complexe
modifications	portes logiques	portes quantiques
lecture	0 ou 1, déterministe	0 ou 1, probabiliste

Dans un qubit, rien à voir ! Si les qubits sont généralement initialisés à 0, les opérations portant dessus vont généralement les amener à avoir un état de superposition entre 0 et 1. Ces états correspondent à l'état de base "(“ground state”) et à l'état excité (“excited state”) d'un système quantique à deux états possibles. Ces qubits peuvent donc être à la fois à la valeur 0 et 1, et dans une proportion qui est variable et qui correspond à la notion de superposition d'états évoquée dans la partie précédente sur les fondements de la mécanique quantique. A la fin des calculs, lorsque l'on lit la valeur d'un qubit, on retrouve 0 ou 1. La richesse des valeurs du qubits se manifeste donc uniquement pendant les calculs et non pas à leur initialisation où lors de leur lecture à la fin des calculs. C'est un concept que vous ne comprendrez complètement que lorsque nous aurons décrit quelques algorithmes quantiques lors d'une partie suivante de cette série.

Voici en résumé les trois principes de base les plus importants sur les huit de la partie précédente qui sont utilisés dans les qubits :

- La **superposition** permet d'avoir des qubits qui sont à la fois dans un état 0 et 1 et nous verrons plus tard dans quelle proportion et comment on la représente mathématiquement. C'est elle qui apporte une bonne part de la puissance de calcul des ordinateurs quantiques.
- L'**intrication** permet de relier entre eux les qubits pour les synchroniser, mais sans pouvoir en lire leur contenu ni les modifier de manière indépendante ni les copier. Elle est mise en œuvre dans les ordinateurs quantiques à portes universelles par le biais des portes quantiques à deux qubits.
- La **dualité onde-particule** permet d'interagir dans certains cas avec les qubits ou de faire interagir les qubits entre eux par interférences dans le cadre d'algorithmes quantiques. C'est une des manières de générer des résultats dans des algorithmes quantiques.



Ici, nous allons d'abord creuser le modèle mathématique de représentation des qubits et comprendre comment on peut se le représenter physiquement et mentalement.

Nous ferons alors un tour des différents types de qubits physiques. Les modèles mathématiques de représentation des qubits ne dépendent pas de leur type physique. Seules les caractéristiques de l'ordinateur sont affectées comme le taux d'erreur et la nature des portes quantiques physiques de base dites "universelles" agissant sur les qubits sachant que toutes les portes quantiques sont exécutables sur les ordinateurs quantiques.

Les qubits ne sont pas les seules manières de gérer de l'information quantique. Des ordinateurs quantiques peuvent être construits à partir de qudits (d = nombre d'états quantiques possibles) ou de qutrits (trois états possibles).

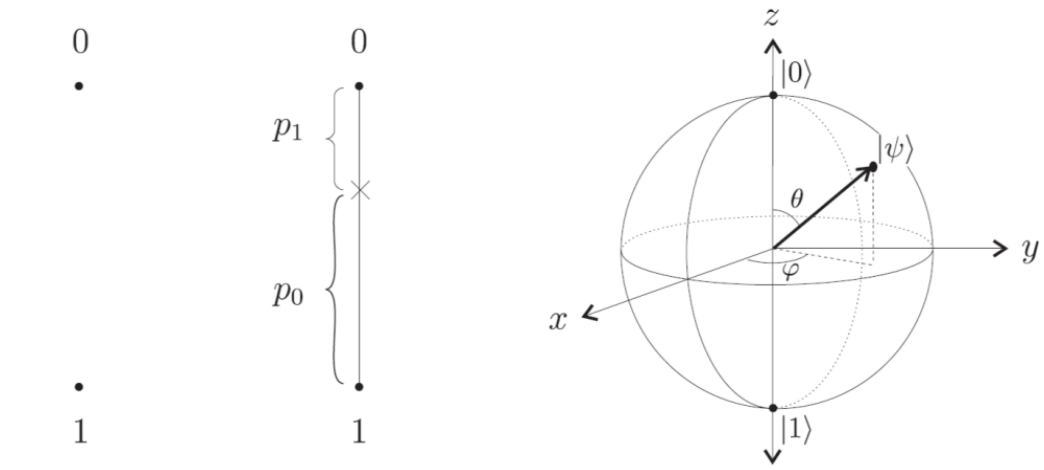
Cela reste cependant des objets de recherche théorique et de laboratoires. Je ne connais pas de projet d'ordinateurs commerciaux basés sur ces types d'objets quantiques qui, d'ailleurs, reposent sur des objets quantiques différents de ceux qui sont exploités pour créer des qubits. Par ailleurs, ils auraient un impact sur la conception d'algorithmes quantique. La plupart des algorithmes sont conçus pour des ordinateurs quantiques à portes universelles à base de qubits.

Sphère de Bloch

Dans un modèle probabiliste classique, un pbit ou bit probabiliste aurait une probabilité p d'avoir la valeur 0 et 1-p d'avoir la valeur 1. Ce serait un modèle probabiliste linéaire.

Dans un qubit, c'est bien différent !

Le modèle de représentation mathématique de l'état d'un qubit s'appuie sur la fameuse **sphère de Bloch**, qui m'a donné bien du fil à retordre en termes de compréhension. Mais j'en suis venu à peu près à bout.

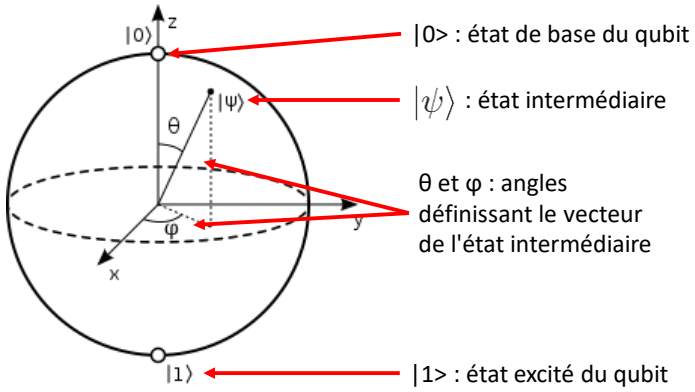


Je vais partager avec vous ce que j'ai pu en comprendre après des mois de recherche dans des dizaines de cours, articles scientifiques et livres sur le calcul quantique.

Ce modèle est lié à la représentation de l'état d'un qubit ou de tout quantum à deux états par un vecteur à deux dimensions dont la longueur dite "norme" est toujours de 1. Ce vecteur a la particularité de comporter deux éléments : un nombre réel (alpha) et un nombre complexe (beta). On pourrait s'amuser à utiliser des quantums ayant plus que deux états, mais ce n'est pas ce qui a été retenu par les physiciens du calcul quantique sauf rares exceptions.

Dans la sphère de Bloch, l'état |0> d'un quantum à deux états est figuré par la position d'un vecteur de longueur 1 allant du centre de la sphère vers le pôle Nord de la sphère et l'état |1> est un vecteur allant du centre de la sphère à son pôle Sud.

Les états intermédiaires sont représentés par des vecteurs partant du centre de la sphère qui sont toujours de longueur 1 avec un angle θ par rapport à la verticale z et un angle φ par rapport à l'axe x situé allant du centre de la sphère à son équateur et autour de l'axe z.



Histoire de simplifier les choses, les états |0> et |1> qui sont opposés dans la sphère de Bloch sont dits "orthogonaux" alors qu'ils sont opposés dans la sphère. Nous allons rapidement comprendre pourquoi.

Règle de Max Born

Les équations décrivant l'état d'un qubit indiquent que celui-ci est la superposition de l'état |0> et de l'état |1>.

Dans les équations, α est un nombre réel dont le carré décrit la probabilité d'obtenir l'état |0> et β est un nombre complexe dont le carré décrit celle d'avoir l'état |1>.

La somme des probabilités des deux états doit donner 1. Ce n'est effectivement pas $\alpha + \beta$ mais $\alpha^2 + \beta^2$ qui donnent 1. Pourquoi donc ? La réponse est loin d'être triviale, d'autant plus que sa traçabilité est assez complexe à reconstituer.

Ce modèle probabiliste a été élaboré par **Max Born** en 1926. Il donne au carré du module de la fonction d'onde d'un quantum la signification d'une densité de probabilité de présence d'une particule élémentaire. C'est lié au fait que l'état |0> et l'état |1> correspondent non pas à une position précise d'une particule mais sont représentés par la fonction d'onde de **Schrödinger** qui décrit la distribution probabiliste de l'état du quantum dans le temps et dans l'espace. Elle est ici appliquée dans l'espace.

L'état d'un qubit est représenté par un vecteur à deux dimensions dans un espace dit de Hilbert, ce qui est une information bien plus riche qu'un 0 ou un 1 d'un simple bit ou même qu'une probabilité linéaire entre 0 et 1. Ce vecteur à deux dimensions comprend les deux composantes α et β que nous venons de définir.

amplitude de l'état 0 — amplitude de l'état 1

état du qubit → $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

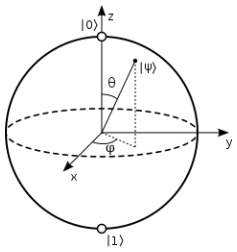
$|\alpha|^2 + |\beta|^2 = 1$

relation entre alpha et beta selon la règle de **Max Born**, liée à la fonction d'onde de **Schrödinger** qui définit les états |0> et |1>

ket de ψ

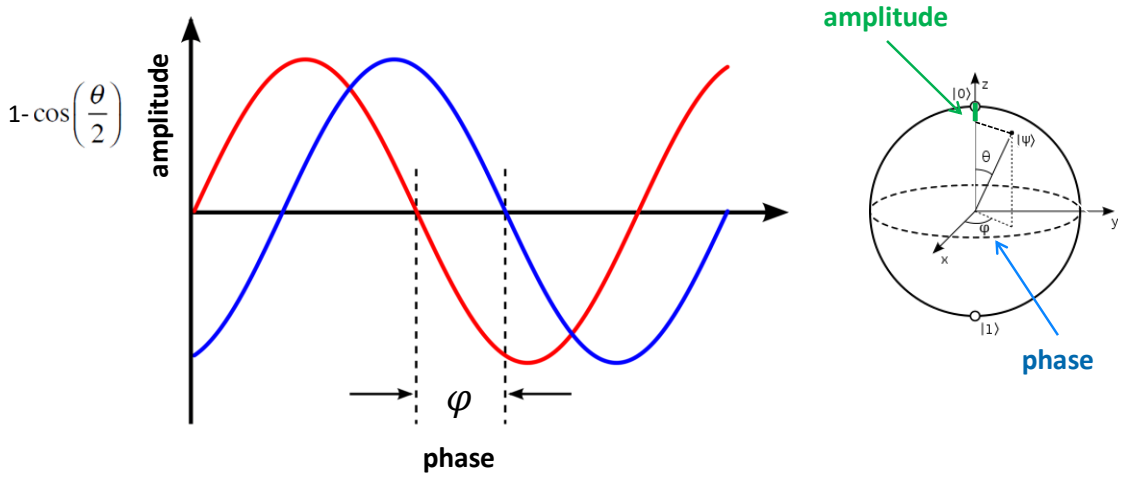
$$|\psi\rangle = \begin{bmatrix} \alpha \rightarrow \cos\left(\frac{\theta}{2}\right) \\ \beta \rightarrow e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$e^{i\varphi} = \cos\varphi + i\sin\varphi$

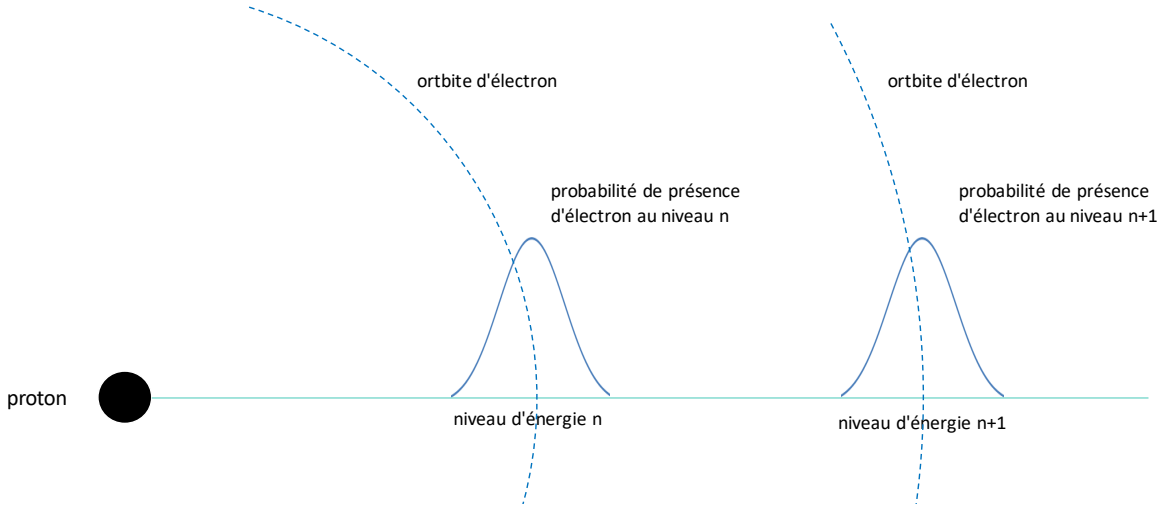


formule d'**Euler** qui fait correspondre l'exponentielle de $i\varphi$ à un nombre complexe avec un cosinus et un sinus du même angle φ

Le passage de la fonction d'onde de Schrödinger à la représentation α/β du qubit avec un nombre réel et un nombre complexe est liée à la nature ondulatoire des quantum. La partie complexe (β) intègre en fait la phase de l'onde du quantum tandis que sa partie réelle (α) représente son amplitude.



Voici une autre explication. Si on prend par exemple deux orbites possibles d'un électron autour du noyau d'un atome dans un modèle d'hydrogène simple (il en existe plein…), la fonction d'onde de l'orbite basse dans l'espace sera une sorte de courbe de Gauss décalée de celle de l'orbite haute. La probabilité d'avoir l'électron dans l'orbite haute ou basse est proportionnelle à l'intégrale des fonctions d'onde correspondantes à ces orbites. D'où le carré qui serait une approximation de la valeur du pic de la gaussienne, à supposer que ce pic corresponde à la taille des vecteurs alpha et beta de représentation des états des qubits.



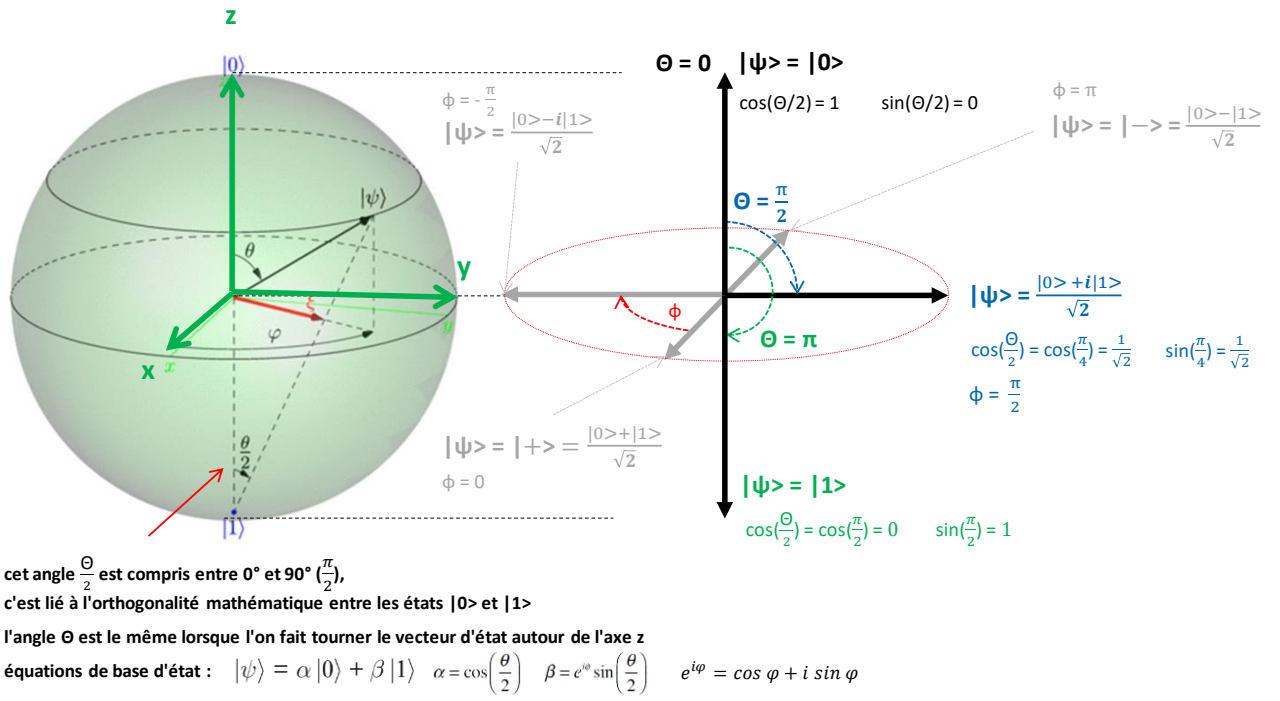
Le paradoxe à bien comprendre est le suivant : comme il existe un nombre infini de positions dans la sphère de Bloch, un qubit pourrait stocker en théorie une quantité importante d'information, en tout cas, bien plus qu'un bit.

Malheureusement, comme à la lecture, on ne peut obtenir qu'un 0 ou un 1, ou une moyenne des deux en répétant la lecture plusieurs fois après le même calcul et que celui comprend des erreurs incontournables, on ne peut pas récupérer plus d'information qu'un bit. Toujours à cause de ce sacré théorème de Holevo [66]!

Trigonométrie dans la sphère de Bloch

Second mystère à résoudre, pourquoi donc l'angle θ est-il divisé par deux dans les équations décrivant un état quantique dans la sphère de Bloch dans les calculs de sinus et de cosinus des formules donnant α et β ? Cela vient de ce que l'état |1> est placé en bas de la sphère pour que l'espace des états du qubit occupe toute la sphère et pas seulement son hémisphère nord.

J'ai du compiler plusieurs sources d'informations pour comprendre cela et l'expliquer avec le schéma *ci-dessous*[67] ! C'est un peu tarabiscoté et vous n'êtes pas obligés d'y passer du temps.



Comme l'état |1> est mathématiquement orthogonal par construction à l'état |0>, leur angle "mathématique" calculé doit être de 90° (π/2). Or, l'angle θ est du double de cet angle dans la sphère car il est de π (pour mémoire π*2 = circonférence de 360°).

---

[66] Pour en savoir plus et avec une meilleure exactitude scientifique, vous pouvez consulter la fiche Wikipedia de la fonction d'onde ainsi que celle de la probabilité d'amplitude. On trouve d'autres explications dans l'exemple des niveaux d'orbites d'électrons dans l'atome d'hydrogène dans Quantum Mechanics and the hydrogen atom (19 slides). L'interprétation physique de la règle statistique de Max Born reste en tout cas ouverte si l'on en juge par ce papier de juin 2018 d'Arkady Bolotin, Quantum probabilities and the Born rule in the intuitionistic interpretation of quantum mechanics (14 pages).

[67] C'est décrypté dans The Bloch Sphere de Ian Glendinning, 2005 (33 slides) qui explique cela par l'orthogonalité mathématique des deux états |0> et |1> qui sont pourtant opposés dans la sphère de Bloch. C'est encore mieux expliqué dans Why is theta/2 used for a Bloch sphere instead of theta ? qui a définitivement éclaircit ce mystère pour moi.

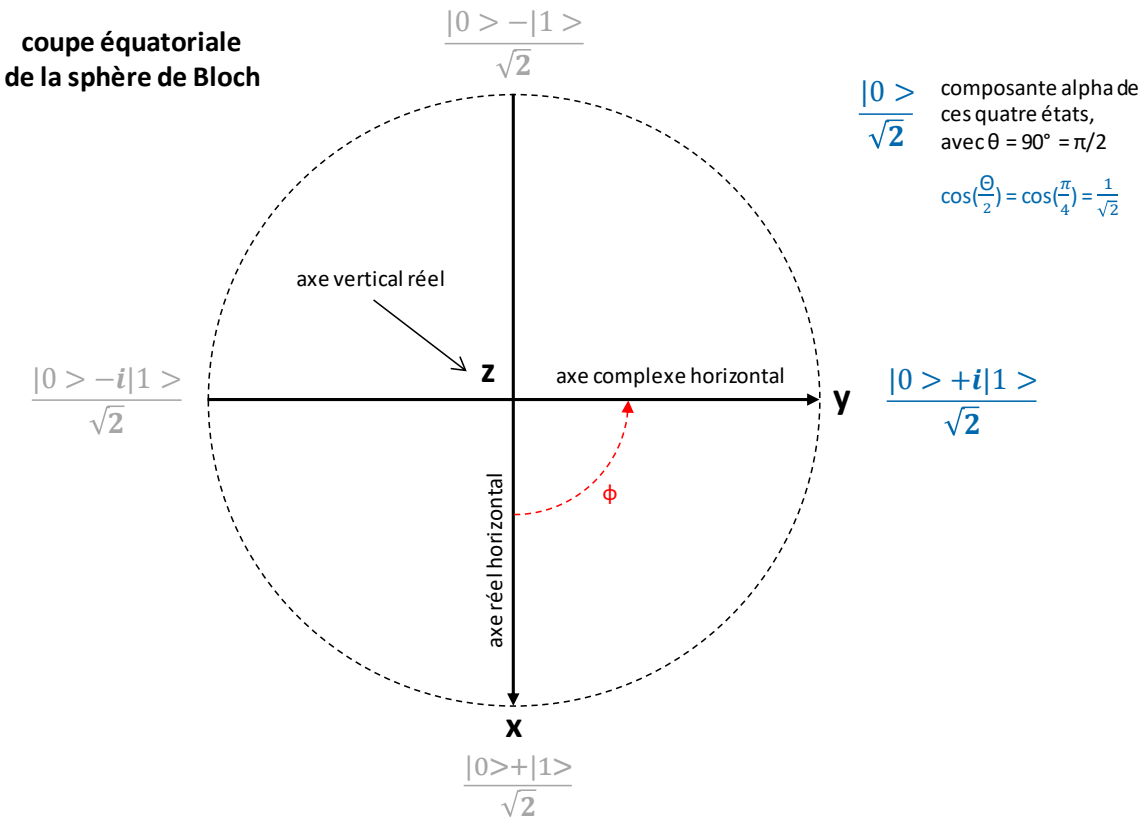
Donc, on divise θ par deux pour relier la représentation géométrique dans la sphère avec la représentation mathématique de l'état du qubit. Et surtout, pour permettre un étalement de tous les états d'un qubits sur l'ensemble de la sphère.

J'illustre ceci dans le schéma composite *ci-dessus* qui sert à comprendre la chose pour les lecteurs patients et comprenant les bases de la trigonométrie et des nombres complexes.

Dans l'histoire, α est toujours un nombre réel car c'est un simple cosinus. Seul β peut-être un nombre complexe. Il l'est dès lors que le qubit n'est pas dans le plan croisant l'axe x (θ = 0) et l'axe z (φ= 0) de la sphère de Bloch. Ce nombre complexe associe une partie réelle pour la direction x et une partie complexe pour la dimension y qui est orthogonale à x.

Un point important à noter est que la représentation sur la sphère de Bloch est un modèle mathématique probabiliste. Elle ne correspond pas à un modèle physique, comme l'angle de polarisation d'un photon ou le spin d'un électron, malgré les similitudes. Sachant néanmoins que ce modèle a été créé à l'origine pour représenter le spin d'électrons.

Lorsque le vecteur d'état du qubit est horizontal dans la sphère, c'est-à-dire qu'il va jusqu'à son équateur (*schéma ci-dessous*), nous sommes dans un état superposant l'état 0 et l'état 1 à égalité, mais avec une phase variable qui est liée à l'angle horizontal du vecteur φ par rapport à l'axe z comme dans le schéma ci-dessous. Pourquoi une phase ? Parce que ce vecteur est lié à la fonction d'onde de Schrödinger et que l'état d'un quantum est une fonction d'onde additionnant les fonctions d'onde de ses états de base !



Cette information riche d'un qubit est modifiée ensuite par des portes quantiques. Une porte quantique unitaire, à savoir, qui s'applique à un seul qubit, applique une rotation à l'état du qubit dans sa sphère de Bloch. Cette rotation est appliquée via une matrice de nombres complexes 2x2, dite matrice orthogonale de déterminant 1. De déterminant 1 car elle ne va pas modifier la longueur du vecteur après son application. Cette longueur restera toujours de 1. Nous examinerons la diversité de ces portes quantiques dans la partie suivante de cette série.

En règle générale, les portes quantiques ne génèrent pas toutes les positions de vecteurs dans la sphère de Bloch. Ce sont souvent des quarts de tours. Les points de la sphère les plus souvent utilisés sont les points cardinaux : le 0, le 1, puis les quatre points correspondant à la superposition 0 et 1 qui sont sur l'équateur de la sphère.

On doit finalement cette sphère de Bloch à trois scientifiques : **Erwin Schrödinger** pour sa fonction d'onde de 1926, **Max Born** pour son modèle probabiliste associé, créé la même année et à **Felix Bloch** (1903-1983, Suisse) qui a représenté l'état d'un quantum à deux niveaux sur la sphère en 1946. En optique et pour décrire la polarisation d'un photon, la sphère de Bloch s'appelle la sphère de Poincaré, du nom du mathématicien français **Henri Poincaré**, mort en 1912 et cousin germain du président Raymond Poincaré[68].

Cycle de vie d'un qubit

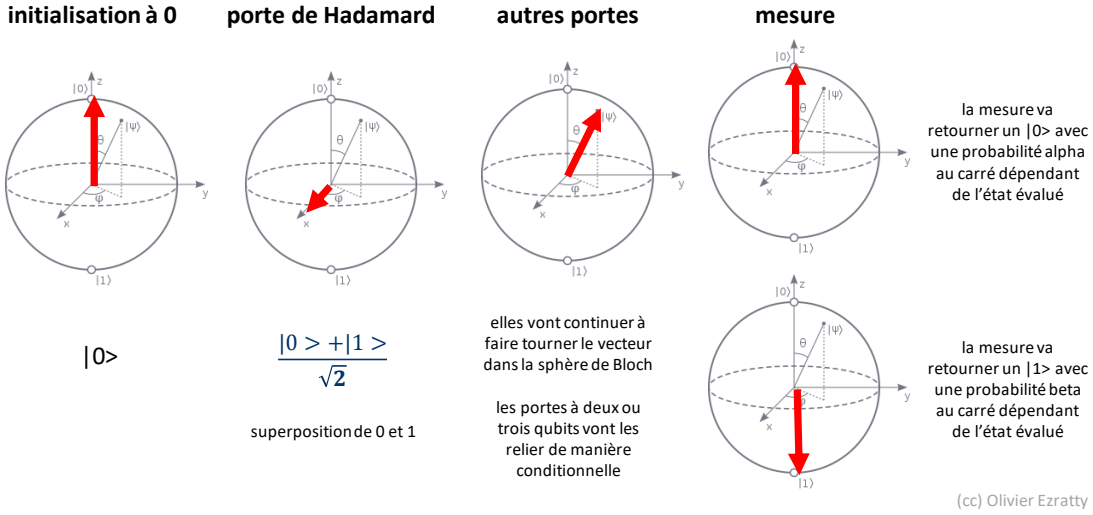
Une manière de comprendre le fonctionnement d'un ordinateur quantique à portes universelles est de suivre la vie d'un qubit lors des traitements. C'est un objet mathématique un peu particulier :

- On l'**initialise** toujours à 0, correspondant à l'état de base du qubit. Cette initialisation consomme d'ailleurs de l'énergie.
- On le **modifie** ensuite de manière programmatique avec des portes quantiques pour lui faire prendre des valeurs qui sont des vecteurs dans la sphère de Bloch. La porte de Hadamard est l'une des plus courantes et elle créé un état de superposition entre un 0 et un 1. Les manipulations mathématiques de ce vecteur consistent ensuite à le faire tourner dans la sphère de Bloch avec des portes quantiques unitaires que nous verrons dans la partie suivante consacrée à la description du fonctionnement d'un ordinateur quantique. Ces manipulations reviennent à multiplier le vecteur représentant le qubit [α, β] par une matrice de deux lignes et deux colonnes de nombres complexes conservant la norme du vecteur, qui doit rester à 1. Les portes quantiques non unitaires relient les qubits entre eux et en font évaluer les valeurs d'un qubit de manière conditionnelle en fonction des valeurs d'un ou deux autres qubits. Sans ces différentes portes quantiques, on ne pourrait pas faire grand chose avec les qubits.

[68] Voici quelques sources d'information associées à cette partie : Lectures on Quantum Computing de Dan C. Marinescu et Gabriela M. Marinescu, 2003 (274 pages), The Bloch Sphere de Ian Glendinning, 2005 (33 slides), The statistical interpretation of quantum mechanics, discours d'acceptation du prix Nobel de physique de Max Born en 1954 (12 pages) ainsi que l'excellent livre The mathematics of quantum mechanics de Martin Laforest, 2015 (111 pages), qui décrit les basiques mathématiques de l'informatique quantique avec les nombres complexes, les vecteurs, les matrices et tout le toutim.

- L'**information dans les qubits** qui est manipulée lors des calculs est "riche" avec une dimension de deux nombres réels, les angles θ et φ, ou le vecteur [α, β].
- A part le cas où le qubit est initialisé à l'état |0> ou inversé à l'état |1>, celui-ci est en **état de superposition** entre ces deux états. La représentation mathématique d'un qubit et son incarnation visuelle dans la sphère de Bloch montrent qu'un qubit peut-être dans une infinité d'états superposés différents.
- Lorsque l'on **lit la valeur du qubit**, on retombe sur un 0 ou un 1 avec un retour probabiliste dépendant des paramètres du vecteur de l'état du qubit dans la sphère de Bloch.
- Donc, nous avons un 0 en entrée, un 0 ou un 1 en sortie, et une **infinité d'états** entre les deux pendant les calculs !

Voici cela illustré dans le schéma *ci-dessous* :



Tout ça pour dire que la richesse mathématique du qubit intervient pendant les traitements et seulement pendant les traitements. Mais ni au départ, ni à l'arrivée des traitements. La magie mathématique de l'ordinateur quantique est là !

Algèbre linéaire et qubits

Le calcul quantique nécessite d'appréhender tout un tas de concepts de l'algèbre linéaire que nous allons balayer rapidement ici-même. Ils sont associés à un formalisme mathématique de description des phénomènes quantiques qui sont indispensables pour créer un algorithme quantique[69].

C'en est au point où, du fait des mécanismes de l'intrication quantique, il est préférable d'utiliser et manipuler la notation mathématique de description de l'état des qubits et des opérations les concernant que d'essayer se créer une image mentale physique de ce qui se passe dans les qubits eux-mêmes. On ne peut pas « visualiser » facilement dans l'espace le fonctionnement de cette intrication à grande échelle.

[69] Voir notamment Calcul quantique : algèbre et géométrie projective, thèse d'Anne-Céline Baboin, 2013 (186 pages) et A propos du formalisme mathématique de la mécanique quantique de Thierry Paul (28 pages).

On retrouve cela dans la description des fameux états de Bell qui décrivent deux qubits intriqués. Cette intrication se démontre mathématiquement. La démonstration que nous ferons plus loin prouve qu'un tel état ne peut pas se décomposer en deux états de qubits indépendants.

Manque de bol, ce formalisme mathématique est plutôt abscons et difficile à digérer pour ceux qui n'en ont pas la patience, y compris votre serviteur !

Je vais tout de même tenter de vulgariser quelques concepts et conventions mathématiques de la mécanique quantique qui s'appliquent au cadre du calcul quantique. Ce sont d'ailleurs des notations, outils et conventions dont je ne fournirai pas forcément l'origine à chaque fois. Cela vous permettra surtout de s'y retrouver dans certaines des publications scientifiques sur le sujet.

Un **observable** est un état de base mesurable par un capteur sur un quantum ou un qubit. La mesure provoque l'écrasement de la fonction d'onde (ou la réduction du paquet d'onde) du quantum sur l'un des états de base. Si on mesure deux fois de suite l'état d'un quantum ou d'un qubit, la mesure donnera le même résultat. Dans la nature, un quantum peut avoir plusieurs états, comme le niveau d'excitation d'un électron d'un atome d'hydrogène. Dans les qubits, les observables sont généralement matérialisés mathématiquement par un 0 ou un 1 qui représentent leurs deux états quantiques distincts. La base des observables est l'ensemble des états de base d'un système quantique, donc ce qui correspond à 0 et 1 pour un qubit.

Une **base orthonormée** d'un espace vectoriel comprend des vecteurs de base qui sont mathématiquement tous orthogonaux les uns avec les autres et dont la longueur est de 1. Dans la représentation de l'état des qubits, cette base de vecteurs est constituée des états |0> et |1>. Leur orthogonalité mathématique est une base de départ malgré le fait qu'ils sont plutôt opposés dans la sphère de Bloch pour des raisons de représentation dans cette sphère. Mais, histoire de compliquer les choses, d'autres bases de référence orthonormées peuvent servir d'observables, en particulier lorsque des photons sont manipulés, avec des références de phase différentes de la référence de départ. C'est le cas des états situés sur la sphère de Bloch dans l'axe x :

$$|+> = \frac{|0>+|1>}{\sqrt{2}} \qquad |-> = \frac{|0>-|1>}{\sqrt{2}}$$

L'état d'un qubit est donc représenté dans cet espace orthonormé à deux dimensions comprenant les vecteurs d'état représentant les états de base |0> et |1>. C'est un **vecteur de nombres complexes** dans un **espace de Hilbert** à deux dimensions. On le représente verticalement avec les nombres complexes α et β associés aux états |0> et |1> et dont la somme des carrés fait 1. Cette représentation décrit l'état de superposition entre |0> et |1> dans le qubit. Cette combinaison linéaire des états |0> et |1> décrit le phénomème de la **superposition** d'états au sein d'un qubit.

Cet espace à deux dimensions remplace l'espace de dimension infini qui caractérise une fonction d'onde f(x) de Schrödinger, x pouvant prendre n'importe quelle valeur. C'est donc une **représentation simplifiée** de l'état quantique d'un qubit. En manipulant ces symboles, les vecteurs et matrices, on en oublie la nature ondulatoire des quantums manipulés. Cela isole la représentation physique des qubits de leur traitement mathématique dans les calculs.

Dans la **notation de Dirac**, un état quantique est représenté par |Ψ>, le **ket** de l'état quantique Ψ. Le **bra** du même vecteur d'état, représenté par <Ψ| est la transposée conjuguée (ou transconjugée ou adjointe) du « ket ». C'est le vecteur « horizontal » $[\bar{\alpha}, \bar{\beta}]$. La barre au dessus des α et β décrit l'opération de conjugaison des nombres complexes avec inversion du signe de la partie complexe du nombre (-i au lieu de +i ou le contraire).

ket de Ψ : $|\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ bra de Ψ : $\langle\Psi| = [\bar{\alpha}, \bar{\beta}]$ $|\Psi\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}$ $\langle\Psi| = [\frac{1}{\sqrt{2}}, \frac{-i}{\sqrt{2}}]$

$\bar{\alpha}$ est le conjugué de α avec négation de la partie complexe, idem pour $\bar{\beta}$.

Le **produit scalaire** de deux qubits $<\Psi_1|\ \Psi_2>$ est la projection mathématique du vecteur d'état Ψ_2 sur le vecteur Ψ_1. Cela donne un nombre complexe. Lorsque les vecteurs sont orthogonaux, le produit scalaire est égal à 0. Lorsque les deux vecteurs sont identiques, <Ψ| Ψ> est la norme de Ψ et est toujours égale à 1. En anglais : produit scalaire = scalar product ou inner product.

produit scalaire (inner product)

$$\langle\Psi|\Psi\rangle = \left[\bar{\alpha}, \bar{\beta}\right] \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha^2 + \beta^2 = 1$$

Le **produit externe** de deux vecteurs représentant un qubit, l'un en bra et l'autre en ket, donne un opérateur ou matrice de densité qui est une matrice 2x2. En anglais, produit externe = outer product. Lorsque le bra correspond à la transconjuguée du ket, il s'agit d'un opérateur de densité d'un état pur (pure state). Cette notion d'opérateur de densité sera ensuite élargie à une combinaison de qubits.

produit externe (outer product)

$$|\Psi\rangle\langle\Psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \times \left[\bar{\alpha}, \bar{\beta}\right] = \begin{bmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta} \end{bmatrix}$$

Les **produits tensoriels** sont utilisés pour décrire l'état de registres quantiques de plusieurs qubits. L'état d'un registre de N qubits est le produit tensoriel de ces N qubits représentés par leur vecteur ket vertical. Cela donne un vecteur (vertical) pouvant prendre 2^N valeurs différentes, représentant chacune une combinaison différente de 0 et de 1. Un registre quantique superpose ces 2^N états différents avec un poids de chacun de ces états représenté par un nombre complexe.

La somme de ces poids au carré donne 1. D'une manière générale, le produit tensoriel de deux vecteurs de dimension m et n donne un vecteur de dimension m*n.

un état d'un registre de 8 qubits est un produit tensoriel de 8 qubits, un état basique (« basic state »).

$$|0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle$$
$$= \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}$$

un état basique est le produit tensoriel est un vecteur de dimention 2^8 soit 256, chaque élément étant 0 ou 1.

$$|01010001\rangle = \begin{matrix}|00000000\rangle\\|00000001\rangle\\\vdots\\|01010000\rangle\\|01010001\rangle\\\vdots\\|11111110\rangle\\|11111111\rangle\end{matrix} \begin{bmatrix}0\\0\\\vdots\\0\\1\\\vdots\\0\\0\end{bmatrix}$$

l'état d'un registre est donc la somme des probabilités d'état de chaque combinaison de 0 et de 1 et la somme des probabilités c_i au carré fait 1.

$$|\psi\rangle = c_1 |00000000\rangle + \cdots + c_{82} |01010001\rangle + \cdots + c_{255} |11111110\rangle + c_{256} |11111111\rangle$$
$$= \sum_{i=1}^{N} c_i |i\rangle$$

En algèbre linéaire, les transformations (U) qui s'appliquent à un jeu de qubits sont linéaires et à ce titre ont des propriétés diverses qui sont liées au calcul matriciel dont voici quelques exemples *ci-dessous*.

$$(A+B)|\Psi\rangle = A|\Psi\rangle + B|\Psi\rangle \qquad \langle\Psi|A|\phi\rangle = \langle\phi|A|\Psi\rangle^*$$

$$A|\Psi\rangle = \langle\Psi|A^\dagger$$ ↖ conjuguée ou adjointe de de A

Tous ces éléments de notation d'algèbre linéaire quantique sont bien résumés dans le tableau *ci-contre*[70].

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*.
$\langle\varphi\|\psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = (A^T)^*$. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

Un **état pur** (pure state) décrit l'état d'un qubit isolé. C'est la combinaison des deux états observables du qubit respectant la distribution probabiliste de Max Born.

[70] Il provient de Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages).

Un **état basique** d'un registre de qubits, représenté par un ket, est une combinaison donnée de 0 et de 1 de qubits dans un registre. Un registre de N qubits peut donc avoir 2^N états basiques différents.

Des **états quantiques** sont séparables lorsqu'ils sont mathématiquement le résultat du produit tensoriel de chacun des états purs qui le composent.

L'**intrication** ou un état intriqué de deux qubits se produit lorsqu'il ne peut pas être évalué sous la forme du produit tensoriel de deux états purs. En clair, il ne peut pas être la combinaison de deux qubits indépendants. Cela se démontre mathématiquement simplement par l'absurde pour les états |00> et |11> d'un registre de deux qubits. Dans ces paires, la mesure de la valeur de l'un des qubits détermine celle de l'autre, ici, identique.

démonstration de l'impossibilité de créer un état EPR par le produit tensoriel de deux qubits, ici $|\Psi_1\rangle$ et $|\Psi_2\rangle$

$$|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$$
$$|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

calcul du produit tensoriel de deux qubits hypothétiques

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle)$$

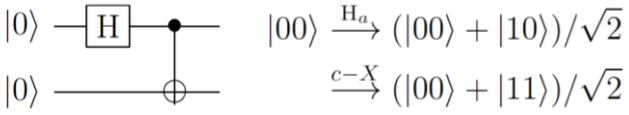
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle)$$

$\alpha_1\beta_2 = 0$ et $\beta_1\alpha_2 = 0$ *incompatibles avec* $\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}$ et $\beta_1\beta_2 = \frac{1}{\sqrt{2}}$

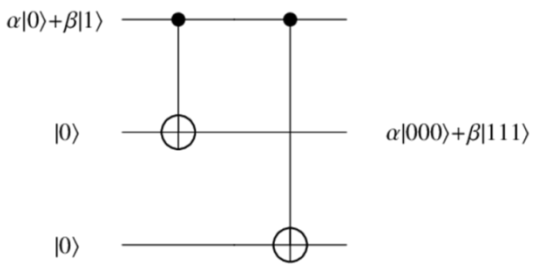
car si $\alpha_1 = 0$ alors $\alpha_1\alpha_2 = 0$

car si $\beta_2 = 0$ alors $\beta_1\beta_2 = 0$

Sachant que la création de telles paires intriquées de qubits passe par des opérations de préparation. Deux qubits placés côte à côte ne sont pas intriqués par magie ! La paire utilisée dans l'exemple *ci-dessus* peut-être générée par deux portes quantiques, une porte H (Hadamard) et une porte CNOT, que nous verrons plus loin. Seules les portes quantiques à plusieurs qubits génèrent des qubits intriqués dans un registre de qubits.



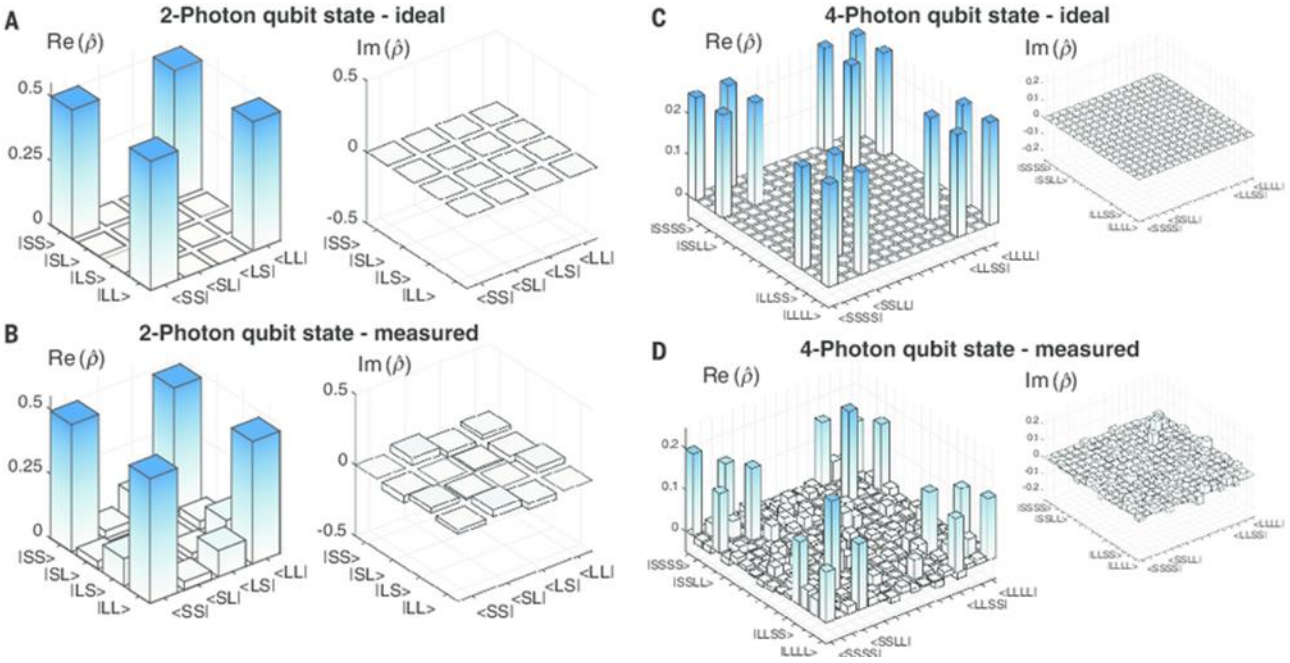
Un état dit **GHZ** avec trois qubits intriqués superposant les états |000> et |111> est préparé avec deux portes CNOT consécutives comme indiqué dans le schéma *ci-contre*.



Nous définirons cette porte un peu plus loin.

Une **matrice densité,** représentée par ρ, est une matrice de nombres complexes qui sert à décrire un système physique, ici, un registre de qubits. Elle décrit des états appelés mélanges statistiques qui associent plusieurs états possibles du registre (combinaison de 0 et de 1).

La matrice comprend l'ensemble des états quantiques possibles d'un registre, associant la mécanique quantique et la physique statistique. On peut déduire de la matrice densité les valeurs espérées des observables, à savoir le poids des 0 et 1 pour chaque qubit. Ces matrices sont hermitiennes (symétriques) et de norme 1. La représentation graphique de ces matrices est souvent utilisée pour évaluer la fidélité de portes quantiques à deux ou trois qubits dans les publications de chercheurs. L'exemple ci-dessous illustre cela en comparant l'état théorique d'une matrice de densité pour 2 qubits et 4 qubits et le résultat de la mesure[71].



Les vecteurs d'état, ou kets, décrivent un **état pur**. Les matrices densités générées à partir d'un état d'un seul qubit (ket) sont dites pures.

Leur combinaison statistique classique donne un **état mixte** qui est incarné par la matrice densité qui en résulte comme illustré *ci-dessous*. Ces états mixtes correspondent à des états difficiles à isoler d'un point de vue pratique.

un état mixte est une combinaison probabiliste de plusieurs états de registres quantiques. Ψ_i est un de ces états représenté sous la forme d'un vecteur vertical avec 2^N entrées, N étant le nombre de qubits du registre.

$$\{(p_i|\Psi_i)\}$$

l'opérateur ou matrice de densité de cet état mixte est l'addition de ces différents états multiplié par leur probabilité (la somme des probabilités fait 1, sans passer par le carré comme pour un état pur). Avec N qubits, l'opérateur de densité est une matrice carrée de 2^N de côté.

$$\rho = \sum_i p_i \, |\Psi_i\rangle\langle\Psi_i|$$

$$\sum_i p_i = 1$$

la matrice de densité d'un seul qubit est une matrice 2x2 résultat du produit intérieur de l'état $\langle\Psi|$.

$$\rho = |\Psi\rangle\langle\Psi|$$

[71] Source : Generation of multiphoton entangled quantum states by means of integrated frequency combs, 2016.

Voici ce à quoi ressemble un des états de cet état mixte, **|Ψi⟩⟨Ψi|** :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} \begin{pmatrix} \bar{a}_1 & \bar{a}_2 & \cdots & \bar{a}_N \end{pmatrix} = \begin{pmatrix} a_1\bar{a}_1 & a_1\bar{a}_2 & \cdots & a_1\bar{a}_N \\ a_2\bar{a}_2 & a_1\bar{a}_2 & \cdots & a_2\bar{a}_N \\ \vdots & & & \vdots \\ a_N\bar{a}_1 & a_N\bar{a}_2 & \cdots & a_N\bar{a}_N \end{pmatrix}$$

Les matrices densité sont particulièrement utiles pour décrire des **états intriqués** comme les paires de Bell.

exemple avec une paire EPR rassemblant deux vecteurs d'état |00⟩ et |11⟩

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(1,0,0,1)^T$$

une matrice densité d'une paire de Bell est simple à créer à partir du vecteur ket représentant l'état superposé |00⟩ et |11⟩

$$\frac{1}{\sqrt{2}}(1,0,0,1)^T \frac{1}{\sqrt{2}}(1,0,0,1) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Un **mélange statistique** est la partie diagonale de la matrice de densité.

La **trace** d'une matrice est la somme de ses valeurs des éléments de sa diagonale.

Reste à définir les notions d'**eigenvector**, **eigenvalue**, **eigenstate** et **eigenspace** qui sont souvent utilisées en mécanique et en calcul quantiques ainsi d'ailleurs que dans le machine learning, en particulier dans les algorithmes de réduction de dimensions comme la PCA (Principal Components Analysis). Ces notions permettent de définir la structure de certaines matrices carrées. Pour une telle matrice A, un eigenvector x ou vecteur propre de A est un vecteur qui vérifie l'équation $Ax = \lambda x$, λ étant un nombre réel que l'on nomme eigenvalue. Ces eigenvectors ont la particularité de ne pas changer de direction une fois multipliés par la matrice A. Pour une eigenvalue λ, l'eigenspace associé est l'ensemble des vecteurs x qui satisfont $Ax = \lambda x$.

Ces eigenvalues s'évaluent en calculant le déterminant de la matrice $A - \lambda I$, I étant la matrice d'identité (1 dans les cases de la diagonale et 0 ailleurs). On trouve alors les valeurs de qui résolvent $0 = A - \lambda I$. C'est une équation polynomiale ayant un degré inférieur ou égal à la taille de la matrice carrée.

Les eigenvectors de référence d'une matrice A permettent de reconstituer un espace orthonormé lié à la matrice. Par exemple, une matrice de projection dans un plan en 3D aura comme eigenvectors principaux deux vecteurs orthogonaux situés dans le plan et un vecteur orthogonal au plan. Cette multiplication donne λx avec λ étant non nul si l'eigenvector est dans le plan en question et 0 si le vecteur est orthogonal au plan[72]. Une matrice A peut être celle d'une porte quantique. Un eigenvector d'une porte quantique est donc un ket dont la valeur n'est pas modifiée par la porte quantique.

[72] C'est bien expliqué dans le cours de Gilbert Strang du MIT, 2011 (51 minutes).

C'est facile à se représenter pour la porte S, de changement de phase, que nous verrons plus loin. Les kets |0> et |1> étant dans l'axe de rotation, ils ne sont pas modifiés par celle-ci.

Ce sont donc des eigenvectors de la porte S et l'eigenvalue correspondante est de 1. C'est toujours le cas pour les matrices des portes quantiques puisque les vecteurs représentant les états quantiques, les kets, ont toujours une longueur de 1.

La recherche des eigenvectors et eigenvalues d'une matrice A revient à la diagnonaliser. La diagnonalisation d'une matrice carrée consiste à trouver la matrice qui la multipliera pour la transformer en matrice remplie uniquement dans sa diagonale.

Et les eigenstates ? C'est un autre nom donné aux eigenvectors, mais par les physiciens !

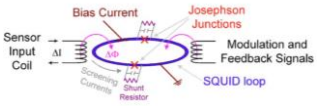
Je ne vous embêterai pas plus sur les eigentrucs mais cela vous servira peut-être à compulser une partie de la littérature scientifique sur le calcul quantique.

Voilà pour la définition des basiques de l'algèbre linéaire du calcul quantique. J'ai zappé plein d'autres définitions et règles de calcul. Il s'agissait de préciser certaines notions qui sont fréquemment utilisées dans la littérature scientifique sur le calcul quantique et dans nombre d'ouvrages de référence cités dans cet ebook.

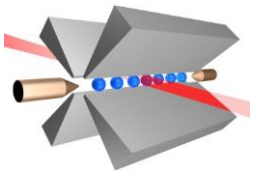
Types de qubits

D'un point de vue physique, les qubits des calculateurs quantiques sont des dispositifs matériels qui intègrent des particules élémentaires qui ont deux états possibles que l'on peut initialiser, modifier avec des portes quantiques puis dont on peut évaluer l'état par observation ou mesure.

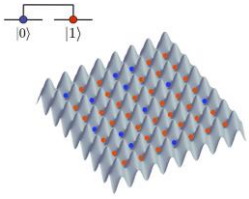
Il s'agit parfois de particules élémentaires unitaires, comme avec les ions piégés, des atomes froids ou des élections ! Une seule à la fois ! Dans le cas des supraconducteurs, l'état quantique s'appuie sur un grand nombre de particules, ici, des électrons, et en l'occurrence, arrangés en paires de Cooper, les paires d'électrons qui créént à température supraconductrice.



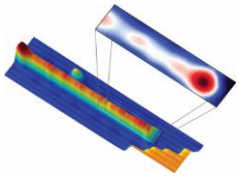
supraconducteurs



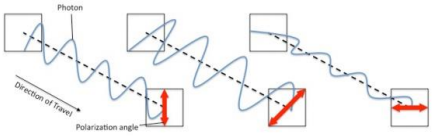
ions piégés



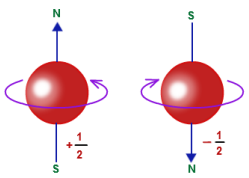
atomes froids



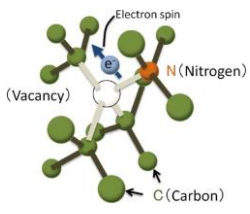
fermions de Majorana



photons



spin d'électrons piégés



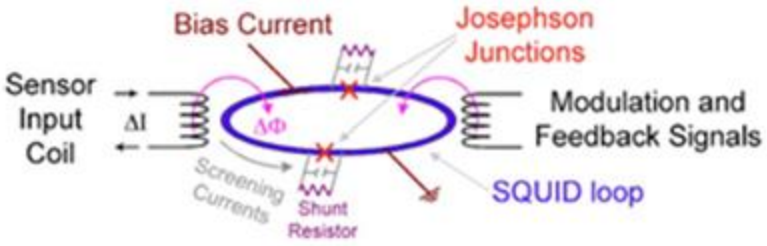
centres NV (diamant)

Voici les principaux types de qubits qui sont étudiés, expérimentés ou utilisés en production actuellement :

Les **supraconducteurs** : le qubit prend la forme de l'état d'un courant supraconducteur qui traverse une barrière très fine en s'appuyant sur l'effet Josephson. Il existe plusieurs types de qubits supraconducteurs, de flux, de phase et de charge. Ne rentrons pas dans les détails. Dans tous les cas, il s'agit de créer une superposition de deux états bien distincts d'un courant oscillant à haute fréquence et traversant la jonction Josephson dans une boucle supraconductrice. L'oscillation est rendue possible par le fait que la boucle intègre l'équivalent d'une inductance et d'une résistance.

L'oscillation du courant est activée par l'application de micro-ondes de fréquences situées entre 5 et 10 GHz transmises par voie conductrice et physique.

Ce ne sont pas des ondes émises par la voie "radio". L'état du qubit est pour sa part mesuré avec un magnétomètre intégré dans le circuit.



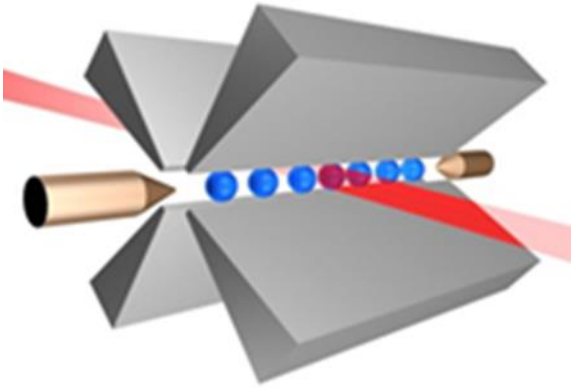
C'est la technique la plus couramment employée aujourd'hui, notamment par IBM, Google et Intel pour des ordinateurs quantiques à circuits universels et avec les ordinateurs quantiques adiabatiques du Canadien D-Wave qui utilisent un autre arrangement de qubits de qualité moins bonne du côté du bruit et du taux d'erreurs. Elle est relativement facile à fabriquer car elle s'appuie sur les techniques de création de circuits CMOS même si certains des matériaux sont différents, comme le niobium qui est utilisé chez D-Wave[73]. Notons, nous le verrons plus tard, que l'équipe de Daniel Estève au CEA de Saclay fait partie des précurseurs de la création de tels qubits supraconducteurs.

La technique présente des inconvénients : les générateurs de radiofréquence sont généralement situés à l'extérieur de l'enceinte cryogénisée du processeur quantique, ce qui multiplie le câblage. Les fréquences de contrôle des qubits doivent être différentes pour des qubits adjacents ce qui donne des plans d'allocation de fréquences voisins de ceux que les opérateurs télécoms utilisent pour le téléphone cellulaire.

Les **ions piégés** : il s'agit d'ions d'atomes qui sont maintenus sous vide et suspendus par suspension électrostatique. Un pompage optique est réalisé pour leur initialisation. Un laser sert à la mesure et exploite le phénomène de fluorescence des ions excités par le laser. Le magnétisme est utilisé pour l'activation des portes quantiques. Les lasers permetent d'intriquer des qubits. La startup IonQ issue de l'Université de Maryland planche là-dessus tout comme l'université d'Innsbruck en Autriche et sa spinoff AQT.

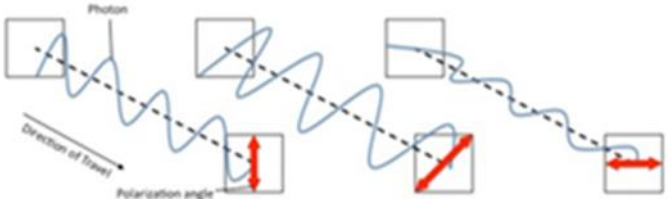
[73] Voir Practical realization of Quantum Computation Supraconducting (36 slides).

Dans un tel système, plusieurs ions sont piégés de manière équidistante les uns des autres. Ils sont alignés en rang d'oignons. Il est difficile de faire "scaler" ce genre d'arrangement au-delà d'une centaine et quelques d'ions. Par contre, ils présentent l'avantage de bien pouvoir être intriqués les uns avec les autres, ce qui est moins le cas des qubits à base de supraconducteurs.



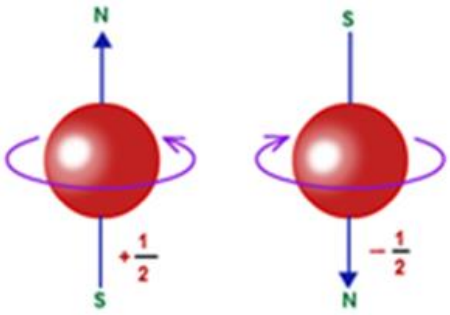
Les **photons** : leur état quantique est leur polarisation horizontale ou verticale. Cela fait partie du champ de l'optique linéaire. Il manipule des photons individuels. Les portes quantiques sont réalisées à l'aide de dispositifs optiques avec des filtres dichroïques ou polarisants. Il faut un grand nombre de lasers pour piloter l'ensemble. C'est donc pour l'instant assez embarrassant. L'avantage est que ces qubits fonctionnent à température ambiante.

Mais ce type de qubit n'est pour l'instant utilisé qu'en laboratoire et à petite échelle. Les qubits à base de photons sont dits « volants » (flying) à contrario des autres qui sont statiques.



Le **spin d'électron** : haut ou bas, une sorte de sens de polarisation magnétique, que l'on retrouve dans les ordinateurs à base de quantum dots, notamment chez Intel ou dans des prototypes de qubits réalisés au CEA LETI à Grenoble. Ces qubits sont intégrés dans des circuits à base de semi-conducteurs CMOS.

Ils bénéficient donc de la réutilisation de processus de fabrication de composants CMOS déjà bien maitrisés. Ces qubits sont cependant pour l'instant plutôt "bruyants", même en les exploitant à des températures proches du zéro absolu. Le plan consiste à en aligner des batteries pour créer des qubits logiques, un concept que nous étudierons dans la prochaine partie.

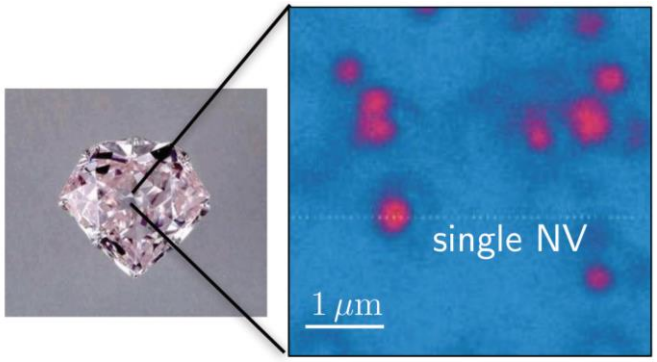


Ce serait à ce jour la seule technologie réellement scalable en termes de nombre de qubits. Les qubits des autres technologies sont en effet difficilement miniaturisables. Qui plus est, fonctionnant à une température très basse, inférieure à 20 mK, ils limitent la puissance qui peut être consommée pour les contrôler dans leur enceinte cryogénique. A contrario, les qubits CMOS pourraient fonctionner à une température moins froide de 1K, qui permettrait de dépenser un peu plus d'énergie pour les contrôler dans l'enceinte cryogénique.

Les **centres NV** (pour Nitrogen Vacancy) : ce sont des structures de diamant artificiel dans lesquelles un atome de carbone a été remplacé par un atome d'azote et à proximité duquel se situe une lacune d'atome de carbone.

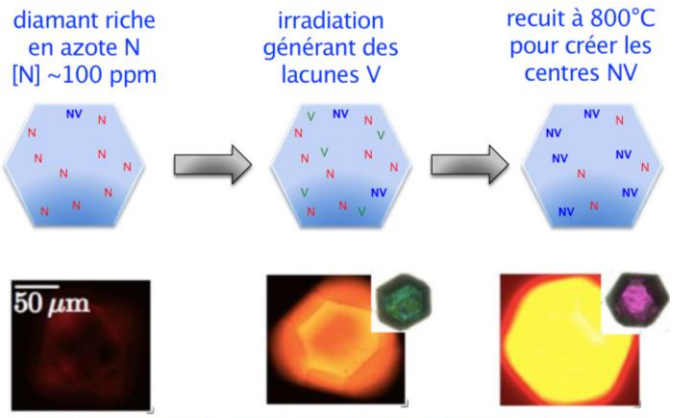
Les défauts dans les diamants ont été étudiés à partir de 1930 avec d'examen de l'absorbtion de l'infrarouge[74]. Cela permettait de distinguer deux catégories de diamants : type I avec une bande d'absorbtion de 8 µm dans l'infrarouge et type II sans cette bande. Les défauts expliquent la couleur des gemmes de diamants. Il a fallut attendre 1959 pour découvrir que ces impuretés étaient liées à la présence d'azote, à 7,8 µm et que les atomes d'azote étaient bien isolés dans le diamant. En 1975, on découvrait qu'un traitement thermique permettait de contrôler la diffusion des atomes d'azote dans le diamant. Ces centres d'azote donnent une couleur au diamant. Avec quatre formes : un atome d'azote isolé par une lacune, deux atomes d'azote, trois atomes d'azote entourant une lacune et et quatre atomes d'azote.

C'est la première forme qui est intéressante dans les différents usages évoqués dans cet ouvrage, notamment en métrologie quantique. On peut visualiser ces défauts avec un microscope confocal (à faible profondeur de champ) en les illuminant avec un faisceau laser vert qui va générer de la lumière rouge[75]. Ces diamants à NV centers sont légèrement roses.



Ces propriétés permettent de générer des sources de photons uniques grâce à l'isolation d'un NV center.

Pour produire ces NV centers, on utilise des diamants artificiels riches en azote. Les lacunes sont générées par irradiation. Un recuit sous vide à environ 800°C-900°C déplace les lacunes à côté des atomes d'azote dans la structure cristalline[76]. C'est lié au fait que les atomes d'azotes sont aussi grands que ceux du carbone. La lacune crée une petite barre d'électrons qui servent d'aimant virtuel via leur spin.



Photoluminescence d'un micro-cristal de diamant sous excitation verte

Ils ont deux orientations possibles : parallèle ou orthogonale au champ magnétique ambiant. On peut les contrôler individuellement.

---

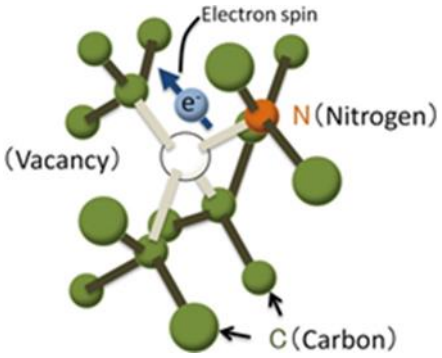
[74] Dans Les défauts du diamant : de la couleur des gemmes à un outil pour les nanosciences de Jean-François Roch, 2011 (42 minutes) et Centres NV du diamant du matériau aux applications, 2015 (52 slides) racontent très bien la découverte des centres NV.

[75] Voir Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers de A. Gruber & Al, 1997 (4 pages) qui est la source de l'illustration vus également dans les slides de Jean-François Roch.

[76] Source de l'illustration : Centres NV du diamant du matériau aux applications, de Jean-François Roch, 2015 (52 slides). Une thèse décrit bien les différentes techniques de création de centers NV : Engineering of NV color centers in diamond for their applications in quantum information and magnetometry, Margarita Lesik, 2015 (139 pages).

On peut aussi produire des diamants à NV centers avec du dépôt sous vide d'hydrogène et de méthane (CVD, pour Chemical Vapor Deposition) pour créer une structure cristalline parfaite de diamant puis avec de l'implantation ionique avec des faisceaux d'ions d'azote.

La structure du carbone environnant un NV center protège bien la zone de la cavité. L'état de la lacune est instable et quantique. Il est excité par lasers et micro-ondes. La lecture de l'état du qubit est réalisée par une mesure de brillance de fluorescence.



Seule la startup **QDTI** planche commercialement sur cette technique pour créer des qubits. Ce n'est visiblement pas encore au point.

Voici, *ci-dessous*, un schéma d'ensemble du mécanisme de contrôle de ces qubits[77].

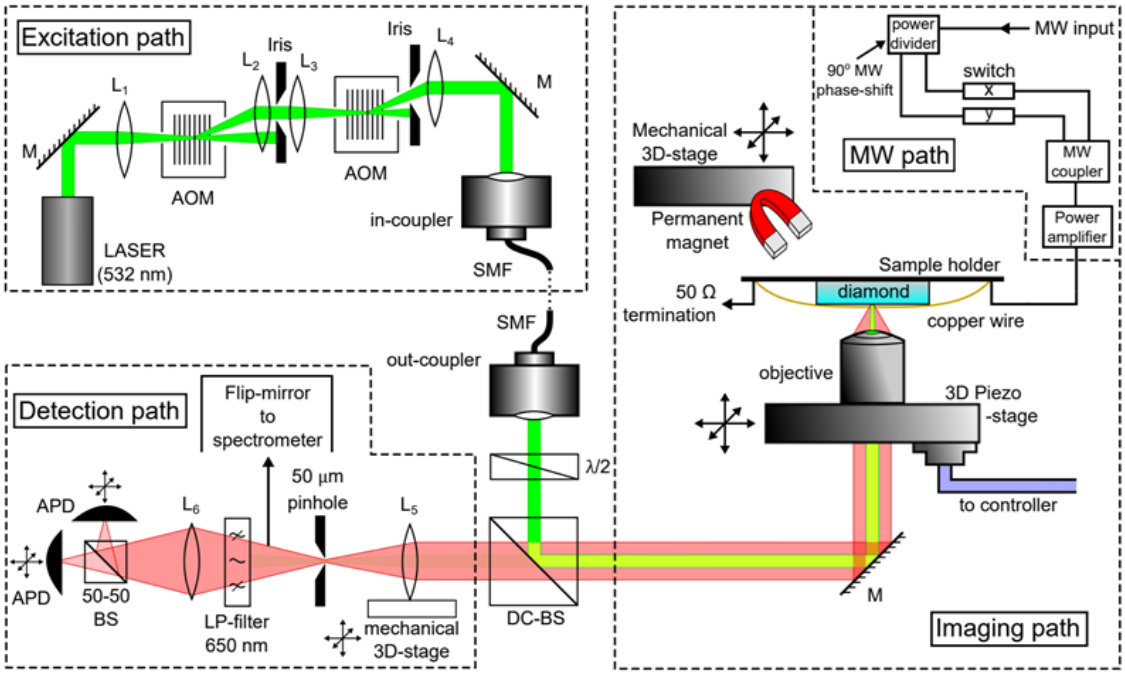
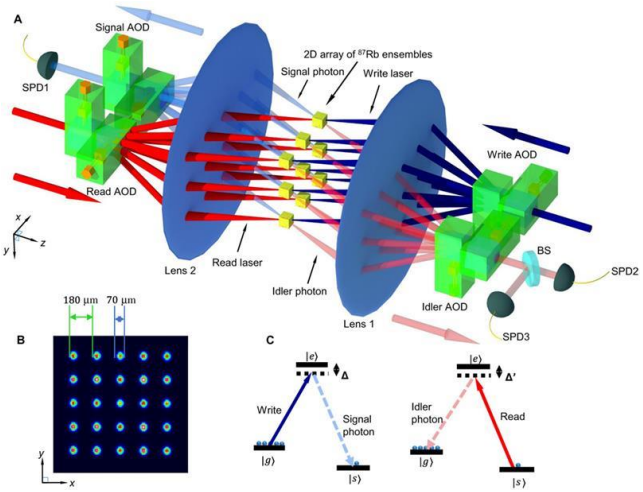


Figure A.1.: Schematic representation of the utilized setup for the characterization of NV centers. Experimental setup utilized for optical characterization and coherent spin manipulation of NV centers, comprising of a home-built confocal microscope, a scanning-stage for the imaging of diamond, and external magnet and microwave apparatus. The excitation wavelength is 532 nm. In the figure, mirrors are represented by M, lenses by L_i, single-mode optical fiber by SMF, beam-splitters by BS, and avalanche photo-diodes by APD.

Les **atomes froids** : ce sont des atomes refroidis à très basse température, en général avec des techniques utilisant des lasers et l'effet Doppler. Les atomes utilisés sont des atomes neutres (pas ionisés) et assez souvent, le rubidium, un métal alcalin. On utilise aussi des atomes dits de Rydberg avec un grand nombre de couches d'électrons et que l'on excite avec de hauts niveaux d'énergie.

[77] Vu dans Forefront engineering of nitrogen-vacancy centers in diamond for quantum technologies 2017 (235 pages).

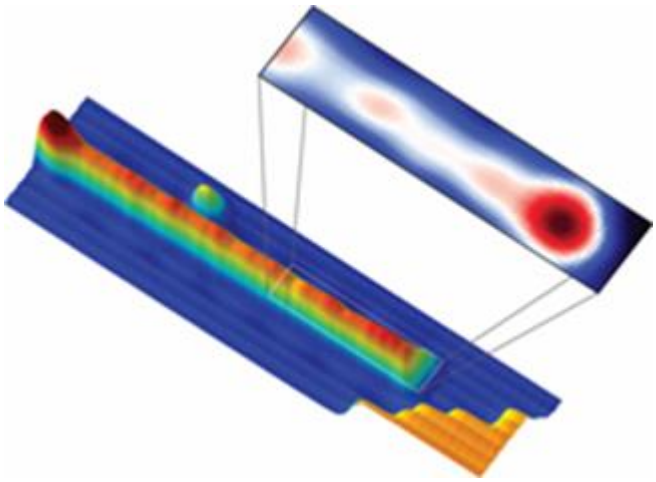
L'état quantique de ces atomes froids est leur niveau d'énergie. Les atomes froids servent à créer aussi bien des qubits pour ordinateurs quantiques à portes quantiques universelles ou des simulateurs quantiques analogiques. Les atomes de Rydberg sont notamment étudiés par l'équipe de Michel Brune et Igor Dotsenko au LKB de l'ENS à Paris. La startup française **Pasqal** planche sur cette piste.



Nous examinerons son activité et sa technologie page 305. Des chercheurs chinois et américains ont à ce jour réussi à intriquer jusqu'à 25 qubits faits à partir d'atomes de rubidium[78].

Les **fermions de Majorana** : ce sont des anyons ou quasi-particules qui sont des états particuliers de nuages d'électrons organisées par paires. Pratiquement, ce sont des spins d'électrons aux deux bouts de fils supraconducteurs. On peut d'ailleurs considérer à ce titre là que c'est une variation des qubits supraconducteurs.

De ce fait, ces ordinateurs quantiques doivent aussi être refroidis à une température voisine du zéro absolu, aux alentours de 10mK. C'est la voie choisie par Microsoft et une équipe de Nokia aux USA. Sachant que l'existence des fermions de Majorana est à peine prouvée. Et les quasi-particules sur lesquelles planchent les équipes de Microsoft ne seraient pas des fermions de Majorana. Il y a de quoi y perdre son latin ! Nous reviendrons dessus plus loin.



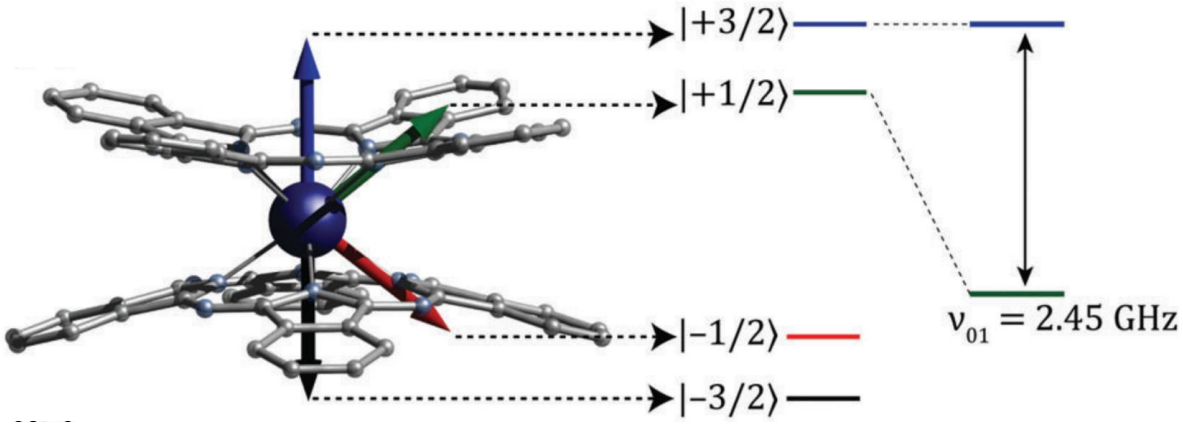
La technique des **aimants moléculaires** est aussi explorée, notamment à l'Institut Néel de Grenoble. Ils y sont fabriqués avec du terbium et ont quatre niveaux quantiques possibles. Le petit nom de ces aimants est SMM pour Single Molecule Magnets. Ils permettent donc de créer non pas des qubits mais des qudits, avec d=4. La molécule utilisée est du TbPc2 aussi dénommée bis(phthalocyaninato)terbium(III) (source).

On mesure leur état avec un interféromètre de mesure de phase. L'avantage de ces qudits est qu'ils sont très stables. L'inconvénient est qu'il est relativement difficile de les contrôler[79].

---

[78] Voir Experimental entanglement of 25 individually accessible atomic quantum interfaces, 2018 (11 pages) qui est la source du schéma.

SMM en TbPc2 (terbium)
aimants moléculaires avec quatre niveaux de spin



source : Molecular spin qudits for quantum algorithms, 2017 (13 pages)

Enfin, les qubits à **résonance magnétique nucléaire** (NMR) ont été testés par le passé et visiblement complètement abandonnés car ils ne scalent pas du tout.

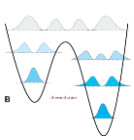
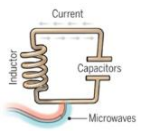
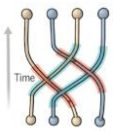
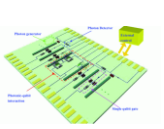
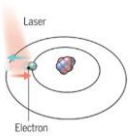
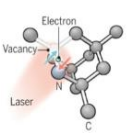
Aucune de ces techniques n'est pour l'instant éprouvée à grande échelle. Elles ont toutes leurs avantages et inconvénients qui se situent dans plusieurs dimensions :

- La **stabilité des qubits** qui s'évalue notamment par leur durée de cohérence des qubits. Associé au temps d'activation des portes quantiques et au taux d'erreur, il conditionne le nombre de portes quantiques que l'on peut enchaîner dans un algorithme.
- La possibilité de les **intriquer à grande échelle** et, si possible, sans être limité aux qubits immédiatement voisins.
- Le **niveau d'erreurs** dans les qubits qui s'évalue au niveau des portes quantiques unitaires (un seul qubit) et à deux qubits ainsi que de la mesure en fin de calcul.
- La **température de fonctionnement** des qubits et de l'électronique d'accompagnement. Il est fréquent d'avoir besoin de réfrigérer tout ou partie de l'ensemble à des températures cryogéniques inférieures à 20 mK. Cela génère quelques inconvénients que nous verrons plus loin.
- Le **niveau de miniaturisation** des qubits et de ce qui les entoure, qui conditionne la capacité à en augmenter le nombre. Cela favorise plutôt les qubits à spin d'électrons.
- Le **processus de fabrication** qui est moins cher lorsque c'est du silicium en technologie CMOS.

Nous verrons tout cela plus tard quand nous aborderons les différentes offres et projets d'ordinateurs quantiques.

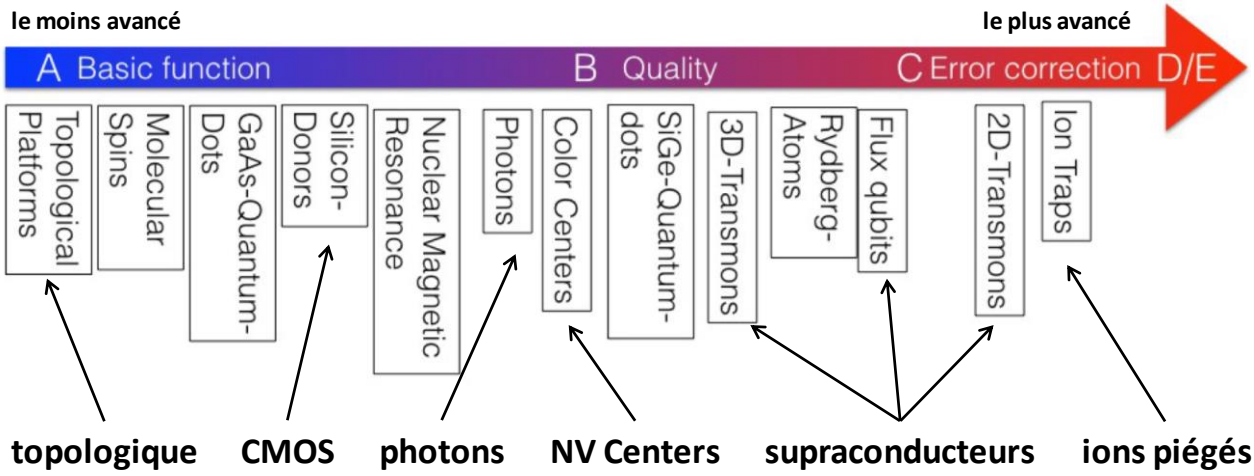
---

[79] Voir Molecular spin qudits for quantum algorithms, 2017 (13 pages). Ces travaux sont réalisés en partenariat avec L'institut Technologique de Karlsruhe en Allemagne. Et aussi la thèse Quantum information processing using a molecular magnet single nuclear spin qudit de Clement Godfrin, 2017 (191 pages).

							
	recuit quantique	**boucles supra-conductrices**	**qubits topologiques**	**optique linéaire**	**quantum dots silicium**	**ions piégés**	**cavités diamants**
qubit	supraconducteur effet Josephson	supraconducteur effet Josephson	quasi-particules faites de paires d'anyons	photons individuels	spin d'électrons dans semi-conducteur	ions piégés magnétiquement	spin de noyau d'atomes
# qubit	**2048 qubits** (D-Wave)	**50 qubits** (IBM) **72 qubits** (Google)	**N/A**	**quelques-uns**	**49 qubits** (Intel)	**53 qubits** (IonQ) **51 qubits** (MIT) **20 qubits** (IQOQI)	**6 qubits** (QDTI)
état	sens du courant	phase ou énergie de résonnance ou sens du courant	sens de l'anyon	phase de photon	spins d'électrons	niveau énergétique de l'ion piégé	niveau d'énergie de la cavité
portes	micro-ondes 5 GHz et effet Josephson	micro-ondes 5 GHz et effet Josephson	inversions 2D d'anyons	filtres polarisants et dichroïques	micro-ondes	laser	laser
mesure	magnétomètre	magnétomètre	fusion d'anyons	détecteurs de photons	consersion spins to charge	fluorescence	fluorescence

En résumé, voici *ci-dessus* les principaux types de qubits et leurs caractéristiques clés avec la nature des qubits, la manière de stocker leur état, la nature des portes quantiques qui les modifient et de la mesure de l'état des qubits. Le nombre de qubits annoncés par les uns et les autres est à prendre avec des pincettes. En effet, certains constructeurs annoncent des nombres de qubits qui ne sont pas « audité », en particulier en termes de niveau d'erreur et d'intrication.

Leur niveau d'avancement est décrit dans cet excellent document de l'équivalent allemand de l'ANSSI, Entwicklungsstand Quantencomputer (*état des lieux de l'informatique quantique*, 231 pages, en anglais). Il évoque d'autres technologies que celles qui sont citées dans mon inventaire et que je ne cite pas car elles ont pour l'instant peu de chances d'aboutir et n'ont été adoptées par aucun industriel ou aucune startup.



source : Entwicklungsstand Quantencomputer 2018 (231 pages)

Ordinateur quantique

Après avoir décrit les principes de base de la physique quantique puis ceux des qubits, nous allons aller plus loin et décrire le fonctionnement opérationnel et physique d'un ordinateur quantique[80].

Il ne suffit en effet pas de répéter à l'envie que les qubits sont capables d'avoir à la fois la valeur 0 et 1. Il reste à comprendre comment ils sont mis en œuvre d'un point de vue pratique ! La compréhension de cette mise en œuvre est ensuite à relier aux algorithmes quantiques. Qui plus est, les architectures d'ordinateurs quantiques dépendent étroitement des caractéristiques de leurs qubits et les algorithmes utilisés ne sont pas forcément les mêmes selon ces architectures !

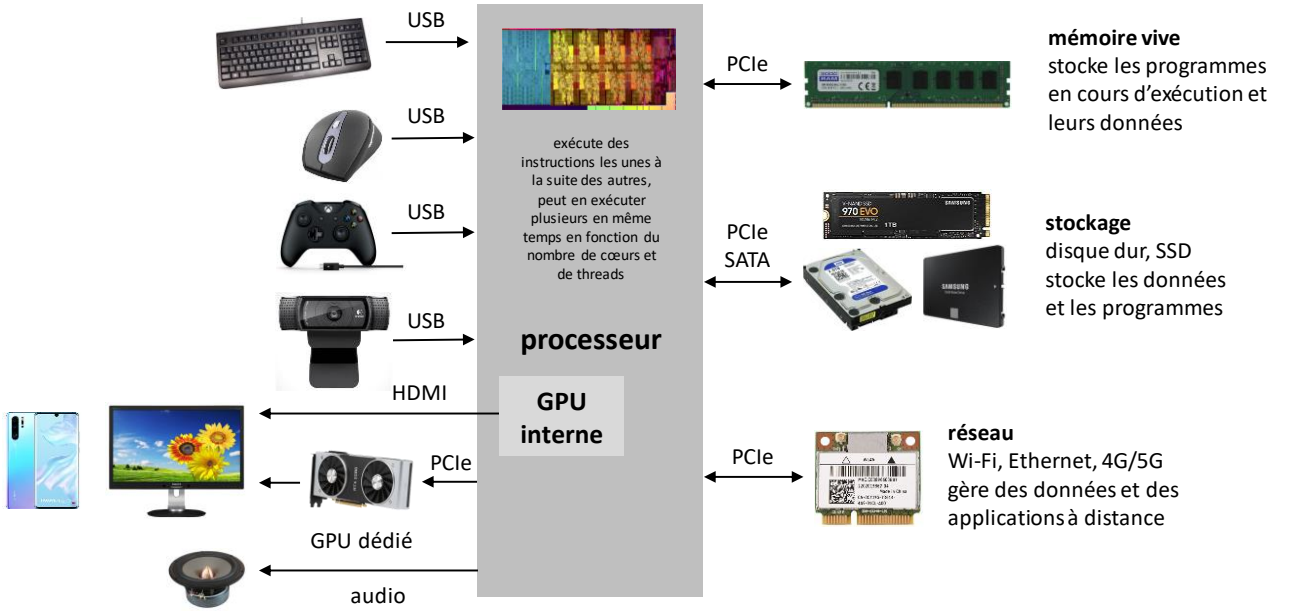
Certains comme le Français **Atos** ont cependant créé des outils de programmation quantiques qui se veulent indépendants des architectures matérielles. Un peu comme un compilateur C ou C++ qui peut générer du code binaire exécutable sur des processeurs différents. Cela peut fonctionner s'il existe une équivalence théorique entre les différents modèles d'ordinateurs quantiques. Il se trouve que c'est à peu près le cas donc tout va bien.

Pour être précis, dans ce qui suit, nous allons nous appuyer sur l'architecture d'ordinateurs quantiques universels à portes quantiques qui est la plus courante, celle des qubits à base de supraconducteurs à effet Josephson. Elle est notamment utilisée par IBM, Google, Intel et la startup américaine Rigetti. Une bonne part des éléments évoqués ici sont cependant applicables aux calculateurs quantiques utilisant d'autres types de qubits.

Mais avant, et comme rappel pédagogique, voici les grandes composantes d'un ordinateur traditionnel qui sont valables pour les smartphones, les tablettes, les ordinateurs personnels, les consoles de jeux et les serveurs. Le nœud gordien de l'ordinateur classique est son processeur qui est de plus en plus généraliste. Il récupère les données et programmes dans un système de stockage pour les copier en mémoire vive entièrement ou à la volée en fonction des besoins. Le processeur va ensuite lire les instructions des programmes en mémoire pour les exécuter les unes après les autres. Les données et programmes peuvent être récupérés à distance sur un réseau ou sur des serveurs distants sur Internet. L'ensemble est contrôlé par des interfaces physiques en entrée (clavier, souris, touchpad, manette de jeu, webcam, micros) et en sortie (un ou plusieurs écrans, audio). L'écran est alimenté par un processeur graphique qui est soit externe au processeur, pour les besoins de puissance comme en CAO ou pour les jeux vidéo, ou intégré au processeur comme c'est le cas pour tous les processeurs Intel de laptops et desktops.

---

[80] J'ai consulté un très grand nombre de sources d'informations pour réaliser cette partie, à la fois côté recherche et côté fournisseurs comme chez IBM ou D-Wave. A noter Quantum Computing Gentle Introduction du MIT, publié en 2011 (386 pages) qui décrit avec précision certains mécanismes des ordinateurs quantiques comme les méthodes de lecture de l'état des qubits. Il décrit aussi assez bien les fondements mathématiques utilisés dans les calculateurs quantiques. Vous pouvez aussi profiter d'une vidéo de 8 minutes d'un beau gosse américain, Dominic Walliman, qui vulgarise bien les basiques de l'ordinateur quantique !



Selon les configurations, le processeur est entouré d'un nombre plus ou moins grand de composants externes qui sont intégrés dans la carte mère. C'est le cas du chipset Z390 d'Intel qui complète les processeurs Core et gère une bonne part des entrées/sorties de l'ordinateur. Les modems Wi-Fi et cellulaires sont associés à des antennes. Il faut évidemment ajouter une alimentation interne et externe et une batterie pour les dispositifs mobiles.

Du côté thermique, c'est le processeur et le GPU qui chauffent le plus dans cet ensemble et qui requièrent une forme de refroidissement. Dans les systèmes embarqués comme dans les smartphones, celui-ci se fait par conductance de la chaleur et par air. Dans les PC, c'est complété par un ou plusieurs ventilateurs. Dans les cas les plus extrêmes, on utilise un circuit d'eau comme caloriporteur pour améliorer le dégagement de chaleur.

L'une des raisons du dégagement de cette chaleur est l'aspect non résersible des traitements des processeurs classiques. Nous verrons plus loin que les portes quantiques des processeurs quantiques sont réversibles ce qui modifie favorablement l'équation énergétique !

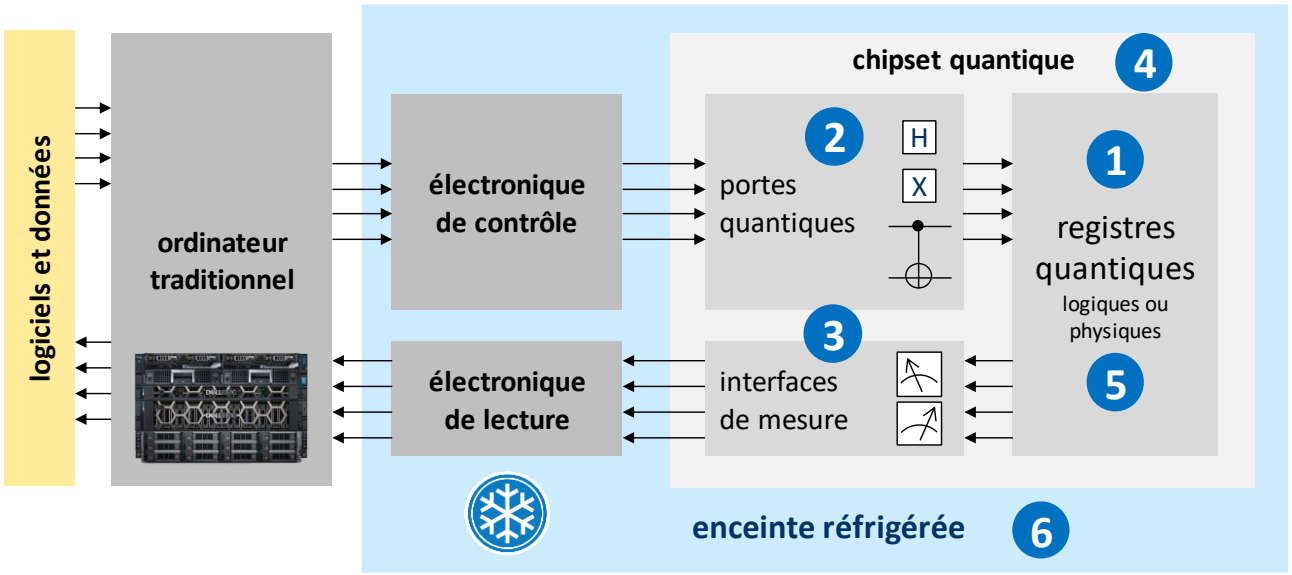
Poupées russes

Nous allons démarrer ici par une vue d'ensemble de l'architecture générale d'un ordinateur quantique.

Tout d'abord, un peu comme pour les GPU externes, les ordinateurs quantiques sont mis en œuvre comme des coprocesseurs d'ordinateurs traditionnels qui les alimentent. Un ordinateur quantique est toujours un coprocesseur d'un ordinateur traditionnel, comme peut l'être un GPU pour les jeux vidéos ou pour l'entrainement de réseaux de neurones dans le deep learning.

Ces ordinateurs classiques servent à exécuter les programmes destinés au processeur quantique pour les traduire en opérations physiques à réaliser sur les qubits et à en interpréter les résultats. Des données sont utilisées pour initialiser l'état des qubits.

L'ordinateur traditionnel pilote de près le fonctionnement de l'ordinateur quantique en déclenchant à un rythme précis les opérations sur les qubits qui sont réalisées par les portes quantiques. Ce déclenchement tient compte du temps d'exécution des portes quantiques et du temps de cohérence connu des qubits, c'est-à-dire, le temps pendant lequel les qubits restent en état de superposition.



En plus de son ordinateur classique de contrôle, notre ordinateur quantique comprend au minimum les composantes labellisées de 1 à 6 que nous allons analyser une par une, d'abord avec une vue d'ensemble ci-dessous, puis avec une vue plus détaillée juste après[81].

(1) Les **registres quantiques** sont des collections de qubits. En 2018, ils n'en comprennent qu'à peine quelques dizaines. Ce sont eux qui stockent l'information manipulée dans l'ordinateur et exploitent le principe de superposition permettant de faire cohabiter un grand nombre de valeurs dans ces registres et d'opérer des opérations dessus simultanément.

(2) Les **portes quantiques** sont des dispositifs physiques agissant sur les qubits des registres quantiques, à la fois pour les initialiser et pour y effectuer des opérations de calcul. Ces portes sont appliquées de manière itérative, au gré des algorithmes à exécuter. L'électronique de commande des qubits pilote les dispositifs physiques qui servent à initialiser, modifier et lire l'état des qubits. Dans les qubits supraconducteurs, les portes quantiques sont activées avec des générateurs de micro-ondes de fréquences comprises entre 5 et 10 Ghz. Ces micro-ondes circulent sur des fils électriques conducteurs entre leur source et le processeur quantique. Leurs générateurs prennent encore de la place. Ils ne sont pas très miniaturisés à ce stade, générant un facteur limitant du nombre de qubits qui sont intégrables dans un calculateur quantique.

[81] Pour réaliser le schéma *ci-dessus* qui explique tout cela, je me suis inspiré du slide 14 de la présentation Quantum Computing (and Quantum Information Science) de Steve Binkley, US Department of Energy, 2016 (23 slides).

(3) Des **dispositifs physiques de mesure de l'état des qubits** permettent d'obtenir le résultat des calculs à la fin du processus d'exécution séquentielle des portes quantiques. On applique généralement ce cycle d'initialisation, de calculs et de mesure plusieurs fois pour évaluer le résultat. On obtient alors par moyenne une valeur comprise entre 0 et 1 pour chaque qubit des registres de l'ordinateur quantique. Les valeurs lues par les dispositifs physiques de lecture sont ensuite converties en valeurs numériques et transmises à l'ordinateur classique qui pilote l'ensemble et permet l'interprétation des résultats. Dans les cas courants, comme chez D-Wave ou IBM, le calcul est répété au moins 1000 fois dans l'ordinateur quantique.

Les dispositifs de lecture sont reliés à leur électronique de contrôle via des fils supraconducteurs dans le cas des qubits d'ordinateurs supraconducteurs.

(4) Le **chipset quantique** comprend les registres quantiques, les portes quantiques et les dispositifs de mesure lorsqu'il s'agit de qubits à supraconducteurs ou à quantum dots. Les dispositifs sont plus hétérogènes pour les autres types de qubits, notamment ceux qui exploitent des lasers et des photons pour l'initialisation, les portes quantiques et la mesure des qubits. Les chipsets actuels ne sont pas très grands. Ils font la taille d'un capteur photo full-frame ou double-format pour les plus grands d'entre eux. Chaque qubit est relativement grand, leur taille se mesurant en microns alors que les transistors de processeurs modernes en CMOS ont des tailles maintenant inférieures à 20 nanomètres.

(5) Les **qubits logiques** regroupent des qubits physiques pour permettre une mise en œuvre de correction d'erreurs à l'échelle physique de l'ordinateur. D'autres méthodes utilisent des corrections d'erreurs au niveau algorithmique par l'utilisation de codes de correction d'erreurs à base de portes quantiques. La gestion des erreurs engendrées par les opérations effectuées sur les qubits est un des plus gros casse-tête de la mise au point d'ordinateurs quantiques.

(6) Une **enceinte cryogénisée** maintient généralement l'intérieur de l'ordinateur à une température voisine du zéro absolu. Elle contient une partie de l'électronique de commande et le ou les chipsets quantiques pour éviter de générer des perturbations empêchant les qubits de fonctionner, notamment au niveau de leur intrication et cohérence ainsi que pour réduire le bruit de leur fonctionnement. Le Graal serait de pouvoir faire fonctionner des qubits à température ambiante mais les architectures correspondantes comme dans les NV Vacancy ou cavités de diamants ne sont pas encore opérationnelles.

Voyons donc tout cela en détail !

Registres

Dans un ordinateur quantique, les qubits sont organisés par blocs qui constituent des registres. Un peu comme les registres 32 ou 64 bits des processeurs classiques actuels. L'histoire ne dit pas encore si les ordinateurs de plusieurs millions de qubits utiliseront des registres de cette taille ou des registres de taille raisonnable.

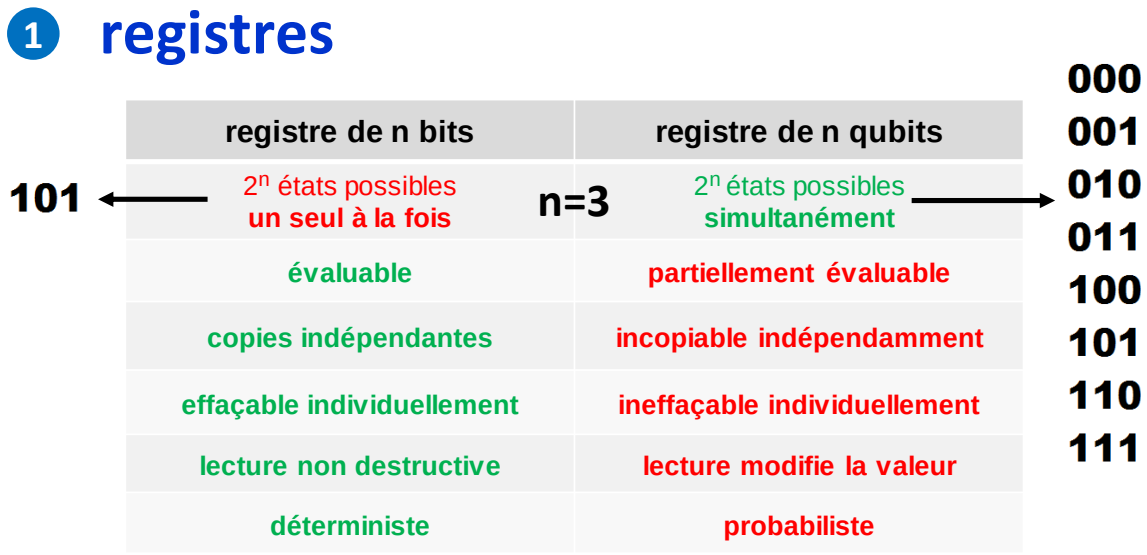
Les architectures envisagées sont diverses, comme celles qui utiliseraient des registres de qubits qui seraient ensuite reliés entre eux de diverses manières, via des portes quantiques et/ou de l'intrication.

La principale différence entre un registre de n qubits et un registre traditionnel de n bits est la quantité d'information qui peut y être manipulée simultanément.

Dans les ordinateurs classiques, ce sont par exemple des registres de 32 ou 64 bits qui stockent des entiers ou des nombres flottants sur lesquels sont réalisées des opérations mathématiques élémentaires.

Les qubits présentent l'avantage de pouvoir osciller en permanence entre la valeur 0 et 1, selon le principe de la superposition des états quantiques. L'oscillation est une vue de l'esprit qui ne correspond pas forcément à la réalité physique mais permet de se faire une idée conceptuelle de cette notion de superposition.

Un registre de n qubits peut donc avoir toutes les valeurs possibles à un moment donné. Pour prendre l'exemple d'un registre de 3 bits et de 3 qubits, le premier stockera une seule valeur à la fois comme 101 (5 en base 2) tandis que le registre de trois qubits va faire cohabiter par superposition toutes les valeurs possibles de ce registre, qui sont au nombre de 2 puissance 3, soient 8. C'est ce qui permet de faire des calculs à combinatoire exponentielle.



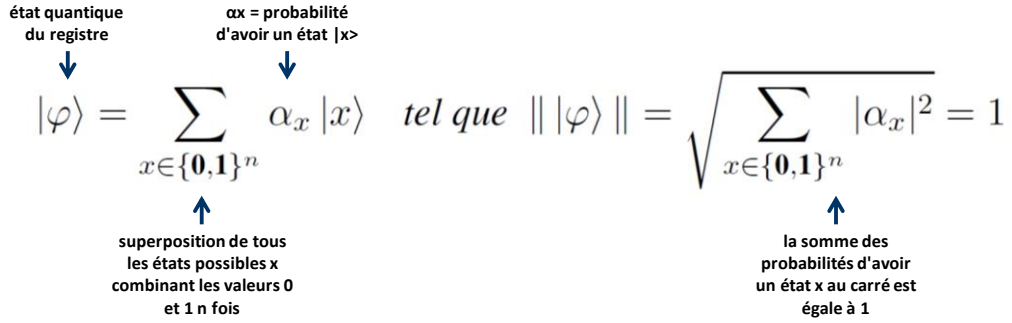
Ces 2^n états ne correspondent toutefois pas véritablement à une capacité de stockage d'information. C'est une capacité de superposition d'états auxquels on applique ensuite des traitements pour faire ressortir les combinaisons que l'on recherche selon un algorithme donné. Cela permet de tester plein d'hypothèses en parallèle pour faire ressortir la meilleure. L'information pertinente est ce résultat qui se manifeste après lecture sous la forme d'un registre classique de bits. La combinatoire de toutes les valeurs de registres pendant les calculs n'est pas une information utile en soi. C'est l'information qui en est extraite qui a de la valeur.

Ne croyez donc pas ceux qui vous font miroiter des applications de type "big data" grâce à la combinatoire des états des qubits. Comme cette combinatoire n'intervient que pendant les calculs et ni en entrée ni en sortie, il faut raison garder !

Si vous voyez cela dans un rapport d'analyste ou le marketing d'un fournisseur, vous serez à peu près sûr que leur auteur n'a pas compris grand chose au calcul quantique ou tout du moins aux questions d'échelles en termes de nombre de qubits à aligner.

Qui plus est, les algorithmes quantiques ne sont dans la pratique pas efficaces pour réaliser des traitements de big data[82]. Et à supposer que cela puisse fonctionner, il faudrait prendre en compte le temps de chargement d'éventuels gros jeux de données dans les ordinateurs quantiques, qui pourraient aussi leur faire perdre leur avantage algorithmique[83].

Les états superposés des registres vérifient une loi de distribution probabiliste selon laquelle le total de la probabilité de chaque état superposé au carré est égal à 1 comme indiqué dans les formules *ci-dessous*[84].



un algorithme quantique va créer un état de superposition de valeurs dans un registre quantique et va faire évoluer de poids de ces valeurs pour atténuer certaines et en faire ressortir une en particulier qui est la réponse à la question posée

Un calcul quantique va faire évoluer dans le temps la probabilité de chacune des combinaisons d'états de qubits (|x> dans la formule ci-dessous). L'idée est de faire converger après plusieurs opérations la valeur du registre quantique vers la valeur recherchée que l'on lit ensuite de manière classique pour obtenir une suite de n 0 et 1 contenant la réponse. Comme par exemple un nombre premier diviseur d'un nombre entier fourni en entrée.

Ceci est renforcé par le fait que lorsqu'on lit le contenu d'un qubit, on récupère 0 ou 1 et donc une seule combinaison des 0 et 1 des qubits du registre. En le faisant plusieurs fois de suite après avoir exécuté l'ensemble de l'algorithme, on récupère un % de 0 et un % de 1. Idem pour tous les qubits d'un registre.

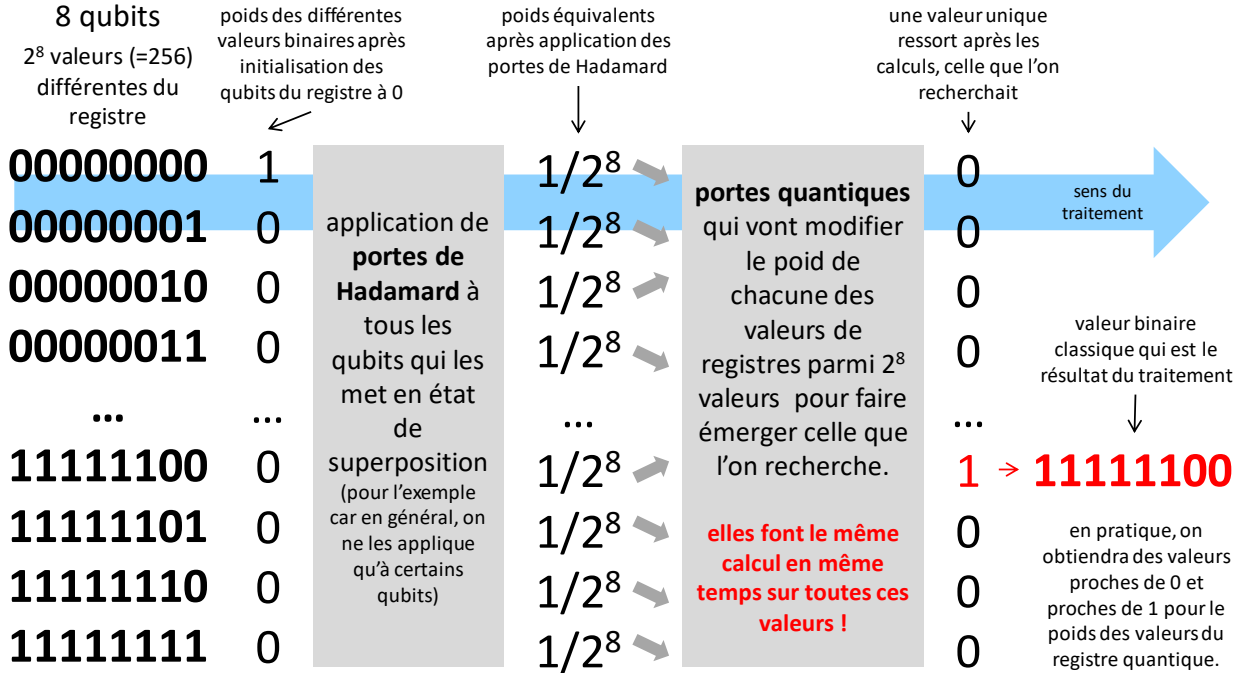
---

[82] Il commence cependant à apparaître des exceptions avec des méthodes hybrides d'accélération d'accès à des bases de données combinant des algorithmes classiques sur ordinateurs traditionnel et des algorithmes quantiques. Voir Quantum computers tackle big data with machine learning de Sarah Olson, Purdue University, octobre 2018.

[83] C'est très bien expliqué dans l'excellent panorama Quantum Computing: Progress and Prospects de l'académie des sciences US, 2019 (272 pages) : "*Large data inputs cannot be loaded into a QC efficiently. While a quantum computer can use a small number of qubits to represent an exponentially larger amount of data, there is not currently a method to rapidly convert a large amount of classical data to a quantum state (this does not apply if the data can be generated algorithmically). For problems that require large inputs, the amount of time needed to create the input quantum state would typically dominate the computation time, and greatly reduce the quantum advantage.*".

[84] Ce schéma est inspiré de Modèles de Calcul Quantique (30 pages), de Pablo Arrighi et Simon Perdrix, un document très bien fait qui explique avec quelques formules mathématiques pas trop compliquées comment fonctionne le calcul quantique. Il explique notamment très bien l'algorithme de Deutsch-Jozsa sur lequel je reviendrai dans la partie suivante de cette série.

Voici une autre représentation graphique du principe évoqué ci-dessous. C'est juste pour la pédagogie car dans la pratique, on n'applique pas de porte de Hadamard à tous les qubits d'un registre et les valeurs qui ressortent ne sont pas pile poil 0 et 1 pour le poids de chacune des valeurs possibles du registre. On obtient fait généralement des valeurs proches de 0 et 1.



On ne récupère donc pas 2^n valeurs dans la pratique, mais n nombres flottants compris entre 0 et 1 avec une précision dépendante de la précision de la mesure de l'état des qubits et du bruit qu'ils subissent de l'environnement et qui perturbe leur état de superposition. Mais cela dépend des algorithmes. Pour la majorité d'entre eux, une information binaire en sortie est suffisante comme pour l'algorithme de factorisation de nombres entiers de Peter Shor.

On est sinon contraint par le **théorème de Holevo** de 1973 qui prouve qu'avec n qubits, on ne peut pas récupérer plus que n bits d'information après un calcul quantique (source) !

Au stade actuel de mise au point des qubits, leur taux d'erreur est situé aux environs de 0,5% environ et il faudrait idéalement qu'il soit de 0,01% voire 0,0001%. Ce taux d'erreur s'évalue d'ailleurs au niveau de la stabilité de chaque qubit pris isolément et des opérations de portes quantiques portant sur deux qubits. La superposition des valeurs dans les registres quantiques est préservée pendant les opérations de portes quantiques qui présentent la particularité de ne pas faire sortir les qubits de leur état de superposition. Seule la mesure le fait. C'est la magie des algorithmes quantiques que de l'exploiter pour faire ressortir à la fin le résultat recherché. Vous suivez ?

Cela ne présente donc pas grand intérêt de comparer l'énorme combinatoire des registres qubits avec le nombre de particules dans l'Univers comme certains le font souvent. Ce ne sont pas des données équivalentes. Une combinatoire d'états n'est pas homothétique avec un nombre d'objets.

Avec un nombre d'objets donné, la combinatoire de ces objets représentera toujours un nombre largement supérieur au nombre d'objets pris en référence. Imaginez donc la combinatoire pour positionner dans l'espace toutes les particules élémentaires de l'Univers !

Par contre, sorti de cette combinatoire, les qubits ont plein d'inconvénients en opposition totale avec les bits classiques. On ne peut ni copier classiquement ni effacer individuellement la valeur des qubits lorsqu'ils sont ensuite intriqués entre eux. Leur mesure les modifie. Ce sont des objets probabilistes délicats à manipuler. Par contre, sans en connaître la valeur interne (le fameux vecteur représenté par la sphère de Bloch vue dans la partie précédente), on peut agir dessus avec des portes quantiques, que l'on va voir juste après.

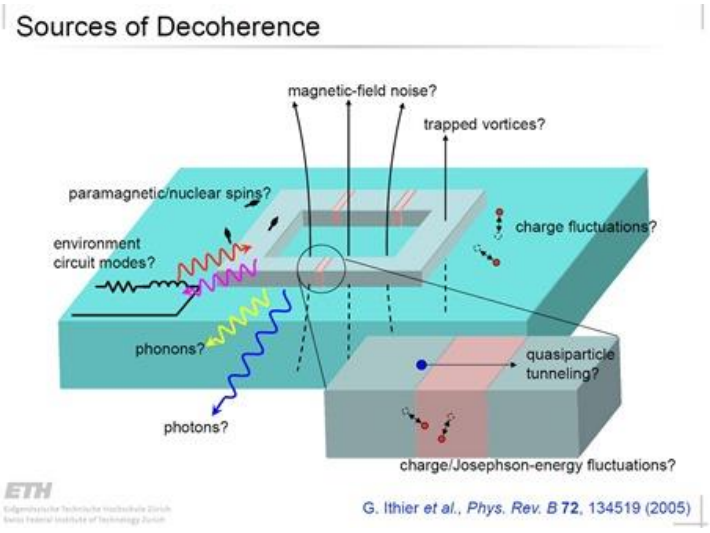
Un qubit est cohérent lorsqu'il est bien en état de superposition entre les deux niveaux possibles du qubit physique. Le temps de cohérence est une indication de la durée pendant laquelle les qubits d'un registre restent cohérents, donc en état de superposition.

Pour être précis, le temps de cohérence est celui au bout duquel les qubits perdent leur cohérence. Il se mesure généralement avec deux paramètres :

- **T1** pour la fin de cohérence liée à une perte d'amplitude (« energy relaxation »).
- **T2** pour un déphasage (rotation autour de l'axe z dans la sphère de Bloch).

Lorsque l'on effectue une mesure de l'état d'un qubit, on provoque sa décohérence puisque la mesure amène le qubit dans l'un de ses deux états de base possibles, en supprimant la superposition.

D'autres événements physiques peuvent provoquer cette fin de superposition, ou décohérence. Ils proviennent du "bruit", des chocs entre atomes et autres perturbations physiques[85].



On y voit notamment évoqué le bruit magnétique, ce qui explique pourquoi D-Wave isole ses enceintes d'ordinateur quantique avec 16 couches métalliques pour limiter l'impact du magnétisme terrestre sur ses qubits. La gravitation contribue aussi à la décohérence des qubits[86].

[85] Voici un petit inventaire des sources de bruit pour ce qui est des qubits supraconducteurs. Le schéma de cette page est issu de la présentation Sources of decohence, de l'ETH Zurich, 2005 (23 slides).

[86] Voir notamment Gravitational Decoherence, 2017 (78 pages).

On évite une partie de ces effets en refroidissant les qubits à une température proche du zéro absolu, mais ce n'est pas suffisant. Les chercheurs travaillent donc d'arrache-pied pour faire en sorte que le temps de cohérence des qubits soit le plus long possible et le bruit qui affecte les qubits le plus faible possible.

C'est une situation paradoxale : les qubits restent cohérents, donc en état de superposition, si on ne les dérange pas, mais on passe son temps à les déranger avec les opérations des portes quantiques qui agissent dessus ! En termes physiques, on veut donc en obtenir le beurre et l'argent du beurre !

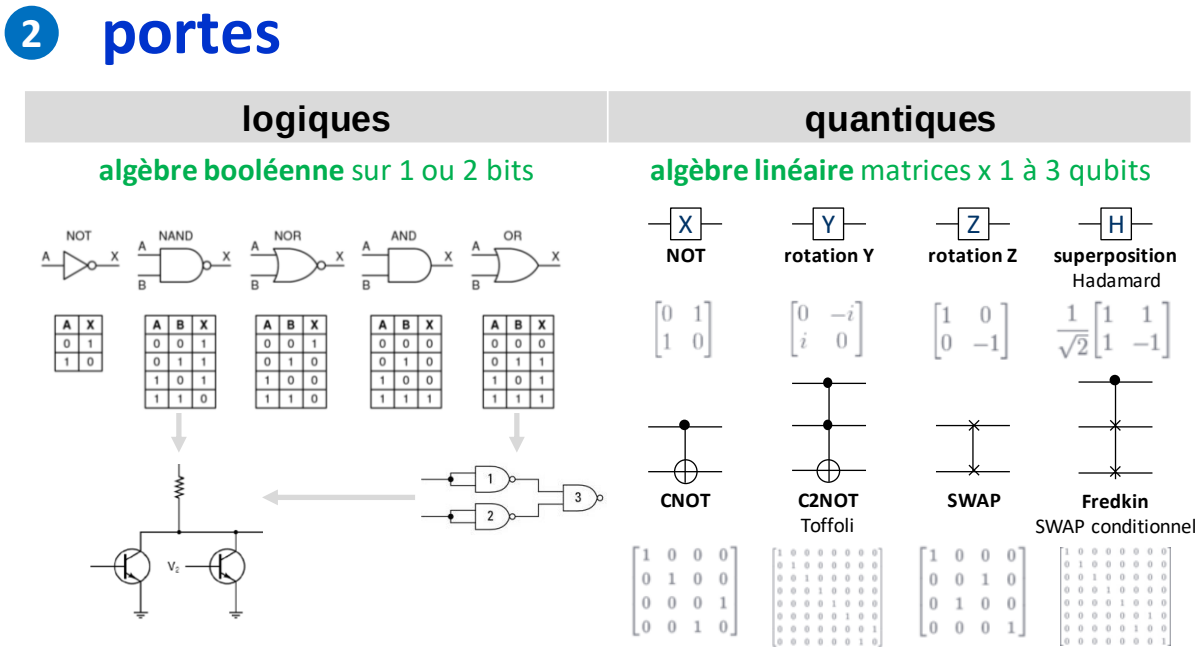
Portes

Dans l'informatique classique, les portes logiques exécutent de l'algèbre booléenne avec des tables de décision en fonction des bits en entrée. Il y a plusieurs types de portes logiques à une et deux entrées, dont la porte NAND qui est intéressante car elle est universelle et n'utilise que deux transistors. On peut théoriquement créer les autres portes booléennes avec des portes NAND.

En général, les portes logiques sont cependant panachées dans les circuits. Un processeur **Intel** Core i5/7 avec de 5 milliards de transistors va comprendre au moins 1 à 2 milliards de portes logiques.

Un processeur est évidemment très complexe avec des portes qui gèrent l'accès à une mémoire cache et aux registres et la lecture de programmes qui définissent les portes à utiliser dans les calculs.

A partir de là, on peut presque tout faire ! Ces opérations sont générées à la fréquence d'horloge du processeur, exprimée en MHz ou, le plus souvent, en GHz.



Les qubits qui stockent chacun un vecteur à deux dimensions subissent de leur côté des opérations via des portes quantiques qui leur appliquent des opérations d'algèbre linéaire sous forme de matrices 2x2 de nombres réels et complexes comme représentées *ci-dessus,* pour les portes unitaires. Ces matrices ont une particularité : multipliées par leurs transconjuguées, elles donnent une matrice d'identité, soit 1 dans la diagonale et 0 ailleurs. Elles sont dites « unitaires ».

Les portes quantiques modifient l'information des qubits sans la lire. Elles permettent aussi à l'information de circuler entre les qubits. Elles ne sont pas destructrices de l'état des qubits ou de leur cohérence contrairement aux systèmes de mesure qui interviennent en fin de calcul.

Comme pour la logique booléenne, il existe des portes unitaires agissant sur un seul qubit et des portes agissant sur plusieurs qubits de manière conditionnelle.

Dans les portes unitaires, les vecteurs à deux dimensions représentant l'état des qubits sont multipliés par des matrices unitaires. L'opération provoque une rotation du vecteur représentant la valeur du qubit en état de superposition dans la sphère de Bloch qui le représente géométriquement. Mais la norme du vecteur est stable, à 1.

Les principales portes unitaires sont :

- La **porte X** ou **NOT** qui réalise une inversion. Un 0 devient un 1 et réciproquement. Mathématiquement, elle intervertit le α et le β du vecteur à deux composantes qui représente l'état du qubit. Cette porte est souvent utilisée pour initialiser à 1 l'état d'un qubit en début de processus qui est par défaut à 0.
- La **porte Y** qui réalise une rotation d'un demi tour autour de l'axe Y dans la sphère de Bloch.
- La **porte Z** qui est un changement de signe appliqué sur la composante beta du vecteur du qubit. Les portes X, Y et Z sont dites "portes de Pauli"[87].

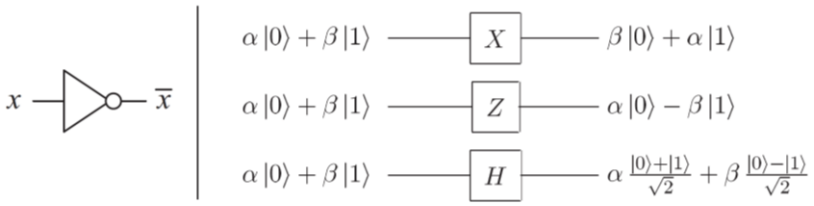


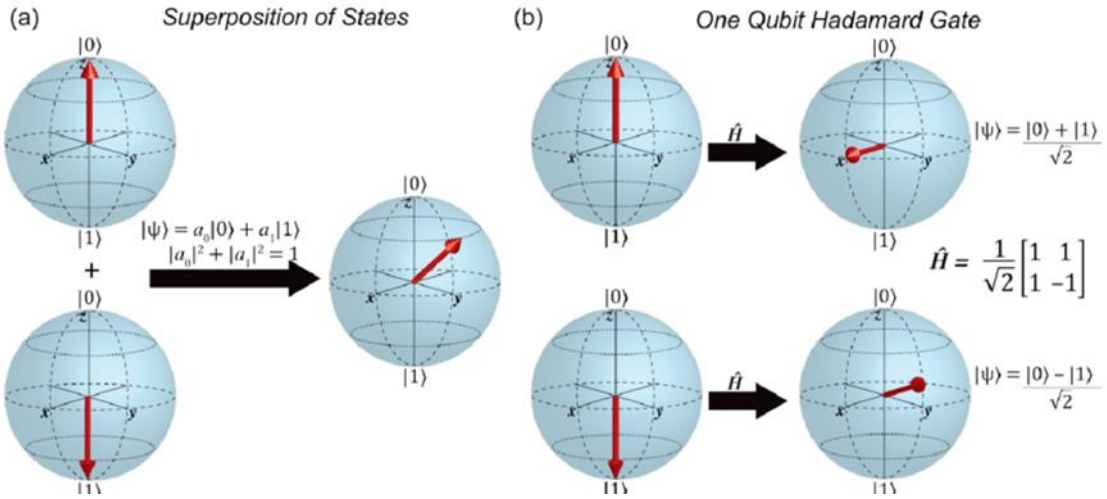
Figure 1.5. Single bit (left) and qubit (right) logic gates.

- La porte **S** qui génère un changement de phase, ou une rotation d'un quart de tour autour de l'axe Z (vertical).

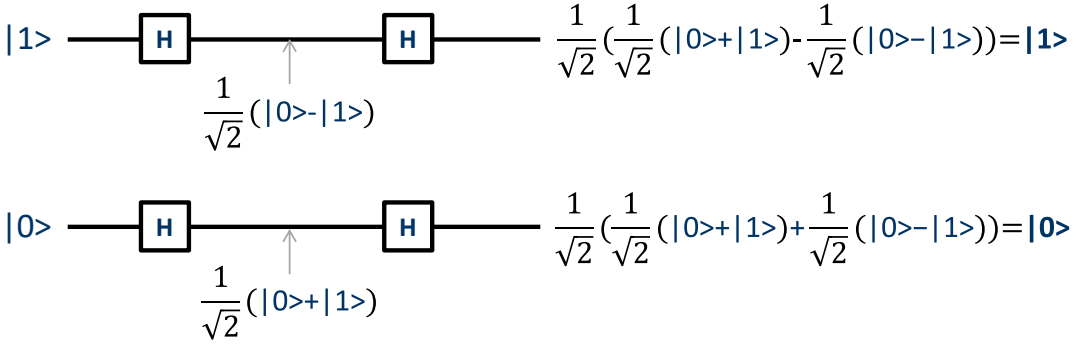
$$S \quad \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

[87] Source de l'illustration : Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages).

- La **porte Hadamard-Walsh** qui met un qubit à 0 ou 1 dans un état superposé "0 et 1". Elle est fondamentale pour générer cette superposition d'états dans les registres que nous avons décrite dans la partie sur les registres. La porte de Hadamard est très souvent utilisée pour initialiser un registre quantique afin de générer cette combinatoire de 2^n valeurs différentes cohabitant simultanément dans un registre de n qubits. Par contre, les portes quantiques qui vont intriquer entre eux des qubits vont réduire cette combinatoire car les qubits intriqués vont être en quelque sorte synchronisés, et réduire la combinatoire de superposition d'états du registre quantique[88]. Voici une représentation de l'effet de cette porte sur un qubit initialisé à 0 ou 1 dans la sphère de Bloch (source).



Notons que si l'on applique deux fois de suite une porte de Hadamard à un qubit, on revient au point de départ. Le formalisme mathématique appliqué à un seul qubit l'illustre simplement. Mais ceci fonctionne en théorie, seulement si le taux d'erreur des portes est nul. Comme il ne l'est pas, on n'obtient pas un |0> ou un |1> parfaits.



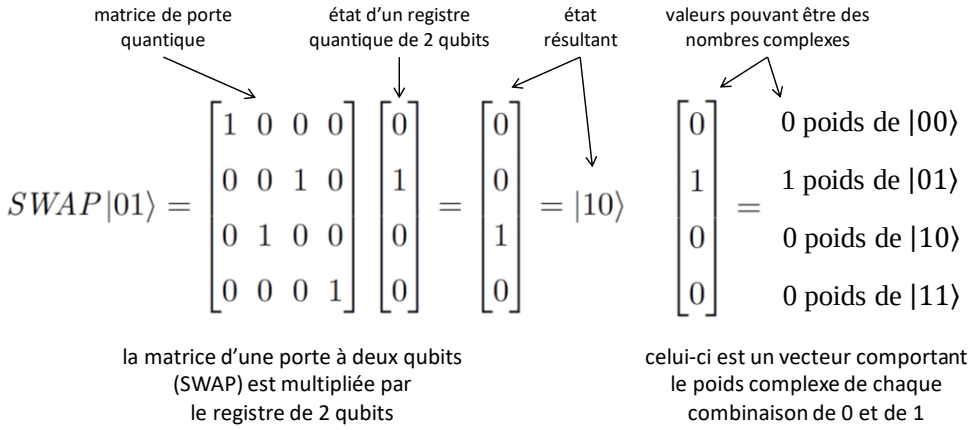
une porte de Hadamard chaînée deux fois regénère le même état de départ pour |0> et |1>

[88] Certains spécialistes indiquent que la puissance exponentielle de calcul de l'ordinateur quantique vient de l'intrication. J'ai l'impression qu'elle vient plutôt de la superposition des états des qubits dans les registres. L'intrication est utilisée dans les portes quantiques à plusieurs qubits pour relier conditionnellement les qubits entre eux et dans la pratique réduire la superposition d'état. A la fin du calcul, les registres ont convergé via ces portes quantiques vers le résultat attendu. Bref, on part d'une sorte d'exponentielle de N (N = le nombre de qubits) et on termine avec N bits.

Nous avons ensuite des portes à deux ou trois qubits comme :

- La **porte CNOT**, ou « où exclusif », qui est une inversion de la valeur d'un qubit conditionnée par la valeur 1 d'un autre qubit.
- La **porte C2NOT** ou de **Toffoli** est une inversion de la valeur d'un qubit conditionnée par la valeur 1 de deux autres qubits.
- La **porte CZ**, ou Control-Z, qui est une porte Z conditionnelle.
- La **porte SWAP** intervertit les valeurs quantiques de deux qubits. Elle peut d'ailleurs être générée à partir de l'enchaînement de trois portes CNOT consécutives.
- La **porte de Fredkin** est une porte SWAP conditionnée par l'état d'un troisième qubit. Elle a donc trois entrées.
- La **porte Control-S** qui permet un changement de phase d'un qubit contrôlé par l'état d'un qubit.

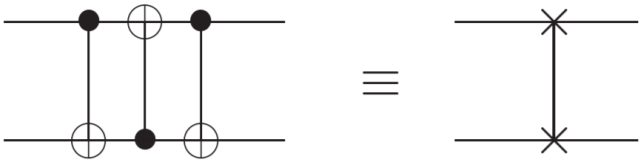
Ces portes à 2 ou 3 qubits y appliquent donc des transformations matricielles de respectivement 4x4 ou 8x8 entrées aux qubits en entrée. Soit 1 qubit = 2 nombres, 2 qubits = 4 nombres, 3 qubits = 8 nombres, la taille des matrices de transformation de l'état des qubits étant de 2 puissance le nombre de qubits transformés. Pourquoi donc ? Parce que ces matrices s'appliquent à un vecteur dont les éléments sont chacun des états superposés possibles de la combinaison des qubits, et ce nombre d'états est 2^N, N étant le nombre de qubits.



Les portes de Toffoli et Fredkin sont dites complètes, car elles sont capables d'engendrer toutes les portes logiques de la combinatoire des circuits.

Un jeu de portes est dit universel lorsqu'il permet de recréer par assemblage temporel toutes les portes requises par les algorithmes courants. Plusieurs combinaisons de portes universelles sont possibles comme une porte CNOT et une SWAP, ou bien une porte de Hadamard complétée d'une porte CNOT. Une seule porte Toffoli est universelle.

Selon Artur Ekert, presque toutes les portes à deux qubits sont universelles. La combinaison de portes universelles mises en œuvre physiquement dans les ordinateurs quantiques dépend de leur type et des dispositifs physiques qui agissent sur les qubits.



trois portes CNOT **une porte SWAP**

les portes universelles permettent de reconstituer les autres portes logiques
il en faut deux, une simple et une à deux qubits pour tout faire

Les ordinateurs quantiques utilisent aussi des "*ancillae qubits*" ou qubits de contrôle de valeurs déterminée (0 en général) pouvant être combinées avec des qubits indéterminés (ceux du calcul).

Ils sont aussi utilisés pour la correction quantique d'erreurs (QEC) expliquée plus loin. On n'en lit pas la valeur à la fin des traitements. C'est une sorte de poubelle de qubits utilisés pendant les calculs !

Les portes quantiques ont la particularité d'être théoriquement réversibles. On peut revenir en arrière si bon nous chante et sans perdre d'information en appliquant dans l'ordre inverse les portes quantiques qui viennent d'être appliquées à un registre de qubits. L'intérêt de la réversibilité est de ne pas consommer autant d'énergie qu'avec des portes réverssibles comme dans l'informatique traditionnelle. Mais cela dépend de nombreux paramètres et des technologies de qubits, notamment le coût énergétique du déclenchement de chaque porte quantique.

C'est d'ailleurs une voie possible de réduction de consommation d'énergie pour les ordinateurs traditionnels, mais dont l'exploration est laborieuse. Il est en effet possible de créer des portes logiques traditionnelles réversibles[89] ! Cela n'a pas aboutit pour autant industriellement à ce jour.

La notion de réversibilité d'un calcul quantique permettrait d'éviter de jetter de l'énergie par la fenêtre. On pourrait exécuter un algorithme quantique, lire le résultat de manière non destructrice si il aboutit à des qubits dans des états de base 0 ou 1, dite base computationnelle, puis dérouler à l'envers cet algorithme et revenir au point de départ initial… avec des qubits initialisés à 0 ! Autre point à noter : elle aurait un autre impact qui serait de doubler le temps de calcul. Le bruit quantique perturberait probablement l'opération et introduirait des erreurs mais pas suffisamment pour réduire l'impact énergétique de la méthode[90].

---

[89] Voir par exemple Generalized Reversible Computing and the Unconventional Computing Landscape de Michael Frank, 2017 (34 slides) et Foundations of Generalized Reversible Computing de Michael Frank, 2017 (18 pages).

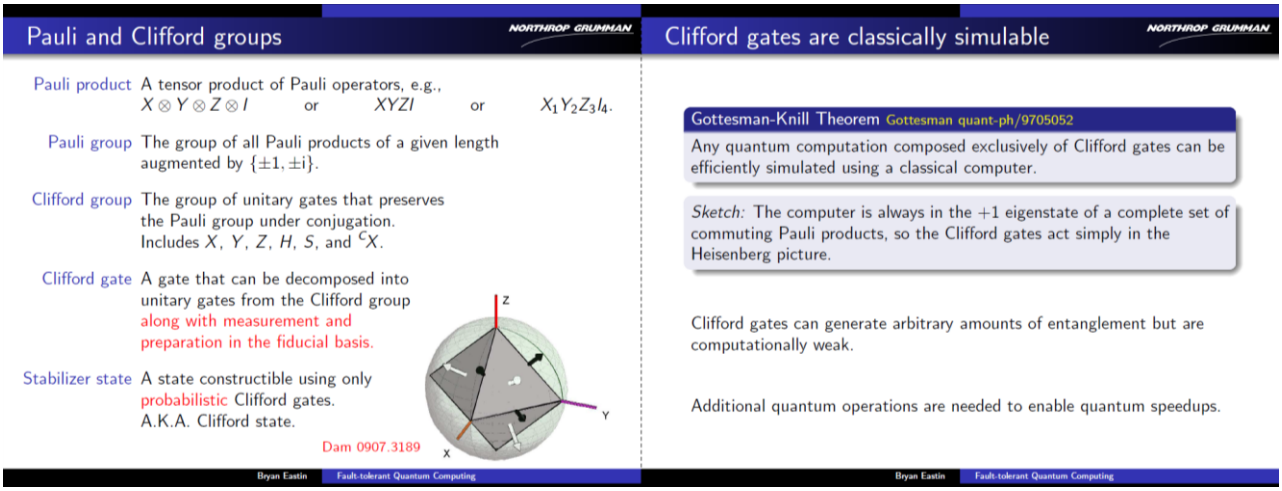
[90] Voici quelques sources d'information sur le sujet des portes quantiques qui ont éclairé ma lanterne : Universality of Quantum Gates de Markus Schmassmann, 2007 (22 slides), An introduction to Quantum Algorithms de Emma Strubell, 2011 (35 pages), L'ordinateur quantique, note de l'Ambassade de France à Washington de Daniel Ochoa, 2008 (70 pages), Equivalent Quantum Circuits de Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada, 2011 (12 pages) et The Future of Computing Depends on Making It Reversible de Michael P. Frank, 2017.

Ceci étant dit, les qubits peuvent subir d'autres opérations. Ils peuvent être stockés en mémoire quantique comme nous le verrons plus loin. Ils peuvent aussi servir à encoder deux bits au lieu d'un seul, dans ce que l'on dénomme le « superdense coding » que je n'ai pas eu le temps de bien creuser[91] mais qui ne fonctionne que dans des conditions particulières.

Les mathématiques des portes quantiques ont donné lieu à la création de nombreux concepts et théorèmes que je ne vais pas détailler ici. A la fois parce qu'ils sont très complexes et aussi… parce que je ne les ai pas bien assimilés !

Il y a notamment le **groupe de Clifford**, qui contient des portes unitaires qui sont simulables facilement et en temps polynomial sur ordinateurs classiques selon le théorème de Gottesman-Knill. Une porte de Clifford est une porte quantique qui peut être décomposée en portes du groupe de Clifford.

Ces notions d'algèbre linéaire ont un lien avec les techniques de correction d'erreurs du calcul quantique[92].



Entrées et sorties

Les microprocesseurs traditionnels sont composés de portes logiques fixes, gravées dans le silicium, et de bits 'mobiles', se présentant comme des impulsions électriques qui se propagent dans le circuit à travers les différentes portes. Le tout à une certaine fréquence, qui se compte souvent en GHz, réglée par une horloge à quartz.

Dans un ordinateur quantique, la première étape des traitements consiste à mettre le système quantique représenté par son ou ses registres quantiques dans un état initial. On dit que l'on "prépare le système". Les différents registres sont d'abord configurés physiquement dans l'état 0, chaque qubit étant à 0. L'initialisation qui suit consiste à faire agir différents opérateurs comme la transformation de Hadamard pour créer une superposition 0+1 ou la porte X pour modifier cette valeur 0 en 1.

---

[91] Voir From Classical to Quantum Shannon Theory 2019 (768 pages) qui décrit l'application de la théorie de l'information de Shannong à l'informatique quantique. Ainsi que On superdense coding, août 2018, de Fred Bellaiche, un ingénieur d'Econocom qui publie de très intéressants articles scientifiques bien vulgarisés sur le quantique.

[92] Voir Fault-tolerant Quantum Computing de Brian Easti, 2014 (55 slides), d'où proviennent les deux slides de cette page.

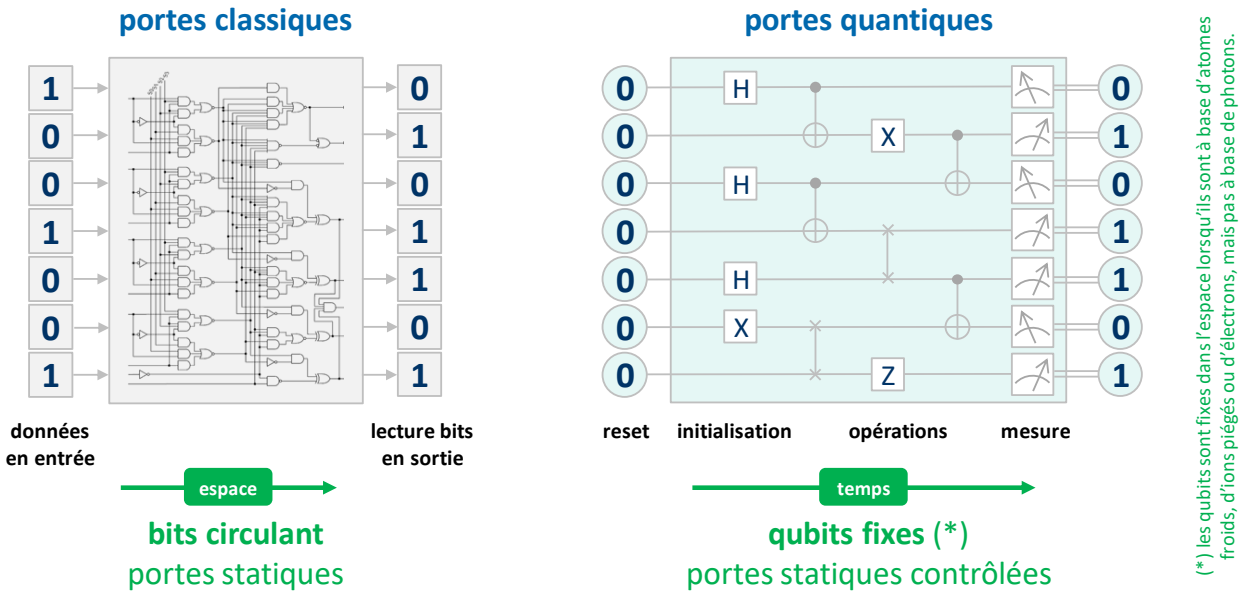
Une fois cette initialisation réalisée sont lancées séquentiellement des opérations de portes sur les qubits en fonction de l'algorithme à exécuter. Enfin, on lit la valeur des qubits à la fin des traitements, ce qui a pour effet de modifier leur état quantique.

Physiquement, les qubits sont de deux sortes : stationaires ou mouvants (flying). Ceux qui reposent sur des électrons piégés, des ions piégés et des courants supraconducteurs sont stationnaires. Les flying qubits sont à base de photons qui eux circulent physiquement de portes quantiques en portes quantiques.

Dans les cas de qubits stationnaires, les portes quantiques ne bougent pas non plus. Elles sont activées dynamiquement par des circuits électroniques ou des lasers et opèrent sur les qubits.

Les diagrammes de représentation des algorithmes quantiques pour ordinateurs quantiques à portes universelles (*ci-dessous* à droite) sont en fait le plus souvent des schémas temporels alors que pour les portes logiques classiques, il s'agit un diagramme physique.

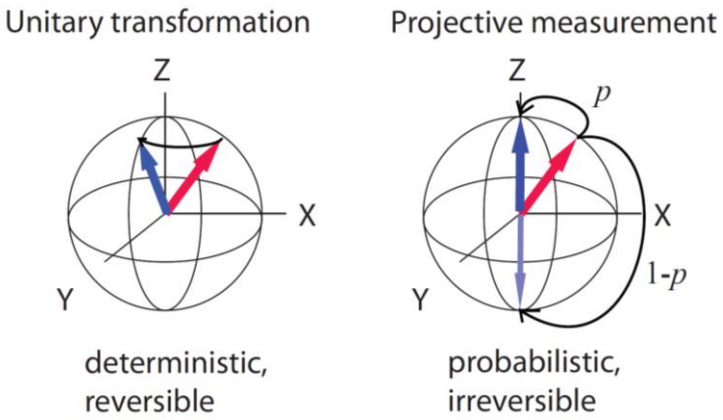
3 entrées et sorties



J'ai mis beaucoup de temps à comprendre cela car une partie de la littérature technique sur les processeurs quantiques assimile les lignes horizontales de ces algorithmes à des "fils" reliant les qubits en entrée à des qubits en sortie, ce qui est entièrement faux.

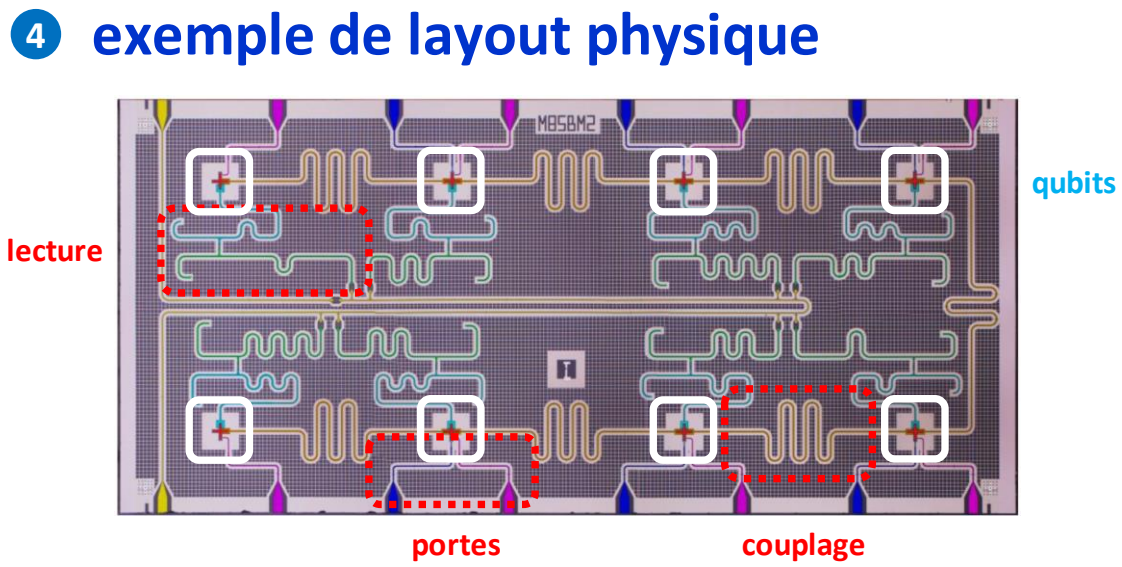
Dans la partie droite décrivant un algorithme quantique, il n'y a pas de fils physiques reliant les qbits entre une entrée et une sortie, les portes étant sur leur chemin. C'est un schéma temporel, en tout cas pour toutes les architectures de qubits à l'exception de ceux qui exploitent des photons qui eux se déplacent dans l'espace !

Alors que les portes quantiques sont réversibles, la lecture de l'état des portes est irréversible. Ce n'est pas une rotation dans la sphère de Bloch mais une projection sur l'axe Z de l'amplitude, qui va rendre un 0 ou un 1 avec une probabilité dépendante de l'état du qubit[93]. La mesure de l'état d'un qubit modifie cet état. Il se retrouve dans l'état 0 ou 1.



Layout physique

Pour mieux comprendre l'explication précédente, voici un *layout* de chipset de 8 qubits supraconducteurs, issu de l'ETH Zurich qui date déjà de quelques années[94]. Ce n'est qu'un exemple illustratif car les layouts physiques sont très variables d'un type de qubit à un autre. Mais le principe décrit ici est commun à tous les ordinateurs quantiques à base de supraconducteurs. L'exception qui confirme la règle est celle des ordinateurs utilisant des qubits à base de photons qui circulent – très rapidement – dans les circuits et qui traversent des portes quantiques.



8 supraconducting qubits, ETH Zurich

On y voit très bien que, dans le circuit :

- Les **qubits** sont situés dans les rectangles blancs. Ce sont eux qui intègrent une boucle à effet Josephson. Ils sont physiquement immobiles dans le circuit.

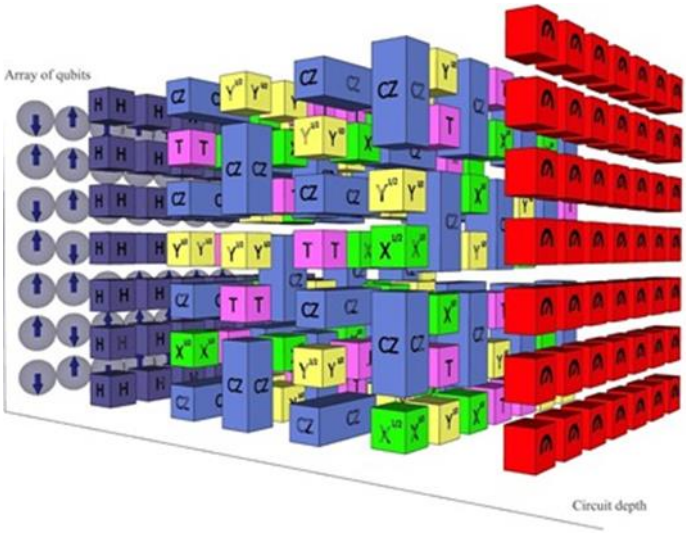
[93] Source du schéma : A computationally universal phase of quantum matter de Robert Raussendorf (41 slides).

[94] Source de l'image : The European Quantum Technologies Roadmap 2017 (30 pages).

- Ils sont reliés entre eux par des **circuits de couplage** qui servent à contrôler leur intrication.
- Des **contacts bleus et violets** permettent d'agir sur les qubits et d'activer, selon la fréquence, des portes quantiques. Ils permettent avec le circuit d'intrication d'activer des portes universelles utilisées par combinaison pour recréer les autres portes quantiques nécessaires à l'exécution des algorithmes. Dans la pratique, avec les qubits supraconducteurs, ces "pins" sont alimentés via des câbles par des sources de courants à très haute fréquence, dites micro-ondes, comprises entre 5 et 10 GHz. Ces fréquences doivent être différentes entre les qubits adjacents d'un même circuit. C'est la combinaison de ces fréquences qui va déclencher différents types de portes quantiques et d'intrications entre qubits adjacents.
- La **mesure** a lieu avec d'autres circuits, eux aussi fixes dans le composant. Dans les qubits supraconducteurs, ce sont des magnétomètres qui sont ensuite reliés avec l'extérieur de l'enceinte sous vide et réfrigérée par des câbles supraconducteurs.

Dans un ordinateur quantique, on cherche à faire en sorte que les qubits interagissent entre eux mais le moins possible avec leur environnement jusqu'à ce que l'on mesure leur état ! C'est pour cela qu'ils sont généralement refroidis à une température proche du zéro absolu et isolés magnétiquement de l'extérieur. Le choix des matériaux des chipsets joue aussi un rôle pour minimiser le bruit qui pourrait affecter les qubits et les faire sortir de leur état de superposition.

Et voici une autre représentation, originaire de Google, expliquant la même chose, vue dans : The Question of Quantum Supremacy, paru en mai 2018 et qui référence deux papiers sur la suprématie quantique recherchée par Google : Characterizing Quantum Supremacy in Near-Term Devices, 2016 (23 pages) et A blueprint for demonstrating quantum supremacy with superconducting qubits, 2017 (22 pages).



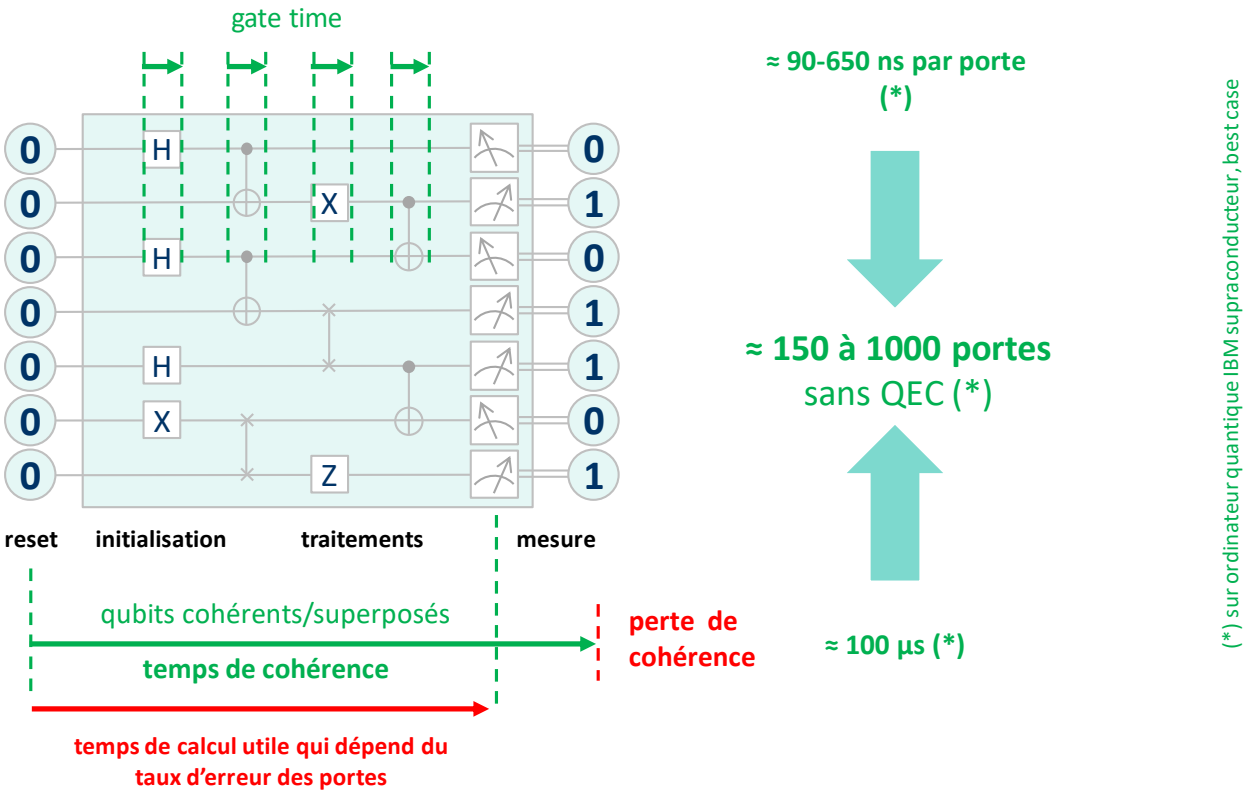
Dans le schéma *ci-dessous*, voici le pourquoi du comment de la relation entre le temps d'activation des portes ("gate time") et le temps de cohérence pendant lequel les qubits restent en place et surtout, restent intriqués et en état de superposition. Et je vous passe les histoires de temps de "relaxation" après l'activation des portes.

Sachant que l'intrication ne concerne a priori qu'une partie des qubits des registres. Les ordres de grandeur de ces temps pour un ordinateur quantique classique, notamment supraconducteur, donnent au mieux un rapport de 1 à 500 entre temps de portes et durée de cohérence. Ce qui veut dire que l'on sera limité pour ce qui est du nombre de portes quantiques utilisables dans un algorithme, ce d'autant plus qu'une bonne

part de ces portes sera utilisée pour les codes de correction d'erreurs. Dans les premières générations d'ordinateurs quantiques d'IBM, les portes X, d'Hadamard et CNOT duraient respectivement 130 ns, 130 ns et 650 ns.

Ces indications fournissent une limite haute du nombre de portes qui peuvent être enchaînées dans un algorithme quantique. A noter que ces temps sont plus longs pour les ordinateurs quantiques à ions piégés mais les gate time y sont aussi plus longs. Dans les qubits CMOS, les temps de cohérence sont plus longs et les gate time sont faibles.

Le temps de calcul effectif est cependant souvent encore plus limité par le taux d'erreurs des portes quantiques. Il contraint ce que l'on appelle la profondeur du calcul, à savoir le nombre de portes quantiques que l'on peut enchaîner sans que le taux d'erreur des portes pollue trop les résultats. Les algorithmes doivent donc optimiser le nombre de cycles de portes à exécuter, celui-ci étant par ailleurs contraint par la connectivité physique entre les qubits.



Dans les schémas décrivant des algorithmes quantiques, comme celui *ci-dessus*, la double barre après la mesure de l'état d'un qubit indique par convention que l'on a récupéré un bit normal, à 0 ou 1. Au passage, tout ceci rappelle qu'il y a autant de qubits en sortie qu'en entrée dans un calcul quantique puisque ce sont physiquement les mêmes !

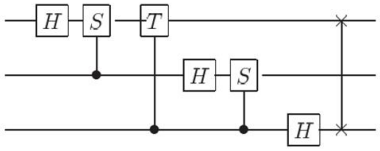
Mathématiquement parlant, une suite de portes quantiques dans un ordinateur quantique est représentable par une matrice de 2^N x 2^N nombres complexes, N étant le nombre de qubits utilisés.

Elle peut être donc immense dès que N dépasse 10. Multipliée par le "tenseur" comprenant les N qubits en entrées (initialisés à 0), elle génère une combinaison de N qubits en sortie.

Le schéma *ci-contre* en est un exemple avec la matrice correspondant à un algorithme de transformée de Fourier quantique appliquée à un jeu de 3 qubits[95]. 2^3 donne 8 qui correspond aux deux dimensions de la matrice de transformation de l'algorithme. Imaginez alors la taille de la matrice pour 2^{1024} ! La taille de cette matrice devient gigantesque dès que N dépasse 50. On utilise de telles matrices dans les simulateurs d'algorithmes quantiques à base de supercalculateurs classiques.

Box 5.1: Three qubit quantum Fourier transform

For concreteness it may help to look at the explicit circuit for the three qubit quantum Fourier transform:



Recall that S and T are the phase and $\pi/8$ gates (see page xxiii). As a matrix the quantum Fourier transform in this instance may be written out explicitly, using $\omega = e^{2\pi i/8} = \sqrt{i}$, as

$$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}. \quad (5.19)$$

Au-delà d'une cinquantaine de qubits, la taille de la matrice devient trop grande pour rentrer en mémoire des plus grands super-calculateurs. Cela explique pourquoi les simulateurs d'ordinateurs quantiques sur supercalculateurs sont limités à environ une cinquantaine de qubits. Au-delà, la taille de la matrice à simuler est bien trop grande par rapport à la capacité mémoire de ces supercalculateurs.

On n'est cependant peut-être pas obligé de simuler une matrice entière. Il est peut-être possible de simuler en mémoire l'état du registre des qubits avec un vecteur de N fois deux nombres complexes. En fait, je ne sais pas trop !

Correction d'erreurs

L'un des écueils des qubits est qu'ils génèrent un taux d'erreurs non négligeable pendant que l'on agit sur eux avec des portes quantiques ainsi que lors de la mesure de leur état.

Ces erreurs ne sont pas seulement de rares inversions simples de 0 et de 1 comme dans l'informatique traditionnelle, mais des glissements de valeurs des vecteurs représentant les qubits avec des modifications de phases lors de la superposition des qubits. Dans la sphère de Bloch, ce sont des vecteurs horizontaux qui peuvent tourner légèrement autour de l'axe vertical. Ces erreurs sont liées aux interactions entre les qubits et leur environnement, en plus du problème du temps de cohérence, qui est le temps pendant lequel les qubits restent en état de superposition.

Dans un ordinateur quantique à portes universelles, on identifie trois sources d'erreurs : les erreurs sur les portes quantiques unitaires (à un seul qubit), celles des portes à deux qubits puis celles de la mesure de la valeur des qubits.

[95] Source du schéma : Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages).

Avec les qubits actuels, ces taux d'erreurs sont compris entre 0,1% et plusieurs 1%, ce qui est bien supérieur aux taux d'erreurs courants de l'informatique traditionnelle.

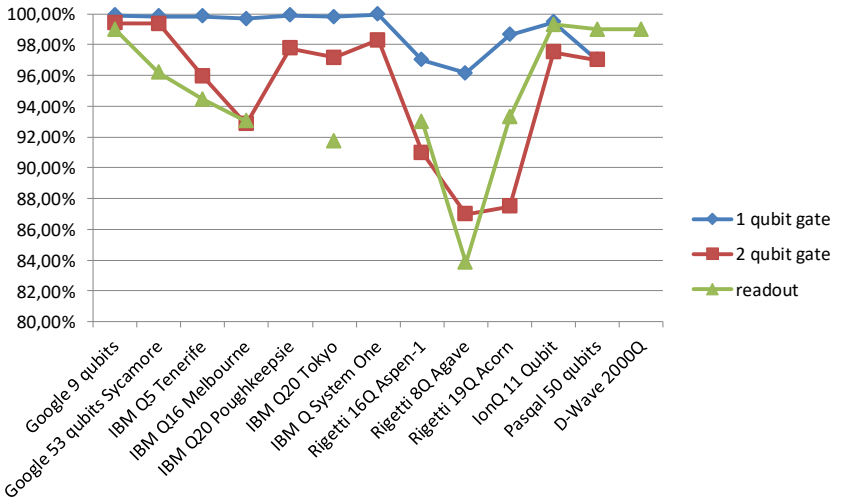
Dans le schéma suivant[96], vous trouverez une comparaison de quelques taux d'erreurs d'ordinateurs quantiques supraconducteurs, ces taux étant fournis par leurs fournisseurs. On y constate que le taux d'erreur de portes à deux qubits et de la lecture est bien plus élevé que le taux d'erreur des portes unitaires[97]. Le meilleur taux actuellement obtenu est de 0,62% pour le processeur Google Sycomore de 53 qubits, évoqué en septembre 2019[98].

chaque porte quantique unitaire ou à deux qubits génère des erreurs tout comme la lecture des résultats à la fin des opérations

ces erreurs s'accumulent avec le nombre de portes quantiques enchaînées

cela fausse complètement les calculs !

des méthodes de correction d'erreurs permettent de limiter la casse



taux de fiabilité des portes unitaires (1 qubit), à deux qubits et de la mesure des résultats en %.
le plus proche de 100% est le meilleur. il faudrait avoir moins de 0,001% d'erreurs pour que cela fonctionne bien !
source des données : https://quantumcomputingreport.com/scorecards/qubit-quality/ et Google, D-Wave.
intègre le record de 53 qubits de Google rendu public le 20 septembre 2019.

Ces taux d'erreurs s'additionnent (ou se multiplient) à chaque opération. Imaginez l'enchaînement de quelques dizaines de portes quantiques à deux qubits ! Le taux d'erreur va largement dépasser 50% à la fin de l'algorithme et bien avant que l'on atteigne le temps fatidigue de la décohérence des qubits. C'est une situation intenable. D'où le fait que l'on peut évaluer la puissance d'un ordinateur quantique non pas simplement au nombre de qubits alignés mais au nombre d'opérations enchaînables avec un taux d'erreur raisonnable. Pour éviter ce genre de contrainte quantitative, il faudrait avoir des qubits présentant des taux d'erreurs de portes quantiques de l'ordre de 10^{-10} !

Une formule permet d'évaluer la dépendance entre le taux d'erreur des portes quantiques (e), le nombre de qubits (n) et le nombre de portes enchaînables (d), appelé « profondeurs de circuit » (circuit depth) : $nd < 1/e$ [99]. Plus le taux d'erreurs baissera, plus la profondeur des circuits augmentera et le périmètre des algorithmes exploitables s'élargira.

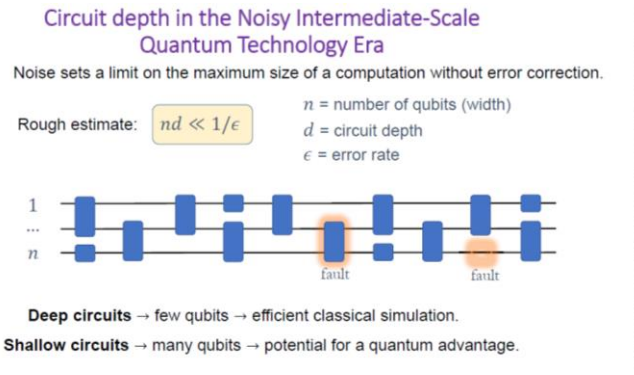
---

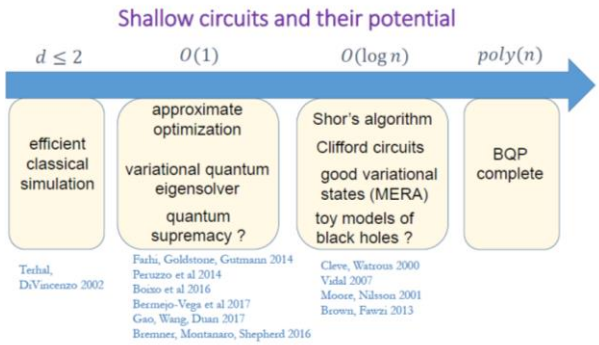
[96] Source des données sur la fiabilité des qubits : Qubit Quality sur le site Quantum Computing Report, avril 2019.

[97] Voir An introduction to quantum error correction de Mazyar Mirrahimi, 2018 (31 slides).

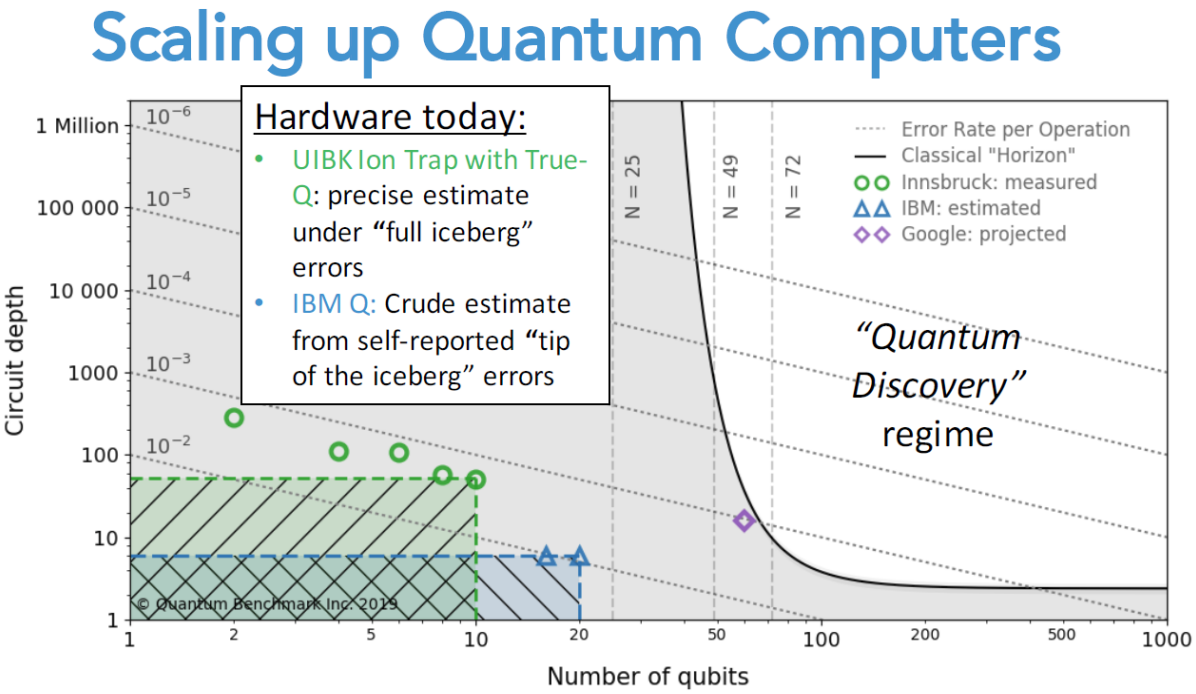
[98] Voir le papier de la NASA qui décrit la performance de Google : Quantum Supremacy Using a Programmable Superconducting Processor par Eleanor G. Rieffel, août 2019 (12 pages).

[99] Source du schéma : Quantum advantage with shallow circuits Robert König, 2018 (97 slides)





C'est présenté d'une autre manière avec un graphique de Quantum Benchmark avec en abscisses le nombre de qubits, en ordonnées la profondeur des circuits (nombre de portes enchaînables dans un calcul quantique), conditionné par les pointillés en biais qui sont les taux d'erreur des portes quantiques. La zone blanche est celle de la suprématie quantique[100]. Ils positionnent Google tout près de la zone d'intérêt avec leurs 72 qubits, mais des benchmarks publics de ces qubits n'ont pas encore été publiés après l'annonce de leur réalisation en mars 2018.



La principale solution de contournement actuellement explorée consiste à mettre en œuvre des systèmes de correction d'erreurs que l'on appelle QEC pour **Quantum Error Correction**.

Ils conduisent à répliquer plusieurs fois par intrication les qubits de calcul pour leur faire subir le même traitement en parallèle et à comparer les résultats en sortie d'algorithmes pour conserver les résultats statistiquement dominants. Le tout sans lire la valeur des qubits qui ferait effondrer tout le système !

[100] Slides présentés par Joseph Emerson de Quantum Benchmark à la conférence Quantum Computing Business organisée à Paris le 20 juin 2019 par Bpifrance.

L'un des algorithmes les plus couramment utilisé duplique un qubit deux fois (dans le cadre rouge de l'illustration *ci-dessous*). Après le passage par un processus de calcul générateur de bruit (E), la différence entre les trois versions est évaluée. S'il y a une différence, on retient les qubits inchangés majoritairement. Le code de Shor est une déclinaison par trois de cette méthode, ce qui conduit un qubit donné à être répliqué 8 fois en tout. Ce code de correction d'erreur corrige les erreurs d'amplitude (flip) et de phase.

L'intérêt de la méthode qui s'appuie sur des portes quantiques classiques CNOT est qu'il ne nécessite pas de lire – et donc de détruire – la valeur des qubits. C'est un code de correction d'erreurs non destructif[101] !

5 correction d'erreurs

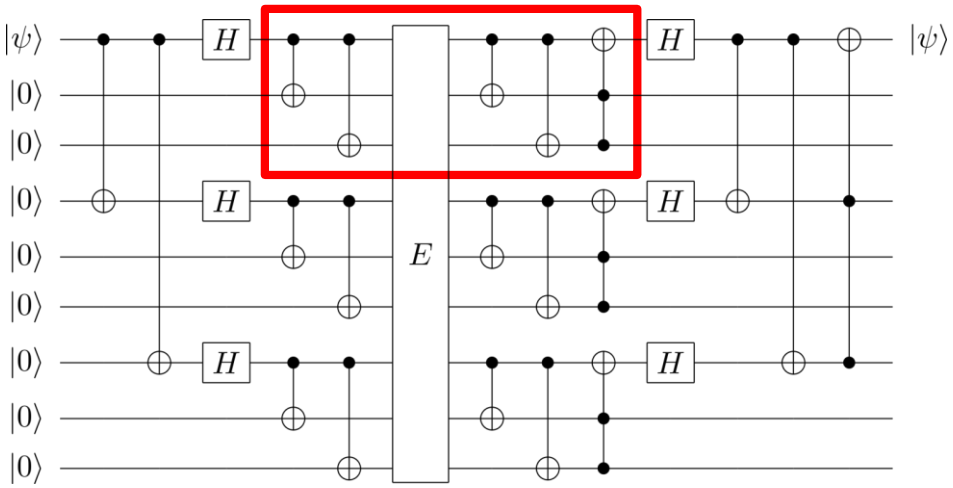
double réplication de qubits par porte CNOT

E = noisy channel

comparaison des résultats par paires

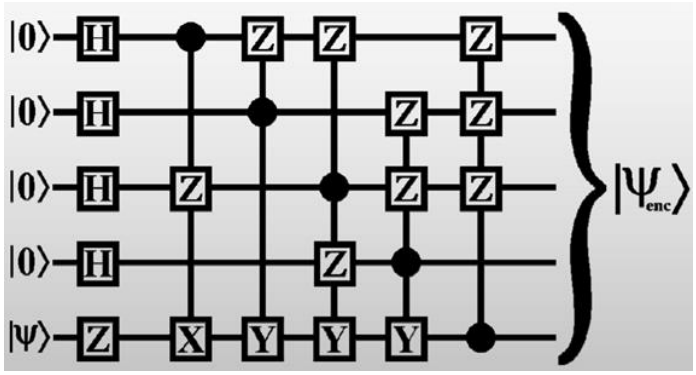
le "Shor Code" réplique trois fois ce principe, donc x9 au total

prend du temps et multiplie le besoin en qubits



Ce code de correction d'erreurs à 9 qubits permet de corriger à la fois les erreurs d'inversion (0 à la place de 1 et réciproquement) et les erreurs de phase (modification de la composante verticale du qubits dans sa sphère de Bloch).

Il semblerait qu'il faille au moins cinq qubits "physiques" pour créer un qubit logique intégrant la correction d'erreurs. Voir l'algorithme *ci-contre*[102].



Mais avec les taux d'erreurs actuels, il sera nécessaire d'assembler des milliers de qubits physiques pour créer un qubit logique.

[101] Le détail du processus est bien documenté dans la fiche Wikipedia de la correction d'erreur quantique.

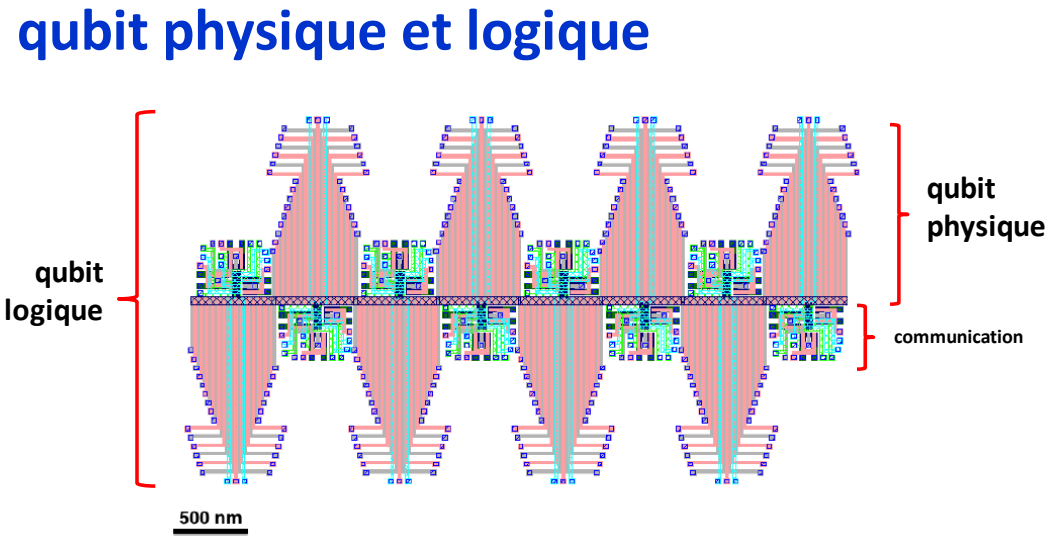
[102] Voir Magic States de Nathan Babcock (28 slides).

Dans la pratique, on va donc assembler des qubits physiques en qubits logiques avec de la redondance et des systèmes de correction d'erreurs au niveau des circuits et processeurs quantiques. La notion de qubits logiques peut être mise en œuvre soit par logiciel, soit au niveau matériel. Lorsqu'elle est logicielle, c'est le rôle des algorithmes que de mettre en œuvre des codes de correction d'erreur dynamiques.

Lorsque l'on utilise les 14 qubits physiques en cloud proposée par IBM, c'est au développeur de mettre en œuvre ses propres codes de correction d'erreur.

Dans une QEC (Quantum Error Correction) réalisée au niveau matériel, celle-ci est mise en œuvre par création d'assemblage de qubits qui génèreront des qubits logiques physiques prêts à l'emploi. En voici un exemple avec sept qubits physiques pour constituer un qubit logique[103]. La raison d'être de cette architecture est liée au fait que les qubits en CMOS génèrent un peu plus de bruit que les qubits en supraconducteurs à effet Josephson, tout du moins en l'état actuel des choses. On doit donc en passer par là pour réduire le bruit. Sachant… que cela ne fonctionne pas encore ! Et que l'usage de seulement huit qubits physiques pour créer un qubit logique est sujet à caution.

Le nombre de qubits physiques à assembler pour créer un qubit logique dépend du taux d'erreurs des qubits. Plus le taux d'erreurs des qubits est élevé, plus grand doit être le nombre de qubits assemblés. Ce nombre peut atteindre plusieurs milliers de qubits [104] ! Pour Alain Aspect, il faudrait avoir un million de qubits physiques par qubit logique pour créer un ordinateur quantique utilisable[105].



Maximum density of quantum information in a scalable CMOS implementation of the hybrid qubit architecture, 2015

[103] Il vient de Maximum density of quantum information in a scalable CMOS implementation of the hybrid qubit architecture, 2015 (17 pages).

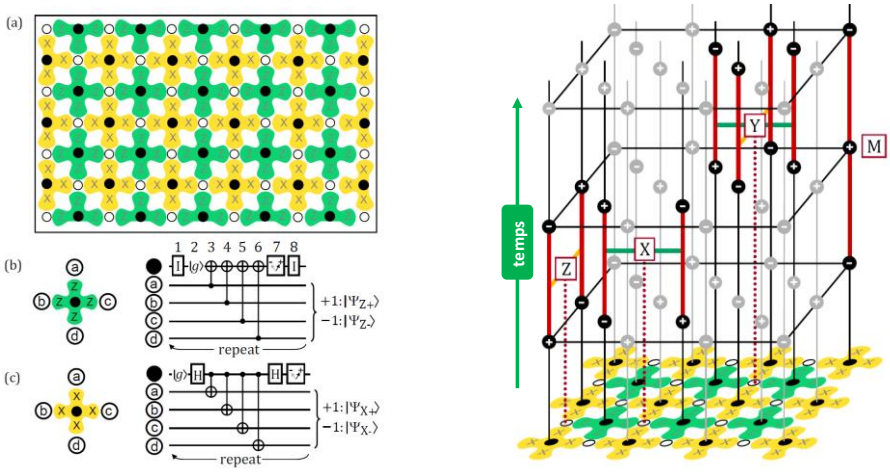
[104] Voir What determines the ultimate precision of a quantum computer? par Xavier Waintal, 2019 (6 pages) qui décrit pour sa part les limites des codes de correction d'erreur.

[105] Voici quelques autres contenus utiles sur la correction d'erreurs : Error mitigation in quantum simulation, Xiao Yuan, IBM Research, 2017 (42 minutes), Code Used To Reduce Quantum Error In Logic Gates For First Time, 2019, Scientists find a way to enhance the performance of quantum computers par l'University of Southern California, 2018 et Cramming More Power Into a Quantum Device de Jay Gambetta et Sarah Sheldon, mars 2019 à propos du niveau d'erreurs de l'IBM Q System One annoncé en janvier 2019.

Ce qui veut dire que pour avoir ne serait-ce que quelques centaines de qubits logiques à même d'atteindre la suprématie quantique pour des algorithmes quantiques assez simples, il faudrait disposer de plusieurs dizaines de millions de qubits physiques. On en est encore bien loin !

Dans le supraconducteur à effet Josephson ou les qubits CMOS, la technologie de correction d'erreurs la plus souvent envisagée s'appelle le "surface code", datant de 2012[106]. Elle comprend des matrices de qubits de traitement (en blanc dans le schéma *ci-dessous*) reliés reliés à des qubits de mesure (en noir) via des portes unitaires de **Pauli X** (inversion) et **Pauli Z** (changement de phase).

Leur programmation dans le temps permet de corriger des erreurs. Mais elle ajoute une série de portes quantiques qui allongent la durée des opérations. On peut voir à droite une timeline verticale ascendante de l'évolution de la valeur des qubits au gré de l'activation des portes pour la correction d'erreurs.



Surface codes: Towards practical large-scale quantum computation, 2012

Il existe en fait de nombreux types de corrections d'erreurs avec leur propre formalisme mathématique. C'est le cas de **codes stabilisateurs** (stabilizer codes)[107].

Il y a aussi les « **non stabilizer states** » et la « **magic state distillation** », une alternative qui utilise des qubits de réserve (ancilae). Elle consiste à préparer des qubits dédiés à la correction d'erreur dans un état particulier, un magic state. La distillation consiste à utiliser plusieurs qubits « magic states » pour en préparer d'autres, où le taux d'erreur est réduit[108].

Il existe aussi une méthode de création de QEC à base de **réseaux de neurones**, issue de chercheurs de l'Université d'Erlangen en Allemagne[109].

---

[106] Dans Surface codes towards practical large-scale quantum computation, 2012 (54 pages).

[107] Voir une description de divers codes de correction d'erreurs dans Software for Quantum Computation, une thèse de Daniel Matthias Herr de l'ETZ Zurich, 2019 (164 pages).

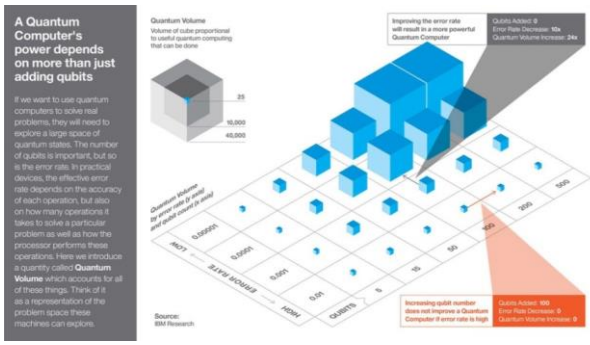
[108] Voir Magic-State Functional Units, 2018 (13 pages), Resource Optimized Quantum Architectures for Surface Code Implementations of Magic-State Distillation, 2019 (16 pages) et Hybrid magic state distillation for universal fault-tolerant quantum computation, 2015 (9 pages).

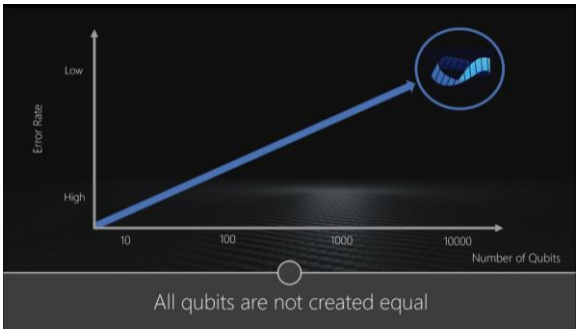
[109] Voir Neural networks enable learning of error correction strategies for quantum computers, octobre 2018 et Reinforcement Learning with Neural Networks for Quantum Feedback, Thomas Fösel et al, 2018 (7 pages).

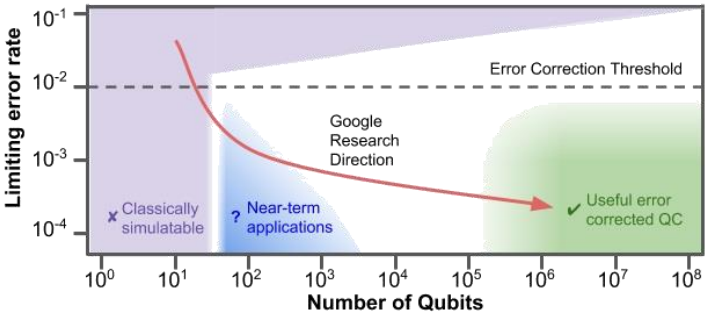
L'un des problèmes est que la correction d'erreur génère un overhead qui croîtrait plus vite que le gain exponentiel de l'ordinateur quantique (2^{4n} vs 2^n selon Quantum Benchmark)[110].

Tout ceci explique pourquoi IBM communique sur le couple nombre de qubits et le taux d'erreurs et sur la notion de volume quantique que nous décrirons plus loin. Microsoft et Google font de même. Microsoft est d'ailleurs celui qui simplifie le plus la présentation. Une fois n'est pas coutume !

Pour qu'un ordinateur quantique serve à quelque chose, il faut à la fois avoir beaucoup de qubits, un faible taux d'erreurs des portes et de la mesure et un long temps de cohérence des qubits[111].







Mais au juste, comment évalue-t-on le taux d'erreur des portes quantiques et de la mesure de l'état des qubits[112] ?

On utilise un processus dit de "Randomized Benchmarking" (RBM) qui consiste à enchaîner une sequence de portes quantiques aléatoire dont on connaît à l'avance le résultat et à comparer le résultat obtenu avec celui que l'on connaît.

---

[110] Pour en savoir plus au sujet de la correction d'erreur, voir notamment cette présentation Surprising facts about quantum error correction d'Andrew Darmawan, Nicolas Delfosse, Pavithran Iyer et David Poulin, 2017 (178 slides).

[111] Sources : IBM Bolsters Quantum Capability, Emphasizes Device Differentiation, 2017, et pour Microsoft, un extrait de la vidéo Future Decoded Quantum Computing Keynote, novembre 2017.

[112] J'ai trouvé cette information dans Quantum Computing: Progress and Prospects 2018 (206 pages), page 2-20. Le processus de benchmarking de portes quantiques est détaillé dans Randomized benchmarking for individual quantum gates de Emilio Onorati & Al, 2018 (16 pages). L'origine de la méthode est Scalable noise estimation with random unitary operators de Joseph Emerson & Al, 2005 (8 pages).

Le taux d'erreur augmente au gré de l'augmentation du nombre de portes quantiques enchaînées et de leur type. On peut évaluer le taux d'erreur d'une porte donnée avec l'Interleaved RBM qui injecte ladite porte périodiquement dans le jeu de portes aléatoires utilisé. On mesure alors la différence de taux d'erreur entre la séquence avec et sans ces portes quantiques ajoutées.

Il faut fouiller ailleurs pour en savoir plus, comme dans l'excellent rapport Entwicklungsstand Quantencomputer (*état des lieux de l'informatique quantique*) de l'ANSSI allemande qui met en évidence l'énorme décalage entre les performances actuelles des qubits, notamment chez IBM et Google, et le besoin lié à la factorisation de nombres entiers pour casser des clés RSA courantes. Même si ce besoin référent n'est pas le plus "constructif" parmi les domaines d'applications des ordinateurs quantiques.

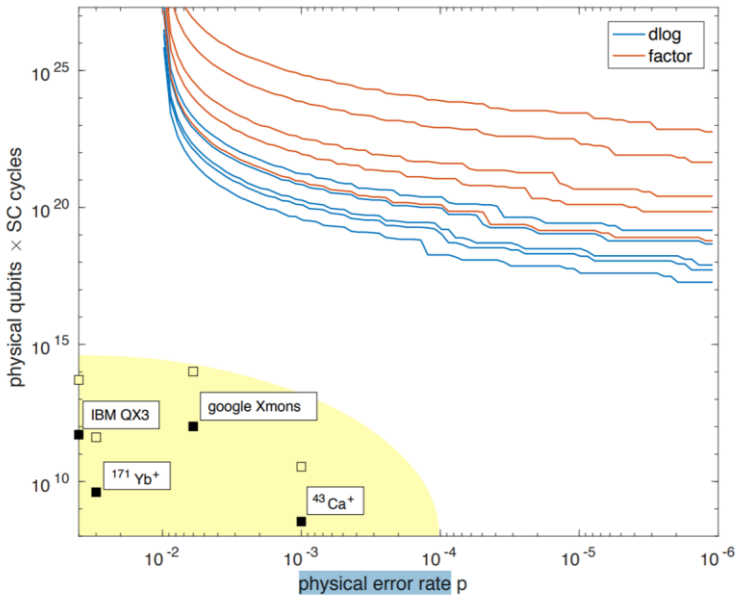


Figure 2.4: Comparison of algorithmic demands with currently achieved hardware performance. The plot shows required resources as number of qubits times rounds of error correction in the surface code for dlog (blue) and factoring (orange) for common key sizes as a function of the physical error rate p. The squares show current realizations assuming one day run time (solid) or 100 days (empty), the yellow area shows expected near-term progress. Both scales are logarithmic.

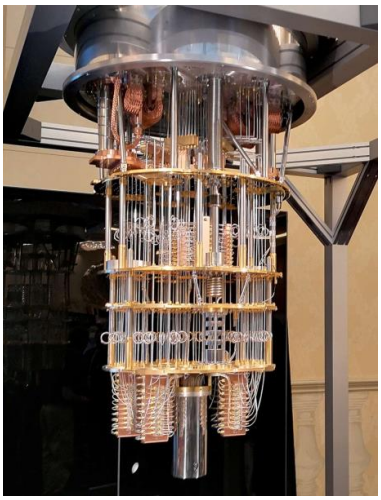
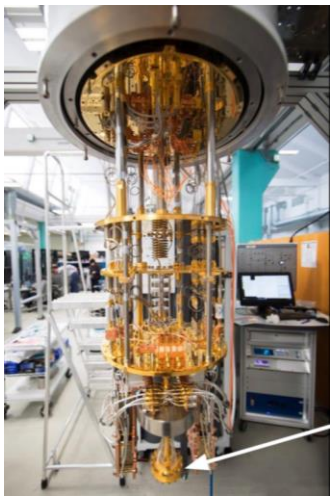
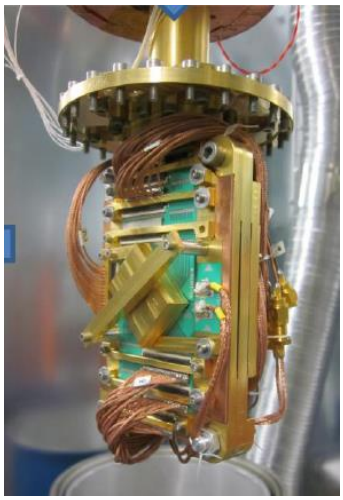
Il semblerait cependant que cette notion de taux d'erreurs puisse être "scalable". A savoir que lorsque l'on saura baisser le taux d'erreurs des qubits à un niveau acceptable, on pourra facilement démultiplier le nombre de qubits dans les circuits et conserver ce taux d'erreurs. Tout ça pour dire que l'abaissement du taux d'erreur des qubits est indépendant de leur nombre dans un circuit. Ce qui sous-tend, une fois ce problème de taux d'erreur réglé, que la montée en puissance des calculateurs quantiques en nombre de qubits pourrait être ensuite très rapide. C'est en tout cas ce que m'a raconté un chercheur d'IBM rencontré sur Vivatech en mai 2018. D'autres publications ne sont pas aussi radicales sur ce point et évoquent de nombreux obstacles pour faire "scaler" le nombre de qubits en préservant leur fiabilité.

Mais les codes de correction d'erreurs ne sont pas les seuls dans l'arsenal contre les erreurs. On peut aussi y intégrer les algorithmes quantiques qui sont résistants aux erreurs.

Cryogénie

Pour terminer le tour de l'architecture d'un ordinateur quantique type, passons à la partie cryogénie. Lorsque l'on observe de près un ordinateur quantique issu des grands acteurs du secteur, on y décèle un petit air de famille comme ci-dessous avec les cas d'IBM, de Rigetti et de D-Wave. Ils présentent la particularité d'utiliser tous les trois des qubits à base de supraconducteurs.

Cette technologie nécessite de refroidir les qubits à une température aussi basse que possible pour éviter toutes les perturbations du monde extérieur. L'isolation de l'ensemble doit être la plus totale au niveau de la température, du magnétisme et même des vibrations mécaniques.

Passons en revue cette partie d'un calculateur quantique. Elle comprend des étages représentés par des disques métalliques sur lesquels sont fixés des fils supraconducteurs et des dispositifs physiques et électroniques de contrôle.

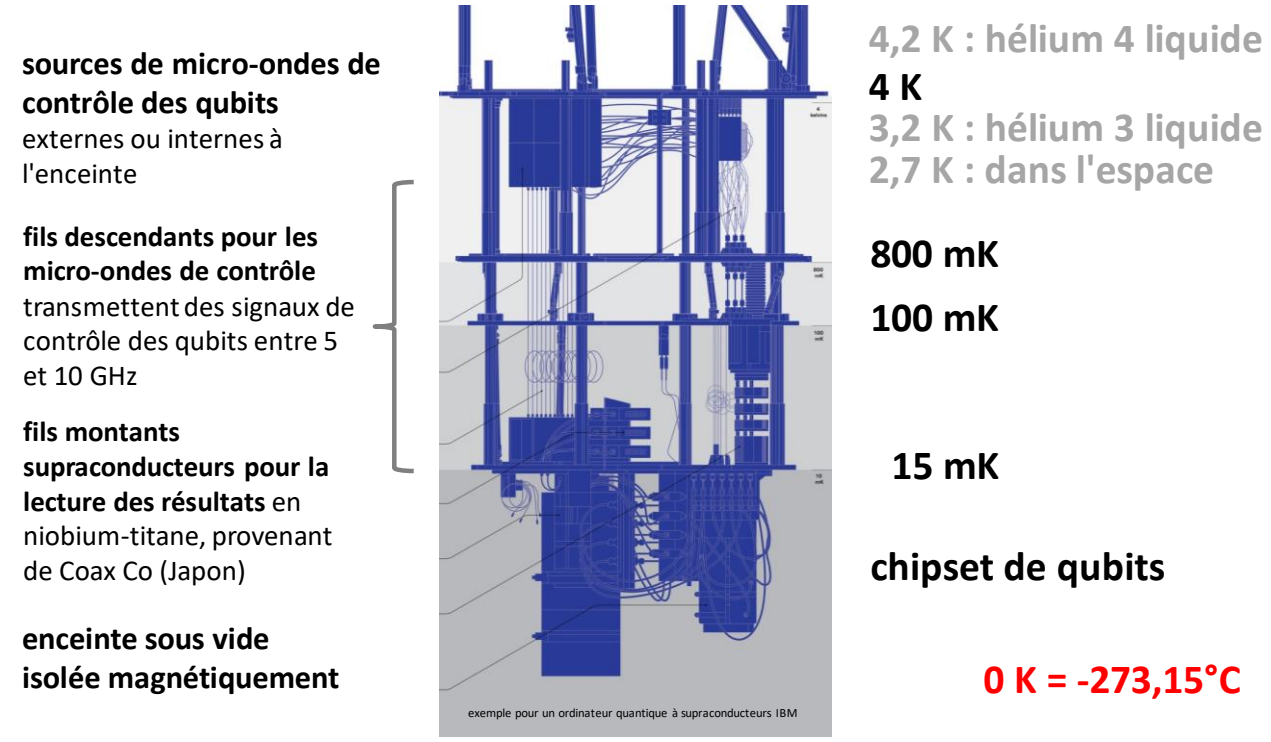
Plus on descend dans les étages, plus il fait froid.

- Au niveau supérieur, on atteint 4K, soient 4° au-dessus du zéro absolu qui est de –273,15°C. L'échelle de Kelvin démarre au zéro absolu. Cette température où la matière ne bouge littéralement plus est inatteignable. On s'en approche de manière asymptotique. Le record de la température la plus basse est de 450 pK (pico-kelvins) atteinte grâce à l'étonnante technique de refroidissement d'atomes par laser et effet Doppler, déjà décrit page 68. Dans les ordinateurs quantiques supraconducteurs, on se contente d'une température située entre 10 mK et 20 mK (milli-Kelvins).
- L'étage du dessous est à 800 mK dans cet exemple d'ordinateur quantique IBM. Entre ces deux étages se situe la température la plus basse de l'espace qui est de 2,7 K.

Le refroidissement est réalisé à l'aide de réfrigérateurs à dilution fonctionnant à sec. Un premier système réfrigère l'enceinte à 4K avec de l'hélium 4 liquide. Un second système exploite un mélange d'hélium liquide 3 et 4 avec un flux circulant dans des conduits cylindriques ou en serpentin verticaux reliant les plaques métalliques pour descendre à moins de 20mK[113].

[113] J'ai trouvé le schéma dans la thèse Superconducting Silicon On Insulator and silicide-based superconducting MOSFET for quantum technologies de Anaïs Francheteau, 2006 (152 pages).

Le système fait circuler de l'hélium dans l'ensemble et il n'a pas besoin d'être re-chargé régulièrement sauf pour compenser d'éventuelles pertes. Ce type de cryogénie est dit « à sec ». Dans d'autres cas, l'ensemble du dispositif baigne dans de l'hélium liquide, mais il a l'air d'être rare pour ce qui est des ordinateurs quantiques.



Le schéma *ci-dessus*, hors commentaires, est issu de Quantum Computers Strive to Break Out of the Lab, 2018.

Les plaques de chaque étage sont généralement réalisées en cuivre pur à 99,99% et à très faible teneur en oxygène, pour maximiser sa conductivité thermique[114]. Elles sont recouvertes d'une fine couche d'or de quelques µm d'épaisseur qui joue un rôle de protection contre l'oxydation et contre les radiations.

Pour le refroidissement des étages les plus froids, la cryogénie s'appuie sur un mélange d'hélium 4 et d'hélium 3 dont la température de fusion est respectivement de 4,2K et 3,2K. Qui plus est, ils sont tous les deux superfluides aux alentours de 2K.

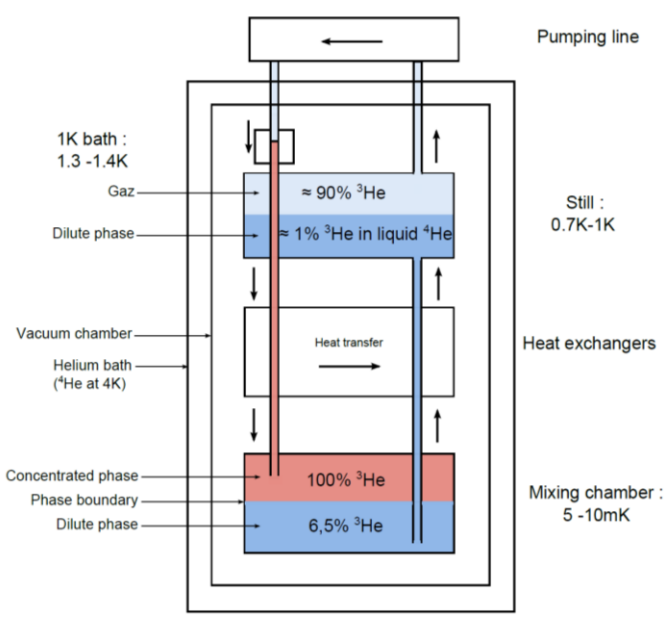
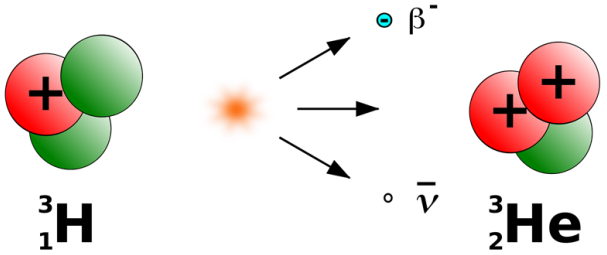


Figure 2.2: Schematic ^{3}He-^{4}He dilution refrigerator.

[114] C'est de l'OFHC pour oxygen-free high thermal conductivity. Source de cette information : Flying Qubit Operations in Superconducting Circuits d'Anirudh Narla 2018 (219 pages).

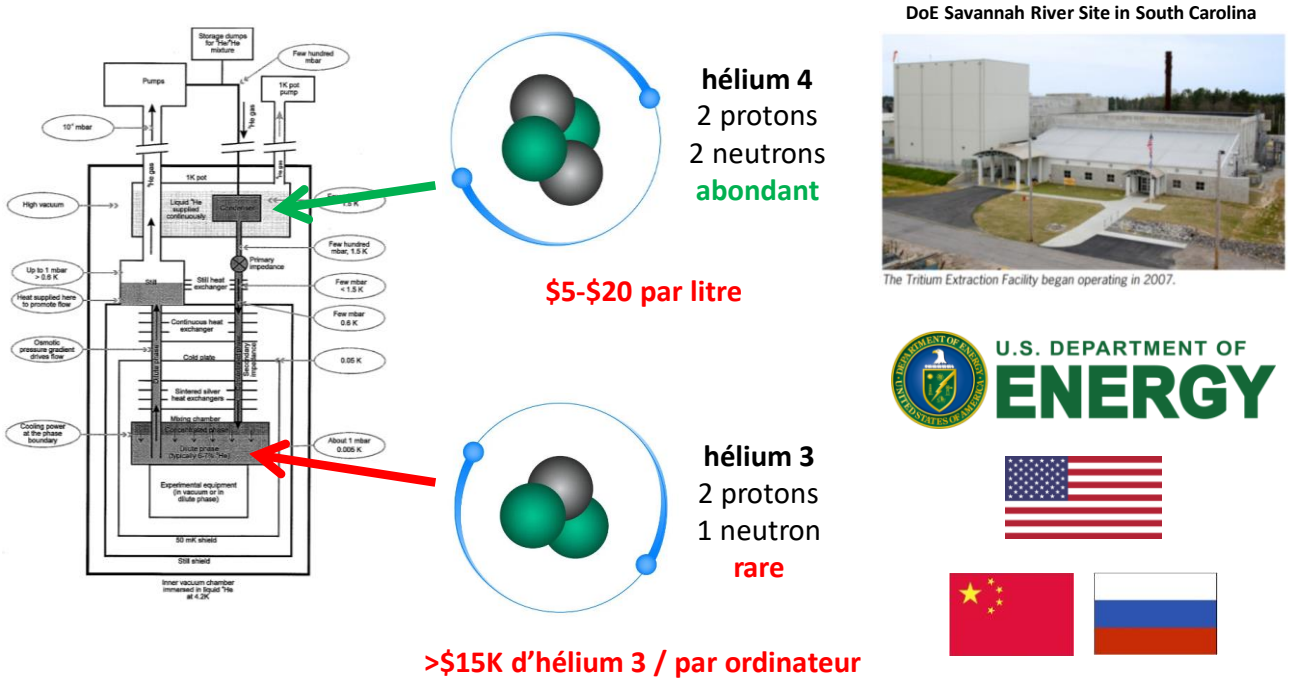
Le premier est l'isotope d'hélium le plus courant et le plus stable. Le second qui contient un neutron et deux protons est plutôt rare.

C'était historiquement un sous-produit du stockage de bombes H à base de tritium, ce dernier se désintégrant progressivement pour produire de l'hélium 3 (schéma *ci-contre*). Il était donc récupéré dans les stocks de bombes H !



Avec les réductions de stocks d'armes nucléaires, la tendance n'est donc pas une production d'hélium 3 à la hausse par ce biais. On peut produire du tritium par irradiation du lithium ou désintégration contrôlée du tritium, un isotope de l'hydrogène avec un proton et deux neutrons, dans des installations nucléaires spécialisées, comme celles qui sont maîtrisées par le Département de l'Energie US.

Actuellement, cet Hélium 3 est produit dans le site de Savannah du Département de l'Energie US en Caroline du Sud[115] ainsi que dans la centrale Canadienne CANDU[116]. Il en faut une dizaine de litres coutant entre $15K et $40K par ordinateur selon l'origine et le cours de l'hélium 4.



[115] Voir Savannah River Tritium Enterprise (6 pages) et Savannah River Tritium Enterprise (4 pages). L'hélium 3 est aussi exploité dans diverses applications spécialisées : dans les détecteurs de neutrons utilisés dans les systèmes de sécurité, dans l'exploration pétrolière, dans l'imagerie médicale ainsi que dans les recherches dans la fusion nucléaire.

[116] Voir CANDU Reactor, Wikipedia.

La France a des capacités de production de ce type situées notamment dans un réacteur nucléaire du CEA à Grenoble. Mais elle ne les exploite pas forcément pour les ordinateurs quantiques car cette production est trop chère[117].

On peut aussi trouver de l'hélium 3 sur la surface de la Lune mais il n'est pas très pratique d'aller l'y extraire et le récupérer même si c'est technologiquement possible[118] ! L'intérêt de sa récupération est que cet isotope pourrait être intéressant pour alimenter des réactions à fusion nucléaire, le jour où cela fonctionnera.

L'hélium 3 est donc un véritable goulot d'étranglement insoupçonné de la fabrication d'ordinateurs quantiques supraconducteurs ! L'un des moyens d'éviter l'usage de l'hélium 3 est de ne refroidir l'enceinte qu'à environ 1K. Dans ce cas là, on peut se contenter d'hélium 4 pour le circuit de refroidissement[119].

Cette cryogénie est spécifique aux ordinateurs quantiques dont les qubits doient être réfrigérés, essentiellement ceux qui sont à base d'électrons (CMOS ou supraconducteurs) ou d'atomes froids. Dans les ordinateurs quantiques à ions piégés, les qubits ne sont pas réfrigérées. Dans les processeurs quantiques à base de photons, l'optronique n'est pas réfrigérée mais les sources de photons et les outils de mesure le sont, à des températures comprises entre 1K et 10K.

Le calculateur quantique est placé sous vide et aussi isolé magnétiquement de l'extérieur. L'isolation magnétique utilise plusieurs enceintes en poupées russes réalisées dans des alliages divers, dont le **Mumetal**, un alliage de nickel, fer et mobdylène, des alliages en aluminium et d'autres alliages supraconducteurs.

Dans les ordinateurs de D-Wave, le champ magnétique est réduit à un nano-Tesla (nT) dans l'enceinte du calculateur, à comparer au champ magnétique terrestre qui peut atteindre 65 micro-Teslas, ce qui nous fait donc un ratio de 1 pour 65 000. D-Wave communique sur un ratio de 1 pour 50 000.

Les techniques de refroidissement utilisées sont inspirées de celles des télescopes spatiaux qui opèrent dans l'infrarouge et que nous avions vues l'année dernière dans ma longue série sur l'astronomie. Ces derniers se contentent cependant d'une température de 5K pour le refroidissement des capteurs infrarouges CCD.

Des fils supraconducteurs (ayant une résistance nulle à basse température) relient les qubits à leur système de mesure (donc, dans le sens montant dans le schéma). Ils sont réalisés en alliage de niobium et de titane (NbTi).

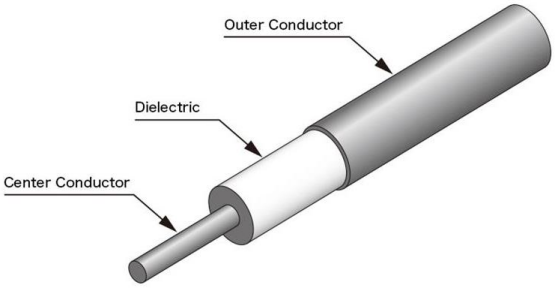
---

[117] Voir Crise de l'hélium l'inquiétude persiste 2013 (2 pages), Isotope Development & Production for Research and Applications (IDPRA), Supply and Demand of Helium-3, 2016 et Responding to The U.S. Research Community's Liquid Helium Crisis, 2016 (29 pages).

[118] Voir There's Helium in Them Thar Craters!.

[119] L'hélium 4 est utilize pour refroidir les aimants supraconducteurs des systèmes d'IRM. Il sert aussi à refroidir les aimants du LHC au CERN, ce qui en nécessite 96 tonnes.

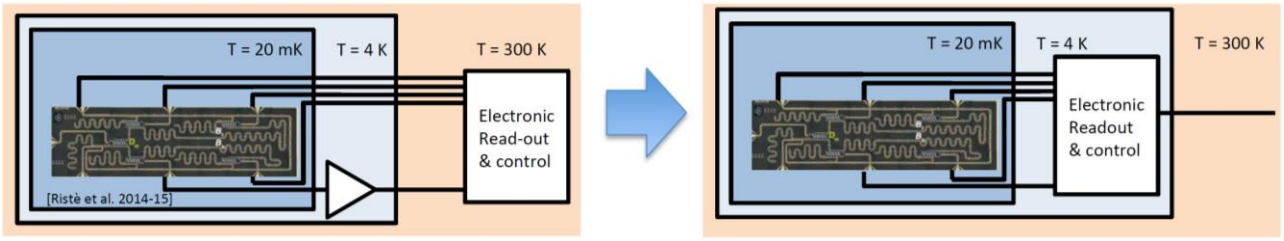
Ils proviennent du Japonais **Coax Co**. Il semblerait que cette société soit la seule au monde capable de les produire[120]. Le câble qui fait 2 mm de diamètre comprend une enveloppe extérieure conductrice et un conducteur central, tous deux en niobium-titane (source), qui sont séparés par un isolant en téflon (PFTE).



Vous remarquerez que nombre de ces câbles comprennent une boucle. Elle sert à absorber les variations de taille liées au refroidissement cryogénique et de charge thermique entre chaque étage de cryogénie.

Les câbles qui pilotent les qubits transportent des fréquences situées entre 5 et 10 GHz. Les fréquences inférieures à 5 GHz et supérieures à 10 GHz sont éliminées par filtrage.

Chez IBM, toute l'électronique de contrôle est extérieure à l'enceinte réfrigérée. Dans d'autres cas, comme pour les qubits CMOS, les chercheurs essayent de caser une partie de l'électronique de contrôle dans l'enceinte cryogénisée.



On peut déplacer une partie de l'électronique de contrôle dans la zone à 4K voir même dans la partie qui fonctionne en-dessous de 20mK. Ce doit répondre à un cahier des charges rigoureux. On ne peut pas placer sa carte mère de PC comme cela à ces basses températures. L'exemple *ci-dessous* décrit la grande variété des composants qui peuvent être intégrée dans l'étage 1K-4K et dans l'étage du processeur à moins de 20 mK[121].

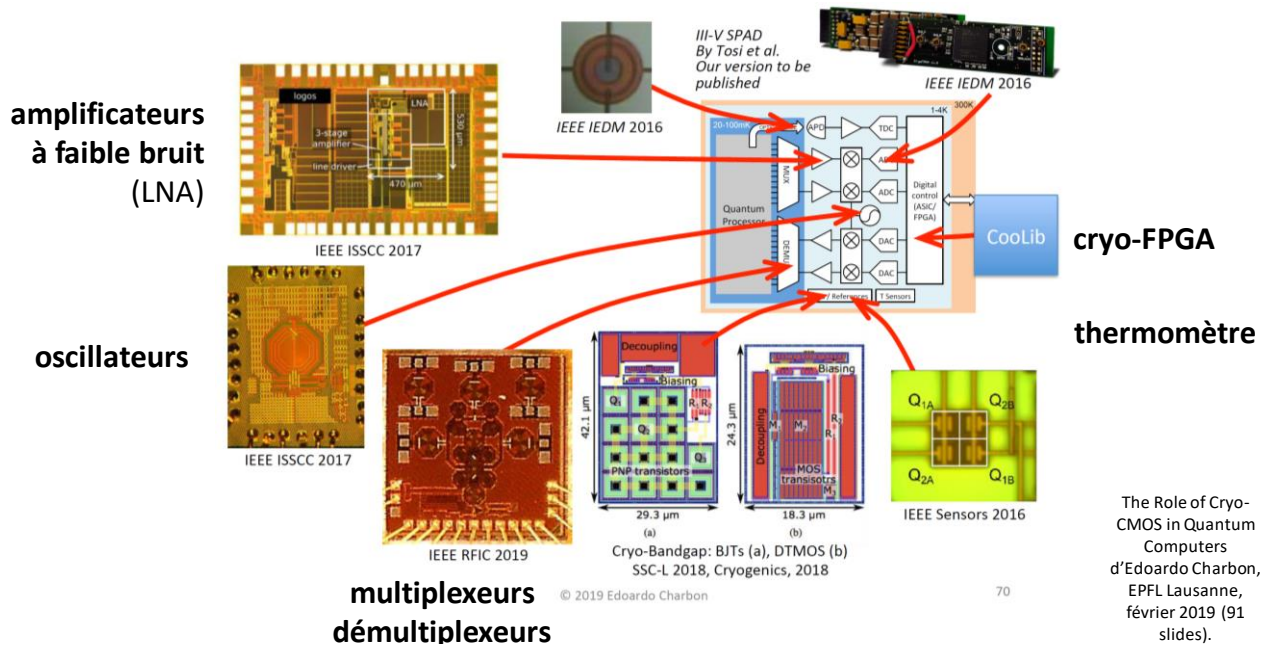
Il faut donc créer des composants certifiés pour fonctionner à ces températures-là : amplificateurs, multiplexeurs de données, oscillateurs de fréquences, contrôle électronique de la mesure de l'état des qubits, thermomètre et autres capteurs divers, etc. Qui plus est, il faut que la chaleur qu'ils dégagent soit limitée pour ne pas augmenter la température des qubits[122].

---

[120] Voir We'd have more quantum computers if it weren't so hard to find the damn cables, de Martin Giles, janvier 2019.

[121] Source du schéma : The Role of Cryo-CMOS in Quantum Computers d'Edoardo Charbon, EPFL Lausanne, février 2019 (91 slides).

[122] Voir Cryogenic Control Beyond 100 Qubits de Ian Conway Lamb, 2017 (103 pages) qui décrit bien les enjeux technologiques des composants fonctionnant à temperature cryogénique, ici pour des qubits supraconducteurs. Et la version courte : Cryogenic Control Architecture for Large-Scale Quantum Computing, de Ian Conway Lamb & Al, 2017 (8 pages). Voir aussi Semiconductor devices for cryogenic amplification de Damien Prêle, 2013 (30 slides) et Cryo-CMOS Circuits and Systems for Quantum Computing Applications de Bishnu Patra & Al, 2018 (14 pages).



A 10-20mK, cela ne représente qu'à peine 1 mW de puissance ! A 4K, on peut consommer environ 100 mW et cela représente environ 3,6 mW par qubit supraconducteur.

La photo *ci-contre* présente l'intérieur d'un ordinateur quantique d'IBM avec ses rangées de fils reliant différents étages du calculateur (ceux qui montent, difficile à distinguer, sont des fils supraconducteurs, les fils descendants de contrôle des qubits sont en cuivre)[123]. Et c'est le câblage pour seulement 20 qubits !

D'où viennent ces réfrigérateurs quantiques ? Quelques rares sociétés sont spécialisées dans le domaine, et alimentent aussi bien les laboratoires de recherche que les fabricants d'ordinateurs quantiques.

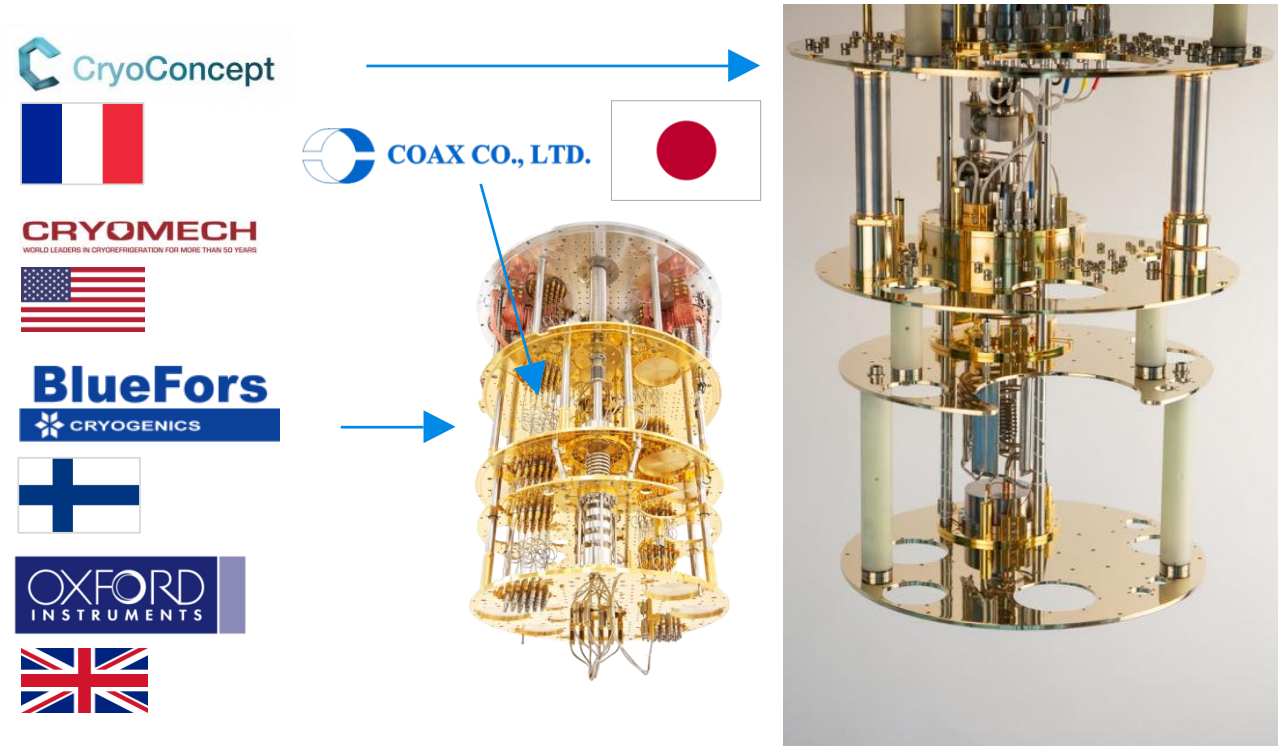
Les principaux fournisseurs sont les Finlandais **BlueFors Cryogenics**, l'anglais **Oxford Instruments** et l'Américain **Cryomech.** IBM et Rigetti font appel à BlueFors pour leurs ordinateurs quantiques et D-Wave utilise les systèmes de Cryomech. On en trouve aussi chez **Leiden Cryogenics**[124].

La startup française **CryoConcept** est une spécialiste du secteur. Située en région parisienne, elle créé notamment les plateaux de refroidissement, utilisant une technologie provenant du CEA. Ses clients sont essentiellement Japonais, Français et côté USA, à l'Université de Yale.

---

[123] Une visite du laboratoire IBM Q est disponible dans la vidéo A Tour of an IBM Q Lab datant de 2016.

[124] Voir la brochure Leiden Cryogenics BV (28 pages).



Les systèmes de cryogénie de CryoConcept ont été testés par différents acteurs dont le CEA à Saclay. Ils sont aussi utilisés à l'ENS[125]. CryoConcept se focalise notamment sur la réduction des vibrations mécaniques associées au refroidissement, via leur technologie UltraQuiet.

A l'Institut Néel du CNRS à Grenoble, les équipes ont créé leur propre système de cryogénie, capable de thermaliser un système quantique en seulement trois heures. A noter que la taille des plaques métalliques est limitée, ayant un impact sur celle des processeurs quantiques utilisés et de l'électronique qui les accompagne. Les circuits quantiques doivent aussi être dotés de radiateurs miniatures pour dégager l'énergie générée par les portes quantiques.

Selon le CEA, ces radiateurs feraient entre 1 mm et 1 micron de largeur[126].

Le CEA-IRIG de Grenoble déployait en juin 2019 deux systèmes commerciaux du leader mondial du secteur, **Bluefors** (Finlande). Ce dernier système contient le système de réfrigération au-dessus de la colonne blanche (*ci-dessous à gauche*).

[125] Voir l'équipement quantique de l'ENS dans leur Labtour.

[126] Selon Robert Whitney dans Energetics of quantum computing, 2018 (13 slides).

Il est couplé à des réservoirs et outils techniques dans une salle adjacente (*ci-dessous à droite*, l'équipement lié à deux systèmes de cryogénie). Ce sont des systèmes à environ 1M€ la pièce. Ils refroidissent l'installation par étages en partant du haut dans l'installation ouverte que l'on appelle parfois le chandelier quantique. On démarre en haut à 4K, puis descend à 1K et enfin, on se retrouve à moins de 20 mK.

La thermalisation, ou la baisse de température à moins de 20 mK dure au minimum 24 heures pour une installation à température ambiante. Mais les équipes du CEA ont installé un dispositif qui permet de changer l'échantillon testé en seulement 7 heures. La thermalisation peut ainsi être déclenchée pendant la nuit et au petit matin, les expériences peuvent reprendre.

Au passage, comment mesure-t-on des températures si basses ? Avec des thermomètres cryogéniques pardi ! J'en ai trouvé chez **Lake Shore Cryotronics** (source) ainsi que chez **Janis** (source) qui conçoit aussi des frigos cryogéniques.

Au final, un ordinateur quantique est de taille raisonnable. Dans les laboratoires, le calculateur quantique lui-même tient dans un cylindre d'environ 50 cm de diamètre et un mètre de haut. L'électronique de commande externe tient dans quelques racks de serveurs et dispositifs de contrôle. Le système de cryogénie occupe environ deux mètres cubes.

Chez D-Wave qui est le seul fournisseur d'ordinateurs quantiques commerciaux, les machines font environ quatre mètres cube. C'est plutôt raisonnable compte-tenu de la puissance de calcul qui sera un jour accessible à ces ordinateurs et qui dépassera largement celle de supercalculateurs qui occupent de leur côté de vastes salles blanches et consomment des mégawatts d'électricité.

Mémoire quantique

Evoquons la mémoire quantique ou la **qRAM,** une mémoire quantique capable de stocker l'état quantique de qubits pour les utiliser ensuite pour alimenter des registres d'ordinateurs quantiques[127]. L'état quantique d'un registre va devoir stocker des qubits en état de superposition. L'une des méthodes les plus prometteuses de mémoire quantique utilise des phases de photons[128].

Avec n qubits, cette mémoire pourra donc stocker en théorie 2^n états différents de ce registre. Elle ne servira pas à stocker autant d'information provenant d'un ordinateur traditionnel mais à conserver l'état d'un registre de qubits d'un ordinateur quantique. Elle est nécessaire à certains types d'algorithmes quantiques comme l'algorithme de recherche de Grover que nous verrons dans la partie suivante.

Petit détail de taille : aucune des différentes architectures de mémoires quantiques étudiées depuis deux décennies n'est au point ! Les recherches vont cependant bon train mais avec des usages visés qui sont plutôt dans les télécommunications sécurisées et pour la création de répéteurs optiques.

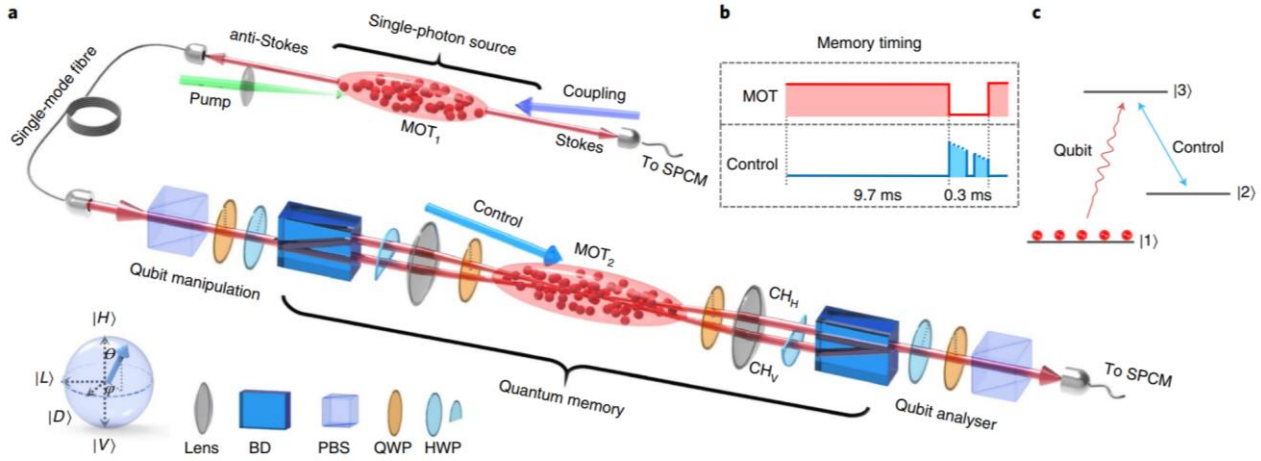


Fig. 1 | Experimental set-up and energy level scheme of the single-photon quantum memory. a, Schematic of the experimental optical set-up. The cold atoms in the first magneto-optical trap (MOT_1) serve as a nonlinear optical medium for producing time-frequency entangled photon pairs, while the cold atoms in the second magneto-optical trap (MOT_2) are the medium for the quantum memory. The anti-Stokes photon is coded with an arbitrary polarization state through the QMU consisting of a QWP and HWP. After the QMU, the two orthogonal linear polarizations are separated into two beams by a polarization beam displacer (BD) that are coupled into the two balanced spatial channels CH_H and CH_V of the quantum memory. The memory read-outs are recombined at the second BD and the polarization state is measured by the qubit analyser. **b**, The memory operation timing shows the MOT sequence and the optimized control laser intensity time-varying profile in each experimental cycle. **c**, The atomic energy level scheme of the quantum memory based on EIT.

Les travaux les plus avancés sont réalisés avec le stockage de l'état de polarisarion circulaire d'un photon unique piégé dans une structure en rubidium refroidie par laser dans un piège magnéto-optique et ainsi rendue transparente.

---

[127] Voir Architectures for a quantum random access memory, des Italiens Vittorio Giovannetti et Lorenzo Maccone et de l'Américain Seth Lloyd, 2008 (12 pages).

[128] Comme dans Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble, 2017 (13 pages), un papier auquel a contribué le Français Julien Laurat du CNRS.

C'est ce qu'on réalisé des scientifiques chinois[129]. Les atomes de rubidium sont refroidis à 200 µK, ce qui est bien bas par rapport aux 15mK d'un ordinateur quantique supraconducteur. On trouve des travaux voisins au Canada, avec l'exploitation du rubidium dont la transparence est contrôlée dynamiquement pour piéger un photon unique[130].

En pratique, les photons sont mémorisés pendant un millième de seconde. C'est suffisant pour un traitement dans un répéteur de télécommunication optique mais moins évident pour du calcul quantique.

Des mémoires optiques sont aussi testés avec de l'ytterbium, une terre rare contrôlable à haute fréquence.

Le procédé est voisin du précédent et consiste à conserver la polarisation d'un photon unique dans un piège magnétique mais plutôt pour des applications de répéteurs optiques dans des lignes de communication sécurisée à longue distance[131]. Le stockage d'un état quantique est aussi possible dans des spins d'électrons[132].

Energie

Qu'en est-il de la puissance électrique consommée par l'ensemble ? A ce jour, elle est relativement raisonnable. Un ordinateur quantique consomme environ 15 KW, soit l'équivalent d'une trentaine de serveurs Intel, dont 14KW uniquement pour la réfrigération.

Lorsque l'on alignera des milliers de qubits dans ces machines, leur consommation pourra cependant augmenter du fait de l'énergie à dépenser pour maintenir le calculateur à basse température et du coût énergétique des portes quantiques et de la correction d'erreurs[133].

L'avantage quantique énergétique vient des portes quantiques qui sont réversibles. Cela procure un avantage énergétique certain par rapport aux ordinateurs traditionnels qui utilisent des portes logiques non réversibles. La réversibilité permet de consommer beaucoup moins d'énergie. Les arbitrages sont complexes à réaliser : la correction d'erreurs génère de l'entropie car on fait un reset des registres quantiques à chaque correction d'erreur et cela consomme de l'énergie. La consommation d'énergie des portes quantiques actuelles est de l'ordre de 10^{-17} Joule. La limite basse théorique régie par la fameuse loi de Landauer est de l'ordre de 10^{-21} Joule.

---

[129] Comme relaté dans HKUST Physicist Contributes To New Record Of Quantum Memory Efficiency, 2019, qui fait référence à Efficient quantum memory for single-photon polarization qubits (8 pages).

[130] Avec Physicists create new, simpler-than-ever quantum 'hard drive for light', de Kate Willis, Université d'Alberta, 2018. L'article d'origine est Coherent storage and manipulation of broadband photons via dynamically controlled Autler-Townes splitting, octobre 2017 (17 pages).

[131] Voir Des mémoires quantiques grâce à l'ytterbium par Alexandre Couto, août 2018, qui fait référence à Simultaneous coherence enhancement of optical and microwave transitions in solid-state electronic spins, décembre 2017 (10 pages). Ce sont des travaux conjoits entre l'Université de Genève, notamment Nicolas Gisin, et le CNRS.

[132] Voir Storing quantum information in spins and high-sensitivity ESR, par deux chercheurs dont Patrice Bertet du groupe Quantronics du CEA/CNRS, septembre 2017 (13 pages).

[133] C'est la thèse de Joni Ikonen, Juha Salmilehto et Mikko Mottonen dans Energy-Efficient Quantum Computing 2016 (12 pages).

Autre contrainte thermique à prendre en compte : le "budget" de chaleur qui peut être généré par les circuits quantiques et ce qui les accompagne. A 50 mK, il n'est que de 1 milliwatt. Il monte lorsque l'on atteint 1K. On peut alors dépenser environ 100 milliwatt. Or un transistor classique consomme 10 microwatts et il est actif environ 1% du temps. Ce qui donne un budget d'environ 10^6 transistors. Voilà une autre limite en nombre de qubits… !

Même sans avantage quantique, avec juste une "égalité quantique", à savoir la capacité à traiter certains calculs uniquement réalisables sur les plus grands supercalculateurs, les ordinateurs quantiques pourront procurer un avantage énergétique certain.

Les plus grands supercalculateurs du monde consomment plusieurs MW (mégawatts), dont deux ordres de grandeur de plus que les ordinateurs quantiques. Et ils prennent bien plus de place. Livré en 2019 au centre de recherche d'Oak Ridge du Département de l'Energie dans le Tennessee, l'IBM Summit consomme ainsi 13 MW pour une puissance crête de 200 petaflops et dont 3,9 MW pour le refroidissement (source).

Ces MW consommés par des milliers de chipsets CPU Power9s et des Nvidia V100 nécessitent un complexe système de refroidissement par eau qui pompe deux tonnes d'eau par minute. Le Summit occupe 500 m^2 et pèse 349 tonnes. A comparer à environ 2 tonnes pour un ordinateur quantique qui tient dans une pièce à température ambiante faisant à peu près 25 m^2, ce qui donne aussi un "avantage masse" et un "avantage surface".

Un supercalculateur de 2 petaflops de 2009 consommait déjà 6 MW (source). Le Titan d'Oak Ridge fourni par Cray et équipé de processeurs AMD atteint 27 petaflops pour 9 MW. Le supercalculateur le plus puissant du monde début 2018 était le chinois Sunway Taihulight avec une puissance de 125 petaflops et une consommation de 15 MW.

Le plus grand supercalculateur commercial début 2019 était le HPC4 du groupe Italien ENI, avec 18,6 petaflops sur 1600 nœuds HPE Proliant DL380 équipés de chipsets 24 cœurs Intel Skylake et 15 Po de stockage, pour une consommation supérieure à 10 MW et un coût total de $100M[134].

En France, le supercalculateur Joliot-Curie conçu par Atos était inauguré en juin 2019 au CEA à Bruyères-le-Chatel pour le GENCI (Grand Equipement National de Calcul Intensif). Il a une puissance de 9,4 petaflops et devrait atteindre après ses évolutions planifiées 22 pétaflops.

Cout et prix

Au vu de la faible maturité du marché, c'est presque une question qui n'a pas de sens. Les seuls ordinateurs quantiques qui sont commercialisés aujourd'hui sont ceux du canadien D-Wave, et à un prix unitaire de $15M.

[134] Voir Eni Launches 18.6-Petaflop Supercomputer, Michael Feldman, janvier 2019.

Le prix d'un ordinateur dépend de plusieurs paramètres dont le coût de fabrication et d'intégration de ses composants, les économies d'échelle, la marge du constructeur, le coût de maintenance et celui d'éventuels consommables. Ce sont des composantes dynamiques : plus le volume de ventes augmente, plus grandes sont les économies d'échelle. Or les volumes sont pour l'instant très faibles. Ils pourraient le rester longtemps jusqu'au jour où des applications émergeront qui toucheront un grand nombre d'utilisateurs et justifieront la fabrication en volume de ces ordinateurs. Il faut bien entendu y ajouter les coûts fixes de la R&D qui sont plus long à amortir si les volumes de vente sont limités.

Reprenons une par une les grandes composantes matérielles d'un ordinateur quantique avec cette analyse d'économies d'échelle :

- L'**ordinateur de contrôle** : c'est du standard.
- Les **composants électroniques** de contrôle des portes quantiques : leur technologie dépend du type de qubit utilisé. Dans les ordinateurs supraconducteurs, ce sont des générateurs de micro-ondes.
- Le **chipset** : celui a beau être fabriqué en technologies CMOS ou avoisinantes, leur volume de fabrication est très faible. Les économies d'échelle sont donc quasiment inexistantes.
- La **cryogénie** : ce sont des systèmes standards mais commercialisés en faible volume. Ils peuvent couter jusqu'à $1M.
- Les **consommables** : dans les ordinateurs quantiques fonctionnant à très basse température, il y a au minimum de l'azote liquide, de l'hélium 4 liquide (courant) et de l'hélium 3 liquide (beaucoup plus rare et cher). Il semble cependant que ces derniers ne soient pas des consommables et fonctionnent en circuit fermé dans le système de cryogénie.

Par contre, cette liste de composants pourrait rester à peu près stable au gré de l'augmentation de la capacité des ordinateurs quantiques en termes de qubits. Au nez, on peut donc considérer que le prix des D-Wave à $15M puisse rester quelques temps une fourchette haute du prix d'un ordinateur quantique. Ce prix pourra décroître au gré de l'accroissement du volume de production, qui dépendra étroitement des usages.

Dans la pratique, nombre d'ordinateurs quantiques seront utilisables comme des ressources dans le cloud et avec un coût plus modéré. C'est ce que proposent déjà IBM, Rigetti et D-Wave et proposeront Google et Microsoft.

Seul Intel pourrait être amené à vendre des ordinateurs ou des processeurs sans les proposer dans le cloud. Et encore, on n'en sait vraiment rien !

Paramètres clés d'un ordinateur quantique

Avant de décrire les différents types d'ordinateurs quantiques, faisons un détour par la définition des paramètres clés de performance d'un ordinateur quantique définis en 2000 par **David DiVicenzo**, alors chercheur chez IBM et maintenant enseignant checheur à l'Université d'Aix la Chapelle en Allemagne[135].

Alors que les qubits individuels existaient à peine, il définissait les caractéristiques techniques de base d'un tel ordinateur comme suit :

- Des **qubits bien caractérisés** : l'ordinateur quantique utilise des qubits qui exploitent des particules élémentaires pouvant avoir deux états distincts et mesurables. On en connait bien les caractéristiques physiques. L'architecture est scalable au sens où elle permet d'aligner un grand nombre de qubits en batterie. Aujourd'hui existent plusieurs types de qubits déjà évoqués avec les supraconducteurs, les ions piégés, les lacunes de carbone dans le diamant de synthèse, les photons, les fermions de Majorana ou encore les quantum dots de silicium. Dans la pratique, seuls les qubits à base de supraconducteurs sont opérationnels et à petite échelle.
- Des **qubits initialisables** : en général, à la valeur 0 appelée souvent "ground state" pour les quantums associés, correspondant, par exemple, au niveau d'énergie le plus faible d'une particule élémentaire.
- Des **temps de cohérence** largement supérieurs au temps d'activation des portes quantiques : nous l'avions déjà évoqué dans une partie précédente. Le temps pendant lequel les qubits sont en état de cohérence (superposition d'états) et intriqués (liens entre qubits via des portes doubles) doit être supérieur à la durée d'activation des portes pour que l'on puisse exécuter un algorithme contenant un enchainement d'un grand nombre de portes quantiques. Le ratio espéré est au moins de 1000 pour 1 pour pouvoir exécuter jusqu'à quelques centaines de portes quantiques d'affilée sachant que cette quantité va intégrer les longues suites de portes quantiques utilisées par les codes de correction d'erreurs.
- Un jeu de **portes quantiques universelles** : les qubits doivent pouvoir être contrôlés physiquement avec au moins deux portes quantiques jouant le rôle de portes quantiques universelles à partir desquelles on va pouvoir reproduire toutes les portes quantiques classiques. Il faut au minimum une porte unitaire (agissant sur un seul qubit comme la porte X) et une porte à deux qubits comme la CNOT. L'architecture physique des qubits conditionne la nature des portes quantiques universelles qui agissent sur les qubits. Elles ne sont pas les mêmes d'une technologie à l'autre.
- La **capacité à mesurer l'état des qubits** à la fin des calculs : qui semble évidente. Cette mesure ne doit pas influencer l'état des autres qubits du système. Il faudrait idéalement avoir un taux d'erreur de la mesure qui soit largement inférieur à 0,1%.

[135] Dans The Physical Implementation of Quantum Computation de David P. DiVincenzo, 2000 (9 pages).

David DiVicenzo ajoutait deux autres critères optionnels qui servent plutôt aux communications quantiques :

- La possibilité de **convertir des qubits statiques** en qubits pouvant se déplacer, notamment des photons. Ces qubits mouvants sont appelés en anglais des flying qubits.
- Puis une manière de **transporter ces qubits mouvants** d'un point à l'autre de manière fiable et à distance. Cela permettra de gérer des architectures distribuées de calculateurs quantiques et de mettre en place des architectures de *blind computing* permettant de distribuer des traitements en protégeant leur confidentialité. La technologie deviendra vite indispensable pour permettre la répartition de calculs quantiques sur plusieurs processeurs quantiques, un peu comme on le fait avec les chipsets multi-coeurs ou avec les architectures de répartition de traitement sur plusieurs CPU et plusieurs serveurs. Cela sera utile pour les architectures de qubits qui seront limitées en nombre de qubits par systèmes de cryogénie qui ne pourront en consolider que quelques centaines grand maximum. Il faudra donc pouvoir relier des qubits de processeurs distants pour permettre leur intrication selon les algorithmes utilisés. Différentes techniques d'interconnexion quantiques sont possibles. La plus générique est optique et elle est faiblement contrainte par la distance. A courte distance, des liaisons par micro-ondes sont envisageables, notamment pour coupler des qubits supraconducteurs.

  L'Université de **Princeton** associée à celle de **Konztanz** en Allemagne travaille de son côté sur l'interconnexion optique entre processeurs quantiques CMOS[136]. La magie consiste à transférer l'état quantique d'un spin d'électron à un photon au niveau de sa phase.

critères de DiVincenzo (IBM, 2000)	**valeurs courantes**
qubits bien caractérisés	supraconducteurs, ions piégés, …
initialiser tous les qubits	à valeur 0 (ground state)
temps cohérence >> activation porte quantique	100 µs vs 10-650 ns
jeu de portes quantiques universelles	X, H, CNOT, SWAP, …
mesurer les qubits à la fin du calcul	avec erreur < 0,1%

autres critères pratiques	**valeurs courantes**
nombre de qubits	<=72 en UQ et 2048 en QA
température d'opérations	15 mK ou température ambiante

D'un point de vue pratique, on caractérise aussi les ordinateurs quantiques par leur nombre de qubits et par leur température de fonctionnement.

[136] C'est documenté dans Quantum Computing Advances With Demo of Spin–Photon Interface in Silicon, 2018.

Le nombre de qubits est à évaluer à la fois dans le temps présent mais dans sa capacité à évoluer. Certaines technologies sont plus faciles à miniaturiser que d'autres. Et il faut intégrer dans cette miniaturisation à la fois les chipsets quantiques de qubits et les éléments qui les contrôlent. Aujourd'hui, les qubits à ions piégés ou en photonique scalent mal. Les qubits supraconducteurs scalent moyennement. Et les qubits en CMOS (spins d'électrons et quantum dots) scalent le mieux.

Les ordinateurs quantiques actuellement opérationnels, à base de supraconducteurs, fonctionnent tous à très basse température autour de 15 mK (1 mK = 1 milli-kelvin, 0 kelvin = 0 absolu situé à –273,15°C), mais certains types de qubits à l'état de recherche sont censés fonctionner à température ambiante, comme ceux de l'optique linéaire à base de photons et les NV Centers (cavités dans du diamant dopé à l'azote). Le fonctionnement à très basse température est un moyen de préserver la cohérence des qubits. Mais il limite la quantité d'énergie consommable autour des qubits pour en contrôler localement l'état. Un fonctionnement à 1K ou 4K permettra de consommer plus d'énergie pour contrôler les qubits qu'un fonctionnement à 15 mK. En effet, le budget thermique de refroidissement est proportionnel au carré de la température et est donc très faible à 15 mK.

Ces considérations permettant de jauger les capacités d'un ordinateur quantique impliquent la création d'une nouvelle discipline : le benchmarking d'ordinateurs quantiques ! Elle nécessite évidemment des moyens intellectuels et physiques qui dépassent ceux du test de simples smartphones ou laptops !

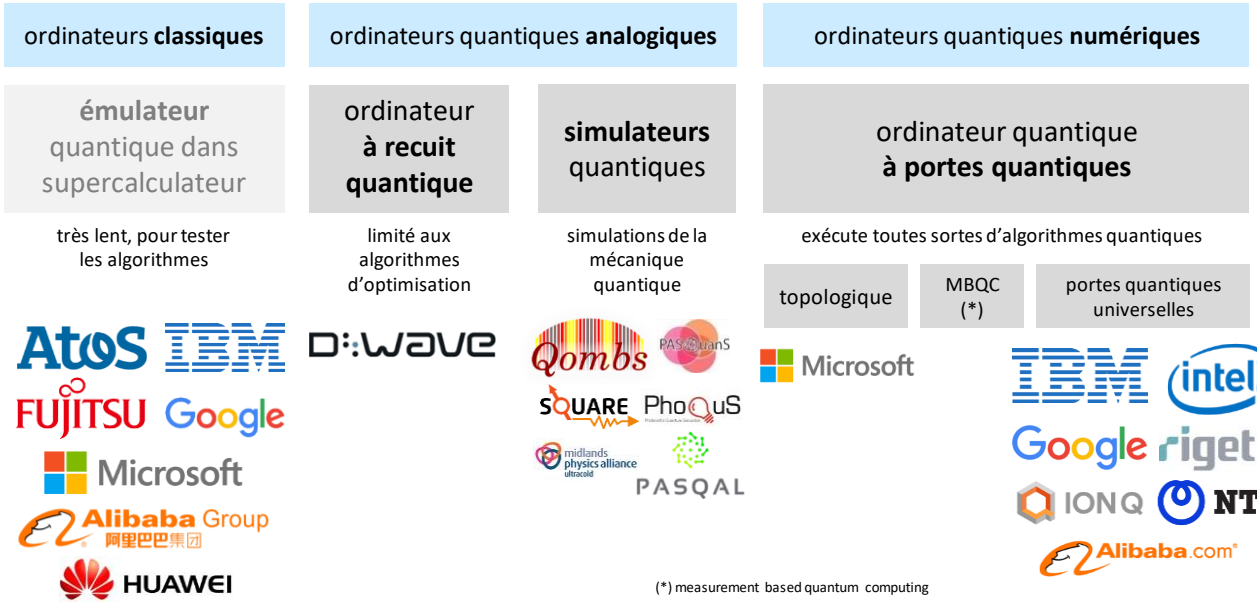
Comme l'indique Kristel Michielsen[137], les benchmarks peuvent s'appuyer lorsque le nombre de qubits est inférieur à 50 à une comparaison du rendu des algorithmes entre ordinateurs quantiques et leur simulation sur supercalculateurs.

Les ordinateurs quantiques benchmarkés auront généralement des caractéristiques dissemblables : des portes quantiques universelles différentes nécessitant l'assemblage de différentes portes quantiques par les compilateurs pour exécuter un même algorithme, et des codes de correction d'erreurs différents, adaptés au taux d'erreurs des qubits et des portes quantiques des ordinateurs comparés. Les dissemblances seront bien plus importantes qu'entre deux processeurs Intel et AMD ou deux processeurs de smartphones !

Grandes catégories d'ordinateurs quantiques

Il y a ordinateur quantique et ordinateur quantique. On oppose souvent les ordinateurs quantiques adiabatiques du Canadien D-Wave aux ordinateurs quantiques universels d'IBM ou Google.

[137] Dans Benchmarking gate-based quantum computers, 2017 (33 pages).



Mais il faut compter en tout avec au moins quatre catégories d'ordinateurs quantiques que voici :

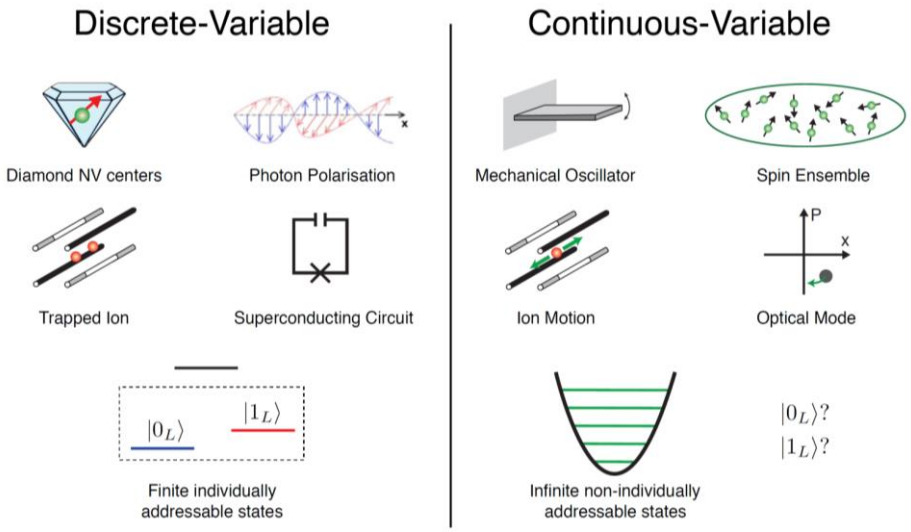
- Les **émulateurs quantiques** qui sont utilisés pour réaliser des simulations de l'exécution d'algorithmes quantiques dans des ordinateurs traditionnels qui vont de simples laptops à des supercalculateurs, selon le nombre de qubits à émuler. Ils transforment ces algorithmes, les portes quantiques et les qubits pour exploiter les capacités de traitement d'ordinateurs traditionnels. Cela permet de tester des algorithmes quantiques sans ordinateurs quantiques. Mais c'est bien plus lent !

  A ce jour, les supercalculateurs peuvent simuler jusqu'à l'équivalent d'une quarantaine à une cinquantaine de qubits, mais nous avons vu précédemment que des records avaient été battus avec plus de 100 qubits, avec un faible nombre de portes quantiques. C'est ce que proposent IBM, Microsoft, Google et le Français Atos. Simuler des ordinateurs quantiques de cette manière demande beaucoup de puissance à la fois côté mémoire, pour stocker 2^N états de registres quantiques à N qubits, ainsi que pour les traitements associés qui reposent sur des multiplications de matrices en nombres flottants. Des records dans ce domaine sont régulièrement battus.

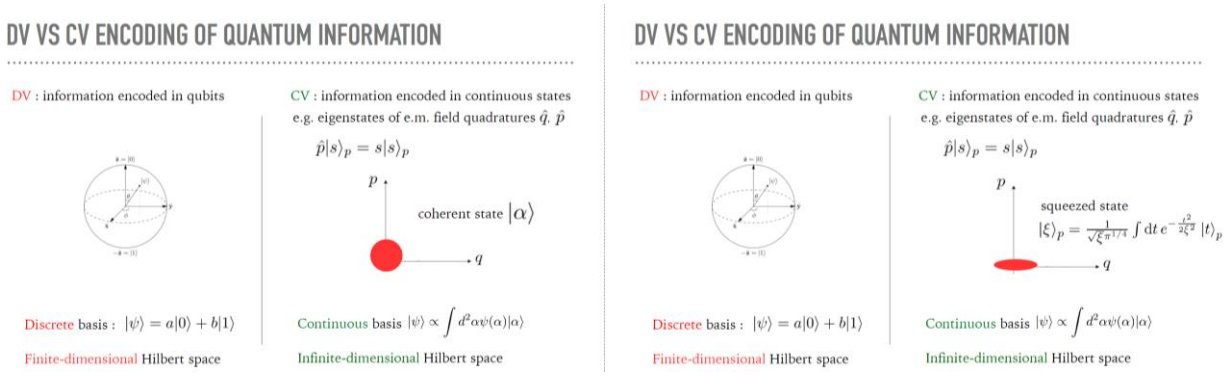
  En 2017, la simulation de 45 qubits était réalisée sur un supercalculateur du Département de l'Energie US (du National Energy Research Scientific Computing Center ou NERSC) exploitant 8192 processeurs Intel Xeon Phi, ce qui s'explique par la présence d'un centre de recherche conjoint avec Intel au NERSC. Le record était battu la même année par IBM avec la simulation de 56 qubits. Pour simuler 49 qubits, il faut rien moins qu'un Péta-Octets de mémoire vive !

- Les **ordinateurs quantiques à recuit simulé** comme ceux du Canadien D-Wave. Ils s'appuient sur des qubits de qualité moyenne et sont adaptés à l'exécution d'une partie seulement des algorithmes quantiques connus et avec un gain en puissance de calcul intéressant mais contesté par certains spécialistes. Cette technique utilise une évolution lente et contrôlée d'un ensemble de qubits reliés entre eux dans des matrices de qubits ("lattice"). On l'initialise dans un état voisin de la solution et le système converge vers la solution qui relève souvent de la recherche d'un minimum énergétique comme pour la simulation d'interactions atomiques dans des molécules ou l'optimisation de la durée d'un parcours complexe.
- Les s**imulateurs quantiques analogiques** servent de simulateurs de phénomènes quantiques sans passer par la case qubits avec ses 0 et 1. Ils fonctionnent de manière analogique et non numérique, à savoir que les valeurs utilisées sont continues. Ce sont pour l'instant surtout des outils de laboratoires. Les techniques les plus couramment utilisées sont les atomes froids contrôlés par laser. Elle peut d'ailleurs être exploitée aussi bien pour créer des ordinateurs quantiques analogiques que des ordinateurs quantiques universels à base de qubits et de portes quantiques. On peut considérer que les ordinateurs quantiques à recuit simulé et les simulateurs quantiques analogiques font partie tous deux de la catégorie des ordinateurs quantiques analogiques, avec des nuances d'architecture.
- Les **ordinateurs quantiques à variables continues**, ou analogiques à portes universelles. Ils utilisent des qubits qui stockent des grandeurs variables entre 0 et 1 mais sont manipulables avec des portes quantiques[138].

les CV qubits permettraient de faire des calculs analogiques avec des ordinateurs quantiques à portes universelles.



[138] Voir Universal Quantum Computing with Arbitrary Continuous-Variable Encoding, 2016 (5 pages).



- Les **ordinateurs quantiques universels** utilisent des qubits avec des portes quantiques capables d'exécuter tous les algorithmes quantiques et avec un gain de vitesse optimum par rapport aux supercalculateurs ainsi que vis à vis des ordinateurs quantiques adiabatiques[139]. Ils sont pour l'instant limités à une cinquantaine de qubits. Le niveau de bruit quantique des qubits nuit à l'efficacité des calculs et impose de démultiplier les qubits et l'enchaînement des portes quantiques pour gérer des codes de correction d'erreurs quantiques (QEC). En attendant que ces ordinateurs quantiques montent en puissance avec des qubits de qualité, on se contente de qubits de qualité intermédiaire. Cette sous-catégorie d'ordinateurs quantiques universels est baptisée NISQ pour "Noisy Intermediate-Scale Quantum" par John Preskill[140]. Elle décrit les ordinateurs quantiques universels existants et à venir dans un futur proche supportant 50 à quelques centaines de qubits et à même de dépasser les capacités des supercalculateurs.
- Les MBQC, ou **Measurement Based Quantum Computers**, sont une variante d'ordinateurs qui utilisent des qubits, mais exploités différemment, avec une mise en intrication de l'ensemble des qubits suivie d'une lecture de l'état de certains qui permet d'avancer pas à pas dans la résolution d'algorithmes en simulant des portes quantiques.

Incertitude quantique

La prospective dans l'informatique quantique est art difficile. On navigue entre les optimistes et les pessimistes. **Google**, **IBM** et **Microsoft** pensent atteindre relativement rapidement la suprématie quantique et réaliser des ordinateurs quantiques de plus de 100 qubits de qualité d'ici moins d'une décennie. Leur communication se fait à plusieurs niveaux : pour le grand public, elle est simplificatrice et destinée à marquer les esprits, quitte à enjoliver la mariée.

Pour les spécialistes qui peuvent décortiquer leurs publications scientifiques, le regard est évidemment plus nuancé, notamment au sujet de la fiabilité des qubits qu'ils génèrent. Ils communiquent beaucoup sur leurs efforts pour réduire le bruit des qubits pour les rendre plus fiables[141].

---

[139] En voici un panorama rapide dans Quantum Computing Circuits and Devices, avril 2018 (18 pages).

[140] Dans Quantum Computing in the NISQ era and beyond en 2018.

[141] Voir The Era of quantum computing is here. Outlook: cloudy de Philipp Ball paru en avril 2018 dans Science.

Les pessimistes comprennent notamment le chercheur israélien **Gil Kalai** qui pense que l'on n'arrivera jamais à créer des ordinateurs quantiques avec un faible taux d'erreurs[142]. Selon Gil Kalai, on ne peut pas créer d'ordinateurs quantiques stables à cause du bruit qui affecte les qubits.

Il travaille même sur la réalisation de modèles mathématiques visant à prouver l'impossibilité d'outrepasser ces erreurs, même avec les codes de correction d'erreurs quantiques.

L'un des autres détracteurs du calcul quantique est le chercheur russe **Mikhail Dyakonov** (né en 1940 en URSS) qui officie dans le Laboratoire Charles Coulomb (L2C) du CNRS et de l'Université de Montpellier. Il a exprimé son point de vue dans un article largement relayé dans le monde fin 2018[143]. Son argumentaire est plus intuitif et moins bien documenté que celui de Gil Kalai[144].

Cristian Calude et **Alastair Abbot** évoquent le fait que l'avantage des principaux algorithmes quantiques utilisables en pratique généreraient une accélération modeste quadratique (racine carrée du temps classique) qui pourrait être atteinte sur ordinateurs classiques avec des approches heuristiques[145]. Cette réserve est aussi manifeste chez **Ed Sperling** qui faisait le point du domaine en novembre 2017 en rappelant tous les obstacles à surmonter[146].

Kenneth Regan pensait en 2017 qu'un industriel – probablement Google – devait prétendre avoir atteint la suprématie quantique en 2018 et qu'il serait rapidement contredit par la communauté scientifique[147]. Il semblerait que cela soit pour 2019.

Il est difficile de faire la part des choses entre l'incertitude scientifique et l'incertitude technologique. La première est généralement plus difficile à lever que la seconde.

Pour le Français **Alain Aspect**, il n'y aurait pas d'obstacle scientifique à la création d'ordinateurs quantiques fiables. Il pense que l'incertitude est uniquement technologique mais qu'il faudra quelques décennies pour la lever. Ce ne serait donc qu'une affaire de patience !

Ce lot d'incertitudes pose des questions existentielles sur la manière de gérer un tel cycle d'innovation au long cours. Quand faut-il investir ? Quand les positions sont-elles prises ? Est-ce que la recherche fondamentale est découplée de l'industrialisation ? Je traite de la question dans la partie dédiée aux stratégies industrielles des pays qui s'investissent avec volontarisme dans le quantique.

---

[142] Il documente son point de vue dans la présentation Why Quantum Computers Cannot Work qui date de 2013 (60 slides) qui reprend les points de How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation de 2011 (16 pages) ainsi que The Argument Against Quantum Computers de Katia Moskwitch publié en février 2017.

[143] Voir The Case Against Quantum Computing, 2018. Ainsi qu'un débat sur le sujet lancé par Scott Aaronson dans Happy New Year! My response to M. I. Dyakonov. Voir aussi Skepticism of Quantum Computing de Scott Aaronson qui décortique 11 objections sur l'ordinateur quantique.

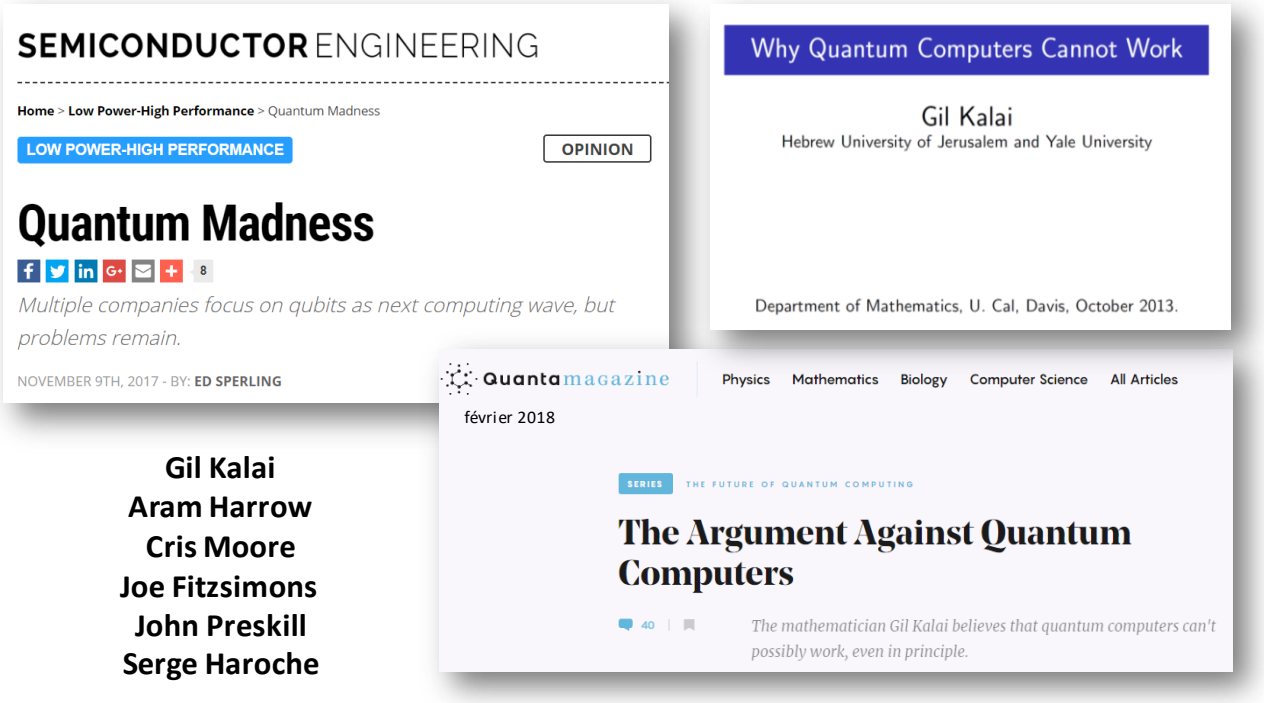
[144] Voir une réponse à cet argumentaire dans The Case Against 'The Case Against Quantum Computing' par Ben Crige, janvier 2019.

[145] Dans The development of a scientific field par Alastair Abbott et Cristian Calude, juin 2016.

[146] Dans Quantum Madness, de Ed Sterling, novembre 2017.

[147] Dans Predictions we didn't make, en janvier 2018.

Mais on peut déjà constater que les variantes de cultures d'innovation et économiques ont un impact sur les approches industrielles. Les grands industriels du numérique tels que IBM, Google, Intel et Microsoft peuvent se permettre d'investir en R&D sur le quantique avec une vision très long terme. Ils ont la profitabilité, le cash et les compétences qui le permettent.

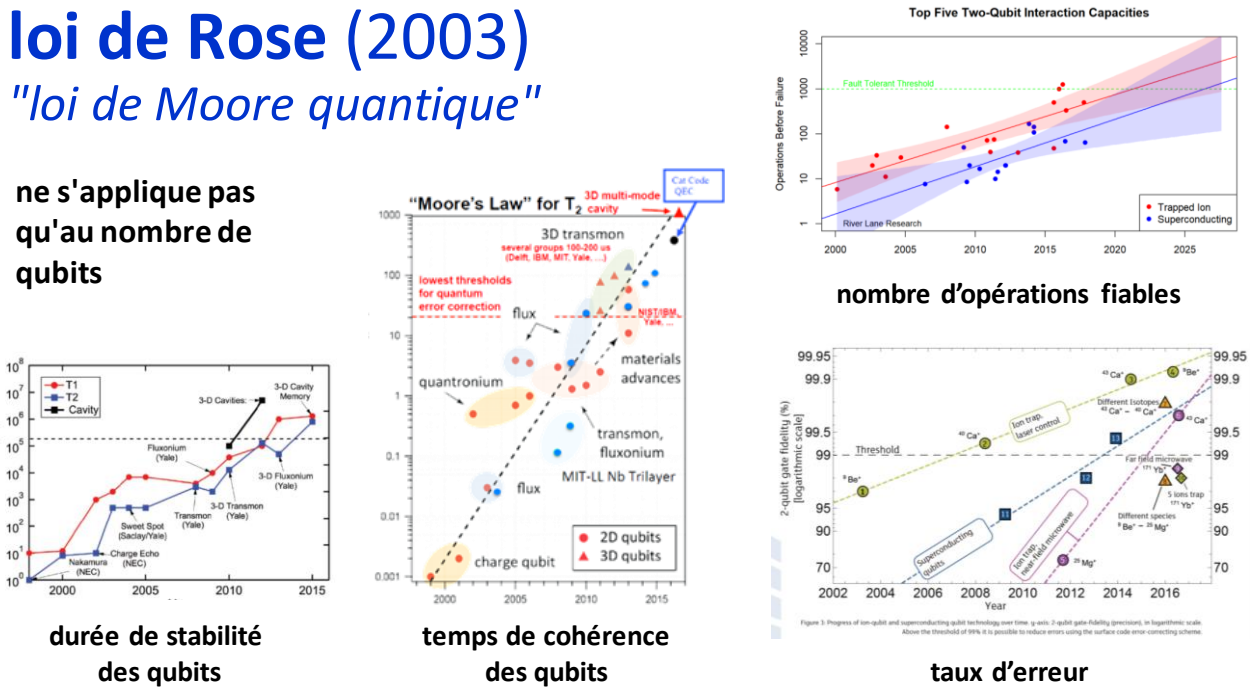


Des startups plus ou moins bien financées au Canada et aux USA comme D-Wave, Rigetti ou IonQ peuvent aussi adopter une vision assez long terme, même si elle dépend toujours de leur capacité à commercialiser des prototypes d'ordinateurs quantiques et d'avoir des investisseurs à même de les accompagner sur de nombreuses années avant de voir la couleur de leur retour sur investissement. Les montants correspondants ne sont pas forcément délirants. Rigetti n'a levé à ce jour que $70M, un montant maintenant accessible à des startups françaises dans les biotechs ou le numérique en général.

Les problèmes technologiques à résoudre concernent les matériaux utilisés dans les qubits, la correction d'erreurs, la cryogénie à grande échelle pour pouvoir intégrer un grand nombre de qubits dans un ordinateur et bien évidemment les avancées algorithmiques. L'approche requise est éminemment pluridisciplinaire avec des mathématiques, de la physique fondamentale, de la thermodynamique et de la chimie.

On peut aussi extrapoler les évolutions de ces dix dernières années dans l'informatique quantique. Cofondateur de D-Wave en 1999, Georgie Rose édicta en 2003 son propre équivalent de la loi empirique de Moore, la loi de Rose, prédisant un doublement tous les ans du nombre de qubits dans un ordinateur quantique. Jusqu'à présent et depuis 2007, D-Wave a tenu cette promesse.

Mais cette loi exponentielle est aussi observée dans l'évolution d'autres paramètres de fonctionnement des ordinateurs quantiques comme la durée de stabilité des qubits, leur taux d'erreur et le nombre d'opérations consécutives réalisées de manière fiable[148].



J'ai cherché à comprendre pourquoi les prévisions de création d'ordinateurs quantiques viables étaient toujours à assez long terme, entre 5 et 50 ans.

L'une des réponses vient de la durée des cycles dans la recherche associée.

Par exemple, pour obtenir un prototype de chipset de qubits CMOS, il faut compter entre un et six mois de fabrication selon le nombre d'étapes de la fabrication qui va de 20 à une centaine selon les cas. Le temps est allongé lorsque le processus de fabrication est nouveau et qu'il faut régler les machines.

Après cette fabrication, il faut passer par l'étape de caractérisation et de packaging des composants. La caractérisation vise à tester qualitativement et à sélectionner les composants fabriqués. Cela peut durer jusqu'à un mois et dans le meilleur des cas descendre à une semaine.

Ensuite, pour mener les tests, la thermalisation de l'ordinateur dure environ 24 heures et le changement de chipset à tester dure au minimum entre 3 et 7 heures comme nous l'avons découvert dans la partie sur la cryogénie. Finalement, les cycles de *test & learn* sont longs, bien plus longs que dans le logiciel !

[148] Une partie des schémas ci-dessous proviennent de Technical Roadmap for Fault-Tolerant Quantum Computing, un rapport UK publié en octobre 2016 et de cette autre source

Algorithmes et usages

Après avoir désossé un ordinateur quantique avec ses qubits, ses registres, ses portes et son frigo, voyons-donc comment on peut l'exploiter.

L'ordinateur quantique utilise des algorithmes dits quantiques qui ont la particularité d'être bien théoriquement plus efficaces que leurs équivalents conçus pour des ordinateurs traditionnels. Ces algorithmes ne sont pour l'instant pas très nombreux et leur performance relative vis-à-vis d'algorithmes traditionnels pas toujours évidente à prouver. Elle est même parfois contestée. L'assertion « *l'ordinateur quantique est plus rapide que les ordinateurs traditionnels* » est donc discutable et discutée et s'analyse au cas par cas.

Richard Feynman avait décrit l'idée de créer des simulateurs quantiques en 1982[149]. Son idée consistait à créer des dispositifs exploitant les effets de la mécanique quantique pour les simuler tandis que cette simulation serait quasiment impossible avec des ordinateurs traditionnels. Cela correspond aujourd'hui à l'un des usages des ordinateurs quantiques, comprenant notamment la simulation des interactions atomiques dans des structures inertes ou biologiques. On doit même faire la distinction entre simulateurs quantiques analogiques et ordinateurs quantiques numériques, à base de qubits et de portes quantiques, un sujet que nous aborderons dans la partie concernant les différents types d'ordinateurs quantiques du marché.

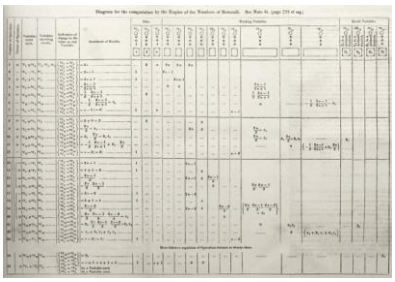
Des mathématiciens planchent depuis le milieu et la fin des années 1980 sur la création d'algorithmes adaptés aux simulateurs et ordinateurs quantiques, bien avant que l'on ait vu l'ombre de la couleur de ces derniers.

Ainsi, les premiers algorithmes quantiques ont été publiés au début des années 1990 alors que les premiers systèmes quantiques à deux qubits ont apparus aux alentours de 2000/2002. Les chercheurs créent régulièrement de nouveaux algorithmes depuis 25 ans, indépendamment des lents progrès du côté des ordinateurs. Le Quantum Algorithm Zoo en identifie une soixantaine de classes dans la littérature scientifique. C'est un nombre encore modeste au regard des algorithmes non quantiques qui se comptent en milliers.

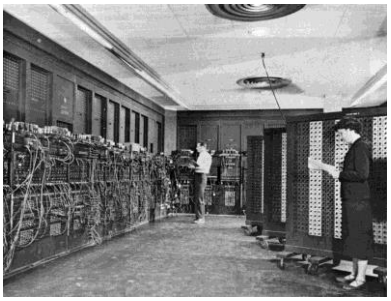
La création d'agorithmes quantiques est donc un objet de recherche parallèle avec la partie matérielle des ordinateurs quantiques. Ce n'est pas la première fois dans l'Histoire qu'il en est ainsi. L'emblématique **Ada Lovelace** planchait sur la création des premiers algorithmes et lignes de code devant tourner sur la machine de **Charles Babbage**, qui ne vit jamais le jour (voir l'exemple de programme *ci-dessous*). Elle avait annoté en 1842/1843 une traduction de son cru d'un papier de l'Italien **Luigi Federico Menabrea** qui décrivait la machine de Babbage. Il fallut attendre 102 ans pour que les premiers ordinateurs voient le jour à la fin de la seconde guerre mondiale ! Un beau jeu de patience !

---

[149] Dans Simulating Physics with Computers, Richard Feynman, 1982 (22 pages).

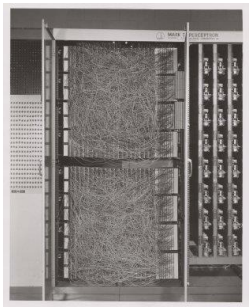


Ada Lovelace
1842, premier programme pour la machine de Babbage qui ne vit jamais je jour



ENIAC
1945, premier ordinateur

McCulloch & Pitts
1943, concept des neurones artificiels



Mark I Perceptron computer
1957, premier processeur synaptique

Alexnet sur Nvidia GTX 580
2012, premier réseau de neurones avec un taux de reconnaissance d'image avec moins de 30% d'erreurs !

Léonard de Vinci
1487, vis aérienne

Paul Cornu, 1907
premier vol d'hélicoptère motorisé
1,5 m d'altitude

AeroVelo, 2013
premier vol d'hélicoptère à force humaine

Cela rappelle aussi les schémas d'hélicoptères de **Léonard de Vinci** qui datent de 1487-1490. Un premier hélicoptère propulsé par l'énergie humaine et créé par l'Université de Toronto a volé en 2013, AeroVelo (vidéo) suivi d'un autre spécimen assez voisin issu de l'Université de Maryland qui volait en 2018 (vidéo) ! Donc, avec plus de cinq siècles de décalage ! Et même en tenant compte le vol du premier hélicoptère motorisé en 1907, le décalage reste supérieur à quatre siècles.

Cette même Université de Maryland est d'ailleurs l'une des plus en pointe dans le monde dans les ordinateurs quantiques à base d'ions piégés ! Comme quoi !

Après-guerre, l'Histoire se répéta en partie pour nombre de travaux du vaste champ de l'intelligence artificielle, où les chercheurs planchaient également sur des algorithmes, notamment à base de réseaux de neurones, avant que les ordinateurs puissent les exécuter convenablement. Les premièrs ordinateurs gérant en 1957 des perceptrons, les ancêtres des réseaux de neurones artificiels d'aujourd'hui, étaient rudimentaires. L'essor du deep learning depuis 2012 est en partie lié à la puissance des machines et des GPU à même d'entraîner de tels réseaux de neurones. Le matériel a une fois encore rejoint les algorithmes qui étaient en avance sur leur temps.

Aujourd'hui encore, une bonne part des algorithmes quantiques qui sont inventés ne sont pas encore exécutables à grande échelle sur les ordinateurs quantiques disponibles ni même sur des simulateurs quantiques à base d'ordinateurs traditionnels. Les qubits sont disponibles dans un nombre bien trop faible pour qu'ils servent à quelque chose et surtout, qu'ils soient plus performants que des ordinateurs traditionnels. Les supercalculateurs émulent difficilement plus de 50 qubits et aucun ordinateur quantique opérationnel ne dépasse ce nombre de qubits.

Dans une autre analogie avec le passé de l'Histoire de l'Informatique, nous en sommes encore dans le quantique à aborder la programmation via des « couches basses » de langage machine.

Un peu comme pour les programmeurs en langage machine ou en assembleur d'il y-a 30 à 50 ans, ou plus récemment, pour ceux qui ont programmé à bas niveau des systèmes embarqués ou des pilotes de périphériques dans la micro-informatique. Les algorithmes quantiques actuels sont les couches les plus basses des solutions logicielles qui restent à inventer puis à assembler.

La création d'algorithmes quantiques requiert une capacité d'abstraction sans commune mesure avec celle des algorithmes et programmes traditionnels. Une nouvelle génération de mathématiciens et développeurs capables de raisonner avec le formalisme mathématique de la programmation quantique devra se développer au gré de la maturation des ordinateurs quantiques. Ils devront être capables de conceptualiser des algorithmes qui ne sont pas faciles à se représenter physiquement. Qui plus est, ces algorithmes devront aussi, c'est la moindre des choses, être bien plus efficaces que leurs équivalents pour ordinateurs traditionnels ou supercalculateurs.

Les principaux algorithmes quantiques exploitent les portes quantiques que nous avons vues dans la partie précédente. Il est cependant possible qu'un jour, le niveau d'abstraction de création de logiciels quantique s'élève au point qu'il ne soit plus nécessaire de comprendre le fonctionnement à bas niveau des portes quantiques. C'est une conjecture, rien de plus !

Qui plus est, l'algorithmie quantique est aussi variée que les types d'ordinateurs quantiques qu'il est ou sera possible de créer.

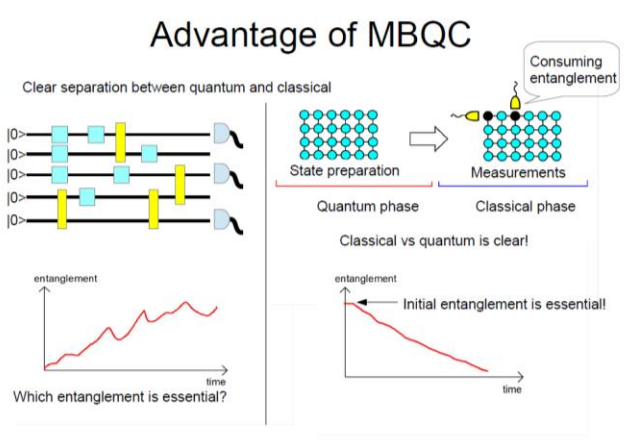
En plus des algorithmes à base de portes quantiques[150], il faut en effet ajouter :

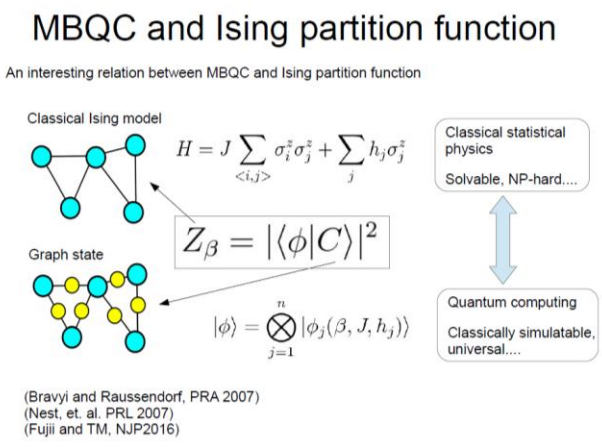
- Les algorithmes pour **ordinateurs à recuit quantique** comme ceux de D-Wave qui sont basés sur l'initialisation de relations entre qubits de qualité moyenne dans des matrices et sur la recherche d'un minimum énergétique s'appuyant notamment sur l'effet tunnel. Ils permettent l'exécution d'un grand nombre d'algorithmes quantiques.
- Les **simulateurs quantiques analogiques** qui servent à simuler des phénomènes quantiques permettant de prédire par exemple l'organisation des atomes dans des molécules. On y trouve notamment les simulateurs quantiques à atomes froids.
- Les **ordinateurs quantiques à variables continues** qui utilisent des objets quantiques dont on peut mesurer une grandeur physique continue et non pas binaire. Ils sont principalement à base de photonique[151].

[150] Aussi appelés UQCM pour Universal Quantum Cloning Machine.

[151] Voir par exemple Perspective: Toward large-scale fault-tolerant universal photonic quantum computing de S. Takeda & Al, April 2019 (13 pages).

- Les **ordinateurs quantiques topologiques**, qui n'existent pas encore. C'est la voie de recherche de Microsoft et de quelques laboratoires de recherche, notamment en Chine. Nous en reparlerons page 285.
- Les **algorithmes hybrides** associant algorithmes traditionnels et algorithmes quantiques ou bien des algorithmes à portes quantiques classiques et à base de MBQC[152]. C'est notamment le cas du Variational Quantum Eigensolver (VQE) qui permet la résolution de problèmes de simulation chimique aussi bien que d'entraînement de réseaux de neurones.
- Les méthodes du **Measurement-Based Quantum Computing (MBQC)** qui comprennent deux variantes, le *one way quantum computing*[153] et le *measurement-only QC*. Il s'agit d'ordinateurs qui exploitent l'initialisation de qubits intriqués dans des matrices bidimentionnelles (« cluster state ») (sauf dans le *measurement-only QC* qui ne fait que de la mesure, sans intrication). Les portes quantiques sont simulées par des actions de mesure de qubits de la matrice. Deux formes de mesures affectent le fonctionnement de la matrice de qubits : des mesures Z séparent les qubits en creusant des « sillons » dans la matrice, puis des mesures classiques le long des « fils » ou sur les « ponts » entre ces fils simulent des portes unitaires comme celle de Hadamard et la porte CNOT à deux qubits. L'enchaînement des opérations dépend du résultat des mesures. Le résultat du calcul est situé dans les derniers qubits dont l'état n'est pas encore mesuré… et qui sera mesuré en dernier lieu[154]. Ces algorithmes sont donc par définition des algorithmes hybrides puisque leur déroulement dépend d'interactions entre la partie quantique et l'exploitation des mesures par un ordinateur classique de pilotage de l'ensemble.





[152] Voir Hybrid Quantum Computation de Arun, 2011 (155 pages). C'est aussi la source du schéma des portes réalisées en MBQC.

[153] Le procédé a été conçu en 2000 par Robert Raussendor et Hans Briegel. Voir A computationally universal phase of quantum matter, de Robert Raussendorf, 2018 (41 slides), Measurement-based Quantum Computation d'Elham Kashefi, University of Edinburgh (50 slides) et Introduction to measurementbased quantum computation de Tzu-Chieh Wei de l'Université Stone Brook, 2012 (88 slides) et un one pager : Universal measurement-based quantum computation with Mølmer-Sørensen interactions and just two measurement bases. D'autres sources d'information à creuser : Blind quantum computation de Charles Herder (10 pages), Cluster-state quantum computation, de Michael Nielsen, 2005 (15 pages), Fault-tolerant quantum computation with cluster states, 2005 (26 pages), 2D cluster state (50 slides), Quantum Computing with Cluster States de Gelo Noel Tabia, 2011 (18 pages), Quantum picturalism for topological cluster-state Computing de Clare Horsman 2011 (18 pages) et Cluster State Quantum Computing de Dileep Reddy & al, 2018 (11 pages.

[154] Source des illustrations : Basics of quantum computing and some recent results de Tomoyuki Morimae, 2018 (70 slides).

Des ordinateurs de ce type sont réalisés à l'état expérimental en optique linéaire et avec des atomes froids. Je n'ai pas encore bien compris à quoi cela servait à part le fait que l'architecture est tolérante aux taux d'erreurs des qubits. Les startups qui se sont lancées dans ce créneau sont PsiQuantum (USA) et Pasqal (France). Les algorithmes sont spécifiques à ce genre d'architecture[155].

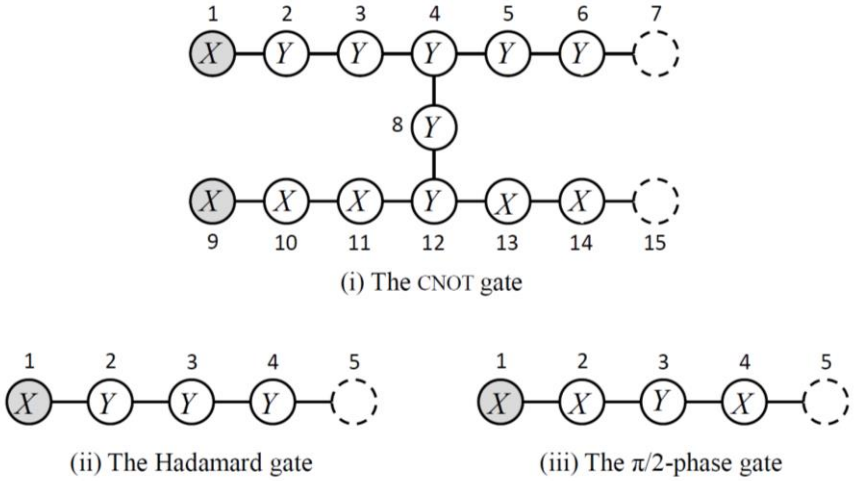


Figure 3.4: The measurement patterns (i), (ii), and (iii) on the 15-qubit, five-qubit, and five-qubit graphs are for simulating the CNOT, the Hadamard, and the $\pi/2$-phase gates, respectively. Qubits shown by gray and dotted circles are the input and the output qubits, respectively. The label X or Y on a qubit illustrates that the respective qubit will be measured in the X eigenbasis or in the Y eigenbasis.

- Les **algorithmes « quantum inspired »** qui sont des algorithmes destinés à des ordinateurs non quantiques mais qui s'inspirent d'algorithmes quantiques pour la résolution de problèmes complexes.

Suprématie et avantage quantiques

Avant de rentrer dans le détail des algorithmes quantiques, il nous faut expliquer la signification de la notion de "suprématie quantique" qui fleurit dans la communication de certains acteurs tels que Google. L'appellation a été créée en 2011 par l'Américain John Preskill dans une communication au Congrès de Solvay[156]. C'est un terme un peu galvaudé dont vous entendrez parler dans diverses annonces tonitruantes à venir[157]. Elle est maintenant souvent remplacée par avantage quantique qui est plus *politically correct*.

Une "suprématie quantique" est atteinte lorsqu'un algorithme traitant un problème donné n'est exécutable que sur un ordinateur quantique, ce problème ne pouvant pas être résolu sur le plus puissant des supercalculateurs.

---

[155] Voir par exemple Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states, mai 2019 (16 pages). L'article décrit une méthode de MBQC basée sur l'exploitation de portes de Toffoli (CCZ) et Hadamard (H). Elles permettent de simuler du calcul quantique topologique, réducteur du taux d'erreur du calcul quantique.

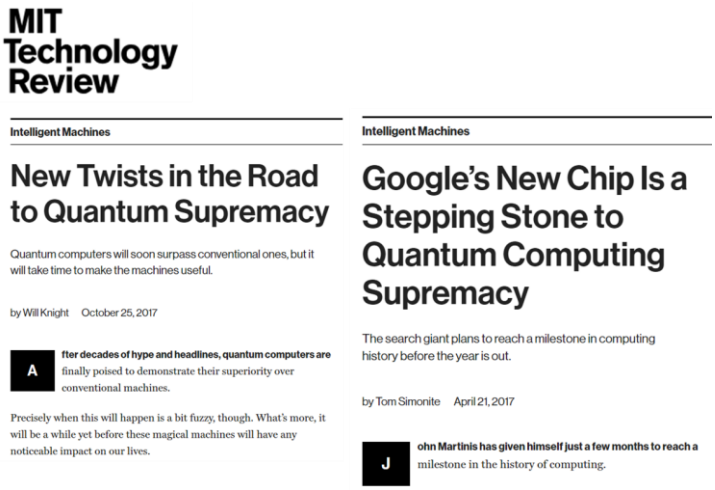
[156] Elle est décrite dans Quantum Computing and the Entanglement Frontier, 2011.

[157] Voir par exemple New twists in the road to quantum supremacy et Google's new chip is a stepping stone to quantum computing supremacy publiés dans la sérieuse MIT Technology Review en 2017.

Un « avantage quantique » correspond au cas où un ordinateur quantique exécute un algorithme bien plus rapidement que sur les supercalculateurs les plus puissants.

De nombreux spécialistes affirment que le seuil de 50 qubits de qualité - avec un faible taux d'erreurs et un long temps de décohérence - constituera une étape clé de l'atteinte d'une suprématie quantique. « Une » parce qu'elle est définie au cas par cas.

Cette appellation ne signifiera pas qu'un ordinateur quantique donné est suprêmement plus puissant que tous les supercalculateurs du moment. L'appellation devra être utilisée pour des couples d'algorithmes quantiques et d'ordinateurs quantiques, et avec des tests réalisés sérieusement avec le meilleur possible des algorithmes adapté aux meilleurs supercalculateurs sachant que ceux-ci sont aussi mouvants.



MIT Technology Review

Intelligent Machines

New Twists in the Road to Quantum Supremacy

Quantum computers will soon surpass conventional ones, but it will take time to make the machines useful.

by Will Knight October 25, 2017

After decades of hype and headlines, quantum computers are finally poised to demonstrate their superiority over conventional machines.

Precisely when this will happen is a bit fuzzy, though. What's more, it will be a while yet before these magical machines will have any noticeable impact on our lives.

Intelligent Machines

Google's New Chip Is a Stepping Stone to Quantum Computing Supremacy

The search giant plans to reach a milestone in computing history before the year is out.

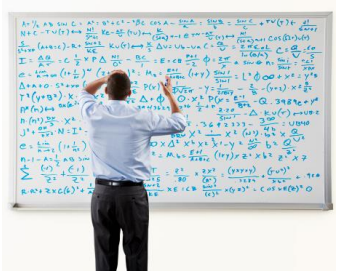
by Tom Simonite April 21, 2017

John Martinis has given himself just a few months to reach a milestone in the history of computing.

Robert König (Université Technique de Munich), David Gosset (Université de Waterloo au Canada) et Sergey Bravyi (IBM) démontraient ainsi en octobre 2018 que les ordinateurs quantiques peuvent réellement réaliser des opérations inaccessibles aux ordinateurs classiques, mais en s'appuyant seulement sur le cas d'un algorithme particulier[158].

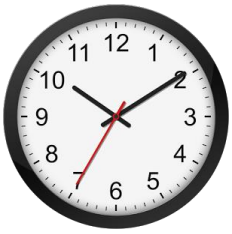
Certains benchmarks de D-Wave et Google réalisés en 2015 et montrant la supériorité de la solution quantique (dite adiabatique ou à recuit quantique) ont été ensuite contredits par la création d'algorithmes optimisés pour des supercalculateurs sous certaines conditions. Cette suprématie quantique naviguera donc dans un premier temps dans des sables mouvants.

avantage quantique… au cas par cas



problème complexe
insoluble avec des ordinateurs traditionnels

et / ou



plus rapide
qu'avec des ordinateurs traditionnels

et / ou

coût et énergie
avantageux en résolution quantique

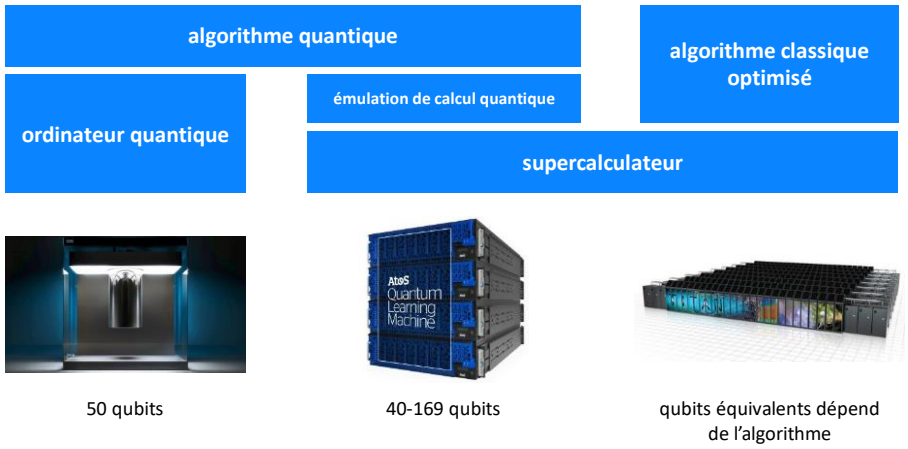
[158] Voir First proof of quantum computer advantage, octobre 2018 et Quantum advantage with shallow circuits, avril 2017 (23 pages).

Elle interviendra certainement d'ici quelques années pour quelques algorithmes qui ne peuvent avoir d'équivalents optimisés pour les supercalculateurs. On apprenait le 20 septembre 2019 que Google avait atteint cette suprématie, avec un algorithme de *random numbers sampling* et sur 53 qubits. L'algorithme ne sert pas à grand-chose et exploite la superposition sur l'ensemble des 53 qubits supraconducteurs utilisés. C'est une annonce symbolique intéressante mais à décoder !

Ariel Bleicher rappelle à juste titre que les supercalculateurs et ceux qui les exploitent n'ont pas dit leur dernier mot et cherchent aussi à améliorer leurs propres algorithmes[159]. A long terme, le quantique supplantera certainement les supercalculateurs pour un grand nombre d'algorithmes.

La comparaison entre ordinateurs quantiques et supercalculateurs peut se faire de deux principales manières. La première consiste à exécuter sur ces derniers un algorithme classique équivalent fonctionnellement à l'algorithme quantique évalué (à droite dans le schéma *ci-dessous*). La seconde exploite des émulateurs quantiques à architecture non quantique, le plus souvent, des supercalculateurs qui émulent l'exécution d'un algorithme quantique (au centre dans le schéma *ci-dessous*).

La dynamique de progrès de ces deux comparables face au quantique est différente. Dans le premier cas, c'est la combinaison de l'ingénuité humaine à créer de nouveaux algorithmes classiques et à l'évolution de la performance des supercalculateurs.



Dans le second cas, il s'agit de l'amélioration de cette performance matérielle mais aussi de méta-algorithmes d'exécution d'algorithmes quantiques sur des machines traditionnelles, et généralement réparties sur plusieurs processeurs et serveurs.

Les principales limitations des supercalculateurs pour simuler des algorithmes quantiques relèvent plus de leur mémoire vive que de leur capacité de traitement. Il faudrait 16 Po de mémoire pour simuler complètement 50 qubits en double-flottant. Si on passe à 96 qubits, la mémoire nécessaire pour simuler l'ensemble sur supercalculateur est multipliée par 2^{46*2}. La loi de Moore de la mémoire ne peut donc pas suivre le rythme d'une augmentation linéaire du nombre de qubits alignés dans un ordinateur quantique.

[159] Voir Quantum Algorithms Struggle Against Old Foe: Clever Computers d'Ariel Bleicher, février 2018. Cela fait écho aux découvertes d'algorithmes pour ordinateurs classiques aussi performants que ceux qui sont conçus pour ordinateurs quantiques, comme celui d'Ewin Tang dans la recommandation, déjà évoqué page 61.

Malgré tout, le nombre de qubits simulables sur des supercalculateurs est aussi en augmentation constante, avec de nombreux diables dans les détails. Les chinois sont les plus actifs dans cette course à la simulation, notamment chez Alibaba et Huawei avec plusieurs records établis en 2018.

Il existerait trois principales méthodes de simulation d'un circuit de N qubits et d'un certain niveau de profondeur d'enchaînements de portes quantiques[160] :

- La première méthode consiste à gérer en mémoire le vecteur d'état complet du registre quantique en mémoire. Avec N qubits, c'est le produit tensoriel des vecteurs d'état de chaque qubits qui comprennent deux nombres complexes alpha et beta. Cela donne un vecteur de 2^N nombres complexes, soient 2^{N+1} nombres flottants. L'action de portes quantique sur ce grand vecteur consiste à lui appliquer les matrices de transformation de portes quantiques à une, deux ou trois qubits qui font respectivement 2x2, 4x4 ou 8x8 nombres complexes. Cette méthode est mise en œuvre sur des supercalculateurs dotés d'énormes capacités de mémoire, de l'ordre de plusieurs Po. La méthode est pour l'instant limitée à une cinquantaine de qubits. On peut l'optimiser dans la mesure où ces vecteurs sont généralement remplis d'un grand nombre de zéros. A noter qu'après application de portes quantiques impliquant de l'intrication, le vecteur d'état ne sera plus factorisable en état de qubits individuels.
- La seconde méthode consiste à mesurer les amplitudes des 2^N combinaisons de 0 et de 1 de chaque qubit. Cela donne donc 2^N nombres flottants à évaluer pour chaque rang de portes quantiques, soient, si je comprends bien, deux fois moins d'informations qu'avec la première méthode. La méthode est plus facile à distribuer sur plusieurs serveurs[161]. Alibaba utilisait ainsi un cluster de 10 000 serveurs à 96 CPUs.
- La troisième consiste à gérer la matrice de transformation des qubits contenant 2^{2N+2} nombres flottants. Pourquoi ? Parce qu'elle a comme côté le vecteur d'état du registre de qubits de 2^{N+1} nombres flottants. C'est la méthode la plus consommatrice de mémoire qui est peu utilisée pour les nombres élevés de qubits.

Il y a tout d'abord le cas d'**Origin Quantum**, une startup chinoise multirôles (matériel, logiciel) en partenariat avec l'équipe de Guang-Can Guo de l'**Université des Sciences et Technologies de Chine** qui ont simulé 64 qubits avec un algorithme de 22 couches (layers, depth, nombre de séquences de portes quantiques enchaînées) sur un cluster de 128 nœuds[162]. Ils utilisent une méthode permettant de transformer des combinaisons de portes CZ (porte de Pauli Z conditionnelle) et de portes unitaires en sous-circuits plus simples qui n'ont pas besoin d'être intriqués. Ils pensaient aussi pouvoir simuler 72 qubits sur une profondeur de 23 couches de portes quantiques sur un supercalculateur tournant pendant 16 heures.

---

[160] Voir Classical Simulation of Intermediate-Size Quantum Circuits, Alibaba, 2018 (12 pages).

[161] Les méthodes de partitionnement de la simulation quantique sont bien décrites dans Distributed Memory Techniques for Classical Simulation of Quantum Circuits, Ryan LaRose de l'Université du Michgan, juin 2018 (11 pages).

[162] Voir Researchers successfully simulate a 64-qubit circuit, Science China Press, juin 2018.

Ces travaux montrent que deux paramètres clés conditionnent les capacités de simulation : non seulement le nombre de qubits mais également le nombre de séquences de portes quantiques à enchaîner. Plus on augmente le nombre de qubits, moins on peut simuler de séquences de portes quantiques. Mais cela reste utile pour quelques algorithmes quantiques tels que les QFT (transformées de Fourier quantiques).

Second record, celui d'**Alibaba** sur 81 qubits et quarante séquences de portes quantiques[163]. Leur simulation Taizhang exploite une méthode créée par Igor Markov et Shi Yaoyun en 2005[164] qui permet de ventiler un algorithme quantique de manière distribuée sur une ferme de milliers de serveurs. L'Alibaba Quantum Laboratory est géré par ce même Shi Yaoyun, professeur à l'Université du Michigan. Leurs simulations portaient notamment sur des architectures de 100 qubits sur 35 couches (10x10x35), 121 qubits sur 31 couches (11x11x31) et 144 qubits sur 27 couches (12x12x27). Les architectures retenues sont celles de matrices de qubits, d'où les nombres carrés de qubits.

Reference	General Technique	Qubits	Depth	# of Amplitudes
Intel [6]	Full amplitude-vector update	42	High	All
ETH [5]	Optimized full amplitude-vector update	5×9	25	All
IBM [7]	Tensor-slicing with minimized communication	7×7 7×8	27 23	All 2^{37} out of 2^{56}
Google [8]	Preprocessing using undirected graphical model	7×8	30	1
USTC [9]	Qubit partition with partial vector update	8×9	22	1
Sunway [10]	Dynamic programming qubit partition	7×7 7×7	39 55	All 1
Alibaba	Undirected graphical model with parallelization	9×9	40	1

TABLE I: A very broad overview of existing simulators. The final column reports the number of amplitudes that are computed by that simulator.

Troisième record en 2018, celui de **Huawei** et de son service « HiQ Cloud » capable de simuler de 42 à 169 qubits[165]. La méthode est voisine de celle d'Alibaba. Les 42 qubits sont simulés en « pleine amplitude ». 81 qubits étaient simulés avec « une seule amplitude » et 169 qubits sur une seule amplitude et avec un petit nombre de portes quantiques.

D'autres records ont été battus aux USA comme celui de **Google** avec la NASA, l'Université d'Illinois et le laboratoire d'Oak Ridge avec 49 à 121 qubits sur le supercalculateur Summit de ce dernier, comprenant 9216 CPUs PowerPC et 26 648 Nvidia V100[166].

Ce même laboratoire d'Oak Ridge est à l'origine de **XAAC** (eXtreme-scale ACCelerator programming framework) un framework pour Eclipse qui permet de gérer des des calculs hybrides associant ordinateurs quantiques et supercalculateurs comme le

[163] Voir Alibaba Says Its New "Tai Zhang" Is the World's Most Powerful Quantum Circuit Simulator, mai 2018 et Alibaba announced that it has developed the world's strongest quantum circuit simulator "Taizhang", mai 2018.

[164] Voir Simulating quantum computation by contracting tensor networks, Igor Markov et Shi Yaoyun, 2005 (21 pages).

[165] Voir Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform, octobre 2018.

[166] Voir Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation, mai 2019 (11 pages). Ce Summit a dû consommer une bonne part de la production de Nvidia V100 ! Voici également la liste des records de qubits et de simulation de qubits dans https://quantumcomputingreport.com/scorecards/qubit-count/.

Titan équipé de GPU Nvidia installé à Oak Ridge[167]. Il est capable de transformer du code quantique pour ordinateurs à portes quantiques ou à modèles adiabatiques en code exécutable sur toute architecture quantique.

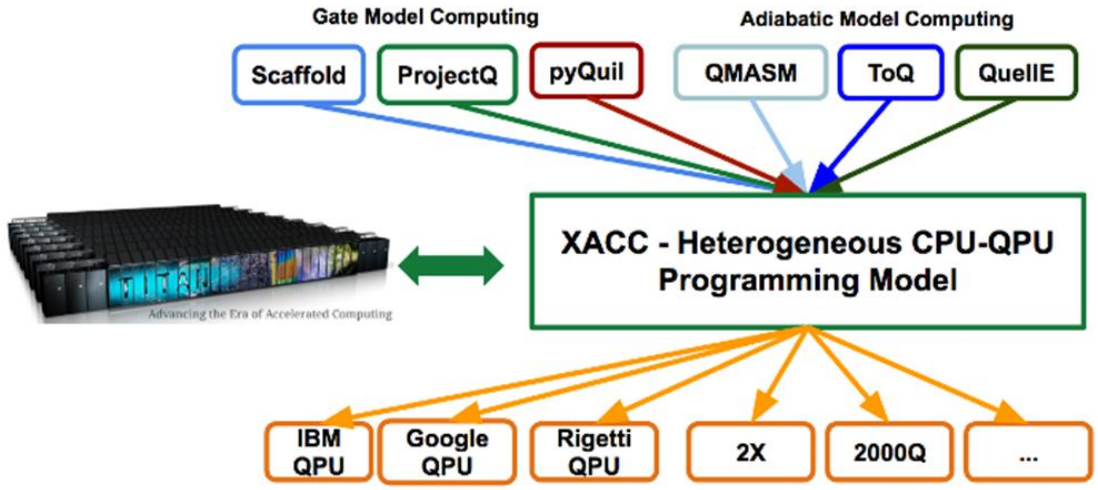
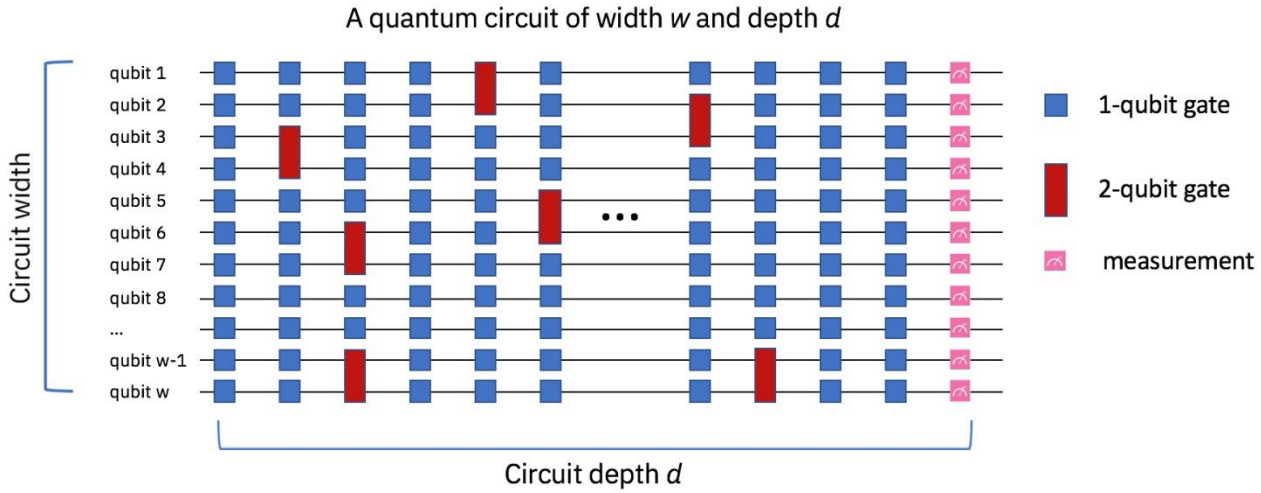


Figure 1: The XACC CPU-QPU programming model enables quantum acceleration in classical HPC applications in a quantum language and hardware agnostic manner.

En 2018, des chercheurs d'IBM démontraient en tout cas que la suprématie quantique était assurée à terme, même avec des ordinateurs quantiques pouvant enchaîner un nombre fini et contraint de portes quantiques[168].



Il faudra en tout cas se méfier des annonces des IBM et autres Google lorsqu'ils prétendront avoir atteint cette suprématie quantique, ou, tout du moins, de la manière dont ces annonces seront décrites dans les médias. Et la découverte inopinée de l'atteinte de la suprématie quantique par Google en septembre 2019 avec 53 qubits et un algorithme optimisé pour ne doit pas échapper à notre vigilance[169] !

---

[167] Le schéma vient de Eclipse Science and Open Source Software for Quantum Computing, 2017. Voir l'article qui décrit XAAC : A Language and Hardware Independent Approach to Quantum-Classical Computing, juillet 2018 (15 pages).

[168] Voir Scientists Prove a Quantum Computing Advantage over Classical, par Bob Sutor, octobre 2018, Quantum advantage with shallow circuits, Sergey Bravyi, David Gosset, Robert Koenig, 2017 (23 pages) et la video Quantum advantage with shallow circuits, IBM Research, décembre 2017 (44 minutes).

[169] Voir Interpréter la suprématie quantique de Google par Olivier Ezratty, septembre 2019.

Le jour même où je publiais l'édition 2019 de l'ebook Comprendre l'informatique quantique (504 pages), un rapport de recherche était éventé temporairement sur le site de la NASA selon lequel...

Lorsque Google communiquait en mars 2018 sur la création d'un ordinateur quantique de 72 qubits, donc bien au-delà de 50 qubits, il se gardait bien de préciser le temps de cohérence de l'ensemble ainsi que du niveau du bruit généré, sans compter le fait qu'il n'avait pas encore été benchmarké avec un algorithme donné. Sans ces informations, une annonce d'ordinateur quantique reste du vent !

Il faut donc attendre d'avoir des éléments d'informations complets pour juger, comme l'indiquent fort bien Cristian et Elena Calude de l'Université d'Auckland en Nouvelle Zélande[170]. Ils arguent aussi du fait que l'on compare une limite haute de performance, celle d'un ordinateur quantique précis, à une limite basse qui est la meilleure performance dans la résolution du même problème dans un supercalculateur. Or, il est plus facile de démontrer qu'un truc existe que son inexistence.

Une suprématie quantique est donc un comparable entre l'existence d'une performance quantique et la supposition de la non-existence d'une performance équivalente dans le non-quantique. Les auteurs rappellent aussi un critère qui manque parfois à l'analyse : il vaudrait mieux que l'algorithme testé serve à quelque chose ! Ce qui n'est pas toujours évident avec certains algorithmes quantiques, comme nous le verrons plus loin.

Usages des applications quantiques

Avant de rentrer dans le lard des algorithmes quantiques, faisons un détour de leur utilité pratique connue à ce jour.

Je les ai organisés ci-dessous en trois niveaux verticaux : les fonctions de base, les algorithmes puis les applications concrètes.

Tout ceci relève encore largement de la prospective car nombre de ces solutions demanderont des puissances en termes de nombre et de qualité de qubits qui ne seront pas disponibles avant plusieurs années voire décennies.

Dans un ordre vaguement chronologique, nous aurons tout d'abord des applications d'algorithmes de recherche et d'optimisation basés sur les équations linéaires en général sachant que tous les algorithmes quantiques reposent sur des équations linéaires. On peut y caser les solutions de résolution de problèmes complexes, comme la détermination du parcours optimal d'un commercial, un sujet bien connu. Sa variante est la solution d'optimisation du trafic individuel de nombreux véhicules dans une ville en tenant compte de l'ensemble des trajets planifiés pour chacun d'entre eux.

Cette catégorie de solutions comprend aussi l'accélération de l'entraînement des réseaux de neurones du deep learning. L'avantage par rapport aux techniques existantes

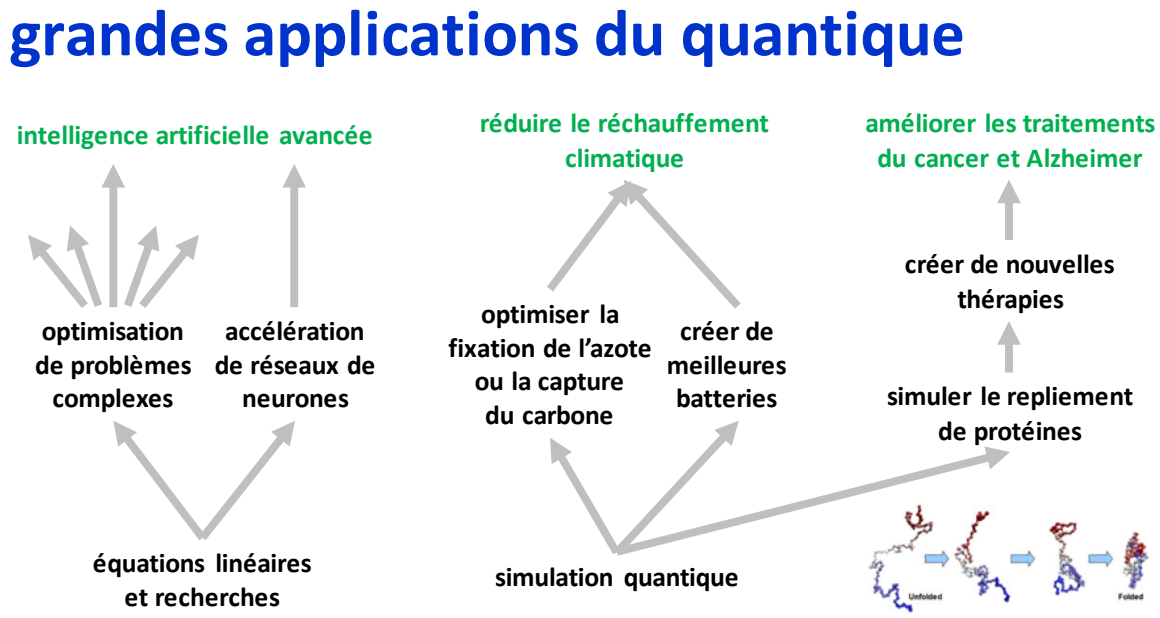
[170] Dans The road to quantum computing suppremacy, publié fin 2017.

s'appuyant sur des processeurs neuromorphiques n'est pas encore évidente et démontrée.

Qui plus est, la faisabilité de ces réseaux de neurones est établie sur architectures traditionnelles, à base de GPUs comme ceux de Nvidia ou de TPU (Tensor Processing Units) comme ceux de Google, sans compter les processeurs à base de memristors qui sont encore au stade du laboratoire.

En second lieu, dans le vaste champ de la simulation quantique, nous aurons d'abord des applications dans la chimie et la physique des matériaux pour simuler les interactions entre atomes dans les molécules et les structures cristallines, qui dépendent elles-mêmes des lois de la mécanique quantique. Cela servira si tout va bien à inventer de nouvelles solutions comme des batteries plus efficaces, chargeables plus rapidement et avec une plus grande densité énergétique, des procédés chimiques de captation du carbone ou de fixation de l'azote, ainsi que la création de matériaux supraconducteurs à température ambiante. Ce sont des hypothèses non encore validées à savoir que les algorithmes quantiques complétés d'ordinateurs quantiques bien dimensionnés avec des centaines de qubits logiques seront à même de permettre aux chercheurs d'avancer dans ces domaines-là.

En dernier lieu et avec des quantités de qubits bien plus importantes, donc à plus lointaine échéance, la simulation quantique pourra éventuellement passer à la simulation de molécules biologiques. Cela commencera avec celle de peptides, puis de polypeptides, et enfin, de protéines et d'enzymes. Les molécules biologiques ont la particularité d'être très complexes, avec des structures pouvant atteindre des dizaines de milliers d'atomes.



Le top du top serait la capacité à simuler l'assemblage puis le fonctionnement d'un ribosome, qui fait plus de 100 000 atomes. C'est la structure moléculaire la plus magique du vivant, celle qui assemble les acides aminés pour construire les protéines à partir du code de l'ARN messager issu de la transposition de l'ADN des gênes. Suivrait alors la simulation du fonctionnement d'une cellule entière.

Mais là, on est à la frontière de la science-fiction, même en étant très optimiste sur l'informatique quantique ! Ce d'autant plus qu'à ce niveau de complexité, le chaos règne !

Classes d'algorithmes quantiques

Comme nous l'avons vu dans la partie précédente qui décrit la structure d'un ordinateur quantique, un algorithme quantique va intégrer à la fois la partie initialisation des données puis celle des calculs et enfin de la mesure du résultat. Elle s'appliquera à un registre de n qubits qui sont physiquement initialisés à zéro, puis modifiés par des portes quantiques.

Le résultat correspond à la mesure de l'état de ces mêmes qubits à la fin de l'exécution de l'algorithme. En général, il faudra effectuer le calcul dans son intégralité et mesurer à chaque fois l'état des qubits en sortie, puis faire une moyenne des valeurs obtenues. La question étant de savoir : combien de fois doit-on répéter le calcul ? Cela dépend de sa nature et de la vitesse à laquelle il fait converger vers 0 et 1 l'état des qubits.

L'algorithme doit être compatible avec les caractéristiques de l'ordinateur quantique. Les principales sont le temps de cohérence et la durée d'exécution des portes quantiques.

Le nombre de portes quantiques à exécuter devra permettre d'exécuter l'algorithme dans un temps inférieur au temps de cohérence au bout duquel les qubits perdront leur état de superposition. Cette vérification est généralement réalisée par les compilateurs de code quantique.

Elle devra tenir compte des codes de correction d'erreurs qui sont souvent mis en œuvre sous la forme de sous algorithmes préfabriqués intégrés dans l'algorithme "métier" créé par le développeur.

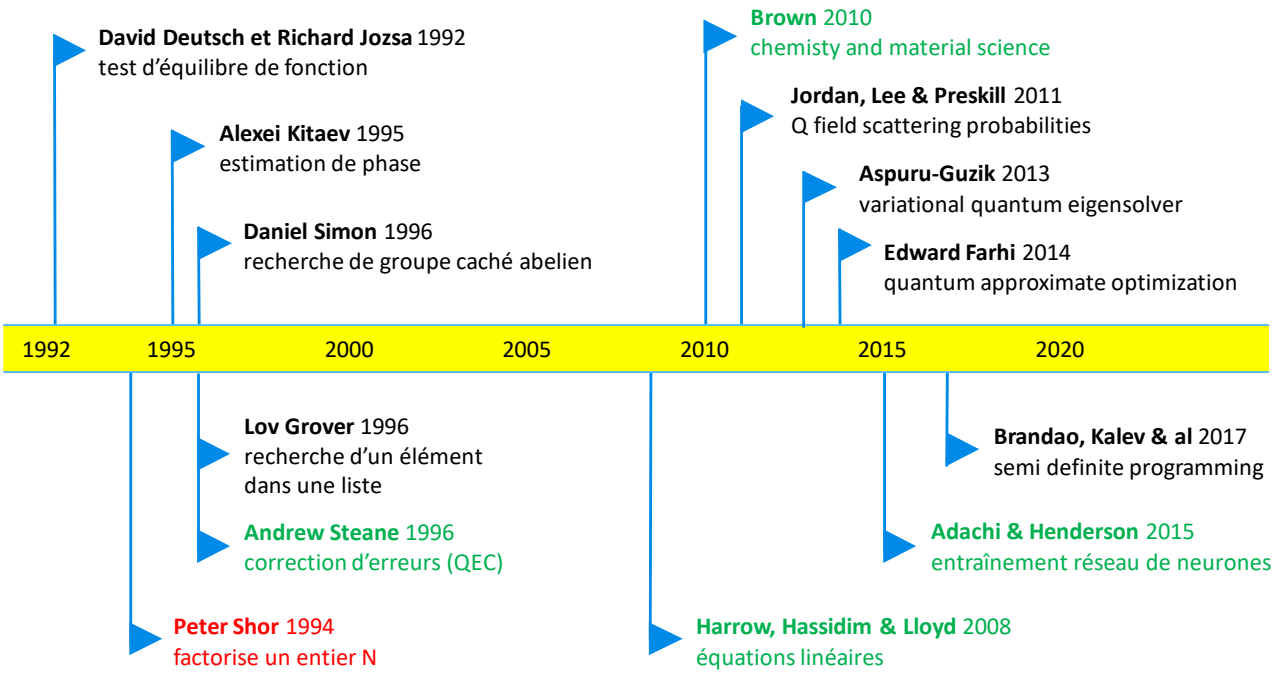
Il en va de même des portes quantiques utilisées dans les outils de développement. Certaines portes quantiques, notamment s'appliquant sur deux ou trois qubits, sont utilisées par les développeurs mais seront converties par le compilateur en un jeu de portes quantiques universelles supportées par l'ordinateur quantique. Cela va aussi multiplier le nombre de portes quantiques par rapport à l'algorithme initial. Dans la pratique, l'ordinateur va donc exécuter un nombre de portes quantiques bien plus grand que celles de l'algorithme conçu par le développeur.

L'une des considérations importantes de la création d'algorithmes quantiques est de s'assurer qu'ils sont plus efficaces que leurs équivalents optimisés pour des ordinateurs ou supercalculateurs traditionnels. Des théories permettent de vérifier cela pour évaluer la montée en puissance exponentielle, polynomiale, logarithmique ou linéaire du temps de calcul en fonction de la taille du problème à réaliser, ou une combinaison des quatre. Mais rien ne remplace l'expérience !

Les algorithmes quantiques sont des applications pratiques de l'algèbre linéaire, cette branche des mathématiques qui gère des espaces vectoriels et des transformations linéaires à base de matrices. Elles sont appliquées dans des espaces à deux dimen-

sions, les vecteurs qui définissent les états de qubits. Leur manipulation s'appuie sur des calculs matriciels qui permettent de modifier l'état des qubits sans en lire le contenu. Leur lecture n'intervient qu'à la fin des calculs.

Cela rend difficile la programmation conditionnelle, du genre : faire tel calcul si tel résultat intermédiaire a telle valeur ou vérifie telle condition. Mais les portes quantiques conditionnelles (CNOT & co) permettent d'émuler ce genre de comportement dans un algorithme quantique.



A ce jour, quatre principales catégories d'algorithmes quantiques sont disponibles et que nous détaillerons plus loin :

- Les **algorithmes de recherches** basés sur ceux de Deutsch-Jozsa, Simon et de Grover.
- Les **algorithmes basés sur les transformées de Fourier quantiques** (QFT), comme celui de Shor qui sert à la factorisation de nombres entiers qui a déclenché un phénomène de pompiers-pyromanes, les pyromanes étant ceux qui veulent créer des ordinateurs quantiques capables de casser les clés de sécurité publiques de type RSA et les pompiers étant ceux qui cherchent à protéger les communications numérique avec des algorithmes résistant à la factorisation rapide de nombres entiers.
- Les **algorithmes qui cherchent un point d'équilibre d'un système complexe** comme dans l'entraînement de réseaux de neurones, la recherche de chemin optimal dans des réseaux ou l'optimisation de processus.
- Les **algorithmes de simulation de mécanismes quantiques** qui servent notamment à simuler les interactions entre atomes dans des structures moléculaires diverses, inorganiques et organiques.

- Les **autres algorithmes** divers. Certains visent à simplement reproduire des algorithmes classiques avec des qubits comme cet algorithme de multiplications quantiques[171].

La roadmap *ci-dessus* illustre le rythme de création de ces nouveaux algorithmes sur les trois dernières décennies. Et l'histoire ne fait que commencer parce que la dynamique d'innovation exponentielle du thème est pour l'instant limitée par l'imagination humaine et surtout, par les capacités d'expérimentation.

Dans la pratique cependant, de nombreux algorihmes sont dérivés des mêmes souches, comme la QFT (transformée de Fourier quantique)[172].

Les algorithmes quantiques sont classifiables et explicables à haut niveau, mais leur compréhension détaillée n'est pas une partie de plaisir. Il faut soit avoir une capacité de vision conceptuelle assez développée, et en particulier une maitrise des mathématiques poussée[173].

Algorithm	Description	Reference
Algorithms Based on QFT		
Shor's; $O\left(n^2 (\log N)^3\right)$	Integer factorization (given integer N find its prime numbers); discrete logarithms, hidden subgroup problem, and order finding	Peter W. Shor, "Algorithms for Quantum Computation Discrete Log and Factoring," AT&T Bell Labs, shor@research.att.com
Simon's; *exponential*	Exponential quantum-classical separation. Searches for patterns in functions	Simon, D.R. (1995), *"On the power of quantum computation"*, Foundations of Computer Science, 1996 Proceedings., 35th Annual Symposium on: 116–123, retrieved 2011-06-06
Deutsch's, Deutsch's – Jozsa, an extension Deutsch's algorithm	Depicts quantum parallelism and superposition. "Black Box" inside. Can evaluate the input function, but cannot see if the function is balanced or constant	David Deutsch (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". Proceedings of the Royal Society of London A. 400: 97 David Deutsch and Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". Proceedings of the Royal Society of London A. 439: 553
Bernstein/Vazirani; *polynomial*	Superpolynomial quantum-classical separation	Ethan Bernstein and Umesh Vazirani. *Quantum complexity theory.* In Proc. 25th STOC, pages 11–20, 1993
Kitaev	Abelian hidden subgroup problem	A. Yu. Kitaev. *Quantum measurements and the Abelian stabilizer problem,* arXiv:quant-ph/9511026, 1995
van Dam/Hallgren	Quadratic character problems	Wim van Dam, Sean Hallgren, *Efficient Quantum Algorithms for Shifted Quadratic Character Problems.* CoRR quant-ph/0011067 (2000)
Watrous	Algorithms for solvable groups	John Watrous, Quantum algorithms for solvable groups, arXiv:quant-ph/0011023, (2001)
Hallgren	Pell's equation	Sean Hallgren. *Polynomial-time quantum algorithms for pell's equation and the principal ideal problem,* Proceedings of the thirty-fourth annual ACM symposium on the theory of computing, pages 653–658. ACM Press, 2002.
Algorithms Based on Amplitude Amplification		
Grover's; $O\left(\sqrt{N}\right)$	Search algorithm from an unordered list (database) for a marked element, and statistical analysis	Lov Grover, *A fast quantum mechanical algorithm for database search,* In Proceedings of 28th ACM Symposium on Theory of Computing, pages 212–219, 1996
Traveling Salesman Problem; $O\left(\sqrt{N}\right)$	Special case of Grover's algorithm	https://en.wikipedia.org/wiki/Travelling_salesman_problem

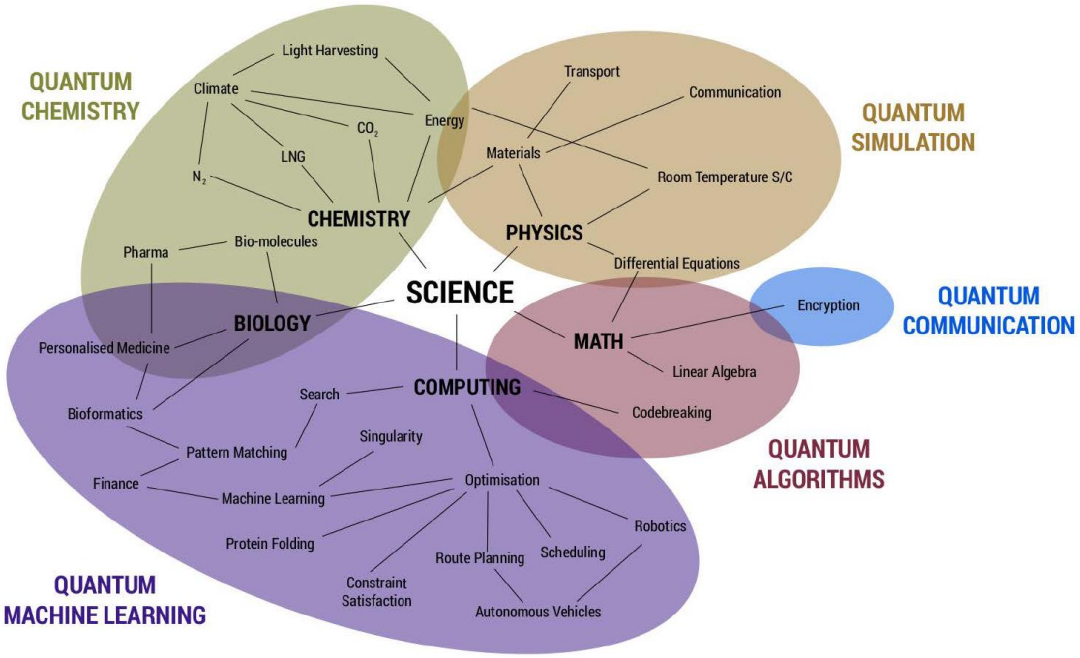
[171] Voir A New Approach to Multiplication Opens the Door to Better Quantum Computers, par Kevin Harnett, 2019.

[172] Voir Quantum computing (QC) Overview par Sunil Dixit de Northrop Grumman, septembre 2018 (94 slides) d'où est extrait le tableau d'algorithmes de cette page.

[173] Voici quelques sources d'information pour creuser la question : Quantum Computing Applications d'Ashley Montanaro de l'Université de Bristol, 2013 (69 slides), Introduction à l'information quantique de Yves Leroyer et Géraud Sénizergues de l'ENSEIRB-MATMECA, 2016-2017 (110 pages), un cours récent intéressant sur la partie algorithmique, An Introduction to Quantum Computing de Phillip Kaye, Raymond Laflamme et Michele Mosca, Oxford, 2017 (284 pages), Lecture Notes on Quantum Algorithms de Andrew M. Childs, University of Maryland, 2017 (174 pages), Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages) et A Course in Quantum Computing for the Community College de Michael Locef, 2016 (742 pages) qui pose de manière très détaillée les fondements mathématiques de l'algèbre linéaire avec les nombres complexes, les formules d'Euler, les espaces vectoriels et de Hilbert, le calcul matriciel, les tenseurs, eigenvectors et eigenvalues, et les algorithmes quantiques. Il nécessite plusieurs semaines pour être parcouru et compris. C'est un cours pour la seconde et troisième année du Foothill Community College de Los Altos Hills en Californie (donc Bac+1/+2 en équivalent français). En complément, voici quelques vidéos sur ce même sujet : Quantum Algorithms d'Andrew Childs en 2011 (2h31), Language, Compiler, and Optimization Issues in Quantum Computing de Margaret Martonosi, 2015 (39 minutes et slides) et What Will We Do With Quantum Computing? de Aram Harrow, MIT, 2018 (32 minutes).

Dans ce qui suit, je vais donc vous décrire quelques algorithmes mais en reconnaissant que je n'ai pas véritablement tout compris de leur fonctionnement dans les qubits et opérations de portes quantiques appliquées dessus. Le quantique est ainsi fait en général : on n'a jamais tout compris ! Décrire cela est donc un véritable exercice d'humilité intellectuelle.

Voir aussi cette cartographie d'applications du calcul quantique qui est cependant un peu fantaisiste, reliant le machine learning à « singularity », ce qui ne veut pas dire grand-chose (*ci-dessous*)[174].



Algorithmes de recherche

L'un des premiers algorithmes quantiques inventés est celui de David Deutsch, avec sa déclinaison dite de **Deutsch-Jozsa**, coinventée avec Richard Jozsa et qui date de 1992. Cet algorithme permet de caractériser la fonction d'une "boite noire" que l'on appelle un "oracle" dont on sait à l'avance qu'elle va retourner pour toutes ses entrées, soit toujours la même valeur, 0 ou 1, soit les valeurs 0 et 1 à parts égales. L'algorithme permet donc de savoir si la fonction f() est équilibrée ou pas. Elle est appliquée à un ensemble de qubits n.

Les qubits en entrée sont tous initialisés à 0 sauf un qui l'est à 1 puis ils sont chacun mis en superposition entre 0 et 1 via des portes de Hadamard. Les qubits ont donc simultanément toutes les valeurs possible avec 2 puissance n+1 combinaisons de valeurs.

Il est facile de comprendre pourquoi cet algorithme quantique est bien plus efficace que sa version traditionnelle : en calcul traditionnel, il faudrait scanner plus de la moitié des valeurs possibles en entrée de manière séquentielle alors que dans la version quantique, elles sont toutes analysées en même temps.

[174] Source : Silicon Photonic Quantum Computing de Syrus Ziai, PsiQuantum, 2018 (72 slides).

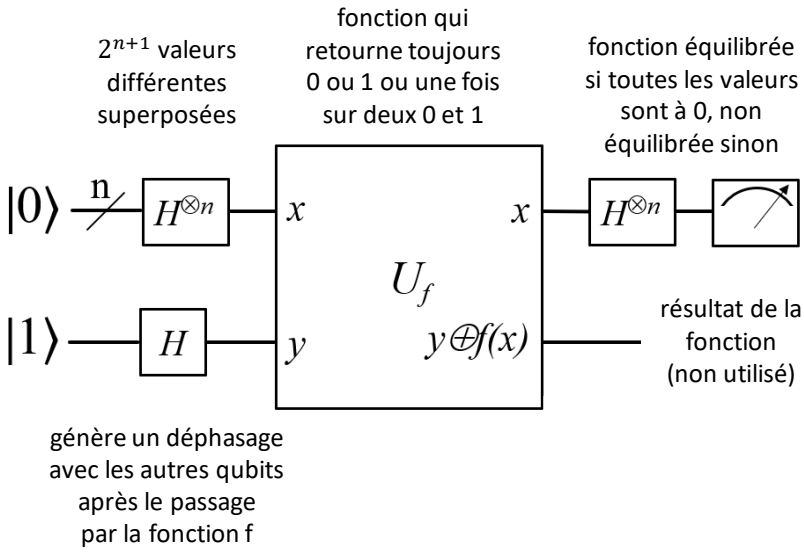
Le résultat est donc obtenu avec quelques séries de portes quantiques, presque instantanément, et il est parfaitement déterministe.

Ces qubits en superposition traversent la boîte noire qui contient un ensemble de portes avec une fonction à évaluer. On mesure alors en sortie le résultat pour voir si la fonction est équilibrée ou pas grâce à d'autres portes de Hadamard.

Deutsch-Jozsa

vérifie qu'une fonction f est équilibrée ou non

$$O(2^{N-1} - 1) \Rightarrow O(4)$$



L'initialisation du dernier qubit à 1 sert à générer une interférence avec les autres qubits qui va impacter les valeurs sortant des portes H après le passage par l'oracle. La fonction f est constante si la totalité des mesures donne 0 et déséquilibrée si au moins d'un des qubits en sortie retourne 1[175]. Les explications données sont toujours incomplètes pour bien comprendre ces algorithmes. Elles n'indiquent pas bien où se retrouve le bit de sortie de la fonction de l'oracle qui est soit de 0 soit de 1.

L'intérêt pratique ? C'est un exemple d'algorithme ultra puissant qui n'a aucune utilité pratique connue à ce jour. On est bien avancés ! Qui plus est, il existe des algorithmes probabilistes classiques très efficaces qui effacent une bonne part du gain de puissance quantique de l'algorithme de Deutsch-Jozsa. C'est le cas en particulier de l'algorithme de recherche de Monte Carlo qui évalue la fonction d'oracle sur un nombre limité d'entrées choisies aléatoirement. La probabilité d'erreurs est dépendante du nombre d'évaluations et décroit très rapidement[176].

Alors, le quantique ne sert donc à rien ? Non, bien sûr. D'autres algorithmes moins performants mais bien plus utiles ont vu le jour depuis ce patient zéro de l'algorithmie quantique !

L'algorithme de **Simon** est une variante plus sophistiquée de celui de Deutsch-Jozsa. Il consiste à trouves les combinaisons de valeurs qui vérifient une condition imposée par la fonction "boite noire".

---

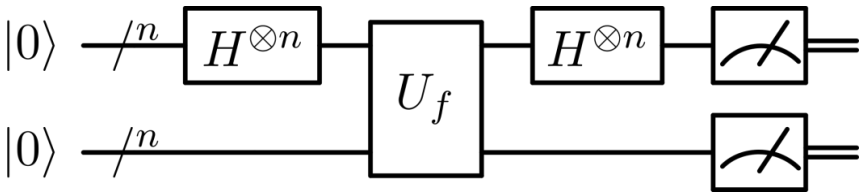
[175] Pour savoir comment cela fonctionne dans le détail, vous pouvez voir les formules mathématiques associées ainsi que la présentation Deutsch-Jozsa Algorithm d'Eisuke Abe, 2005 (29 slides). Mais ce n'est pas des plus évident !

[176] Voir à ce sujet le document Modèles de Calcul Quantique (30 pages).

Le gain de performance est très intéressant et cette fois-ci, les applications existent, notamment pour résoudre des problèmes de parcours dans des graphes. Le gain de performance est typique de ce que le quantique apporte : on passe d'un calcul classique qui est de temps exponentiel ($2^{N/2}$) à un temps linéaire en N.

Simon

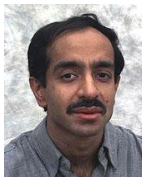
recherche de sous-ensemble dont les membres vérifient une condition imposée par une fonction f



$O(\sqrt{2^N}) \Rightarrow O(N)$

L'autre algorithme le plus connu de cette catégorie est celui de **Grover**, créé en 1996. Il permet de réaliser une recherche quantique rapide dans une base de données. Un peu comme l'algorithme de Deutsch-Jorza, il permet de scanner une liste d'éléments pour trouver ceux qui vérifient un critère.

Il utilise aussi la superposition d'états de qubits pour accélérer le traitement par rapport à une recherche séquentielle traditionnelle dans une base non triée et non indexée. L'amélioration de performance est significative par rapport à une base non triée, à ceci près que dans la vraie vie, on utilise généralement des bases indexées !



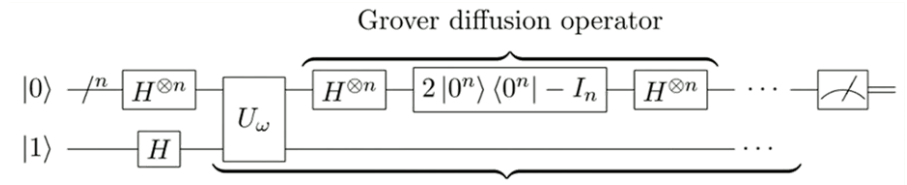
recherche un élément donné dans une base non indexée

$O(N) \Rightarrow O(\sqrt{N})$

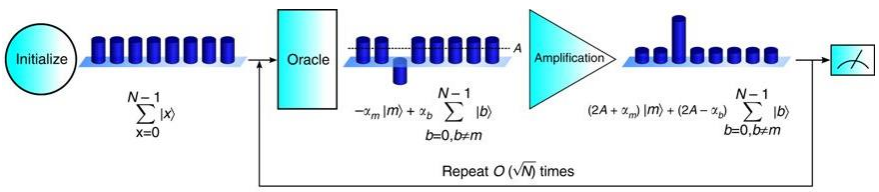
fonction qui indique si la valeur trouvée est la bonne

suite d'opérations qui va amplifier la bonne réponse et atténuer les autres réponses

mesure de la bonne réponse qui émerge



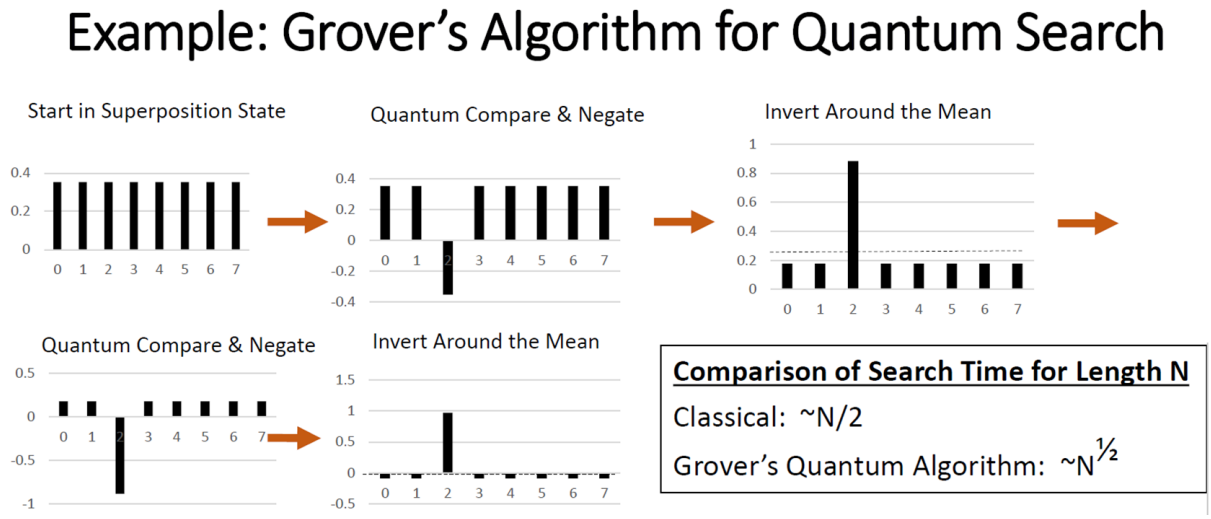
initialisation identique à celle de l'algorithme de Deutsch-Jozsa



L'algorithme de Grover utilise aussi une fonction "oracle" ou "boite noire" qui va indiquer si un ensemble de qubits en entrée vérifie un critère de recherche ou non, comme pour vérifier qu'un numéro de téléphone donné a été trouvé dans une liste de numéros de téléphone.

Dans un tel cas, la fonction compare le numéro de téléphone recherché et celui qui lui est soumis pour répondre 1 s'ils sont identiques et 0 sinon. La boite noire étant quantique, elle va évaluer cette fonction pour 2^N registres de qubits en même temps. Elle sortira donc un 1 une fois et des 0 autrement.

La question étant de savoir si un 1 est sorti une fois et à quelle entrée il correspond. Pour ce faire, là aussi avec des portes de Hadamard, l'algorithme va amplifier graduellement la combinaison de qubits du résultat à une valeur 1 et faire converger les autres combinaisons de qubits vers 0. Il sera alors possible de mesurer le résultat et on obtiendra la combinaison de qubits avec la valeur recherchée. C'est bien expliqué dans le schéma *ci-dessous*[177].



Le temps de calcul est proportionnel à la racine carrée de la taille de la base et l'espace de stockage nécessaire est proportionnel au logarithme de la taille de la base. Un algorithme classique a un temps de calcul proportionnel à la taille de la base. Passer d'un temps N à sqrt(N) est donc un gain intéressant, mais il ne transformera pas un problème de taille exponentielle en problème de taille polynomial (2 puissance N vers N puissance M).

Par contre, cet algorithme peut ensuite être exploité pour être intégré dans d'autres algorithmes comme ceux qui permettent de découvrir le chemin optimal dans un graphe ou le nombre minimal ou maximal d'une série de N nombres.

Notons cependant que l'algorithme de recherche de Grover nécessite l'emploi d'une mémoire quantique (QRAM) qui n'est pas encore au point[178] !

Ces différents algorithmes de recherche sont déclinés en diverses variantes et sont exploités en pièces détachées dans d'autres algorithmes quantiques.

[177] Source du schéma : Quantum Computing Explained for Classical Computing Engineers de Doug Finke, 2017 (55 slides). Le lien ne semble plus opérationnel en juillet 2019.

[178] C'est notamment documenté dans Quantum algorithms for linear algebra de Anupam Prakash, 2015 (92 slides).

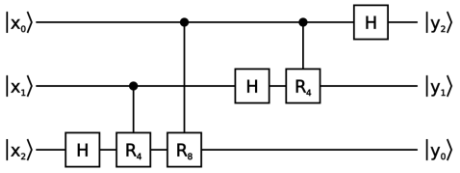
Transformées de Fourier quantiques

Les transformées de Fourier classiques permettent d'identifier les fréquences qui composent un signal. En théorie du signal, cela permet d'identifier les composantes de base d'un son en le décomposant en fréquences. En astrophysique, on détermine la composition atomique des étoiles par une décomposition du spectre lumineux, mais celle-ci est opérée par un prisme optique et pas par transformée de Fourier. Il en va de même pour les capteurs en proche infrarouge de type Scio qui déterminent la composition des aliments. Un prisme et le principe de la diffraction permettent donc de réaliser optiquement une transformée de Fourier.

algo : **transformée quantique de Fourier**

décompose une suite de qubits en fréquences

utilisé notamment dans l'algorithme de Shor



nbr	temps classique	temps quantique
5	3,5	0,5
48	81	2,8
128	270	4,4
512	1387	7,3
1024	3082	9,1

$$N * \log(N) \Rightarrow \log^2(N)$$

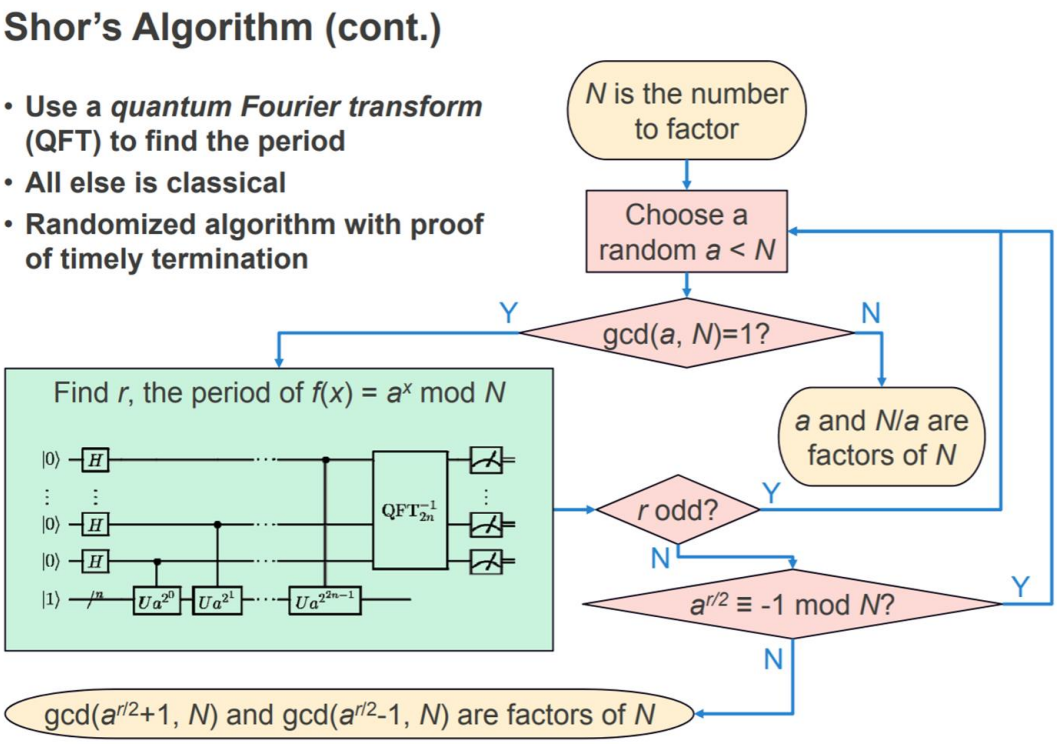
La transformée de Fourier quantique est utilisée dans divers autres algorithmes et en particulier dans celui de Shor qui sert à factoriser des nombres entiers. Elle n'est pas une transformée parfaite qui réalise une décomposition complète en fréquences d'un signal.

Elle sert à identifier la fréquence d'amplitude la plus forte d'un signal donné. Elle ne peut pas servir à du traitement fin du signal comme on le fait dans des DSP (Digital Signal Processors) traditionnels.

Le gain de vitesse généré ? Le temps de calcul passe de N*log(N) pour les meilleures transformées de Fourier simples à $\log^2(N)$ pour la QFT. On passe donc d'un ordre de grandeur linéaire à un ordre de grandeur logarithmique. C'est un gain appréciable mais pas très impressionnant. Mais comme il peut s'appliquer à des N qui sont eux-mêmes des puissances de 2, l'accélération est intéressante.

La factorisation de **Shor** permet de décomposer des entiers en nombres premiers bien plus rapidement qu'avec un ordinateur traditionnel. Elle utilise une QFT vue précédemment. Je vous passe les détails du fonctionnement de l'algorithme qui est décrit dans le schéma *ci-dessous*[179] et dans cette explication assez claire vue dans une vidéo de PBS.

[179] Source du schéma : Quantum Annealing de Scott Pakin, NSF/DOE Quantum Science Summer School juin 2017 (59 slides).



L'une des premières mises en œuvre de l'algorithme de Shor eu lieu en 2001 chez IBM avec un ordinateur quantique expérimental de 7 qubits, pour factoriser le nombre 15. Depuis, on est juste passé à un nombre à 5 chiffres, 56153[180], mais avec un autre algorithme de factorisation que celui de Shor. C'est en fait un algorithme d'optimisation qui fonctionnait sur ordinateur à recuit quantique du Canadien D-Wave ! Le record à ce jour atteint en 2016 serait la factorisation de 200 099 avec 897 qubits sur D-Wave mais avec un autre algorithme que celui de Peter Shor. Comme quoi il ne faut pas jeter le bébé D-Wave avec l'eau du bain du quantique universel !

Il faut surtout retenir que l'algorithme de Shor permet en théorie de casser les clés publiques de la cryptographie RSA qui est couramment utilisée dans la sécurité sur Internet. Les clés publiques fonctionnent en envoyant un très long nombre entier à un destinataire qui possède déjà son diviseur.

Il lui suffit de diviser le grand nombre envoyé par son diviseur pour récupérer l'autre diviseur et décoder le message ainsi chiffré.

Celui qui ne possède pas le diviseur ne peut pas exploiter la clé complète sauf à disposer d'une énorme puissance de calcul traditionnelle pour trouver ses diviseurs. Jusqu'à présent, seuls les supercalculateurs de la NSA pouvaient casser les clés de taille raisonnable comprises aux alentours de 256 à 400 bits. Mais à 512, 1024 bits et au-delà, la tâche est inaccessible en un temps raisonnable pour ces supercalculateurs.

[180] C'est documenté dans Quantum factorization of 56153 with only 4 qubits, 2014 (6 pages).

factorisation de Shor

factorise un nombre entier en nombres premiers

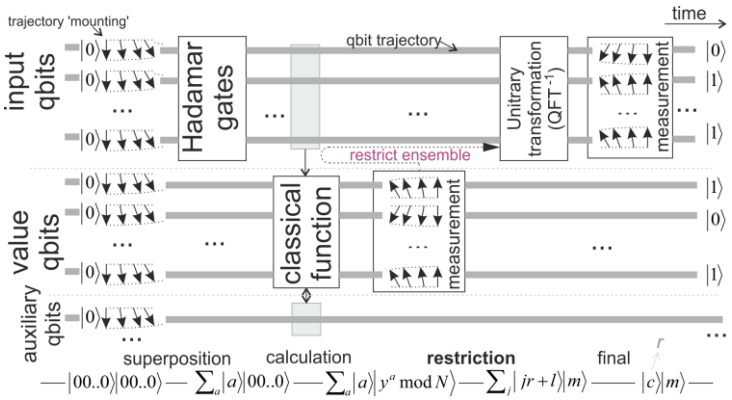
record : 56153 (241 x 233)

clé RSA 1024 bits :

166 millions de qubits / taux d'erreur de 0,1%

5,5 millions de qubits / 0,01% d'erreur et 6,6 semaines de calcul à 1 MHz !

$$O(\frac{\sqrt{N}}{2}) \Rightarrow O(\log(N)^3)$$



En théorie, cela deviendrait accessible à des ordinateurs quantiques. Mais pour casser une clé publique RSA de 1024 bits, il faudra encore patienter car cela nécessite de créer des ordinateurs quantiques avec un très grand nombre de qubits fonctionnant en cohérence. On en est très très loin. A noter que l'algorithme de Shor permet aussi de casser la cryptographie utilisant des courbes elliptiques, qui concurrencent la cryptographie RSA. Au passage, une part de la cryptographie utilisée dans le protocole du Bitcoin passerait également à la moulinette Shor, ce que nous verrons plus loin dans ce document.

En tout cas, l'algorithme de Shor terrorise les spécialistes de la sécurité depuis une bonne dizaine d'années. Cela explique l'intérêt pour l'exploitation de clés quantiques, censées être inviolables car leur interception peut être détectée par son récipiendaire légitime, ainsi que de la "post quantum cryptographie" consistant à faire évoluer les algorithmes et méthodes de cryptographie pour les rendre (théoriquement) inviolables par des ordinateurs quantiques utilisant l'algorithme de Shor. Les deux méthodes étant probablement combinables. Nous aurons l'occasion de traiter de cela plus tard.

Simulation de physique quantique

Les algorithmes de simulation quantique servent à reproduire dans un ordinateur les phénomènes de la mécanique quantique qui gouvernement le comportement de quantums dans des ordinateurs traditionnels ou quantiques.

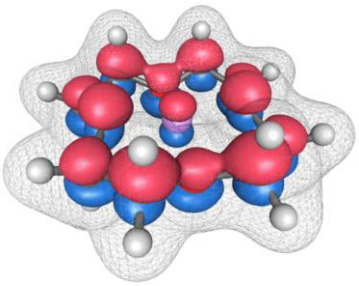
Ils sont exploitables en particulier pour simuler l'interaction entre les atomes dans des molécules pour la création de nouveaux matériaux.

Ils peuvent aussi simuler des phénomènes physiques liés au magnétisme ou à l'interaction entre les photons et la matière. Cela revient à résoudre des « problèmes à N-corps », soit calculer l'interaction entre plusieurs particules en fonction des lois physiques qui régissent leur interaction.

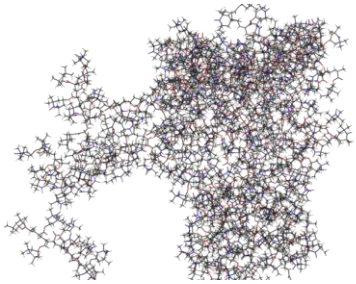
L'un des problèmes théoriques le plus souvent étudié en simulation quantique est celui de l'échantillonnage de bosons, dont font partie les photons. Il sert à modéliser le comportement des photons dans l'interférométrie.

La simulation quantique concerne aussi l'étude des matériaux supraconducteur (notamment à (relativement) haute température, -70°C), de la superfluidité à basse température et du magnétisme de certains matériaux qui dépend de la température ainsi qu'aux interactions entre le graphène et la lumière[181].

supraconductivité
interactions graphène/lumière
superfluidité



capture du carbone
photosynthèse
nouvelles batteries



repliement de protéines
interactions entre protéines
drug discovery

A plus haut niveau se situe la simulation des interactions atomiques dans des molécules de la biologie moléculaire, donc, de la chimie organique, allant progressivement des plus petites aux plus grandes des molécules : acide aminés, peptides, polypeptides, protéines et peut-être bien plus tard, de molécules ultra complexes comme les ribosomes qui fabriquent les protéines à partir des acides aminés. La constitution et le fonctionnement de ces grosses molécules font partie des plus grands mystères chimiques de la vie que l'Homme aimerait bien expliquer.

Tous ces algorithmes ambitionnent de simuler les processus atomiques ou moléculaires qui interviennent dans la nature ou à créer de tels mécanismes artificiels qui n'existent pas encore dans la nature.

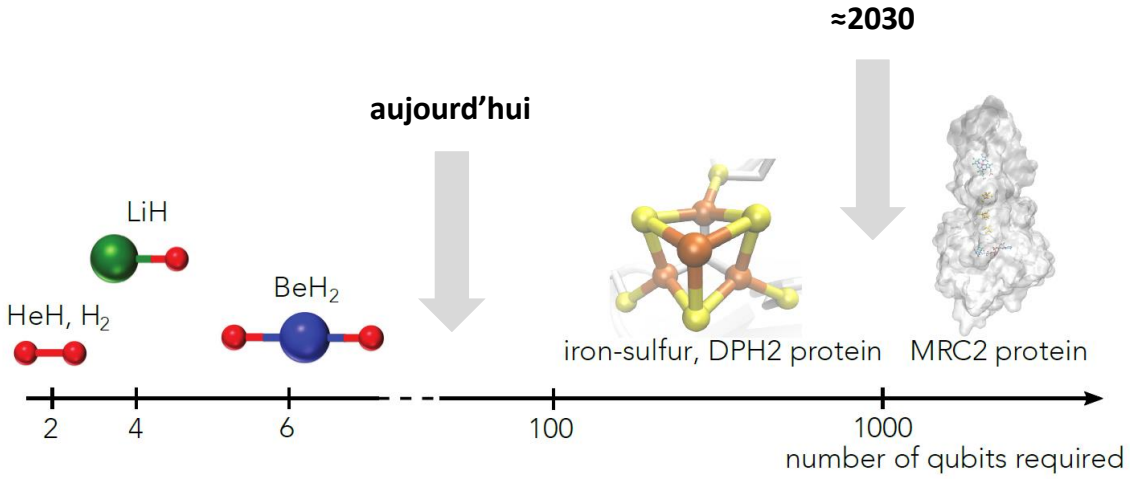
Cela peut aussi servir à faire des simulations "macro" comme celle du fonctionnement de trous noirs ou d'étoiles à neutrons en astronomie.

Ces algorithmes s'exécutent de manière la plus performante dans les ordinateurs quantiques universels à base de qubits. En attendant, on les exécute dans des ordinateurs à recuit quantique comme ceux de D-Wave voire dans des ordinateur quantiques dits analogiques, sans architectures à base de registres de qubits. Les plus courants et qui sont encore des objets de laboratoire sont les ordinateurs à base d'atomes froids comme le rubidium. Comme ces algorithmes visent souvent à déterminer un niveau d'énergie minimum d'un système complexe, le système adiabatique à recuit simulé de D-Wave est assez adapté à la tâche pour des problèmes relativement simples.

[181] Voir cette intéressante conférence de Jacqueline Bloch à l'Académie des Sciences qui en fait un excellent panorama : Simulateurs quantiques : résoudre des problèmes difficiles, mai 2018 (29 mn).

A partir de 50 électrons dans une molécule, les ordinateurs classiques ne peuvent plus simuler leur dynamique, ce qui correspond à quelques atomes à peine. Pour les molécules simples, les applications relèvent de la physique des matériaux : capture du carbone ou de l'azote, nouvelles batteries, découverte de mécanismes supraconducteurs utilisables ensuite dans les scanners médicaux, idéalement fonctionnant à température ambiante.

Ceci devrait être accessible avec des ordinateurs quantiques universels dotés de 50 à quelques centaines de qubits de qualité. Pour les simulations de biologie moléculaire, il faudra probablement attendre bien plus longtemps avant que cela soit possible et disposer d'ordinateur avec des milliers voir des centaines de milliers de qubits. Le schéma *ci-dessous* positionne de manière assez optimiste le nombre de qubits nécessaires pour simuler le fonctionnement une protéine des mitochondries, la MRC2[182].



source : Quantum optimization using variational algorithms on near-term quantum devices, 2017

Voici quelques exemples d'algorithmes de simulation quantique :

- Simulating a quantum field theory with a quantum computer de John Preskill, 2018 (22 pages) qui porte sur la simulation de champs quantiques qui régissent l'interaction de la matière à très bas niveau.
- Computation of Molecular Spectra on a Quantum Processor with an Error-Resilient Algorithm, 2018 (7 pages) sur la simulation du fonctionnement des atomes d'hydrogène dans des ordinateurs quantiques à qubits supraconducteurs.
- Des chercheurs réussissent le contrôle quantique d'une molécule, de Román Ikonicoff, mai 2017 qui pointe sur Preparation and coherent manipulation of pure quantum states of a single molecular ion, 2017 (38 pages), décrivant un algorithme de simulation hybride associant calcul classique et calcul quantique pour étudier le spectre de l'hydrogène. La partie quantique n'utilise que deux qubits supraconducteurs !

[182] Il est issu de Quantum optimization using variational algorithms on near-term quantum devices, issu de chercheurs d'IBM en 2017 (30 pages).

- Un exemple de simulation de molécule d'hydrure de béryllium (3 atomes, BeH2) avec seulement 6 qubits par IBM en 2017 dans Tiny Quantum Computer Simulates Complex Molecules par Katherine Bourzac.
- La simulation de l'électrolyse de l'eau provoquée par de la lumière avec des usages évidents pour la production d'énergie stockable, notamment dans les piles à combustible (à base d'hydrogène). C'est l'un des très nombreux exemples issus de la présentation Enabling Scientific Discovery in Chemical Sciences on Quantum Computers, décembre 2017 (34 slides) par Ber De Jong de Berkeley.
- Solving strongly correlated electron models on a quantum computer de Wecker, Troyer, Hastings, Nayak et Clark, 2015 (27 pages), qui utilise les ordinateurs quantiques à recuit quantique pour simuler la dynamique des semi-conducteurs.
- Faster phase estimation de Svore, Hastings et Freedman, 2013 (14 pages) qui est utilisé dans les simulations quantiques de molécules.
- Simulated Quantum Computation of Molecular Energies de Wiebe, Wecker et Troyer, 2006 (21 pages) qui porte sur la détermination de l'état d'équilibre de molécules simples.
- Simulation of Electronic Structure Hamiltonians Using Quantum Computers de James Whitfield, Jacob Biamonte et Alan Aspuru-Guzik, 2010 (22 pages) qui porte aussi sur la simulation du fonctionnement de molécules simples. Alan Aspuru-Guzik est l'une des grandes références mondiales dans le domaine.
- Des simulations moléculaires hybrides associant algorithmes classiques et quantiques vues dans Quantum Machine Learning for Electronic Structure Calculations, octobre 2018 (16 pages).

Dans Quantum Computation for Chemistry, d'Alán Aspuru-Guzik, 2009 (51 slides), on découvre que les caractéristiques des ordinateurs quantiques nécessaires pour simuler l'état de molécules organiques de complexité moyenne telle que le cholestérol, il faudrait 1500 qubits et surtout, pouvoir enquiller des milliards de portes quantiques, ce qui est actuellement impossible au vu des temps de cohérence bien trop courts des ordinateurs quantiques existants. Et on parle probablement d'un nombre de qubits logiques et pas physiques.

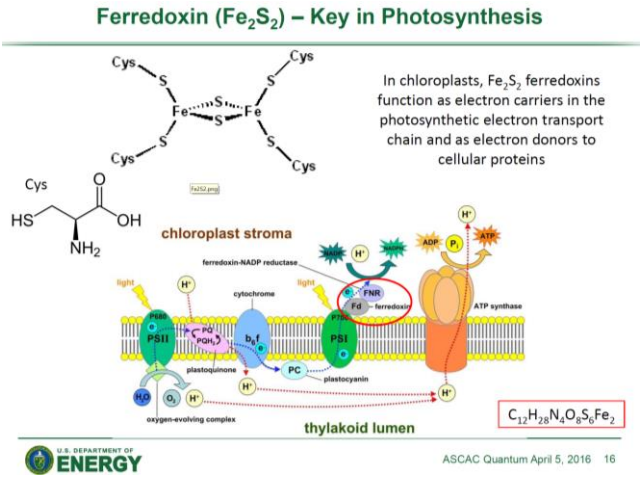
Il faudrait donc probablement aligner des millions de qubits physiques pour pouvoir réaliser ce genre de simulation[183]. Alan Aspuru-Guzik est notamment le coinventeur de la classe des algorithmes hybrides **Variational Quantum Eigensolver** (VQE) qui permet de découvrir un minimum énergétique d'une équation complexe et est réalisable avec un ordinateur quantique à portes universelles avec une profondeur raisonnable de portes quantiques (nombre d'étapes dans l'algorithme)[184].

---

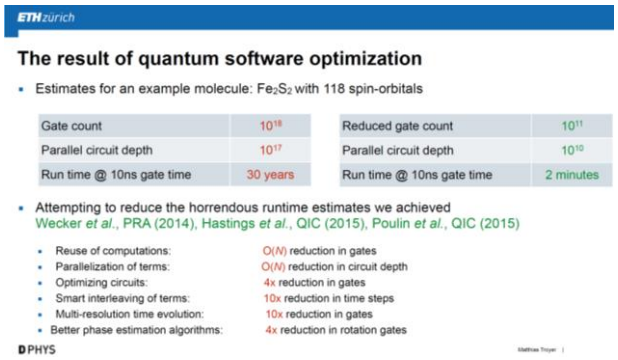
[183] Voir aussi dans le même registre, Quantum Computation for Chemistry and Materials de Jarrod McClean, Google 2018 (36 slides).

[184] Voir An adaptive variational algorithm for exact molecular simulations on a quantum computer par Sophia Economou & Al, 2019 (9 pages) qui indique notamment : "*VQE is much more suitable for NISQ devices, trading in the long circuit depths for shorter state preparation circuits, at the expense of a much higher number of measurements*".

L'une des applications de la simulation quantique moléculaire est de mieux comprendre le fonctionnement de la photosynthèse pour éventuellement l'améliorer ou l'imiter, comme ci-dessous avec l'implication des différentes formes de ferrédoxine, des molécules relativement simples à base de fer et de souffre qui servent à transporter les électrons de l'effet photoélectrique mis en œuvre dans la photosynthèse dans les plantes[185].

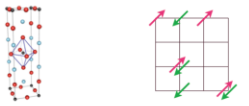


Les recherches algorithmiques sur la simulation de cette molécule ont fait passer en quelques années la durée de simulation théorique quantique de 24 milliards d'années à une heure ! La simulation de la photosynthèse peut ouvrir la voie à une meilleure capture du carbone, entre autres pour produire du fuel synthétique. Des recherches font d'ailleurs aussi progresser le domaine, sans quantique pour l'instant[186]. Matthias Troyer explique comment cet algorithme a été optimisé[187].



From materials to models on quantum computers

	Material	Model
Orbitals per unit cell	≈ 50	1
Unit cells needed	20x20	20x20
Number of orbitals	$N \approx 20'000$	$N \approx 800$
Number of terms	N^4	$O(N)$
Scaling of algorithm	$O(N^{5.5})$	$O(N^{0.5})$
Estimated runtime	age of the universe	seconds



Dans le même domaine, la simulation de l'enzyme nitrogénase qui transforme l'azote en ammoniaque dans les cyanobactéries permettrait de produire des engrais avec beaucoup moins d'énergie que les processus habituels Haber-Bosch de production de l'ammoniaque qui sont très consommateurs d'énergie. L'idée est de réduire les besoins de chauffage du catalyseur.

Il y présente les bénéfices d'autres formes d'optimisations, par simplification du modèle, pour la simulation de supraconducteurs.

---

[185] Le schéma sur la ferredoxine provient de Quantum Computing (and Quantum Information Science) de Steve Binkley, US Department of Energy, 2016 (23 slides).

[186] Comme vu dans Semi-Artificial Photosynthesis Method Produces Fuel More Efficiently Than Nature, septembre 2018

[187] Dans What Can We Do with a Quantum Computer, Matthias Troyer, ETZ Zurich, 2016 (41 slides), source de l'illustration de droite.

S'il faudra être patient pour voir la couleur de nombre de ces simulations, cela n'empêche pas de nombreux chercheurs d'explorer des moyens de simuler le repliement de protéines, l'une des tâches de simulation de molécule organique les plus complexes[188].

Le top du top de la simulation moléculaire quantique arrivera probablement bien plus tardivement. Il s'agit de la simulation du repliement des protéines, une voie clé pour créer de nouvelles thérapies diverses, notamment pour traiter certaines pathologie neurodégénératives ou divers cancers. Différents algorithmes quantiques ont déjà été créés pour ce faire et notamment celui de Aspuru-Guzik de Harvard en 2012, qui a même été testé à petite échelle sur le premier ordinateur quantique adiabatique, le D-Wave One. Reste à évaluer les ordres de grandeur des ordinateurs quantiques nécessaires pour résoudre ces problèmes de chimie organique. Il n'est pas impossible qu'ils relèvent de l'impossible ou de l'extrême long-terme [189]!

Machine learning

Et si le calcul quantique permettait d'accélérer les traitements de l'intelligence artificielle, notamment dans le machine learning et le deep learning ? C'est un de ses domaines d'applications mais nous verrons qu'il n'est pas si évident que cela. Et surtout, à ce stade de maturité de l'IA, le calcul quantique n'a pas l'air de rendre possible ce qui ne le serait pas avec les processeurs classiques, y compris les processeurs matriciels et neuromorphiques du moment.

Divers algorithmes d'optimisation quantiques sont disponibles. L'un de ces algorithmes relève de l'entraînement de réseaux de neurones. Mais cela va encore plus compliquer la situation du côté de l'explicabilité des algorithmes car on ne pourra pas facilement en expliquer les résultats. La décomposition du processus d'entraînement et d'inférence de ces réseaux de neurones quantiques sera probablement différente par rapport à leur mise en œuvre dans des ordinateurs plus traditionnels.

Ces algorithmes quantiques de réseaux de neurones doivent contourner le fait que les fonctions d'activation des neurones sont généralement non linéaires, comme les sigmoïdes qui sont couramment utilisées alors que les portes quantiques appliquent toutes des transformations linéaires[190].

Ces techniques seront concurrencées par les futurs processeurs neuromorphiques à base de memristors qui permettront de faire converger plus rapidement les réseaux par rétropropagation. Les memristors permettront de placer au même endroit dans un circuit les fonctions de calcul du neurone et la mémoire associée, accélérant de plusieurs ordres de grandeur l'accès à celle-ci lors des calculs.

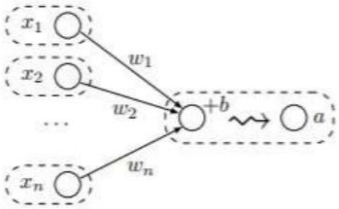
---

[188] Voir par exemple Evolution, energy landscapes and the paradoxes of protein folding de Peter Wolynes, 2015 (13 pages).

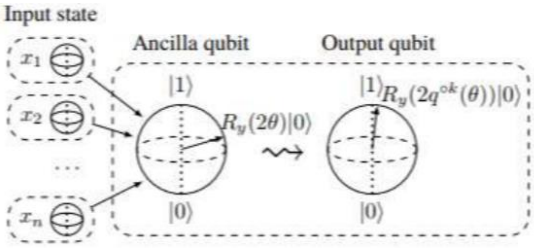
[189] Pour en savoir plus, voir Quantum Information and Computation for Chemistry, 2016 (60 pages), qui inventorie très bien les divers travaux algorithmiques de simulation quantique de chimie organique.

[190] L'astuce est expliquée dans Quantum Neuron: an elementary building block for machine learning on quantum computers, de Yudong Cao, Gian Giacomo Guerreschi et Alan Aspuru-Guzik en 2017 (30 pages).

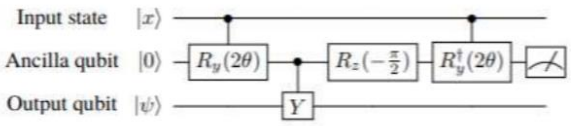
C'est encore un domaine de recherche, opéré notamment par Julie Grollier du laboratoire du CNRS situé chez Thalès TRT à Palaiseau, et que j'ai pu rencontrer en mai 2018.



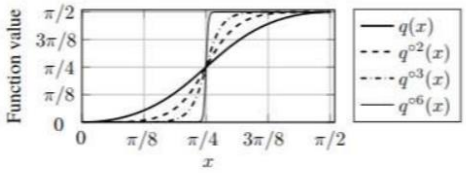
Classical Neuron



Quantum Neuron



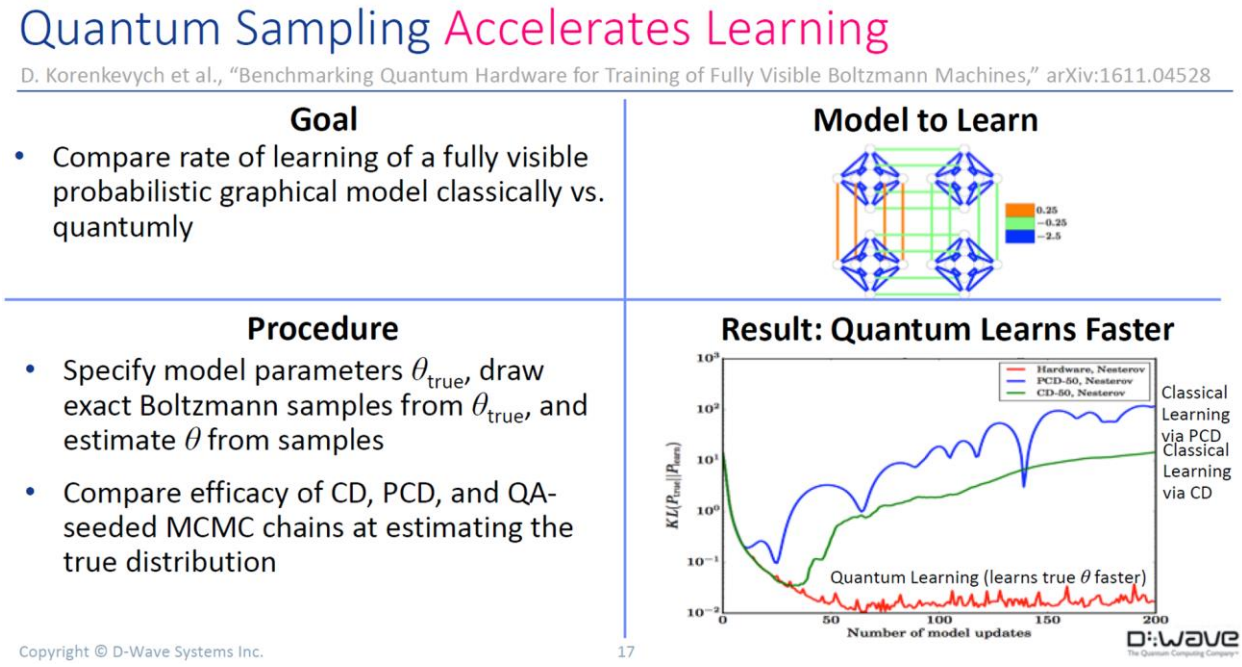
Repeat Until Success circuit



Non-linear Transfer Function

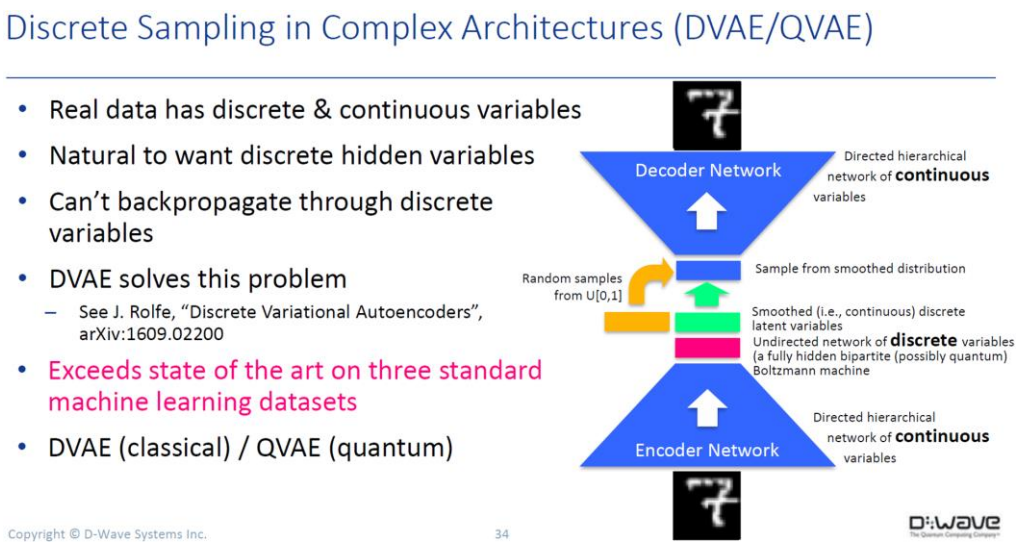
Collaboration: Yudong Cao and Alán Aspuru-Guzik, Harvard University

Voici quelques autres exemples d'algorithmes d'entraînement de machine learning provenant de D-Wave et exploitant leurs ordinateurs à recuit quantique[191]. Avec une réserve souvent émise : l'avantage quantique apporté par le recuit quantique est souvent contesté a posteriori par de nouveaux algorithmes classiques.

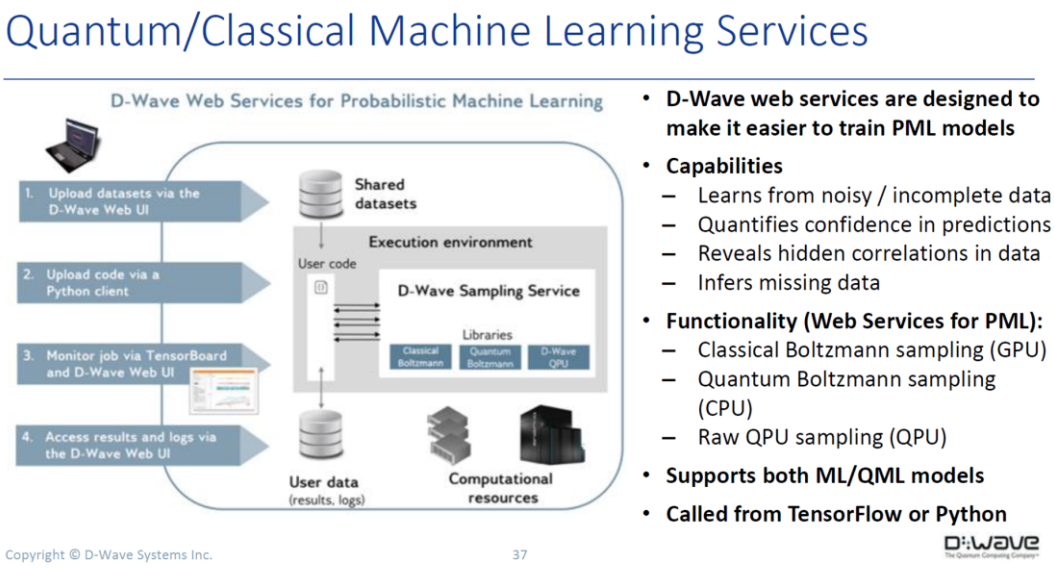


[191] Source des exemples : D-Wave Quantum Computing – Access & application via cloud deployment, Colin Williams, 2017 (43 slides).

Comme ils sont adaptés à la recherche d'un minimum énergétique de systèmes complexes, ils peuvent en effets servir à entrainer des réseaux de neurones, celui-ci correspondant à la recherche d'un niveau minimum d'erreur dans l'ajustement du poids des neurones.



D-Wave fournit d'ailleurs les ressources de ses calculateurs quantiques en mode "cloud" dans le cadre de son offre Leap.



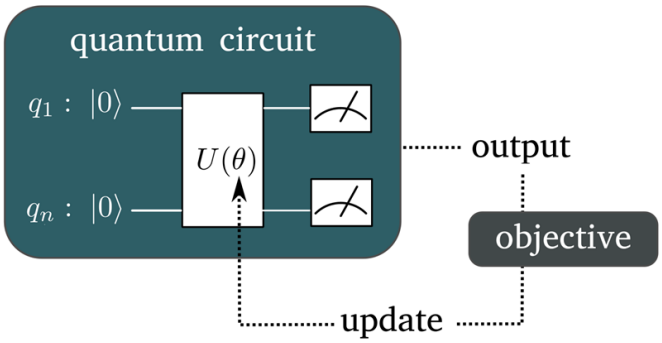
Le calcul quantique permet théoriquement d'accélérer tout un tas d'algorithmes de machine learning sans passer nécessairement par la case des réseaux de neurones et du deep learning.

Voici quelques algorithmes quantiques de bas niveau qui sont très utiles au machine learning et au deep learning :

- La **descente de gradient** pour la rétropropagation dans l'entraînement des réseaux de neurones[192].

[192] Voir Quantum algorithms for feedforward neural networks de Jonathan Allcock, Iordanis Kerenedis & Al, 2018 (18 pages).

- La **PCA** pour déterminer les variables clés d'un jeu de données (Principal Component Analysis, utilisée dans le machine learning traditionnel).
- Le **SVM** (support vector machine), une méthode traditionnelle de segmentation dans le machine learning.
- Le **feature mapping** dans le deep learning, pour détecter des formes de manière efficace[193].
- Les **circuits variationnels** (variational circuits) sont une famille d'algorithmes hybrides qui associent un algorithme quantique et un algorithme traditionnel qui pilote ce dernier[194]. Le VQE, déjà cité, en fait partie.



- Des algorithmes quantiques de **réseaux de neurones convolutionnels**[195], de taille encore modeste pour l'instant.
- Des algorithmes quantiques de **GAN** (Generative Adversarial Networks) qui génèrent des contenus synthétiques à partir de contenus existants en vérifiant leur plausibilité via un réseau de neurones de reconnaissance[196].
- Il existe aussi un algorithme quantique hybride de **régression non linéaire**, une des méthodes de base de prédiction de valeur quantitative du machine learning[197].
- Le quantique peut aussi servir aux systèmes de machine learning pour de la **recommandation**[198].

Dans Quantum Machine Learning, mai 2018, on trouve ce tableau qui positionne clairement les différentes accélérations quantiques associées à divers algorithmes utilisés dans le machine learning et le deep learning. Les accélérations en log(N) sont plus importantes que celles qui sont exprimées en racine carré de N[199].

---

[193] Voir Supervised learning with quantum enhanced feature spaces, Aram Harrow & Al, 2018 (22 pages) décrit l'usage du quantique pour détecter des formes complexes, bien au-delà de ce que peuvent faire les réseaux de neurones convolutionnels ("feature mapping").

[194] Voir Universal Variational Quantum Computation de Jacob Diamonte, 2019 (5 pages).

[195] Voir Quantum Convolutional Neural Networks, par Iris Cong & Al, mai 2019 (12 pages).

[196] C'est bien documenté dans Quantum generative adversarial learning de Seth Lloyd et Christian Weedbrook, 2018 (5 pages) ainsi que dans Quantum generative adversarial learning in a superconducting quantum circuit, 2018 (5 pages).

[197] Voir Nonlinear regression based on a hybrid quantum computer, 2018 (7 pages), issu de chercheurs de plusieurs laboratoires en Chine.

[198] Voir Quantum Recommendation Systems de Iordanis Kerenidis, 2016 (22 pages, et vidéo) est une proposition d'algorithme de machine learning quantique pour de la recommandation.

[199] Côté sources d'information sur ce sujet, j'ai aussi parcouru Application of Quantum Annealing to Training of Deep Neural Networks. (2015), Machine learning & artificial intelligence in the quantum domain, 2017 (106 pages), On the Challenges of Physical Implementations of RBMs, 2014, avec notamment Yoshua Bengio et Ian Goodfellow parmi les auteurs, illustrant l'intérêt des spécialistes de l'IA pour le quantique et Quantum Deep Learning, 2014, le tout étant extrait de Near-Term Applications of Quantum Annealing, 2016, Lockheed Martin (34 slides).Voir aussi Quantum machine learning for data scientists, 2018 (46 pages).

Method	Speedup	AA	HHL	Adiabatic	QRAM
Bayesian Inference [107, 108]	$O(\sqrt{N})$	Y	Y	N	N
Online Perceptron [109]	$O(\sqrt{N})$	Y	N	N	optional
Least squares fitting [9]	$O(\log N^{(*)})$	Y	Y	N	Y
Classical BM [20]	$O(\sqrt{N})$	Y/N	optional/N	N/Y	optional
Quantum BM [22, 62]	$O(\log N^{(*)})$	optional/N	N	N/Y	N
Quantum PCA [11]	$O(\log N^{(*)})$	N	Y	N	optional
Quantum SVM [13]	$O(\log N^{(*)})$	N	Y	N	Y
Quantum reinforcement learning [30]	$O(\sqrt{N})$	Y	N	N	N

Le tout, avec une amélioration souvent exponentielle de vitesse de traitement, modulo le nombre de fois où le calcul doit être réalisé qui dépend de la profondeur du calcul en nombre de portes à exécuter[200].

Table 1.1 The Characteristics of the Main Approaches to Quantum Machine Learning

Algorithm	Reference	Grover	Speedup	Quantum Data	Generalization Performance	Implementation
K-medians	Aïmeur et al. (2013)	Yes	Quadratic	No	No	No
Hierarchical clustering	Aïmeur et al. (2013)	Yes	Quadratic	No	No	No
K-means	Lloyd et al. (2013a)	Optional	Exponential	Yes	No	No
Principal components	Lloyd et al. (2013b)	No	Exponential	Yes	No	No
Associative memory	Ventura and Martinez (2000)	Yes		No	No	No
	Trugenberger (2001)	No		No	No	No
Neural networks	Narayanan and Menneer (2000)	Yes		No	Numerical	Yes
Support vector machines	Anguita et al. (2003)	Yes	Quadratic	No	Analytical	No
	Rebentrost et al. (2013)	No	Exponential	Yes	No	No
Nearest neighbors	Wiebe et al. (2014)	Yes	Quadratic	No	Numerical	No
Regression	Bisio et al. (2010)	No		Yes	No	No
Boosting	Neven et al. (2009)	No	Quadratic	No	Analytical	Yes

The column headed "Algorithm" lists the classical learning method. The column headed "Reference" lists the most important articles related to the quantum variant. The column headed "Grover" indicates whether the algorithm uses Grover's search or an extension thereof. The column headed "Speedup" indicates how much faster the quantum variant is compared with the best known classical version. "Quantum data" refers to whether the input, output, or both are quantum states, as opposed to states prepared from classical vectors. The column headed "Generalization performance" states whether this quality of the learning algorithm was studied in the relevant articles. "Implementation" refers to attempts to develop a physical realization.

L'entraînement de réseaux de neurones pose un problème en quantique car les modèles mathématiques des portes quantiques sont à base d'algèbre linéaire. Or l'entraînement et l'inférence de réseaux de neurones exploite de l'algèbre non linéaire, ne serait-ce que dans les fonctions d'activation des neurones de type sigmoïde. Il existe cependant des parades[201].

Dans le registre de l'IA, le projet **Quromorphic** vise à créer un processeur quantique pouvant exécuter des réseaux de neurones[202]. Il n'est pas du tout évident de comprendre ce qui est quantique ou simplement photonique dans ce genre de processeur qui s'appuie sur le couplage de spin d'électron et de photons micro-ondes associé à la détection de photons par quantum dots.

---

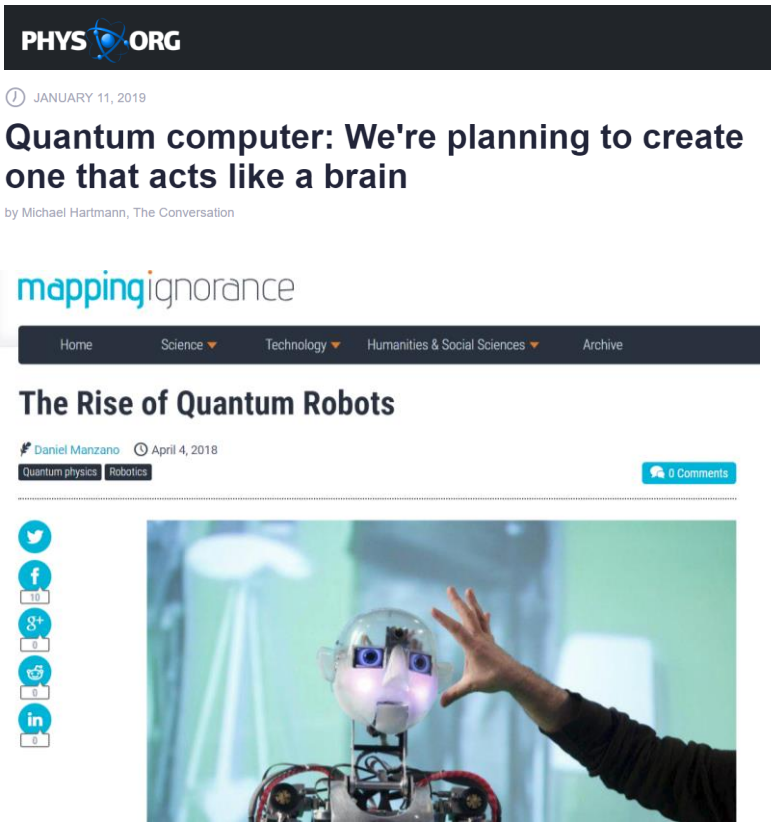
[200] Voir Accelerated Variational Quantum Eigensolver, de Daochen Wang, Oscar Higgott, et Stephen Brierley, 2019 (11 pages) qui propose une méthode de machine learning permettant de réduire la profondeur des circuits quantiques utilisés (nombre de portes quantiques à exécuter). Voir aussi Quantum advantage with shallow circuits de Robert König & Al, 2018 (97 slides). On retrouve cette liste d'algorithmes de machine learning en version quantique dans Quantum Machine Learning What Quantum Computing Means to Data Mining de Peter Wittek, 2014 (178 pages).

[201] Voir par exemple Continuous-variable quantum neural networks, par Nathan Killoran et Al, juin 2018 (21 pages). Le système utilise des circuits quantiques à variables continues.

[202] Voir Quantum computer: We're planning to create one that acts like a brain de Michael Hartmann et Heriot-Watt leads on next-gen computers, novembre 2018. Le projet est piloté par Michael Hartmann de l'IPaQS (Institute of Photonics and Quantum Sciences) de l'Université Heriot Watt au Royaume Uni, conjointement avec l'ETH Zurich, l'Université de Delft (Pays-Bas), l'Université Basque (Espagne), IBM Zurich et Volkswagen (Allemagne). 2,2M€ issus du programme FET Open ont été attribués au projet par la Commission Européenne (détails). Mon interprétation ? L'objectif du projet a été accomodé à la sauce de la science fiction pour récupérer des financements communautaires. Le reste est de la photonique.

Aucune documentation scientifique publique ne permet de valider le contenu de ce projet qui semble quelque peu survendu. Notamment du fait qu'il n'évoque rien côté logiciels.

Bon, de là à utiliser ces algorithmes dans la robotique comme décrit dans The Rise of Quantum Robots de Daniel Manzano (avril 2018), il faudra patienter un peu ! Ce n'est plus de la technologie, c'est de la science-fiction et du click-bait. C'est l'un des nombreux exemples d'escroquerie intellectuelle quantique sur lesquels nous reviendrons en évoquant les « fumisteries quantiques ».


PHYS.ORG

JANUARY 11, 2019

Quantum computer: We're planning to create one that acts like a brain

by Michael Hartmann, The Conversation

mappingignorance

Home | Science | Technology | Humanities & Social Sciences | Archive

The Rise of Quantum Robots

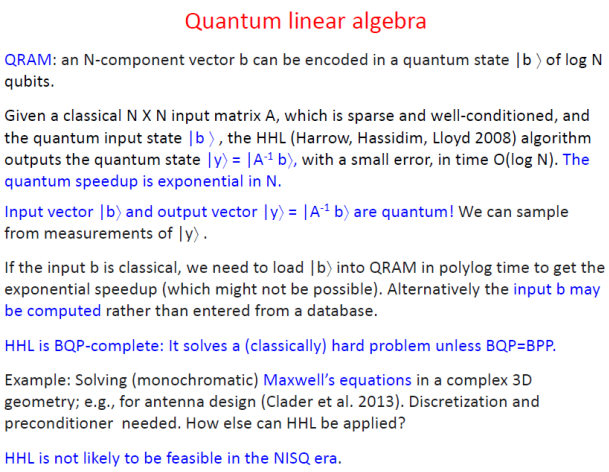
Daniel Manzano | April 4, 2018

Quantum physics | Robotics | 0 Comments

Equations linéaires

De nombreux autres algorithmes quantiques existent qui permettent de réaliser des opérations mathématiques complexes comme la résolution d'équations différentielles, l'inversion de matrices ou le traitement de divers problèmes d'algèbre linéaire. Ils sont ensuite utilisés… ailleurs !

L'algorithme le plus connu est le **HHL** qui reprend le nom de ses créateurs Harrow, Hassidim et Lloyd, créé en 2009.


Quantum linear algebra

QRAM: an N-component vector b can be encoded in a quantum state $|b\rangle$ of log N qubits.

Given a classical N X N input matrix A, which is sparse and well-conditioned, and the quantum input state $|b\rangle$, the HHL (Harrow, Hassidim, Lloyd 2008) algorithm outputs the quantum state $|y\rangle = |A^{-1} b\rangle$, with a small error, in time O(log N). The quantum speedup is exponential in N.

Input vector $|b\rangle$ and output vector $|y\rangle = |A^{-1} b\rangle$ are quantum! We can sample from measurements of $|y\rangle$.

If the input b is classical, we need to load $|b\rangle$ into QRAM in polylog time to get the exponential speedup (which might not be possible). Alternatively the input b may be computed rather than entered from a database.

HHL is BQP-complete: It solves a (classically) hard problem unless BQP=BPP.

Example: Solving (monochromatic) Maxwell's equations in a complex 3D geometry; e.g., for antenna design (Clader et al. 2013). Discretization and preconditioner needed. How else can HHL be applied?

HHL is not likely to be feasible in the NISQ era.

Il permet de résoudre des équations linéaires, avec un gain de performance exponentiel.

Téléportation

L'un des algorithmes quantiques à base de portes quantiques le plus intriguant est celui de la téléportation de qubits. Cet algorithme a été créé par Charles H. Bennett (USA), Gilles Brassard (Canada), Claude Crépeau (Canada), Richard Jozsa (USA), Asher Peres (Israël) et William K. Wootters (USA) en 1993[203].

[203] Voir Teleportation as a quantum computation de Gilles Brassard, 1996 (3 pages).

Le principe de cet algorithme consiste à exploiter un canal d'intrication quantique préexistant pour transmettre d'une extrémité à l'autre de ce canal l'état d'un qubit.

Du fait du théorème de non clonage quantique, cette téléportation est un « move » et pas un « copy » (ou un « cut & paste » au lieu d'un « copy & paste »). L'état du qubit transféré est ainsi détruit de son point de départ[204].

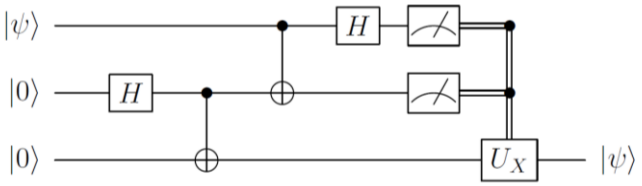


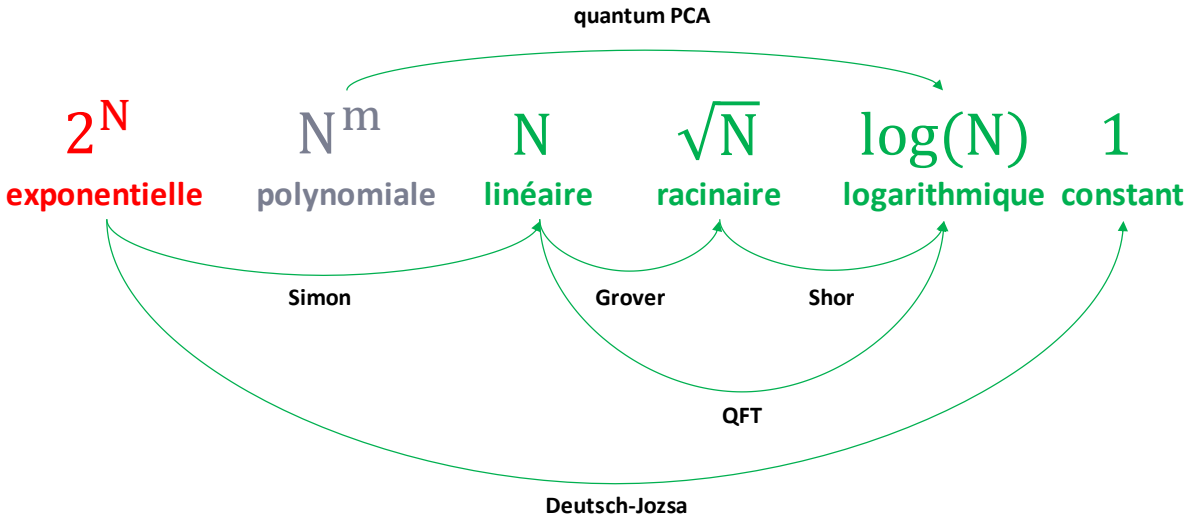
Figure 1.9: Quantum teleportation circuit.

La principale utilisation de cet algorithme se situe dans les systèmes de cryptographie quantique que nous découvrirons plus loin. Elle pourrait également se manifester plus tard dans des architectures distribuées d'ordinateurs quantiques. Cette téléportation pourrait servir à gérer des algorithmes répartis sur des clusters d'ordinateurs quantiques. Mais je n'en suis pas sûr.

Gains de performance quantiques

Pour conclure, j'ai consolidé le petit schéma *ci-dessous* qui résume les gains de performance de quelques-uns des algorithmes déterministes que nous venons de voir. Les niveaux de complexité (exponentielle, polynomiale, linéaire, …) sont génériques.

Les niveaux précis de complexité de chaque algorithme sont associés à ces classes de manière approximative.



Ainsi, N*log(N) qui est la complexité d'une transformée de Fourier classique est linéaire car N grandit bien plus vite que log(N) et log(N) puissance 3 est une complexité de niveau logarithmique (pour l'algorithme de Shor et une QFT, Quantum Fourier Transform).

Attention au fait qu'un gain exponentiel est aussi obtenu lorsque l'on passe de N ou Racine de N vers log(N). Une QFT génère donc un gain similaire à l'algorithme de Deutsch-Jozsa.

---

[204] Voir Quantum Teleportation in a Nutshell de Fabian Kössel, 2013 (35 slides).

Les échelles de temps sont plus parlantes dans ce tableau [205] :

Complexité	n	$n \log_2 n$	n^2	n^3	1.5^n	2^n	$n!$
$n = 10$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	4 s
$n = 30$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	18 min	10^{25} ans
$n = 50$	< 1 s	< 1 s	< 1 s	< 1 s	11 min	36 ans	∞
$n = 100$	< 1 s	< 1 s	< 1 s	1s	12, 9 ans	10^{17} ans	∞
$n = 1000$	< 1 s	< 1 s	1s	18 min	∞	∞	∞
$n = 10000$	< 1 s	< 1 s	2 min	12 jours	∞	∞	∞
$n = 100000$	< 1 s	2 s	3 heures	32 ans	∞	∞	∞
$n = 1000000$	1s	20s	12 jours	31, 710 ans	∞	∞	∞

L'idéal en gains de performances est de traverser plusieurs classes de complexité, et surtout, à partir d'un problème exponentiel. Dans la pratique, les principaux algorithmes sautent une à deux classes de complexité mais pas forcément à partir de la classe des problèmes exponentiels. Mais mon schéma est trompeur. N peut aussi croitre de manière exponentielle selon la taille d'un problème. L'exemple classique est celui de l'algorithme de Shor.

Le point de départ est un N qui est en fait une taille de clé RSA qui elle-même est évaluée en puissance de 2. Une clé de 1024 bits fait 2^{1024}. Si on passe de 2^{256} à 2^{1024}, la croissance de la taille de la clé est exponentielle. Et là, on obtient donc avec l'algorithme de Shor un gain de performance exponentiel en passant d'une racine carrée de 2^{1024} à $\log(2^{1024})$, soit 1024 (en base 2) ! On passe donc de 2^{512} à 1024, ce qui représente bien un gain parfaitement exponentiel.

L'algorithme de Deutsch-Jozsa a la particularité de traverser tous les niveaux de complexité mais nous avons vu qu'il n'avait malheureusement pas d'application pratique connue.

Il faut aussi intégrer le fait que la complexité de certains problèmes peut être contournée sur des ordinateurs classiques avec des approches probabilistes qui permettent aussi de réduire de un ou plusieurs étages le niveau de complexité de problèmes exponentiels.

En conclusion, les algorithmes quantiques sont séduisants mais ils ne sont pas pour autant toujours la panacée.

Algorithmes hybrides

Une autre branche d'algorithmes quantiques se développe depuis quelques années, celle des algorithms hybrides qui associent une composante traditionnelle et une composante quantique. A vrai dire, tout algorithme quantique a besoin d'un soutien d'un ordinateur classique pour le pilotage de l'ordinateur quantique et l'activation de ses portes quantiques[206].

---

[205] Source du tableau : Complexité en temps, Ecole Polytechnique (25 pages).

[206] Voir A Hybrid Quantum-Classical Approach to Solving Scheduling Problems, Tony T. Tran & al, (9 pages), Hybrid Quantum Computing Apocalypse 2018 (6 pages) selon lequel les Chinois auraient réussi à faire tourner un fermion de Majorana, The theory of variational hybrid quantum-classical algorithms Jarrod McClean & Al (23 pages).

Les algorithmes hybrides répartissent les calculs de part et d'autre et font en sorte que la partie quantique de l'algorithme ne couvre que la partie qui ne peut pas l'être dans la partie classique. A terme, il est probable qu'une majorité d'algorithmes quantiques seront hybrides[207].

Ces algorithmes hybrides pourront être mis en œuvre dans des outils de développement et langages à même de contrôler à la fois la partie classique et la partie quantique d'un supercalculateur ou d'un système distribué.

C'est notamment le cas du modèle de programmation **XACC** (eXtreme-scale ACCelerator)[208]. Il permet de développer un code hybride qui tient compte des caractéristiques du calculateur quantique, notamment de son taux d'erreurs. Il s'interface avec les modèles de programmation d'ordinateurs quantiques d'IBM et Rigetti.

L'un des algorithmes pouvant être traité dans des architectures hybrides est le **Quantum Approximate Optimization Algorithm,** créé par Edward Farhi en 2014. C'est un algorithme d'optimisation combinatoire notamment utilisé dans des problèmes de graphes et de gestion de coupes (MaxCut). Il présente l'intérêt de requérir une faible profondeur de portes quantiques[209].

Quick history of the variational quantum eigensolver (VQE)

1. First paper on VQE and implementation with quantum optics (April 2013):
A. Peruzzo, J. McClean, P. Shadbolt, M. Yung, X. Zhou, P. Love, A. Aspuru-Guzik, J. O'Brien
Nature Communications, 5:4213, (2014)

2. Theoretical implementation with ion trap (July 2013)
M. Yung, J. Casanova, A. Mezzacapo, J. McClean, L. Lamata, A. Aspuru-Guzik, E. Solano
Scientific Reports, 4:3589 (2014)

3. Analysis of measurements needed for chemistry (July 2014)
J. McClean, R. Babbush, P. Love, A. Aspuru-Guzik
Journal of Physical Chemistry Letters, 5 (24): 4368–4380 (2014)

4. First implementation with ion trap (June 2015)
Y. Shen, X. Zhang, S. Zhang, J. Zhang, M. Yung, K. Kim
arXiv preprint: 1506.00443

5. Application to Fermi-Hubbard and numerics (July 2015):
D. Wecker, M. B. Hastings, M. Troyer
Physical Review A, 92:042303 (2015)

6. First implementation with superconducting qubits (August 2015):
C. Eichler, J. Mlynek, J. Butscher, P. Kurpiers, K. Hammerer, T. Osborne, A. Wallraff
Physical Review X, 5:041044 (2015)

7. Theory generalization and error robustness (September 2015):
J. McClean, J. Romero, R. Babbush, A. Aspuru-Guzik
New Journal of Physics 18 (2): 023023 (2016)

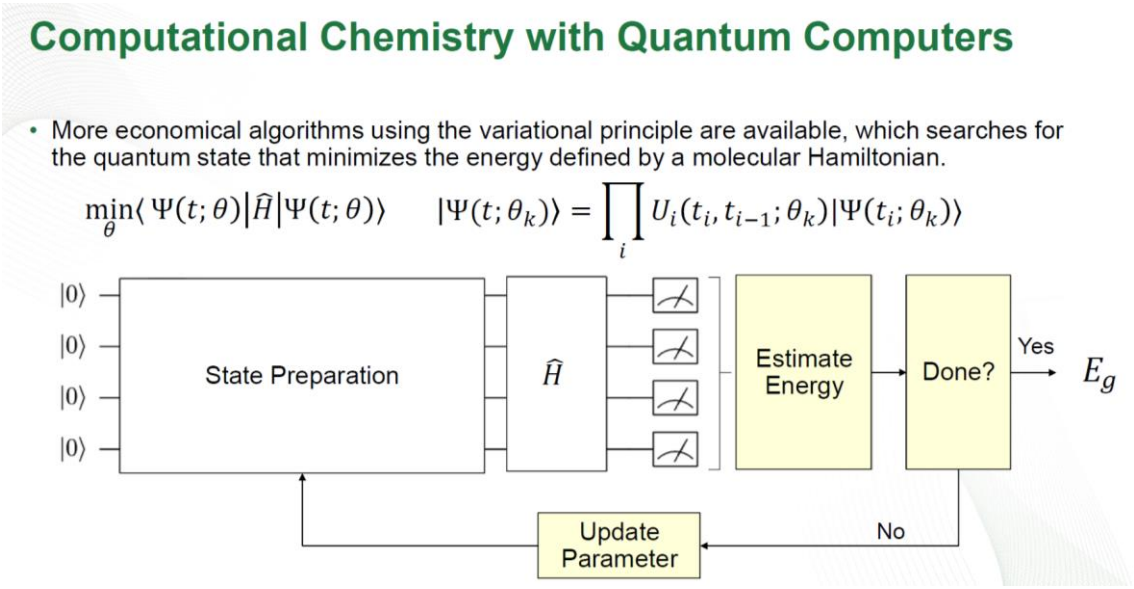
8. First scalable quantum chemistry simulation (December 2015):
P. O'Malley, R. Babbush, I. Kivlichan, J. Romero, J. McClean, R. Barends, J. Kelly, P. Roushan, A. Tranter, N. Ding, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, A. Fowler, E. Jeffrey, A. Megrant, J. Mutus, C. Neill, C. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. White, P. Coveney, P. Love, H. Neven, A. Aspuru-Guzik, J. Martinis
arXiv preprint: 1512.06860

[207] A ce titre, les brevets d'algorithmes quantiques déposés par Accenture sont inquiétants car ils sont à la limite des *patent trolls*. Voir par exemple le brevet Multi-state quantum optimization engine, USPTO 10,095,981B1, validé en octobre 2018 (20 pages). Un second brevet validé en avril 2019 concerne une solution de machine learning qui aide un algorithme à décider quelle partie exécuter en classique et quelle partie exécuter en quantique. C'est l'USPTO 10,275,721.

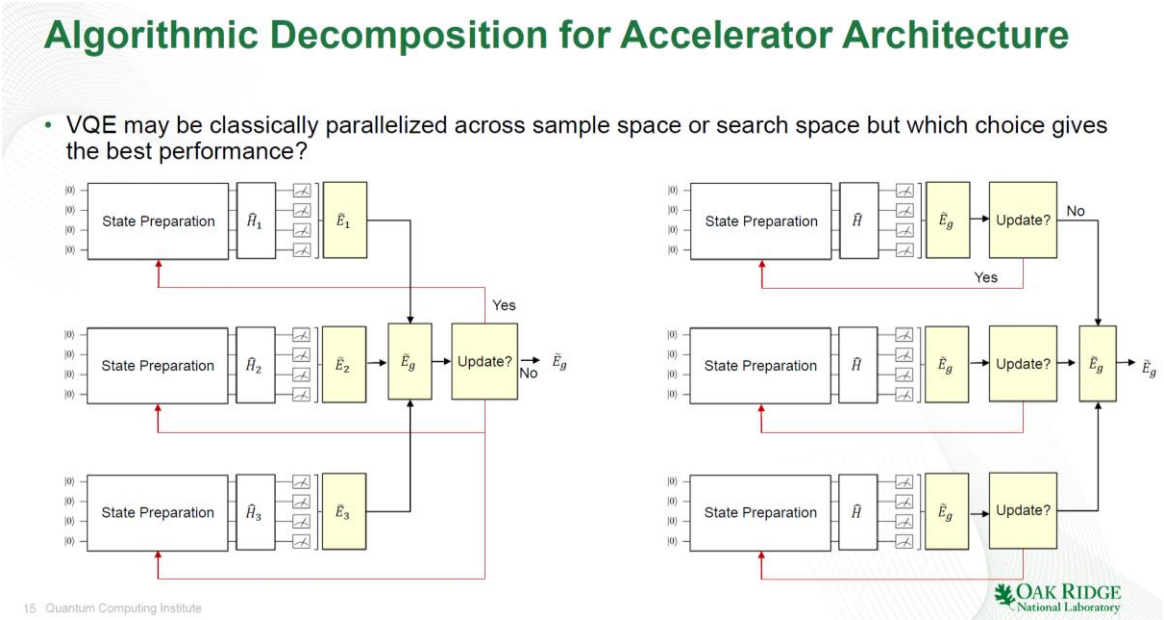
[208] Voir Hybrid Programming for Near-term Quantum Computing Systems, de A. J. McCaskey & al, du laboratoire d'Oak Ridge, 2018 (9 pages).

[209] Voir An Introduction to Quantum Optimization Approximation Algorithm de Qingfeng Wang et Tauqir Abdullah, décembre 2018 (16 pages) et QAOA: Quantum Approximate Optimization Algorithm de Peter Shor (25 slides).

L'autre algorithme hybride le plus prisé est le **Variational Quantum Eigensolver** (VQE)[210]. Créé en 2013[211], il sert à la recherche d'un minimum énergétique d'un système complexe. Il sert notamment à faire de la simulation de structures de molécules dans la chimie inorganique et organique. Il combine une partie classique qui détermine un point de départ approximatif et une partie quantique qui affine le résultat. Il peut même servir pour l'entraînement d'un modèle de machine learning[212].



Ce type d'algorithme présente l'avantage de pouvoir être traité dans des architectures distribuées avec plusieurs processeurs classiques et quantiques.



[210] Source des schémas : Quantum Computing for Scientific Discovery: Methods, Interfaces, and Results de Travis Humble du Quantum Computing Institute, Oak Ridge National Laboratory, mars 2018 (47 slides).

[211] L'historique vient de Towards an experimentally viable variational quantum eigensolver with superconducting qubits, 2016 (18 slides).

[212] Il est maintenant possible de se passer de la partie classique de l'algorithme comme expliqué dans An adaptive variational algorithm for exact molecular simulations on a quantum computer, de Sophia Economou & Al, 2019 (9 pages).

Certification d'algorithmes

La vérification et la certification d'algorithmes quantiques et des résultats de leur utilisation est un nouveau sujet important. La factorisation de nombres entiers est évidemment facile à vérifier. Mais lorsqu'un algorithme quantique sert à simuler des interactions physiques comme celles d'atomes dans des molécules, c'est moins évident.

Des travaux théoriques montrent que l'on peut prouver de manière polynomiale qu'un résultat d'algorithme quantique est exact[213]. Malheureusement, par contre, on ne peut pas expliquer dans le détail l'origine du résultat en le décomposant.

Voir aussi Quantum cloud computing with self-check, de Rainer Blat & Al, mai 2019, qui évoque des calculs de simulation quantique sur 20 qubits à ions piégés avec un contrôle des résultats sur l'ordinateur quantique aussi rapide que sur PC.

[213] Voir How to Verify a Quantum Computation d'Anne Broadbent, 2016 (37 pages) qui démontre que tous les résultats d'algorithmes quantiques peuvent être vérifiés avec des algorithmes classiques polynomiaux en réalisant plusieurs tests et en chiffrant les données en entrée. Je n'ai pas compris plus que cela de la méthode ! Voir aussi Verification of quantum computation: An overview of existing approaches, Alexandru Gheorghiu, Theodoros Kapourniotis et Elham Kashefi, 2018 (65 pages).

Complexité

Dans la partie précédente, nous avons fait le tour des principaux algorithmes quantiques connus, de leurs domaines d'applications et de leur performance relative.

Le calcul quantique est parfois présenté comme étant une solution miracle aux limites du calcul sur supercalculateurs. Il permettrait de résoudre des problèmes dits "intractables" sur des ordinateurs classiques. Mais au juste, quelle est la nature des problèmes qui peuvent être résolus avec un ordinateur quantique et qui ne peuvent pas l'être avec des ordinateurs classiques ? Et surtout, quelles sont les limites des ordinateurs quantiques ? Comment se situent-elles par rapport aux limites de l'intelligence artificielle ?

Nous allons voir que ces limites sont plutôt floues et mouvantes. Elles sont traitées dans un champ complet et méconnu de la science, celui des **théories de la complexité**. C'est un monde on ne peut plus abstrait où les spécialistes parlent un langage abscons fait de P, NP, BQP et autres complétudes. Ils gambergent depuis près d'un demi-siècle pour déterminer si **P = NP ou pas**, une question aussi importante que le rôle exact du nombre 42 dans le fonctionnement de l'Univers. C'est la science des classes de complexité de problèmes. Derrière ces mathématiques de la complexité se cachent des considérations techniques mais aussi philosophiques fondamentales pour l'Homme et son désir de toute puissance.

Les classes de complexité de problèmes sont des poupées russes plus ou moins emboitées les unes dans les autres. Elles tournent surtout autour de la question de la montée en charge du temps de résolution des problèmes en fonction de leur taille.

On ne sait résoudre dans un temps raisonnable que les problèmes dits polynomiaux ou plus simples que les polynomiaux. Un temps polynomial est proportionnel à une puissance donnée de N, N étant la dimension du problème à résoudre. L'informatique quantique permet dans certaines conditions de résoudre certains problèmes dits exponentiels, qui croissent de manière exponentielle avec leur taille. Au-delà se situent divers problèmes inaccessibles qui relèvent souvent de simulations complexes ou de résolutions par force brute. Les ordinateurs quantiques ne pourront pas résoudre tous les problèmes qui nous passeront par la tête, même le jour où l'on pourra aligner des gazillions de qubits avec un taux d'erreur infinitésimal.

Ces limites ont un impact indirect sur les prévisions concernant la création d'intelligences artificielles omniscientes capables de transcender le raisonnement humain et de résoudre tous les problèmes. Ces hypothétiques AGI (Artificial General Intelligence) seront limitées par les données et concepts qui les alimentent et par l'impossibilité de résoudre certains problèmes complexes, notamment ceux qui relèvent de la prévision et de la simulation et qui reposent sur la force brute plutôt sur des astuces algorithmiques permettant d'aboutir rapidement à la solution.

Le calcul ultime n'existe donc pas encore et l'Homme continuera à faire face à l'impossible et ne pourra pas résoudre tous les problèmes complexes qu'il rencontrera ! Le calcul quantique ne permet pas de dominer la nature et de mettre en équation l'Univers et d'en prévoir le fonctionnement au quantum près. Le hasard, l'imprévu et le libre arbitre continueront de jouer un rôle dans un monde très indéterministe et c'est tant mieux comme cela. C'est une petite leçon d'humilité pour l'Homme que de passer son temps à découvrir des limites scientifiques à ses besoins de contrôle !

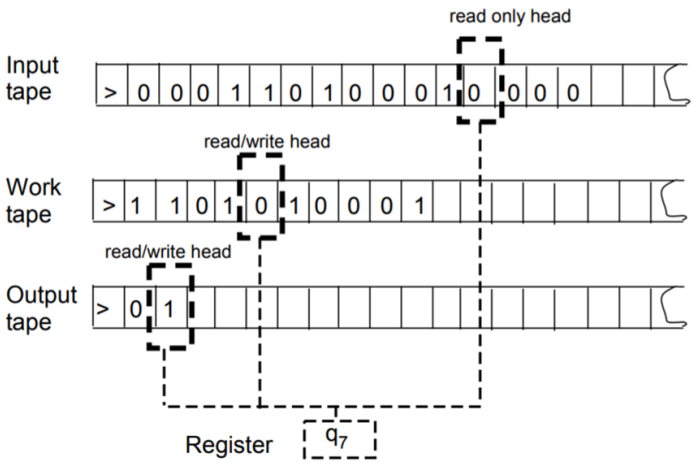
Classes de complexité de problèmes

Pour rentrer dans ce sujet, il faut en passer par définir les grandes classes de problèmes par niveau de complexité. Elles font partie d'un champ entier de la logique et des mathématiques qui agite un petit monde de spécialistes. Me voilà donc une fois encore amené à devoir simplifier la complexité, et cette fois-ci, au sens littéral du terme.

Dans la pratique, les classes de complexité décrivent des problèmes que l'on résout par force brute en testant plusieurs combinatoires. Ils ne relèvent pas d'équations mathématiques simples que l'on résout avec des formules permettant d'aboutir directement à la solution comme on le fait pour prédire la position des planètes en s'appuyant sur les lois de la mécanique newtonienne.

Les classes de problèmes font appel à une notion de machines déterministes et non déterministes de Turing. De quoi s'agit-il ?

Les machines de Turing sont les modèles conceptuels d'ordinateurs créés par Alan Turing avant la seconde guerre mondiale. Elles modélisent les traitements informatiques en s'appuyant sur la notion de programmes et de données, incarnées par des rouleaux de papier continus, le premier pour le programme, le second pour les données en entrée et le troisième pour générer les résultats (*ci-contre*[214]).



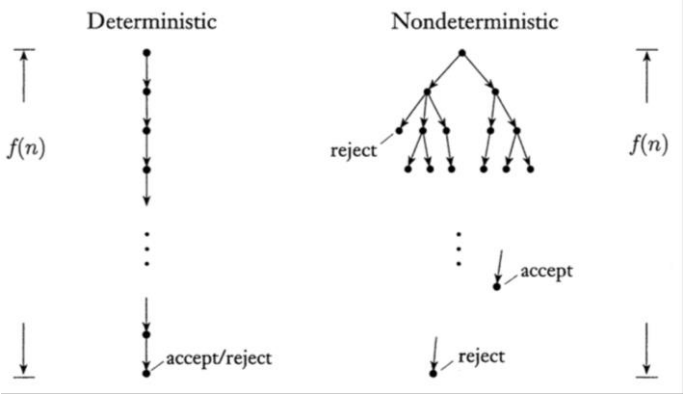
Des étudiants d'un master de l'ENS Lyon ont réalisé une machine de Turing en Lego en 2012 à l'occasion du centenaire de la naissance d'Alan Turing (vidéo) et ce n'était pas la seule du genre (vidéo) ! Un Anglais en a aussi réalisé une en bois en 2015 (vidéo). Voilà de quoi s'éduquer ludiquement !

[214] Source du schéma : Computational Complexity: A Modern Approach, Sanjeev Arora et Boaz Barak, 2007 (489 pages). C'est un bon document de référence sur les théories de la complexité.

Le modèle théorique de Turing est utilisé depuis longtemps pour définir les classes de problèmes que l'on peut résoudre ou pas avec un ordinateur. Les ordinateurs sont tous métaphoriquement des machines de Turing, reproduisent cette logique en lisant des instructions de programmes et en gérant les données en mémoire vive (RAM) ou en stockage persistent (disque dur, SSD, …). Est associée à la notion de machine de Turing celle de la **thèse de Church-Turing**, des noms d'Alonzo Church et Alan Turing selon laquelle il existe une équivalence entre problèmes de calcul réalisable à la main et avec des ressources non limitées, ceux qui sont traitables avec une machine de Turing et ceux qui peuvent être résolus avec des fonctions dites récursives.

Dans une machine déterministe, la séquence des actions à réaliser est prédéfinie et séquentielle.

Dans le modèle conceptuel de machine de Turing non déterministe, les règles de calcul peuvent imposer de réaliser plusieurs opérations différentes pour chaque situation évaluée. En gros, en explorant plusieurs voies en parallèle et en cherchant une réponse positive à une composante d'algorithme et en fermant des boucles de tests parallèles une fois les sous-solutions trouvées.



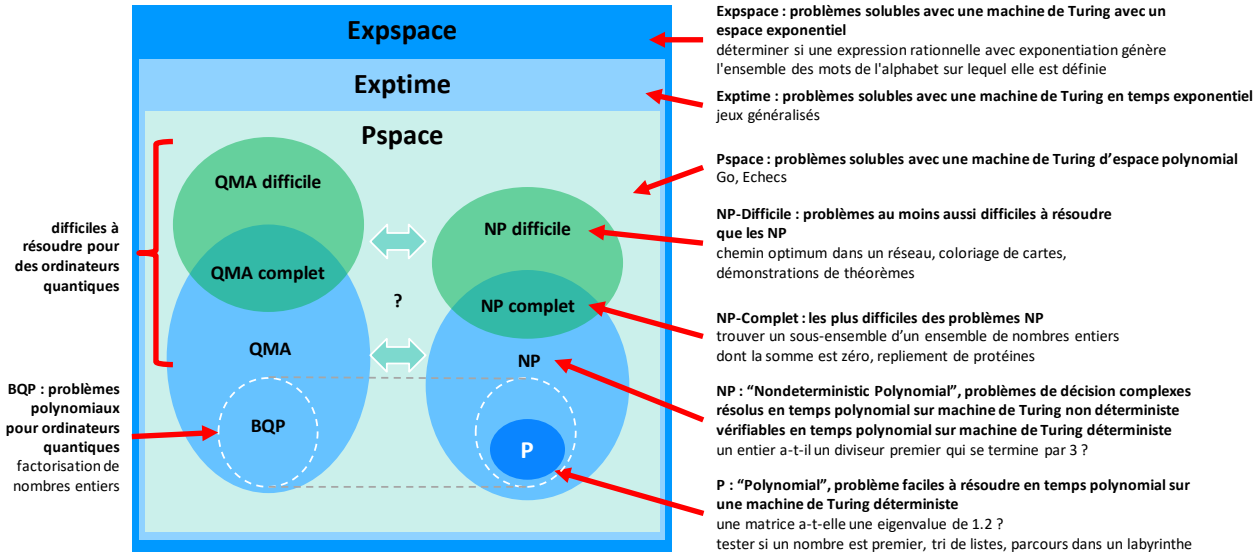
C'est plus ou moins le modèle de navigation dans l'arbre de décision de la version 2017 d'AlphaGo, dite AlphaGo Zero, qui évalue dans un réseau de neurones différents scénarios de jeu. Une machine non déterministe augmente la combinatoire de calcul par rapport à une machine déterministe. Et cette combinatoire passe de polynomiale à exponentielle. La force d'AlphaGo Zero est d'utiliser des réseaux de neurones en quelque sorte récursifs pour réduire le nombre de branches de l'arbre de décision à tester pour sortir partiellement de la fatalité exponentielle de ce jeu.

Classes de complexité génériques

Le niveau de complexité s'entend vis à vis du temps de calcul nécessaire et de l'espace mémoire nécessaire pour ces calculs.

En règle générale, on est bloqué par le temps de calcul avant de l'être par la capacité mémoire. L'association d'un problème à une classe de complexité est liée à la performance du meilleur algorithme connu pour résoudre ledit problème.

Les niveaux de classes de problèmes dans les théories de la complexité reposent souvent sur des modèles de boite noire ou d'oracles à qui un système pose des questions et obtient des réponses en fonctions des données fournies. C'est une logique de "force brute" et de scan d'hypothèses. La combinatoire à tester est plus ou moins grande selon les classes de problèmes.



Voici donc ces classes par niveau croissant de complexité sachant que nous passerons le plus de temps sur les classes NP et NP Complet.

L : ou LSPACE, ou DLOGSPACE, qui définit la classe des problèmes que l'on peut résoudre à une échelle logarithmique de mémoire consommée et sur une machine de Turing déterministe, soit, sur un ordinateur traditionnel. C'est le genre de classe idéale ! La complexité de calcul diminue rapidement avec la taille du problème. Malheureusement, très peu de problèmes complexes sont dans cette classe là. On y trouve notamment les requêtes dans des bases de données relationnelles préalablement indexées, les recherches de séquences d'ADN et d'une manière générale les techniques de recherche utilisant des pointeurs et qui optimisent l'utilisation de la mémoire des ordinateurs.

NL : la classe des problèmes résolus à une échelle logarithmique sur une machine non-déterministe. Les logiciens cherchent toujours à savoir si si L=NL ! Cela pourrait durer quelque temps. Cela les occupe moins que P=NP.

P : qui définit les problèmes que l'on peut résoudre avec un temps qui croit de manière polynomiale avec le nombre de données à traiter et sur une machine déterministe. Si N est la taille du problème, la durée de traitement est proportionnelle à N puissance M, M étant un entier, si possible 2. C'est un problème facile à résoudre. Il est dit "tractable". Cela comprend le tri de listes, la validation de l'existence d'un chemin dans un graphe, la recherche d'un chemin minimum dans un graphe, la multiplication de matrices ou l'évaluation d'un nombre pour savoir s'il est premier.

BPP : est une classe de problèmes qui peuvent être résolus par des approches aléatoires ("Bounded-Error Probabilistic Polynomial-Time"). Il semblerait que BPP=P mais ce n'est pas encore démontré.

NP : décrit la classe des problèmes dont il est facile de vérifier la validité d'une solution, à savoir que celle-ci peut être réalisée en un temps polynomial par une machine déterministe. L'autre définition de la classe est qu'elle contient les problèmes dont le temps de résolution est polynomial sur une machine non déterministe.

Ces problèmes plus complexes ont un temps de calcul au minimum exponentiel lorsque la méthode utilisée est dite naïve, pour tester toutes les hypothèses possibles. Ils sont dits intractables. En pratique, ce sont des problèmes particulièrement adaptés aux ordinateurs quantiques du fait de leur capacité à évaluer en parallèle 2 puissance N combinaisons.

Quelques exemples de problèmes NP : l'arbre de Stein pour déterminer si un réseau électrique permet de relier un nombre de maison à un certain prix, vérifier qu'une séquence d'ADN se retrouve dans plusieurs gênes et la distribution de tâches à différents agents pour minimiser le temps de leur réalisation. Les exemples théoriques des cours de complexité ont l'air de relever de problèmes futiles, nous en verrons quelques-uns plus tard. Mais côté métiers, ces problèmes ont des équivalents très concrets dans la logistique, la planification, la production, les transports, les télécoms, les utilities, la finance ainsi que dans la cryptographie.

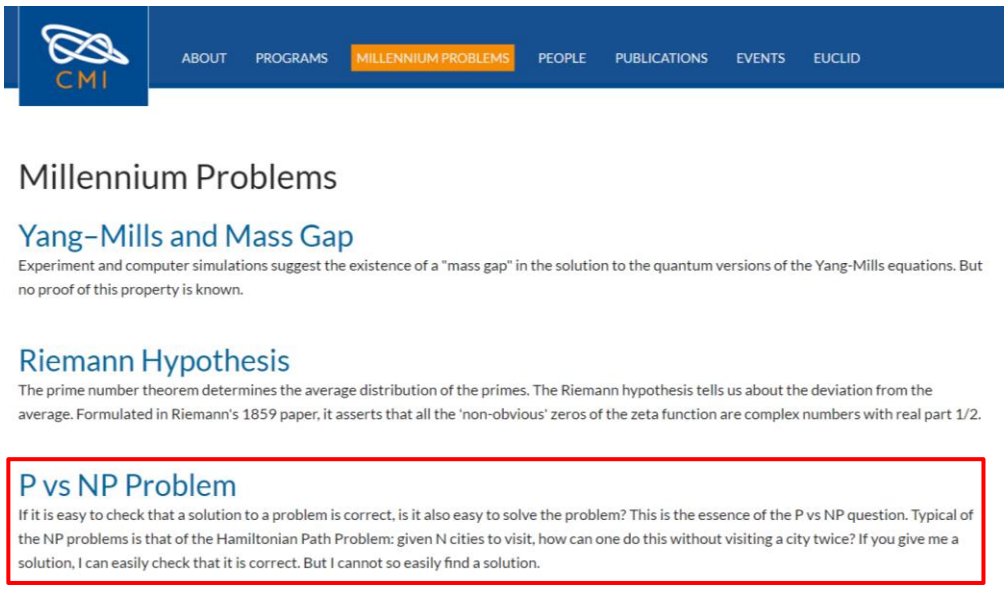
A noter qu'un problème "décidable", c'est à dire qui requiert d'explorer un espace fini d'options, n'est pas forcément faisable d'un point de vue pratique. Même s'il peut être résolu en un temps fini, sa résolution peut prendre un temps trop long. Un problème exponentiel a une solution élégante si on peut en trouver une qui ait une durée polynomiale voir, dans le meilleur des cas, linéaire. Les temps polynomiaux *scalent* mieux que les temps exponentiels !

Un problème décidable n'est pas forcément faisable d'un point de vue pratique. Un problème décidable requiert d'explorer un espace fini d'options. Cela peut prendre un temps très long mais c'est un temps fini. Mais s'il est trop long à traiter, il n'est pas faisable, avec les techniques de calcul à un moment donné. Un problème exponentiel a une solution élégante si on peut en trouver une qui ait une durée polynomiale voir, dans le meilleur des cas, linéaire. Les temps polynomiaux scalent mieux que les temps exponentiels !

Un gros débat a cours depuis 1956 (Kurt Gödel) pour savoir si la classe P égale la classe NP. Si P = NP, il serait aussi simple de trouver un résultat quand on sait aussi le vérifier simplement. Le consensus général est que P n'est pas égal à NP. La démonstration de P<>NP ou de son contraire fait partie de l'un des sept défis mathématiques du Clay Mathematics Institute lancés en 2000 chacun dotés d'un prix de $1M (*ci-dessus*).

Parmi ces défis, on trouve la démonstration des équations de Navier-Stokes sur la mécanique des fluides et celle de l'hypothèse de Riemann sur la distribution des nombres premiers. Voilà de beaux problèmes à résoudre pour une hypothétique AGI (Artificial General Intelligence) capable de dépasser l'Homme dans sa capacité de conceptualisation. Et $7M à la clé, si le principe de l'AGI était vérifié, à savoir sa capacité à résoudre n'importe quel problème, à supposer que celui-ci soit décidable !

Le chercheur brésilien André Luiz Barbosa a publié en 2010 P ≠ NP Proof (25 pages) tout comme un papier invalidant le théorème de Cook selon lequel un problème booléen SAT est NP-Complet, The Cook-Levin Theorem is False, 2010 (11 pages). Il ne fait visiblement pas l'unanimité, ses travaux n'étant ni cités, ni repris.



$1M à la clé !

Du côté P vs NP, la formulation du défi à relever donne un exemple d'un tel problème : vous devez allouer 50 chambres de deux étudiants à 400 candidats mais certains candidats ne doivent pas cohabiter dans la même chambre. La combinatoire de choix des 100 étudiants parmi 400 est monstrueusement énorme, donc le problème n'est pas traitable facilement avec un supercalculateur et avec de la force brute. C'est bien un problème NP car une solution donnée est facile à vérifier car il suffit de vérifier qu'aucune des chambres ne contient une paire d'individus interdite. C'est un peu la théorie du tout ou du rien car si P = NP, tous les problèmes NP ont une solution efficace polynomiale. Si P ≠ NP, aucun des problèmes NP n'a de solution efficace.

La définition des classes de problèmes NP et NP-Complet est relativement récente[215]. J'ai parcouru un grand nombre de publications pour m'y retrouver mais elles étaient assez redondantes dans l'ensemble.

NP Complet : ils se définissent selon Richard Karp comme les problèmes dans lesquels les autres problèmes NP peuvent être réduits de manière polynomiale. A fortiori, ils n'ont pas de solution P (polynomiale) connue.

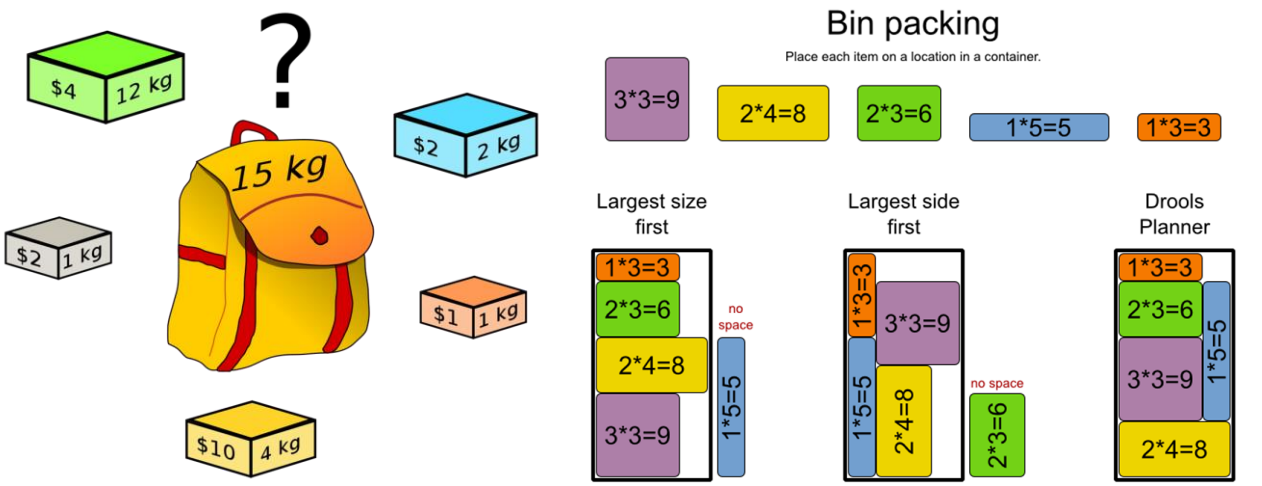
Ils sont encore non accessibles aux ordinateurs quantiques. C'est dans cette classe que l'on trouve les problèmes de logique booléenne de type SAT ou 3SAT dont je vous passe les détails car je risquerai de vous perdre et de me perdre par la même occasion ! Plus de 3000 problèmes NP-Complets sont identifiés à ce jour (liste).

On y trouve notamment le problème du remplissage optimum du coffre de la voiture lorsque l'on part en vacances ou lorsque l'on revient du Noël dans sa famille avec une flopée de cadeaux. Et puis le **problème du sac à dos** consistant à le remplir de manière optimale avec un jeu d'objets, pour obtenir la plus grande charge et sans dépasser un poids maximum ("Bin packing")[216].

---

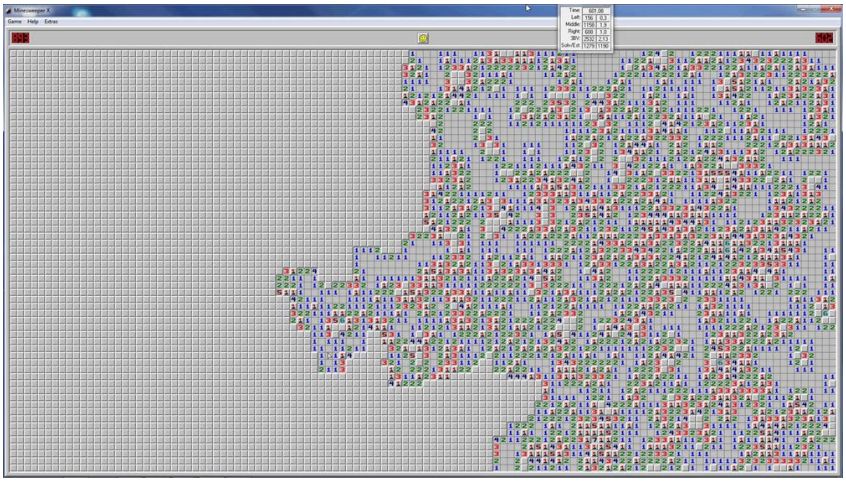
[215] Elle est issue de The complexity of theorem-proving procedures de Stephen Cook de l'Université de Toronto, 1971 (8 pages), mieux vulgarisé dans An overview of computational complexity (8 pages) et Reducibility about combinatorial problems, de Richard Karp, 1972 (19 pages) ainsi que dans Complexité et calculabilité d'Anca Muscholl du LaBRI, 2017 (128 slides).

[216] Sources des illustrations : Wikipedia et Stackoverflow.



Il comprend aussi le **problème de la somme de sous-ensemble** consistant à trouver un sous-ensemble d'un ensemble de nombres entiers dont la somme est égale à un entier arbitraire.

Le **problème du démineur** consiste à localiser des mines cachées dans un terrain avec pour seules indications le nombre de mines dans les zones adjacentes et le nombre de mines total dans le champ. Le tout sans les faire exploser. C'est un jeu bien connu des utilisateurs de Windows, lancé en 1989 [217]!



Il semblerait enfin que la simulation du repliement de protéines complexes soit un problème NP-Complet[218]. Ce serait donc un problème potentiellement très difficile à résoudre avec un ordinateur quantique avec de grandes protéines.

Il est démontré que si l'on trouvait une solution optimale à un problème NP-Complet, on trouverait toutes les solutions aux problèmes de cette classe. C'est la notion importante de réduction de problèmes.

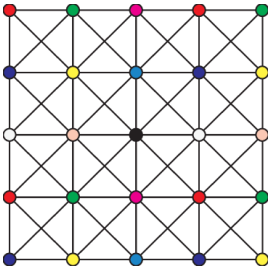
Le coloriage de graphes avec des couleurs différentes pour les nœuds, les branches ou les surfaces fait partie des problèmes NP, NP-Complet et NP-Difficile selon les cas. Les deux premiers cas nécessitant un nombre de couleurs dépendant du nombre maximum de connexions entre éléments du graphe et le dernier cas, relevant du coloriage de cartes dans des couleurs adjacentes différentes qui n'en nécessite que quatre au maximum, grâce à la démonstration informatique du théorème des quatre couleurs en 1976 par Kenneth Appel et Wolfgang Haken.

---

[217] Source de l'illustration.

[218] Voir Is protein folding problem really a NP-complete one ? First investigations, 2013 (31 pages).

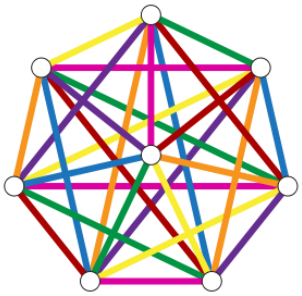
coloriage de graphes



nœuds

coloriage avec k couleurs : **NP-complet**
trouver le nombre minimum de couleurs : **NP-difficile**

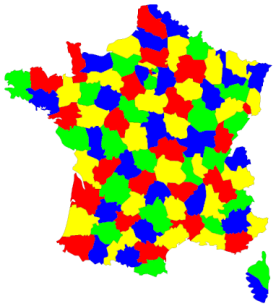
allocation de fréquences radio télécoms



segments

coloriage avec k couleurs : **P**
coloriage optimum : **NP-difficile**

allocation de fréquences de fibres optiques multimodes



zones

déterminer si coloriage possible avec 3 couleurs : **NP-complet**
coloriage avec 4 couleurs : **P**

définition de zones de couverture d'antennes de réseaux télécoms
allocation de fréquences micro-ondes dans des réseaux de qubits supraconducteurs

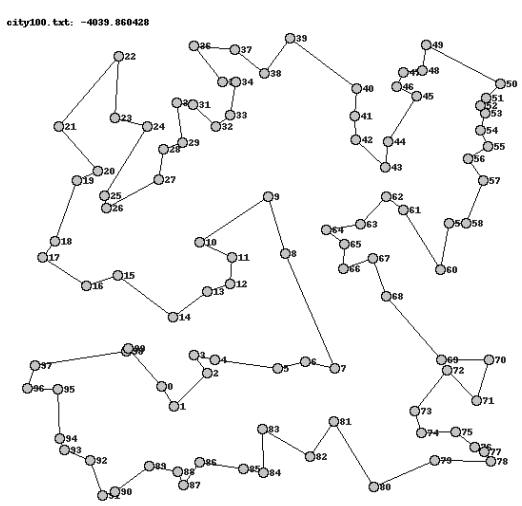
- Le coloriage de **nœuds** de graphes a des applications dans le placement d'antennes mobiles et dans l'allocation de registres mémoires pour un compilateur. Le problème est NP-Complet pour sa résolution et NP-Difficile pour trouver sa solution optimale.
- Celui des **branches** a des applications dans l'allocation de fréquences de réseaux de fibres optiques multimodes. Il permet aussi d'optimiser le placement d'objets ou personnes en fonction de leur compatibilité ou incompatibilités. Le coloriage optimum est un problème NP-Difficile.
- Celui des **zones** peut servir à définir les zones de couvertures d'antennes radio mobiles ou de satellites de télécommunications. Il peut même servir à allouer les fréquences micro-ondes d'activation de qubits supraconducteurs. Le coloriage avec trois couleurs est un problème NP-Complet.

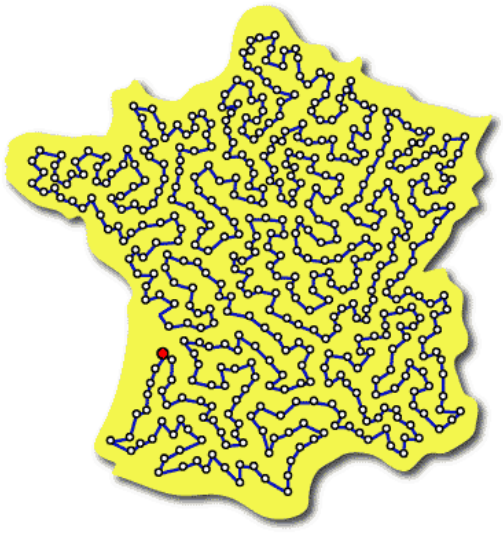
D'une manière générale, de nombreuses classes de problèmes C ont une sous-classe C-Complet et C-Difficile. Un problème est C-Difficile s'il existe un type de réduction des problèmes de la classe C vers ce problème. Si le problème C-Difficile fait partie de la classe C, alors il est dit "C-Complet"[219].

NP Difficile : concerne les problèmes d'optimisation où l'on recherche un minimum ou un maximum avec une grande combinatoire. Un problème est NP-Difficile si tous les problèmes NP-Complets peuvent se réduire par simplification polynomiale à ce problème. C'est le cas de la résolution du **problème du voyageur du commerce** où l'on doit tester une grande combinatoire de parcours pour trouver celui qui est réalisé le plus rapidement pour passer via un nombre déterminé de villes. Il faut alors tester toutes les solutions.

[219] Pour en savoir plus, voir notamment Complexity Theory Part I (81 slides) et part II (83 slides), qui fait partie d'un cours de Stanford sur les théories de la complexité, Calculabilite et Complexite - Quelques resultats que je connais d'Etienne Grandjean de l'Université de Caen, 2017 (43 slides) ainsi que cette vidéo d'Olivier Bailleux (2017, 20 minutes). Elle est très claire mais vous serez très forts si vous arrivez à suivre et à tout assimiler ! L'auteur précise qu'il faut la regarder plusieurs fois en faisant souvent une pause !

problème du voyageur de commerce





comment parcourir un graphe en un temps minimum, sans passer deux fois au même endroit et qui se termine au point de départ : **NP-difficile**

Si un voyageur de commerce doit traverser 125 villes en moins de 30 jours, s'il existe une solution qui fonctionne dans ce laps de temps, alors le problème est NP. Mais rien ne dit que l'on a trouvé toutes les solutions ! La résolution du problème en-dessous d'un temps de parcourt arbitraire avec un retour au point de départ est un problème NP-complet. C'est ce que l'on appelle un circuit hamiltonien : un chemin parcourant un graphe passant une fois et une seule par chacun des nœuds et revenant à son point de départ. La détermination du temps de parcours le plus court est NP-difficile. L'algorithme de force brute pour le résoudre a un temps qui dépend de N! , N étant le nombre de nœuds du réseau. Le temps optimum connu est $N^2 * 2^N$. Le problème est difficile à résoudre au-delà de 20 étapes[220] !

La classe des problèmes NP-Difficile contient aussi nombre de jeux de **Nintendo** comme Super Mario Bros, La Légende de Zelda et Pokemon[221]. Le calcul quantique ne permettrait pas de solutionner les plus complexes des problèmes NP-difficile.

PSPACE : est la classe des problèmes qui peuvent être résolus en espace polynomial sur une machine déterministe. NPSPACE est la classe des problèmes pouvant être résolus en espace polynomial sur une machine non déterministe. NPSPACE = PSPACE selon le théorème de Savitch.

EXPTIME : est la classe des problèmes décidés en temps exponentiel par une machine déterministe. Précisément, le temps de calcul de ces problèmes est une puissance de 2 exprimée sous forme d'un polynome de N, N étant le niveau de complexité du problème. Ils sont intractables avec des machines traditionnelles.

---

[220] Voir le site The Traveling Salesman Problem qui donne quelques exemples de tels problèmes comme le parcours de tous les 49 687 pubs anglais ou des 49 603 lieux touristiques aux USA.

[221] Voir Classic Nintendo Games are (Computationally) Hard, 2012 (36 pages).

Certains de ces problèmes peuvent être convertis en problèmes traitables de manière polynomiale par des ordinateurs quantiques. Les jeux d'échecs et de Go sur grille de taille arbitraire font partie de cette catégorie. Dans les grilles à taille limitée, l'effet exponentiel a des limites. Celles-ci ont été dépassées pour les échecs par Deep Blue en 1996 et pour le jeu de Go par AlphaGo de DeepMind en 2016 et 2017.

NEXPTIME : est la classe des problèmes décidés en temps exponentiel par une machine non-déterministe et avec un espace mémoire illimité.

EXPSPACE : est la classe des problèmes qui peuvent être résolus en espace exponentiel. Autant dire qu'ils sont difficiles d'accès aux machines d'aujourd'hui et même de demain.

Les quatre classes précédentes (PSPACE, EXPTIME, NEXPTIME, EXPSPACE) ne correspondent pas à des problèmes pratiques faciles à identifier dans la vie courante. En tout cas, je n'en ai pas trouvé dans la littérature. Ils couvrent dans l'ensemble les problèmes de prévision de comportement de systèmes ultra-complexes avec de fortes interactions. S'il est possible que la modélisation du repliement d'une protéine soit un problème NP, quelle serait la classe du problème de simulation du fonctionnement d'une cellule vivante entière, voir d'un organisme multicellulaire ? Les interactions sont tellement nombreuses au niveau atomique, moléculaire et cellulaire que la classe de ce genre de problème est probablement située bien au-delà de NP-Difficile.

Il existe bien d'autres classes de complexité de problèmes que je ne vais pas décrire ici : EXP, IP, MIP, BPP, RP, ZPP, SL, NC, AC0, TC0, MA, AM et SZK ! Elles sont listées dans le site Complexity Zoo qui inventorie le zoo des classes de complexité de problèmes. Il semble il y en avoir plus d'une centaine[222].

[222] Pour en savoir plus sur le sujet des théories de la complexité, vous pouvez notamment parcourir le très documenté Computational Complexity A Modern Approach, de Sanjeev Arora et Boaz Barak de l'Université de Princeton, 2007 (489 pages).

Classes de complexité quantiques

On peut y ajouter une classification de problèmes par niveau de difficulté pour les ordinateurs quantiques, la correspondance avec les classes *ci-dessus* étant encore un problème… non entièrement résolu ! La classification est différente car les ordinateurs quantiques peuvent paralléliser les traitements tandis que les ordinateurs classiques qui sont assimilables à des machines de Turing ne peuvent le faire.

Il faudrait y ajouter une contrainte connue des ordinateurs quantiques : leur temps de cohérence qui est non seulement fini mais relativement court. Il contraint par la durée le nombre de portes quantiques que l'on peut enchaîner pour résoudre un problème. Et ce temps est inférieur au dixième de seconde pour un ordinateur quantique à base de supraconducteurs. C'est une contrainte que n'ont pas les ordinateurs traditionnels.

On peut y faire tourner un algorithme jusqu'à plus soif. Un problème trop complexe pour un ordinateur quantique serait donc aussi un problème qui nécessiterait d'enquiller un nombre de portes quantiques trop grand pour s'exécuter plus rapidement que le temps de cohérence.

PH : est la classe des problèmes qui peuvent être résolus par des ordinateurs traditionnels du présent et, surtout, par tout ordinateur traditionnel du futur ! PH signifie "Polynomial Hierarchy".

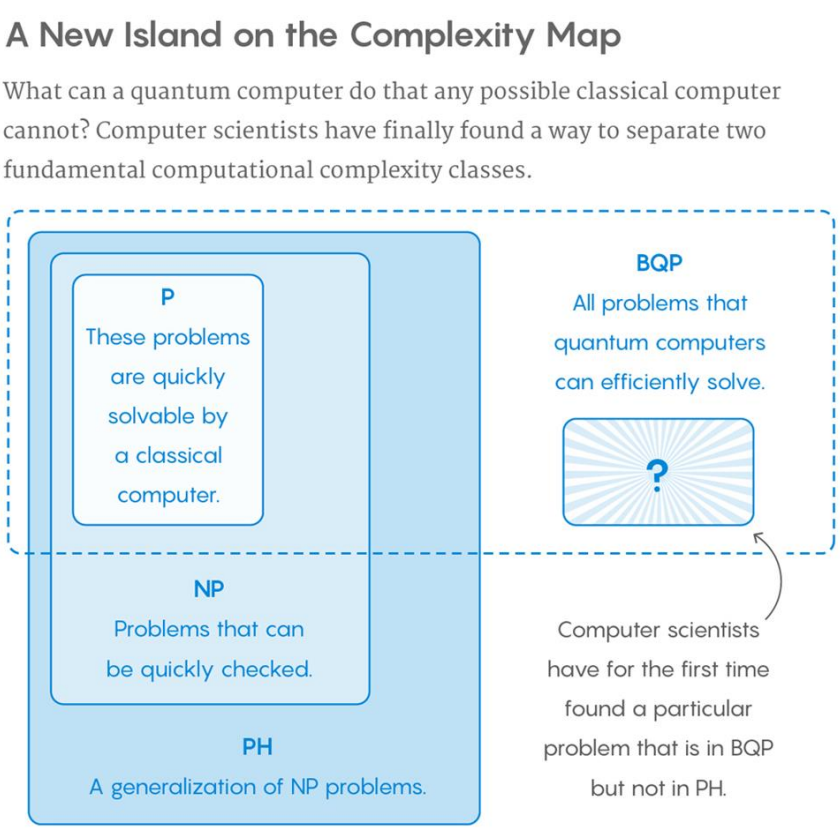
BQP : définit une classe de problème qui est traitable en temps polynomial sur un ordinateur quantique avec un taux d'erreur contraint. Cela peut dans certains cas correspondre à des problèmes P. La classe a été définie en 1993, au moment où apparaissaient les premiers algorithmes quantiques.

En débat, le fait de savoir si la classe BQP est véritablement différente de la classe P ! Il est déjà démontré que la classe P des problèmes polynomiaux est dans BQP. Mais est-ce que NP est dans BQP ? A priori non. Mais c'est difficile à prouver de manière générique. Mais on sait déjà que BQP est dans NP. C'est là que l'on trouve une bonne part des meilleurs algorithmes quantiques comme ceux de Grover et de Shor.

Le point clé est de trouver des algorithmes qui font partie de BQP (traitables en quantique) et qui ne sont pas dans PH (traitables avec n'importe quelle architecture traditionnelle du présent et du futur). Cette incertitude a été levée très récemment[223]. Les deux logiciens ont trouvé des algorithmes à base d'oracles (boites noires) qui sont dans BQP mais pas dans PH. Donc, qui ont un temps de résolution polynomial sur ordinateur quantique mais qui reste exponentiel sur ordinateur classique. Alea jacta est ! Mais je ne vais pas prétendre avoir compris cette belle démonstration !

[223] Voir Finally, a Problem That Only Quantum Computers Will Ever Be Able to Solve de Kevin Hartnett, 2018, qui fait référence à Oracle Separation of BQP and PH des Israéliens Ran Raz et Avishay Tal, mai 2018 (22 pages), présenté dans la conférence Electronic Colloquium on Computational Complexity. C'est la source de l'illustration de cette page.

Qu'en est-il au passage d'une éventuelle différence de complexité de problèmes gérable avec des ordinateurs quantiques à portes universelles vs les ordinateurs à recuit quantique de style D-Wave ? D'après plusieurs chercheurs[224], il n'y en aurait pas. Divers théorèmes montrent qu'un problème qui peut être résolu avec des portes quantiques universelles peut aussi l'être avec une architecture de recuit quantique à la D-Wave et réciproquement et dans un ordre de grandeur de temps équivalent.



QMA (pour Quantum Merlin Arthur) définit une classe de problèmes qui est vérifiable en temps polynomial sur un ordinateur quantique avec une probabilité supérieure aux 2/3. C'est l'analogue quantique de la classe de complexité "traditionnelle" NP. La classe QMA contient les classes P, BQP et NP[225]. Comme la classe NP, la classe QMA a deux sous-classes, QMA Complet et QMA Difficile. En pratique, ce sont des problèmes difficiles à résoudre avec des ordinateurs quantiques.

Malheureusement, la littérature sur le sujet n'en décrit pas la nature ou ne fournit pas d'exemples. C'est bien dommage pour ceux qui apprécient d'adopter un sens pratique des choses !

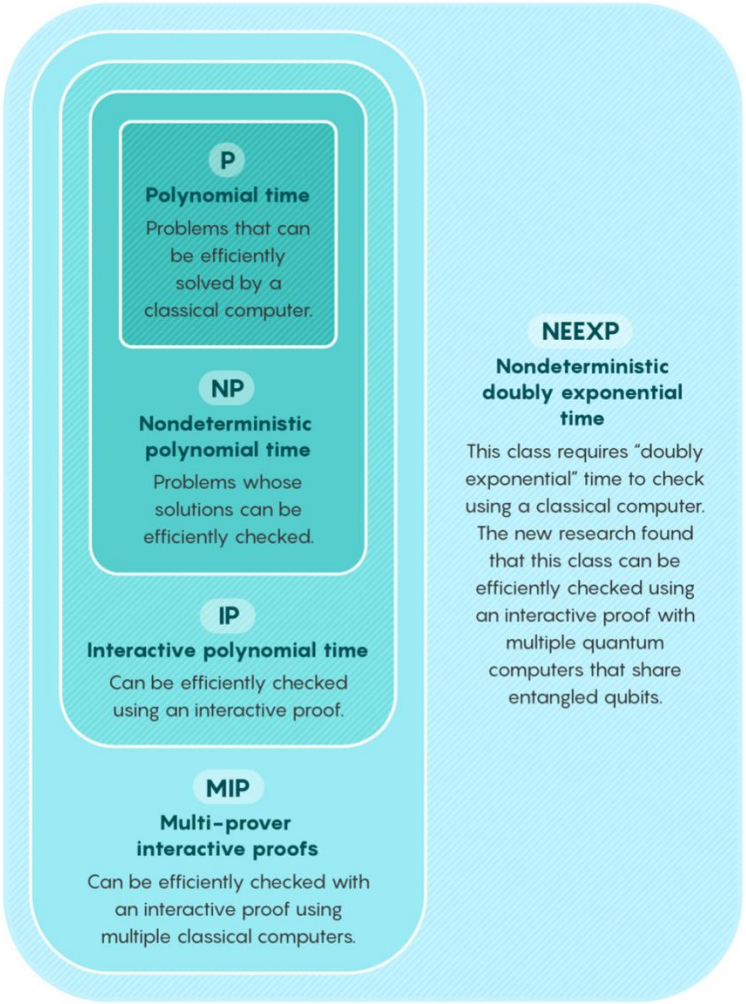
QCMA est une classe hybride entre QMA et NP. La preuve est fournie en temps classique polynomial mais la résolution relève du niveau QMA et est réalisée de manière quantique. Je n'ai pas bien compris et ce n'est pas bien grave.

Nombre de publications relèvent les limitations des algorithmes et ordinateurs quantiques. Un problème BQP qui n'est pas dans PH donne l'avantage au quantique. Mais des problèmes intractables exponentiels pour lesquels l'amélioration apportée par le quantique n'est que racinaire (racine carrée du temps classique) ne modifie pas leur nature exponentielle.

[224] Voir Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation de Dorit Aharonov, Wim van Dam et Julia Kempe (du CNRS), 2008 (30 pages).

[225] Voir QMA-complete problems de Adam Bookatz, 2013 (18 pages).

C'est ce que relève Scott Aaronson[226]. Les problèmes NP Complets et au-delà restent inaccessibles aux ordinateurs quantiques. La force brute a des limites que même le calcul quantique ne permet pas de dépasser en théorie ! Cela explique en partie la difficulté à créer des algorithmes quantiques efficaces.



Enfin, **NEEXP** est une classe de problèmes qui requiert un temps de calcul doublement exponentiel pour sa résolution. Des travaux récents démontrent qu'un résultat peut être vérifié avec plusieurs ordinateurs quantiques avec des qubits intriqués. On est bien avancé car cela ne permet pas pour autant de résoudre les problèmes de ce type[227] !

Il faut prendre en compte le fait que certains problèmes sont indécidables, à savoir qu'ils ne peuvent pas être résolus par un algorithme, quel que soit le temps dont on dispose[228].

Il en va ainsi de la détermination de l'arrêt d'un programme dans une machine de Turing. En d'autres termes, il n'existe pas de programme permettant de savoir si n'importe quel programme écrit dans un langage de programmation courant va s'arrêter ou boucler pendant une durée infinie.

Dans le même ordre, le **théorème de Rice** démontre qu'aucune propriété non triviale d'un programme ne peut être décidée de manière algorithmique. Tout cela pour dire qu'il n'existerait pas de méthode automatique de détection de bugs dans un programme ou de certification qu'il s'exécute bien. Il existe cependant des méthodes de preuve formelle permettant de certifier l'exécution de programmes spécifiques.

---

[226] Voir The Limits of Quantum Computers (16 pages) ainsi que dans NP-complete Problems and Physical Reality (23 pages).

[227] Voir NEEXP in MIP* de Anand Natarajan et John Wright, 2019 (122 pages) et Computer Scientists Expand the Frontier of Verifiable Knowledge, 2019.

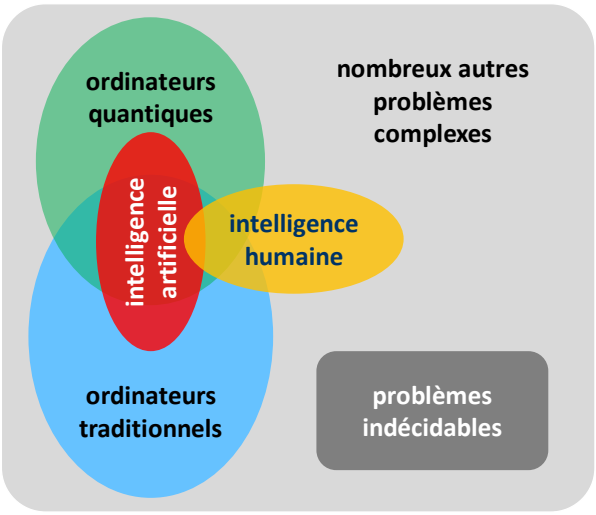
[228] Comme vu dans Complexite algorithmique de Sylvain Perifel, 2014 (430 pages).

Cela passe par l'utilisation de spécifications formelles des programmes qui servent de référence pour l'évaluation de leur bon fonctionnement. C'est déjà très utilisé, sans quantique, dans l'informatique industrielle et dans les systèmes critiques comme dans l'aérospatial.

version plus simple

conséquence : l'Homme ne pourra jamais résoudre tous les problèmes !

la toute puissance (de l'IA ou autre) est un mythe

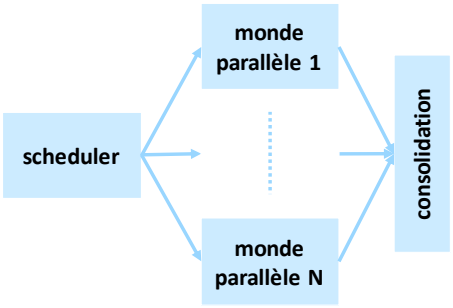


Contournements de science-fiction

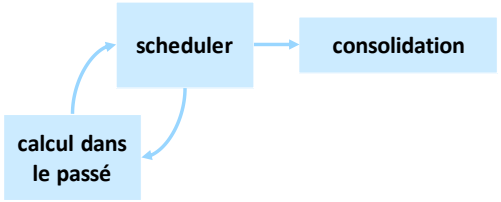
Une autre barrière semble infranchissable aux ordinateurs de tout type : la barrière du temps de Planck, qui est de 10^{-43} secondes. Il serait impossible de réaliser un calcul élémentaire en moins de temps que ce temps de Planck. C'est une limite de la loi de Moore en plus de la barrière de la chaleur de Landauer qui définit la quantité d'énergie minimale nécessaire pour modifier une information. Mais cette barrière temporelle de Planck est loin d'être atteinte. Les ordinateurs à base de processeurs CMOS sont limités à une fréquence d'horloge de 4 à 6 GHz, donc $2*10^{-10}$ secondes.

Avec un processeur photonique pouvant atteindre théoriquement 100 GHz, on en serait à 10^{-11} secondes mais ceux-ci sont très difficiles à réaliser. Et cela donne de la marge, 10^{32}, avant d'atteindre la barrière temporelle de Planck.

solutions Shadokiennes pour accélérer les calculs



paralléliser les calculs dans des mondes parallèles en nombre exponentiel



paralléliser les calculs en remontant dans le temps autant de fois que nécessaire

Autre solution pour transcender les calculateurs quantique d'architecture connue et qui relève de la science-fiction : faire des calculs dans des mondes parallèles pour tester toutes les solutions à un problème complexe et consolider les résultats obtenus. C'est l'application du scénario de la série TV "Fringe" au calcul quantique.

Il va sans dire que pour que cela ait un intérêt, il faudrait pouvoir faire cela dans un nombre exponentiel d'univers parallèles. Il faudrait donc aussi que la méthode soit "scalable". Si on ne pouvait l'utiliser que dans un nombre limité de mondes parallèles, cela n'aurait pas un grand intérêt !

On peut aussi imaginer remonter dans le temps pour refaire les calculs plusieurs fois et consolider également les résultats. Dans ces deux scénarios shadokiens, l'une des difficultés parmi d'autres serait de créer un goulot d'étranglement dans la consolidation des résultats. Il faudrait un bus de données suffisamment rapide pour absorber une grande quantité d'information. On pourrait d'ailleurs se demander s'il n'est pas possible de réduire l'un des cas à l'autre voir de les combiner. Ainsi, si on calcule dans le passé, on peut choisir de le faire dans des passés simultanés ou dans des passés différents, histoire d'éviter de trop encombrer les passés.

Les deux méthodes pourraient peut-être aussi être opérantes avec des ordinateurs traditionnels. Mais l'ajout du quantique rend la chose plus crédible, si l'on peut dire. Revenir dans le passé ou se déplacer instantanément dans des mondes parallèles est probablement bien plus aisé avec des quantums.

Ce sont évidemment des hypothèses qui ne relèvent pas du domaine du possible, même en tortillant les lois de la physique au gré de ses désirs les plus fous. Scott Aaronson évoque pourtant quelques-uns de ces scénarios[229]. En pratique, au mieux peut-on tirer partie de la vitesse supraluminique de connexion entre qubits intriqués, qui peut servir dans certaines circonstances que nous aurons l'occasion d'explorer, mais qui n'accélèrent pas les calculs pour autant.

L'intractabilité des problèmes NP Complets et QMA pourrait faire partie des principes de base de la physique et rester des limites infranchissables. Jusqu'à ce que l'on trouve une parade astucieuse insoupçonnée ! Une AGI ou intelligence artificielle générale pourrait-t-elle le faire ? Cela devient un problème récursif… !

En attendant, les recherches vont surtout bon train pour permettre la création d'ordinateurs quantiques avec un grand nombre de qubits dotés de caractéristiques opérationnelles clés comme un long temps de cohérence et des taux d'erreurs aussi faibles que possibles. C'est le point de passage obligé pour pouvoir traiter des problèmes exponentiels de grande taille dans des applications métier courantes.

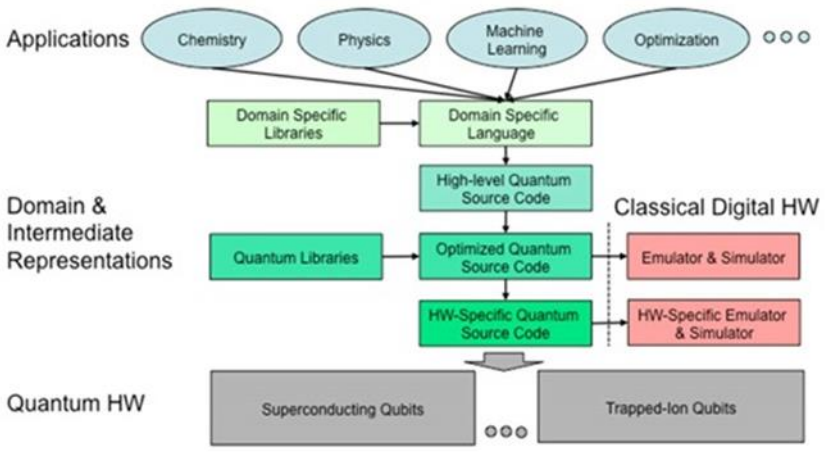
[229] Dans NP-complete Problems and Physical Reality, 2005 (23 pages).

Outils de développement

Après avoir fait le tour de quelques algorithmes quantiques de base puis des théories de la complexité qui permettent de détourer vaguement l'univers du possible pour le calcul quantique, il nous faut maintenant explorer les outils logiciels de l'informatique quantique. Comme pour tout le reste, c'est un monde entièrement nouveau et avec des paradigmes très différents par rapport à la création de logiciels classiques. On peut cependant y retrouver ses petits.

Qui dit algorithme dit programmation, langages de programmation et environnements de développement.

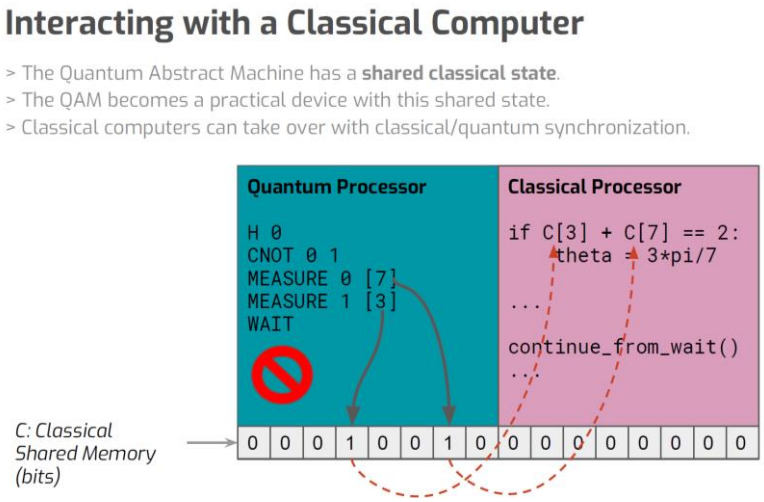
Comme l'indique le schéma *ci-contre* (dont j'ai malheureusement perdu la source…), les logiciels quantiques sont organisés en couches superposées avec en partant du bas, les qubits physiques suivi du langage machine spécifique permettant de les piloter à base niveau.



Suit le "high level quantum source code" qui est en fait une sorte de macro-assembleur, pouvant tirer parti de bibliothèques de fonctions avec des algorithmes prêts à l'emploi (transformée de Fourier quantique, etc.) et enfin, d'éventuels langages de haut niveau adaptés à des besoins métiers spécifiques.

Dans les couches basses entre langage machine et le macro-assembleur se trouvent des fonctions de conversion des portes quantiques en portes quantiques universelles supportées par l'ordinateur quantique ainsi que les systèmes de codes de correction d'erreur qui peuvent demander l'exécution d'un grand nombre de portes quantiques.

Un compilateur quantique va aussi faire de l'optimisation en supprimant par exemple les séquences de portes quantiques qui ne changent pas l'état d'un qubit, comme deux portes unitaires de Hadamard ou X (NOT) consécutives. Il va aussi les arranger pour minimiser le nombre d'étapes de portes quantiques de la solution.



Les architectures logicielles du quantique sont généralement hybrides et permettent de contrôler un ordinateur quantique à partir de logiciels procéduraux assez traditionnels. Ils gèrent côte à côte l'exécution de logiciels classiques et de logiciels quantiques et manipulent de la mémoire traditionnelle en plus de celle des qubits, comme illustré dans le schéma *ci-dessus* originaire de la startup Rigetti.

L'ordinateur classique sert au minimum à contrôler l'exécution des algorithmes quantiques, ne serait-ce que pour déclencher les portes quantiques au bon moment, de manière séquentielle. Il peut aussi déclencher plusieurs algorithmes quantiques les uns après les autres. On peut imaginer qu'une application fera appel à plusieurs algorithmes quantiques et pas un seul.

Les classes d'outils de développement

On peut identifier quelques grandes classes d'outils de création de logiciels quantiques : les outils de programmation graphiques, les langages de scripting, les langages intermédiaires, les langages machine et les compilateurs.

Outils de programmation graphique

Ils permettent de spécifier la séquence des portes quantiques à exploiter pour créer des algorithmes directement exploitables dans des ordinateurs quantiques du cloud ou des simulateurs HPC dans le cloud. Ces outils peuvent faire fonctionner et visualiser l'état des qubits lorsque leur nombre est raisonnable.

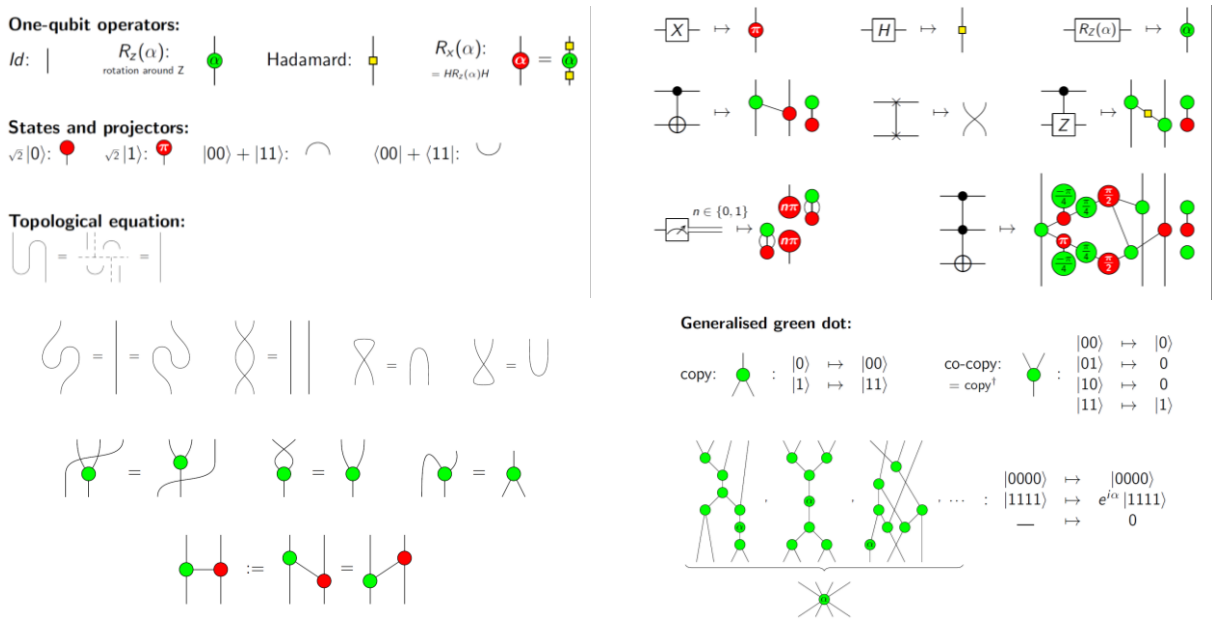
Ils permettent de vérifier la faisabilité de l'exécution de l'algorithme.

L'un des exemples de tels outils est l'IBM Q Experience ou IBM Composer qui est proposé dans le cloud depuis 2016 (*ci-contre*).

On y trouve aussi des simulateurs graphiques de qubits avec lesquels on peut se faire la main pour comprendre comment enchaîner les portes quantiques sur quelques qubits et visualiser le résultat visuellement.

C'est notamment le cas de QuantumPlayground originaire de Google et de l'outil open source Quirk, ce dernier pouvant simuler jusqu'à 16 qubits. Il fonctionne en ligne et on peut le télécharger pour l'exécuter sur son propre ordinateur en local. Sa capacité n'est limitée que par la RAM dont vous disposez. Voici ci-dessous, un exemple de transformée de Fourier quantique réalisée en Quirk.

Enfin, ajoutons à cette catégorie d'outils un cas particulier, celui du **ZX-calculus**. C'est un langage de programmation graphique qui utilise des règles de composition topologiques. Il a été créé en 2008 par Bob Coecke et Ross Duncan[230]. Il permet de visualiser les modifications apportées à un jeu de qubits. Il s'appuie sur des transformations applicables à la représentation géométrique des portes quantiques qui permettent de simplifier les modèles. Il est notamment utile pour programmer un ordinateur quantique en MBQC (measurement base quantum computing).



Il est associé à un outil de développement, **Quantomatic**, créé par Aleks Kissinger et Vladimir Zamdzhiev de l'Université d'Oxford[231]. Les contributeurs des travaux autour du ZX-Calculus comprennent des chercheurs du Loria, un laboratoire de recherche situé à Nancy[232].

---

[230] Voir Interacting Quantum Observables: Categorical Algebra and Diagrammatics de Bob Coecke1 et Ross Duncan, 2009 (80 pages).

[231] Voir Quantomatic: A Proof Assistant for Diagrammatic Reasoning, 2015 (11 pages).

[232] Voir Completeness of the ZX-Calculus par Renaud Vilmart, 2018 (123 slides) qui est la source des illustrations et Completeness of the ZX-Calculus par Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart (73 pages) qui les explique.

Langages de scripting

Ils permettent de programmer en mode texte la structure des portes quantiques d'une solution. Ces outils permettent d'associer de la programmation classique avec enchainement de fonctions quantiques conditionnées par l'état de variables en mémoire classique.

On compte deux principaux types de langages quantiques : les langages impératifs et les langages fonctionnels.

- Les **langages impératifs** sont les langages de programmation procéduraux (objets ou pas) où l'on décrit les algorithmes pas à pas. On y range les langages habituels tels que C, C++, PHP ou Java.
- Les **langages fonctionnels** sont utilisés en définissant des fonctions diverses qui sont appelées de manière ad-hoc par le programme. Les boucles (for, while) sont remplacées par la récursivité de fonctions et il n'y a pas de variables modifiables. Ils permettent d'utiliser des types de données abstraits de haut niveau manipulés par les fonctions. L'ensemble est plus concis.

Table 1: A selection of some quantum programming languages.

Name	Style	Notes
QCL	Imperative	Has classical sublanguage, multiple high-level programming features.
qGCL	Imperative	Emphasis on algorithm derivation and verification.
LanQ	Imperative	Full operational semantics, proven type soundness.
Quipper	Functional	Focus on scalability, plans to include linear types for static checks (currently done at run-time).
QPL	Functional	Statically typed, denotational semantics in terms of CPOs of superoperators.
QML	Functional	Linearly typed, focused on weakening - not contraction. Quantum control and quantum data.
Qumin	Functional	Two sublanguages (untyped and linearly typed). Focus on ease of use and clean, functional style of programming.

source du tableau : Qumin, a minimalist quantum programming language, 2017 (34 pages).

Une bonne part des langages de programmation traditionnels peuvent être exploités en programmation impérative ou fonctionnelle, notamment dès lors qu'ils disposent de pointeurs de fonctions ou qu'ils supportent une logique événementielle. Dans une certaine mesure, JavaScript et Jquery peuvent-être utilisés comme des langages fonctionnels via leurs *call-back functions*. C'est aussi le cas du C++.

Chez les fournisseurs d'ordinateurs quantiques tels qu'IBM ou Rigetti, deux types de langages sont parfois proposés : un langage intermédiaire (Quil chez Rigetti) et un langage de plus haut niveau sous la forme d'extensions du langage de programmation Python (pyQuil chez Rigetti). Un outil de conversion converti le second dans le premier langage.

Langages machine

Ce sont les langages de plus bas niveau de programmation de l'ordinateur quantique, qui programment l'initialisation des qubits et l'activation des portes universelles qui agissent dessus puis la mesure des résultats. Ils sont généralement spécifiques à chaque type d'ordinateur quantique, voir à chaque ordinateur quantique.

Compilateurs

Les compilateurs exploitent le contenu des précédents outils, et surtout des langages de scripting, pour générer la séquence de contrôle des portes physiques de l'ordinateur quantique cible en langage machine, intégrant au passage les fonctions de corrections d'erreurs quantiques (QEC). Ces compilateurs vont transformer les portes logiques utilisées dans la programmation en portes physiques universelles exploitées par l'ordinateur quantique.

Ils vont aussi calculer les temps d'activation des portes et vérifier que l'accumulation de ces temps d'activation est inférieure au temps de cohérence des qubits de l'ordinateur cible.

Comme l'aASM d'Atos, ces outils de compilation peuvent être "multiplateformes" et supporter différentes architectures d'ordinateurs quantiques, au moins universels. La compilation n'est pas la même sur des ordinateurs quantiques topologiques. Ces compilateurs utilisent des langages de programmation quantiques. Les langages de programmation quantique sont généralement capables d'associer de la programmation procédurale classique avec de la programmation de registres et portes quantiques. Ils permettent de gérer parallèlement de la mémoire classique à des registres quantiques. Ils proviennent de la recherche ou de concepteurs d'ordinateurs quantiques comme IBM, Microsoft, Rigetti et D-Wave[233].

Emulateurs

Les émulateurs, parfois appelés à tort simulateurs, sont des outils logiciels qui émulent l'exécution d'algorithmes quantiques sur des ordinateurs traditionnels. Leur capacité est étroitement liée à la quantité de mémoire disponible[234]. Sur un laptop avec 16 Go de mémoire, on peut simuler environ 20 qubits.

Il ne faut pas les confondre avec les simulateurs quantiques, le nom donné aux ordinateurs quantiques analogiques à variables continues.

On compte dans ce domaine des outils comme **Quirk** et **Quantum Inspire**, ce dernier étant proposé par QuTech. **Quantum Circuit Simulator** est pour sa part disponible sous Android dans Google Play.

---

[233] Voir cette présentation qui décrit bien quelques-unes des tâches réalisées par des compilateurs quantiques : Opportunities and Challenges in Intermediate-Scale Quantum Computing de Fred Chong, 2018 (34 slides).

[234] Voir la liste des outils de simulation d'algorithmes quantiques sur https://quantiki.org/wiki/list-qc-simulators.

JÜLICH QUANTUM COMPUTER SIMULATOR (JUQCS)

JUQUEEN, Jülich, Germany

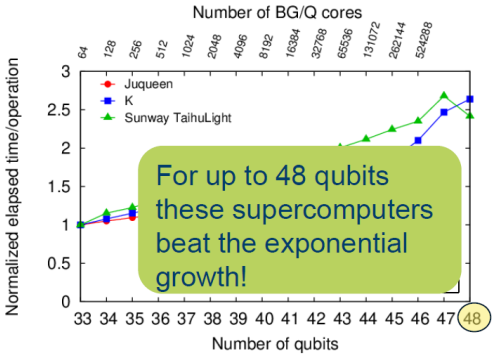

K, Kobe, Japan


Sunway TaihuLight, Wuxi, China

- N qubits → $|\psi\rangle$ is a superposition of 2^N basis states
- Represent a quantum state with 2 bytes → N qubits requires at least 2^{N+1} bytes of memory → new world record in 2018

N	Memory
27	256 MB
39	1 TB
48	0.5 PB
49*	1 PB

* Could be run on Trinity, Los Alamos



Outils de mise au point

Les logiciels quantiques ne sont pas faciles à déboguer ! Cela va certainement requérir de nouveaux outils de mise au point. Pour l'instant, ils sont intégrés dans les environnements et outils de développement proposés. On peut déboguer un algorithme pas à pas avec un simulateur de logiciel quantique tournant sur ordinateur traditionnel, pour comprendre comment évolue l'état des qubits étape par étape.

Lorsque les algorithmes tourneront sur des ordinateurs quantiques dépassant la suprématie quantique et impossibles à émuler sur ordinateur traditionnel, il faudra passer par d'autres moyens comme l'arrêt d'un algorithme quantique à une étape d'un programme, suivi de la lecture - probabiliste et répétée plusieurs fois – de l'état intermédiaire des qubits.

Ressources de calcul dans le cloud

Un bon nombre d'ordinateurs quantiques sont disponibles dans le cloud :

- **IBM** Q Experience propose l'accès ouvert à 14 qubits et à 20 qubits à des clients privés.
- **Alibaba** propose son Quantum Computing Cloud Service avec jusqu'à 11 qubits supraconducteurs depuis début 2018. L'ordinateur provient de la Chinese Academy of Sciences Innovative Center in Quantum Information and Quantum Physics de Shanghai.
- **Rigetti** propose son Quantum Cloud Services avec 19 qubits supraconducteurs. Ils prévoient de passer à 128 qubits.
- **D-Wave** propose l'accès à 1000 qubits à recuit quantique dans son programme Leap.

- **IonQ** prévoit de mettre à disposition un ordinateur quantique à ions piégés de 79 qubits dans le cloud courant 2019.

Le "blind computing" est une appellation qui recouvre l'usage d'ordinateurs quantiques dans le cloud de manière sécurisée. Le principe consiste à préparer les traitements de manière quantique au point de départ et de l'envoyer par une liaison quantique par téléportation à l'ordinateur quantique à distance.

C'est un peu l'équivalent en quantique du chiffrage homomorphe utilisé dans le machine learning. Une manière de gérer la confidentialité des traitements est de partitionner le traitement sur plusieurs ordinateurs quantiques[235].

Outils de développement quantiques issus de la recherche

Voici un aperçu des principaux langages quantiques créés à ce jour, avec tout d'abord les langages indépendants des architectures matérielles et qui sont souvent issus de laboratoires de recherche.

Ils présentent l'inconvénient de ne pas être généralement reliés à des offres d'ordinateurs quantiques dans le cloud. Ils ont par contre souvent un certain privilège d'antériorité par rapport aux outils de développement des fournisseurs d'ordinateurs quantiques que nous verrons plus loin. C'est bien normal puisque les chercheurs sont les premiers à s'embarquer dans les domaines émergents, bien avant les acteurs privés. Ils ont souvent conçu les premiers langages de programmation quantique à une époque où l'on n'arrivait à aligner qu'à peine un à deux qubits !

Ce sont un peu les Kernighan et Richie (créateurs du langage C) et Bjarne Stroustrup (créateur du C++) du domaine ! Vous remarquerez au passage qu'un bon nombre de ces langages provient d'Europe.

- **QCL** ou Quantum Computation Language dispose d'une syntaxe et des types de données proches de ceux du langage C.

  Ce langage est l'un des premiers qui soit pour la programmation quantique, créé en 1998 par le chercheur Autrichien **Bernhard Ömer** de l'Austrian Institute of Technology à Vienne. Il est décrit dans Structured Quantum Programming, 2009 (130 pages) qui positionne très bien les différences conceptuelles entre langages de programmation classiques et quantiques.

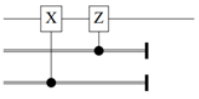
Classical concept	Quantum analogue
classical machine model	hybrid quantum architecture
variables	quantum registers
variable assignments	elementary gates
classical input	quantum measurement
subroutines	operators
argument and return types	quantum data types
local variables	scratch registers
dynamic memory	scratch space management
boolean expressions	quantum conditions
conditional execution	conditional operators
selection	quantum if-statement
conditional loops	quantum forking

Table 2.1: *Classical and quantum programming concepts*

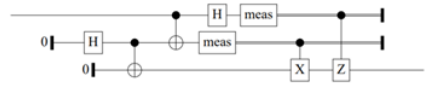
[235] Voir Universal blind quantum computation de Anne Broadbent, Joseph Fitzsimons et Elham Kashefi, 2008 (20 pages) et la présentation associée (25 slides), Blind quantum computing can always be made verifiable de Tomoyuki Morimae, 2018 (5 pages), Experimental Blind Quantum Computing for a Classical Client, 2017 (5 pages) et Blind Quantum Computation de Charler Herder (5 pages).

- **Q Language** est une extension du langage C++ qui fournit des classes permettant de programmer des portes quantiques (Hadamard, CNOT, SWAP, QFT pour transformée de Fourier quantique)[236].
- **QFC** et **QPL** sont deux langages fonctionnels définis par le Canadien Peter Selinger, le premier utilisant une syntaxe graphique et le second, une syntaxe textuelle[237].
- **QML** est un langage de programmation fonctionnel créé par les Anglais Thorsten Altenkirch et Jonathan Grattage[238].
- **qGCL** ou Quantum Guarded Command Language a été créé par Paolo Zuliani de l'Université de Newcastle[239].
- **Quipper** est un langage créé en 2013 qui s'appuie sur le langage classique Haskell, créé en 1990, auquel il fournit des extensions sous forme de types de données et de bibliothèques de fonctions[240]. Il manipule une version logicielle de QRAM, l'état des registres quantiques, indispensable à l'exécution d'algorithmes quantiques comme celui de Grover. Malgré tout cela, le langage ne semble pas avoir évolué depuis 2016. A noter que l'un de ses créateurs est le Français Benoît Valiron qui enseigne la programmation quantique à CentraleSupelec[241].

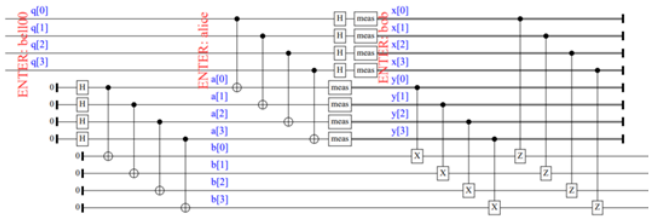
```
bob :: Qubit -> (Bit,Bit) -> Circ Qubit
bob b (x,y) = do
    b <- gate_X b `controlled` y
    b <- gate_Z b `controlled` x
    cdiscard (x,y)
    return b
```




```
teleport :: Qubit -> Circ Qubit
teleport q = do
    (a,b) <- bell00
    (x,y) <- alice q a
    b <- bob b (x,y)
    return b
```




```
teleport_generic_labeled :: (QData qa) => qa -> Circ qa
teleport_generic_labeled q = do
    comment_with_label "ENTER: bell00" q "q"
    (a,b) <- bell00_generic (qc_false q)
    comment_with_label "ENTER: alice" (a,b) ("a","b")
    (x,y) <- alice_generic q a
    comment_with_label "ENTER: bob" (x,y) ("x","y")
    b <- bob_generic b (x,y)
    return b
```



---

[236] Il est documenté dans Toward an architecture for quantum programming, 2003 (23 pages), avec comme coauteur un certain Stefano Bettelli du Laboratoire de Physique Quantique de l'Université Paul Sabatier de Toulouse.

[237] Ils sont décrits dans Towards a Quantum Programming Language, 2003 (56 pages).

[238] Voir A functional quantum programming language, 2004 (15 pages). Les principes sont bien décrits dans la présentation Functional Quantum Programming (151 slides).

[239] Voir Compiling quantum programs, 2005 (39 pages).

[240] Il est documenté dans An Introduction to Quantum Programming in Quipper, 2013 (15 pages). Sa création a été financée par l'IARPA, l'agence fédérale du renseignement américain qui finance de la R&D comme le fait la DARPA dans la défense. L'IARPA est rattachée au DNI (Director of national Intelligence), le coordinateur du renseignement US rattaché à la Maison Blanche et à qui reportent les 17 patrons du renseignement US dont ceux de la CIA et de la NSA.

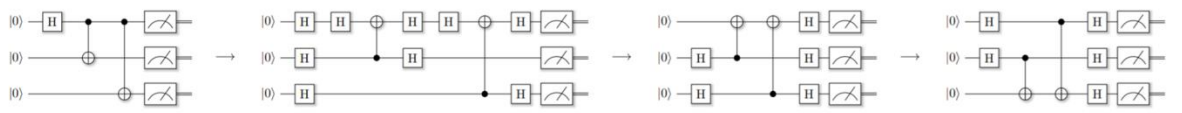
[241] Voir sa présentation Programmer un Ordinateur Quantique, 2017 (38 slides) et Quantum Computation Model and Programming Paradigm, 2018 (67 slides).

- **Scaffold** est un langage issu de l'Université de Princeton[242]. Il permet notamment de programmer du code traditionnel qui est ensuite transformé automatiquement en portes quantiques via sa fonction C2QG (Classical code to Quantum Gates). Scaffold peut notamment générer du QASM.

  En voici *ci-contre* un exemple de code, presque facile à comprendre ! Son développement a été également financé par l'IARPA.

```
// Pauli X, Pauli Y, Pauli Z, Hadamard, S, and T gates
gate X(qreg input[1]);
gate Y(qreg input[1]);
gate Z(qreg input[1]);
gate H(qreg input[1]);
gate S(qreg input[1]);
gate T(qreg input[1]);

// Daggered gates
gate Tdag(qreg input[1]);
gate Sdag(qreg input[1]);

// CNOT gate defined on two 1-qubit registers
gate CNOT(qreg target[1], qreg control[1]);

// Toffoli (CCNOT) gate
gate Toffoli(qreg target[1], qreg control1[1], qreg control2[1]);

// Rotation gates
gate Rz(qreg target[1], float angle);        //Arbitrary Rotation

// Controlled rotation
gate controlledRz(qreg target[1], qubit control[1], float angle);

// One-qubit measurement gates
gate measZ(qreg input[1], bit data);
gate measX(qreg input[1], bit data);

//One-qubit prepare gates: initializes to 0
gate prepZ(qreg input[1]);
gate prepX(qreg input[1]);

//Fredkin (controlled swap) gate
gate fredkin(qreg targ[1], qreg control1[1], qreg control2[1])
```

- **ProjectQ** est un langage de scripting l'ETH Zurich qui prend la forme d'un framework Python open source, diffusé sur GitHub depuis 2016. Il comprend notamment un compilateur convertissant le code quantique en langage C++ pour son exécution dans un simulateur quantique à processeur traditionnel.[243]. Lancé début 2017, il supporte les ordinateurs quantiques d'IBM via leur langage OpenQASM Ce qui est normal puisque l'ETH Zurich est partenaire de ce dernier, ainsi que la simulation sur ordinateur traditionnel via une implémentation développées en C++ qui supporte jusqu'à 28 qubits. ProjectQ est compatible avec OpenFermion de Rigetti et Google, cité plus loin.



(a) After decomposing. (b) After CNOT mapping. (c) After optimization. (d) After mapping to hardware.

Figure 5: Individual stages of compiling an entangling operation for the IBM back-end. The high-level Entangle-gate is decomposed into its definition (Hadamard gate on the first qubit, followed by a sequence of controlled NOT gates on all other qubits). Then, the CNOT gates are remapped to satisfy the logical constraint that controlled NOT gates are allowed to act on one qubit only, followed by optimizing and mapping the circuit to the actual hardware.

- **QWire** est un autre langage de programmation quantique, issu de l'Université de Pennsylvanie (Upenn)[244].
- **Qubiter** est un langage open source développé en Python utilisable au-dessus d'OpenQASM d'IBM et OpenFermion de Google. Il a donc une application industrielle plus directe que les langages cités ci-dessus. Il date aussi de 2017.

---

[242] Voir Scaffold: Quantum Programming Language, 2012 (43 pages).

[243] Voir ProjectQ: An Open Source Software Framework for Quantum Computing de Damian Steiger, Thomas Häner et Matthias Troyer, 2018 (13 pages) qui explique bien comment le compilateur optimise le code en fonction des portes disponibles dans l'ordinateur quantique.

[244] Voir QWIRE: A Core Language for Quantum Circuits (13 pages) et A core language for quantum circuits, 2017 (97 slides).

- **Qumin** est un langage quantique minimaliste conçu en Grèce en 2017[245]. Il est disponible en open source.
- **QuEST** (Quantum Exact Simulation Toolkit) est un simulateur quantique développé en langage C et supportant les APIs QUDA et les GPU de Nvidia, créé par des chercheurs de l'Université d'Oxford et open source. Le système permet de simuler de 26 à 45 qubits selon la mémoire RAM disponible, respectivement de 2 Go et 256 Go. Il date aussi de 2017.
- S'ensuivent des langages de mise en œuvre quantique du **lambda calculus**, conceptualisé par Alonzo Church et Stephen Cole Kleene pendant les années 1930. Traduction en langage naturel ? Ce type de calcul permet de résoudre des problèmes très complexes et de type NP-complet, la classe des problèmes vérifiable en temps polynomial et dont la résolution requiert un temps exponentiel sur ordinateurs classiques et potentiellement polynomial sur ordinateurs quantiques !
- **eQASM** est un langage machine quantique intermédiaire issu de Delft University et de sa filiale QuTech. Il s'intercale entre des outils de programmation de haut niveau (QASM) et l'ordinateur quantique. C'est un langage compilé, d'où le « e » pour « exécutable ». C'est le compilateur qui va gérer les dépendances vis-à-vis des spécificités de l'implémentation matérielle du processeur quantique utilisé. Les tests ont pour l'instant été réalisés avec un chipset supraconducteur à 7 qubits[246].

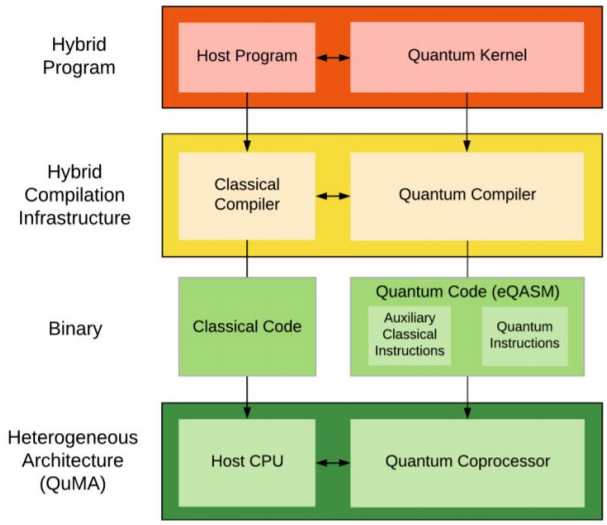


Fig. 1. Heterogeneous quantum programming and compilation model.

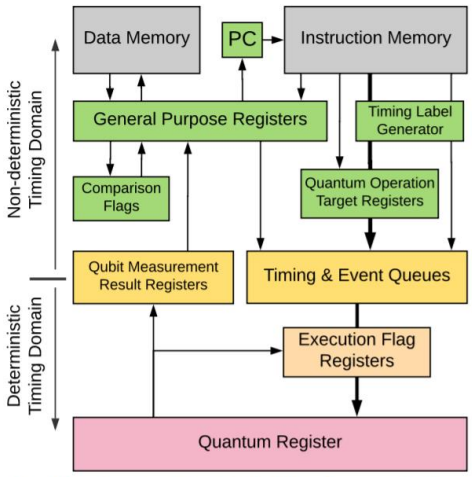


Fig. 2. Architectural state of eQASM. Arrows indicates the possible information flow. The thick arrows represent quantum operations, which read information from the modules passed through.

- Des chercheurs du laboratoire **EPiQC** (Enabling Practical-scale Quantum Computation) de l'Université de Chicago proposent un compilateur permettant d'améliorer jusqu'à un facteur 10 la vitesse et la fiabilité des ordinateurs quantiques[247].

---

[245] Voir Qumin, a minimalist quantum programming language, 2017 (34 pages).

[246] Voir eQASM: An Executable Quantum Instruction Set Architecture, mars 2019 (14 pages).

[247] Voir Research provides speed boost to quantum computers, avril 2019.

Là encore, il s'agit pour le compilateur de s'adapter à l'architecture matérielle sous-jacente. Leur vidéo explique le processus. L'équipe a notamment utilisé la bibliothèque TensorFlow de Google pour optimiser les paramètres de contrôle physiques des qubits.

Une bonne majorité des outils logiciels de la programmation quantique sont open source. Open source software in quantum computing, de Mark Fingerhuth, Thomas Babej et Peter Wittek, décembre 2018 (28 pages), fait un inventaire détaillé de ces différents outils et les jauge à l'aune des canons de l'open source, le tableau colorié ci-dessous en étant la synthèse.

On y constate que la différenciation est surtout concentrée sur la documentation et les tutoriels.

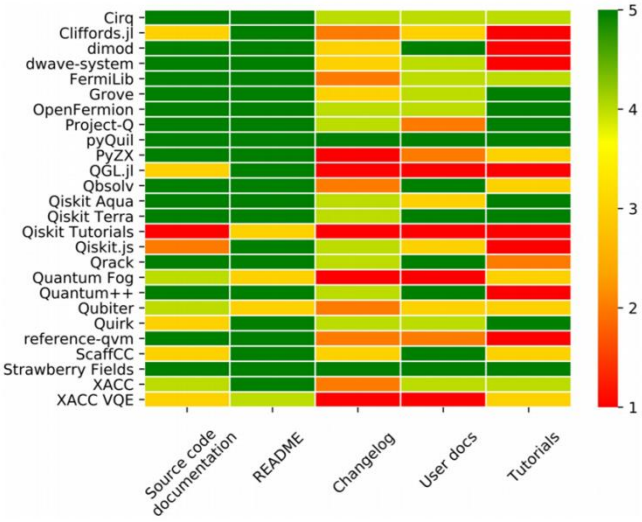


Fig 4. Heatmap of documentation analysis results. The heatmap shows the evaluation results for source code documentation, README files, changelogs, user documentation and tutorials on a scale from 1 (bad) to 5 (good). The evaluation rubrik used for scoring can be found in S1 Table. Data was obtained in August 2018.

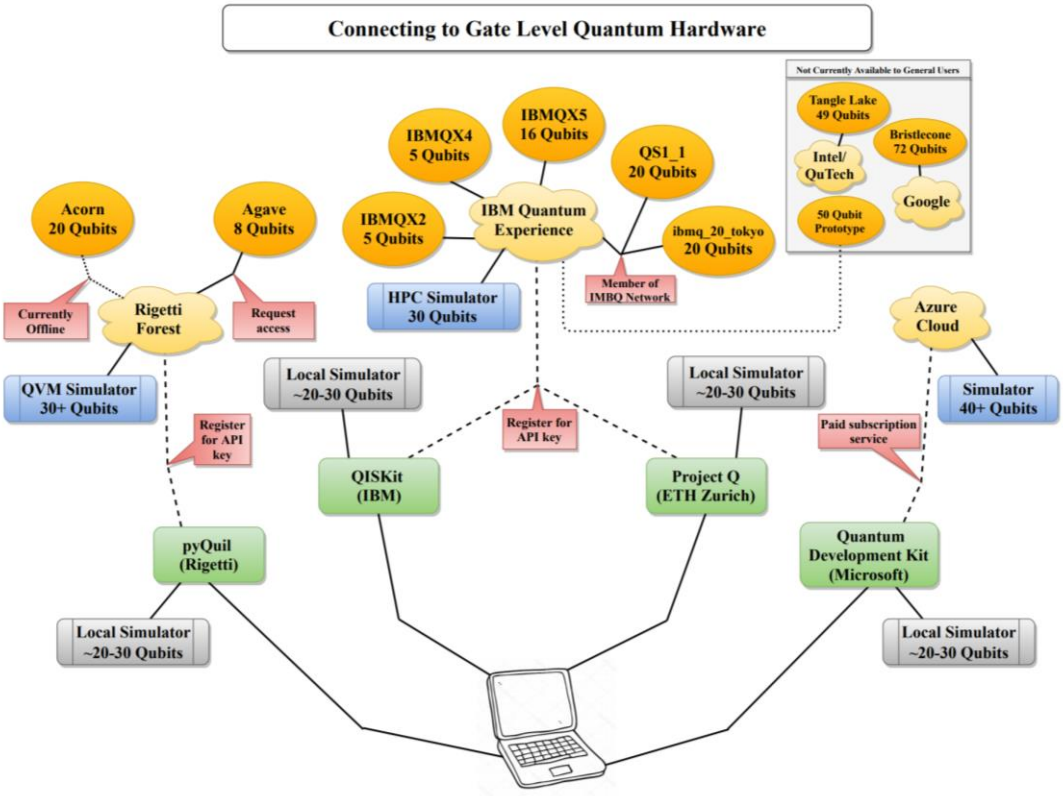
Dans la pratique, peu de développeurs d'applications commerciales vont exploiter les langages évoqués dans cette partie. Ils vont plutôt s'ancrer dans les langages issus des fournisseurs d'ordinateurs quantiques commerciaux que voici *ci-dessous*, même s'ils sont aussi open source. Ils se font facilement enfermer dans des approches « full stack » qui sont propriétaires dans la pratique.

Outils de développement des concepteurs de calculateurs quantiques

Avant même que les ordinateurs quantiques universels soient opérationnels à une échelle exploitable, la bataille des plateformes est déjà enclenchée. Les grands acteurs de l'ordinateur quantique ont presque tous adopté une approche d'intégration verticale de bout en bout allant de l'ordinateur aux outils de développement. C'est en particulier le cas chez IBM, Microsoft, Rigetti et D-Wave.

C'est bien illustré dans le schéma *ci-dessous* de synthèse découvert dans Overview and Comparison of Gate Level Quantum Software Platforms de Ryan LaRose, mars 2019 (24 pages) qui décrit par ailleurs fort bien les principaux environnements de développement d'applications quantiques de Rigetti et IBM et dont est inspirée la partie qui les concerne ici même.

L'offre verticalisée des acteurs cités intègre souvent un langage quantique de bas niveau assimilable au langage machine, puis un langage de plus haut niveau assimilable au macro-assembleur des ordinateurs traditionnels, puis un framework open source exploitable le plus souvent en Python avec des fonctions prêtes à l'emploi, un environnement de développement, éventuellement, un simulateur graphique de portes quantiques et souvent, une offre d'accès à l'ensemble en cloud.



Reste à inventer les langages avec un très haut niveau d'abstraction permettant de s'affranchir des portes quantiques ! Pour l'instant, il n'en existe pas à ma connaissance, sauf dans une certaine mesure autour des ordinateurs quantiques de D-Wave dont le modèle de programmation est particulier.

D-Wave

D-Wave est le plus ancien acteur du marché. Il propose une gamme complète d'outils logiciels qui ont bien évolué depuis sa création. L'architecture n'est d'ailleurs pas évidente à suivre[248]. La dernière itération de la plateforme logicielle de D-Wave s'appelle Ocean, qui comprend les briques de bas et de haut niveau pour le développement d'applications quantiques[249].

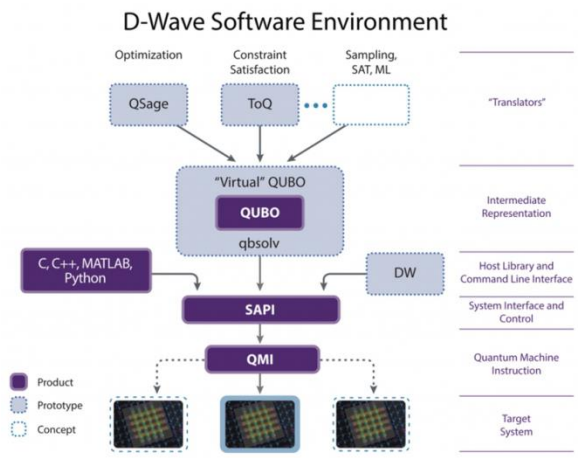
Le plus bas niveau d'accès aux ordinateurs D-Wave est le langage **QMI**, sorte de langage machine de définition des liens entre les qubits reliés entre eux dans le processeur quantique de l'ordinateur adiabatique. QMI est exploitable à partir des langages C, C++ Python et même Matlab, via l'interface SAPI (Solver API).

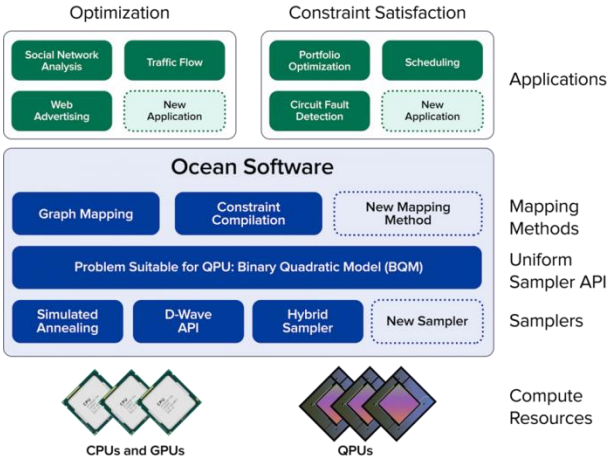
Au-dessus de QMI se situe une surcouche avec un plus haut niveau d'abstraction, **qbsolv**, qui est une bibliothèque open source depuis fin 2017. Elle permet de résoudre des problèmes d'optimisation en décomposant un problème QUBO (Quadratic Unconstrained Binary Optimization) pour le faire traiter par un ordinateur D-Wave ou un ordinateur traditionnel.

---

[248] La source du schéma de gauche est D-Wave Initiates Open Quantum Software Environment, janvier 2017. Et celle du schéma de droite, plus récent : https://www.dwavesys.com/software.

[249] D-Wave fournit un très bon document décrivant les problèmes qui peuvent être résolus avec leurs ordinateurs : D-Wave Problem-Solving Handbook, octobre 2018 (114 pages).





Les développeurs peuvent aussi faire appel au langage open source **QMASM** (Quantum Macro Assembler) qui est un langage de bas niveau adapté à la programmation sur ordinateur à recuit quantique D-Wave. C'est un outil tierce partie de D-Wave. Comme qbsolv, QMASM permet de décrire un "hamiltonien" fait de relations entre qubits à base de coupleurs qui sont dotés d'un poids comme le poids des synapses dans un réseau de neurone. Lors de l'exécution, l'ordinateur D-Wave cherche ensuite à déterminer un minimum énergétique de ce système pour le faire converger vers une solution. Cette méthode présente un inconvénient : il est préférable d'initialiser le système dans un état voisin de la solution recherchée et cet état ne peut être déterminé que par des calculs traditionnels. C'est un peu le serpent qui se mort la queue !

C'est en tout cas un modèle de programmation très différente de celui des portes quantiques universelles même s'il existe une équivalence théorique entre les modèles adiabatiques et à portes quantiques universelles comme nous l'avons vu dans la partie précédente.

QMASM est aussi intégré dans **Quadrant**, une plateforme complète pour le développement de solutions D-Wave dans le cloud appliquées au machine learning et lancée par D-Wave en 2018[250].

Le SDK Ocean de D-Wave comprend aussi **Hybrid**, un framework open source de création d'algorithmes hybrides.

On peut ajouter des surcouches tierces-parties comme **QSage**, un framework destiné à la résolution de problèmes d'optimisation et **ToQ**, un autre framework, pour résoudre des problèmes de satisfaction de contraintes ainsi que le SDK de la startup canadienne **1Qbit**. Avec ces surcouches, on commence à se rapprocher des solutions métiers.

En date d'août 2019, D-Wave, ses partenaires et clients avaient prototypé 150 algorithmes et solutions. Ils n'ont pas forcément généré d'avantage quantique certain, mais permettent aux clients de s'éduquer sur la programmation quantique. Nous les évoquerons dans une partie à venir sur les applications par marchés et sur l'offre des différents acteurs du marché.

[250] Voir D-Wave Announces Quadrant Machine Learning Business Unit, mai 2018.

IBM

La plateforme de développement logicielle quantique d'IBM est sous l'ombrelle **Qiskit**. Elle comprend **OpenQASM**, un langage de programmation qui complète son outil de programmation graphique en ligne Q Experience. OpenQASM comprend une douzaine de commandes[251].

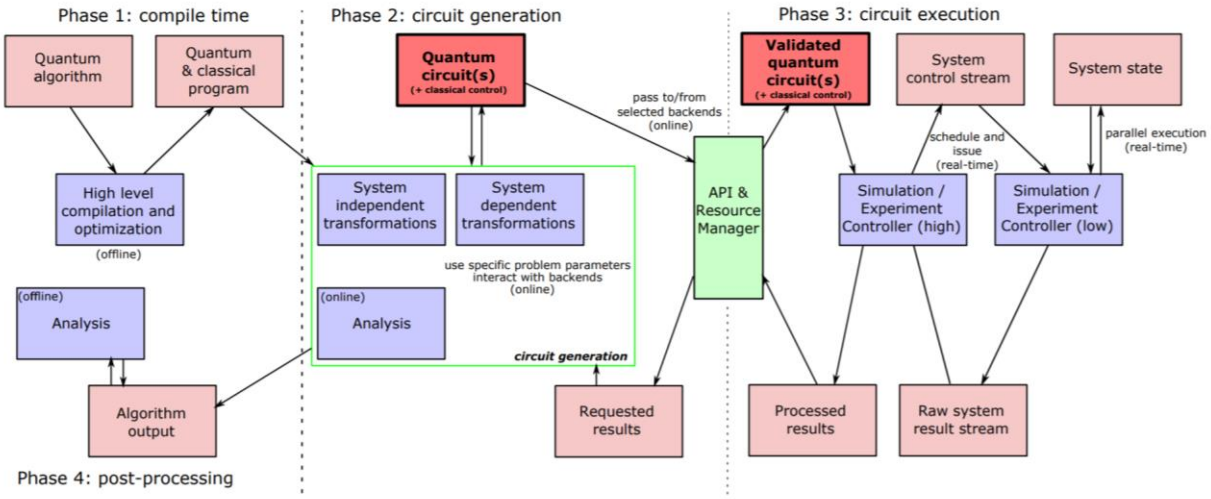


Figure 1: Block diagrams of processes (blue) and abstractions (red) to transform and execute a quantum algorithm. The emphasized quantum circuit abstraction is the main focus of this document. The API and Resource Manager (green) represents the gateway to backend processes for circuit execution. Dashed vertical lines separate offline, online, and real-time processes.

Un langage de scripting de haut niveau associé à OpenQASM est proposé par IBM : **Qiskit**, exploitable en Python, JavaScript et Swift (un langage généraliste d'Apple) et sur Windows, Linux et MacOS. Il a été lancé début 2017 et est publié en open source[252].

Qiskit est fourni avec de nombreux templates et exemples de codes permettant d'exploiter une vaste gamme d'algorithmes quantiques connus. Il comprend une fonction "circuit-drawer" qui génère une visualisation graphique des circuits quantiques programmés en passant par le langage de composition de documents open source LaTeX.

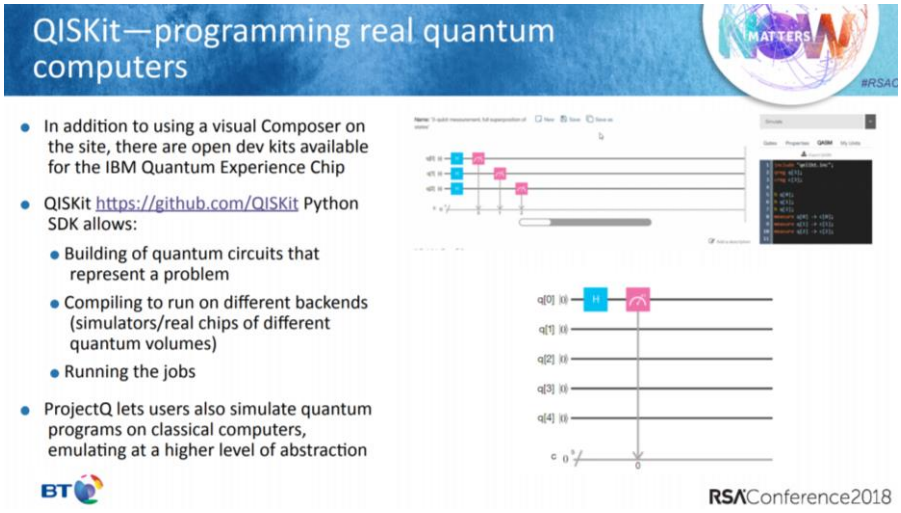
La bibliothèque Aqua de Qiskit permet quant à elle de développer pour des NISQ, les premiers ordinateurs quantiques universels (Noisy Intermediate-Scale Quantum selon l'appellation de John Preskill). Elle comprend des algorithmes quantiques pour des applications diverses comme dans la simulation chimique, le machine learning et la finance.

---

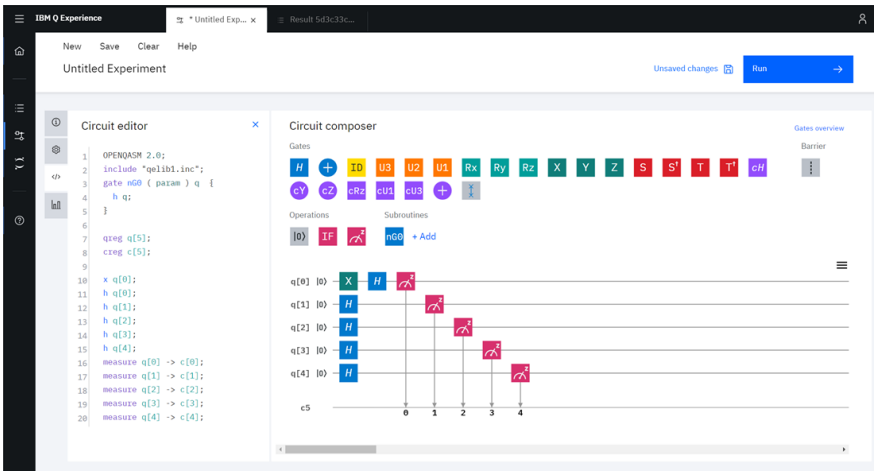
[251] Il est spécifié dans Open Quantum Assembly Language, 2017 (24 pages), ce document décrivant au passage les nombreuses tâches réalisées par le compilateur associé.

[252] Le slide ci-dessus qui décrit Qiskit est issu de la présentation Quantum Computing is Here Powered by Open Source 2018 (41 slides, vidéo).

La compilation du code quantique a ensuite lieu pour exécuter l'ensemble soit sur le simulateur HPC classique en cloud d'IBM soit sur un ordinateur quantique universel comme ceux d'IBM qui sont également accessibles dans le cloud, avec 5 ou 14 qubits.



L'IBM Quantum Composer permet de programmer graphiquement en ligne son code pour l'exécuter sur un émulateur quantique ou sur deux ordinateurs quantiques en ligne : Tenerife et Yorktown (5 qubits) ou Melbourne (14 qubits)[253].



L'émulateur simule pour sa part jusqu'à 32 qubits et il répond bien plus rapidement que les ordinateurs quantiques, en tout cas avec peu de qubits. On peut exécuter son code une fois ou 1024, 4096 ou 8192 fois pour obtenir une moyenne des résultats. Comme les batchs sont soumis les uns après les autres, on peut attendre jusqu'à une demi-heure pour que son code soit exécuté. La création de compte y est gratuite[254].

IBM propose aussi l'application mobile **Hello Quantum** qui permet de programmer avec quelques qubits.

Rigetti

La startup américaine développe des ordinateurs quantiques universels à base de qubits supraconducteurs dans la lignée de ce que fait IBM. Elle propose aussi une plateforme intégrée avec le langage de bas niveau **Quil** qui supporte un modèle de mémoire mixte classique et quantique[255].

---

[253] Voir A taste of quantum computing: a gentle introduction using the IBM Quantum Computer de Chris Bernhardt (21 pages) qui fournit les bases de l'utilisation de l'IBM Quantum Composer.

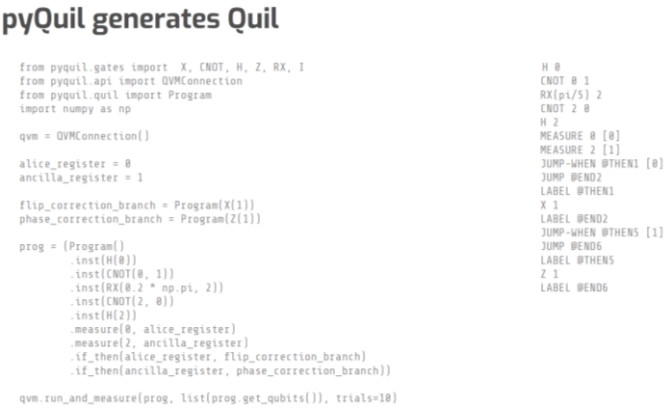
[254] Les conditions d'utilisation précisent cependant : *"You may not use IBM Q in any application or situation where failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage, such as aircraft, motor vehicles or mass transport, nuclear or chemical facilities, life support or medical equipment, or weaponry systems"*. Sachant qu'avec 5 qubits émulés, il devrait être difficile de faire tout cela.

[255] Il est documenté dans A Practical Quantum Instruction Set Architecture, 2017 (15 pages). Non daté.

Il fonctionne sur Windows, Linux et MacOS. Le langage utilise la classe gates pour décrire les opérations à opérer sur les qubits, indexés de 0 à n-1, pour n qubits et avec des portes quantiques. Le langage permet de créer de la programmation conditionnelle en fonction de l'état des qubits.

Il est complété par la bibliothèque **pyQuil** open source lancé début 2017 qui est comprend la bibliothèque Grove d'algorithmes quantiques de base (documentation).

Il s'exploite avec le langage de programmation Python. Le pyQuil de haut niveau (assembleur) génère le langage Quil de bas niveau (code machine).



En voici un simple exemple avec un seul qubit activé par une porte de Hadamard qui créé une superposition d'état 0 et 1 permettant de créer un générateur de nombre vraiment aléatoire. Utilisé de manière itérative dans une boucle classique, le programme peut générer une série aléatoire de 0 et de 1 avec 50% de chances d'avoir l'un ou l'autre permettant de créer un code binaire unique complètement aléatoire.

```
1  # random number generator circuit in pyQuil
2  from pyquil.quil import Program
3  import pyquil.gates as gates
4  from pyquil import api
5
6  qprog = Program()
7  qprog += [gates.H(0),
8            gates.MEASURE(0, 0)]
9
10 qvm = api.QVMConnection()
11 print(qvm.run(qprog))
```

porte de Hadamard sur qubit 1

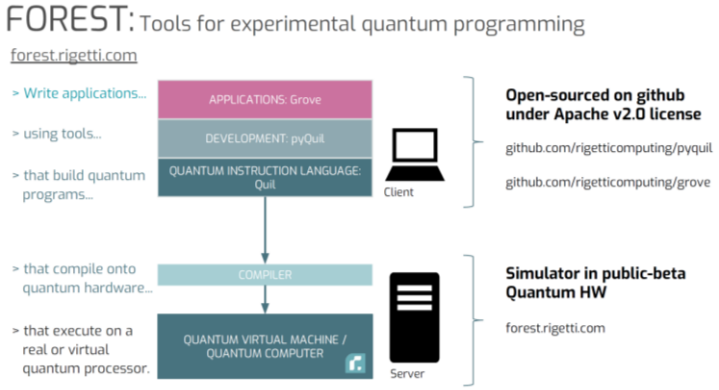
lecture de l'état du qubit superposé

sortie du résultat

Listing 2: pyQuil code for a random number generator.

Rigetti propose l'exécution de programmes quantiques dans ses ordinateurs en cloud et sur des simulateurs classiques via ses QVM, pour **Quantum Virtual Machines**[256].

Quil est utilisable à partir de l'environnement de développement **Forest** proposé par Rigetti. Ces outils sont open source, mais pas multiplateforme. Dommage !



Robert Smith, Michael Curtis, William Zeng. *A Practical Quantum Instruction Set Architecture*. arXiv:1608.03355

[256] C'est documenté dans pyQuil Documentation, juin 2018 (120 pages) qui contient de nombreux exemples de code comme celui *ci-dessus*.

Fin 2017, Google et Rigetti, lançaient l'initiative open source **OpenFermion**. Ce framework développé en Python exploite aussi les travaux des universités de Delft (Pays-Bas) et de Leiden.

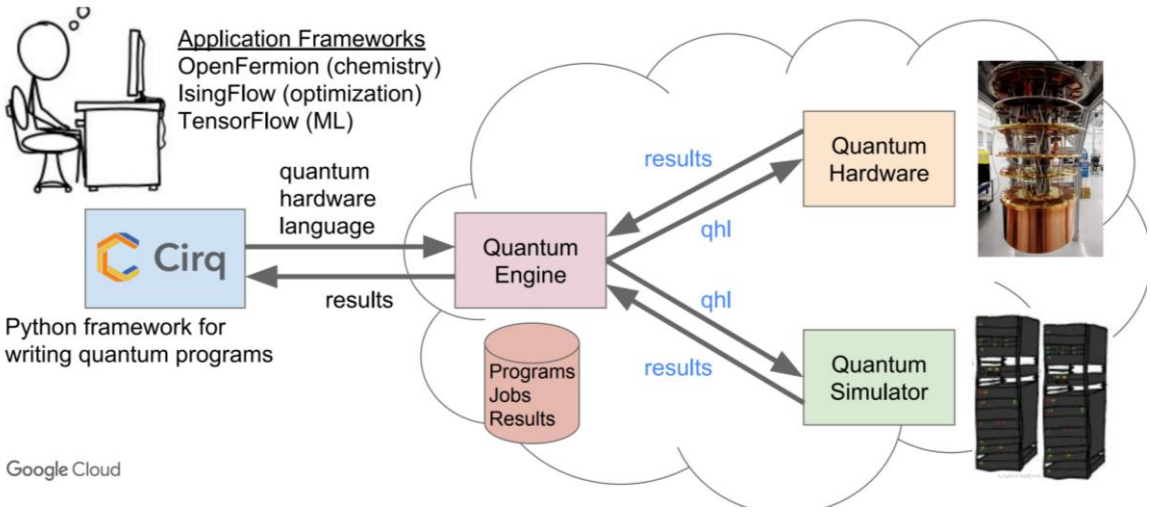
C'est une solution logicielle de création d'algorithmes quantiques de simulation de fonctions chimiques supportant tout ordinateur quantique, des ordinateurs quantiques universels aux ordinateurs quantiques adiabatiques de D-Wave.

C'est une initiative intéressante car elle créé une ouverture multiplateforme sur un domaine d'application clé des ordinateurs quantiques. Elle complète l'approche multiplateforme d'Atos[257].

En 2018, Rigetti lançait enfin un concours d'algorithmes quantiques avec $1M de prix mais avec un biais intéressant, mettant en regard les créateurs d'algorithmes quantiques et d'autres cherchant à en créer des équivalents fonctionnant sur ordinateurs classiques. Le processus pourrait durer de 3 à 5 ans et n'est pas sans rappeler celui des XPrize[258].

Google

En plus d'OpenFermion qui est plutôt un framework de haut niveau, Google lançait le 19 juillet 2018 son propre langage quantique dénommé **Cirq** en open source. Il cible les NISQ, l'appellation de John Preskill déjà évoquée, des ordinateurs à portes quantiques universelles de taille et performance intermédiaire côté taux d'erreurs. C'est un framework pour Python. Il servira notamment à programmer les ordinateurs quantiques de Google notamment celui de 72 qubits qui a été annoncé en mars 2018 mais n'est toujours pas opérationnel.



source du schéma : An Update on Google's Quantum Computing Initiative, Kevin Kissel, novembre 2018 (40 slides).

[257] Voir l'annonce en octobre 2017, OpenFermion: The Electronic Structure Package for Quantum Computers, 2018 (19 pages) et la documentation d'Openfermion.

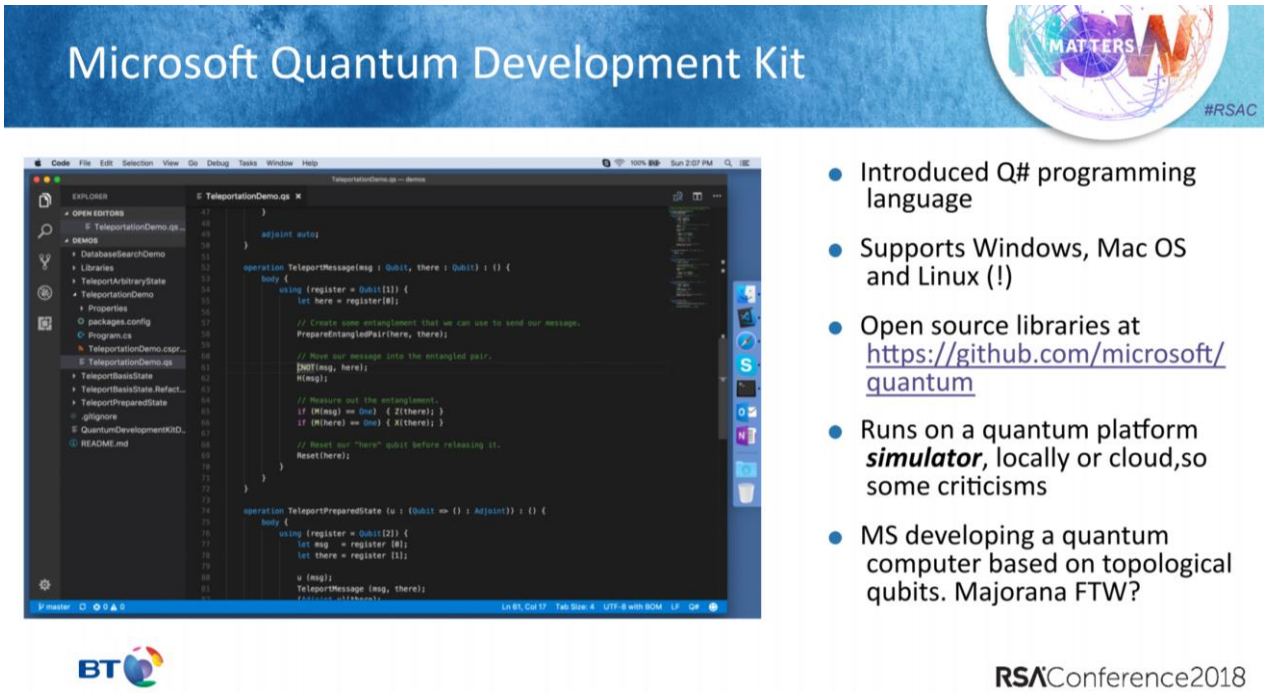
[258] Voir Can You Make A Quantum Computer Live Up To The Hype? Then Rigetti Computing Has $1 Million For You d'Alex Knapp, Forbes, octobre 2018.

Il doit supporter d'autres ordinateurs quantiques, pas encore précisés à ce stade. Il est aussi accompagné d'un simulateur[259]. Un outil de compilation de code OpenFermion en Cirq est aussi proposé.

Microsoft

L'éditeur a d'abord proposé trois briques pour les développeurs avec l'extension **LIQUi|>** du langage de scripting F# qui permet de faire de la simulation de programme quantique.

En décembre 2017, l'éditeur lançait le langage **Q#** qui semble surtout adapté à la programmation d'ordinateurs quantiques topologiques, qui n'existent pas encore, mais sont simulables sur ordinateurs classiques dans le cloud avec jusqu'à 30 qubits.



Q# a une syntaxe dérivée du langage C# de Microsoft[260]. Le tout est fourni sous la forme d'extensions de l'environnement de développement Visual Studio et dans le QDK, pour Quantum Development Kit. Un langage intermédiaire est généré par le compilateur, QIL. Il est censé être multiplateforme mais ne l'est pas encore. Microsoft aura certainement intérêt à rendre multiplateformes ses outils de développement pour capter l'attention et le temps des développeurs.

En juillet 2018, Microsoft lançait aussi **Quantum Katas**, un projet open source contenant des exemples de code quantique en Q# intégrés dans des tutoriels interactifs[261].

---

[259] Voir les explications dans Google Cirq and the New World of Quantum Programming de Jesus Rodriguez, juillet 2018.

[260] Voir Q#: Enabling scalable quantum computing and development with a high-level domain-specific language, 2018 (11 pages).

[261] Voir Learn at your own pace with Microsoft Quantum Katas, juillet 2018.

Ils annonçaient en décembre 2018 une bibliothèque de simulation chimique codéveloppée avec Pacific Northwest National Labs [262], une sorte d'équivalent d'OpenFermion, qui est codéveloppé par Rigetti et Google. La bibliothèque complète le package logiciel de simulation de chimie quantique NWChem de PNNL.

Et en mai 2019, Microsoft annonçait qu'il allait rendre open source ses outils de développement quantiques, donc, au minimum Q# et le Quantum Development Kit.

IonQ

La startup issue de l'Université de Maryland planche sur la création d'ordinateurs quantiques à base d'ions piégés. Nous détaillerons cela plus tard. Comme Rigetti, ils veulent aussi créer une offre logicielle "full stack" adaptée à leur architecture d'ordinateur quantique, et proposée en cloud.

Intel

A ce stade, Intel n'est pas très avancé côté développement de logiciels quantiques. Ils ont créé à ce stade un logiciel de simulation quantique pour ordinateurs classiques[263], les deux premiers auteurs travaillant chez Intel et de dernier à Harvard. Il peut simuler jusqu'à une quarantaine de qubits.

Huawei

Fin 2018, Huawei lançait son propre framework de développement d'application quantique, compatible avec ProjectQ, et comprenant une interface graphique de création d'algorithme. Le tout s'intègre dans leur service en cloud HiQ de simulation quantique[264].

Atos

Atos n'est pas encore un fabricant d'ordinateurs quantiques même si leurs partenariats avec le CEA laissent indiquer que cela pourrait les intéresser. Ils proposent pour l'instant un simulateur de logiciels quantiques à base de supercalculateur à processeurs Intel et avec leur propre architecture mémoire optimisée, les aQML. Ils simulent de 30 à 40 qubits.

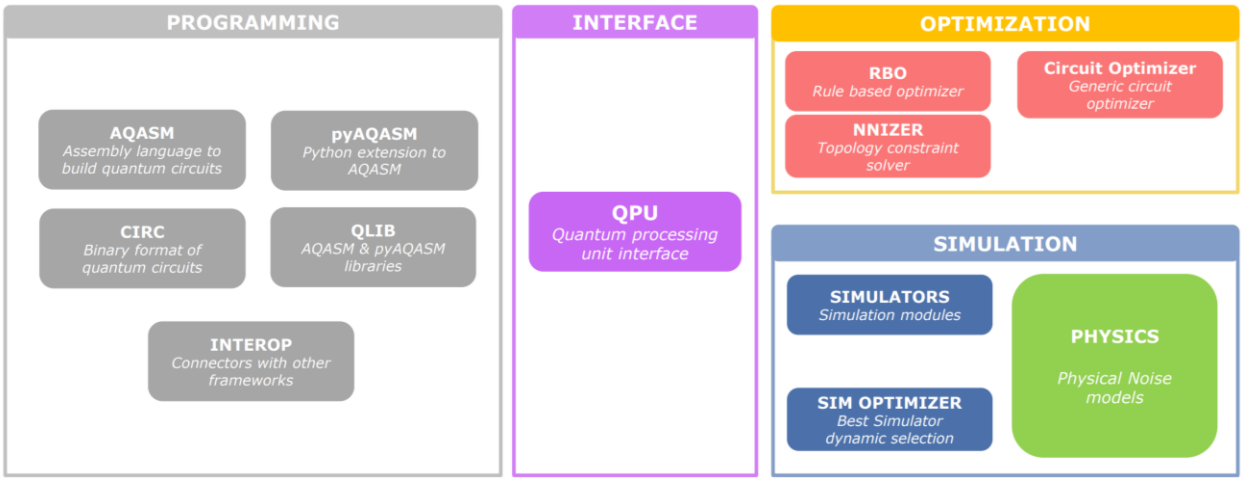
aQASM (Atos Quantum Assemby Programming Language) est un langage de programmation complétant Python qui permet de créer des algorithmes quantiques exécutables sur les simulateurs aQML ou sur toute architecture physique d'ordinateur quantique universel (à terme). Le langage permet de définir des portes quantiques utilisant d'autres portes quantiques, l'équivalent des objets, fonctions ou des macros dans la programmation traditionnelle. Source du schéma *ci-dessous*.

---

[262] Voir Simulating nature with the new Microsoft Quantum Development Kit chemistry library, décembre 2018. Le PNNL est un laboratoire de recherche cofinancé par le Département de l'Energie US et opéré par la fondation à buts non lucratifs Batelle Memorial Institute. Batelle opère de nombreux laboratoires US comme le Lawrence Livermoort National Laboratory, le Los Alamos National Laboratory et le Oak Ridge National Laboratory.

[263] Documenté dans qHiPSTER: The Quantum High Performance Software Testing Environment de Mikhail Smelyanskiy, Nicolas Sawaya, et Alan Aspuru-Guzik, 2016 (9 pages)

[264] Voir Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform, octobre 2018.



aQASM est une déclinaison du langage standard OpenQASM, évoqué plus haut. Ce langage est complété par une bibliothèque Python dénommée PyAQASM qui permet de générer des fichiers aQUASM. Le langage permet de programmer l'exécution répétitive de portes en boucles et de créer des fonctions réutilisables.

Le compilateur du code aQASM génère un code binaire CIRC qui est le langage pivot de bas niveau, ensuite converti dans le langage de contrôle d'ordinateurs quantiques universels spécifiques ou pour des supercalculateurs de simulation via l'interface QPU (Quantum Processing Unit Interface). Il est complété de plugins d'optimisation divers qui vont éliminer les portes qui ne servent à rien et adapter le code à l'architecture matérielle ciblée.

Vue d'ensemble

J'ai essayé de consolider une vue d'ensemble des offres "propriétaires" de programmation quantique, en mettant de côté les langages de programmation fonctionnels et impératifs issus des laboratoires de recherche.

Cela donne le schéma maison suivant qui positionne les outils de développement des grands acteurs du marché en fonction de leur niveau[265]. A l'exception d'Atos, tous ces acteurs ont une approche d'intégration verticale allant du langage de programmation jusqu'aux architectures matérielles de qubits.

[265] Je me suis notamment inspiré du schéma intégré dans l'article Quantum Computing languages landscape, AlbaCervera-Lierta de la Quantum World Association, septembre 2018. Je l'ai complété et y ai ajouté une colonne avec Atos.

langages quantiques universels	**XAAC**						
	ProjectQ				**CirqProjectQ**		
	IBM	rigetti	D-Wave	XANADU	Google	Microsoft	Atos
programmation visuelle / environnement de développement	**Q Experience**	**Forest**			**Quantum Playground**	Visual Studio	
bibliothèques quantiques thématiques (chimie, finance, machine learning, …)	**QisKit Aqua**	OpenFermion	**Quadrant, Qsage, ToQ**	PENNY LANE	OpenFermion	**Quantum Chemisty PNNL**	**QLIB**
bibliothèques quantiques généralistes / full-stack	**QisKit**	**Grove QAOA**	**QUBO qbsolv**	STRAWBERRY FIELDS	Cirq	**Quantum Developer Kit**	**pyAQASM**
langage marchine de haut niveau (circuits quantiques)	**QisKit Terra**	**pyquil**	**QMASM**			**Q#**	**AQASM**
langage machine de bas niveau	**Open QUASM**	**quil**	**QMI**	**Blackbird**	**multiples langages machine**		**Cirq QPU**
qubits et portes quantiques	supra-conducteurs	supra-conducteurs	recuit quantique	photons	supra-conducteurs	topologique	any

schéma inspiré de Alba Cervera-Lierta for the QWA 2018
https://medium.com/@quantum_wa/quantum-computing-languages-landscape-1bc6dedb2a35

Le plus intéressant dans tout cela est que nombreux sont les outils de développement qui permettent de se faire la main sur des algorithmes quantiques à petite échelle avant que de "gros" ordinateurs quantiques soient disponibles. A vous de jouer si le cœur vous en dit ! Et ils sont pour la plupart en open source[266].

Open source quantum (2016 -)

2016	QETLAB	Matlab	University of Waterloo,Canada
2016	Liquil>	F#	Microsoft
2016	Quantum Fog	**Python**	Artiste-qb
2016	Qubiter	**Python**	Artiste-qb
2016	IBM Q Experience	-	IBM
2017	ProjectQ	**Python**	ETH Zurich
2017	Forest (QUIL)	**Python**	Rigetti
2017	QISKit	**Python**	IBM
2017	Quantum Optics.jl	Julia	Universität Innsbruck
2017	PsiQuaSP	C++.	Gegg M, Richter M
2018	Strawberry Fields	**Python**	Xanadu, Canada
2018	Quantum Dev Kit	Q#.	Microsoft
2018	QCGPU	Rust, OpenCl	Adam Kelly
2018	NetKet	C++	The Simons Foundation
2018	OpenFermion	**Python**	Google, Harvard,UMich, ETH ..

https://github.com/markf94/os_quantum_software

[266] Voir à ce sujet les présentations de la conférence FOSDEM 2019.

Applications métiers

Les algorithmes évoqués dans une partie précédente sont dans l'ensemble de bien bas niveau. Il reste à les assembler dans des solutions métiers, marché par marché. Le secteur du calcul quantique est encore des plus immatures. Et pour cause puisque les ordinateurs quantiques sont très limités à ce stade.

Nous en sommes aujourd'hui dans une étape équivalente à celle de l'industrie informatique au milieu des années 1950, une époque où l'industrie du logiciel était plus que balbutiante. C'était aussi les débuts de l'intelligence artificielle avec le fameux Summer Camp de Darmouth de l'été 1956 dont certains des travaux, notamment sur la vision artificielle, n'ont pu aboutir que plus de 30 ans après, avec l'invention des réseaux convolutionnels de Yann LeCun, et depuis moins d'une demi-douzaine d'années, grâce aux progrès des GPU et autres processeurs spécialisés.

Scénario d'évolution du marché

Bien malin serait celui qui prédirait à quelle vitesse les applications quantiques émergeront marché par marché. Suivra-t-elle une exponentielle de croissance du marché fulgurante digne de celles de la microinformatique et des smartphones ?

Je vais tenter l'exercice en reliant cette vitesse à quelques grandes évolutions à venir :

- L'apparition de **calculateurs quantiques universels** de plus d'une centaine de qubits logiques, ce qui pourrait arriver d'ici une dizaine d'années. En parallèle vont continuer à se développer les solutions d'optimisation adaptées aux ordinateurs à recuit quantique de D-Wave.
- La consolidation du marché des **outils de modélisation et de développement** de solutions quantiques. Les outils sont déjà bien nombreux comme nous avons pu le voir dans la partie précédente. Ils vont continuer de gagner en maturation, notamment en élevant leur niveau d'abstraction, et s'adapter aux évolutions du matériel. Des bibliothèques adaptées aux besoins de marchés spécifiques feront sans doutes leur apparition comme dans la simulation moléculaire ou la finance.
- La **formation de développeurs** de solutions d'un nouveau genre capables de gérer des abstractions qui n'ont rien à voir avec les différentes formes de programmation procédurale qui dominent l'informatique actuelle, même dans ses variantes de programmation événementielle qui sont courantes dans la création de sites web et applications graphiques. Une nouvelle génération de concepteurs d'algorithmes et de développeurs verra le jour. Ce seront probablement des professionnels jeunes qui auront pu digérer les nouveaux concepts du quantique avec un esprit neuf.
- Les **premiers retours d'expériences** de projets pilotes, déjà engagés, notamment sur D-Wave. On continuera à se poser d'épineuses questions sur la comparaison objective entre algorithmes quantiques, architectures matérielles quantiques et leurs équivalents tournant (ou pas) sur supercalculateurs.

Il faudra aussi faire le tri en “proof of concepts” et projets réellement déployés. Dans de nombreux marchés, l’ordinateur quantique sera d’abord un instrument de travail pour les chercheurs.

- L’émergence d’un **tissu de startups** qui dynamisera le marché, probablement légèrement en avance de phase par rapport aux éditeurs de logiciels traditionnels et aux entreprises de services numériques qui ne s’aventureront pas forcément en premier dans ce nouveau monde du quantique. Elles sont peu nombreuses à ce stade comme nous le verrons dans une partie à venir. Les places restent à prendre.
- L’apparition de solutions à base d’ordinateurs quantiques qui auront un **impact sur notre vie de tous les jours**. Donc, des applications grand public. Nous devrions en effet voir les usages du quantique évoluer progressivement des milieux de la recherche, à ceux des entreprises, puis des applications grand public. La première application grand public que l’on peut avoir en tête est celle de l’optimisation des transports. Mais d’autres applications restent à inventer.

Comme avant chaque grande révolution technologique, les prévisions sont difficiles à faire. Aucune de celles qui précédaient l’arrivée des micro-ordinateurs, d’Internet, du web 2.0 ou de la mobilité ont vu juste, notamment sur la hiérarchie d’importance de l’adoption des solutions à la fois dans les marchés grand public et professionnels.

Les prévisions de croissance du business autour du quantique du **BCG** illustrent cette forte incertitude. Elles sont présentées avec plusieurs scénarios : l’un, optimiste, qui fait démarrer la croissance vers 2030 et l’autre, très conservateur, qui le fait décoller seulement après 2040[267].

autres prévisions

$553M en 2023 selon MarketsandMarkets (2017).

$1,9B en 2023 selon CIR et de $2,64B en 2022 selon Market Research Future (2018).

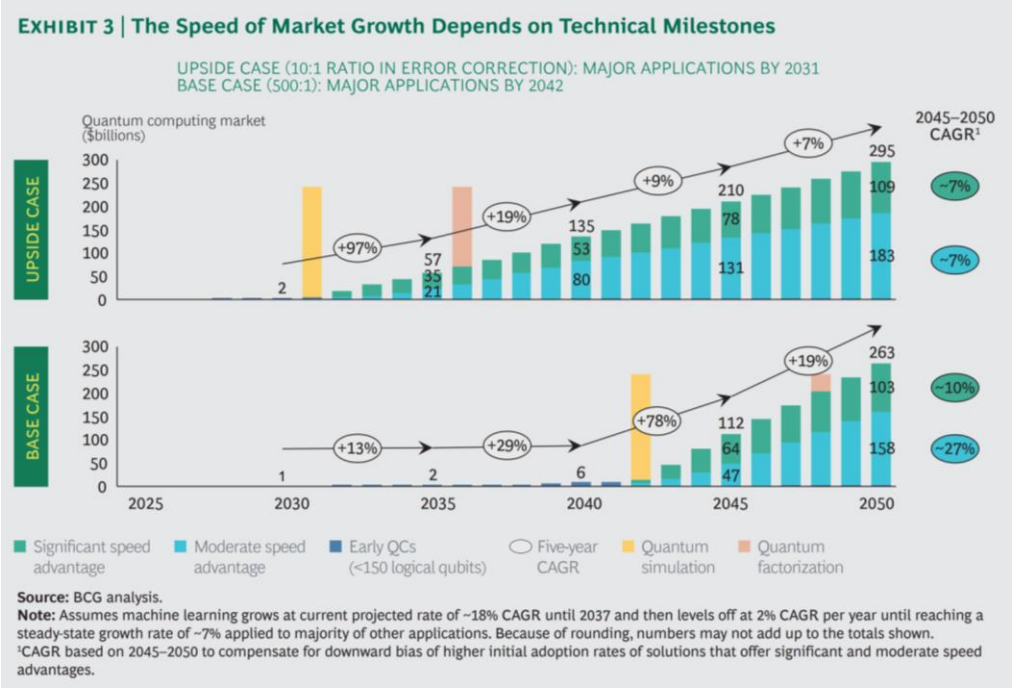
$8,45B en 2024 selon Homeland Security (en 2018)

$10B en 2028 selon Morgan Stanley (2017)

$15B d’ici 2028 selon ABI Research (2018).

Repères :

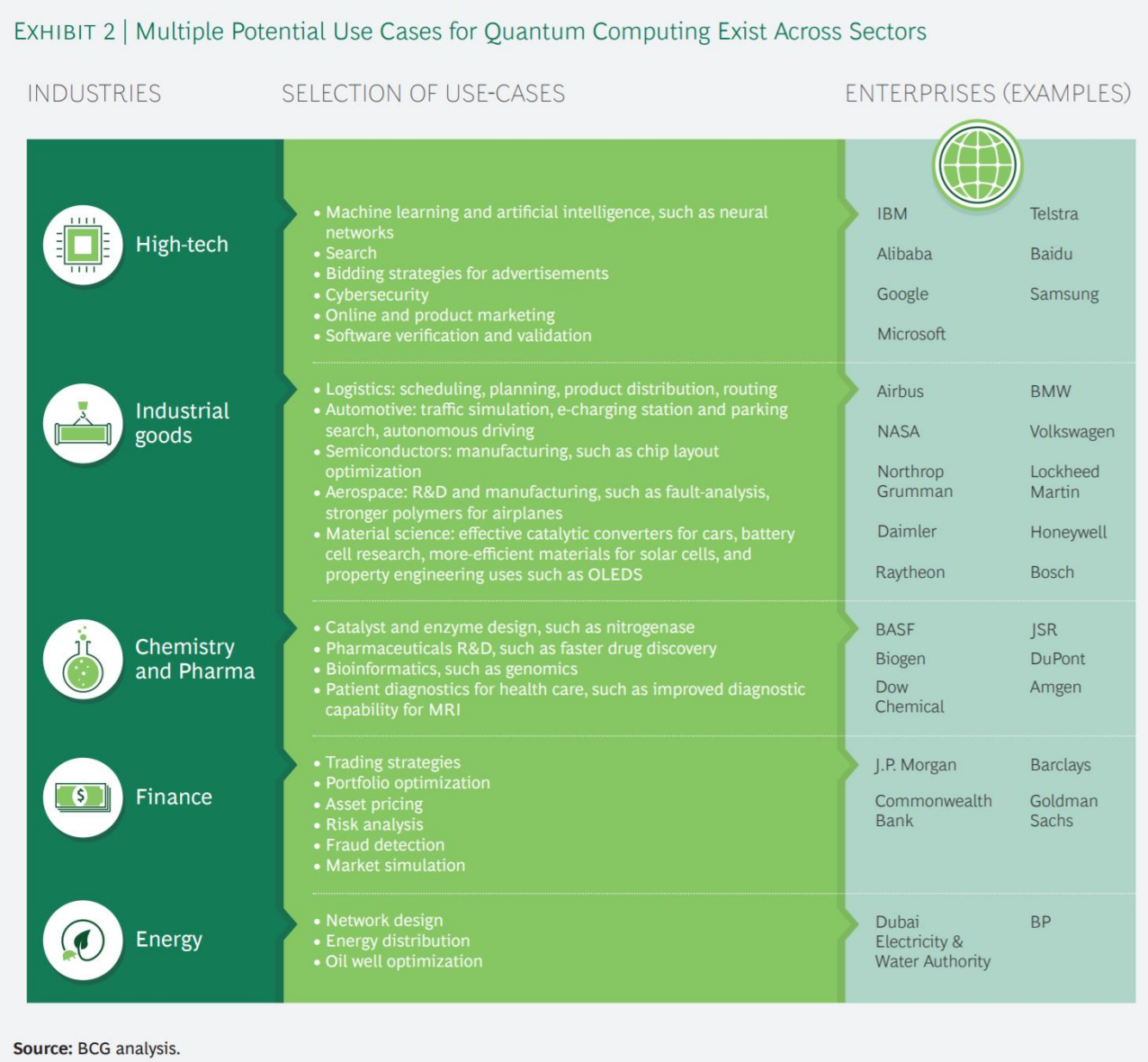
2018 worldwide markets
serveurs : < $90B
logiciel d’entreprise : $431B



[267] Dans The coming quantum leap in computing, mai 2018 (19 pages).

Ils n'intègrent visiblement pas le scénario de l'émergence du NISQ, ou "Noisy Intermediate-Scale Quantum", décrit par John Preskill[268]. Il recouvre les calculateurs quantiques à venir dans un futur proche, ayant un nombre intermédiaire de qubits avec un bruit quantique acceptable pour démarrer des applications scientifiques.

Voici cependant ce que nous pouvons nous mettre sous la dent avec un inventaire à date des applications de l'informatique quantique classifiées par secteurs d'activités. Cela couvre à la fois quelques études de cas d'usage du quantique, souvent réalisées avec les seuls ordinateurs quantiques commerciaux, ceux de D-Wave, et sinon, des applications prospectives mais qui attendent encore les ordinateurs quantiques universels de taille critique qui pourront les exécuter.

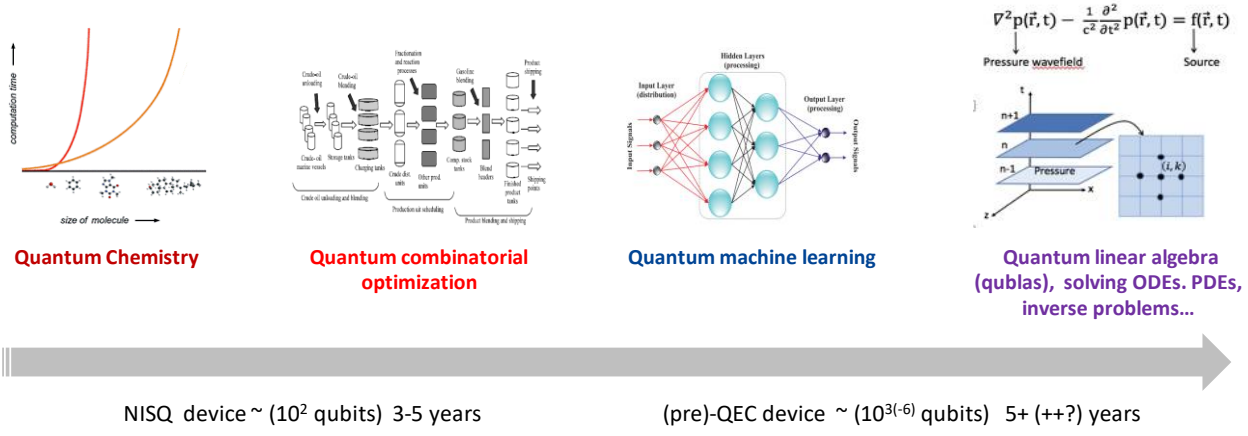


source des panoramas : The Next Decade in Quantum Computing and How to Play du BCG, 2018 (30 pages).

[268] Dans Quantum Computing in the NISQ era and beyond début 2018.

A noter que d'une manière générale, il n'y a pas de corrélation directe entre les applications de l'IA et celles du quantique. Le critère principal de l'intérêt du quantique est la complexité du problème plus que le volume de données à gérer. Le "big data" est loin d'être le cœur d'applications du quantique.

Chez **Total**, on a construit cette roadmap permettant de se faire une idée de l'ordre dans lequel les applications quantiques pratiques vont voir le jour en fonction du nombre de qubits disponibles.

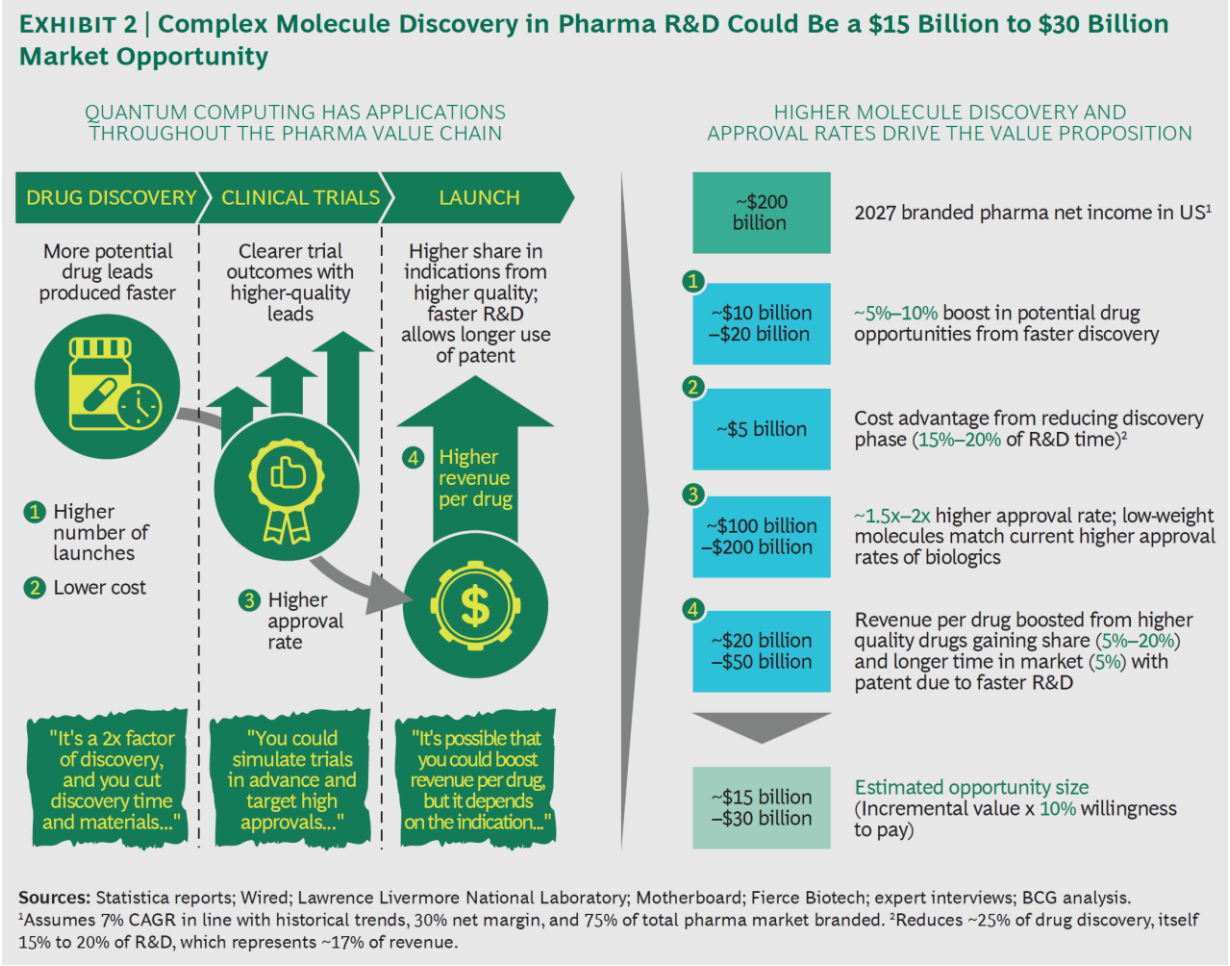


source : Total, QCB Conference, 20 juin 2019

Santé

La principale application de l'informatique quantique en santé est la découverte de thérapies via la simulation moléculaire de leur fonctionnement et de celle de leurs cibles, tout en évitant d'éventuelles contre-indications, le tout "in silico".

La simulation peut porter sur l'articulation de molécules organiques simples comme le cholestérol ou le repliement des protéines qui est de plusieurs ordres de grandeur plus complexe. Cette dernière prouesse relève donc du très long terme. Elle est aussi à la limite du faisable en termes de complexité car elle est dans la classe des problèmes NP-Complet comme vu dans la partie dédiée aux théories de la complexité, à partir de la page 189.



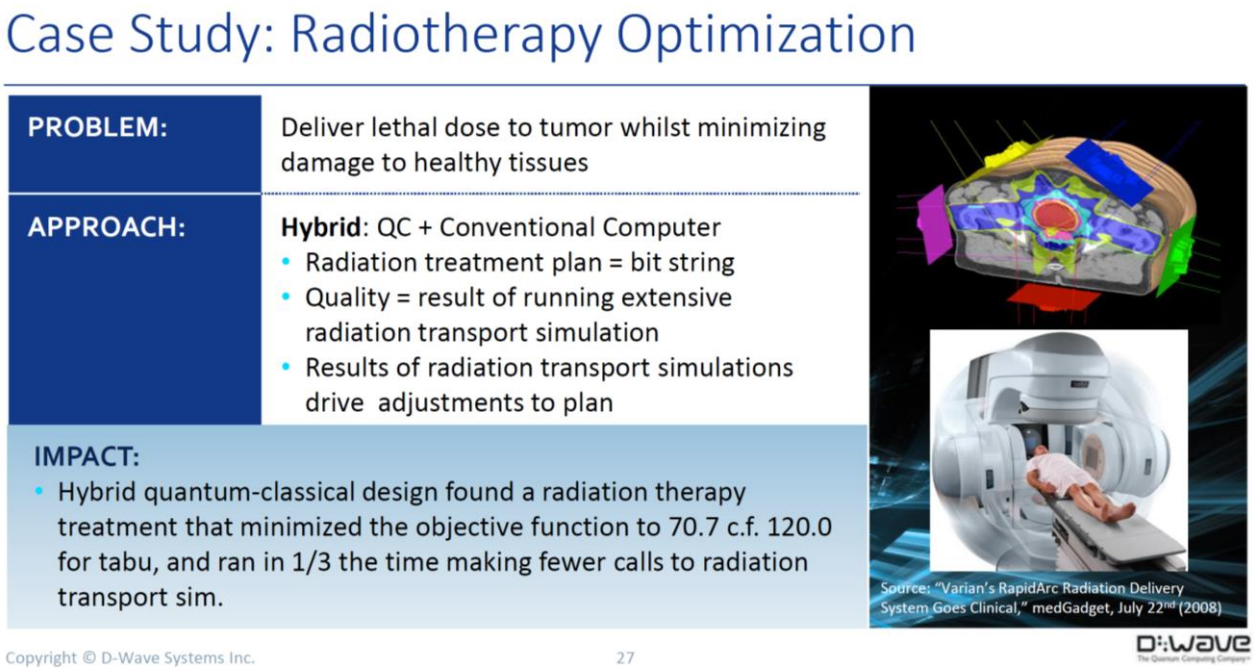
Les premières expérimentations de simulation moléculaire ont été à ce jour réalisées sur les D-Wave à recuit quantique. Ces ordinateurs sont particulièrement adaptés à la recherche de minimums énergétiques, ce qui convient à la simulation de l'organisation de molécules.

Une collaboration a été lancée en juin 2017 entre **Biogen**, la société de logiciels quantiques canadienne **1QBit** et **Accenture** pour la création de nouvelles molécules.

Biogen (1978, USA) est une entreprise de biotechs de taille intermédiaire avec ses 7300 collaborateurs spécialisée dans le traitement de maladies neurodégénératives et de leucémies. Leur usage du quantique visait le reciblage de molécules thérapeutiques. Il s'agit de trouver des correspondances entre des traitements existants et des cibles thérapeutiques, ici, dans les maladies neurodégénératives ou inflammatoires. Cela reste un usage expérimental du quantique mais cela ouvre la voie.

L'Américain **Amgen** est aussi actif dans la recherche de nouvelles thérapies mais sans grandes précisions publiques à ce stade.

Toujours avec D-Wave, une application d'optimisation de radiothérapie est mise en avant (*ci-dessous*). Le principe algorithmique consiste à minimiser l'exposition des patients aux rayons X tout en optimisant leur efficacité. C'est un problème complexe de simulation de diffusion d'ondes électromagnétiques dans le corps humain.



En juin 2019, **Merck** annonçait un partenariat de trois ans avec la startup **HQS Quantum Simulations** basée à Karlsruhe en Allemagne pour le développement d'algorithmes quantiques de simulation chimique.

A l'origine de sa propre société de conseil **Eigenmed**, David Sahner est un des promoteurs de la médecine de precision à base de techniques de machine learning de prédiction exploitant le quantum annealing de D-Wave[269]. Les exemples qu'il met en avant n'ont pas l'air d'être dimensionnés au point d'être réalisables uniquement sur D-Wave et pas de manière classique.

Omnicom Healthcare n'hésitait pas de son côté à promouvoir l'usage du quantique dans la santé avec son livre blanc Exponential Biometrics: How Quantum Computing Will Revolutionize Health Tracking, 2017 (7 pages) qui ne contient strictement aucune information pertinente sur le sujet, ce d'autant plus qu'ils ont l'air de confondre les applications du machine learning analysant les données issues d'objets connectés avec la capacité des ordinateurs quantiques à gérer des problèmes intractables par les ordinateurs traditionnels.

Enfin, citons la **DNA-Seq Alliance** qui associe la startup DNA-Seq et D Wave, qui fait aussi du drugs retargetting en associant génomique, cristallographie des protéines kinase, calcul quantique et recherche de traitements efficaces en cancérologie.

[269] Voir Predictive Health Analytics de David Sahner, 2018 (54 slides).

Energie et chimie

Lorsque l'on s'éloigne des molécules organiques et du vivant, tout devient soudainement presque réaliste ! En effet, les premières applications de simulation moléculaires envisagées et plausibles concernent les matériaux innovants. Le secteur de l'énergie et de la chimie est intéressé par la résolution de problèmes complexes d'analyse et d'optimisation et par la simulation in silico de molécules, et pour créer de nouveaux matériaux. Les premières études de cas sont généralement réalisées avec les générations récentes d'ordinateurs à recuit quantique de D-Wave. Ceux-ci sont bien indiqués pour des simulations d'interactions atomiques dans des matériaux.

Les premiers ordinateurs quantiques universels commerciaux qui dépasseront 50 qubits et font partie des NISQ de John Preskill sont tout aussi adaptés aux simulations moléculaires à un premier niveau. Cela restera évidemment des outils destinés aux chercheurs. La simulation d'un matériau n'est en rien une garantie de la découverte d'un matériau utile. C'est un outil de travail de plus pour les chercheurs.

Les simulations peuvent toucher les flux d'air, d'eau et de tous liquides et notamment leurs turbulences. Elles peuvent notamment exploiter les équations de Navier-Stokes[270].

Les recherches vont bon train pour créer des batteries plus efficaces côté densité énergétique et vitesse de charge[271]. C'est d'ailleurs l'un des axes de recherche de Volkswagen qui prévoit de faire cela à terme avec le futur ordinateur quantique universel de Google comme documenté dans cette annonce de novembre 2017.

La capture du carbone est un autre enjeu et des chercheurs simulent son fonctionnement moléculaire par biomimétisme. C'est un domaine d'application mis en avant par les chercheurs de Microsoft.

Chez le chimiste allemand **BASF**, l'idée est de simuler des polymères de synthèse, d'abord sur des supercalculateurs HP, puis à terme sur ordinateurs quantiques. **Dow Chemicals** collabore depuis 2017 avec l'éditeur de logiciels canadien **1Qbit** pour créer de nouvelles molécules, en s'appuyant sur les D-Wave. De son côté, **IBM** simulait en septembre 2017 sur ordinateur quantique supraconducteur à 16 qubits le fonctionnement de molécules d'hydrure de bérylium et leur équilibre énergétique minimum, ce qui ne sert à rien en soi, mais est un bon début[272].

La **Dubai Electricity** and Water Authority planche de son côté avec Microsoft pour résoudre des problèmes complexes de distribution d'énergie et d'eau (source). A ceci près qu'à ce stade, il ne s'agit que de tester quelques algorithmes sur des simulateurs Intel tournant sur Azure. Et pour cause, Microsoft ne dispose pas encore d'ordinateur quantique !

---

[270] Voir Quantum Navier–Stokes equations, de Pina Milišić de l'Université de Zagreb, 2012 (12 pages).

[271] Voir The Promise and Challenges of Quantum Computing for Energy Storage (4 pages).

[272] Voir Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, octobre 2017 (22 pages).

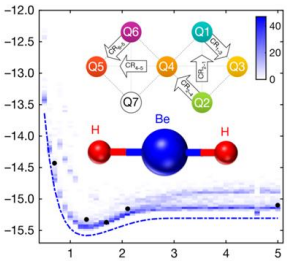
Chez **BP**, on travaille à la conception d'algorithmes d'optimisation de la prospection pétrolière. Il s'agit d'exploiter les données de différents capteurs, notamment sismiques, pour consolider des modèles de simulation de ce que le sol recèle.

Total est un des grands industriels français à s'intéresser de très près aux usages du calcul quantique. Ils veulent aussi optimiser la prospection et l'évaluation des réserves à partir de sondes sismiques. Ils envisagent de traiter les problèmes d'optimisation complexes du type **MINLP** (Mixed Integer Non Linear programming[273]) pour optimiser le raffinage, la planification, la production et le transport. Enfin, ils s'intéressent aussi à la simulation chimique quantique[274].

ExxonMobil était pour sa part l'une des grandes entreprises associées à IBM dans l'IBM Q Network, une communauté de grandes entreprises et laboratoires de recherche intéressés par les applications du calcul quantique.

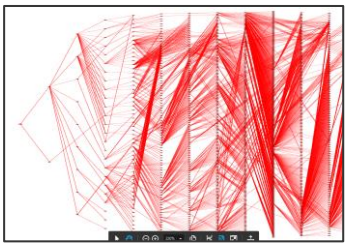
EDF est une autre grande entreprise française qui étudie de très près les usages du calcul quantique : l'évaluation de l'usage de matériaux, des statistiques de sécurité, l'optimisation combinatoire pour la gestion de smart grids et la gestion de batteries.

material ageing modelling



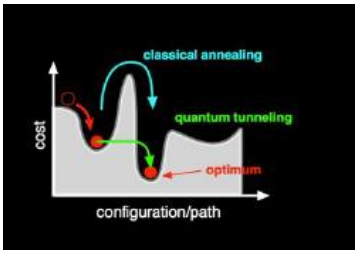
- Modelling ageing phenomena's with quantum physic laws.
- Stake : foresee material ageing patterns to gain operational margin.
- Contribute to regulatory studies for ASN IRSN

safety probabilistic study



- Decision support tool for real time risk analysis
- Recalculate risk based on operation current state and maintenance operation
- Avoid roll back in case uninttended events

combinatorial Optimization for energy management



- Smart charging : optimizing VEs charging for the grid operator/charging operator/user Decentralized energy systems, exploiting large data volume

source : EDF, QCB Conference, 20 juin 2019

D'autres industriels tâtent aussi du quantique. **Dow Chemical** est partenaire de **1Qbit** depuis juin 2017 pour des PoC de simulation chimique quantique. **BP** s'intéresse aux applications de la cryptographie quantique (QKD) avec le Suisse **IDQ**. Enfin, **Mitsubish Chemical** ainsi que la filiale **Materials Magic** d'**Hitachi Metals** teste aussi le calcul quantique, avec IBM.

[273] Une version d'algorithme de résolution de problème MINLP existe pour D-Wave via leur framework QUBO. Voir Quantum Computing and Non-Linear Integer Optimization de Sridhar Tayur février 2019 (42 slides).

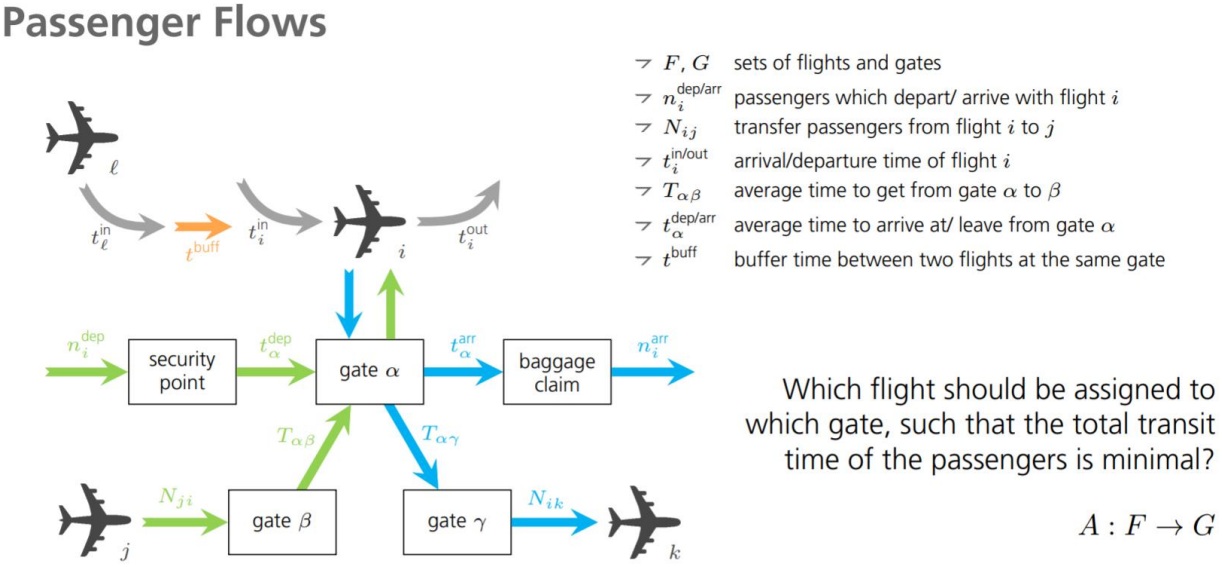
[274] Total s'est associé à des acteurs privés (IBM, Atos, Rigetti Qcware, Google) et divers laboratoires de recherche dans le monde : le PCQC (Paris), le LIRMM de Montpellier, le CERFACS, l'Université ParisSud, Jülich Forschungszentrum (Allemagne) et l'Université de Leiden.

Transports

Au-delà des questions énergétiques évoquées ci-dessus, le marché des transports est surtout intéressé par les algorithmes d'optimisation de systèmes complexes[275].

En ligne de mire, l'optimisation de la planification de flottes d'avions pour le transport aérien, pour maximiser la capacité à répondre à la demande tout en optimisant le taux de remplissage des avions.

Le calcul quantique permet aussi l'optimisation de la gestion des aéroports et des portes pour les avions, pour minimiser le temps d'attente des passagers[276]. C'est un problème NP-difficile difficile à traiter avec des algorithmes classiques.



Ce sont des besoins qui peuvent être d'ailleurs traités à la fois par des algorithmes de machine learning pour tenir compte du passé ou avec des algorithmes quantiques d'optimisation qui s'appuient sur une description des paramètres du problème.

Les premiers font de la prédiction et les seconds de la simulation. La simulation permet d'éviter le biais du rétroviseur qui peut être induit par les méthodes de prédiction s'appuyant sur les données du passé. Une combinaison des deux méthodes est par ailleurs possible.

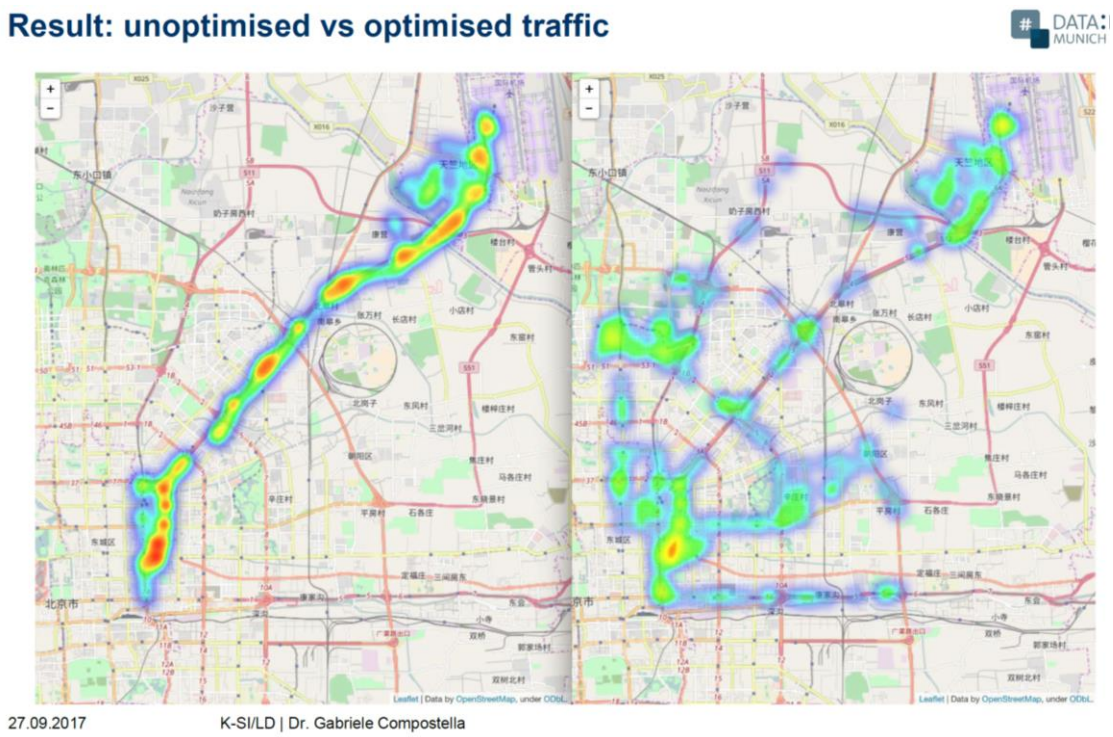
Le déploiement de flottes de véhicules autonomes est aussi une belle application cible des ordinateurs quantiques. Plus les véhicules seront autonomes, plus il faudra en automatiser et coordonner les parcours. Les problèmes à résoudre consisteront à déterminer pas à pas les trajets de flottes de véhicules pour optimiser le temps de parcours de chacun de ces véhicules. C'est l'objet d'une expérimentation réalisée en 2017 par **Volskwagen** sur D-Wave qui visait à optimiser les parcours d'une flotte de

[275] Voir cet inventaire de besoins, mais pas de solutions dans : Quantum Applications Transportation and Manufacturing de Yianni Gamvros, IBM, 2017 (20 slides).

[276] Voir Flight Gate Assignment with a Quantum Annealer par Elisabeth Lobe et Tobias Stollenwerk, du German Aerospace Center (ou DLR pour Deutsches Zentrum für Luft- und Raumfahrt e.V.), mars 2019 (15 slides). Le DLR est un équivalent d'un mélange de l'Onera et du CNES français. L'étude de cas exploite un D-Wave. Elle montre que la solution n'est pas évidente à mettre au point.

taxis à Beijing[277]. L'expérience utilise le jeu de données T-Drive publié par Microsoft datant de 2008 décrivant le parcours de 10 357 taxis.

L'algorithme utilisé était le QUBO (Quadratic Unconstraint Binary Optimisation) qui est un mécanisme de recherche de niveau minimum d'énergie d'un système complexe. Le schéma ci-dessous présente le résultat de l'optimisation du parcours de 418 taxis faisant le trajet centre-ville-aéroport compte-tenu de celui des 10 357 véhicules[278].



On manque de recul pour estimer le dimensionnement des ordinateurs quantiques nécessaires pour gérer pratiquement ce genre de problèmes à grande échelle. De quelle capacité en qubits faudrait-il disposer pour optimiser un parc de centaines voir de millions de véhicules autonomes ?

Chaque chose en son temps… ! Ce genre de problème sera, si cela se trouve, trop lourd à gérer, même pour les ordinateurs quantiques les plus sophistiqués.

Daimler AG fait partie des grandes entreprises travaillant sur le quantique avec IBM, avec en tête des applications d'optimisation de logistique et de planification ainsi que tout ce qui touche au parcours des véhicules autonomes.

Son confère allemand **BMW** étudie aussi les usages du quantique, en partenariat avec la startup **QCWare**.

---

[277] Elle est documentée dans Quantum Computing at Volkswagen Traffic Flow Optimization using the D-Wave Quantum Annealer 2017 (23 slides).

[278] Les résultats sont publiés dans Traffic flow optimization using a quantum annealer, août 2017 (12 pages). Comme pour de nombreuses études de cas issues de D-Wave, celle-ci est aussi contestée par les spécialistes du calcul haute performance.

Airbus est aussi impliqué dans le quantique. En 2015, une de leurs équipes basées à Newport au Royaume Uni se lançait sur le sujet. En 2016, l'avionneur investissait dans la startup américaine QC Ware. Ils ont expérimenté l'usage d'un D-Wave pour une analyse d'arbres de défaillances (FTA : fault tree analysis) qui sert à déterminer l'origine de pannes complexes avec un gain d'un facteur 4 par rapport aux méthodes traditionnelles. C'est un problème combinatoire NP-difficile plus facile à résoudre en programmation quantique. Airbus organise aussi depuis début 2019 son "Quantum Computing Challenge", une manière d'outsourcer le développement de solutions quantiques pour les aider à résoudre leurs problèmes métiers, dans la mécanique des fluides, les équations différentielles, l'optimisation du vol, la conception des ailes, le remplissage des soutes, etc[279].

En mai 2019, 475 équipes issues de de 57 avaient concurru à ce challenge. Elles viennent principalement des USA et de l'Inde, suivis de l'Europe.

Finance

La finance est un autre beau terrain de jeu pour expérimenter des algorithmes quantiques[280]. A la fois parce que les entreprises du secteur sont assez friandes d'outils de prévision et d'optimisation et aussi parce que c'est un marché plutôt bien solvable. Ce n'est pas par hasard que ma première intervention de conférencier sur l'informatique quantique dans une entreprise ait eu lieu le 5 juillet 2018 à la **Société Générale** suivie d'une autre, en octobre 2018 chez **BNP-Paribas**.

Les banques ont un besoin pressant de se transformer pour s'adapter aux changements technologiques et sociétaux constants. Elles manipulent des tombereaux de données qui ont de la valeur.

Elles ont à optimiser de nombreuses facettes de leurs activités, à commencer par celle de portefeuilles d'investissements. Elles veulent aussi détecter au plus près les risques de fraudes. L'optimisation d'actifs est la principale application imaginée pour l'informatique quantique. C'est de l'optimisation sous contraintes. Et là, sous un grand nombre de contraintes. Les actifs sont interdépendants. Les coûts de transactions sont variables selon les types d'actifs.

Question	Broad approach solution
Which assets should be included in an optimum portfolio? How should the composition of the portfolio change according to what happens in the market?	Optimization models
How to detect opportunities in the different assets in the market, and take profit by trading with them?	Machine learning methods, including neural networks and deep learning
How to estimate the risk and return of a portfolio, or even a company?	Monte Carlo-based methods

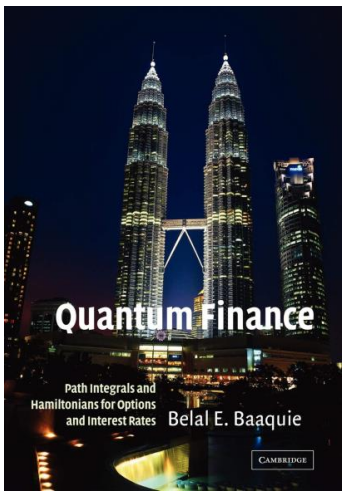
Table I. Financial problems addressed in this paper, and possible approaches.

Leur évolution répond à des niveaux d'incertitude et de risques variables.

[279] Voir Airbus gets aerodynamic with quantum computing par Michael Feldman, janvier 2019.

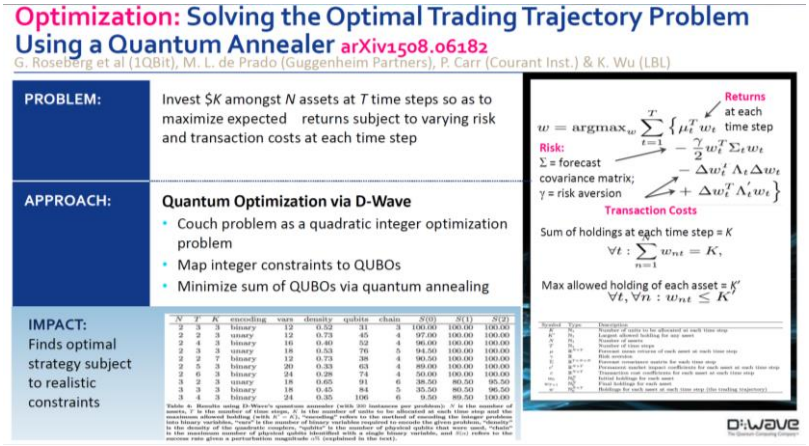
[280] Voir de panorama dans Quantum Computing and Finance de la Quantum World Association, août 2018, qui fait référence à Quantum computing for finance: overview and prospects, 2018 (13 pages).

Il existe d'ailleurs un lien de parenté mathématique entre certaines équations de la finance et la physique quantique. C'est le cas de l'équation différentielle de Black-Scholes qui permet de prédire le prix de produits dérivés financiers qui sont indexés sur des cours tiers. Elle peut être en effet considérée comme une variante de la fonction d'onde de Schrödinger !

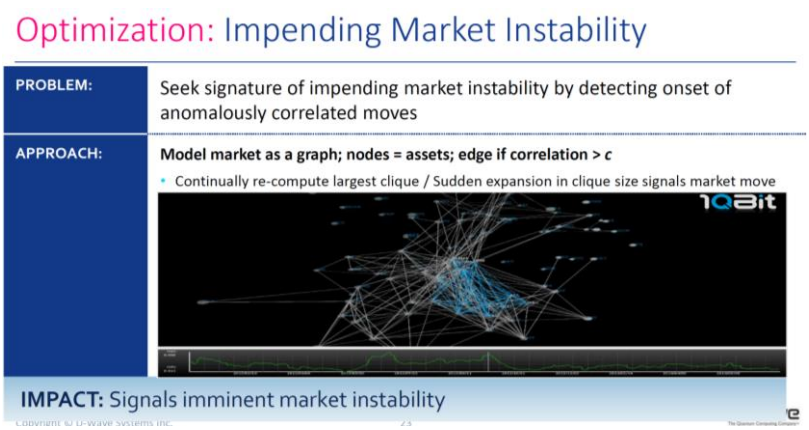


Ces équations sont décrites dans l'ouvrage "Quantum Finance" de Belal Baaquie qui date de 2007 ! Il en existe maintenant une très grande variété qui sont exploitables sur ordinateurs quantiques.

Un modèle d'optimisation quantique s'appuyant sur un D-Wave a été publié en 2015 [281]. Il s'agissait d'optimiser les placements d'un montant donné dans un nombre d'actifs et sur une période donnée. L'algorithme principal utilisé était encore une fois le QUBO.



En s'appuyant sur la modélisation de graphes, aussi adaptée aux D-Wave, une autre étude de cas permettait de modéliser l'instabilité des marchés[282].



Mais le recuit quantique n'est pas la seule technique utilisable pour traiter ce genre de problème.

Avant même qu'ils soient un tant soi peu opérationnels, les ordinateurs quantiques à architecture topologique que Microsoft essaye de mettre au point pourraient aussi servir à faire des prévisions de valeurs d'actions[283].

Atos a aussi publié un libre blanc sur les applications du quantique dans la finance[284].

---

[281] Dans Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer, 2015 (13 pages).

[282] Voir ces slides dans cette présentation de D–Wave. Voir également cette présentation de D-Wave : Applications of Quantum Annealing in Computational Finance 2016 (29 slides) ainsi que le site QuantumForQuants créé par leurs soins.

[283] Comme documenté dans Decoding Stock Market Behavior with the Topological Quantum Computer 2014 (24 pages).

Depuis 2017, IBM met en avant des partenariats avec **JPMorgan Chase** et **Barclays** qui étudieraient les usages du quantique dans l'optimisation de stratégies de trading, l'optimisation de portefeuille d'investissement, le pricing et l'analyse de risques[285]. Un peu comme avec Watson à partir de 2013, ces banques en sont encore à l'évaluation du possible. Même si l'on peut envisager des algorithmes quantiques qui répondent à leurs besoins métiers, les capacités d'aujourd'hui des ordinateurs quantiques d'IBM sont tout à fait insuffisantes pour mettre quoi que ce soit en production.

De son côté, **D-Wave** est à l'origine avec quelques-uns de ses clients tels que la **Deutsche Bank** de la création du site web Quantumforquants, dédié aux usages du quantiques dans la finance.

La **NatWest** utilise des algorithmes « inspirés par le quantique » et s'exécutant sur calculateurs traditionnels pour optimiser ses portefeuilles d'investissement (HQLA pour High Quality Liquid Assets).

A noter également l'investissement de la **Royal Bank of Scotland** (RBS) dans la startup 1Qbits, avec Fujitsu et Allianz.

Marketing

Le marketing est aussi un domaine où les algorithmes d'optimisation de systèmes complexes réalisés à base d'ordinateurs quantiques pourraient être intéressants.

Cela concerne l'optimisation du mix marketing, celui de plans médias, ou la maximisation de revenus publicitaires, divers domaines qui sont également investis par le champ de l'IA[286].

Chez **Volskwagen**, on expérimente un système de recommandation de véhicules dans les sites de vente en ligne, avec un D-Wave.

S'opposent ainsi encore une fois des logiques prédictives basées sur l'exploitation de données passées (modèle connexionnistes) et des logiques de simulation basées sur la connaissance de règles de fonctionnement du marché. Ces règles ne relèvent cependant pas de la notion de systèmes experts de l'IA, qui gèrent des prédicats logiques (machin entraîne bidule), mais des modèles de causalité plus complexes[287].

---

[284] Voir Quantum finance opportunities: security and computation, 2016 (20 pages). C'est aussi le cas de Everest Group avec Quantum Computing in the Financial Services Industry – Infinite Possibilities or Extreme Chaos, 2018 (15 pages, $990… qui n'en valent pas trop la peine).

[285] Voir JPMorgan Chase Prepares for FinTech's Quantum Leap, par Constantin Gonciulea, 2017 ainsi que Why banks like Barclays are testing quantum computing, de Penny Crossman, juillet 2018.

[286] Comme vu dans Les usages de l'intelligence artificielle en novembre 2018, Olivier Ezratty (522 pages).

[287] Voir par exemple Display Advertising optimisation by quantum annealing processor de Shinichi Takayanagi Kotaro Tanahashi et Shu Tanaka de la Waseda University ainsi que A quantum-inspired classical algorithm for recommendation systems d'Ewin Tang, juillet 2018 (36 pages). Ce dernier algorithme classique dépasse la performance d'un algorithme quantique réalisé pour ordinateurs quantiques de D-Wave.

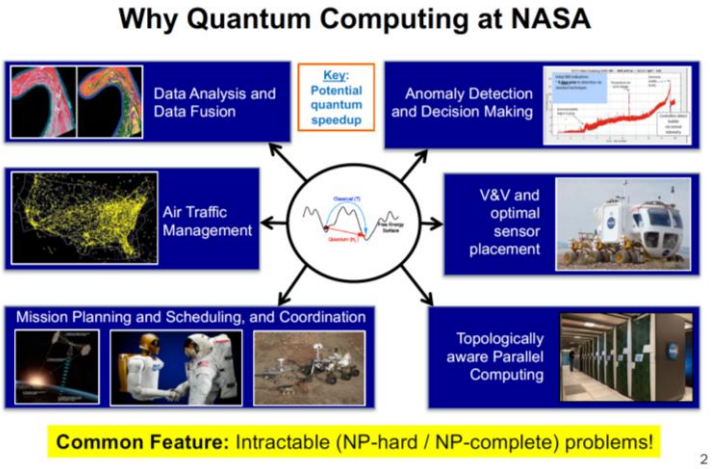
Défense et aérospatial

Le complexe militaro-industriel a toujours été un grand consommateur d'informatique de pointe. Il n'est donc pas étonnant qu'il s'intéresse au quantique. C'est évidemment le cas aux USA mais aussi en Europe, avec Airbus qui est l'un des premiers industriels à s'intéresser aux applications du quantique.

Voici quelques études de cas publiées d'utilisation du quantique dans ce vaste secteur.

Cela commence avec **Lockheed Martin** qui s'est associée avec **Google** et la **NASA** pour tester des ordinateurs de D-Wave. Ils ont développé une solution de preuve formelle de fonctionnement de logiciels. La NASA a cofondé le laboratoire QuAIL (Quantum Artificial Intelligence Laboratory) avec Google, exploitant un D-Wave Two.

Ils testent des algorithmes quantiques d'optimisation dans différentes directions. Pour optimiser le remplissage de vaisseaux spatiaux, une variante de l'algorithme du remplissage du coffre de voiture, sur les versions quantiques d'algorithmes de machine learning et deep learning, sur la décomposition de problèmes et l'informatique embarquée[288].



En 2015, **Raytheon** et **IBM** démontraient l'efficacité d'un algorithme quantique utilisant une "boite noire" ou "oracle" pour reconstruire une chaine de bits inconnue, le tout fonctionnant sur un ordinateur quantique universel d'IBM de 5 qubits[289]. On est cependant loin d'un cas d'usage.

Le groupe **Airbus** a de son côté créé une équipe basée sur leur site de Newport au Pays de Galle, qui s'attaque aux usages du quantique, notamment dans l'analyse d'imagerie aérienne (pas évident…) ou pour la conception de nouveaux matériaux (plus évident). Ils veulent aussi optimiser l'écoulement d'air sur les ailes, un problème qui relève aujourd'hui de la simulation par éléments finis. Ils pourraient essayer d'optimiser les souffleries d'air climatisé dans les avions, la plus grosse source de bruit d'habitacle, devant les moteurs de l'avion !

Dans un domaine différent, les marines sont intéressées par la métrologie quantique et plus précisément par les outils de mesure de précision de la gravité qui permettent de détecter des sous-marins. En fait, des sonars quantiques ! Ce genre de métrologie est la spécialité de la startup française **Muquans**. Il faut aussi compter avec **Thales**.

---

[288] C'est bien décrit dans Quantum Computing at NASA: Current Status de Rupak Biswas, septembre 2017 (21 slides) d'où provient le schéma de cette page.

[289] C'est documenté dans dans Demonstration of quantum advantage in machine learning (12 pages).

Renseignement

Le monde du renseignement et des écoutes ciblées est évidemment à l'affut du quantique. L'algorithme de Shor est la principale application visée par les organisations gérant les écoutes électroniques comme la **NSA** et tous ses confrères. Ce sont des pompiers pyromanes qui sont à la fois impatients de pouvoir décoder les informations interceptées auprès de cibles diverses (dépêches d'ambassades, informations techniques dans l'industrie, etc) et de protéger les communications sensibles de leurs propres Etats contre ce type de décryptage. Ils investissent donc simultanément dans l'informatique quantique (la dimension "pyromane") et dans les clés quantiques et cryptographies post-quantiques (la dimension "pompier").

Par contre, ces investissements ne sont pas très publics. La NSA a bien communiqué depuis presque une dizaine d'années sur la dimension pompier mais très peu sur la dimension pyromane. Ils ont sûrement fait l'acquisition des diverses générations d'ordinateurs D-Wave pour se faire la main dessus, en liaison avec **Lockheed Martin** qui est l'un de leurs grands fournisseurs.

D'autres service de renseignement occidentaux ont peut-être aussi fait l'acquisition de D-Wave, notamment les britanniques du CGHQ. La NSA est aussi en relation avec IBM et Google pour explorer la voie des ordinateurs quantiques universels supraconducteurs.

On peut lever un bout de voile de ces activités en détectant les subventions de laboratoires et de startups attribuées par l'IARPA, cette agence d'innovation du renseignement qui est pilotée par le DNI (Director of National Intelligence) qui coiffe l'ensemble du renseignement américain.

Industrie

L'industrie au sens large du terme est un autre débouché pour l'informatique quantique. Dès qu'il y a un problème complexe d'optimisation pour de l'ordonnancement, de la logistique ou de l'aide à la conception de systèmes complexes, le quantique aura son mot à dire.

Le Japonais **JSR Corporation** fait partie des entreprises travaillant avec IBM dans le quantique, principalement pour la création de nouveaux matériaux.

Enfin, il semblerait que le quantique puisse servir aux outils de conception assistée par ordinateur[290]. Mais le document de Robert Wille revient sur les basiques du calcul quantique sans être très dissert sur les usages dans la CAO.

[290] Selon Quantum computing dans la CAO. Computer-Aided Design for Quantum Computation de Robert Wille, Austin Fowler et Yehuda Naveh (Google et IBM), 2018 (6 pages).

Approche expérimentale

Comme pour nombre d'applications de l'intelligence artificielle à leurs débuts, l'adoption de l'informatique quantique par les entreprises passera par l'évaluation des techniques, des outils et par l'expérimentation. Les grandes entreprises des marchés cités dans cette partie peuvent lancer quelques expérimentations.

Le démarrage ne sera pas évident car peu d'entreprises de services ou même d'éditeurs de logiciels et de startups maitrisent le développement d'applications quantiques. Tout du moins en France. Dans un premier temps, les grandes entreprises françaises peuvent se tourner vers Atos, la seule entreprise du numérique en France à avoir des ressources et compétences dans l'informatique quantique. Elles peuvent aussi se tourner vers IBM qui commence à investir localement en compétences.

Un gros travail d'acculturation général à l'informatique quantique est à mener. C'est une tâche intellectuelle assez ardue. C'est un peu l'objet de de cette série d'articles que de vous mettre le pied à l'étrier en vous indiquant diverses pistes à explorer selon vos centres d'intérêt. Il faut en passer par là pour faire des choix éclairés sur le sujet.

Comme je vais le détailler dans les parties suivantes, la situation de l'offre d'ordinateurs quantiques est difficile à décoder. Nous avons d'une part l'offre commerciale opérationnelle du Canadien D-Wave qui est très décriée et qui est par contre opérationnelle, et de l'autre, des roadmaps d'ordinateurs quantiques universels comme chez IBM et Google, mais qui nécessitent encore de patienter au minimum quelques années avant de pouvoir les exploiter opérationnellement. J'en conclue que, malgré la polémique qui entoure D-Wave, il faut s'y intéresser et examiner ce que l'on peut faire avec. On n'est pas obligé de s'acheter un ordinateur quantique D-Wave à $15M pour commencer ! On peut les utiliser en cloud comme pour AWS ou un équivalent. Le coût technique de l'expérimentation est donc modeste. C'est surtout un coût en temps et intellectuel.

Acteurs des calculateurs quantiques

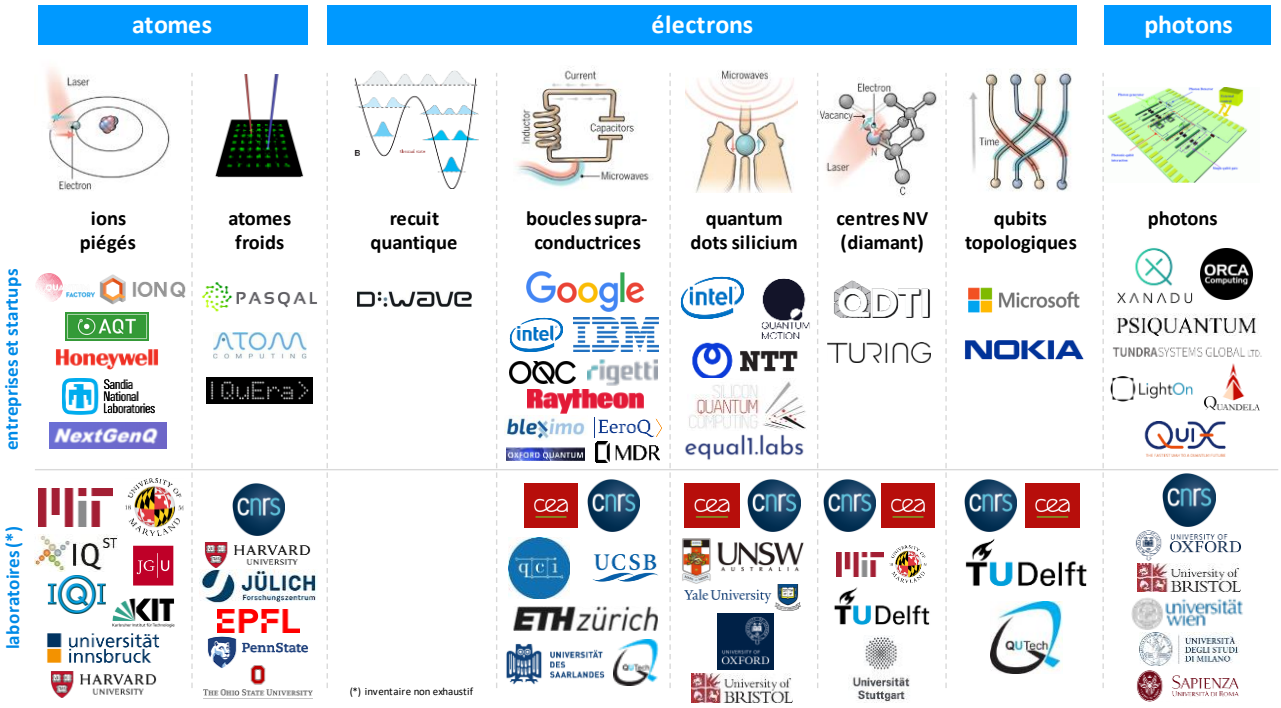
Nous voici à l'étape d'un panorama des acteurs que sont les constructeurs d'ordinateurs quantiques. Ils sont principalement Américains ou Canadiens. Cependant, pour quasiment toutes les technologies d'ordinateurs quantiques, divers laboratoires de recherche veillent au grain pour faire avancer l'état de l'art sans qu'il soit encore récupéré par une entreprise privée. Je les évoquerai lorsque cela sera nécessaire.

Comme nous l'avions vu dans la partie dédiée aux types de qubits, il se dégage six grandes catégories d'ordinateurs quantiques :

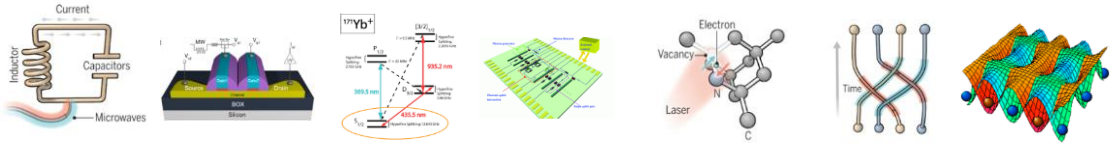
- Le **supraconducteur** à effet Josephson utilisé par les ordinateurs quantiques universels d'IBM, Google, au CEA ainsi que dans les ordinateurs adiabatiques de D-Wave.
- Les **ions piégés** que l'on trouve notamment chez IonQ, une spin-off de l'Université de Maryland.
- Le **topologique** avec les fermions de Majorana de Microsoft ainsi que Nokia qui n'existent pas encore.
- L'**optique linéaire** qui n'est pas très scalable mais potentiellement prometteuse.
- Les **CMOS** poussés notamment par Intel et le CEA.
- Les **atomes froids** comme le rubidium qui servent aussi bien à créer des ordinateurs quantiques analogiques que des ordinateurs à portes quantiques.
- Les **NV centers** à base de diamants, poussées notamment par la startup QDTI ainsi que par le CEA dans une approche hybride cavités diamants et supraconducteurs.

La technique de la résonnance magnétique nucléaire a été aussi envisagée mais abandonnée car elle ne donnait pas de résultats satisfaisants.

Nombre des entreprises privées de ce cheptel sont associées avec des laboratoires de recherche américains ou européens. Google collabore avec l'Université de Santa Barbara en Californie, IBM et Microsoft avec celle de l'Université de Delft aux Pays Bas, et IBM avec celle de Zurich. On voit qu'il y a déjà beaucoup de monde qui travaille sur les calculateurs quantiques !



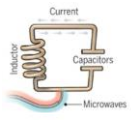
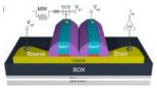
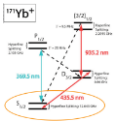
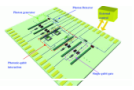
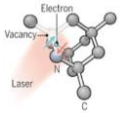
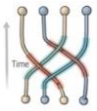
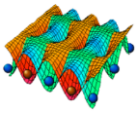
Ces catégories de technologies ont des niveaux de maturité très différents. Les qubits à base de supraconducteurs sont à ce jour les plus éprouvés. Les ions piégés, l'optique linéaire et les NV Centers ont du mal à "scaler". Les systèmes à base de spins d'électrons pourraient scaler mais il est difficile d'y gérer l'intrication des qubits. Enfin, les fermions de Majorana sont encore dans les limbes.



	supra-conducteurs	Si spin CMOS	ions piégés Yt ou Ca	photons	centres NV (diamant)	fermions de Majorana	atomes froids
qubits	supracon-ducteurs + effet Josephson	spin d'électrons dans semi-conducteur	ions piégés magnéti-quement	photons	spin électronique du centre NV	quasi-particules faites de paires d'anyons	niveau électronique de l'atome
état	phase de résonnance ou sens du courant	spins d'électrons	niveau énergétique de l'ion piégé	polarisation, temps, espace, couleur	état du spin électronique	sens de l'anyon	niveau orbital d'électron
portes	micro-ondes 5 GHz et effet Josephson	micro-ondes	laser	interférence quantique	micro-ondes	inversions 2D d'anyons	micro-ondes, émission de photons
mesure	magnétomètre ou couplage à un résonateur micro-onde	consersion spins to charge	fluorescence	détecteur de photons	fluorescence	fusion d'anyons	ionisation et recueil d'électron
# max de qubits	53 qubits (IBM et Google)	2 qubits (UNSW)	**79 (IonQ)**	20 (Chine)	10 qubits (QDTI)	0	51

en rouge : chipsets non caractérisés et benchmarkés.

source : Olivier Ezratty, « Comprendre l'informatique quantique », 2020

	 supra-conducteurs	 Si spin CMOS	 ions piégés Yt ou Ca	 photons	 NV centers (diamant)	 fermions de Majorana	 atomes froids
taille qubits	$(100\mu)^2$	$(100nm)^2$	$(1mm)^2$	$(100\mu)^2$			atomes
fidélité porte	99,4%	>98%	99,9%	98%	92%		98%
fidélité mesure	95%	98%	99,9%	50%	93%		99%
vitesse	250 ns	≈5µs	100µs	1ms			
variabilité	3%	0,1%-0,5%	0,01%	0,5%			
température	15mK	1K	300K	4K	300K	15mK	15mK
qubits intriqués	53 (IBM et Google)	2 (UNSW)	20 (IonQ)	20 (Chine)	6		
fabrication							
scale	53	2 (so far)	79				51

sources : Maud Vinet, CEA-Leti, janvier 2019 + compléments Pascale Sénellart et Olivier Ezratty,février 2020

Autre point, les startups ne sont pas si nombreuses dans ce tableau. D-Wave se porte bien mais Rigetti évolue plus lentement tout comme QDTI et IonQ. Enfin, ce paysage est largement dominé par les USA, même s'il n'intègre pas les initiatives chinoises comme celle d'Alibaba.

Recuit quantique

Après avoir brossé un tableau général des acteurs du marché des ordinateurs quantiques, nous allons creuser l'offre des ordinateurs quantiques adiabatiques utilisant le recuit quantique.

Le recuit quantique, "quantum annealing" en anglais, est une technologie particulière d'ordinateur quantique qui repose bien sur la mécanique quantique et des qubits, mais avec des caractéristiques et niveaux de performance intermédiaires entre ceux des supercalculateurs traditionnels et ceux des ordinateurs quantiques universels. Il n'existe qu'un seul acteur commercial sur ce marché : le Canadien **D-Wave**. Le principe général consiste à établir des liaisons entre qubits avec des poids, comme dans des réseaux de neurone du deep learning, puis à faire trouver un point d'équilibre au système en modifiant ces poids pour identifier un minimum énergétique de l'ensemble. Ce minimum doit correspondre à la solution recherchée du problème. Le processus est dit adiabatique car il n'y a pas de transfert énergétique entre le chipset de l'ordinateur et son environnement. Le système doit cependant être initialisé dans un état proche de la solution du problème, évaluée avec un ordinateur classique. Les algorithmes adiabatiques sont donc souvent des algorithmes hybrides.

Côté recherche, cette voie est aussi explorée par la IARPA. C'est intégré dans le projet **Quantum-Enhanced Optimization** (QEO) qui vise à créer un calculateur adiabatique n'ayant pas certaines des limitations de ceux de D-Wave, notamment en termes de connectivité et de qualité des qubits employés. Comme il se doit, au vu de la mission de l'IARPA, l'objectif est d'accélérer la mise en production d'ordinateurs quan-

tiques capables d'exécuter l'algorithme de Shor de factorisation de nombres entiers pour casser la sécurité à clés publiques de communications interceptées.

Je cite également ici le Japonais **Fujitsu** qui annonçait début juin 2018 un ordinateur à recuit digital fonctionnant à température ambiante, mais sans faire appel à du quantique. Il concurrence directement l'offre de D-Wave mais avec une solution qui semble plus simple à mettre en œuvre.

Situé à Vancouver, le Canadien **D-Wave** (1999, $205M) est le seul fournisseur d'ordinateurs quantiques commerciaux à ce jour, en mettant de côté ceux qui proposent l'accès à des ordinateurs quantiques limités en nombre de qubits dans le cloud. Même s'il s'agit d'ordinateurs adiabatiques présentant des limitations techniques par rapport aux ordinateurs quantiques universels, ils ont l'avantage d'exister, de faire avancer le secteur et de permettre le test d'algorithmes quantiques dans une large gamme d'applications. Celles-ci semblent cependant demeurer des "proofs of concept" d'après les études de cas publiées.

L'histoire de cette startup qui a levé $194M est fascinante pour ce qui est du timing. Créée en 1999, elle met 8 ans à prototyper sa première puce de qubits, contenant 4 qubits. Il leur faut en tout 10 ans pour vendre un premier ordinateur quantique. Quelle patience pour leurs investisseurs ! Pendant ces 10 ans, ils lèvent $31M. Ils obtiennent ensuite un financement de $1,2M en 2012 de la part d'InQTel, le fonds d'investissement de la CIA. Les levées de fonds suivantes, dont une partie est en obligations convertibles, leur permettent de tenir le coup, en plus des premières commandes dont certaines sont publiques et d'autres confidentielles. Ces dernières viennent au minimum de la NSA, si ce n'est d'autres services de renseignement occidentaux, probablement chez les partenaires de l'alliance "five eyes" que sont les pays du Commonwealth comme UK, l'Australie, le Canada et la Nouvelle-Zélande. En 2011, D-Wave signait d'ailleurs un partenariat avec Lockheed Martin, qui travaille beaucoup pour la NSA. En tout, la startup a obtenu 13 tours de financements !

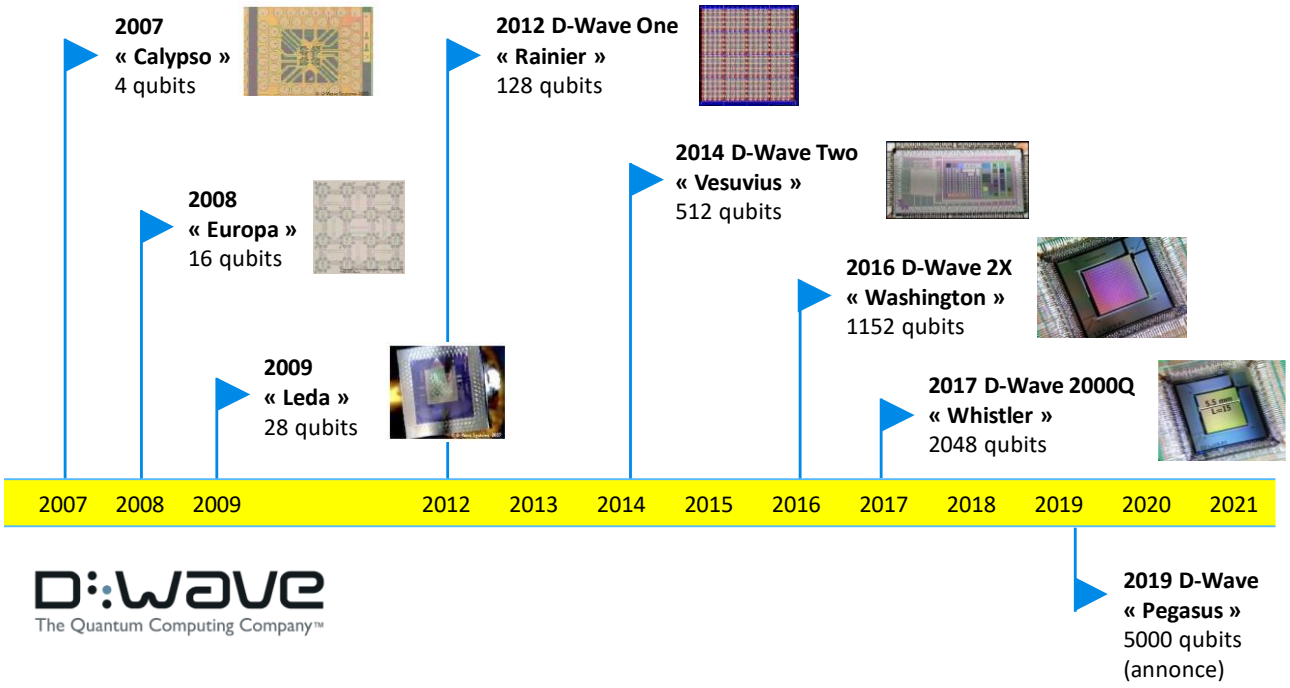
D-Wave a été créé par Geordie Rose (leur premier CTO et un moment CEO), Haig Farris, Bob Wiens et Alexandre Zagoskin, anciennement en charge de la recherche. Geordie Rose a obtenu un doctorat en physique des matériaux au milieu des années 1990 à l'University of British Columbia. La création de D-Wave est donc en ligne droite de ces travaux. Il rencontra Haig Farris pendant ses études alors que ce dernier enseignait l'économie.

L'équipe de direction de D-Wave de 2018 n'a plus grand chose à voir avec celle de ses créateurs. Un seul des cofondateurs en fait encore partie, Eric Ladizinsky, qui joue un rôle de Chief Scientist.

Le CEO depuis 2009 est Vern Brownell, qui intervenait en juin 2019 dans une table ronde que j'animais dans la conférence Quantum Computing Business organisée par Bpifrance.

Leur CTO Alan Baratz a rejoint la société en 2017. On sent une forme de reprise en main[291].

D-Wave a développé sa solution de bout en bout d'ordinateur adiabatique à recuit quantique. Cela commence avec les puces quantiques, puis va jusqu'à l'ordinateur complet avec une enceinte de cinq couches d'isolation magnétique plus un système de réfrigération utilisant de l'hélium 3 et 4 liquide, dont la combinaison est nécessaire pour atteindre les 10 à 20 mK (milli-Kelvin, sachant que 0K = –273,15°C). Le système de cryogénie consomme environ 20KW. C'est à peu près l'essentiel de la consommation électrique de l'ordinateur qui s'élève au total à 25 KW. Les 5K qui restent sont surtout liés aux systèmes de contrôle informatique traditionnels qui sont externes à l'unité quantique de l'ordinateur. Un ordinateur quantique, hors refroidissement présente en effet la particularité d'être plutôt économe en énergie, surtout en comparaison de leurs équivalents dans les supercalculateurs.



Leur roadmap a avancé régulièrement avec les trois premières générations de prototypes entre 2007 et 2009 puis, à partir de 2012, quatre générations d'ordinateurs commerciaux, à commencer par le D-Wave One en 2012 avec ses 128 qubits et jusqu'au D-Wave 2000Q de 2017 avec ses 2048 qubits et 5600 coupleurs reliant les qubits par paires et 128 000 jonctions Josephson.

Les chipsets de D-Wave sont fabriqués aux USA dans une unité de production de composants du Californien **Cypress Semiconductors**. Le D-Wave 2000Q est commercialisé au prix catalogue de $15M. La puce quantique de cet ordinateur fait 5,5 mm de côté.

[291] Le cofondateur Geordie Rose a ensuite créé **Kindred.ai**, une startup qui vise à intégrer une intelligence générale (AGI) dans les robots. Il est devenu un véritable "singulariste". Ses interventions publiques sont assez déjantées. Il s'exprime ainsi sur les démons et sur les extraterrestres. Il quitte Kindred.ai début 2018 pour créer Sanctuary, une spin-off de Kindred, dédiée à l'AGI, la quête du Graal de l'intelligence artificielle générale !

Début 2019, D-Wave annonçait la prochaine génération de leurs systèmes à base de 5000 qubits de la génération Pegasus qui devrait être disponible d'ici mi 2020. Dans cette nouvelle archirecture, chaque qubit sera relié à 15 autres qubits versus 6 dans la génération précédente ce qui permettra de résoudre des problèmes plus complexes avec un nombre équivalent de qubits. Le tout avec des qubits dont le taux d'erreur serait diminué.

Le principe de base de l'ordinateur quantique adiabatique consiste à préparer ce que l'on appelle un "hamiltonien", un système quantique avec plusieurs qubits interconnectés. Cet hamiltonien est initialisé dans un état qui est proche de la solution du problème que l'on souhaite résoudre.

L'ordinateur va alors faire évoluer cet hamiltonien de façon adiabatique vers l'hamiltonien de la solution du problème posé en respectant un grand nombre de contraintes préalables que je ne vais pas décrire ici.

Quantum Machine Language Programming

QUBIT	q_i	**Quantum bit** which participates in annealing cycle and settles into one of two possible final states: {0,1}
COUPLER	$q_i q_j$	Physical device that allows one **qubit to influence another qubit**
WEIGHT	a_i	Real-valued **constant associated with each qubit**, which influences the qubit's tendency to collapse into its two possible final states; controlled by the programmer
STRENGTH	b_{ij}	Real-valued **constant associated with each coupler**, which controls the influence exerted by one qubit on another; controlled by the programmer
OBJECTIVE	Obj	Real-valued **function which is minimized** during the annealing cycle

$$Obj(a_i, b_{ij}; q_i) = \sum_i a_i q_i + \sum_{ij} b_{ij} q_i q_j$$

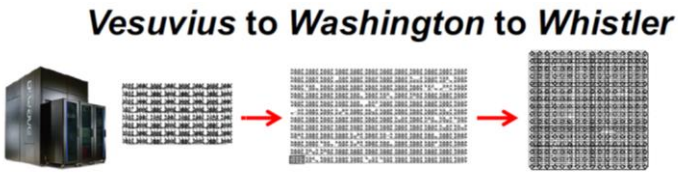
Source de l'illustration *ci-dessus* Practical Quantum Computing - An Introduction par Alexander Condello, D-Wave, février 2019 (50 slides).

Cela relève de la recherche d'un minimum énergétique. Elle est facilitée par l'effet tunnel quantique qui permet au système de trouver facilement des minimums globaux au lieu d'être coincé dans des minimums locaux, un problème qui rappelle celui de la descente de gradient dans l'entraînement de réseaux de neurones.

Ce type d'ordinateur est capable de résoudre des problèmes dits NP-complets, une catégorie des problèmes de logique théoriquement résolus dans un temps polynomial mais qui le sont en pratique en temps exponentiel. Je vous passe les détails sur les débats sur les problèmes P, NP, NP-complet et sur l'équivalence recherchée entre problèmes P et NP ! C'est le cas des problèmes de routage, de définition de parcours de voyageurs du commerce et équivalents.

En théorie, les algorithmes conçus pour des ordinateurs quantiques universels avec des portes quantiques exécutées séquentiellement peuvent être convertis en algorithmes exécutables sur ce type d'ordinateur et réciproquement[292].

Les qubits des ordinateurs de D-Wave sont connectés à leurs voisins immédiats, pas à l'ensemble des qubits du système. Ils peuvent tout de même être mis en cohérence avec de nombreux qubits distants. C'est une architecture que l'on retrouve cependant dans les architectures de qubits « 2D » comme celles des qubits supraconducteurs universels.



D-Wave Two	D-Wave 2X	D-Wave 2000Q
512 (8x8x8) qubit "Vesuvius" processor	**1152** (8x12x12) qubit "Washington" processor	**2048** (8x16x16) qubit "Whistler" processor
509 qubits working – 95% yield	**1097** qubits working – 95% yield	**2038** qubits working – 97% yield
1472 *J* programmable couplers	**3360** *J* programmable couplers	**6016** *J* programmable couplers
20 mK max operating temperature (**18 mK** nominal)	**15 mK** max operating temperature (**13 mK** nominal)	**15 mK** max operating temperature (*nominal to be measured*)
5% and **3.5%** precision level for *h* and *J*	**3.5%** and **2%** precision level for *h* and *J*	*To be measured*
20 us annealing time **12 ms** programming time	**5 us** annealing time (4X better) **12 ms** programming time	**5 us** annealing time **9 ms** programming time (25% better) **New:** anneal offset, pause, quench
6 graph connectivity per qubit	**6** graph connectivity per qubit	**6** graph connectivity per qubit

Elle présente divers inconvénients comme une montée en puissance qui n'est pas exponentielle avec l'ajout de qubits, mais dite quadratique, soit, en fonction de la racine carrée de leur nombre. Elle n'offre donc pas les améliorations de performance qui sont apportées par les ordinateurs quantiques universels[293].

L'initialisation du D-Wave 2000Q dure 25 ms, le temps de convergence du système (annealing) est de 20 µs et le temps de lecture dure 260 µs, ces deux étapes étant généralement répétées plusieurs fois et les résultats moyennés, une pratique qui ne semble pas être de rigueur avec les ordinateurs quantiques à portes universelles.

Selon John Preskill[294], il n'existe pas de base théorique convaincante de l'avantage du recruit quantique qui est une des formes d'ordinateur quantique adiabatique. Selon lui, cette architecture n'est pas théoriquement aussi scalable que les ordinateurs quantiques universels. Qui plus est, un même algorithme va demander beaucoup plus de qubits avec D-Wave qu'avec un ordinateur quantique universel, sachant que le rapport actuel est de 2048 vs 50 côté disponibilité, ce qui égalise les choses.

Comme tous les grands acteurs du quantique, D-Wave a développé une plateforme logicielle supportant les couches basses de la création d'algorithmes quantiques pour ses machines.

---

[292] C'est documenté dans Adiabatic quantum computation is equivalent to standard quantum computation, 2005 (30 pages) que nous avons déjà cité dans une partie précédente portant sur la complexité des problèmes gérables par des ordinateurs quantiques ainsi que dans How Powerful is Adiabatic Quantum Computation? de Wim van Dam, Michele Mosca et Umesh Vazirani, 2001 (12 pages).

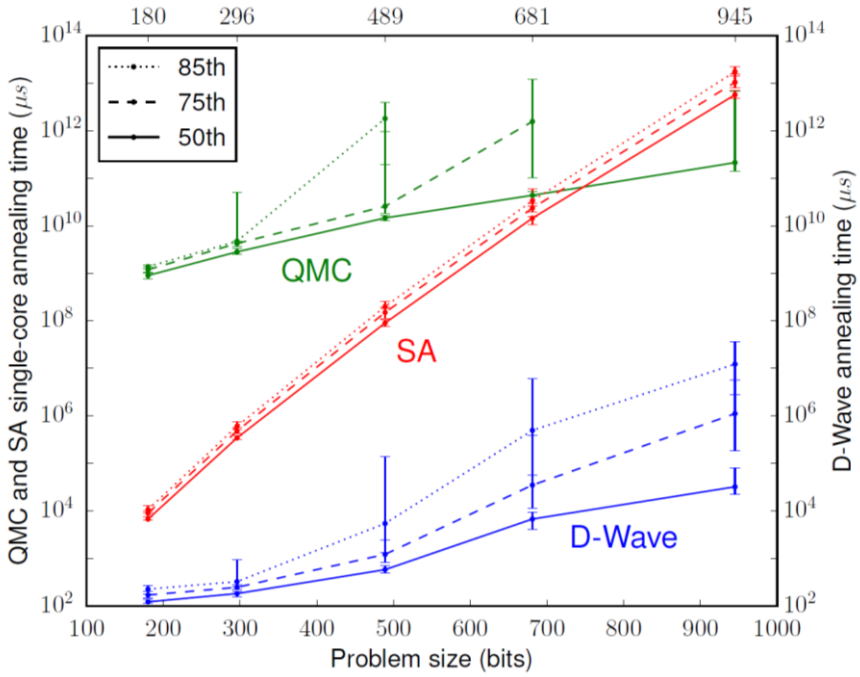
[293] Voir à ce sujet Limits of quantum computing de Jon Borwein (2016).

[294] Dans Quantum Computing for Business, 2017 (41 slides).

Ils ont aussi quelques partenaires logiciels comme **1QBit**. Les outils proposés comprennent à haut niveau Qsage, un outil qui sert à définir des problèmes d'optimisation, ToQ, un outil équivalent pour la programmation par contraintes, puis à un niveau intermédiaire, qbsolv qui permet de distribuer un problème complexe sur plusieurs passes de D-Wave et au niveau le plus bas, les instructions QMI pour piloter les qubits. Ils proposent aussi Quadrant, un framework permettant de préparer des D-Wave pour résoudre des problèmes de machine learning.

Comme les ordinateurs D-Wave sont les seuls qui soient utilisés chez des clients, les études de cas d'usage sont les plus nombreuses, même si elles sont assez exotiques et relèvent le plus souvent de "proof of concepts" et pas encore de mise en production.

La plus connue est celle Google et de la NASA réalisée avec un D-Wave de 2013 pour la résolution d'un problème d'optimisation et de combinatoire dans un graphe dont l'algorithme avait été conçu en 1994.



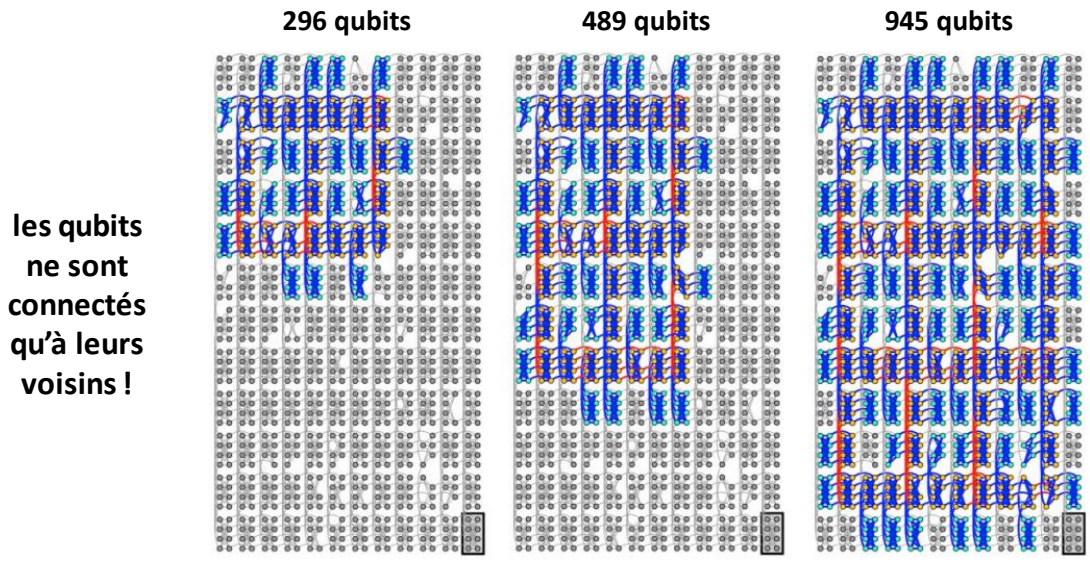
Google annonçait avoir obtenu une performance 100 millions de fois supérieure à celle d'ordinateurs traditionnels[295]. Les éléments de comparaison portaient sur deux algorithmes leur étant destiné le "simulated annealing", simulant l'ordinateur D-Wave sur ordinateurs classiques et une QMC (Quantum Monte Carlo) optimisée pour ordinateur traditionnel, et qui donne de meilleurs résultats en termes de montée en puissance que l'émulation du quantique sur HPC. Les critiques ont été nombreuses sur cette performance[296].

Le layout physique de qubits utilisé pour résoudre ce problème exploitait respectivement 296, 489 et 945 qubits, comme illustré *ci-dessous*.

---

[295] Dans Google's D-Wave 2X Quantum Computer 100 Million Times Faster Than Regular Computer Chip par Alyssa Navarro dans Tech Times, novembre 2015. Et documentée dans What is the Computational Value of Finite Range Tunneling (17 pages).

[296] Dont Temperature scaling law for quantum annealing optimizers, 2017 (13 pages), qui pointe les limitations du recuit quantique.



"What is the Computational Value of Finite Range Tunneling" – Google, janvier 2016

D-Wave communique sur quelques-unes de ses références :

- Chez l'équipementier japonais **Denso**, présentée au CES 2017 de Las Vegas, qui sert à gérer l'optimisation d'une flotte de véhicules de livraison de Toyota.
- Avec **Volkswagen** pour gérer l'exploitation d'une flotte de taxis à Beijing et pour mettre au point de nouvelles batteries (source).

VOLKSWAGEN

optimisation de trafic

exploitation de la position de 10 000 taxis à Beijing.

accenture 1QBit Biogen

criblage de molécules

avec Biogen, l'éditeur de logiciels 1QBit et la recherche d'Accenture

DENSO

optimisation de flotte

Denso et Toyota, présentée au CES 2017 sur le stand de Denso.

QXBranch

modélisation d'élections

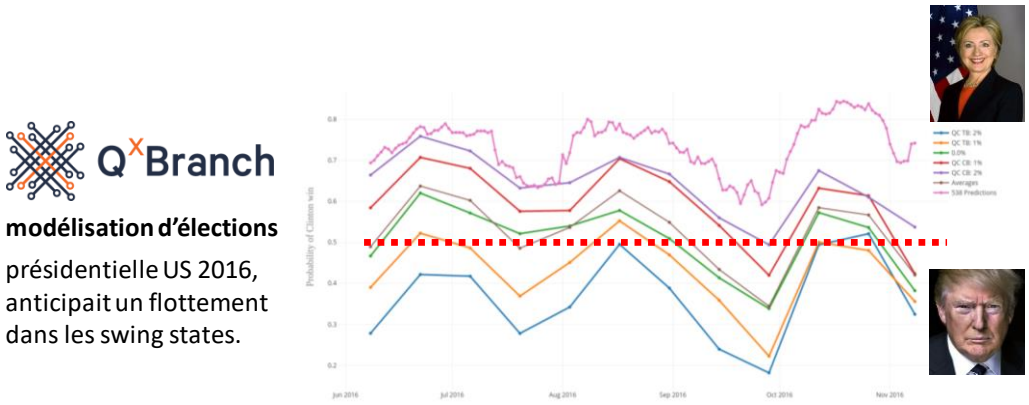
présidentielle US 2016, anticipait un flottement dans les swing states.

- Avec **Biogen**, **1Qbit** et **Accenture** pour du criblage de molécules visant à identifier des molécules pour un reciblage thérapeutique, avec un problème de colorisation de carte[297].
- Avec **Lockheed-Martin** qui a pu réduire la durée de procédures de validation de logiciels embarqués de 8 mois à 6 semaines avec un D-Wave et son outil QVTRace[298].

[297] Décrit dans Programming with D-Wave Map Coloring Problem 2013 (12 pages).

[298] Voir Quantum Computing Approach to V&V of Complex Systems Overview, 2014 (31 slides) et Experimental Evaluation of an Adiabatic Quantum System for Combinatorial Optimization, 2013 (11 pages).

- Avec la **NASA** qui a également expérimenté les D-Wave dans différents domaines, y compris pour la détection d'exoplanètes par analyse d'observations télescopiques par la méthode des transits ainsi que pour divers problèmes d'optimisation et de planification[299].
- La plus étonnante est cette analyse de sondages a posteriori de l'élection présidentielle par **QxBranch**. Elle anticipe un flottement dans les *swing states* qui ont décidé de l'élection de Trump via des analyses de corrélations entre états avec des matrices de corrélation difficiles à calculer en temps normal. En gros, l'algorithme amplifie les phénomènes "de battements d'ailes de papillons" à l'aide de machines de Boltzmann. Petit détail : cette prévision a été réalisée après l'élection en question, ce qui enlève une bonne partie de son intérêt ! **Qxbranch** est une startup australienne qui a aussi créé une solution quantique dans la finance.



comparaison du modèle de prédiction du site 538 et des prédictions quantiques de QxBranch

- Avec des **simulations physiques de matière topologique et de changement de phase** comme dans Observation of topological phenomena in a programmabale lattice of 1,800 qubits, août 2018 (37 slides).

En résumé : le recuit quantique a beau être une technique contestée par nombre de spécialistes, elle a le mérite d'exister et d'être testable dans de nombreux cas d'usages. Il serait bête de s'en priver pour commencer à explorer les possibilités du calcul quantique quitte à se rabattre ensuite sur les ordinateurs quantiques universels lorsque ceux-ci dépasseront la centaine de qubits logiques[300].

---

[299] Voir la très intéressante présentation Quantum Computing at NASA: Current Status de Rupak Biswas, 2017 (21 slides) ainsi que Adiabatic Quantum Computers: Testing and Selecting Applications de Mark A. Novotny, 2016 (48 slides), dont de nombreux slides sont caviardés pour des raisons de confidentialité.

[300] Pour en savoir plus sur D-Wave, voici leurs explications sur la structure de leur matériel, une vidéo d'explication de la structure des chipsets de D-Wave, une vidéo de Linus, un bloggeur qui rentre dans les entrailles d'un D-Wave 2000Q de manière assez détaillée, D-Wave quantum computer de Gradu Amaierako Lana, 2016 (33 pages), la vidéo de l'intervention de Colin Williams à USI en juin 2018 à Paris (33 minutes) ainsi que Near-Term Applications of Quantum Annealing, 2016, une présentation de Lockheed Martin intéressantes sur les usages d'un ordinateur D-Wave (34 slides). Et les témoignages de leurs clients dans Qubits 2017. Voir aussi Brief description on the state of the art of some local optimization methods: Quantum annealing, Alfonso de la Fuente Ruiz, 2014 (21 pages).

A ce jour (mi 2019), D-Wave a installé 4 ordinateurs quantiques chez des clients et en opère une trentaine dans ses propres locaux, une bonne moitié étant dédiés à leur offre d'accès en cloud.

FUJITSU

Fujitsu est un des leaders mondiaux du marché des supercalculateurs. Il était donc logique, comme pour le Français Atos, qu'ils explorent des moyens de continuer à faire monter en puissance leur offre.

Fin mai 2018, le Japonais annonçait avoir mis au point un ordinateur utilisant le recuit digital à température ambiante. Il scalerait bien mieux que ceux de D-Wave[301].

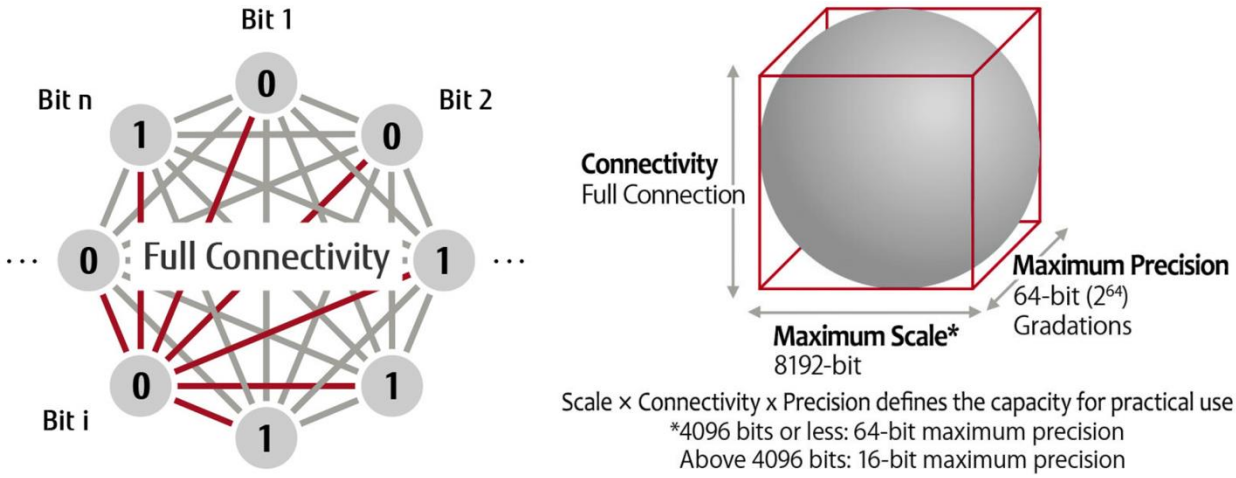
La technologie dénommée "Digital Annealer" est développée sur silicium en CMOS et en partenariat avec l'Université de Toronto. Elle serait déjà proposée dans le cloud. Elle sert à résoudre des problèmes d'optimisation et notamment à réaliser du criblage de molécules dans les biotechs.

Le "Digital Annealer" est un chipset dédié comportant 1 024 blocs de mise à jour de bits intégrant de la mémoire pour stocker leurs poids et avec une précision de 16 bits, des blocs logiques pour réaliser des inversion de valeurs, et les circuits de contrôle associés.

Cela fait penser à des réseaux de neurones à base de memristors dans le principe. Comme pour les D-Wave, les problèmes sont chargés dans le système sous forme de matrices avec des biais dans les liaisons entre éléments et le système recherche un état d'énergie minimum pour résoudre le problème. La partie logicielle est fournie par le Canadien 1QBit, dans lequel ils ont investi. Le DAU doit être fourni sous forme de services dans le cloud.

Ce système n'est cependant pas du tout quantique ! Il concurrence malgré tout directement D-Wave. Son concepteur, Hidetoshi Nishimori, du Tokyo Institute of Technology, pense que Fujitsu arrivera à créer des solutions plus performantes que celles de D-Wave. Fujitsu annonçait en 2019 sa seconde génération des puces, dotées de 8192 blocs. Ils prévoient d'atteindre ensuite un million de blocs alors que la montée en puissance prévue de D-Wave est bien plus lente. Finalement, le CMOS classique n'a pas dit son dernier mot !

[301] Voir Fujitsu's CMOS Digital Annealer Produces Quantum Computer Speeds, 2018.



MemComputing, Inc.

J'ajoute ici le cas de la mystérieuse startup **MemComputing** (2016, USA) que l'on peut ranger dans une catégorie voisine de l'offre de Fujitsu. Ce n'est pas une solution quantique, mais elle s'inspire visiblement du calcul à recuit quantique. Et elle concurrence ce dernier si ce n'est le calcul à portes quantiques universelles. Tout du moins, elle espère !

Leur solution matérielle MemCPU Co-processor consiste à placer la mémoire près des unités de calcul dans des unités de traitement[302]. Mais ce n'est pas tout.

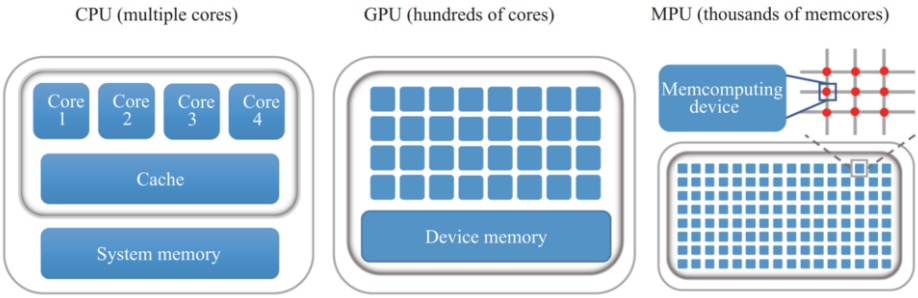
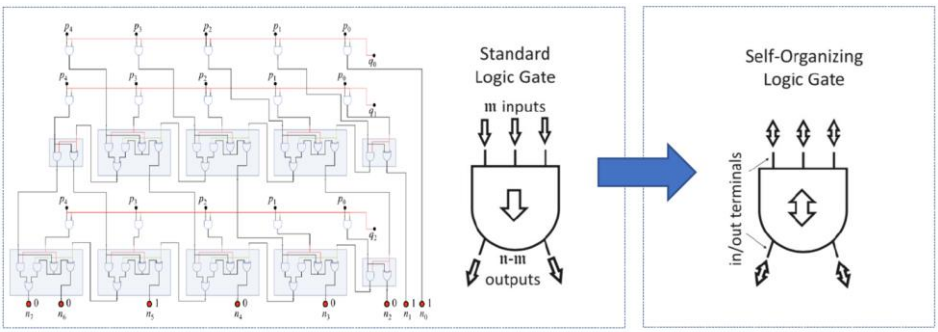


Figure 1 (Color online) Comparison of CPU, GPU, and MPU.

Ces cellules de calcul qui ressemblent à des memristors auraient des entrées et sorties symétriques interconnectées aux cellules avoisinantes et elles gèrent des nombres entiers.



A traditional Boolean circuit using logic Gate for prime factorization
It multiplies two integers p and q to give pq = n = 35 = (100011)$_2$ (in the little-endian notation).

Moving from traditional gates to terminal-agnostic gates

Elles permettraient de trouver automatiquement un équilibre complexe d'un système paramétré. C'est le principe des SOLGs (Self Organizing Logic Gates) du schéma *ci-dessus*[303].

[302] Elle est décrite dans Memcomputing: fusion of memory and computing par Yi Li & Al, 2017 (3 pages) d'où provient ce schéma.

[303] Les SOLGs sont décrites dans le brevet Self-Organizing Logic Gates and Circuits and Complex Problem Solving With Self-Organizing Circuits, mars 2018 (37 pages).

La société a été créée par le serial entrepreneur John Beane et deux chercheurs en physique, Massimiliano Di Ventra et Fabio Traversa qui ont une belle bibliographie sur le sujet du « memory computing » dont ils sont à l'origine[304].

Leu architecture permettrait de résoudre diverses classes de problèmes NP-complets et NP-difficiles[305] en temps polynomiaux. Ils annoncent des gains de performance significatifs : quatre ordres de grandeur pour les applications de machine learning, donc une performance multipliée par 10 000 ! Les domaines d'applications annoncés comprennent la résolution de problèmes de planification et d'optimisation comme celui du voyageur de commerce, de combinatoire [306], de bioinformatique, d'entraînement de réseaux de neurones[307] et même de factorisation de nombres entiers[308], à chaque fois, avec un gain exponentiel de temps de calcul par rapport aux méthodes classiques.

Pour l'instant, leur solution est émulée dans des ordinateurs classiques et fournie sous forme de SDK opéré dans le cloud qu'ils ont conçu en partenariat avec **Canvass Labs** (2017, USA). Leur composant électronique n'est pas encore fabriqué, même à l'état de prototype, et il n'est d'ailleurs pas évident de déterminer s'il est possible de le fabriquer.

Ils ont notamment réussi à traiter des problèmes de type MIPLIB (Mixed Integer Programming Library) considérés comme intractables avec une réponse en 60 secondes sur un serveur tournant sous Linux et avoir même battu un D-Wave. Cela sert à trouver une combinaison de nombres entiers donnés pouvant générer zéro une fois additionnés (le « Subset Sum problem »). La startup arrive à obtenir un avantage d'échelle quantique avec l'émulation de son procédé sur des processeurs traditionnels. Ce qui revient à remettre en cause toutes les théories actuelles de la complexité. Bref, à en donner le tournis.

Alors, cette technologie est-elle tout bonnement révolutionnaire et pourrait rendre caduque bon nombre d'efforts dans le calcul quantique ou il y a-t-il un ou plusieurs lézards ? Il y en a plein. Comment initialiser le système pour qu'il soit proche d'un minimum global ? Quelle est leur capacité réelle à créer ces SOLGs dans des composants CMOS actuels ? Comment gérer le bruit du système qui pollue les calculs ?

---

[304] Voir Universal Memcomputing Machines, par Fabio Traversa et Max Di Ventra, 2014 (14 pages) et Perspective: Memcomputing: Leveraging memory and physics to compute efficiently, par Fabio Traversa et Massimilio Di Ventra 2018 (16 pages).

[305] Voir Memcomputing NP-complete problems in polynomial time using polynomial resources and collective states, par Fabio Traversa, Massimilio Di Ventra & Al, 2014 (10 pages) et Evidence of an exponential speed-up in the solution of hard optimization problems, Fabio Traversa & Al, 2018. Enfin, voir cette Conférence de Massimiliano Di Ventra à Berkeley en 2016 (26 minutes).

[306] Voir Stress-testing memcomputing on hard combinatorial optimization problems par Fabio Traversa, Max Di Ventra & Al, 2018 (6 pages).

[307] Voir Accelerating Deep Learning with Memcomputing par Haik Manukian, Fabio Traversa et Massimiliano Di Ventra, 2018 (8 pages).

[308] Voir Polynomial-time solution of prime factorization and NP-hard problems with digital memcomputing machines, par Fabio Traversa et Max Di Ventra, 2017 (22 pages).

En fait, leur approche n'est pas scalable d'après plusieurs spécialistes dont le renommé Scott Aaronson [309]! Oubliez donc tout ce que vous venez de lire à leur sujet !

Supraconducteurs

Après avoir décrit l'offre de D-Wave, passons à celle des ordinateurs quantiques supraconducteurs à portes quantiques universelles. En effet, d'un point de vue physique, les ordinateurs adiabatiques de D-Wave et ceux de cette partie sont assez voisins, utilisant des variantes de l'effet Josephson dans des circuits supraconducteurs. La programmation et les capacités ne sont par contre pas du tout les mêmes.

Les supraconducteurs occupent pour l'instant la voie royale de l'ordinateur quantique, étant exploités à la fois par D-Wave avec ses ordinateurs adiabatiques et par IBM, Google, Intel et Rigetti sans compter le CEA français qui planche dessus et est même à l'origine d'une bonne part des technologies de ce domaine.

Dans le quantique universel, ce sont les ordinateurs qui scalent le mieux pour l'instant, même si le résultat est modeste avec un record en date de 72 qubits pour Google, qui n'est pour l'instant pas documenté au niveau du taux d'erreurs. Le record opérationnel en septembre 2019 est 53 qubits chez IBM.

Dans les qubits supraconducteurs, la circulation du courant est contrôlée par des portes à effet Josephson qui s'ouvrent en fonction de l'application d'un champ magnétique externe. C'est une sorte de robinet, un peu comme la base d'un transistor bipolaire.

Il existe plusieurs types de qubits supraconducteurs. Ils diffèrent par la manière d'encoder l'information quantique avec deux états bien distincts[310].

On distingue donc plusieurs types de qubits supraconducteurs :

- **Qubits de flux** : leur état correspond au sens de circulation du courant supraconducteur dans sa boucle. C'est le plus facile à comprendre et à visualiser. La mesure de l'état d'un tel qubit utilise un SQUID (superconducting quantum interference device), un magnétomètre qui va être capable de mesurer le sens du courant dans le qubit, donc son état 0 ou 1. C'est l'approche de D-Wave, de Rigetti, du MIT et de TU-Delft aux Pays-Bas.
- **Qubits de charge / transmon** : leur état correspond à des seuils de passage de courant dans la jonction Josephson de la boucle supraconductrice. De petites jonctions Josephson délimitent un îlot supraconducteur avec une charge électrique bien définie. Les états de base de tels qubits de charge sont les états de charge de l'îlot en couples d'électrons supraconducteurs appelés paires de Cooper.

---

[309] Voir A Note on `Memcomputing NP-complete problems...' and (Strong) Church's Thesis par Ken Steiglitz, 2015 (2 pages) qui démontre rapidement que cela n'est pas possible. Il en va de même pour Memrefuting par Scott Aaronson en 2017 et pour A review of « Memcomputing NP-complete problems in polynomial time using polynomial resources » par Igor Markov, 2015 (3 pages).

[310] C'est bien expliqué dans Practical realization of Quantum Computation (36 slides) ainsi que dans une conférence de Serge Haroche du Collège de France de 2011 (mais il faut s'accrocher…).

Ces qubits sont alimentés par des oscillateurs harmoniques utilisant des radio-fréquences allant de 5 à 10 GHz qui leur sont transmises par fils conducteurs électriques. L'approche d'IBM est une variante de qubit de charge dénommée transmon[311]. Google utilise aussi des transmons. C'est aussi l'approche du CEA à Saclay qui en est d'ailleurs à l'origine.

- **Qubits de phase** : ils utilisent des jonctions Josephson plus grandes que dans les qubits de charge. L'état du qubit correspond à deux niveaux d'énergie de courants dans une jonction Josephson. Cette approche est expérimentée par le NIST aux USA.

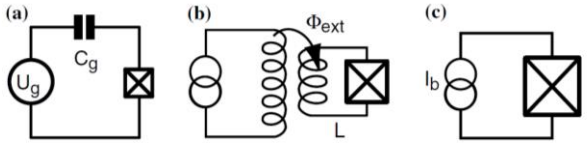
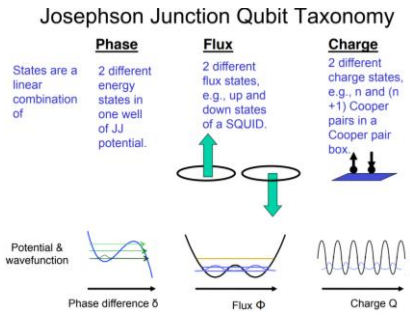


Fig. 4. The three basic superconducting qubits. (a) Cooper pair box (prototypal charge qubit); (b) RF-SQUID (prototypal flux qubit); and (c) current-biased junction (prototypal phase qubit). The charge qubit and the flux qubit requires small junctions fabricated with e-beam lithography while the phase qubit can be fabricated with conventional optical lithography.



source des schémas : Implementing Qubits with Superconducting Integrated Circuits de Michel Devoret, 2004 (41 pages) et Flux Noise in Superconducting Qubits, 2015 (44 slides).

Les limitations technologiques sont liées à la taille des qubits qui est de l'ordre du micron, ce qui rend difficile la création de grandes puces avec des millions de qubits, à la place qui est prise par les générateurs de micro-ondes allant de 4 à 7 GHz qui poserait encore plus de problèmes avec l'augmentation du nombre de qubits, au taux d'erreurs des qubits, aux limites de capacité des systèmes de cryogénie, notamment au niveau de la dimension des disques métalliques qui supportent les systèmes à chaque étage du "frigo". Divers travaux visent à prouver que l'on peut miniaturiser une partie de ces circuits de contrôle des qubits supraconducteurs mais ils ne semblent pas avoir aboutit à ce stade à des réalisations concrètes.

L'autre difficulté rencontrée concerne le câblage. Il faut plusieurs câbles reliés à l'extérieur de l'enceinte cryogénique pour contrôler et lire leur état[312].

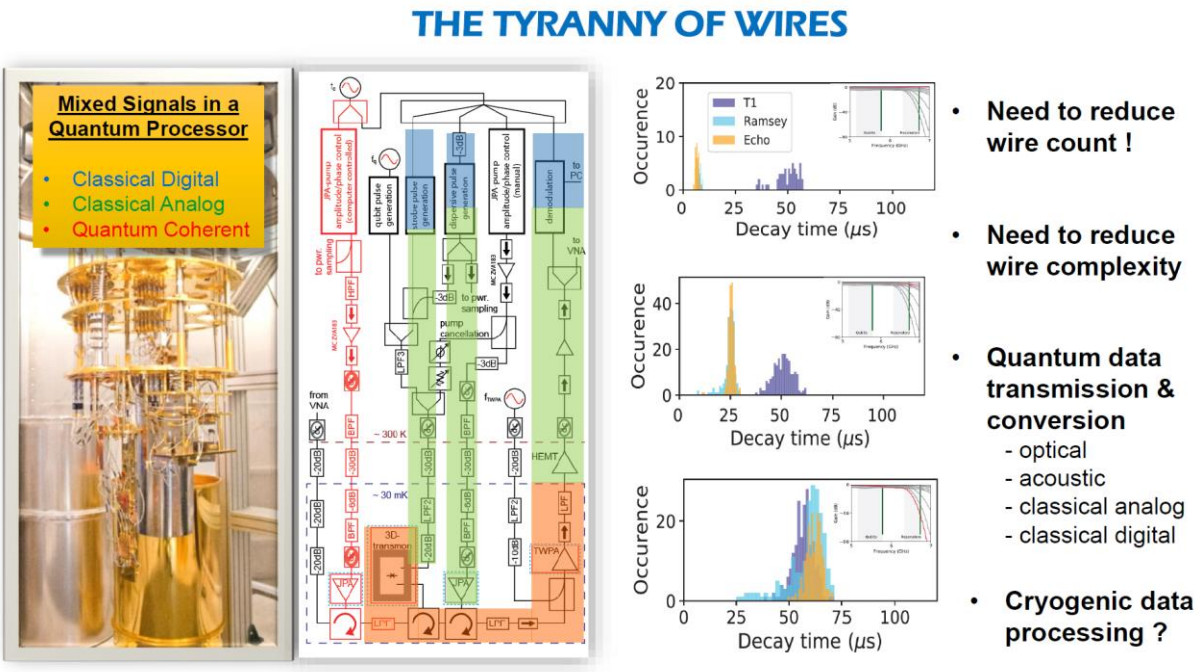
Les progrès sont constants dans la réduction du bruit des qubits dans cette technologie. Ce bruit a plusieurs origines comme les fluctuations de charge, les électrons baladeurs, les impuretés dans les matériaux notamment comportant des atomes d'oxygène et les perturbations magnétiques, ce qui explique pourquoi les ordinateurs quantiques comme ceux de D-Wave sont isolés dans des cages de Faraday avec jusqu'à 16 couches de protection contre les perturbations magnétiques.

[311] Pour « transmission-line shunted plasma oscillation qubit ».

[312] C'est bien expliqué dans Superconducting Circuits Balancing Art and Architecture de Irfan Siddiqi, 2019 (34 slides) d'où est extrait le schema suivant.

Pour ce qui est de la mesure de l'état des qubits supraconducteurs, une équipe de chercheurs canado-américaine propose une méthode optique de mesure miniaturisable[313].

Une variante a été proposée en 2018 par Robert McDermott de l'Université Wisconsin-Madison, l'objectif étant d'améliorer la fiabilité de la mesure. Elle serait pour l'instant de 92% et pourrait monter à 99%[314].



Les qubits supraconducteurs utilisent sinon souvent du **niobium** pour ses portes à effet Josephson, qui peut être remplacé par de l'**aluminium**, utilisé notamment chez Rigetti.Le niobium est un métal qui n'est pas rare. Sous-produit de l'extraction de minerais, il est généré à raison de plus de 60 000 tonnes par an, provenant essentiellement du Canada et du Brésil. Il est surtout utilisé dans des alliages spéciaux ainsi que dans les aimants supraconducteurs comme dans ceux de l'accélérateur de particules géant LHC du CERN à Genève.

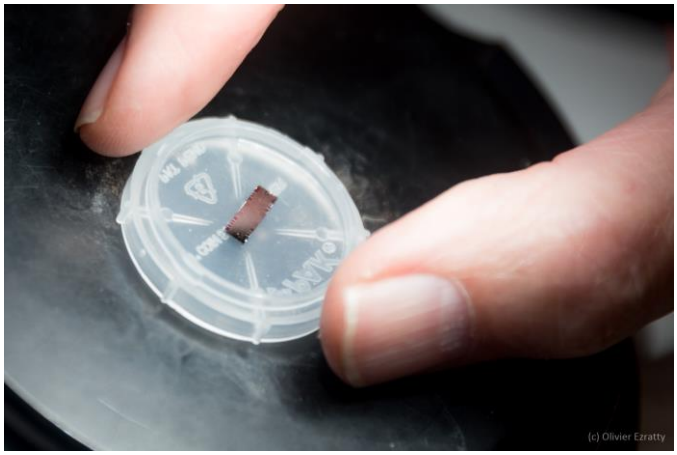
D'un côté historique, les premières boites de paires de Cooper ont été créées expérimentalement en 1997 au CEA de Saclay par Vincent Bouchiat. NEC a créé le premier qubit supraconducteur en 1999. Le laboratoire de Daniel Estève au CEA Saclay a créé son premier qubit supraconducteur en 2002.

Ci-dessous, Daniel Esteve présentant ce premier qubit supraconducteur (à moins que cela soit le premier chipset à deux qubits…). Le premier processeur complet intégrant deux qubits supraconducteurs est arrivé en 2012.

[313] Voir Heisenberg-limited qubit readout with two-mode squeezed light, 2015 (12 pages).

[314] Dans Measurement of a Superconducting Qubit with a Microwave Photon Counter, mars 2018 (11 pages).

Comme les paires de Cooper sont l'une des rares ensembles de particules qui sont des bosons, ils peuvent être condensés dans le même état quantique, ce qui permet à un qubit de charge ou de flux d'avoir une propriété quantique "macro" de plusieurs (des millions) quantums, ces paires de Cooper. C'est un des cas de qubits à base de plusieurs particules élémentaires au lieu d'une seule.



L'équipe de physiciens de Daniel Estève au CEA de Saclay continue de travailler sur les qubits supraconducteurs tendance transmon avec en ligne de mire la création de qubits plus stables et générant moins d'erreurs. C'est une approche de recherche long terme qui fait partie du champ de la physique de la matière condensée. En d'autres termes, de la matière à très basse température[315].

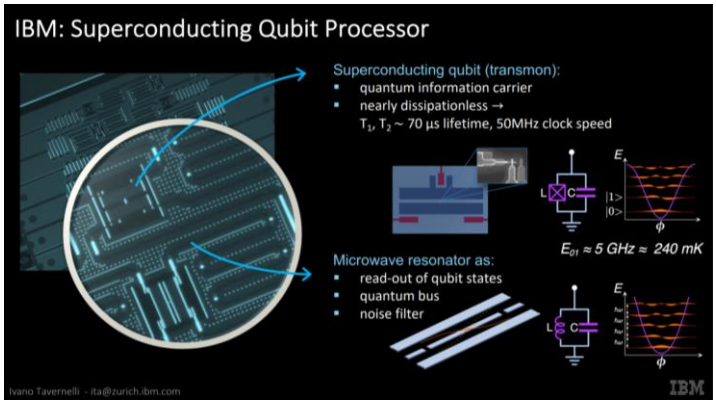
IBM est un des rares grands acteurs du numérique qui investit dans la recherche fondamentale et depuis très longtemps. Qui fait de la recherche fondamentale ? Principalement IBM, Microsoft, Google, les équipementiers et les opérateurs télécoms. Les Bell Labs issus du démantèlement d'AT&T en 1982 font maintenant partie de Nokia après être passée par Lucent et Alcatel-Lucent. Le reste des acteurs, tels qu'Apple se contente de créer des produits. Facebook fait un peu de recherche fondamentale en IA mais peu en physique fondamentale.

A ce titre, IBM est l'un des plus avancés dans la recherche sur le quantique universel, ayant tout misé sur les supraconducteurs à effet Josephson. Les efforts d'IBM dans le quantique sont sous l'aile de la marque IBM Q. Ils sont pilotés par les chercheurs de leur site de Yorktown dans l'Etat de New York, en liaison avec différents laboratoires d'IBM dans le monde dont celui de Zurich, avec diverses universités américaines et avec l'Université ETH Zurich.

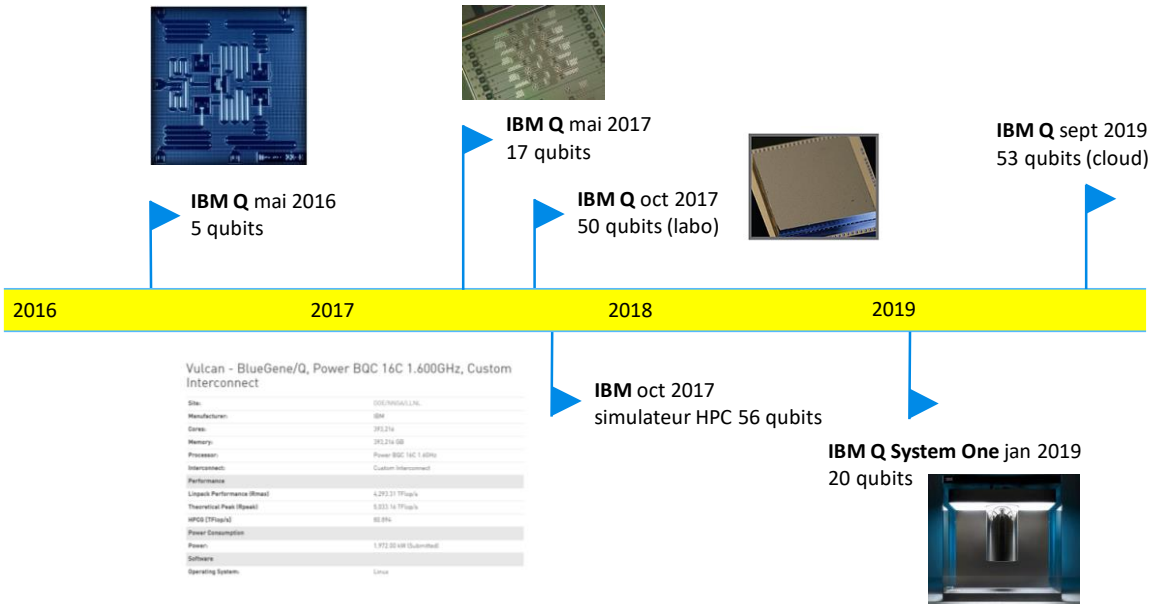
Ils ont annoncé divers partenariats en Europe comme avec l'Université de Montpellier ou le Franhauffer en Allemagne, pour en gros évangéliser le marché des développeurs et des chercheurs et les pousser à développer des logiciels avec leurs outils de développement et leurs ordinateurs quantiques dans le cloud.

[315] Pour en savoir plus sur les qubits supraconducteurs et les défis de leur mise au point, voir notamment cette excellente présentation du MIT : Quantum Engineering of Superconducting Qubits, 2018 (58 slides) ainsi que Quantum Physics with Superconducting Qubits de Andreas Wallraff, de l'ETH Zurich, 2016 (49 slides). Voir également Quantum Computing: State of Play de Justin Dressel, 2018 (34 slides) qui comprend une bonne explication sur le fonctionnement des qubits supraconducteurs.

La technologie retenue par IBM est celle des qubits supraconducteurs « transmon » déjà couverte plus haut dans ce document[316]. En quelques années, IBM a fait évoluer rapidement le nombre de qubit de ses prototypes d'ordinateurs quantiques. On est ainsi passé de 5 Qubits en 2016 (vidéo) à 14 qubits vers 2017.



En 2017, IBM annonçait avoir atteint 50 qubits mais ceux-ci ont nécessité deux années de mise au point[317]. En septembre 2019, IBM annonçait enfin la mise à disposition de 53 qubits opérationnels et bien intriqués dans le cloud, le même jour que la fuite sur la suprématie quantique de Google. Leurs efforts portent surtout sur la réduction du bruit pouvant affecter la qualité des calculs quantiques. Ils travaillent aussi sur l'utilisation de "surface codes", ces arrangements de qubits en matrices qui permettent de gérer la correction des erreurs.



IBM propose ses qubits dans le cloud. Ils avaient démarré avec 5 qubits en 2016, puis étaient passés à 16 qubits et en sont à 20 qubits, depuis novembre 2017 (source). Ils proposent un outil graphique en ligne de création de son algorithme quantique (*ci-dessous*, avec la version 5 qubits lancée en 2016)[318]. Les qubits d'IBM dans le cloud sont déjà utilisés par des milliers de chercheurs, entrepreneurs et étudiants dans le monde.

---

[316] Le schéma est issu de Quantum Computing with superconducting qubits: Applications in Chemistry and Physics, Ivano Tavernelli d'IBM Research, février 2019 (58 slides).

[317] Je m'y perds d'ailleurs un peu dans les annonces d'IBM avec leurs 5, 14, 17, 20, 50 et 53 qubits qui se sont succédées ces dernières années et qui mélangent des prouesses de laboratoire et des disponibilités opérationnelles dans le cloud.

[318] Voici un petit tutoriel de programmation utilisant le SDK open source Qiskit qui supporte de son côté le langage de bas niveau OpenQASM qui pilote les qubits d'IBM. Voir aussi cette vidéo de vulgarisation de haut niveau par Talia Gershon.

Ceci étant, les qubits d'IBM ont été benchmarkés par Kristel Michielsen et leur qualité semble bien faible[319]. En particulier, les portes CNOT semblent générer un fort taux d'erreurs.

IBM battait aussi un record d'émulation de 56 qubits en 2017, sur un supercalculateur classique de leur cru, le Vulcan BlueGene installé au Lawrence Livermore National Laboratory en Californie[320]. Il a été battu depuis par d'autres, déjà évoqués.

En janvier 2019 au CES de Las Vegas, IBM annonçait le Q System One, présenté comme étant le premier système informatique quantique universel intégré du monde, à usage scientifique et commercial. C'est un ordinateur quantique à qubits supraconducteurs à portes universelles de 20 qubits (vidéo).

L'innovation de cet ordinateur quantique mise en avant était à chercher du côté du design, créé avec les studios de design Map Project Office et **Universal Design Studio** (UK) et **Goppion** (Italie), un constructeur de dispositifs d'exposition haut de gamme pour musées qui a notamment conçu le dispositif de protection de La Joconde au Louvre et des bijoux de la Reine à la Tour de Londres. L'ordinateur ferait 2,75 m de large, donc à peu près la taille d'un D-Wave.

Cette annonce a donné l'impression à certains que cela préfigurait l'arrivée d'ordinateurs quantiques dans les foyers. Il n'en est évidemment rien. Ces ordinateurs sont juste des machines permettant de se faire la main avec des algorithmes quantiques très simples qui sont d'ailleurs simulables sur un simple laptop dont le TCO (total cost of ownership) sera bien plus faible que celui de cette belle machine dont ni le prix ni la date de disponibilité n'ont encore été annoncés. Pour qu'un tel ordinateur quantique soit utilisable dans des applications industrielles, il faudrait qu'il dispose de centaines à des millions de qubits. Il faudra attendre quelques années si ce n'est décennies pour y parvenir.

---

[319] Dans Benchmarking gate-based quantum computers, 2017 (33 pages).

[320] Voir IBM Simulates a 56-Qubit Machine, 2017. La performance est documentée dans Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits, 2017 (24 pages).

Le Q System One représente cependant un progrès pour faire sortir l'ordinateur quantique des laboratoires. Il est censé gérer tout seul son calibrage. Par ailleurs, en mars 2019, IBM communiquait sur l'obtention du « *volume quantique le plus élevé à ce jour* » qui est un indicateur maison associant cinq paramètres : le nombre de qubits physiques, la connectivité entre ces qubits, le nombre de portes quantiques qui peuvent être enchaînées avant que le taux d'erreur ne rende les résultats invalides, les portes quantiques disponibles et le nombre d'opérations qui peuvent être traitées en parallèle. Ce volume aurait doublé, passant de 8 à 16, ce qui ne veut pas dire grand-chose si on ne comprend pas la signification du volume quantique. En pratique, ils ont surtout diminué le taux d'erreur des portes qubits à deux qubits à moins de 2%. Il était auparavant compris entre 2% et 4%.

IBM lançait par la même occasion son premier IBM Q Quantum Computation Center pour ses clients à Poughkeepsie dans l'Etat de New York. A noter qu'IBM a aussi lancé en 2018 un centre de recherche quantique à Montpellier. Ils jouent aussi la carte de la création d'une communauté avec l'IBM Q network lancé en 2017 et qui rassemble les grandes entreprises Fortune 500, laboratoires de recherche et startups intéressées par le développement de solutions quantique. Ce réseau propose l'accès à des ordinateurs quantiques de 5, 16 et 20 qubits dans le Cloud IBM, du support et de la formation.

En mai 2019, IBM indiquait qu'il faudrait tout de même attendre de trois à cinq ans pour qu'ils commercialisent des ordinateurs quantiques, indiquant indirectement que l'annonce du CES 2019 n'était pas une véritable annonce commerciale. IBM semble attendre d'atteindre la suprématie quantique pour cette commercialisation, soit la cinquantaine de qubits de qualité et bien intriqués[321].

La notion de volume quantique est définie dans Quantum Volume de Lev Bishop, Sergey Bravyi, Andrew Cross, Jay Gambetta et John Smolin, 2017 (5 pages)[322]. Voilà une situation intéressante : un indicateur incompréhensible au commun des mortels qui est utilisé dans le marketing.

3.2 Quantum volume

For any given instance of a quantum algorithm, there is a lower bound on the number of qubits, n, required to run the algorithm as well as the achievable circuit depth, $d \simeq 1/(n\epsilon_{\text{eff}})$ needed to execute the algorithm with reasonable fidelity to the correct answer.

If it is desired to have a single metric for comparing systems, then it seems reasonable to take the product $dn = 1/\epsilon_{\text{eff}}$. However, this has some undesirable properties in that it can be gamed in various ways. For example, in many cases the best ϵ_{eff} will result from very few qubits, even $n = 2$, since in this case there will be less connectivity and paralellization overhead, and fewer issues with crosstalk between qubits. But clearly $n = 2$ is a completely uninteresting limit, where all algorithms can be trivially simulated classically. Therefore, we define $V_Q = \min(n, d)^2$, and since ϵ_{eff} and d in general depend on n, we should maximize over the number of active qubits, n', choosing a subset of n on which to execute the model algorithm (the remaining qubits may nevertheless participate as helpers, for example to reduce the permutations needed to implement the model algorithm)

$$V_Q = \max_{n' \leq n} \min\left[n', \frac{1}{n'\epsilon_{\text{eff}}(n')}\right]^2. \quad (1)$$

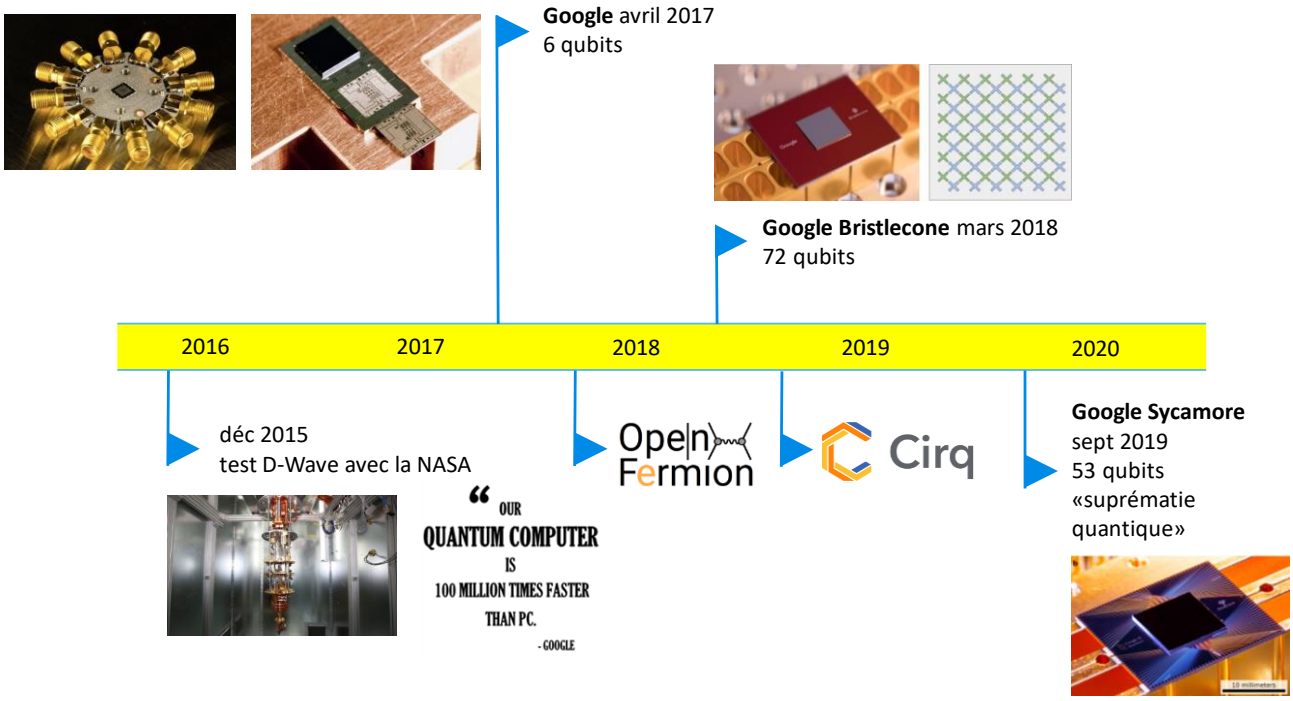
This metric quantifies the space-time volume occupied by a model circuit with random two-qubit gates that can be reliably executed on a given device.

[321] Source : Norishige Morimoto, directeur d'IBM Research à Tokyo lors de l'IBM think Summit Taipei de mai 2019.

[322] On la trouve aussi bien présentée dans Quantum computing with superconducting qubits Towards useful applications de Stefan Filipp, au Forum Teratec 2018 (26 slides). Dans A volumetric framework for quantum computer benchmarks, février 2019 (24 pages), Robin Blume-Kohout et Kevin Young proposent des benchmarks volumique pour évaluer la performance des ordinateurs quantiques en s'appuyant sur le quantum volume d'IBM.

Google a trois fers au feu pour ce qui est du calcul quantique. Il offre d'abord des capacités de simulation d'algorithmes quantiques sur ses serveurs traditionnels, puis teste des algorithmes sur des D-Wave dans le laboratoire QUAIL conjoint avec la NASA situé au Ames Research Center de Mountain View, et enfin, planche sur ses propres ordinateurs quantiques universels à base de qubits supraconducteurs, en partenariat avec l'Université de Santa Barbara en Californie, d'où provient John Martinis qui pilote l'activité quantique de Google.

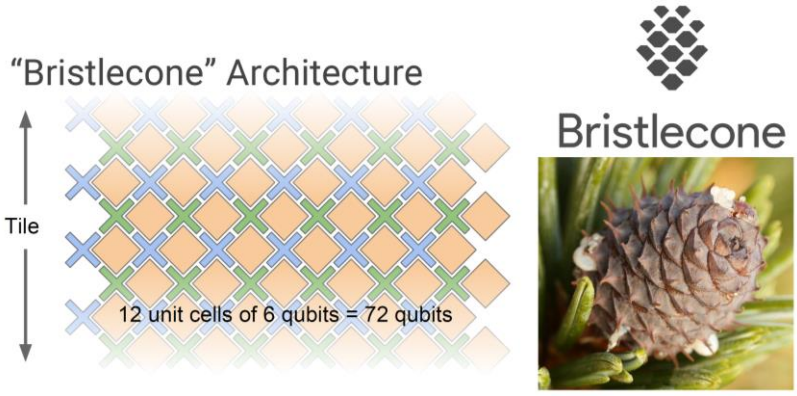
Comme IBM, ils cherchent à en augmenter le nombre tout en diminuant le taux d'erreur. Le géant de Mountain View n'est pas un fournisseur de supercalculateurs. Il prévoit sans doute d'utiliser ses ordinateurs quantiques pour ses propres besoins destinés aux usages grand public et pour ses offres de cloud computing destinées aux entreprises. Cela pourra aussi servir plus largement aux autres filiales du groupe Alphabet et en particulier celle qui travaille dans la santé, Verily, qui sera très intéressée par les capacités de simulation moléculaires du quantique, pour inventer de nouveaux traitements.



Google a fait régulièrement évoluer le nombre de qubits de ses prototypes d'ordinateurs quantiques. En avril 2017, on en était à 6 qubits. En juin 2017, Google annonçait vouloir atteindre 49 qubits stables.

En mars 2018, c'était le tour d'une annonce d'un record de 72 qubits avec la génération Bristlecone, promettant un taux d'erreurs inférieur à 0,5% dans les paires de qubits couplées entre elles.

Ce record n'a pas donné lieu à une publication scientifique vérifiable.

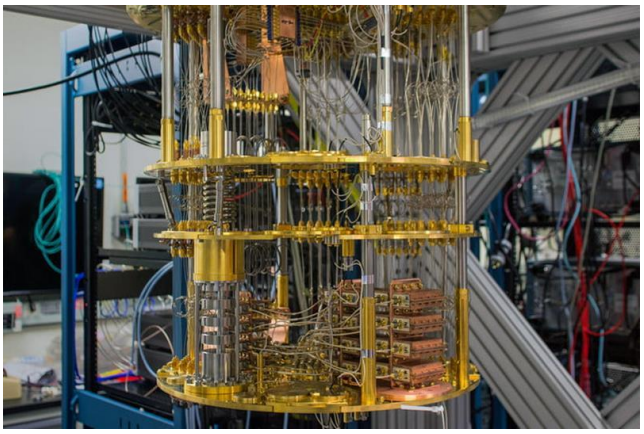


Google anticipait dès début 2018 l'avènement rapide de la fameuse suprématie quantique avec ses processeurs à qubits supraconducteurs.

Une communication scientifique sur le sujet doit être précise, faisant la part des choses entre le taux d'erreur des qubits individuels, celui des portes reliant des paires de qubits, sur la manière dont les qubits sont reliés entre eux, sur le temps de cohérence des qubits ainsi que sur la durée d'exécution des portes quantiques.

En juin 2019, Google remettait le couvert en annonçant que les ordinateurs quantiques allaient apporter non pas un progrès exponentiel par rapport aux ordinateurs classiques, mais un avantage doublement exponentiel.

C'est ce qu'affirmait Hartmut Neven, le Directeur de Google en charge du laboratoire d'IA quantique. Mais c'est franchement exagéré quand on examine leur méthode d'évaluation.



72 qubits, cela fait beaucoup de câbles !

En effet, si les ordinateurs quantiques peuvent en effet théoriquement générer une accélération exponentielle pour certains algorithmes et dans certaines conditions (pas toujours réunies…), la double accélération exponentielle ne tient pas à moyen terme. Leur seconde accélération exponentielle concerne les caractéristiques des ordinateurs quantiques. Or celles-ci concernent surtout des caractéristiques comme le bruit ou le temps de cohérence. Elles visent à permettre la première accélération quantique. Ils font quasiment du double booking [323]!

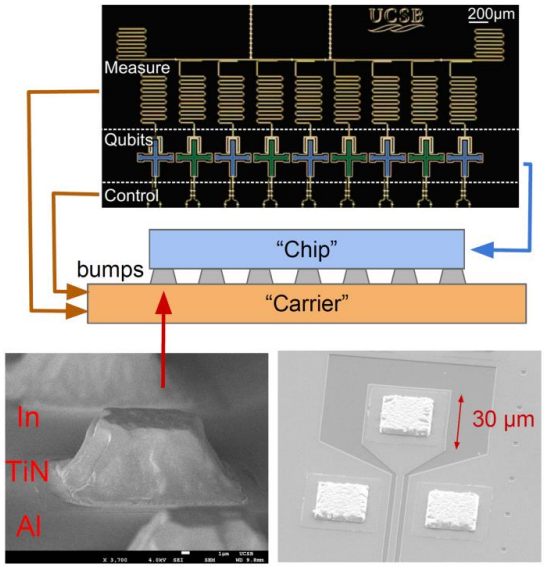
A très long terme, on pourra probablement améliorer la densité des qubits et générer une autre accélération exponentielle, comme pour la densité des transistors de la Loi de Moore. On est encore loin du compte. Qui plus est, la technologie que Google a choisi, celle des qubits supraconducteurs, est celle qui scale le moins bien.

Le 20 septembre 2019, le **Financial Times** annonçait que Google aurait enfin atteint la tant attendue suprématie quantique, sur un chipset de seulement 53 qubits et sur un algorithme voisin de celui de l'échantillonnage du boson imaginé par Scott Aaronson en 2012.

[323] Voir A New Law to Describe Quantum Computing's Rise?, juin 2019.

La publication scientifique de la NASA et Google initialement publiée avait été retirée. Ils comparaient leurs qubits avec le supercalculateur le plus puissant au monde, l'IBM Summit[324]. L'officialisation de la performance était faite en octobre 2019.

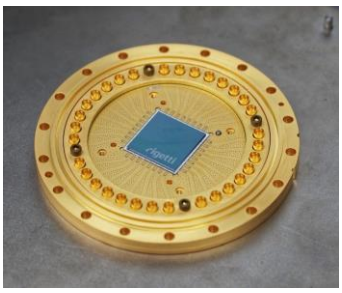
Les équipes de Google réduisent le bruit dans les qubits en séparant la couche des qubits (« chip » dans le schéma *ci-contre*) et la couche qui contient les résonnateurs servant à la mesure de l'état des qubits (« carrier ») [325] . Du côté logiciel, nous avons déjà vu dans la partie dédiée aux outils de développement que Google proposait d'un côté **Circ**, un outil de programmation de bas niveau, complété par OpenFermion, un framework de plus haut niveau codéveloppé avec Rigetti, et dédié notamment à la simulation de l'interaction entre atomes.

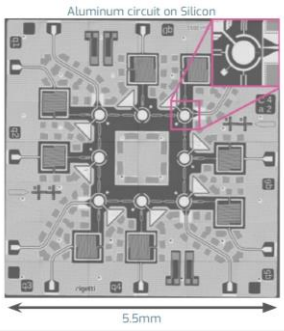


Rigetti (2013, USA, $119M) est le troisième larron du supraconducteur universel "commercial". Ils en sont actuellement à 19 qubits avec leurs chipsets avec une version à 128 qubits en cours de mise au point, annoncée début août 2018. Elle s'appuie sur la démultiplication en 2D d'une architecture de 16 qubits.

Avec D-Wave, c'est la seconde startup la mieux financée du secteur, ayant levé en tout $119M. La startup a été lancée par Chad Rigetti en 2013.

Ce dernier avait obtenu une thèse de doctorat à l'Université de Yale sur les qubits supraconducteurs en 2009[326].





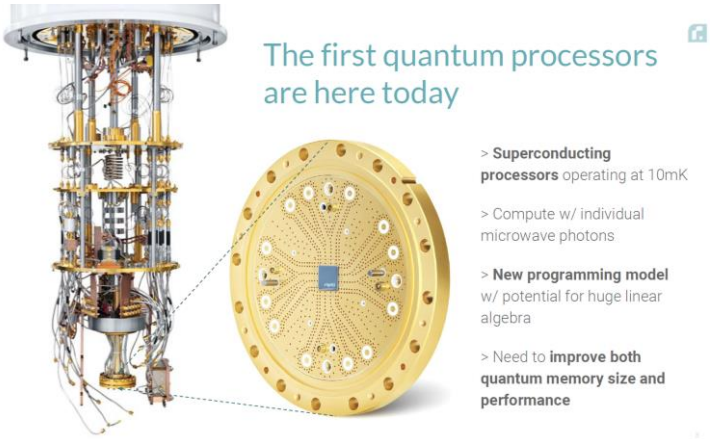
Circuit Quantum Electrodynamics (cQED) à 8 qubits
supraconducteurs à 10 mK et jonctions Josephson

[324] Voir Google researchers have reportedly achieved "quantum supremacy" par Martin Giles, dans la MIT Technology Review, septembre 2019 et la source du papier sur Internet, avec les illustrations. Ils utilisent un type d'algorithme qui ne sert pas à grand-chose mais qui favorise nettement le calcul quantique et requiert un nombre limité de portes quantiques, ce qui va bien aux processeurs quantiques générateurs de bruit. L'algorithme utilise en effet la superposition de tous les (53) qubits utilisés ce qui n'est pas le cas de tous les algorithmes. Voir aussi Why I Coined the Term 'Quantum Supremacy' par John Preskill, octobre 2019.

[325] Voir An Update on the Google's Quantum Computing Initiative, mars 2018 (39 slides), An Update on Google's Quantum Computing Initiative, juin 2018 (33 slides) et Quantum Computing at Google and in the Cloud An update on Google's quantum computing program and its open source tools, février 2019 (42 mn), tous de Kevin Kissel. Et A blueprint for demonstrating quantum supremacy with superconducting qubits, 2017 (22 pages).

[326] Voir Quantum Gates for Superconducting Qubits, 2009 (248 pages).

Il est difficile d'apprécier la manière dont Rigetti fait avancer l'état de l'art avec ses qubits supraconducteurs. Leur nombre est en ligne avec ceux d'IBM. Leurs taux d'erreur et temps de cohérence sont moins bons que ceux d'IBM.



Comme IBM et D-Wave, ils ont une approche d'intégration verticale.

Cela va jusqu'à leur propre petite unité de fabrication pour leurs chipsets maison. Ils peuvent se le permettre car l'équipement revient à environ $10M, ce qui est raisonnable. Ce cout modéré vient de ce que la création de circuits de qubits supraconducteurs se fait avec un niveau d'intégration très faible.

Dans le cas de qubits CMOS, il faut par contre disposer d'un équipement d'au moins $1B [327]!

Leurs outils de développement proposés par Rigetti comprennent pyQuil pour le scripting et Quil pour la gestion des portes quantiques. Ils sont tous deux open source et publiés sur Github.

Quil permet de synchroniser des tâches sur la partie quantique et la partie traditionnelle de l'ordinateur (documentation), ce qui en soi, n'a rien d'extraordinaire par rapport à l'approche des autres acteurs de ce marché.

Côté "Go to market", Rigetti propose l'accès à ses ordinateurs quantiques via le cloud, un peu comme le font IBM et D-Wave, avec leurs Quantum Cloud Services, en bêta depuis janvier 2019.

Ils démontraient aussi en 2018 un usage de leur ordinateur quantique pour un algorithme de machine learning qui ne nécessite pas de passer par un algorithme hybride[328].

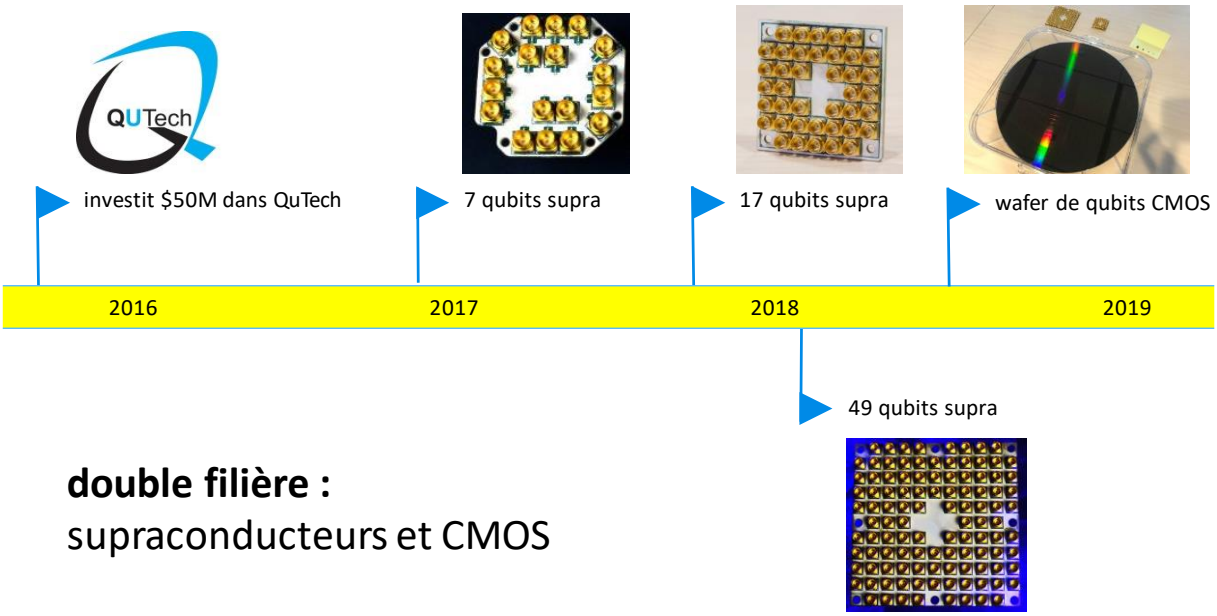
---

[327] Voir Quantum Cloud Computing Rigetti de Johannes Otterbach, 2018 (107 slides) et la vidéo correspondante. C'est la source de la double illustration avec la salle « jeune » de production et le chipset.

[328] Dans Quantum Kitchen Sinks: An algorithm for machine learning on near-term quantum computers de juillet 2018 (8 pages).

Au CES 2018, le CEO d'Intel avait fièrement brandi un chipset de 49 qubits lors de son keynote dans la grande salle de l'hôtel Monte Carlo, entre une démonstration de drone de passager et un discours sur l'intelligence artificielle. Ce processeur en technologie supraconductrice était impressionnant mais ne semble pas encore opérationnel. Dénommé Tangle Lake, ce chipset utilise une technologie supraconductrice voisine de celles d'IBM et Google. Il est en cours de test chez **Qutech** aux Pays-Bas;

Il représente un enjeu clé pour Intel qui devrait éviter de rater cette grande vague technologique qu'est l'informatique quantique. Ils ont raté celle du mobile et ne sont pas bien en point dans l'intelligence artificielle face à Nvidia qui leur taille des croupières.



Intel a plusieurs fers au feu dans le quantique. Ils creusent à la fois la piste des qubits supraconducteurs et ont présenté à ce jour plusieurs puces allant jusqu'à une cinquantaine de qubits comme Tangle Lake, et celle des qubits CMOS, que nous évoquerons dans la prochaine partie, qui s'appuiera sur leur savoir-faire en industrialisation de production de composants de ce type, un savoir qui est rare et cher dans l'industrie.

Leurs chipsets quantiques supraconducteurs évoluent à un rythme voisin de ceux de Google et IBM dans les supraconducteurs. Ils en étaient ainsi à 7 qubits fin 2016, 17 qubits fin 2017 puis 49 qubits présentés en janvier 2017, tous en supraconducteurs. Ces chipsets doivent être refroidis à 20 mK. Intel pense pouvoir monter la température opérationnelle à 1K, ce qui réduirait les exigences et le coût du refroidissement. Mais on ne sait pas comment, à part, via la filière CMOS que nous évoquerons dans la prochaine partie.

Nous avons déjà vu qu'Alibaba était très actif pour utiliser les ressources de ses data-centers pour faire de la simulation d'algorithmes quantiques dépassant les 50 qubits.

Il se trouve que le leader chinois du commerce en ligne est aussi partenaire l'**University of Science and Technology of China** (USTC) de l'Académie des Sciences Chinoises (CAS) pour la création d'ordinateurs quantiques à qubits supra-conducteurs. Ils proposent l'accès dans le cloud à 11 qubits depuis début 2018, sur une plateforme technologique développée avec l'USTC.

Ils ont même annoncé en 2018 qu'ils créaient une filiale, Ping-Tou-Ge qui développe des NPU (processeurs neuromorphiques pour l'IA) et, à terme, des chipsets quantiques supraconducteurs[329].

Ions piégés

Cette technique a été imaginée dans les années 1950 par **Wolfgang Paul**, prix Nobel de physique en 1989. Les premiers à les tester furent Juan Cirac et Peter Zoller en 1995. Les ions piégés sont des ions qui sont piégés magnétiquement dans un espace confiné, et placés les uns à côté des autres. Les atomes utilisés ont un électron manquant, dans la seconde colonne du tableau de Mendeleïev. Le calcium et l'ytterbium sont est les plus courants.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est le niveau d'énergie de l'ion piégé.
- Les **portes quantiques unitaires** sont activées par micro-ondes, par lasers ou par des dipôles magnétiques.
- Les **portes quantiques à deux qubits** utilisent des lasers avec des photons intriqués.
- La **mesure de l'état d'un qubit** utilise la captation de la fluorescence de la cavité avec un capteur CCD après excitation par un laser.

L'Autrichien Rainer Blatt de l'**Université d'Innsbruck** est un des pionniers de cette filière. Il créé un registre intriqué de 14 qubits adressables en 2011. Il passe à 20 qubits adressables et individuellement contrôlables en 2018. Ce sont des qubits à base d'ions calcium organisés en ligne servant de qubits et intriqués via un système de lasers.

Les ions piégés ont un temps de décohérence long, de plusieurs dizaines de secondes, mais c'est compensé par des *gate time* tout aussi longs en proportion. Ils présentent l'avantage de générer un taux d'erreur assez faible et de pouvoir être tous intriqués les uns avec les autres dans leur confinement[330].

---

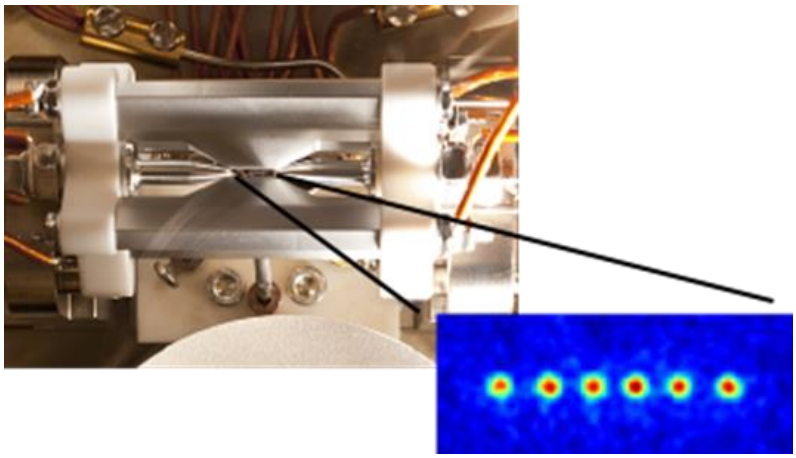
[329] Voir Alibaba Launches Chip Company "Ping-Tou-Ge"; Pledges Quantum Chip, septembre 2018.

[330] Voir Benchmarking an 11-qubit quantum computer par Christopher Monroe & Al, mars 2019 (8 pages).

Dans les technologies supraconductrices, seuls les qubits voisins d'un qubit donné peuvent être intriqués, ce qui créé des contraintes dans la conception et/ou la compilation d'algorithmes quantiques.

L'inconvénient principal est que la solution ne sera probablement pas facile à faire grandir en nombre de qubits confinés. Ne serait-ce que par le nombre de lasers à aligner pour leur contrôle et par l'espacement entre les ions alignés en rangs d'on-ions (facile…) qui est de quelques µm. Enfin, la technique est difficile à miniaturiser à cause des systèmes de contrôles divers et à l'inexistence de lignes de production adaptées.

Les ions piégés sont explorés par quelques acteurs et surtout par les laboratoires de recherche[331]. Le plus connu est celui de l'**Université de Maryland,** où officie un grand spécialiste du sujet, Christopher Monroe. Sa spin-off **IonQ** est le principal acteur commercial de cette typologie de qubits.



Côté laboratoire[332], il Il faut aussi compter avec **IQOQI** (Autriche, cf Rainer Blatt) et l'**IQST** (Allemagne), à l'origine d'un prototype de 20 qubits réalisé avec des ions calciums[333]. Il y a aussi l'**University of West Sussex** au Royaume Uni qui travaille sur un prototype de 10 qubits et recherche du financement pour créer un ordinateur quantique à 1000 qubits à base de grappe de processeurs quantiques[334]. En France, divers laboratoires du CNRS travaillent sur des ions piégés, ainsi qu'une startup située en Bretagne, **NextGenQ**. Enfin, il faut ajouter l'Américain **Honeywell**.

IonQ (2016, USA, $75M) est une spin-off de l'Université de Maryland spécialisée dans la conception d'ordinateurs quantiques universels à base d'ions piégés, avec une trentaine de collaborateurs. Créé par Christopher Monroe, la startup a levé $75M, dont une partie chez Google Ventures et Amazon, et en 2019, chez Samsung Ventures.

---

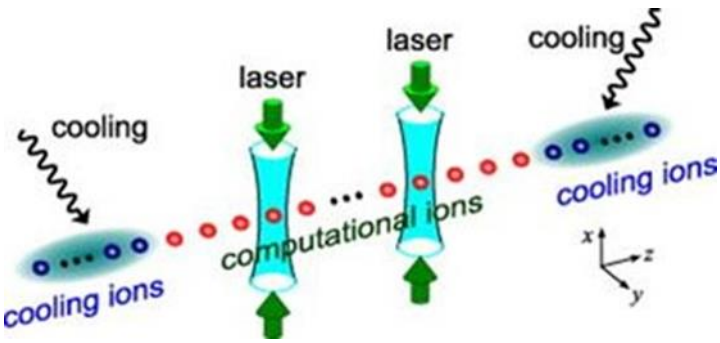
[331] Source de l'illustration : Quantum Computation with Trapped Ions de l'Université d'Innsbruck.

[332] Il y aurait en fait 80 laboratoires de recherche dans le monde travaillant sur les ions piégés. Voir ce tableau dans List of Ion Trapping Groups, mars 2019.

[333] Ils sont coauteurs de Observation of Entangled States of a Fully Controlled 20-Qubit System, avril 2018 (20 pages).

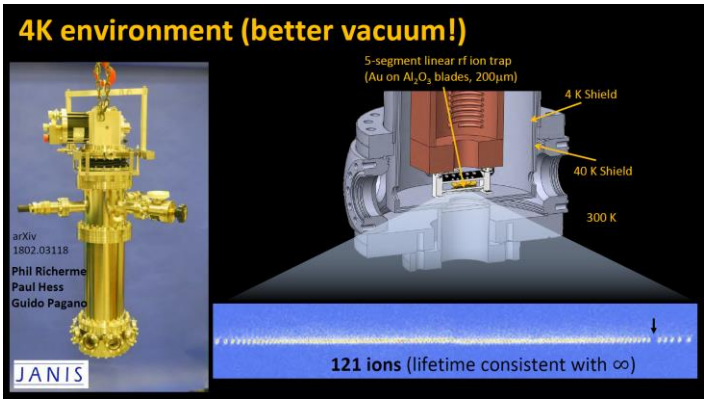
[334] Voir Blueprint for a microwave trapped ion quantum computer de Winfried Hensinger & al, 2017 (12 pages).

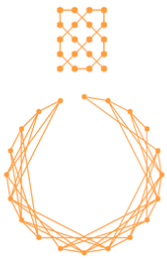
Les ions sont des atomes d'ytterbium, une terre rare aussi utilisée dans la production de certains lasers. Le record de début 2018 était de 53 qubits cohérents et intriqués. Fin 2018, IonQ annonçait avoir atteint 79 qubits associés à 160 qubits de stockage (utiles pour l'algorithme de Grover)[335].

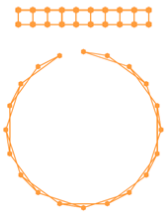


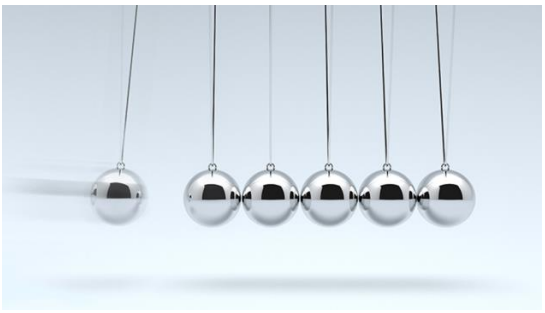
L'Université de Maryland teste de son côté un dispositif à 121 qubits refroidi à 4K [336]. Ils anticipant d'atteindre rapidement un millier de qubits

Leurs portes quantiques auraient un taux de fidélité de 99,9% pour les portes unitaires et de 99% pour les portes à deux qubits.









Le cofondateur d'IonQ et Chief Scientist est **Christopher Monroe**, un professeur de cette université[337]. La topologie du système permet de créer des portes arbitraires de deux à trois qubits reliant n'importe lequel des qubits alignés.

C'est dû aux couplages entre les ions qui exploitent des forces de Coulomb de longue portée, un peu comme lorsque dans un boulier le choc d'une bille d'un côté entraîne le mouvement de la bille à l'extrémité de l'autre côté. Cela permet d'optimiser les algorithmes quantiques pour minimiser le nombre de portes à exécuter comme l'illustre l'exemple *ci-dessous*[338].

Ils proposent une offre logicielle de programmation en cloud. L'approche est aussi "full stack". Mais l'approche logicielle a l'air d'être très propriétaire.

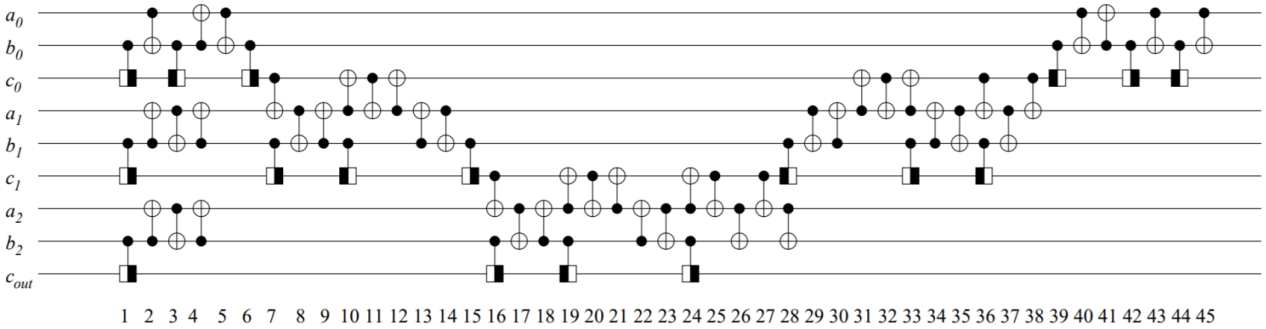
---

[335] Voir IonQ Has the Most Powerful Quantum Computers With 79 Trapped Ion Qubits and 160 Stored Qubits de Brian Wang, décembre 2018.

[336] Source de l'illustration : Quantum Circuits and Simulation with Individual Atoms par Christopher Monroe, 2018 (36 slides). Ils utilisetn des systems de cryogénie d'origine Janis.

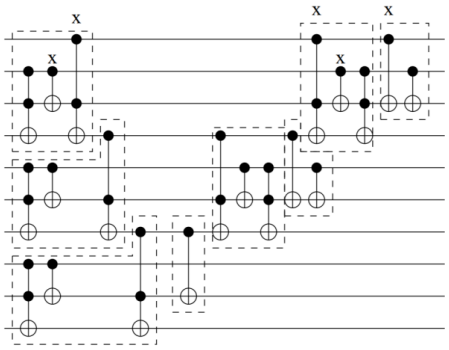
[337] Voir A Reconfigurable Quantum Computer par David Moehring, 2017 (20 slides).

[338] Source : Fast Quantum Modular Exponentiation de Rodney Van Meter et Kohei Itoh, 2005 (12 pages).



version d'algorithme d'addition de 3 bits avec liaison des qubits uniquement adjacents les uns des autres

version du même algorithme avec liaison de tous les qubits entre eux



source : Fast Quantum Modular Exponentiation de Rodney Van Meter et Kohei Itoh, 2005 (12 pages)

En novembre 2019, **Microsoft** annonçait intégrer le support d'accélérateurs quantiques d'IonQ (en plus de ceux de **QCI** – en supraconducteurs - et **Honeywell** – en ions piégés) dans son offre en cloud Azure et avec ses outils de développement Q#, QDK et Visual Studio. Tout ceci est censé être mis à disposition des développeurs, mais à une date non précisée.

Spin d'électrons

Les qubits à base de semi-conducteurs CMOS sont une voie en devenir permettant d'utiliser des processus de fabrication existants de composants CMOS au silicium. Pour mémoire, le CMOS qui veut dire "Complementary Metal Oxyde Semiconductor", est la technologie utilisée de manière dominante pour produire des processeurs dans le monde, pour les CPU (Intel, AMD), les GPU (Nvidia, AMD), les chipsets de smartphones (Qualcomm, Mediatek, HiSilicon, etc) et dans tout un tas de secteurs spécialisés (micro-contrôleurs, composants radio, …).

Dans les processeurs quantiques, c'est la voie choisie par quelques laboratoires de recherche dans le monde et par quelques entreprises privées telles que Nokia / Bell Labs, les NTT Basic Research Laboratories au Japon, et surtout, par Intel aux USA. En France, c'est l'une des deux voies d'exploration sérieusement étudiées au CEA-Leti, en collaboration avec le CNRS – Institut Néel.

Les qubits de spin sont intéressants de part la potentielle immunité du spin d'électron piégé au bruit de l'environnement. Aujourd'hui, le nombre de qubits à base de silicium (Si, SiGe) démontré est de deux avec une fidélité supérieure à 98% pour toutes les opérations, des temps de lecture de l'ordre de 5µs sachant que les temps de manipulations peuvent être plus rapides suivant les techniques utilisées et des dimensions de l'ordre de 100 nm².

C'est à la fois cette dimension, le potentiel intrinsèque du silicium avec 10^{-7} de fidélité démontrée dans des échantillons de silicium massif et la possibilité d'intégrer l'électronique de contrôle qui en font un candidat sérieux pour le calcul quantique à grande échelle.

Le principe général utilisé pour créer des qubits de ce type est le suivant :

- L'**état quantique** du qubit est le spin d'un électron individuel d'un atome piégé dans une structure semi-conductrice comprenant un puît de potentiel. Le spin est assimilable à l'orientation magnétique de l'électron.
- Les **portes quantiques unitaires** utilisent le principe de l'ESR, ou "electron spin resonance". Comme pour les qubits supraconducteurs, ces portes s'appuient sur l'émission de micro-ondes envoyées par conduction vers les qubits, soit en utilisant des cavités électro-magnétiques, soit avec des lignes radio-fréquence dans lesquelles circulent un courant alternatif qui crée un champ magnétique, soit enfin, en utilisant des micro-aimants.
- Les **portes quantiques à deux qubits** sont créées en jouant sur l'interaction d'échange entre deux qubits voisins. Ces qubits sont mis en interaction l'un avec l'autre en jouant sur la barrière de potentiel qui sépare les deux qubits. Les manipulations, comme dans les portes à un qubit, sont effectuées via l'application de pulsations de champ magnétique micro-onde.
- La **mesure de l'état d'un qubit** utilise la conversion du spin d'électron, son orientation magnétique, en charge électrique.

L'intérêt de cette technique est de permettre l'intégration d'un grand nombre de qubits dans un circuit, avec potentiellement jusqu'à des milliards de qubits sur un seul chipset. C'est même d'ailleurs semble-t-il la seule technologie qui permettrait d'atteindre ce niveau d'intégration.

Le tout se ferait avec un temps de cohérence assez long des qubits et un taux d'erreur au moins aussi bon qu'avec les qubits supraconducteurs universels. L'une des difficultés est de relier les qubits entre eux par couplage pour permettre l'exécution de portes quantiques à deux qubits, et à grande échelle. Ce couplage pourrait notamment passer par l'utilisation de photons et de couplage photons-spins.

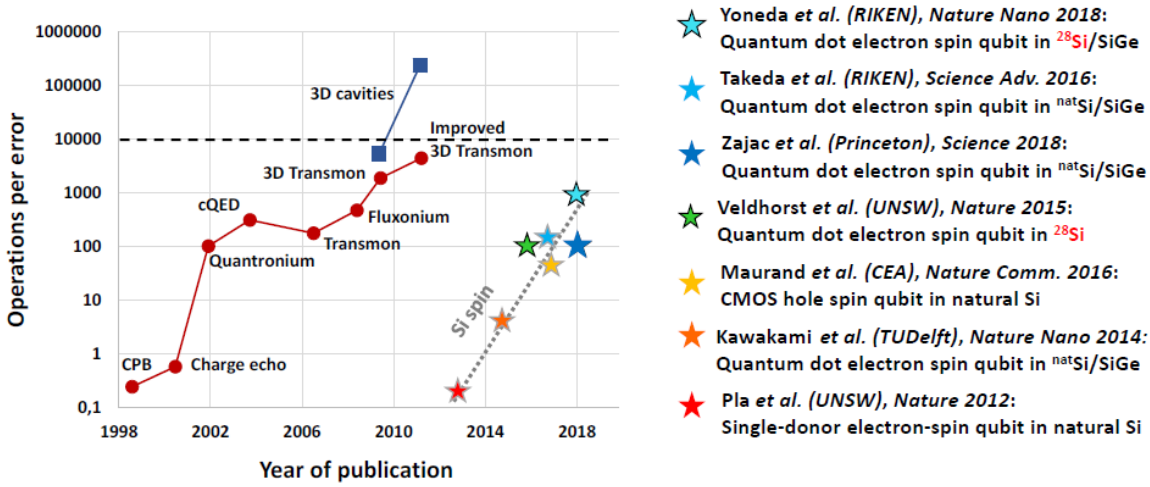
Ces qubits CMOS pourraient fonctionner en théorie à une température moins basse que les qubits supraconducteurs, de l'ordre de 1 K au lieu de 15 mK. Ces qubits manipulant des électrons individuels, ils seraient moins sujets aux perturbations extérieures que les qubits supraconducteurs qui s'appuient sur des courants portés par des millions d'électrons.

C'est l'une des raisons qui permettrait à cette technologie de mieux "scaler" en nombre de qubits. En effet, cette température plus élevée permet de placer une électronique de commande plus dense autour des qubits sans que cela n'échauffe trop le circuit. En effet, cette électronique dégage de la chaleur et cette chaleur acceptable est conditionnée par la température de fonctionnement des qubits.

Plus cette température est basse, plus la chaleur acceptable dégagée par l'électronique de contrôle des qubits est basse.

Les données de références sont les suivantes : on ne peut consommer qu'un milliwatt d'énergie à 20 mK. Cela limite l'électronique de contrôle à environ 10 000 transistors (en CMOS)[339]. Ces chipsets CMOS nécessitent l'emploi de codes de correction d'erreurs en masse, comme les "surface codes" qui sont évoqués dans une partie précédente.

Les progrès dans le CMOS sont plus récents et font la course par rapport aux qubits supraconducteurs en termes de qualité. Le schéma *ci-dessous* illustre cette évolution dans le temps entre 2013 et 2018[340].



adapted by Maud Vinet from Superconducting Circuits for Quantum Information: An Outlook de Michel Devoret et R. J. Schoelkopf, 2013

Au niveau de l'état de l'art, les Australiens, les chercheurs hollandais de QuTech[341] et Jason Petta à Princeton ont démontré des portes à deux qubits dans différentes géométries. Pour aller à l'étape suivante, la difficulté est de maîtriser le potentiel électrostatique entre les puits quantiques où sont stockés les électrons - et donc leur spin - avec un nombre de grilles qui permettent de disposer les qubits pas trop loin les uns des autres, typiquement de l'ordre de quelques dizaines de nanomètres.

Notons que l'on peut associer des qubits CMOS et de la photonique. Ainsi, les états de qubits CMOS qui sont des spins d'électrons uniques peuvent être transmis à distance via des photons ce qui permet d'imaginer des architectures de calcul quantique distribuées[342].

---

[339] C'est expliqué dans 28nm Fully-Depleted SOI Technology Cryogenic Control Electronics for Quantum Computing, 2018 (2 pages), issu du CEA-Leti et de STMicroelectronics.

[340] Ce schéma est de Maud Vinet et s'inspire de Superconducting Circuits for Quantum Information: An Outlook de Michel Devoret et Robert Schoelkopf, 2013 (7 pages). A noter qu'il date de 2013 donc n'indique pas les progrès réalisés depuis dans les qubits supraconducteurs. Operations per error est proportionnel au ratio de la vitesse de manipulation des qubits sur leur durée de vie.

[341] Voir A Crossbar Network for Silicon Quantum Dot Qubits, de R Li & Al, 2017 (24 pages).

[342] Voir Coherent shuttle of electron-spin states par Lieven Mark Koenraad Vandersypen & Al, 2017 (21 pages).

Voici les principaux laboratoires de recherche qui creusent la piste du CMOS, très souvent dans de la recherche partenariale multi-laboratoires et multi-pays.

Le laboratoire hollandais **Qutech** issu de l'Université TU Delft et de la collaboration avec Intel travaille sur une architecture CMOS, sur des gaz bidimensionnels d'électrons à base de Si/SiGe et sur des qubits à base de Germanium et SOI. Le SOI pour "silicon on insulator" ou "silicium sur isolant" est une technologie issue des français CEA-Leti et SOITEC. Elle ajoute une couche d'isolant en oxyde de silicium (SiO2 ou "BOX", buried oxyde) au-dessus des wafers de silicium et sur laquelle sont ensuite gravés les transistors et autres conducteurs des circuits à créer.

Le laboratoire **CQC²T** (Center for Quantum Computing & Communication Technology) de l'**UNSW** qui est piloté par Michelle Simmons collabore avec le CEA-Leti dans la voix SOI. L'UNSW fait avancer la fidélité des qubits CMOS, quantifie la variabilité des qubits et leur fidélité en fonction de la température. Ils obtiennent maintenant un taux d'erreur de portes quantiques à deux qubits de 2% et atteignent une fidélité de 99,96% pour des portes unitaires[343].

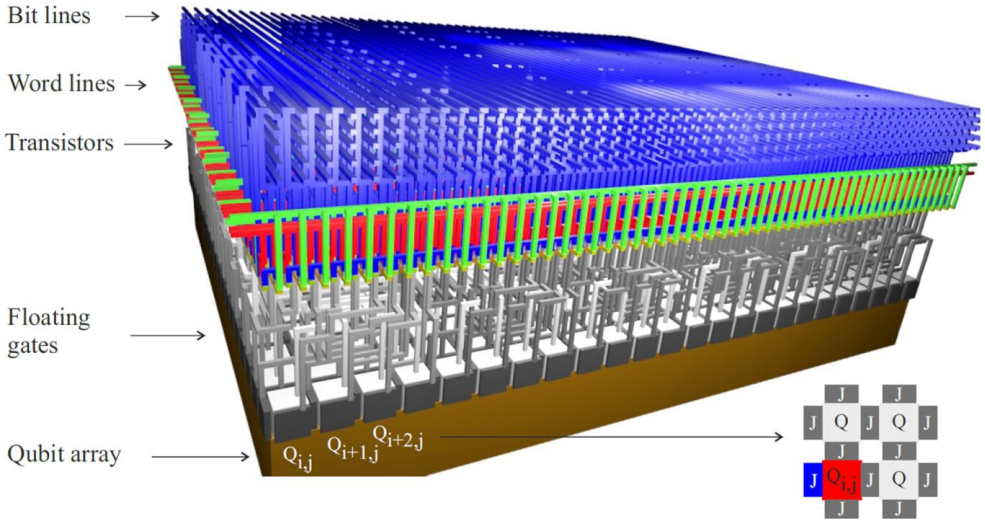


FIG. 1. **Physical quantum processor. a** A silicon-on-insulator (SOI) wafer is processed, such that the bottom layer of isotopically enriched silicon-28 contains the 2D qubit array and the top layer of silicon forms the transistors to operate the qubits. These are interconnected through the oxide regions using polysilicon vias. **b** Electrical circuit for the control of one Q-gate and one J-gate allowing the required individual, row-by-row, or global operations, as explained in the main text. **c** Physical architecture to operate one unit module containing 480 qubits. The inset on the bottom right shows a plan view cross-section through the qubit plane. Each J gate and qubit is connected via the circuit shown in **(b)**.

UNSW / Purdue : l'University of New South Wales en Australie et de la Purdue University aux USA (qui est financée par Microsoft) ont aussi expérimenté un système d'atomes de phosphore intégrés dans un substrat de silicium, les états des qubits étant le spin d'électrons des atomes de phosphore. La recherche porte surtout sur le couplage entre qubits, à base de liaisons entre dipôles électriques. Ils prévoient d'atteindre 10 qubits d'ici 2022 [344]. L'UNSW a bénéficié d'un financement de $53M originaires de l'opérateur télécom Telstra, de la Commonwealth Bank et des gouvernements australiens et de la région Nouvelles-Galles du Sud.

[343] Voir Quantum World-First: Researchers Reveal Accuracy Of Two-Qubit Calculations In Silicon, mai 2019.

[344] C'est documenté dans Silicon quantum processor with robust long-distance qubit couplings, 2017 (17 pages).

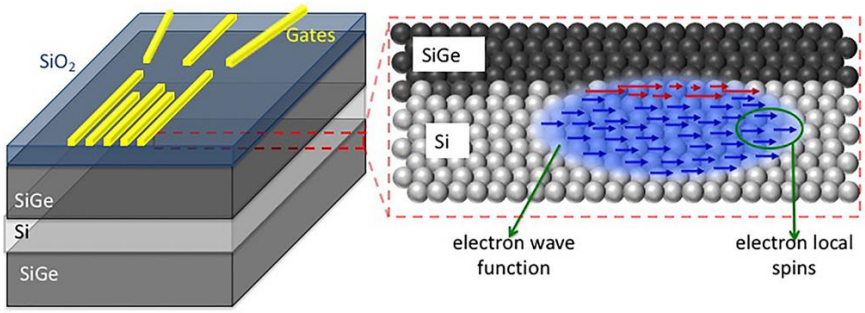
L'équipe de l'UNSW a prouvé la faisabilité de la création de qubits dans des structures CMOS et mis au point des protocoles de lecture de l'état des spins de ces qubits sans avoir de recours au moyennage via un processus dénommé "Pauli spin blockade" ouvrant la voie à la mise en œuvre de codes de correction d'erreurs et de la création d'ordinateurs quantiques à grande échelle en nombre de qubits[345].

L'équipe d'Andrea Morello du **CQC²T** de l'UNSW étudie le couplage à distance de spins d'électrons via des liaisons photoniques dans le visible ou les ondes radio.

La spin-off **SQC** (Silicon Quantum Computing) de l'UNSW veut produire un démonstrateur de 10 qubits d'ici 2022. Ceci pourrait s'inscrire dans le cadre d'un partenariat entre la France et l'Australie qui étudie l'opportunité de la création d'une *joint venture* de commercialisation de qubits CMOS, associant l'équipe d'Andrew Dzurak de l'UNSW avec celle de Maud Vinet du CEA-Leti. Les questions de souveraineté et de propriété intellectuelle ne sont pas faciles à traiter.

Purdue / TU Delft / Wisconsin : des travaux conjoints de l'Université de Purdue dans l'Indiana, de TU Delft aux Pays-Bas et de l'Université du Wisconsin-Madison évoquent la possibilité d'intégrer des millions de qubits dans des circuits en silicium et germanium exploitant les spins d'électrons[346].

Le germanium est un des matériaux III-V. Son avantage dans les qubits est de permettre de créer des portes quantiques très rapides allant de 0,5 à 5 ns[347].



Sandia Labs, USA est une filiale du groupe Honeywell qui travaille surtout pour le Département de l'Energie US (DoE) avec des laboratoires dans le Nouveau Mexique et en Californie. C'est une sorte de CEA US. Ils travaillent ainsi sur l'armement nucléaire des USA ! Ils travaillent notamment sur la physique des qubits CMOS et leurs codes de correction d'erreurs.

Ils visent une température d'opération intermédiaire de 100 mK. *Ci-contre*, leur architecture de qubit à base de double quantum dot de silicium (source).

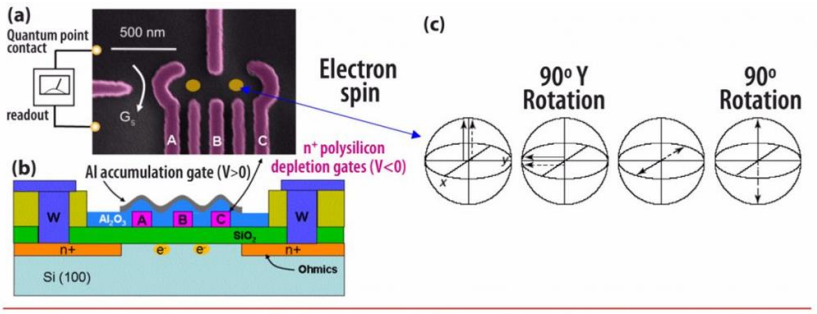


Figure 1: (a) scanning electron microscope image of Sandia's dual quantum dot structure fabricated in silicon (the dots suggest the approximate location of the electron position); (b) schematic cross section of the quantum dot structure showing the position of the single electron locations; and (c) schematic representation of spin manipulation using rotation and precession of two different spins.

[345] Voir Tests show integrated quantum chip operations posible, octobre 2018.

[346] Dans Silicon provides means to control quantum bits for faster algorithms, juin 2018.

[347] Voir aussi Quantum control and process tomography of a semiconductor quantum dot hybrid qubit, 2014 (12 pages).

Princeton, USA, travaille notamment sur réalisation de porte CNOT à deux qubits en CMOS à très haut niveau de fiabilité et faible temps d'opération, respectivement de 200ns et 99%[348]. Ce sont aussi des qubits à double quantum dots utilisant du silicium et du germanium. En octobre 2018, on apprenait que cette équipe de Princeton avait réussi à contrôler l'état de ses qubits CMOS avec de la lumière et exploiter un champ de micro-ondes pour échanger un quantum entre un électron et un photon[349].

Les laboratoires de **HRL Malibu**, filiale de recherche commune de Boeing et General Motors, située en Californie et **Nokia** travaillent sur des qubits en arséniure de gallium qui nécessitent un refroidissement à moins de 1K. Ce seraient des qubits avec de longs temps de cohérence permettant de faire des calculs avec un grand nombre de portes quantiques et codes de corrections d'erreurs.

En **Chine**, toutes les pistes technologiques d'ordinateurs quantiques sont explorées les unes parallèlement aux autres et le CMOS n'y échappe pas. Leurs travaux sont difficiles à évaluer[350].

MOS-based Quantum Information Technology

Le projet collaboratif européen **Mos-quito** associe les laboratoires de recherche européens planchant sur les qubits silicium fabriqués en technologie CMOS sur wafers 300 mm fabriqués par le CEA-Leti. En plus de ce dernier sont impliqués le Royaume Uni (London UCL, l'Université de Cambridge), la Suisse (EPFL), la Finlande, le Danemark et l'Italie (IMM). C'est un projet de trois ans financé par les deniers européens et qui est maintenant terminé. L'un des objectifs était d'étudier la performance de différents types de qubits individuels à base de spin dans le silicium pour fournir des recommandations pour les mettre en pratique à grande échelle.

Le CEA-Leti de Grenoble est le laboratoire européen en pointe sur la recherche appliquée dans les qubits CMOS à spins d'électrons et surtout, pour leur fabrication.

[348] Vu dans Quantum CNOT Gate for Spins in Silicon, 2017 (27 pages).

[349] Voir How old-school silicon could bring quantum computers to the masses, octobre 2018.

[350] Voir Semiconductor quantum computation de Xin Zhang Hai-Ou Li Gang Cao Ming Xiao Guang-Can Guo et Guo-Ping Guo, décembre 2018 (23 pages). Le document fait un état des lieux de la technologie des qubits CMOS mais sans préciser l'apport spécifique des laboratoires de recherche chinois.

L'équipe en charge du quantique y est dirigée par **Maud Vinet**. Le laboratoire est au cœur d'un écosystème de recherche quantique qui comprend le CNRS avec l'Institut Néel, l'IRIG du CEA et l'Université Grenoble Alpes. L'approche est pluridisciplinaire, ce qui est assez rare dans la recherche, avec un beau panel de chercheurs.

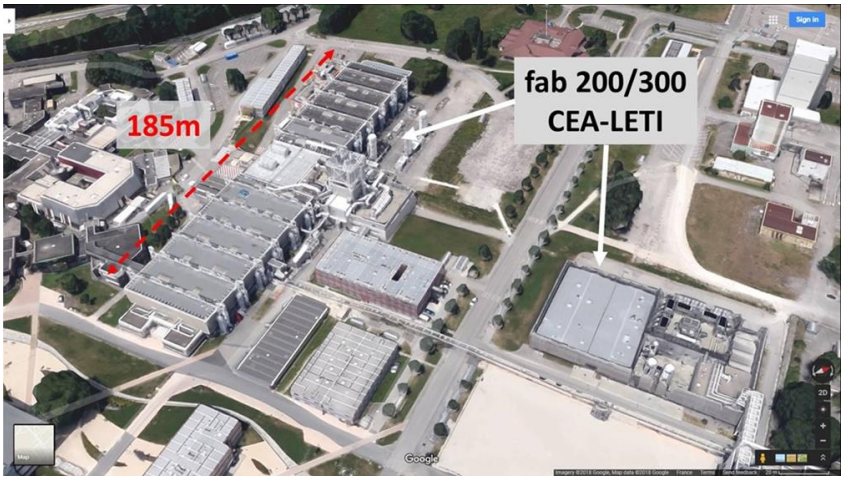
Cette équipe grenobloise propose de s'appuyer d'une part sur les capacités technologiques du Leti, les connaissances des propriétés quantiques des nanostructures de silicium de l'IRIG et l'expertise de manipulation de spin de Néel pour dépasser l'état de l'art tant en qualité qu'en nombre des qubits. D'autre part, une recherche plus en amont sur la manipulation du spin dans les aimants moléculaires et dans les semiconducteurs III-V (non silicium) permet en parallèle d'accumuler des connaissances fondamentales sur les propriétés de spin et de développer en avance de phase de l'électronique ultra-rapide.

L'équipe de l'IRIG qui associe le CEA et l'Université de Grenoble et celles de l'Institut Néel implique aussi le CNRS et l'Université Joseph Fourier de Grenoble qui fait partie du CNRS apportent leur expertise dans la création d'électronique de contrôle fonctionnant à température cryogénique, dans le contrôle d'électrons individuels dans des structures semiconductrices.

D'autres chercheurs de l'IRIG aident à modéliser les composants semi-conducteurs des qubits. Les ingénieurs en microélectronique du Leti complètent l'ensemble avec une connaissance des processus de conception, d'intégration, de fabrication et de tests des circuits semiconducteurs.

L'objectif de cette équipée est de créer des qubits CMOS à forte intégration et surtout une capacité à monter en puissance en termes de nombre de qubits. Les premiers qubits en technologie CMOS industrielle ont été créés en 2016.

Le CEA-Leti est l'un des rares laboratoires publics au monde disposant d'une plateforme de production de test de composants CMOS.



Basée à Grenoble, elle comprend tout l'outillage de production de composants CMOS sur wafers de 200 et 300 mm.

Elle permet de produire des composants en tout genre en CMOS silicium et en matériaux III-V (photonique, arséniure de gallium, nitrure de gallium, etc). La salle blanche comprend des machines de lithogravure, notamment originaires du leader mondial ASML, avec une résolution pouvant descendre à 20 nm, des machines pour le dépôt de matériaux semiconducteurs et conducteurs utilisant toutes les techniques imaginables (plasma, …) ainsi que pour l'ajout de dispositifs MEMS (micro-électromechanical systems).

Le tout occupe plusieurs bâtiments, dont le principal qui fait 185 m de long (vue Google Maps *ci-dessus*, sachant que la zone est maintenant floutée suite, probablement à la demande du CEA) sur 8000 m^2 [351].

A Grenoble, le procédé de fabrication des qubits CMOS utilise des wafers SOI (silicon on insulator, avec un isolant en oxyde de silicium) de 300 mm sur lesquels est déposée une fine couche de silicium d'isotope 28 purifié à 99,992%.

Le silicium 28 a un spin de noyau nul grâce à ses 14 neutrons et autant de protons. Ce spin nul évite que le spin du noyau influence celui de l'électron piégé dans des puîts de potentiel qui servent à gérer les qubits.

Le silicium 28 est le plus abondant sur Terre mais il est associé à l'isotope 29 à plus de 4% dans les wafers habituels destinés à la production de composants CMOS. La production de silicium 28 nécessite un raffinage particulier. Il semblerait que seule la Russie produise ce type de silicium raffiné. D'où un partenariat avec le laboratoire Russe Institute of Chemistry of High Purity Substances et Air Liquide pour la création du procédé de dépôt CVD (chemical vapor deposition) de silicium 28 sur une couche mince de 30 à 60 nm pure à 99,992%[352].

La production validée pourrait ensuite être transférée vers de la production en volume dans des fabs commerciales comme celles de STMicroelectronics, Global Foundries ou Samsung qui supportent les processus FD-SOI sur lesquels le CEA s'appuie en général. Mais à ses débuts, la taille du marché des ordinateurs quantiques sera modeste. Et rien que dans un batch classique de 25 wafers, on pourra produire d'un seul coup quelques milliers de puces quantiques, de quoi alimenter une belle base de supercalculateurs quantiques.

À Grenoble, le Leti dispose aussi d'une plateforme de nanocaractérisation (PFNC ou NanoCarac) qui comprend sur 2500 m^2 des dizaines d'outils de métrologie permettant de vérifier la qualité des composants CMOS fabriqués. Avec Fanny Bouton, j'ai pu visiter tout cela en juillet 2018 et c'était impressionnant ! La double salle blanche du Leti cumule environ un milliard d'euros d'équipements avec des machines dont le coût s'étale de quelques millions à 80 millions d'Euros !

Ce sont des moyens bien plus lourds que pour produire des qubits supraconducteurs à cause du niveau d'intégration qui est plus élevé. Les qubits supraconducteurs sont en effet bien moins intégrés, faisant plusieurs dizaines de microns de largeur. Rigetti produit ses chipsets supraconducteurs en interne avec $10M d'équipement. Les qubits CMOS pourront descendre à une taille de $100nm^2$.

---

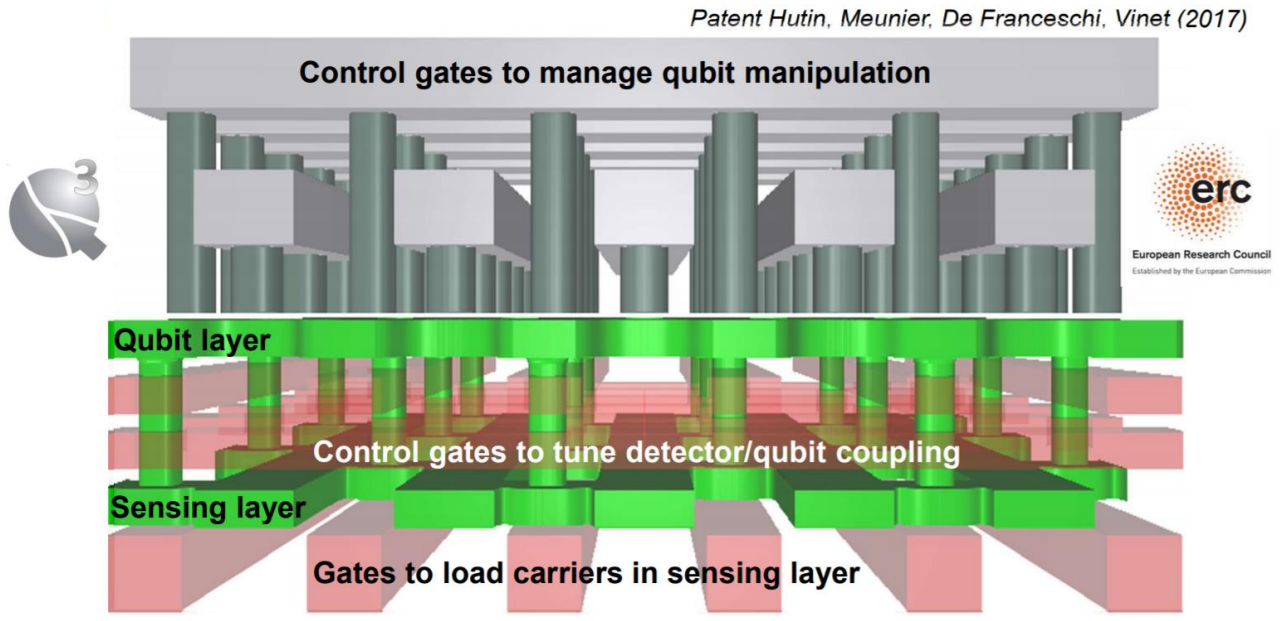
[351] D'autres salles blanches de recherche existent en France : celle du C2N à Maroussis, l'IEF à Orsay, celle de Thales TRT à Palaiseau, de l'IEMN à Lille, de Femto-ST à Besançon et le Laas à Toulouse. En production il y a surtout les fab 200 et 300 de STMicroelectronics à Crolles, près de Grenoble. Une partie de ces laboratoires sont associés dans le Réseau National des Grandes Centrales de Technologies (Renatech). Ils mettent leurs plateformes à disposition des entreprises en mode projet et contrats.

[352] Voir Quantum computing: progress toward silicon-28, avril 2018 ainsi que Purer-than-pure silicon solves problem for quantum tech de Jonathan Webb, 2014.

Les fabs classiques ne sont pas optimisées dans leurs processus de fabrication pour créer des qubits CMOS. Cela nécessiterait un gros travail de tuning et un besoin de flexibilité pas évident à obtenir. Avec une densité de 100 nm, on pourrait théoriquement caser un milliard de qubits dans une puce CMOS de 1 cm2.

L'équipe grenobloise prévoit de progresser par étapes dans les six ans qui viennent, à partir de 2019 : démonstration d'une porte à deux qubits à base de silicium d'ici un an, démonstration de simulation quantique dans un réseau 4x4 à base de matériau III-V d'ici un an, démonstration de six qubits intriqués dans du silicium d'ici trois ans, développement de codes de corrections d'erreurs et algorithmes adaptés d'ici cinq ans et fabrication de 100 qubits en réseau 2D dans du silicium d'ici six ans.

L'archirecture 2D de ces chipsets CMOS est conçue au sein de cette équipe pluridisciplinaire. Elle comprend plusieurs couches avec les qubits en silicium puis l'électronique intégrée de contrôle et de mesure d'état. Les qubits sont répartis en 2D, mais l'intégration des composants est également verticale dans les composants. La couche de mesure est située en-dessous des qubits tandis que la couche permettant d'activer les qubits avec des portes quantiques est au-dessus. Pour N^2 qubits, il leur faut 2N lignes de contrôle (horizontale, verticale). Le grand défi de ces architectures est leur variabilité, à savoir les différences de comportement d'un qubit à l'autre et d'un circuit à l'autre. Ils utilisent des matériaux supraconducteurs pour la couche métal de ces circuits, à base de nitrure de titane. Cela procure une faible résistance et réduit le bruit de mesure de l'état des qubits. Il y a donc aussi de la supraconductivité dans les qubits au silicium !



source du schéma *ci-dessus*

Le CEA travaille aussi sur la technologie **CoolCube** permettant de disposer les composants en 3D (détails), ce qui permettrait de résoudre divers problèmes de mise à l'échelle.

Elle serait applicable aux qubits CMOS et plus largement, à d'autres applications du CMOS.

Les publications de référence de ces équipes sur les qubits CMOS sont nombreuses[353]. En octobre 2018, l'équipe grenobloise associant Silvano De Franceschi (INAC, CEA), Tristan Meunier (Institut Néel, CNRS) et Maud Vinet (CEA-Leti) obtenait un financement européen ERC Synergy Grant de 14M€ pour leur projet QuQube qui sera étalé sur 6 ans pour produire un processeur quantique de 100 qubits CMOS à spin d'électrons[354].

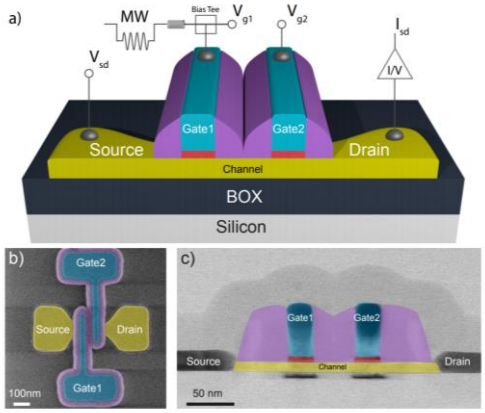
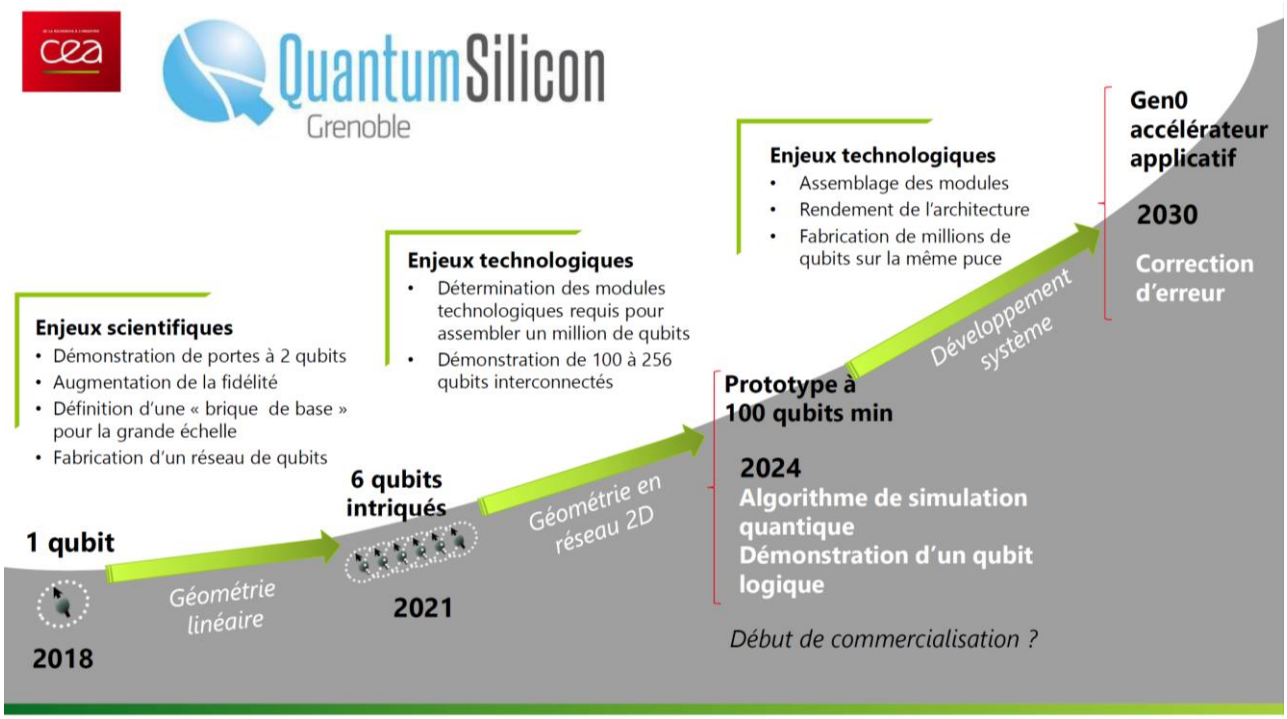


FIG. 1. **CMOS qubit device.** **a**, Simplified 3-dimensional schematic of a SOI nanowire field-effect transistor with two gates Gate1 and Gate2. Using a bias-T, Gate 1 is connected to a low-pass-filtered line, used to apply a static gate voltage V_{g1}, and to a 20-GHz bandwidth line, used to apply the high-frequency modulation necessary for qubit initialization, manipulation and readout. **b**, Colorized device top view obtained by scanning electron microscopy just after the fabrication of gates and spacers. **c**, Colorized transmission-electron-microscopy image of the device along a longitudinal cross-sectional plane.



Dans les pistes complémentaires explorées à Grenoble, le Leti conçoit des circuits électroniques cryogéniques ("CryoCMOS Circuits") qui pourront se rapprocher des circuits de contrôle des qubits dans l'enceinte thermalisée.

---

[353] On compte notamment A CMOS silicon spin qubit, 2016 (12 pages) qui définit les bases du qubit CMOS à double quantum dots (*schéma ci-contre*), SOI technology for quantum information processing, 2016 qui complète cette description ainsi que Conditional Dispersive Readout of a CMOS Single-Electron Memory Cell 2018 (9 pages) qui décrit dans le cadre d'un partenariat avec l'Université de Londres, le travail sur la lecture de l'état d'un qubit quantum dot CMOS. Et puis Towards scalable silicon quantum computing de Maud Vinet & Al, 2018 (4 pages).

[354] Voir Un ERC Synergy Grant pour la recherche grenobloise sur les technologies quantiques, octobre 2018 (6 pages). Un European Research Council Synergy Grand finance des « moonshots » dans la recherche européenne associant au moins deux laboratoires de recherche. 14M€ est le financement maximum d'un tel projet. 10M€ de financement de base et 4M€ qui peut notamment financer des investissements lourds où l'accès à de grosses infrastructures. On pense immédiatement à la fab 200/300 du CEA-LETI à Grenoble !

Il faut en effet répartir des générateurs de courant continu et des démodulateurs (à température ambiante), des amplificateurs et mélangeurs (à 4K), des résonateurs utilisant une technologie Cryo CMOS (fonctionnant à 1K) et des composants électroniques devant tourner à moins de 1K.

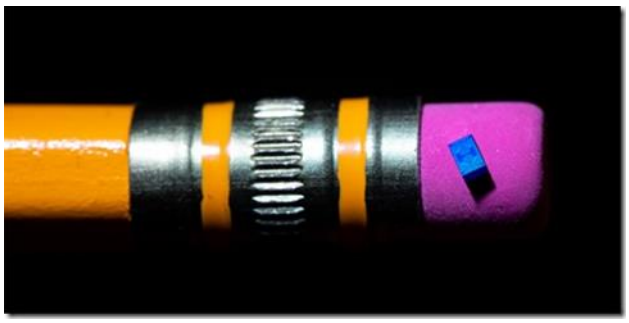
Grenoble travaille sur la conception de circuits de couplage entre spin d'électrons et photons ("Spin-Photon Coupling"). Ils doivent servir à créer des systèmes de couplages entre qubits distants. Les photons micro-ondes utilisent des bandes de fréquence comprises entre 5 et 10 GHz (cela recouvre des fréquences de la 5G entre 5 et 6 GHz, mais qui sont utilisées via des ondes hertziennes, ici, on passe par des matériaux conducteurs). Ces micro-ondes peuvent servir à concevoir des bus quantiques de données entre processeurs quantiques. Ils exploitent des résonateurs micro-ondes supraconducteurs.

Et à l'Institut Néel, on cherche à déplacer sur de longues distances des spins d'électrons ("Long distance coherent spin shuttling"). Ici, une longue distance signifie 5 µm ! Mais cela fait de quoi relier des qubits entre eux, donc cela vaut le coup[355].

Tout cela pour dire que les équipes de Grenoble mettent au point de nombreuses briques centrales et périphériques du puzzle que constitue la création d'un ordinateur quantique CMOS.

Intel travaille aussi sur la piste des composants CMOS utilisant des spins d'électrons avec un premier wafer produit avec des chipsets de 26 qubits en 2017. Le choix des qubits à base de silicium et de spins d'électron résulte d'une forme de biais cognitif : Intel maitrise la fabrication de composants CMOS et recherche donc une technologie quantique qui puisse s'appuyer sur ce savoir-faire. Mais comme nous l'avons vu au-dessus, il y a une grande logique à poursuivre cette voie qui semble l'une des rares capable de scaler en nombre de qubits. Ses qubits sont fabriqués dans les Intel Labs à Portland.

En juin 2018, Intel faisait une annonce de plus avec une puce très intégrée utilisant cette technologie CMOS, censée pouvoir compter jusqu'à 1500 qubits (*ci-contre*). Elle est fabriquée dans la fab D1D située dans l'Oregon, avec une densité de gravure de 50 nm, six fois plus grande que la génération du début de 2018.



[355] Voir à ce sujet Coherent long-distance displacement of individual electron spins, 2017 (27 pages).

Mais bien entendu, sans aucune information sur le bruit généré, qui est indispensable pour le bon fonctionnement du système ni d'ailleurs, le nombre exact de qubits de la puce en question. Que ce soit pour Tangle Lake en supraconducteurs ou pour les différentes versions à spins d'électrons, on est donc dans un brouillard quantique sur la qualité de l'ensemble.

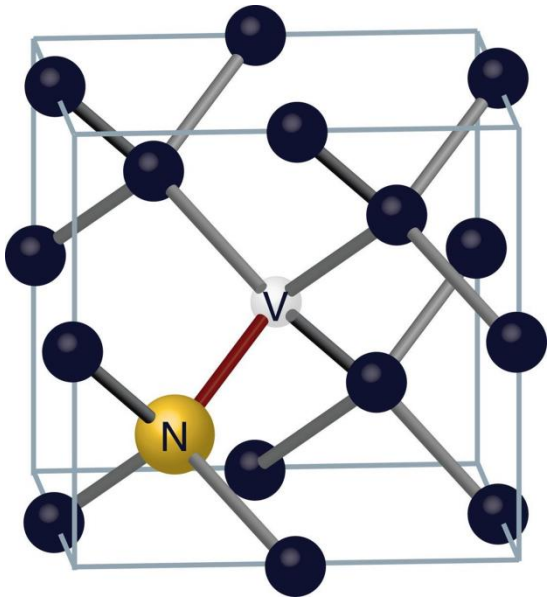
Le hollandais QuTech et Intel travaillent bien ensemble. QuTech a bénéficié de $50M d'investissements de la part d'Intel depuis 2015 pour explorer la voie du qubit en CMOS. L'investissement global d'Intel reste modeste sur le quantique. Il peut l'être tant que l'on n'en est pas au niveau de la fabrication en série.

Intel annoncait avoir réussi à contrôler un processeur CMOS à 2 qubits avec la gestion de portes quantiques unitaires et sur deux qubits intriqués exécutant les algorithmes de Deutsch-Josza et Grover à toute petite échelle. Ces qubits en silicium et germanium fabriqués par Intel dans l'Oregon étaient testés par le Laboratoire Vandersypen de l'Université de Delft qui fait partie de Qutech[356]. Les travaux quantiques d'Intel sont gérés sous la direction d'**Anne Matsuura**[357] et de **James Clark** pour le hardware.

Cavités de diamants

Cette technique consiste à créer un défaut artificiel dans une structure cristalline de carbone avec un atome de carbone remplacé par un atome d'azote et un autre atome de carbone remplacé par un vide sans atome.

Le résultat est une structure de spin 1 qui peut être contrôlé optiquement et par micro-ondes. L'ensemble fonctionnerait à température ambiante. A vrai dire, la littérature évoque parfois la température de 4K, qui est loin d'être ambiante mais dans le grand froid, tout est relatif [358]!



Il existe des variantes de cette technique avec des défauts introduits dans du carbure de silicium dopé au phosphore qui présenteraient l'avantage de créer des qubits dont la mesure est plus précise car reposant sur l'émission d'une fluorescence de fréquence étroite[359].

[356] Voir A programmable two-qubit quantum processor in silicon, mai 2018 (22 pages).

[357] Voir Intel's quantum efforts tied to next-gen materials applications, janvier 2019 et Intel's spin on qubits and quantum manufacturability tous deux de Nicole Hemsoth, novembre 2018 ainsi que Leading the evolution of compute, Anne Matsuura, juin 2018 (26 slides).

[358] La technique est notamment documentée dans NV-centers in Nanodiamonds How good they are 2017 (18 pages) ainsi que dans Diamond NV centers for quantum computing and quantum networks de Lilian Childress et Ronald Hanson, 2017 (5 pages).

[359] Voir Study Takes Step Toward Mass-Producible Quantum Computers, 2017.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est le spin des électrons situés dans la cavité.
- Les **portes quantiques unitaires** sont activées par laser.
- Les **portes quantiques à deux qubits** utilisent aussi des lasers.
- La **mesure de l'état d'un qubit** utilise la captation de la fluorescence de la cavité avec un capteur CCD.

La technologie n'est pas facile à industrialiser à grande échelle, qu'il s'agisse du chipset lui-même où des lasers de contrôle.

QDTI est la seule startup connue s'étant lancée dans la mise au point d'un ordinateur quantique à base de NV Centers. Créée par une équipe issue de l'Université d'Harvard, elle est basée logiquement dans le Massachusetts. La startup a plusieurs cordes à son arc en plus de la création de processeurs quantiques.

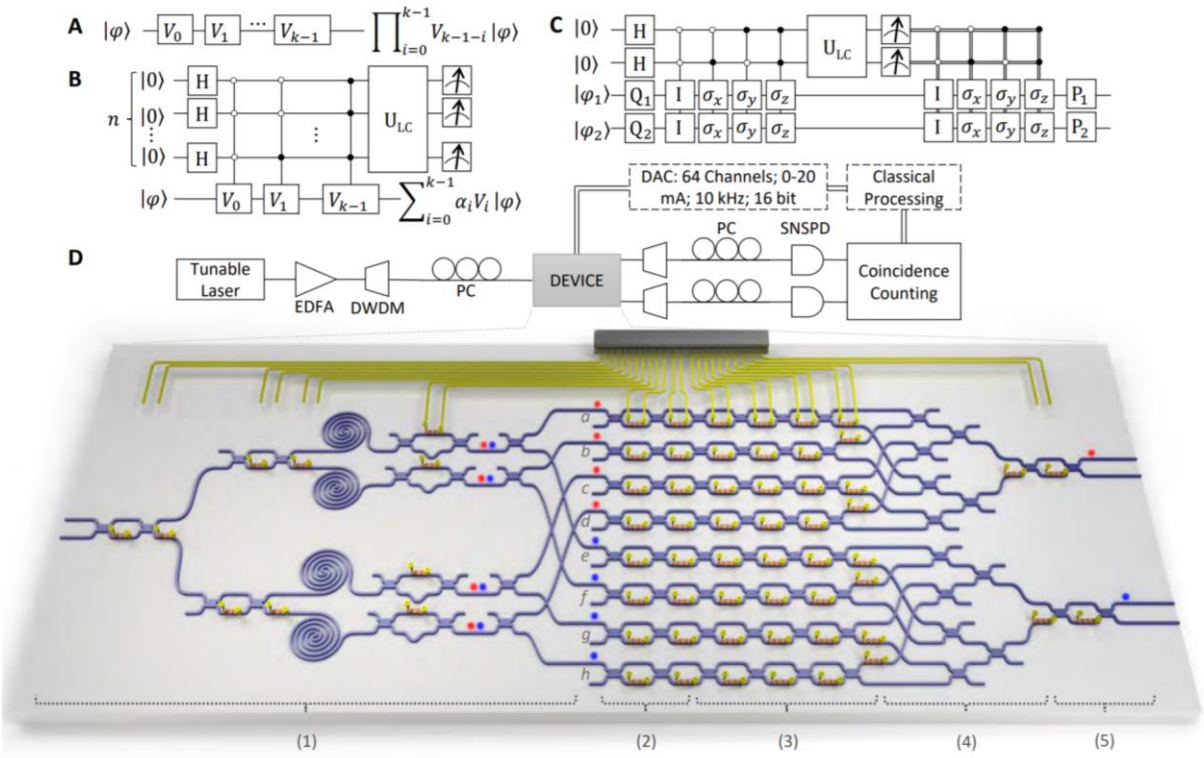
Elle planche notamment sur des systèmes d'imagerie médicale utilisant aussi ces NV centers, avec la création de magnétomètres de précision associés à de l'IRM. La société n'a pas l'air d'être particulièrement active depuis 2016.

Optique linéaire

L'optique linéaire est utilisée pour créer des qubits exploitant la polarisation ou d'autres caractéristiques de photons (fréquence, amplitude, …). La technologie commence à être prise en main par quelques startups qui se sont lancées dans le créneau comme **PsiQuantum**, **Tundra Systems Global**, **Quix** et **Xanadu**.

Les avantages de la photonique sont de permettre de gérer des qubits assez stables avec un taux d'erreurs très faible au niveau des portes quantiques, surtout au regard de celui des qubits à supraconducteurs. Ils fonctionnent aussi à température ambiante[360], n'impliquent pas des techniques de fabrication couteuses au niveau nanoscopique, peuvent s'appuyer cependant sur des architectures CMOS de fabrication, et sont directement liés à des techniques de télécommunication quantique photonique permettant une distribution potentielle des traitements.

[360] Mais en général, leur source de lumière doit être refroidie à 10K et les détecteurs en sortie à 2K.Au moins, on évite de descendre à moins de 1K ce qui permet d'utiliser des systèmes de cryogénie se contentant d'hélium 4 et ne nécessitant pas d'hélium 3 qui est plus rare.



Leur inconvénient réside dans la difficulté à assembler plus que quelques qubits tout du moins pour l'instant. Les détecteurs de l'état de photons ne sont pas très fiables, avec un taux d'erreur compris entre 5% et 50%.

Les Chinois communiquent beaucoup sur le sujet comme nous le verrons dans une partie à venir mais sans force détails[361].

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est une propriété de photons uniques. Cela peut être leur polarisation, leur chemin, leur phase, leur amplitude ou leur fréquence.
- Les **portes quantiques unitaires** sont activées par des circuits optiques.
- Les **portes quantiques à deux qubits** utilisent aussi des circuits optiques.
- La **mesure de l'état d'un qubit** utilise des détecteurs de photons uniques.

D'un point de vue physique, les composants s'appuient sur des briques connues dans la photonique en gérénal : des sources de photons (comme ceux du Français **Quandela**), des guides de lumière, des lignes à retard, des splitters, des filtres biréfringents, des déphaseurs et des détecteurs de photons[362].

[361] Voir Des chercheurs chinois sur la voie du processeur quantique 'ultime' ?, de Bruno Cormier, septembre 2018 qui pointe sur Building Quantum Computers With Photons Silicon chip creates two-qubit processor de Neil Savage, septembre 2018 qui évoque la création d'un processeur quantique à deux qubits. L'article d'origine est Large-scale silicon quantum photonics implementing arbitrary two-qubit processing, septembre 2018 (23 pages) d'où provient l'illustration de cette page.

[362] C'est bien expliqué dans la présentation Silicon photonic quantum computing de Syrus Ziai, PsiQuantum, 2018 (72 slides) ainsi que dans Large-scale quantum photonic circuits in silicon, 2016 (13 pages).

Comme les photons ne restent pas en place et sont par nature circulants, nous sommes dans un rare cas où le diagramme d'un algorithme quantique correspond aussi à un schéma de circulation des qubits dans l'espace. Les portes sont programmées dynamiquement par le routage conditionnel des photons dans les circuits optiques. Ces circuits sont souvent gravés sur des composants CMOS (silicium) ou III/V (notamment en germanium).

Les laboratoires qui bossent dessus ? Ils sont surtout issus du Royaume Uni et des USA, notamment dans les Universités d'Oxford, de Bristol, de Cambridge et de Southhampton[363]. Quelques laboratoires français sont aussi impliqués de près ou de loin dans la filière (C2N, LKB, …).

Une équipe de l'Université de Vienne annonçait en mai 2019 qu'elle planchait sur la création de portes quantiques pour ce type de qubits réalisée en graphène[364].

En juin 2019, le laboratoire chinois d'Hefei annonçait pour sa part avoir créé un processeur quantique photonique utilisnt six photons avec trois degrés de liberté, donc, à base de qutrits (qubits à trois états)[365]. Les états des photons sont le chemin parcouru, la polarisation et le moment angulaire orbital. Avec un taux d'erreur de portes de 29%.

XANADU

Xanadu est une startup de Toronto créée en septembre 2016 par Christian Weedbrook, un chercheur prolifique, et financée à hauteur de $7M. La société prévoit de proposer ses ressources de calcul quantiques en cloud. Elle a développé une plateforme logicielle Strawberry Fields qui est adaptée au développement de solutions quantiques adaptées aux calculateurs quantiques optiques.

Ils proposent leur bibliothèque de simulation quantique PennyLane positionnée comme le TensorFlow du quantique. Ils ont aussi créé les qubits "qumodes" qui permettent de manipuler de l'information continue permettant d'avoir plus de stockage quantique dans le calculateur[366].

[363] Selon Quantum Age technological opportunities du gouvernement UK Office of Science en 2016 (64 pages). Pour en savoir plus, voir aussi Why I am optimistic about the silicon-photonic route to quantum computing, de Terry Rudolph, publié en 2016 (14 pages) ainsi que l'application de l'échantillonnage de bosons.

[364] Voir Quantum Computing With Graphene Plasmons, mai 2019 qui fait reference à Quantum computing with graphene plasmons d'Alonso Calafell & Al, 2019.

[365] Voir 18-Qubit Entanglement with Six Photons' Three Degrees of Freedom de Xi-Lin Wang & Al, juin 2019 (14 pages).

[366] C'est documenté dans The power of one qumode for quantum computation, 2016 (10 pages).

TundraSystems Global est une startup de Cardiff au Royaume Uni créée en 2015 qui ambitionne de créer une solution d'ordinateur quantique optique full-stack. Leur Advisory Board comprend deux scientifiques chinois, Xinliang Zhang et Pochi Yeh qui sont spécialisés en optronique (site).

HP fait de la recherche en informatique quantique dans son laboratoire de Bristol au Royaume-Uni. Cela couvre à la fois le calcul quantique, la cryptographie et les communications quantiques. Ils ont investi dans leur projet "The Machine" qui est conceptuellement un peu éloigné d'un ordinateur quantique universel et utilise un bus optique pour relier les différents composants de ce supercalculateur. Tout cela n'est pas bien clair ni bien avancé.

En partenariat avec HP, des scientifiques américains et japonais proposaient en 2008 la création d'un HPQC, High Performance Quantum Computer, avec des matrices 3D de qubits réalisés en optique linéaire contenant 7,5 milliards de qubits physiques permettant d'accumuler 2,5 millions de qubits logiques dans High performance quantum computing (7 pages). Ce projet n'a pas été suivi d'effets ! En fait, HPE a abandonné cette voie et s'en est expliqué en 2019. Ils préfèrent se focaliser sur les processeurs neuromorphiques et les memristors[367].

Atomes froids

L'Université du Wisconsin est l'un des laboratoires de recherche qui creuse la piste des qubits à base d'atomes neutres. C'est aussi la voie choisie par la startup française **Pasqal**.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est l'état "hyperfin" – un niveau d'énergie - d'un atome neutre unique. Les qubits sont arrangés en matrice sur une plaque. Ils sont refroidis par laser. Un qubit peut utiliser un seul atome ou un groupe d'atomes selon les méthodes employées.
- Les **portes quantiques unitaires** sont activées par micro-ondes ou lasers.

[367] Voir Why HPE abandoned quantum computing research de Nicole Hemsoth, avril 2019.

- Les **portes quantiques à deux qubits** utilisent également des micro-ondes et lasers[368].
- La **mesure de l'état d'un qubit** utilise une caméra CCD qui détecte la fluorescence des atomes.

Ils ont de longs temps de cohérence mais des taux d'erreurs encore élevés, de l'ordre de 1%. On assemble jusqu'à une cinquantaine de qubits en laboratoires. C'est ce qu'a réalisé l'équipe de Mikhail Lukin de l'Université d'**Harvard** en 2017 avec des atomes de rubidium contrôlés par lasers[369]. La startup française **Pasqal** est sur ce créneau.

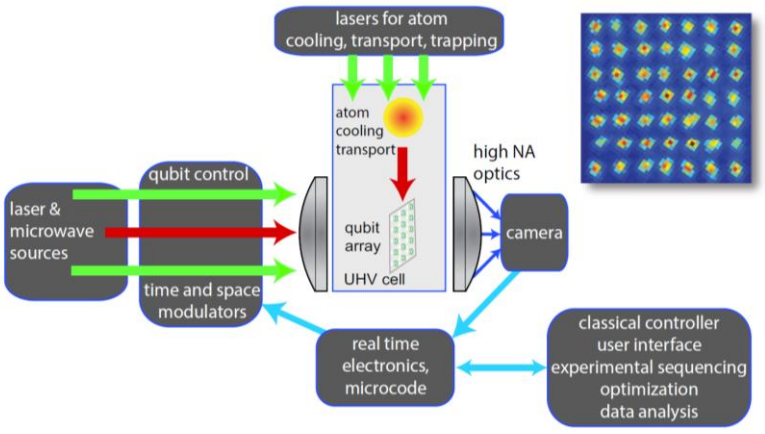


Figure 1. Architecture for a neutral atom quantum computer. The inset shows a fluorescence image of a 49 site qubit array[13].

Le rubidium est un métal alcalin, mou et argenté dont la température de fusion n'est que de 39,3 °C. Il est utilisé dans divers usages spécialisés et il en est produit 5 tonnes par an dans le monde, notamment au Canada. Les principales réserves minières sont situées en Namibie et au Zimbabwe.

Topologique

Il faut distinguer dans cette catégorie d'ordinateurs quantique la notion de "topologique" qui définit un type de qubits à base d'anyons et les "fermions de Majorana" qui ne sont qu'une variante d'anyons pour créer des qubits topologiques. De tous les types de qubits, ce sont les plus mystérieux et complexes à appréhender, et donc à vulgariser en langage naturel. On nage en pleine méta-complexité !

Le principe du quantique topologique repose sur la notion d'anyons qui sont des "quasi-particules" intégrées dans des systèmes à deux dimensions. Sachant qu'il y a des anyons abéliens et non abéliens !

Pour faire simple, les anyons sont des structures physiques asymétriques et à deux dimensions dont la symétrie peut être modifiée. Cela permet d'appliquer des principes de topologie avec des ensembles de permutations successives appliquées aux couples d'anyons qui se trouvent à proximité dans des circuits.

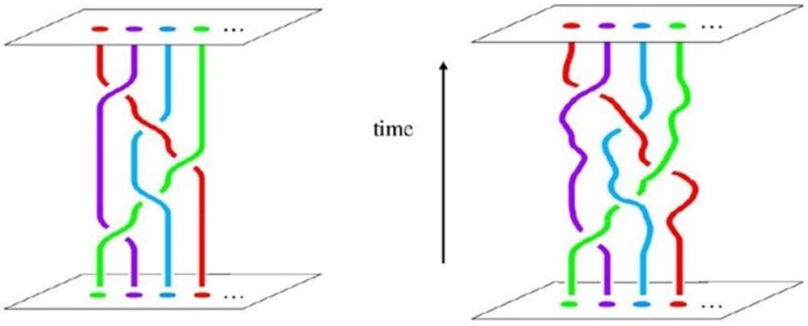
---

[368] En août 2019, des chercheurs américains arrivaient à créer des portes quantiques à plusieurs qubits fidèles à 95% à base d'atomes froids. Voir Parallel implementation of high-fidelity multi-qubit gates with neutral atoms, par H. Levine & Al, août 2019 (16 pages).

[369] Voir Quantum simulator with 51 qubits is largest ever, par Matt Reynolds, 2017. Pour en savoir plus, direction Quantum computing with atomic qubits and Rydberg interactions: Progress and challenges, 2016 (28 pages, d'où est extrait le schéma *ci-dessus*), Randomized benchmarking of single qubit gates in a 2D array of neutral atom qubits, 2015 (7 pages), Scientists demonstrate one of largest quantum simulators yet, with 51 atoms, 2017, Quantum read-out for cold atomic quantum simulators, 2018 et Quantum simulations with ultracold atoms in optical lattices, 2017 (8 pages) et Quantum simulations with ultracold atoms in optical lattices, 2017 (8 pages).

Les algorithmes associés s'appuient sur les concepts d'organisations topologiques de tresses ou de nœuds ("braids").

La représentation *ci-contre* explique cela, avec une évolution temporelle des permutations d'anyons temporelle allant du bas vers le haut sachant que dans d'autres représentations, elle va de haut en bas[370].



Le schéma suivant issu de Computing with Quantum Knots de **Graham Collins** publié en 2006 dans Scientific American (8 pages) précise un peu les choses. On y apprend notamment que les portes quantiques topologiques nécessitent un long enchaînement de permutations anyoniques comme avec la porte CNOT présentée en bas du schéma. Le tout, en conservant bien les notions de superposition et d'intrication ! C'est **Alexei Kitaev**, à l'époque chercheur chez Microsoft, qui eu cette idée en 1997 d'utiliser des anyons pour des calculs quantiques.

D'un point de vue physique, les anyons sont des "quasi-particules", à savoir des modèles de représentation de particules qui décrivent l'état de nuages d'électrons autour d'atomes (pour faire simple).

Les fermions de Majorana sont un type spécifique de quasi-particules. Ils ont des comportements collectifs d'électrons dans des réseaux cristallins à très basse température[371].

La complexité du sujet pourrait déclencher une véritable onde de choc dans l'enseignement de l'informatique car ces concepts associent mathématiques, physique et informatique à un niveau doctorat[372]. On est loin de l'Ecole 42 !

Pour comprendre le topologique et les fermions de Majorana, il faut se replonger dans le bestiaire de la physique des particules. Les fermions sont les particules de la matière et comprennent les leptons (électrons, neutrinos) et les baryons (protons, neutrons, à base de quarks) et qui composent les noyaux des atomes.

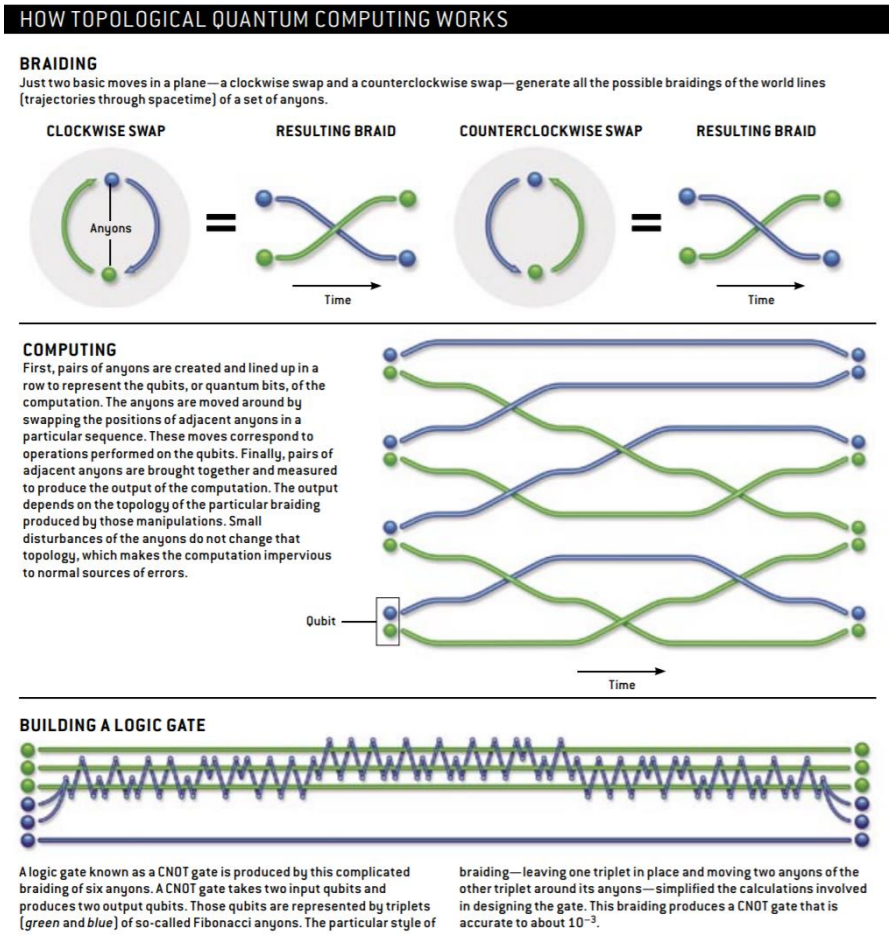
Les fermions de Majorana en sont un cas particulier qui correspondent à une sorte d'état de nuages d'électrons autour du noyau d'atomes et qui se manifestent aux deux bouts de fils supraconducteurs. Un débat court chez les physiciens sur l'existence même de ces fermions. Leo Kouwenhoven des Delft Lab (puis MSR) annonçait la détection de quasi-particules en 2012 à TU Delft.

---

[370] Des qubits topologiques pourraient être aussi réalisés en architecture à base de photonique. Voir New photonic chip promises more robust quantum computers, septembre 2018, qui associe des chercheurs en Australie, en Italie et en Suisse.

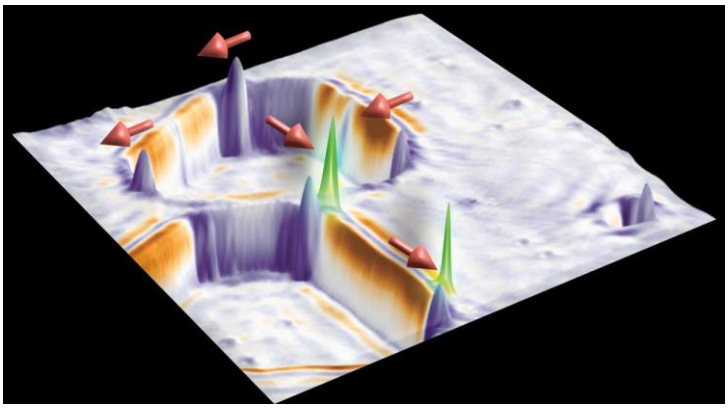
[371] L'explication, en français, la plus proche de la notion de compréhension humaine est un article de **La Recherche** de novembre 2017, Les promesses des fermions de Majorana de Manuel Houzet, Julia Meyer et Pascal Simon.

[372] C'est la thèse de Hugo de Garis dans Topological Quantum Computin The TQC Shock Wave and its Impact on University Computer Science Teaching, 2011 (29 pages).



Cette découverte était ensuite confirmée en 2016 au MIT. Plus récemment, un groupe de trois universités américaines UC Irvine, UCLA et Stanford aurait découvert de vrais fermions de Majorana. La source française de cette annonce Une particule théorique pour créer un ordinateur quantique impossible à hacker (2018) illustre au passage la difficulté de vulgariser le domaine. Les inexactitudes et approximations y sont énormes. En effet, le hacking d'ordinateur quantique n'est pas plus facile avec des fermions de Majorana qu'avec la totalité des autres technologies de qubits. Le hack, s'il a lieu, sera d'ailleurs toujours possible au niveau de l'indispensable ordinateur traditionnel qui pilote le processeur quantique.

Plus récemment, en mai/juin 2019, des chercheurs allemands et autrichiens auraient réussi à créer des phénomènes topologiques assimilables à des fermions de Majorana dans deux dimensions, mais on est encore loin de leur usage dans un ordinateur quantique[373].



[373] Voir Computing Faster With Quasi-Particles, mai 2019.

Il en va de même de chercheurs de Princeton qui publiaient en juin 2019 les résultats de travaux les ayant mené à contrôler l'état d'une quasi-particule[374].

Enfin, en août 2019, des physiciens du NIST conduits par Nick Butch annonçaient la découverte par hasard de propriétés intéressantes du ditellurure d'uranium (UTe2). Il serait supraconducteur à 1,7K avec la capacité de le faire via des paires de Cooper avec des spins identiques en plus de spins opposés, permettant d'avoir trois types de paires. Cela lui procurerait une rare capacité d'avoir une supraconductivité résistante aux flux magnétiques. Ce matériau aurait ainsi des propriétés topologiques dans ce cadre permettant de créer des qubits topologiques plus stables et moins sujets à la décohérence[375].

Avec cela en tête, voyons où en sont les deux acteurs principaux de ce domaine, Microsoft et Nokia. Leur investissement parallèle n'ayant rien à voir avec la mésaventure dans les smartphones qui a relié les deux marques il y a quelques années.

Microsoft Research planche sur le quantique topologique et les fermions de Majorana depuis pas mal n'années mais n'a pas encore de prototype à ce stade. Microsoft fait un pari de s'appuyer sur une particule virtuelle dont on n'a pas encore véritablement vérifié l'existence. C'est un pari très risqué, avec plein d'avantages stratégiques si cela fonctionne !

En effet, les qubits Majorana seraient bien plus fiables et générant moins d'erreurs, de l'ordre de 10 puissance moins 30, avec comme implication, le fait que l'on peut se passer des codes de correction d'erreurs utilisés avec les qubits supraconducteurs[376].

Médaille Fields en 1986 pour ses travaux sur la conjecture de Poincaré, **Michael Freedman** de l'Université de Santa Barbara rejoint Microsoft en 1997. Il démontre avec Alexei Kitaev la possibilité de faire du quantique avec une particule hypothétique, le fermion de Majorana, conceptualisé en 1937 par l'Italien Ettore Majorana à partir de la résolution d'équations mathématiques de Dirac[377].

---

[374] Voir Mysterious Majorana Quasiparticle Is Now Closer To Being Controlled For Quantum Computing, juin 2019 qui fait référence à Observation of a Majorana zero mode in a topologically protected edge channel, de Ali Yazdani & Al, Science, juin 2019 (12 pages).

[375] Voir Newfound Superconductor Material Could Be the 'Silicon of Quantum Computers' Possible "topological superconductor" could overcome industry's problem of quantum decoherence, août 2019, qui fait référence à Nearly ferromagnetic spin-triplet superconductivity par Sheng Ran & Al, 2019.

[376] Voici quelques pistes pour en savoir plus : Microsoft prêt à bâtir un ordinateur quantique de Juliette Raynal, en 2016 !, A Software Design Architecture and Domain-Specific Language for Quantum Computing 2014 (14 pages), Quantum Computing at Microsoft (56 slides) et Quantum Computing Research at Microsoft (59 slides) de Dave Wecker et A short introduction to topological quantum computation de Ville Lahtinen et Jiannis Pachos, 2017, (43 pages). Et quelques vidéos : keynote de novembre 2017 avec notamment Leo Kouwenhoven (43 mn), conférence Build de mai 2018 sur Q# (1h15mn) et Majorana qubits de Xiao Hu, en mai 2017 (22 mn).

[377] Dans Topological Quantum Computation publié en 2002 et mis à jour en 2008 (12 pages).

Ce fermion est une particule étrange, dont la charge et l'énergie sont nulles et qui est sa propre antiparticule. Freedman et Kitaev seront recrutés par Microsoft Research. Piloté par Michael Freedman, Microsoft Quantum Santa Barbara (Station Q) est installé sur le campus de l'Université de Santa Barbara en Californie d'où il vient. Microsoft valorise ainsi des résultats de la recherche européenne : Pays-Bas (Delft), Danemark (Niels Bohr Institute) et Italie (Majorana, OK, il est mort il a plus de 80 ans). Mais pas que, puisqu'il s'appuie aussi sur des recherches provenant des USA.

Ettore Majorana
1906-1938

fermions théorisés en 1937, particule virtuelle sans énergie ni charge qui est sa propre antiparticule

Michael Freedman et Alexei Kitaev
MSR

publient « Topological Quantum Computation » en 2002, jettant les bases de l'informatique quantique topologique

Leo Kouwenhoven
Delft Lab puis MSR

détection de quasi-particules en 2012 à TU Delft puis en 2016 au MIT

Charles M. Marcus
Niels Bohr Institute et MSR

mise au point des qubits à base de fermions de Majorana

D'un point de vue pratique et matériel, les fermions de Majorana sont en fait des comportements étranges d'électrons et de leur spin que l'on trouve aux deux bouts de fils supraconducteurs. Les fermions de Majorana opèrent donc aussi à très basses températures, comme pour les qubits supraconducteurs.

Vus de près, ces qubits sont des variantes sophistiquées de qubits supraconducteurs. Ils doivent eux aussi être refroidis à environ 15-20 mK[378].

Ces associations "topologiques" en mailles apportent une protection contre la décohérence des qubits car la forme des tresses importe peu tant que leur topologie est stable.

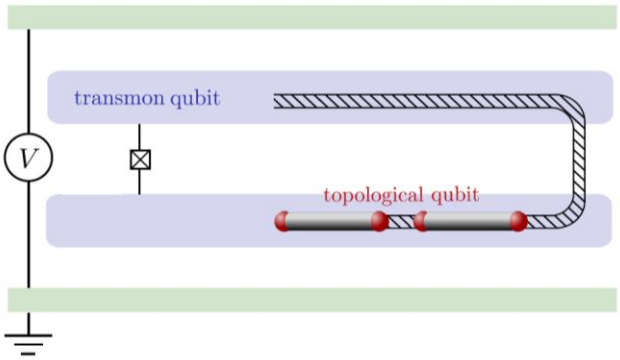
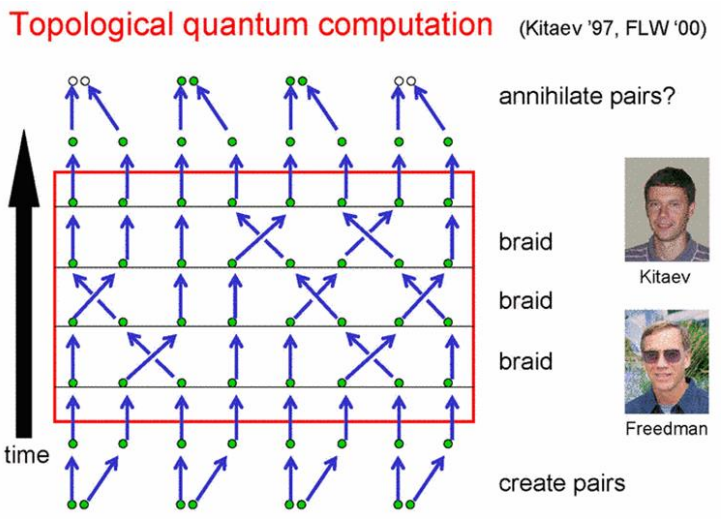


Fig. 6: *Read out of a parity qubit in a Cooper pair box. Two superconducting islands (blue), connected by a split Josephson junction (crosses) form the Cooper pair box. The topological Majorana qubit is formed by four Majorana fermions (red spheres), at the end points of two undepleted segments of a semiconductor nanowire (striped ribbon indicates the depleted region). A magnetic flux Φ enclosed by the Josephson junction controls the charge sensitivity of the Cooper pair box. To read out the topological qubit, two of the four Majorana fermions that encode the logical qubit are moved from one island to the other. Depending on the quasiparticle parity, the resonance frequency in a superconducting transmission line enclosing the Cooper pair box (green) is shifted upwards or downwards by the amount which is exponentially small in E_J/E_C.*

[378] Source du schéma : Majorana Qubits de Fabian Hassler, 2014 (21 pages).

Microsoft annonçaient à la conférence Build de mai 2018 qu'ils sortiraient leur premier ordinateur quantique à base de fermions de Majorana en 2023, ce qui est un peu loin, surtout dans la mesure où ils ne précisent pas le nombre de qubits associés. En 2023, les prévisions de marché des ordinateurs quantiques sont autour de $1,9B, ce qui n'est pas grand-chose et est déjà pas mal compte-tenu de sa maturité actuelle[379].



Microsoft a évidemment investi côté logiciels, d'abord avec sa plateforme Liquid, puis avec F# pour le scripting et avec le langage Q# servant à la programmation quantique, lancé fin 2017. Contrairement à d'autres approches, ce n'est pas un langage quantique "cross-platform" adapté aux autres types de qubits.

	Realizations	Lifetimes	Gate Speed
supraconducteurs	Topological (Majorana)	1 minute	Nanoseconds
	Flux Qubit	/ 10^{10}	same
	Charge Qubit	/ 10^{10}	same
	Transmon	/ 10^{7}	same
	Ion Trap	/ 10^{2}	10^{3} slower

qubits plus stables
faible bruit de décohérence
peu d'erreurs
temps de decohérence long
rapidité des portes

rien démontré
prototype en cours de réalisation
algorithmes différents

L'une des contributrices de ces efforts est la chercheuse Krysta Svore qui vient de l'Université de Columbia. A noter que Microsoft a recruté en 2018 un certain **Helmut Katzgraber**, l'un des apôtres du recuit quantique façon D Wave ainsi que du MBQC (measurement based quantum computers)[380].

NOKIA

Les Bell Labs de Nokia aux USA, situés à Murray Hill dans le New Jersey, travaillent aussi sur le topologique mais sont relativement discrets sur le sujet[381]. Nokia soutient aussi l'initiative Quopal de l'Université d'Oxford sur l'usage du quantique dans le machine learning.

Au passage, Nokia aime à rappeler que les algorithmes de Grover et Shor ont été découverts par leurs créateurs dans les Bell Labs. Et logiquement, Nokia planche aussi sur la cryptographie quantique, au moins au niveau de son transport sur fibres optiques comme en témoigne ce partenariat avec le Coréen SK Telecom de 2017.

---

[379] Source du schéma : http://online.kitp.ucsb.edu/online/plecture/preskill/oh/140.html, par John Preskill.

[380] Voir Quantum Driven Classical Optimizations, août 2018 (vidéo de 28 mn).

[381] Voir Quantum computing using novel topological qubits at Nokia Bell Labs publié en 2017 qui décrit leur approche dans le topologique sachant qu'aucune roadmap n'est communiquée.

Startups du calcul quantique

Après voir fait le tour des solutions matérielles d'ordinateurs quantiques, voici un tour d'horizon très large et presque exhaustif des startups de l'informatique quantique dans le monde.

La cartographie est relativement aisée car elles ne sont pas encore très nombreuses. Il y en a environ 160 à l'échelle mondiale. On est loin des 5000 startups de l'univers du marketing !

Cet écosystème commence à se structurer avant même que les ordinateurs quantiques fonctionnent à grande échelle. Les systèmes de cryptographie quantique sont opérationnels et correspondent à un marché bien à part, tout comme le marché fragmenté de la métrologie quantique. Il est fascinant de découvrir des startups qui font des paris à long terme, surtout dans le matériel.

Dans le logiciel, le risque est atténué car nombre de startups créent des solutions pour les ordinateurs adiabatiques de D-Wave qui, même s'ils n'ont pas été commercialisés en volume, sont d'ores et déjà disponibles. Leurs clients sont de grandes entreprises, surtout américaines, qui font des tests d'algorithmes à petite échelle pour se faire la main sur la programmation quantique. A ce jour, aucune application ne semble avoir été déployée en production. On est donc dans le champ de la recherche appliquée dans les entreprises clientes.

Les startups identifiées sont surtout américaines et européennes. L'écosystème logiciel est à observer de prêt. Il est prêt à dégainer lorsque le matériel fonctionnera.

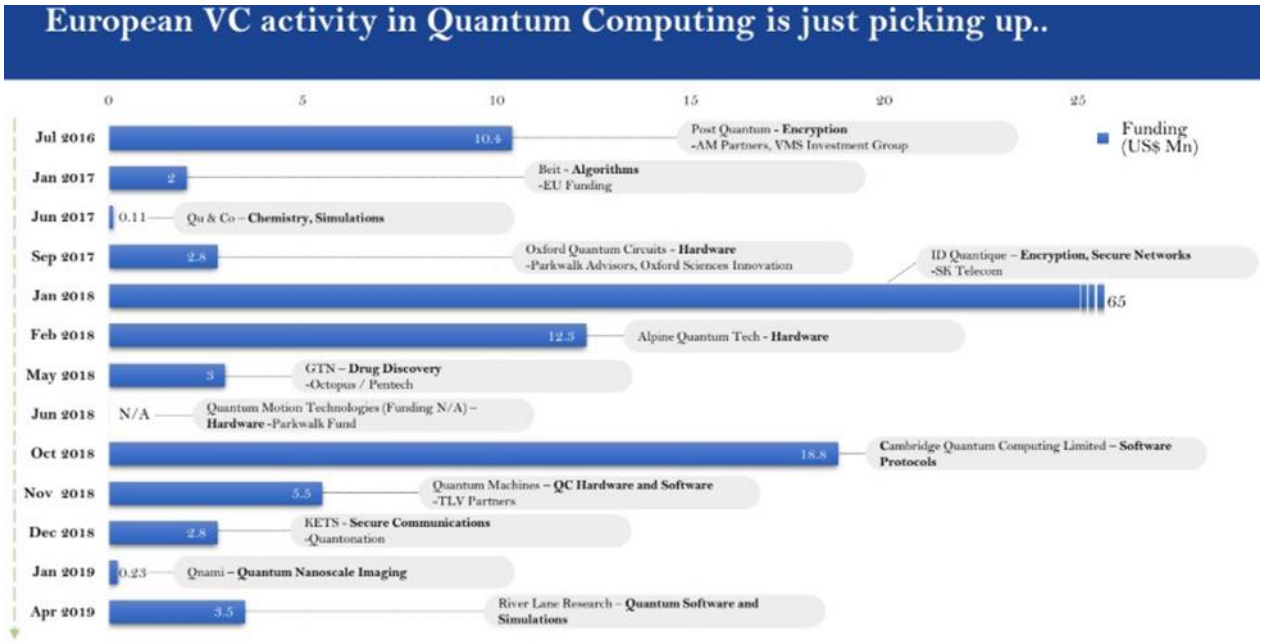
Investisseurs

Les premiers fonds d'investissements plus ou moins spécialisés dans les technologies quantiques ont déjà émergé avec notamment :

- **Quantum Wave Fund** créé par des Russes dans la Silicon Valley et ayant déjà investi dans les Suisses d'IDQ ainsi que dans l'Américain Nano-Meta Technologies. Leur fonds n'est pas 100% spécialisé dans le quantique. Ils investissent aussi dans la robotique, les drones, les capteurs et les objets connectés.
- **Quantonation**, un fonds d'amorçage français créé par Charles Beigbeder et géré par Christophe Jurczak, un physicien issu de l'Ecole Normale et ancien chercheur ayant travaillé avec Alain Aspect. Ils ont déjà investi dans six startups dont **LightOn** (France), **Spark Lasers,** qui propose des sources laser pas spécifiquement dédiées aux ordinateurs quantiques, **Pasqal** (France, atomes froids), **Quantum Benchmark** (Canada, logiciels) et **Kets Quantum Security** (UK, composant QKD). Ils organisent des meetups quantiques à Paris, la première édition ayant eu lieu en octobre 2018 et la dernière en juin 2019. C'est aujourd'hui le principal animateur de l'écosystème entrepreneurial quantique en France.

- **Quantum Valley Investments** (QVI), un fonds d'investissements canadien de $100M$, levés en 2013, dédié aux technologies quantiques. Leurs fondateurs avaient investi en 1984 dans Blackberry / RIM. Ils ne communiquent pas sur leurs investissements dont une part sont des spin-offs du laboratoire de recherche canadien Institute for Quantum Computing de l'Université de Waterloo dans l'Ontario.
- **Parkwalk Advisors** est un fonds de deep techs britannique qui a notamment investi dans Quantum Motion Technologies et Oxford Quantum Circuits.
- **Machine Capital**, un fonds britannique focalisé sur le quantique et sur l'IA, qui a pour l'instant investi dans **QuantumX Incubator,** un incubateur de projets logiciels quantiques lancé conjointement avec la startup **Cambridge Quantum Computing**, qui est spécialisée dans le développement de logiciels quantiques, avec une incubation qui dure 20 semaines.
- **SpeedInvest** est un fonds d'investissement autrichien spécialisé dans les startups deep techs, qui s'investit entre autres dans les technologies quantiques. Ils investissent en amorçage avec des tours allant jusqu'à 1M€.

L'investissement dans les startups a commencé à décoller à l'échelle mondiale à partir de 2017[382].



Un inventaire des startups du secteur est disponible sur le site QuantumComputingReport. Il m'a permis d'identifier une majorité des startups citées dans cette partie. Certaines startups diffusent tellement peu d'informations à leur sujet que l'on peut se demander si elles ne sont pas des scams.

Ce manque de communication peut simplement provenir du fait que les créateurs peuvent être des chercheurs non férus de communication, qu'ils sont mal financés et que leurs projets ont des perspectives business trop lointaines et hasardeuses.

[382] Voir European Seed Investment: Quantum Applications, de Patrick Gilday, avril 2019.

Une bonne part des startups citées ici n'en sont pas encore à la forme "pure" du modèle startupien, à savoir qu'elles sont loin d'avoir un modèle scalable. Ce sont souvent soit des TPE industrielles ciblant des marchés de niche à très faible volume, soit des startups où le risque scientifique et technologique est encore très élevé avant de pouvoir vendre quoi que ce soit. Et souvent, avec la combinaison des deux. Elles peuvent alors se financer avec de la recherche sous contrat pour de grandes entreprises ou des institutions publiques.

Dans la grande majorité des cas, je m'appuie sur les informations publiques disponibles sur Internet pour décrire ce que font ces startups. Sauf de rares cas que je signale, je n'ai pas d'information plus poussée.

Nous allons donc maintenant faire le tour des startups de l'informatique quantique avec trois parties : les composants, les ordinateurs quantiques et les logiciels, comprenant les outils de développement.

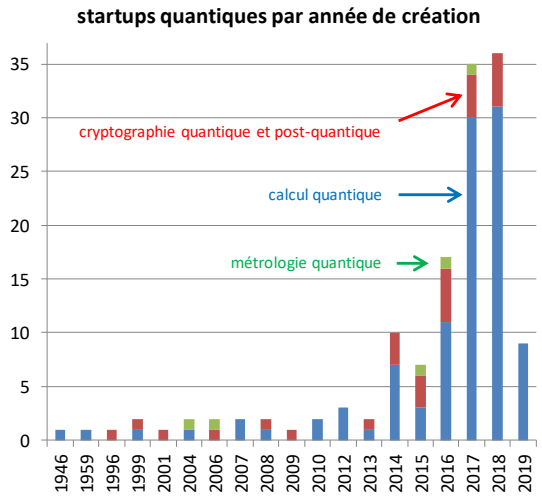
Ma cartographie ne comprend pas non plus les sociétés qui ont l'air de ne proposer que du service et du conseil dans l'informatique quantique, sans avoir de technologie en propre ou de produit. Depuis la parution initiale de cet ebook, je continue de mettre à jour cette liste au fil de l'eau au gré des découvertes.

startups par pays et année de création

la position de la France en nombre de startups est assez bonne (vs dans l'IA)

la liste ne comprend pas les industriels comme Atos et Thales

source : compilation Olivier Ezratty, septembre 2019, mais il en manque probablement.



Country	Computing	QKC & PQC	Sensing	Total
USA	32	7	1	40
UK	14	8	2	24
Canada	19	3		22
France	8	6	1	15
Germany	4	4	1	9
Netherlands	8			8
Japan	5			5
Singapore	4	1		5
Spain	4	1		5
Australia	3	1		4
Swisserland	2	1	1	4
China	1	2		3
Denmark	2			2
India	1	1		2
Estonia	2			2
Israel	1			1
Bielorussia	1			1
Sweden	1			1
Hong-Kong	1			1
Norway	1			1
Austria	1			1
Italy	1			1
Bulgaria	1			1
Luxembourg	1			1
Poland	1			1
Finland	1			1
EAU	1			1
Total	**121**	**34**	**6**	**162**

Composants

Ces startups développent des composants physiques qui peuvent jouer un rôle dans la construction d'ordinateurs quantiques. Le plus souvent, comme ce marché reste cantonné à la recherche, ces startups sont plus généralistes et visent des marchés plus larges que l'informatique quantique couvrant la recherche en physique en général voir des applications industrielles diverses.

Aurea Technology (2010, France) est une PME de Besançon qui propose des solutions de génération de photons jumeaux et de comptage de photons uniques exploitables notamment dans le domaine de la cryptographie quantique.

AuroraQ (2017, Toronto) est une société spécialisée dans la création de systèmes de communication avec des qubits supraconducteurs. C'est complété par le logiciel QSPICE Design qui permet de concevoir des circuits quantiques supraconducteurs. Autant dire qu'il s'agit d'un marché ultra-niche[383].

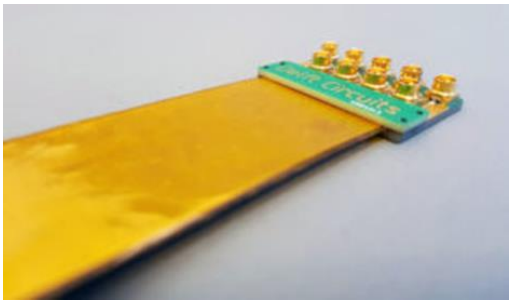
bra-ket science (2017, Texas) est une startup qui veut créer des systèmes de stockage d'information dans des qubits fonctionnant à température ambiante. La société qui n'a que deux personnes est silencieuse sur sa technologie dont les brevets sont en cours de dépôt.

[383] Voir The Geometry of a Quantum Circuit and its Impact on Electromagnetic Noise, 2018 (15 pages).

ColdQuanta (2007, USA, $6,8M) est une startup créée par Dana Anderson qui a une solution de refroidissement d'atomes dits froids à base de lasers. Cela peut servir à créer les conditions cryogéniques de fonctionnement de certains types d'ordinateurs quantiques ou à créer des systèmes d'horloges quantiques ultra-précises. Depuis mars 2019, son CEO est Bo Ewald qui était auparavant Président de D-Wave en charge des ventes internationales. Ils collaborent aussi avec IonQ pour la production de leurs ordinateurs quantiques à base d'ions piégés.

Delft Circuits (2016, Pays-Bas) fournit des composants supraconducteurs divers qui peuvent rentrer dans la composition d'ordinateurs quantiques à supraconducteurs à effet Josephson.

Ils proposent notamment des circuits de contrôle d'entrées/sorties de contrôle de systèmes cryogéniques comme le CF3 (Cri/oFlex, *ci-contre*) et des guides supraconducteurs de micro-ondes supportant des fréquences allant de 2 à 40 GHz.



Element 6 (1946, Luxembourg) n'est pas à proprement parler une startup. C'est une filiale du leader mondial de la production de diamants, De Beers Group, qui fabrique entre autres choses des diamants synthétiques utilisables dans les qubits à base de cavités de diamants, un type de qubit très peu courant et qui n'a donné lieu pour l'instant qu'à une seule création de startup, QDTI. Mais ces NV centers sont par contre très utilisés en métrologie, notamment dans des magnétomètres quantiques.

Intelline (2018, Canada) produit des systèmes de réfrigération cryogéniques sur mesure censés être plus abordables que ceux de ses concurrents.

IQM (2018, Finlande) est une startup qui développe un système de réfrigération de chipsets supraconducteurs à base d'envoi d'électrons (vidéo). Cela pourrait permettre d'agencer un plus grand nombre de qubits dans ce type d'ordinateurs quantiques. Elle est issue du groupe Quantum Computing and Devices de l'Université d'Aalto.

Kiutra (2018, Allemagne) développe un système de cryogénie à très basse température à base de magnétisme qui permet de se passer de l'hélium 3 utilisé dans les systèmes de cryogénie à dillution. C'est une spin-off de TUM (Technical University of Munich). Leur gamme de cryostats descend à 100 mK, ce qui est insuffisant pour refroidir des ordinateurs quantiques supraconducteurs mais pourrait éventuellement convenir pour des chipsets CMOS à spin d'électrons.

Labber Quantum (2016, USA) développe des solutions logicielles de contrôle des qubits d'ordinateurs quantiques expérimentaux. Elles servent notamment à calibrer les qubits.

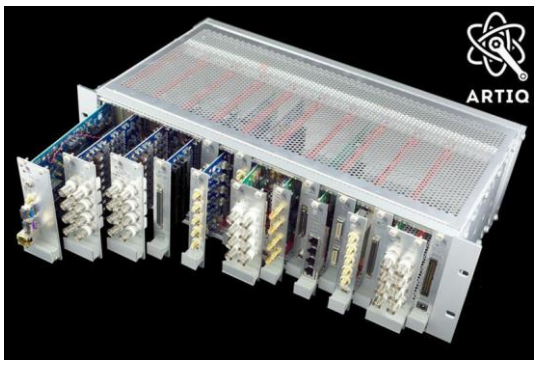
LakeDiamond (Suisse) produit des diamants de synthèse pouvant être utilisés pour créer des qubits à base de lacunes dans les diamants. Ils utilisent du dépôt sous vide avec la méthode CVD (Chemical Vapor Deposition).

M-Labs (2007, Hong-Kong), anciennement dénommée Milkymist, travaille sur le projet ARTIQ (Advanced Real-Time Infrastructure for Quantum physics), un système qui associe le matériel et un système d'exploitation temps réel qui sert à contrôler le matériel d'ordinateurs quantiques à base d'ions piégés.

Ils ont développé leur propre circuit FPGA pour ARTIQ, l'ensemble se programmant en Python.

Cette solution a été développée avec l'équipe Ion Storage Group du NIST aux USA qui travaille sur des qubits à ions piégés.

La société a été créée par un ingénieur français, Sébastien Bourdeauducq.



Nano-Meta Technologies (2010, USA) est une startup issue de l'Université de Perdue qui ambitionne de créer un système de stockage d'information quantique.

C'est en fait un laboratoire de recherche privé qui commercialise des travaux associant photonique et nanomatériaux sous forme de propriété intellectuelle et dans des domaines variés tels qu'un système de nano-délivrance de médicaments ou des sources de photons individuelles à base de diamants dédiées à des systèmes de cryptographie quantique. Certains de ses composants innovants peuvent se retrouver dans des ordinateurs quantiques.

Photon Spot (USA) développe des détecteurs de photons uniques à base de nanofils. Ils ont bénéficié de financements significatifs de la DARPA de $100K en 2014 et $1,5M en 2015.

Plassys Bestek (1987, France) n'est pas une startup mais une PME qui fabrique des équipements sous vide. Ils sont leaders dans les équipements dédiés à la réalisation des jonctions Josephson et fournissent des laboratoires de recherches investis dans les qubits supraconducteurs (Yale, ETH Zurich, Rigetti, NTT, CEA Saclay, ….). Ils produisent aussi des diamants artificiels utilisables dans les qubits à base de centres NV. Ils concurrencent à ce titre element 6 et Lake Diamond. La société fait environ 7M€ de CA.

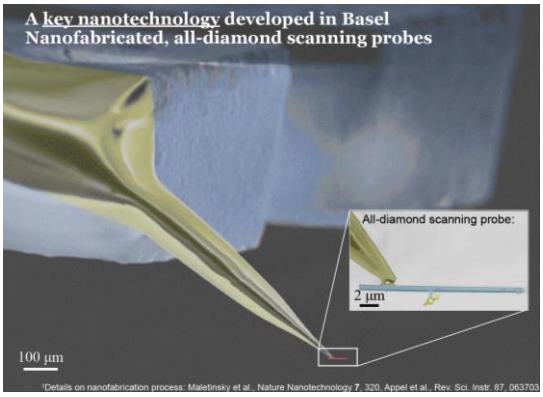
Oxford Instruments (1959, UK) est une entreprise britannique établie, coté à Londres depuis 1999, qui est spécialisée dans l'instrumentation scientifique qui propose notamment des systèmes de cryogénie capables de descendre à 5 mK. Ils fournissent aussi des caméras CCD servant de détecteur de l'état de qubits à base d'ions piégés.

Qblox (2018, Pays-Bas) est une spin-off de QuTech qui développe de l'électronique de commande « scalable » de qubits supraconducteurs.

Q-Lion (2019, Espagne) développe une solution de code de corrections d'erreurs pour qubits à ions piégés.

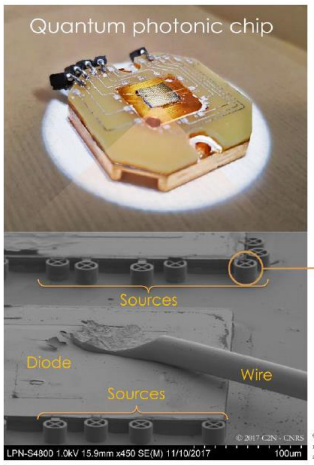
Qnami (2017, Suisse) est une spin-off du laboratoire de recherche en métrologie quantique de l'Université de Bâle.

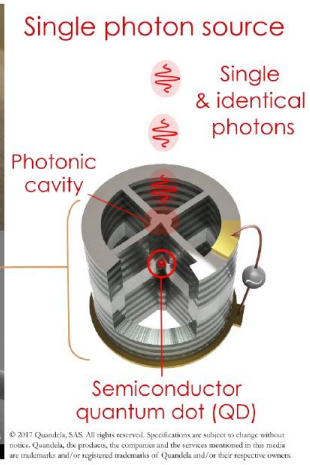
Ils produisent notamment des diamants artificiels destinés à diverses applications de photonique. Ils pourraient cibler le marché du calcul quantique mais cela n'a pas l'air d'être encore le cas. Leur premier marché est pour l'instant celui de la métrologie quantique qui s'appuie sur des nano-diamants comprenant des NV-centers (atome d'azote à côté d'une lacune de carbone).

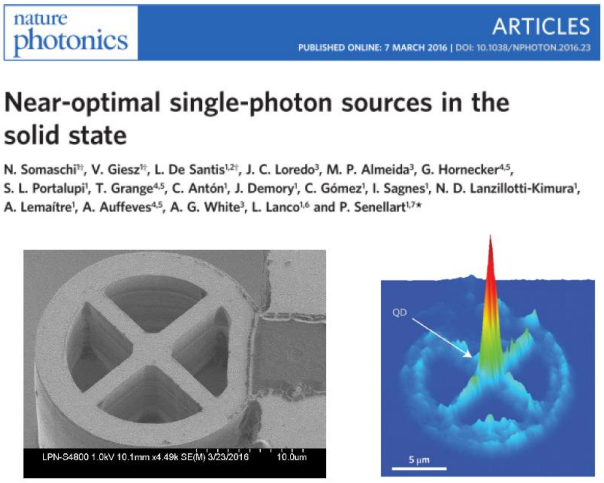


Quandela (2017, France) est une startup basée à Palaiseau sur le plateau de Saclay dans le sud de l'Ile de France, qui est spécialisée dans la création de sources de photons uniques destinées au monde de la recherche, des télécommunications et du calcul quantique.

Avec un seul atome piégé contrôlé dans un quantum dot, ils arrivent à générer des trains de photons bien séparés dans le temps[384]. Ses sources de photons peuvent servir dans la cryptographie quantique et, à terme, à créer des ordinateurs quantiques à base d'optique linéaire ou autres techniques.







Ils ont notamment développé un système d'intrication de quatre photons à partir d'un seul photon source, qui est piégé dans une boucle à fibre optique[385]. Cela génère plusieurs photons intriqués qui sont ensuite exploitables pour des communications quantiques.

L'équipe de quandela est composée de Valerian Giesz (CEO). ingénieur Supoptique avec un doctorat en photonique, Niccolo Somaschi (CTO), docteur de l'Université de Southampton et Pascale Senellart (CSO), directrice de recherche au C2N (CNRS, Université Paris-Saclay) dont la startup est issue.

La startup était lauréate du grand prix du concours i-Lab 2018 et compte 7 salariés en septembre 2019 et plusieurs clients à l'international.

	State-of-the-art laser sources (from Optica Vol.5, issue 5, p. 514-517 – 2018) Indistinguishability = 90%	eDelight Indistinguishability > 90%	
Single photon rate	1.3 MHz	> 25 MHz	X 20
Three-photon rate	55 Hz	9 kHz	X 160
Eight - photon rate	10^{-8} Hz	0.5 mHz	X 50 000

[384] Voir Near optimal single-photon sources in the solid state, Valerian Giez, Pascale Senellart & Al, 2016 (23 pages).

[385] Voir Generating multi-photon entangled states from a single deterministic single-photon source, S. Eisenberg, Pascale Senellart & Al, 2019 et Single photon generation and manipulation with semiconductor quantum dot devices de Lorenzo De Santis, 2018 (206 pages).

Quantum Machines (2018, Israël, $5,5M) développe une couche de contrôle des qubits pour des ordinateurs quantiques supraconducteurs qui associe matériel et logiciel[386]. C'est une spin-off du laboratoire de recherche Braun Center for Submicron Research de l'Institut Weizmann.

Quantum Opus (USA) développe des détecteurs de photons uniques à base de nano-fil, les Opus One. Cette société a aussi bénéficié de financements fédéraux US, dont $100K en 2015 et $1,5M en 2015 provenant de la DARPA puis $125K de la NASA en 2018.

Qubitekk (2012, San Diego) est comme le Français Quandella un fournisseur de sources de photons et de photons intriqués utilisables dans le contexte de la cryptographie quantique (QKD). Cette technologie peut aussi servir pour gérer une partie de la communication entre qubits dans certains types d'ordinateurs quantiques.

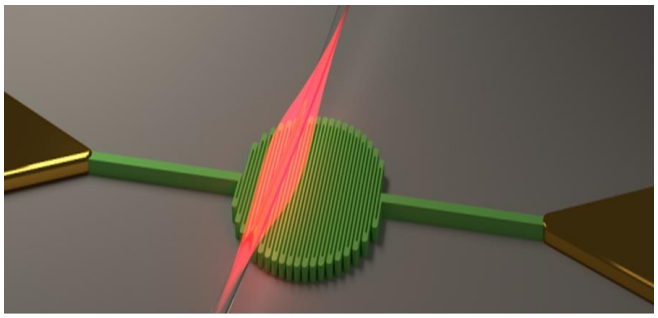
QuTech (2014, Pays-Bas) est la spin off "hardware quantique" de l'Université TU Delft. Elle collabore notamment avec Intel dans la mise au point de qubits supraconducteurs et avec Microsoft dans le quantique topologique. La société se positionne plutôt comme un laboratoire de recherche appliquée que comme une startup "produit".

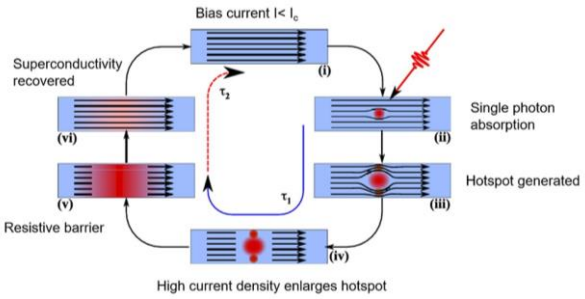
SeeQC (2017, Italie) est une spin-off du groupe américain Hypres, spécialisée dans la création d'électronique supraconductrice. Elle se focalise dans la création de circuits de contrôle de qubits supraconducteurs dotés de mémoires à base de technologique spintronique (spin d'électrons).

[386] Voir The Story of the First Israeli Quantum Computing Startup, par Eliran Rubin, décembre 2018.

S-Fifteen Instruments (Singapour) est une spin-off du laboratoire CQT qui développe des systèmes de contrôle de qubits et des solutions de cryptographie quantique.

Single Quantum (2012, Pays-Bas) propose des détecteurs de photons uniques Qos, intégré dans un cryostat refroidi à l'hélium liquide à 2,5K. Leur capteur utilise la technique SNSPD (superconducting nanowire single photon detector) qui comprend un film mince de nanofils supraconducteurs en forme de serpentin applati. Ce dispositif permet de capter un photon unique issu d'une fibre optique.



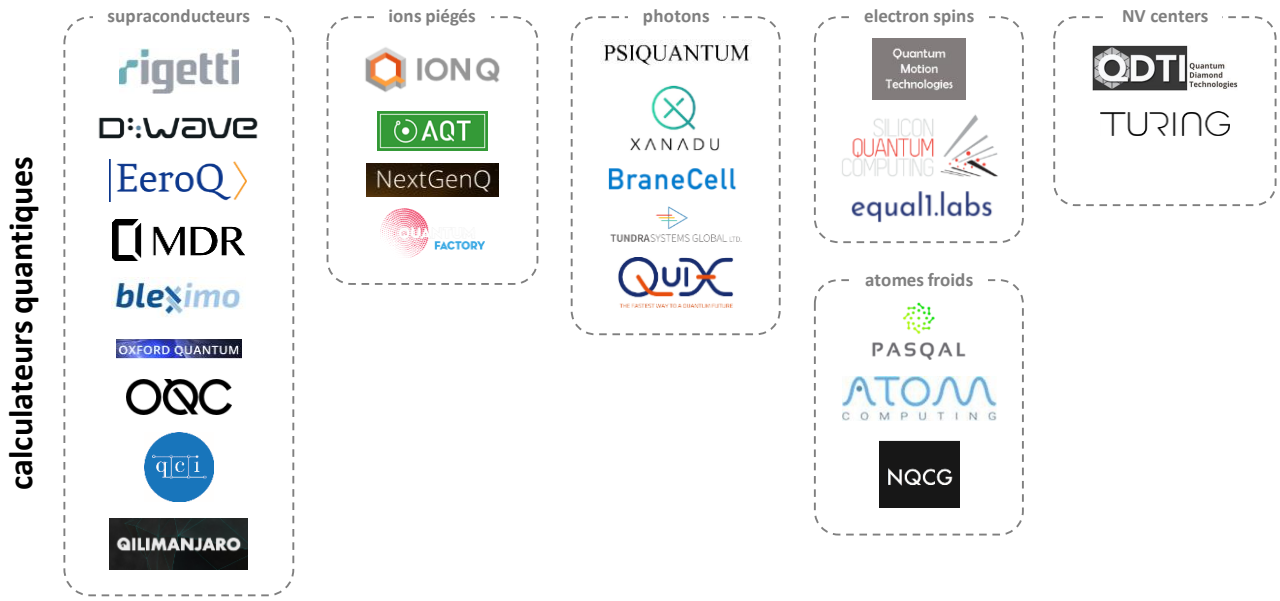


Sparrow Quantum (2016, Danemark) est une spin-off du laboratoire de recherche en photonique Niels Bohr. Comme Quandella et Qubitek, ils proposent des sources de photons uniques.

Enfin, sans rentrer dans les détails, citons à nouveau **BlueFors Cryogenics** (Finlande), **Cryomech** (USA), **CryoConcept** (France) et **Janis** (USA) qui sont spécialisés dans la production de systèmes de cryogénie utilisés pour les ordinateurs quantiques qui doivent fonctionner à de très basses températures, situées entre 10 et 20 mK.

Ordinateurs

Voici quelques PME et startups qui cherchent à créer des processeurs ou ordinateurs quantiques en plus de D-Wave, IonQ et Rigetti que nous avons déjà couverts en détail.



Très souvent, ces entreprises s'affichent comme étant "full stack", ce qui veut dire qu'elles ambitionnent de créer à la fois un ordinateur quantique et toute l'infrastructure logicielle qui l'accompagne. C'est souvent justifié pour les couches basses logicielles qui peuvent dépendre de l'architecture des qubits de l'ordinateur créé. Pour les couches plus hautes, notamment au niveau des frameworks de développement, ce n'est pas forcément bien vu. Il vaudrait mieux se raccrocher aux frameworks qui commencent à s'imposer ou à ceux d'entre eux qui sont open source et multi-plateformes. Dans d'autres cas, les startups ici citées en sont au stade de la recherche appliquée pour créer un processeur quantique. Elles sont généralement loin d'avoir créé une infrastructure logicielle.

Alpine Quantum Technologies (2017, Autriche, $12,3M) est une spin-off de l'Université d'Innsbruck créée par Rainer Blatt. Peter Zoller et Thomas Monz et qui se focalise sur les systèmes de qubits à base d'ions piégés, le premier d'entre eux en étant l'un des pionniers. Leur financement est pour l'instant d'origine publique, issu des équivalents autrichiens de notre Ministère de la Recherche et de l'ANR. La société n'a pas encore de site web ni de logo, c'est dire si elle est jeune !

Atom Computing (2018, USA) ambitionne de créer un ordinateur quantique à base d'atomes neutres contrôlés optiquement. C'est une technique que nous avons creusée très rapidement dans les parties précédentes. Elle semble bien marginale, tout du moins dans la sphère entrepreneuriale. Voici quelques éléments d'informations dans Neutral Atom Quantum Computing du Anderson Group Optical Physics ainsi que dans Quantum computing with neutral atoms, de David Weiss 2017 (7 pages).

Bleximo (2017, USA, $1,5M) veut développer des coprocesseurs quantiques adaptés à différents marchés dont les biotechs, les qASIC, à base de qubits supraconducteurs à effet Josephson. Ils sont partenaires de Q-CTRL qui développe des logiciels quantiques de codes de correction d'erreur. La startup a été créée par Alexei Marchenkov et Richard Maydra, deux anciens de Rigetti. Il est très difficile de savoir ce qu'ils font exactement ni quelle technologie de qubits ils maîtrisent.

BraneCell (2015, Cambridge Massachusetts et Dusseldorf, $1,8M) est une startup lancée par Wassim Estephan et Christopher Papile (*ci-dessous*). Elle développe un processeur quantique fonctionnant à température ambiante.

Ses qubits utilisent un processus permettant de faire cohabiter un état condensé et non condensé de molécules, sans conduction électrique ni silicium, avec un procédé qui s'appuierait sur de la lumière infrarouge. Ce n'est pas bien documenté. L'idée est de permettre d'exécuter des programmes quantiques de manière décentralisée et pas dans des data centers. L'approche est originale mais on demande à voir sur pièces !

Ils ont déposé quelques brevets sur la question notamment le brevet USPTO 9607271 validé en mars 2017 et dont voici la description : "*The subject matter relates to multiple parallel ensembles of early stage spherical pulses radiated through engineered arrays forming the foundation for quantized computer processors taking advantage of integer thermodynamics. The materials, architecture and methods for constructing micro- and/or nano-scale three-dimensional cellular arrays, cellular series logic gates, and signature logic form the basis of small- and large-scale apparatuses used to execute logic, data bases, memory, mathematics, artificial intelligence, prime factorization, optical routing and artificial thought tasks not otherwise replicated in electron-based circuits*".

Leur communication est pour le moins cryptique, comme BraneCell Systems Presents Distributed Quantum Information Processing for Future Cities en avril 2018 et un partenariat annoncé avec le prestataire de services du gouvernement US, AST, en juillet 2018, dans AST and BraneCell Announce Their Partnership to Improve Critical Government Functions Through the Power of Quantum Computing. Ils ne fournissent aucune information technique ni de vulgarisation sur leur solution, sur le nombre de qubits et le taux d'erreurs. Ils planifieraient aussi une ICO qui serait la première du genre pour une startup de l'informatique quantique. Ils visent surtout à créer un système de communication sécurisé. Ils ciblent la finance, l'énergie, la santé, la chimie et le secteur public. Un Theranos du quantique ? Au minimum, on est en droit de douter.

CNT Nanotech (2019, France) est une société lancée par Mathieu Desjardins et Michael Rosticher. C'est un projet issu de l'ENS Paris devenu une startup en phase de création ayant Maud Vinet comme scientific advisor. Leur piste consiste à utiliser des nanotubes de carbone pour piéger les électrons utilisés dans des qubits CMOS. Cela permettrait d'améliorer leur isolation et leur temps de cohérence d'un facteur 100 atteignant une seconde. Ils se contrôleraient par couplage spin-photon. Les défis se situent au niveau des matériaux, du design, de l'électronique de contrôle, de la connectivité, de la topologie et des codes de correction d'erreurs. Les nanotubes sont intégrés au circuit mécaniquement à la fin du processus de fabrication. Les nanotubes de carbone proviennent de la société allemande Micromotive. La liaison entre deux qubits s'appuie sur des cavités à micro-ondes, exploitant le principe de la cQED (cavity Quantum Electrodynamic). Il subsiste évidemment de nombreux défis pour mettre au point ce genre de qubits mais la voie mérite d'être explorée.

EeroQ

EeroQ (2017, New York) développe un processeur quantique qui serait plus-mieux que les autres, sans plus de précision autre que cela s'appuie sur des principes connus de la physique. La startup est fondée par Johannes Pollanen de l'Université du Michigan, Nick Farina et Faye Wattleton. Elle a bénéficié de financements publics US (NSF) et privés. Leur site web est pourri avec une page "The Science" qui décrit les avantages basiques du calcul quantique mais aucunement les caractéristiques de leur solution. C'est du quantum washing du premier degré. La bio de Johannes Pollanen indique qu'il a mené des recherches dans les qubits supraconducteurs et bidimentionnels (silicium, graphène) qui font penser aux principes du quantique topologique. Ca donne quelques pistes de ce qu'ils doivent bien tramer !

equal1.labs

equal1.labs (2017, USA) développe en collaboration avec l'Université de Dublin un processeur quantique à spins d'électrons fonctionnant à 4K et fabriqués en technologie FD-SOI 22 nm chez Global Foundries. Ils annoncent avoir développé un chipset de test de 422 qubits. Mais qui reste à tester et à mettre au point !

MDR

MDR (2008, Japon) est une énigmatique société japonaise qui ambitionne de créer son propre ordinateur quantique universel et de développer des algorithmes intégrant l'IA et la chimie. En attendant leur ordinateur, ils travaillent avec D-Wave.

NextGenQ (2019, France) ambitionne de concevoir des ordinateurs quantiques à ions piégés qui seront intégrés dans une offre de « Blind Quantum Computing » permettant de les solliciter via le cloud tout en assurant la confidentialité des traitements et données soumis et sans passer par des liaisons physiquement protégées par de la QKD. Les marchés visés sont classiques : la finance, la chimie, l'IA et la cybersécurité. Le projet est très ambitieux mais risque de manquer de moyens[387].

Nordic Quantum Computing Group (NQCG) (2004, Norvège) fait de la R&D dans des domaines à la croisée des chemins entre l'IA et l'informatique quantique. Ils sont sur la piste du développement d'un simulateur quantique analogique.

Oxford Quantum Circuits (2017, Oxford, UK, $18M) a été lancée par Peter Leek, qui provient du Clarendon Laboratory Oxford. Elle veut produire des qubits supraconducteurs et lever les barrières identifiées qui empêchent ceux-ci de scaler en nombre. Leur architecture comprendrait des qubits "planar" à grande cohérence avec un contrôle 3D miniaturisé des portes et de la lecture à base de résonnateurs[388]. Ils sont associés à Cambridge Quantum Computing (CQC) qui développe un compilateur quantique dédié à leurs qubits.

Pasqal (2019, France) est la première startup de calcul quantique en France basée sur la filière du refroidissement d'atomes de rubidium confinés magnétiquement et refroidis à 30 µK, notamment par laser à effet Doppler pour atteindre le mK et avec une variante de l'effet sisyphe atomique pour atteindre 30 µK[389]. Les portes quantiques sont activées par laser pour modifier l'état énergétique des atomes.

Les atomes sont piégés dans des matrices 2D ou des structures toriques 3D avec un espacement de quelques microns entre chacun d'entre eux.

---

[387] Voir Comme en IA, il faut, peut être, éviter le piège des "biais" concernant les technologies des ordinateurs quantiques à suivre : votre avis?, par Yann Allain, avril 2019.

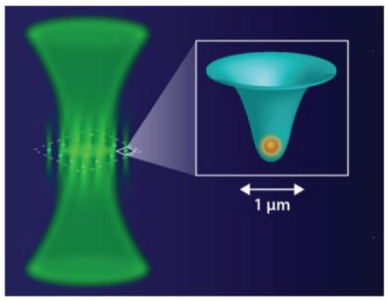
[388] Voir Surface acoustic wave resonators in the quantum regime (40 slides).

[389] Cette méthode utilise aussi des lasers émettant des photons polarisés orthogonalement. La méthode a été inventée par Claude Cohen-Tanoudji qui a obtenu pour cela le prix Nobel de physique en 1997.

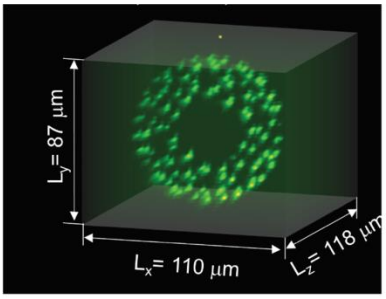
Ils sont gérés avec deux niveaux d'énergie. L'intrication est provoquée par l'excitation des atomes dans l'état de Rydberg qui leur permet d'interagir avec d'autres atomes à longue distance.

La technologie serait prometteuse et permettrait d'atteindre rapidement une cinquantaine de qubits de qualité puis des centaines d'ici 5 ans[390].

Ils se positionnent dans un premier temps sur les PQS (Programmable Quantum Simulator, ou ordinateurs quantiques analogiques) puis ensuite sur les NISQ (Noisy Intermediate-Scale Quantum), des ordinateurs à portes quantiques universelles.



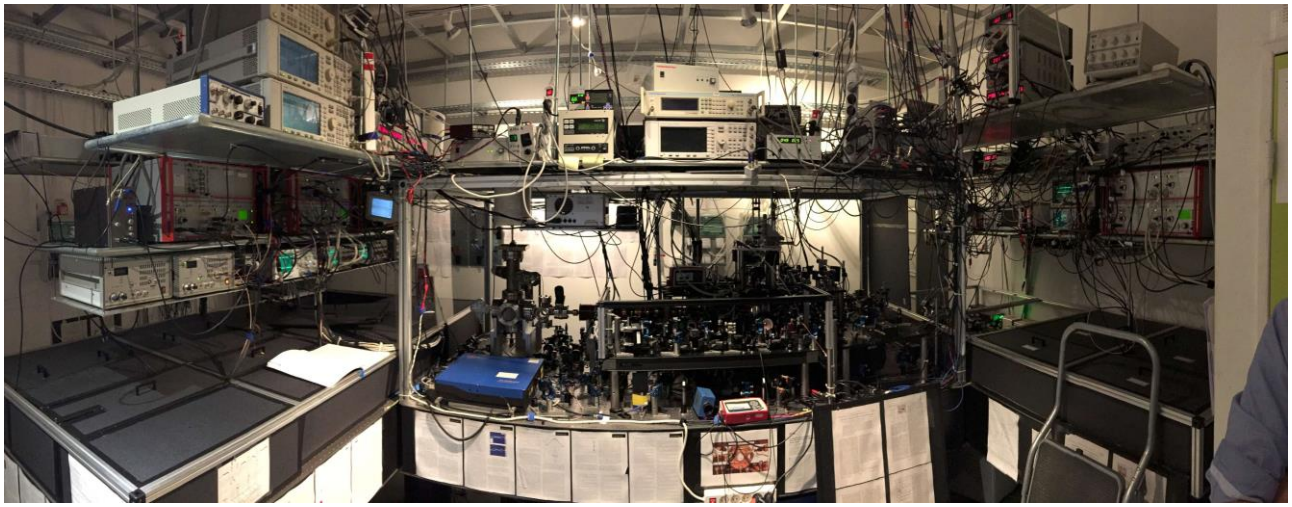
Single atoms are trapped in an energy potential pattern created by lasers



Each green dot is a Rubidium atom arranged within a torus

Côté performance et qualité des qubits, ils atteignent un temps de cohérence de 1 ms avec des portes de 1 µs, donc de quoi enquiller un millier de portes quantiques, hors codes de correction d'erreur. Le taux d'erreur des portes serait de 3% et le taux d'erreur de mesure de 1% ce qui est tout à fait raisonnable, tout du moins pour de la simulation quantique. L'ordinateur tiendra à terme dans un rack de data center et fonctionnera à température ambiante et sous vide. Ils développent leur propre environnement de programmation à bas niveau qui aura pour vocation à s'interfacer avec des langages de programmation à haut niveau du marché.

C'est un investissement « actif » du fonds Quantonation à savoir que Christophe Jurczak, le general partner du fonds, est le Chairman de la startup. Alain Aspect en est conseil scientifique. L'équipe comprend trois fondateurs autour du CEO, Georges-Olivier Reymond.



L'un des laboratoires de tests de la startup Pasqal à l'école Supoptique à Palaiseau. L'installation comprend un émetteur de rubidium suivi d'un décélérateur magnétique et d'une cuve sous vide qui permet de les confiner. Ils sont ensuite contrôlés par lasers.

[390] Les atomes de Rydberg ont des usages insoupçonnés comme pour gérer de la musique aléatoire. Voir Quantum music to my ears, juin 2019. Cela change de la musique générée par du deep learning !

PSIQUANTUM

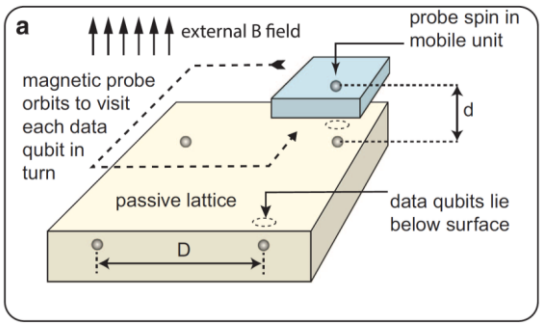
PsiQuantum (2016, Palo Alto, California, $230M) est une startup créé par Jeremy O'Brien, un chercheur de Stanford et de Bristol, qui veut créer un processeur quantique en CMOS et photonique. Il est accompagné de Pete Shadbolt et Terry Rudolph. Ses travaux de recherche sont nombreux dans le domaine, notamment dans les quantum dots en arséniure de gallium, dans les qubits en spin de diamant, la conception de systèmes cryogéniques et de systèmes de contrôle haute fréquence. L'architecture de leur ordinateur quantique s'appuierait sur du MBQC (Measurement Based Quantum Computing) qui est une variante spécifique des ordinateurs à portes quantiques.

Quantum Motion Technologies

Quantum Motion Technologies (2017, UK) est une spin-off de l'Université d'Oxford qui ambitionne de créer une plateforme d'ordinateur quantique CMOS permettant de créer des puces avec une grande densité de qubits. Ils ont bénéficié d'un financement d'amorçage non précisé du fonds britannique Parkwalk Advisors en 2017.

La startup ambitionne d'industrialiser un procédé créé par l'équipe de Joe O'Gorman de l'Université d'Oxford consistant à séparer nettement des qubits CMOS et à mesurer leur valeur en fin de calcul avec une sonde magnétique déplacée mécaniquement en surface faisant des mouvements « carrés » comme décrit dans le schéma suivant. C'est une structure guidée mécaniquement par un MEMS (micro-electro-mechanical device).

Les qubits sont espacés de 400 nm (D) tandis que les sondes sont à 40 nm des qubits (d). Le tout est complété par un système de « surface code » associant plusieurs qubits physiques pour créer des qubits logiques.



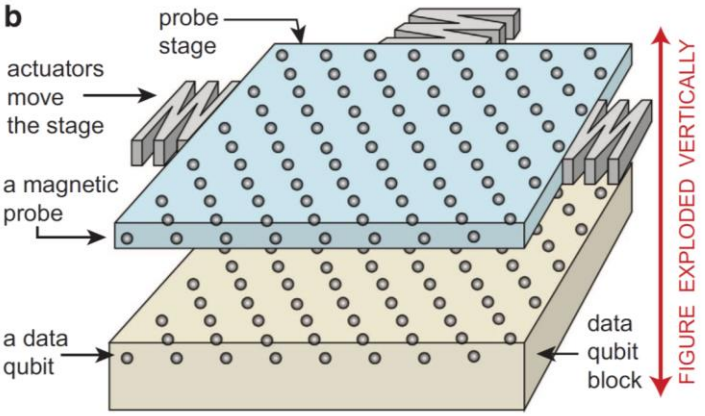


Figure 1. (**a**) The principle of the orbital probe parity measurement: a probe spin comes into proximity with four data qubits in turn during one cycle. (**b**) Simplified schematic of a scalable device showing that the probe layer and the data qubit layer both contain extended spin arrays (details of the their relative positions are shown in Figure 3). We depict the probe stage as mobile, whereas the data qubit stage is static, but in fact either may move; it is their relative motion that is key.

Ce système de sondes évite l'usage d'électronique de commande prenant de la place dans le circuit CMOS[391] et permet une meilleure séparation entre les qubits. Ils utilisent aussi un procédé de séparation des qubits de données avec des dots de médiation intermédiaires, limitant les effets de fuite[392]. Ce procédé est protégé par un brevet US validé et quatre brevets en cours de dépôt.

Leur roadmap consiste dans les trois ans qui viennent (2019-2022) à produire des « small cells » de 5 qubits dans une structure qui pourrait alors être reproduite dans une matrice. Ils pensent ensuite pouvoir aboutir à la création d'un ordinateur quantique avec 100 qubits logiques d'ici 2029.

Et la fabrication des composants ? Ils prévoient de la réaliser dans des fonderies classiques, notamment celle du laboratoire IMEC en Belgique qui est un peu l'analogue du CEA-Leti chez eux.

Ils n'ont pas encore décidé s'ils iraient jusqu'au bout de la création d'un ordinateur quantique. Ils sont actuellement une dizaine de personnes dans la startup.

QCI (2015, USA, $18M) ou Quantum Circuits Inc est une spin-off de l'Université de Yale cofondée par Rob Schoelkopf, Luigi Frunzio et le français Michel Devoret (ex CEA). Ils veulent créer des qubits supraconducteurs avec l'objectif, plus que courant dans le domaine, de résoudre les problèmes de bruit et de cohérence de cette technologie. Leur technologie est à base de qubits supraconducteurs transmon. Leur originalité se situerait dans la méthode de gestion des corrections d'erreurs des qubits réduisant le besoin de redondances en nombre de qubits. Leur communication parle d'ordinateurs génériques faciles à reconfigurer selon les besoins. Ce qui semble être une caractéristique commune des ordinateurs quantiques universels.

Quantum Factory (2018, Allemagne) veut commercialiser des ordinateurs quantiques à base d'ions piégés sous la forme de ressources dans le cloud.

[391] Voir A silicon-based surface code quantum computer de Joe O'Gorman & Al, 2015 (14 pages). Le papier est cosigné par John Motin et Simon Benjamin qui sont deux cofondateurs de la startup Quantum Motion Technologies.

[392] Voir A Silicon Surface Code Architecture Resilient Against Leakage Errors de Zhenyu Cai (Quantum Motion Technologies) & Al, avril 2018 (19 pages).

Quix Photonics (2019, Pays-Bas) développe un processeur quantique photonique utilisant des nitrures de silicium (SiN^4) comme guides d'ondes. C'est un projet issu de l'Université de Twente et du laboratoire AMOLF d'Amsterdam.

Silicon Quantum Computing (2017, Australie, $66M) est une spinoff de l'University of New South Wales (UNSW) et de son laboratoire Centre of Excellence for Quantum Computation and Communication Technology (CQC2T). Ils planchent sur une technologie CMOS proche de celle du CEA-Leti de Grenoble. A court terme, ils veulent sortir un circuit de 10 qubits d'ici 2022. La société a été créée par Michelle Simmons, une des rares femmes de l'écosystème entrepreneurial du quantique.

TundraSystems (2014, UK) développe un processeur quantique en optique linéaire fonctionnant à température ambiante. Difficile de savoir où ils en sont exactement. Ils ont l'air de vouloir créer un microprocesseur en photonique, et pas forcément, un ordinateur quantique avec des qubits utilisant l'optique linéaire.

Turing Inc (USA) est une startup qui ambitionne comme Rigetti de créer une offre matérielle et logicielle d'ordinateur quantique, à base de qubits utilisant des cavités de diamants (NV Centers) et fonctionnant à 4K, une température certes basse, mais gérable avec une cryogénie plus simple, à base d'hélium 4[393]. Ils développent aussi des systèmes de correction d'erreurs qu'ils commercialisent auprès d'autres spécialistes du secteur. Une manière de ne pas mettre tous ses œufs dans le même panier !

Universal Quantum (2019, UK) est une spin-off du Ion Quantum Technology Group de l'University of Sussex dirigée par Winfried Hensinger. Ils développent un ordinateur quantique à ions piégés exploitant de longues longueurs d'onde et des champs magnétiques pour leur contrôle en lieu et place de lasers.

[393] Voir Turing Inc: Large Scale Universal Machines, 2017, qui détaille un peu cela.

Xanadu (2016, Canada, $2,5M) développe un ordinateur quantique en optique linéaire avec un nombre de qubits non précisé et probablement très faible. L'ordinateur doit fonctionner théoriquement à température ambiante.

Leurs qubits dénommés qumodes utilisent un encodage utilisant le principe de "Continuous Variable", qui stocke une information plus riche que les qubits. Cela rappelle le CV-QKD, une variante des clés quantiques utilisant un principe voisin de communication utilisant la phase et l'amplitude des photons, dont nous parlerons dans la partie suivante de cette série, dédiée à la cybersécurité[394]. Xanadu développe la plateforme logicielle qui va avec, dénommée Strawberry Fields et créée sans surprise en Python[395]. La plateforme comprend le langage Blackbird. Ils visent notamment le marché de la chimie, la théorie des graphes et le machine learning quantique. Tout cela est proposé en open source.

Logiciels et outils

Les startups de logiciels et d'outils de développement quantiques ne sont pas encore très nombreuses. Une bonne part d'entre elle travaille autour de D-Wave qui est le seul fournisseur d'ordinateurs quantiques commerciaux, même si ceux-ci ne sont pas des ordinateurs quantiques universels. Elles sont d'ailleurs souvent canadiennes, comme D-Wave.

[394] Leur procédé est décrit dans Continuous-variable gate decomposition for the Bose-Hubbard model, 2018 (9 pages).

[395] Elle est documentée dans Strawberry Fields: A Software Platform for Photonic Quantum Computing, 2018 (25 pages).

Il y a de véritables opportunités à se positionner sur ce marché naissant ! Vous remarquerez que cet inventaire ne comprend pas de startup chinoise. Ce n'est probablement pas par hasard.

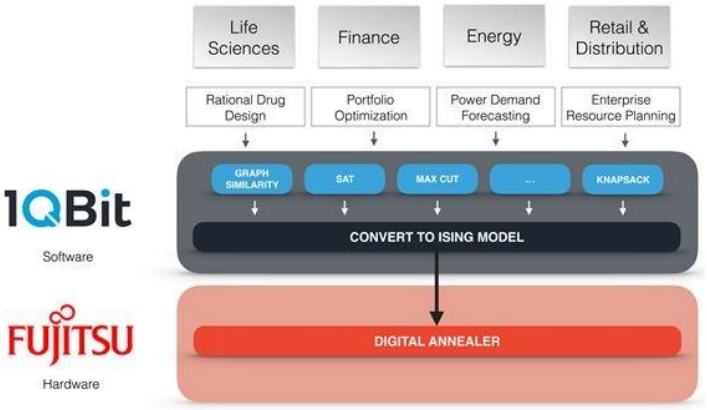
Cet écosystème est donc encore très jeune. Il évoluera en parallèle avec la mise au point d'ordinateurs quantiques commerciaux.

Le pays n'est pas très versé dans le logiciel comparativement au matériel et il semble avoir mis la priorité quantique sur la cybersécurité plus que sur le calcul quantique.

1QBit (2012, Canada, $35M) est un éditeur de logiciels quantiques multi-sectoriel. La société a été notamment financée par Fujitsu avec qui ils sont partenaires, ainsi qu'auprès d'Accenture et d'Allianz.

Ils sont comme il se doit également partenaires de D-Wave qui les met bien en avant dans son marketing. Ils ont développé des briques algorithmiques quantiques diverses de bas niveau qui sont indépendantes des architectures matérielles cibles. Cela comprend par exemple le traitement de graphes qu'ils appliquent dans un grand nombre de marché, via une activité de consulting.

Ils couvrent notamment les marchés financiers, pour l'optimisation dynamique de portefeuille d'investissement[396] ou pour simplifier l'allocation de classes d'actifs dans un portefeuille. En plus d'être un partenaire historique de D-Wave, ils le sont aussi avec IBM. La startup a déjà une centaine de collaborateurs. Ils ont aussi comme clients Dow Chemical (chimie), Biogen (biotechs) et Allianz.



1QBit Software running on Fujitsu Hardware – Source: Fujitsu

Aliro Quantum (2018, USA, $2,7M) est une startup sortie du bois en septembre 2019 qui développe des briques logicielles permettant d'indiquer aux développeurs si des ressources cloud de calcul quantique sont disponibles pour réaliser des calculs plus rapidement que sur des processeurs traditionnels, notamment de type GPU. La startup a été crée par Prineha Narang et Jim Ricotta. Bref, une sorte de « quantum cloud resources provisioning ».

[396] Voir Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer, 2015 (13 pages).

Evidemment, ce cloud se veut neutre du point de vue des technologies d'ordinateurs quantiques utilisées. Mais ce genre d'outil devrait être relié aux technologies de compilateurs qui savent tirer parti des caractéristiques spécifiques de chaque type d'ordinateur quantique.

Anyon Systems (2014, Canada) développe des outils de simulation du comportement d'ordinateurs quantiques supraconducteurs pour optimiser leur conception. Ils ont notamment aidé Google à mettre au point ses premiers prototypes d'ordinateurs quantiques supraconducteurs.

ApexQubit (2018, Biélorussie) développe des solutions logicielles quantiques pour le secteur de la finance. Ils fonctionnent en mode projet.

A*Quantum (2018, Japon) est spécialisé dans le développement de solutions logicielles quantiques pour les ordinateurs à recuit quantique comme à ceux qui utilisent des portes quantiques universelles. Leur ambition est de créer des briques logicielles de haut niveau destinées à des utilisateurs.

Ankh.1 (2018, USA) a développé Anubis Cloud, une machine virtuelle dans le cloud pour les data scientists s'intégrant avec la solution open source Jupyter ainsi qu'avec les frameworks de machine learning Tensorflow et Keras.

AppliedQubit (UK) se présente comme un éditeur de logiciels quantiques pour les entreprises. Ils ciblent notamment les deux principaux marchés du moment : la finance et la simulation chimique en plus de problèmes génériques d'optimisation et d'analyses prédictives. Ils développent à la fois des solutions de calcul hybrides classique/quantique et de quantum machine learning.

Artiste-qb.net (Canada) a un modèle d'activité voisin de celui de 1Qbit : ils développent des briques algorithmiques de niveau intermédiaires qu'ils assemblent ensuite au gré des besoins de leurs clients. Ils ont même déposé des brevets pour certaines méthodes. La startup a été créée par une équipe internationale comprenant notamment des chercheurs allemands.

Automatski (2014, USA) est une société de services établie d'abord à Londres, puis en Inde à Bengalore et récemment en Californie. Ils font de la recherche appliquée sous contrat de développement d'algorithmes quantiques sur toute forme d'ordinateur et de simulateur quantique. Ils ont notamment développé une solution logicielle permettant de simuler un grand nombre, non précisé, de qubits sur ordinateur classique. Ils développent des algorithmes en biochimie. Sur la forme, cette société est curieuse.

C'est une holding de sociétés de recherche qui tire dans tous les sens : informatique quantique, intelligence artificielle générale, robotique, blockchain, voyage spatial, guérison du cancer, etc, le tout associé à une mystique indienne[397].

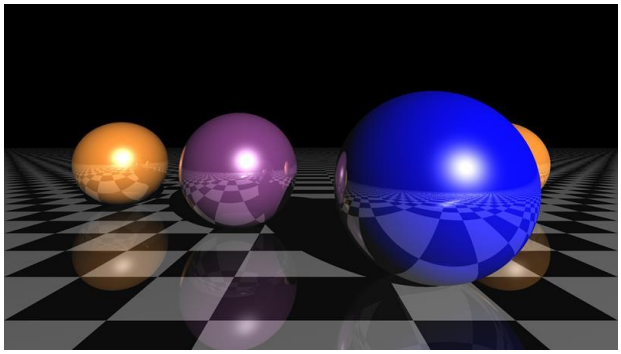
Beit.tech (2016, Pologne) est spécialisé dans le quantum machine learning. C'est surtout un projet de recherche financé par l'Union Européenne, couvrant la période 2017-2010. Le créateur Wojtek Burkot est un ancien de Google qui cherche même à rendre les D-Wave inutiles en créant des algorithmes d'optimisation de graphes complexes pouvant tourner sur ordinateurs traditionnels.

[397] Voici ce qu'indique leur site web : « *One of the earliest breakthroughs at Automatski Fundamental Research has been to (i) discover the working of the Human Mind and Brain, Consciousness and Soul, and explain Heaven, Hell, Rebirth, Consciousness etc. in a purely scientific non-religious or non-philosophical manner. And also (ii) to explain the Begining, Evolution and End of the Universe also explaining everything like Blackholes, Worm Holes, Space-Time, The Creation of Time, Particle-Wave Duality, Matter-Antimatter, Dark Matter, Dark Energy etc. without any contradictions in a single theory. In the next phases of Research, Automatski Fundamental Research made breathroughs in Science and Technology. From Robotics, to Artificial General Intelligence, NP Complete Problem Solutions, Quantum Computing and Quantum Simulations, Environment, Finance, Drug Research, Machine Learning, Operations Research, Chip Design, Computing, Mathematics, Algorithms, Automatic Theorem Proving, Drug Research, Space Travel etc. Our Mission is to Solve The Toughest Problems Facing Humanity and to Democratize and Guarantee the Health, Prosperity and the Survival of the Human Race.*".

Black Brane Systems (2016, Canada) est une startup focalisée dans le développement de solutions de machine learning quantiques. Ils sont très "stealth" à ce stade.

Boxcat (2017, Canada) développe des solutions de traitement de l'image et de video à partir d'algorithmes quantiques. Ils visent les marchés des médias et de l'imagerie médicale.

Leurs algorithmes sont hybrides et s'appuient sur les architectures matérielles disponibles du moment (D-Wave, IBM, Rigetti). La prouesse qu'ils présentent sur leur site est une image réalisée sur un D-Wave, qui aurait pu l'être avec les derniers GPU de Nvidia.



Cambridge Quantum Computing Limited (2015, UK, $50M) développe le système d'exploitation quantique (**ti|ket>**) et divers algorithmes quantiques dont Arrow dans le machine learning. Ils sont comme nous l'avons vu plus haut partenaires d'**Oxford Quantum Circuits** qui travaille sur la partie hardware. Et aussi d'IBM. CQC est aussi actif dans la cryptographie post-quantique.

CogniFrame (2016, USA) est un éditeur de logiciel de plateforme d'analyse de données exploitant le machine learning. Ils développent aussi des algorithmes hybrides pour le secteur financier en s'appuyant sur les ordinateurs de D-Wave. L'un de leurs premiers clients est la banque d'investissement américaine Alterna Savings. Les applications proposées sont classiques dans le domaine financier : évaluation de risque de crédit et optimisation de portefeuille d'investissements.

$$\frac{d\vec{v}}{dt}$$

dividiti (2014, UK) développe des algorithmes quantiques notamment dans le machine learning et des méthodes hybrides. Leurs solutions sont open source. C'est donc un modèle de services, qui est plutôt la norme dans ce marché pour l'instant.

D Slit Technologies

D Slit Technologies (2018, Japon) développe des solutions logicielles quantiques sur mesure pour créer des preuves de concept. Leur site web n'est pas très bavard sur leurs réalisations.

ELYAH

Elyah (2018, Dubaï) développe des applications quantiques non précisées. Ils créent aussi des solutions classiques de deep learning de reconnaissance d'images.

ENTROPICA LABS

Entropica Labs (2018, Singapour) est une startup dédiée à la création d'algorithmes quantiques (et non quantiques) pour les sciences du vivant et en particulier pour faire de la génomique, à base de quantum machine learning. Avec à la clé, le développement plus rapide de thérapies, en partenariat avec les boites de pharma. La société a été créée par Tommaso Demarie et Ewan Munro.

EVERETTIAN

Everettian Technologies (2017, Canada) est une autre startup logicielle focalisée sur les usages du quantique dans le machine learning.

GTN Limited (2017, UK, $2,7M) développe un “Generative Tensorial Networks” pour faire du QML (quantum machine learning) afin de simuler, filtrer et faire des recherches de nouveaux traitements thérapeutiques.

Horizon Quantum Computing (2018, Singapour) créé des outils de développement quantiques, sans plus de précisions.

HQS Quantum Simulations (2018, Allemagne) est une startup de Karlsruhe qui développe des algorithmes quantiques dans le domaine de la simulation moléculaire organique et inorganique de molécules simples (méthane, émission de lumière dans des OLED, diffusion de molécules dans des liquides). Ils ont annoncé en juillet 2018 un outil de portage open source de code ProjectQ (plateforme IBM) vers Cirq (plateforme Google). Ils ont déjà BASF et Bosch comme clients. Ils s‘appelaient avant Heisenberg.

Innovatus Q (Singapour) est une spin-off du Centre for Quantum Technologies de Singapour. Ils travaillent des des algorithmes quantiques hybrides à base d’ions piégés et de supraconducteurs.

JoS Quantum (2018, Allemagne) développe des solutions logicielles quantiques destinées aux services financiers et notamment dans la gestion de risques et la détection de fraudes. Ils font aussi de la recherche sous contrat.

Ketita Labs (2018, Estonie) développe des logiciels quantiques non précisés pour des ordinateurs NISQ, et pour cause, puisqu'il n'y a que cela à se mettre sous la dent. C'est une spin-off d'université.

Menten.ai (2018, Canada) développe des algorithmes hybrides associant machine learning et programmation quantique pour simuler la chimie organique et concevoir des enzymes.

Multiverse Computing (2017, Espagne) développe des logiciels quantiques pour la finance, pour l'optimisation de portefeuilles, l'analyse de risques et la simulation de marchés.

NetraMark (2015, Canada) développe des solutions logicielles quantiques pour les industries pharmaceutiques pour définir des cibles thérapeutiques. Ils sont issus du programme Quantum Machine Learning du Creative Destruction Lab de Toronto.

Origin Quantum Computing (2017, Chine) est une startup basée à Hefei en Chine qui semble développer des algorithmes quantiques. Ils sont notamment à l'origine de l'un des records de simulation d'algorithme quantique de 64 qubits sur un supercalcu-

lateur[398]. Ils indiquent aussi développer leurs propres chipsets quantiques dont une version supraconductrice de 6 qubits (KF C6-130). Ils ont développé l'OriginQ Quantum AIO, un système de contrôle d'ordinateur quantique ainsi que le langage QRunes, l'architecture QPanda intégrant langage et compilateur et la machine virtuelle EmuWare. Côté applicative, ils ont notamment investi dans la simulation chimique. Ils font de tout et doivent légèrement survendre l'ensemble !

Phase Space Computing (2017, Suède) est une spin-off de l'Université de Linköping qui développe des solutions de formation sur l'informatique quantique desinées à l'enseignement secondaire et supérieur.

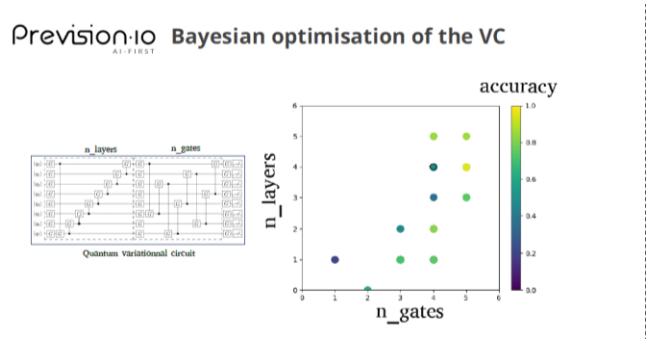
PhaseCraft (2018, UK, $1M) est une société de logiciels quaniques issue de l'University College London et de l'Université de Bristol.

Ils sont aussi partenaires de Google. Ils veulent exploiter le calcul quantique pour créer de meilleurs systèmes de collecte et de stockage de l'énergie (batteries, solaire PV, …).

Prevision.io (2016, France, 1,5M€) est une startup spécialisée dans le machine learning. Ils ont développé une plateforme qui automatise le choix de modèles de machine learning pour exploiter des données structurées. Ils envisagent d'utiliser des algorithmes quantiques, notamment de QML (Quantum Machine Learning) pour compléter leur bibliothèque d'outils.

Cela a du sens, d'autant plus que pour faire cela, la startup n'a pas besoin d'acquérir un ordinateur quantique ! On en trouve quelques-uns dans le cloud pour faire ses premiers tests sans compter les outils de simulation fonctionnant sur ordinateurs traditionnels ou supercalculateurs. Le quantique, ce sera surtout du cloud computing !

[398] Voir Researchers successfully simulate a 64-qubit circuit, juin 2018.



Previsionio Benchmark

	Classic			Quantum	
$n_{classes}$	DT	LR	NN	VC	VC-BO
2	0.993	0.996	0.996	0.920	0.969
3	0.922	0.977	0.968	0.752	0.807

En mai 2019, le fondateur de la startup Nicolas Gaude, et un chercheur de la startup, Michel Nowak, PhD, présentaient les résultats de leur étude d'accélération quantique d'un algorithme de machine learning hybride, « Quantum Variational Circuits » sur un test de reconnaissance d'écriture du MNIST, le même que pour les débuts de réseaux de neurones convolutionnels de Yann LeCun en 1988. Le principe consiste à optimiser les hyperparamètres d'un réseau de neurones dans la partie quantique du calcul, couplé à une optimisation bayésienne fonctionnant de manière classique. C'est donc un algorithme quantique hybride.

Leur modèle illustrait l'intérêt d'une accélération quantique avec juste 20 qubits[399], simulés sur la bibliothèque de simulation quantique PennyLane de Xanadu. Ils estiment qu'un avantage quantique serait démontrable sur leur algorithme à partir de 28 qubits permettant de superposer l'équivalent d'un milliard d'hyperparamètres d'un réseau de neurones.

ProteinQure

ProteinQure (2017, Canada) est une startup basée à Toronto qui utilise différentes technologies dont du calcul quantique pour créer et simuler de nouvelles thérapies "*in silico*". Ils utilisent des algorithmes quantiques pour simuler le repliement de protéines. Ils développent aussi des algorithmes hybrides exploitant aussi des GPUs. Ils supportent différentes architectures matérielles dont les ordinateurs de D-Wave. Dans leurs expériences, ils arrivent à simuler des molécules avec 6 atomes dans des ordinateurs quantiques universels et atteignent 11 atomes avec les D-Wave.

QBITLOGIC

QbitLogic (2014, USA, $1,5M) est une autre startup qui développe des applications de machine learning en quantique, sans plus de précision dans leur communication.

[399] Voir leur publication "One step towards quantum hyper parameter search", Michel Nowak et Nicolas Gaude (juin 2019).

Q-Ctrl (2017, Australie) est une startup créée par Michael Biercuk, de l'Université de Sydney. Ils développent un firmware en cloud pour ordinateur quantique focalisé sur la gestion des codes de correction d'erreurs, Black Opal. Ils ont aussi un outil de visualisation de l'effet de la modification de l'état des qubits par des portes quantiques… dans la sphère de Bloch. Ils sont notamment partenaires d'IBM.

QC Ware (2014, USA, $8M) développe une plateforme de développement de logiciels quantiques en cloud. Ils créent des algorithmes quantiques et logiciels pour de grandes entreprises. L'une d'entre elles est le groupe Airbus qui fait partie de leurs investisseurs.

Ils ciblent le marché aérospatial, la défense, la finance et la cybersécurité. Ils ont aussi reçu un financement public US de $1M via la NSF en 2017. Ils sont notamment partenaires d'IBM.

Qilimanjaro Quantum Hub (2018, Espagne) est une startup de Barcelone, donc plutôt Catalane ! Eux-aussi développent une plateforme logicielle quantique en cloud[400]. Ils veulent aussi développer leur propre ordinateur quantique adiabatique à base de qubits de flux. Ils prévoient aussi de se faire financer via une ICO, les tokens associés étant le QBIT, une cryptomonnaie d'usage de leurs ressources en cloud. Qui n'existent pas encore !

Qindom Inc. (2018, Canada, $2M) est une startup spécialisée dans le développement de logiciels de QML (quantum machine learning) sur ordinateurs quantiques D-Wave.

Qrithm (2018, USA) développe des algorithmes quantiques dans des domains divers et plutôt disparates: machine learning, science des matériaux, cryptographie et finance.

[400] Voir leur livre blanc : Qilimanjaro White paper (53 pages).

Quandco (2016, Pays-Bas) développe des solutions logicielles quantiques sur mesure pour de grandes entreprises, accompagnés par des outils de benchmark. Ils visent en particulier les applications de l'IA quantique ainsi que de la simulation chimique. Ils sont partenaires d'IBM et de Microsoft.

QuantFi (2019, France) est une jeune startup spécialisée dans la création de solutions logicielles quantiques pour la finance.

Quantum Benchmark Inc (2017, Canada) fournit une solution logicielle de code de correction d'erreurs pour ordinateurs quantiques universels et d'évaluation de ces erreurs. C'est donc en apparence un concurrent de l'Australien Q-Ctrl. Ils proposent aussi un système de validation de performance d'ordinateur quantique.

L'ensemble est intégré dans la suite True-Q, lancée en 2018, avec True-Q Design qui sert à évaluer le taux d'erreurs d'un ordinateur quantique et à en optimiser l'architecture et True-Q OS qui permet d'optimiser la précision des solutions logicielles.

Le marché visé est au départ celui des constructeurs d'ordinateurs quantiques et ceux qui les évaluent. A terme, cela sera celui des clients utilisateurs. A noter qu'ils ont déjà testé le framework Cirq de Google, ayant fait partie du programme de beta test de ce langage de Google et que ce dernier utilise leur solution. Ils sont aussi partenaires d'IBM.

Quantastica (2019, Estonie et Serbie) développe des outils logiciels d'algorithmes quantiques hybrides dont le Quantum Programming Studio, un environnement de développement web graphique pour créer des algorithmes quantiques exécutables sur ordinateurs quantiques ou sur simulateurs, dont un simulateur classique qu'ils ont eux-mêmes développé.

Quantopo LLC (2017, USA) est une société spécialisée dans les algorithmes de quantum machine learning. Ils se focalisent sur les biotechs.

Qubitera (2018, USA) développe des solutions associant IA et quantique. N'a pu qu'à !

QuDot (2018, USA) développe des logiciels de simulation de circuits quantiques sur ordinateurs traditionnels, le QuDot Net. Ils utilisent des techniques à base de réseaux bayésiens pour optimiser la représentation en mémoire des qubits.

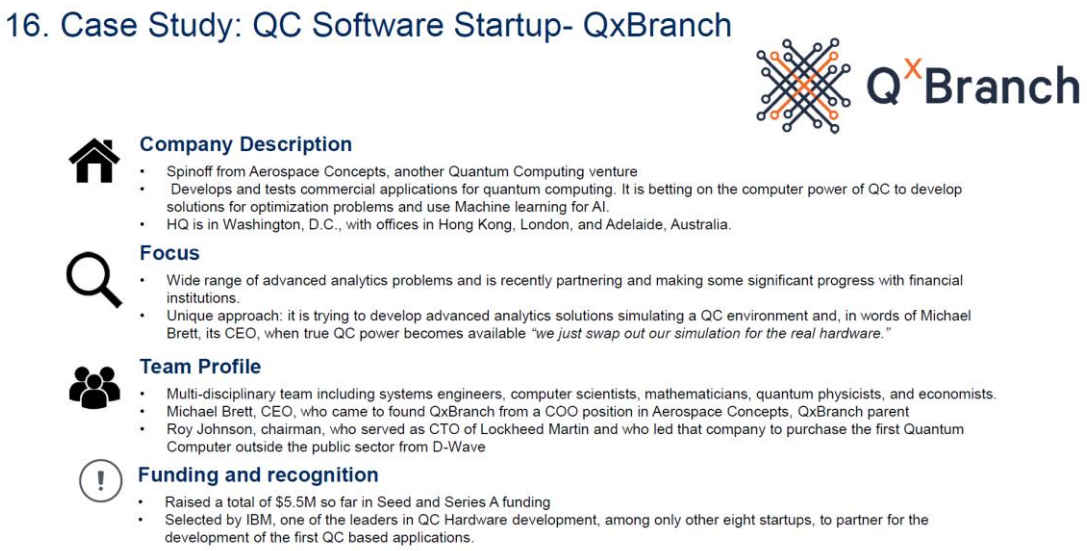
QuLab (2017, USA) est une startup spécialisée dans les algorithmes quantiques pour la conception de molécules thérapeutiques.

QunaSys (2018, Japon) développe aussi des algorithmes quantiques pour la santé. Issue des université de Tokyo, Osaka et Kyoto, ils assurent aussi la maintenance du simulateur Qulacs développé à l'Université de Kyoto.

QuSoft (2014, Pays-Bas) est la spin-off de l'Université TU Delft spécialisée dans les algorithmes et logiciels quantiques. Comme sa sister-company QuTech, c'est plutôt un laboratoire privé de recherche appliquée qu'une startup.

Q^{x}Branch (2014, USA) a été créé par des anciens de Lockheed Martin. Elle propose des solutions, probablement sur mesure, pour les marchés de la finance, de l'assurance, de l'aérospatial et de la cybersécurité.

Basé à Washington DC, ils ont déjà des bureaux à Hong Kong, Londres et Adelaide en Australie. Ils sont partenaires de D-Wave et d'IBM.



source : VC investment analysis Quantum Computing, Insead, 2018 (18 slides).

Rahko (2018, UK) est une société de développement de logiciels de quantum machine learning basée à Londres.

River Lane Research (2016, UK) est une spin-off de l'Université de Cambridge qui fournit du service dans l'informatique quantique et développe de nouveaux algorithmes associant machine learning et le quantique dans le domaine de la chimie.

Ils développent avec dividiti Ltd (un one man shop créé par un certain Grigori Fursin), le Quantum Collective Knowledge, un SDK de benchmark de matériels et logiciels quantiques.

SHYN (2016, Bulgarie) développe des solutions de visualisation de données issues de calculs quantiques. Donc, du dataviz quantique ! Elle a été cofinancée par Google et des fonds européens.

SoftwareQ (2017, Canada) propose des logiciels de développement pour le calcul quantique : compilateur, simulateur, optimisateurs. La société a été cofondée par Michele Mosca et Vlad Gheorghiu de l'Institute of Quantum Computing canadien.

Solid State AI (2017, Canada) développe une plateforme logicielle quantique en cloud exploitant des algorithms hybrides adaptés aux besoins de l'industrie. C'est une startup issue du programme Quantum Machine Learning du Creative Destruction Lab de Toronto.

Strangeworks (2018, USA, $4M) développe des logiciels quantiques. De manière pas spécialement originale, ils ciblent les marchés de l'aérospatial, de l'énergie, de la finance et de la santé. Ils sont notamment partenaires d'IBM. Ils sont à l'origine de la création d'un site de questions/réponses sur l'informatique quantique, Quantum Computing Stack Exchange.

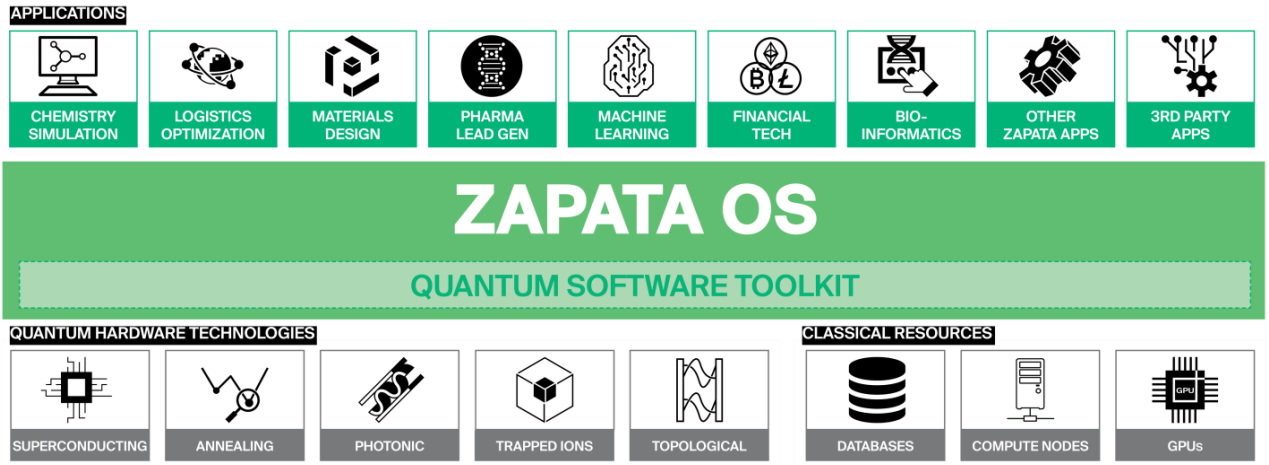
Stratum.ai (2018, Canada) développe un logiciel quantique dédié à un marché très pointu, l'optimisation de la prospection minière, notamment dans l'or.

Tokyo Quantum Computing (2017, Tokyo) veut développer un logiciel de simulation d'ordinateur à recuit quantique.

Xofia (2019, USA) développe des solutions logicielles à base de quantum machine learning de classification.

Zapata Computing (2017, $26,45M, USA) est une société de logiciels et services quantiques créée par des chercheurs de Harvard dont Christoper Savoie et le fameux Alán Aspuru-Guzik de l'Université de Toronto qui est spécialisé dans les applications du quantique dans la chimie. Ils sont notamment partenaires de Google et IBM.

Ils développent un système d'exploitation quantique complet, Zapata OS qui joue le rôle de plaque tournante entre algorithmes applicatifs et ordinateurs quantiques de tous types. C'est en fait du marketing qui regroupe une approche de service outillé.



Voilà, ce petit tour est terminé. Si vous découvrez des startups du calcul quantique qui ne figurent pas dans cet inventaire ou disposez d'informations complémentaires sur celles qui sont citées, je suis preneur ! J'utiliserai vos informations pour actualiser cette liste au fil de l'eau[401].

[401] Voir This Startup Just Raised $21 Million To Bring Quantum Computing To Enterprise Applications, 2019.

Cryptographie quantique

L'algorithme de Peter Shor inventé en 1994 et qui permet de factoriser rapidement des nombres entiers secoue le monde de la sécurité informatique depuis au moins une bonne quinzaine d'années. En effet, il permet en théorie de casser les codes de nombre de systèmes de cryptographie à clés publiques qui sont couramment utilisés sur Internet.

Alors qu'il est loin d'être opérationnel à grande échelle du fait de l'absence d'ordinateurs quantiques universels avec un très grand nombre de qubits logiques, les services de contre-espionnage, de renseignement et les entreprises s'en inquiètent sérieusement lorsqu'ils sont au courant de la menace. Elle pèse même sur une partie du fonctionnement du Bitcoin et de la BlockChain !

Avant donc même que la menace fantôme de Shor se matérialise concrètement, l'industrie de la protection des communications et des contenus se met en ordre de bataille pour y faire face, et plus ou moins rapidement selon les parties prenantes. Les marchés touchés en premier seront l'industrie informatique et des télécoms en général qui va devoir mettre à jour de nombreuses offres logicielles si ce n'est matérielles, les banques, la distribution, la santé et les activités régaliennes des services publics.

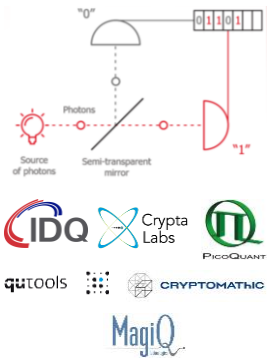
Dans cette partie, nous allons décrire dans l'ordre :

- Les principes de base de la **cryptographie**, notamment à clé publique, avec l'exemple des clés publiques RSA.
- La **menace** provenant de la factorisation de nombres entiers et les solutions de cryptographie concernées.
- Les **générateurs de nombres aléatoires quantiques**, compléments devenus indispensables des solutions de cryptographie de haut vol.
- Les **clés quantiques** qui permettent de sécuriser la partie physique des communications pour l'usage de clés symétriques.
- La **cryptographie post-quantique** qui sert à protéger la partie logique des communications cryptées dans le cas de l'usage de clés publiques.
- Les **startups et offres commerciales** de ces secteurs dans le monde, dans un marché qui comprend déjà de nombreux acteurs.

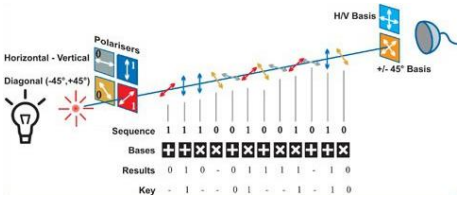
Comme d'habitude, ce genre de texte est le résultat d'une intense recherche bibliographique. Je n'invente rien ! Tout est là, prêt à être synthétisé. Je cite à chaque fois que possible les sources d'informations que j'utilise dans ce travail de vulgarisation.

Je me suis heurté à un domaine que les spécialistes ne vulgarisent vraiment pas bien du tout. C'est d'un cryptique, c'est le cas de le dire ! J'ai donc eu ici l'impression d'être encore plus largué que lorsque je m'attaquais au modèle de représentation mathématique des qubits, aux registres quantiques ou aux algorithmes quantiques.

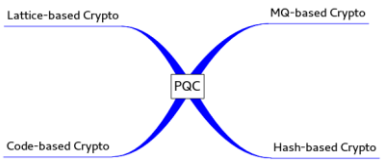
générateur quantique de nombres aléatoires
assure la qualité des clés utilisées



clés quantiques QKD / BB84
protège les clés symétriques par liaison optique



cryptographie post-quantique
cryptographie à clés publiques résiliente à l'agorithme de Shor



Je préfère le dire et l'assumer ! Sans vous décourager pour autant car ce que j'ai compris permet déjà se dégrossir le sujet à grosses mailles avant d'essayer de creuser les mathématiques associées si cela vous chante, ou si vous l'avez déjà fait[402].

Cryptographie par clé publique

Côté vocabulaire, précisons que la cryptologie est la science des secrets. Elle permet la transmission d'informations sensibles entre un émetteur et un récepteur et de manière sure. La cryptologie comprend la cryptographie, qui sécurise l'information émise et la cryptanalyse qui cherche à la décrypter par attaque. Les puristes francophones parlent de chiffrement et de déchiffrement, lorsque l'on encode et décode l'information puis de décryptage, lorsqu'un attaquant décode les messages.

Dans le cas de la cryptographie asymétrique à clé publique, le chiffrement n'exploite que les clés publiques et le déchiffrement s'appuie sur les clés publiques et privées. Le décryptage exploite uniquement les clés publiques en cherchant à en déduire les clés privées par du calcul, souvent intensif.

La cryptographie sécurise l'information transmise de plusieurs manières :

- Par la **confidentialité** : seul le destinataire peut récupérer la version non cryptée de l'information transmise.
- Par l'**intégrité** : l'information n'a pas été modifiée pendant sa transmission.
- Par l'**authentification** : chacun est bien celui qu'il prétend être.
- La **non-répudiation** : l'émetteur ne peut pas nier avoir transmis l'information cryptée.
- Le **contrôle d'accès** : seules les personnes autorisées par l'émetteur et le récipiendaire peuvent accéder à l'information non cryptée.

[402] Voici un appercu général de la QKD et de la PQC : The Impact of Quantum Computing on Present Cryptography, mars 2018 (10 pages).

Avant les télécommunications informatiques, la confidentialité était assurée par la connaissance d'un secret commun entre émetteurs et récepteurs, les fameux codes de chiffrement et de déchiffrement, pouvant être la position des roues d'une machine **Enigma** allemande pendant la seconde guerre mondiale. Cela fonctionnait dans des environnements fermés comme pour les communications militaires ou entre ambassades et pays d'origine.

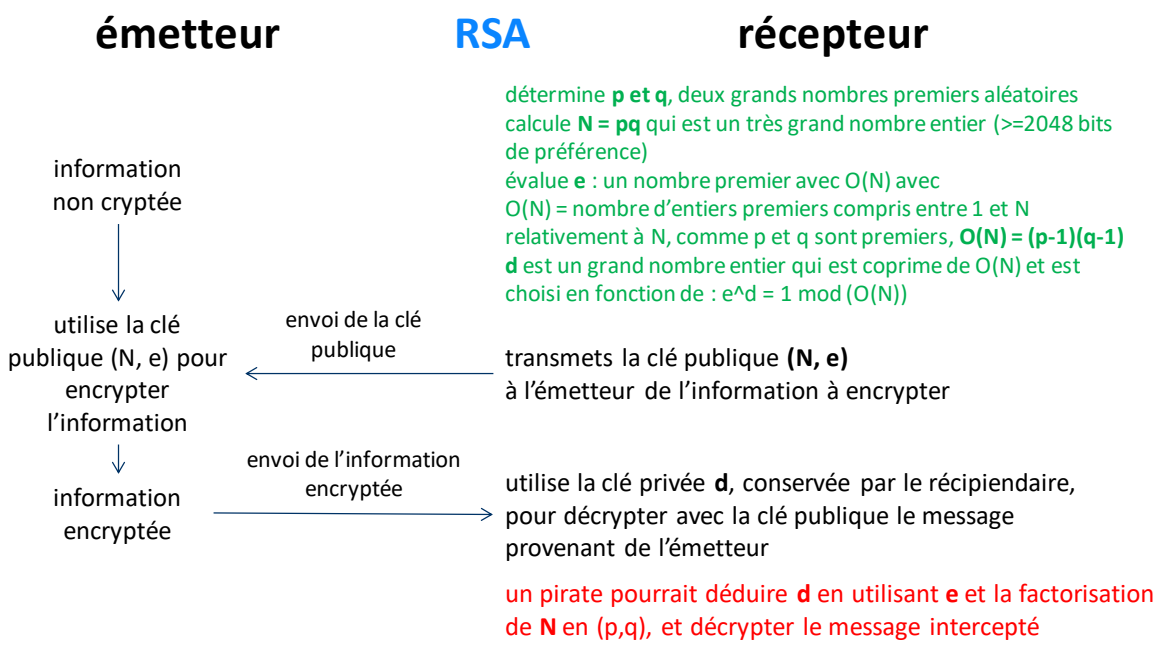
Avec les communications sur Internet, ce mode opératoire est inapplicable pour des applications grand public et pour les relations entre les entreprises en général. D'où les systèmes de cryptographie à clés publiques, notamment RSA, qui servent à un grand nombre d'échanges d'informations. Il subsiste des systèmes très protégés à base de clés privées et symétriques et qui sont principalement utilisés dans le cadre des applications régaliennes (armée, sécurité, renseignement) ainsi que dans divers autres cas (transferts de fichiers, chiffrage de mails, échanges serveur/client, dans les cartes à puces et terminaux de paiement associés).

La cryptographie asymétrique (à clés publique) est aussi exploitée pour l'établissement préalable de clés de chiffrement communes entre les utilisateurs de systèmes à clés privées, pour gérer l'intégrité des communications et pour l'authentification comme dans le protocole TLS sur Internet. Les informations sensibles sont alors cryptées avec ces clés et un algorithme symétrique type AES. AES est ainsi utilisé pour chiffrer les communications dans Whatsapp, Messenger et Telegram. Ces applications utilisent souvent également de la cryptographie asymétrique pour l'authentification, les échanges de clés et la gestion de l'intégrité des communications. Dans de très nombreux cas, les systèmes de cryptographie symétriques cohabitent avec des systèmes de cryptographie asymétriques (à clés publiques). Donc, lorsque vous communiquez sur Internet de manière sécurisée, ce sont plusieurs protocoles de sécurité complémentaires qui sont activés.

Dans les systèmes à clé publique, des clés différentes sont utilisées pour le chiffrement et le déchiffrement des informations transmises, de telle manière qu'il est très difficile (si ce n'est parfois impossible) de déduire la clé privée de déchiffrement à partir de la clé publique de chiffrement. C'est le récepteur du message qui envoie sa clé publique à l'émetteur, qui l'utilise à son tour pour chiffrer le message. Le récepteur utilise la clé privée qu'il a conservée pour déchiffrer le message reçu.

Comme l'explique le schéma *ci-dessous*, la clé privée n'est jamais transmise. C'est ce que l'on appelle aussi une PKI, pour "Public Key Infrastructure".

L'algorithme **RSA** est le plus connu et le plus utilisé des systèmes de protection des transmissions d'information par clé publique sur Internet. Il a été créé en 1978 par **Ron Rivest** (1947, Américain), **Adi Shamir** (1952, Israélien) et **Leonard Adleman** (1945, Américain).



Vous n'avez pas forcément besoin de comprendre la tambouille interne que voici et qui explique comment les clés sont construites. Cela commence par la détermination de p et q, deux grands nombres premiers aléatoires, avec un "bon" générateur de nombres aléatoires. Nous verrons plus loin que la physique quantique permet de créer des générateurs de nombres vraiment aléatoires. On calcule N = pq qui est un très grand nombre entier. Une bonne clé RSA requiert d'avoir N stocké sur au moins 2048 bits sachant que la NSA recommande des clés de 3072 bits pour les applications critiques.

On évalue ensuite **e**, un nombre premier en exploitant O(N) qui égale le nombre d'entiers premiers compris entre 1 et N relativement à N, et qui, comme p et q sont premiers, égale (p-1)(q-1). d est un grand nombre entier qui est copremier de O(N) et est choisi en fonction de : e^d = 1 mod (O(N)). A la fin, on obtient une clé publique qui comprend les entiers N et e, et une clé privée qui comprend d. L'ensemble s'appuie sur la théorie des nombres et utilise notamment le petit théorème de Fermat et le théorème d'Euler qui permettent de créer deux clés distinctes et inverses l'une de l'autre.

La beauté du système permet à n'importe qui d'encrypter un message à partir de la clé publique, ce message n'étant déchiffrable que par celui qui dispose de la clé privée qui décompose la clé publique en primitives.

Un pirate pourrait décrypter l'information envoyée en exploitant e (le bout de la clé publique) et en factorisant N, l'autre bout de la clé publique, en entiers p et q, puis en déduire la clé privée d.

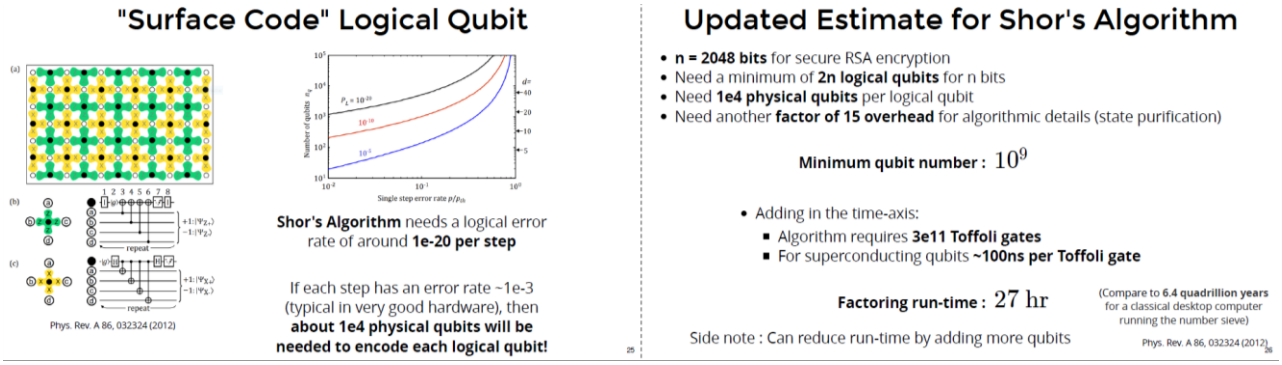
A ce jour, la factorisation de nombres premier demande une puissance machine traditionnelle qui croit à la vitesse de la racine carrée du nombre à factoriser. A ce jour, le record de factorisation officiel de clé RSA est de 768 bits, réalisé en 2010. Cela n'inventorie visiblement pas les records non communiqués de la NSA. Et il est recommandé d'utiliser des clés situées entre 1024 et 2048 bits !

Menace fantôme de Shor

Lorsque nous avons abordé les algorithmes quantiques, nous avons décrit celui de **Peter Shor** inventé en 1994. C'est l'un des premiers algorithmes quantiques après celui de **Deutsch-Jozsa** dont nous avions vu qu'il ne servait quasiment à rien. L'algorithme de Shor a provoqué un intérêt pour le calcul quantique alors que les chercheurs n'avaient pas encore réussi à créer un seul qubit contrôlable par une porte quantique unitaire !

L'algorithme de Shor permet dans un temps raisonnable de factoriser des nombres entiers, proportionnel à leur logarithme. C'est donc une factorisation de temps linéaire en fonction du nombre de bits de la clé. Il se trouve que cela met à mal les systèmes de cryptographiques courants qui reposent sur la notion de clé publique.

Mais uniquement dans un futur relativement lointain ! En effet, pour factoriser un entier sur 1024 bits, il faudrait environ 166 millions de qubits universels avec un taux d'erreur de 0,1% ou 5,5 millions de qubits avec 0,01% d'erreur et 6,6 semaines de calcul à 1 MHz. Ce qui sera hors de portée des ordinateurs quantiques universels pour encore quelques années, au moins une dizaine.



En 2019, des chercheurs de Google publiaient un algorithme permettant de casser plus rapidement une clé RSA (de 2048 bits) et avec moins de qubits. Ils se contentent de seulement 23 millions de qubits avec un taux d'erreur de 0,1% et un calcul réalisé en 8 heures.

Les ordinateurs quantiques actuels ont un temps de cohérence bien court largement inférieur à la seconde, mais le compteur de la décohérence est remis à zéro après chaque code de correction d'erreur qui est utilisé dans l'algorithme [403]?

Selon le **NIST** (National Institute of Standards and Technology US), il faudrait de 3000 à 5000 qubits logiques pour casser une clé RSA de 2048 bits. Selon les technologies utilisées, il faut multiplier ce chiffre par 200 à 20 000 pour le nombre de qubits physiques par qubits logiques, donc entre 1 million et 1 milliard de qubits physiques "universels". Cela donne un peu de marge !

[403] Voir How a quantum computer could break 2048-bit RSA encryption in 8 hours et How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits de Craig Gidney et Martin Ekerå, 2019 (25 pages). Par contre, le titre de l'article Un ordinateur quantique casse le chiffrement RSA sur 2048 bits en 8 heures d'Arthur Vera (2019) est totalement faux. L'ordinateur en question n'existe pas encore !

TechCrunch

The quantum computing apocalypse is imminent

Shlomi Dolev 1 year ago (janvier 2018)

Connectivity

Quantum Computing Paranoia Creates a New Industry

Even though quantum computers don't exist yet, security companies are preparing to protect against them.

by Tom Simonite January 30, 2017

MIT Technology Review

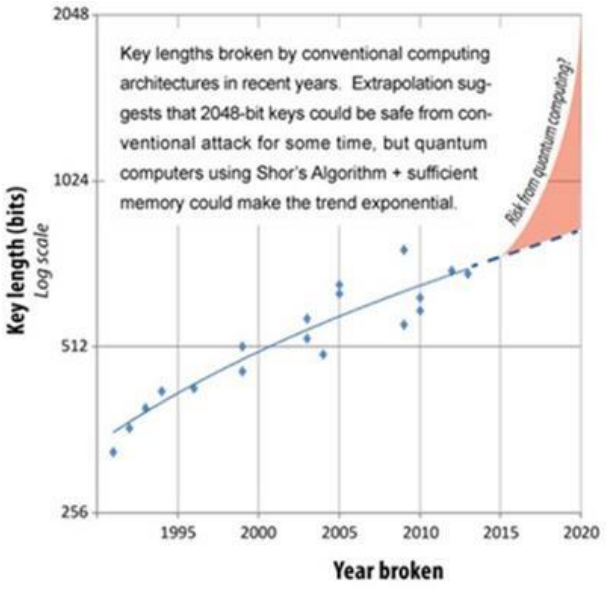
Fear sells in the computer security business. And in late 2015 Massachusetts-based Security Innovation got an unexpected boost from one of the scariest organizations around—the National Security Agency.

For six years the company had been trying to create a new revenue stream by licensing an unusual encryption technology called NTRU, which it acquired from four Brown University mathematicians. It was

Une clé RSA de 762 bits proche du record de 2010 demanderait un ordinateur à recuit quantique du Canadien **D-Wave** avec 5,5 milliards de qubits, loin des 2048 existants[404]. Ils évaluaient qu'un D-Wave de 5893 qubits pourrait faire l'affaire si tous les qubits étaient couplables de manière arbitraire, ce qui n'est pas possible du fait de la conception en matrice 2D des chipsets de D-Wave.

La menace de Shor est visualisée dans le temps dans ce schéma originaire de l'organisme de standardisation européen ETSI dont le siège est à Sophia-Antipolis, dans Quantum Safe Cryptography and Security, 2015 (64 pages).

Elle s'appuie sur des prévisions très optimistes concernant les capacités des ordinateurs quantiques à exploiter l'algorithme de Shor. Il faudrait décaler vers le futur d'au moins 5 à 10 ans la partie orange du graphe.

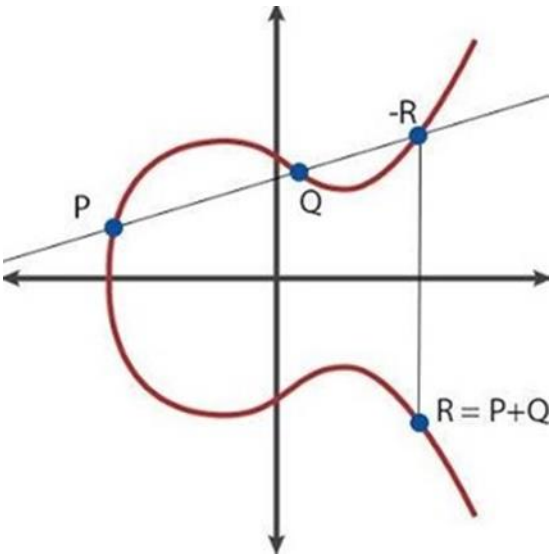


La raison pour laquelle l'impact potentiel du quantique sur la cryptographie RSA est son large usage sur Internet. Il couvre les protocoles **TLS** et **SSL** qui protègent les sites web et les transferts de fichiers via **FTP**, le protocole **IPSEC** qui protège IP V4 dans le sous-protocole IKE, le protocole **SSH** d'accès à distance à une machine et **PGP** qui est parfois utilisé pour chiffrer les emails. La menace est encore plus large, au-delà de RSA.

[404] Selon High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311, de Nike Dattani, Xinhua Peng et Jiangfeng Du, juin 2017 (6 pages).

Elle couvrirait aussi la **signature électronique** de logiciels et donc leurs mises à jour automatiques, les **VPN** pour l'accès à distance aux réseaux d'entreprises protégés, la sécurisation des emails avec **S/MIME**, les systèmes de **paiement**, **DSA** (Digital Signature Algorithm, un protocole de signature électronique), **Diffie-Hellman** (pour l'envoi de clés symétriques) et la cryptographie à courbes elliptiques **ECDH, ECDSA** et **3-DES**. Le protocole **Signal** utilisé dans Whatsapp serait aussi en ligne de mire. Une bonne part de la sécurité d'Internet est donc plus ou moins en ligne de mire.

ECC (Elliptic Curve Cryptography) est le premier algorithme à courbes elliptiques, créé en 1985 par Neal Koblitz et Victor Miller. Les variantes les plus courantes d'aujourd'hui sont **ECDH** (Elliptic-curve Diffie–Hellman) et **ECDSA** (Elliptic Curve Digital Signature Algorithm, lancé en 2005). Ces variantes ont été déployées à partir de 2005 et plus largement seulement à partir de 2015, donc 30 ans après la création du premier ECC ! Au passage, les courbes elliptiques ont permis à Andrew Wiles de démontrer le dernier théorème de Fermat en 1992, qui n'a pas de rapport avec la cryptographie.



Je vous en passe les détails car je n'ai pas compris grand chose aux explications que j'ai pu trouver[405]. Mais peu importe. L'un des intérêts des codes à base de courbes elliptiques est d'utiliser des clés publiques plus courtes qu'avec le chiffrement RSA. Mais voilà, ces courbes elliptiques sont aussi cassables en quantique avec un temps raisonnable à cause de notre ami Peter Shor[406] et de la résolution du problème du logarithme discret (DLP : discrete logarithm problem)[407].

Qui plus est, une porte dérobée de l'ECDSA a été révélée par Edward Snowden en 2013, logée par la NSA dans son générateur de nombre aléatoire Dual EC DRBG. L'abandon de son usage était ensuite recommandé par le NIST en 2014 et la NSA en 2015 pour la transmission d'informations sensibles[408].

La seconde raison est que des communications sensibles d'aujourd'hui peuvent être stockées par des pirates privés ou d'Etats, conservées et exploitées bien plus tard, le jour où les ordinateurs quantiques seront à la hauteur. Nombre d'informations d'aujourd'hui auront de la valeur plus tard, qu'ils s'agisse de transactions financières, de communications privées diverses, de secrets industriels ou autres secrets d'Etats.

---

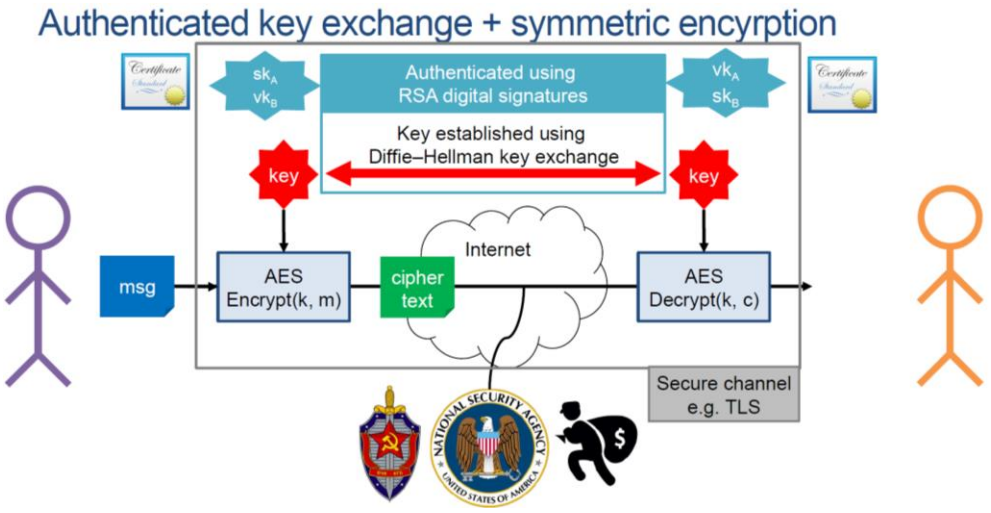
[405] Comme dans Elliptic curves cryptography and factorization (86 slides).

[406] Comme documenté dans Shor's discrete logarithm quantum algorithm for elliptic curves, de John Proos and Christof Zalka, 2003 (34 pages).

[407] Le problème du log discret consiste à trouver un entier k vérifiant a^k = b modulo p, a, b et p étant des entiers connus. Cela permet de casser les clés de courves élliptiques et Diffie-Hellman.

[408] Voir à ce sujet Elliptic Curve Cryptography and Government Backdoors de Ben Schwennesen, 2016 (20 pages).

Le calcul quantique est une véritable épée de Damoclès dont la chute est difficile à prévoir et plutôt éloignée dans le temps d'au moins une bonne décennie. Au-delà d'un tel délai, il est quasiment impossible de faire des prévisions.



source : Introduction to post-quantum cryptography and learning with errors, Douglas Stebila, 2018 (106 slides).

Les systèmes de cryptographie symétriques ne sont pas concernés par l'algorithme de Shor. Il s'agit notamment du **Data Encryption Standard** (DES) qui utilise des clés de 64 bits ou plus et qui est dépassé, remplacé par l'**Advanced Encryption Standard** (AES) qui est un standard du gouvernement US depuis 2002, avec des clés privées allant de 128 à 256 bits.

Les clés sont partagées en amont des échanges et généralement elles-mêmes chiffrées avec l'algorithme **Diffie-Hellman**. Les clés Diffie-Hellman sont cassables en quantique avec l'algorithme de Shor ! Le problème est la vulnérabilité de la majorité des systèmes de chiffrement à clés asymétriques et auxquels on fait appel pour partager des clefs symétriques.

A ce jour, les meilleurs algorithmes de cassage quantique des clés symétriques **AES** mettraient plus que l'ancienneté de l'Univers (13,8 milliards d'années) pour s'exécuter sur des clés de 128 bits. Avec l'AES-256 bits, on est donc des plus tranquille ! Ils reposent sur des mécanismes bien différents de la résolution de problèmes mathématiques des chiffrements à clés publiques.

Une fonction de hash convertit une donnée de taille arbitraire comme un fichier en un nombre de taille fixe. Cela permet de faire des recherches rapides pour comparer des fichiers. Elle peut par exemple servir à vérifier qu'un fichier n'a pas été altéré pendant sa transmission.

L'algorithme de hashage **SHA-1** résiste bien à l'algorithme de Shor, mais il a été cassé par d'autres méthodes et est donc jugé dépassé. C'est le **SHA-3** qui est le plus à jour et depuis 2015. L'algorithme SHA peut être cassé par l'algorithme de recherche de Grover, mais avec une grande quantité de qubits, au minimum 6000 qubits logiques pour les clés courantes[409].

Cela représente un ordre de grandeur voisin des besoins en qubits pour casser les clés RSA. Les algorithmes SHA (Secure Hash Algorithms) sont des standards de fonctions de hachage qui consistent à remplacer une donnée de taille arbitraire par une clé de taille unique.

Une clé de hachage ou empreinte permet par exemple de vérifier l'intégrité d'un contenu comme un logiciel ou plus simplement, un mot de passe. Le problème étant de résister aux collisions, à savoir, aux méthodes permettant de trouver ou créer un objet dont l'empreinte serait celle dont on dispose, ce qui est bien différent que de retrouver l'objet (comme une image) d'origine à partir de son empreinte, qui est plutôt difficile.

		SHA-256	SHA3-256
Grover	T-count	1.27×10^{44}	2.71×10^{44}
	T-depth	3.76×10^{43}	2.31×10^{41}
	Logical qubits	2402	3200
	Surface code distance	43	44
	Physical qubits	1.39×10^{7}	1.94×10^{7}
Distilleries	Logical qubits per distillery	3600	3600
	Number of distilleries	1	294
	Surface code distances	$\{33, 13, 7\}$	$\{33, 13, 7\}$
	Physical qubits	5.54×10^{5}	1.63×10^{8}
Total	Logical qubits	$2^{12.6}$	2^{20}
	Surface code cycles	$2^{153.8}$	$2^{146.5}$
	Total cost	$2^{166.4}$	$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

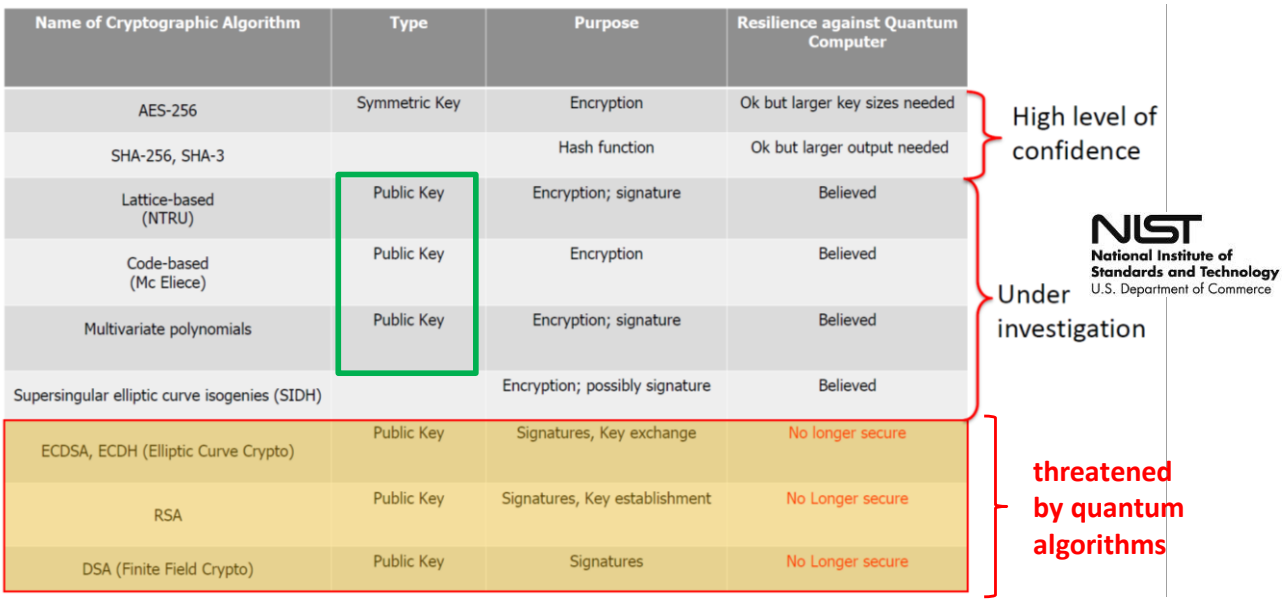
Le nombre de qubits nécessaires au cassage des clés dépend de la taille de la clé. SHA-1 et SHA-2 ont des tailles de clés faibles qui peuvent être récupérées en un temps considéré raisonnable avec l'algorithme quantique de recherche de **Grover** mais ce n'est pas le cas de SHA-3 qui exploite des clés plus grandes. C'est la même logique que pour AES.

Le schéma *ci-dessous* pointe du doigt les principaux algorithmes de chiffrement vulnérables ou pas aux algorithmes quantique connus[410].

[409] D'après Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3, 2016 (21 pages), qui est aussi la source du tableau de cette page.

[410] Vu dans IDQ : Quantum-Safe Security elevance for Central Banks, 2018 (27 slides) et légèrement complété par quelques légendes.

En gros, les systèmes de chiffrement courants à clés publics sont vulnérables. Seuls les systèmes de cryptographie post-quantiques sont résilients. Mais ils ne sont pas encore en production.



Qu'en est-il du **Bitcoin**, des crypto-monnaies et de la **BlockChain** ? J'ai trouvé une réponse que je vous résume *ci-dessous*[411]. Ils font pour commencer un bon inventaire des systèmes de cryptographie utilisés par usage.

Table 3. Main Algorithms Types Used for Cryptography, and Uses For Smart Ledgers[19]

Type of Algorithm	General Use	Example Algorithms of This Type	Example Uses for Smart Ledgers
Symmetric	Secret communications	AES, DES, 3DES, RC4	Protection of resources stored on ledger
Public key	Secret communications (including key exchange) or digital signature	RSA, Diffie-Hellman, El Gamal, ECDSA	User authentication; signature of transactions, data or software
Hash	Generating fixed-length digest of arbitrary-length text	SHA-256, SHA-512, SHA-3	Ensuring authenticity of blockchain

[411] La réponse est fort bien documentée dans The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption, de Long Finance, 2018 (60 pages).

En gros, la Blockchain s'appuie sur un patchwork d'algorithmes de cryptographie comprenant l'AES, RSA et SHA-3. Elle exploite un algorithme de hash pour s'assurer de l'intégrité de la chaine de confiance, et une signature numérique pour authentifier les nouvelles transactions qui s'ajoutent à la Blockchain de manière incrémentale. Dans le cas du Bitcoin, celui-ci utilise la crypto hash SHA-256 qui est résistante au quantique et une signature qui exploite des courbes elliptiques ECDSA qui elle ne l'est pas. **Ethereum** utilise un hash SHA-3 qui résiste au quantique et une signature ECDSA qui est vulnérable.

In fine, le calcul quantique ne permettra pas d'altérer la Blockchain ni la preuve de travail utilisée par le Bitcoin qui s'appuie sur l'usage répété de hash résistant au quantique. La vulnérabilité de la Blockchain se situe dans la signature qui s'appuie sur l'algorithme à courbes elliptiques ECDSA qui peut être cassée avec l'algorithme de Shor. Cela permettrait de se faire passer pour quelqu'un d'autre dans une transaction impliquant une Blockchain ou des Bitcoins.

Si une transaction Bitcoin était interceptée pour récupérer la signature ECDSA de l'émetteur, celle-ci pourrait être exploitée pour transférer des Bitcoins à partir du porte-monnaie de cet émetteur.

Des solutions de contournement pourront évidemment être créées d'ici la confirmation d'une menace quantique sur l'intégrité des transactions. Cela peut passer par le chiffrement en PQC des signatures utilisées par les blockchains[412].

On peut aussi d'emblée chiffrer les données circulant dans une Blockchain avec un algorithme résistant au calcul quantique comme AES-256, avec l'inconvénient qu'il est symétrique et nécessite donc que des clés soient échangées au préalable.

Il existe cependant déjà des parades. Un protocole utilisant un temps de validation plus long des transactions en Bitcoin permettrait de contourner l'usage de la factorisation d'entiers pour casser l'algorithme de signature électronique du Bitcoin, ECDSA[413]. Mais cela ne ferait qu'amplifier un défaut clé du Bitcoin en tant que monnaie : un rallongement des temps de transaction qui est déjà loin d'être temps réel ! On peut aussi citer le projet open source de Blockchain résistante aux sournoises attaques du quantique : Quantum Resistant Ledger. Il s'appuie sur le protocole de signature électronique XMSS (Extended Merkle Signature Scheme)[414].

Le document de **Long Finance** d'où est extrait le tableau suivant résume tous ces risques sur les Smart Ledgers en séparant les transactions qui sont relativement protégées et celles qui s'appuient sur des signatures électroniques vulnérables qui ne le sont pas.

---

[412] Voir Blockchained Post-Quantum Signatures, Chalkias Browny Hearnz, 2018 (8 pages).

[413] C'est documenté dans Committing to Quantum Resistance A Slow Defence for Bitcoin against a Fast Quantum Computing Attack, 2018 (18 pages).

[414] Voir aussi Blockchained Post-Quantum Signatures, Chalkias Browny Hearnz, 2018 (8 pages).

Il rappelle aussi que les échanges Internet sur lesquels s'appuient la Blockchain sont aussi vulnérables au hacking des protocoles SSL et TLS qui les protègent[415].

The Quantum Countdown
Quantum Computing And The Future Of Smart Ledger Encryption

Table 4. Risks to Blockchain Architectures from Quantum Computing

	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
Alter historical records	No	No	May be able to run software without authorisation if signature used
Spoof ongoing records	Yes, possibly	Yes, possibly	Yes, possibly

Cette partie sur les menaces ne serait pas complète sans évoquer les désaccords qui règnent dans l'industrie et la recherche. Certains spécialistes de la cryptographie sont plutôt conservateurs et considèrent qu'il ne faut pas trop toucher à ce qui fonctionne bien.

Ils pensent que l'on en fait trop avec la menace de Shor. D'autres, comme le NIST aux USA, sont plus alarmistes et sont d'avis qu'il ne faut pas tarder à mettre à jour les systèmes de cryptographie les plus critiques.

Génération de clés aléatoires quantiques

Nous allons maintenant passer à la description des trois briques de la cryptographie quantique avec pour commencer, la génération de clés aléatoires.

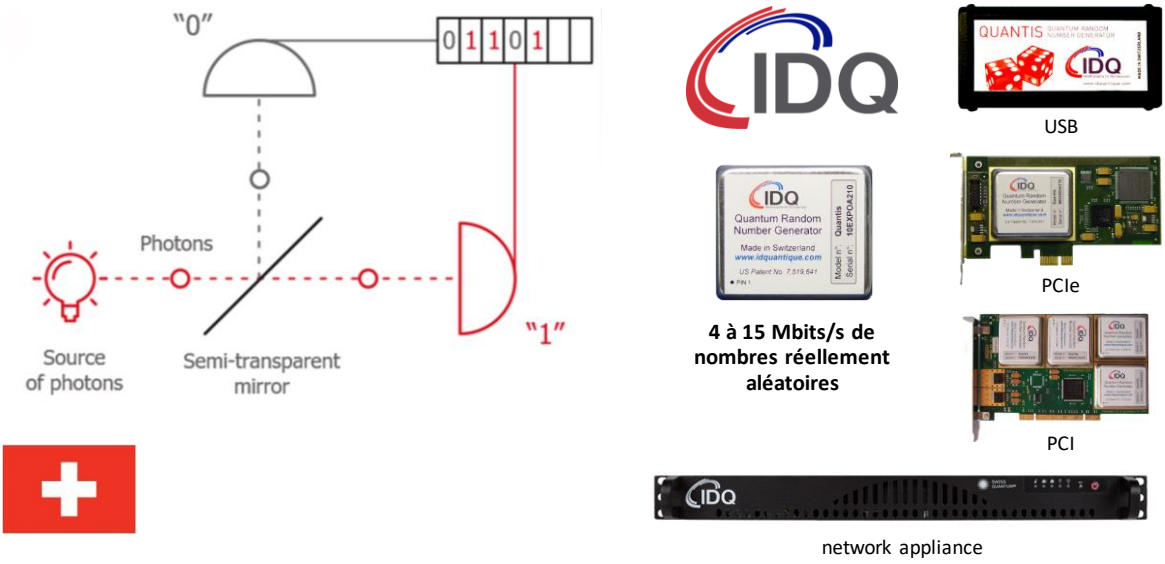
Les systèmes de cryptographie quantique et traditionnels sont tous alimentés par des générateurs de nombres aléatoires. Il en existe depuis des lustres. N'importe quel microprocesseur peut générer des nombres plus ou moins aléatoires. Le souci des cryptographes est de disposer de nombres véritablement aléatoires. A savoir des suites de 0 et de 1 sans répétitions avec une proportion de 0 et de 1 équilibrée. Comme le sont les décimales du nombre pi ! Il faut de plus que la génération soit non déterministe et que l'on ne puisse pas la reproduire.

Une bonne part des générateurs de nombres aléatoires utilisés couramment sont pseudo-aléatoires et déterministes. Ce sont des **PRNG**, pour Pseudorandom Number Generators.

[415] Pour en savoir plus, voir aussi The quantum threat to payment systems de Michele Mosca de l'Université de Waterloo, 2017 (52 minutes). Mosca est une des références mondiales du domaine.

On introduit de l'aléatoire en utilisant comme paramètres de l'algorithme de génération des éléments variables comme l'heure à la milliseconde près, les coordonnées GPS ou d'autres informations de contexte. Malheureusement, malgré ces variables d'initialisation, les algorithmes courants génèrent des périodes dans les nombres générés.

générateur de nombres aléatoires



La solution consiste à utiliser un processus physique réellement aléatoire dans la génération de nombres. L'un des processus connus consiste à mesurer le bruit d'origine thermique d'un composant électronique comme dans un amplificateur.

La méthode la plus aléatoire repose sur la physique quantique et en particulier sur un système conceptuellement assez simple reposant sur la mesure de photons uniques émis individuellement en série sur deux détecteurs après avoir traversé un miroir semi-transparent[416].

Elle permet de créer des nombres véritablement aléatoires de toute taille et assez rapidement, à raison d'un débit pouvant atteindre 1,5 Mbits aléatoires par seconde, voir même plusieurs dizaines de Gbits/s. Ils varient selon les processus utilisés. La technique est notamment maitrisée par la startup suisse IDQ ou ID Quantique, créée par le chercheur Nicolas Gisin, ainsi que par MagiQ, cryptomathic, Crypta Labs et PicoQuant.

[416] Voir Quantum Random Number Generators de Miguel Herrero-Collantes, 2016 (54 pages).

Cryptographie quantique

Le principe de base de la cryptographie quantique est celui de la QKD ou "quantum key distribution". Il consiste à permettre l'échange de clés de chiffrement, en général symétriques, par voie optique (fibre optique, liaison aérienne ou satellite) en s'appuyant sur un système de protection de sa transmission contre les intrusions. Sa première mouture fut le protocole BB84 inventé par l'Américain **Charles Bennett** et le Canadien **Gilles Brassard** en 1984 [417]. Ils sont les créateurs en 1982 de l'appellation de "cryptographie quantique".

Nous l'avions déjà évoqué dans une partie précédente : en 1992, un certain **Artur Ekert** né en 1961, Polonais et Anglais, rencontre le physicien français Alain Aspect en 1992 pour lui soumettre l'idée d'utiliser l'intrication quantique de photons qu'il a vérifié dans son expérience en 1982 pour l'envoi de clés quantiques inviolables.

Alain Aspect trouve l'idée intéressante. Artur Ekert venait de publier en 1991 l'article Quantum Cryptography Based on Bell's Theorem (3 pages). Il est à l'origine du protocole E91 utilisant l'intrication quantique.

L'idée a depuis fait son chemin. Elle est même à l'origine de la création du champ entier de la cryptographie quantique qui est même sorti du domaine de l'expérimentation pour entrer dans la sphère industrielle ! Artur Ekert fait partie depuis 2016 du conseil scientifique d'Atos en compagnie d'Alain Aspect, Daniel Estève, Serge Haroche, Cédric Villani et David DiVicenzo.

Artur Ekert a donc perfectionné BB84 en utilisant l'intrication quantique, évitant la transmission explicite d'information (de phase de photon) pouvant être interceptée par un intrus.

La QKD a ensuite évolué, notamment avec le protocole **BBM92** qui ajoute l'intrication au protocole BB84 et de manière plus sécurisée que le E91 d'Artur Ekert.

Il y a aussi le protocole CV-QKD pour "continuous variable"-QKD, qui module à la fois la phase et l'amplitude du signal optique transmis et permet notamment le multiplexage de plusieurs communications sur une même fibre optique. Philippe Grangier en est l'un des concepteurs.

Les protocoles de QKD ont la particularité de permettre la détection de toute intrusion dans la chaine de transmission et d'indiquer que quelqu'un a tenté d'en lire le contenu ou si des perturbations sont intervenues "sur la ligne". Dans le protocole BB84, cela repose sur l'envoi de l'information sur des photons avec quatre types de polarisations rectilignes : 0°, 45°, 90° et 135°. Histoire de faire simple car c'est en fait plus compliqué, leur lecture par un intrus va modifier la clé, en projetant leur polarisation à 0° ou 90°. Toute intrusion en lecture sera détectée à l'arrivée. Si le protocole détecte un intrus, il peut en tenir compte et bloquer la communication de l'information sensible parce que la clé d'encodage a été captée.

---

[417] Dans Quantum cryptography : public key distribution and coin tossing, 1984 (5 pages).

L'encodage d'une QKD est dit superdense (*superdense coding*) car on l'utilise pour envoyer deux bits sur un qubit transmis par voie optique entre deux points lorsqu'ils sont déjà reliés par un état intriqué de photons. C'est un protocole de communication imaginé par Charles Bennett et Stephen Weisner en 1992 et expérimenté en 1996 par Klaus Mattle, Harald Weinfurter, Paul Kwiat et Anton Zeilinger avec des paires de photons. L'intrication initiale précédant l'envoi des deux bits dans le qubits permet d'éviter de violer le théorème d'Holevo, déjà cité plusieurs fois, selon lequel un jeu de qubits ne peut pas transporter plus d'information que le nombre équivalent de bits classiques.

De son côté, l'information chiffrée avec la clé transmise est envoyée sur un canal traditionnel. Et en clair, même si elle est elle-même chiffrée généralement par des protocoles comme SSL qui protège les relations entre votre navigateur et les sites web que vous visitez et qui supportent le protocole sécurisé https[418].

En pratique, la transmission de clé par QKD s'accompagne d'un système complexe de "distillation de clé" qui gère les imperfections de la communication avec des codes de correction d'erreurs, une amplification de la confidentialité et un système d'authentification par clés privées déjà partagées par les correspondants, permettant d'éviter les attaques "man in the middle" de pirates qui se feraient passer pour l'un des interlocuteurs. Les codes de correction d'erreurs et le reste du protocole génèrent des pertes en ligne d'environ 80% de la communication des clés quantiques[419].

La mise en œuvre d'une QKD est encore complexe. On combine en général un générateur de clés aléatoires quantiques comme ceux de la startup Suisse IDQ, puis un système de génération de clé QKD logique, puis un encodage optique de cette clé qui va circuler généralement sur fibre optique noire d'un opérateur télécom B2B.

Séparément, le signal encrypté avec la clé (qui a été préalablement envoyée par le récipiendaire de l'information s'il s'agit d'une clé publique) est envoyé sur un canal traditionnel, pouvant passer aussi par fibre optique ou un autre support de communication physique. C'est bien documenté par l'ETSI[420].

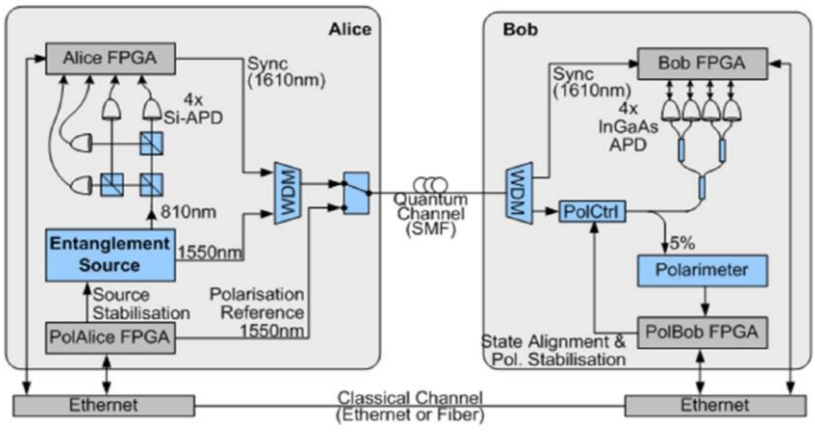


Figure 4.6: Schematic of an entanglement-based QKD system

[418] C'est d'ailleurs une modification que j'ai mise en place dans le blog Opinions Libres fin juillet 2018. Cela ne change pas grand chose dans la mesure où les lecteurs que vous êtes ne se connectent pas de manière sécurisée sur le site. Cela sécurise un peu mieux la connexion administrateur.

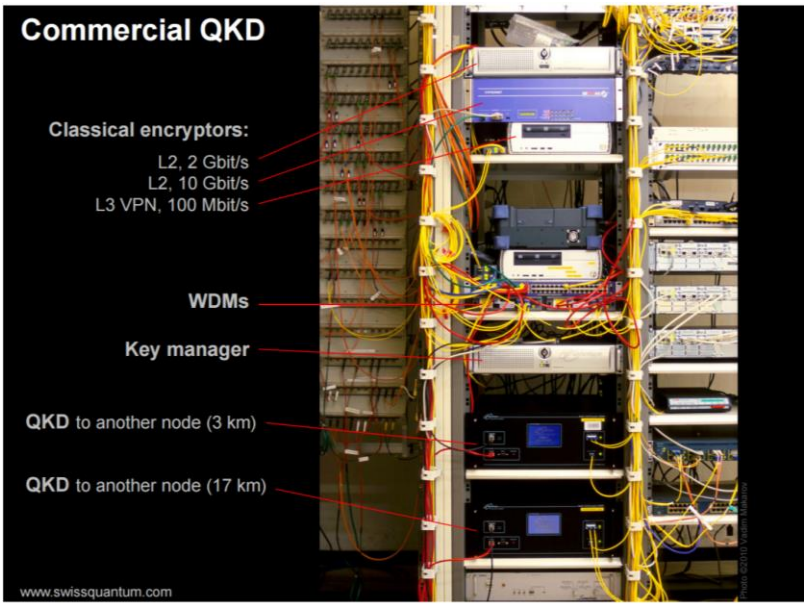
[419] Selon l'excellent panorama de Sheila Cobourne de l'Université de Londres Quantum Key Distribution Protocols and Applications, 2011 (95 pages).

[420] Dans Quantum Key Distribution (QKD) Components and Internal Interfaces de l'ETSI, 2018 (47 pages) qui décrit les différentes techniques de QKD disponibles à ce jour et d'où le schéma de la page est issu.

A l'arrivée, il faut le lecteur de clé quantique puis le système de déchiffrage du signal arrivé par voie normale. Cela donne pour l'instant des systèmes avec deux racks d'équipements comme en témoigne cette illustration *ci-dessous*[421].

Le canal protégé transportant la clé QKD peut cohabiter sur une même fibre optique avec le signal utile qui est transmis normalement et pour servir plusieurs utilisateurs simultanément[422].

Une QKD peut être utilisée pour gérer de clés symétriques comme AES ainsi que des clés résistantes au quantique (PQC), que nous verrons plus loin.



Le débit des clés secrètes est une question importante et se chiffre actuellement au grand maximum en Mbits/s vs les Tbits/s des liaisons optiques des opérateurs. La portée sans répéteurs s'améliore régulièrement. Le débit de transfert de clés quantiques peut être inférieur à celui des données transmises.

Il existe de nombreuses variétés de protocoles de QKD comme le DV-QKD (la première version datant de 1984, basée sur un seul photon et qui a besoin de refroidissement des infrastructures donc couteux), le HD-QKD (plusieurs bits d'encodage de clés par photon), CV-QKD (qui s'appuie sur un faisceau de lumière cohérente issue d'un laser, mais génère plus de bruit) et MDI-QKD[423].

La portée de la transmission a été régulièrement améliorée dans le temps avec seulement 30 cm en 1989 (IBM avec Charles Bennett), 1100 m à l'Université de Genève en 1993, puis 23 km en 1995 avec le protocole BB84, le tout via une fibre optique. Les démonstrations de QKD à l'air libre démarraient en 1996 (sur 75m) puis 144 km (en 2007)[424].

Les expériences symboliques de mise en œuvre de QKD se sont succédées ces dernières années. Les premières datent de 2005, menées par la **DARPA** à Boston. Une expérimentation a eu lieu à **Vienne** en 2008 dans le cadre du projet européen **SECOQC** (*SE*cure *CO*mmunication based on *Q*uantum *C*ryptography) lancé en 2004 et

---

[421] Elle est issue de A tale of quantum computers de Alexandru Gheorghiu (131 slides).

[422] C'est décrit dans Quantum Encrypted Signals on Multiuser Optical Fiber Networks Simulation Analysis of Next Generation Services and Technologies de l'Anglais Rameez Asif, 2017 (6 pages).

[423] Voir ce bon panorama sur la QKD et de ses enjeux techniques dans Practical challenges in quantum cryptography, d'Eleni Diamanti & Al, 2016 (25 pages).

[424] Source : Second Generation QKD System over Commercial Fibers, 2016 (5 pages).

associant une quarantaine de laboratoires de recherche et d'entreprises privées, en exploitant une architecture "mesh"[425].

Un test de liaison sur 144 km a été mené par des Autrichiens en 2010 pour relier les iles de La Palma et Tenerife aux **Canaries**, en utilisant le protocole **BBM92**[426]. Cela a continué en Suisse avec **IDQ** pour relier entre elles des banques locales. Ils ont aussi mis en place en 2007 un système de décompte de votes d'élections s'appuyant sur une QKD. Si les machines à voter sont elles-mêmes sécurisées, cela peut avoir un intérêt. Sinon, bien non ! La sécurité doit être de bout en bout !

SECOQC, Vienna (2008)

5 nodes, 20/25 km of QKD secured fiber link

5-11 kbits/s


NewScientist

News Technology Space Physics Health Environment Mind Video | Travel Events Jobs

Quantum cryptography to protect Swiss election

TECHNOLOGY 15 October 2007

By Paul Marks

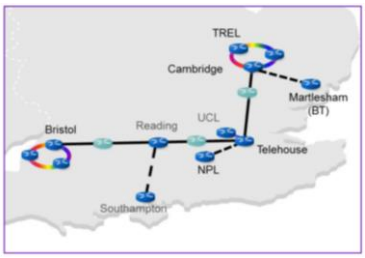
Quantum cryptography is to be used to protect a Swiss election against hacking or accidental data corruption. But some electoral technology experts warn that this novel approach does not address the most vulnerable aspects of an election.

When federal elections take place in the State of Geneva on 21 October 2007, the transmission of results from a data entry centre – where paper votes are keyed into computers – to the state government's central data repository in Geneva will be secured using a quantum connection.

The aim, says Geneva state chancellor Robert Hensler, is to "verify that data has not been corrupted in transit between entry and storage".

Quantum cryptography harnesses quantum mechanics to generate an encryption key – a secret sequences of 0s and 1s – in such a way that a hacker cannot intercept it without being detected. This key can then be used to scramble a message and decode it at the receiving end.

Cambridge QC Hub (2018)



Les USA s'y sont également mis pour déployer un réseau inter-états de communication par QKD, piloté par **Batelle**.

Des tests avaient déjà été réalisés en 2015 au **MIT** pour relier entre eux deux sites distants de 43 km, un type d'expérience aussi réalisée au Royaume Uni[427] et leur UK Quantum Communications hub entre Bristol et Londres/Cambridge.

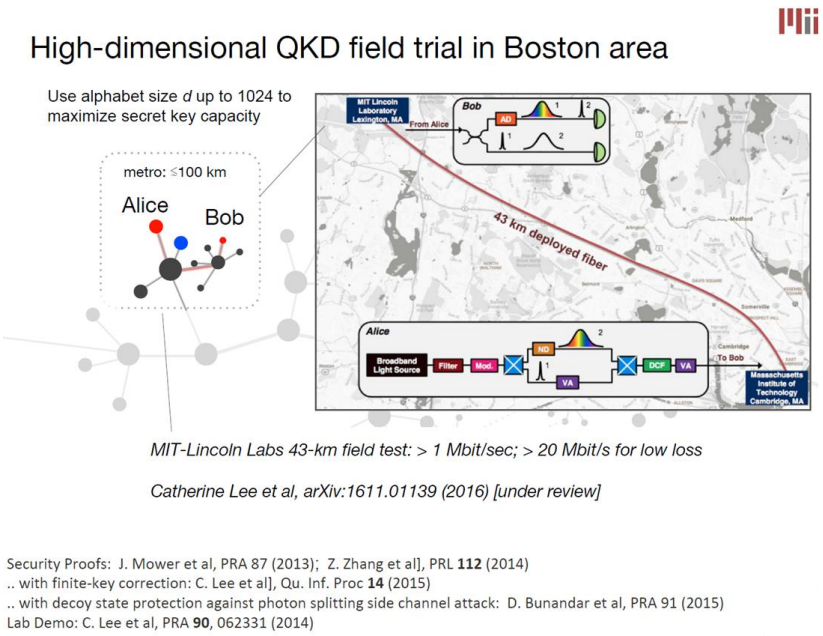
[425] Voir The SECOQC quantum key distribution network in Vienna 2016 (39 pages).

[426] C'est documenté dans Feasibility of 300 km Quantum Key Distribution with Entangled States, 2010 (14 pages).

[427] Vue dans IDQ : Quantum-Safe Security elevance for Central Banks, 2018 (27 slides).

Un déploiement commercial de QKD sur un réseau de fibre optique inutilisé de 800 km reliant Boston à Washington DC est aussi en cours de réalisation par **Quantum Xchange** et **Zayo**, pour connecter des sociétés financières de Wall Street avec leur backoffice dans le New Jersey.

Il utilise des répéteurs sécurisés (« trusted node technology")[428].



En France, **Orange** annonçait en mai 2019 lancer les tests d'une communication protégée par QKD avec l'Université Côte d'Azur (UCA) qui en fournit la solution. Elle relie le campus Valrose et l'Inria de Sophia Antipolis avec un point d'accès sur le campus de la Plaine du Var IMREDD à Nice, le tout s'appuyant sur des fibres noires fournies par l'opérateur télécom[429]. Ce dernier étudie notamment la question des répéteurs dans une telle configuration. Il cherche aussi à associer les solutions de QKD pour protéger les liaisons physiques et de PQC qui pourraient servir de méthode de chiffrement de données transmises en association avec une QKD.

En septembre 2018, **Toshiba** annonçait une solution de QKD codéveloppée avec la Tohoku Medical Megabank Organization (ToMMo) de la l'Université de Tohoku avoir atteint un débit supérieur à 10 Mbits/s pendant un mois d'envoi de clés QKD.

Ce sont les Chinois qui se font le plus remarquer avec des démonstrations et projets destinés à marquer les esprits. Comme nombre de pays, la Chine investit dans les QKD pour des raisons de souveraineté et pour protéger ses communications sensibles. Un premier déploiement avait été réalisé en 2012 dans la zone d'Hefei pour relier diverses entités du gouvernement chinois[430]. Il a eu ensuite la mise en place d'une liaison par fibre optique sécurisée par QKD entre Shanghaï et Beiking, faisant 2000 km.

Le projet lancé en 2016 et déployé par la startup chinoise **QuantumCTek** serait terminé. Sachant que sur 2000 km, il faut installer aux alentours de 25 répéteurs et en sécuriser l'accès physique ! En effet, l'atténuation du signal est trop forte au-delà d'environ 80 km sur une fibre optique.

---

[428] Voir New plans aim to deploy the first US quantum network from Boston to Washington, DC, octobre 2018. Source du schéma: From MIT : Semiconductor Quantum Technologies for Communications and Computing, 2017, 32 slides).

[429] Voir Université Côte d'Azur et Orange collaborent pour la mise en place d'une expérimentation en matière de cryptographie quantique, mai 2019.

[430] Voir Unhackable Chinese Communication Network Launches Soon, de Rechelle Ann Fuertes, 2017.

QKD en Chine

Chinese city to launch 'unhackable' quantum network

Tests on system in Jinan in Shandong province complete and service for nearly 200 users to begin next month, state-run media report

PUBLISHED : Monday, 10 July, 2017, 7:02am
UPDATED : Monday, 10 July, 2017, 10:14am

COMMENTS: 19

Beijing-Shanghaï Network (2017)

32 nodes, 2000 km of QKD secured fiber link

20 kbits/s

La seconde performance chinoise concerne l'usage du satellite **Micius** pour téléporter des états quantiques de photons par voie optique en 2017, à 1400 km de distance entre le satellite et la Terre, à 5100 m d'altitude dans la préfecture de Ngari dans le Tibet chinois[431].

Une communication de clé quantique QKD a ensuite été réalisée en utilisant un procédé différent, en 2018, entre la Chine et l'Autriche pour mener une vidéo-conférence sécurisée par cette clé (*ci-dessous*)[432]. Pourquoi donc avec l'Autriche ? Parce que Jian-Wei Pan, le pape du quantique Chinois à l'origine de cette expérience a fait sa thèse de doctorat en Autriche sous la supervision d'Anton Zeilinger, qui pilotait la partie européenne de l'expérience !

En juin 2019, des chercheurs chinois annonçaient avoir démontré la mise en œuvre de liaisons optiques QKD aériennes établies au sein d'un réseau de drones octocoptères de 35 kg espacés de 200 m pendant un vol de 40 mn à 100 m d'altitude[433]. La charge utile gérant la communication quantique était de 11,8 kg. Elle reste miniaturisable, l'ambition des chinois étant de l'intégrer dans des drones grand-public. On imagine les impacts de cette technologie dans leur société de la surveillance continue des citoyens.

---

[431] Les détails sont dans Ground-to-satellite quantum teleportation, 2017 (16 pages). Le principe a été décrit pour la première fois en 1993 dans Teleporting an Unknown Quantum State via Dual Classical and EPR Channels de Charles Bennett, Gilles Brassard (de Montréal), Claude Crépeau (un français de Normale Sup), Richard Jozsa, Asher Peres et William Wootters. Voir aussi Quantum Communication at 7,600km and Beyond de Chao-Yang Lu et Cheng-Zhi Peng, Jian-Wei Pan, novembre 2018.

[432] Des expériences équivalentes ont été réalisées par des équipes européennes et françaises. Voir Quantum Photonics Technologies for Space, octobre 2018 (22 pages) et Nanobob CubeSat mission 2018 (31 pages).

[433] Voir Drone-based all-weather entanglement distribution, Hua-Ying Liu & Al, mai 2019 (16 pages) et World's First "Quantum Drone" for Impenetrable Air-to-Ground Data Links Takes Off de Charles Q. Choi, IEEE Spectrum.

Qu'en est-il donc des répéteurs, indispensables pour distribuer des clés quantiques sur de grandes distances, au-delà de 80 km [434]?

Des chercheurs chinois ont créé une connexion en fibre en QKD de 404 km sans répéteur[435], mais à cette distance les taux d'erreurs sont tellement élevés que cela ne sert pas à grand chose. Il existe des technologies de répéteurs quantiques pour fibres optiques à l'état de la recherche fondamentale mais avec quelques limitations[436]. On en serait déjà à la troisième génération de ces répéteurs mais ils seraient déjà hackables[437]. Ce n'est donc pas encore au point !

Une technique plus sûre consisterait à utiliser une mémoire quantique dans les répéteurs pour répliquer l'état des photons à transmettre. C'est l'objet de travaux de l'équipe de **Nicolas Gisin** de l'Université de Genève (et ID Quantique) accompagné d'une équipe du CNRS en France. Ils s'appuient sur une terre rare, l'ytterbium[438]. Ce n'est pas encore commercialisé.

Dans la même veine, des chercheurs du **Key Lab of Quantum Information** de l'Académie des Sciences chinoise publiaient en août 2018[439] une étude sur la création de mémoires quantiques à base d'ions de terre rare (de praseodymium) dopés à trois degrés de liberté, pilotable par envoi de photons (schéma de l'expérience *ci-dessous* qui illustre le fait que l'on est encore loin de la miniaturisation).

---

[434] Sachant que le record de distance de telecommunication quantique sans répéreur est de 421 km. Voir Viewpoint: Record Distance for Quantum Cryptography de Marco Lucamarini, Toshiba & Cambridge, novembre 2018 et Recent progress on Measurement-Device-Independent (MDI) Quantum Key Distribution (QKD), Marco Lucamarini, 2018 (71 slides).

[435] Documentée dans Measurement device independent quantum key distribution over 404 km optical fibre, 2016 (15 pages).

[436] Voir Tutorial on quantum repeaters de Rodney Van Meter et Tracy Northup, 2019 (178 slides), Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, 2018 (5 pages) et An Information-Theoretic Framework for Quantum Repeaters de Roberto Ferrara, 2018 (144 pages).

[437] Selon The network impact of hijacking a quantum repeater 2018 (23 pages).

[438] Selon Ytterbium: The quantum memory of tomorrow, juillet 2018.

[439] Voir Multiplexed storage and real-time manipulation based on a multiple-degree-of-freedom quantum memory, 2018 (9 pages).

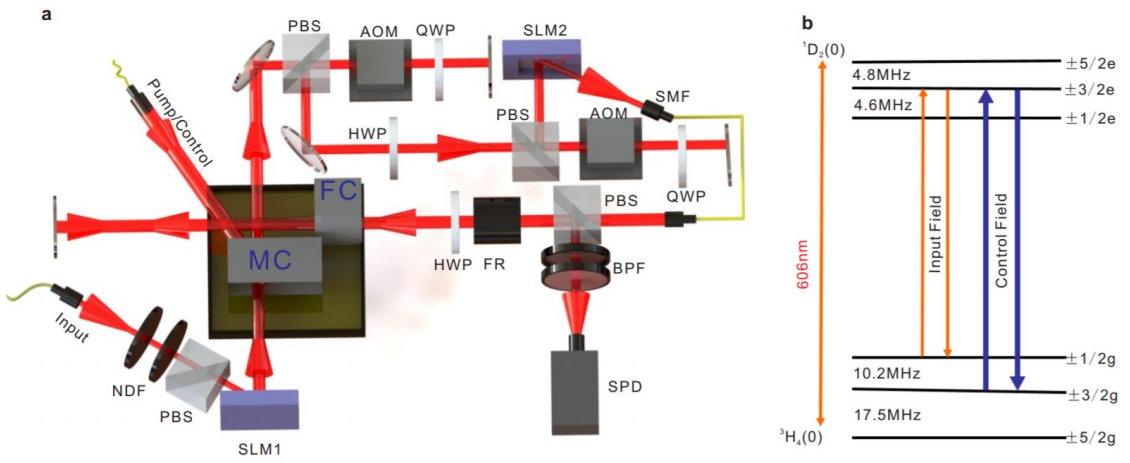


Fig. 1 Experimental setup and atomic levels. **a**, Schematic illustrations of the experiment. The AFC is prepared in a memory crystal (MC) and a narrow spectral filter has been prepared in a filter crystal (FC). The beam waist of the input light is 65 μm at the middle of the MC. The pump/control light has a beam waist of 300 μm inside the MC to ensure good overlap with the high-dimensional input light. The input pulses are attenuated to single-photon level by neutral density filters (NDF). The spatial modes of these photons are converted into OAM superposition states by a spatial light modulator (SLM1). After storage in the MC, the retrieved signal passes through two consecutive acousto-optical modulators (AOM) [35], which act as a temporal gate and a frequency shifter [36]. The AOM are used in double-pass configuration to ensure the photons' spatial mode unchanged when the frequency of photons is swept over tens of MHz. The SLM2 and a single mode fiber (SMF) are employed to analyze the OAM states of the retrieved photons. The FC is double-passed with help of a polarization beam splitter (PBS), a half-wave plate (HWP) and a Faraday rotator (FR). Two band-pass filters (BPF) centered at 606 nm are employed to further suppress noises before the final detection of signal photons using single-photon detector (SPD). QWP: quarter-wave plate. **b**, Hyperfine states of the first sublevels of the ground and the excited states of Pr^{3+} in Y_2SiO_5. The input field is resonant with 1/2g - 3/2e, and the control field is resonant with 3/2g - 3/2e (See Methods section for details).

Cette technique pourrait servir à la fois à la création de répéteurs pour des réseaux de QKD et pour créer des mémoires quantiques pour ordinateurs quantiques à base d'optique linéaire.

En juillet 2019, des chercheurs chinois annonçaient enfin avoir réussi à expérimenter une technologie de répéteurs "photoniques » à base d'interféromètres à 12 photons et permettant de se passer de mémoire quantique. Cela les rend théoriquement très sécurisés[440]. Mi-2019, d'autres chercheurs chinois présentaient une nouvelle prouesse : la téléportation de qutrits, permettant de transmettre quantiquement plus d'information par photons[441]. Cela pourrait notamment servir à augmenter le débit de la transmission de clés en QKD. D'autres débouchés sont aussi envisageables dans des domaines très différents comme celui des radars quantiques qui sont évoqués page 382.

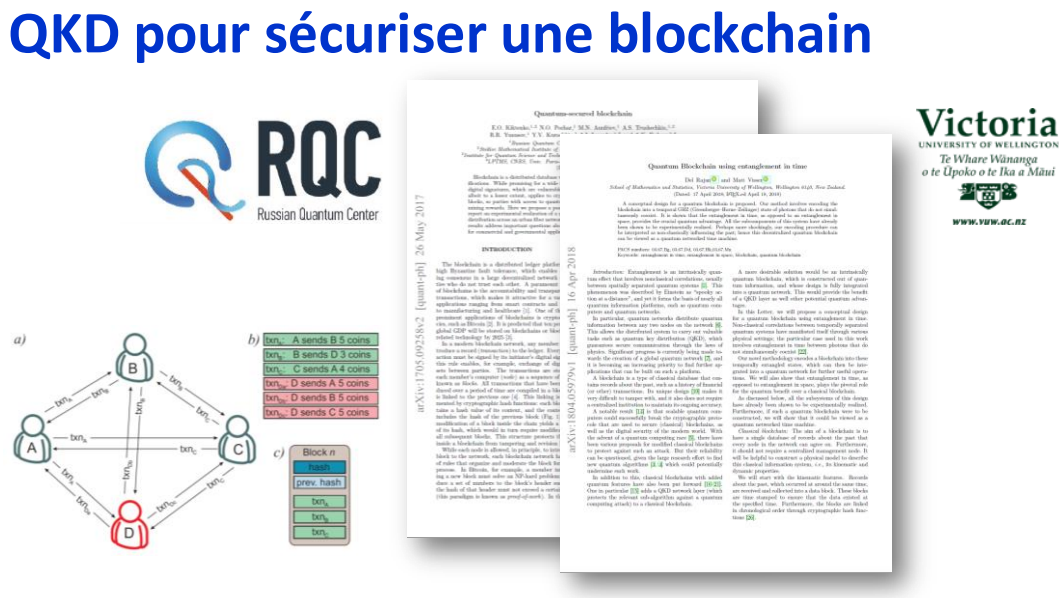
La sécurisation d'une chaîne dépend de ses maillons les plus faibles et ici, ce sont les émetteurs et les récepteurs avant même qu'ils n'échangent via une QKD. Par ailleurs, les QKD ne sont pas la panacée car elles dépendent d'une liaison point à point et pas d'une technique de routage permettant d'emprunter plusieurs chemins.

[440] Voir Scientists Firstly Realize All-photonic Quantum Repeater, juillet 2019 et Experimental quantum repeater without quantum memory de Zheng-Da Li & Al, 2019.

[441] Voir Voir Qutrits experiments are a first in quantum teleportation, par Daniel Garisto dans Scientific American, août 2019, qui fait référence à Experimental multi-level quantum teleportation par Xiao-Min Hu & Al, avril 2019 (12 pages) et Quantum teleportation in high dimensions par Yi-Han Luo, juin 2019 (23 pages).

Cela pourrait aboutir à une forme de déni de service par blocage de la communication physique employée[442].

Autre exemple, ce projet d'utiliser les QKD pour sécuriser une Blockchain. C'est évidemment délicat à déployer de bout en bout à grande échelle. En effet, les utilisateurs de Blockchain n'ont pas une liaison satellite en montagne ou une fibre sécurisée sous la main, ne serait-ce que lorsqu'ils sont mobiles. Mais soit.



C'est la proposition d'Evgeny Kiktenko du "Russian Quantum Center" de Moscou[443], ainsi que de Del Rajan et Matt Visser de l'Université Victoria de Wellington en Nouvelle Zélande[444]. Au juste, pourquoi ne protège-t-on pas l'ensemble des données transmises avec le même principe que la QKD ? Ce qui s'y oppose semble être la limitation en débit du procédé.

La cryptographie est fascinante pour la vitesse à laquelle des dispositifs de sécurité peuvent être cassés par des chercheurs avant même d'avoir été déployés en masse. Ainsi les QKD seraient vulnérables du fait d'une faille du théorème de Bell[445]. C'est une course sans fin !

Dernier point concernant les QKD, elles s'inscrivent dans le cadre plus général des télécommunications quantiques. Cela permet en théorie de mettre en place des moyens de communication ultra-rapides, même si c'est en supportant de nombreuses contraintes. Est-ce que cela aurait des applications pratiques ?

---

[442] Au sujet des vulnérabilités de la QKD et des méthodes pour les éviter, voir QKD Measurement Devices Independant Joshua Slater, 2014 (83 slides).

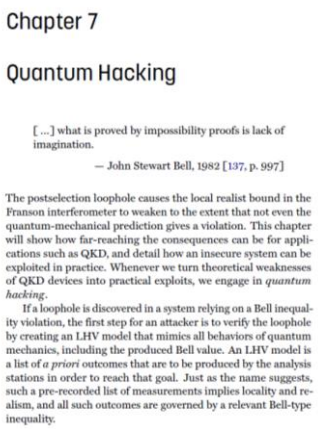
[443] Documenté dans First Quantum-Secured Blockchain Technology Tested in Moscow, juin 2017.

[444] Dans Quantum Blockchain using entanglement in time, 2018 (5 pages).

[445] C'est comme documenté par Jonathan Jogenfors dans Breaking the Unbreakable Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography, 2017 (254 pages).

On peut imaginer de créer des systèmes permettant de distribuer des traitements sur plusieurs processeurs quantiques et de les coordonner[446]. Cela fait aussi partie du champ du blind computing que nous avons déjà évoqué.

manque de bol…



Chapter 7

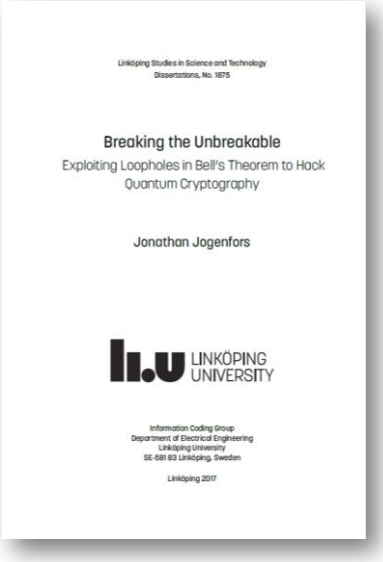
Quantum Hacking

[...] what is proved by impossibility proofs is lack of imagination.

— John Stewart Bell, 1982 [137, p. 997]

The postselection loophole causes the local realist bound in the Franson interferometer to weaken to the extent that not even the quantum-mechanical prediction gives a violation. This chapter will show how far-reaching the consequences can be for applications such as QKD, and detail how an insecure system can be exploited in practice. Whenever we turn theoretical weaknesses of QKD devices into practical exploits, we engage in *quantum hacking*.

If a loophole is discovered in a system relying on a Bell inequality violation, the first step for an attacker is to verify the loophole by creating an LHV model that mimics all behaviors of quantum mechanics, including the produced Bell value. An LHV model is a list of *a priori* outcomes that are to be produced by the analysis stations in order to reach that goal. Just as the name suggests, such a pre-recorded list of measurements implies locality and realism, and all such outcomes are governed by a relevant Bell-type inequality.



Linköping Studies in Science and Technology
Dissertations, No. 1875

Breaking the Unbreakable

Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography

Jonathan Jogenfors

LINKÖPING UNIVERSITY

Information Coding Group
Department of Electrical Engineering
Linköping University
SE-581 83 Linköping, Sweden

Linköping 2017

Cryptographie post-quantique

La protection physique de l'envoi de clés symétriques n'est pas facilement applicable de manière généralisée, ne serait-ce parce qu'elle impose une liaison optique (directe ou par fibre optique) entre émetteurs et récepteurs. Ce qui, par exemple, ne fonctionne pas avec les liaisons radio comme avec les smartphones. Too bad !

L'objectif que se sont donnés les spécialistes est donc de créer et exploiter des systèmes capables de résister aux assauts des ordinateurs quantiques et en particulier à l'algorithme de Shor (factorisation d'entiers mais aussi logarithme discret) comme de Grover (recherche brute) sans protection quantique de la liaison physique. Le décryptage de messages chiffrés - sans les clés privées - doit être un problème NP-Complet ou NP-Difficile pour résister aux assauts futurs du quantique.

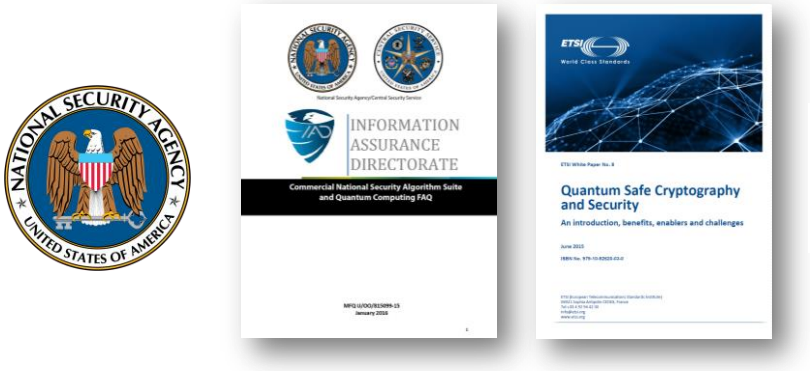
La Post-Quantum Cryptography (PQC) est en quelque sorte concurrente de la Quantum Key Distribution (QKD) même si certains les jugent complémentaires ! Et elle est certainement plus facile à déployer à grande échelle car elle est indépendante des infrastructures physiques utilisées pour les télécommunications. Mais on peut toutefois les combiner en envoyant des clés publiques de PQC via des QKD.

Les différents systèmes de PQC se distinguent par de nombreux paramètres et présentent des compromis différents entre taille de signature, vitesse de traitement pour le chiffrement et le déchiffrement et par la taille de la clé publique.

[446] Voir par exemple Milestone Experiment Proves Quantum Communication Really Is Faster, de Kevin Hartnett, Quanta Magazine, décembre 2018, qui fait référence à Experimental demonstration of quantum advantage for one-way communication complexity, de Niraj Kumar, Iordanis Kerenidis et Eleni Diamanti, décembre 2018 (12 pages) ainsi que One step closer to complex quantum teleportation de l'Université de Vienne, novembre 2018.

La chronologie mérite le détour pour sa dimension “long terme” [447]:

- **1978** : le premier algorithme résistant aux ordinateurs quantiques est créé par l’Américain **Robert McEliece** (détails plus loin) avant même que l’on parle d’ordinateurs quantiques.
- **2003** : Le terme de “post quantum cryptographie” (PQC) est créé par l’Américain Daniel Bernstein. C’est l’auteur avec Johannes Buchmann et Erik Dahmen de l’imposant ouvrage Post-Quantum Cryptography en 2009 (254 pages) qui pose bien les enjeux de la PQC.
- **2006** : le premier workshop international **PQCrypto** se tient en mai en Belgique pour étudier les moyens de contourner les attaques d’ordinateurs quantiques à une époque où l’on peut à peine faire fonctionner deux qubits ensemble. Le programme consiste à trouver des successeurs aux algorithmes de cryptographie à clés publique RSA et ECC qui résistent au quantique[448]. Le comité de programme de 12 personnes comprend trois français : Louis Goubin de Université de Versailles ainsi que Phong Nguyen et Christopher Wolf de l’ENS. Dès cette première édition, quatre des cinq piliers de la PQC sont établis avec la code-based crypto, les lattice codes, hash Lamport signature et multivariate cryptography. Les isogénies arriveront plus tard. Deux français interviennent pour proposer deux de ces quatre pistes : Nicolas Sendrier, de l’Inria, avec "Post-quantum code-based cryptography" et Jacques Stern de l’ENS avec "Post-quantum multivariate-quadratic public key schemes."[449]. Ces workshops ont depuis lieu tous les un à deux ans un peu partout dans le monde. L’édition 2013 avait eu lieu à Limoges.
- **2012** : le NIST (National Institute for Standards & Technologies), qui est une sorte d’équivalent de l’AFNOR française, lançait ses premiers projets et une équipe sur la PQC.
- **2014** : l’Union Européenne lançait un appel à projets dans le cadre d’Horizon 2020 sur la PQC. Au même moment, l’ETSI qui est l’organisme européen de standardisation des télécoms, lançait aussi son groupe de travail sur la PQC.



[447] Sachant que j’en ai extrait un bout dans Quantum cryptanalysis – the catastrophe we know and don’t know de Tanja Lange, une des spécialistes du sujet et chercheuse aux Pays Bas, 2017 (33 slides).

[448] Les actes sont ici : https://postquantum.cr.yp.to/pqcrypto2006record.pdf.

[449] Source : Quantum Computing and Cryptography Today de Travis L. Swaim, University of Maryland University College (22 pages).

- **2015** : le NIST organise son premier workshop sur la PQC. L'ETSI publie un document de référence sur la PQC[450]. La NSA se réveille un peu tardivement et déclare que le passage à la PQC va devenir une priorité[451]. La NSA joue à chaque fois dans deux cours : elle veut se protéger et protéger les communications sensibles de l'Etat US avec de bons systèmes de chiffrement mais en même temps conserver des capacités à décrypter les communications commerciales standards et celles des autres pays. Cela repose sur la force brute de supercalculateurs géants et une forte asymétrie de moyens techniques. Cette asymétrie pourrait très bien disparaître avec les ordinateurs quantiques qui, sommes-toutes, seront peut-être bien plus abordables que les supercalculateurs géants. En 2015, le projet Européen PQCrypto coordonné par Tanja Lange est lancé[452].
- **2016** : le NIST publie un rapport d'étape sur la PQC (15 pages) et une roadmap de standardisation associée. Lancement du programme d'Investissement d'Avenir RISQ (**R**egroupement de l'**I**ndustrie française pour la **S**écurité Post – **Q**uantique) qui comprend outre divers laboratoires (CEA, CNRS, INRIA, UMPC), des entreprises privées comme CryptoExperts, CS, Secure-IC et Thalès. Ils ont fait des soumissions de propositions de standards au NIST en 2017. RISQ est piloté par Secure-IC.
- **2017** : fin des soumissions de propositions de standardisation de PQC au NIST. Fin 2017, 69 candidats étaients acceptés parmi 82 candidats, principalement avec des réseaux euclidiens (lattice codes) et des codes de correction d'erreur (code based PQC). La même année avait lieu le 8eme workshop PQCrypto à Utrecht aux Pays-Bas.
- **2019** : 26 candidats étaient sélectionnés par le NIST en février 2019 pour passer à la seconde étape avec 17 candidats pour des solutions de chiffrement à base de clés publiques et 9 pour des signatures[453].

  Parmi ces projets se trouvent trois projets où est impliqué Worldline, qui faisait partie jusqu'à 2019 du groupe Atos. L'Inria était de son côté impliquée dans 7 projets sur les 26 retenus[454].

Second Round Candidates

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

[450] Voir Quantum Safe Cryptography and Security (64 pages).

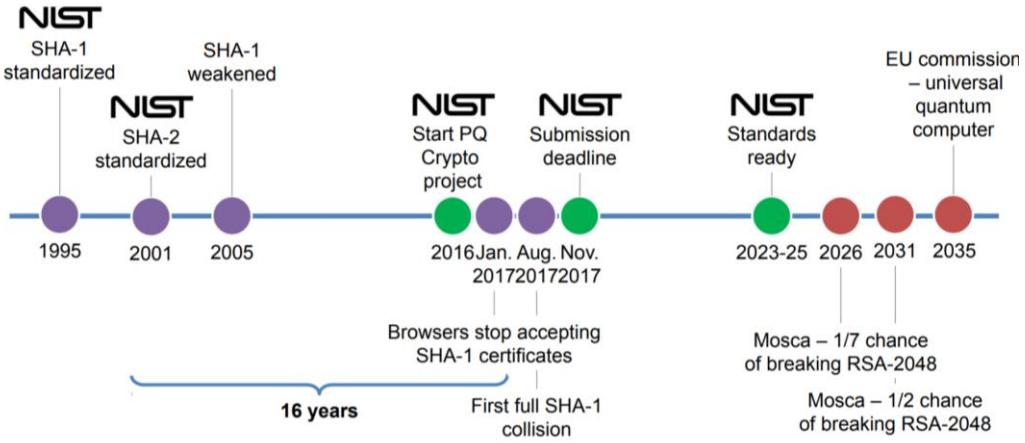
[451] Voir Commercial national security algorithm suite and quantum computing FAQ IAD (11 pages).

[452] Il est documenté dans Post-Quantum Cryptography for Long-Term Security (10 pages).

[453] Voir NIST Post-Quantum Cryptography - A Hardware Evaluation Study, 2019 (16 pages) et Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process 2019 (27 pages) et Voir Recent Developments in Post Quantum Cryptography de Tsuyoshi Takagi, novembre 2018 (38 slides).

[454] Voir Cryptographie post-quantique : forte présence d'Inria dans une compétition internationale, mai 2019. Ils sont gérés par quatre équipes : ARIC, SECRET, POLSYS et GRACE et dans quatre des catégories de systèmes de cryptographie PQC : réseaux euclidiens, isogénies, codes de correction d'erreur et systèmes polynomiaux multivariés.

- **2020/2021** : troisième tour de sélection de candidats du NIST.
- **2022/2024** : draft de standards du NIST.
- **2025** : c'est l'échéance que s'est donné le NIST pour finaliser les standards de la PQC aux USA. Les déploiements de ces standards démarreront avec la commercialisation rapide de solutions logicielles supportant ces standards. Rapide pour la simple raison que les candidats sont souvent issus de consortiums comprenant des acteurs privés de cet écosystème.



source : Introduction to post-quantum cryptography and learning with errors, Douglas Stebila, 2018 (106 slides).

Quels sont au juste donc les standards en lice de la PQC ? Ils sont dans cinq catégories distinctes que voici. Je ne vais pas pouvoir les décrire convenablement dans leur dimension mathématique sauf pour la première catégorie[455].

Table 2 - Comparison on encryption schemes (RSA decryption = 1, size in bits, k security strength)

Algorithm	*KeyGen (time compared to RSA decrypt)*	*Decryption (time compared to RSA decrypt)*	*Encryption (time compared to RSA decrypt)*	*PubKey (key size in bits to achieve 128 bits of security)*	*PrivateKey (key size in bits to achieve 128 bits of security*	*Cipher text (size of resulting cipher text)*	*Time Scaling*	*Key Scaling*
NTRU	*5*	*0.05*	*0.05*	*4939*	*1398*	*4939*	k^2	*k*
McEliece	*2*	*0.5*	*0.01*	*1537536*	*64861*	*2860*	k^2	k^2
Quasi-Cyclic MDPC McEliece	*5*	*0.5*	*0.1*	*9857*	*19714*	*19714*	k^2	*k*
RSA	*50*	*1*	*0.01*	*3072*	*24,576*	*3072*	k^6	k^3
DH	*0.2*	*0.2*	*0.2*	*3072*	*3238*	*3072*	k^4	k^3
ECDH	*0.05*	*0.05*	*0.05*	*256*	*256*	*512*	k^2	*k*

Note: in key scaling, the factor log k is omitted.

source : Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges, ETSI, 2015 (64 pages).

[455] Voir notamment de la vulgarisation du sujet dans A Guide to Post-Quantum Cryptography, par Ben Perez, octobre 2018.

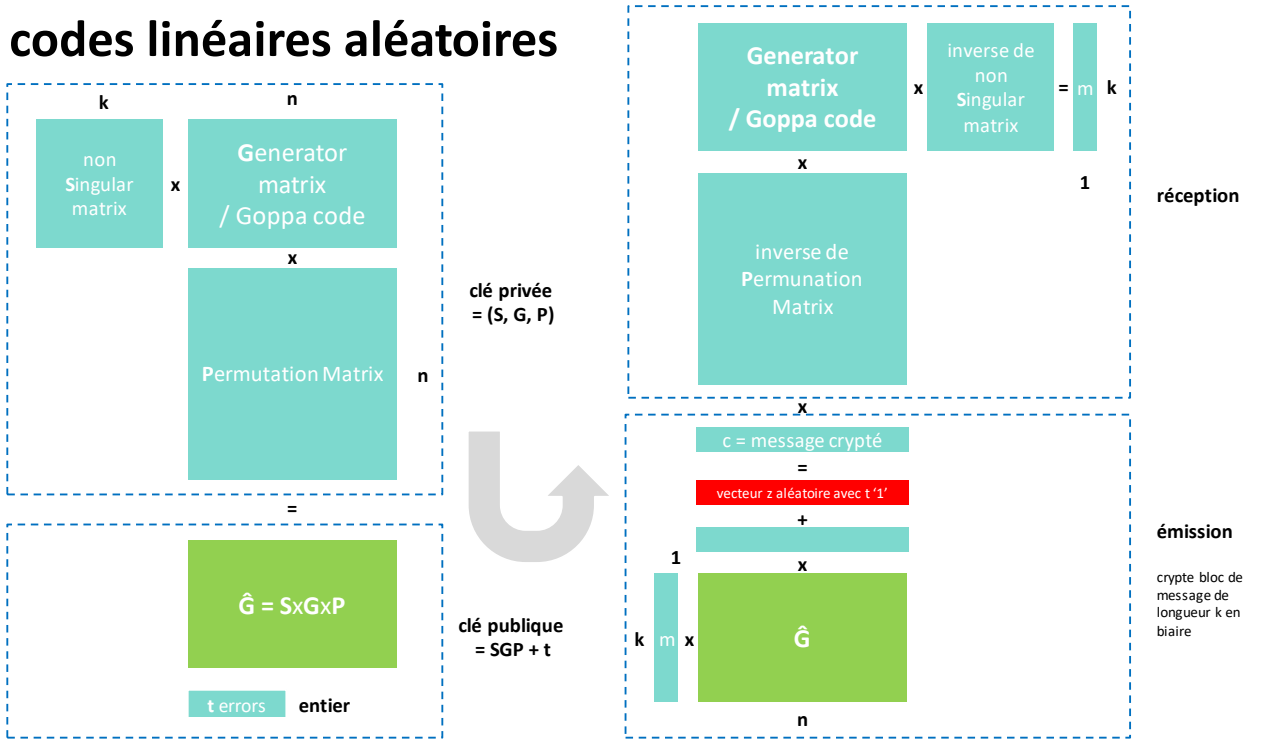
Nous évoquerons le cas de quelques startups qui s'attaquent à ce marché dans la dernière partie de cette rubrique sur la cryptographie. A noter en sus l'annonce par **IBM** en août 2019 d'un système d'archivage d'information sur banque magnétique qui intègre une cryptographie post-quantique[456]. Ils utilisent un chiffrement à base de réseaux euclidiens. Comme il s'agit généralement de stockage long terme, il faut bien conserver le logiciel de déchiffrement sur la même durée pour éviter de se retrouver avec un tas de données non réutilisables !

Code-based cryptography (EN) ou codes linéaires aléatoires (FR)

Ce système de cryptographie inventé en 1978 par **Robert McEliece**, bien avant l'existence de la menace de l'algorithme de Shor, a résisté depuis à toutes les attaques de cryptanalyse, soit classiques soit conçues avec des algorithmes quantiques. C'est le plus ancien des codes PQC qui était même "PQC" avant l'heure.

La méthode consiste à multiplier les données à encrypter représentées sous forme de vecteurs binaires par une matrice publique et statique avec plus de colonnes que de lignes, elle aussi binaire qui est un "*code de Goppa binaire*".

Allons donc. Cette multiplication génère un vecteur plus grand que le vecteur d'origine. On lui ajoute ensuite un vecteur binaire qui ajoute des erreurs aléatoires au résultat mais de nombre constant. Les spécialistes le décrivent comme un "*uniformly random word of weight t*" ce qui n'est pas bien clair pour le néophyte, et qui fournit un exemple de plus du manque de pédagogie de certains. En langage un peu plus naturel, il s'agit d'une série de bits aléatoire contenant un nombre fixe "t" de 1 que l'on appelle le poids de Hamming.



[456] Voir IBM's quantum-resistant magnetic tape storage is not actually snake oil, par Kevin Coldewey dans TechCrunch, août 2019.

La clé publique envoyée par le récepteur à l'émetteur est la matrice et ce nombre d'erreurs t. Ce sont les composantes génératrices de la matrice qui constituent la clé privée. En effet, cette matrice est la multiplication de trois matrices dites SGP pour "non singular", "generator matrix / Goppa code" et "permutation matrix". Le décodage du message utilise des inverses de la matrice S et de la matrice P, et la matrice G. C'est assez alambiqué et j'ai essayé de représenter cela graphiquement dans le schéma *ci-dessus*. La matrice G permet de supprimer les "t" erreurs introduites dans la phase de chiffrement. Elle est conçue pour cela au moment de la création des clés. Par contre, allez comprendre dans la phase d'émission l'effet mathématique de cette matrice de correction d'erreur au message à transmettre avant l'ajout de la dite erreur !

Ce système génère des clés publiques cent fois plus grande qu'avec RSA, de l'ordre de 80 Ko. Et si on veut réduire leur taille, cela génère des vulnérabilités. L'avantage est une bonne vitesse de chiffrement et de déchiffrement des messages. On peut même l'accélérer en utilisant un composant électronique dédié de type FPGA[457].

Casser ce genre de chiffrement est un problème NP-Hard (NP-dur) inaccessible au quantique à ce jour même si, pour résister au quantique, il faudrait une clé assez grande, de 1 Mo[458].

Lattice-based cryptography (EN) ou réseaux euclidiens (FR)

La technique a été proposée par le Hongrois Miklos Ajtai, chercheur chez IBM, en 1996, mise en œuvre dans un système à base de clé publique en 2005 par Oded Regev avec son système LWE (Learning with errors) et améliorée depuis par de nombreux chercheurs.

[457] Comme vu dans Code-Based Cryptography for FPGAs de Ruben Niederhagen, 2018 (73 slides).

[458] La résistance de cette méthode aux attaques est documentée dans Code-Based Cryptography de Tanja Lange, 2016 (38 slides). Pour en savoir plus, voir aussi Code Based Cryptography d'Alain Couvreur, 2018 (122 slides) et Some Notes on Code-Based Cryptography, une thèse de Carl Löndahl, 2014 (192 pages).

La littérature sur le sujet est complètement inabordable pour les non spécialistes. Il n'est pas évident de comprendre le fonctionnement de cette méthode de chiffrement malgré l'élégance des schémas qui présentent la notion de réseau euclidien comme celui *ci-contre*[459]. En gros, c'est une matrice de points qui permet de repérer des points en fonction de leurs coordonnées selon un repère de vecteurs différents entre la clé publique et la clé privée.

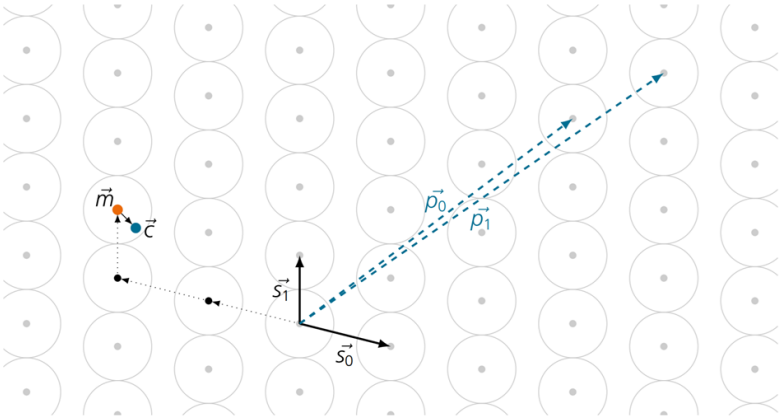


Figure 3.2: Example for lattice-based encryption in a two-dimensional lattice: The secret, well-formed base is $\{\vec{s_0}, \vec{s_1}\}$; the public, "scrambled" base is $\{\vec{p_0}, \vec{p_1}\}$. The sender uses $\{\vec{p_0}, \vec{p_1}\}$ to map the message to a lattice point $\vec{m}$ and adds an error vector to obtain the point $\vec{c}$. The point $\vec{c}$ is closer to $\vec{m}$ than to any other lattice point. Therefore, the receiver can use the well-formed secret base $\{\vec{s_0}, \vec{s_1}\}$ to easily recover $\vec{m}$ (dotted vectors); this is a hard computation for an attacker who only has the scrambled base $\{\vec{p_0}, \vec{p_1}\}$. For a secure scheme, the dimension of the lattice must be much higher than 2 as in this example.

Une erreur est ajoutée aux coordonnées générées avec le vecteur de la clé publique. Seuls les vecteurs de coordonnées de la clé privée permettent de retrouver la coordonnée de la valeur chiffrée. Bon, c'est ce que j'ai compris !

Initialement, elle souffrait de problèmes de performances mais des solutions efficaces sont apparues comme NTRU, créé en 1998 par Jeffrey Hoffstein, Jill Pipher et Joseph Silverman. L'avantage de la méthode est d'utiliser des clés publiques de petite taille. Son décryptage est un problème NP-complet inaccessible aux ordinateurs quantiques. Dans les inconvénients, c'est une méthode protégée par de nombreux brevets, donc propriétaire et potentiellement couteuse[460].

C'est dans cette classe de méthodes que l'on peut ranger la solution de PQC **New Hope** (CECPQ1) qui a été testée en 2016 pendant quelques mois par **Google** dans Chrome et qui s'appuie sur Ring-LWE. Depuis 2019, ils sont passés à CECPQ2 qui comprend une variante du système d'échange de clés HRSS qui fait partie des soumissionnaires au concours du NIST[461] et des sélectionnés de la dernière vague, dans le projet NTRU.

En France, une équipe du laboratoire de l'IRISA-EMSEC développe une solution de cryptographie à base de réseaux euclidiens.

---

[459] Source : On the Security of Lattice-Based Cryptography Against Lattice Reduction and Hybrid Attacks, de Thomas Wunderer, 2018 (188 pages).

[460] Pour en savoir plus, voir la thèse Lattice-based cryptography : a practical implementation, de Michael Rose, 2011 (103 pages), Lattice-based Cryptography de Daniele Micciancio et Oded Regev, 2008 (33 pages) et le tantinet plus pédagogique mais tout de même incompréhensible Overview of Lattice based Cryptography from Geometric de Leo Ducas, 2017 (53 slides).

[461] Voir Experimenting with Post-Quantum Cryptography, par Matt Braithwaite, juillet 2016. Puis Google starts CECPQ2, a new postquantum key exchange for TLS, janvier 2019.

Isogeny-based cryptography (EN) ou isogénie (FR)

Cette variante des courbes elliptiques est encore moins facile à appréhender que tout ce qui précède. En français, c'est un "*morphisme de groupe surjectif et de noyau fini entre deux courbes elliptiques*.". Fastoche ! Le système a été proposé en 2006 par Alexander Rostovtsev et Anton Stolbunov puis cassé par cryptoanalyse quantique par Andrew Childs, David Jao et Vladimir Soukharev. Ce qui a conduit David Jao et Luca de Feo (Inria) à proposer en 2011 l'utilisation de courbes "super-singulières" pour corriger cette faille[462].

A noter le fait que l'éditeur de logiciels **Cloudflare** a sorti une solution de sécurité en open source s'appuyant sur les isogénies, CIRCL (Cloudflare Interoperable Reusable Cryptographic Library). Elle est publiée sur GitHub. Leur solution d'encapsulation de clés SIKE a été soumise au NIST dans son appel d'offre de solutions de cryptographie post-quantique. Ils faisaient partie en janvier 2019 des 17 candidats finalistes pour les solutions de chiffrement à clés publiques ou de création de clés[463].

Hash-based signatures (EN) ou arbres de hashage (FR)

Cette autre méthode de cryptographie post-quantique est aussi antérieure à la notion même d'ordinateur quantique imaginée par Richard Feynman en 1982, puisqu'elle repose sur les travaux de Leslie Lamport du SRI en 1979 et ses "signatures" à base de hash à usage unique.

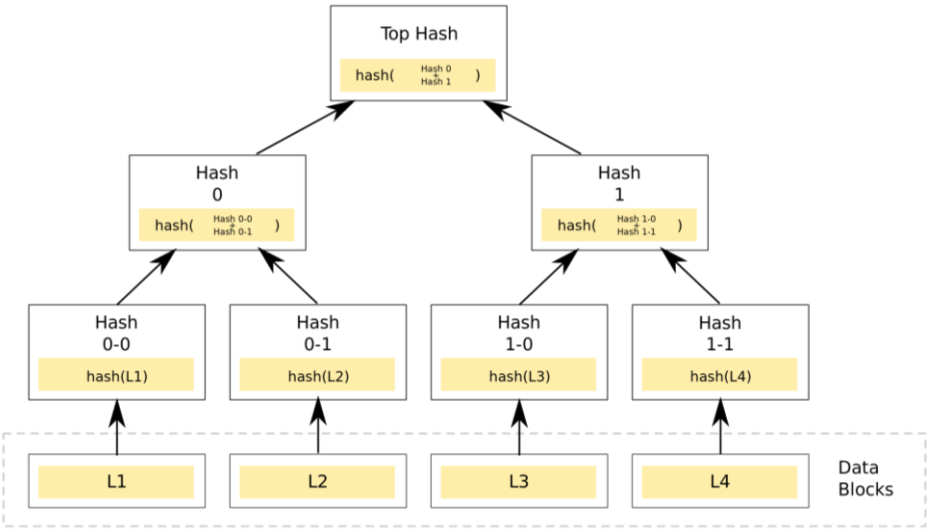
La méthode a été ensuite améliorée en utilisant des arbres de hashage aussi appelé arbres de Merkle pour signer plusieurs messages. Le tout s'appuie sur des clés publiques de taille réduite, descendant à 1 kbits. Cette méthode est surtout utilisée pour de la signature électronique[464].

---

[462] Pour en savoir plus si le cœur vous en dit, voir 20 years of isogeny-based cryptography de Luca De Feo, 2017 (84 slides), An introduction to supersingular isogeny-based cryptography, de Craig Costello (Microsoft Research), 2017 (78 slides), Isogeny Graphs in Cryptography de Luca De Feo, 2018 (73 slides) ou encore An introduction to isogeny-based crypto de Chloe Martindale, 2017 (78 slides).

[463] Voir Cloudflare wants to protect the internet from quantum computing, juin 2019 et Introducing CIRCL: An Advanced Cryptographic Library, juin 2019.

[464] Pour en savoir plus si vous êtes un crack des maths et de la crypto, voir notamment Hash-based Signatures: An Outline for a New Standard (12 pages), Design and implementation of a post-quantum hash-based cryptographic signature scheme de Guillaume Endignoux, 2017 (102 pages) et SPHINCS: practical stateless hash-based signatures, 2015 (30 pages).

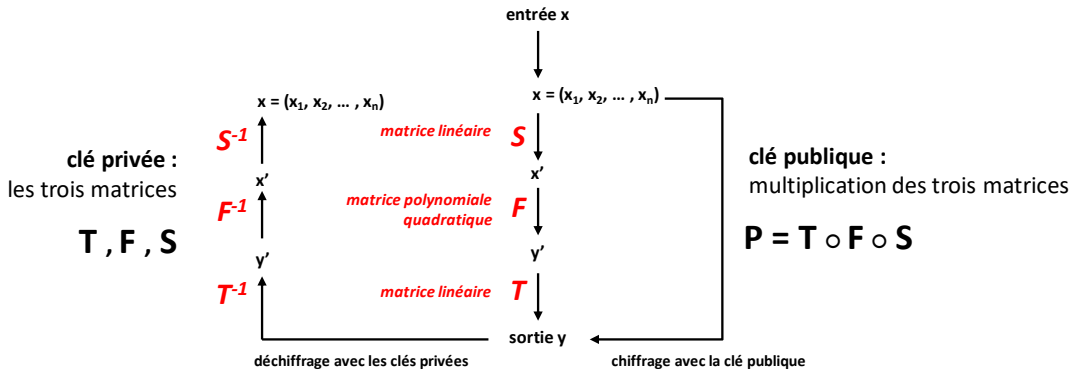


source : Merkle Tree, Wikipedia.

Multivariate polynomial cryptography (EN) ou inversion de polynômes multivariés (FR)

Ce dernier groupe de méthodes fait penser aux codes de correction d'erreurs. La clé publique est une multiplication de plusieurs matrices dont deux sont linéaires et une quadratique (avec des valeurs au carré), les trois matrices séparées constituant la clé privée qui sert à reconstituer le message chiffré.

Le décryptage (donc, par des pirates) est un problème NP-Difficile, hors de portée des ordinateurs quantiques, sinon la méthode ne ferait pas partie de cet inventaire, pardi. La méthode date de 2009 et a évidemment été ensuite déclinée sous plusieurs variantes.



Les clés publiques sont assez grandes, allant par exemple jusqu'à 130 Ko (avec la variante HFEBoost)[465]. Cette méthode de chiffrement est plutôt utilisée pour les signatures électroniques.

[465] A noter la contribution de Jacques Stern de l'ENS "Post-quantum multivariate-quadratic public key schemes" lors de PQCRYPTO 2006.

En préparant cette partie, j'imaginais que l'on pouvait combiner de la QKD (protection physique de la distribution de clés) et de la PQC (protection logique du chiffrement contre le décryptage par ordinateur quantique). Et bien, pas vraiment. La QKD est plutôt dédiée aux algorithmes à clés symétriques qui supposent une protection de la communication physique entre correspondants tandis que la PQC s'appuie sur des clés publiques qui n'ont donc pas besoin d'être protégées par QKD car leur interception (sans la QKD) ne servirait déjà à rien à des pirates.

On peut cependant combiner de la QKD pour l'échange de clés avec de la cryptographie post-quantique pour l'authentification et le chiffrement des données. La QKD a besoin d'authentification qui peut être assurée en amont par de la PQC. Par contre, la QKD peut être redondante avec de la PQC utilisée pour l'échange de clés[466].

Cryptographie homomorphe quantique

La cryptographie homomorphe consiste à chiffrer des données qui peuvent ensuite traverser un traitement classique en mode chiffré et donner un résultat chiffré qui sera déchiffrable à la fin du traitement.

Dans le machine learning et le deep learning, ce mode de chiffrement permet de distribuer dans le cloud des traitements d'entraînement et d'inférence de modèles de machine learning sans que le piratage des données transmises permette de révéler le contenu de données qui alimentent le modèle. L'inconvénient de cette méthode est qu'elle ne fonctionne pas avec tous les modèles de machine learning et qu'elle est très couteuse en temps machine pour le chiffrement et le déchiffrement des données.

Le chiffrement homomorphe quantique relève de la même démarche pour chiffrer des données qui vont alimenter un ordinateur quantique, dans le cloud, et déchiffrer ensuite le résultat des traitements. C'est l'un des outils qui permet de mettre en œuvre ce que l'on appelle le « blind computing » dans le cloud, où les serveurs ne peuvent pas comprendre et interpréter les données qu'ils traitent.

Divers algorithmes de chiffrement de programmes de contrôle de portes quantiques ont été proposés mais ne sont pas encore couramment utilisés[467]. Une partie des clés peut être transmise de manière quantique à l'instar d'une QKD. C'est d'ailleurs l'une des conditions pour être sûr que la partie serveur ne puisse par intépréter les traitements qu'elle réalise[468].

---

[466] Pour en savoir plus sur la PQC, voir notamment Post-quantum cryptography – dealing with the fallout of physics success de Daniel Bernstein et Tanja Lange, 2017 (20 pages), Post-Quantum Cryptography de Thomas Pöppelmann (Infineon), 2017 (32 slides), Le grand défi du post-quantique de Jean-Charles Faugère, 2018.

[467] Voir Classical Homomorphic Encryption for Quantum Circuits, de Urmila Mahadev, 2018 (7 pages), Quantum Fully Homomorphic Encryption With Verification, 2017 (30 pages et slides, 28 slides), Quantum Homomorphic Encryption: A Survey, 2017 (11 pages) et Quantum homomorphic encryption for circuits of low T-gate complexity par Anne Broadbent et Stacey Jeffery, 2015 (35 pages).

[468] Comme l'indique On the implausibility of classical client blind quantum computing de Scott Aaronson, Elham Kashefi & Al, 2017 (43 pages).

Chez les constructeurs d'ordinateurs quantiques, on considère qu'une suite de portes quantiques pilotant un processeur quantique est déjà difficile à interpréter dans l'absolu !

Startups de la cryptographie quantique

Passons maintenant en revue les startups de ce vaste secteur d'activité de la cryptographie quantique et post-quantique, en essayant de bien décrire la nature de leur offre et de leur différenciation lorsque l'information est publiquement disponible ! Je n'ai conservé ici que les startups proposant des solutions technologies et pas intégré les sociétés de conseil et d'intégration.

Notons que du côté taille de marché, celui de la cryptographie quantique et post-quantique est pour l'instant modeste. Un rapport de 2017 l'évaluait à $2,5B d'ici 2022[469]. Il devrait cependant monter en puissance à partir de cette période, après la finalisation de la standardisation par le NIST et par l'ETSI.

Hors startups, des offres commerciales de cryptographie quantique et post-quantique sont aussi proposées ou sur le point d'être proposées par divers acteurs industriels tels que Batelle, Infineon, Raytheon, IBM, Cisco, Atos, Gemalto, Microsoft, NEC, Toshiba, Huawei[470], KT et Samsung.

AgilePQ (2014, USA) fournit une plateforme logicielle de sécurisation "post-quantum" de la communication entre objets connectés et le cloud, comme des drones.

[469] Voir New CIR Report States Quantum Encryption Market To Reach $2.5 Billion Revenues By 2022: Mobile Systems Will Ultimately Dominate, 2017.

[470] Voir Continuous-Variable Quantum Key Distribution with Gaussian Modulation, the Theory of Practical Implementations, 2018 (71 pages). L'équipe de Huawei qui planche sur la QKD est en partie située dans leur centre de recherché de Dusseldorf.

Il comprend AgilePQ C-code un bout de logiciel qui fonctionne sur les micro-contrôleurs d'objets connectés et consomme peu d'énergie et de l'autre, AgilePQ DEFEND, un système de génération de clé de taille adaptable. DEFEND génère des codes qui sont plus difficiles à casser que l'AES 256 et avec 429 ordres de grandeur de différence. Précisément, on passe d'un espace de clés de 10 puissance 77 à 8*10 puissance 506 (factorielle de 256)[471]. Le système qui est breveté semble être une variante de codes linéaires aléatoires mais avec des clés de taille raisonnable. Il a été soumis à la standardisation au NIST et s'interface avec les systèmes de contrôle et de supervision SCADA (Supervisory control and data acquisition). La société est partenaire de Microsoft Azure. Pour une startup, ses dirigeants et fondateurs n'ont pas l'air bien jeunes, mais ils ont de l'expérience !

Citypassenger (France) est un intégrateur dans la sécurité qui a développé une solution de CV-QKD en partenariat avec la startup française SeQureNet (qui a visiblement mis la clé sous la porte en 2017) et Telecom ParisTech. La solution est particulièrement adaptée au déploiement de VPN (virtual private networks, des réseaux sécurisés reliant les différentes entités physique d'une même organisation).

Crypta Labs (2013, UK, $300K) développe des solutions de chiffrement post-quantiques adaptées aux objets connectés. Ils proposent notamment le seul générateur de nombres aléatoire quantique intégrable dans un mobile. Ils travaillent de concert avec l'Université de Bristol.

CryptoExperts (2008, France) est une startup qui développe une offre de chiffrage homomorphe et de cryptographie post-quantique et qui propose aussi des services autour de ces technologies.

[471] Voir AgilePQ DEFEND Cryptographic Tests (11 pages).

CryptoNext Security (2019, France) est une startup qui développe une solution de cryptographie post-quantique fondée par Ludovic Perret (CEO, ex Inria) et Jean-Charles Faugères (CTO, ex LIP6 Sorbonne). Ils ont notamment Philippe Duluc (Atos) et Denis Mercier (ex Otan) dans leur board. Leur solution logicielle est développée en langage C et en assembleur pour des questions de performance. Elle associe des polynomes multivariés et du hashage. Leur solution peut s'intégrer dans des schémas RSA/ECC par hybridation.

CryptoNext est aussi l'une des équipes françaises ayant soumis une proposition de PQC au NIST américain. Avec un bémol car le NIST demande à ce qu'il n'y ait pas de brevets sur les algorithmes qui seront retenus. Les processeurs de standardisation de la PQC passent en pratique par de nombreux organismes tels que l'ISO, ITU (X509), IETF (TLS) et ETSI (algorithmes). Leur PQC devrait s'intégrer dans la solution de blockchain CORDA de R3 qui est destinée aux banques. A noter que les Chinois organisent également un processus concurrent du NIST avec un calendrier de sélection plus rapide que celui du NIST.

Crypto Quantique (2015, UK) est une startup qui propose une solution de cryptographie destinée à sécuriser la communication avec des objets connectés. Elle exploite un chipset qui est installé dans l'objet.

C'est un « processeur quantique » en technologie silicium qui sert à générer une clé d'identification unique de l'objet, inclonable et inviolable. Il exploite probablement de la photonique avec un générateur de nombres aléatoires similaire aux technologies du Suisse IDQ. Leur technologie s'appelle Quantum Driven Physically Unclonable Function (QD-PUF) mais ils n'expliquent rien sur son fonctionnement exact ni sur le modèle de chiffrement utilisé[472]. La startup faisait partie de l'accélérateur de Thales à Station F dans la promotion démarrant en septembre 2018. Les fondateurs sont d'origine iranienne, italienne et grecque, un beau patchwork. Ils visent des marchés divers allant de l'automobile à la finance.

[472] Voir Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions.de Roel Maes et Ingrid Verbauwhede (36 pages) et Quantum readout of Physical Unclonable Functions, de B. Skoric (21 pages).

evolutionQ (2015, Canada) est une startup qui se distingue surtout par le pédigrée de son créateur, Michele Mosca, un spécialiste Italien de la cryptographie post-quantique. C'est aussi le fondateur de l'Institut for Quantum Computing de l'Université de Waterloo au Canada. La société fait ce que l'on appelle du service outillé pour accompagner les entreprises dans l'adoption de cryptographie post-quantique. Cela commence par un produit d'évaluation du risque quantique ("Quantum Risk Assessment") qui comporte six phases, documentées dans A Methodology for Quantum Risk Assessment, publié en 2017. Est-ce vraiment un produit ? Cela ressemble surtout à une méthodologie à mettre en œuvre avec des consultants. Le reste est de la même crème avec des services d'intégration et de formation pour faire évoluer les systèmes de cryptographie de l'entreprise.

ID Quantique (2001, Suisse, $5,6M) est l'une des plus anciennes sociétés du secteur, créée par le chercheur Suisse Nicolas Gisin, spécialiste de la photonique et de l'intrication quantique. La société propose surtout Quantis, son générateur de nombres aléatoires, déjà décrit au début de cette partie. C'est complété par Cerberis, une solution de QKD pour protéger la circulation des clés de chiffrement et Centauris, une gamme de serveurs de chiffrement supportant des liaisons optiques de 100 GBits/s. Ce serveur à base de FPGA supporte pour l'instant des systèmes à base de courbes elliptiques ainsi que de l'AES-256, dans l'attente de la standardisation des protocoles de PQC (post-quantum-crypto)[473].

La startup appartient depuis début 2018 au groupe coréen SKT Invest qui est la branche de Corporate Venture de SK Telecom. Le fonds a investi $65M dans la startup dans ce qui est pudiquement présenté comme un partenariat alors que c'est une prise de contrôle. La société avait 60 salariés en juin 2018.

Quantis : génération de nombre aléatoire

Centauris : préparation des clés et chiffrement

Cerberis QKD Blade : protection quantique des clés publiques

[473] Dans L'arme anti-NSA de la France, sabordée en 2010 ?, de Guerric Poncet dans Le Point, 2013, est racontée l'histoire de SmartQuantum, une startup française spécialisée dans la QKD et fermée en 2010. Son créateur s'y plaint de l'influence néfaste de Thales qui aurait bloqué son développement. Neuf ans plus tard, le marché de la QKD ne fait que démarrer. Dans le meilleur des cas, SmartQuantum était juste un peu trop en avance de phase par rapport à la maturité de ce marché. Et ce n'est pas une société américaine qui est devenue leader, mais le Suisse IDQ.

InfiniQuant (Allemagne) est une spin-off du Max Planck Institute for the Science of Light. Ils mettent au point un système de clé quantique QKD dénommé CV-QKD pour "Continuous Variable Quantum Key Distribution" utilisable sur fibre optique et liaison satellite. Cette technique utilise une modulation d'amplitude en plus d'une modulation de phase pour transmettre les clés quantiques. La startup travaille aussi sur un générateur de nombres aléatoire quantique, concurrent de ceux d'IDQ.

ISARA (2015, Canada, $1,6M de CA en 2017) développe des solutions logicielles de chiffrement post-quantiques et du conseil de mise en œuvre de PQC. Leur produit est la "ISARA Radiate Security Solution Suite" qui fournit des clés publiques et algorithmes de chiffrement non attaquables par des ordinateurs quantiques du futur. Ils s'appuient visiblement sur des arbres de hashage et associent de la PQC (post-quantum crypto) et de la PKI (public-key infrastructure) traditionnelle.

C'est documenté dans le livre blanc Enabling Quantum-Safe Migration with Crypto-Agile Certificates, 2018 (7 pages). L'un de leurs investisseurs est le fonds Quantum Valley Investments, géré notamment par Mike Lazaridis, le cofondateur de Blackberry RIM. Ce dernier est une sorte de Xavier Niel canadien, ayant réinvesti sa fortune liée à Blackberry dans le développement de l'écosystème scientifique et entrepreneurial canadien, en particulier dans le quantique où il a investit en tout $450M (source).

KETS Quantum Security (2016, UK, £2M) développe un générateur de nombres aléatoire (QRNG = quantum random number generator) et un générateur de clé quantique QKD, le tout intégré dans une photonique miniaturisée dans un simple composant.

Le tout est combiné à une activité de conseil pour le déploiement des solutions. La société a été créée par des chercheurs en photonique de l'Université de Bristol. Ils ciblent les marchés financiers et du secteur public. Ils prototypent des drones avec Airbus pour la mise en place de QKD dans des domaines militaires ou de sécurité publique, avec Airbus Defense. Leur chipset QKD peut aussi équiper des micro-satellites type Cubesat.

Magiq (1999, USA) est une startup qui s'était lancé initialement en 2003 dans la création d'un système de QKD. Depuis une dizaine d'année, cette société semble s'être repositionnée dans le service et pour la défense US. Ils ont développé l'Agile Interference Mitigation System (AIMS), un système de réduction d'interférences de communications électromagnétiques.

Nu Quantum (2018, UK) développe des solutions matérielles de sécurité quantique, probablement autour de la QKD. C'est une spin-off du Cavendish Lab de l'Université de Cambridge.

Origone (2014, UK) est une étrange startup basée au Royaume-Uni après avoir été située à Paris (jusqu'à sa liquidation en France en 2017) qui développe des solutions de cryptographie en s'appuyant notamment sur les ordinateurs de D-Wave. Elle vise notamment le marché de la défense ainsi que le ferroviaire. Leur activité de cryptographie quantique/post-quantique est une évolution d'une activité dans la cybersécurité classique.

PicoQuant (1996, Allemagne) est une PME de Berlin spécialisée en photonique et qui commercialise notamment des compteurs de photons. Mais ils sont ici parce qu'ils proposent aussi un générateur de nombres aléatoire quantique.

Post-Quantum ou **PQ Solutions** (2009, UK, $10,4M) est une startup initialement créée sous l'appellation SRD Wireless qui avait créé la messagerie sécurisée PQ Chat utilisant les codes linéaires aléatoires inventés par Robert McEliece.

La société a été renommée en Post-Quantum ou PQ Solutions Limited en 2014. Ils proposent une ligne de produits de sécurisation intégrant des algorithmes de crypto post-quantique. L'un des cofondateurs Martin Tomlinson, a développé le préencodage Tomlinson-Harashima qui permet de corriger les interférences dans les signaux de télécommunications et divers codes de correction d'erreur. Leurs produits comprennent aussi notamment PQ Guard, un système de chiffrement post-quantique.

Ravel Technologies (2018, France) propose Ravel Homomorphic Encryption, une solution de chiffrement post-quantique et homomorphe.

QEYnet (2016, Canada, $7M) développe un réseau de satellite de cryptographie quantique QKD. Le financement de la startup vient du gouvernement canadien.

QuantumCTek (Chine) est un fournisseur de solution de cryptographie quantique de bout en bout : QKD, répéteurs de QKD, routeurs optiques. La société est issue du Hefei National Laboratory for Physical Science at Micro-scale (HFNL) et de l'University of Science and Technology of China (USTC). Ils sont à l'origine de la création en 2014 du "Quantum-Safe Security Working Group" avec ID Quantique et Battelle, qui fait la promotion de la PQC. Ils ont comme nous l'avons vu plus haut déployé la liaison protégée par QKD de 2000 km reliant Shanghaï et Beijing.

Qasky (2016, Chine) commercialise le produit de la recherche de l'académie chinoise des sciences. Les financements proviennent de Wuhu Construction and Investment Ltd et de l'Université des Sciences et de Technologie de Chine. Ils proposent des solutions de crypto post-quantique, QKD et des composants de photonique. Leur nom est dérivé de CAS Key laboratory, CAS = Chine Academy of Sciences.

Qrypt (2017, USA) est une jeune startup de faisant de la PQC (post quantum crypto) créée par des anciens du gouvernement fédéral US, sans plus de précisions.

Ils annonçaient en août 2018 utiliser sous licence le générateur de nombres aléatoire quantique à photons du laboratoire d'Oak Ridge du Département de l'Energie US.

QuantiCor Security (2017, Allemage) développe des solutions de cryptographie post-quantique (PQC), notamment pour les applications de la blockchain et pour les objets connectés. Ils sont issus de TU Darmstadt.

Quantum Impenetrable (2018, UK) est une startup écossaise qui développe un module de sécurité (HSM) exploitant un générateur de nombres aléatoire quantique et résistant aux algorithmes quantiques de cassage de clés.

Quantum Xchange (2016, USA) propose un réseau optique sécurisé par QKD aux USA, dénommé Phio. Ils sont partenaires de l'opérateur d'infrastructures télécoms Zayo Group et exploitent leurs fibres noires et utilisent les solutions de QKD d'ID Quantique. Ils ont commencé par déployer leur réseau entre New York et le New Jersey.

QuBalt (2015, Allemagne) est une startup établie entre l'Allemagne et la Lettonie qui développe des solutions de cryptographie post-quantique (PQC) ainsi que sur des algorithmes quantiques.

Qubit Reset (2018, USA) développe des répéteurs quantiques pour des réseaux de QKD. La société a été crée par deux argentins basés à Miami. Elle ne figure pas dans la Crunchbase et ne semble pas avoir levé de fonds ce qui semble être un mauvais présage.

Quintessence Labs (2006, Australie) propose un générateur de nombres aléatoires quantiques et un système de QKD. Ils utilisent la technique CV-QKD qui permet d'utiliser des infrastructures de fibre optique existantes d'opérateurs télécoms à très haut débit.

Qunnect (2017, USA) est une toute jeune spin-off de la Stony Brook University de Long Island. Ils proposent des composants qui permettent d'upgrader des installations télécom existantes avec de la QKD et de la PQC, dont des sources de photons et une mémoire quantique fonctionnant à température ambiante pouvant servir à la mise en place de répéteurs de QKD (*ci-contre*).

QuNu Labs (2016, Inde) développe des solutions à base de QKD issues de L'Institut de Technologie de Madras. Ils proposent aussi leur propre générateur de nombres aléatoires quantique et planchent aussi sur la création d'une solution de QKD opérant sur du Li-Fi, le W-FI qui utilise les fréquences de la lumière visible.

Quside (2017, Espagne) propose un générateur de nombre aléatoire quantique.

Secure-IC (France) est le porteur du projet RISQ, de création d'une solution de crypto post-quantique française. La société développe des solutions matérielles et logicielles de sécurité qui servent à évaluer la robustesse de solutions de sécurité. La société est issue de l'Institut Mines-Télécom.

SeQureNet (2008-2017, France) était une spin-off de Telecom ParisTech spécialisée dans la distribution de CV-QKD fonctionnant à longue distance (source). Elle avait été financée dans le cadre du projet de recherche Européen SECOQC (secure communication based on quantum cryptography).

La startup valorisait des travaux issus de l'équipe de Philippe Grangier de l'Institut d'Optique et du laboratoire du CNRS situé chez Thales TRT à Palaiseau. La société a fermé boutique en 2017 ! Dommage.

SpeQtral (Singapour), anciennement S-Fifteen Space Systems, est spécialisée dans la distribution de QKD par satellite. Ils valorisent des travaux de l'Université de Singapour dans la conception de pico-satellites de type CubeSat, pour la distribution de clés QKD.

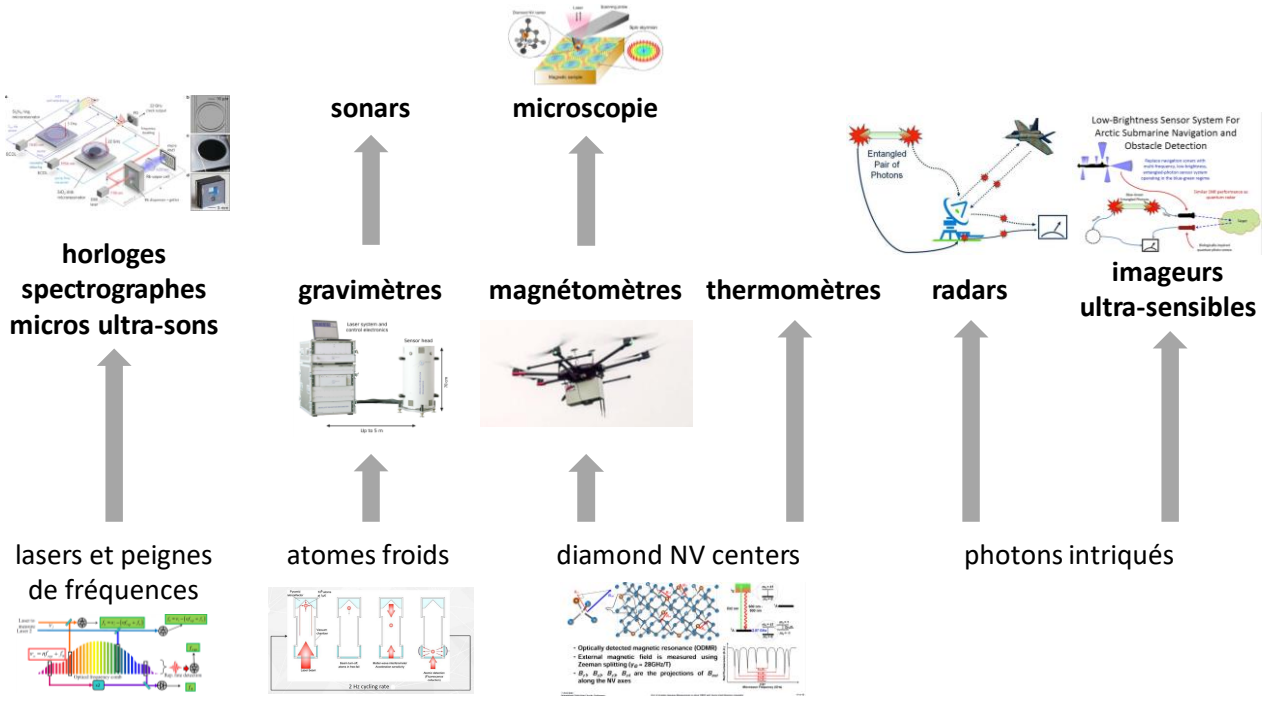
Surrey Satellite Technology ou SSTL (UK) veut déployer un satellite de communication quantique à base de QKD, en partenariat avec Eutelsat et l'ESA. Le lancement du satellite est planifié pour début 2020.

VeriQloud (2017, France) est une startup créée par Elham Kashefi et Marc Kaplan (France) et Joshua Nunn (UK). Elle est spécialisée dans la création d'algorithmes quantiques adaptés aux télécommunications quantiques (QKD).

ZY4 (2014, Canada) développe des solutions de cryptographie post-quantique.

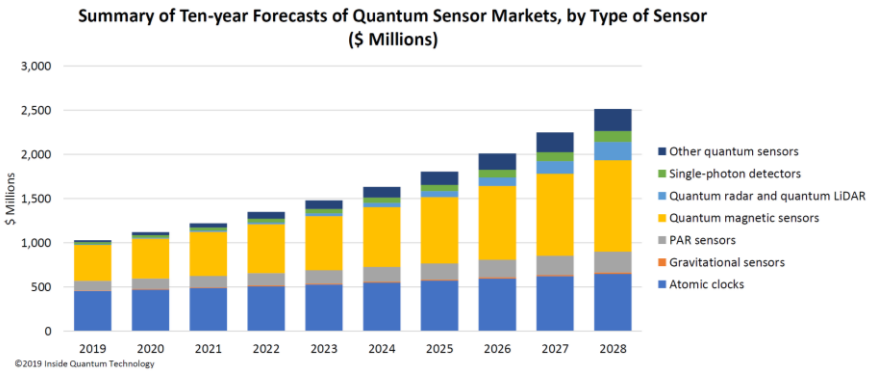
Métrologie quantique

Dans cette nouvelle partie de cet ebook, nous allons rentrer un peu dans le détail de ce domaine scientifique et marché un peu à part du quantique : la métrologie. Il s'agit des différentes solutions de mesure de précision qui s'appuient sur des mécanismes quantiques.

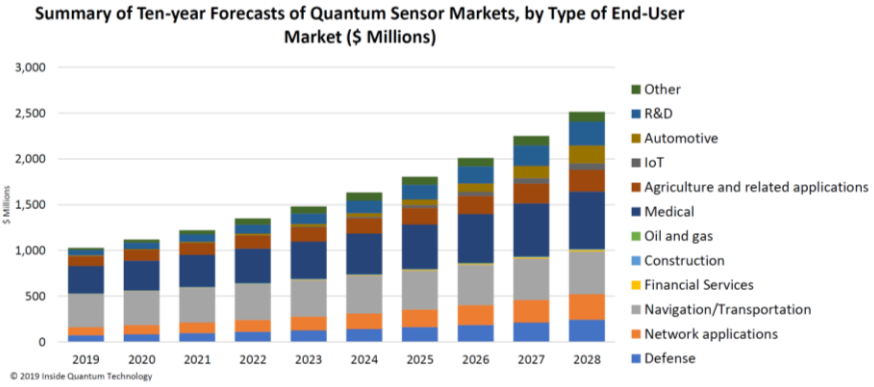


Les mesures concernées sont celles du temps, de la gravité, du magnétisme, de la température et du temps. Les applications dérivées sont nombreuses dans les radars, les sonars, les microphones très haute sensibilité ou encore le domaine de l'imagerie en général et médicale en particulier. Ces technologies sont exploitables commercialement et continuent de progresser régulièrement.

Ce serait toutefois un marché de taille plus limitée, démarrant aujourd'hui à $1B pour en faire deux d'ici une dizaine d'années et à l'échelle mondiale, bien moins que pour le calcul et la cryptographie quantiques.



Qui plus est, ce marché est fragmenté en un grand nombre de sous-marchés que nous allons détailler dans cette partie [474]. Les deux plus gros étant ceux des transports et de l'imagerie médicale.



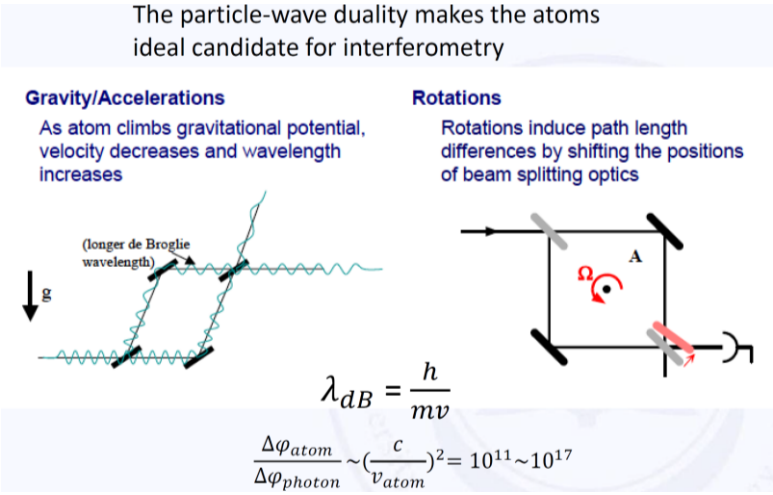
Gravimètres quantiques

Les gravimètres quantiques permettent de mesurer la gravité avec une très grande précision. C'est utile dans de nombreux scénarios : dans les détecteurs sismiques, pour la mesure et la définition du kilogramme de référence, pour la navigation autonome de précision complétant les GPS dans les avions, navires, sous-marins et drones, pour la cartographie de champ gravitationnel, pour la prospection de pétrole et de minerais et pour la détection d'ondes gravitationnelles en astonomie.

La mesure de la gravité est généralement réalisée avec des interféromètres d'atomes froids, tirant partie de la dualité onde-particules s'appliquant aussi aux atomes.

La technique a été mise au point étape par étape à partir de 1991 et perfectionnée depuis[475].

Elle consiste à créer une source d'atomes froids en suspension, à préparer leur état avec des lasers, puis à les faire traverser un interféromètre et ensuite analyser les résultats. Cela peut servir à la mesure de la gravité, d'une accélération et de rotations[476].



La technique est utilisée, perfectionnée et rendue transportable par la startup française **Muquans**. Leur gravimètre quantique cible par exemple la détection de cavités pour le BTP, la prospection pétrolière et la surveillance de volcans comme pour l'Etna en Italie. Le produit s'appelle « Absolute Quantum Gravimeter »[477].

---

[474] Source des données : Quantum Sensors: Ten Year Market Projections par Lawrence Gasman, 2019 (7 slides).

[475] Voir Young s double-slit experiment with atoms : A simple atom interferometer, de O. Carnal, J. Mlynek, 1991 (6 pages) qui décrit une experience d'interférométrie de fentes de Young à base d'atomes d'hélium. Voir aussi Experimental gravitation and geophysics with matter wave sensors, LP2N, 2018 (234 slides).

[476] Source du schéma : Compact and Portable Atom Gravimeter de Shuai Chen, University of Science and Technology of China, juin 2019 (22 slides).

[477] Le procédé de Muquans est documenté dans Gravity measurements below 10^{-9} g with a transportable absolute quantum gravimeter, 2018 (12 pages) et valorisé dans Digging Into Quantum Sensors par Stewart Wills dans Optics & Photonics, septembre 2019.

Ils utilisent un petit nuage d'une centaine d'atomes de rubidium refroidis à 1 µK par lasers dans 6 directions et piégés magnétiquement sous vide. Ils sont stimulés par des transitions de Raman à base de doubles photons[478] avec des durées et polarisations différentes (π/2, −π, −π/2).

Le système mesure alors la chute gravitationnelle du nuage d'atome qui est différente selon la préparation des atomes.

Un système à base de fluorescence et de diodes mesure la vitesse de la chute et le fait dans la durée pour évaluer sa variation temporelle. Les diodes mesurent la proportion des atomes dans chaque sortie de l'interféromètre. La source des atomes contient aussi un accéléromètre qui corrige en temps-réel la phase des lasers.

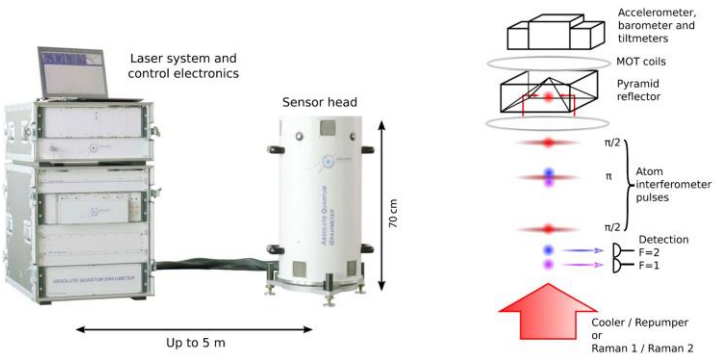
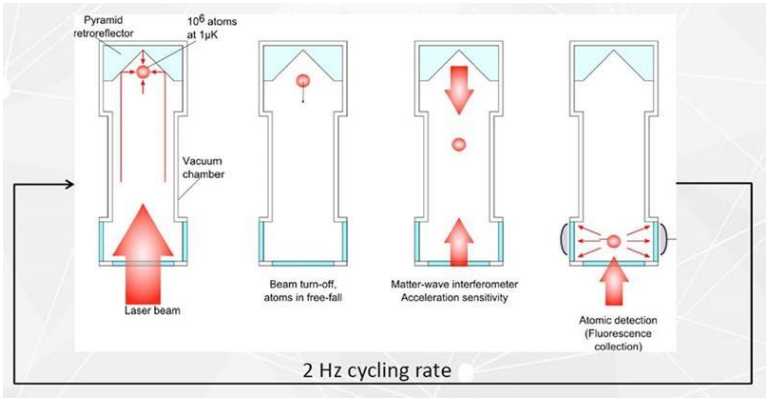


Figure 1. Left: picture of the first Absolute Quantum Gravimeter (AQG-A01). The system can be setup at a measurement location in less than 20 min, warm-up time is of the order of 1 h. The sensor head weighs approximately 30 kg. It is mounted on an adjustable tripod with precision leveling titanium-tipped feet that can be adapted to various terrains. The measurement height is 55 cm. Right: sketch of the sensor head and measurement principle[24]. Approximately 10^7 atoms are loaded in a magneto-optical trap (MOT) inside the pyramid and cooled down to 2 μK. The $\pi/2 - \pi - \pi/2$ atom interferometry sequence is performed once the atoms are in free-fall. At the end of the sequence, we collect fluorescence on a set of photodiodes and compute the proportion of atoms in each output port of the interferometer, labeled by their internal state. A high-precision accelerometer is attached to the top of the vacuum chamber, as close as possible to the pyramidal reflector. Its signal is used to apply a real-time correction to the laser phase, in order to reject seismic noise. Two tiltmeters and a barometer are also attached to the sensor to ensure high accuracy and long-term stability of the gravity measurement.



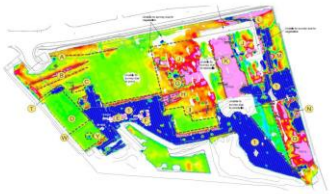
La maîtrise des atomes froids a d'autres applications. Ainsi, Muquans participe aux projets du flasgship européen **Quantum Internet Alliance** pour créer un matériel d'extension de la portée des systèmes de QKD et avec la startup française **Pasqal** qui créé des processeurs quantiques à base d'atomes froids.

D'autres sociétés sont aussi dans ce marché :

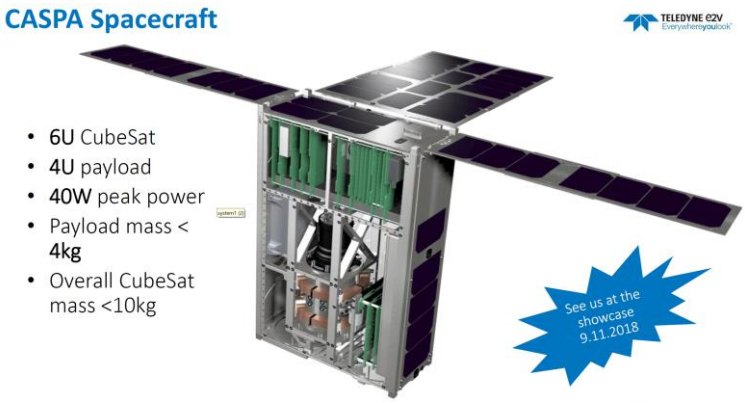
- **Thales** (France) développe des gravimètres de petite taille, moins précis, mais qui peuvent être embarqués. Il me semble qu'ils fonctionnent aussi à base d'atomes froids et d'interférométrie.

[478] Le refroidissement Raman à double photon utilise deux lasers. Un premier excite les atomes pour les faire atteindre un état excité élevé et un autre désexcite l'atom pour le faire dedescendre à un état excité supérieur à l'état initial. C'est cette technique qui permet de descendre la température en-dessous du micro-Kelvin.

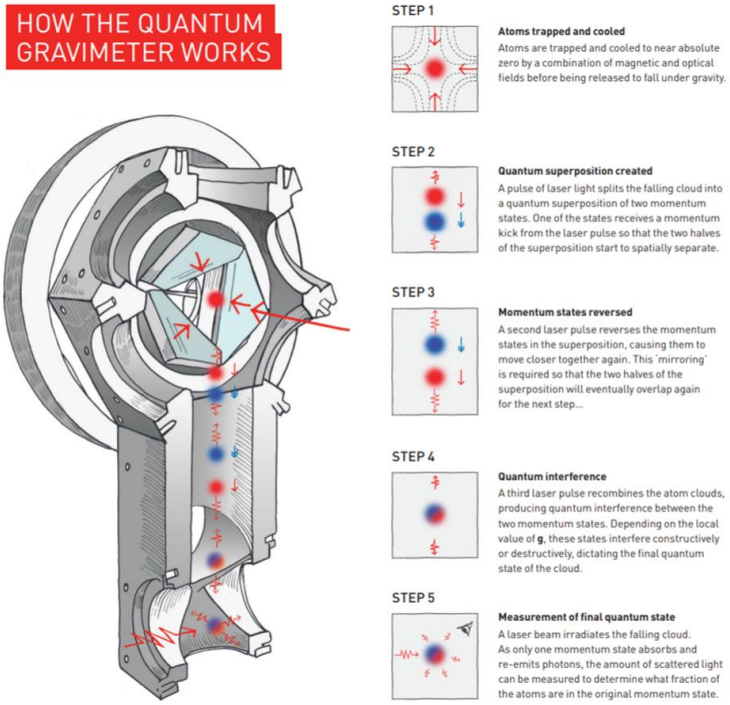
- **Teledyne e2v** (UK, filiale de Teledyne US) vise la maintenance d'infrastructures avec la détection d'obstacles sous-terrains ou de cavités avant les travaux de BTP, la recherche d'énergies géothermiques et de réserves d'eaux souterraines.



  Ils sont aussi partie prenante de la création de **CASPA** (Cold Atom Space PAyload), un petit satellite de 14 kg rassemblant 6 CubeSat dans un volume de 30x20 x10cm, comprenant un gravimètre à atomes froids, qui serait le premier à fonctionner dans l'espace. Il doit être lancé par l'ESA en 2020.



- **M Squared** (2006, UK) développe un gravimètre quantique à atomes froids utilisant un procédé voisin de celui de Muquans [479], en partenariat avec l'Université de Birmingham. Le projet a été financé dans le cadre de l'initiative quantique du gouvernement UK lancée dès 2013 (« UK Quantum Technology Programme »). La startup commercialise sinon la gamme de laser SolsTiS couvrant le spectre de 200 nm à 4000 nm, notamment pour l'industrie. Leurs produits sont aussi exploités dans des horloges optiques.



[479] Source de l'illustration : M Squared quantum gravimetry (4 pages).

- **AOSense** (2004, USA) qui crée des gyroscopes quantiques, un gravimètre quantique et des horloges optiques commerciaux. Il fournit aussi de l'appareillage d'instrumentation pour la recherche dans ces domaines avec des générateurs d'atomes froids et des générateurs de peignes de fréquences lasers (voir la définition dans la partie suivante sur les horloges optiques). Ils collaborent avec IonQ pour leurs ordinateurs quantiques à base d'ions piégés.

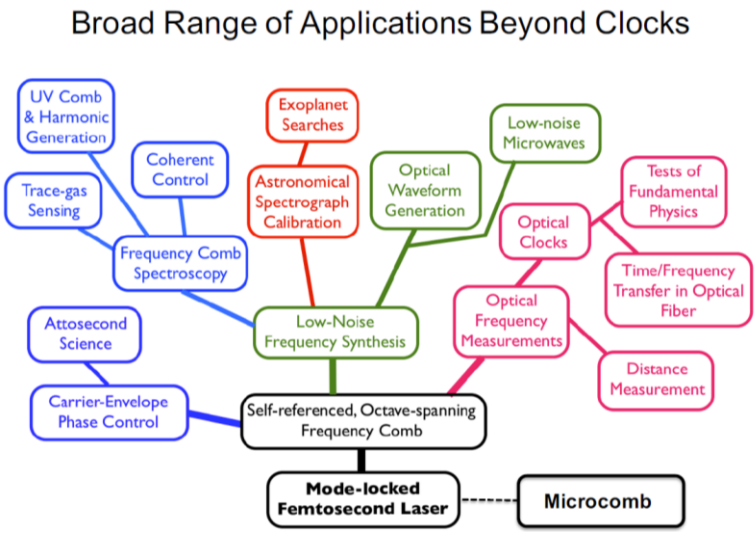
Horloges quantiques

La mesure du temps a régulièrement progressé depuis les premières horloges mécaniques entre le 14e et le 19e siècle. C'est entre deux guerres que sont apparus les horloges à quartz exploitant l'effet piézoélectrique démontré par Pierre et Jacques Curie en 1880. L'effet a une fréquence de 2^{15} Hz et on décompte le temps après application de diviseurs de fréquences. Le tout avec une dérive de quelques centaines de microsecondes par jour.

Les premières horloges atomiques au césium datent des années 1950. Elles ont une fréquence de l'ordre de 9 GHz et fournissent un étalon de fréquence de 10^{-13}. La seconde est définie depuis comme la durée de 9 192 631 770 périodes de la radiation correspondant à la transition entre les deux niveaux « hyperfins » de l'état électronique fondamental du césium 133.

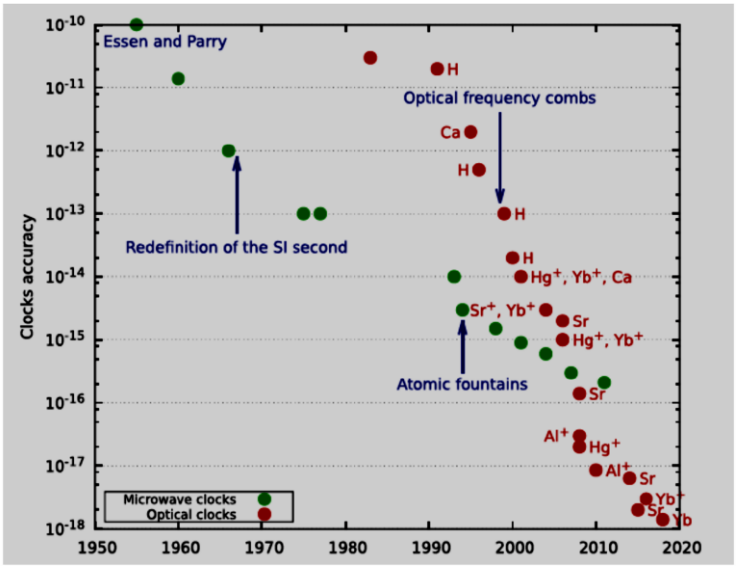
La variante récente de ces horloges dite « fontaine » fonctionne à très basse température, avec un refroidissement laser amenant les atomes à 1 µK. C'est bien plus froid qu'un qubit supraconducteur qui se contente de 15 mK. Un oscillateur de fréquence génère une transition entre deux niveaux d'énergie du césium. La fréquence est verrouillée avec une boucle d'asservissement.

La mesure précise des fréquences a de nombreuses applications : la mesure du temps, la synchronisation des appareils sur Internet, celle d'objets en mouvement pour mesurer leur position, l'astronomie (exoplanètes, ondes gravitationnelles[480]), la spectroscopie de précision d'absorbtion ou d'émission, la gestion de transmissions par fibres optiques et la génération d'ondes radios de forme arbitraire.

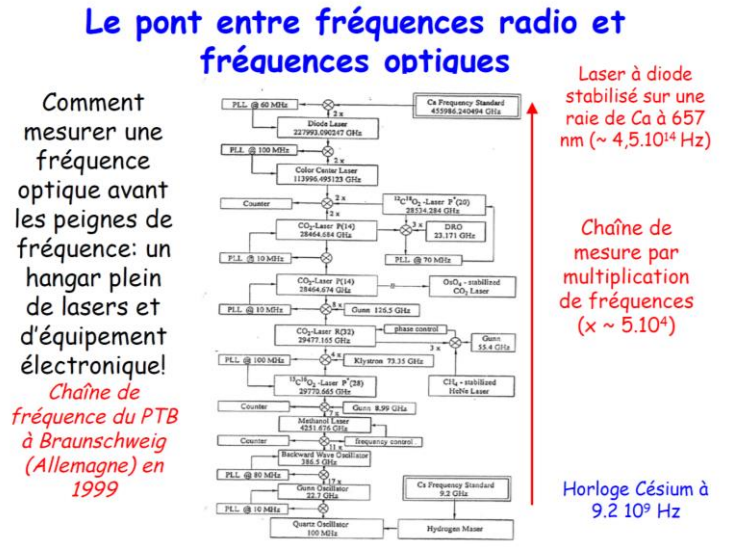


[480] Voir Atomic Clocks as Detectors of Gravitational Waves de Sergei Kopeikin, University of Missouri (43 slides). Qui est aussi la source du graphe sur l'évolution dans le temps de la precision des horloges.

Une meilleure précision est cependant nécessaire. Depuis une vingtaine d'année, elle est obtenue grâce à la mesure optique des fréquences et du temps. Pour cela, on a remplacé la mesure de vibrations atomiques par celle d'ondes lumineuses générées par des lasers et à 10^{15} Hz. Elle a permis de gagner une précision d'un facteur 10^5. Le principe a été démontré en 2000 pour générer une précision de l'ordre de la femtoseconde.



Cela a valut le prix Nobel de Physique en 2005 à Theodor Hänsch et John Hall[481]. Les peignes de fréquences avaient été découverts avec les premiers lasers à mode bloqué par Logan Hargrove en 1964. Avant les peignes optiques, on utilisait des générateurs d'harmoniques de fréquences lumineuses avec une combinaison de plusieurs lasers dans des montages compliqués, comme *ci-contre*[482].



Pour mesurer les fréquences élevées de la lumière, ces horloges utilisent des peignes de fréquences optiques (frequency combs) qui permettent de subdiviser des fréquences optiques (élevées) en fréquences micro-ondes (moins élevées) pour la mesure de fréquence et le décompte temporel.

Cette mesure exploite des lasers dits « à mode bloqué » qui génèrent des impulsions très courtes, pouvant descendre jusqu'à quelques femtosecondes, contrairement aux lasers continus.

---

[481] Voir Nobel Lecture: Defining and measuring optical frequencies de John Hall, 2006 (17 pages) et Des règles de lumière : les peignes de fréquence de Steven Cundiff, Jun Ye et John Hall dans Pour la Science, 2008 (8 pages). John Hall y raconte que les peignes de fréquence sont le croisement de quatre champs de recherche au départ indépendants : les lasers ultra-stables, les lasers à impulsions rapides, les matériaux optiques non linéaires et la spectroscopie laser de précision. A l'image de l'informatique quantique.

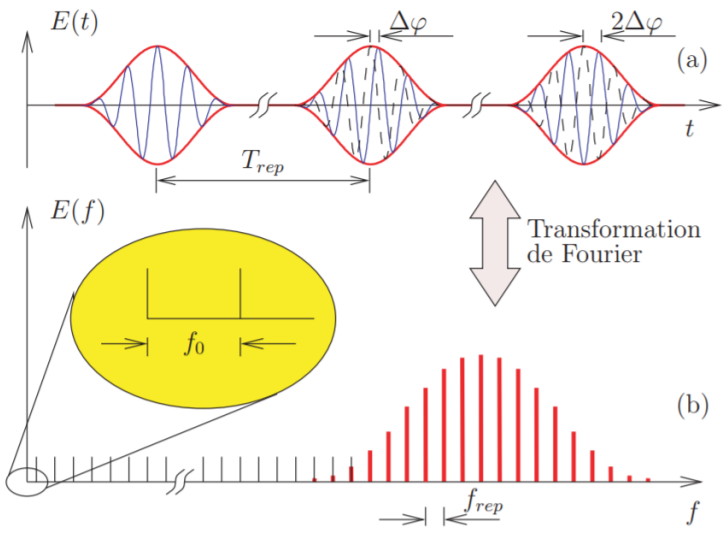
[482] Source de l'illustration : Chaire de Physique Quantique-Cours 2014-2015, 5ème leçon - 7 Avril 2015, V. La passion de la précision et la mesure du temps de Serge Haroche, Collège de France (72 slides).

La décomposition en fréquence de ce genre de signal donne un peigne de fréquences en forme de gaussienne et dont chaque dent est espacée régulièrement d'une fréquence équivalente à celle de l'impulsion du laser.

C'est lié au fait que la longueur de la cavité du laser est un multiple de la longueur des ondes électromagnétiques émises par le laser. Plus le multiple est grand, plus l'est la fréquence générée.

Le spectre de fréquence ressemble à une gaussienne. Son enveloppe est égale à l'enveloppe du spectre d'une impulsion isolée, qui est continue. La largeur du spectre de fréquence couvert peut être étroit, de quelques nm de longueur d'onde, ou couvrir tout le spectre visible, donc quelques centaines de nm. Un calcul permet de déterminer les fréquences très élevées du peigne de fréquence (f_n).

Il exploite plusieurs paramètres : la fréquence de référence f_{rep} des pulsations du laser qui est de l'ordre de 250 MHz à 1GHz, n, le nombre de fréquences détectées via spectroscopie (il peut y en avoir des centaines de milliers) et la phase d'émission du laser à mode bloqué qui s'ajoute à chaque impulsion et génère le décalage de fréquence f_0, que l'on évalue avec une méthode décrite plus loin et qui est aussi d'un ordre inférieur au GHz [483].



Grâce à la mesure de fréquences du domaine des ondes radio en MHz/GHz, on aboutit à la mesure de fréquences en dizaines et centaines de THz au Hz près. Le système agit ainsi comme un multiplicateur de fréquences. La mesure de fréquences lumineuses est impossible avec de l'électronique traditionnelle du fait des fréquences utilisées qui sont de plusieurs dizaines ou centaines de tera-Hertz. Ces peignes de fréquences étalonnés servent aussi à mesurer une différence de fréquences avec cet étalon[484].

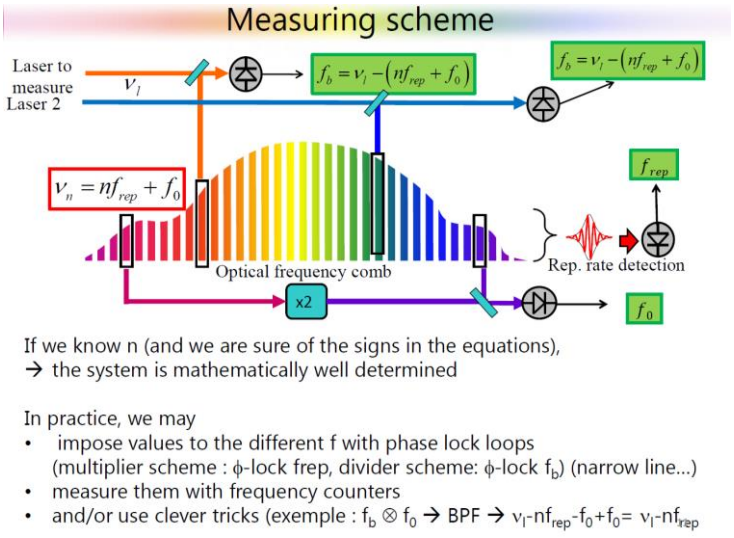
[483] Source de l'illustration : Impulsions lumineuses ultra-courtes pour la métrologie de fréquences, CNRS (6 pages).

[484] Voir A la recherche d'une précision extrême les peignes de fréquences d'Alexandre Parriaux, 2016 (7 pages), Phase Coherent Vacuum-Ultraviolet to Radio Frequency Comparison with a Mode-Locked Laser de J. Reichert & Al, 2005 (5 pages), Direct Link between Microwave and Optical Frequencies with a 300 THz Femtosecond Laser Comb de Scott Diddams & Al, 2000 (4 pages), Fundamentals of frequency combs What they are and how they work de Scott Diddams (46 slides) et Optical frequency combs and optical frequency measurements de Yann Le Coq, 2014 (38 slides). Voir aussi les explications dans Chip-scale Optical Atomic Clocks and Integrated Photonics par Matthew Hummon, NIST, 2018 (35 slides).

Le peigne de fréquences couvre une octave, soit d'une fréquence (n) jusqu'à son double (2n). L'évaluation de f_0 s'effectue en extrayant la fréquence f_n, et en la doublant avec un cristal. En additionnant cette fréquence doublée avec f_{2n}, on obtient un battement à la fréquence de f_0[485].

$$2(f_0 + n \times f_{rep}) - (f_0 + 2n \times f_{rep}) = f_0$$

C'est ce que l'on appelle la détection hétérodyne.



Le peigne de fréquences devient une sorte de règle graduée qui est ensuite utilisée pour positionner une fréquence à mesurer par rapport à la règle. Comment crée-t-on une horloge atomique optique avec tout cela ? Je n'ai pas encore compris[486] !

La lecture des résultats de spectroscopie utilisant des peignes de fréquence peut utiliser des caméras CCD ou CMOS selon les fréquences utilisées dans ou autour du visible[487]. La précision de cette mesure évolue avec l'usage de lasers utilisant une haute fréquence d'impulsion. Ils sont notamment à base de titane-saphir avec des impulsions de quelques femtosecondes (10^{-15} à 10^{-14} secondes).

A ce jour, le record de précision d'une horloge atomique utilisant de la spectroscopie est celle du **NIST.** Elle est bâtie avec un ion d'aluminium associé à un anion de magnésium. L'ion d'aluminium est excité par deux lasers à l'ytterbium. La mesure est réalisée à l'aide d'une « quantum logic spectroscopy » qui fait elle-même appel aux peignes de fréquences vus plus haut[488]. L'horloge atteint une précision de 10^{-18} seconde, soit une dérive d'une seconde sur 33 milliards d'années, ce qui représente 2,5 fois l'âge de l'Univers[489].

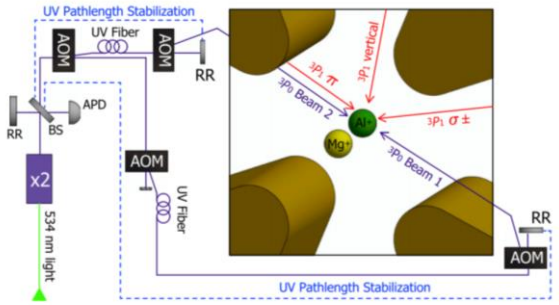


FIG. 1. Simplified schematic of the quantum-logic clock experimental setup. A frequency-quadrupled Yb-doped fiber laser is locked to the $^1S_0 \leftrightarrow {}^3P_0$ transition ($\lambda \simeq 267$ nm) by alternating the probe direction between two counterpropagating laser beams (shown in violet). An enlarged view of the trapping region is shown on the right. Three nominally orthogonal beams used for micromotion measurements are shown in red. Acousto-optic modulator (AOM), beam splitter (BS), retro-reflector (RR), frequency doubling stage (x2).

---

[485] Source du schéma : Optical frequency combs and optical frequency measurements de Yann Le Coq, 2014 (38 slides), slide 11.

[486] C'est expliqué dans Optical Atomic Clocks, de Andrew Ludlow, Martin Boyd, Jun Ye, E. Peil et P.O. Schmidt, 2015 (65 pages) et Optical atomic clocks de N. Poli & Al, 2014 (70 pages). Voir aussi Photonic integration of an optical atomic clock de Z. L. Newman & Al, novembre 2018 (12 pages).

[487] Voir Impulsions lumineuses ultra-courtes pour la métrologie de fréquences, 2005 (6 pages) et Peignes de fréquences femtosecondes : aux limites de la spectroscopie de Theodor Hänsch Nathalie Picqué, 2010 (8 pages).

[488] Voir cette explication : Quantum Logic for Precision Spectroscopy par Piet Schmidt & Al, 2009 (6 pages).

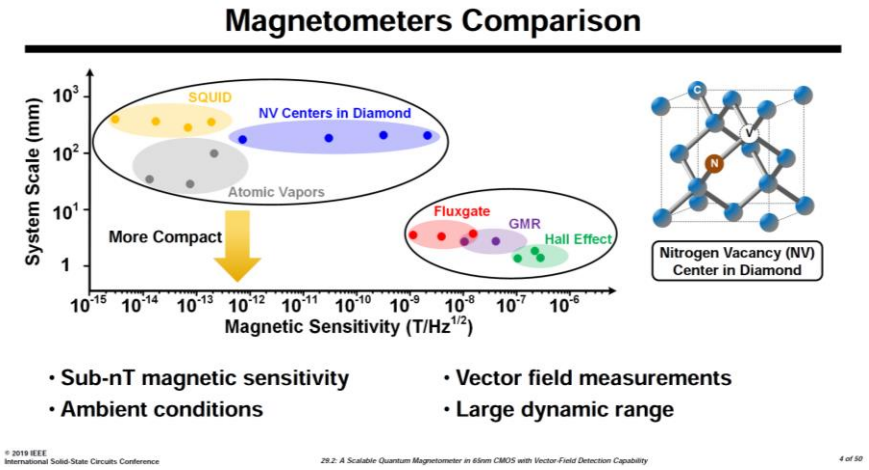
[489] Voir $^{27}Al^+$ Quantum-Logic Clock with a Systematic Uncertainty below 10^{-18}, 2019 (6 pages).

Dans ce marché des horloges quantiques optiques, on trouve de nombreux laboratoires de recherche qui produisent leur propre appareillage. Dans le privé, on compte notamment **Teledyne** avec une offre variée : Minac (horloge atomique au césium), T-CSAC (également au césium, intégrée dans une puce) et Synchronicity (à base d'ytterbium).

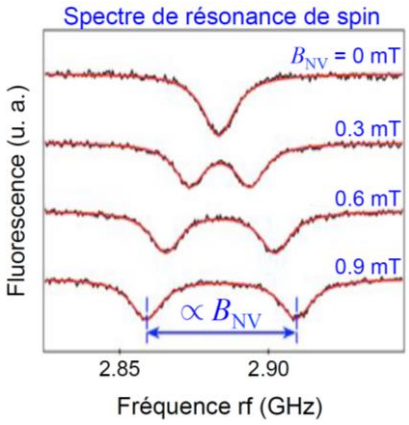
Magnétomètres quantiques

Les magnétomètres quantiques servent à détecter les faibles variations ou niveaux de magnétisme et avec une grande précision spatiale. Les usages sont variés : pour la navigation, l'exploration de minerais, la détection de courant, la magnétocardiographie, la magnétoencéphalographie, l'orientation de drones dans des tunnels, là où le GPS ne fonctionne pas[490], les sonars, la détection d'objets métalliques mouvants comme des véhicules et l'imagerie cellulaire.

Différentes techniques sont disponibles dont les atomes froids[491], les SQUID (effet supraconducteur Josephson) et les systèmes à base de cavités dans les diamants (NV-centers) dont nous avons vu qu'ils peuvent aussi servir de qubits.



La mesure du magnétisme utilise la variation du spectre de résonance du spin de la cavité de diamant, qui dépend du champ magnétique ambiant. On mesure la distance entre les deux impulsions lumineuses fluorescentes (Y) générées en fonction de la fréquence d'excitation électromagnétique utilisée (X)[492]. La préparation des spins est réalisée avec un laser et sa modification avec des impulsions micro-ondes autour de 3 GHz. La précision de la mesure du magnétisme atteint le pico-Tesla[493] soit des milliards de fois moins que le magnétisme terrestre[494].



[490] Une solution de drones utilisant un GPS en tunnel est proposée par la startup **Hovering Solutions** (Espagne).

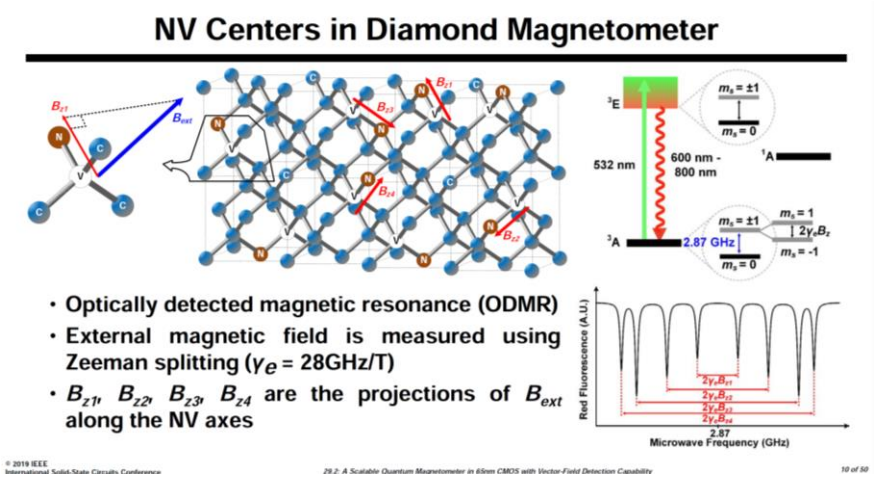
[491] Voir la technique à base d'atomes de Rydberg décrite dans Quantum sensing using circular Rydberg states de Rémi Richaud, LKB, novembre 2018 (41 slides).

[492] Après agrandissement optique, la fluorescente peut être analysée par un capteur d'image CCD.

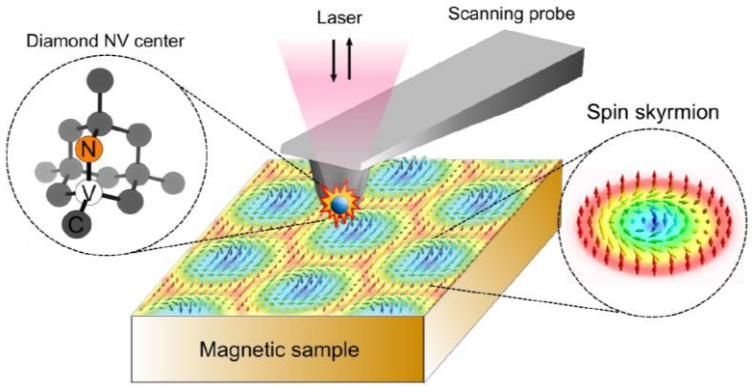
[493] Source de l'illustration : Centres NV du diamant : du matériau aux applications de Jean-François Roch, Collège de France, 2015 (52 slides).

[494] La précision de la magnétométrie à centres NV s'évalue avec une formule du type $1\mu T/\sqrt{Hz}$.

Cette dernière technique à NV-centers est apparue en 2009. Elle est développée à Palaiseau chez **Thales**. Ils apportent une moins bonne précision que les atomes froids mais leur usage est plus pratique car l'instrument est plus facile à miniaturiser[495].

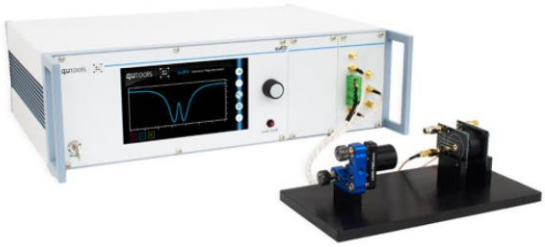


Les magnétomètres à pointe utilisent un nano-cristal de diamant contenant une seule cavité et un atome d'azote, ce qui assure la précision de la mesure. La pointe peut être déplacée dans l'espace et servir à analyser le magnétisme d'un matériau en 2D[496].



Habituellement, les NV-centers sont utilisés en température cryogénique pour pouvoir fonctionner. Les laboratoires de Bristol, de l'Université d'Ulm en Allemagne et de Microsoft travaillent sur l'utilisation de techniques de NV Centers couplée à du machine learning et de méthodes d'inférence bayésiennes permettant de corriger le bruit constaté à plus haute température[497].

Qutools (Allemagne) propose son magnétomètre quantique quNV, à base de NV-centers de diamants comme son nom l'indique. Il tient dans un rack 3U. Toujours, en Allemagne, l'Université de Stuttgart travaille avec le Fraunhoffer Institute pour transférer la technologie de la magnétométrie à base de NV-centers das le cadre du projet **QMag**[498].



[495] L'illustration provient de A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability par Mohamed Ibrahim du MIT 2019 (51 slides). Elle décrit un procédé de miniaturisation de magnétomètre quantique associant un circuit CMOS 65 nm fabriqué par TSMC et un système à base de NV-center en diamant.

[496] Source de l'illustration : Probing and imaging nanoscale magnetism with scanning magnetometers based on diamond quantum defects, 2016 (35 slides).

[497] Voir Magnetic-Field Learning Using a Single Electronic Spin in Diamond with One-Photon Readout at Room Temperature de Raffaele Santagati & Al, 2018 (18 pages).

[498] Voir Quantum Magnetometers for Industrial Applications, avril 2019.

QLM Technology (2017, UK) propose une solution de magnétomètre quantique qui détecte les fuites de méthane dans les pipelines jusqu'à une distance de 100 mètres. Le système de mesure pesant quelques kg peut-être embarqué dans un drone de grande envergure volant à 50 km/h.

Thermomètres quantiques

La technique des NV centers a un autre usage : la mesure de la température avec une précision de quelques mK et avec une très grande résolution spatiale, le tout avec des capteurs miniaturisés. C'est à ce jour la technologie de mesure de température la plus performance sur ces différentes dimensions. Cela permet par exemple de déterminer la température au sein de cellules vivantes[499].

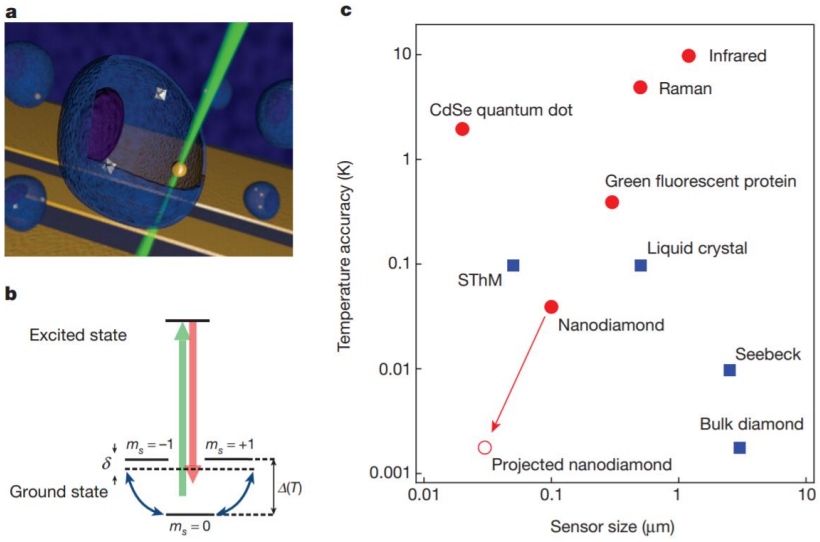


Figure 1 | Nitrogen–vacancy-based nanoscale thermometry. a, Schematic image depicting nanodiamonds (grey diamonds) and a gold nanoparticle (yellow sphere) within a living cell (central blue object; others are similar) with coplanar waveguide (yellow stripes) in the background. The controlled application of local heat is achieved by laser illumination of the gold nanoparticle, and nanoscale thermometry is achieved by precision spectroscopy of the nitrogen–vacancy spins in the nanodiamonds. **b**, Simplified nitrogen–vacancy level diagram showing a ground-state spin triplet and an excited state. At zero magnetic field, the $|\pm1\rangle$ sublevels are split from the $|0\rangle$ state by a temperature-dependent zero field splitting $\Delta(T)$. Pulsed microwave radiation is applied (detuning, δ) to perform Ramsey-type spectroscopy. **c**, Comparison of sensor sizes and temperature accuracies for the nitrogen–vacancy quantum thermometer and other reported techniques. Red circles indicate methods that are biologically compatible. The open red circle indicates the ultimate expected accuracy for our measurement technique in solution (Methods).

Il existe aussi des solutions de mesure de température dans la matière biologique par fluorescence à base de quantum dots[500].

Imagerie et microscopes

Des microscopes de nouvelle génération s'appuient sur des effets quantiques. C'est notamment le cas des microscopes utilisant des magnétomètres à base de NV-centers de diamants. Nous allons aussi faire un tour du côté des mystérieux systèmes de « ghost imaging » qui font des photos d'objets avec un capteur à un seul pixel.

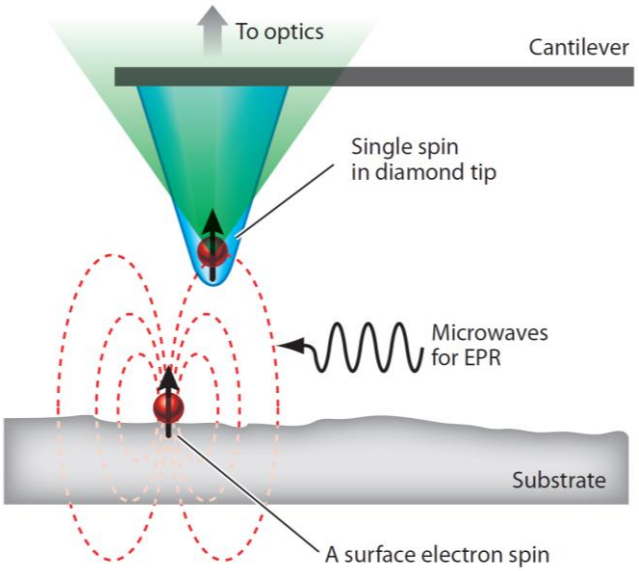
---

[499] Voir Nanometre-scale thermometry in a living cell, 2013 (6 pages).

[500] Voir Intracellular thermometry with fluorescent sensors for thermal biology par Kohki Okabe & Al, 2018 (15 pages).

L'imagerie à base de NV-centers est l'un des axes du laboratoire **Max Planck Institute for Solid State Research** et du **Fraunhofer Institute** for Applied Solid State Physics (IAF) à Fribourg en Allemagne. Leurs microscopes servent à analyser des molécules organiques avec une excellente résolution spatiale. Ils travaillent aussi sur des spectroscopes à spins d'électrons (ESR : electron spin resonance spectroscopy) à température cryogénique qui permettent d'examiner des atomes et des molécules au niveau du spin de leurs électrons. La technique est intégrée dans des microscopes à effet tunnel. Le spin des électrons des matériaux examinés est excité par un champ magnétique et des micro-ondes.

La technique des NV-centers permet d'examiner un disque dur avec une sonde dotée d'un seul NV-center (*ci-dessous*[501] *et ci-contre*[502]). Elle sert aussi à faire de la caractérisation (contrôle qualité) de circuits intégrés travaillant dans des fréquences millimétriques comme ceux de la 5G[503]. D'autres encore travaillent sur la microscopie de cellules vivantes [504] . Une application existe même pour qualifier les patients atteints de malaria, par l'analyse de nanocristaux de l'hémozoïne qui apparait dans les globules rouges affectés par le parasite de la maladie[505].



Ces techniques sont utilisées dans la microscopie confocale. Celle-ci génère des images avec une très faible profondeur de champ d'environ 400 nm générant des sections optiques de l'échantillon à analyser.

En modifiant la position du plan focal en profondeur, on réalise des séries d'images servant ensuite à générer sur ordinateur une vue en 3D de l'échantillon analysé. La source lumineuse est réfléchie ou obtenue par fluorescence en réaction à un rayon laser. Ce qui donne un microscope confocal à balayage laser, et, en anglais, un CLSM pour Confocal Laser Scanning Microscope.

---

[501] Source de l'illustration : Solid-State Spin Quantum Computers (21 slides) et Optical far-field super-resolution microscopy using nitrogen vacancy center ensemble in bulk diamond, 2016 (5 pages) qui décrit une technique de microscopie avec une résolution descendant à 6 nm.

[502] Source de l'illustration : Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology, 2014 (27 pages).

[503] Voir Microwave Device Characterization Using a Widefield Diamond Microscope, 2018 (10 pages) qui implique notamment le LSPM de Paris.

[504] Voir A fluorescent nanodiamond foundation for quantum sensing in cells, 2018 (147 pages) qui évoque la microscopie de cellules vivantes.

[505] Voir Diamond magnetic microscopy of malarial hemozoin nanocrystals d'Ilja Fescenko & A, septembre 2018 (17 pages),

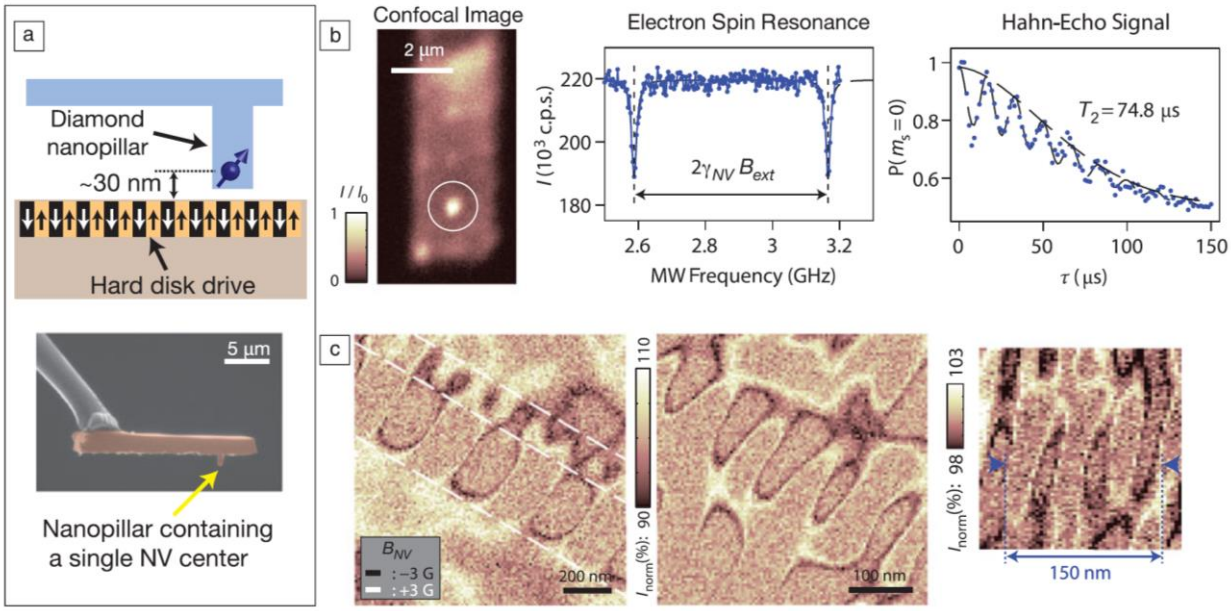
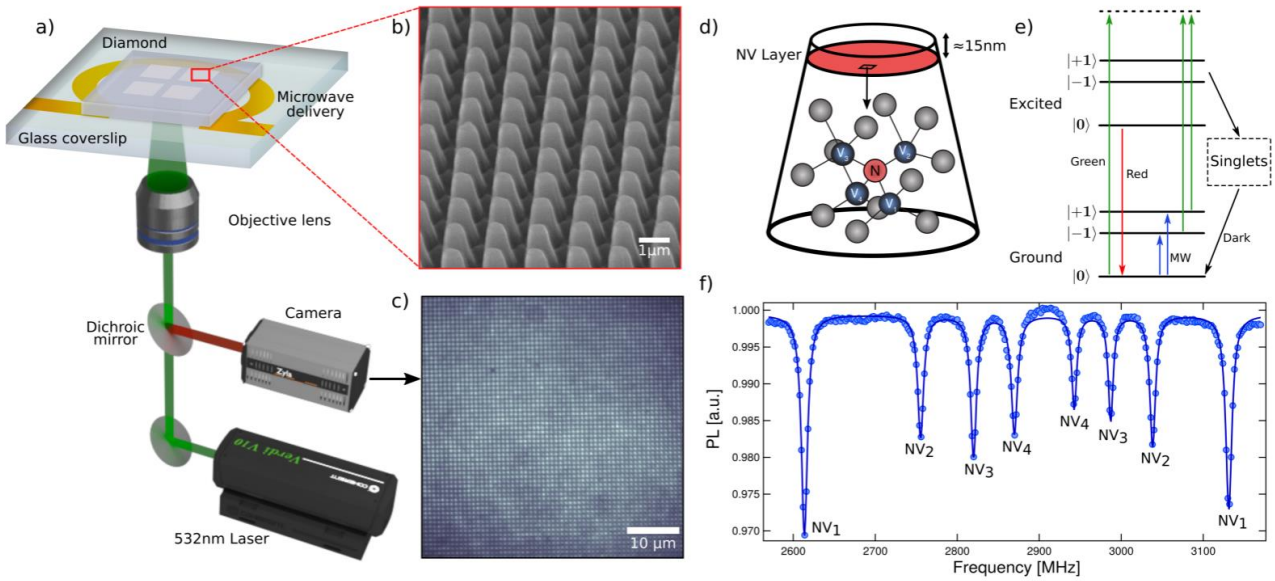


Figure 4. (a) Schematic of a monolithic diamond nanopillar probe (top) and representative SEM image of the nanopillar probe (bottom). (b) Characteristics of a nanopillar probe device. Confocal image of the device (left) clearly shows a localized fluorescence spot from a single NV center at the position of the nanopillar. Electron spin resonance (middle) was acquired with an enhanced fluorescence of 220,000 photons/sec. The coherence time of the measured Hahn-echo signal (right) is 74.8 μs, an order of magnitude longer than a typical Hahn-echo coherence time of commercial diamond nanocrystals (~5 μs). (c) Magnetic images of a hard disk drive acquired by the nanopillar probe. Alternating magnetic bits were imaged with varying sizes down to 25 nm (right), indicating the distance between a single NV center at the probe and the hard disk sample is roughly within 25 nm. Adapted with permission from Reference 19. © 2012 Nature Publishing Group.

Les NV-centers permettent aussi d'améliorer la précision des optiques adaptatives qui sont notamment utilisées en astronomie[506].

D'autres techniques utilisant de l'interférométrie laser permettent d'examiner les molécules au niveau atomique dans leur milieu et non pas sous vide et dans un froid cryogénique[507].

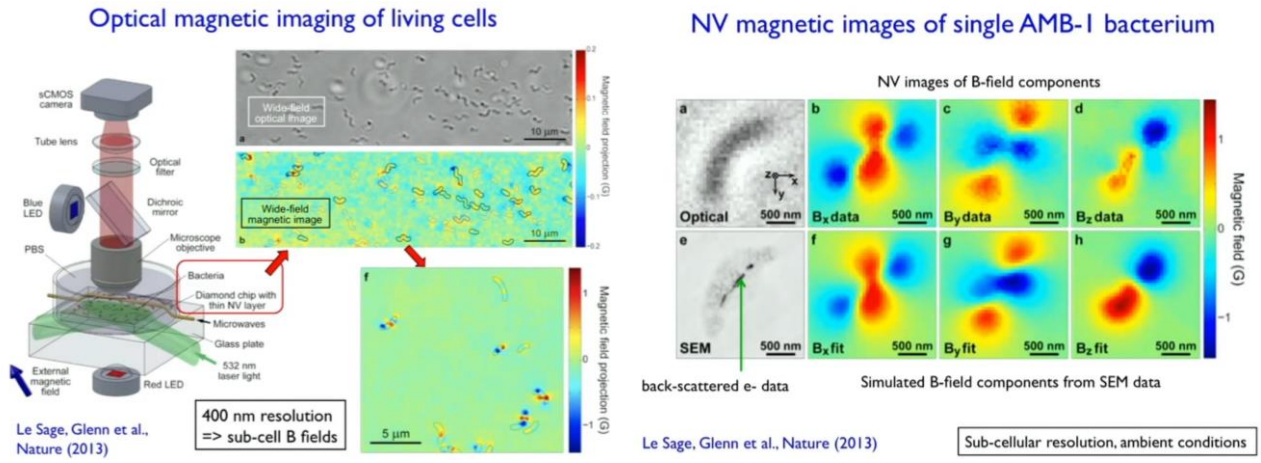


[506] Voir Nanodiamonds enable adaptive-optics enhanced, super-resolution, two-photon excitation microscopy, 2019 (7 pages).

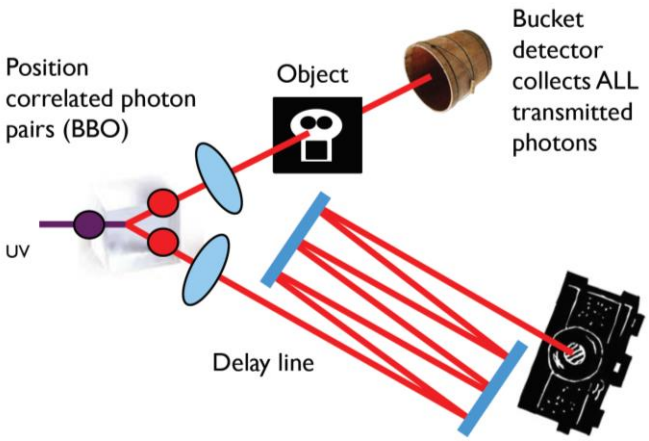
[507] Voir An Entanglement-Enhanced Microscope de Takafumi Ono, Ryo Okamoto, Shigeki Takeuchi, 2014 (8 pages).

Enfin, l'imagerie peut exploiter une matrice de centres NV de petite taille qui procure une bien meilleure résolution que les systèmes d'imagerie à base de SQUID. Les deux exemples *ci-dessus* en montrent l'architecture[508].

Pour le second, il s'agissait d'étudier des bactéries qui contiennent de micro-éléments magnétiques. Dans d'autres cas, on peut utiliser des marqueurs magnétiques qui vont s'attacher aux cellules à détecter, typiquement en cancérologie.



L'imagerie quantique peut aussi faire appel à la curieuse technique du ghost imaging ou imagerie fantôme quantique. Elle existe sous de nombreuses déclinaisons. La première en date utilisait un générateur de photons infrarouges intriqués en 1995[509]. Une moitié des photons éclaire l'objet et l'autre un capteur photo, en traversant une ligne à retard optique[510].



Les photons qui éclairent l'objet sont intriqués avec ceux qui éclairent la caméra, ces derniers n'ayant pas vu l'objet ! L'image obtenue est très bruitée et nécessite un traitement idoine. A quoi cela peut-il bien servir ?

Principalement à analyser des objets avec un très faible nombre de photons pour éviter que ceux-ci modifient l'objet à analyser. Cela peut-être intéressant en microbiologie[511]. Visiblement, les objets analysés sont toujours de petite taille[512].

---

[508] Voir Enhanced widefield quantum sensing with nitrogen-vacancy ensembles using diamond nanopillar arrays de D. J. McCloskey, 2019 (7 pages). Les matrices de centres NV expérimentées font 100 µm de côté. L'illustration provient d'autres travaux publiés en 2013, cités dans la conférence Magnetic imaging using NV-diamond: techniques & applications de Ronald Walsworth, 2015 (51 mn). Notamment Optical magnetic imaging of living cells, Le Sage & Al, Nature, 2013 (11 pages).

[509] Voir Optical imaging by means of two-photon quantum entanglement, par Yanhua Shih & Al, 1995 (4 pages), de l'Université de Maryland. Et Observation of two-photon 'ghost' interference and diffraction, Yanhua Shih, 1995 (4 pages).

[510] An introduction to ghost imaging: quantum and classical par Miles Padgett et Robert Boyd, 2016 (10 pages) fait un bon tour d'horizon du sujet. Voir aussi Quantum Ghost Image Identification with Correlated Photon Pairs, 2010 (4 pages).

[511] Voir The Dawn of Quantum Biophotonics de Dmitri Voronine & Al, 2016 (30 pages).

D'autres techniques, non quantiques, utilisent un imageur couleur doté d'un seul pixel et exploitant 1300 éclairages structurés par seconde éclairant l'objet pendant quelques secondes. Le capteur comprend quatre photodiodes positionnées à des endroits différents[513].

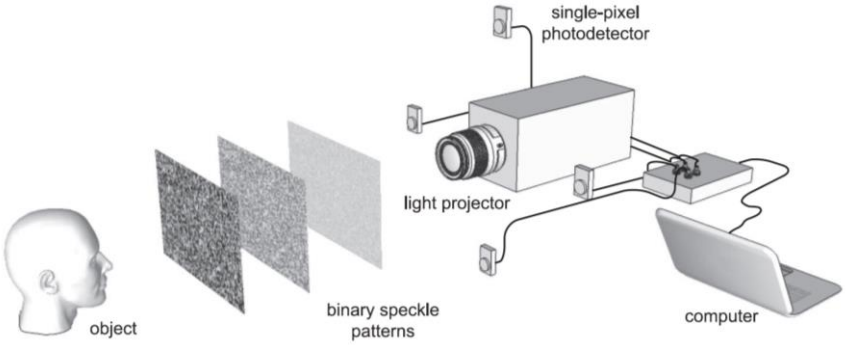


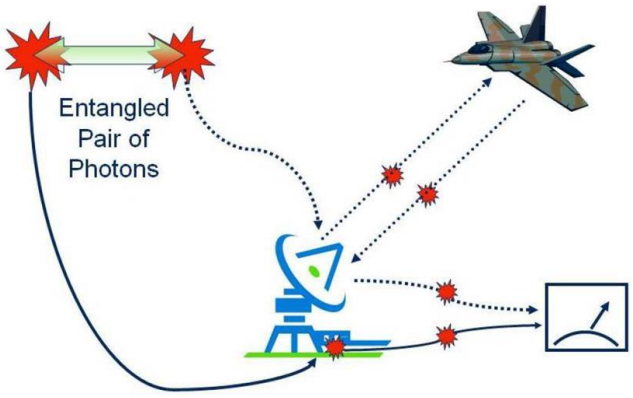
Fig. 1. Experimental setup used for 3D surface reconstructions. The light projector illuminates the object (head) with computer-generated random binary speckle patterns. The light reflected from the object is collected on four spatially separated single-pixel photodetectors. The signals from the photodetectors are measured and used to reconstruct a computational image for each photodetector.

Cela permet de générer une vue 3D de l'objet.

Radars quantiques

Les radars quantiques sont en train d'émerger lentement de la recherche. Ils s'appuient sur des photons dans le visible, et de trois manières différentes :

- Le radar émet des photons classiques dans le visible et reçoit le photon réfléchi par la cible. Cela ne fonctionne pas très bien à cause des nuages et du bruit lumineux environnant l'objet.
- Le radar émet des photons mais utilise des capteurs photo-sensibles quantiques pour améliorer sa performance. Cela ne fonctionne pas suffisamment mieux.
- Le radar prépare des paires de photons intriqués. L'un est envoyé vers la cible et réfléchi et l'autre reste dans le radar. Le photon réfléchi est comparé avec celui qui est resté sur place. Comme ils ont un passé commun, il est possible de faire le tri dans les photons reçus par le radar pour ne conserver que les photons réfléchis par la cible.



[512] Voir ce panorama de nombreux méthodes de ghost imaging : The promise of quantum imaging de Robert Boyd, 2016 (53 slides).

[513] Voir Fast full-color computational imaging with single-pixel detectors de Stephen Welsh & Al, 2013 (7 pages). Vu aussi dans 3D Computational Imaging with Single-Pixel Detectors, 2013 (4 pages) qui étend cela à la capture d'objets en 3D grâce à quatre capteurs à un pixel. Le projecteur vidéo créé des patterns qui éclairent l'objet et alternent avec leur négatif. Voir enfin Imaging with a small number of photons, Peter Morris & Al, 2014 (9 pages) et Quantum-inspired computational imaging, 2019 (9 pages).

C'est en fait une variante de la troisième manière qui est étudiée. Elle consiste à convertir les photons envoyés vers la cible en onde radio, tout en préservant une partie de leur état quantique. Une conversion du même genre a lieu pour le photon resté dans le radar. Cela permet aux ondes radar de traverser les intempéries ce que les photons dans le visible ne peuvent pas faire.

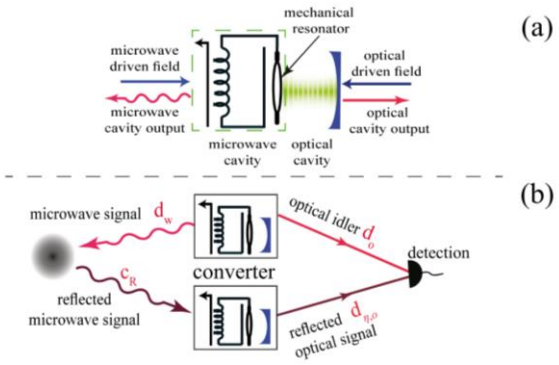


FIG. 1. (a) Schematic of the electro-opto-mechanical (EOM) converter in which driven microwave and optical cavities are coupled by a mechanical resonator. (b) Microwave-optical QI using EOM converters. The transmitter's EOM converter entangles microwave and optical fields. The receiver's EOM converter transforms the returning microwave field to the optical domain while performing a phase-conjugate operation.

Cette technique est censée améliorer la précision des radars traditionnels et d'améliorer sa résistance au bruit et au brouillage.

Ce genre de radar pourrait en théorie détecter des avions furtifs, modulo le fait que leurs surfaces réfléchissantes planes réduisent leur signature radar quelle que soit la fréquence employée. Autant dire néanmoins que cela intéresse beaucoup les Chinois qui travaillent d'arrache pied dessus pour pouvoir détecter les avions furtifs américains comme les F-22 et B-2. Ils ont annoncé avoir testé leur premier radar quantique en 2016 qui passait à l'état de prototype en 2018, réalisé par la société gouvernementale **China Electronics Technology Group**[514]. Sans que ses performances précises soient détaillées, au-delà d'une portée de 100 km.

D'autres laboratoires et entreprises mettent au point de tels radars, comme l'**Institute for Quantum Computing** de l'Université de Waterloo au Canada[515]. C'est un projet financé par le Ministère de la Défense canadien pour $2,7M. Il y en a aussi en Autriche à l'Institute of Science and Technology de Klosterneuburg. Aux USA, **Lockheed Martin** est aussi investi dans ce domaine émergent.

L'utilisation de photons intriqués permet aussi de résister efficacement aux systèmes de brouillage. Les premiers concepts ont vu le jour en 2015[516].

Elle pourrait être employée dans des LiDARs pour vérifier que les photons qui arrivent dedans correspondent bien à ceux qui ont été émis par ses lasers, échappant ainsi à un brouillage optique inopportun. Sans brouillage malintentionné, cela sera très utile lorsque de nombreux véhicules autonomes équipés de LiDARs devront cohabiter sur la route[517].

---

[514] Voir China's claim of developing "quantum radar" for detecting stealth planes: beyond skepticism par Ashish Gupta, 2016 (4 pages) qui analyse cette information avec circonspection, sans pour autant affirmer clairement que les Chinois racontent des salads sur le sujet et The US and China are in a quantum arms race that will transform warfare, par Martin Giles, janvier 2019.

[515] Voir Quantum radar will expose stealth aircraft, avril 2018.

[516] Voir Focus: Quantum Mechanics Could Improve Radar, 2015, Microwave Quantum Illumination de Shabir Barzanjeh & Al, 2015 (5 pages) qui est la source de l'illustration FIG 1, et Enhanced Sensitivity of Photodetection via Quantum Illumination par Seth Lloyd, 2018 (4 pages).

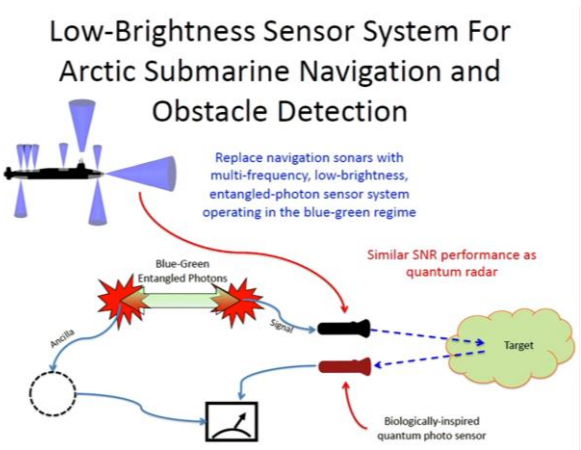
[517] Cette approche est étudiée depuis au moins 2009. Voir Quantum Lidar – Remote Sensing at the Ultimate Limit, 2009 (97 pages).

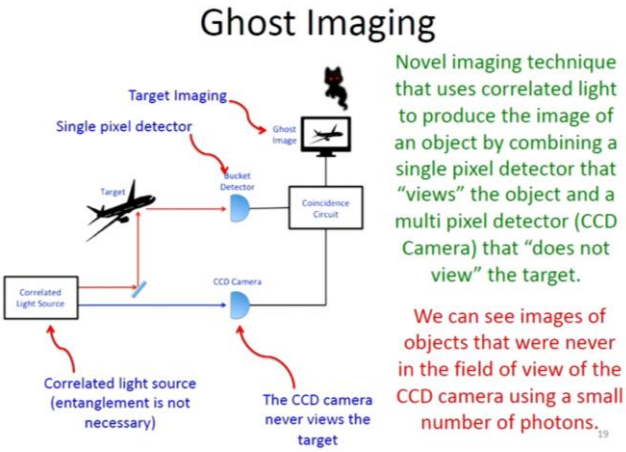
Des spécialistes du sujet comme Marco Lanzagorta de l'US Naval Researh Laboratory pensent que les satellites de QKD lancés par les Chinois comme Micius auraient des applications militaires de ce type[518].

Dans un domaine voisin des radars, les sonars quantiques pourraient aussi émerger, si l'on peut dire. Ils utilisent des photons dans la zone bleue-verte du spectre visible et seraient utilisables pour la navigation dans l'océan artique.

Ce serait en quelque sorte des LiDAR quantiques. Ces systèmes pourraient aussi mettre en œuvre une communication optique avec les sous-marins passant par satellite, histoire de remplacer les ondes radios qui pénètrent mal sous l'eau et sont exploitables pour des liaisons à très bas débit.

Autre technique envisagée, celle de la génération d'images fantômes, générée par un système couplant une caméra qui ne voit pas l'objet à capter et un capteur de pixel unique qui voit l'objet. Ce genre de technique peut s'appuyer sur l'intrication de photons dans le visible entre les deux capteurs.





Capteurs chimiques quantiques

La métrologie quantique est aussi applicable dans les capteurs chimiques qui servent à analyser la composition chimique de matériaux et substances diverses. Elle est couramment employée avec des interféromètres optiques[519].

Projets du Flasgship européen

La première phase du projet Flagship européen lancée en 2018 comprenait cinq projets de métrologie quantique que voici :

- **MetaboliQs** (Allemagne, 6,7M€) est un projet d'imagerie médicale cardiaque de résonance magnétique nucléaire à base de diamants. Il semble légèrement redondant avec le projet ASTERIQS, et réciproquement.

[518] Voir The Future of Quantum Sensing & Communications, par Marco Lanzagorta de l'US Naval Research Laboratory (USA), septembre 2018 (37 minutes). J'ai extrait deux illustrations de cette page de la vidéo de son intervention (sur les sonars et les caméras fantomes. Il est l'auteur du livre Quantum Radar qui a été traduit en chinois par la Chine, et officiellement en achetant les droits.

[519] Voir Quantum Optical Technologies for Metrology, Sensing, and Imaging de Jonathan Dowling, 2014 (20 slides) et 12 pages, Advanced Micro- and Nano-Gas Sensor Technology: A Review de Haleh Nazemi & Al, 2019 (23 pages).

- **macQsimal** (Suisse, 10,2M€) ou “Miniature Atomic vapor-Cells Quantum devices for SensIng and Metrology AppLications”, est un projet de création de capteurs quantiques visant le marché du pilotage des véhicules autonomes et pour l’imagerie médicale. Cela comprend la création d'horloges atomiques, de gyroscopes, de magnétomètres, de systèmes d'imagerie exploitant des micro-ondes et des champs électromagnétiques de l'ordre du tera-Hertz ainsi que des détecteurs de gaz.
- **ASTERIQS** (France, 9,7M€) ou “Advancing Science and Technology through diamond Quantum Sensing” est un projet de métrologie à base de diamants mené par Thales. Il devrait permettre de faire avancer les techniques de mesure de champs magnétiques, électriques, de température et de pression. Les applications sont nombreuses comme les capteurs de contrôle des batteries de véhicules, les capteurs haute résolution pour l’imagerie médicale nucléaire (RMN, résonance magnétique nucléaire). ou pour créer des analyseurs de spectre de radiofréquences. La startup suisse **Qnami** est impliquée dans le projet et fournit des diamants artificiels.
- **iqClock** (Pays-Bas, 10M€) est un projet d’horloge quantique à très haute précision.
- **PhoG** (Royaume Uni, 2,6M€) ou "Sub-Poissonian Photon Gun by Coherent Diffusive Photonics", est un projet de création de sources de lumières stables pour des applications diverses, notamment en métrologie quantique. Il implique aussi des chercheurs en Biélorussie, Allemagne et en Suisse.

Toutes ces initiatives sont des projets de recherche. A charge pour celles des parties prenantes qui sont dans le privé de les valoriser économiquement. Sachant que dans une bonne partie des cas, il s’agit de marchés d’entreprises ou d’états très spécialisés.

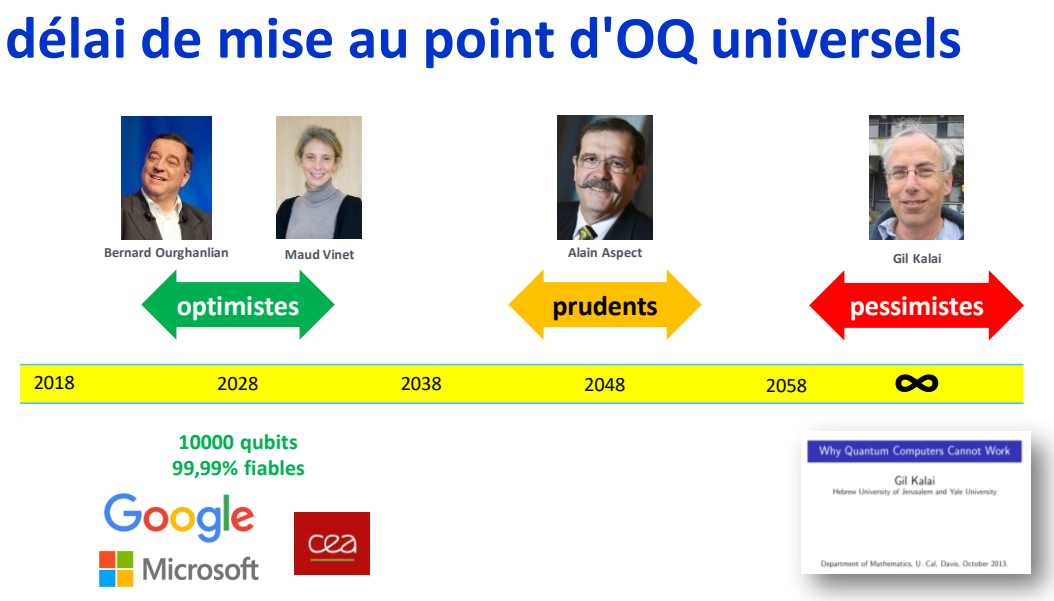
Stratégies industrielles

L'informatique quantique au sens large du terme est un secteur technologique stratégique à différents titres. Dans la cryptographie, il en va de la souveraineté avec l'enjeu de la protection des communications sensibles. Le calcul quantique est pour sa part porteur d'applications critiques qui vont étendre le champ du numérique au-delà de ce qui est faisable aujourd'hui, notamment dans le domaine de la santé, de l'environnement et de l'intelligence artificielle, prise dans une définition large.

En termes de maturité, la cryptographie quantique et post-quantique sont des champs plus établis avec des acteurs économiques et des solutions, même si la standardisation de la cryptographie post-quantique n'est pas achevée. Elle comporte cependant peu d'inconnues scientifiques fondamentales.

Le calcul quantique est moins mature. Si l'incertitude scientifique semble en partie levée pour ce qui est de la faisabilité des ordinateurs quantiques exploitables commercialement, les obstacles technologiques restent encore importants à surmonter pour y arriver, notamment l'épineuse question du bruit dans les qubits et de la correction d'erreurs quantiques.

Les avis sont partagés sur la vitesse de la levée de ces incertitudes : elle va de quelques années pour certains comme chez Google ou Microsoft, à quelques décennies pour des scientifiques comme Alain Aspect, pour atteindre le "jamais" pour des chercheurs tels que l'Israélien Gil Kalai.



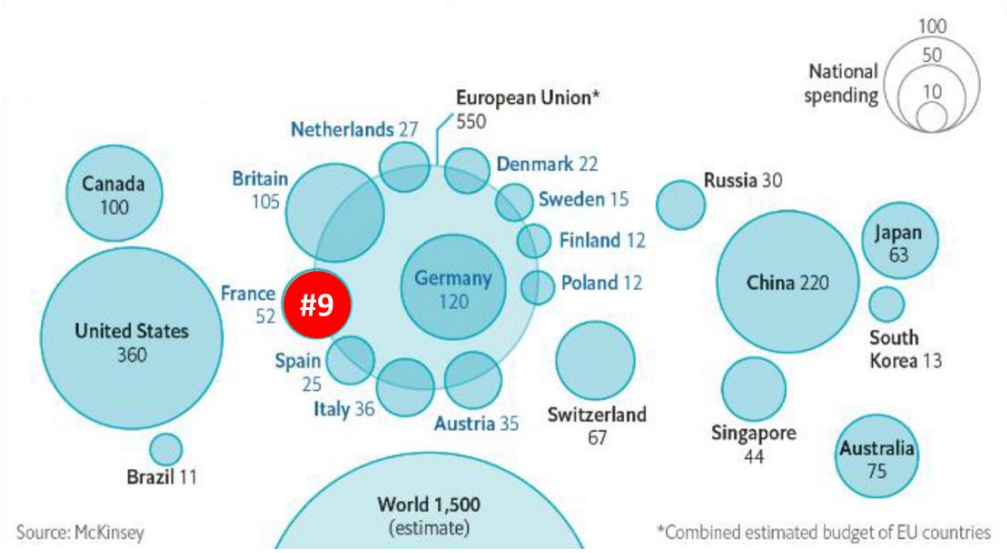
C'est donc un domaine à cheval entre l'incertitude scientifique et l'incertitude technologique. La recherche est pour l'instant issue essentiellement du secteur public dans les grands pays qui s'y investissent, puis de très grands acteurs du numérique qui ont de quoi faire plein de paris technologiques en parallèle (Google, Intel, Microsoft, IBM, Alibaba) puis de quelques startups plus ou moins bien financées ou avancées, essentiellement en Amérique du Nord (D-Wave, IonQ, Rigetti).

L'industrie des logiciels destinés aux ordinateurs quantiques est balbutiante. La majeure partie des "pure players" de ce secteur sont dédiés aux ordinateurs quantiques adiabatiques du Canadien D-Wave, tels que QxBranch et 1QBit qui sont respectivement Américains et Canadiens. Les grands acteurs et startups qui planchent sur les calculateurs quantiques ont tous investi dans le logiciel, à commencer par les outils de développement d'algorithmes et d'applications quantiques. Chacun ambitionne évidemment de créer des plateformes logicielles leaders. Certaines sont déjà disponibles dans le cloud, comme chez IBM. D'autres, tels le Français Atos et Microsoft proposent l'accès via le cloud à des simulateurs quantiques à base d'ordinateurs traditionnels.

Investissements mondiaux

Qu'en est-il des investissements mondiaux dans l'informatique quantique ? Une étude de McKinsey de 2015 faisait un tour d'horizon des investissements qui compilaient sans doute des budgets de recherche publique. Il y avait alors 1500 chercheurs dans le monde dotés d'un budget total de $1,5B. Même si ce nombre a dû augmenter depuis, il est très faible. Nous en étions en 2018 à l'état où l'informatique traditionnelle en était en 1955 !

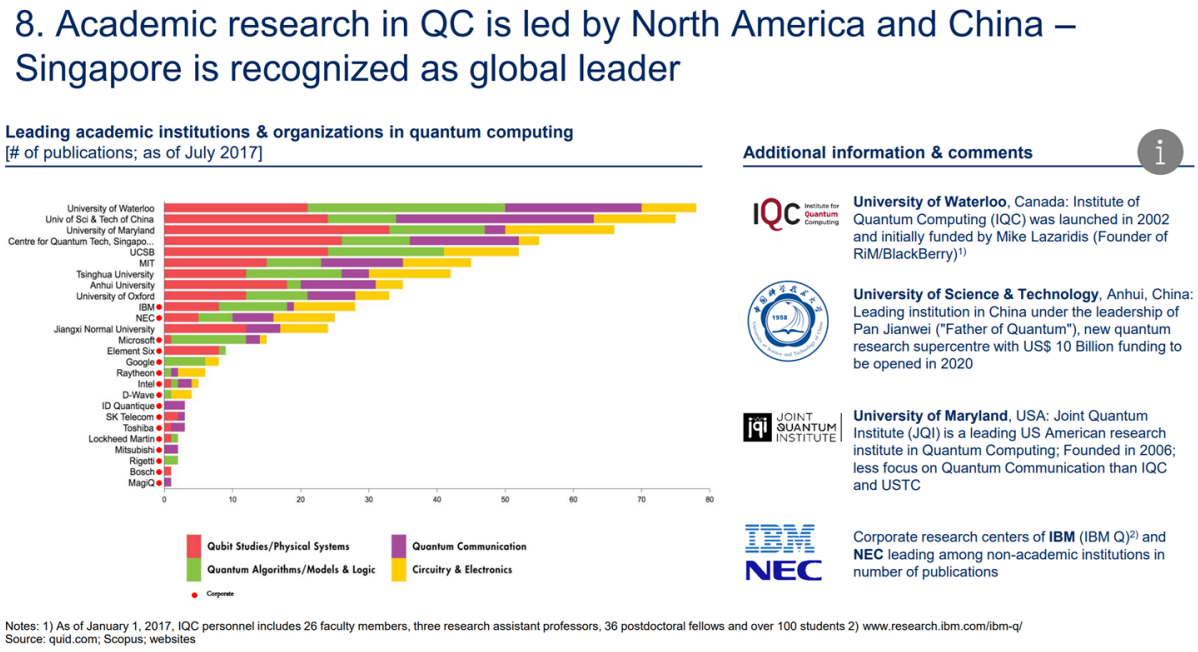
Les USA et la Chine y figuraient évidemment en tête. Mais la répartition de ces investissements, qui intègrent probablement aussi bien la cryptographie quantique que les calculateurs quantiques est intrigante pour les autres pays. La France y était en neuvième position, derrière l'Allemagne, le Royaume Uni, le Canada, le Japon la Suisse et l'Australie. Sachant que ces données ont dû évoluer depuis, avec, notamment, un accroissement significatif de l'effort de la recherche de la Chine.



Une étude européenne produite en 2016 reprenait les mêmes chiffres en y ajoutant les effectifs. Avec donc 224 chercheurs en France à comparer à 1217 chercheurs aux USA, ce qui est un ratio tout à fait normal de 1 à 6. Mais le décompte du nombre de ces chercheurs relève de la logique floue, tant il est difficile de départager ceux qui font de la recherche dans la physique fondamentale et ceux qui mettent au point des qubits. Et ces chiffres commencent à dater.

Les pouvoirs publics de ces différents pays se sont mobilisés de manière très différenciée sur le quantique. La plupart des pays développés se sont mobilisés au niveau de leurs pouvoirs publics pour coordonner les efforts dans le quantique. Un pays fait curieusement défaut dans ce panorama : la France. Nous verrons ce qu'il en est plus loin.

Une évaluation des publications scientifiques dans l'informatique quantique est présentée dans une intéressante étude produite par des étudiants de l'Insead en 2018[520]. On y découvre sans surprise que les USA, le Canada et la Chine sont les premiers pays à publier.



[520] Voir VC investment analysis Quantum Computing, 2018 (18 slides).

C'est l'effet de la masse. Mais la première Université est celle de Waterloo au Canada. Ce dernier pays est un véritable pionnier dans l'informatique quantique, et pas seulement grâce à D-Wave.

De son côté, l'**IDA**, l'Institute for Defense Analysis, une organisation parapublique US qui gère trois fonds d'investissements financés par l'état fédéral faisait un bon tour d'horizon des domaines d'applications du quantique, y compris dans le petit marché de la métrologie quantique[521].

On y trouve cet intéressant tableau qui classifie les principaux pays par dépense, publications scientifiques et dépôts de brevets, les données datant de 2016. La France y arrive en 8e à 10e position selon les indicateurs. C'est un classement habituel. On a cependant plusieurs pays dont le PIB est inférieur à celui de la France qui arrivent devant elle : le Canada et l'Australie !

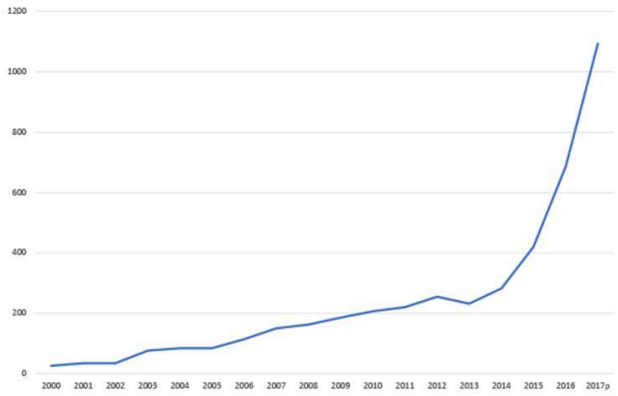
La Corée du Sud est devant la France en termes de dépôt de brevets, ce qui n'est pas une grande surprise au vu de la force de son industrie électronique, dominée par Samsung qui représente près du cinquième du PIB du pays. Une bonne partie des projets financés par les gouvernements de nombreux pays cités dans cette partie proviennent de ce document de l'IDA.

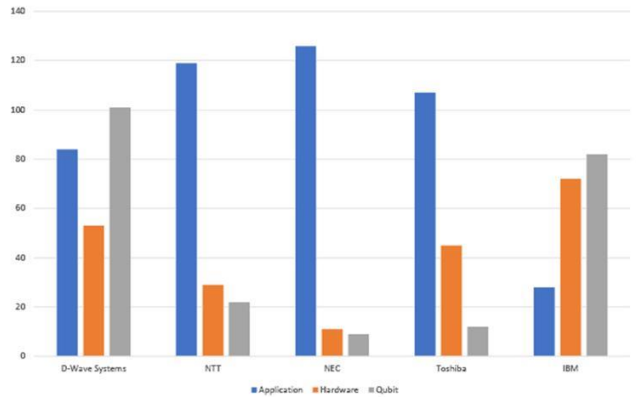
Table 5. World Ranking of Countries in Quantum Science and Technology

Country	World ranking based on spending	World ranking based on scientific publications	World ranking based on patent applications	Total world ranking
United States	1	2	1	1
China	2	1	2	2
Germany	3	3	6	3
United Kingdom	4	4	4	3
Japan	8	5	3	5
Canada	5	6	5	5
Australia	6	11	7	7
France	9	8	10	8
Italy	11	9	12	9
South Korea	17	10	8	10

Source: U.K. Government Office for Science (2016).

La recherche dans le quantique est-elle juste une affaire de gros sous ? Pas seulement. Il ne suffit pas d'aligner des milliards de dollars pour résoudre les problèmes de la matière condensée des qubits supraconducteurs. La réussite dans le quantique est aussi une question d'intégration de disciplines scientifiques nombreuses, puis de valorisation industrielle.





[521] Voir Assessment of the Future Economic Impact of Quantum Information Science, 2017 (133 pages).

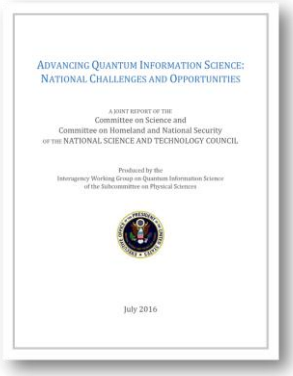
Autre vue, celle des brevets. Leur dépôt dans le quantique connaît une croissance soutenue depuis 2014. Sans grande surprise, on découvre que D-Wave est le plus gros déposant de brevets, suivi d'IBM, NEC, NTT et Toshiba, ces derniers étant pourtant plutôt discrets sur le sujet[522].

Passons à une revue de détail pays par pays, continent par continent.

Amérique du Nord

Aux **USA**, la mobilisation apparente des pouvoirs publics est plus molle ou discrète, même si elle dépasse celle de l'Europe en quantité, ne serait-ce que du fait des investissements des grands acteurs du privé dans la recherche fondamentale ou de ceux de la NSA, qui sont probablement massifs, mais confidentiels.

La coordination de la recherche dans les différentes branches du quantique a démarré en octobre 2014. A l'époque où l'on s'intéressait aux sciences à la Maison Blanche, avec un véritable conseiller scientifique du Président, John Holdren, qui a traversé les deux mandats de Barack Obama[523], celle-ci avait produit le rapport Advancing Quantum Information Science : National Challenges and Opportunities (juillet 2016, 23 pages) suivie d'une réunion de travail en octobre de la même année. Ce n'était pas un plan mais plutôt un inventaire de l'existant.



Comme presque tous les pays, le découpage du quantique y est réalisé en quatre parties : la communication quantique, la métrologie quantique, le calcul quantique et les simulateurs quantiques, la distinction entre ces deux derniers étant subtile.

L'état fédéral finance des projets de recherche de startups avec des financements issus du programme SBIR, l'une des composantes du fameux Small Business Act. Cela concerne notamment **Axion Technologies** qui a créé un générateur de nombres aléatoires concurrent de ceux du Suisse IDQ.

Les laboratoires publics qui investissent dans l'informatique quantique traversent à peu près tout le complexe militaro-industriel fédéral avec de la recherche interne ou de la recherche externe subventionnée sur appels à projets :

- La **DARPA** finance trois programmes dans le quantique, dans les communications quantiques à longue distance, dans la métrologie quantique appliquée à l'imagerie ainsi que dans le diagnostic de traumatismes neurologiques et le PTSD.

[522] Voir Quantum Computing and Beyond: Can Patent Landscaping Predict the Future?, juillet 2018.

[523] Le remplaçant de John Holdren était nommé par Donald Trump après 18 mois de Présidence, un certain Kelvin Droegemeier, un météorologiste qui a même obtenu l'aval de son prédécesseur ce qui est plutôt rare dans cette Administration.

Les financements vont à des projets menés par des Universités, startups et entreprises établies.

- L'**IARPA** (Intelligence Advanced Research Projects Agency) que nous avons déjà eu l'occasion de citer plusieurs fois finance des projets tiers sur les calculateurs et les algorithmes quantiques, notamment dans l'entrainement de réseaux de neurones, dans le test de circuits. Leur programme LogiQ vise à améliorer la qualité des qubits. L'IARPA finance également des programmes conduits par des entités tierces.
- La **NSA** investit beaucoup dans le quantique à la fois dans la course à la mise en œuvre de l'algorithme de Shor pour décrypter les communications protégées par clés publiques de type RSA et pour protéger les communications sensibles avec clés et cryptographie quantiques. Ses travaux ne sont évidemment pas publics. La NSA sous-traite également une partie de sa recherche à des entreprises privées telles que Lockheed-Martin.
- L'**US Air Force** et son Quantum Communications qui est focalisé sur la cryptographie quantique (QKD). Un autre laboratoire fait de la recherche appliquée dans les qubits supraconducteurs et étudie l'application des algorithmes quantiques à ses besoins opérationnels.
- L'**Office of Naval Research** (ONR) travaille sur les usages des QKD pour la marine et sur l'exploitation d'algorithmes quantiques liés aux besoins opérationnels de la marine.
- L'**Army Research Office** a aussi son propre programme de recherche dans le quantique couvrant tout le spectre allant de la métrologie au calcul quantique en passant par la cryptographie et les communications quantiques.
- La **NASA** a créé en 2013 le Quantum Artificial Intelligence Laboratory (QuAIL) conjointement avec Google au Ames Research Center à proximité du siège de ce dernier à Mountain Views pour explorer le champ des algorithmes quantiques, en particulier sur un ordinateur quantique adiabatique de D-Wave qu'ils ont installé à cette époque là.
- Le **Los Alamos National Laboratory** (LANL) a un Quantum Institute (QI) lancé en 2002 qui investi aussi dans l'informatique et la cryptographie quantique. Ils financent notamment des recherches de l'UNSW en Australie ainsi que dans celle du Maryland. Ce laboratoire est financé par le Département de l'Energie (DoE). Ce dernier finance également le **Sandia National Laboratories** qui conduit aussi de la recherche appliquée tout azimut dans le quantique.
- La **NSF** finance des projets de recherche divers, un peu comme l'ANR en France. A noter deux initiatives de recherche collaborative aux USA : la **National Photonics Initiative** lancée en 2013 et la proposition d'une **National Quantum Initiative** évoquée en 2017 avec un financement fédéral demandé par les scientifiques de $500M sur cinq ans.

En 2018, la communauté scientifique US s'inquiétait toutefois d'un risque de perte de leadership des USA sur le sujet comme le soulignait cette note de l'Ambassade de France aux USA d'avril 2018. Vis à vis de l'Europe ? Non ! De la Chine qui investit massivement dans le quantique.

La Chambre des Représentants US a même organisé autour de ce sujet une audition en octobre 2017 (vidéo). Durant trois heures, on y voit des élus interroger une brochette de scientifiques dont James Kurose de la NSF et John Stephen Binkley du Département de l'Energie, qui leur expliquent les basiques des qubits et les enjeux de souveraineté associés. Les élus démocrates s'y inquiétèrent des coupes budgétaires proposées par l'administration Trump dans le financement de la recherche civile, au profit d'augmentations du budget de la défense et de réductions d'impôts.

In fine, le Congrès US a au contraire solidement augmenté les budgets de la recherche fédérale sur l'année fiscale 2018 (source), sachant que ceux-ci sont ensuite traditionnellement fléchés pour l'essentiel vers des organismes privés, notamment les laboratoires des grandes universités américaines. Avec +8,3% pour le NIH (santé), +3,9% pour la NSF (recherche généraliste), +15% pour la recherche au DoE (énergie), +,7,9% pour les programmes scientifiques de la NASA et +26% pour le NIST qui gère les standards et travaille notamment sur la cryptographie quantique. C'est un des rares cas où le Congrès contrôlé par les Républicains s'est opposé à l'administration Trump.

La commission des sciences de la Chambre des Représentant introduisait le 26 juin 2018 le **National Quantum Initiative Act** (H.R. 6227, 25 pages) qui ambitionne de sédimenter les objectifs, les responsabilités et les moyens publics autour du quantique. Une proposition équivalente était déposée au Sénat le même jour.

Ce projet de loi proposait de mobiliser $1,275B sur cinq ans pour financer la R&D civile dans le quantique, répartis au Département de l'Energie ($625M), à la NSF ($250M) et au NIST qui est focalisé sur les questions de cryptographie ($400M). Lorsque l'on fait les comptes, cela ferait passer les investissements annuels de $200M à $255M, ce qui semble modeste, mais ce dernier montant n'intègre pas les fonds alloués à la NSA et au Département de la Défense.

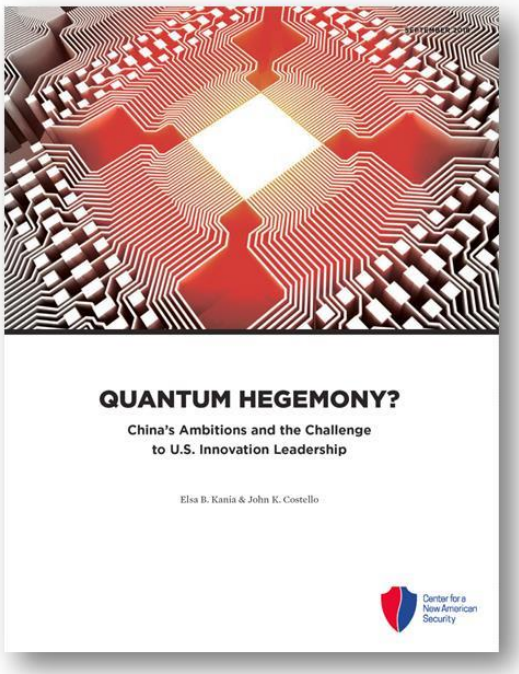
Ce National Quantum Initiative Act propose la création d'un National Quantum Coordination Office au sein de l'Office of Science and Technology Policy qui a maintenant son nouveau dirigeant en place. Il demande au Président des USA de créer un plan à 10 ans sur le quantique, avec une première étape devant être un plan de 5 ans livrables un an après le vote de la loi. Pas sûr que cela soit une grande priorité du Président, plus préoccupé par la construction de son mur-frontière avec le Mexique !

Ce projet n'est évidemment pas tombé du ciel. Il résulte d'une proposition, le National Quantum Initiative—Action Plan, préparée par des intervenants de la recherche publique et du privé (IBM, Google, Rigetti). Elle comprend d'ailleurs une promesse un peu délirante sur le calcul quantique, qui permettrait un jour de trier des bases de données trop grandes pour être stockées dans des ordinateurs conventionnels.

Une erreur magistrale quand on sait que les qubits n'ont pas les capacités de stockage d'information qu'on leur prête ! On confond toujours abusivement la notion de superposition d'états des qubits avec une supposée capacité de stockage d'information.

En fait, ce projet de loi a été poussé par les élus car ils craignent que la Chine prenne le dessus sur le quantique, notamment dans la sécurité informatique. Les USA aiment se faire peur.

Mais dans le domaine du quantique, ils n'ont pas à rougir : ils ont une densité de laboratoires de recherche publics et privés sans égal, leurs grands acteurs ont une capacité d'industrialisation à grande échelle que quasiment aucun pays ne peut concurrencer et leur marché intérieur reste le plus grand au monde pour les applications informatiques d'entreprise, là par où le quantique va démarrer.



President Trump has signed a $1.2 billon law to boost US quantum tech december 21st, 2018

The new National Quantum Initiative Act will give America a national master plan for advancing quantum technologies.

The news: The US president just signed into law a bill that commits the government to providing $1.2 billion to fund activities promoting quantum information science over an initial five-year period. The new law, which was signed just as a partial US government shutdown began, will provide a significant boost to research, and to efforts to develop a future quantum workforce in the country.

The background: Quantum computers leverage exotic phenomena from quantum physics to produce exponential leaps in computing power. The hope is that these machines will ultimately be able to outstrip even the most powerful classical supercomputers. Those same quantum phenomena can also be tapped to create highly secure communications networks and other advances.

Ce projet de loi de la Chambre des Représentants était voté en plénière le 13 septembre 2018[524] puis par le Sénat en décembre 2018. La Maison Blanche avait publié en septembre 2018 un document qui reprend les termes de la proposition du Congrès, dans le National Strategic Overview for Quantum Information Science. Ils insistaient notamment sur la recherche, sur la formation des scientifiques et sur la collaboration internationale. Donald Trump a ensuite signé sans broncher et plutôt en cati-mini cette loi le 21 décembre 2018[525].

[524] Voir SIA Welcomes House Passage of Quantum Computing Legislation, septembre 2018.

[525] Voir President Trump has signed a $1.2 billon law to boost US quantum tech, par Martin Giles dans la MIT Technology Review, décembre 2018. Dans la signature dans le bureau oval, le Président est entouré de sa fille Ivanka Trump et par deux conseillers scientifiques de la Maison Blanche. Aucun représentant de l'écosystème de la recherche quantique ou du Congrès n'est présent. Le lendemain démarrait le fameux « shutdown » qui dura 35 jours, provoqué par ce même Président !

Il est probable que ces conseillers n'ont pas passé beaucoup de temps à expliquer le fonctionnement de l'informatique quantique au Président. Il était plus simple pour eux de mettre en avant les avancées de la Chine dans le domaine et le risque que cela fait peser sur les USA[526].

Un peu avant, le **NIST** avait décidé de créer avec **SRI International** (l'ancien laboratoire de valorisation industrielle de Stanford) le consortium **Quantum Economic Development Consortium** (QEDC) destiné à développer l'industrie quantique américaine dans les domaines de la communication et de la métrologie[527]. Ce QECD sera probablement un bon réceptacle des fonds destinés à la recherche du plan des deux chambres du Congrès signé par Donald Trump en décembre 2018.

On peut faire un parallèle entre l'intelligence artificielle et l'informatique quantique pour ce qui concerne ce pays.

Dans les deux cas, son influence du secteur est bien plus grande que le poids économique du pays, aussi bien au niveau de la recherche fondamentale que des entreprises. C'est notamment dû à un investissement constant et en avance de phase du gouvernement dans la recherche et à un dynamisme entrepreneurial certain.

Le Canada se distingue par un fort investissement dans la recherche fondamentale dans l'informatique quantique, notamment avec plus de $1B d'investissements publics sur une décennie répartis principalement dans trois institutions[528] :

- L'Institute for Quantum Computing de l'**Université de Waterloo**, proche de Toronto. L'Université de Waterloo a obtenu en 2017 un budget de $120M pour ses différents instituts de recherche dans le quantique. Etonnamment, elle a aussi obtenu un financement australien de $53M provenant de l'UNSW, de l'opérateur Telstra et de la Commonwealth Bank of Australia. L'IQC fait à la fois de la recherche et de l'enseignement. Ils proposent notamment des formations courtes de une à deux semaines en été sur la crypto et le calcul quantiques.

---

[526] Voir The Race to Develop the World's Best Quantum Tech de Jeremy Tsu dans IEEE Spectrum, décembre 2018, qui évoque le rapport Quantum Hegemony - China's Ambitions and the Challenge to U.S. Innovation Leadership du CNAS publié en septembre 2018 qui décrit la stratégie quantique de la Chine (52 pages). Voir aussi US intelligence community says quantum computing and AI pose an 'emerging threat' to national security de Zack Whittaker, décembre 2018.

[527] Voir NIST Launches Consortium to Support Development of Quantum Industry, septembre 2018. Et plus de details dans U.S. Consortium Pulls Ecosystem Into Quantum par Susan Rambo, août 2019.

[528] Voir Quantum Canada, par Ben Sussman, Paul Corkum, Alexandre Blais, David Cory et Andrea Damascelli, février 2019 (6 pages) qui fait le point sur les investissements quantiques dans le pays.

- Le Quantum Matter Institute (QMI) de l'**University of British Columbia** située principalement à Vancouver.
- L'Institut Quantique de l'**Université de Sherbrooke**, près de Montréal.

Le Canada a deux stars quantiques dans la recherche avec Gilles Brassard de l'Université de Montréal qui est avec Charles Bennett d'IBM Research le coinventeur du protocole BB84 de QKD introduit en 1984.

Du côté entrepreneurial, ils ont en tête de pont le fameux **D-Wave** ainsi que le spécialiste des logiciels quantiques, **1QBit**. Les financements privés notables comprennent surtout les donations de Michael Lazaridis, un des cofondateurs de RIM BlackBerry, avec $75M à l'**Institute for Quantum Computing** de l'Université de Waterloo et $128M en 1999 au **Perimeter Institute for Theoretical Physics** qui est aussi situé à Waterloo. Avec Doug Fregin, également cofondateur de RIM, ils ont également créé le Quantum Valley Investment Fund avec un financement total de $100M.

Europe

C'est le **Royaume-Uni** qui semble s'être mobilisé le premier en Europe, et ce, dès 2013 avec le plan The UK National Quantum Technologies Programme Current and Future Opportunities de Derek Gillespie (version print), de l'Engineering and Physical Sciences Research Council (EPSRC), un organisme non gouvernemental financé par les derniers publics et sous la supervision de l'exécutif.

C'est une sorte d'équivalent britannique de notre Agence Nationale de la Recherche et qui finance des projets de recherche. Le plan UK vise tous les marchés habituels du quantique : métrologie, calcul, sécurité et imagerie médicale.

Son rapport d'étape de 2015 montre que l'approche est assez symbolique avec des montants publics investis assez modestes, de l'ordre de 100M€ étalés sur plusieurs années et sur plusieurs hubs d'innovation. Mais le timing est plutôt bon ! Le plan initial prévoyait d'investir £270M sur 5 ans avec un objectif de valoriser les travaux de recherche dans des startups aussi rapidement que possible. Le gouvernement anglais se préoccupe surtout du transfert de technologies des laboratoires vers les entreprises.

Le plan UK prévoit la création d'un réseau de hubs d'innovation dans le quantique, avec les thématiques habituelles : métrologie (avec les Universités de Birmingham, Glasgow, Nottingham, Southampton, Strathclyde et Sussex), les télécommunications quantiques et le calcul quantique. Il se distinguait avec un effort préemptif dans la formation avec notamment celle de doctorants financée à hauteur de $210 sur deux ans.

En juin 2019, le Royaume-Uni annonçait un nouveau plan de financement de $193M destiné à financer la commercialisation d'ordinateurs quantiques[529], avec les investissements prévus du secteur privé, le total serait de $1,227B. Dans le cadre de ce plan, leur Strategy Challenge Fund organisera des concours et appels à projets pour financer des projets de recherche et d'industrialisation, à l'image de ce que Bpifrance et la DGE font régulièrement en France (mais pas encore sur le quantique).

Côté recherche, de nombreux laboratoires sont impliqués dans le quantique, notamment à **Oxford** (avec le hub NQIT, sur le calcul et la sécurité et l'initiative QuOpaL - Quantum Optimisation and Machine Learning financée par Nokia et Lockheed Martin), **Cambridge** (Centre for Quantum Information and Foundations, qui planche sur la partie physique comme mathématique du quantique), **Glasgow** (avec le hub Quantic, spécialisé dans l'imagerie), **York** (avec un hub sur la communication quantique, donc sur des QKD) et **Bristol** (Quantum Engineering Centre for Doctoral Training, focalisé sur la formation ainsi que sur la photonique).

Du côté entrepreneurial, on peut citer **Oxford Instruments** (cryogénie), **Oxford Quantum Circuits** (qubits supraconducteurs), **Quantum Motion Technologies** (qubits CMOS), **Cambridge Quantum Computing** (système d'exploitation, logiciels, services), **TundraSystems** (qubits photoniques) et **River Lane Research** (logiciels). Aucune grande entreprise UK ne semble être particulièrement investie dans l'informatique quantique.

La **Suisse** est aussi mobilisée sur le quantique, notamment à l'**Université ETH** de Zurich qui collabore d'ailleurs avec IBM et surtout autour de la cryptographie quantique, notamment avec sa startup **IDQ** qui est leader de la génération de nombres aléatoires utilisée dans la crypto quantique.

Le pays a publié un manifeste de promotion de ses efforts de recherche et industriels dans le quantique, Switzerland: At the Quantum Crossroads. Le **Swiss Quantum Hub** fédère de son côté l'écosystème suisse du quantique.

L'initiative **Quantum Science and Technology** (QIST) commune à l'ETH Zurich et l'Université de Bâle et qui associe aussi l'Université de Genève et l'EPFL de Lausanne comprend 34 enseignants et 300 étudiants. Elle a été financée à hauteur de $120M entre 2010 et 2017.

[529] Voir UK government invests $194M to commercialize quantum computing de Frederic Lardinois.

Elle couvre tous les domaines habituels du quantique avec, semble-t-il, un effort plus particulier dans les télécommunications quantiques.

En **Allemagne**, l'agence fédérale qui protège les systèmes d'information homologue de l'ANSSI française a publié en mai 2018 le rapport Entwicklungsstand Quanten-computer (*état des lieux de l'informatique quantique*) qui fait un point sur l'informatique quantique, focalisé notamment sur les questions de cybersécurité (231 pages, en anglais). Cet excellent document a été créé par une demi-douzaine d'universitaires allemands faisant de la recherche à l'Université de Saarland à Sarrebruck et à l'Université de Floride à Boca Raton aux USA. Ce sont des physiciens spécialistes de la matière condensée et des qubits supraconducteurs, des mathématiciens et des spécialistes de la cybersécurité.

C'est l'un des meilleurs tours d'horizon de la recherche mondial en informatique quantique que j'ai pu consulter. Il fait un inventaire étonnamment précis des efforts dans le domaine, notamment dans la recherche publique US.

Les principaux laboratoires de recherche impliqués de manière visible dans le quantique sont le **Max Planck-Institute for Quantum Optics** (MPQ, qubits à base d'atomes neutres) situé près de Munich, puis l'**Institute for Quantum Control** et l'**Institut für Quanteninformation** d'Aix La Chapelle (recherche au niveau de la physique dans les qubits supraconducteurs et en silicium quantum-dots), l'**Institute for Complex Quantum Systems** de l'Université d'Ulm entre Stuttgart et Munich et le laboratoire quantique de **Jülich Forschungszentrum** (situé entre Aix-la-Chapelle et Cologne et piloté par Kristel Michielsen[530]).

En septembre 2018, le Ministère de la Recherche du gouvernement fédéral allemand annonçait un financement de 650M€ dans les technologies quantiques étalé sur quatre ans (2018 à 2022)[531]. Comme tous les plans du genre, il finance des projets dans le calcul quantique, dans la communication quantique et dans la métrologie quantique.

En septembre 2019, l'Allemagne annonçait un nouveau plan de 650M€ dans le quantique associant **IBM** et l'Institut **Fraunhofer-Gesellschaft**. Il doit s'étaler jusqu'en 2022 et semble faire doublon avec le plan annoncé un an avant. IBM va installer un ordinateur quantique en Allemagne qui sera exploitable pour les chercheurs dans le cloud. Il n'est pas certain que ce soit la meilleure approche pour développer une industrie allemande et européenne du quantique, tout du moins du côté du matériel.

---

[530] Jülich Forschungszentrum est un peu l'équivalent du CEA en Allemagne. Il avait démarré en 1956 dans la recherche nucléaire. Il héberge aussi de nombreux supercalculateurs, à l'instar de la DAM du CEA à Bruyère le Chatel.

[531] Voir German Government Allocates 650M€ for quantum technologies, l'annonce du gouvernement allemand (en allemand) et le plan lui-même (51 pages).

L'Allemagne est située juste derrière la France avec huit startups dans le quantique dont **InfiniQuant** (cryptographie CV-QKD), **PicoQuant** (compteurs de photons), **Kiutra** (cryogénie sans hélium 3), **HQS Quantum Simulations** (algorithmes), **JoS Quantum** (logiciels dans la finance), **Quantum Factory** (ions piégés dans le cloud), **QuantiCor Security** et **QuBalt** (tous deux dans la post-quantum cryptography).

Les **Pays-Bas** sont aussi actifs dans le quantique, principalement autour de l'Université de Delft (**TU Delft**). Le gouvernement lançait en 2015 un plan de création d'ordinateur quantique étalé sur 10 ans et doté de 135M€. L'investissement était fait dans **QuTech**, le centre de recherche quantique de TU Delft dont le budget sur 10 ans est de 145M€. Cf le rapport d'activité 2017 de QuTech. Qutech occupe plus de 180 personnes en tout dont 37% de Hollandais.

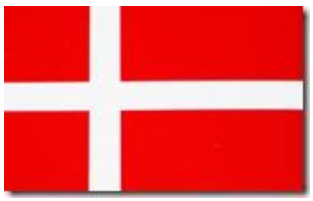
QuTech est aussi associé à **Intel** et **Microsoft**. QuTech a reçu un financement de $50M en 2015 d'Intel dans le cadre d'un partenariat sur leurs qubits supraconducteurs. Microsoft est aussi partenaire de QuTech, ce depuis 2010, qu'ils ont d'ailleurs déplumé en embauchant Leo Kouwenhoven dans leur laboratoire de Microsoft Research qui est sur place et planche sur le quantique topologique et le fermion de Majorana en liaison avec une équipe de QuTech dédiée au même sujet.

On peut dire que les Pays-Bas se positionnent donc pour l'instant comme réservoir à cerveaux pour l'industrie quantique américaine. Dans la pratique, c'est à cela que mènent leurs investissements dans la recherche.

Les approches de recherche collaborative vont bon train, notamment dans l'optique de récupérer des financements européens. En octobre 2017, QuTech lançait un partenariat avec l'Institute of Photonic Sciences, l'Université d'Innsbruck en Autriche et le Paris Centre for Quantum Computer. QuTech est aussi partenaire de l'Université d'Aix la Chapelle dans le qubit CMOS.

D'autres initiatives aux contours flous ont été lancées comme **Quantum Helix**, qui ambitionne d'être financée dans le cadre du programme flagship quantique européen et Horizon 2020. Un autre programme dénommé **Quantum Software Consortium** devant durer 10 ans à partir de 2017 a reçu 18,8M€ de financements publics du pays dans le cadre du Gravitation Program. Il associe divers laboratoires hollandais : **TU Delft**, **QuTech** (qui fait partie de cette dernière), **QuSoft** (laboratoire de recherche dédié aux logiciels quantiques, lancé par CWI, UvA et VU en 2015), **CWI** (*Centrum Wiskunde & Informatica*, l'équivalent hollandais de l'Inria français), l'**Université de Leiden**, **UvA** (Université d'Amsterdam) et **VU** (Université libre d'Amsterdam) pour mener de la recherche en logiciels quantiques et en cryptographie.

Sinon, côté entreprises, j'ai juste identifié une startup, **Delft Circuits**, spécialisée dans la fabrication de circuits supraconducteurs.



L'investissement de l'**Autriche** dans l'informatique quantique est concentré dans l'**IQOQI**, l'Institut für Quantenoptik und Quanteninformation d'Innsbruck et Vienne. Il se focalise en particulier dans la conception de qubits à base d'ions piégés. En est issue la startup **Alpine Quantum Technologies**, créée par Rainer Blatt de l'IQOQI, pour commercialiser des ordinateurs quantiques à ions piégés. Elle a bénéficié de financements publics à hauteur de 12,3M€. Elle concurrence la startup américaine **IonQ** issue de l'Université de Maryland qui est positionnée sur le même créneau des qubits à ions piégés.

Le **VQC** (Vienna Center for Quantum Science and Technology) est issu d'un partenariat entre l'Université de Vienne, l'Université de Technologie de Vienne et l'Académie des Sciences d'Autriche. Il regroupe une masse critique d'une vingtaine de laboratoires de recherche en physique quantique.

L'Autriche est aussi investie dans la cryptographie quantique et associée avec la Chine, avec qui elle a mené des expériences d'envoi de clés quantiques par le satellite Micius pour mettre en place une communication vidéo sécurisée. L'**IQOQI** collabore aussi avec le **Centre Spatial Universitaire de Grenoble** (CSUG) dans la mise au point d'un satellite de relai de clés quantiques de type CubeSat, similaire à celui de Singapour, dans le projet **Nanobob** (présentation, 13 slides).

La recherche dans le quantique au **Danemark** est organisée autour du Center for Quantum Devices (**QDev**) de l'Institut Niels Bohr de l'Université de Copenhague.

C'est un laboratoire de qualité focalisé notamment sur les qubits topologiques, avec son dirigeant Charles M. Marcus qui travaille aussi pour Microsoft Research dans cette filière conjointement avec les équipes de MSR de Leo Kouwenhoven aux Pays-Bas. QDev est un laboratoire de physiciens focalisé sur l'étude de la matière condensée, à savoir les couches basses physiques des qubits, comme on peut l'observer dans leurs publications.

L'équipe semble ne faire qu'une dizaine de personnes. Ils ne peuvent malheureusement pas s'appuyer ensuite sur des industriels danois ou européens pour envisager le transfert de leur recherche dans la production d'ordinateurs quantiques. C'est un problème français mais aussi européen !

L'**Espagne** a quelques cordes quantiques à son arc. Côté recherche, l'essentiel des efforts est concentré dans l'**ICFO** (Instituto de ciencias fotónicas) de Barcelone qui est surtout spécialisé en photonique. D'autres recherches dans le quantique sont menées au laboratoire Quantum Information and Computation (GIC-UB) de l'**Université de Barcelone** ainsi que dans le Grup d'Informació Quàntica (GIQ) de l'**Université Autonome de Barcelone**.

Du côté du privé, ils ont une startup, **Qilimanjaro Quantum Hub** déjà citée, qui développe surtout une plateforme logicielle quantique en cloud, ainsi que **Entanglement Partners**, un prestataire de services qui arrive visiblement à vendre des prestations dans le domaine de la cybersécurité liées au quantique. Ils animent sinon l'écosystème du pays, font de l'évangélisation et organisent des événements.

En 2017, la plateforme d'innovation ouverte **Open Trends** lançait **The Carrot Cake** pour encourage les projets dans le quantique. Ceci complète le think tank **Barcelona QBIT** lancé en 2015 ainsi que la **Quantum World Association** lancée au MWC 2017 qui associe la Suisse, le Canada, l'Australie et la Catalogne avec notamment les startups ID Quantique, evolutionQ, h-bar et Entanglement Partners. L'Espagne travaille en réseau, ayant compris que toute seule elle ne pourrait pas aller bien loin.

La **Pologne** a notamment un Centre de recherche en physique quantique à Gdansk qui est focalisé sur la cryptographie quantique. Il a été lancé en 2007. L'Université de Varsovie est également très impliquée dans la recherche quantique.

Le National Science Centre polonais coordonne aussi le réseau de recherche international **QuantERA** lui-même financé par les budgets Europe 2020 de l'Union Européenne. Il fait cela en coordination avec l'ANR française. Les pays impliqués, outre ceux de l'Union Européenne sont la Suisse, Israël (Université Bar-Ilan) et la Turquie.

Une trentaine de projets de recherche avaient été financés après un appel à projets en 2017, certains s'étant ensuite retrouvés financés dans le Flagship quantique européen, comme SQUARE. Ce sont tous des projets de physique quantique (photonique, atomes froids, ..).

Le quantique est un domaine où l'**Union Européenne** se mobilise collectivement. Initié en 2016, un "flagship project" a germé en 2016 et était formellement lancé en 2018 pour financer de la recherche collaborative sur l'ensemble des pans de l'information quantique : métrologie, communications, calcul et simulation quantiques[532].

Il est doté *en théorie* de 1 Md€ servant aux programmes de développement et de diffusion des technologies quantiques, étalés sur 10 ans. En théorie car les budgets n'ont pas été véritablement alloués à ce niveau par l'Union Européenne. Ils le sont par tranches étalées dans le temps.

Le flagship est surtout focalisé sur les couches physiques fondamentales de l'informatique quantique. Il est dommage qu'il ne prenne pas aussi bien en compte la dimension algorithmique et logicielle de l'informatique quantique qui est un domaine où l'Europe pourrait se distinguer. Il semblerait qu'il faille attendre pour cela les prochains appels d'offre du flagship.

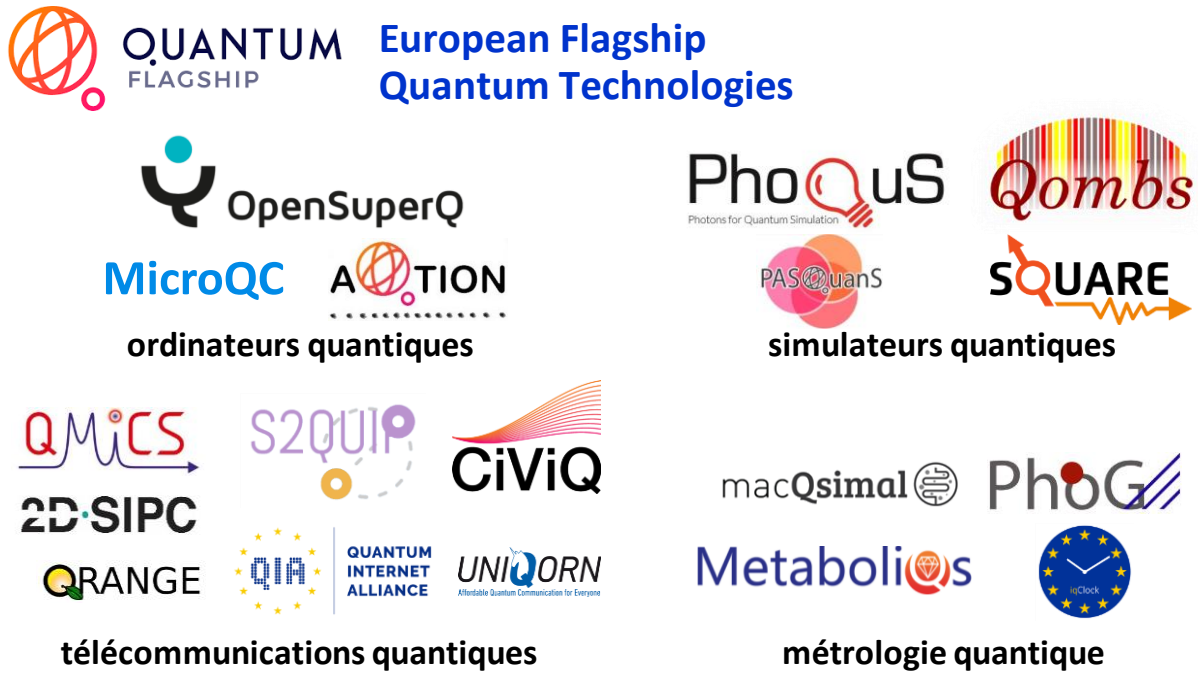
Ce **Quantum Technologies Flagship** est un des trois "flagships" européens qui visent à placer l'Europe en tête de pont de ruptures technologiques majeures avec un fort investissement communautaire dans la recherche. Le ticket de base est de 1 milliard d'Euros, étalés sur plusieurs années. Les deux autres Flagship sont le "Human Brain Project" piloté par le Suisse Henri Markram et le projet Graphene dans les nanotechnologies.

La première phase du Flagship a été annoncée en octobre 2018. Elle comprend une première tranche de 132M€ alloués à 20 projets sélectionnés sur 140 candidats. Ce montant couvre trois années de besoins. A terme 130 projets supplémentaires seront sélectionnés dans le cadre d'appels à projets complémentaires. Lancé par la Commission Européenne le 29 octobre 2018 à Vienne (vidéos), le programme couvre quatre secteurs : le calcul quantique, la simulation quantique, la communication quantique et la métrologie quantique. Cette répartition est assez habituelle et on la retrouve dans les plans de pays comme les USA ou la Chine[533].

---

[532] Voir les motivations qui ont about it à ce Flagship : The Impact of quantum technologies on the EU's future policies: Part 1 Quantum Time, 2017 et Part 2.

[533] Voir le Dossier de Presse (28 pages), la liste complète des projets et L'Europe accélère l'industrialisation des technologies quantiques du 31 octobre 2018, dont le titre est quelque peu trompeur dans la mesure où la majorité des projets financés sont des projets de recherche et pas des projets d'industrialisation. Et puis aussi The quantum technologies roadmap: a European community view, octobre 2017 (25 pages) qui fait un point sur l'état de l'art en Europe et dans le monde. Voir aussi The EU Quantum Technology Flagship par Elisabeth Giacobino, 2018 (41 slides et vidéo).



Parcourons la liste de ces projets financés dans cette première tranche. A chaque fois, j'indique le pays leader du projet et les montants européens accordés au projet. Ces projets impliquent en moyenne au minimum une demi-douzaine d'autres pays européens, voire limitrophes comme la Suisse et même Israël. Il n'est pas toujours facile d'obtenir la liste des parties impliquées dans les projets.

Cela commence avec trois projets côté liés au calcul quantique, probablement l'aspect le plus stratégique du plan et pourtant le moins bien représenté et financé :

- **OpenSuperQ** (Allemagne, 10,33M€) est un projet d'ordinateur quantique à base de supraconducteurs, piloté par l'Université de Saarlandes. Le projet associe également l'Espagne, la Suède, la Suisse et la Finlande et en tout 10 laboratoires de recherche. C'est une filière classique et la concurrence industrielle est rude avec Outre-Atlantique, au minimum, IBM, Google, Intel et Rigetti. L'ambition est de créer dans un premier temps un ordinateur quantique supraconducteur à 100 qubits. Pour mémoire, Rigetti pensait arriver à 128 qubits en 2019. Il semblerait que ce projet consiste surtout à créer un calculateur quantique disponible via le cloud, et focalisé sur des recherches en chimie. En étant mauvaise langue, c'est une sorte de Cloudwatt du quantique.
- **AQTION** (Autriche, 9,57M€) est un projet d'ordinateurs quantiques à base d'ions piégés qui vise une capacité de 50 qubits. L'Autriche a un long historique sur le sujet et y est tout à fait légitime. Elle fait notamment face à IonQ, une startup issue de l'Université de Maryland aux USA. Atos participe à ce projet.
- **MicroQC** (Bulgarie, 2,36M€) pour la création d'un autre ordinateur quantique à base d'ions piégés. Ce projet de recherche est moins connu. Mais on sent l'approche européenne consistant à ne pas défavoriser les membres les plus récents de l'Union Européenne.

Nous avons ensuite quatre projets de simulateurs quantiques. Ces simulateurs sont des ordinateurs quantiques qui permettent de simuler des processus physiques quantiques. Ils sont utilisables en particulier pour simuler la physique des matériaux. On ne les programme pas comme les ordinateurs quantiques universels à portes quantiques de la catégorie précédente. Ces simulateurs sont pour l'instant des objets de recherche. Je n'ai pas encore identifié d'entreprise privée, établie ou startup, se lançant dans cette voie. C'est donc pour l'instant surtout une voie de recherche. Elle est cependant en train de passer doucement de la recherche fondamentale à la recherche appliquée, ne serait-ce que pour créer des algorithmes destinés aux applications cibles.

- **PASQuanS** (Allemagne, 9,25M€) est un projet de simulateur quantique à base d'ions piégés allant jusqu'à 1000 qubits. Il implique aussi le Royaume-Uni et Atos en France.
- **Qombs** (Italie, 9,3M€) est un projet de simulateur quantique à base de photonique.
- **PhoQuS** (France, 3M€) est un projet de simulateur quantique également à base de photonique. Il est piloté par une équipe de chercheurs de PSL.
- **SQUARE** (Allemagne, 2,99M€) est un projet de simulateur quantique à base d'ions de terres rares (rubidium, …). Il est piloté par l'Université de Karlsruhe et implique des laboratoires du Danemark, de Suède, Espagne et de France, comprenant Thales.

Continuons avec les projets dans la communication quantique et la sécurisation des télécoms. On peut y constater une apparente redondance entre les projets financés qui sont tous positionnés sur la crypto quantique à base de clés symétriques et de QKD (Quantum Key Distribution, la technique d'envoi sécurisée de clés par voie optique). Curieusement, il n'y a rien sur la "cryptographie post-quantique" qui semble être plus prometteuse sur le marché de la cybersécurité. Elle ne rentre visiblement pas dans le cadre de ce Flagship puisque les techniques et algorithmes utilisés ne sont pas quantiques. Ils permettent de résister au décryptage de clés publiques classiques par des ordinateurs quantiques. Donc, exit.

- **Quantum Internet Alliance** (Pays-Bas, 10M€) (QIA) vise à déployer un réseau Internet protégé par clés quantiques (QKD) en mode réseau maillé et non seulement point à point. Les nœuds ou relais quantiques seront constitués de systèmes exploitant des atomes froids. Ils vont commencer par un réseau à trois ou quatre nœuds. Le projet est piloté par l'Université TU Delft. Le CNRS y participe et notamment Elena Diamanti que j'avais eu l'occasion de voir et croiser lors de l'Échappée Volée en juillet 2018 ainsi qu'Elham Kashefi et Iordanis Kerenidis. L'Université de la Sorbonne y participe également. On y trouve sinon des Suisses, des Allemands, des Danois et des Autrichiens (liste complète).
- **QRANGE** (Suisse, 3,87M€) est un projet d'amélioration des techniques de génération quantiques de nombres aléatoires. La startup suisse ID Quantique ne doit pas être loin derrière puisqu'elle est leader sur ce marché.

- **CiViQ** (Espagne, 9,9M€), ou Continuous Variable Quantum Communications, est un autre projet de sécurisation de télécommunications par fibre à base de QKD. Le projet comprend 21 parties prenantes couvrant le monde académique et industriel dont le CNRS, Intitut Mines-Telecoms, Nokia Bell Labs France, Inria, Orange, ainsi que l'Israélien Mellanox qui est spécialisé dans les produits de communication très haut débit entre serveurs dans les data-centers exploitant l'architecture Infiniband. Il est probable qu'ils aient dans leurs cartons des produits exploitant des QKD.
- **Uniqorn** (Autriche, 9,9M€) est dans le même créneau et travaille sur un générateur de nombres aléatoires et un système de QKD. Il associe 17 organisations de 9 pays (Autriche, Pays-Bas, Italie). L'Israélien Mellanox est aussi de la partie.
- **S2QUIP** (Pays Bas, 3M€), Scalable Two-Dimensional Quantum Integrated Photonics, est un autre projet de communication sécurisée à base de QKD.
- **2D-SIPC** (Espagne, 2,9M€) est un projet de développement de composants de photo-électronique potentiellement exploitable pour créer des réseaux Internet sécurisés par clés quantiques (QKD).
- **QMICS** (Allemagne, 3M€) ou "Quantum Microwave Communication and Sensing" planche une une technologie de création de réseau local à base de micro-ondes sur câble reliant des nœuds de réseaux supraconducteurs. Elle pourrait avoir des applications dans la communication entre processeurs de calcul quantique. Ils travaillent notamment sur la création de détecteurs de photons uniques.

Nous avons ensuite cinq projets en métrologie quantique déjà vus page 384.

S'y ajoute enfin le projet **QFLAG** (Allemagne, 3,48M€) qui est la structure de pilotage et de coordination des projets du Flagship quantique européen. Il est curieux que la Commission Européenne présente ça comme un projet.

Pour comprendre la structure de ces projets avec leurs forces et faiblesses, il faut intégrer les conditions dans lesquels ils sont montés. La politique de la Commission Européenne consiste à gérer équilibre délicat entre les pays de l'Union, petits comme grands.

Les aides à la R&D favorisent aussi la recherche partenariale multi-partenaires et multi-pays. On se retrouve ainsi avec jusqu'à 20 partenaires et 9 pays impliqués dans ces différents projets. Les leaders des projets sont tous des laboratoires de recherche, en général publics. Il est difficile dans ces conditions d'identifier les voies d'industrialisation associées. Des pays externes à l'Union Européenne sont impliqués comme la Suisse, Israël, la Biélorussie, et bientôt, le Royaume Uni.

On note la forte prédominance de projets pilotés par des laboratoires de recherche allemands (5), suivis par les Pays-Bas (3), puis la France, l'Espagne et l'Autriche qui pilotent chacun 2 projets. Suivent l'Italie, le Royaume Uni et la Suisse qui pilotent chacun un seul projet. La France est aussi impliquée dans nombre de ces projets mais sans en avoir lead. En tout, les laboratoires du CNRS sont impliqués dans 13 des 19 projets scientifiques du Flagship.

High-Level Steering Committee
of the QT Flagship Project

Prof. Dr. Jürgen Mlynek, Chairman, Humboldt University Berlin
Prof. Dr. Rainer Blatt, University of Innsbruck
Prof. Dr. Vladimir Bužek, Slovak Academy of Sciences Bratislava
Prof. Dr. Tommaso Calarco, University of Ulm
Prof. Dr. Per Delsing, Chalmers University Gothenburg
Prof. Dr. Elisabeth Giacobino, CNRS Lab Kastler-Brossel Paris
Prof. Dr. Marek Kuś, Polish Academy of Sciences Warsaw
Prof. Dr. Eugene Simon Polzik, Niels Bohr Institute Copenhagen
Dr. Maria Luisa Rastello, INRIM Torino
Prof. Dr. ir. Wim Van Saarloos, KNAW Amsterdam
Prof. Dr. Lluis Torner, Institute of Photonic Sciences Barcelona
Prof. Dr. Ian Walmsley, University of Oxford

Dr. Cyril Allouche, Atos SE
Jaya Baloo, KPN
Dr. Paolo Bianco, Airbus D&S UK
Dr. Michael Bolle, Bosch GmbH
Dr. Fabio Cavaliere, Ericsson
Dr. Guido Chiaretti, ST Micro
Dr. Daniel Dolfi, Thales
Dr. Norbert Lütke-Entrup, Siemens AG
Dr. Graeme Malcolm, M2 Lasers
Dr. Iñigo A. Martinez, VLC Photonics
Dr. Markus Matthes, ASML
Dr. Grégoire Ribordy, ID Quantique

Observer: Prof. Dr. Maria Chiara Carrozza, Sant'Anna School Pisa

source : Quantum Technology European Flagship, Jürgen Mlynek, décembre 2017 (28 slides).

On peut observer une certaine dispersion des efforts, que ce soit dans les simulateurs quantiques ou les systèmes de protection des télécommunications à base de clés quantiques (QKD).

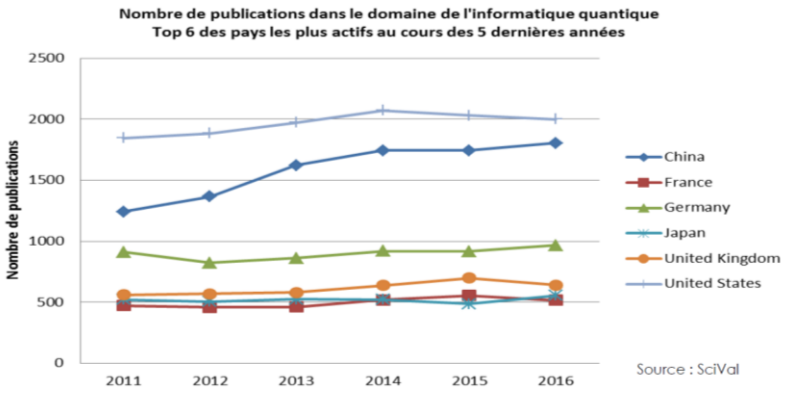
Ces projets ont un autre point commun : ils sont tous pilotés par des physiciens et concernent exclusivement le matériel. Il est très inquiétant de constater que ces projets ne comprennent pas d'efforts dans le logiciel, pour créer des algorithmes, des outils de développement et des solutions logicielles métier adaptées aux ordinateurs quantiques.

On peut espérer que de tels projets seront financés dans les phases suivantes de ce Flagship. Il en va de même de l'absence de projets de cryptographie post-quantique, même si cela peut s'expliquer comme nous l'avons déjà vu.

Dans le même temps, de nombreux industriels américains collaborent avec les laboratoires européens. Microsoft a recruté à l'Université de Delft des spécialistes du quantique, notamment dans les qubits topologiques. Intel a aussi chassé à Delft. Et IBM a une partie de ses équipes dans le quantique qui sont basées dans son laboratoire de recherche de Zurich, près de l'ETH Zurich qui abrite pas mal de spécialistes du quantique.

Nous avons ici la reproduction d'un scénario assez classique avec une excellence de recherche européenne qui se transforme en produits via les grands acteurs américains. Ceci dit, les grands acteurs américains exploitent aussi abondamment la recherche fondamentale issue de leur propre pays. Ainsi, Google et IBM collaborent-ils avec l'Université de Santa Barbara en Californie. Le poids relatif de l'apport des laboratoires de recherche US vis à vis des laboratoires européens aux acteurs américains dépend des acteurs. Il semble plus faible pour Microsoft que pour Google et IBM.

Une note de l'ambassade de France[534] met en évidence un point notable : l'**Allemagne** arriverait en troisième position mondiale en termes de publications scientifiques dans le secteur de l'informatique quantique, après les USA et la Chine et devant le Royaume Uni et le Japon.



Cela ne se traduit visiblement pas en un écosystème entrepreneurial sur le domaine ni par une action particulière des grands acteurs du numérique du pays, sauf peut-être avec **Infineon**, la spin-off de semiconducteurs de Siemens qui s'intéresse à la cryptographie quantique. Ce syndrome est voisin en France avec une recherche assez active sur le sujet mais un côté plutôt atone du secteur privé, à l'exception notable d'Atos.

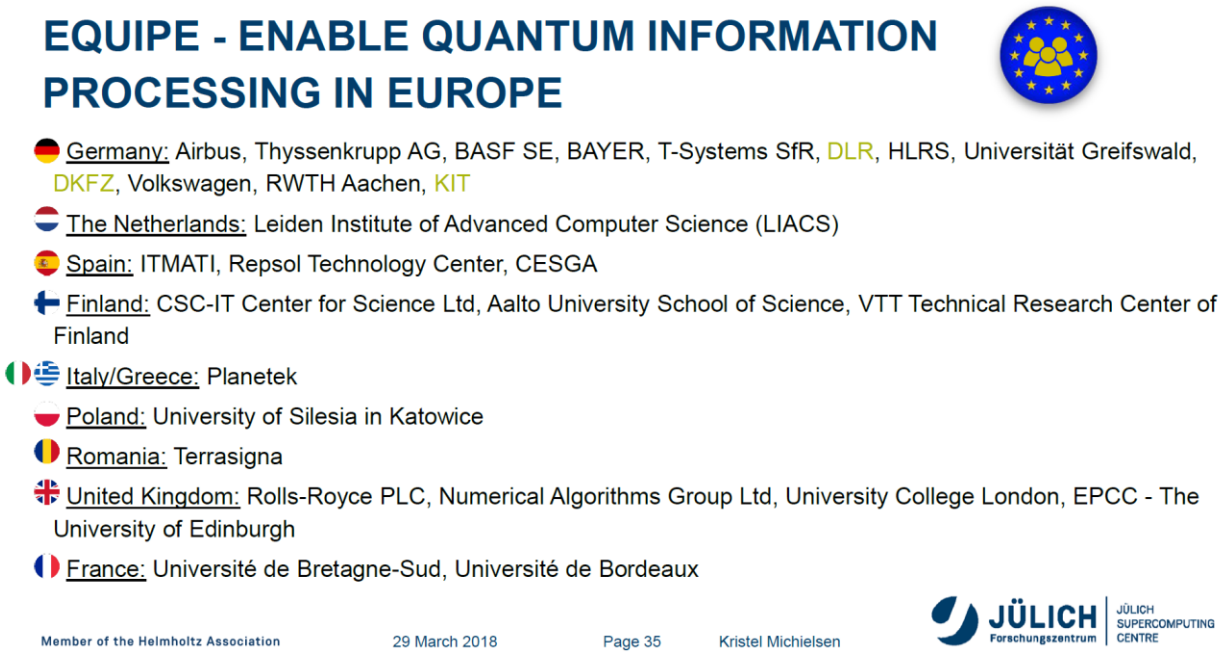
C'est lié au traditionnel différentiel entre recherche et entreprises. L'absence de grands acteurs du numérique en Europe à même de prendre le relai de la recherche est pénalisante. Qui plus est, le tissu de startups n'est pas assez bien financé et ne peut donc pas miser sur le long terme comme le fonds les homologues d'Amérique du Nord. D-Wave a été lancé en 1999, a produit son premier qubit en 2007, huit ans après et a commercialisé ses premiers ordinateurs quantiques vers 2012, donc 13 ans après sa création. Soit bien plus que la durée de vie moyenne d'un fonds d'investissement (à ne pas confondre avec celle des sociétés de gestion) !

L'Europe est par ailleurs assez active dans l'organisation de conférences scientifiques sur l'informatique quantique. Avec quelques exemples : la conférence QIP en janvier 2018 à l'Université de Delft aux Pays-Bas suivie de la conférence Quantum Europe 2018 des 17 et 18 mai 2018, également aux Pays-Bas. D'autres conférences de 2018 sur l'informatique quantique ont eu lieu ou vont avoir lieu en Suisse, au Portugal, en Espagne, en France, en Allemagne, en Autriche et même en Grèce. Parfois, la présence d'intervenants français y est négligeable, comme à Quantum Simulation & Computation de Bilbao en février 2018.

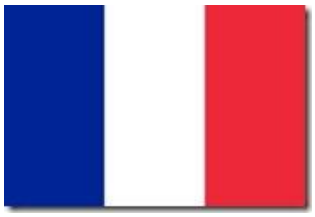
Enfin, citons le projet collaboratif européen **EQUIPE** (Enable Quantum Information Processing in Europe) qui vise à faire avancer l'industrialisation de la création de solutions quantiques pour l'industrie[535].

[534] Voir L'Informatique Quantique au Japon par Emma-Louise Scappaticci, novembre 2017 (27 pages).

[535] Voir Simulation on / of various types of quantum computers de Kristel Michielsen (40 slides).



France



Dans le benchmark mondial, la France se distingue d'une manière encore plus radicale que dans l'intelligence artificielle. Nous avons une recherche de qualité mais pas encore assez de transformation de sa production en initiatives entrepreneuriales même si nous avons vu que le nombre de startups quantiques en France était déjà respectable.

Les stars françaises de la physique quantique sont Alain Aspect et Serge Haroche, le premier ayant invalidé les inégalités de Bell en 1982 et vérifié le principe de non localité de quantum intriqués, un élément clé servant notamment à la cryptographie quantique. Prix Nobel de physiques en 2012, Serge Haroche est pionnier de l'électrodynamique quantique en cavité et sur l'interaction entre les photons d'une cavité supraconductrice et des atomes de Rydberg qui traversent la cavité[536]. Ancien collègue d'Alain Aspect, Philipe Grangier est un spécialiste mondial de la cryptographie quantique. Comme d'habitude, les cerveaux brillants ne manquent pas.

Michel Devoret est en quelque sorte le "Yann LeCun" du quantique, à savoir qu'il travaille maintenant à l'Université de Yale aux USA (vs l'Université de New York) et dans la startup qu'il a cofondée aux USA, QCI. Mais nuance, il n'est pas (encore) dans un GAFA !

[536] Voir ses cours de physique quantique au Collège de France entre 2001 et 2015. En photonique, sur le contrôle d'atomes froids, sur les questions de décohérence, etc.

Nombre de laboratoires de recherche planchent sur les différentes briques du quantique, que ce soit au CEA à Saclay (supraconducteurs) et à Grenoble (CMOS), au CNRS ou à l'Inria, au Laboratoire Circuits Quantiques Hybrides de l'ENS Ulm, dans le Quantum Circuit Group de l'ENS Lyon et dans plein de régions, notamment à Toulouse, Montpellier, Bordeaux (LaBRI) et Grenoble, en plus de l'Ile de France.

Du côté des entreprises, nous avons quelques acteurs des couches basses physiques **CryoConcept** et **MyCryoFirm** et leurs systèmes de cryogénie, **Quandela** avec ses sources de photons uniques utilisables dans des ordinateurs quantiques à base de photons ou dans les télécommunications et la cryptographie quantiques et **Pasqal** et son projet de simulateur analogique. La startup **Prevision.io** est de son côté en train d'évaluer l'intérêt des algorithmes quantiques à intégrer dans sa boîte à outils d'algorithmes de machine learning.

Seul **Atos** sort du lot. Leur stratégie lancée en 2016 consiste à se préparer à devenir un acteur du cloud dans le calcul quantique en prenant le problème "par le haut", par le logiciel, avec une focalisation sur les applications b2b et industrielles du quantique et enfin, en privilégiant le calcul hybride, qui associe le calcul sur des supercalculateurs et sur calculateurs quantiques. Ils développent des compétences dans les algorithmes et la programmation de calculateurs quantiques, notamment avec le langage aQasm qui peut fonctionner sur tout ordinateur quantique présent ou futur.

J'avais eu l'occasion de rencontrer Mounir Mahjoubi à Bercy en novembre 2018 pour souligner le besoin de consolider une stratégie française du quantique. Avec quelques autres acteurs de l'écosystème quantique tels que Christophe Jurczak du fonds Quantonation[537], Bpifrance (avec son plan Deeptech lancé en janvier 2019) et la DGE (qui s'intéresse sérieusement au sujet depuis mi 2018), nous étions persuadés du besoin d'un affichage politique, face aux équivalents du Royaume Uni (2013), des

[537] Voir Les technologies quantiques sont en passe de révolutionner des pans entiers de l'économie de Christophe Jurczak et Charles Beigbeder, mars 2019.

USA (2018), du Canada (2015) et de la Chine (2015). En parallèle Cédric O s'était saisi du sujet alors qu'il était conseiller sur le numérique à l'Elysée.

Cela semble avoir porté ses fruits avec la création d'une mission d'étude parlementaire commanditée officiellement par le Premier Ministre en mars/avril 2018 et confiée à la députée LREM **Paula Forteza**[538] qui était déjà très engagée autour des sujets numériques. Elle est accompagnée par **Iordanis Kerenidis** (chercheur au CNRS et cofondateur de la startup US QCWare) et **Jean-Paul Herteman** (ancien PDG de Safran). J'ai été auditionné en avril 2019 pour évoquer les questions relatives à l'écosystème du quantique et aux enjeux stratégiques du secteur.

La mission parlementaire a terminé ses auditions en juin 2019 et devait remettre son rapport en octobre 2019, le gouvernement emboîtant le pas immédiatement et proposant un plan quantique pour le pays reprenant tout ou partie des propositions de la mission parlementaire, devant être annoncé avant la fin 2019.

Russie

Terminons ce tour du continent européen avec la **Russie**. Elle n'est pas très visible dans la bataille industrielle qui se prépare autour de l'informatique quantique.

Cependant, s'est créé en 2012 le **Russian Quantum Center**, un centre de recherche dédié aux différents domaines d'applications de l'informatique quantique, cryptographie quantique comprise comme il se doit. Il occuperait en tout environ 200 chercheurs.

Ses travaux couvrent de nombreuses branches de l'informatique quantique : les supraconducteurs, la photonique et les cavités de diamants. Ils travaillent aussi dans le domaine de la métrologie quantique. Ils ont notamment développé leur propre solution de QKD et un détecteur de photon unique. Mais à ce jour, ils n'ont rien communiqué sur des avancées côté qubits.

Ils collaborent avec de nombreux organismes de recherche internationaux aux USA (MIT), Canada (Université de Calgary), Allemagne (Max Planck Institute for Quantum Optics), UK (Université de Bath), etc[539].

[538] Voir le communiqué de Paula Forteza : Technologies quantiques : un tournant numérique majeur à ne pas manquer pour la France ?, 10 avril 2019.

[539] Ces informations proviennent de Evaluation Report of Russian Quantum Center, 2017 (7 pages).

Il ne serait pas étonnant que l'on voit émerger de tout cela au moins quelques startups dans la cryptographie quantique, ne serait-ce que pour des raisons de souveraineté pour ce pays qui tient à sa position dans le monde, face à la Chine, aux USA autant que face à l'Europe.

Proche et Moyen-Orient

Israël est un pays relativement discret sur le quantique, à part l'affreux Gil Kalai de l'Université Hébraïque de Jérusalem qui affiche son scepticisme bien ancré sur le devenir des ordinateurs quantiques. Ils n'ont pas de startups visibles dans le domaine, en particulier côté ordinateurs quantiques.

Néanmoins, ils sont actifs tout azimut côté recherche comme nombre de pays. En juillet 2018, une initiative de financement de la recherche quantique était lancée par le gouvernement du pays et dotée de 75M€ sur un nombre d'années non précisé. Ce financement ira surtout au Technion, l'Université de Haïfa au nord du pays, qui veut concevoir son propre ordinateur quantique et a par ailleurs bénéficié d'une donation de $50M. Ce Quantum Information Processing lab travaille sur de nombreuses pistes, presque trop avec des qubits à résonnance magnétique nucléaire, en photonique et en CMOS. Il est possible que la proximité d'un laboratoire de recherche d'Intel explique cette dernière piste même si elle semble être très récente dans ce laboratoire.

La recherche quantique est aussi au programme du Quantum Information Science Center de l'Université Hébraïque de Jérusalem créé en 2013 et qui est focalisé sur la communication quantique sécurisée (QKD). Il est financé à hauteur de $2M par le Ministère de la Défense. Ils travaillent aussi sur la création de portes quantiques servant à échanger des états de qubits entre processeurs quantiques. Le QISC comprend une équipe d'une vingtaine de chercheurs.

L'Université de Nanotechnologies de Bar-Ilan situé à Ramat Gan près de Tel Aviv dispose de son propre laboratoire quantique, le Quantum Entanglement in Science and Technology (QUEST), lancé en 2017 et visiblement investi dans la physique quantique à bas niveau et surtout, la communication quantique.

En juillet, la **Ben-Gurion University of the Negev** (BGU) annonçait un partenariat avec le Ministère de la Défense israélien sur le quantique, sans préciser les applications visées. La startup **Accubeat** qui produit des horloges atomiques quantiques au rubidium est issue de cette université.

Israël n'est pas le seul pays du proche et du moyen orient qui semble investi dans la recherche quantique.

L'**Iran** est aussi de la partie avec au moins deux laboratoires de recherche, l'**Université de Sharif** qui travaille sur la physique quantique en partenariat avec le Canada et le **Quantronics Lab** de l'Université Technologique d'Iran qui est dédié à la communication quantique (QKD) [540] . Le pays organise même sa conférence sur l'informatique quantique, l'**IICQI**, ce depuis 2007[541].

Asie-Pacifique

L'**Australie** est un pays qui s'investit aussi dans le quantique à différents niveaux. Le plan National Innovation and Science Agenda annoncé en 2015 comprend 24 initiatives et $820M de financement sur 4 ans dont $19M sont alloués au Center for Quantum Computation and Communication Technology (CQCCT) sur 5 ans dans l'informatique quantique. Le pays est aussi prolixe en projets partenariaux public-privé et associant l'Australie à d'autres pays.

Côté militaire, un fonds d'investissement du Ministère de la Défense, l'**Australian Next Generation Technologies Fund** allouait $730M à 9 domaines dont un sur le quantique[542]. Il faut ici comme ailleurs lire entre les lignes : ces fonds étaient alloués sur 10 ans à partir de 2016. Supposons qu'ils soient distribués équitablement entre les 9 initiatives, cela nous fait $8M de fonds additionnels par an sur le quantique pour des usages militaires, métrologie compris. Vu comme cela, c'est toujours moins impressionnant !

L'UNSW (Université de Nouvelle Galle), la Commonwealth Bank of Australia et l'opérateur télécom Telstra financent à hauteur de de $52M les efforts de création d'un processeur quantique CMOS. On pourrait espérer qu'Orange fasse la même chose en France avec le CEA et/ou une startup !

Côté partenariats internationaux, le pays est associé avec l'Université de Singapour pour la création de satellites de télécommunication quantique. L'Université de Sydney fait partie d'un consortium international intégré dans le programme **LogiQ** de l'IARPA US. Enfin, l'UNSW est partenaire du CEA-Leti dans la recherche appliquée de qubits CMOS.

---

[540] Source : Iranian research in quantum information and computation, juin 2016.

[541] Voir http://iicqi.sharif.edu/.

[542] Voir Next Generation Technologies Fund, 2016.

Le partenariat entre le CEA et l'UNSW a été signé en mai 2018 en présence d'Emmanuel Macron et du Premier Ministre australien Malcolm Turnbull. Ce partenariat associe aussi la société **Silicon Quantum Computing** (SQC) issue de l'UNSW, créée par **Michelle Simmons**, et dont les actionnaires comprennent le gouvernement australien ainsi que l'opérateur Telstra. Il porte sur le développement de technologies quantiques CMOS. Il associe aussi Andrew Dzurak, un physicien de l'UNSW spécialisé dans les CMOS quantiques.

Du côté entrepreneurial, on compte trois startups australiennes dans le domaine du quantique avec **QuintessenceLabs** (clés optiques QKD), **QxBranch** (logiciels et conseil) et **Silicon Quantum Computing** (qubits CMOS) que nous venions de citer.

Passons à l'Asie en démarrant avec le **Japon**. Une note de l'ambassade de France au Japon de fin 2017 faisant le point de l'informatique quantique au Japon (27 pages) illustrait un investissement de long terme du pays dans l'exploration de l'informatique quantique, dans la lignée de leurs efforts dans les supercalculateurs, pilotés notamment par **Fujitsu**. C'est une approche qui n'est pas sans rappeler celle de la France avec Atos. A noter que le fonds d'investissements de Softbank abondé par de l'argent de la famille Saoud et doté de $100B doit aussi investir tout azimut dans le quantique (source).

Le pays lançait la création des **National Institutes for Quantum and Radiological Science and Technology** (QST) en avril 2016 dotés de $487M de budget annuel. Ce montant impressionnant n'est pas dédié à l'informatique quantique. Il semble qu'il le soit bien plus au vaste secteur de la métrologie quantique et en particulier dans celui de l'imagerie médicale.

En 2017, l'opérateur télécom **NTT** lançait un prototype de réseau de neurones quantique (QNN) à base de photonique, en collaboration avec le **National Institute of Informatics** et l'**Université de Tokyo**. Il était disponible sur le cloud sur qnncloud.com (vidéo) mais le service a été arrêté en mars 2019[543].

En 2017, le **NICT** (National Institute of Information and Communication Technologies) réalisait une démonstration de télécommunication quantique exploitant un microsatellite. Cela ressemble à l'expérience chinoise avec le satellite Micius réalisée la même année. En juillet 2017, le NICT (National Institute of Information and Communication Technologies) a réalisé une démonstration de communication quantique à l'aide d'un microsatellite qui constitue une première mondiale.

[543] Voir Japan launches its first quantum computer de Walter Sim, novembre 2017.

Le JFLI est un laboratoire franco-japonais basé à Tokyo créé en 2009 et qui associe des chercheurs des Universités de Tokyo, de Keio et du National Institute of Informatics avec ceux du CNRS, de l'UPMC (Pierre et Marie Curie), de l'Inria et de l'Université Paris-Sud.

Ils travaillent de concert avec l'équipe de Michelle Simmons Center à Sydney en Australie (comme le CEA-Leti à Grenoble) ainsi qu'avec l'**IQOQI** autrichien. Cette équipe pluridisciplinaire va de la physique fondamentale à l'algorithmique et étudie la faisabilité du calcul quantique à grande échelle tout comme la cryptographie quantique.

Dans le privé, les grands groupes industriels japonais sont surtout focalisés sur les télécommunications et la cryptographie quantiques, un peu comme en Chine et en Corée du Sud.

C'est le cas de **Toshiba Corporation** qui s'est lancé dans la cryptographie quantique dès 2003. Ils travaillent dessus avec le Quantum Information Group (QIG) à l'Université de Cambridge, UK. Ils ont réalisé une première démonstration de communication quantique en 2014, en envoyant 878 gbits de données sécurisées sur une fibre de 45 km entre deux zones de la région de Tokyo sur une durée cumulée de 34 jours, à raison de 300 kbits/s. Ils poursuivaient les expérience en 2016 et avec British Telecom au Royaume-Uni.

Hitachi a aussi un laboratoire de recherche situé à l'Université de Cambridge qui planche sur les clés quantiques, l'informatique quantique et la création de composants SQUID pour qubits supraconducteurs. **NEC** est aussi versé dans les clés quantiques (QKD).

NTT entretient quatre laboratoires de recherche appliquée dans le quantique, focalisés dans les télécommunications et la cryptographie quantiques. Ils travaillent aussi dans la filière des qubits CMOS à quantum dots.

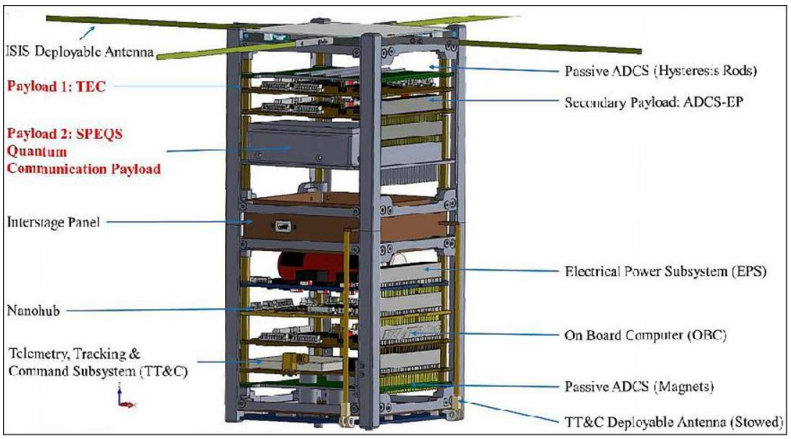
Le tout avec une quarantaine de chercheurs. En novembre 2017, ils annonçaient mettre au point QNNcloud, un ordinateur quantique utilisant l'optique linéaire (photons) mis en service dans le cloud pour simuler des réseaux de neurones avec une boucle optique alimentée par des impulsions laser (vidéo). Le procédé qui ne s'appuie pas sur la notion de qubits est décrit dans Universal Quantum Computing with Measurement-Induced Continuous-Variable, 2017 (5 pages). Il serait très peu consommateur d'énergie, de l'ordre de 1 KW/h.

C'est en fait plutôt un concurrent de D-Wave. QNNcloud est un projet financé dans le cadre du programme d'innovation ImPACT et en partenariat avec le National Institute of Informatics (NII), l'Université de Stanford, celles de Tokyo, Osaka et Tohoku. Le projet avait démarré en 2011.

En **Corée du Sud,** l'opérateur télécom **SK Telecom** investit dans les télécommunications quantiques[544]. Ils sont partenaires de la Florida Atlantic University. Ils ont aussi investi en 2016 dans la startup suisse ID Quantique. Ils sont partenaires depuis 2017 avec Nokia dans le domaine des QKD tout comme avec Deutsche Telekom avec qui ils ont établi une "Quantum Alliance" pour créer des télécommunications sécurisées. De son côté, **Samsung** investit aussi dans les QKD et la cryptographie quantiques.

Le petit état de **Singapour** est connu pour son dynamisme économique et entrepreneurial. Au sein de l'Université de Singapour, la recherche dans le quantique est assurée depuis 2007 dans le **Center for Quantum Technologies** (CQT) avec un financement d'environ $15M annuels. Il est comme c'est souvent le cas investi à la fois dans le calcul quantique et la cryptographie quantique.

Côté partenariats, Singapour est notamment associé à la Chine voisine. Singapour a lancé en 2015 son nanosatellite Galassia-2U, créé par le CQT et servant à expérimenter des communications quantiques cryptées via QKD. Galassia est intégré dans un format CubeSat à deux unités (deux cubes l'un sur l'autre, cf *ci-contre*). Il ne fait que 3,4 Kg au total.



source : https://directory.eoportal.org/web/eoportal/satellite-missions/g/galassia

Il a été lancé avec 5 autres satellites dont le satellite de télécommunications TeLEOS-1 (400 kg) fin 2015 par un lanceur indien. La durée de vie de ce genre de satellite est de 6 mois. Voir Quantum Tech demos on CubeSat nanosatellites (41 slides). Ces expériences ont mené, visiblement, à la création de la startup S-Fifteen Space Systems. Mais, il reste à trouver des solutions pour que ces satellites durent plus longtemps sur leur orbite basse et ne contribuent pas encore plus à poubelliser l'espace autour de la Terre.

[544] Voir SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies, march 2019.

Auparavant, le CQT avait eu l'occasion de tester involontairement l'envoi d'un satellite (ComX-2) dans une fusée ayant explosé en 2014 après le décollage. Non sans humour, il explique que ComX-2 n'a pas survécu à l'expérience dans Extreme Environmental Testing of a Rugged Correlated Photon Source, 2015 (2 pages). Mais ils ont récupéré un ComX-2 après un autre lancement raté.

Comme dans pas mal de secteurs technologiques, la **Chine** affirme haut et fort ses ambitions et sa puissance dans le secteur du quantique. Elle s'est aussi lancée dans des efforts tout azimut, touchant la cryptographie, les télécommunications, la simulation et le calcul quantiques[545].

De même qu'au Royaume-Uni, cet investissement a été pris en main assez tôt par l'exécutif et dès 2013 avec l'implication de Xi Jinping, le président Chinois, lors d'une visite du laboratoire d'Anhui, portant surtout sur la cryptographie quantique, associée à une session de formation. Dès 2015, Xi Jinping intégrait la communication quantique dans les priorités scientifiques du pays. L'informatique quantique était intégrée de son côté dans les priorités du 13ième plan couvrant la période 2016-2020. Une roadmap quantique de la Chine datant de 2016 est disponible dans "Quantum Leap: The Strategic Implications of Quantum Technologies de Elsa Kania" et John Costello (part 1 and part 2). Voir aussi Chinese QC Funding de Xiaobo Zhu, 2017 (35 slides). Les montants investis dans le quantique étaient respectivement de $160M dans le 11e plan couvrant la période 2006-2010, de $800M dans le 12e plan couvrant 2011-2016 et de $320M dans le 13e plan démarrant en 2016, complétés par $640M de financement des régions.

Le financement total de la recherche publique en quantique depuis 2006 se monte donc à près de $2B. Le projet le plus ambitieux est le centre de recherche à $10B qui doit ouvrir en 2020, le **National Laboratory for Quantum Information Sciences**, situé à Hefei, à près de 500 km à l'ouest de Shanghaï.

[545] Voir Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership CNAS, 2018 (52 pages).

Le montant est à prendre avec des pincettes car, même sur 10 ans, un Centre de Recherche aussi grand soit-il ne couterait pas cette somme là. Ce laboratoire sera focalisé sur l'informatique et la métrologie quantiques, aussi bien pour des applications militaires que civiles.

Jusqu'à présent, l'entité la plus active dans l'informatique semblait être l'**University of Science and Technology of China** (USTC) de l'Académie des Sciences Chinoises (CAS). Elle annonçait avoir préparé et mesuré l'état de 600 paires de qubits intriqués en 2016 (source) puis avoir développé des portes quantiques avec un faible taux d'erreurs. Il est difficile d'évaluer l'intérêt d'avoir 600 paires de qubits si ceux-ci ne sont pas reliés entre eux. En 2017, ce même laboratoire annonçait la réalisation d'un système de test de 10 qubits supraconducteurs intriqués en aluminium et saphire (source). Le taux d'erreurs serait élevé, à 0,9% pour les portes à deux qubits. Le leadership de ce laboratoire est assuré par un certain Jian-Wei Pan, le pape du quantique Chinois[546]. Son équipe prévoit de créer un ordinateur quantique universel à base de 50 qubits d'ici 2023 ! Et il pense qu'il faudra attendre 30 à 50 ans pour qu'un ordinateur quantique universel voit le jour.

En mai 2017 était annoncée la création d'un prototype d'ordinateur quantique photonique par l'**Institute for Quantum Information** de l'Académie des Sciences Chinoise de Shanghaï (source). Petit détail : il ne comporte qu'un seul qubit à base de photon unique (*ci-dessous*) (source).

La branche "optique linéaire" de l'informatique quantique est prometteuse mais pour l'instant a bien du mal à "scaler". Il est cependant tout à fait normal que, comme bien d'autres pays, plusieurs voies de création de qubits physiques soient explorées.

En août 2018 était annoncée une autre prouesse dans la lignée de la précédente avec deux qubits manipulant des photons, fabriqués en technologie CMOS, dans Large-scale silicon quantum photonics implementing arbitrary two-qubit processing, août 2018 (7 pages). La nouveauté résidait dans l'exploitation de portes quantiques opérant sur ces deux qubits.

Mais contrairement à la couverture presse qui s'enthousiasme sur la question (par exemple, dans Des chercheurs chinois sur la voie du processeur quantique 'ultime' ? Effectivement ça sent bon ! de Bruno Cormier dans Tom's Hardware), il faut raison garder. Il est difficile d'intriquer correctement ces qubits à grande échelle et leurs taux d'erreurs sont largement supérieurs à 1% alors qu'il faudrait être situé entre 0,001% et 0,1% pour que cela soit intéressant.

Qui plus est, la technologie n'est pas si facile que cela à miniaturiser. Comme son taux d'erreurs est très élevé, il faudra créer des qubits logiques avec un très grand nombre de qubits physiques pour qu'un tel ordinateur quantique soit pratiquement utilisable. Petits détails utiles : ce projet conduit par plusieurs laboratoires de recherche chinois a été mené en partenariat avec le laboratoire de photonique de Jeremy O'Brien à l'Université de Bristol et un laboratoire australien à Brisbane.

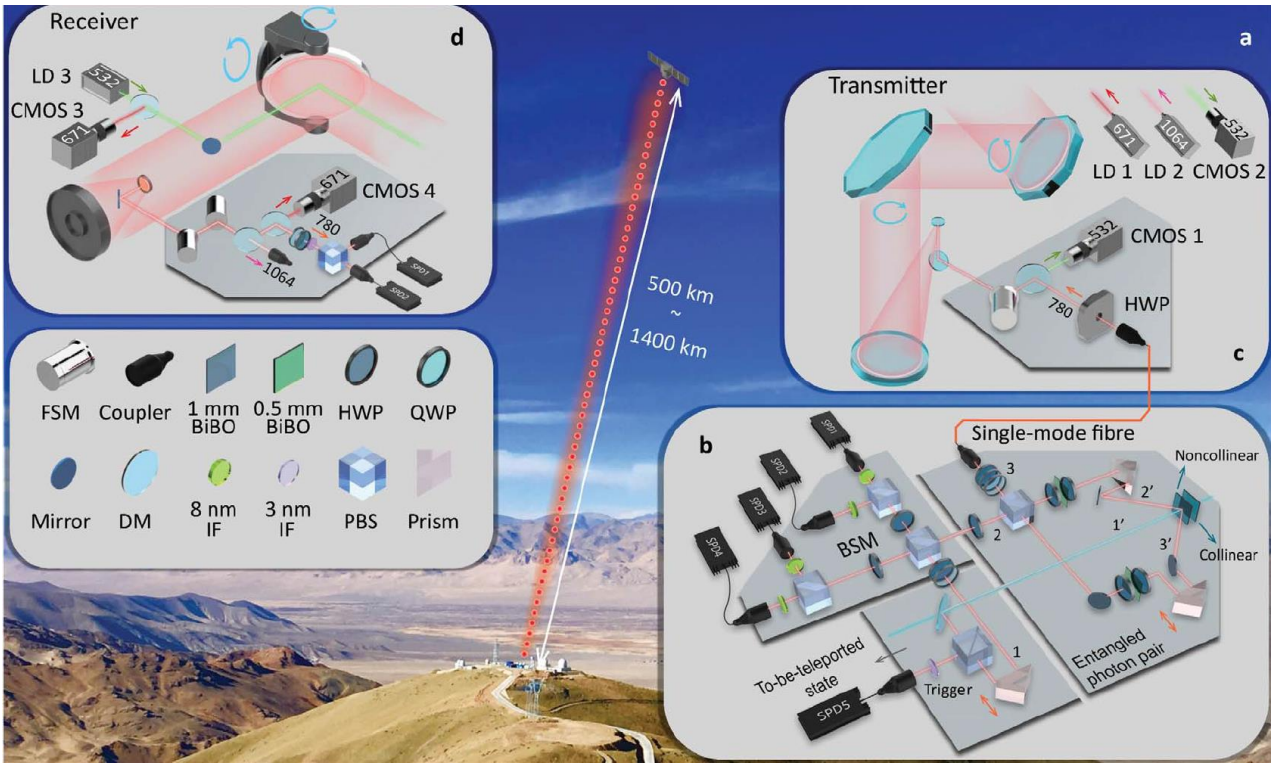
---

[546] Voir The man turning China into a quantum superpower, de Martin Giles dans MIT Technology Review, décembre 2018.

Des partenariats public-privé sont aussi établis en Chine, le plus connu étant celui d'**Alibaba** qui a investi 1 Md$ dans l'USTC de Jian-Wei Pan pour lancer en 2015 l'Alibaba Quantum Computing Laboratory à Shanghai, qui s'intéresse à la crypto quantique et à l'ordinateur quantique. La crypto quantique pourrait servir à sécuriser certaines transactions de commerce en ligne et de liaisons entre data centers.

Alibaba lançait même en janvier 2018 la mise en ligne dans le cloud d'un ordinateur quantique de 11 qubits développé par l'USTC, faisant suite au lancement d'un simulateur quantique à base d'ordinateurs traditionnels de 22 qubits fin 2017. Cette offre de tests d'algorithmes quantiques dans le cloud est très similaire à celle que propose IBM depuis 2016, sachant néanmoins qu'il est difficile de les comparer sans un benchmark précis des caractéristiques des qubits en termes de temps de cohérence.

Tout cela est très bien mais pas spécialement plus au point que ce que l'on trouve aux USA ou en Europe. Par contre, la Chine est en avance du côté de la cryptographie quantique, au moins au niveau du livre des records. Cela commence avec une expérience record d'intrication de photons à longue distance menée mi 2017.



La téléportation d'un photon dupliqué était réalisée à 5100 m d'altitude à Ngari au Tibet vers le satellite Micius qui orbite à 500 km d'altitude, et à une distance maximale de 1400 km. Les photons émis provenaient d'un laser opérant dans l'ultraviolet.

Ce genre d'expérience avait déjà été faite sur Terre avec des distance allant jusqu'à 100 km correspondant à la longueur maximale d'une fibre optique sans répéteur[547]. En gros, la performance chinoise revenait à reprendre à longue distance l'expérience d'Alain Aspect de 1982. Elle permet notamment d'envoyer des clés quantiques protégées contre les interceptions.

L'expérience a été renouvelée début 2018 avec l'organisation d'une vidéoconférence entre la Chine et l'Autriche utilisant une clé quantique envoyée toutes les minutes (source). La Chine prévoit en fait de lancer d'ici 2030 une nuée de satellites dédiée à l'envoi de clés quantiques en reprenant ce processus. Enfin, une liaison en fibre optique protégée par clé quantique de 2000 km a été déployée entre Shanghaï et Beijing. En tout cas, on voit que la Chine prend très au sérieux cette histoire de sécurisation des communications !

Du côté des entreprises, on peut citer **ZTE** et les startups **QuantumCTek** et **Qasky Science** qui sont spécialisées dans la cryptographie quantique. Les deux dernières ont rejoint avec le Suisse ID Quantique et l'Américain Battelle le **Quantum-Safe Security Working Group**, qui fédère l'industrie de la cryptographie quantique. La Chine met donc le paquet sur le quantique dans toutes ses dimensions, mais surtout dans la cryptographie quantique !

Sur le calcul quantique, la Chine semble par contre un peu en retrait. Elle ne semble pas avoir d'influence dans le monde académique sur la partie algorithmique et programmation. Aucun outil de développement ou framework de développement d'application quantique n'est proposé au monde par la Chine. Même pour la sécurité, ils mettent le paquet sur la QKD pour la gestion de clés symétriques alors que la communauté scientifique de la sécurité considère que c'est une chimère et qu'il vaudrait mieux se focaliser sur la cryptographie post-quantique et des architectures de clés publiques résistantes aux ordinateurs quantiques. Là encore, cela repose plutôt sur des mathématiques et du logiciel.

Il ne faut jamais oublier le rôle stratégique du logiciel et des plateformes dans les batailles économiques du numérique ! J'ai l'impression que l'Histoire se répète en Chine de ce côté-là.

Quelles stratégies industrielles ?

Le marché potentiel de l'informatique quantique est et restera probablement assez longtemps un marché de niche. Les prévisions des analystes qui sont d'habitude tout feu tout flamme sur les marchés émergents comme sur l'Internet des objets sont assez prudents, et à juste titre, sur la taille de ce marché. Il serait de $553M en 2023 selon MarketsandMarkets, une prévision datant d'aout 2017. Il serait de $1,9B en 2023 selon CIR et de $2,64B en 2022 selon Market Research Future, une prévision datant de 2018. Homeland Security Research voit plus large avec $8,45B en 2024 (en 2018), intégrant produits et services, auxquels s'additionneraient $2,24B de financements publics.

[547] Voir la source du schéma et détails de l'expérience.

Une étude de Morgan Stanley de 2017 évalue la taille du marché de l'informatique quantique à plus de $10B en 2028 tout en la comparant au marché de l'informatique grand public ($590B, en y intégrant les PC, les smartphones et les tablettes) et d'entreprise ($185B). Les marchés visés mis en avant sont souvent celui des transports, de la défense et de la lutte contre le cybercriminalité. Ces prévisions intègrent parfois le marché de la cryptographie quantique. Par comparaison, le marché des supercalculateurs était situé aux alentours de $5B à $6B en 2017. En juillet 2018, ABI Research évaluait pour sa part le marché du quantique à $15B d'ici 2028.

Le marché de l'informatique quantique est en fait bien moins mature et prêt à être lancé que celui de la cryptographie quantique. L'ordinateur quantique est incertain et assez éloigné dans le temps. Cela explique l'investissement de presque tous les pays en parallèle dans l'informatique quantique, la cryptographie quantique et la métrologie quantique, cette dernière ayant un marché cible très professionnel et limité.

Les Etats sont motivés à investir sur le quantique pour des raisons stratégiques : à la fois dans l'idée de pouvoir décrypter les télécommunications existantes ou passées dans le cadre de l'activité de leurs services de renseignement (Direction Technique de la DGSE en France, NSA aux USA, GCHQ au Royaume-Uni…) et de protéger les leurs via la cryptographie quantique. Le quantique est donc, plus que presque toute autre technologie numérique, un outil de souveraineté stratégique des états.

Les partenariats dans l'informatique quantique sont de nature différente : entre laboratoires de recherche intra-pays (comme dans l'initiative Quantum Silicon Grenoble), inter-pays (comme le CEA-Leti et USNW, ou les Chinois avec les Australiens et les Britanniques), puis entre la recherche publique et le privé au sein du même pays (CEA et Atos) ou entre pays différents (Intel avec Qutech). La raison d'être de tous ces partenariats est identifiable : l'informatique quantique est un sujet scientifique complexe qui ne peut pas être maitrisé par un seul laboratoire ou une seule entreprise. La collaboration est nécessaire pour rassembler des talents de spécialités différentes, entre la physique de la matière condensée, les technologies de capteurs et de contrôle, l'optronique, la cryogénie, la production de semiconducteurs, l'algorithmie et le développement logiciel.

Au-delà de cet aspect stratégique se posent des questions sur la vitesse à laquelle le secteur privé pourrait et devrait prendre le relai de la recherche fondamentale publique. C'est un enjeu technologique au long cours qui relève d'un risque presque aussi grand que le risque et l'incertitude scientifique. Quel serait le meilleur timing de l'investissement privé et la capacité de le faire avec une incertitude technologique très forte ? Il existe quelques "best practices" comme ID Quantique, lancé en Suisse par le chercheur Nicolas Gisin.

Malgré la belle dynamique autour des deep techs que l'on sent en Europe et en France, ce type de financement semble pour l'instant accessible uniquement en Amérique du Nord. Il nous faut inventer des modèles entrepreneuriaux et de financement permettant de conduire des aventures au long cours dans le secteur privé, à l'image de la longue histoire de D-Wave.

Comme d'habitude, nombre de pays se demandent comment encourager la création de startups par des chercheurs ou l'exploitation de leurs travaux par des entrepreneurs qui ne sont pas des chercheurs. A part Atos qui s'est déjà engagé sur le quantique, quelles autres entreprises établies et orientée "produits" pourraient se lancer sur le quantique ? On pense au complexe militaro-industriel avec des entreprises comme Thalès. Le quantique est peut-être le seul endroit où un "CloudWatt" aurait eu du sens avec un financement public/privé, voir même une approche transnationale européenne.

La situation actuelle met en lumière une autre déficience française : l'absence d'un office scientifique rattaché à l'exécutif comme il en existe aux USA ou en Israël. Lorsque l'exécutif a besoin de lumières pour comprendre les enjeux scientifiques du moment, vers qui se tourne-t-il ? Comme on l'a vu sur l'intelligence artificielle, il doit lui-même jouer le rôle d'intégrateur et enquêter auprès de centaines de personnalités et organisations représentatives.

C'est long, séquentiel, souvent biaisé et réalisé de manière ponctuelle alors que cela devrait être une tâche permanente et centralisée quelque part et piloté par une personnalité reconnue par la communauté scientifique. Ce n'est cependant pas le rôle d'une Académie comme celle des sciences ou celle des technologies.

Ainsi, aux USA, l'Académie des Sciences est une organisation privée distincte de l'Office Scientifique et Technologique du Président (OSTP) établi par le Congrès en 1976. L'OSTP s'appuie sur le National Science and Technology Council, créé sous la Présidence Clinton en 1993.

Enfin, nous avons aussi l'opportunité de créer un écosystème logiciel avec des outils de modélisation, de développement et des applicatifs métiers. La cartographie des acteurs privés de l'informatique quantique que j'ai compilée à partir de sources diverses est encore éparse. Une industrie nouvelle va probablement émerger de l'informatique quantique, même si elle sera plus modeste en taille que le marché de l'informatique d'entreprise actuel. L'un des enjeux clés me semble être celui de la création d'applications "grand public" du quantique.

A savoir, des applications qui pourraient générer des économies d'échelle et permettre à ce marché de dépasser le cadre d'un marché étroit dédié à la recherche et à quelques applications b2b.

Nous avons aussi besoin de mathématiciens et d'une nouvelle génération de développeurs qui vont devoir tout apprendre ou réapprendre pour créer et utiliser des algorithmes quantiques.

Il faudra se bouger si l'on veut éviter de se voir une fois de plus dominés par des acteurs américains, canadiens si ce n'est chinois. Le syndrome de la dominance des GAFA peut se reproduire facilement dans le quantique si l'on n'y prend gare. Si la France annonçait la couleur sur le sujet, il vaudrait mieux que cela se fasse très rapidement. Pas dans 5 ans avec un "plan de rattrapage" comme l'est le Rapport Villani pour ce qui est de l'intelligence artificielle.

Société

Nous allons ici quitter les mathématiques, les algorithmes, les logiciels et la physique pour nous intéresser aux liens entre le quantique et la société. Ceux qui avaient du mal à digérer les éléments scientifiques de l'histoire vont pouvoir respirer !

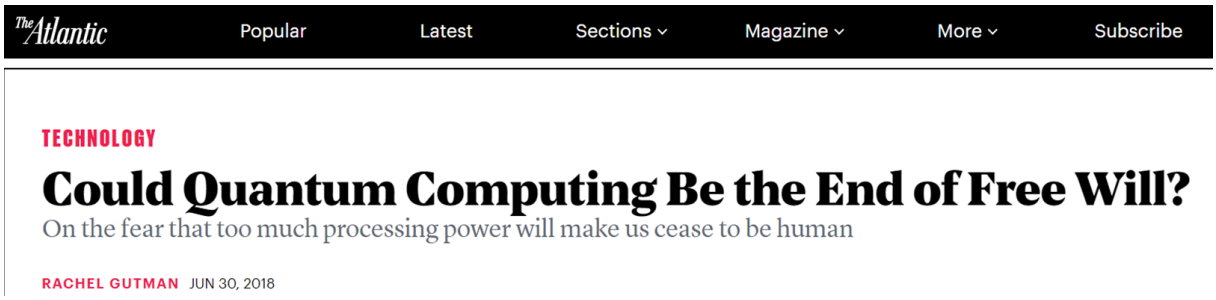
Nous sommes encore aux tous débuts de l'Histoire. Ce qui va suivre est un mélange d'observations et d'interpolations. Comme toute vague technologique du numérique, celle du quantique touchera la société et les industries à plusieurs niveaux dont certains peuvent être anticipés.

Je vais tour à tour, m'intéresser à l'ambition humaine associée au quantique, à la manière dont les religions et le spirituel s'approprient le quantique, à l'éthique des usages du calcul quantique, à l'éducation et la formation à l'informatique quantique, au rôle des femmes dans le secteur et au marketing du quantique par les fournisseurs.

Ambition humaine et quantique

L'informatique quantique est facilement présentée au grand public comme apportant une capacité de calcul défiant l'entendement allant au-delà de ce tout ce que l'on faisait jusqu'à présent. L'informatique quantique serait donc le moyen de détourner ou de provoquer la prolongation de l'application empirique de la loi de Moore. Elle permettrait d'entretenir l'exponentialité éternelle des technologies. Cela peut donner l'impression qu'avec l'informatique quantique, l'Homme va disposer d'un outil lui apportant une puissance infinie et un contrôle total de l'information, dans la lignée de nombreux mythes construits autour de l'intelligence artificielle et de sa destinée ultime, l'intelligence artificielle générale (AGI). Dans cette source, le physicien et auteur futuriste américain **Michio Kaku** prévoit que les calculateurs quantiques seront les ordinateurs ultimes capables de dépasser l'intelligence humaine. C'est reparti de plus belle dans le n-importe-quoi-isme !

L'intelligence artificielle et l'informatique quantique semblent ne pas avoir de bornes. Elles illustrent cette volonté de puissance et d'omniscience de l'Homme, de modeler la matière si ce n'est les esprits et de disposer d'une capacité à prévoir le futur, quasiment à le rendre déterministe. A tel point que ce serait l'abandon du libre arbitre[548].



[548] Comme le laisse entendre cet article de The Atlantic de juin 2018, dont le titre n'a d'ailleurs pas grand chose à voir avec le contenu !

A elle toute-seule, la physique quantique a généré son lot de questionnements et de certitudes sur la nature du monde. L'indéterminisme de la mesure de l'état des quantums est devenu celui de la vie. L'intrication quantique a fait germer des explications pseudo-scientifiques de la télékinésie et de la transmission de pensée. Nous avons vu dans la partie précédente comment la médecine quantique mélange le nano et le macro de manière quelque peu cavalière.

La nature mécanique ou pas de la conscience est en jeu. Pour l'**épiphénoménisme** (définition), notre conscience est le résultat de phénomènes physiques dans notre corps et notre cerveau mais sans effets physiques externes directs. Le comportement est le résultat de l'action du cerveau sur les muscles.

Pour le **mystérianisme**, la compréhension de la conscience est hors de portée de l'Homme. Comme la conscience dépend à bas niveau de phénomènes quantiques qui régissent a-minima les relations entre atomes des molécules de notre cerveau, certains en déduisent un peu rapidement que l'informatique quantique permettrait à l'IA de devenir générale comme dans ce débat ! Mais ce ne sont à ce stade que des élucubrations.

Là-dessus, des projets ambitieux comme le **Human Brain Project** européen piloté par le Suisse Henri Markram visent à simuler dans un ordinateur le comportement du cerveau et donc à en comprendre le fonctionnement de bout en bout, même si ce n'est pas envisageable de le faire à une échelle ne serait-ce que moléculaire. Dans une autre veine, la capacité des ordinateurs quantiques de simuler des phénomènes quantiques a aussi entretenu l'idée que nous étions nous-même les objets d'une grande simulation.

Une exploration des arcanes du calcul quantique et des théories de la complexité permet de remettre les pieds sur Terre. Les théories de la complexité décrivent diverses limites à la nature des problèmes qui peuvent être résolus avec l'informatique quantique. La toute puissance calculatoire n'existe pas encore. On sera toujours obligé d'utiliser diverses formes de réductionnisme pour simuler le monde, à savoir qu'on ne pourra le faire correctement qu'à des échelles "macro" et pas "micro" ou "nano" pour des questions d'ordre de grandeur de calcul. Un peu comme on prédit la météo grâce à la méthode des éléments finis applicable à de grandes portions de ciel et pas au niveau de chaque molécule d'eau.

Les limites du possible seront sans cesse repoussées mais elles subsisteront. Nos moyens physiques ne permettront probablement jamais de simuler notre monde in-extenso. Il ne faut pas oublier que la physique quantique introduit aussi beaucoup de chaos et de l'aléatoire dans le biologique qu'aucun ordinateur ne pourra jamais entièrement simuler et contrôler.

Finalement, cette citation de Scott Aaronson résume bien d'ailleurs la quête du calcul quantique.

Celle-ci serait justifiée par la volonté de contrer ceux qui disent que c'est impossible. Le reste étant la cerise sur le gâteau [549]. C'est évidemment un trait d'humour à prendre au second degré !

"For me, the single most important application of a quantum computer is disproving the people who said it's impossible. The rest is just icing on the cake"
Scott Aaronson

source : A tale of quantum computers de Alexandru Gheorghiu (131 slides)

Religions et mysticisme

Depuis quelques millénaires, l'espèce humaine a pris l'habitude de consacrer un culte à une ou plusieurs puissances divines supérieures de nature imprécise, mais expliquant tout et le reste. L'Homme a probablement commencé à attribuer cette puissance aux phénomènes naturels qu'il ne pouvait pas expliquer comme le Soleil ou les étoiles. L'Homme est ensuite passé de systèmes de dieux multiples à un Dieu unique tout puissant. En quelque sorte, les religions monothéistes ont réalisé avant l'heure la théorie de l'unification tant recherchée par les physiciens. Cette Histoire est racontée avec recul par **Yuval Harari** dans Sapiens et avec cynisme par **Richard Dawkins** dans The God Delusion.

Pour certains scientifiques ou croyants en un au-delà, la physique quantique renouvèle les velléités d'expliquer le fonctionnement de l'Univers par une puissance divine. Elle donne l'impression de se fournir une explication scientifique ultime du tout, de Dieu, et de sa capacité à tout contrôler et superviser[550].

La fonction quantique la plus souvent mise en avant est l'intrication. Elle permet d'envisager l'existence d'un être suprême qui, grâce à ce phénomène physique, peut contrôler toutes les particules de l'Univers et à distance. Elle expliquerait aussi des phénomènes étranges de synchronicité. La dualité onde-particule permet aussi d'imaginer ou expliquer plein de scénarios magiques comme la guérison à distance, la télékinésie ou la télépathie[551].

Certains des protagonistes de ces théories sont eux-mêmes des scientifiques de la physique quantique.

---

[549] La citation provient de A tale of quantum computers de Alexandru Gheorghiu (131 slides, slide 31). Pour en savoir plus sur ces débats, voir notamment Quantum Darwinism, Decoherence, and the Randomness of Quantum Jumps de Wojciech Zurek, 2014 (8 pages), The Combination Problem for Panpsychism de David Chalmers (37 pages) et Why Philosophers Should Care About Computational Complexity de Scott Aaronson (59 pages) ?

[550] Voir à ce sujet la fiche Wikipedia qui décrit succinctement le mysticisme quantique.

[551] On trouve un bon inventaire de ces différents débats dans The Quantum God An Investigation of the Image of God from Quantum Science, 2015 (81 pages) qui évoque notamment la notion de conscience de l'Univers. Voir aussi le presque parodique Rien n'est solide « Tout est énergie ».

L'un des plus connus est **David Bohm** (1917-1992) qui se rapprocha du spiritualisme indien à partir des années 1960… au même moment que les Beatles ! Il était convaincu que les lois de l'Univers étaient gouvernées par un esprit[552]. Il est l'un des initiateurs des théories de la **cognition quantique**, un champ des théories cognitives qui s'appuie sur le formalisme mathématique de la mécanique quantique, et en s'appuyant sur des analogies.

La littérature sur cette question est parfois édifiante comme Google's Quantum Computer May Point People to God, qui date de 2013.

Selon l'auteur (anonyme), un ordinateur quantique parfait pourrait tenter de simuler l'apparition de la vie sur Terre et démontrer par l'absurde qu'elle ne serait pas possible sans une intervention divine. Mais qui dit que le résultat ne serait pas le contraire ?

L'informatique quantique permettrait d'invalider les théories classiques de l'évolution. Ils ne précisent pas le nombre de zillions de qubits intriqués dont il faudrait disposer pour étayer cela. Bien entendu, car ils n'ont aucune idée des algorithmes à utiliser. C'est de la fumette !

Tout cela relève de la religion-science-fiction et peut générer des débats enflammés avec des interlocuteurs qui ne seront jamais sur la même longueur d'onde, les uns adoptant une démarche scientifique classique et les autres, relevant du mysticisme et d'une approche plus émotionnelle. Quoi qu'il arrive, cela sera un débat de sourds.

Ethique des usages du calcul quantique

L'éthique des usages de l'intelligence artificielle est devenue relativement récemment un véritable sujet politique. Il était très apparent dans le **Rapport de la Mission Villani sur l'intelligence artificielle** en mars 2018 ainsi que dans un rapport de la Chambre des Lords au même moment et sur le même sujet au Royaume-Uni. Il mettait en avant le besoin de s'assurer, au minimum moralement, que les solutions à base d'IA respectaient la société et évitait notamment de générer ou de perpétuer des discriminations du fait des données utilisées.

D'où deux sujets saillants comme l'explicabilité des algorithmes et les limites de la manipulation de nos émotions, notamment via des robots plus ou moins humanoïdes.

[552] Voir à ce sujet Lifework of David Bohm - River of Truth de Will Keepin, 2016 (22 pages).

La difficulté à expliquer le fonctionnement de certains algorithmes de deep learning a été quelque peu montée en épingle. S'il est vrai que le fonctionnement de réseaux de neurones multicouches est quelque peu abstrait pour le commun des mortels, il l'est tout autant pour quasiment n'importe quel logiciel, avec ou sans IA, qui peut affecter notre vie courante. Mais on l'a un peu oublié. Lorsqu'un logiciel du groupe Visa vous refuse votre paiement de carte bancaire à l'étranger, on ne vous explique quasiment jamais le pourquoi du comment. Les techniques bayésiennes de détection de fraude ne sont pas documentées pour le grand public. Et on ne les rattache pas forcément à l'intelligence artificielle !

Le calcul quantique risque d'amplifier cette quête d'explicabilité. Elle est encore moins évidente à assouvir avec les algorithmes quantiques dont nous avons pu voir qu'ils suivaient une logique que peu de développeurs d'aujourd'hui peuvent appréhender. Les algorithmes quantiques risquent bien d'être encore plus compliqués et moins compréhensibles que ceux de l'IA d'aujourd'hui. Leurs biais éventuels ne viendront pas forcément des données qui les alimentent car, pour un temps certain, les calculateurs quantiques n'exploiteront pas de gros volumes de données. On pourra donc parler au sens propre du terme de biais des algorithmes alors que lorsqu'on évoque ce terme au sujet de l'IA, on évoque en fait beaucoup plus le biais des données qui alimentent les algorithmes que le biais de ces derniers.

Mais on jugera au cas par cas. Selon que les applications du calcul quantique gèrent la circulation automobile, la gestion de la distribution d'énergie, la création de nouvelles molécules en chimie ou biologie ou aident la NSA à décrypter les communications privées, les enjeux ne seront pas les mêmes.

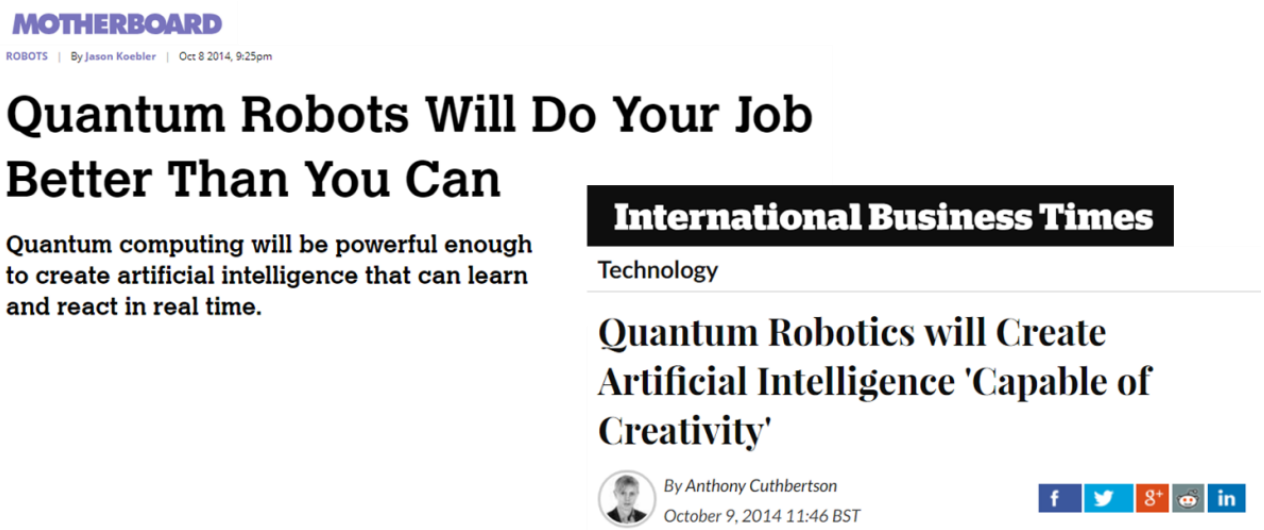
Une question éthique émergera sans doute devant les autres. Elle sera associée à un pan entier des applications du calcul quantique : la simulation de la dynamique de molécules organiques. Elle sera probablement limitée aux débuts à la simulation de molécules relativement simples. La simulation du repliement de protéines complexes est une hypothèse qui n'est pas encore validée. Dans un futur hypothétique lointain, on saura peut-être simuler l'assemblage d'un ribosome, l'une des molécules du vivant les plus sophistiquées qui soit avec ses 300 000 atomes et 74 composantes qui se regroupent un peu magiquement, et qui servent à fabriquer des protéines à partir des acides aminés et du code de l'ARN messager, issu de la réplication du code des gênes de l'ADN.

L'une des grandes avancées dans l'explicabilité des algorithmes quantiques vient de la chercheuse **Urmila Mahadev** dont les travaux étalés entre 2012 et 2018 ont permis de créer une méthode de vérification des traitements d'ordinateurs quantiques. Elle était postdoc à Berkeley et soutenue par Scott Aaronson et Umesh Vazirani, deux éminences de la recherche en algorithmie quantique.

Ses travaux, pas du tout évidents à saisir, visent à permettre de prouver qu'un ordinateur quantique a bien réalisé les traitements qu'on lui a demandés de faire. Elle montre qu'un ordinateur classique couplé à un ordinateur quantique simple peut vérifier de manière polynomiale les résultats d'un ordinateur quantique[553]. La méthode exploite une technique de cryptographie post-quantique que le vérifieur ne peut pas casser (LWE : Learning With Errors). Les LWE font partie de la classe des Lattice-based cryptography (EN) ou réseaux euclidiens (FR)[554].

Lorsque l'on simulera ce fonctionnement pour ensuite l'altérer, par exemple pour créer de nouvelles thérapies, le rejet des OGM ou des vaccins sembleront être de lointains soubresauts du passé. De nouvelles peurs se construiront et les scientifiques devront redoubler d'efforts pour éviter qu'elles se propagent.

Des peurs irrationnelles vont émerger du fait d'exagérations sur les capacités des ordinateurs quantiques. On entend déjà parler de "robots quantiques", ce qui ne veut rien dire, mais peut impressionner.


MOTHERBOARD

ROBOTS | By Jason Koebler | Oct 8 2014, 9:25pm

Quantum Robots Will Do Your Job Better Than You Can

Quantum computing will be powerful enough to create artificial intelligence that can learn and react in real time.

International Business Times

Technology

Quantum Robotics will Create Artificial Intelligence 'Capable of Creativity'

By Anthony Cuthbertson
October 9, 2014 11:46 BST

L'exemple *ci-dessus* est éloquent de ce point de vue-là avec deux titres tapageurs dans la presse US en 2014[555] qui ne font, en pratique, que relayer une publication scientifique assez banale, Quantum speedup for active learning agents (15 pages) décrivant des algorithmes quantiques pour l'exécution de réseaux d'agents servant à la robotique apportant un gain de performance dit "quadratique", donc… pas exponentiel, donc, pas extraordinaire. On n'a pas fini d'en voir passer de cette couleur ! Il faudra à chaque fois décoder et prendre du recul. Le fact checking du quantique va devenir un boulot à temps plein !

---

[553] Voir une description de la méthode en langage presque natural dans Graduate Student Solves Quantum Verification Problem, octobre 2018 et deux publications de référence : Classical Verification of Quantum Computations, septembre 2018 (53 pages) et Interactive Proofs For Quantum Computations, avril 2017 (75 pages).

[554] Voir cette présentation décrivant le protocole LWE : An Introduction to the Learning with Errors Problem in 3 Hours (76 slides).

[555] Voir article 1 et article 2.

Formation et éducation

L'informatique quantique va faire perdurer et amplifier un paysage commun avec celui de l'intelligence artificielle : un gouffre entre ceux qui comprennent et ceux qui utilisent et une pénurie de compétences. Le premier va intervenir assez rapidement tandis que la seconde se manifestera avec un délai plus long.

L'informatique quantique est définitivement un monde de spécialistes, et il est encore plus abscons que nombre d'autres domaines liés au numérique. Aujourd'hui, ce monde est équilibré entre spécialistes de la physique de la matière condensée et des algorithmes et logiciels quantiques.

En extrapolant un peu et en s'inspirant de l'Histoire de l'informatique, on peut anticiper que la partie logicielle prendra progressivement le dessus lorsque le calcul quantique deviendra monnaie courante, surtout s'il débouche sur des applications dans l'ensemble des secteurs de l'industrie.

Dans l'économie numérique d'aujourd'hui, il y a bien plus de spécialistes du logiciel que des semi-conducteurs. Les économies d'échelle sont en fait bien plus grandes avec ces derniers entre producteurs et utilisateurs. Le quantique n'y échappera probablement pas, même si dans un premier temps, le marché des ordinateurs quantiques ne sera pas un marché de volume.

Nous aurons besoin de développeurs d'un nouveau genre qui auront des capacités d'abstraction bien meilleures, ou tout du moins différentes de celles des développeurs d'aujourd'hui. Au pire, des développeurs seront capables de créer des outils de développement qui permettront de se passer de ce niveau d'abstraction assez bas au même titre qu'aujourd'hui il n'est plus du tout nécessaire de maitriser le développement en macro-assembleur pour créer un site web en Wordpress !

A court terme, le besoin est grand de vulgariser le domaine et de sortir de son jargon technique. La lecture d'une bonne partie des parties de cette série en a probablement rebuté quelques-uns de ce point de vue-là. Je ne prétendais cependant pas adopter une démarche très grand public. Il faut procéder pas à pas. Il faut déjà commencer avec les habitués du numérique et du développement logiciel. S'ils peuvent appréhender les enjeux de l'informatique quantique, cela sera déjà un bon pas de fait. Ensuite, il faudra élargir progressivement l'audience.

La prochaine étape est celle de la formation et de la vulgarisation auprès des décideurs d'entreprises et aussi institutionnels. Elle deviendra d'autant plus importante que l'effet de mode va commencer à décoller, du fait des annonces tonitruantes qui ne manqueront pas d'arriver, notamment de la part des grands acteurs du secteur, et surtout Américains et Chinois. De ce point de vue-là, les acteurs européens du quantique devront aussi investir sur le terrain pour ne pas se laisser dépasser par les acteurs Américains puis Chinois.

Nous ferons aussi face à une pénurie de spécialistes et au manque de diversité chez ces spécialistes. Ce monde est déjà très masculin, avec peu de femmes chez les scientifiques du secteur, dans la lignée de l'informatique et de l'intelligence artificielle. Cette pénurie pourrait être encore plus forte qu'avec l'intelligence artificielle[556].

La spécialité est encore trop masculine en l'état. Je l'ai constaté en faisant le tour des stars du secteur côté scientifique comme entrepreneurial. Malgré tout, nous avons pu voir dans l'inventaire des scientifiques du quantique que l'on peut identifier des dizaines de femmes dans cette discipline qui peuvent servir de *role models*.

Il y a encore peu de startups crées par des femmes dans l'inventaire que j'ai pu en faire à part Silicon Quantum Computing (SQC, Australie), créée par la chercheuse **Michelle Simmons**, Quandela, cofondée par **Pascale Senellart** et VeriQloud cofondée par **Elham Kashefi**.

Le langage qui est utilisé autour du quantique est très masculin dans la forme[557]. C'est un langage où l'on évoque les notions de supériorité (supremacy) et d'auxiliaires (ancillae), le premier faisant écho à une autorité supérieure, et à l'actuelle "white supremacy" issue de l'Apartheid Sud-Africain et qui remue la sphère politique US. La seconde notion reprend la notion de "servante femme" en latin, d'esclavage et de ségrégation raciale, alors que le terme technique a été inventé en 1995. Ce sont de petites choses symboliques mais qui mériteraient d'être corrigées. On ne veut pas d'Handmaid's Tale dans le quantique ! La solution consiste à parler d'avantage quantique (« quantum advantage ») même si le sens est légèrement différent de celui de la suprématie quantique.

Qu'en est-il enfin du futur de l'emploi lié au quantique, question que se pose Sophia Chen dans Wired en juin 2018 ? C'est difficile à évaluer car on raisonne sur plusieurs décennies et sur des usages pas encore bien détourés.


WIRED

SOPHIA CHEN SCIENCE 08.06.18 08:00 AM

QUANTUM COMPUTING WILL CREATE JOBS. BUT WHICH ONES?

Il y aura comme avec l'IA, ceux qui savent et les autres, ceux qui codent et ceux qui exécutent ou utilisent, ceux qui créent la richesse et ceux dont l'emploi est menacé. Mais le calcul quantique ne génère pour l'instant pas de menaces spécifiques sur l'emploi car il permettra de faire des choses que l'Homme ne sait de toutes manières pas réaliser de manière traditionnelle aujourd'hui. Il n'y a pas de logique de remplacement, tout au plus d'optimisation comme pour les applications basées sur l'optimisation de graphes comme celui du "voyageur du commerce".

---

[556] La pénurie de compétences qui démarre dans le quantique est bien décrite dans The Next Tech Talent Shortage: Quantum Computing Researchers, octobre 2018.

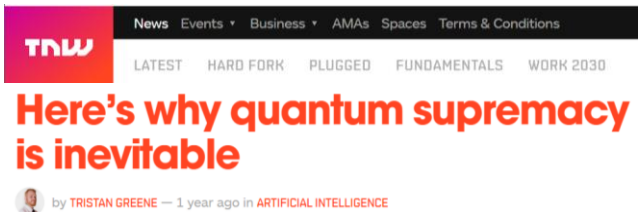
[557] Comme le relève très bien **Karoline Wiesner** de l'Université de Bristol dans son succinct The careless use of language in quantum information, 2017 (2 pages).

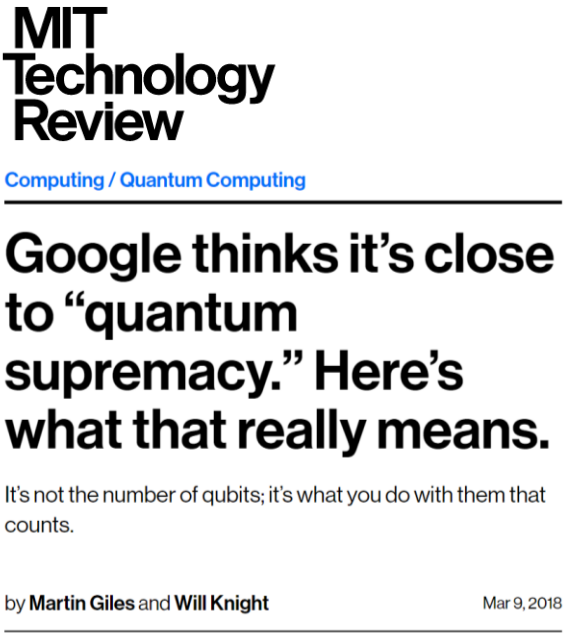
Il faudra en tout cas préparer de nouvelles générations d'ingénieurs dans un grand nombre de disciplines et en particulier dans celles des mathématiques et de la création de logiciels quantiques. Avec l'IA, c'est un nouveau défi pour l'enseignement supérieur qui se prépare[558]. Très peu d'écoles d'ingénieurs proposent des cours sur l'informatique quantique en France. Les premiers sont apparus à CentraleSupelec (Benoît Valiron, Zeno Toffano, Thomas Antoni), à l'Ecole Polytechnique (Alain Aspect, Silke Biermann), à l'ESGI à Paris (Alain Lioret) ainsi qu'à l'Ensimag (Grenoble). D'autres cours doivent exister dans d'autres écoles d'ingénieurs et universités, qui restent à inventorier.

Marketing du quantique par les acteurs du marché

Dernier point à évoquer, celui du rôle du marketing de l'offre. Comme je l'ai traité dans une série de 2014 sur les Propagandes de l'innovation, le marketing des fournisseurs et des analystes est celui qui fera le plus de bruit dans le domaine du quantique.

Nous allons être noyés sous une propagande innovationnelle qui brouillera le message. Les scientifiques du domaine ne reconnaitront plus leurs créations. Les articles de vulgarisation sur le calcul quantique vont continuer à démarrer les explications sur les qubits avec leur état superposé 0 et 1 et s'arrêter là [559]!





Le propre du marketing et de la communication sera d'embellir la mariée et de simplifier les faits par exagérations. Cela va commencer avec la notion de suprématie quantique qui sera valorisée à tort et à travers. On retiendra l'expression mais pas les détails de l'explication.

---

[558] Voir à ce sujet A la recherche des métiers quantiques de Fabien Goubet dans le journal suisse Le Temps, août 2018.

[559] Je vais plus loin que cela dans cet ebook mais ai conscience qu'il peut contenir des erreurs factuelles, interprétations erronées ou exagérations. Par contre, je les corrige au fil de l'eau lorsque je les découvre ou que l'on me les signale !

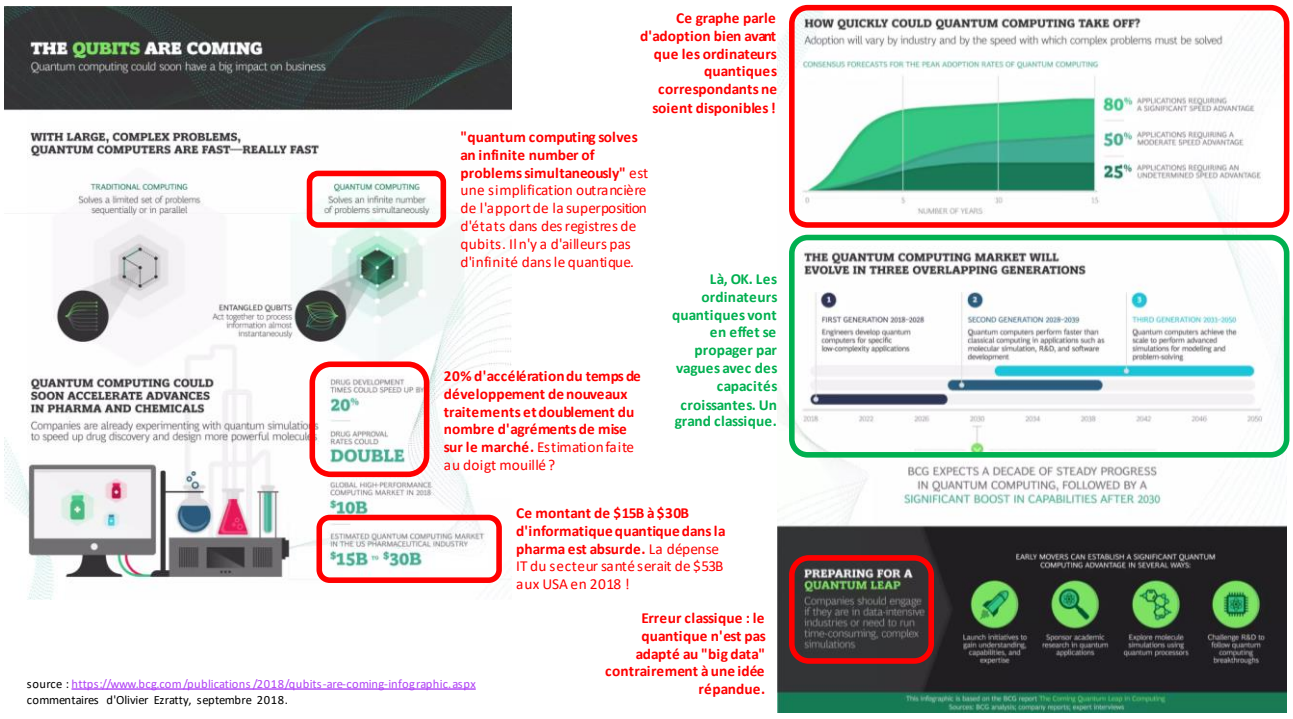
Dans certains cas, des offres accoleront le label “quantique” à des produits qui n’ont rien de quantique. C’est par exemple le cas des pico-serveurs en cloud distribués par la startup française R136.fr. L’enquête de Science et Avenir sur cette entreprise montre bien qu’il n’y a pas que le quantique qui y soit louche.

On voit déjà apparaître des analyses à l’emporte-pièce sur les usages du calcul quantique dans le big data, alors que ce n’est pas le premier domaine concerné. Cela se retrouve dans Informatique quantique et Big Data : une révolution pour l’analyse de données en août 2018.

Cet article est assez imprécis voire à côté de la plaque sur quelques points, et c'est un grand classique : *"Les ordinateurs quantiques ... peuvent être utilisés pour trouver des nombres premiers très larges. Il serait donc possible d’appliquer cette technologie au domaine de la cryptographie pour créer des systèmes de cybersécurité plus résistants."* alors que les ordinateurs quantiques permettent de factoriser des nombres entiers très grands en nombres premiers, mais les systèmes de cybersécurité plus résistants ne passent pas forcément par l'ordinateur quantique !

Ils s'appuient sur des clés quantiques QKD pour les systèmes à clés privées ou sur de la cryptographie post-quantique pour les systèmes à clés publiques, et sans passer par des ordinateurs quantiques.

Quant à l'exploitation en mémoire de grosses bases de données, elle nécessiterait un très grand nombre de qubits qui est difficile à obtenir, et qui plus est, de la mémoire quantique nécessaire pour exécuter le fameux algorithme de recherche de Grover et qui n'est pas du tout au point. Cela arrivera bien un jour, mais assez lointain.



Ce graphe parle d'adoption bien avant que les ordinateurs quantiques correspondants ne soient disponibles !

"quantum computing solves an infinite number of problems simultaneously" est une simplification outrancière de l'apport de la superposition d'états dans des registres de qubits. Il n'y a d'ailleurs pas d'infinité dans le quantique.

Là, OK. Les ordinateurs quantiques vont en effet se propager par vagues avec des capacités croissantes. Un grand classique.

20% d'accélération du temps de développement de nouveaux traitements et doublement du nombre d'agréments de mise sur le marché. Estimation faite au doigt mouillé ?

Ce montant de $15B à $30B d'informatique quantique dans la pharma est absurde. La dépense IT du secteur santé serait de $53B aux USA en 2018 !

Erreur classique : le quantique n'est pas adapté au "big data" contrairement à une idée répandue.

source : https://www.bcg.com/publications/2018/qubits-are-coming-infographic.aspx
commentaires d'Olivier Ezratty, septembre 2018.

Autre exemple de dérive, cette fois-ci dans un cabinet de conseil, avec cette infographie du **BCG** erronée à 80% qui fait la promotion du calcul quantique dans les industries pharamaceutiques[560] (*ci-dessus*).

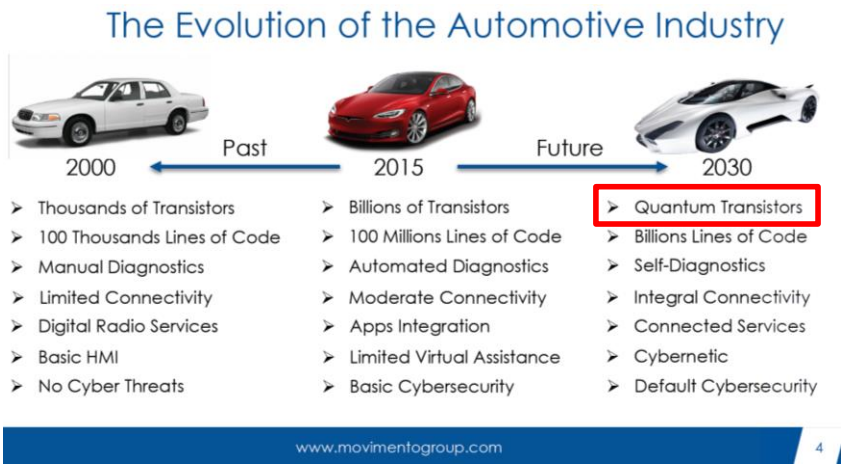
A force de grossir le trait, cela en devient absurde. Ainsi, en va-t-il lorsqu'ils évoquent la capacité d'un ordinateur quantique à résoudre une « *infinité de problèmes simultanément* » ! Tout d'abord, il ne s'agit pas d'infinité mais d'exponentialité et ensuite, la superposition dans un registre quantique n'est pas celle de problèmes mais d'états. Et cela permet de résoudre un seul problème à la fois. La nuance est peut-être sémantique et subtile mais importante.

Autre délire, celui de l'estimation du marché de l'informatique quantique dans les industries pharamaceutiques aux USA. Il est estimé entre $15B à $30B sans précision de date alors que l'ordre de grandeur de la dépense en informatique de l'ensemble du secteur de la santé aux USA serait de $53B aux USA en 2018 [561]!

Enfin, nous avons une courbe d'adoption des ordinateurs quantiques dans les entreprises selon le niveau de complexité des problèmes à résoudre, avant même qu'ils ne soient disponibles, surtout pour ceux qui ciblent les problèmes les plus complexes !

Et pourtant, je suis le premier des convaincus des bénéfices du calcul quantique dans les applications de pharmacie et notamment de simulation du comportement de molécules organiques ! Ces exagérations à l'emporte-pièce sont délirantes et me rappellent celles qui portaient sur les objets connectés il y a quelques années[562].

Dans la même veine, les **transistors quantiques** évoqués dans cette présentation de Movimento Group pour les véhicules autonomes de 2030, relèvent d'une méconnaissance de l'état de l'art du calcul quantique, de sa vitesse de progression et de la nature physique des qubits (source).



Sachant que les transistors font depuis leur création appel à des phénomènes quantiques ! C'est donc une exagération relativement sage !

---

[560] Source : https://www.bcg.com/publications/2018/qubits-are-coming-infographic.aspx.

[561] Source : https://www.ranosys.com/blog/industry/healthcare/healthcare-technology-trends-predictions-for-2018/.

[562] Voir La grande intox des objets connectés, août 2015.

Fumisteries quantiques

L'un des sujets les plus fascinants de l'impact grand public de la physique quantique est la manière dont certains s'emparent de la thématique pour l'intégrer dans des approches scientifiques alternatives, généralement douteuses. Le vaste cadre de la "médecine quantique" est un courant de pensées et de pratiques assez cohérent de ce point de vue-là, nous allons le voir. D'autres domaines comme le management et le marketing sans compter la politique[563] se sont aussi anecdotiquement emparés de la mécanique quantique, mais plutôt comme une source d'inspiration par analogies.

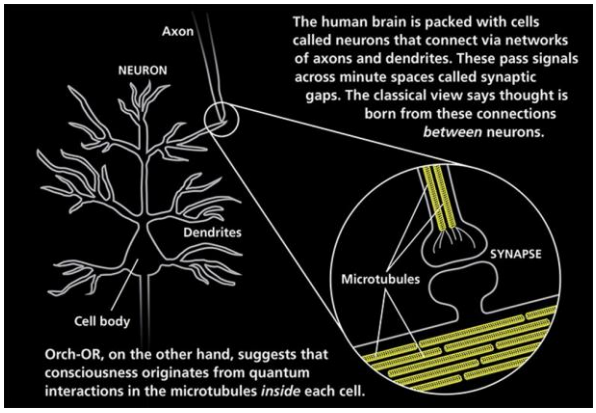
Biologie quantique

Le point de départ de la médecine quantique est pourtant scientifiquement pertinent et intéressant. Certains phénomènes biologiques s'expliquent bien à bas niveau par la physique quantique.

Pour n'en citer que quelques exemples, c'est évidemment le cas de la **photosynthèse** dans les plantes, qui fait jouer l'effet photoélectrique transformant un photon en déplacement d'électron, entraînant la génération de glucose, servant au stockage de l'énergie. Il en va de même dans le fonctionnement des **cônes et bâtonnets dans la rétine** qui captent la lumière. Les **rayons UV-B** participent à la synthèse des précurseurs de la Vitamine D3 dans la peau (source).

La physique quantique explique aussi la **captation du magnétisme terrestre** dans le cerveau de nombreux oiseaux via une protéine spéciale appelée cryptochrome. Il semblerait que ce mécanisme fasse appel à la capacité de la protéine à détecter des variations magnétiques grâce à l'intrication quantique d'électrons (source).

Des scientifiques de renom cherchent aussi à expliquer l'origine de la conscience par la physique quantique. Plusieurs grandes écoles de pensée sont reliées entre elles : la **théorie Orch-OR** de Roger Penrose et Stuart Hameroff, celle de la dimension **holographique de l'ADN**, portée notamment par Peter Gariaev et Luc Montagnier et celle des **biophotons** de Frantz Popp.

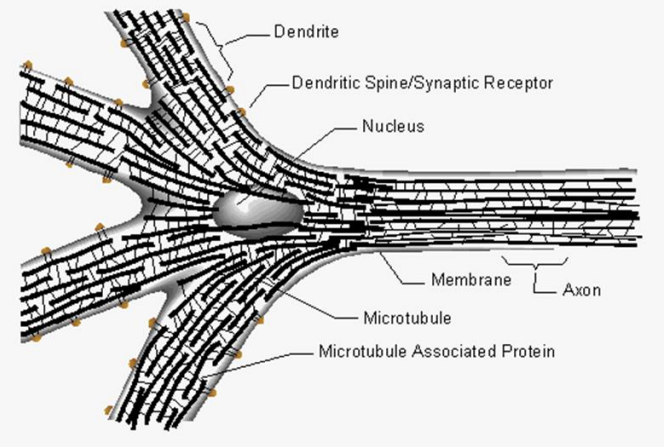


Elles n'ont pas l'assentiment d'une majorité de scientifiques mais méritent tout de même un petit examen.

---

[563] Le concept de politique quantique est encore balbutiant, même du côté du fumage de moquette. J'ai trouvé un peu de littérature de chercheurs en économie et en sciences sociales sur le sujet, mais ils ne mènent pas bien loin. Voir par exemple Quantum like modelling of the non-separability of voters' preferences in the US political system de PolinaKhrennikova, Université de Leicester (13 pages) cherche à modéliser les choix des électeurs américains et l'intrication ou pas du choix du candidat à la présidentiel et des candidats aux élections pour le Congrès montrant que celui-ci peut se découpler sous certaines conditions. Et Quantum Politics: New Methodological Perspective de Asghar Kazemi, 2011 (15 pages) fait un lien avec la théorie du chaos et l'effet papillon. Le papier a été écrit juste après les révolutions arabes de l'année.

Selon **Roger Penrose** (Anglais, 1931) et **Stuart Hameroff** (Américain, 1947), la conscience serait logée et gérée par les microtubules, ces structures fibreuses complexes qui constituent avec les filaments d'actine et les filaments intermédiaires la structure des cellules, dénommée cytosquelette, et dans le cas des neurones, celle des dendrites, synapses et axones[564].



Ils ont proposé en 1996 le modèle **Orch-OR** (Orchestrated Objective Reduction) selon lequel ces microtubules étaient des systèmes quantiques cohérents expliquant la conscience.

Pour eux, la conscience est gérée dans les neurones dans ces microtubules et non pas par leurs interconnexions via les couples dendrites/synapses. D'ailleurs, ils parlent de conscience, mais la question se pose sur la mémoire elle-même que l'on ne sait pas encore loger avec précision dans les structures neuronales du cerveau.

En 2011, Penrose et Hameroff ont même avancé que ces microtubules seraient des nano-ordinateurs quantiques capables de gérer des qubits et des calculs associés[565]. Si c'était vrai, la puissance de cet ordinateur en nombre de qubits serait incommensurable car un neurone comprend environ 100 millions de tubules, le cerveau 86 milliards de neurones et plus de 600 trillions de liaisons entre neurones !

L'impact indirect de ce dimensionnement énorme est de repousser encore plus loin dans le temps une éventuelle singularité, moment où un ordinateur atteindrait la capacité de calcul d'un cerveau humain en puissance de calcul brute[566].

Largement contestée par d'autres scientifiques, la théorie Orch-OR a connu un regain d'intérêt en 2014 avec la découverte de vibrations quantiques dans les microtubules par un certain Anirban Bandyopadhyay du National Institute for Materials Science au Japon[567].

---

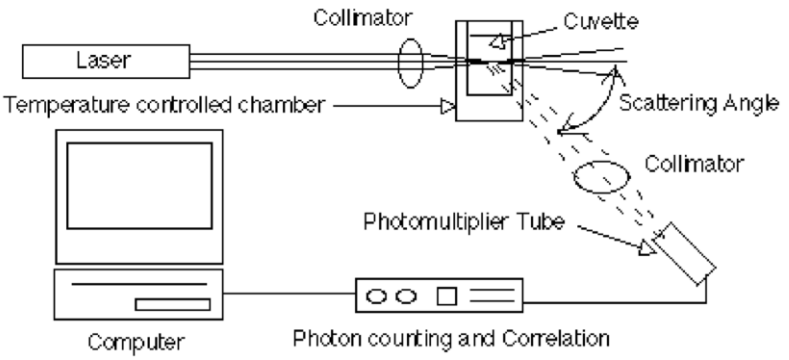
[564] Source de l'illustration : Notre cerveau est-il un ordinateur quantique ?, de Laurent Sacco, avril 2018.

[565] D'autres théories pensent que l'intrication quantique fonctionne également ailleurs dans le cerveau, au niveau des atomes de phosphore associés à du calcium. Cela permettrait la création de liaisons quantiques entre neurones. Voir Un nouveau spin dans le cerveau quantique de Jacqueline Charpentier, 2016. Le papier fait référence à Quantum Cognition: The possibility of processing with nuclear spins in the brain de Matthew Fisher, 2015 (8 pages). Comme l'indique l'article, cela pose des questions mais ne fournit pas de réponses ! Donc, toute interprétation un peu rapide sur le « cerveau quantique » est à prendre avec des pincettes.

[566] Voir Consciousness in the Universe Neuroscience, Quantum Space-Time Geometry and Orch OR Theory de Roger Penrose, 2011, 50 pages). Tout cela est documenté dans Orchestrated Objective Reduction of Quantum Coherence in Brain Microtubules: The "Orch OR" Model for Consciousness, 1996 (28 pages) ainsi que dans Consciousness, Microtubules, & 'Orch OR' A 'Space-time Odyssey' de Stuart Hameroff, 2013 (28 pages), Are Microtubules the Brain of the Neuron de Jon Lieff, 2015 et vulgarisé dans The strange link between the human mind and quantum de Philipp Ball, 2017.

[567] La découverte est contestée par Matti Pitkanen dans New Results about Microtubules as Quantum Systems, 2014 (18 pages).

L'ADN aurait aussi une fonction quantique. Un curieux papier d'origine Russe, Allemande et Anglaise décrit des phénomènes quantiques et de non localité dans l'ADN, vérifiés dans une fameuse expérience à base de diffraction de lumière laser (*ci-contre*)[568].



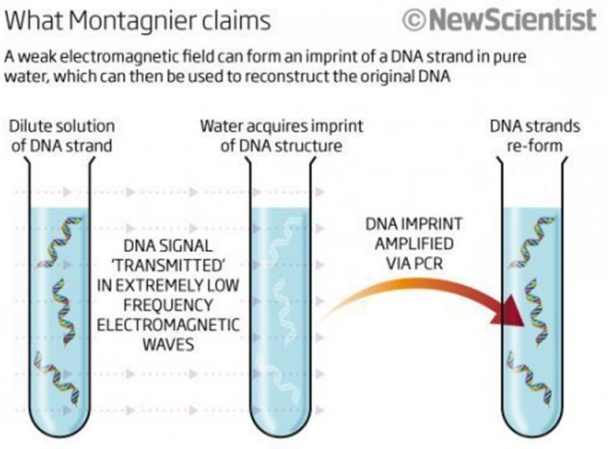
L'onde ADN bio-numérique (20 pages) explique que l'ADN est en fait un hologramme, qui interagit avec son environnement avec des radiations lasers. Via l'intrication quantique, les chromosomes de plusieurs cellules interagiraient entre eux via ces radiations.

Le Russe de l'histoire et leader de ces travaux est un certain **Peter Gariaev**, créateur de la notion de BioHologrammes au sein de son **Wave Genetics Institute** à Moscou[569].

Plus près de chez nous, **Luc Montagnier**, à l'origine du premier traitement contre le SIDA et prix Nobel de médecine en 2008, décrit les ondes de basse fréquence (7 Hz) émises par les brins d'ADN, ondes qui seraient transmises à de l'eau et réutilisées pour régénérer de l'ADN par PCR (processus de démultiplication d'ADN, "réaction en chaîne par polymérase") à partir d'eau purifiée.

Une thèse qui néglige un tant soit peu le besoin de disposer de quelques atomes de carbone, de phosphore et d'azote qui composent l'ADN en plus que l'oxygène et l'hydrogène qui sont déjà dans l'eau.

En fait, ceux-ci proviennent peut-être bien des molécules organiques fournies par la PCR elle-même[570].



Les travaux de Luc Montagnier ont un lien de parenté avec ceux de l'Italien **Emilio Del Giudice** sur la structure de l'eau liquide[571].

---

[568] Voir DNA as Basis for Quantum Biocomputer 2011 (22 pages),

[569] L'Histoire de la thématique est explorée dans Quantum BioHolography A Review of the Field from 1973-2002, de Richard Alan Miller, Iona Miller et Burt Webb (23 pages) mais sans que ces textes puissent permettre de s'en faire une idée de la validité scientifique.

[570] Voir les explications dans La téléportation quantique de l'ADN, 2011 et dans l'article de Luc Montagnier DNA waves and water de janvier 2010 (10 pages). Montagnier et la téléportation quantique de l'ADN de Vincent Verschoore, janvier 2011, est la source de l'illustration.

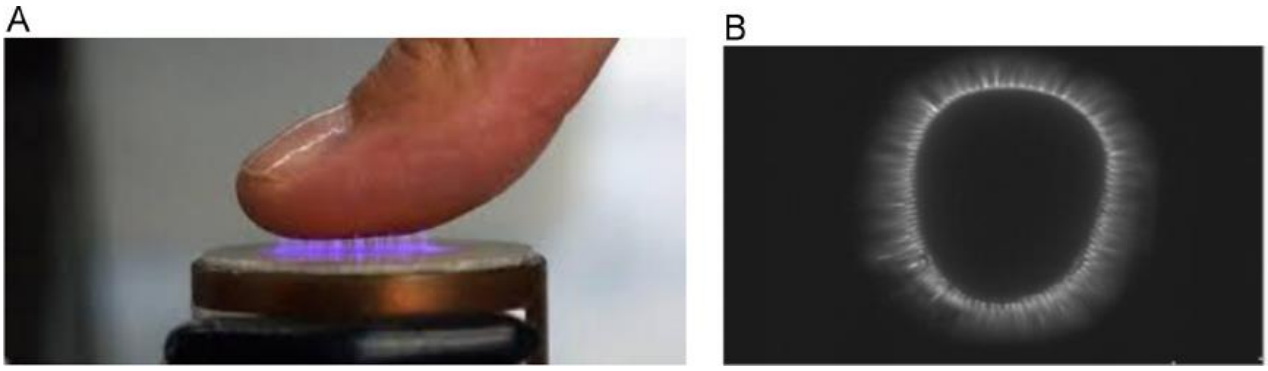
[571] Voir Illuminating Water and Life de Mae-Wan Ho, 2014 (18 pages) qui décrit les théories de Emilio Del Giudice, qui est décédé cette même année.

Cela ne vous surprendra pas d'apprendre que ce genre de découverte est plutôt controversé chez les spécialistes.

Dernière école "alternative", celle des **biophotons**. Ce sont les faibles émissions de lumière dans le visible générées par les êtres vivants. Elles ont été découvertes en 1922 par le Russe **Alexander Gurwitsch**. La théorie des biophotons a été perfectionnée par l'Allemand **Fritz Albert Popp** et complète à bas niveau celle de l'ADN hologramme. Elle décrit l'émission de photons par les molécules comme l'ADN, mais aussi celle qui est liée au métabolisme énergétique des cellules comme la transformation des molécules d'ADP en ATP dans les mitochondries des cellules. Les biophotons seraient des émissions d'ultra-violet et de lumière visible, à des niveaux bien plus faibles que l'émission d'infrarouge moyen qui intervient autour des 12 microns de longueur d'onde. On pourrait détecter jusqu'à quelques centaines de photons par centimètre carré d'organe analysé, souvent, au niveau de la peau.

Ces biophotons seraient aussi une lumière cohérente – faite de photons de même fréquence - qui constituerait la composante clé d'une forme de communication intercellulaire[572]. Je me demande comment fonctionne cette communication : à quelle portée, du fait de l'atténuation évidente de la diffusion des photons et avec quel ciblage (direction, orientation).

Selon Fritz Albert Popp, les aliments crus émettraient plus de biophotons que les aliments cuits, et les végétaux crus bios cinq fois plus que les végétaux cultivés traditionnellement. Conclusion : mangez du cru et du bio ! Voilà aussi de quoi faire regretter à l'Homme préhistorique d'avoir découvert le feu !



En tout cas, la détection de biophotons sur les 10 doigts de la main permettrait de détecter des pathologies cardiaques[573]. Le scanner ClearView utilisé exploite un procédé curieux : il envoie une impulsion à haute tension qui créé un champ électromagnétique autour du doigt qui amplifie les biophotons qui sont émis. Cela excite les molécules dans l'air, créant un plasma entre le capteur et le doigt (*ci-dessus à gauche*) qui ionise l'air, générant l'émission d'UV et de lumière visible.

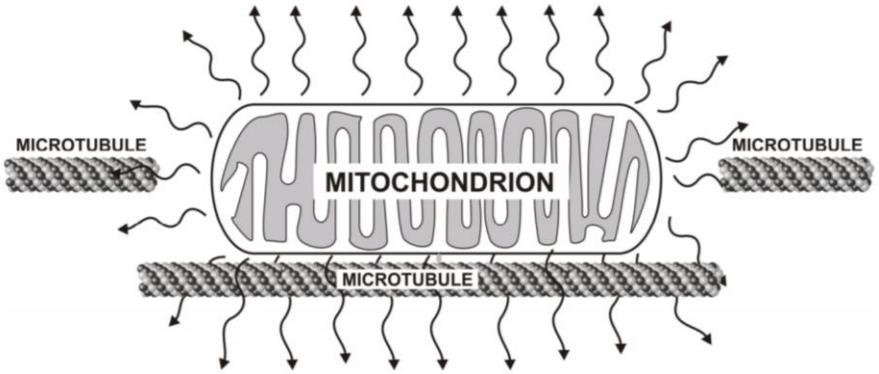
---

[572] Comme décrit dans Photonic Communications and Information Encoding in Biological Systems de S.N. Mayburov, 2012 (10 pages) et vulgarisé dans Biophoton Communication: Can Cells Talk Using Light?, 2012 dans la MIT Technology Review.

[573] Selon Detecting presence of cardiovascular disease through mitochondria respiration as depicted through biophotonic emission (11 pages).

C'est l'ionisation qui est captée par la caméra (*ci-dessus à droite*). Le logiciel analyse la forme générée et la compare à une base de pathologies. J'ai bien du mal à faire le lien entre la bioluminescence et ce procédé !

Et quid des récepteurs de ces biophotons ? Et bien, les microtubules des neurones, pardi [574] ! De quoi boucler la boucle. Dans les raccourcis proposés, selon Popp : "*la matière ne serait que de la lumière condensée*"[575].



Ah, et puis, les biophotons seraient une manière d'expliquer le chi. David Muehsam évoque de nombreux effets biologiques des biophotons, qui seraient notamment impliqués dans la régulation de la sécrétion de neurotransmetteurs (pour des rats) mais sans que la distinction entre corrélation et causalité soit visiblement faite dans les publications associées[576].

Les acquis scientifiques établis, comme ceux qui sont encore sujets à caution, indiquent bien que le vivant dépend de la physique quantique à l'échelle subatomique voire moléculaire. Et il faut un sacré bagage scientifique et du temps pour évaluer ces différentes théories et comparer le pour et le contre.

Mais de là à utiliser tout cela pour vendre des guérisons miracles par le contrôle du corps par la conscience ! Les praticiens de la médecine quantique sont ainsi très souvent des psychosomaticiens exploitant le mysticisme et la méthode Coué pour générer, dans le meilleur des cas, un bon effet placebo qui peut fonctionner sur certaines pathologies légères. Quand bien même ils justifient leurs méthodes sur les travaux contestés de chercheurs tels que Roger Penrose et Stuart Hameroff, déjà cités, mais aussi Karl Pribram et Henry Stapp, qui veulent expliquer la conscience humaine par des phénomènes quantiques intervenant à bas niveau dans le cerveau. Voir qui expliqueraient une soi-disante immortalité[577].

La fiche Quantum Mind de Wikipedia relate les évolutions de cette branche et les critiques associées. Elle souligne surtout le fait que rien ne permet d'appliquer d'éventuels phénomènes quantiques comme l'intrication à l'échelle de structures macroscopiques moléculaires ou cellulaires dans le cerveau.

---

[574] C'est ce qui ressort de Emission of Mitochondrial Biophotons and their Effect on Electrical Activity of Membrane via Microtubules, 2010 (22 pages, schéma *de cette page*).

[575] Voir à ce sujet Introduction de la conscience dans la matière de la physique quantique à la biologie (18 pages) de Jacqueline Bousquet ancienne du CNRS, décédée en 2013.

[576] Voir The Energy That Heals Part II: Biophoton Emissions and The Body of Light, David Muehsam, avril 2018.

[577] Voir Des physiciens apportent la preuve que l'âme est immortelle et qu'elle subsiste après la mort, sur InfoChrétienne, novembre 2016.

Cette intrication est encore moins justifiable pour relier à longue distance le cerveau à la "*conscience globale holographique de l'Univers*" promue par **Karl Pribram** et **Paola Zizzi**[578]. Au même titre, cela n'a pas forcément de sens de relier esprit et matière comme ondes et particules et leur fameuse dualité. Cela mène sinon à des absurdités qui expliquent des phénomènes psychiques de synchronicité par l'effondrement de la fonction d'onde de la conscience, une explication aussi absurde que l'expérience de pensée du chat de Schrödinger[579]. Même si les théories de Penrose et Hameroff étaient vérifiées, le raccourci serait un peu trop rapide, passant très abusivement du nano-phénomène au macro-phénomène !

L'autre méthode couramment proposée relève de l'utilisation d'ondes électromagnétiques diverses, dont les fameuses et fumeuses **ondes scalaires**. L'idée consiste à les exploiter pour rétablir des équilibres d'organes déséquilibrés, exploitant la dualité ondes-particules et la capacité à rétablir le niveau énergétique de base de… on ne sait pas trop. Surtout dans la mesure où les ondes proposées sont faiblement ciblées[580].

Il est notable, par contre, que peu de spécialistes scientifiques de la médecine quantique n'évoquent les capacités des futurs calculateurs quantiques pour simuler le fonctionnement de molécules organiques et créer de nouvelles thérapies. C'est explicable car les applications connues du calcul quantique dans la santé font partie de la médecine allopathique traditionnelle qu'ils cherchent à éviter ou tout du moins à compléter.

J'en ai cependant trouvé une vague trace chez le Finlandais **Matti Pitkanen** qui, dans le cadre de ses travaux sur la TGD (Topological Geometrodynamics), propose une théorie unifiée de la physique, et émet l'idée de créer des ordinateurs quantiques à base d'ADN[581]. Il pense que l'ADN communique "avec l'Univers". Il s'appuie aussi sur les expériences de Luc Montagnier sur l'ADN. Matti Pitkanen fournit les bases de théories très spéculatives sur la conscience supposée de l'Univers[582]. Ses théories d'unification de la physique sont tellement complexes qu'elles sont impossibles à comprendre, et, éventuellement, à valider par l'expérience ou à réfuter.

Médecine quantique

Comme le souligne la maigre fiche Wikipedia sur la médecine quantique, cette discipline utilise abusivement le jargon de la physique quantique pour noyer le poisson et faire avaler des couleuvres à des gens qui sont prêts à tout pour trouver des remèdes à certaines pathologies que la médecine traditionnelle, bien ou mal exercée, ne peut pas traiter[583].

---

[578] Dans Consciousness and Logic in a Quantum-Computing Universe, 2006 (25 pages).

[579] Voir Mécanique quantique et psychisme, de Giuliana Galli Carminati et et François Martin, 2007 (32 pages).

[580] Voir à ce sujet L'enjeu actuel du quantique par Jean-Michel Vaysse, 2016 (12 pages) qui positionne cette branche de la médecine quantique en faisant notamment référence à de nombreux travaux de chercheurs russes.

[581] Dans Quantum Mind, Magnetic Body, and Biological Body, Matti Pitkanen, août 2018 (186 pages).

[582] Dans TGD Universe as a conscious hologram, publié en février 2018 (612 pages).

[583] Voir aussi Sept idées fausses sur la physique quantique, de Julien Bobroff dans TheConversation, mars 2019.

Ces méthodes sont aussi bien décrites dans Quantox - Mésusages idéologiques de la mécanique quantique" de Richard Monvoisin, paru en 2013. Je crains fort qu'avec le bruit médiatique que l'informatique quantique va générer, on assiste à une recrudescence de la visibilité de la médecine quantique, en plus de l'effet Streisand limité qui sera généré par cet article.

Les méthodes utilisées sont assez facilement détectables pour l'esprit éveillé avec :

- Un **propos scientifique** associant un peu rapidement sciences humaines et biologie et faisant des raccourcis très rapides et approximatifs sur la physique quantique. Exemple avec "L'Univers Quantique", un livret gratuit de 26 pages de mybebooda (surtout slides 20 avec un baratin sur l'ADN et les photons, et qui cite un certain Wladimir Popenon alors qu'il s'agit de Vladimir Poponin et de son expérience d'ADN fantôme). Un charabia limite manipulateur.
- Quand ils existent, les **tests sont réalisés avec des échantillons trop faibles** pour être statistiquement représentatifs. Le propos associe souvent un bon nombre d'anecdotes ponctuelles non vérifiables. Les guérisons miraculeuses constatées à Lourdes sont même mieux documentées et d'ailleurs, aussi probables que celles qui interviennent en milieu hospitalier (source), à savoir comprises entre 1/350 000 et 1/100 000 cas.
- Nombre de spécialistes proposent la vente de **matériels de guérison divers**, assez chers, qui ne sont pas des dispositifs médicaux remboursés, et dont l'efficacité relève visiblement aussi de l'effet placebo. La brochure du 2e Congrès International des thérapies quantiques de Lyon en 2011 contient une très belle brochette d'exposants de ces appareils pour gogos. Parfois, c'est plus léger techniquement comme ce jeu de cartes de conscience quantique proposé par Richard Gandon aux voyants professionnels.
- Le **côté vague des pathologies couvertes**. Certaines relèvent de la gestion de la douleur ou de ce qui peut être traité par effet placebo, comme la psychonomie[584]. D'autres ciblent pèle-mêle toutes les grandes pathologies du moment : maladies chroniques, cancers et dans certains cas, même les maladies neurodégénératives.
- Des **CV à rallonge** avec des diplômes impressionnants et des cautions scientifiques à prendre avec des pincettes pour une bonne part des spécialistes de la médecine quantique. Il existerait même des "usines à diplômes" aux USA, où l'on peut à bon compte s'acheter un titre de docteur en médecine ou autre discipline de pacotille. Un peu comme dans feu l'Université Trump.
- Des **publications scientifiques** rares et quand elles existent, tout aussi rarement réalisées dans des revues avec validation par des pairs, sachant que cette validation n'est déjà pas suffisante pour être un gage de sérieux. Cela devient donc des publications "privées".

[584] Qui est une fausse science de plus associant l'esprit et le corps.

J'évoque ici les publications sur les traitements proposés et les explications somatiques, pas sur les sous-jacents scientifiques de bas niveau vus précédemment.

Ces différentes méthodes sont décrites avec humour par l'Institut Supérieur de Charlatologie et son générateur automatique d'argumentaire !

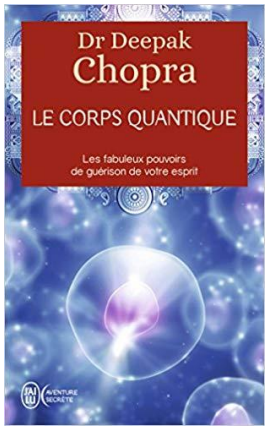
Il n'empêche que l'on trouvera des commentaires positifs des lecteurs de ces livres qui montrent que le marché des gogos est un marché florissant. Il s'inscrit dans un contexte de perte de confiance dans les politiques, dans les médias et dans les sciences et du développement de nombreuses théories du complot, alimentées par la fluidité d'Internet et des réseaux sociaux.

Des conférences sur le sujet de la médecine quantique ont été organisées, surtout entre 2011 et 2013, comme le Congrès Quantique Planète 2012 de Reims avec un large panel d'intervenants dont le fameux cancérologue Henri Joyeux connu pour ses positions contre les vaccins, notamment celui de l'hépatite B. Le Programme de l'édition 2013 est aussi consultable, avec un grand nombre de praticiens du monde de la santé qui se sont convertis à la médecine quantique et autres médecines alternatives.

Certaines de ces pratiques sont dénoncées dans des sites spécialisés tels que Psiram qui est lui-même d'origine douteuse ou tout du moins pas documentée. Il a son propre anti-site, Antispiram visiblement lancé par l'un des praticiens mis en cause, Christian Daniel Assoun et qui a obtenu par décision de justice en 2016 leur déréférencement sur Google pour la page le concernant (mais pas une modification de son contenu qui est toujours en ligne).

La médecine quantique est aussi dénoncée dans Vers une critique de la raison quantique: les approches transcendantales en mécanique quantique de Patricia Kauark-Leite, 2010 (509 pages) ainsi que dans La médecine quantique, révolution scientifique ou arnaque? de Coline Vasquez et Bruno Lus, dans Slate en décembre 2017.

Passons en revue quelques-uns des thèses et des ouvrages de référence qui font la promotion de cette curieuse médecine quantique.

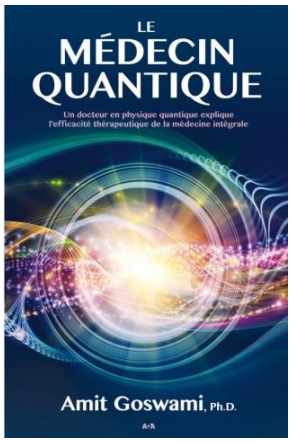


Le corps quantique, de Deepak Chopra (2009), ex-endocrinologue. L'auteur est issu du filon de la méditation transcendantale et devenu praticien ayurvédique, la médecine traditionnelle indienne. Selon lui, la pensée quantique explique certains cas de guérisons psychosomatiques qui ressemblaient à de l'auto-guérison. L'auteur est une star du domaine, surtout en Inde et aux USA, avec une prose vendue au total à plus de 10 millions d'exemplaires et une fortune personnelle estimée à plus de $80M (source). Le Corps Quantique semble être la traduction en français de *Quantum Healing* paru en 1988.

Le contenu de ses ouvrages est faiblement scientifique, surtout lorsqu'il évoque les notions de quantique, qui sont souvent plus métaphoriques que physiques. J'ai visionné à ce sujet l'éclairant débat entre Deepak Chopra et Richard Dawkins (Mexique, 2013, 1h13) qui met en avant la difficulté de réconcilier l'approche émotionnelle et symbolique de Chopra avec l'approche rationaliste et scientifique de Dawkins. Le débat porte à un moment sur l'intelligence supposée de l'Univers qui existe selon Chopra et à tous les niveaux, des particules élémentaires à l'Univers tout entier. Alors que cela n'a pas de sens pour Dawkins au-delà des êtres biologiques dotés d'un cerveau, ou d'ordinateurs l'imitant.

C'est un débat homothétique avec le lien entre la conscience et les pathologies que la conscience contrôlerait ou ne contrôle pas forcément. L'autre partie intéressante de ce débat concerne la notion de saut quantique sur l'apparition du langage ou certaines évolutions biologiques qui sont une vue de l'esprit pour Dawkins.

Ce dernier dénonce même "l'obscurantisme délibéré" de Chopra. Pour Dawkins, la conscience s'explique ou s'expliquera par les neurosciences et sûrement pas par le galimatias de la méta-conscience de Chopra.



Le médecin quantique d'Amit Goswami (2013) est dans la même veine que les théories de Deepak Chopra. L'auteur est un enseignant en physique indo-américain qui a exercé dans l'Oregon entre 1968 et 1997, mais pas dans la physique quantique. Il a un PhD en physique nucléaire et se définit comme un activiste quantique qui a même sa propre Université Quantique qui semble être à la santé ce qu'était la Trump University aux business schools. Selon lui, l'activisme quantique par la conscience peut sauver la civilisation. Il démontre aussi scientifiquement (!) l'existence de Dieu en reprenant des thèses de Deepak Chopra sur la conscience de l'Univers.

Dans son ouvrage qui est la traduction en français d'un livre paru la première fois en 2004, il explique l'efficacité thérapeutique de la "médecine intégrale" qui associe la médecine allopathique et les médecines plus ou moins douces, alternatives et traditionnelles, surtout indiennes mais aussi chinoises.

Le contenu scientifique de l'ensemble tient sur un timbre poste. Ca parle de causalité descendante du quantique et de la conscience sur la matière, un propos qui associe les pathologies d'un organe du corps humain à l'effondrement quantique de ses fonctions provoqué par la conscience. L'ouvrage cherche à expliquer les effets et préceptes de médecines orientales (chakras, réincarnation, médecine ayurvédique, acuponcture) par de la physique quantique de café du commerce[585].

[585] Source de l'illustration : Messengers and Messages—then, now, and yet to come (15 pages).

En voici quelques morceaux choisis avec les "*champs morphogénétiques du corps vital*", "*quand l'esprit crée la maladie, il arrive que la guérison soit impossible à réaliser sur le plan de l'esprit. On doit alors faire un saut quantique jusqu'au supramental pour guérir*" ou "*l'effondrement quantique est aussi fondamentalement non local. Par conséquent, la non-localité de la guérison, comme dans la guérison par la prière, trouve une explication limpide dans le cadre de la pensée quantique.*".

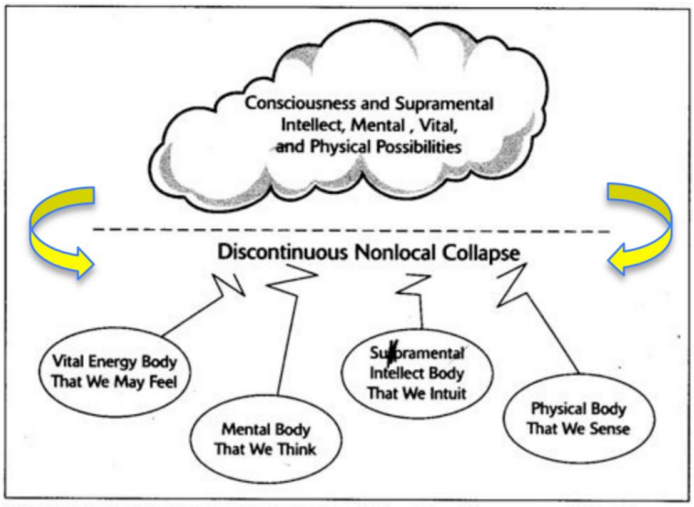


FIGURE 1-5. Quantum psychophysical parallelism. Consciousness mediates for physical, vital, mental, and supramental domains of quantum possibilities functioning in parallel.

Donc, avec de l'intrication quantique, on peut relier tout à tout et tout expliquer.

D'autres que lui ont une vision légèrement plus scientifique de la nature quantique de la conscience, comme Ervin Laszlo même si ce dernier s'appuie un peu abusivement sur l'intrication quantique dans ses explications[586].

Amit Goswami évoque des guérisons à distance par la prière en faisant référence à une expérience du physicien **Randolph Byrd** réalisée en 1988. La représentation statistique y était très faible avec 6 guérisons sur 26 malades, de pathologies cardiaques pas bien précisées. Il a été en fait démontré que les prières n'avaient pas d'effets à grande échelle[587].

Il cite aussi l'expérience du Mexicain **Jacobo Grinberg-Zylberbaum** de télépathie[588]. Il s'agissait de la mesure d'ondes EEG sur un participant pour évaluer l'impact sur lui d'un éclair de lumière arrivant sur l'un des participants, les deux étant dans des cages de Faraday. L'expérience a été répétée plus tard entre 2000 et 2004 en s'appuyant sur de l'IRM[589].

Petit détail technique : il n'y a pas de transmission d'ondes radio entre les participants qui sont dans des cages de Faraday, pas de photon non plus, ni de particules ayant une histoire commune dans le cerveau des participants. Donc, a minima, l'explication quantique sauce "expérience d'intrication d'Alain Aspect" est douteuse.

---

[586] Dans Why Your Brain Is A Quantum Computer, 2010. Cette thèse est en partie déconstruite dans The Myth of Quantum Consciousness, 2002 (19 pages), même si c'est un écrit antérieur.

[587] Voir Studies on intercessory prayer, Wikipedia.

[588] Documentée dans The Einstein-Podolsky-Rosen Paradox in the Brain: The Transferred Potential, 1994 (7 pages).

[589] Voir les détails et les résultats.

La santé, applications quantiques 2012 est un ouvrage collectif avec une douzaine de contributeurs, coordonné par Lara Lellouche, présidente de l'ARTTIQ (Association de Recherche sur les Technologies et techniques Informationnelles Intégrées et Quantiques), qu'elle a fondée en 2009 et dont le site n'a pas été mis à jour depuis 2011.

L'ouvrage reprend les communications d'un colloque organisé par ses soins en 2011 et sponsorisé par Glycan, la société de Christian Daniel Assoun dont nous parlerons plus loin.

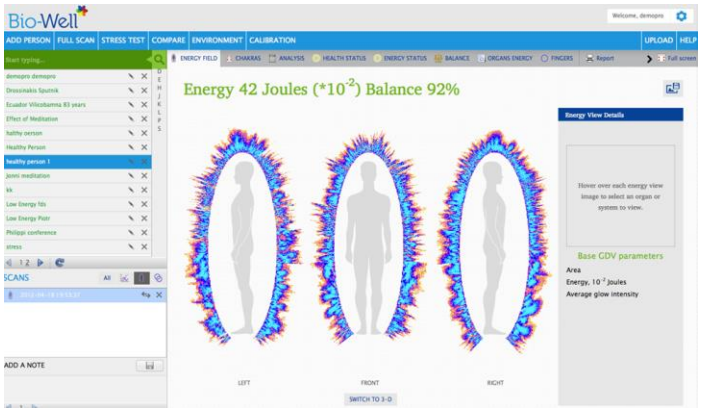
Les contributeurs sont des adeptes internationaux de médecines alternatives.

- **Christian Agrapart** propose des traitements de chromatothérapie, à savoir l'usage de rayonnements colorés à des fins thérapeutiques, ciblés organe par organe, avec délivrance par transmission oculaire, par acupuncture sur les zones malades ou par exposition directe sur la peau. Au menu, les engelures et brûlures sont traitées avec du rouge et de l'orange ("*L'orange neutralise l'excès de chaleur en appelant localement de l'énergie froide.*"). Le vert assécherait les pieds restés trop longtemps dans l'eau (une pathologie bien connue) et le pourpre traiterait la frigidité. Heureusement, ces techniques ne prétendent pas guérir les infarctus, les maladies neurodégénératives, les diabètes ou les cancers. Cela a en tout cas toutes les couleurs de la fausse science selon Sébastien Point (source, 2015). Mais bon, cela pourrait peut-être marcher dans certaines circonstances.
- **Nadine Schuster** fait de la psycho-neuro-immunologie opérant sur les états d'oscillation des cellules. On raccroche vite lorsque l'on voit comment elle relie la physique quantique au vivant : "*physique qui MESURE les photons par « paquets », c'est-à-dire les grains de lumière (ou quanta) intervenant dans TOUS les processus du vivant en tant que porteurs des informations qui l'organisent. Quand un photon frappe un atome de métal (en biophysique et en biochimie également), il chasse un électron d'une orbite à l'autre, d'un niveau d'énergie à l'autre en provoquant un rayonnement : on pourrait dire que la VIE « est » ce jaillissement permanent de lumières au sein même du corps humain*". Elle en oublie que le quantique ne concerne pas que les photons et que la photosynthèse fonctionne mieux sur les plantes que sur l'Homme ! Sa médecine "*répare les déséquilibres oscillatoires des cellules afin de ramener l'ordre, qu'on appelle néguentropie (la néguentropie est la transformation de l'antimatière en énergie), au sein du tissu vivant.*". C'est bien la première fois que j'entends parler du rôle de l'antimatière dans la biologie humaine. Elle affirme que "*les maladies auto-immunes sont en fait des processus d'autodestruction liés au manque d'amour",* une technique de manipulation qui permet d'éloigner les adeptes de leur propre entourage. La page de présentation de ses recherches est un panaché détonnant où elle fait notamment la promotion des systèmes à base d'ondes scalaires, que nous étudierons plus loin. Son activité est liée à IVI "Invitation à la Vie Intense", citée aussi plus loin.

- **Olivier Abossolo** est un anesthésiste qui fait la promotion de la médecine intégrative dans le cadre de chirurgie orthopédique. Il réduit le stress d'opérations avec des médecines douces diverses : surtout de l'aromathérapie, de l'homéopathie, des champs photoniques pulsés et magnéto-infrarouge laser. Cela permettrait la réduction de prises d'antalgiques.

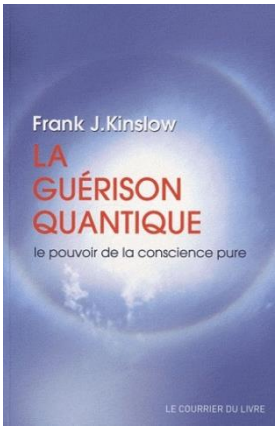
  Il est surtout le promoteur en France des bains de pieds dans l'eau salée et électrisée de l'Anglais Pura Détox dont une variante fonctionne à l'ozone et aux infrarouges. Il fournit des huiles essentielles de son cru pour agrémenter ces bains de pieds. Au minimum, cela doit bien détendre.

- **James Oschman** promeut un concept sur l'énergie vitale, à base de courants électriques. Il invente la notion des cellules périneurales du cerveau, qui ne sont visiblement que les cellules gliales qui entourent les neurones, mais avec un autre nom et qui génèrent de l'énergie qui va jusqu'aux mains.
- **Ravi Roy** est un Indien adepte de la médecine holistique séphirotique, qui utilise l'arbre séfirotique de la Kabbale (tradition ésotérique juive) comme support de méthode d'examen, de diagnostic, de traitement, applicable à toutes les disciplines médicales. Il utilise aussi l'astrologie appliquée à la médecine. Il n'y a rien de quantique ni de fantastique dans tout cela.
- **Christine Fageot** pratique le Feng Shui et son texte n'évoque rien de quantique du tout du tout. Le Feng Shui est référencé couramment comme une pseudo-science. Des descriptions extensives de la notion de pseudo-science sont fournies par Rory Coker dans Distinguishing Science and Pseudoscience, publié en 2011 ainsi que dans Seven Warning Signs of Bogus Science de Robert Park, publié en 2003. Le Feng Shui est décrit de manière critique comme un bric à brac ésotérique incohérent dans Alternative Medicine An Alternative Magical Mystery Tour de Steven Ranson, 2012 (129 pages, pages 72 à 77).
- **Luc Bodin** parle de l'homme créateur de l'Univers, du pouvoir de la pensée sur le corps, de magnétisme et de médecine énergétique. L'onde peut se transformer en matière et réciproquement. Toussa.
- **Konstantin Korotkov** est un Russe qui fait la promotion des caméras DGV Bio Well, des systèmes de détection d'aura autour des malades qui matérialiserait les chakras, via l'analyse de la "décharge gazeuse". Même pas de biophotons dans l'histoire ! Son texte est un amalgame de l'Histoire de l'Humanité et de la médecine, mais avec rien de quantique.



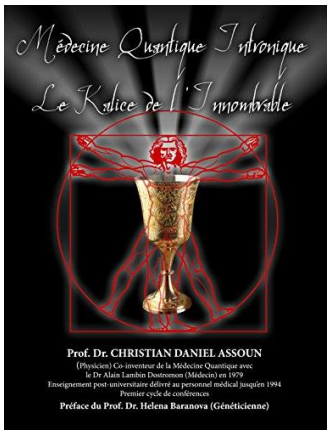
- **Kiran Schmidt** est un Allemand qui fait de la “médecine informationnelle”. Lui aussi fait la promotion de machines bizarres qui sont censée guérir de tout, notamment sous la marque **Inergetix**, qui n’a pas ou plus de site web.
- **Audun Myjska** parle aussi de médecine intégrée, qui fait l’association entre allopathie et médecines douces dans la lignée des méthodes d’Amit Goswami.
- **Nassim Haramein** parle de l’énergie de la création et aussi de la mémoire de l’eau, qui est comme il se doit quantique.
- **Vlady Sténanovich** est un Serbe qui veut aller dans le sens de la vie ce qui est plutôt sympa pour un médecin. Il parle d’émetteur d’ondes vives et de l’art du Chi. C’est le fondateur de “l’Ecole de la Voie Intérieure” en 1988, semble-t-il répertoriée comme une secte en 1995 en France.
- **Rav Michaël Laitman** est un Biélorusse qui promeut la force motrice de la nature et est aussi féru de la Kabbale.
- **Claude Lagarde** décrit l’énergétique des cellules et des réactions catalytiques diverses, de maintien du gradient sodium/potassium dans les cellules, notamment nerveuses ainsi que du rôle des oligoéléments. C’est la partie en apparence la plus sérieuse et la plus longue du livre. Le gars est le créateur du laboratoire **Nutergia**, spécialiste de la nutrition cellulaire active, en gros, de compléments alimentaires.

Voilà une sacrée équipée pour s’occuper de votre santé !



La guérison quantique de Frank J. Kinslow (2012) reprend si ce n’est singe les mêmes théories d’Amit Goswami sur la guérison par la conscience. Il introduit la notion de “Quantum Entrainment”, une méthode “*scientifique, rapide et efficace, qui permet de diminuer la douleur et de favoriser la guérison*”. En quelques mots, il s’agit de faire envoyer par votre conscience des ondes vibratoires à vos organes pour les guérir. Par le jeu des interférences, elles vont annuler le mal. Encore un coup à la sauce du chat de Schrödinger avec application de la mécanique quantique du pico (particules élémentaires) au macro (les organes).

Il s'adresse surtout aux douleurs physiques et émotionnelles. C'est une variante de la méditation. Pour le traitement de l'hypothyroïdie, il faudra éviter ! Ce genre d'ouvrage a la particularité d'être toujours très vague sur la notion de pathologie traitée, surtout si un appareil pseudo-médical est en jeu comme c'est ici le cas. Même si le "Quantum Entrainment" est censé fonctionner à distance[590].



Médecine Quantique Intronique du Suisse Christian Daniel Assoun traite de la biologie quantique. C'est une forme de traité d'épigénétique décrivant la mémoire de l'ADN par la mécanique quantique. Selon lui, "*L'EAU est le premier liquide quantique : son état actuel est liquide alors* (que) *son état devrait être gazeux !".* Hum hum.

ll met en avant les "*lois radiatives à l'ADN*-" correspondant aux thèses évoquées en début d'article. Ce livre décrit la présence d'un troisième caténaire d'ADN sous forme de plasma physique (hydrogène).

C'est aussi documenté dans Le 3ème Brin (ou 3ème Caténaire) de l'ADN ou DNA du même auteur et qui date de 2011/2012. Il y indique que son "*travail porte actuellement sur les parties INTRONIQUES qui représentent 95% de notre ADN et classées de injustement de silencieuses ou voire inutiles.".*

Intronique au sens des "introns" de l'ADN, la partie des gênes qui est transcrite en ARN lors de l'expression des gênes, mais éliminée lors de l'épissage qui permet de générer un ARN mature qui sera ensuite utilisé dans les ribosomes pour fabriquer des protéines. A vrai dire, les introns ne représentent que 25% de l'ADN humain.

Le reste, environ 73%, correspond à des séquences effectivement non codantes de l'ADN de nos chromosomes, mais dont le rôle dans les processus de régulation des gênes se révèle progressivement avec la recherche. Les exons, la partie codante des gênes représente 1,5% de l'ADN humain (source).

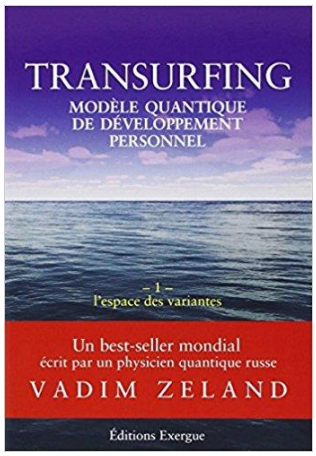
Christian Daniel Assoun pense que l'ADN pourrait se renforcer avec "*l'aide de nouveaux éléments tétravalents tels que le Germanium ou le Silicium (propriétés opto-quantiques reverses).*". Pourquoi le germanium et le silicium ? Car ils sont dans la même colonne du tableau de Mendeleïev que le carbone avec quatre électrons libres. Voilà une bonne idée pour créer de la vie extra-terrestre. Pourquoi donc la vie sur Terre n'a-t-elle pas utilisé le silicium qui est aussi abondant que le carbone ? L'une des raisons est que l'oxyde de silicium (SiO_2) est inerte et solide tandis que les oxydes de carbone (CO, CO_2) sont gazeux donc, plus facilement recombinables avec d'autres atomes et molécules. Enfin, le carbone est plus abondant que le silicium sur la surface de la Terre. Par contre, le SiO_2 est très utile dans les chipsets quantiques CMOS du CEA-Leti (procédé SOI et FD-SOI) !

[590] Si vous adhérez, l'auteur organise des séminaires en France sur sa méthode et la version anglaise de son ouvrage est téléchargeable ici.

Christian Daniel Assoun est aussi le fondateur de **Glycan Group**, en 1996. La société commercialise du silicium organique pour différents usages et notamment comme complément alimentaire. Leur filiale Glycan Pharma a été radiée du registre du commerce en 2012. La société est en concurrence avec Silicium Espana, une société liée à Loic Le Ribault, décédé en 2007, lui aussi passionné de silicium organique. Les deux sociétés ont connu un différent juridique en 2011, sur l'usage de la marque G5.

Enfin, Christian Daniel Assoun est aussi président du comité scientifique du Collège Francophone de médecine quantique et alternative lancé en 2015.

Deux autres ouvrages reprennent des thèses composites des précédents : **Transurfing, modèle quantique de développement personnel** de Vadim Zeland pour qui « *Quand les paramètres de l'énergie mentale changent, l'organisme se déplace vers une autre ligne de vie.* » et **Médecine, le grand tournant vers la médecine quantique** de Simone Brousse. En France, un certain Olivier Masselot propose du coaching et de la formation et des conférences de transurfing (exemple).



Il y a mieux puisque vous pouvez aussi gérer votre cheval avec des soins quantiques. Une conférence était organisée sur le sujet en 2017 sans qu'il soit possible de savoir si l'expérience avait été répétée. Il existe aussi de la permaculture quantique si vous jardinez.

J'attends avec une impatience fébrile l'arroseur quantique de Gardena qui évite de tirer les tuyaux dans le jardin !

Les générateurs d'ondes scalaires

Le top du top de l'escroquerie de la médecine quantique sont les **générateurs d'ondes scalaires**. Le procédé est décrit dans Les ondes scalaires, 2014 dans Alternative Santé par un certain Docteur Hervé Janecek. Ca commence très mal avec le préliminaire qui dit que *"Des chercheurs de l'Université du Pirée avancent que notre métabolisme de base nécessite quelques 12 000 calories à fournir chaque jour, dont un quart au maximum proviendrait des aliments solides ; un autre quart serait tiré - grâce à nos mitochondries - **de l'hydrogène de l'eau bue** ! Et enfin 50% de nos besoins énergétiques seraient fournis par la **lumière cosmique touchant la terre** !* [NDLR : celle du Soleil ?] *Certaines personnes seraient même capables de se passer de nourriture physique et de ne **se nourrir que d'air, d'eau et de lumière** !".*

On aimerait bien voir la tête de ces personnes ! Le malheureux auteur de ces inepties a loupé toutes ses classes de biologie moléculaire et ne connait visiblement pas le cycle de Krebs qui décrit le métabolisme énergétique des cellules à base de glucoses ! Pourtant, c'est un docteur ! Au passage, il est bien entendu impossible de trouver des traces web des travaux de ces chercheurs du Pirée !

Dès qu'on a lu cela, le pipomètre n'est plus dans un état superposé. Il explose en "Alerte Rouge" ! C'est confirmé avec Les ondes scalaires, la médecine de demain. Tout cela est déjà bien entendu déjà référencé comme faisant partie des pseudo-sciences (Wikipedia, RationalWiki). Concrètement, il s'agit d'ondes électromagnétiques associant une onde à polarisation horizontale et une autre à polarisation verticale de même fréquence mais déphasée de 90° ou d'un quart de longueur d'onde. Il n'est pas impossible que ces ondes aient un effet sur les tissus biologiques mais il n'est pas véritablement qualifié.

Les ondes scalaires ont été promues initialement par un certain **Thomas Bearden** aux USA. Il explique cela dans une interview de 1991 ! Il avait aussi inventé un **MEG** (Motionless Electromagnetic Generator) capable d'extraire l'énergie libre du vide et donc, de générer plus d'énergie qu'il en consommait.

Produit qui n'a bien entendu jamais été commercialisé et qui rappelle les théories **synergétiques** du professeur Vallée des années 1970. Les ondes scalaires permettraient aussi de traiter le diabète (I ou II ?), les calculs rénaux, la maladie de Parkinson, les infarctus, l'arthrose, le cancer et aussi le vieillissement. N'a pu qu'à ! Pour ce qui est des calculs rénaux, il vaudrait mieux faire appel à des ultrasons. Quant au diabète type I, lié à la destruction auto-immune des cellules bêta des îlots de Langherans dans le pancréas, on ne voit pas comment des ondes ramèneraient des cellules mortes à la vie.

La solution proposée ? Des générateurs d'ondes scalaires comme le SWD de l'Allemand **INDEL** à 8820€ qui est distribué en France par la société **Cytobiotech** depuis 2013.

Vu son prix, il cible les professionnels dans une sorte de modèle de Ponzi. Ce générateur produit un champ d'ondes scalaires d'une tension de 2V. Il comprend aussi un accessoire de modulation par la musique destiné aux cabinets de thérapie et aux centres de bien-être.

Il y a aussi l'**EPFX-SCIO Biofeedback** du Professeur William Nelson qui combine les thérapies globales et la physique quantique avancée (*ci-dessus*). Le dispositif scanne le corps sur 10 400 fréquences différentes pour détecter les pathologies. Il rééquilibre ensuite l'énergie du corps avec un biofeedback quantique. Le joujou propose 200 thérapies de biofeedback avec le plus grand logiciel de santé du monde (qui pourtant n'a pas été développé par Donald Trump ni par SAP) intégrant les philosophies occidentales et orientales[591].

Ce dispositif est proposé en France pour faire de la médecine prédictive par la thérapeute quantique **Jacqueline Jacques**. Elle forme les profanes à l'usage de l'EPFX-SCIO qui comprend un boîtier diffuseur d'ondes, relié au patient par des capteurs attachés à ses chevilles, poignets et crâne. On pourrait presque faire à la fois un EEG et un ECG avec ! Le tout n'a d'effet que placebo.

Une autre société vend un produit équivalent, **Physioquanta** lancée en 2005 et avec 1700 machines vendues à ce jour et 4M€ de CA en 2016. Le Physioscan «*repère et corrige les déséquilibres énergétiques*», l'Oligoscan, «*évalue en un instant minéraux, oligoéléments, stress oxydatif et métaux lourds*» et le Milta, «*associe de façon synergique des émetteur lasers, des diodes infrarouges et des diodes RVB, fonctionnant dans un tunnel magnétique*».

Tant qu'à faire des miracles, on pourrait aussi prescrire des séances avec ce machin aux jeunes pour leur permettre de réussir leur CAP, leur Bac et autres concours !

La médecine quantique émergera peut-être un jour au gré des découvertes scientifiques, mais celle qui est proposée aujourd'hui relève pour l'instant essentiellement du charlatanisme. Elles ont l'avantage de générer au minimum un effet placebo pour les utilisateurs et de remplir le porte-monnaie de leurs promoteurs. Sauf que cela peut être dangereux si l'effet placebo est utilisé en lieu et place d'un traitement traditionnel incontournable pour rester en vie. Je ne jetterai pas pour autant aux orties toutes les techniques et approches évoquées dans ce texte. Dans le tas, il y en a peut-être qui ont du sens, même s'il manque encore à la fois un corpus scientifique et des preuves plus solides pour les étayer.

Management quantique

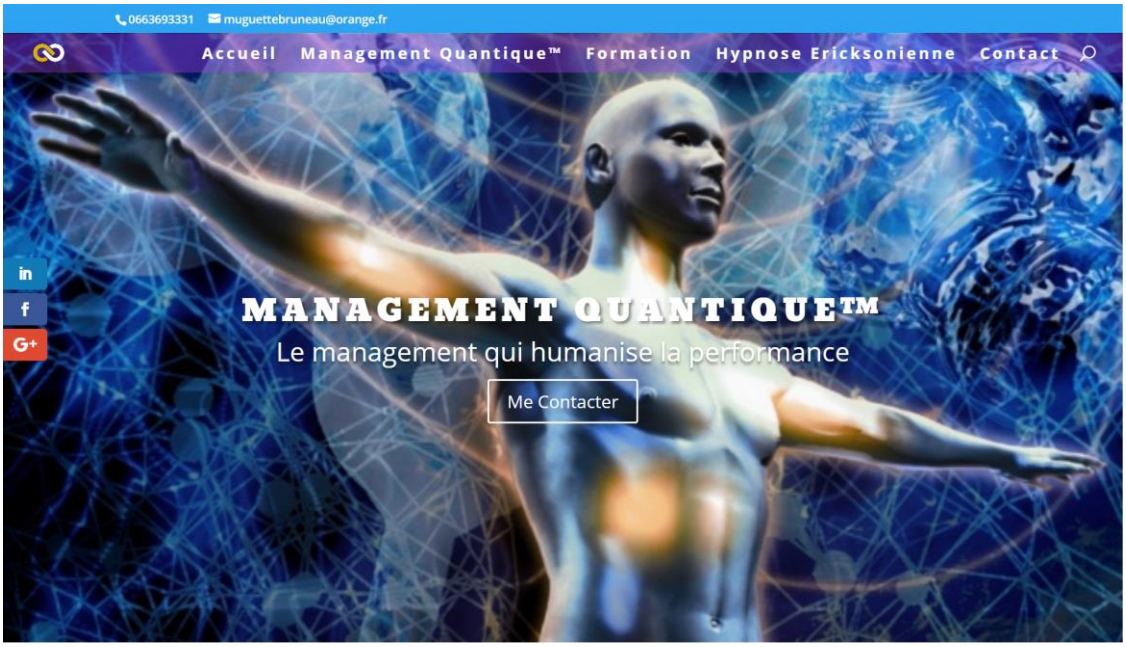
Le management quantique est une nouvelle pratique en vogue qui cherche à s'inspirer des principes généraux de la mécanique quantique. Très souvent, ses praticiens sont des adeptes de sciences plus ou moins occultes qui se sont reconvertis pour attaquer des marchés b2b plus solvables que celui des gogos du grand public.

[591] Voir How one man's invention is part of a growing worlwide scam that snares the desperate ill.

Solvable mais pas moins crédule, malheureusement. La vulnérabilité de cadres et dirigeants éduqués, BAC+5 ou plus, aux thèses les plus farfelues est toujours déconcertante.

J'ai ainsi dégotté le coaching quantique d'un certain Olivier Honsperger (vidéo, 2016) qui mélange allègrement mécanique quantique, épigénétique et modifications des gênes par l'action de la pensée pour prodiguer ses conseils aux entreprises. On n'est pas loin de Deepak Chopra. Alors, Etes vous prêts pour le management quantique ?. A vrai dire, il n'y a pas le feu au lac. Ne vous lancez pas tête baissée dans l'organisation d'un offsite Métaplan quantique dédié au travail d'équipe et au leadership dans un Chateauform de circonstance. Sauf si vous avez le budget pour et de bonnes activités extra-scolaires prévues au programme.

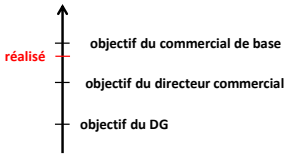
Mais si vous y tenez vraiment, vous pourrez aussi faire appel aux services de Muguette Bruneau, hypno-thérapeute après avoir été spécialiste de la défiscalisation. Son site Management Quantique fait la promotion d'un management qui « humanise la performance ». Personne ne sera contre car peu de managers sont opposés à toute forme d'humanisation, même d'un tableau Excel ou d'un reporting Salesforce.



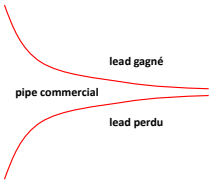
La description de l'approche fera évidemment sourire les spécialistes de la mécanique quantique : *« Le Management Quantique s'inspire des dernières découvertes en matière de neuro-sciences. La mécanique quantique nous explique que tout existe déjà et donc que le champ des possibles est infini. […] La théorie des cordes* [qu'elle se garde bien d'expliquer] *affirme que tout ce qui compose l'univers est fait d'infimes parties VIBRANTES et qu'elles nous informent en permanence* [via son smartphone ou la fibre ?]*. Nous sommes donc entourés d'informations. Mais savons-nous les décrypter ? A partir de ces observations, le management quantique nous apprend à développer notre sens de l'observation, nos ressentis afin de percevoir un maximum d'informations* ». Nous avons droit à une théorie du non-déterminisme et de la force de la volonté. Le management quantique serait la capacité à remettre en question nos perceptions. Donc, en ayant de l'empathie. Tout ça pour ça !

Pour autant, on peut en effet identifier de nombreuses analogies entre la physique quantique et le management au sens large du terme. J'ai repris pour cela les principales bases de la mécanique quantique et les ai appliquées à la vie en entreprise. Toute ressemblance avec une situation vécue serait totalement fortuite ou voulue, comme vous le souhaitez.

quantique, management et vente



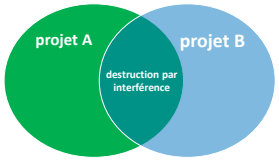
quantification
gestion des effectifs, objectif commerciaux et sand-bagging des managers



superposition d'états
état des collaborateurs perso/travail, état d'un lead dans un pipe commercial.

indétermination
sondages d'opinion des collaborateurs, mesure de la satisfaction clients avec des questions biaisées.

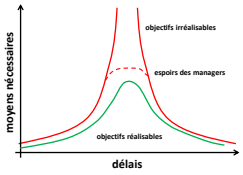
réduction d'états
mesure du chiffre d'affaire au closing trimestriel et pour l'attribution du bonus



dualité onde-particule
concurrence interne qui s'annihile dans les entreprises, caractère des grandes gueules

intrication
startups et grandes entreprises, mais avec fort risque de décohérence

non clonage
les cimetières sont pleins de gens irremplaçables



effet tunnel
faire passer des vessies pour des lanternes et donner des objectifs irréalisables

La **quantification** veut que certaines valeurs physiques ne puissent être que très précises, discontinues et pas arbitraires. Comme le niveau d'énergie d'un atome d'hydrogène ou le spin d'un électron.

Après tout, un salarié n'est qu'une case dans un tableur. Il est là un jour et hop, il disparaît le lendemain. La gestion des effectifs est en effet quantique. L'effectif d'une entreprise à un moment précis est un entier. Mais si on en fait la moyenne sur une période en tenant compte des départs en cours de période, des temps partiels, des CDD, des contrats d'apprentissage, des sous-traitants et des gens dont on n'est pas sûr de leur activité réelle, ce n'est plus un entier mais un nombre de FTEs (full time employees) ou ETPs (équivalents temps plein) qui est au minimum l'addition de fractions. Heureusement, ce n'est jamais un nombre complexe et on échappe aux espaces de Hilbert pour les représenter. Ouf !

La quantification se manifeste aussi dans le *sand bagging* qui veut qu'un manager commercial va transmettre ses objectifs au niveau du dessous en ajoutant une marge de sécurité « quantique ». Le dernier maillon de la chaîne, le malheureux commercial de base, va récupérer un objectif plus grand que celui de toutes les couches de management du dessus. Seules certaines strates de management ont cette latitude. Pour les spécialistes, il devient un atome de Rydberg : on l'excite avec un très haut niveau d'énergie. Ce système est conçu pour que le commercial de base n'atteigne pas son objectif et soit pénalisé côté bonus contrairement à celui des managers au-dessus. Surtout si on souhaite le virer. Ceci n'est qu'une fiction bien entendu !

Le jugement sur les individus est aussi sujet à la quantification. Une personne est souvent smart ou sympa ou alors, c'est un abruti total. Les jugements sont rarement nuancés, entre les deux.

La **superposition d'états** a très couramment lieu à cause des smartphones et autres laptops grâce à qui les collaborateurs sont à la fois au travail et dans leur vie personnelle toute la journée. Elle peut se manifester également dans la conformité aux règlements qui est à géométrie variable dans nombre d'entreprises. Et puis bien entendu, dans l'application des valeurs définies à coup de slides Powerpoint rabâchés par les dirigeants ou la DRH.

La superposition des états se manifeste aussi dans l'évaluation des *leads* qui sont *closés* ou pas dans un *pipe* commercial. On leur attribue généralement un taux de *closing* qui est un pourcentage jusqu'au moment où l'on sait si le deal est perdu ou gagné, ce qui relève de l'écrasement de la fonction d'onde de Schrödinger sur un état de base (perdu ou gagné). Cet écrasement peut aussi intervenir si un élément extérieur intervient et génère une décohérence de l'état du lead. Par exemple, un concurrent qui rafle l'affaire au nez et à la barbe du commercial, fort marri de cette mésaventure. Son manager lui en fera porter l'intégralité de la responsabilité, ce qui constitue une autre forme d'écrasement. Ce genre d'analogie quantique ne vous aidera cependant pas à améliorer votre taux de closing de pipe commercial.

Le principe d'**indétermination** d'Heisenberg s'applique ainsi à la mesure de la satisfaction des collaborateurs, où l'outil de mesure influe toujours sur la grandeur à mesurer ! C'est vrai dans l'infiniment petit ainsi que dans les questions posées dans les sondages d'opinion qui sont souvent orientées, aussi bien en politique que pour évaluer la satisfaction des collaborateurs d'une entreprise. Et on navigue allègrement entre le béni-ouiouisme et le courage de s'exprimer, qui dépend de l'anonymat et de l'existence de champs de commentaires en texte libre qui permettent d'ajouter un peu de logique floue. Le top du top de l'insupportable ? Ces popups Internet où le choix donné est "OK" ou "Plus tard".

Plus généralement, la mesure de n'importe quel paramètre dans une entreprise, notamment lors d'un audit, va probablement aboutir à modifier les grandeurs mesurées (élagage d'effectif, mutation de manager, modification de processus).

La définition d'origine du principe d'indétermination d'Heisenberg est que l'on ne peut pas mesurer avec précision la position et la vitesse d'une particule dans l'infiniment petit, du fait notamment de sa grande rapidité de mouvement. L'analogie dans les affaires serait l'observation d'une startup en pleine croissance : le temps que l'on comprenne où elle en est à un moment donné, elle a déjà changé de situation (de siège, d'effectif, de CEO, de chiffre d'affaires, un petit pivot, etc). C'est la raison pour laquelle il faut une énergie infinie pour créer une base de startups à jour sur un pays ou au niveau du monde entier.

Dans un autre cadre, l'immobilisme dans l'entreprise est facilement associable à la constante de planque.

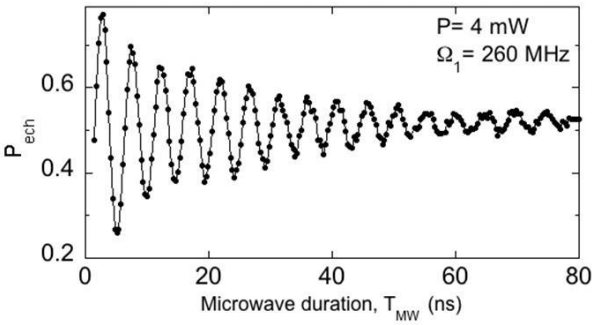
La **réduction d'états** rejoint l'histoire de la quantification des états lorsque l'on mesure le chiffre d'affaire en fin de trimestre. Là, on est bien obligé de fournir des chiffres et de ne pas s'appuyer sur la logique floue des taux de closing. Ne serait-ce que pour déterminer les bonus des commerciaux. Dans le cas de la superposition travail/vie personnelle, seule une observation de l'écran va permettre d'en savoir plus. Elle génère souvent un écrasement de la fonction d'onde de Schrödinger sur l'état « travail », sauf pour les jmenfoutistes.

Sinon, Bill Gates affirmait haut et fort en 1997 que les "mauvaises nouvelles devaient circuler vite dans les entreprises efficaces" ("bad news should travel fast"). Mais pas trop tout de même. L'écrasement de la fonction d'onde de Schrödinger s'applique très bien à la situation, lorsque les collaborateurs et managers pleutres s'écrasent en pareille situation, de peur des retombées négatives. Ou alors, au contraire, lorsqu'un salarié prend son courage à deux mains et dénonce l'insupportable, jusqu'à parfois devenir un lanceur d'alertes.

La **dualité onde-particule** se manifeste avec de vrais gens dans les entreprises qui travaillent sur des projets concurrents et s'annihilent allègrement. C'est le phénomène d'interférences lié à la forme d'onde des projets ! Il y a aussi les managers grandes gueules face à leurs équipes (donc, à l'état de particules solides) qui se transforment en lavettes face à leur propre management (donc, à l'état d'ondes flasques).

Cette dualité comportementale se manifeste aussi souvent chez les managers irascibles qui deviennent des moutons dociles une fois chez eux, ou qui n'arrivent pas à éduquer convenablement leurs enfants.

Et le Chief Happiness Officer de la startup branchée, il peut être quantique [592]? Il doit en tout cas lutter contre un phénomène universel : un bon nombre de passions s'estompent rapidement avec le temps comme l'amplitude d'une **oscillation de Rabi**, qui est couramment observée en mécanique quantique et dans les qubits supraconducteurs (*ci-contre*).



Un bon leader est en phase avec ses équipes. Il émet des ondes qui entrent en résonnance avec elles, un peu comme dans l'algorithme de tri quantique de Grover. L'effet Doppler permet aussi de stopper un projet foireux avec de la lumière, par exemple, via une fuite bien gérée dans les médias.

L'**intrication** quantique s'applique aux startups qui sont intégrées dans les programmes d'innovation ouverte des grandes entreprises. Tout va bien jusqu'à l'apparition de la **décohérence** des objectifs entre la startup et la grande entreprise ! Je fais un produit et tu veux un projet-service, j'ai besoin de rapidité et tu es trop lent à la détente, etc !

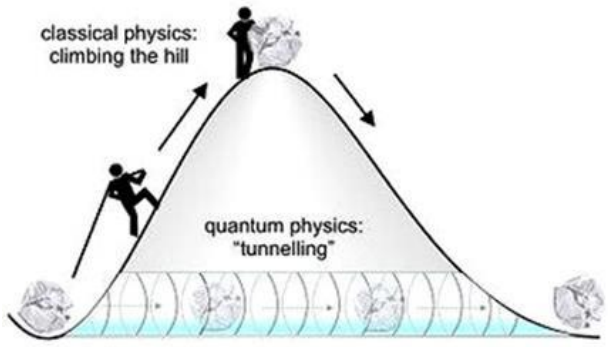
[592] Voir l'excellente parodie du rôle dans la vidéo USI 2019 - "Depuis deux ans, je conquiers le bonheur" | Confessions Digitales.

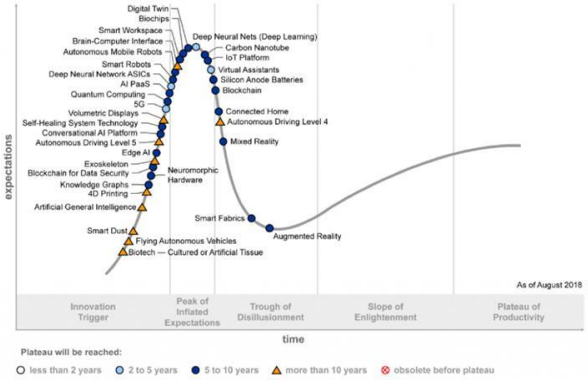
L'intrication se produit également dans le phénomène couramment dénommé radio-moquette, couplé à la téléportation des rumeurs plus rapidement que la lumière. On sait aussi que le temps de cohérence des qubits est lié à leur bonne isolation physique, magnétique, sous vide, et, souvent à très basse température, histoire d'éviter toute perturbation externe. Tout le contraire des open spaces des entreprises où l'on entasse les collaborateurs ! On a longtemps prétendu que cela améliorait le travail en équipe alors que cela servait principalement à réduire les coûts immobiliers !

Le **théorème de non clonage** quantique qui dit qu'il est impossible de cloner à l'identique l'état d'un qubit ou d'un quantum a une application dans la vie des entreprises avec tous ces gens que l'on croit irremplaçables jusqu'au jour où ils s'en vont. Le théorème s'applique notamment lorsque le manager qui s'en va n'est pas remplacé et dont on répartit ensuite le rôle sur plusieurs managers en place. Et comme le veut l'adage, les cimetières sont pleins de gens irremplaçables ! Le théorème s'applique aussi aux entrepreneurs à succès qui ont du mal à répliquer un succès dans un domaine à un autre secteur d'activité.

L'**effet tunnel** permet de faire passer des vessies pour des lanternes et gérer les bases du changement. Cela consiste à présenter une situation future mirifique en faisant oublier les difficultés pour y arriver. L'effet tunnel s'appelle la méthode Coué dans la vie courante. Le principe pourrait d'ailleurs être adopté par le Gartner Group avec ses fameuses courbes de cycle d'adoption de l'innovation (« hype cycle »), certaines technologies ne passant pas forcément par la vallée de la mort, comme ce fut le cas pour les smartphones.

Il faut dire qu'ils ont bénéficié du champ de déformation de la réalité d'un certain Steve Jobs, autre grand adepte de la mécanique quantique managériale. Imbuvable avec ses collaborateurs directs mais admiré quoi qu'il arrive !





Dans le plus fumeux, on peut trouver une analogie entre la **supraconductivité** et la réunionite aiguë dans les entreprises. Les salariés et cadres sont conditionnés pour être des bosons à spin pairs donc assemblables dans une salle de réunion, comme des photons ou comme des paires d'électrons dites de Cooper qui se manifestent dans la supraconductivité, alors que s'ils étaient des bosons à spin demi-entier comme des électrons libres classiques, on ne pourrait pas facilement les mettre au même endroit. On pourrait prolonger le raisonnement avec le remplissage des open spaces.

Il vaut mieux que les salariés proches les uns des autres soient compatibles donc appairables comme dans des paires de Cooper. Libre à vous de passer ensuite, par effet tunnel, de l'état de boson à celui de bozo, très cher à Guy Kawasaki.

La supraconductivité organisationnelle permet d'ailleurs d'éviter la résistance au changement. Vous congelez les collaborateurs et leur résistance au changement disparaît. Ce qui est un peu paradoxal car une fois congelé, on est solide comme un roc, et la décongélation n'est pas évidente.

Si on reprend les principes de la pseudo-médecine quantique de Deepak Chopra, une entreprise est dans un état superposé entre celui de leader en bonne santé et de société en perte de vitesse. La force du leadership devrait théoriquement permettre d'écraser la fonction d'onde de l'état quantique de l'entreprise dans l'état leader en bonne santé. Dans la vraie vie, cet écrasement est délicat à réaliser. Les processus qui amènent l'entreprise à se trouver en situation de déclin sont le plus souvent irréversibles et liés à l'environnement, aux concurrents et aux clients qui eux, n'ont pas attendu pour s'adapter.

La vie des entreprises n'est pas une porte quantique réversible ! Essayez par exemple de transformer Nokia en leader des smartphones sous Android ou Technicolor en Samsung !

Le **calcul quantique à portes universelles** a une belle analogie dans la vie des entreprises avec la gestion des appels d'offre comme ceux qui portent sur les agences de communication. Les réponses des agences candidates sont des états superposés de registre quantique. Elles subissent un processus d'évaluation simultané, comme dans le calcul quantique. A la fin, un seul état (offre) ressort : le gagnant.

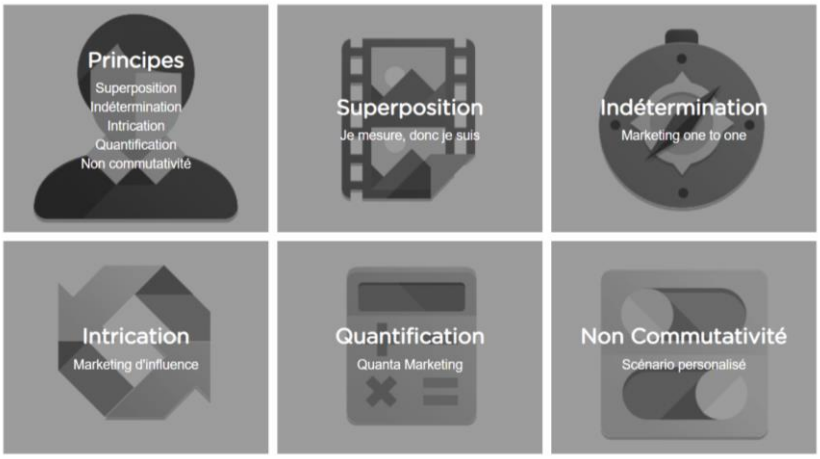
Mais dans le calcul, il peut y avoir un peu de mélange des états quantiques affectant le résultat. Traduction : les éléments de certaines réponses vont se retrouver comme par magie dans la réponse du gagnant. Là encore, peut-être via le fameux effet tunnel. En plein, le même processus s'applique aux projets open source bénéficiant d'un grand nombre de contributeurs.

Enfin, citons cet autre principe universel, la **téléportation quantique** de la bêtise humaine auprès de larges pans de l'entreprise ou de la population. Elle est tellement rapide que cela ne peut être que la seule explication plausible !

Toutes ces analogies créent des nœuds dans le cerveau et sont parfois amusantes. Elles ne servent pas à grand-chose pour améliorer le management. Elles sont plutôt utiles pour rappeler l'absurdité de certaines pratiques managériales dans les entreprises et leurs contradictions éternelles. En positivant un peu, même si sa dimension scientifique est plus que sujette à caution, la parodie est finalement une intéressante forme de pédagogie !

Marketing quantique

Cette grille de lecture sur le management et la vente est adoptée sérieusement par quelques rares adeptes du marketing quantique. Ainsi, le site Quantum-Marketing est lié à la société GetQuanty dont l'offre logicielle est une solution de scoring prédictif B2B[593], donc, de la gestion de leads[594].



Le fondateur, Hervé Gonay, que j'ai rencontré, ne prétend pas faire de la physique quantique mais cherche à s'en inspirer. Il m'a fait découvrir le groupe de chercheurs du Quantum Interaction qui se sont réunis dans leur 8ième congrès en 2018 à Nice et dont les interventions sont disponibles sur Youtube. Il a même co-écrit un papier de recherche avec Ariane Lambert Mongiliansky (PSE) qui travaille avec Michel Bitboll (CNRS, ENS Lyon) et Bob Coecke (Oxford), lui-même co-auteur de Picturing Quantum Processes.

Ces chercheurs bâtissent des modèles inspirés de la physique quantique dans des domaines variés tels que l'économie, la recherche d'information et la dynamique des organisations. Ca a l'air plus sérieux que les fumisteries évoquées dans ces pages. La frontière entre sciences humaines et fumisteries reste cependant très ténue.

Dans Innovation quantique, ou cantique de l'innovation, un certain Philippe Cartau recommande de ne pas trop mesurer ses actions lorsque l'on innove en mode startup, ce qui fera naturellement s'étranger les adeptes du growth hacking, ce dernier reposant sur la mesure constante de la performance du mix marketing. Quel monde paradoxal !

Autres fumisteries

La physique quantique donne lieu à d'autres propagations de théories ou affirmations fumeuses, malgré le fait qu'elles s'appuient parfois sur des travaux de recherche sérieux. Le biais de ces exagérations vient souvent d'extrapolations abusives de phénomènes constatables à une échelle nanoscopique à la vie macroscopique.

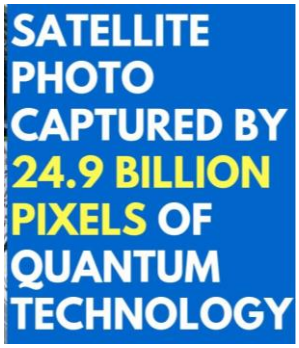
---

[593] Voir la vidéo sur « le marketing quantique expliqué à mon boss » par Hervé Gonay.

[594] Le problème ? Des marketeurs sans formation scientifique qui s'emmêlent les paluches dans l'histoire du quantique : « C'est Albert Einstein qui, le premier, a affirmé qu'une particule de lumière pouvait à la fois se comporter comme un objet (un corpuscule) et comme une onde. Il l'a démontré par la logique, puis cette réalité a été prouvée par l'expérimentation (expérience des deux fentes de Thomas Young [en fait, l'expérience des fentes de Young date de 1806 et le texte d'Einstein de 1905]). Plus tard, le français Louis de Broglie a émis l'hypothèse, vérifiée ensuite, que les électrons, qui sont au cœur de la matière, possédaient la même dualité. C'est pourquoi on parle de superposition [le lien entre dualité et superposition est un peu rapide] : toute particule se situe dans plusieurs états à la fois. De plus, ce n'est qu'au moment où on l'observe que la particule « choisit » d'être soit un corpuscule, soit une onde [la superposition n'est pas entre un état « particule » et un état « onde »]. On parle alors de « réduction de la fonction d'onde »… ».

En Chine, nous avons par exemple vu apparaître une soi-disante **caméra quantique satellite** servant à réaliser des panoramas haute-résolution. La vue présentée est celle de Shanghaï avec 195 milliards de pixels.

En y regardant de près, les images ont été captées en haut d'un gratte-ciel – il n'en manque pas à Shanghaï - et pas par satellite et par des caméras haute résolution classiques qui n'ont rien de plus quantique que le très classique effet photo-électrique.



Ce dernier permet à un capteur photo CMOS de transformer des photons en courant électrique. L'information est totalement bidon et ne servait qu'à générer du buzz. Malheureusement, nombre de médias on mordu à l'hameçon dans le monde entier sans douter de la chose[595].

Vous avez aussi droit à un beau **réfrigérateur quantique** (« Quantum Cooler ») de Chillout Systems qui n'a de quantique que le nom. Il utilise un compresseur classique compact[596].

D'autres cas de figure extrapolent à l'échelle macro des phénomènes quantiques observés à une échelle nano.

C'est le cas de l'**inversion du temps** avec du calcul quantique, une vision de l'esprit qui est liée à la nature réversible des portes quantiques mais ne signifie aucunement que l'ont peut revenir en arrière sur l'échelle du temps dans la pratique macroscopique[597].

[595] Voir 60 seconds over sinoland: quantum satellite camera used to do movable, panoramic photos of Shanghaï, décembre 2018 (vidéo) et Truth Behind Viral 24.9 Billion Pixel Image Taken By Chinese "Quantum Satellite" par Anmol Sachdeva, décembre 2018 et le site Bigpixel pour consulter la vue.

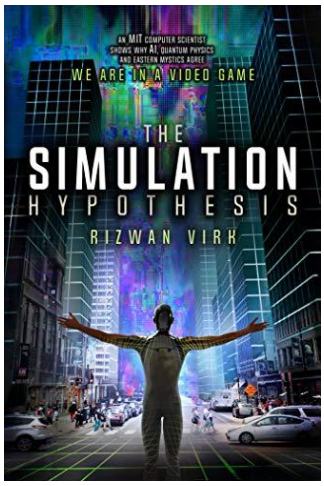
[596] Voir Chillout Systems Quantum Cooler. Il est vendu $2199.

[597] Voir Des physiciens ont réussi à "inverser" la flèche du temps grâce à un ordinateur quantique de Stéphanie Schmidt, mars 2019, qui fait référence à Arrow of time and its reversal on the IBM quantum computer, de G. B. Lesovik & Al, 2018 (14 pages). Voir aussi L'ordinateur quantique d'IBM viole-t-il le second principe de la thermodynamique ?, 2019.

Nous avons aussi des théories tout aussi fumeuses visant à **prédire le futur** grâce au calcul quantique. S'il est vrai que le calcul quantique permet d'évaluer toutes les solutions d'un problème complexe, il est réduit à des problèmes simples au vu de la complexité de la vie macroscopique, quand bien même celle-ci pourrait être déterministe[598].

L'étape suivante consiste à considérer que nous vivons en fait dans une **simulation**.

C'est la théorie évoquée dans The Simulation Hypothesis de Rizwan Virh. Comme cela peut arriver en pareil cas, l'auteur survend son parcours personnel en se présentant comme un MIT Computer Scientist alors que c'est plutôt un entrepreneur dans le jeu vidéo plutôt habitué aux ouvrages sur l'entrepreneuriat que sur les sciences. Ce genre de scénario de la simulation équivaut à la croyance en une sorte de Dieu omnipotent qui contrôle tout ou qui a créé l'outil de simulation en question. La question peut d'ailleurs être déclinée récursivement : si ce créateur a développé un outil de simulation, qui a créé son univers et celui-ci n'est-il pas également une simulation ?



Les lois de la physique que l'Homme découvre petit à petit permettent de décrire le comportement de la matière et des ondes. Plus on avance, plus elles permettent d'imaginer un monde déterministe gouverné par ces lois. Mais cela ne signifie par que ces lois soient gouvernées par un système qui les contrôle.

Autre cas de figure qui devrait inspirer la plus grande prudence, celui de cette curieuse société **Precog Technologies** qui prétend proposer des solutions de téléportation, de voyage dans le temps et de systèmes anti-gravitation. La totale ! La société a été créée pour valoriser la propriété intellectuelle d'un certaine Anisse Zerouta qui est décrite dans un papier scientifique douteux[599].

Un autre olibrius, de **Qaunta QB** (d'Afrique du Sud) pense avoir aussi trouvé la pierre philosophale et l'archirecture de qubits qui fait tout ce qu'il faut et avec un miraculeux 0% d'erreurs[600].

---

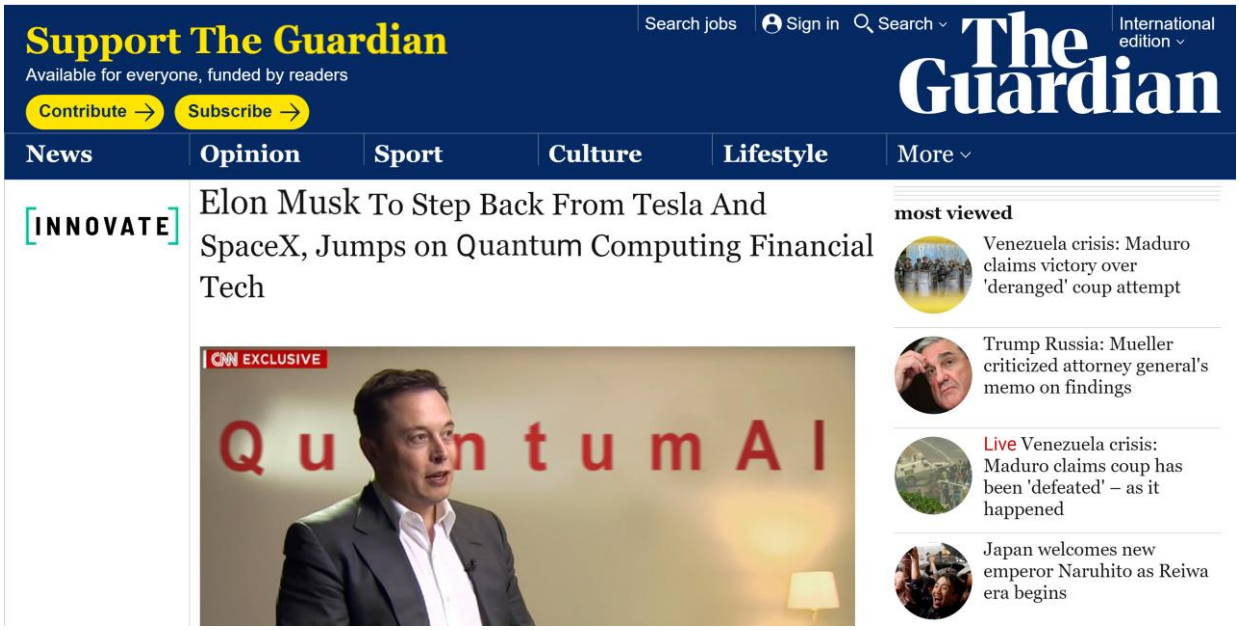
[598] Voir Des scientifiques construisent une machine permettant de voir tous les futurs possibles de manière simultanée de Jonathan Paiano, avril 2019 et Interfering trajectories in experimental quantum-enhanced stochastic simulation de Farzad Ghafari & Al, 2019 (7 pages).

[599] Voir The Seed Theory: Unifying and replacing quantum physics and general relativity with "state physics" d'Anisse Zerouta, 2017 (28 pages) qui développe une théorie de mondes parallèles et qui n'a pas du tout l'air de remplir les critères d'une publication scientifique digne de ce nom. Anisse Zerouta est un gérant d'entreprises à Paris né en 1973, d'abord avec Elysee Communication (2008-2011) puis avec Avenir Optique, un opticien (2011-*), des sociétés n'ayant qu'un salarié, son fondateur (source). Créé en septembre 2018, Precogtec aurait un CTO, un certain François Bissege, qui possède un doctorat en sociologie (source) et un autre salarié, Julien Darivel, qui possède un DUT et a travaillé chez PSA. C'est du bizarre !

[600] Voir I made the Quantum Breakthrough, juin 2019.

On a aussi vu apparaître le premier scam quantique en 2018 avec ce faux article du Guardian faisant état d'un projet d'ordinateur quantique pour la finance d'Elon Musk[601]. L'œil exercé dans l'informatique quantique détecte rapidement qu'il s'agit d'un montage, comme cette série d'ordinateurs quantiques **QuantumAI** qui ne sont que des D-Wave dont le logo a été photoshoppé.

Second point, l'article serait issu du Guardian… mais pas l'url ! L'article cite un nombre de scientifiques de laboratoires de recherche du monde entier, mais ayant tous un nom russe. L'article pointe sur le service en ligne de **QuantumAI** qui serait capable de boursicoter pour dépouiller les riches et redistribuer l'argent aux plus pauvres. Le site ose tout, comme indiquer que la startup a comme advisors Jeff Bezos et Bill Gates et comme partenaires IBM, Microsoft et OpenAI.

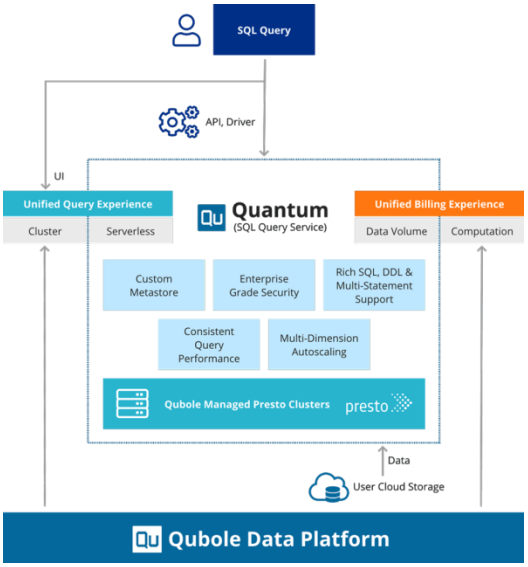


Il en existe un autre, dénommé **Quantum Code**. Evidemment, fuyez ! C'est en fait un scam destiné à détrousser les utilisateurs de leurs économies mais de manière indirecte. Le site propose de créer un compte en fournissant ses coordonnées. Celles-ci sont alors revendues à des sociétés peu scrupuleuses de produits financiers louches qui exploitent ainsi des leads de prospects faciles à berner[602].

[601] Voir To Step Back From Tesla And SpaceX, Jumps on Qm Computing Financial Tech (non daté).

[602] Voir QuantumAI review – is Quantum-aix.com a scam?, juin 2019.

On peut aussi citer **Qubole** qui lançait son serveur SQL Quantum, qui n'a rien de quantique[603]. Le processeur **Samsung** Quantum 8K lancé en 2018 n'était pas non plus particulièrement quantique à part via ses transistors CMOS classiques. Le quantique risque de laver plus blanc que blanc, comme cette lessive "Quantum Max" de la marque **Finish** du groupe Reckitt Benckiser !



[603] Voir Qubole launches Quantum, its serverless database engine de Frederic Lardinois, juin 2019.

Entreprises

Cet ouvrage est destiné à un large public intéressé par le sujet de l'informatique quantique. Il comprend en particulier les entreprises qui peuvent se demander quoi faire devant un tel déluge d'informations, de complexité et d'incertitudes. Et cela s'ajoute aux autres vagues technologiques à assimiler comme l'intelligence artificielle, la Blockchain, les objets connectés et la 5G qui pointe du nez.

La vague de l'informatique quantique a ceci de particulier qu'elle est encore plus imprédictible et difficile à saisir que les autres vagues du numérique. Et pourtant, elle mérite bien l'attention des entreprises, en particulier dans certains secteurs clés comme la finance, la santé, les transports et tout ce qui relève du régalien.

Je propose une approche relativement simple et somme toute assez classique que voici, en onze points.

Veille technologique

- Comprendre la **dimension technologique** des ordinateurs quantiques et des questions de cryptographie associées. La lecture de cet ouvrage peut aider. De nombreux autres supports de vulgarisation sont disponibles en texte[604] et vidéo[605].
- Apprendre à **décoder les annonces** des laboratoires de recherche et fournisseurs. Je fournis quelques exemples dans cet ebook, au sujet notamment du fait que le calcul quantique n'est pas une solution miracle qui peut accélérer tous les traitements informatiques. De même, ce n'est pas une voie naturelle pour les applications de big data.
- Comprendre ce que l'on peut faire avec les **algorithmes quantiques** en consultant les parties de cet ebook sur les algorithmes et les applications métiers classées par marché vertical. Si votre marché n'y est pas, cela ne veut pas forcément dire que vous n'êtes pas concerné.
- Participez aux **événements de l'écosystème** comme les meetups de Quantonation ou les conférences organisées par les chercheurs (CNRS, CEA-Leti, LIP6, PCQC, etc).

Analyse des besoins

- Identifier les **problèmes de nature exponentielle** dans le portefeuille applicatif de l'entreprise. C'est une question à laquelle les développeurs et les data scientists peuvent répondre. Ce sont par exemple les problèmes d'optimisation complexe impliquant l'orchestration de nombreuses ressources.

---

[604] Voir par exemple Pédagogie sur l'informatique quantique : L'ordinateur quantique : tout comprendre en partant de zéro, décembre 2016 qui est assez bien fait.

[605] J'assure de mon côté une formation de découverte de l'informatique quantique d'une journée qui est proposée dans le catalogue de Capgemini Institut. Voir le synopsis et les dates.

- Lancer une cartographie de l'usage de **protocoles de sécurité** menacés par les ordinateurs quantiques à une échéance imprécise. Quelles sont les données du présent dont le piratage dans le futur pourrait poser un problème de confidentialité à l'entreprise ? Si les données du présent ont de la valeur dans plus de 5 ans, il faut commencer à s'inquiéter.
- Impliquer les **RSSI** dans les processus de standardisation de nouvelles clés publiques résilientes au quantique (post-quantum cryptography). Une entreprise seule n'imposera pas un standard de cryptographie post-quantique mais les grandes entreprises ont chacune un rôle d'influence dans leur marché vertical.

Formation

- Former **quelques développeurs** à la programmation quantique. Cela peut se faire en laissant les gens intéressés par le sujet y consacrer du temps par leurs propres moyens. L'information et les outils sont disponibles en ligne comme chez IBM ou Microsoft. Les outils open source en cloud sont déjà là. Les plus jeunes seront probablement ceux qui s'adapteront le mieux aux méthodes de programmation du calcul quantique qu'il est difficile d'assimiler lorsque l'on a été formatté à la programmation classique[606].
- Comprendre les liens entre le **calcul quantique et l'intelligence artificielle**. Le « quantum machine learning » est une nouvelle sous-discipline de l'algorithmie quantique qui mérite d'être explorée et comprise.

Evaluation

- Tester **quelques algorithmes** dans le cloud avec des ordinateurs quantiques universels (IBM, Rigetti) ou à recuit quantique (D-Wave) ou avec des émulateurs à base de supercalculateurs (Atos, IBM, Microsoft, Google). Les études de cas disponibles sont évoquées dans cet ebook dans la partie sur les algorithmes et sur les applications par marchés.
- Ne pas hésiter à tester des algorithmes sur les **ordinateurs à recuit quantique** de D-Wave malgré leur relative mauvaise image chez les puristes du calculateur quantique universel. C'est autour de cette société que les premiers éditeurs de logiciels quantiques comme le Canadien 1Qbit gravitent. Les algorithmes quantiques pour ces ordinateurs sont adaptés à la résolution de problèmes d'optimisation complexes et représentent une bonne part de ce que peut apporter le calcul quantique, que ce soit en biologie ou dans la finance pour ne prendre que deux exemples.

Bravo, vous avez ainsi économisé une étude de McKinsey ou du BCG !

[606] Petite publicité : je propose une journée de séminaire de découverte de l'informatique quantique, notamment chez CapGemini Institut. Voir l'agenda et le programme.

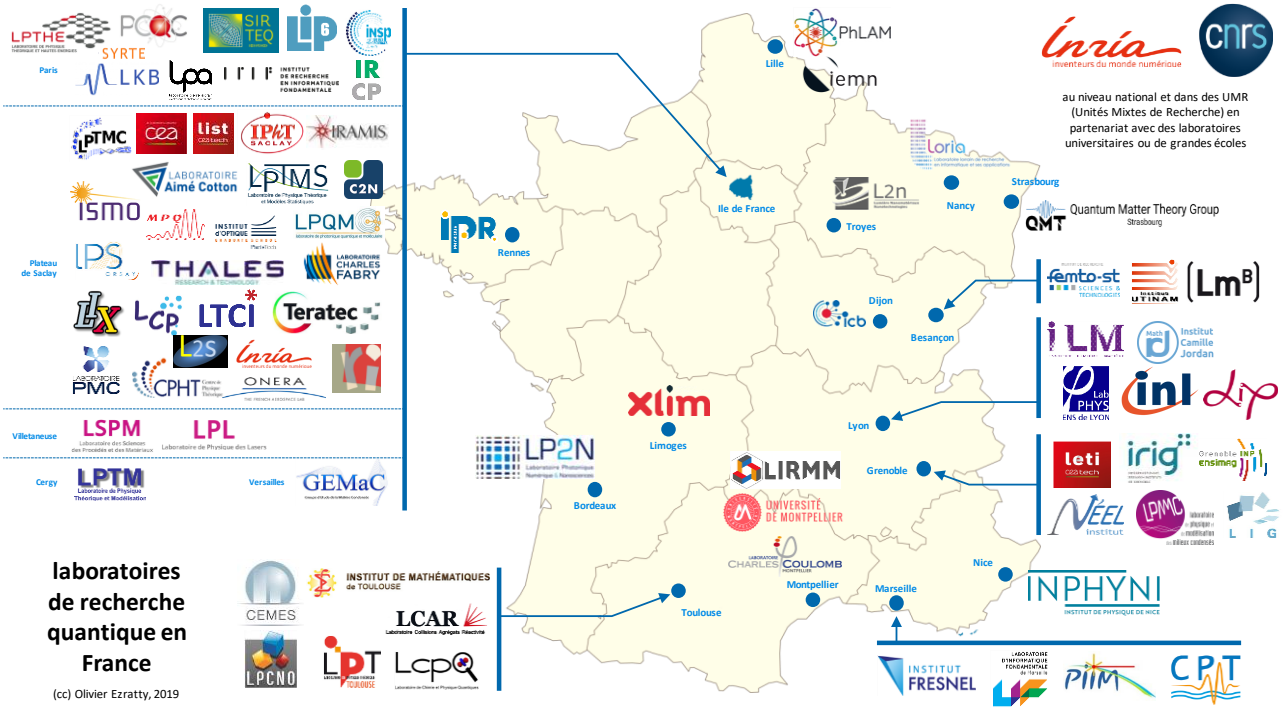
Ecosystème quantique en France

Dans cette nouvelle rubrique de l'édition été 2019 de cet ouvrage, nous allons faire un tour aussi large que possible de l'écosystème quantique en France en couvrant la recherche publique, la recherche privée, les startups, les entreprises utilisatrices, les événements et l'activité associative.

Recherche

De nombreux laboratoires de recherche français sont actifs dans les différentes branches du quantique, principalement autour du CEA, du CNRS et de l'Inria. Une bonne part de ces laboratoires de recherche sont des UMR, Unités Mixtes de Recherche, qui associent le CNRS et des laboratoires d'Universités, grandes écoles ou d'un autre organisme national de recherche. Ces laboratoires quantiques sont fédérés par le **GDR IQFA**[607] fondé par Jean-Philippe Poizat dans les années 2000 puis repris depuis 2010 par Sébastien Tanzilli d'InPhyni (Nice).

Les deux plus grands pôles de recherche sont en Ile de France et à Grenoble, mais d'autres métropoles sont actives comme Toulouse, Montpellier, Marseille, Besançon et Lille. Et encore, cet inventaire est probablement incomplet. Il comprend les laboratoires de recherche publics qui travaillent de près ou de loin sur le quantique en consolidant diverses listes et cartographies du secteur[608].



[607] Un GDR est un Groupement de Recherche qui coordonne la recherche nationale dans un domaine scientifique donné. Son rôle est surtout d'animer la communauté des chercheurs du domaine, notamment via des colloques, mais aussi de coordonner les axes de recherche. Voir Les Groupements de Recherche, novembre 2018.

[608] J'ai pour cela consulté les sites web de ces laboratoires et les domaines de recherche qu'ils y présentent, plus, lorsqu'elles étaient faciles à trouver, les publications scientifiques deschercheurs de ces laboratoires.

La majorité de ces laboratoires opèrent dans le champ de la physique fondamentale avec de nombreuses redondances apparentes et très peu sont engagés dans la recherche pratique sur la création de qubits. Mais ces recherches fondamentales peuvent à terme y servir. Je les cite dès lors qu'ils font de la recherche fondamentale dans la physique quantique qui pourrait avoir un intérêt de près ou de loin avec le calcul ou les télécommunications quantiques. Les laboratoires français explorent en parallèle de nombreuses pistes de qubits : les supraconducteurs, la photonique, les atomes froids, les spins d'électrons et même les ions piégés et les fermions de Majorana.

J'ai par contre trouvé très peu de laboratoires directement impliqués dans la recherche en algorithmie quantique parmi les dizaines de laboratoires spécialisés en mathématiques.

Avec les restrictions budgétaires endémiques du secteur, les chercheurs du secteur public ont appris à se financer en soumettant et défendant leurs projets pour obtenir des financements publics et privés[609]. L'étape suivante, franchie par certains, consiste à passer à la création de startups avec ses codes et coutumes. Statutairement et d'un point de vue pratique, elle est plus encouragée au CEA et à l'Inria qu'elle ne l'est au CNRS.

Si l'on évalue la recherche française quantique de manière traditionnelle avec ses publications scientifiques et ses brevets, le pays se positionne habituellement entre la 8e et la 10e position mondiale, les premiers étant les USA, la Chine et le Canada. C'est un classement que l'on retrouve dans de nombreuses disciplines scientifiques.

Le monde de la recherche publique recèle quelques différences de générations. En moyenne, certains anciens comme Serge Haroche sont plutôt sceptiques et prudents sur le calcul quantique tandis que les jeunes chercheurs sont plus optimistes et à l'affût de nouvelles approches. D'autres comme Alain Aspect font le pont entre les deux. Certains comme ce dernier ou Julien Bobroff, Philippe Chomaz[610] et Etienne Klein s'investissent à fond dans la vulgarisation destinée à un public aussi large que possible, un point de passage obligé pour se faire connaître et faire rayonner la discipline. Le CEA s'y est même mis en créant un jeu pédagogique, le Prisonnier Quantique[611].

Ile de France

L'Ile de France concentre une bonne moitié des laboratoires de recherche du pays consacrés au quantique aussi bien côté création de qubits que dans le domaine des algorithmes, et des télécommunications et de la cryptographie quantique et post-quantique.

---

[609] Certains obtiennent des ERC Grants (European Research Council) : les Synergy Grants pour quelques poignées d'équipes (jusqu'à 14M€ su 6 ans), et plus souvent des Starting (jeunes chercheurs, jusqu'à 1,5M€), Consolidators (chercheurs expérimentés, jusqu'à 2M€) et des Advanced (chercheurs émérites, jusqu'à 2,5M€ étalés sur 5 ans). Puis des financements FET Européens, des financements via le Flagship Européen quantique, ou enfin par des appels à projets divers à l'échelon national (ANR).

[610] Voir la vidéo du TEDx Versailles Grand Parc de Philippe Chomaz en 2019.

[611] Voir Le CEA présente Le Prisonnier quantique, un jeu vidéo inédit d'aventure au cœur des sciences et des technologies, juin 2019. Je jeu doit être publié à l'automne 2019 lors de la fête de la science.

Commençons par les laboratoires qui sont situés dans Paris intra-muros.

Les efforts de l'**Inria** en région parisienne sont concentrés dans l'équipe Quantic (Quantum Information Circuits) de Pierre Rouchon, Mazyar Mirrahimi, Zaki Leghtas et Alain Sarlette qui est conjointe entre le CNRS, l'ENS et l'école des Mines de Paris.

Elle travaille sur les modèles mathématiques des qubits supraconducteurs, sur des codes de correction d'erreur, sur la preuve de la supériorité d'algorithmes quantiques ainsi que sur les questions de cryptographie[612]. Il faut y ajouter l'équipe Secret, basée à Paris, dirigée par Anne Canteaut, qui travaille sur les algorithmes de cryptographie.

Le **LIP6** (Laboratoire d'Informatique de la Sorbonne) est situé à Jussieu. On y trouve plusieurs spécialistes reconnus de la cryptographie et des télécommunications quantiques (QKD) : Eleni Diamanti et Elham Kashefi. Eleni a obtenu un ERC Synergy Grand européen pour ses travaux dans le projet QUSCO (Quantum Superiority with Coherent State). Elham Kashefi est cofondatrice de la startup Veriqloud.

Ils travaillent aussi sur le calcul quantique vérifié, sur le calcul quantique multipartite sécurisé et sur les caractéristiques qui permettent d'obtenir des avantages quantiques.

Le **LPA** (Laboratoire Pierre Aigrain) de l'ENS Paris est spécialisé en nanotechnologies et en photonique. Ils planchent sur de nombreuses nanotechnologies servant à la création de qubits et au tranport d'informations quantiques : films minces supraconducteurs, circuits supraconducteurs et micro-ondes pour leur contrôle, gaz bidimensionnels d'électrons de très haute mobilité, boîtes quantiques semiconductrices.

Ils sont à l'origine de la création de nanotubes de carbone servant de pièges à électrons potentiellement utilisables dans des qubits à spin d'électron, ce qui a mené à la création de la startup CNT Technologies, déjà citée.

Leurs travaux dans les qubits supraconducteurs visent à les les protéger contre les erreurs avec un plus faible nombre de qubits physiques intégrables dans un qubit logique en 1D au lieu d'être en 2D comme avec les surface codes classiques. Les codes de correction d'erreurs Cat-Qubit fonctionneraient avec seulement 9 qubits physiques et apporteraient un gain exponentiel dans la suppression des erreurs. Ils permettent aussi de se passer de la "magic state distillation", une technique complexe de codes de correction d'erreurs. Ces travaux sont pilotés par une équipe mixte associant l'ENS, Inria (l'incontournable Mazyar Mirrahimi) et l'Ecole des Mines de Paris[613].

---

[612] C'est précisé dans leur plan stratégique scientifique 2018-2022, 2018 (93 pages), pages 47 et 48.

[613] Voir à ce sujet Repetition cat-qubits: fault-tolerant quantum computation with highly reduced overhead, de Jérémie Guillaud et Mazyar Mirrahimi, avril 2019 (22 pages).

Le **LKB** (Laboratoire Kastler Brossel) est un autre laboratoire de l'ENS Paris où travaille notamment le prix Nobel Serge Haroche.

Ils sont focalisés sur l'information et l'optique quantique, les interactions entre matière et lumière, la simulation quantique et de la métrologie de précision avec des atomes de Rydberg (du rubidium) piégés magnétiquement dans des cavités optiques et excités par laser, qui est à l'origine de la startup Pasqal.

Dans ce laboratoire, Thibault Jacqmin travaille sur la génération de photons micro-ondes avec des NEMS. Traduction : NEMS = MEMS mais au lieu de l'échelle micro, c'est de l'échelle nanoscopique. Ce sont des dispositifs nano-mécaniques tels que ceux que l'on trouve dans les nombreux capteurs qui équipent nos smartphones. Pourquoi générer des micro-ondes de cette manière ? C'est probablement pour permettre le contrôle de qubits de types divers, notamment supraconducteurs, avec des dispositifs miniaturisés.

Le **LTCI** (Laboratoire Traitement et Communication de l'Information) de TelecomParistech est un laboratoire industriel fonctionnant avec des partenariats avec le privé et via des chaires. Son équipe « Information Quantique et Applications » (IQA) est spécialisée dans les aspects théoriques et expérimentaux des communications quantiques.

Ils développent des protocoles de cryptographie quantique hybrides à base de CV-QKD compatibles avec les réseaux de fibres des opérateurs télécoms ainsi que des répéteurs de QKD.

Ils sont contributeur, membre fondateur et rapporteur à l'ETSI QKD-ISG sur le processeur de standardisation de QKD. L'équipe est pilotée par Isabelle Zaquine et on y trouve notamment Romain Alléaume.

L'IRIF (Institut de Recherche en Informatique Fondamentale) est une UMR associant le CNRS et l'Université Paris Diderot.

Elle héberge notamment deux équipes de l'Inria. Au CNRS, l'IRIF est rattaché à l'INS2I (Institut National des Sciences de l'Information et de leurs Interactions) et à l'INSMI (Institut National des Sciences Mathématiques et de leurs Interactions). Le laboratoire travaille dans le calcul quantique, la cryptographie et les communications. On y trouve l'équipe de Iordanis Kerenidis qui travaille notamment sur les algorithmes quantiques, en particulier dans le machine learning.

Le laboratoire **MPQ** (Matériaux et Physique Quantique) de l'Université Paris Diderot s'intéresse notamment à la technique des ions piégés dans les groupes Quantum Physics and Devices (QUAD) et QITE (Quantum Information and Technologies).

Le **LPTHE** (Laboratoire de Physique Théorique et Hautes Energies) de l'Université Paris Sorbonne travaille dans la matière condensée et la physique statistique avec des applications dans les qubits supraconducteurs.

L'**INSP** (Institut des Nanosciences de Paris) de l'Université Paris-Sorbonne est un laboratoire généraliste sur les nanosciences. Ils travaillent notamment sur les NV centers de diamants, sur le spin et le magnétisme et sur le développement de composants de photonique en III-V.

L'**IRCP** (Institut de Recherche de Chimie Paris) associé à l'Ecole Nationale Supérieure de Chimie ParisTech fait de la recherche dans les matériaux innovants.

Au sein de l'école, Philippe Goldner travaille sur la création de qubits à base de nanocristaux dopés par ions de terres rares (europium ou l'erbium) et est impliqué dans le projet SQUARE du Quantum Flagship européen, coordonné par le Karlsruhe Institute of Technology et impliquant aussi Thales. Le laboratoire est aussi impliqué dans le projet ASTERIQS qui planche sur les qubits à base de NV centers dans les diamants.

Le **LPEM** (Laboratoire de Physique et d'Etude des Matériaux) de l'ESPCI et de l'UMPC travaille notamment dans la supraconductivité ainsi que sur les fermions de Majorana.

Le **LPTMC** (Laboratoire de Physique Théorique de la Matière Condensée) de l'Université Paris-Sorbonne (Jussieu) n'a pas l'air d'être impliqué dans la physique quantique en relation avec l'informatique quantique. Néanmoins, ils s'intéressent à la simulation du vivant, qui est une des applications clés, à long terme, du calcul quantique.

SYRTE (Laboratoire Systèmes de Référence Temps-Espace) situé à l'Observatoire de Paris travaille dans le domaine de la métrologie quantique, notamment la gravitométrie, les gyroscopes quantiques et sur la mesure du temps dans des horloges atomiques et optiques. Ils sont partenaires du NIST aux USA.

Le **plateau de Saclay** comprend une densité de laboratoires encore plus forte que dans Paris intra-muros. Ils sont situés aussi bien du côté Ouest de la N118 avec l'Université d'Orsay et ses nombreux laboratoires, le CEA de Saclay, l'école d'ingénieurs CentraleSupelec et l'ENS ex-Cachan, puis du côté Est avec l'Ecole Polytechnique et ses écoles d'application, en particulier l'Institut d'Optique ainsi que le CEA List.

Au **CEA**, l'équipe Quantronics de Daniel Estève dans le laboratoire Iramis de Saclay planche depuis près de 20 ans sur les qubits supraconducteurs. Le laboratoire de Daniel Estève comprend une quinzaine de personnes.

Son homologue à l'Université de Yale aux USA en comprend une trentaine. Selon lui, il ne suffit pas d'aligner en parallèle plus de chercheurs pour accélérer la recherche dans ce domaine !

Christian Gamrat fait de son côté partie du CEA List dans la branche CEA Tech et planche sur les outils de développement et algorithmes quantiques.

L'**IphT** (Institut de Physique Théorique de Saclay) associe le CEA et le CNRS. Ils planchent sur la physique de la matière condensée, dont les supraconducteurs à haute température, et sur les fermions de Majorana. Mais leur principal centre d'intérêt a l'air d'être surtout l'astrophysique.

Le **LAC** (Laboratoire Aimé Cotton) de l'Université Paris-Sud (Orsay) est situé à l'ENS Cachan. Il travaille aussi sur les atomes froids et les interactions entre atomes et lumière.

Ils créent notamment des qubits en combinant un ion optiquement actif d'erbium et un spin nucléaire d'yttrium.

Le **C2N** (Centre des Nanosciences et des Nanotechnologies) de l'Université Paris-Sud est un autre laboratoire de photonique quantique. On y trouve notamment Jacqueline Bloch et Pascale Senellart, toutes deux médailles d'argent du CNRS, cette dernière étant à l'origine de la startup Quandela. Ils travaillent notamment sur le couplage lumière-matière dans les semiconducteurs. On y trouve aussi notamment des équipes en électronique quantique (Frédéric Pierre).

Le **LPS** (Laboratoire de Physique des Solides) de l'Université Parisud travaille sur le magnétisme, les supraconducteurs à jonctions Josephson, la thermodynamique, la spintronique supraconductrice et la dynamique quantique. Ils développent aussi des codes de dynamique quantique et semi-classique et de contrôle quantique avec des applications en information quantique.

Le **LPTMS** (Laboratoire de Phyique Théorique et de Modèles Statistiques) de l'Université Parisud a plusieurs cordes à son arc dans la physique quantique sans que le lien avec le calcul quantique soit immédiatement décelable.

Le **LCP** (Laboratoire de Chimie Parisud) travaille les supraconducteurs et sur la dynamique et contrôle d'ions piégés par impulsions laser. Ils développent des modèles de calcul hybrides de chimie quantique (quantiques+traditionnels) mettant en œuvre la MCTDH (Multi-configuration time-dependent Hartree) qui permet de résoudre l'équation de Schrödinger pour la simulation d'interactions entre atomes dans des molécules.

Au programme : physique de la matière condensée, modélisation de systèmes classiques et quantiques via la physique statistique, chaos quantique, théorie des nombres et chaos quantique, aspects théoriques de l'information quantique; atomes froids, systèmes intégrables quantiques, groupes quantiques, etc.

L'**ISMO** (Institut des Sciences Moléculaires d'Orsay) est de l'Université Parisud travaille sur la dynamique quantique, les interactions entre particules lourdes et électrons à basse température, le couplage lumière/matière et sur les logiciels de simulation de la physique quantique.

Le **CPht** (Centre de Physique Théorique de Polytechnique) est spécialisé entre autres choses dans la physique de la matière condensée. Mais pas au point de créer des qubits supraconducteurs ! On y trouve notamment le groupe de Karyn Le Hur qui est spécialisée dans la physique de la matière condensée.

Le **Laboratoire Charles Fabry** de l'Institut d'Optique est spécialisé dans les lasers et l'optique quantique. On y trouve Alain Aspect (bien qu'il ait dépassé l'âge de la retraite), Philippe Grangier (notamment spécialisé dans la CV-QKD) ainsi qu'Antoine Browaeys, cofondateur de la startup Pasqal et ses qubits à atomes froids contrôlés par lasers.

Le **LIX** (Laboratoire d'Informatique de l'Ecole Polytechnique) est notamment actif dans les algorithmes de cryptographie post-quantique.

Le **PMC** (Laboratoire de Physique de la Matière Condensée) est un autre laboratoire de l'école Polytechnique. Ils travaillent notamment sur la dynamique de spin dans les semi-conducteurs et les couches minces magnétiques.

Le **L2S** (Laboratoire Signaux et Systèmes) de CentraleSupelec est actif dans la recherche en systèmes quantiques. On y trouve notamment l'enseignant-chercheur Zeno Toffano qui s'intéresse en particulier à la mesure des états quantiques et aux valeurs propres (eigenvalues).

Le **LPQM** (Laboratoire de Photonique Quantique et Moléculaire) associe l'ENS Paris Saclay et l'école CentraleSupelec. Leurs domaines sont la cohérence et les corrélations quantiques.

Le **LRI** (Laboratoire de Recherche en Informatique) situé à CentraleSupélec est géré par Benoît Valiron qui y fait de l'enseignement et de la recherche en calcul quantique, un domaine encore assez peu enseigné dans les grandes écoles d'ingénieurs.

Thales RT (Thales Research and Technology) fait de la R&D pour créer des solutions de métrologie quantique industrialisées. Ils ont notamment développé une expertise dans les NV centers de diamants.

L'**Onera** étudie l'optique quantique sur son site de Palaiseau.

C'est à ce titre qu'il coordonne le projet ASTERIQS du Flagship Quantique Européen, "Advancing Science and Technology through diamond Quantum Sensing".

Ils ont aussi des équipes de chercheurs en photonique, dans les matériaux semiconducteurs dits III-V (gallium, …) avec une unité de fabrication de prototypes située dans leurs locaux à Palaiseau, dans la métrologie (gravimètre, horloge atomique, accéléromètre) et dans la QKD.

Passons à d'autres parties de l'Ile de France : Cergy-Pontoise, Villetaneuse et Versailles.

Le **LPTM** (Laboratoire de Physique Théorique et Modélisation) de l'Université de Cergy-Pontoise s'intéresse aux atomes froids, en liaison avec l'Institut Francilien de Recherche sur les Atomes Froids (IFRAF).

Ils étudient aussi le graphène, le transport quantique électronique, les phases topologiques et l'intrication.

Le **LSPM** (Laboratoire des Sciences des Procédés et des Matériaux) de l'Université Paris 13 à Villetaneuse travaille sur les procédés de fabrication de NV centers de diamants, de nanotubes de carbone et de graphène et sur les applications associées.

Le **LPL** (Laboratoire de Physique des Lasers) de l'Université Paris 13 à Villetaneuse travaille dans la photonique et les atomes froids, leurs pièges et sur la métrologie quantique. C'est le laboratoire d'Hélène Perrin, déjà citée, qui en est Directrice Adjointe.

Le **GEMaC** (Groupe d'Etude de la Matière Condensée) de Versailles travaille aussi dans le domaine des diamants et du graphène, sur l'électronique de spin et le magnétisme. On y trouve aussi de la QKD et de la mémoire quantique photonique. .

Du côté des approches de recherche collaboratives en Ile de France…

Le GDR[614] **IQFA** (Quantum Engineering, from Fundamental Aspects) regroupe une cinquantaine de laboratoires de recherché en physique quantique ainsi qu'en informatique quantique. D'un point de vue pratique, ce genre de groupe se matérialise sous la forme de congrès de chercheurs et d'une coordination nationale de la recherche dans son domaine.

L'Initiative de Projet Stratégique **IQUPS** (Ingénierie Quantique à l'Université Paris-Saclay) est répartie sur plusieurs sites de l'Université Paris-Saclay aussi bien côté Palaiseau/X que côté Orsay. Elle regroupe une dizaine d'UMR (Unités mixtes de recherche) associant outre le CNRS, le CEA, l'Institut Mines Télécom et l'Ecole Polytechnique situées dans la zone Est du plâteau de Saclay. Lancée en 2017, elle vise à coordonner les efforts d'ingénierie en informatique quantique. Il ne semble pas, néanmoins, qu'ils aient choisi une voie spécifique de qubits entre les supraconducteurs, les spins d'électrons et la photonique.

Le groupe **Paris Center for Quantum Computing** (PCQC) qui associe 22 chercheurs franciliens issus de divers laboratoires, dont Philippe Grangier. Le **CNRS** a regroupé informellement ses efforts avec le groupe de travail Informatique Quantique qui travaille plutôt sur la dimension algorithmique.

On peut aussi signaler l'initiative du pôle de compétences en calcul haute performance **Teratec** (basé à Bruyère le Chatel, près de la Direction des Affaires Militaires du CEA) autour du quantique[615].

Elle vise à développer des algorithmes quantiques, des méthodes de développement hybrides, des cas d'usage, et d'informer, former et animer une communauté.

[614] Groupement de recherche, entité de recherche collaborative qui aggrège plusieurs laboratoires de recherche.

[615] Teratec fédère plusieurs acteurs privés et publics du calcul haute performance dont Atos, le CEA, le CERFACS (Centre Européen de Recherche et de Formation Avancée en Calcul Scientifique), Dassault-Aviation, EDF, l'IFPEN, le PCQC (Paris Centre for Quantum Computing), Total et l'Université de Reims.

Ils bénéficient d'un simulateur QLM d'Atos installé au CRTT (Centre de Calcul, Recherche et Technologie) du CEA à Bruyères-le-Châtel.

Enfin, le **SIRTEQ** (Science et Ingénierie en Région Ile de France pour les Technologies Quantiques) est une communauté qui groupe les laboratoires de recherche de l'Ile de France qui sont focalisés sur les technologies de communications quantiques.

Selon eux, il y a en Ile de France 650 chercheurs dans le quantique en tout (physique, algorithmes, télécommunications, cryptographie) répartis dans 100 équipes de 30 laboratoires de recherche.

Grenoble

L'écosystème quantique de Grenoble est dense, bien organisé et très focalisé sur la création de qubits à base de spins d'électron mais aussi en supraconducteurs, le tout avec de bonnes compétences en photonique. C'est probablement l'endroit où la coordination entre les équipes de recherche fonctionne le mieux, notamment en intégrant les étapes clés de l'industrialisation.

La recherche quantique à Grenoble est pilotée par différentes branches du CEA (Leti en nanoélectronique et IRIG en physique), du CNRS (dans l'Institut Néel) et du LPMMC et notamment par deux équipes mixtes CNRS et CEA : NPSC (NanoPhysique et Semi Conducteurs) qui planche sur de la métrologie quantique, de la photonique quantique, de la thermodynamique quantique et des fondements de la mécanique quantique et Quanteca, créé en 2019, qui concerne toutes sortes de qubits statiques (CMOS, supraconducteurs, etc).

L'**Institut Néel** est un laboratoire du CNRS spécialisé dans la physique de la matière condensée et disposant d'une masse critique de chercheurs dans le quantique. Ils sont situés sur la presque-île de Grenoble à deux pas du CEA-Leti. Ils explorent les pistes des qubits à spin d'électrons, supraconducteurs et en photonique. On y trouve notamment Tristan Meunier et Alexia Auffèves.

Le **CEA-Leti** de Grenoble est le laboratoire de micro et nanoélectronique du CEA. Il est notamment à l'origine de la technologie de wafer SOI qui a donné lieu à la création de SOITEC. Le Leti est focalisé sur l'ingénierie de qubits à spins d'électrons CMOS. L'équipe de Maud Vinet a fédéré les efforts de plusieurs laboratoires du CEA et du CNRS.

L'**IRIG** (Institut de Recherche Interdisciplinaire de Grenoble) est un peu le pendant de l'Institut Néel du côté de la recherche fondamentale au CEA et en amont de ce que le Leti peut ensuite étudier côté ingénierie et fabrication. Il comprend notamment le laboratoire Laboratoire PHotonique ELectronique et Ingénierie QuantiqueS qui travaille sur la physique de la matière condensée.

Le **LPMMC** (physique de la matière condensée) de l'Université Grenoble Alpes est une UMR du CNRS tournée vers la physique théorique de la matière condensée et la physique quantique, les interactions quantiques à N-corps, la supraconductivité et la superfluidité, et sur l'évolution temporelle de systèmes quantique sous l'effet de champs magnétiques et électriques.

L'**IJF** (Institut Joseph Fourier) de l'Université de Grenoble travaille sur la dynamique quantique et en particulier sur les questions de décohérence et de bruit quantique thermique..

L'école d'ingénieurs en informatique **Ensimag** a lancé en 2019 un partenariat avec IBM qui est devenu parrain de la promotion 2021, avec en tête l'idée de former les élèves à la programmation quantique sur la plateforme IBM Q / Qiskit.

Le **LIG** (Laboratoire d'Informatique de Grenoble) s'intéresse aux algorithmes quantiques en général. On y trouve notamment le chercheur Mehdi Mhalla qui se penche sur la résolution quantique de problèmes de graphes.

La recherche en ordinateur quantique à Grenoble est actuellement structurée autour de trois initiatives : **QuEnG**, **QuantECA** et **QuCube** qui ne sont d'ailleurs pas du même niveau.

QuEnG (Quantum Engineering Grenoble) est un écosystème qui va du philosophe à l'industriel. C'est une initiative chapeau trans-laboratoire, trans-disciplinaire et trans-sectorielle. Elle s'attaque à la réalisation de qubits en CMOS et électrons piégés. Les équipes travaillent en physique sur de nombreuses autres filières : en photonique, sur des qubits supraconducteurs, à spins d'électrons et à base d'aimants moléculaires. Ces branches sont complémentaires. Ainsi, la photonique peut permettre la création de liens entre processeurs quantiques pour distribuer les traitements.

Le travail sur les capteurs joue un rôle pour mesurer l'état des qubits, quels qu'ils soient. Ils creusent aussi les questions de thermodynamique. Alexia Auffèves, de l'Institut Néel du CNRS, en est une grande spécialiste. Ils s'intéressent aux capteurs, aux codes de correction d'erreurs et aux algorithmes quantiques, notamment en partenariat avec Atos.

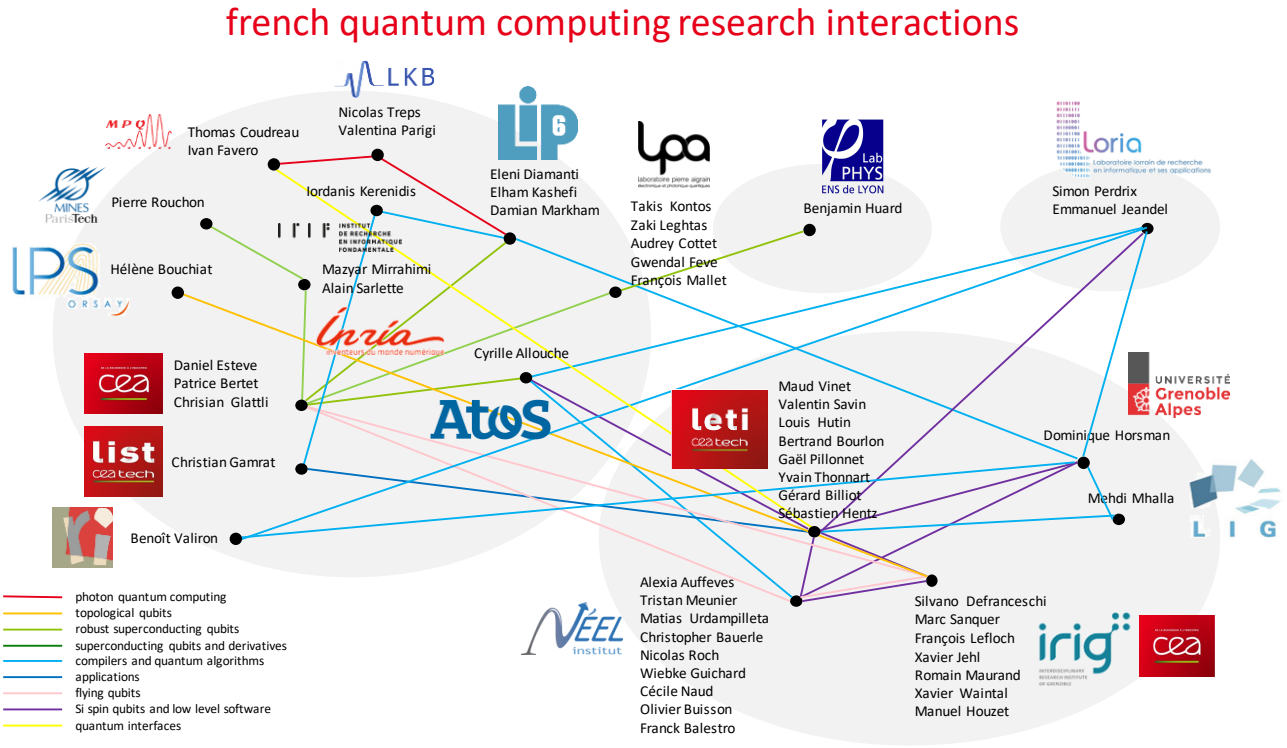
Des équipes font aussi le lien entre physique quantique et philosophie avec Vincent Lam. L'initiative comprend aussi la formation d'ingénieurs en physique et en calcul quantique avec des cursus divers dont un projet avec l'Ensimag, la grande école d'informatique de Grenoble. Ils sont aussi partenaires d'IBM.

QuEnG est une initiative non pérenne financée notamment par l'IDEX (Initiative d'Excellence) des Programmes d'Investissements d'Avenir (PIA) de l'UGA (Université Grenoble-Alpes) avec 1,7M€ complétés par un financement européen FP7 de 1,9M€ couvrant notamment des bourses de thésards. Le tout bénéficie aussi du financement de 14M€ de l'ERC Synergy Grant obtenu par l'équipe QuCube en 2018 (financement européen de recherche d'excellence). En tout, l'initiative a bénéficié de 23M€ de financements publics étalés sur 3 ans. QuEnG regroupe une centaine de chercheurs en sciences fondamentales. S'y ajoutent ce qu'ils appellent des avantages en nature avec l'accès aux salles blanches du CNRS, du CEA-Leti, de SOITEC à Bernin et de STMicroelectronics à Crolles près de Grenoble qui permettent la fabrication de nombreux composants critiques : wafers SOI (silicon on insulators), prototypes de composants et industrialisation de leur fabrication.

QuantECA ou Quantum Electronic Circuits Alps est une initiative qui se situe au-dessous de QuEnG et couvre la partie intégration à grande échelle de qubits dans des puces. Elle regroupe le CEA-Leti, le département de physique de l'IRIG (ancien INAC, Interdisciplinary Research Institute of Grenoble, qui fait partie du CEA) et l'Institut Néel du CNRS. Leur champ d'action est la création de circuits de qubits stables, scalables et bien intriqués. Ils planchent aussi sur les technologies de stockage et de transport de l'information quantique. Ils s'appuient sur trois branches technologiques (supra-conducteurs/optique/spin d'électron spin). Ils maîtrisent en particulier une technologie unique au monde : l'optomécanique intégrée dans des circuits CMOS. Le CMOS est une partie de l'effort. C'est au sein de Quanteca que se situe l'équipe de Maud Vinet, Tristan Meunier et Silvano De Franceschi qui ont obtenu un financement ERC Synergy Grant pour le projet QuQube.

QuCube est l'initiative qui a récupéré le financement ERC Synergy Grant de 14M€ fin 2018. Son objectif est de créer un ordinateur quantique avec plus de 100 qubits d'ici moins de 10 ans en technologie CMOS / spin d'électron. Les qubits auront une taille de 100 nm avec la possibilité à terme d'en intégrer des millions dans un chipset. L'une des technologies clés à miniaturiser sont les briques de conversion du spin des électrons piégés en charge électrique. Les capteurs associés sont placés dans une couche qui est située en-dessous des qubits. Les éléments de contrôle des qubits (initialisation, portes quantiques) sont placés au-dessus des qubits.

Et voici comment sont reliés les divers laboratoires de recherche en France autour du pôle de Grenoble. Ce visuel est dérivé d'un schéma de Maud Vinet du CEA-Leti.



Lyon

La recherche à Lyon est bien équilibrée entre la partie physique et la partie mathématique et logicielle du quantique.

L'**INL** (Institut des Nanotechnologies de Lyon) est situé à Centrale Lyon (Ecully). Ils planchent sur les semiconducteurs et la photonique. Ils disposent d'une plateforme technologique de prototypage de composants, notamment en photonique.

L'**iLM** (Institut Lumière Matière) de Lyon est spécialisé comme son nom l'indique en photonique. Je n'ai par contre pas trouvé de liens directs avec le calcul quantique.

L'**Institut Camille Jordan** de Lyon est un laboratoire de recherche en mathématiques qui travaille notamment sur les probabilités quantiques. Il est distribué sur plusieurs sites : Villeurbanne, Saint-Étienne et sur le campus de Centrale Lyon à Écully.

Le **Laboratoire de Physique de l'ENS Lyon** est focalisé sur l'étude de la matière condensée et de l'information contenue dans les dispositifs quantiques, à son amplification, à leur fluctuation, à la thermodynamique de l'informatique quantique, à la mesure quantique et à l'optique quantique. On y trouve notamment Benjamin Huard qui travaille sur les qubits supraconducteurs et leurs codes de correction d'erreurs.

Le **LIP** (Laboratoire de l'Informatique du Parallélisme) de l'ENS Lyon associe le CNRS, l'Inria et l'Université Claude Bernard Lyon 1. Son équipe MC2 travaille sur l'informatique théorique et la théorie de la complexité. On y trouve notamment Omar Fawzi, médaille de bronze 2019 du CNRS et spécialiste de la théorie de l'information quantique. Il mène ses travaux dans l'équipe MC2 du LIP.

Occitanie

La recherche quantique à Toulouse est très centrée sur la physique de base et assez éloignée de l'informatique quantique à l'exception du **LPTT**. On trouve sinon deux laboratoires à Montpellier dont un est associé à IBM.

Le **CEMES** (Centre d'Élaboration de Matériaux et d'Etudes Structurales) de Toulouse est spécialisé en physique et en optronique. Il s'intéresse au couplage lumière-matière à l'échelle et la création de capteurs plutôt orientés vers les objets connectés que les applications quantiques.

Le **LCAR** (Laboratoire Collisions Agrégats Réactivité) de l'Université Paul Sabatier de Toulouse travaille notamment sur les atomes de Rydberg mais sans aller jusqu'à créer des qubits basés dessus.

Le **LPCNO** (Laboratoire de Physique et Chimie des Nano-objets) de l'INSA Toulouse est spécialisé en photonique et électronique quantique. Ils étudient les spins d'électrons et de noyaux, les quasi-particules et les quantum dots. Ils visent des applications dans l'informatique quantique. Leurs recherches visent aussi des applications dans le secteur de la santé.

L'**IMT** (Institut de Mathématiques de Toulouse) de l'Université de Toulouse étudie la physique statistique et quantique. On y trouve notamment Clément Pellegrini qui étudie la théorie de l'information quantique et la mesure d'états quantiques.

Le **LPTT** (Laboratoire de Physique Théorique de Toulouse) travaille sur les supraconducteurs et les boucles SQUID à effet Josephson. Petite particularité, ils sont impliqués dans le projet Quantware qui a été cofinancé entre autres par la NSA !

Le **LCPQ** (Laboratoire de Chimie et Physique Quantiques) de l'Université Paul Sabatier de Toulouse développe des codes généralistes de chimie quantique, contribuant aux efforts de simulation simulation moléculaire.

Le **L2C** (Laboratoire Charles Coulomb) de l'Université de Montpellier planche sur la métrologie quantique, la dynamique de spin et le graphène, avec des applications dans la microscopie magnétique.

L'Université de Montpellier est partenaire d'IBM dans la mise en place d'un laboratoire commun sur le quantique qui vise en fait à évangéliser les clients sur les principes généraux et les outils de la plateforme quantique IBM Q.

Le **LIRMM** (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier) se penche notamment sur la création d'algorithmes quantiques. Il collabore avec Total dans ce sens.

Sud

On trouve aussi quelques laboratoires de physique quantique à Marseille dont trois ont un lien direct avec les besoins de l'informatique quantique. Et un laboratoire à Nice.

L'**Institut Fresnel** de Marseille fait de la photonique, donc, inévitablement, peut contribuer aux avancée dans la gestion de qubits à base de photons ainsi que dans la cryptographie quantique à base de QKD.

Le **CPT** des Universités de Marseille et de Toulon travaille sur la dynamique quantique et la diffusion d'ondes dans les fibres optiques et guides de lumières, à l'électrodynamique quantique. Ils sont partenaires de diverses universités étrangères : AalboUTINAMrg University (Danemark), Pontificia Universidad Catolica de Chile, Karlsruhe Institute of Technology (Allemagne), Kyoto Institute of Technology et le Moscow Institute of Physics and Technology.

Le laboratoire **PIMM** (Physique des interactions Ioniques et Moléculaires) de l'Université de Marseille fait de la recherche dans les plasmas, plus en lien avec le projet de fusion nucléaire ITER qu'avec l'informatique quantique.

Le **Laboratoire d'Informatique Fondamentale** de Marseille s'intéresse notamment au calcul quantique. Leur projet Discrete Time Quantum Simulator a été lancé en 2018. Ils travaillent sur les Quantum Walks et le Quantum Cellular Automata qui a l'air de s'apparenter au MBQC.

INPHYNI (Institut de Physique de Nice) de l'Université Nice Côte d'Azur s'intéresse aux atomes froids, au transport d'ondes et aux interactions entre lumière et atomes. Le laboratoire quantique est dirigé par Sébastien Tanzilli.

Bourgogne Franche-Comté

Besançon héberge trois laboratoires dans le quantique et Dijon un quatrième.

Le **LmB** (Laboratoire de Mathématiques de Besançon) de l'Université Bourgogne Franche-Comté étudie les groupes quantiques et les probabilités.

L'Institut **UTINAM** (Univers Transport Interfaces Nanostructures Atmosphère et environnement, Molécules) de l'Université de Besançon étudie notamment les phénomènes de décohérence quantique dans des problèmes de contrôle, de diagnostic, de traitement et de transport de l'information quantique. Cela relève plutôt du champ de la métrologie.

Femto-St est un Institut de recherche à Besançon focalisé sur les nanosciences, l'optique et l'optoélectronique. Ils planchent notamment sur les télécommunications optiques, sur l'optique non linéaire et sur l'imagerie quantique.

Le laboratoire **Icb** (Interdisciplinaire Carnot de Bourgogne) de l'Université de Bourgogne, basé à Dijon comprend une équipe étudiant la dynamique quantique et non-linéaire (DQNL).

Grand Est

La région comprend trois laboratoires sur le quantique situés à Strasbourg, Nancy et Troyes.

Le **Quantum Matter Theory Group** de l'Université de Strasbourg fait de la physique de la matière condensée et travaille aussi sur les interactions entre lumière et matière, notamment avec des atomes de Rydberg.

Le **L2n** (Lumière Nanomatériaux Nanotechnologies) de l'Université de Technologie de Troyes travaille dans l'optoélectronique et les sources de photons.

Le **Loria** (Laboratoire lorrain de recherche en informatique et ses applications) est basé à Nancy. Deux enseignants-chercheurs s'y intéressent au calcul quantique et aux algorithmes : Simon Perdrix et Emmanuel Jeandel. Le premier est l'un des principaux contributeurs aux travaux sur le ZX-Calculus qui sert notamment à la correction d'erreurs dans le calcul quantique.

Ils pilotent le projet **SoftQPro**, en association avec le CEA et Atos, qui s'étale entre 2017 et 2020 et vise à optimiser les programmes quantiques. Visiblement, beaucoup avec le ZX-calculus.

Ailleurs en France

Et pour terminer, voici quelques laboratoires de physique touchant au quantique situés dans d'autres régions, à Rennes, Lille, Bordeaux et Limoges mais sans lien direct apparent avec l'informatique quantique.

L'**IPR** (Institut de Physique de Rennes) est rattaché à l'Université de Rennes. Ils s'intéressent à la dynamique quantique, l'évolution des états quantiques dans le temps.

Le **PhLAM** (Laboratoire de Physique des Lasers Atomes et Molécules) de Lille s'intéresse à la photonique et aux atomes froids.

L'**IEMN** (Institute of Electronics, Microelectronics and Nanotechnology) est un laboratoire situé sur quatre sites à Lille, Villeneuve d'Ascq et Valencienne. Ils sont notamment spécialisés dans la conception de nanostructures quantiques.

Le **LP2N** (Laboratoire Photonique, Numérique et Nanosciences) de l'Institut d'Optique de Bordeaux fait de la recherche en photonique et en métrologie à base d'atomes froids (microgravitométrie).

Le **XLIM** (Limoges) fait entre autres choses de la photonique. Ils sont notamment partenaires avec Thales TRT.

Collaborations internationales

Les partenariats internationaux sont très courants dans la recherche. Nombre de travaux de chercheurs français sont réalisés avec des chercheurs d'autres pays, notamment des USA, du Royaume-Uni, d'Autriche, Pays-Bas et Allemagne. Il suffit de consulter la littérature scientifique pour se rendre compte de l'intensité de cette coopération.

Le CEA a lancé en 2018 un partenariat avec l'**UNSW** australienne et la startup Silicon Quantum Computing (SQC) pour créer des processeurs quantiques CMOS. Le CEA-Leti est aussi partenaire de l'**Imec**, son homologue en Belgique, basé à Louvain avec 1600 chercheurs, couvrant l'IA et le calcul quantique.[616] Comme le CEA-Leti à Grenoble, ils disposent d'une salle blanche pour de la gravure jusqu'en 28 nm et sur wafers de 30 cm et une autre sur wafers de 20 cm pour des MEMS.

Le **Centre Spatial Universitaire de Grenoble** collabore depuis 2017 avec l'**IQOQI** autrichien sur l'envoi de clés quantiques par satellite dans le projet Nanobob.

L'**ANR** avait clôt en février 2018 un appel à projets de recherche, lancé dans le cadre d'un partenariat de recherche avec le Japon (CREST).

Et il existe une autre collaboration internationale sur le quantique associant la France, les Pays-Bas (QuSoft) et la Lettonie.

Startups

Les startups quantiques françaises sont les quatrièmes dans le monde en nombre. Elles sont plutôt spécialisées dans les composants (**CryoConcept** pour la cryogénie, **Muquans** pour la métrologie, **Quandela** pour les sources de photons).

Nous avons côté qubits trois startups avec **CNT Nanotech** (nanotubes de graphène), **Pasqal** (atomes froids) et **NextGenQ** (ions piégés).

Côté logiciels, **Prevision.io** s'intéresse à l'intégration d'algorithmes quantiques dans son offre d'automatisation de recherche d'algorithmes de machine learning dans le cloud. D'autres suivront sans doute, mais prudemment.

Enfin, du côté de la cryptographie quantique et post-quantique, nous avons principalement **CryptoNext**, **CryptoExperts** et **Veriqloud**.

Investisseurs et accompagnement

Dans l'investissement, il y a surtout le fonds d'investissement **Quantonation**, déjà cité, et qui joue un rôle clé dans l'animation de l'écosystème quantique en France.

Citons également le **Deep Tech Founders** qui forme des entrepreneurs/chercheurs dans les deep techs. C'est un programme international créé par l'équipe de Hello Tomorrow. Ils planchent sur la création d'un accélérateur en partenariat avec Quantonation, le **Lab Quantique**.

[616] Voir Partners Double-Team AI & Quantum Computing, de Mathew Dirjish, novembre 2018.

Entreprises

Parmi les grands comptes français ayant publiquement annoncé s'intéresser à l'informatique quantique, on peut citer **Airbus** qui, depuis 2015, étudie diverses domaines d'applications aussi bien côté cryptographie que côté calcul quantiques. Les banques sont aussi intéressées, au moins sur la partie crypto quantique, comme à la **Société Générale** ! D'autres industriels font de la veille active sur le quantique, comme **Total**, **EDF** et **Thales**.

C'est **Atos** qui est l'acteur industriel le plus actif en France sur le calcul quantique. Nous avions déjà eu l'occasion de décrire leur offre logicielle quantique.

Ils ont notamment développé un simulateur quantique sur serveurs à base Intel, le Atos Quantum Learning Machine. Des supercalculateurs dont Bull s'est fait une spécialité. Lancé en septembre 2017, le simulateur aQML a été notamment adopté par le centre de recherches américain d'Oak Ridge du Département de l'Energie, qui teste de nombreux types de supercalculateurs. Il est aussi installé au CEA, à l'Université de Reims et depuis juillet 2018, dans le département de recherche en cybersécurité de l'Université de Sciences Appliquées de Haute-Autriche à Hagenberg. Il a enfin été vendu en février 2019 au Centre des installations scientifiques et technologiques (STFC) Hartree du Royaume-Uni ainsi qu'en août 2019, au C-DAC (Centre for Development of Advanced Computing) en Inde qui créait par la même occasion un Quantum Computing Experience Center[617].

Atos est en contacts avec divers laboratoires de recherche dont le CEA de Saclay et l'équipe de Daniel Estève qui travaille sur les qubits supraconducteurs. En mai 2018, Atos et le CEA lançaient aussi une chaire industrielle sur l'informatique quantique, cofinancée par l'ANR. Dirigée par Daniel Estève, elle est baptisée **Nasniq** pour "Nouvelle architecture de spins nucléaires pour l'information quantique". Donc, avec un axe porté sur un type spécifique de qubit. Par contre, l'annonce de cette chaire évoque des recherches pour faire "*face à l'explosion des données entraînée par le Big Data et l'Internet des Objets*". Pourquoi pas, mais l'informatique quantique ne semble pas vraiment adaptée à court et à moyen terme à l'exploitation de très gros volumes de données. On est dans la complexité algorithmique plutôt que dans le traitement de gros volumes de données, tout du moins compte-tenu de l'état de l'art des algorithmes et architectures quantiques.

Le français conduit par Thierry Breton ambitionne de construire à terme un accélérateur quantique complémentaire de leurs supercalculateurs une fois la technologie mise au point. Ils ménagent leurs options côté matériel en observant ce qui se fait dans l'ensemble des filières du quantique.

[617] Voir Atos et C-DAC signent un accord de coopération pour accélérer le développement de l'informatique quantique et exascale et l'Intelligence Artificielle en Inde, août 2019.

Ils participent notamment aux projets du Flagship Européen **AQTION** (accélérateur quantique) et **PASQuanS** (simulateur analogique quantique). Atos s'intéresse aussi à la cryptographie post-quantique.

Atos est aussi très impliqué dans le projet EuroHPC dont fait partie l'**European Processor Initiative**, cette initiative de développement d'un processeur adapté à la fois aux besoins des supercalculateurs et à ceux de l'embarqué comme dans les véhicules autonomes. Ce dernier projet est piloté par Philippe Notton d'Atos (jusqu'en juin 2019) en étroite collaboration avec de nombreuses institutions et entreprises allemandes. L'axe Franco-Allemand est stratégique pour Atos, notamment du fait que Siemens est un de leurs principaux actionnaires depuis l'acquisition de trois filiales de ce dernier entre 2011 et 2017 (Siemens IT Solutions and Services, Unity et Convergence Creators)[618].

La bataille du quantique va rapidement devenir une bataille de plateformes logicielles. L'un des enjeux d'Atos est donc de pousser ses outils de développement auprès d'un maximum de développeurs, décrits dans la partie idoine de cette série. Pour ce faire, il serait bon qu'ils en proposent rapidement l'utilisation via une offre ouverte en cloud exploitant leur machine aQML.

En mai 2019, Atos faisait une marche en avant dans cette bataille de plateforme en lançant myQLM, une offre d'outils de programmation quantique destinée aux chercheurs, étudiants et développeurs. C'est un environnement de développement en Python permettant de simuler des programmes quantiques sur son propre ordinateur. La programmation est réalisée en AQASM (Atos Quantum Assembly Language) et pyAQSM. Pour accéder à un nombre de qubits dépassant les capacités courantes des PC, soit au-delà d'une vingtaine de qubits, les développeurs pourront exécuter leur code sur un simulateur Atos Quantum Learning Machine dans le cloud, mais de manière payante. Atos envisage de permettre le partage de pratiques, bibliothèques et codes d'applications quantiques. Atos propose également un des traducteurs open source de codes myQLM vers d'autres environnements de programmation quantique.

Atos s'est doté d'un conseil scientifique de compétition avec Cédric Villani, Alain Aspect, Serge Haroche, Daniel Estève, David DiVicenzo (IBM) et Artur Ekert (inventeur des clés quantiques QKD). C'est un très beau panel. Malheureusement entièrement masculin !

En décembre 2018, **IBM** créait un laboratoire quantique (IBM Q Hub) à Montpellier en partenariat avec l'Université de Montpellier et avec le soutien de la Région Occitanie. Ce laboratoire dénommé QuantUM (facile à Googleizer…), c'est surtout un centre d'expertise technique pour évangéliser le marché. L'Université de Montpellier serait très active dans les communications quantiques, les capteurs et la simulation.

[618] En juillet 2018, Atos faisait aussi l'acquisition de Syntel pour $3,4B aux USA, un prestataire de services spécialisé dans le développement et le déploiement d'applications dans le cloud faisant $923M de CA avec 22 500 collaborateurs créé en 1980 par des Indo-Américains. Cela ne semble pas avoir de rapport avec le quantique.

Conférences

Diverses conférences internationales sur l'informatique quantique ont lieu en France, soit de manière permanente, soit de manière passagère.

C'est le cas de l'**ICoQC** (International Conference on Quantum Computing) qui se tenait à l'ENS à Paris en novembre 2018[619].

Pour mobiliser l'écosystème, **Bpifrance** organisait la **Conférence QCB** (Quantum Computing Business) le 20 juin 2019 à Paris avec un beau line-up d'intervenants dont Alain Aspect, Cédric Villani, le CEO de D-Wave, des représentants d'IBM, Rigetti, etc ainsi que les grands chercheurs et entrepreneurs français du quantique comme Maud Vinet (CEA-Leti) et Pascale Senellart (Quandela), le tout avec l'intervention de Cédric O, Antoine Petit (Président du CNRS) et Thierry Breton (Atos).

Le **CEA-Leti** organisait le 28 juin 2019 un workshop quantique à l'occasion des Leti Innovation Days (programme). Il regroupait un excellent panel de chercheurs dans la discipline, issus de nombreux laboratoires de recherche français.[620]

Des colloques scientifiques sont sinon organisés par les différents groupements comme le **PCQC** et le **GDR IFQA**, par exemple le 10e colloque de ce dernier qui a lieu à Paris en novembre 2019 (lien).

Plan public

La mission parlementaire lancée en avril 2019 et pilotée par Paula Forteza a terminé ses auditions à la fin du printemps 2019. Elle devrait remettre son rapport au gouvernement d'ici octobre 2019. Le gouvernement devrait alors préparer un plan quantique pour le pays reprenant tout ou partie des propositions de la mission parlementaire. Le rapport et le plan seront probablement annoncés simultanément d'ici la fin 2019.

Au minimum, nous aurons probablement les figures de style habituelles :

- Le **plan devrait couvrir tous les pans technologiques** des applications du quantique, comme ceux des autres pays. En plus du calcul quantique sous toutes ses formes, nous aurons donc aussi la métrologie quantique (mesure de précision) et les télécommunications et cryptographies quantiques. C'est souhaitable car il faut se garder de faire des choix radicaux dans les technologies, tout du moins au niveau de la recherche fondamentale, ce d'autant plus qu'il existe de nombreuses interactions horizontales entre technologies (la photonique permet de relier entre eux des processeurs quantiques de types variés) et verticales (les atomes froids servent à créer des simulateurs quantiques mais aussi des microgravimètres quantiques). La filière CMOS de Grenoble est un beau pari mais cela ne doit pas être le seul. Celle des atomes froids est aussi intéressante. Et les investissements dans les supraconducteurs peuvent être utiles pour créer des composants supraconducteurs et pas seulement des qubits. Et la photonique est partout !

[619] Voir https://icoqc.sciencesconf.org/.

[620] J'en ai fait un compte-rendu dans Vers une stratégie industrielle de l'informatique quantique ?, juin 2019.

- L'**excellence de la recherche française** sera mise en avant pour légitimer une place de choix du pays dans ce nouveau secteur. Même lorsque cette excellence du est avérée, on se la raconte sur chaque nouveau plan. Il faut certes investir dans la recherche et si possible revaloriser la rémunération des chercheurs qui est un véritable cache-misère. Mais ce n'est pas assez. On considère d'habitude qu'il faut améliorer la transformation de la recherche en innovation. Cela sera critique ici aussi, mais avant cela, il faudra améliorer la coordination entre les laboratoires de recherche fondamentale, notamment entre les dimensions physiques, ingénierie et logicielles. Un ordinateur quantique ne germera pas d'un seul laboratoire mais probablement d'un effort collectif public-privé coordonné. Cela fera peut-être germer des équivalents dans le quantique des 3IA, ces instituts de recherche appliquée sur l'IA.
- Le **financement des deep techs** du secteur sera évidemment à l'ordre du jour dans la lignée des plans lancés par Bpifrance entre mi 2018 et janvier 2019[621]. Les montants nécessaires pour se lancer dans l'informatique quantique sont importants mais pas délirants. Ils sont « classiques » pour ce qui est du logiciel, avec quelques millions d'euros pour démarrer. Pour créer un ordinateur quantique, il faut rapidement quelques dizaines de millions d'Euros.
- Il faudra aussi **former les jeunes** et les moins jeunes, surtout dans la création de solutions logicielles quantiques, sachant que dans le cadre du quantique, la barrière intellectuelle est bien plus élevée, en tout cas, avec les outils de développement actuels. La question est de savoir comment l'Etat pourra accélérer le lancement de ces formations dans l'enseignement supérieur autant dans les grandes écoles du secteur public que dans les universités.
- L'**Etat devra être un client** de technologies quantiques, notamment au niveau de la défense et du renseignement. Il pourra jouer le rôle d'aiguillon pour encourager la création d'acteurs du logiciel, concomitamment avec les grandes entreprises de marchés divers (énergie, transports, santé, finance, télécoms) que l'Etat ne pourra pas forcément activer directement. Le rôle actif de ces dernières sera critique pour créer les germes d'un écosystème quantique actif en France. L'Etat devra les encourager à le faire, au moins moralement.
- L'**enjeu de souveraineté sera mis en avant**. Emmanuel Macron déclarait que les technologies numériques étaient devenues un véritable enjeu de souveraineté, lors de son discours auprès de France Digitale le 17 septembre 2019 à l'Elysée. Le quantique en fait partie. C'est aussi un enjeu de souveraineté numérique et très stratégique car il a trait au régalien : dans la cryptographie, dans la sécurisation des télécommunications, et dans l'outillage de la recherche et de l'industrie pour réaliser des calculs performants. En exagérant un peu, c'est l'équivalent de la maîtrise de la dissuasion nucléaire.

[621] Voir mon post de février 2019, La France des deep techs.

- Il faudra éventuellement construire une **stratégie européenne**. On peut rêver d'un Concorde ou d'un Airbus du quantique. Le premier pour sa symbolique d'excellence technologique et le second pour sa réussite industrielle. Reste à assembler les bonnes briques technologiques et acteurs du privé pour bâtir cette stratégie et créer des offres commerciales. Les seuls projets européens ici comme ailleurs relèvent de la recherche collaborative. Le Flagship quantique européen est de cette veine. Le seul acteur de poids européen véritablement engagé dans cette filière est Atos du côté du calcul quantique et de la cryptographie et Thales du côté de la métrologie quantique.
- L'annonce du rapport et du plan gouvernemental associé devrait générer une **visibilité médiatique** sur le sujet. C'est toujours bon à prendre pour développer un intérêt chez les entreprises et aussi pour susciter des vocations chez les plus jeunes. Devrait suivre la création de nouveaux parcours d'enseignement supérieur sur les différentes facettes du quantique.

Tout cela sera insuffisant pour faire émerger un véritable écosystème industriel du quantique. On l'a bien vu avec l'intelligence artificielle où la France rame globalement derrière les pays leaders (USA, Canada, UK, Chine). La France va produire son plan quantique bien après les autres pays développés (UK = 2013, Canada = 2015, USA = 2016 et 2018, Chine = 2015).

Il y a plein de raisons pour lesquelles les plans du passé ont échoué à générer un leadership français digne de ce nom. J'ai notamment en tête le plan objets connectés de 2014. Son principal dispositif était la Cité des Objets Connectés d'Angers que le monde entier devait nous envier. Début 2019, elle changeait de main en passant de celles d'Eolane au cluster technologique WE Work dans le cadre de la création d'un "Technocampus" de l'électronique, mutualisant des moyens industriels et d'innovation de l'industrie d'assemblage électronique avec la participation notable du groupe Lacroix. Entre temps, le marché mondial des objets connectés ne s'est pas développé aussi vite que prévu et très peu d'acteurs français ont réussi à percer à l'échelle internationale, surtout dans les marchés grand public.

Les plans industriels échouent souvent dans la jonction entre la recherche, l'industrialisation et les marchés. On croit naïvement que l'excellence de la recherche se transforme magiquement en succès commercial. Et qu'il suffit de greffer des commerciaux ou des "business developers" pour arriver à percer. Ce n'est bien entendu pas le cas.

Dans les deep techs, comme ailleurs, il faut créer un produit, être différencié et compétitif par rapport au reste du monde, offrir une solution pertinente à des segments clients identifiés et bien entendu bien marketer et vendre sa solution à l'échelle mondiale, le marché US étant souvent critique pour réussir à l'échelle. Une fois cela réalisé, le nirvana de la création d'un produit-plateforme et d'un écosystème associé peut s'en suivre. Un bel alignement de planètes !

Le tout devra se faire en tenant compte d'une spécificité du quantique que l'on ne retrouve pas forcément dans les autres vagues technologiques récentes ayant donné lieu au lancement de plans nationaux : la dimension temporelle. Elle est différente dans les quatre branches du quantique : le temps est court pour la métrologie quantique et la cryptographie quantique car les technologies au point et déployables.

Il en va autrement du calcul et de la simulation quantiques pour lesquels la science est encore dans un temps long. On peut être trompé par les annonces d'IBM et Google qui laissent à penser qu'ils ont engagé une belle exponentielle de progrès avec leurs ordinateurs quantiques au point de laisser tous les autres sur la route. Ils avancent et ils font du marketing mais pas forcément plus rapidement que nombre de laboratoires de recherche et startups dans le monde investis dans d'autres filières.

Quels que soient les moyens employés et leur articulation entre recherche publique et investissements privés (entreprises établies ou startups), il faut savoir les investir dans la durée. La quête de l'ordinateur quantique est un pluri-marathon scientifique et technologique, pas un 100 m du type de ceux qui occupent nombre de licornes de l'univers de l'Internet. Leurs réussites scientifiques et technologiques devraient d'ailleurs moins nous impressionner que ce qu'ils font pour éduquer le marché et se créer un écosystème de chercheurs et développeurs utilisant leurs technologies. Les grandes batailles industrielles du numérique sont toujours des batailles de plateformes technologiques et des écosystèmes associés !

Dans une stratégie, il faut aussi planifier quelques coups d'avance. Pour sécuriser une éventuelle avancée française dans la concurrence mondiale, il faudra s'assurer que les entreprises françaises ou européennes du secteur le restent, que l'approvisionnement en matières premières est bien garanti (silicium purifié d'isotope 28, titane-niobium pour les câblages supraconducteurs, hélium 3 pour la cryogénie), qu'un bon mix de brevets et de secret industriel protège la propriété intellectuelle et que l'on conserve les outils industriels de production des composants clés. Et côté logiciels, il faudra pouvoir compter dans l'inévitable bataille de plateformes qui structurera le marché du développement d'applications.

Avant même de parler de packaging ou de design de produit, il faut pouvoir créer des ordinateurs quantiques fonctionnels "top to bottom", y compris les nombreuses couches logicielles nécessaires pour les piloter et les programmer. C'est un défi scientifique et d'ingénierie qui nécessite de croiser de très nombreuses disciplines.

Un ordinateur quantique peut difficilement sortir d'un simple garage comme le furent les premiers micro-ordinateurs d'Apple. Ces derniers utilisaient d'ailleurs des processeurs Motorola, sans lesquels rien n'aurait été possible, et qui nécessitaient déjà des salles blanches bien équipées pour les fabriquer. Idem pour la mémoire RAM ! C'est dans cette intégration de compétences diverses que les équipes de recherche françaises peuvent faire la différence. Dans le quantique, la recherche collaborative prend tout son sens. Elle implique de nombreux laboratoires et de nombreuses disciplines.

Conclusion

L'informatique quantique est un monde à explorer qui symbolise parfaitement l'univers de l'innovation et de l'entrepreneuriat extrême : il est plein d'incertitudes, de risques et d'échecs. Il y a du "test & learn", du croisement de sciences, le besoin d'investir très en amont de la réussite économique avec un rôle critique des Etats, les seuls à même de voir loin, à plus de 10 ans.Nombreuses sont les voies parallèles d'exploration du possible qui ont été lancées par les chercheurs et les entrepreneurs. Seuls quelques-uns réussiront comme le veut la loi du genre. Une industrie nouvelle émergera de tout cela.

Pour rédiger cet ouvrage, j'ai téléchargé et compulsé plus de 1100 documents librement disponibles sur Internet et visualisé des dizaines d'heures de conférences et de cours sur YouTube.

Il me faut remercier plusieurs personnes de talent ici. A commencer par **Fanny Bouton**, ma *sparring partner* pour la conférence Le quantique, c'est fantastique du Web2day, délivrée le 14 juin 2018 et excellente vulgarisatrice. Nous avons aussi sauvé un chat en remplaçant celui de Schrödinger par un topinambour !

Cette conférence de Nantes, les suivantes et cet ebook tirent aussi parti de rencontres ou d'échanges avec une belle brochette de spécialistes du secteur qu'il nous faut remercier : **Alain Aspect** (X, SupOptique), **Daniel Estève** (CEA-DRF), **Christian Gamrat** (CEA-LIST), **Maud Vinet** (CEA-Leti à Grenoble), **Tristan Meunier** (CNRS Grenoble), **Alexei Tchelnokov** (CEA Grenoble), **Laurent Fulbert** (CEA-Leti Grenoble), **Cyrille Allouche** et **Philippe Duluc** (Atos), **Bernard Ourghanlian** et **David Rousset** (Microsoft), **Pat Gumann** (IBM), **Etienne Klein** (CEA), **Christophe Jurczak** et **Zoé Amblard** (Quantonation), **Nicolas Gaude** (Prevision.io) et **Françoise Gruson** (Société Générale).





Nous avons depuis pu rencontrer encore plus de chercheurs dans le quantique tels que **Philippe Grangier** (Institut d'Optique), **Elham Kashefi** (LIP6), **Pascale Senellart** (C2N et Quandela), **Franck Balestro** et **Alexia Auffèves** (CNRS) et **Mathieu Desjardins** (LNA et CNT Technologies).

Ces textes ont aussi bénéficié des relectures attentives de **Godefroy Troude**, jouant le candide sur le sujet et de **Zoé Amblard** pour la première édition.

La seconde édition a bénéficié de l'apport de **Peter Eid** (élève-ingénieur à Centrale-Supelec) et **Valérian Giesz** (CEO Quandela) pour la partie dédiée à la cryptographie, d'**Alexia Auffèves** (CNRS, Institut Néel), notamment sur l'écosystème de recherche français et les questions de thermodynamique, de **Nicolas Gaude** (CEO de Prevision.io) pour la partie algorithmes quantiques, d'**Harold Ollivier** (LIP6) pour l'introduction et de **Maud Vinet** (CEA-Leti) pour les parties CMOS/electron spins.

A plusieurs, on est toujours meilleurs !

Bibliographie

Voici un peu en vrac quelques ouvrages généralistes et autres sources d'informations sur l'informatique quantique que j'ai pu consulter pour préparer et mettre à jour cet ebook.

Bande dessinée

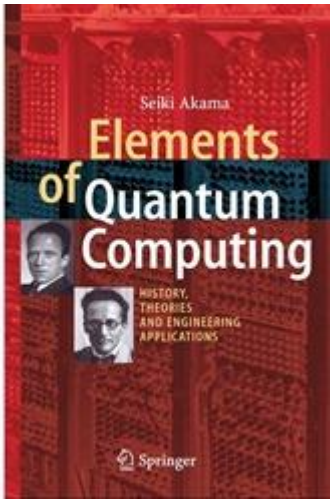
Le Mystère du monde quantique de Thibault Damour et Mathieu Burniat est une bande dessinée destinée à un large public et qui explique les principes de base de la mécanique quantique et leur origine historique.

Livres et ebooks

Les ouvrages cités ici sont majoritairement téléchargeables gratuitement.

Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages) est la référence incontournable sur les bases de l'informatique quantique. Le livre répond à de nombreuses questions clés sur le sujet, en particulier sur les modèles mathématiques de l'algèbre linéaire utilisés dans le calcul quantique.

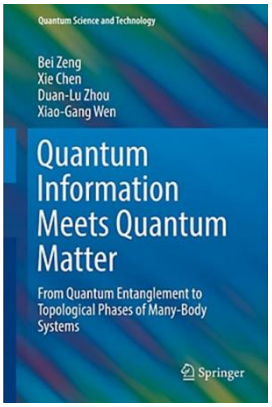
Elements of Quantum Computing de Seiki Akama (133 pages) et qui est à la fois concis, précis et assez complet sur les recoins de la mécanique et de l'informatique quantiques, avec qui plus est une bonne vision historique.

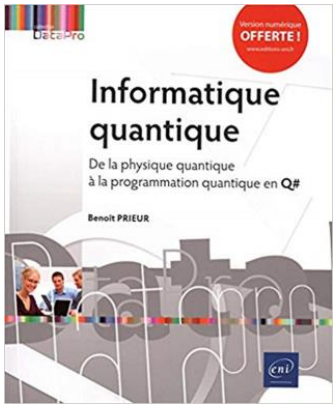


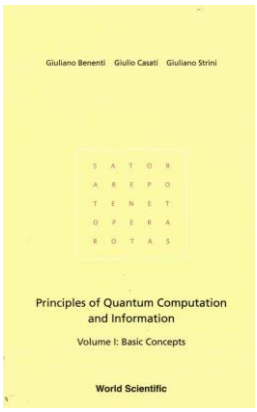
Mon grand Mécano quantique de Julien Bobroff, un ouvrage de vulgarisation de la mécanique quantique qui s'appuie sur l'approche expérimentale. Il y décrit notamment la supraconductivité, l'effet tunnel, l'IRM et les lasers. On trouve de nombreuses conférences de l'auteur sur YouTube où il se focalise surtout sur l'effet supraconducteur (vidéo, 1h54). Voir aussi le site de vulgarisation de la physique La Physique Autrement.

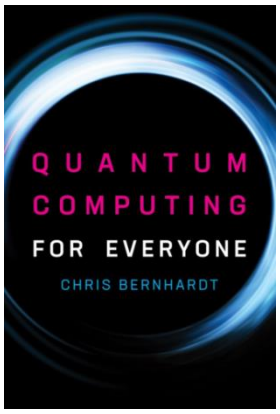
La seconde révolution quantique trouve déjà de nombreuses applications de Xavier Bouju, 2019, un bon travail de vulgarisation.

Quantum Information Meets Quantum Matter de Bei Zeng, Xie Chen, Duan-Lu Zhou et Xiao-Gang Wen. Il est disponible dans une version de février 2018 sur Arxiv en téléchargement libre (373 pages).









Informatique quantique - de la physique quantique à la programmation quantique en Q# de Benoit Prieur, 2019 (244 pages). Il démarre par les príncipes généraux de la physique quantique. La partie sur les ordinateurs quantiques eux-mêmes est assez maigre et n'explore que quelques technologies (supraconducteurs et RMN, qui est peu utilisée). Le reste est dédié à l'apprentissage de la programmation en Q#, le langage de programmation quantique de Microsoft.

L'avantage quantique, enjeux industriels et formation, 2019 (56 pages), un document de qualité créé par la Fondation Mines-Télécom. Il couvre tous les aspects du quantique, du calcul aux télécommunications en passant par la métrologie. Il est certainement plus digeste que « Comprendre l'informatique quantique » mais ne décrit pas trop l'ingénierie des ordinateurs quantique comme je le fais dans cet ebook.

Quantum Internet, un magazine de 60 pages présentant les différentes facettes de l'informatique quantique, édité par TU Delft (2019).

Principles of Quantum Computation and Information, A Comprehensive Textbook de Giuliano Benenti, Giulio Casati, Davide Rossini et Giuliano Strini, décembre 2018 (598 pages).

Quantum computing de Joseph Gruska (non daté, 390 pages), une autre base assez complète couvrant tous les aspects du calcul et de la communication quantiques.

Quantum Computing for Everyone de Chris Bernhardt, 2019 (216 pages).

Unconventional Computation de Bruce MacLennan, Université du Tennessee, novembre 2018 (304 pages).

Introduction to Quantum computing de Suau Adrien, 2018 (64 pages).

Notes de cours sur la Mécanique quantique de Frédéric Faure, 2015 (397 pages) qui m'a donné quelques pistes pour relier la mécanique quantique à son formalisme mathématique et notamment pour expliquer l'équation de Born.

Introduction to quantum computing algorithms d'Arthur Pittenberger, 2001 (152 pages).

An Introduction to Quantum Computing de Phillip Kaye, Raymond Laflamme et Michele Mosca, 2007 (284 pages).

Introduction à l'information quantique de Yves Leroyer et Géraud Sénizergues, 2016 (110 pages).

Présentations

Quantum computing Overview par Sunil Dixit, septembre 2018 (94 slides) est une presentation de Northrop Grumman qui fait un tour assez large du calcul quantique et des modèles mathématiques sous-jacents.

A pedestrian introduction to quantum computing par Jérome Milan, Ecole Polytechnique, 2010 (55 slides) qui explique de manière bien illustrée les grandes principes du calcul quantique et en particulier de l'algorithme de Grover.

Articles

L'ordinateur quantique : tout comprendre en partant de zéro, de Vincent Rollet, Institut Pandore, 2016.

Ordinateur : les promesses de l'aube quantique de Julien Bourdet, CNRS, 2019.

Introduction to Quantum computing, une thèse de Suau Adrien, 2018 (64 pages).

Vidéos

La conférence Introduction à la physique quantique de l'astrophysicien **Roland Lehoucq** donnée à l'Ecole Polytechnique en juin 2018 (1h16). Il est aussi l'auteur du très intéressant Faire des sciences avec Star Wars en 2015 (83 pages).

Les cours de Berkeley de 2013 : Quantum Mechanics and Quantum Computation sur YouTube.

Les vidéos du cours d'informatique quantique de Stanford.

Le workshop sur l'informatique quantique du CERN en novembre 2018 : https://indico.cern.ch/event/719844/timetable/ avec les supports de présentation et vidéos.

Trois conférences d'**Etienne Klein** du CEA sur la physique quantique à la Cité des Sciences de Paris, datant de 2007 et qui sont remarquables de pédagogie (cours 1, cours 2, cours 3) et durent en tout près de cinq heures ainsi que Comprenons nous vraiment la mécanique quantique de Franck Laloe (45 pages) et qui semble dater d'il y a au moins une quinzaine d'années au vu de sa bibliographie mais qui met au clair de nombreux débats scientifiques au sujet de la physique quantique.

Sites web

Toutestquantique, un site français de vulgarisation sur la physique quantique.

Quantum – the open journal for quantum science, un site d'actualités scientifiques sur la mécanique quantique.

Quantiki, un site d'information sur l'informatique quantique.

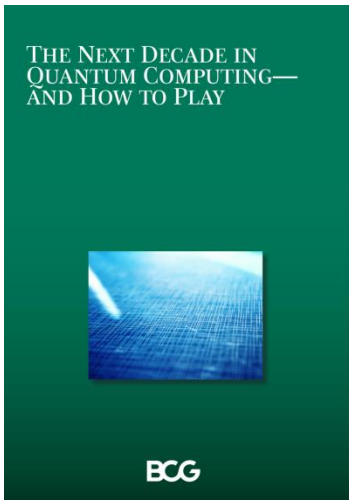
Quantum Info qui liste notamment l'agenda des événements mondiaux sur le quantique.

Qosf : site qui inventorie des guides et formations pour les développeurs d'applications quantiques.

Rapports

Les notes de l'OPECST sur le quantique : Les technologies quantiques : introduction et enjeux, mars 2019 (7 pages), Technologies quantiques : l'ordinateur quantique, juillet 2019 (6 pages) et Technologies quantiques : la programmation quantique, juillet 2019 (5 pages).

The Next Decade in Quantum Computing and How to Play, de Philipp Gerbert et Frank Ruess, BCG, novembre 2018 (30 pages) fait un panorama bien documenté de l'état de l'art de l'informatique quantique et positionne clairement les différents acteurs du marché.



Mon grand Mécano quantique de Julien Bobroff (158 pages, 2019), un ouvrage de vulgarisation de la mécanique quantique et l'interview associée La mécanique quantique pour les nuls.

Glossaire

A quoi sert un glossaire ? Il permet de s'y retrouver dans une terminologie nouvelle et de revenir sur certains concepts pas évidents. Pour l'auteur, c'est un bon checkpoint de compréhension et de capacité à vulgariser des concepts scientifiques et technologiques pas évidents. Mais détrompez-vous, je suis très loin d'avoir tout compris !

Adiabatique : méthode de calcul quantique utilisée notamment dans les ordinateurs à recuit quantique de D-Wave. On détermine d'abord un hamiltonien complexe dont l'état fondamental décrit une solution du problème étudié. On prépare ensuite un système possédant un hamiltonien plus simple, que l'on initialise dans son état fondamental. On fait alors évoluer adiabatiquement cet hamiltonien vers le hamiltonien complexe qu'on a déterminé ; d'après le théorème adiabatique, le système reste dans l'état fondamental, et son état final décrit une solution du problème envisagé.

Algèbre linéaire : branche des mathématiques qui est utilisée dans le calcul quantique. Elle s'appuie sur la manipulation de vecteurs et de matrices. En particulier, l'état d'un qubit est représenté par un vecteur dans un espace à trois dimensions et dont la norme est égale à 1. Les opérations sur un qubit consistent à faire tourner ce vecteur dans la sphère de Bloch qui le représente. Ces rotations correspondent à des opérations d'algèbre linéaire sur le vecteur à deux dimensions qui représente l'état du vecteur. Ce sont des multiplications des vecteurs d'états par des matrices symétriques.

Algorithme : méthode de résolution de problème qui est faite d'une suite finie d'opérations ou d'instructions. Le mot vient du nom du mathématicien perse du IX^{e} siècle, Al-Khwârizmî.

Algorithme quantique hybride : algorithme qui associe des traitements classiques dans des ordinateurs traditionnels et des traitements réalisés sur ordinateurs quantiques, là où ils sont nécessaires.

Anyons : type de particule élémentaire que l'on trouve dans les systèmes de deux dimensions. C'est une généralisation du concept de bosons et de fermions. Les anyons ont des comportements statistiques intermédiaires entre les deux types de particules élémentaires. Ce sont en fait des particules virtuelles qui vivent en deux dimensions spatiales et sont généralement à base d'électrons ou de manques d'électrons se déplaçant dans des structures 2D métalliques supraconductrices. Les anyons sont un type particulier de quasi-particules. Le tout est utilisé dans les ordinateurs quantiques topologiques et le serait en particulier dans les ordinateurs à base des hypothétiques fermions de Majorana étudiés chez Microsoft.

Atomes : le plus petit élément constitutif de la matière et qui manifeste des propriétés chimiques. Il comprend un noyau, avec un ou des protons chargés positivement et un ou des neutrons de charge neutre, autour duquel gravitent des électrons chargés négativement. Dans un atome neutre, le nombre d'électrons est égal au nombre de protons. Autrement, l'atome est chargé négativement ou positivement, et forme un ion. Le nombre de protons détermine la nature de l'atome dans le tableau périodique des éléments de Mendeleïev. Un atome avec un proton est de l'hydrogène, avec deux protons, c'est de l'hélium, etc. L'uranium a 92 protons. Le noyau représente l'essentiel de la masse de l'atome. Les isotopes d'un élément correspondent à des variations du nombre de neutrons dans un atome. En général, le nombre de neutrons d'un élément est équivalent à celui des protons. Les électrons sont répartis par couches dont le nombre dépend du nombre atomique. Elles sont numérotées de 1 à 7. Chaque couche peut contenir au maximum $2*n^2$ électrons, n étant le numéro de la couche (donc 2, 8, 18, 32, 50, 72 et 98). Ce modèle a été élaboré par Niels Bohr entre 1909 et 1913. Les propriétés chimiques de l'élément dépendent du nombre d'électron de la dernière couche que l'on appelle la couche de valence. Si ce nombre est $2*n^2$, l'atome sera inerte et ne se combinera pas chimiquement avec d'autres atomes. Le carbonne a trois couches d'électrons, la dernière en ayant 4 ce qui lui permet de se combiner à d'autres atomes comme l'hydrogène (1 couche, 1 électron) ou l'oxygène (6 électrons en dernière couche).

Atomes froids : atomes refroidis à très basse température, en général avec des techniques utilisant des lasers et l'effet Doppler. Ils sont utilisés dans certains types d'ordinateurs quantiques dits… à atomes froids. Les atomes utilisés sont des atomes neutres (pas ionisés) et assez souvent, le rubidium, un métal alcalin.

Avantage quantique : intervient lorsqu'un ordinateur quantique exécute un traitement plus rapidement que son équivalent optimum adapté à un supercalculateur.

Baryon : classe des particules élémentaires de premier niveau des noyaux des atomes. Elle contient les protons et les neutrons.

Base computationnelle : dénomination des états de base des qubits qui sont mesurables par projection d'états. Cela correspond aux 0 et 1 des qubits, ou avec plus de valeurs possibles pour des qutrits (3) et qudits (au-delà de 3).

Bell (inégalités) : le théorème de Bell de 1964 prouve qu'aucune théorie de variable cachée - imaginée par Einstein en 1935 - ne peut reproduire les phénomènes de la mécanique quantique. Les inégalités de Bell sont les relations que doivent respecter les mesures sur des états intriqués quantiques dans l'hypothèse d'une théorie déterministe locale à variables cachées. L'expérience démontre que les inégalités de Bell sont systématiquement violées, forçant à renoncer à une des trois hypothèses suivantes sur lesquelles sont fondées les inégalités de Bell. La première est le principe de localité selon lequel deux objets distants ne peuvent avoir une influence ins-

tantanée l'un sur l'autre, ce qui revient à dire qu'un signal ne peut se propager à une vitesse plus grande que celle de la lumière dans le vide. La seconde est la causalité selon laquelle l'état des particules quantique est déterminé uniquement par leur expérience, c'est-à-dire leur état initial et l'ensemble des influences reçues dans le passé. La troisième est le réalisme qui signifie que les particules individuelles sont des entités qui possèdent des propriétés propres, véhiculées avec elles (source).

Blind Quantum Computing : technique de répartition des traitements quantiques dans des processeurs quantiques à distance et sécurisant la confidentialité des traitements.

Bloch (sphère) : modèle géométrique de représentation de l'état d'un qubit avec un vecteur dans une sphère de rayon 1. L'état au repos du qubits est un vecteur 0 dirigé vers le haut et l'état exicté est un vecteur 1 dirigé vers le bas. Un vecteur d'état intermédiaire est défini par son amplitude et sa phase, en ligne avec la dualité onde-particule des qubits.

Born (règle) : modèle qui décrit la relation entre la probabilité des états quantiques d'un quantum. La somme de la probabilité de chaque état au carré égale 1 sachant que chaque probabilité se décrit avec un nombre complexe traduisant l'amplitude et la phase de chaque état possible du quantum. On retrouve ce modèle dans la représentation géométrique de la sphère de Bloch.

Boson : particules au comportement grégaire, qui peuvent s'accumuler en nombre arbitrairement grand et dans le même état. On y trouve les photons et les objets composites de spin entier comme les atomes d'hydrogène, de lithium-7, de rubidium-87, de carbonne, de silicium dans des structures cristallines (source : Jean Dalibard). Ces particules échappent au principe d'exclusion de Pauli. Elles ont une fonction d'onde symétrique.

Boson (simulation) : résolution d'un problème de physique quantique avec du calcul quantique ou un simulateur quantique analogique.

Bose-Einstein (condensat) : état de la matière de gaz de bosons à très faible densité refroidi à une température voisine du zero absolu (-273,15°C) lors duquel une grande partie des bosons sont dans l'état énergétique quantique le plus bas possible et manifestent des propriétés particulières comme des interférences. Un cas particulier est celui de l'hélium superfluide, découvert en 1938, et qui, à très basse température, n'a plus de viscosité, à savoir qu'il peut se déplacer sans dissiper d'énergie. Ces condensats ont été imaginés et théorisés le chercheur indien Satyendra Nath Bose puis Albert Einstein en 1924 et leur existence démontrée par l'expérience en 1995 par Wolfgang Ketterle, Eric Cornell et Carl Wieman qui obtinrent pour cela le prix Nobel de physique en 2001. Dans l'informatique quantique, ce domaine a un lien avec le champ des qubits à base d'atomes froids et supraconducteurs.

BQP (classe de problème) : classe de complexité des problèmes qui peuvent être traités par des algorithmes quantiques. Signifie « bounded-error quantum polynomial time ». C'est la classe des problèmes qui peuvent être résolus en temps polynomial par rapport à la taille du problème avec une probabilité d'obtenir une erreur ne dépassant pas le tier des résultats. Cette classe est comprise entre la classe P (problèmes qui peuvent être résolus en temps polynomial sur machine classique) et NP (problèmes dont on peut vérifier une solution en temps polynomial sur une machine classique).

Bra-ket (notation) : modèle de notation décrivant l'état d'un quantum et d'un qubit sous la forme $\langle\phi|\psi\rangle$. Elle a été crée par Paul Dirac en 1939. La partie droite est le vecteur complexe en colonne qui décrit l'état quantique. La partie gauche est un vecteur ligne qui est la transposée de la partie droite.

Chromodynamique quantique : décrit l'interaction forte, l'une des quatre forces fondamentales, qui régit les interactions entre les quarks et les gluons et la cohésion des noyaux des atomes. Pourquoi « chromo » ? Parce que l'on décrit les états des particules élémentaires avec des codes de couleur : bleue, verte et rouge pour les particules puis antibleue, antiverte et antirouge pour les antiparticules. Cette théorie s'apuie sur la théorie quantique des champs. Cette partie de la physique quantique n'est pas utilisé dans le cadre de la création de qubits. Elle l'est pour la physique des particules élémentaires et est vérifiée dans les grands accélérateurs de particules comme le LHC du CERN à Genève.

Clé privée : clé utilisée dans les systèmes de chiffrement à clé privée. Les clés sont échangées au préalable par les parties avec un algorithme de chiffrement, souvent des hash ou des algorithmes Diffie-Helfmann.

Clé publique : système de chiffrement qui passe par l'envoi d'une clé publique à un interlocuteur qui va l'utiliser pour chiffrer un message envoyé dans l'autre sens. Les éléments ayant permis de créer cette clé publique sont utilisés pour le déchiffrement du message envoyé. Il est normalement impossible ou très difficile de décomposer la clé publique pour retrouver les éléments qui ont permis de la créer.

Clifford (groupe) : groupe de portes quantiques unitaires qui sont simulables facilement et en temps polynomial sur ordinateurs classiques selon le théorème de Gottesman-Knill. Une porte de Clifford est une porte quantique qui peut être décomposée en portes du groupe de Clifford. Il suffit d'avoir une porte unitaire réalisant une rotation sur l'axe X et une autre sur l'axe Z pour créer un jeu de portes de Clifford complet. Elles doivent être complétées d'au moins une porte à deux qubits comme une CNOT pour créer un jeu de portes universelles. Ces portes unitaires réalisent des quarts de tours ou des demi-tours dans la sphère de Bloch.

Cluster state : base de départ d'un calcul MBQC (Measurement Based Quantum Computing) avec une grille de qubits intriqués.

CMOS : technique de fabrication courante de semiconducteurs utilisée pour produire des processeurs et de la mémoire, et qui est réutilisée pour créer des qubits manipulant des spins d'électrons.

Codes de correction d'erreurs : décrit à la fois les méthodes logiques et architectures physiques permettant de contourner les erreurs générées par le bruit dans le calcul quantique universal et une variante de cryptographie post-quantique.

Cognition quantique : modèle descriptif du fonctionnement de la connaissance humaine (langage, prise de décision, mémoire, conceptualisation, jugement, perception) qui s'appuie sur le formalisme mathématique de la mécanique quantique, en procédant principalement par analogie, sans passer par des explications physiques ou de quantification des neuro-sciences, qui eux relèvent du champ « quantum mind » issu des travaux de Roger Penrose. Voir la fiche Wikipedia associée. Il n'y a pas de startups dans cette catégorie !

Cohérence : état permettant la superposition d'états dans un quantum. Cette cohérence se termine au bout d'un certain temps pour les qubits (le temps de cohérence) et lors de la mesure de l'état d'un qubit.

Complexité (théorie) : branche de l'informatique théorique et des mathématiques qui joue un rôle important dans le calcul quantique pour évaluer sa performance par rapport au calcul traditionnel sur machine de Turing/Neumann. Elle définit des classes de problèmes par niveau de complexité, en terme de temps de calcul voire d'espace mémoire nécessaire, avec, notamment, des problèmes qui sont résolus en temps polynomial par rapport à leur complexité (classe P) et dont les résultats sont vérifiables en temps polynomial (classe NP). Les méthodes de résolutions de ces problèmes relèvent le plus souvent de la force brute consistant à naviguer dans un espace de plus en plus grand de combinatoires à évaluer en fonction de la taille du problème à résoudre.

Continous variables quantum computing (CV) : type d'ordinateur quantique qui utilise des qubits dont la valeur est continue et non binaire. Utilisée dans deux types d'ordinateurs quantiques : les simulateurs quantiques analogiques (notamment à base d'atomes froids) et les ordinateurs à recuit quantiques de D-Wave.

Corps noir : corps qui est en équilibre thermique avec le rayonnement qu'il émet. Cela peut être l'intérieur d'un four où une étoile. C'est en étudiant le rayonnement du corps noir et sa fréquence en fonction de la température du corps que Planck a découvert l'existance des quanta en 1900.

Courbes elliptiques : type de cryptographie à clés publiques qui est potentiellement cassée par les algorithmes quantiques. Elliptic-curve cryptography (ECC) en anglais. L'un de ses avantages est de nécessiter des clés de petite taille, environ trois fois plus petites en nombre de bits que les clés publiques RSA.

Cryogénie : technique de refroidissement. La cryogénie à très basse température est utilisée dans une bonne partie des ordinateurs quantiques, tous ceux qui sont à base d'électrons ou d'atomes froids. Les températures requises pour stabiliser des qubits et réduire leur taux d'erreur sont très proches du zéro absolu : entre 5 et 20 mK. Les systtèmes les plus utilisés sont des réfrigérateurs à dillution qui exploitent de l'hélium 3 et de l'hélium 4. La cryogénie est aussi utilisée pour les systèmes de lecture de qubits à base de photons.

Décohérence : marque la fin de la cohérence d'un qubit. On utilice souvent indifféremment l'expression temps de cohérence (temps pendant lequel les qubits sont en état de superposition) ou de décohérence (temps au bout duquel cette superposition se termine), ce qui revienta au même.

Deutsch-Jozsa (algorithme) : algorithme quantique crée en 1992 par David Deutsch et Richard Jozsa servant à vérifier si une fonction donnée est équilibrée ou non, à savoir, si elle renvoie toujours 0 ou 1, ou des 0 et 1 à proportion égale. L'alternative entre l'équilibre (autant de 0 que de 1) ou non (que des 0 ou des 1 en sortie) est le postulat de départ. Le gain de performance par rapport à des algorithmes classiques est exponentiel. Dans le cas de N qubits, il faudrait évaluer la fonction sur au moins la moitié des valeurs d'entrée possible, soit 2 puissance N-1 +1. Malheureusement, cet algorithme ne sert pas à grand-chose.

Distillation : technique utilisée dans la gestion de codes de correction d'erreurs à base de magic states. Elle consiste à comhiner plusieurs qubits de type magic state pour en alimenter d'autres avec un taux d'erreur plus faible.

Doppler (effet) : décalage du spectre électromagnétique sous l'effet de la vitesse d'éloignement ou de rapprochement de la source par rapport à l'observateur. Si la source s'éloigne de l'observateur, la lumière est décalée vers le rouge (redshift), dans le cas contraire, vers le bleu. Cet effet est notamment utilisé dans la technique de refroidissement des atomes par laser dans les températures cryogéniques. Il consiste à éclairer des atomes qui sont en mouvement du fait de la température avec une fréquence qui juste en-dessous du niveau d'aborbtion des atomes en question. Ceux qui se déplacent vers la lumière vont absorber le photon ce qui réduira leur énergie cinétique. Ceux qui se déplacent dans l'autre direction ne les absorberont pas car la fréquence apparente du photon sera trop faible pour changer l'état énergétique des atomes. Cette technique permet de refroidir des atomes jusqu'à en-dessous du mK (milli-Kelvin).

Dualité onde particule : propriété de particules élémentaires ayant une masse comme les électrons, les neutrons ou les atomes de se comporter à la fois comme des particules avec une masse et des ondes pouvant générer des interférences. On le vérifie avec la fameuse expérience des fentes de Young qui mettent en évidence ces interférences.

D-Wave : société canadienne concevant des ordinateurs quantiques à recuit quantique. Ils n'ont pas la même puissance que les ordinateurs quantiques à portes universelles à nombre égal de portes. Mais ces derniers sont actuelement situés entre 50 et 100 portes tandis que la génération actuelle des D-Wave comprend 2048 qubits.

Ecrasement de la fonction d'onde de Schrödinger : petit nom donné à la fin de la cohérence d'un qubit (état superposé) qui est notamment généré par la mesure de son état qui le rabat à l'une de ses valeurs de base (0 ou 1). Cet écrasement peut aussi intervenir au terme de la

durée de cohérence. Celui-ci est provoqué par l'interaction avec le qubit et sont environnement.

Effet tunnel : propriété d'un objet quantique de franchir une barrière de potentiel (ou d'énergie) même si son énergie est inférieure à l'énergie minimale requise pour franchir cette barrière. Cet effet est utilisé dans les ordinateurs recuit quantique de D-Wave pour déterminer rapidement un minimum énergétique d'un système complexe (« hamiltonien »).

Eigenstate : voilà un concept quantique que les physiciens ont bien du mal à vulgariser de manière non récursive. L'explication en anglais est « *quantum state whose wave function is an eigenfunction of the linear operator that corresponds with an observable*." Ce qui nous fait une belle jambe puisque cela oblige à comprendre la définition de quatre autres notions. En vaguement clair, cela correspond à l'utilisation de repères orthonormés de décription de l'état d'un quantum.

Electron : particule élémentaire que l'on trouve notamment dans les atomes, en orbite autour du noyau. D'après le modèle de Bohr élaboré en 1913, il existe un nombre fini d'orbites d'électrons autour du noyau des atomes. Le déplacement des électrons d'une orbite à l'autre correspond à l'absorbsion ou l'émission d'un photon. Les électrons sont souvent utilisés dans les qubits, notamment sous forme d'électrons piégés dans des semi-conducteurs et dont on contrôle le spin. L'électron est « élémentaire » car il n'est pas composé de sous-particules, contrairement aux neutrons et aux protons qui sont composés de quarks.

Equations linéaires : opérations mathématiques relevant de l'algèbre linéaire. Dans le cas du calcul quantique, il s'agit de multiplications de matrices de nombres complexes.

Erreurs : gros sujet de préoccupation dans le fonctionnement des ordinateurs quantiques. Les opérations sur les qubits : portes à un ou plusieurs qubits puis mesure de leur état génère des erreurs qu'il faut chercher à minimiser. Les taux d'erreurs sont en 2019 compris entre 0,4% et 4% pour les portes quantiques. Lorsque l'on enchaine plusieurs portes quantiques, les taux de résultats corrects (1-% d'erreur) se multiplient au point de tout fausser. On évite cela soit en réduisant le taux d'erreurs, soit en utilisant des algorithmes de faible profondeur (faible nombre de portes) soit avec des systèmes de code de correction d'erreurs.

Fermions : particules au comportement individualiste. Deux particules de ce type ne peuvent pas être dans le même état au même endroit. Cela comprend les électrons, les quarks, les objets composites de spin demi-entier. Par exemple les atomes de deutérium, de lithium-6, de potassium-40 (source : Jean Dalibard). Par opposition, les bosons de spin entier comme les photons et certains atomes peuvent s'accumuler dans le même état.

Fermion de Majorana : quasi-particule à base d'électrons dans des matériaux supraconducteurs qui pourrait servir à gérer des qubits fiables dans le cadre de ce que l'on appelle le calcul topologique. Cette particule virtuelle a été imaginée par Ettore Majorana en 1937. C'est sur elle que Microsoft compter créer un ordinateur quantique sachant que l'existence de la quasi-particule n'a pas été véritablement démontrée.

Flying qubits : qubits pouvant se déplacer, à contrario des stationary qubits qui ne bougent pas. Ce sont en général des photons.

Friedkin (porte) : porte quantique qui opère sur trois qubits. Elle intervertit l'état du second et du troisième qubit si le premier qubits est à la valeur 1. Aussi dénommée porte CSWAP (conditionnal SWAP).

FTQC : Fault-Tolerant Quantum Computer.

GHZ : veut dire autre chose que giga Hertz en informatique quantique ! Il s'agit d'un état superposé Greenberger-Horne-Zeilinger qui permet de démontrer l'inexistence de variables cachées dans l'intrication quantique d'au moins trois particules et avec un nombre fini de mesures. La notion date de 1989 et sa validation expérimentale de 1999.

Grover (algorithme) : algorithme quantique de recherche d'un élément dans un tableau non indexé.

Hadamard (porte) : porte permettant de générer un état superposé entre 0 et 1 dans un qubit.

Hamiltonien : équations servant à décrire l'énergie totale et potentielle d'un système de particules élémentaires. L'équation de Schrödinger décrit l'évolution dans le temps d'un hamiltonien d'une particule élémentaire. Ce concept est notamment utilisé dans les ordinateurs à recuit quantique de D-Wave. « Préparer un Hamiltonien » dans ce genre d'ordinateur revient à mettre en place une matrice de qubits reliés entre eux par des potentiels et qui va rechercher un minimum énergétique aboutissant à un hamiltonien équilibré correspondant à la solution du problème à résoudre. C'est l'explication la plus simple que j'ai trouvée à ce concept qui nécessite sinon de solides bases mathématiques.

Hélium 3 : isotope rare de l'hélium qui est utilisé dans les systèmes cryogénie d'ordinateurs quantiques pour générer des températures inférieures à 1K. Il est généralement produit à partir de tritium dans des centrales nucléaires spécialisées, notamment celle de Savannah River du Département de l'Energie aux USA.

Heisenberg (principe d'indétermination) : principe fondamental de la mécanique quantique qui postule qu'il existe une limite inférieure à la précision avec laquelle on peut connaître deux paramètres indépendants relatif à un même objet comme sa vitesse et sa position ou l'énergie émise et la durée d'émission.

Hélium 4 : isotope commun de l'hélium qui est également utilisé dans les systèmes de cryogénie. Il est aussi superfluide à très basse température (moins de 2K).

Hilbert (espace) : espace vectoriel de nombres réels ou complexes muni d'un produit scalaire euclidien ou hermitien, qui sert à mesurer des distances et des angles et de définir une orthogonalité. C'est une extension à n dimensions du concept d'espace euclidien à trois dimensions. En mécanique quantique, l'état d'un quantum est représenté par un vecteur dans un espace de Hilbert à autant de dimensions que le nombre d'états de base (ou obser-

vables) de ce quantum. Il s'agit d'espaces géométriques qui servent notamment à mesurer des longueurs et des angles, de faire des projections sur des dimensions et de définir l'orthogonalité entre vecteurs.

HPQC : High Performance Quantum Computing, analogue quantique du HPC (High Performance Computing). Il s'agit pour l'instant de modèles théoriques de mainframes quantiques comprenant des matrices géantes de qubits pouvant être partitionnées pour un usage partagé par plusieurs utilisateurs. Voir High Performance Quantum Computing, 2011 (7 pages).

Intrication : liaison entre deux quantums qui sont reliés entre eux de telle sorte qu'une modification de l'un entraîne celle de l'autre. Ce processus est utilisé pour relier des qubits entre eux par des portes quantiques à deux ou trois qubits dans les ordinateurs quantiques. Il l'est également dans les systèmes de cryptographie et de télécommunications quantiques à base de photons intriqués, exploités dans les QKD.

Ion : atome non neutre, qui a une charge électrique positive ou négative. Elle est négative si son nombre d'électrons dépasse celui des protons (anions) et positive dans le cas contraire (cations).

Ion piégé : ce sont des ions utilisés dans certains types d'ordinateurs quantiques. Ils sont généralement piégés magnétiquement et on contrôle leur état avec des lasers.

IonQ : startup américaine issue de l'Université de Maryland et à l'origine des premiers ordinateurs quantiques commerciaux à ions piégés. Leur record annoncé fin 2019 était de 79 ions piégés.

Ising (modèle) : problème de physique statistique qui peut être simulé et résolu à l'aide d'algorithmes quantiques, en particulier sur ordinateurs à recuit quantique. Il modélise les interactions entre particules à deux états.

Josephson (effet) : effet supraconducteur utilisé dans les qubits de d'ordinateurs quantiques dits à supraconducteurs comme ceux d'IBM et Google.

Ket : vecteur à deux dimensions en nombres complexes qui définit l'état d'un qubit.

Laser : source de lumière cohérente inventée en 1960 et utilisée dans de nombreux domaines comme les lecteurs de CD et DVD, les communications par fibre optique, en chirurgie, ophtalomologie et odontologie. On les retrouve aussi souvent dans l'informatique quantique pour contrôler des atomes froids ou gérer des qubits à base de photons ainsi que dans la cryptographie quantique (QKD & co). Laser signifie Light Amplification by Stimulated Emission of Radiation ». C'est une source de lumière cohérente, à savoir qu'elle est constituée de photons de même polarisation, phase et longueur d'onde, qui sont émis dans une même direction. L'amplification utilise un processus d'émission stimulée dans un milieu actif amplificateur fait de solide, fibre, liquide, gaz ou semiconducteur qui est placé au au centre d'une cavité optique résonnante avec d'un côté, un miroir réfléchissant et de l'autre un miroir semi-réfléchissant qui permet de faire sortir le faisceau lumineux. La fréquence et la puissance du rayonnement lumineux dépendent de nombreux paramètres. L'énergie provient d'un système d'excitation ou de pompage : laser primaire, diode laser, lampe flash ou décharge électrique.

Localité (principe) : principe selon lequel des objets distants ne peuvent avoir une influence directe l'un sur l'autre. Un objet ne peut être influencé que par son environnement immédiat. Ce principe issu de la relativité restreinte d'Albert Einstein est remis en question par la mécanique quantique, la non localité et l'intrication quantique observées expérimentalement depuis au moins 1982 avec des photons, dans le cadre de la fameuse expérience d'Alain Aspect (avec Philippe Grangier et Jean Dalibard).

Log discret (problème) : problème mathématique consistant à trouver un log entier d'un nombre. Est utilisé dans la résolution de problèmes de cryptographie à l'aide d'algorithmes quantiques. L'algorithme de Shor permet de résoudre les problèmes de logarithmes discrets.

Magic states : qubits utilisés dans une méthode de gestion de codes de correction d'erreurs dénommée magic states distillation. Difficile d'en dire plus tellement c'est compliqué !

Matrice : objet mathématique fait de lignes et de colonnes de valeurs.

Matrice densité : objet mathématique en forme de matrice servant à décrire l'état statistique d'un système physique qui est plus précis que le vecteur que l'on utilise en calcul quantique et qui représente une position dans la sphère de Bloch. Cet objet décrit précisément la probabilité de trouver le quantum dans tel état intermédiaire associant par exemple l'amplitude et la phase. Dans le détail, les mathématiques associées à ces matrices sont des plus complexes et je fais l'impasse dessus. L'usage des matrices densité est utile pour gérer des états mixtes (mixed states) de quantum versus les états purs (pure states) qui se satisfont des représentations d'états sous forme de vecteurs.

MBQC ou MQCM : Measurement Based Quantum Computing, méthode de calcul quantique inventée en 2001 par Robert Raussendorf et Hans Briegel qui utilise un nombre élevé de qubits intriqués dans des grilles à deux dimensions et dans lequelles des lectures d'état de qubits sont réalisées pour modifier la structure de la grille. Ces mesures servent aussi à guider l'algorithme.

Médecine quantique : en général, fausse science et charlatanerie qui s'appuie sur une interprétation totalement fantaisiste de la mécanique quantique.

Mélasse optique : gaz d'atomes neutres froids dont la force de cohésion est de type visqueux.

MINLP : Mixed Integer Non Linear programming, classe de problems complexes qui peuvent être potentiellement résolus avec des algorithmes quantiques. Il s'agit de trouver le ou les minimums de fonctions non linéaires et sous contraintes qui visent à respecter des fonctions non linéaires. Les variables de l'équation sont une combinaison de nombres entiers et de nombres flottants. Les applications sont nombreuses dans tous les cas où l'on cherche à optimiser une fonction sous contraintes (distribution d'énergie, décollage optimum d'un avion, optimisation de

portefeuille financier, minimiser le risque dans une assurance ou dans le crédit, etc).

Mixed state : état de quantums qui représentent l'association statistique de deux états purs. Ce genre d'état qui s'oppose à un état pur (pure state) qui est représenté par un vecteur complexe à deux dimensions. Un état mixte est représenté par une matrice densité.

NISQ : Noisy Intermediate-Scale Quantum, dénomination des calculateurs quantiques actuels et à venir dans un futur proche, qui sont de taille intermédiaire en nombre de qubits (quelques dizaines à centaines) et sujets à un bruit quantique qui en limite les capacités. Cette appellation a été créée par le chercheur américain John Preskill.

Noms de chercheurs : les conventions de nommage des chercheurs dans les publications scientifiques donnent du fil à retordre à nombre d'observateurs dont je fais partie. Ils ne comprennent que les initiales de prénoms, créant parfois de situations ubuesques avec des homonymes dans ces conditions (exemple). Visiblement, ce système antédilluvien semble difficile à réformer. Seule explication valable : le besoin de recourcir la liste interminable de contributeurs des articles. Mais aussi, de nombreuses variations culturelles dans la manière de dénommer une personne. Lorsque je cite ces articles, j'utilise la convention « & Al » en ne citant que le premier auteur ou celui ou celle qui est connu(e) pour être le principal contributeur. Et j'enlève le middle name des scientifiques américains au passage ! « Et al » est la compression du latin et alii ou et aliae qui veut dire « et tous les autres ».

Nombre complexe : ensemble des nombres complexes créé comme extension de l'ensemble des nombres réels, contenant en particulier un nombre imaginaire noté i tel que $i^2 = -1$. Tout nombre complexe peut s'écrire sous la forme a + i b où a et b sont des nombres réels. Ces nombres servent notamment à décrire l'état d'un qubit.

Non localité : principe permettant à un objet (quantique) d'influencer l'état d'un autre objet (quantique) à distance, celle-ci pouvant être très grande. Contredit le principe de localité qui veut d'un objet ne puisse influencer qu'un autre objet qu'à proximité. L'intrication quantique de photons à de grandes distances vérifie la non localité.

Non clonage (théorème) : interdit la copie à l'identique de l'état d'un quantum. Il a comme conséquence qu'il est impossible de copier l'état d'un qubits pour l'exploiter indépendamment de son original. Toute copie détruit l'original. !

Notation de Dirac : voir bra-ket.

NP (classe de problème) : classe de problèmes dont la solution est vérifiable dans un tems polynomial relativement à la taille du problème. Comprend notamment les problèmes dits exponentiels ou intractables, dont le temps de la résolution est exponentiel par rapport à leur taille. Un ordinateur quantique permet de résoudre une partie des problèmes NP.

NP-complet (classe de problème) : problème de décision dont il est possible de vérifier une solution en temps polynomial et pour qui tous les problèmes de la classe NP se ramènent à celui-ci via une réduction polynomiale. Cela signifie que le problème est au moins aussi difficile que tous les autres problèmes de la classe NP. Les problèmes du voyageur de commerce et du remplissage du sac à dos sont des problèmes NP Complet. Le concept date de 1971 et provient de Stephen Cook.

NP-difficile (classe de problème) : problème vers lequel on peut ramener tout problème de la classe NP par une réduction polynomiale. S'il est également dans la classe NP, on dit que c'est un problème NP-complet. Si $P \neq NP$, alors, les problèmes NP-difficile ne peuvent pas être résolus en temps polynomial.

Observable : équivalent en mécanique quantique d'une grandeur physique en mécanique classique, comme la position, la quantité de mouvement, le spin ou l'énergie. Pour un qubit d'ordinateur quantique, un observable est l'un des deux états de base, au repos ou excité (0 ou 1) du qubit.

Opération unitaire : opération sur un vecteur qui préserve sa longueur. Dans le cas des qubits dont le vecteur a toujours une longueur de 1, les portes quantiques unitaires appliquent dessus une transformation qui préserve cette longueur. Dans la représentation des qubits dans la sphère de Bloch, l'opération fait tourner le vecteur représentant l'état du qubit dans cette sphère.

Optique linéaire : champ de la mécanique quantique qui manipule des photons. On y retrouve les ordinateurs quantiques qui s'appuient sur la manipulation de photons. Les qubits sont les états de photons comme leur polarisation, leur fréquence ou leur phase. L'optique linéaire est aussi exploitée dans la cryptographie quantique (QKD).

P (classe de problème) : problème qui peut être résolu en temps polynomial par rapport à sa taille, sur une machine de Turing déterministe.

Paire de Cooper : paires d'électrons qui se combinent pour faire circuler le courant électrique dans les matériaux supraconducteurs, en général à très basse température, et sans opposer de résistance. Les paires de Cooper on un spin entier car elles cumulent deux électrons ayant un spin de ½.

Pauli (príncipe d'exclusion) : postule que deux particules de type fermion ne peuvent se trouver dans le même état quantique. Deux électrons ou deux neutrons ne peuvent se trouver au même endroit avec le même niveau d'énergie. Si une force extérieure comme la gravitation les oblige à se trouver au même endroit, ils ne pourront pas avoir la même énergie c'est-à-dire la même vitesse. Si un ensemble de fermions doit se trouver dans un même lieu, ils vont devoir adopter des vitesses toutes différentes.

Phase : situation instantanée d'une grandeur qui varie cycliquement, en physique et en mécanique des ondes. On parle surtout de déphasage d'une onde par rapport à une onde de référence. Le déphasage entre deux ondes s'exprime comme un angle (en radians, degrés ou tours, en considérant un tour comme une période), comme un temps (à comparer avec la période de l'onde) ou comme une distance (à comparer avec la longueur d'onde).

Phase Estimation Algorithm (PEA) : un des premiers algorithmes de simulation de la structure électronique de molecules sur ordinateur quantique. Mais il requiert des temps de cohérence assez longs que les ordinateurs quantiques à porte universelle ne sont pas encore en mesure de fournir. L'algorithme est « concurrencé » par le Variational Quantum Eigensolver (VQE), un algorithme hybride qui fonctionne avec un nombre de portes quantiques plus faible.

Phonon : ondulations d'atomes dans des phénomènes nanoscopiques. Ils se manifestent notamment dans la supraconductivité en suivant et accompagnant le mouvement des électrons arrangés en paires de Cooper.

Photon : quantum d'énergie associé aux ondes électromagnétiques allant des ondes radio (ondes longues, fréquences peu élevées) jusqu'aux rayons gamma (ondes très courtes, fréquences très élevées) en passant par la lumière visible. Depuis 1926, c'est une particule de lumière élémentaire. Sa masse est nulle. Son spin est 1 est il fait donc à ce titre partie des bosons, à savoir qu'ils peuvent s'accumuler au même endroit dans le même état contrairement aux fermions. Les photons sont notaémment générés lors de changements d'états énergétiques d'atomes et, plus précisément, de niveau d'orbite d'électrons tournant autour des noyaux d'atomes.

Physique de la matière condensée : branche de la physique qui étudie les propriétés macroscopiques de la matière (solides, liquides, verres, polymères) et dans les systèmes où le nombre de constituants est grand et les interactions entre eux sont fortes. Les physiciens de la matière condensée cherchent à comprendre les comportements de ces phases en utilisant les lois de la physique (mécanique quantique, électromagnétisme et physique statistique). Ce champ est historiquement limité aux systèmes qui peuvent être étudiés en laboratoire. En pratique, cette science s'intéresse surtout aux phases supraconductrices à basse températur, aux phases ferromagnétique, antiferromagnétique et ferrimagnétique des spins dans des réseaux cristallins d'atomes, les verres de spins, liquide de spins, ainsi que le condensat de Bose-Einstein. Les physiciens qui travaillent sur les qubits supraconducteurs font partie de cette discipline.

Pompage optique : technique qui sert à modifier les états des atomes en augmentant leur niveau d'énergie à l'aide de photons polarisés. Elle a valu le prix Nobel de physique en 1966 au Français Alfred Kastler. La technique est utilisée dans la photonique et notamment dans les lasers et la métrologie quantique.

Portes quantiques : opérations de manipulations de l'état de qubits. On parle de portes unitaires pour les portes quantiques qui n'agissent que sur un seul qubit à la fois. Il existe aussi des portes à plusieurs qubits (Toffoli, Friedkin, …) qui exploitent le principe de l'intrication quantique. Les opérations de portes quantiques sont générées par des actions physiques sur les qubits qui dépendent de leur nature. Pour les qubits supraconducteurs, il s'agit d'envoi de microondes entre 5 et 10 GHz via des conducteurs électriques. Pour les ions piégés, ce sont des opérations pilotées par des lasers. Pour des qubits CMOS, ce sont des tensions électriques. Pour les qubits reposant sur des particules à masse (électrons, ions, atomes froids), les portes quantiques agissent sur les qubits mais ceux-ci ne bougent pas. Pour des qubits à base de photons, ceux-ci circulent et traversent des portes quantiques qui modifient leur état (phase, fréquence, ou autre).

Portes unitaires : portes quantique qui n'agissent que sur un seul qubit à la fois, comme les portes de Pauli X (inversion d'état), Y et Z ou la porte de Hadamard (H).

Portes quantiques universelles : se dit de jeux de portes quantiques à partir desquelles toutes les autres portes quantiques peuvent être reproduites.

PCQC : Paris Center for Quantum Computing, communauté de chercheurs en informatique quantique de la région parisienne. C'est une fédération de recherche associant le CNRS, l'Université Paris Diderot, l'UMPC, Telecom Paristech, le CEA, l'Institut d'Optique et l'Université Paris-Sud (Orsay/Saclay).

PQC : Post Quantum Cryptography, cryptographie résistante aux algorithmes conçus pour les ordinateurs quantiques. Elle repose sur l'usage de clés publiques qui ne sont pas décomposables avec des ordinateurs classiques ou des ordinateurs quantiques. C'est lié au fait qu'il s'agit d'un problème « NP difficile ».

PQS : Programmable Quantum Simulator, ou ordinateurs quantiques analogiques.

Pure state : se dit d'un état d'un quantum ou d'un qubit qui est défini par un vecteur de norme 1 dans la sphère de Bloch. Par opposition, un mixed state est un état combinant plusieurs états purs de quantum ou qubits. Ils s'additionnent avec des probabilités classiques dont la somme fait 1 (et pas la somme au carré comme pour la superposition d'états). Cet état est bien représenté par une matrice densité et c'est un point qui est à l'intérieur de la sphère de Bloch. En pratique, les qubits utilisés dans le calcul quantique avec des registres quantiques et des portes quantiques restent à l'état pur. Par contre, la mesure de l'état d'un qubit intriqué avec un autre qubit va transformer son état de pur en mixte. Je n'ai pas encore compris si le calcul quantique manipulait des mixed states pendant les calculs et l'application de portes quantiques à des qubits.

QFHE : Quantum Fully Homomorphic Encryption. Méthode de chiffrement quantique de l'information permettant de réaliser des traitements sur des données chiffrées.

QFT : Quantum Fourier Transform. Variation quantique de la transformée de Fourier. La transformée de Fourier classique permet de décomposer un signal (comme en audio) en fréquences (ou spectre de fréquences). La QFT fait cela sur une suite de nombres entiers et détermine sa plus grande fréquence observable.

QIP : Quantum Information Processing, appellation parfois utilisée pour décrire le calcul quantique.

QKD : Quantum Key Distribution, protocole de sécurisation d'envoi de clés symétriques via une liaison optique qui s'appuie sur l'intrication quantique (fibre ou satellite). Ces clés sont inviolables ou tout du moins, une interception de la clé est détectable. Malgré tout, il existe des failles qui se situent aux extrémités de la connexion et

aussi au niveau des répéteurs qu'ils faut utiliser si les liaisons sont longues de plusieurs centaines de km.

QMA : Quentin Merlin Arthur, classe de problèmes qui est vérifiable en temps polynomial sur un ordinateur quantique avec une probabilité supérieure aux 2/3. C'est l'analogue quantique de la classe de complexité "traditionnelle" NP. QML : Quantum Machine Learning. Branche des algorithmes quantique qui sert au machine learning.

QRNG : Quantum Random Number Generator, les générateurs de nombres aléatoires optiques utilisés en cryptographie quantique, comme ceux du Suisse IDF.

Quantum Variational Circuits : type d'algorithme quantique servant à faire du machine learning.

Quasi-particules : phénomène correspondant au comportement de particules élémentaires interagissant avec leur environnement. C'est le cas d'électrons circulant dans des semiconducteurs et dont le movement est perturbé par leur interaction avec les autres électrons et noyaux de la structure. Ils se comportent comme des électrons ayant une masse différente. En pratique, les quasiparticules sont des modèles mathématiques permettant de décrire de manière simplifiée le fonctionnement de particules élémentaires dans des structures solides. On les retrouve dans les anyons et les ordinateurs quantiques topologiques.

Qubit : unité d'information élémentaire de l'informatique quantique dans les ordinateurs quantiques universels. Elle stocke un état quantique associant deux états distincts d'une particule ou système quantique (ion piégé, spin d'électron, phase ou fréquence de photon, …).

Qudit : est une forme générique de qubit qui a d états quantiques possibles au lieu de deux. L'approche est rarement utilisée, en tout cas dans des ordinateurs quantiques hors des laboratoires de recherche.

Qutrit : c'est une forme de qubit qui au lieu d'avoir deux états quantiques possibles, en a trois. C'est un cas particulier des qudits.

Rabi (oscillation) : oscillations entre états d'un système à deux niveaux excité à une fréquence proche de sa résonance. Ce phénomène est observé entre deux états de spin dans la résonance magnétique nucléaire aini que lorsqu'un champ électrique agit sur les transitions d'un état électronique d'un système à un autre pour un atome ou une molécule. La courbe décrivant l'oscillation ressemble à une sinusoïdale qui s'atténue dans le temps. Isidor Isaac Rabi est un physicien américain d'origine hongroise (1898 - 1988) prix Nobel de physique en 1944. On retrouve les oscillations de Rabi un peu partout et notamment dans le fonctionnement des qubits supraconducteurs.

Recuit quantique : procédé de calcul quantique utilisé dans les ordinateurs quantiques de D-Wave. Voir hamiltonien et D-Wave.

Réduction d'état : conséquence de la mesure de l'état d'un quantum ou d'un qubit, qui modifie cet état (superposé) en un état stable (non superposé). Pour un qubit, c'est l'un des deux états de base : excité ou non excité, phase horizontale ou verticale pour un photon, spin haut ou bas pour un électron, état excité pour un ion ou un atome froid, etc.

Registre : ensemble de bits ou de qubits.

Réseaux euclidiens : classe d'algorithmes utilisés dans la cryptographie post-quantique (PQC).

Rigetti : startup US créant des ordinateurs quantiques supraconducteurs.

RSA : système de chiffrement à clés publiques s'appuyant sur la difficulté à factoriser une clé publique constituée à partir de la multiplication de deux nombres premiers de très grande taille. Cette factorisation est possible avec l'algorithme quantique de Peter Shor. Cependant, elle nécessite un très grand nombre de qubits pour casser les clés RSA les plus courantes à 1024 ou 2048 bits. Pour les clés 1024 bits, il faudrait disposer de 168 millions de qubits avec un taux d'erreur de 0,1% que l'on n'obtient pas encore aujourd'hui.

Rydberg (atomes) : état excité d'un atome possédant un ou plusieurs électrons et dont le nombre quantique principal n (indice de la couche d'électrons dans l'atome qui est un entier compris entre 1 et le nombre de couches d'électrons dans l'atome) est très élevé. Ces atomes sont généralement de grande taille, proportionnelle à n^2, et avec des interactions inter-atomiques très fortes. Ces interactions permettent l'intrication de sous-ensembles atomiques voire d'atomes uniques. Ces atomes ont été utilisés par l'équipe de Serge Haroche pour détecter de manière non destructive la présence d'un photon dans une cavité, et ainsi étudier la décohérence quantique. Mais l'hydrogène peut aussi être un atome de Rydberg s'il est excité avec de hauts niveaux d'énergie, faisant passer son électron à une couche quantique de nombre élevé.

SAT : classe de problème de logique ou problème de satisfaisabilité booléenne, de logique d'ordre 0. C'est un problème de décision, qui, étant donné une formule de logique propositionnelle, détermine s'il existe une assignation des variables propositionnelles qui rend la formule vraie. Comme lorsque l'on cherche des variables booléennes x, y et z qui satisfont l'équation $(x \vee y \vee z) \wedge (\bar{x} \vee \bar{y}) \wedge (\bar{x} \vee y \vee z)$, $\wedge$ voulant dire « et », et $\vee$ « ou » et $\bar{x}$ étant la négation de x. Le problème devient très complexe si le nombre N de variable devient très élevé car pour tester leur combinatoire avec la force brute, il faudra tester 2^N combinaisons. Ce problème a été mis en lumière par le théorème de Cook selon lequel le problème SAT est NP-complet. Le problème SAT a aussi de nombreuses applications notamment en satisfaction de contraintes, planification classique, vérification de modèles, diagnostic, jusqu'au configurateur d'un PC ou de son système d'exploitation : on se ramène à des formules propositionnelles et on utilise un solveur SAT (Wikipedia et ici).

Schrödinger (équation, fonction d'onde) : décrit l'évolution dans le temps et l'espace de l'état ondulatoire d'un quantum, à savoir les probabilités de trouver le quantum à un endroit donné et moment donné dans le temps.

Seconde révolution quantique : couvre les avancées dans la mécanique quantique depuis les années 1990, où l'on a commencé à contrôler les propriétés quantiques de quantums individuels, au niveau de photons (polarisation, …), d'électrons (spin) et d'atomes. Elle couvre notamment les usages du quantique en cryptographie et télécommunications.

Shor (algorithme) : algorithme de factorisation quantique de nombres entiers inventé par Peter Shor en 1994. Il permettrait en théorie de casser des clés publiques RSA en les décomposants en nombres premiers.

Silicium 28 : isotope de silicium permettant de créer des wafers de silicium adaptés à la création de qubits en silicium. Le silicium 28 a un spin nul qui n'influe pas sur le spin des électrons piégés servant à gérer les qubits. Il est purifié en Russie et peut être ensuite déposé en couche mince en phase gazeuse sur du silicium classique.

Simulateur quantique : nom donné à deux types d'ordinateurs. D'une part, les super-calculateurs quisont capables d'exécuter par simulation numérique des algorithmes quantiques et d'autre part, des ordinateurs quantiques analogiques (PQS) qui sont capables de simuler la mécanique quantique et de résoudre des problèmes associés, en particulier dans la physique des matériaux.

SIRTEQ : réseau de chercheurs en technologies quantiques, veut dire Science et Ingénierie en Région Ile de France pour les Technologies Quantiques. Il regroupe plus de 100 équipes de chercheurs et 728 chercheurs répartis dans 32 laboratoires. Il couvre les quatre pans habituels du quantique : calcul, simulation, télécommunications/cryptographie et métrologie.

Spectre électromagnétique : ensemble des rayonnements électromagnétiques allant des plus grandes ondes radio jusqu'aux rayons X et gamma. La lumière visible n'est qu'une toute petite partie située au milieu de ce spectre.

Spin : état d'une particule décrivant sa rotation sur elle-même ou un moment magnétique. S'applique aux électrons, aux neutrons, neutrons et aux atomes. Le spin de particules composites est l'addition du spin de ses composantes. Un proton et un neutron ont un spin de ½. Un électron a un spin de +1/2 ou -1/2.

SQUID : Superconducting Quantum Interference Device, un magnétomètre qui mesure le sens du courant dans un qubit supraconducteur. Il est notamment utilisé par D-Wave.

Stabilizer gates : portes quantiques qui sont utilisées dans des systèmes de correction d'erreur : CNOT, H (Hadamard) et P (phase).

State vector : vecteur d'état représentant un état pur d'un quantum et d'un qubit. On le retouve sous la forme d'un vecteur de norme 1 dans la sphère de Bloch qui matérialise physiquement l'état d'un qubit en état superposé.

Stationary qubits : qubits stationnaires (ou statiques), qui ne bougent pas dans un circuit. C'est le cas des qubits supraconducteurs, à base d'ions piégés, de spin d'électron et dérivés. S'opposent aux flying qubits qui se déplacent, comme les photons.

Superdense coding : l'encodage superdense coding est utilisé pour envoyer deux bits sur un qubit transmis par voie optique entre deux points lorsqu'ils sont déjà reliés par un paire de photons intriqués. C'est un protocole de communication imaginé par Charles Bennett et Stephen Weisner en 1992 et expérimenté en 1996 par Klaus Mattle, Harald Weinfurter, Paul Kwiat et Anton Zeilinger. L'intrication initiale précédant l'envoi des deux bits dans le qubits permet d'éviter de violer le théorème d'Holevo selon lequel un jeu de qubits ne peut pas transporter plus d'information que le nombre équivalent de bits classiques.

Superposition : propriété de quantum et des qubits d'être capable d'être dans plusieurs états en même temps. Un peu comme si la matière vibrait à très haute fréquence. Cela s'explique par la nature ondulatoire de la matière à l'échelle nanoscopique.

Supraconductivité : capacité de la matière à permettre de conduire l'électricité sans résistance. Elle se manifeste généralement à bassse température. Les qubits de certains types, notamment à base d'électrons, sont refroidis à très basse température pour permettre cet effet, soit au niveau des qubits pour les qubits supraconducteurs, soit pour les dispositifs et câbles de lecture de l'état des qubits. A noter le faux ami : en anglais, on ne dit pas supra, mais superconductivity.

Suprématie quantique : qualifie une situation future où des ordinateurs quantiques permettront de réaliser des calculs inaccessibles aux supercalculateurs actuels et pour certaines applications et algorithmes spécifiques. Elle n'arrivera donc pas d'un seul coup et sera progressive, application par application et ordinateur quantique par ordinateur quantique.

Téléportation quantique : technique consistant à envoyer l'état d'un quantum à un autre quantum et à distance. C'est généralement réalisé avec des photons qui ont été au préalable intriqués et qui ont souvent une source commune. Cela a plein d'usages comme en cryptographie quantique (QKD) mais ne peut pas servir pour autant à transmettre de l'information classique. Le théorème de non clonage dit aussi que l'état d'un quantum téléporté disparait de la source après téléportation.

Tenseur : en algèbre multilinéaire et en géométrie différentielle, un tenseur désigne un objet très général, dont la valeur s'exprime dans un espace vectoriel. En calcul quantique, les tenseurs sont utilisés pour décrire l'état de registre de qubits. Un qubit est représenté par un vecteur de 2 nombres complexes. Un registre de N qubits est représenté par 2^N nombres complexes qui résulte du produit tensoriel de N vecteurs à 2 nombres complexes. En quelque sorte, le produit tensoriel représente l'espace combinatoire des valeurs que peut prendre une combinaison de qubits.

Topologique : le calcul quantique topologique repose sur la notion d'anyons qui sont des "quasi-particules" intégrées dans des systèmes à deux dimensions. Les anyons sont des structures physiques asymétriques et à deux dimensions dont la symétrie peut être modifiée. Cela permet d'appliquer des principes de topologie avec des ensembles de permutations successives appliquées aux couples d'anyons qui se trouvent à proximité dans des circuits. Les algorithmes associés s'appuient sur les concepts d'organisations topologiques de tresses ou de nœuds ("braids"). Il existe une équivalence algorithmique entre le calcul avec des qubits à portes universelle et les qubits topologiques.

Toffoli (porte) : aussi appelée CCNOT, est porte quantique opérant sur trois qubits qui modifie la valeur du troisième qubit si celle des deux premiers est à 1.

Unconventional Computing : méthodes informatiques qui ne relèvent pas des principes de calcul classiques des machines de Turing et de Von Neuman. Couvre les outils et méthodes non traditionnels dont font partie les ordinateurs quantiques, mais pas que. Cela comprend aussi notamment les ordinateurs moléculaires et les processeurs neuromorphiques.

UMR : Unité Mixte de Recherche, laboratoire conjoint entre le CNRS et une autre entité, comme une Université, une Grande Ecole ou un autre laboratoire de recherche publique comme l'Inria ou le CEA.

UQCM : ou Universal Quantum Cloning Machine, le modèle le plus classique d'organisation et de programmation des ordinateurs quantiques à base de portes quantiques universelles.

VQE (Variational Quantum Eigensolver) : algorithme quantique hybride utilisé dans la simulation chimique créé en 2013. Son principal contributeur est Alan Aspuru-Guzik, un chercheur qui fait partie de la startup Zapata Computing.

ZX calculus : langage graphique utilisé pour visualiser dans la programmation quantique les notions d'intrication, la complémentarité, la causalité et leurs interactions. Il peut notamment servir au calcul par la mesure (Measurement Based Quantum Computing ou MBQC), à la création de codes de corrections d'erreurs et à l'optimisation de programmes quantiques dans des compilateurs grâce à sa théorie équationnelle et aux déformations topologiques des graphes. Ses principaux contributeurs sont des chercheurs français.

Historique des révisions

Version	Date	Modifications
1.0 (332 pages)	29 septembre 2018	Première version du document publiée sur https://www.oezratty.net/wordpress/2018/ebook-pour-comprendre-informatique-quantique/.
1.1 (338 pages)	4 novembre 2018	Ajouts des startups Bleximo, GTN, Intelline, LakeDiamond et Qindom, des travaux d'Urmila Mahadev sur l'explicabilité des algorithmes quantiques, de l'annonce de l'ERC Synergy Grant de 14M€ aux équipes de Grenoble autour de Maud Vinet du CEA-Leti et de diverses autres actualités scientifiques.
1.1 (342 pages)	7 novembre 2018	Ajout des détails de la première tranche du Flagship Européen et du dernier plan quantique du gouverment allemand.
1.2 (342 pages)	10 novembre 2018	Ajout de quelques détails au sujet du plan scientifique de l'INRIA.
1.3 (342 pages)	25 novembre 2018	Ajout de la startup Quantum Machines.

2.0 (504 pages)	20 septembre 2019	Intégration de la version haute résolution des illustrations. Ajout d'Emmy Noether dans les créateurs de la physique quantique, de Chien Shiung Wu dans les physiciens de l'informatique quantique et d'un grand nombre d'autres scientifiques dans le panorama historique du quantique. Plus un topo sur le démon de Maxwell. Ajout d'une rubrique sur les supraconducteurs et sur la superfluidité et d'informations au sujet des transistors supraconducteurs pour supercalculateurs. Modification de l'organisation du document sur les parties ordinateur quantique et acteurs du marché. Nouvelle grande partie détaillée sur la métrologie quantique. Nouvelle explication de la représentation de l'état des quantums et de la sphère de Bloch par le couple phase/amplitude d'un quantum. Ajout de la notion de qudits et de qutrits. Plus de détails sur la suprématie quantique, l'avantage quantique et sur l'émulation quantique sur supercalculateurs. Compléments sur la cryogénie et sur la mémoire quantique. Nouvelle rubrique sur les algorithmes hybrides, sur la certification des algorithmes quantiques et sur la mise au point de logiciels quantiques et aussi sur la téléportation de qubits. Ajout de NEEXP dans les classes de complexité quantiques. Ajout du blind computing et du chiffrement homomorphe quantique. Ajout du MBQC (dans les classes d'ordinateurs quantiques) et du ZX calculus (méthode de programmation). Ajout de eQASM dans les outils de développement. Le point sur IBM Q System One. Ajout de la mystérieuse startup MemComputing qui concurrence D-Wave et Fujitsu. Ajout du projet européen Mos-quito. Ajout de CryptoNext, Crypto Quantique, Ravel Technologies et VeriQloud dans les startups de la cryptographie quantique. Ajout de startups dans le calcul quantique : Mentai.ai, Pasqal, Stratum.ai, A*Quantum, Ankh.1, AppliedQubit, Automatski, Boxcat, D SLit Technologies, Elyah, Equal1.labs, JoS Quantum, Ketita Labs, Kiutra, Labber Quantum, M-Labs, Multiverse Computing, NetraMark, Nu Quantum, PhaseCraft, Plassys Bestek, QEYnet, Qirithm, Quantastica, QuantiCor Security, Quantopo, Quantum Factory, Quantum Impenetrable, Quantum Xchange, QuBalt, Qubit Reset, QuDot, Quix, QuLab, QunaSys, Rahko, Shyn, SoftwareQ, Solid State AI, SpeQtral, Universal Quantum, Xofia, ZY4. Graphe de répartition par pays et dans le temps des startups quantiques. Ajout de la Pologne dans les pays de l'Europe investissant dans le quantique. Inventaire et cartographie des laboratoires de recherche quantiques en France. Nouvelles fumisteries quantiques dont le premier scam quantique financier, QuantumAI, et sur le management quantique. Création d'un beau glossaire et d'une bibliographie.


|0>
θ/2
|1>