Opinions Libres
le blog d'Olivier Ezratty

Decode Quantum avec Anthony Leverrier d'Inria

Nous voici dans le 54e épisode des entretiens Decode Quantum où, avec Fanny Bouton, nous recevions **Anthony Leverrier** d'Inria, après avoir reçu Harold Ollivier qui coordonne la recherche dans le quantique chez Inria. Ces épisodes sont également diffusés par **Frenchweb**.

Anthony Leverrier est chercheur Inria depuis 2012, dans l'équipe **COSMIQ** anciennement SECRET (8 chercheurs, en cryptographie symétrique, et cryptographie basée sur les codes, ainsi qu'en algorithmique et correction d'erreur quantique, notamment Jean-Pierre Tillich qui avait encadré la thèse de Harold Ollivier, André Chailloux sur les algorithmes, et Maria Naya-Plasencia qui a développé la cryptanalyse quantique de la crypto symétrique). Au départ, il était ingénieur de l'école Polytechnique. Il a ensuite réalisé une thèse de doctorat à Télécom Paris sur la distribution quantique de clés puis deux post-docs à l'ICFO en Espagne et à l'ETH Zurich. Il est notamment spécialisé en codes de correction d'erreurs.

Voici comme d'habitude les points clés évoqués pendant cet entretien :

- Comment est-il tombé dans la marmite quantique ? Il lisait Science&Vie comme adolescent mais comme c'est souvent le cas, c'est à l'X qu'il a pris goût au sujet, notamment via les cours de physique quantique de Jean-Louis Basdevant, Jean Dalibard, Alain Aspect et Philippe Grangier. Il réalise un stage sur les lasers de puissance à Berkeley, utilisés dans les accélérateurs de particules. Il hésitait entre les lasers, les hautes énergies, la fusion nucléaire et le quantique à très basse énergie, juste avant le lancement du projet ITER à Cadarache. Les moyens mis en œuvre sont différents pour réussir dans la fusion nucléaire et les ordinateurs quantiques.

- Sa thèse **Theoretical study of continuous-variable quantum key distribution** soutenue en 2009. Avec trois directeurs de thèse Gilles Zémor (qui est parti à Bordeaux), Joseph Boutros tous deux de Telecom Paris et surtout Philippe Grangier de l'IOGS. Avec le soutien de Romain Alléaume de Télécom Paris qui l'a aidé à trouver un stage chez MagiQ à Boston. Il a aussi côtoyé Eleni Diamanti à Télécom Paris alors qu'elle y était chercheuse, avant de rejoindre le LIP6. Il a même travaillé avec Marc Kaplan, devenu depuis le CEO de VeriQloud.

- Il a été l'un des trois lauréats 2010 du Prix de Thèse ParisTech. Un prix qui n'a pas duré longtemps.

- Il a ensuite réalisé deux post-docs : l'un dans le groupe d'Antonio Acín à l'ICFO de Barcelone en 2010-2011 sur les inégalités de Bell sans loophole (détecteurs forts, résistant mieux aux pertes et imperfections, qui a abouti à des expériences d'inégalités de Bell sans loophole en 2015, notamment à Delft puis à Vienne chez Anton Zeilinger et à l'ICFO, recherche d'axiomes permettant de dériver les postulats de la physique quantique), puis celui de Renato Renner à ETH Zürich (cryptographie quantique, non-localité, un endroit incroyable côté niveau niveau scientifique où sont passés Fernando Brandao qui maintenant chez Amazon, Richard Kueng chez John Preskill à Caltech, Marco Tomamichel qui est maintenant à Singapour, et Omar Fawzi qui est à l'Inria à Lyon).

- Comment définir ton champ de recherche et ton activité ? Il est théoricien, pas trop coloré maths ou physique et plutôt à l'interface entre ces différents mondes.

- L'une de ses grandes spécialités, ce sont les codes de correction d'erreur, des codes utilisés au départ pour les communications quantiques mais qui ont des dérivations pour le calcul quantique. Il continue d'ailleurs de travailler dans les deux domaines, la QKD et la correction d'erreurs pour le calcul quantique.

- Comment s'y retrouver dans la zoologie des codes de correction d'erreur dans le calcul quantique. Rôles, usages, avantages et inconvénients. Un zoo vient d'être créé par Victor Albert de l'Université de Maryland. **https://errorcorrectionzoo.org/**.

- Les codes de correction d'erreurs sont nés du besoin de créer des ordinateurs quantiques universels de grande taille. L'algorithme de factorisation de Peter Shor nécessite un grand nombre de portes (10^12 à 10^15) pour factoriser une clé RSA 2048 bits. Serge Haroche et Jean-Michel Raimond publient en 1996 un article exprimant un fort scepticisme sur la perspective de créer un ordinateur quantique de grande taille, **Quantum Computing: Dream or Nightmare?**, Physics Today, 1996 (2 pages). La réponse de Peter Shor sont des codes de correction d'erreur pour protéger l'information quantique. Il faut contourner diverses limitations : on ne peut pas copier l'information quantique à l'identique, comment mesurer une erreur sans trop perturber le système et dans le quantique, comment travailler avec un espace plus large avec des erreurs de flip et de phase et qui sont continues et non discrètes. Puis Dorit Aharonov publie son fameux théorème qui indique comment faire du calcul tolérant aux fautes. On protège l'information pendant que l'on fait les calculs. C'est conditionné par un taux d'erreur maximum des qubits physiques et il faut disposer d'un grand nombre de qubits physiques. Pour exécuter l'algorithme de Peter Shor sur une clé RSA 2048 bits avec des "surface code", il faudrait disposer de 20 millions de qubits physiques avec une fidélité de 99,9%. Cela n'a pas changé depuis 2019 et nous en sommes encore très loin. Il faut traiter de la question fondamentale de la préservation de la fidélité des qubits physiques avec l'augmentation de leur nombre.

- Les codes de correction sont exécutés après chaque opération. L'overhead généré en temps de calcul est constant. Mais cela fait exploser le nombre de qubits nécessaires. Les codes de surface ont été inventés par Alexei Kitaev. Ayant appris l'existence de l'algorithme de factorisation de Shor, il en a créé une variante. Il a proposé le "toric code" puis le "surface code" qui font le pont entre codes quantiques et topologie. La plupart des schémas de calcul tolérant aux fautes s'appuient sur ces codes.

- Le surface code a des limitations. Il encode les qubits logiques avec un grand nombre de qubits physiques. La qualité de la protection n'est pas optimale et il existe des erreurs de poids sqrt(N) qui ne peuvent pas

être corrigées. A la fin 2009. Jean-Pierre Tillich et Gilles Zémor ont trouvé une version corrigeant aussi bien mais permettant d'encoder beaucoup de qubits logiques. Ce sont des « produits d'hypergraphes » qui sont à de bons codes classiques ce qu'est le surface code pour le code de répétition. Ils font partie de la famille des codes LDPC où chaque qubit va parler à un petit nombre de qubits.

- Nous évoquons le coût de correction qui est focalisé sur les portes T et Toffoli (utilisant de la distillation d'états magiques, très consommatrice de qubits physiques) puis les notions de tolérance de pannes pour éviter que les erreurs se propagent. La correction d'erreur permet potentiellement de créer des mémoires quantiques.

- Les turbo-codes ont été abandonnés. Pourquoi ? Ce sont des objets classiques des années 1990. Claude Pérou de l'ENST Brest a proposé les versions classiques qui avaient de bonnes performances. C'était inspiré par l'électronique. Les codes LDPC classiques et quantiques en sont des dérivés. Les turbo-codes sont intéressants pour les communications quantiques.

- Anthony travaille sur les codes LDPC avec deux chercheurs de Microsoft, Nicolas Delfosse (basé aux USA) et Vivien Londe (basé en France). Vivien Londe dont il a dirigé la thèse, soutenue en 2019 ! Voir par exemple **Fast erasure decoder for a class of quantum LDPC codes** par Nicholas Connolly, Vivien Londe, Anthony Leverrier et Nicolas Delfosse, Août 2022 (5 pages). Nicolas Delfosse a fait sa thèse avec Gilles Zémor à Bordeaux. Daniel Gottesman a montré que les codes LDPC pouvaient réduire l'overhead de la QEC. Par contre, il faut trouver de bons décodeurs et aller très vite. Les besoins sont énormes en bande passante classique avec des terabits / seconde.

- Nous évoquons le lien entre l'efficacité des codes de correction d'erreurs et l'interconnectivité des qubits. Chaque qubit devrait parler à des qubits éloignés pour réduire l'overhead. Ce n'est pas évident avec les qubits supraconducteurs. C'est plus facile avec les ions, les atomes neutres et les photons.

- Anthony a aussi travaillé sur les Tanner codes qui sont des variantes de codes LDPC. Voir **Quantum Tanner codes** par Anthony Leverrier et Gilles Zémor, Février-Septembre 2022 (35 pages).

- Et les Floquet codes ? Ce sont des codes visant le long terme et qui ont besoin d'une très bonne connectivité entre qubits physiques. C'est une variante du code de surface proposée par chercheurs de Microsoft.

- Enfin, il y a les codes bosoniques avec les variations des qubits de chat de Mazyar Mirrahimi/Zaki Leghtas utilisés par Alice&Bob.

- Nous évoquons aussi le travail d'Aurélie Denys sa thésarde avec **The 2T-qutrit, a two-mode bosonic qutrit** par Aurélie Denys et Anthony Leverrier, Octobre 2022 (20 pages) qui exploite des qutrits (objets quantiques à trois états).

- Notons enfin qu'Anthony coordonne aussi le défi **EQIP** dans le cadre du PEPR (programmes et équipements prioritaires de recherche) quantique lancé en 2021, avec une bonne dizaine de chercheurs Inria et autres comme l'équipe de Cyril Allouche chez Atos. Engineering for Quantum Information Processors.

Cet article a été publié le 4 janvier 2023 et édité en PDF le 4 janvier 2023.