Opinions Libres
le blog d'Olivier Ezratty

Actualités quantiques d’avril 2026

Nous voici dans le 80ième épisode de Quantum, le podcast et la newsletter de l’actualité quantique en France et dans le monde. 80, mazette ! On avait démarré il y a presque 7 ans, en septembre 2019.

Fanny Bouton et moi-même couvrons d’abord l’actualité française avec l’inauguration de l’ordinateur quantique photonique Lucy de Quandela au TGCC du CEA, la conférence Pasqal Thoughts avec un point sur leurs deux qubits logiques, quelques nouveautés scientifiques et un changement de direction, une journée sur la photonique au Collège de France, la journée quantique organisée par l’AID à l’école Polytechnique, et la roadmap de C12.

Sur le front international, on retient la création du Q-CAB européen, le préprint IonQ de 110 pages sur leur architecture FTQC, les résultats expérimentaux de QuEra sur la fidélité de portes CZ, une architecture FTQC originale de Q-CTRL, un papier Google/Oratomic sur un avantage quantique exponentiel en mémoire pour le machine learning quantique, et une estimation Google du coût de simulation de dynamique moléculaire.

Le bêtisier habituel clôture l’épisode avec le “Q-Day Prize” dont le premier lauréat sélectionné utilise un algorithme quantique générant un résultat aléatoire et où tout le calcul est réalisé en pratique classiquement.

Evénements

Inauguration de Lucy au TGCC

Le 14 avril, le TGCC situé sur le site de la Direction des Affaires Militaires (DAM) du CEA à Bruyère le Chatel au sud de l’Ile de France et Quandela inauguraient le lancement de la machine NISQ Lucy avec ses 12 qubits en présence de la Ministre Anne Le Hénanff, Bruno Bonnell du SGPI, Anne-Isabelle Etienvre, l’Administratrice Générale du CEA, Killian Gross de la DG CNECT de la Commission Européenne, Anders Dam Jensen du programme EuroHPC, Mickaël Krajecki du GENCI et Niccolo Somaschi de Quandela (tous ci-dessous, avec Pascale Senellart de Quandela/C2N). L’ordinateur quantique a été acquis par EuroHPC, dans le cadre du consortium EuroQCS-France via GENCI, et co-financé par la stratégie nationale quantique de France 2030. L’ordinateur quantique Lucy est associé au supercalculateur Joliot-Curie du TGCC et accessible gratuitement aux acteurs de la recherche et de l’industrie pour tester des algorithmes quantiques NISQ à petite échelle.

https://www.cea.fr/presse/Pages/actualites-communiques/ntic/inauguration-ordinateur-quantique-lucy-tgcc.aspx

Quelques jours après, OVHcloud annonçait l'accès à la machine Quandela Benelos dans le cloud. C'est la même que celle du TGCC avec 12 qubits. La machine est dans les locaux de Quandela.

https://corporate.ovhcloud.com/fr/newsroom/news/ovhcloud-quandela-belenos-quantum-platform/

Journée Pasqal Thoughts

Pasqal organisait sa **conférence** « écosystème » le 14 avril 2026. Au menu, l'évocation d'études de cas utilisateurs et un point sur la roadmap. Ils présentaient quelques détails techniques sur leurs deux qubits logiques pré-annoncé en septembre 2025. En gros, ce sont deux qubits logiques avec de la détection d'erreurs de flip encodés en [4,2,2]. On est loin d'un véritable qubit logique corrigé. Ils indiquaient avoir réalisé une PDE (résolution d'une équation aux dérivées partielles) avec ces deux qubits logiques. Ils ont du utiliser de la post-sélection. Le papier associé reste à publier. A noter un changement de gouvernance. Loic Henriet n'est plus le CEO et redevient CTO. Et Wasiq Bokhari, auparavant executive chairman, devient le CEO de la société. Les vidéos de l'après-midi sont **disponibles**. Regardez en particulier les interventions d'Antoine Browaeyes, Adrien Signolles et Loic Henriet.

Ils publiaient aussi un intéressant preprint sur le fonctionnement de leur système contrôlant un millier d'atomes en s'appuyant sur de la cryogénie à 4K pour refroidir la pompe ionique servant à créer de l'ultra-vide de qualité dans la chambre où sont pilotés les atomes froids (refroidis de leur côté par des lasers). Cela faisait pas mal d'années qu'ils travaillaient sur le sujet. A noter que la cryogénie semble être un coût fixe au regard du nombre d'atomes contrôlés. Ils devraient pouvoir augmenter le nombre de ces derniers sans augmenter la puissance de cette cryogénie à base de compresseur Sumitomo et de tête pulsée.

Defect-free arrays at the thousand-atom scale in a 4-K cryogenic environment by Desiree Lim, Hadriel Mamann, Grégoire Pichard, Lilian Bourachot, Arvid Lindberg, Clotilde Hamot, Hugo Le Bars, Florian Fasola, Siddhy Tan, Gwennolé Cournez, Sylvain Dutartre, Thierry Cartry, Sylvain Lemettre, Richard Hostein, Julien Paris, Franck Ferreyrol, Andréa Collardey, Adrien Signoles, Thierry Lahaye, Corentin Monmeyran, and Bruno Ximenez, arXiv, April 2026 (8 pages).

Fanny était le même jour au Luxembourg pour une keynote dans l'événement Synergy sur HPC, IA et calcul quantique.

Conférence « Light-based quantum technologies » au Collège de France

Cette journée sur la photonique était organisée le 16 avril au Collège de France par Pascale Senellart en clôture de sa chaire dont les cours s'étaient déroulés entre janvier et février 2026. Avec Serge Haroche, Antoine Heidmann sur la détection des ondes gravitationnelles (j'ai compris comment on pouvait déterminer leur origine, grâce à de la triangulation comme pour le GPS), Alexia Auffèves sur l'énergétique en photonique (et un zeste de QEI), Anaïs Dréau sur les centres colorés dans le silicium, Christine Silberhorn de Paderborn University en Allemagne sur le calcul photonique, et Hugues de Riedmatten sur les mémoires quantiques.

Les vidéos et supports de présentation sont **disponibles**.

Journée Quantique Défense à Polytechnique

Organisée par l'Agence Innovation Défense (DGA). Une journée de conférences donnant l'occasion de rencontrer une bonne partie de l'écosystème entrepreneurial français. A noter l'intervention de Catherine Vautrin, la ministre des Armées, et Patrick Pailloux le nouveau délégué général de l'armement. Fanny animait un panel et participait à un autre panel, en compagnie de Maud Vinet. Cela avait lieu à l'école Polytechnique le 17 avril. Il y avait plus de 400 personnes. Le grand hall de l'école Polytechnique accueillait plusieurs dizaines de stands des acteurs industriels de l'écosystème quantique (startups, Airbus, Thales, …).

Fanny y animait un panel sur les levées de fonds avec Maud Vinet (Quobly), Patrick Aufort (AID), Delphine Roma (Air Liquide) et Olivier Tonneau (Quantonation). Elle participait aussi à un panel sur le calcul quantique animé par Frédéric Barbaresco de Thales, avec Valerian Giesz (Quandela) et Pierre Desjardins (C12) entre autres.

Conférence Devoxx le 23 avril

Lors de cette grande conférence développeurs, Fanny Bouton et moi-même, accompagnés de Guillaume Schurck d'Alice & Bob et Sébastien Marie, CTO et DSI de Matmut, avons délivré une session de 3 heures sur le calcul quantique. Mon intervention d'une heure et demie était la version à jour de mon introduction sur le sujet. On avait 200 participants qui sont restés jusqu'au bout sauf 2 que Fanny a repéré et scanné au laser pour leur faire la leçon plus tard.

Voici mon **support de présentation**.

Réception d'Alain Aspect à l'Académie Française

C'était le 23 avril et en grande pompe avec un discours de forme centré sur le prédécesseur d'Alain au fauteuil 22, M. René de Obaldia (**vidéo**, **texte**). Les scientifiques comprenaient ses blagues de physiciens, mais pas les académiciens (de l'Académie Française). Et réciproquement !

Médaille d'agent du CNRS pour Julien Laurat

Une **belle distinction** pour Julien Laurat, du LKB et aussi Welinq qui travaille sur les mémoires quantiques permettant de créer des réseaux quantiques, notamment pour interconnecter des ordinateurs quantiques entre eux.

Evénements à venir

- J'interviens à Lyon et en ligne le 12 mai dans la conférence « Le quantique au service de l'IA et de la robotique – quels horizons » organisée par « le Printemps de la Robotique » et en compagnie d'Amélie Cordier. **Lien d'inscription**.
- **QEI workshop** à Barcelone des 18 au 22 mai 2026.
- **Q-Expo** organisé par le consortium européen QuIC les 18 et 19 mai à Bilbao où Fanny sera.
- **Q.Stack Italia** à Bologne et Fanny y sera tout comme Quandela et Alice & Bob.
- **Conférence scientifique** en l'honneur de la carrière de Philippe Grangier à l'IOGS le 4 juin. Keynote d'Alain Aspect et de Serge Haroche. J'y interviens pour parler du lien entre l'IA et les sciences quantiques.
- **France Quantum**le 16 juin à Station F. J'y interviens avec un keynote sur les défis scientifiques et technologiques du FTQC. Puis Vivatech le reste de la semaine dans le Hall 7 sur 3 étages avec une machine Belenos de Quandela et un chandelier d'un ordinateur quantique d'IBM.
- **IQT Nordics** à Oslo du 22 au 24 juin où j'y interviens pour la QEI, juste avant Maud Vinet de Quobly. J'y anime aussi un panel sur les logiciels quantiques.
- **Panorama de toutes les voies technologiques de l'ordinateur quantique** les 25 et 26 juin à Grenoble organisé par la Maison du Quantique Grenoble-Alpes. J'y serais.

Annales des Mines

Dossier en deux parties, la **première** vient d'être publiée. Je prépare un article sur l'énergétique du calcul quantique pour la seconde partie, avec Marco Fellous-Asiani (Inria) et Pierre-Emmanuel Emeriau (Quandela).

Podcasts divers

- **Lionel Martillini** d'EHDEC chez Yuval Boger (**lien**).
- **Eleni Diamanti** chez Blond & Quantum (**lien**).
- Moi-même avec **Shahin Khan** et **Doug Black** de InsideHPC (**lien**).

Création du Q-CAB Européen

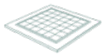
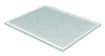
L'UE a annoncé la création du **Quantum Computing Assessment Board** (Q-CAB) dont je fais partie en

compagnie de scientifiques tels que Peter Zoller, Ignacio Cirac, David DiVincenzo et Sabrina Maniscalco. Pourquoi ? A quoi ce comité scientifique va-t-il servir ? Nous expliquons cela dans le podcast.

France

C12 roadmap

C12 annonçait sa **roadmap**. Elle vise l'atteinte de 128 qubits logiques à base de 8 500 qubits physiques d'ici 2032, en ligne, il se doit, avec les objectifs du programme ProQCima. Et puis 792 qubits logiques supportant 10 millions d'opérations avec 100K qubits physiques. Et surtout une consommation d'énergie très faible, avec une puissance de seulement 50 kW. Grâce à différents paris sur l'électronique de contrôle… qui ne sont pas encore bien **documentés**. Leurs premiers qubits physiques doivent de leur côté arriver en 2027. On attend cela depuis longtemps.

C12	2027	2030	2032	2033
	AÏDÔS	ZÉLOS	STYX	PANOPEIA
				
Logical qubits	1	8	128+	792+
Physical qubits	16	236	8,500	100,000
Logical error rate	10^{-3}	10^{-5}	10^{-6}	10^{-7}
Watts per physical qubit	1,500	100	6	0.5
Qubits per square meter	1.4	21	500	6,000

Alice & Bob

La startup n'est plus une PME puisqu'elle vient d'**annoncer** avoir maintenant plus de 250 salariés. Ils ont recruté une centaine de personnes depuis début 2025, soit depuis leur dernière levée de fonds de 100 M€.

International

IonQ

La startup publiait un énorme préprint de 110 pages avec leur architecture FTQC documentée de bout en bout, côté correction d'erreur, tolérance aux fautes et aussi architecture matérielle. On sent l'impact de la lenteur des opérations sur les qubits avec les ions piégés. A noter que le principal auteur (en dernier dans la liste) est le Français Nicolas Delfosse, qui pilote l'équipe QEC/FTQC de la société. Et une technique dite de « chat marchant » (walking cat) qui n'a pas de rapport avec les qubits de chat d'Alice & Bob. Le papier est très complet car il couvre aussi bien la partie QEC/FTQC que la partie hardware, à base de la technologie venant d'Oxford Ionics.

Size	Memory blocks	T gates	SEC	Time (hours)
10	17	71,536	598,520	1
20	17	532,692	4,805,861	7.5
30	34	1,760,876	14,748,419	23
40	34	4,132,048	34,733,136	53.5

Le papier comprend une estimation de l'exécution de l'algorithme de Shor pas glorieuse en temps de calcul. Il leur faut 53 heures pour casser une clé RSA de 40 bits. Sur un laptop en C++, cela dure moins d'une seconde. Ils affichent la capacité d'exécution de quelques millions de portes T par jour, ce qui est assez lent. J'ai fait une comparaison avec un papier récent de Google (sur le cassage de clés ECC) et ils sont 37 fois plus rapides toutes choses égales par ailleurs. Il va falloir qu'ils trouvent le moyen d'améliorer cela.

Fault-Tolerant Quantum Computing with Trapped Ions: The Walking Cat Architecture by Felix Tripier, Woo Chang Chung, Jacob Young, Safwan Alam, Bryce Bjork, Aharon Brodutch, Finn Lasse Buessen, Nolan J. Coble, Thomas Dellaert, Dmitri Maslov, Martin Roetteler, Edwin Tham, Mark Webster, Min Ye, John Gamble, Andrii Maksymov, J. P. Marceaux, and Nicolas Delfosse, arXiv, April 2026 (110 pages).

QuEra

Ils publiaient un papier scientifique sur leur approche de correction d'erreurs et avec une annonce tonitruante : avec un encoding rate de plus de 50%, ils obtiendraient un taux d'erreurs de qubits logiques de seulement 10^-13. Est-ce crédible ? Bien non. Le papier scientifique est sérieux mais liste certaines assomptions qui ont un impact énorme sur ce résultat étonnant. Il s'agit d'un modèle numérique et pas d'une expérience. Ensuite, leur modèle de bruit n'intègre pas toutes les sources de bruit qui peuvent affecter les atomes. Enfin, ils utilisent un système de décodage de syndromes d'erreurs en trois couches, la dernière utilisant un solveur Gurobi qui nécessiterait un supercalculateur et ne pourrait apparemment pas fonctionner en temps réel, le tout avec de la post-sélection. L'**article marketingo-technique** de la startup enfile les exagérations en faisant des comparaisons entre leur modèle et des réalisations pratiques réalisées sur des qubits supraconducteurs. C'est d'une mauvaise foi scientifique !

Towards Ultra-High-Rate Quantum Error Correction with Reconfigurable Atom Arrays by Chen Zhao, Casey Duckering, Andi Gu, Nishad Maskara, and Hengyun Zhou, arXiv, April 2026 (17 pages).

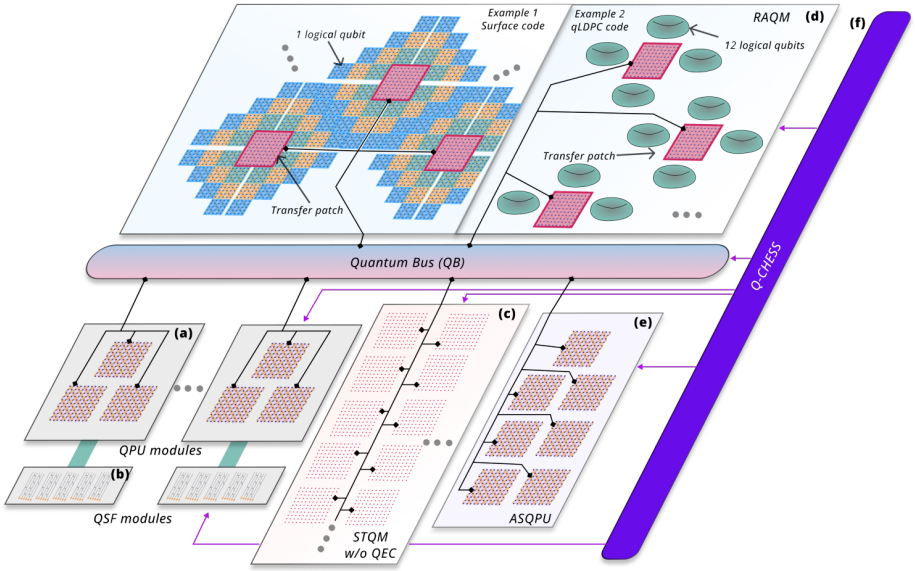
Fin avril 2026, ils publiaient un préprint sur l'amélioration de la fidélité de portes CZ à deux qubits. Elle atteint maintenant 99,854% pour les portes à deux qubits, ce qui est un record et pas loin de 99,9%. Ils exécutent avec cette fidélité jusqu'à 10 portes simultanément, avec 20 atomes déplacés dynamiquement dans la zone adéquate. Là, c'est plus sérieux car c'est expérimental.

High-fidelity entangling gates and nonlocal circuits with neutral atoms by Simon J. Evered, Muqing Xu, Sophie H. Li, Alexandra A. Geim, J. Pablo Bonilla Ataides, Marcin Kalinowski, Dolev Bluvstein, Nishad Maskara, Christian Kokail, Markus Greiner, Vladan Vuleti?, and Mikhail D. Lukin, arXiv, April 2026 (20 pages).

Q-CTRL

La startup australienne Q-CTRL publiait une architecture FTQC end-to-end intéressante montrant comment elle pourrait réduire le coût de la correction d'erreurs et de la tolérance aux fautes. Le titre indique un gain de x138 en qubits physiques. Mais une fois encore, le titre est misleading car le repère est l'estimation de ressources de Craig Gidney de 2019 (26 millions de qubits physiques) et pas celle de 2025 (1 millions) ou celle encore plus faible de leur confère australien Iceberg Quantum (100 à 471K qubits). Ils basent leur architecture sur de l'interconnexion de processeurs quantiques, la spécialisation de certains d'entre eux pour la génération d'états

magiques, et en option, l'hypothèse de l'existence de mémoires quantiques de type qRAM. C'est de l'architecture de haut vol.



Heterogeneous architectures enable a 138x reduction in physical qubit requirements for fault-tolerant quantum computing under detailed accounting by Pranav S. Mundada, Aleksei Khindanov, Yulun Wang, Claire L. Edmunds, Paul Coote, Michael J. Biercuk, Yuval Baum, and Michael Hush, arXiv, April 2026 (34 pages).

Avantage quantique pour l'IA ?

Un papier publié par Google AI et Oratomic indique une possibilité d'obtenir un avantage quantique avec des applications de machine learning quantique grâce à une simplification de la mise en œuvre d'un oracle permettant leur chargement grâce à une méthode d'échantillonnage de données et à un chargement séquentiel optimisé dénommée 'oracle sketching', qui est un oracle approximatif basé sur l'exploitation d'échantillons de données et l'usage de classical shadows pour la mesure. Le circuit et la lecture des données doivent être réalisés plusieurs fois, le nombre augmentant avec la complexité des données.

Le papier est théorique et illustre un avantage quantique potentiel obtensible avec seulement 60 qubits logiques qui requiert du FTQC. L'avantage est exponentiel en mémoire et polynomial en temps de calcul. Plusieurs cas d'usage sont présentés dans le papier, sur le séquençage d'ARN par PCA, sur l'analyse d'appréciation de films sur la base IMDB et sur la résolution de systèmes linéaires dynamiques (Ax=b) pour la détection d'anomalies dans des réseaux massifs. Mais il faut que les données soient creuses et il faut les recharger séquentiellement à chaque exécution de circuit. Bref, ce n'est pas encore la panacée malgré les éloges qui ont fleuri sur ce papier. Cela fait un peu avancer le domaine du Quantum Machine Learning.

Exponential quantum advantage in processing massive classical data by Haimeng Zhao, Alexander Zlokapa, Hartmut Neven, Ryan Babbush, John Preskill, Jarrod R. McClean, and Hsin-Yuan Huang, arXiv, April 2026 (144 pages).

https://quantumfrontiers.com/2026/04/09/unleashing-the-advantage-of-quantum-ai/

Papier de chimie quantique de Google

42 ans à 7000 ans de calcul seraient nécessaires pour simuler de la photodissociation de molécules de cinq à une dizaine d'atomes. La dynamique moléculaire est plus intéressante que le simple calcul d'un état fondamental (ground state). Mais cela coute apparemment très cher, en attendant de futures optimisations.

Molecule	η	L (a_0)	ΔL ($10^{-2} a_0$)	λ_H ($10^5 E_h$)	Logical qubits: State storage (C_{data})	Logical qubits: Ancilla qubits (C_{anc})	Logical qubits: Total	Toffoli gates (C_{Toff}): Nuclear state prep. (10^9)	Toffoli gates (C_{Toff}): Electronic state prep. (10^9)	Toffoli gates (C_{Toff}): Time evolution (10^{12})	Toffoli gates (C_{Toff}): Quantum yield using QAE (10^{12})
CH_4	15	392	4.78	0.85	585	3189	3774	2.79	0.10	1.89	32.1
CH_2OO	29	298	3.64	4.09	1131	3385	4516	3.32	0.42	18.9	322
C_4H_6O	49	595	3.63	7.98	2058	3811	5869	7.39	0.98	60.1	1002
HNO_4	46	276	3.37	9.60	1794	3542	5336	3.84	0.56	64.0	1009
CF_3CO_2H	64	473	2.89	20.1	2688	3904	6592	4.88	1.69	191	3240
C_5-HPALD	78	1066	3.25	19.9	3510	4289	7799	9.87	2.19	239	4070
HCFC-132b	74	520	1.59	64.4	3330	4243	7573	4.72	3.43	742	12 600
CH_3OBr	58	523	0.80	150	2496	4512	7296	4.12	1.25	1350	22 900
$BrCH_2CHO$	65	509	0.78	181	3120	4578	7698	4.10	1.70	1810	30 700

Table 4. Resource estimates for simulating photodissociation yields in molecules whose full quantum dynamics is classically intractable. η is the total number of particles (electrons and nuclei), L is the length of one side of the computational cell, $\Delta L = L/N$ is the spacing of the grid points in real space, and λ_H is the block-encoding parameter. We give both space and time resources for our algorithm, with the qubit counts divided into qubits to store the state (C_{data}) and the ancillas (C_{anc}). The Toffoli gate counts for time evolution indicate one dynamics run for simulation time $t = 30$ fs, and the QAE counts give the cost of calculating the quantum yield to accuracy $\epsilon = 0.095$ (involving multiple simulations of the dynamics).

Estimation du temps de calcul réalisé après plusieurs itérations avec Claude Pro :

Corrected Time Estimates

Molecule	η	N_T^{QAE}	Circuit depth	d	Corrected time
CH_4	15	3.21×10^{13}	2.1×10^{12}	41	**~30 years**
CH_2OO	29	3.22×10^{14}	1.1×10^{13}	43	**~160 years**
C_4H_6O	49	1.00×10^{15}	2.0×10^{13}	45	**~290 years**
HNO_4	46	1.01×10^{15}	2.2×10^{13}	45	**~310 years**
CF_3CO_2H	64	3.24×10^{15}	5.1×10^{13}	45	**~720 years**
C_5-HPALD	78	4.07×10^{15}	5.2×10^{13}	47	**~780 years**
HCFC-132b	74	1.26×10^{16}	1.7×10^{14}	47	**~2,500 years**
CH_3OBr	58	2.29×10^{16}	3.9×10^{14}	47	**~5,900 years**
$BrCH_2CHO$	65	3.07×10^{16}	4.7×10^{14}	49	**~7,300 years**

End-to-End Simulation of Chemical Dynamics on a Quantum Computer by Elliot C. Eklund, Arkin Tikku, Patrick Sinnott, William J. Huggins, Guang Hao Low, Dominic W. Berry, and Ivan Kassal, arXiv, March 2026 (69 pages). Google AI.

Dans le même temps, Garnet Chan de Caltech fait un point sur les défis de la simulation chimique avec un ordinateur quantique, les limites des possibilités du calcul classique étant sans cesse repoussées. Mais il ne jette pas le bébé avec l'eau du bain.

https://www.newquantumera.com/podcast/quantum-chemistrys-classical-limits-with-garnet-chan/

https://quantumfrontier.substack.com/p/the-great-superconducting-qubit-consolidation

Emulation record de circuit quantique

Evaluation de Quantinuum Helios avec ses 98 qubits par le centre de calcul de Jülich. Le système se comporterait bien jusqu'à 95 qubits. Record de simulation de circuit quantique, qui s'appuie sur Jupyter, le HPC exaflops de Jülich.

Large-Scale Quantum Circuit Simulation on an Exascale System for QPU Benchmarking by J. A. Montanez-Barrera, and Kristel Michielsen, arXiv, April 2026 (9 pages).

Cisco

Cisco **annonce** un routeur d'intrication pour la communication entre ordinateurs quantiques. Le système fait de la transduction entre modes de communication quantique photoniques, de/vers path encoding.

A Universal Quantum Information Preserving Photonic Switch for Scalable Quantum Networks by Jiapeng Zhao, Stéphane Vinet, Amir Minoofar, Michael Kilzer, Lucas Wang, Galan Moody, Vijoy Pandey, Ramana Kompella, and Reza Nejabati, arXiv, April 2026 (12 pages).

Bêtisier du bullshit

Une **mise à jour** des investissements par pays par QuReCa où ils ont encore tout faux. Exemple avec les Japonais où ils intègrent $7B d'un plan dont seulement une petite partie est consacrée au quantique. Erreurs aussi pour les USA, l'Allemagne, UK, l'Australie, le Canada, etc. Par contre, c'est bon pour la France. Le gag est sur l'Espagne avec plus de $1B, alors que la réalité est de $45M. Mais seuls ceux qui savent savent, y compris en Espagne !

Le « Project Eleven » a récemment décerné le « Q-Day Prize », doté d'un Bitcoin, au chercheur Giancarlo Lelli. Ce dernier a réussi à casser une clé à courbe elliptique de 15 bits en utilisant un ordinateur quantique IBM. Il a dérivé une clé privée à partir de sa clé publique dans un espace de recherche de 32 767 possibilités, via l'algorithme dlog de Shor. Mais il y avait une grosse entourloupe. Le circuit utilisait 98 000 portes sur 70 qubits avec une machine NISQ IBM ayant une fidélité de 99,5 %. De ce fait, sans QEC/FTQC, la probabilité que le circuit entier s'exécute sans une seule erreur est très faible (10^{-215}). L'absence de correction d'erreurs quantiques (QEC) rend le résultat statistiquement nul. La méthode utilisée consistait à employer un vérificateur classique pour trier le bruit jusqu'à tomber sur la bonne clé par hasard. Un ordinateur classique peut tester l'intégralité des 32 768 possibilités en quelques millisecondes et trouver la bonne solution sans passer par ce chemin de détour inutile. L'organisateur de ce prix est une startup spécialisée dans la cybersécurité post-quantique qui cherche à faire parler d'elle. Bien voilà, c'est fait.

15-Bit ECC Key Broken on Quantum Hardware Wins Q-Day Prize by Mohib Ur Rehman, The Quantum Insider, April 2026.

The predictable failure of the QDay Prize by Craig Gidney, April 2026.

La suite au prochain épisode après un mois de mai bien chargé !

Cet article a été publié le 4 mai 2026 et édité en PDF le 4 mai 2026.