Opinions Libres
le blog d'Olivier Ezratty

Actualités quantiques de décembre 2022

Dans ce 44e épisode de Quantum, le podcast francophone de l'actualité quantique, toujours avec Fanny Bouton d'OVHcloud et votre serviteur, nous faisons un tour des événements et de l'écosystème quantique. Nous terminons par un point sur un cas d'usage (CACIB avec Pasqal et Multiverse) et sur le fameux algorithme chinois qui casserait les clés RSA avec un ordinateur quantique pas si éloigné que cela (ou pas…).

Voici comme d'habitude une bonne partie du verbatim du podcast et les liens associés.

Événements

Remise du Nobel de physique à Alain Aspect

Le 10 décembre 2022, Alain Aspect se faisait remettre **officiellement** le prix Nobel par le Roi de Suède. C'était précédé des **Nobel Lectures** où les trois prix Nobel de physique ont raconté leur parcours scientifique. Plusieurs prix Nobel de différentes disciplines étaient également réunis dans une **émission de TV** produite à l'occasion avec une belle brochette d'une dizaine de prix Nobel toutes disciplines confondues.

Alain Aspect et la princesse de Suède Victoria arrivent au banquet royal en l'honneur des récipiendaires des prix Nobel 2022, le 10 décembre 2022 à Stockholm. Crédit photo : Pontus Lundhal – TT News Agency – AFP.

IEDM

Maud Vinet faisait une keynote lors de la conférence « IEEE International Electron Devices Meeting » en Californie début décembre 2022 à l'occasion de la publication d'un review paper sur les qubits silicium.

Il s'agissait de "Enabling Full Fault Tolerant Quantum Computing with Silicon-Based VLSI Technologies". Les équipes du **CEA-leti** présentaient deux autres papiers, "Methodology for an Efficient Characterization

Flow of Industrial Grade Si-Based Qubit Devices” portant sur la caractérisation des wafers de chipsets de qubits utilisant le cryoprober de Bluefors/afore dont ils sont équipés depuis plus d’un an, puis “FDSOI for cryoCMOS Electronics: Device Characterization Towards Compact Model” portant sur l’usage du FDSOI pour créer des composants cryoCMOS de contrôle de qubits.

Q2B

La Q2B de QC-Ware sous-titrée « Practical Quantum Computing » semble s’être bien passée avec un mélange d’interventions d’utilisateurs et de fournisseurs. Avec les interventions de Pasqal (Georges), Alice&Bob (Jérémie Guillaud), C12 (Pierre Desjardins) et Quandela (Valérian Giesz et Niccolo Somaschi). Et aussi Iordanis Kerenidis (QC-Ware). Jean-François Bobier (BCG). Thierry Botter (QUIC). Sinon, Scott Aaronson et John Preskill. Mais pas de sorties ou d’annonces particulières.

Jérémie Guillaud (Alice&Bob), photo: Valérian Giesz.

Conférence TQCI Teratec/Systematic le 8 décembre

Le séminaire **#TQCI** sur le #Quantique coorganisé par NAFEMS, Systematic Paris-Region & TERATEC avait lieu à l’ENSTA Paris située à Palaiseau. TQCI signifie “Teratec Quantum Computing Initiative”.

La conférence faisait le point de projets menés par les acteurs de l’écosystème quantique francilien, notamment dans le cadre de projets collaboratifs du Pack Quantique de la région IDF et géré en partenariat avec HQI/GENCI. La conférence était d’ailleurs animée par Sabine Mehr du GENCI.

Elle comprenait notamment les présentations de Pasqal (Christophe Legrand), Quandela (Jean Senellart), C12 (Juliette Ginies), QRYOlink (Grégory Golf d’ATEM avec Théau Péronnin d’Alice&Bob), du projet Eduquantum (Davide Boscheto de l’ENSTA), de ColibITD (Laurent Guiraud) et Neil Abroug (SGPI).

J’ai pu aussi y présenter la **Quantum Energy Initiative** pendant environ une demi-heure.

Cette conférence est suivie d'une autre édition aussi coorganisé par Teratec, chez EDF à Palaiseau le 11 janvier 2023 qui portera sur le calcul hybride.

J'y interviens avec Alexia Auffèves et Théau Péronnin pour parler une fois encore de la QEI, avec un zoom sur les avantages énergétiques potentiels dans les régimes FTQC et NISQ.

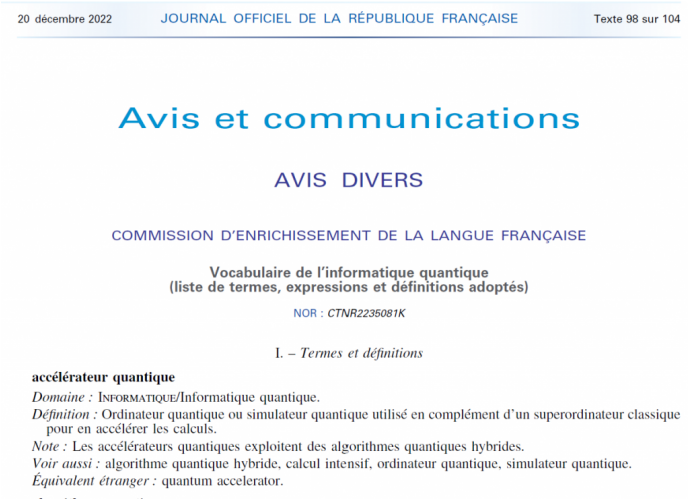
Il y a aussi les interventions de Jacques-Charles La Foucrière de la DAM, d'IBM, Microsoft, Amazon et de Scott Pakin du Los Alamos National Laboratory du DoE.

Agenda et inscriptions.

Côté médias :

- J'ai participé à l'émission **Le Meilleur des mondes** – **Tout comprendre de l'ordinateur quantique : la promesse d'une révolution** par François Saltiel sur France Culture le 23 décembre 2022, en compagnie de Georges Olivier Reymond (Pasqal) et Eleni Diamanti (CNRS LIP6 et WeLinQ).
- Nous étions tous les deux dans une **émission** de **Sqool.tv** avec **Marjorie Paillon** pour parler technologies quantiques et en particulier enjeux dans l'éducation.
- J'étais interviewé dans le **podcast EcranMobile** par Jérôme Bouteiller le 12 décembre 2022 au sujet des ordinateurs quantiques (31 mn).
- Fanny Bouton intervenait dans le **podcast** **Frenchspin** animé par Patrick Beja, en compagnie de Pablo Arrighi d'Inria.

Pascale Senellart est **élue** à l'Académie des Sciences ! Elle y entrera officiellement en juin 2023. Elle se retrouve dans l'intersection applications des sciences du fait de son rôle chez Quandela.



20 décembre 2022 JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE Texte 98 sur 104

Avis et communications

AVIS DIVERS

COMMISSION D'ENRICHISSEMENT DE LA LANGUE FRANÇAISE

Vocabulaire de l'informatique quantique
(liste de termes, expressions et définitions adoptés)

NOR : CTNR2235081K

I. – *Termes et définitions*

accélérateur quantique

Domaine : INFORMATIQUE/Informatique quantique.
Définition : Ordinateur quantique ou simulateur quantique utilisé en complément d'un superordinateur classique pour en accélérer les calculs.
Note : Les accélérateurs quantiques exploitent des algorithmes quantiques hybrides.
Voir aussi : algorithme quantique hybride, calcul intensif, ordinateur quantique, simulateur quantique.
Équivalent étranger : quantum accelerator.

Une **terminologie quantique** a été **publiée** au Journal Officiel du 22 décembre par un décret des services du Premier Ministre. Cette terminologie porte sur la physique et des technologies quantiques. Elle codifie l'usage du vocabulaire quantique dans les textes officiels (appels d'offre, normalisation, etc). J'ai coordonné ce travail pour le service de la terminologie du Ministère de l'Economie entre fin 2020 et octobre 2022. Plusieurs experts ont participé à ce travail : Alain Aspect, Philippe Grangier et Alexia Auffèves (physique) ainsi que Jean-Marie Chauvet et Eric Mahé (informatique). C'était un exercice intéressant et exigeant demandant de la précision dans l'usage du vocabulaire tout en respectant des contraintes de concision.

Startups

Une nouvelle startup liée au quantique est née en France, **HiQuTe Diamond**. Elle a été créée par Alexandre Tallaire, Jocelyn Achard, Ovidiu Brinza, Fabien Benedic et Riadh Issaoui du LSPM le 20 décembre 2022. Ils produisent des plaques de diamants avec cavités pour des capteurs quantiques (NV centers). Ils ont été accompagnés par Technofounders et CNRS Innovation. Cela va renforcer la filière NV centers en France qui comprend quelques startups comme Wainwam-E à Lorient, Chipiron à Paris ainsi que le laboratoire de Jean-François Roch (ENS Saclay + TRT). J'avais rencontré les fondateurs en août 2022 à Villetaneuse et LinkedIn.

Quantique au CES 2023

Il y avait quatre startups du quantique au CES cette année, où Fanny était.

GLOphotonics, une startup basée à Limoges présentait une horloge quantique recevait même un **award** ! Leur "Photonic Microcell Atomic Clock" est censée adopter une forme de stylo et servira à faire de la géolocalisation sans satellite.

Photo : Fanny Bouton.

QSIMPLUS (Korea) présentait QSIMpro, un logiciel d'émulation graphique de réseaux quantiques. La société a été lancée en janvier 2023.

IQM (Finlande) avait un stand. On se demande à quoi cela rime au CES !

QuiX Quantum (Pays Bas) était également présente.

Usages

La branche **CACIB** du Crédit Agricole publiait avec Pasqal et Multiverse un préprint concernant un cas d'usage de credit scoring à base de simulation quantique. Il s'agit d'un algorithme hybride de type QBoost qui permet de prédire les « fallen angels », des entreprises qui ne pourraient pas rembourser leurs emprunts. Ils utilisent un jeu de données d'entraînement étalé sur 20 ans et comprenant 90 000 instances comprenant 150 features basés sur 2000 sociétés de 10 secteurs et 100 sous-secteurs d'activité différents provenant de 70 pays. Le jeu de données était réparti en 65 000 éléments de 2001-2016 pour l'entraînement et 26 000 de 2016-2020 pour les tests. La partie quantique de l'algorithme est réduite à un problème QUBO et utilise un échantillonnage de graphes. Le papier indique qu'un avantage quantique pourrait être obtenu avec de 150 à 342 atomes neutres en comparaison avec des réseaux de tenseurs classiques. Il faudrait disposer de 2800 atomes neutres pour pouvoir mettre en œuvre la méthode de subsampling qui est plus précise.

Tout ceci est plutôt indicateur d'un avantage quantique envisageable plus tôt avec la simulation quantique à base d'atomes neutres qu'avec du NISQ gate-based. Cette étude de cas ne correspond cependant pas aux cas

d'usage les plus exigeants de CACIB qui demanderaient de leur côté plutôt des QPU de type FTQC avec des milliers de qubits logiques, comme pour faire de l'optimisation de portefeuilles d'investissements.

Source : **Financial Risk Management on a Neutral Atom Quantum Processor** by Lucas Leclerc et al, CACIB, Multiverse, IOGS and Pasqal, December 2022 (17 pages).

Brevets quantiques en Chine

La Chine dépose de plus en **plus de brevets** sur les technologies quantiques, avec une multiplication par 5,8 en deux ans des brevets déposés (804 vs 137). Dans le même temps, dans le **top 100 des entreprises**, IBM, Google, D-Wave et Microsoft ont respectivement déposé 1323, 762, 501 et 496 brevets. Les principaux déposants chinois sont Tencent (93 brevets) et Origin Quantum (234 brevets) puis Baidu, Huawei et Alibaba. Atos arrive en 22ieme position dans le classement avec 55 brevets.

A noter également que j'ai enfin trouvé une **source Chinoise** invalidant les chiffres énormes de $10B à $15B d'investissement dans le quantique. La réalité est inférieure à $4B (sur 5 ans). Et cela vient d'un chercheur qui travaille directement avec Jian-Wei Pan, le "czar" chinois sur quantique.

Mieux que Shor ?

Un papier chinois publié juste avant Noël 2022 présentait un record de factorisation de nombre entier réalisé par un ordinateur quantique gate-based avec une clé de 48 bits (261980999226229) factorisée avec 10 qubits supraconducteurs. Le plus étonnant est une estimation selon laquelle leur algorithme nécessiterait seulement 372 qubits physiques pour factoriser une clé RSA 2048. Moins que ceux du dernier processeur d'IBM à 433 qubits. Alors, la menace quantique se rapproche côté cybersécurité ?

L'algorithme s'appuie sur l'algorithme Classique de Schnorr qui utilise des « lattice reductions » et une méthode hybride QAOA. Le nombre de qubits nécessaire serait de 2N/log(N), N étant la taille de la clé RSA à factoriser en nombre de bits ce qui donne une ressource « sous-linéaire ». La profondeur de circuit nécessaire est comprise entre 1118 et 1490 selon la connectivité des qubits.

arXiv > quant-ph > arXiv:2212.12372

Search... Help | Advanced

Quantum Physics

[Submitted on 23 Dec 2022]

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, Lan Luo, Qianheng Duan, Yiting Liu, Wenhao Shi, Yangyang Fei, Xiangdong Meng, Yu Han, Zheng Shan, Jiachen Chen, Xuhao Zhu, Chuanyu Zhang, Feitong Jin, Hekang Li, Chao Song, Zhen Wang, Zhi Ma, H. Wang, Gui-Lu Long

Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is O(logN/loglog N), which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.

Comments: 32 pages, 12 figures
Subjects: **Quantum Physics (quant-ph)**
Cite as: arXiv:2212.12372 **[quant-ph]**
(or arXiv:2212.12372v1 **[quant-ph]** for this version)
https://doi.org/10.48550/arXiv.2212.12372

Alors, la menace s'approche de voir la sécurité d'Internet se casser la figure ?

Et bien NON ! Et pour trois raisons :

- Le papier ne fournit aucune évaluation du temps de calcul de l'algorithme exécuté sur une clé RSA 2048 bits. Il n'indique pas le nombre de fois que le calcul quantique doit être répété. Bref on a un "space advantage" (nombre de qubit) mais on est dans le brouillard sur le « time advantage » (temps de calcul).

- Il manque des informations dans le papier comme les fidélités qui seraient attendues des qubits physiques.

  En apparence, il faudrait qu'elle soit de l'ordre de 10^{-6}, ce qui nécessiterait de mettre en œuvre de la correction d'erreur, et donc, d'augmenter significativement le nombre de qubits physiques nécessaires à hauteur de plusieurs centaines de milliers de qubits.

- L'algorithme QAOA utilisé dans la partie quantique ne scale pas bien, comme l'indique **Scott Aaronson** quit démolit brutalement le papier avec un laconique "No. Just No!".

Le papier d'origine : **Factoring integers with sublinear resources on a superconducting quantum processor** by Bao Yan et al, December 2022 (32 pages).

La suite au prochain épisode !

Cet article a été publié le 9 janvier 2023 et édité en PDF le 15 mars 2024.
(cc) Olivier Ezratty – "Opinions Libres" – **https://www.oezratty.net**