Opinions Libres
le blog d'Olivier Ezratty

Decode Quantum avec Nicolas Sangouard du CEA

Dans ce 60e épisode des entretiens Decode Quantum, Fanny Bouton et moi-même recevions Nicolas Sangouard qui est chercheur au CEA. Il est aussi diffusé sur **Frenchweb**.

Nicolas Sangouard est physicien-chercheur au CEA à Saclay. Depuis quelques années, il travaille à l'Institut de Physique Théorique qui est un laboratoire commun du CEA et du CNRS. Auparavant, il faisait ses recherches à l'Université de Genève avec Nicolas Gisin puis à l'Université de Bâle, après avoir été post-doc en Allemagne à l'Université de Kaiserslautern puis Maître de conférence à l'Université Paris Cité. Il est spécialiste de l'optique et de l'information quantique et participe notamment aux développements des communications quantiques et du calcul quantique. Il a couvert et couvre un champ de recherche très large dans la photonique et la physique atomique et l'optomécanique. Il s'intéresse notamment aux réseaux quantiques, à leurs briques élémentaires comme les mémoires quantiques, à leur architecture, au moyen de vérifier leur fonctionnement et à leurs applications pour le calcul quantique distribué et la distribution quantique de clés. Il est notamment le coauteur de papiers qui ont fait du bruit récemment concernant l'estimation et l'optimisation de ressources permettant de casser des clés RSA avec des ordinateurs quantiques du futur.

Voici comme d'habitude une transcription approximative de la discussion avec les liens utiles associés.

- La question habituelle de la "marmite du quantique". L'intérêt de Nicolas Sangouard pour la physique quantique est né de rencontres et lectures. Il insiste beaucoup sur la confiance transmise par ses parents alors qu'il était initialement un élève médiocre. Il avait eu des difficultés dans l'apprentissage de la lecture.

Il est rapidement tombé dans la case des élèves en qui les enseignants ne croyaient pas au lycée et à qui il était recommandé de faire des études techniques. Mais la confiance de ses parents d'origine modeste a beaucoup compté dans les renforcements positifs. Il a ensuite suivi un cursus scientifique, en commençant l'Université par l'étude des mathématiques. Il est tombé sur un livre de vulgarisation de la physique quantique en seconde année, de Jean-Pierre Pharabod et Sven Ortoli ("Le cantique des quantiques", La découverte, poche 47, 1998). Ce livre et d'autres lectures l'ont convaincu de quitter les mathématiques pour faire une licence de physique. Son premier cours de physique quantique lui a été donné par Hans Rudolf Jauslin, Professeur à l'Université de Bourgogne, qui deviendra son co-directeur de thèse. Le message maintenant qu'il est devenu parent : il faut faire confiance à ses enfants !

- Sa thèse soutenue en 2004 à Dijon. Il s'agissait de la problématique du contrôle cohérent et des interactions entre atomes et lasers. Il a notamment utilisé ces outils pour créer des portes quantiques universelles robustes à certaines imperfections expérimentales. Il était fasciné par l'existence de groupes expérimentaux qui piégeaient et refroidissaient des atomes uniques et manipulaient des photons uniques. Il a toujours été théoricien mais s'intéresse particulièrement à la physique théorique qui accompagne la physique expérimentale.

Préparation de superpositions cohérentes et contrôle d'états quantiques instables sous la direction de Stéphane Guérin et de Hans Rudolf Jauslin.

- En sortant d'un laboratoire qui n'a pas le rayonnement des plus grand laboratoires parisiens, il n'était pas évident de trouver un post-doc. Il a alors décroché un poste en Allemagne dans le laboratoire de Michael Fleischhauer sur le stockage de photons dans des ensembles d'atomes. Il y est resté une année et a ensuite rejoint le groupe de Nicolas Gisin en Suisse qui est une sommité. Il a eu du mal à le convaincre de l'embaucher au début. Il a même dû trouver lui-même un bout de la source de financement publique de son salaire. Il a surtout travaillé sur des solutions pour réaliser des protocoles de cryptographie quantique sur de longues distances. Il a notamment contribué au développement de mémoires quantiques et réseaux quantiques avec Christophe Simon et d'autres scientifiques de renom. Nicolas Gisin avait par ailleurs cofondé ID Quantique quelques années avant. A noter que pour lever leur premier million, ils ont attendu trois ans. C'était l'une des premières startups de la seconde révolution quantique avec MagiQ.

- Il a ensuite obtenu un poste permanent à l'université Paris Diderot (maintenant Paris Cité) comme Maitre de conférences dans le laboratoire MPQ. Du fait d'un système de financement complexe de la recherche, il n'y est resté qu'une année puis est retourné à Genève comme post-doc puis chercheur.

- S'ensuit un passage par Bâle pour monter un groupe de recherche, dans le Département de Physique théorique et avec bourse suisse (FNS). Il s'y est intéressé à la question de la pertinence de la théorie quantique à l'échelle macroscopique en montrant notamment qu'il est nécessaire d'avoir des détecteurs de résolution de plus en plus fine pour détecter des effets quantiques dans des systèmes de plus en plus grands. Dans ce cadre, il a travaillé avec des BECs (condensats de Bose Einstein) pour montrer des corrélations quantiques fortes avec plusieurs centaines d'atomes. Il a aussi proposé avec d'autres chercheurs une méthode permettant de détecter des états quantiques intriqués de photons à l'œil nu en 2016/2017. Il faudrait 10 heures de patience pour y arriver. C'est possible théoriquement mais n'a jamais réalisé. Il a alors rencontré des réactions enthousiastes comme celle de Peter Zoller et d'autres qui, a contrario, trouvaient que ce n'était pas de la belle physique. Le groupe d'Anton Zeilinger en Autriche s'y intéressait.

Bell correlations in a Bose-Einstein condensate par R. Schmied et al , Avril 2016 (20 pages)

Proposal for witnessing non-classical light with the human eye par A. Dodel, Nicolas Sangouard et al, Avril 2017 (9 pages)

What does it take to see entanglement? par Valentina Caprara Vivoli, Pavel Sekatski et Nicolas Sangouard, Février 2016 (7 pages).

- Nous évoquons ensuite le rôle de l'IPHT où il est actuellement. C'est un laboratoire conjoint du CEA et du CNRS. Il dirige un groupe de recherche en information quantique conjointement avec Jean Daniel Bancal. Ce laboratoire de théoriciens est situé juste à côté du groupe SPEC qui comprend plutôt des expérimentateurs, comme **Denis Vion** que nous avons déjà accueilli dans ces entretiens. Il est sur le site de l'Orme des Merisiers à Saclay juste à côté du synchrotron de lumière Soleil.

- Nous évoquons alors le thème des mémoires quantiques. L'une des applications est la réalisation de réseaux quantiques. Le défi est de s'affranchir des pertes sur les fibres optiques à longue distance pour le partage d'intrications à longue distance. A partir de quelques propositions théoriques initiales, l'objectif des premiers travaux étaient d'évaluer la faisabilité de ces réseaux.

- Il a alors travaillé sur des répéteurs quantiques à base d'ions piégés. Les ensembles d'atomes neutres ne permettent pas un traitement déterministe de l'information. Les ions piégés permettent d'éviter les effets néfastes probabilistes. Il a fait des propositions théoriques sur la réalisation de réseaux quantiques avec ces ions piégés dès 2008-2009. C'est un important sujet à Innsbruck. Le travail de Tracy Northrup et Ben Lanyon dans cette université a récemment permis de réaliser plusieurs ingrédients des réseaux proposés en 2008-2009. Des expériences d'intrication longue distance ont permis par exemple d'intriquer des ions piégés à quelques centaines de mètres.

Entanglement of trapped-ion qubits separated by 230 meters by V. Krutyanskiy, N. Sangouard, Tracy. E. Northup et al, August 2022 (22 pages).

A telecom-wavelength quantum repeater node based on a trapped-ion processor par Victor Krutyanskiy, Nicolas Sangouard, Ben P. Lanyon, et al, Février 2023 (5 pages).

- Nous évoquons la distribution de clés quantiques à base d'intrication et leur lien avec le travail d'Artur Ekert. Il y a une différence fondamentale entre les deux modèles de distribution de clés quantiques (sans et avec intrication).

- Il nous explique la notion de "device independence" dans la QKD utilisant de l'intrication. On vérifie la notion de résultats corrélés mais non prédictibles pour générer des clés grâce à un test de Bell. Cette notion de « device indépendance » s'applique aussi aux QRNG à base d'intrications.

Experimental quantum key distribution certified by Bell's theorem par D.P. Nadlinger et al, Septembre 2021 (43 pages).

- Nous terminons cet entretien en discutant de ses travaux réalisés avec son post-doc Elie Gouzien (qui avait fait sa thèse sous la direction de Sébastien Tanzilli et Virginia d'Auria Nice) sur l'optimisation des ressources de calcul quantique, notamment pour casser des clés RSA 2048.

- Le sujet est né de discussions avec le groupe de Daniel Esteve, essentiellement avec Patrice Bertet du

SPEC. Ils travaillent sur des qubits supraconducteurs couplés à des mémoires de spin en cavité. L'idée consiste à stocker l'information dans la mémoire quantique et à réaliser les opérations de calcul à l'aide d'un petit processeur (2 qubits logiques et 13K qubits physiques). Par certains côtés, cette architecture de système quantique est "classical inspired", par opposition aux algorithmes classiques qui sont "quantum inspired".

Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory par Élie Gouzien et Nicolas Sangouard, March-Septembre 2021 (18 pages).

- Il faudrait 350K qubits de chat pour casser une clé RSA 2048 bits au lieu de 22 millions de qubits transmon d'après le papier de Craig Gidney de Google datant de 2019. Nicolas avait aussi évalué la résistance de protocoles à base de courbes elliptiques liée à la protection du Bitcoin et qui sont théoriquement cassables par l'autre version de l'algorithme de Peter Shor. C'est ce à quoi correspondent les 126 133 qubits du papier.

Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126133 Cat Qubits par Élie Gouzien, Diego Ruiz, Francois-Marie Le Régent, Jérémie Guillaud, Nicolas Sangouard, Février 2023 (38 pages).

Nicolas pense que tout cela pourrait être possible d'ici une dizaine d'année. Il est résolument du côté des optimistes !

Cet article a été publié le 21 juin 2023 et édité en PDF le 22 mars 2024.