Pour le physicien, les mémoires quantiques sont vraiment fascinantes. Il est étonnant de pouvoir manipuler l'état quantique de photons uniques avec une telle précision. Par ailleurs, par l'échange de photons, il est possible d'intriquer des mémoires quantiques, des objets macroscopiques qui, à terme, seront à une centaine de kilomètres l'un de l'autre !

Pour les communications à longue distance, qu'en est-il de l'approche consistant à utiliser des satellites ?

Dans ce domaine, la Chine a une longueur d'avance. Elle n'hésite pas à prendre des risques, à investir et à mettre à disposition de ses chercheurs des moyens extraordinaires. Elle a ainsi rattrapé et dépassé les pays occidentaux. L'Europe commence seulement à réagir à cette concurrence. Il faut aussi souligner une différence cruciale de stratégie. L'État chinois est le premier client de ces développements, il soutient activement leur développement. En Europe, on demande au secteur privé d'être porteur. Mais les investissements sont encore lourds et les entreprises restent un peu frileuses. Historiquement, il faut rappeler que le succès phénoménal de l'internet classique n'a été possible que grâce à l'investissement des États et des entreprises nationales. Depuis, tous les grands opérateurs téléphoniques ont été privatisés…

Pour revenir à la Chine, en 2016, ce pays a mis en orbite le satellite *Micius*, dans le cadre de la mission scientifique *Quess*, sous la direction de Jian-Wei Pan, de l'Académie chinoise des sciences. En 2017, le satellite a servi de nœud de confiance dans une communication chiffrée entre Vienne, où Jian-Wei Pan a fait son doctorat, et Pékin.

Le satellite peut-il réaliser une distribution quantique de clé ?

Oui. En 2020, *Micius* a envoyé des paires de photons intriqués à deux stations en Chine, à Nanshan et Delingha, distantes de 1120 kilomètres l'une de l'autre. Les chercheurs chinois ont ainsi battu le record de distance pour une distribution quantique de clé sans nœud de confiance.

On peut aussi imaginer d'utiliser le satellite comme un répéteur quantique, mais il y a une contrainte importante : le satellite doit voir en même temps les deux stations au sol. Or un satellite comme *Micius* se situe en orbite basse, à moins de 600 kilomètres d'altitude ; son horizon est donc limité. Pour une communication entre les États-Unis et l'Europe par exemple, il faudrait une mémoire quantique capable de retenir un photon pendant plusieurs dizaines de minutes, voire une heure !

En outre, pour l'instant, cette technique est loin d'être parfaite. Les photons sont absorbés en grand nombre par l'atmosphère. Même dans l'expérience de 2020, alors que le satellite produisait 6 millions de paires intriquées par seconde, le flux d'information n'était que de 0,12 bit par seconde. L'équipe de Jian-Wei Pan travaille au développement de sources plus intenses pour compenser ce débit très faible. D'autres pays sont aussi dans la course pour développer des satellites de communication quantique. Et des entreprises privées envisagent aussi des constellations de satellites opérant comme des nœuds de confiance.

Que manque-t-il encore pour construire l'internet quantique ?

Il ne faut pas négliger l'aspect logiciel. Il faudra mettre en place des protocoles capables de gérer les flux de données, de les envoyer au bon endroit, transmettre les informations des couches physiques aux applications, etc.

Le succès de l'internet classique vient en partie de l'uniformisation des protocoles. Aujourd'hui, chaque laboratoire et chaque entreprise a développé ses propres méthodes de communication quantique. L'Union internationale des télécommunications, sous l'égide des Nations unies, la Commission européenne (avec un consortium d'entreprises et d'instituts de recherche) et d'autres commencent à travailler sur le cas des communications et de l'internet quantique pour que tout le monde parle le même langage.

En dehors de la sécurité des communications, que peut-on attendre d'autre de l'internet quantique ?

L'internet quantique est un défi technique incroyable. Il est aussi, pour le physicien, un problème fascinant qui soulève des questions conceptuelles nouvelles (*voir l'article pages 28 à 38*). Il suscite également des attentes importantes concernant les ordinateurs quantiques. En téléportant l'information d'un ordinateur quantique à l'autre, l'internet quantique nous permettra d'exploiter pleinement l'association de ces machines pour décupler leur puissance.

Parmi les promesses des ordinateurs quantiques, si l'on parvient à manipuler assez de qubits, il sera possible de simuler des molécules complexes afin de développer de nouveaux médicaments ou des matériaux innovants. L'un des grands défis de l'humanité est la production d'énergie. Pour l'instant, nous n'arrivons pas à exploiter la lumière du soleil avec autant d'efficacité que la nature. Peut-être qu'avec les ordinateurs quantiques reliés par l'internet quantique, il sera possible de percer les secrets de la photosynthèse et d'améliorer les rendements des panneaux solaires. On en est encore loin, mais cet exemple montre que les enjeux sont énormes.

Propos recueillis par Sean Bailly

à lire

THEMA
L'ordinateur quantique. Promesses et réalité

Quel est le principe des ordinateurs quantiques ? Quelles performances en attend-on ? Quels sont leurs enjeux ? Comment va-t-on les réaliser ? Le point dans ce n° 18 de la collection « Thema »

En vente sur notre site uniquement :
boutique.pourlascience.fr

BIBLIOGRAPHIE

J. Yin *et al.*, **Entanglement-based secure quantum cryptography over 1,120 kilometres,** *Nature*, vol. 582, pp. 501-505, 2020.

S. Wehner *et al.*, **Quantum internet : a vision for the road ahead,** *Science*, vol. 362, article eaam9288, 2018.

M. Afzelius, N. Gisin et H. de Riedmatten, **Quantum memory for photons,** *Physics Today*, vol. 68, pp. 42-47, décembre 2015.

N. Gisin, **L'impensable hasard,** Odile Jacob, 2012.

H. J. Kimble, **The quantum internet,** *Nature*, vol. 453, pp. 1023-1030, 2008.

L'ESSENTIEL

> Selon le principe de localité, toute information ou influence se propage continûment à une vitesse inférieure ou égale à celle de la lumière. La physique quantique s'est révélée incompatible avec ce principe.

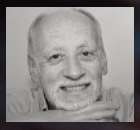
> Dans l'expérience GHZ consistant à mesurer l'état de photons issus d'une source unique, on a montré que les corrélations entre les résultats obtenus ne peuvent s'expliquer en préservant le principe de localité.

> Un futur internet quantique mettra en œuvre de nombreuses sources indépendantes de photons, ce qui amène à étudier la non-localité dans un réseau formé de plusieurs sources.

> Les physiciens étudient les scénarios les plus simples avec deux ou trois sources, des systèmes déjà complexes à analyser.

LES AUTEURS

MARC-OLIVIER RENOU
postdoctorant à l'institut des sciences photoniques de Barcelone



NICOLAS GISIN
professeur à l'université de Genève et à l'institut de technologie de Schaffhausen, à Genève

NICOLAS BRUNNER
professeur à l'université de Genève

La non-localité quantique à l'ère des réseaux

Les lois de la physique quantique semblent incompatibles avec le principe de localité, selon lequel deux objets distants ne peuvent pas s'influencer instantanément. Assez bien comprise pour des photons émis par une source unique, cette non-localité reste à cerner dans le cas d'un internet quantique, réseau où de nombreuses sources indépendantes de photons seront à l'œuvre.

Aujourd'hui, une partie sensible de nos vies circule sur internet : nos données bancaires ou médicales, nos courriers électroniques, nos messages sur les réseaux sociaux, nos photos, etc. Pour garantir une transmission sécurisée de ces informations sans qu'elles soient volées, lues ou altérées, des techniques de chiffrement ont été développées. Elles s'appuient sur des problèmes mathématiques qui, sans la clé de déchiffrement, ne sont pas résolus en un temps raisonnable par des ordinateurs classiques. Par exemple, certains algorithmes reposent sur le fait que la décomposition en facteurs premiers de très grands nombres entiers est un tel problème.

Cependant, le développement d'ordinateurs quantiques à l'horizon de quelques années pourrait rendre obsolètes ces techniques de chiffrement. Des algorithmes, qualifiés de quantiques, exploiteraient toute la puissance de la physique quantique afin de résoudre rapidement des problèmes inaccessibles à leurs concurrents classiques. C'est le cas de l'algorithme proposé en 1994 par le mathématicien américain Peter Shor, qui est en théorie capable de factoriser très vite de très grands nombres entiers. Ainsi, quand les ordinateurs quantiques auront été mis au point, les transmissions de coordonnées bancaires lors d'achats en ligne ne seront plus à l'abri d'une attaque. Quelles seront alors les solutions ? Les phénomènes quantiques, à l'origine des capacités de déchiffrement de