La distribution quantique de clé est l'une des applications les plus simples de la communication quantique, et elle pourrait être disponible dès cette année sur le réseau de démonstration que vous construisez. Quelles applications plus lointaines peut-on imaginer ?

Stephanie Wehner : De nouvelles formes d'informatique à distance deviendront possibles. Supposez que vous avez un concept de matériau breveté dont vous aimeriez tester les propriétés dans une simulation. Pour ce faire, un ordinateur quantique sera bien meilleur qu'un ordinateur classique. Mais tout le monde n'aura pas un ordinateur quantique dans son salon dans un futur proche – et probablement même pas de notre vivant.

Une solution serait de m'envoyer votre concept et que j'exécute les simulations sur l'ordinateur quantique du laboratoire. Promis, je vous enverrai les résultats, mais je dispose désormais de toutes les informations sur votre invention. Grâce au réseau quantique, vous pourriez de chez vous utiliser un appareil quantique très simple – en fait, il peut ne faire qu'un qubit à la fois – et transférer les qubits de votre appareil jusqu'à mon ordinateur quantique plus puissant. Il fera alors tourner les simulations sans rien livrer des caractéristiques de votre nouveau matériau. Vous serez tranquillisée grâce au réseau quantique.

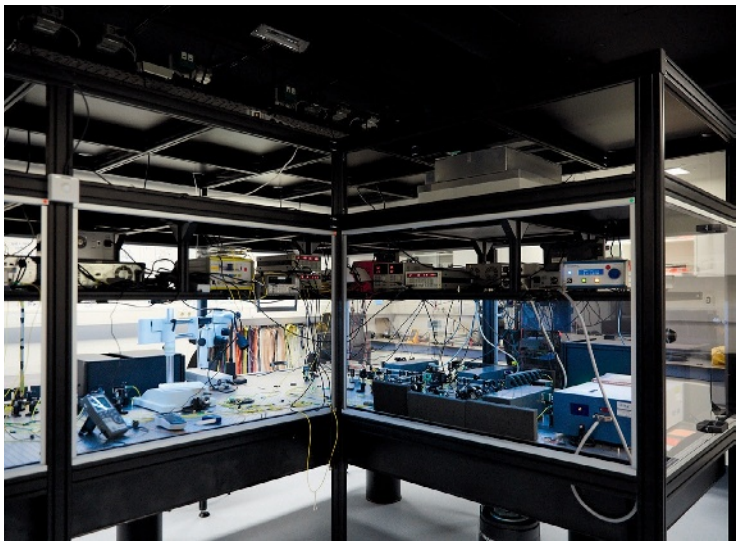
Pour donner un autre exemple, on a aussi montré que l'intrication rend plus précise la synchronisation de deux horloges situées en deux endroits différents. Un tel résultat aura de nombreuses applications, par exemple en géolocalisation.

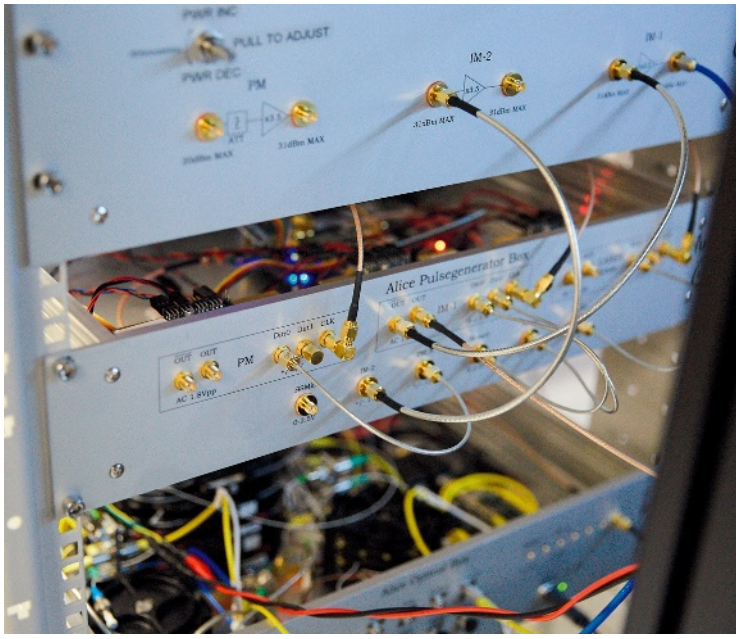
Un internet quantique aiderait aussi à créer un meilleur télescope, en combinant plusieurs télescopes séparés. Les états des particules de lumière captées par un premier télescope seraient téléportés, grâce à l'intrication quantique, vers un second télescope, où ils seraient combinés à ceux de ses photons perçus.

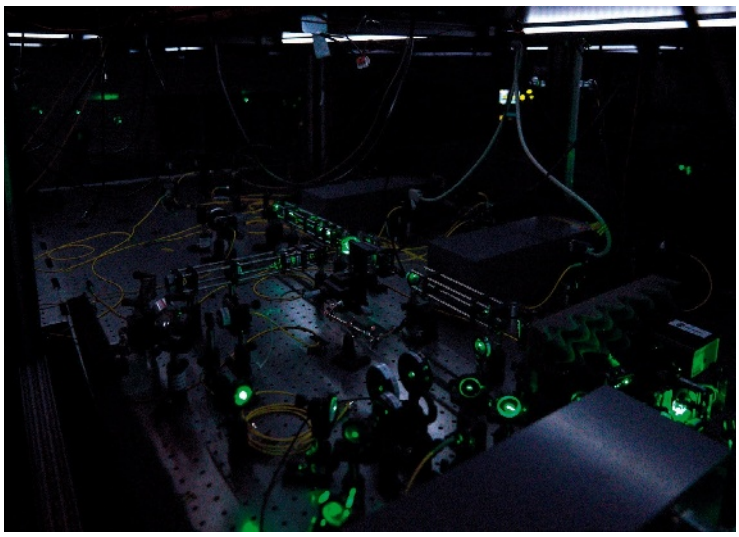
Vous travaillez aussi sur la simulation du futur internet quantique. Pourquoi est-ce nécessaire ?

Stephanie Wehner : Avec la plateforme de simulation très performante que nous avons construite et qui est désormais installée dans un supercalculateur, nous pouvons explorer différentes configurations du réseau quantique et comprendre des propriétés autrement plus difficiles à prédire par des méthodes analytiques classiques. De cette façon, nous espérons mettre au point un concept modulable qui puisse permettre les communications quantiques à travers toute l'Europe.

L'aspect imprédictible des réseaux m'a toujours fascinée. Les ordinateurs sont intéressants, mais ce qui m'importe vraiment, c'est la >







Un laboratoire à l'institut de technologie de Delft, aux Pays-Bas, abrite un cristal spécial, une mémoire quantique servant de nœud de réseau pour la communication quantique à longue distance.

© Julia Gunther pour Quanta Magazine

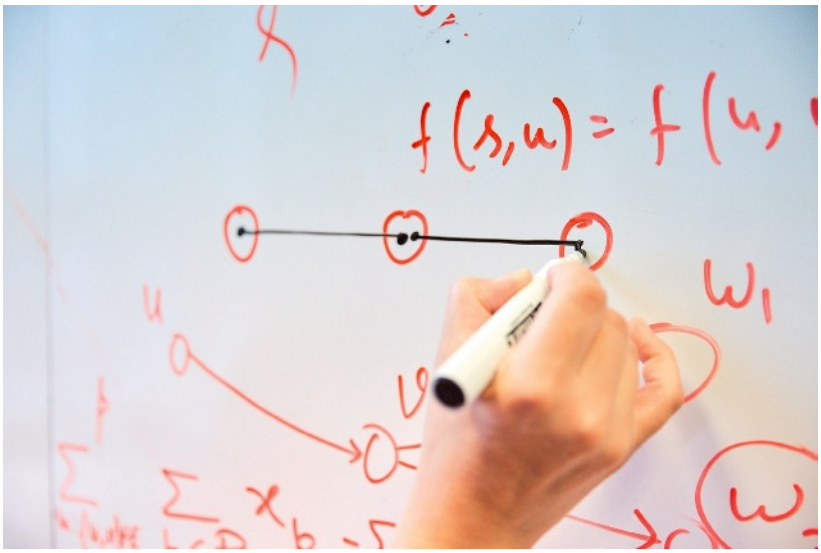
transmission de données d'un point à un autre. C'est pour cette raison que je me suis lancée dans le piratage puis intéressée à l'internet classique. Fondamentalement, comprendre ce qui se passe dans un réseau est très difficile, en raison du nombre important de facteurs non caractérisés. Par exemple, quand vous envoyez un message, vous ne pouvez pas prédire exactement au bout de combien de temps il parviendra au destinataire. Le message peut se perdre, un ordinateur planter, être trop lent, voire corrompre les données. Le protocole de transmission peut se heurter à une vieille version d'un logiciel, une nouvelle version ou une version maligne.

Étiez-vous une méchante pirate avant de devenir une corsaire ?
Stephanie Wehner : Ce n'est pas le genre de révélation que l'on peut faire en public ! Je pense juste qu'à l'époque le monde était un endroit plus sympathique qu'aujourd'hui. Voilà tout…

Pourquoi avez-vous décidé d'arrêter le piratage et de devenir une scientifique ?
Stephanie Wehner : Je sais que le piratage semble très excitant, mais je pratiquais cette activité depuis un certain temps. Bien sûr, on peut améliorer ses méthodes, mais cela reste toujours un peu la même chose. J'ai fini par m'ennuyer et j'ai décidé de me lancer dans une nouvelle aventure. Puis, j'ai découvert la théorie de l'information quantique qui m'a immédiatement fascinée.

L'un des théorèmes que vous avez prouvés sur l'information quantique est le théorème du stockage avec bruit. De quoi s'agit-il ? Et quelles en sont les implications pour la communication quantique ?
Stephanie Wehner : Le stockage avec bruit concerne la cryptographie, avec une hypothèse physique. Dans le monde de l'informatique classique, on formule souvent une hypothèse de départ. Par exemple, on part du principe qu'il est difficile de déterminer les facteurs premiers de grands nombres, et si cette supposition est vraie, alors mon protocole est sûr. Ces preuves de sécurité sont bonnes et elles sont utilisées partout aujourd'hui, mais il ne faut pas oublier qu'elles peuvent être invalidées plus tard.

Demain, ou plus tard, quelqu'un peut inventer une méthode intelligente pour résoudre le problème informatique sur lequel votre sécurité se fonde : elle devient immédiatement obsolète, et de façon rétroactive. Par exemple, grâce à l'algorithme développé par le mathématicien américain Peter Shor, des ordinateurs quantiques factoriseront aisément de grands nombres et réduiront à néant l'efficacité des méthodes de sécurité actuelles fondées sur la factorisation. Quelqu'un enregistrant votre message aujourd'hui pourra le décrypter plus tard.



Les nœuds d'un futur réseau quantique, de la main de Stephanie Wehner.

QUELQU'UN ENREGISTRANT VOTRE MESSAGE SÉCURISÉ AUJOURD'HUI POURRA LE DÉCRYPTER PLUS TARD

Les travaux sur le stockage avec bruit posent la question : peut-on formuler une hypothèse physique qui ne peut pas être rétroactivement rendue caduque ? L'hypothèse physique est ici qu'il est difficile de stocker beaucoup d'états quantiques sans bruit, ce qui n'a besoin d'être vrai que pour un tout petit délai. En partant du principe que, maintenant, vous ne pouvez stocker que jusqu'à un million de qubits avec bruit, je peux modifier les paramètres du protocole de transmission pour augmenter la sécurité en envoyant plus d'informations que n'en peut capturer ce million de qubits. C'est efficace, parce que, si demain vous achetez de la mémoire quantique à hauteur de 2 millions de qubits, il sera trop tard, l'information aura déjà été envoyée de façon sécurisée.

Sur la base de cette idée, toutes sortes de protocoles de communication quantique sont envisageables. Supposons que deux personnes veuillent comparer leur mot de passe sans jamais le révéler. C'est complètement différent de ce que nous faisons aujourd'hui, lorsque nous saisissons notre code à quatre chiffres sur le clavier d'un distributeur de billets. À la place, nous entrerons notre code secret dans notre propre appareil, et il ne sera jamais révélé au distributeur, qui néanmoins nous donnera les billets demandés. Ce protocole devient possible avec l'hypothèse du stockage avec bruit.

La quête de cet internet quantique pourrait-elle nous permettre d'approfondir nos connaissances sur les lois de la nature ?
Stephanie Wehner : En science, on distingue parfois des questions dites « fondamentales »

© Julia Gunther pour Quanta Magazine