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…

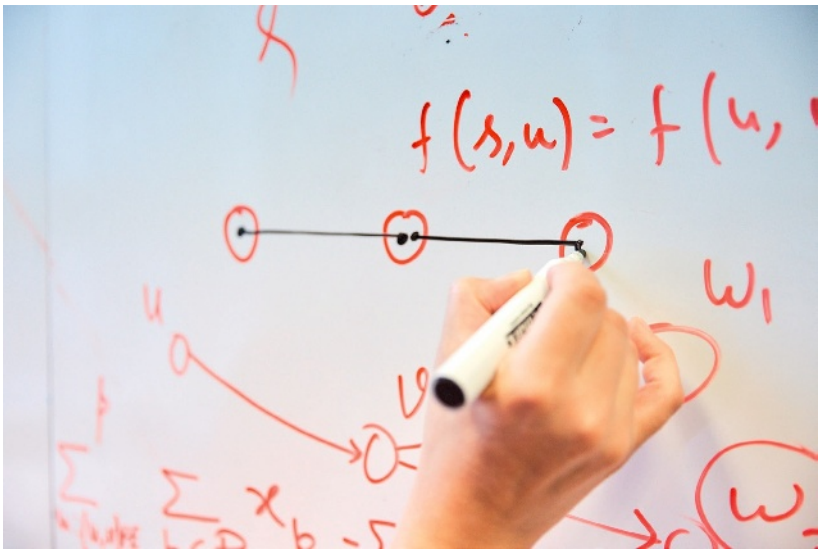
Pourquoi avez-vous décidé d'arrêter le piratage et de devenir une scientifique ?

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

et d'autres plutôt « pratiques », et donc banales. Je pense qu'apporter au monde réel quelque chose d'utilisable par tout le monde n'est jamais banal. C'est extrêmement difficile. Il y a un bond de géant entre : « J'ai une idée géniale, par exemple un écran tactile, discutons-en sur le tableau blanc » et le smartphone que j'utilise actuellement. Avec l'internet quantique, nous sommes dans la même situation, nous essayons de le construire en partant de rien.

Nous partons d'une expérience préliminaire en laboratoire pour essayer de mettre en place un système étendu à tous les Pays-Bas, fonctionnant à distance et utilisable par des individus, qui, à terme, n'auront pas besoin de s'y connaître en physique pour le faire. Si une partie du système existait déjà, nous pourrions simplement dire « améliorons-la ». Mais créer *ex nihilo* est une autre affaire. Passer de rien à une première version est très long.

En faisant cela, je pense que nous accéderons à une compréhension plus fondamentale dans plusieurs domaines. Nous en apprendrons plus sur la physique en rendant possibles ces réseaux parce que, actuellement, nous ne savons pas exactement comment le faire. Nous testons encore différents types de nœuds et de répéteurs quantiques, des appareils qui relaient l'intrication sur de plus grandes distances. Et, dans le domaine des sciences informatiques, nous découvrirons de nouvelles façons de programmer et contrôler de tels réseaux grâce aux différences fondamentales qui existent entre les communications quantique et classique.

Mais je pense aussi que nous obtiendrons des informations sur les processus créatifs et la sociologie en suivant la façon dont les usagers s'empareront de ces nouveaux réseaux. Souvenez-vous des débuts de l'internet classique, la plupart pensaient qu'il ne servirait qu'à envoyer des fichiers un peu partout. Mais la société a fait preuve de bien plus d'imagination !

Il est difficile de définir un calendrier, mais espérez-vous voir de votre vivant cet internet quantique ?

Stephanie Wehner : Je suis assez optimiste à ce propos, je pense que oui. ■

BIBLIOGRAPHIE

G. MURTA *ET AL.*, Towards a realization of device-independent quantum key distribution, *Quantum Physics*, 2019. https://arxiv.org/abs/1811.07983

S. WEHNER *ET AL.*, Quantum internet: A vision for the road ahead, *Science*, vol. 362(6412), eaam9288, 2018.

D. CASTELVECCHI, The quantum internet has arrived (and it hasn't), *Nature*, vol. 554(7692), pp. 289-292, 2018.

S. WEHNER *ET AL.*, Cryptography from Noisy Storage, *Phys. Rev. Lett.*, vol. 100, 220502, 2008.