La première étape est en cours, elle consiste en la construction d'un réseau quantique de démonstration qui connectera quatre villes aux Pays-Bas, une sorte d'analogue quantique de l'Arpanet. Tracy Northup, de l'université d'Innsbruck et membre de la *Quantum Internet Alliance* loue « l'ampleur de la vision de Stephanie et son engagement pour construire le genre de structure nécessaire à la réalisation d'un tel projet. »

Après le piratage, Stephanie Wehner est allée à l'université pour étudier l'informatique et la physique. À Leyde, elle a entendu le théoricien de l'information quantique John Preskill donner une conférence, durant laquelle il décrivait les avantages des bits quantiques pour communiquer. Quelques années plus tard, après avoir son doctorat, elle a abandonné les bits classiques et rejoint le groupe de John Preskill à l'institut de technologie de Californie (Caltech), aux États-Unis, pour un postdoctorat.

Là, en plus d'avoir démontré plusieurs théorèmes notables sur l'information quantique, la cryptographie quantique et la nature de la mécanique quantique elle-même, Stephanie Wehner s'est naturellement imposée comme une « meneuse naturelle », raconte John Preskill ; elle « était souvent le lien qui unissait les gens ». En 2014, après avoir occupé un poste de professeuse à Singapour, elle a déménagé à Delft, où elle a commencé à collaborer avec des expérimentateurs pour poser les fondations de l'internet quantique.

Afin d'en savoir plus, nous avons rencontré Stephanie Wehner en août 2019.

« Nous travaillons à un réseau quantique à travers toute l'Europe »

L'internet quantique est un réseau de transmission de qubits entre deux lieux distants. Pourquoi en a-t-on besoin ?

Stephanie Wehner : L'idée n'est pas de remplacer l'internet que nous utilisons tous aujourd'hui, mais plutôt d'y ajouter des fonctionnalités nouvelles et spéciales. Les réseaux quantiques ont toutes sortes d'applications encore à imaginer, mais nous en connaissons déjà un certain nombre. Bien sûr, la plus célèbre est la communication sécurisée : le fait que l'on puisse utiliser la communication quantique pour distribuer des clés quantiques de cryptographie, garantissant la sécurité, même si l'attaquant est équipé d'un ordinateur quantique. Or une telle machine pourrait vaincre de nombreux protocoles de sécurité existant aujourd'hui.

Qu'est-ce qui rend ces clés quantiques si sûres ?

Stephanie Wehner : Une bonne manière de comprendre ce que l'internet quantique peut faire est de penser à « l'intrication quantique » (*voir Pas d'échappatoire pour l'intrication, par R. Hanson, page 26*), une propriété qui unit deux bits quantiques. La première propriété de l'intrication est sa « coordination maximale » : si j'avais un bit quantique ici, à Delft, et un autre à New York, j'utiliserais l'internet quantique pour les intriquer. Dès lors, une mesure de mon qubit ici et celle du qubit de New York donneraient toujours le même résultat, alors même qu'il n'était pas prédéterminé. Donc, intuitivement, grâce à cette première propriété de l'intrication quantique, l'internet quantique serait très utile pour des tâches nécessitant une coordination à distance.

On peut alors se demander : « Ne serait-ce pas génial de partager cette intrication avec des centaines de personnes ? » Peut-être, mais c'est impossible, car la seconde propriété de l'intrication est son caractère intrinsèquement privé. Si mon qubit d'ici est intriqué avec le vôtre à New York, alors nous savons que rien d'autre ne peut partager cette intrication. C'est pour cela que la communication quantique est si pratique pour les problèmes requérant un certain niveau de sécurité.