tiennent dans des puces de 2 millimètres. Le constructeur de téléphones mobiles Samsung en intègre déjà dans ses appareils commercialisés en Corée du Sud. Des logiciels, notamment bancaires, les utilisent pour chiffrer les communications. Dans trois à cinq ans, cela devrait se généraliser à tous les téléphones.

La sécurité des données et l'espionnage ont toujours existé, mais c'est devenu une préoccupation importante et un enjeu géopolitique majeur ces dernières décennies. Toutes les grandes puissances et les grandes firmes ont un programme de cryptographie quantique. La Corée du Sud a déjà un réseau national qui connecte les grandes villes, l'Europe a aussi un projet à l'étude. Le marché de la communication quantique est en train de décoller. À titre d'exemple, chez ID Quantique, les systèmes de distribution quantique de clés représentent aujourd'hui son activité principale. Les clients sont essentiellement des établissements financiers ou des gouvernements, qui relient par exemple les ministères entre eux.

Peut-on alors déjà parler d'internet quantique ?

Non, la communication quantique avec la QKD n'est qu'une première étape. L'internet quantique, c'est deux choses : pouvoir transmettre de l'information sur des distances arbitrairement grandes et pouvoir connecter des ordinateurs quantiques.

L'obstacle majeur à la mise en place de l'internet quantique est la perte de signal dans les fibres optiques. Dans leur utilisation classique, les impulsions lumineuses perdent 99 % de leurs photons au bout de 100 kilomètres, ce qui laisse tout de même un millier de photons. Pour porter l'information plus loin, on utilise des amplificateurs optiques qui redonnent de l'intensité au signal. Pour une communication classique, cette solution est très efficace. Mais pour un système quantique, un tel processus revient à réaliser une mesure des qubits, donc à faire disparaître leur état de superposition. Or pour construire l'internet quantique, il faut pouvoir transmettre des qubits sur des distances à l'échelle d'un continent, voire du globe !

Quelles sont les solutions ?

L'approche la plus simple consiste à utiliser des « nœuds de confiance ». Supposons qu'Alice veuille envoyer des qubits à Bob, qui habite à plus de 100 kilomètres de chez elle. Elle envoie ses photons à un intermédiaire, Charlie, situé à mi-distance, qui déchiffre le message d'Alice, puis l'envoie avec un nouveau chiffrement à Bob. C'est très simple à mettre en place. La Chine a fait une démonstration impressionnante de cette idée. Elle a construit un réseau long de 2 000 kilomètres reliant Pékin à Shanghai et utilisant 32 nœuds de confiance. Avec cette solution, le risque pour la sécurité de l'information est évident : chaque nœud intermédiaire est un maillon faible qui peut être compromis et exploité par un espion. Pour garantir la protection des données sur toute la ligne (et aussi connecter de façon optimale des ordinateurs quantiques), il faut utiliser une autre technique : les répéteurs quantiques.

Comment un répéteur quantique fonctionne-t-il ?

Le premier ingrédient dont nous avons besoin est l'intrication quantique. En physique quantique, il est possible d'avoir deux objets dont les propriétés sont fortement corrélées de sorte que, mathématiquement, on ne peut pas les décrire séparément. La conséquence est que lorsque cette paire d'objets se retrouve dans une superposition d'états, si l'on effectue une mesure sur l'un des deux, cela influe instantanément sur les propriétés de l'autre, même si les deux objets sont à très grande distance l'un de l'autre, typiquement à des centaines de kilomètres dans le cas pratique de l'internet quantique. Ces corrélations ne peuvent pas s'expliquer par la physique classique, elles sont purement quantiques.

Si Alice et Bob ne sont pas trop éloignés, ils peuvent réaliser la QKD avec une source de

LA DISTRIBUTION QUANTIQUE DE CLÉ DE CHIFFREMENT

La cryptographie quantique repose sur un échange sécurisé de clé de chiffrement entre deux interlocuteurs, nommés traditionnellement Alice et Bob. Dans la version la plus simple, Alice envoie à Bob une suite de photons polarisés (horizontalement, verticalement ou selon les deux premières diagonales, qui codent respectivement un bit 0, 1, 0 et 1). Bob fait passer chaque photon qu'il reçoit à travers un des deux polariseurs à sa disposition, qu'il choisit de façon aléatoire. Le premier filtre laisse passer les polarisations horizontale et verticale, le second les deux polarisations diagonales. Bob communique alors publiquement (c'est-à-dire qu'un espion peut écouter cet échange) à Alice la séquence de polariseurs qu'il a utilisée. Alice lui répond, publiquement aussi, quels photons mesurés il doit garder (ceux dont un des deux axes du polariseur utilisé était aligné sur la polarisation du photon, une information que seule Alice détient). Avec ces photons, Alice et Bob créent une suite de bits qui sera leur clé commune. Comme les polariseurs de Bob laissent passer deux types de photons polarisés codant respectivement un bit 0 ou 1, un espion qui connaît la liste des polariseurs de Bob ne peut pas, pour autant, reconstituer la clé.

Le point important est que l'espion qui intercepterait les photons de la clé sur leur trajet altérerait leur polarisation et donc les mesures de Bob. Or si Alice et Bob comparent un petit échantillon aléatoire du signal et qu'ils notent trop d'erreurs, ils en déduisent qu'un ennemi a interféré. Ils s'envoient alors une nouvelle clé.

paires de photons intriqués (tels que leurs polarisations sont toujours orthogonales). Cette source peut être placée n'importe où sur le trajet : à mi-distance, chez Alice, etc. Quand Alice mesure la polarisation du photon qu'elle reçoit, elle connaît la polarisation du photon qui arrive chez Bob. Ils peuvent alors créer une clé de chiffrement comme avant : Bob fait ses mesures avec deux polariseurs et Alice lui dit quels photons conserver pour constituer la clé.

Mais comment faire si Alice et Bob se trouvent à plusieurs centaines de kilomètres l'un de l'autre ?

À elle seule, la source de photons intriqués ne résout pas le problème de la perte de signal dans la fibre. La solution est la téléportation quantique, un protocole de communication qui s'appuie sur l'intrication quantique.

Supposons qu'Alice et Bob soient en mesure d'envoyer des photons à un intermédiaire, Charlie, qui sera le « répéteur quantique ». Alice et Bob sont chacun équipés d'une source de paires de photons intriqués, respectivement (A1, A2) et (B1, B2). Les photons A1 et B1 sont envoyés à Charlie, qui réalise une mesure simultanée particulière (dite « mesure de Bell ») sur ces deux photons, lesquels se retrouvent alors intriqués. Mais les lois de la physique quantique impliquent que les deux autres photons A2 et B2, restés chez Alice et Bob, forment à leur tour une paire intriquée. Résultat : Alice et Bob partagent une paire de photons dont ils pourront mesurer les polarisations afin d'établir une clé de chiffrement.

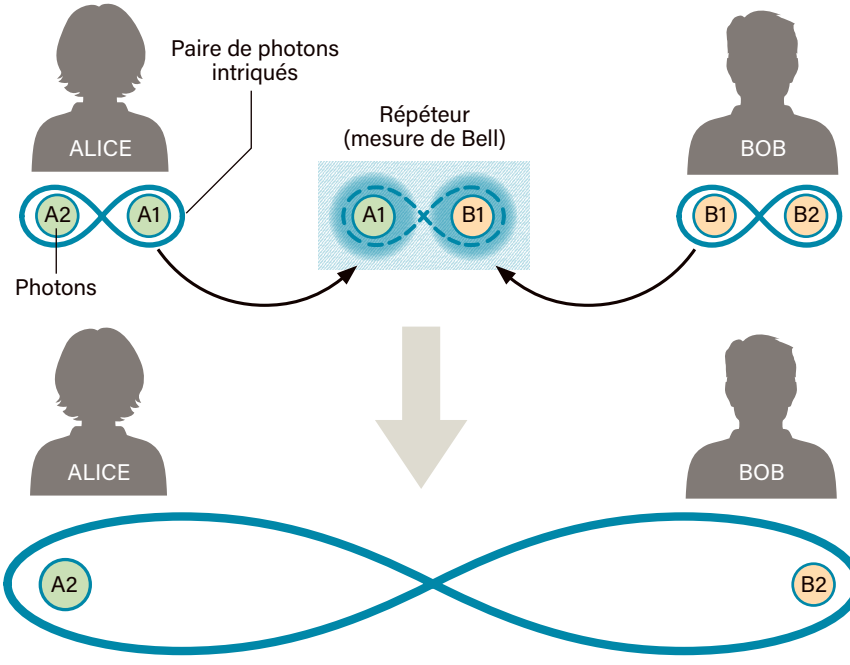
La force du système est que le principe peut se généraliser, en plaçant autant de répéteurs que nécessaire pour couvrir la distance qui sépare Alice et Bob. Il faut aussi souligner que les répéteurs quantiques ne sont pas des nœuds de confiance, car ils n'ont pas accès à l'information partagée entre Alice et Bob. Un espion ne peut pas intercepter la clé en infiltrant un répéteur.

En 1997, les équipes de Francesco de Martini, à l'université de Rome, et d'Anton Zeilinger, à l'université d'Innsbruck, ont réalisé les premières expériences de téléportation quantique en laboratoire. En 2007, mon équipe a mis en œuvre ce phénomène sur une grande distance : nous avons injecté les photons dans le réseau de fibres optiques de Swisscom et la mesure de Bell a été réalisée bien après l'émission des photons qui se trouvaient ainsi à plusieurs centaines de mètres quand la téléportation a opéré.

La technique des répéteurs quantiques est-elle donc accessible ?

Dans les expériences de laboratoire, les photons que Charlie reçoit sont synchronisés pour arriver en même temps afin de réaliser la mesure de Bell. Or, dans des conditions réelles, ce n'est pas le cas. Il faut donc pouvoir stocker le premier photon arrivé en attendant le second. Et cela est extraordinairement difficile. Comment le faire sans détruire le qubit ? À l'université de Genève, notre groupe a commencé à développer en 2008 des mémoires quantiques reposant sur des cristaux dopés avec des terres rares. Le cristal est refroidi à quelques kelvins pour que tous les atomes soient dans l'état fondamental. La différence d'énergie avec le premier état excité correspond à l'énergie du photon incident, qui peut alors être absorbé. Mais comme la probabilité d'absorption par le premier atome rencontré n'est pas de 100 %, il peut être absorbé par le deuxième atome, le troisième, etc. Le système est en fait dans une superposition d'états du premier atome excité, du deuxième, du troisième, etc. Les atomes sont par ailleurs préparés pour définir une sorte d'horloge qui indique quand le système se désexcite et libère un nouveau photon. Ce dernier doit avoir toutes les propriétés quantiques (de superposition et d'intrication) du photon incident et doit être réémis dans la bonne direction, sinon il est perdu. Plusieurs équipes de recherche ont ainsi des prototypes de mémoires quantiques qui fonctionnent. Le défi est cependant de combiner une efficacité élevée (on parvient à restituer environ 10 % des photons incidents) et des temps de stockage qui peuvent être assez longs, de l'ordre du dixième de seconde.

Les mémoires quantiques de mon laboratoire utilisent des cristaux qui font à peine un centimètre de longueur. Mais elles restent de vraies « usines à gaz », car il faut les refroidir avec un système de cryogénie. Si nous sommes encore loin d'une possible commercialisation de ces dispositifs, les progrès de ces dernières années sont encourageants.



Pour implémenter l'internet quantique sur de grandes distances en passant par les fibres optiques, la solution est d'utiliser la téléportation d'intrication quantique. Pour réaliser ce protocole, Alice et Bob ont chacun une paire de photons intriqués, (A1, A2) et (B1, B2). Les photons A1 et B1 sont envoyés à un répéteur, où une mesure dite de Bell intrique les deux photons. D'après les règles de la mécanique quantique, la paire (A2, B2) devient à son tour intriquée. Avec ces photons aux propriétés corrélées, Alice et Bob peuvent alors mettre en place une distribution quantique de clé.