l'espion ne peut pas facilement retrouver ses facteurs premiers car il n'y a à ce jour aucun algorithme classique qui permette de les déterminer rapidement. Cependant, avec l'ordinateur quantique, la donne pourrait changer.

Pour quelle raison ?

En 1994, le mathématicien américain Peter Shor a conçu un algorithme « quantique » qui exploite pleinement les états de superposition des qubits pour décomposer très vite des nombres très grands. Pour l'instant, les prototypes opérationnels d'ordinateurs quantiques manipulent au mieux quelques poignées de qubits. D'ici à quelques années, ces machines seront assez puissantes pour implémenter l'algorithme de Shor, ce qui mettra en danger les méthodes de chiffrement de type RSA. Il existe d'autres types de méthodes de chiffrement, dits « post-quantiques », qui sont construits sur des problèmes dont on ne connaît pas d'algorithme classique ou quantique pour les casser. Mais le risque d'en trouver existera toujours.

Une solution consiste alors à exploiter les propriétés quantiques pour construire des protocoles de chiffrement qui seraient impossibles à attaquer. La cryptographie quantique permet déjà d'établir des communications sécurisées. C'est la partie la plus avancée de l'internet quantique.

En quoi consiste cette cryptographie quantique ?

Imaginons que deux personnes, nommées habituellement Alice et Bob, veuillent établir une communication sécurisée. Elles doivent d'abord se partager une clé de chiffrement qui servira d'un côté à brouiller le message et de l'autre à le rendre lisible. L'idée est ici d'avoir une distribution quantique de cette clé, ou QKD (pour *quantum key distribution*). L'intérêt est qu'en physique quantique, quand un observateur effectue une mesure sur un système, il modifie ce dernier. Ainsi, quand Alice envoie la clé à Bob selon un protocole bien précis (*voir l'encadré page 25*), les deux correspondants peuvent savoir si un espion a lu la clé. Dans ce cas, ils jettent cette clé à la poubelle (qui ne contient aucune information de toute façon) et s'en envoient une nouvelle jusqu'à avoir la garantie que la clé n'a pas été interceptée.

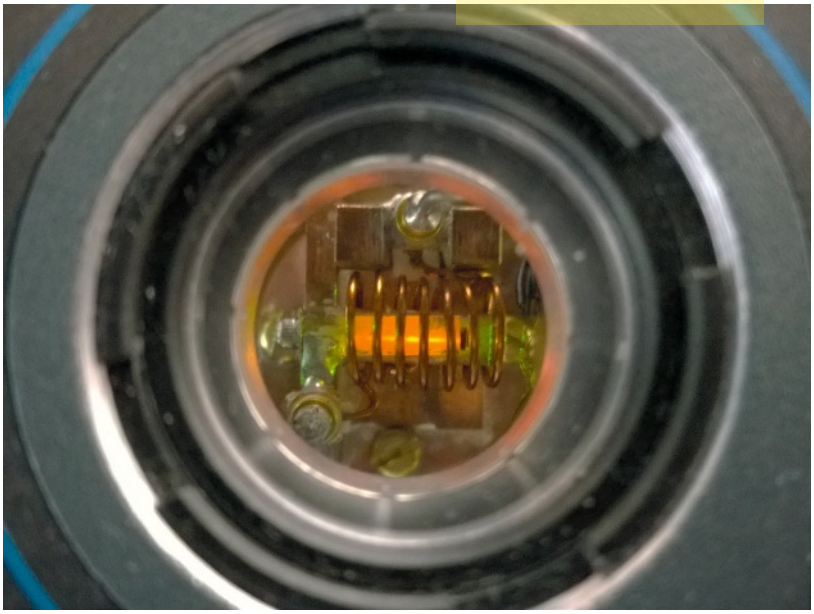
La cryptographie ne garantit pas la solidité de la communication. Si un espion capte systématiquement la clé, il sera impossible d'envoyer un message. En revanche, la QKD garantit la confidentialité : une fois la clé partagée, les messages seront chiffrés de façon robuste et l'espion n'aura aucun moyen de voler l'information transmise. Le premier protocole d'échange quantique de clé a été proposé en 1984 par l'Américain Charles Bennett et le Canadien Gilles Brassard.

Existe-t-il déjà des applications commerciales de la distribution quantique de clés ?

Plusieurs entreprises dans le monde proposent de tels systèmes de communications quantiques. C'est un marché en pleine expansion. Par exemple, il y a tout juste vingt ans, j'ai fondé la société ID Quantique avec des collègues de l'université de Genève. À l'époque, nous étions pionniers dans le domaine, mais surtout vus comme des physiciens illuminés ; on ne nous prenait pas trop au sérieux. Nous vendions essentiellement des détecteurs de photons uniques et des générateurs quantiques de nombres aléatoires.

Ces derniers jouent aussi un rôle important dans la sécurisation des données. Ils sont essentiels pour la cryptographie, car ils permettent de produire des clés de chiffrement de façon parfaitement aléatoire. La plupart des générateurs actuels s'appuient sur des algorithmes déterministes qui ne peuvent produire que des nombres pseudoaléatoires ; autrement dit, si l'on connaît bien l'algorithme et le système, il est possible de prévoir les nombres produits. D'autres approches s'appuient sur des phénomènes physiques chaotiques pour en extraire de l'aléa, mais il faut bien s'assurer qu'ils ne sont pas prévisibles et souvent ces méthodes nécessitent un traitement logiciel qui, lui, peut altérer cet aléa.

Encore une fois, la physique quantique démontre son efficacité. L'idée est simple. On envoie un photon sur un miroir semi-réfléchissant, qui peut le réfléchir ou le laisser traverser. Le photon sera détecté, de façon totalement imprévisible, d'un côté du miroir ou de l'autre. Selon le cas, il code un bit « 0 » ou « 1 ». Au début, de tels générateurs quantiques de nombres aléatoires tenaient dans de petits boîtiers. Maintenant, grâce aux techniques de miniaturisation, ils



Une mémoire quantique conçue par l'équipe de Nicolas Gisin, à l'université de Genève. Le cristal contient des atomes d'ytterbium, élément de la famille des terres rares. Ceux-ci sont maintenus dans leur état d'énergie fondamentale en étant refroidis à quelques kelvins. Le système peut absorber un photon et en émettre un peu plus tard un autre présentant les mêmes propriétés quantiques d'intrication.

© Université de Genève

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.