En quoi consiste l'internet quantique ?

Le réseau internet actuel est un succès technique incroyable qui a connu une croissance explosive ces dernières décennies. On estime qu'en janvier 2021, près de 60% de la population mondiale, soit 4,6 milliards d'individus, y ont accès. Internet fait partie de notre vie. Nous l'utilisons tous les jours pour échanger divers types de données, des textes, des images, des vidéos. Il est difficile d'imaginer comment le monde fonctionnerait sans ce réseau.

D'un point de vue technique, l'internet classique est un réseau décentralisé bâti sur des nœuds répartis à travers le globe et reliés par des fibres optiques. Les unités d'information, les bits, sont transmises sous la forme d'impulsions lumineuses, chacune contenant de l'ordre du million de photons. Selon qu'on reçoit un signal ou non, le bit prend la valeur «1» ou «0».

Ce réseau fonctionne très bien. Mais, d'un point de vue conceptuel, on peut se poser la question suivante: jusqu'où peut-on réduire l'intensité lumineuse? La limite ultime est de n'avoir qu'un seul photon par impulsion. À une telle échelle, les règles de la physique classique ne s'appliquent plus et on entre dans le monde fascinant de la physique quantique. Notamment, le photon peut être dans un état dit «de superposition des états "0" et "1"», c'est-à-dire qu'il peut être, dans un sens mathématiquement précis, dans ces deux états à la fois. Ce phénomène quantique confère une grande richesse au système: le bit classique est remplacé par le bit quantique, ou qubit, qui porte alors une «information quantique». L'idée de l'internet quantique est d'utiliser le réseau actuel de fibres optiques pour échanger des qubits.

Notons que l'on retrouve la même idée de réduction avec l'ordinateur. Pour remplacer les paquets d'électrons qui circulent dans les transistors, de nombreux laboratoires et entreprises travaillent sur le concept d'un ordinateur quantique qui manipulerait des qubits. De telles machines seraient très intéressantes, car on a montré qu'elles pourraient réaliser certains calculs exponentiellement plus vite que les ordinateurs classiques.

Et quels sont les avantages de l'internet quantique ?

Le premier concerne les volumes de données que l'on pourra faire circuler sur le réseau. Les besoins ont décuplé ces dernières années. En réduisant l'information à des photons uniques, on voit tout de suite qu'il sera possible d'augmenter les débits.

Cette idée de photon unique conduit à un deuxième argument en faveur de l'internet quantique. Mais il faut le prendre avec précaution et le considérer comme un idéal à atteindre. À terme, l'internet quantique pourrait être moins énergivore que le réseau actuel.

> En manipulant des photons uniques soumis aux lois de la physique quantique, on obtient automatiquement la sécurité de l'information

Le principe est tout simple: on dépense moins d'énergie à émettre un photon unique qu'un paquet de ces particules de lumière. L'argument s'applique aussi à l'ordinateur quantique, qui pourrait, en principe, un jour réaliser des calculs en consommant moins d'énergie qu'un ordinateur classique.

On est encore loin de cet idéal. Les qubits sont des objets fragiles. S'ils interagissent avec leur environnement, ils perdent leur état de superposition et tous les avantages associés. C'est le phénomène de «décohérence». Cette situation est surtout critique dans les ordinateurs quantiques. La solution pour maintenir l'état quantique du qubit le plus longtemps possible consiste à refroidir l'ordinateur à des températures d'une fraction de degré au-dessus du zéro absolu. Or les dispositifs cryogéniques dépensent beaucoup d'énergie. Mais les progrès dans le domaine de l'ordinateur quantique laissent espérer qu'il sera possible d'en concevoir qui fonctionnent à température ambiante. L'internet quantique est un peu moins sensible à ces problèmes de décohérence, mais certains éléments envisagés pour ce réseau de demain demandent aussi d'être refroidis et ils consomment pour l'instant encore beaucoup d'énergie.

La sécurité est censée être un atout majeur de l'internet quantique. Pourquoi ?

Le fait de manipuler des photons uniques soumis aux lois de la physique quantique procure un avantage qui n'est pas évident *a priori*: on obtient automatiquement la sécurité de l'information. C'est pour moi l'argument principal, il est indiscutable, nous sommes déjà capables de l'exploiter et il n'y a pas d'autre solution aussi efficace.

Tous les dispositifs numériques omniprésents dans notre quotidien (l'ordinateur, les téléphones portables et l'internet classique) ont ouvert de nombreuses portes à des espions, gouvernementaux ou non, capables d'intercepter ou de dérober des données sensibles. La solution actuelle pour protéger ces informations consiste à les rendre illisibles grâce à des algorithmes de chiffrement. Sans la clé de chiffrement, l'espion ne peut pas lire les messages.

Les algorithmes de chiffrement reposent sur des problèmes mathématiques qui sont *a priori* difficiles à résoudre en un temps raisonnable. Par exemple, le chiffrement RSA développé en 1977 par les cryptologues américains Ronald Rivest et Leonard Adleman et l'Israélien Adi Shamir est utilisé pour sécuriser les échanges dans le commerce électronique. Cet algorithme exploite la décomposition en facteurs premiers d'un nombre très grand (actuellement d'au moins 1024 bits, soit des nombres décimaux à 309 chiffres) pour définir la clé de chiffrement. Or, bien que ce nombre très grand ne soit pas secret (d'où la terminologie de clé publique),

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.

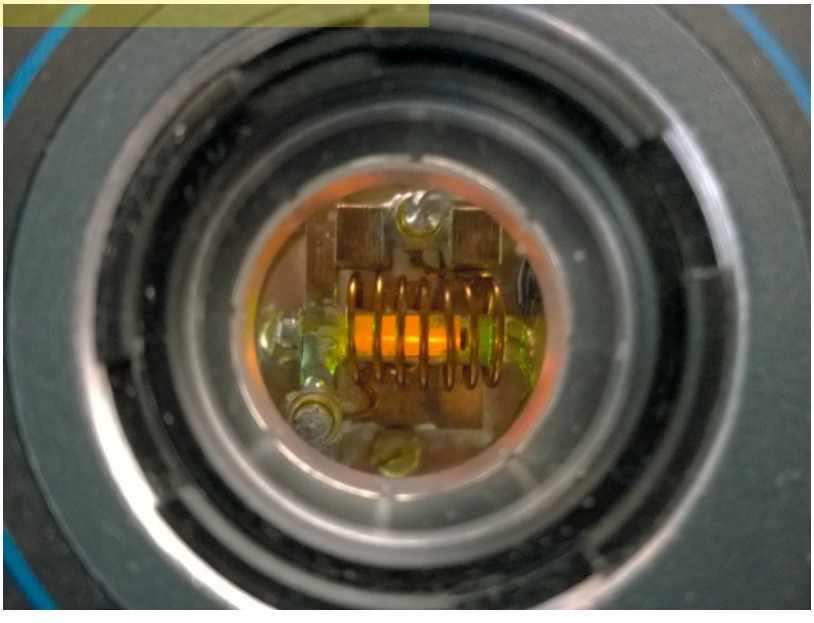
La cryptographie ne garantit pas la solidité de la communication. Si un espion capte systématiquement la clé, il sera impossible d'envoyer un message. En revanche, la QKD garantit la confidentialité : une fois la clé partagée, les messages seront chiffrés de façon robuste et l'espion n'aura aucun moyen 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