

Comment le cryptage quantique veille sur les codes secrets

Innovation - La lumière se met au service de la sécurité, en permettant de s'assurer scientifiquement de la transmission sans interception illicite d'un code secret. Explications.

Comment être sûr qu'un code secret n'a pas été intercepté durant sa transmission? Le cryptage quantique, ou QKD (*Quantum Key Distribution*), apporte une réponse à la question. Sortie des laboratoires de recherche, cette technologie utilise les propriétés quantiques de la lumière pour savoir si un message a été lu. Elle a déjà trouvé des applications pour le grand public et se trouve au cœur d'un VPN que commercialise depuis l'an dernier la société [MagiQ Technologies](#). Par ailleurs, des chercheurs des universités de Harvard et de Boston utilisent un réseau basé sur ce principe à Boston.

Le cryptage quantique résout le problème délicat de la transmission des clés. Lorsque celles-ci sont envoyées de manière traditionnelle, il est impossible de savoir si quelqu'un a pu en prendre connaissance. L'interception d'un message ne laisse en effet aucune trace. L'algorithme RSA à clé publique contourne ce problème de manière géniale, mais il est hélas un gros consommateur de ressources au niveau du décryptage. Ce qui limite quelque peu son intérêt.

Avec le QKD, il devient possible de savoir si le message a été intercepté. Contrairement aux autres méthodes basées sur des limitations technologiques, ou sur des conjectures mathématiques, le cryptage quantique s'appuie sur des lois physiques, ce qui pourrait le rendre beaucoup plus sûr.

Le système BB84, méthode la plus connue

Le système de cryptage quantique le plus connu est le BB84. Il s'agit d'une méthode de génération et de transmission de clés, conçue par Charles Benett et [Gilles Brassard](#). Il utilise deux canaux: le premier est un canal quantique en fibre optique qui sert à transmettre la clé. Le second est un canal classique, utilisé pour transmettre les informations non confidentielles.

Voici une description simplifiée du système. Pour transmettre la clé, A envoie à B des photons polarisés via le canal en fibre optique.

Rappelons que la lumière est constituée de particules appelées photons associées à un champ électromagnétique, et que leur polarisation correspond à la direction de vibration du champ électrique. Dans la lumière naturelle, cette polarisation est aléatoire, mais il est possible d'aligner ce champ dans une direction précise en utilisant certains cristaux ou des filtres Polaroid.

A envoie donc ses photons un par un, selon une direction de polarisation qui peut être droite (verticale ou horizontale), ou inclinée (45° ou à 135°), ce qui fait 4 polarisations possibles. La polarisation choisie change chaque fois.

L'incertitude quantique

Pour recevoir ces photons, B utilise un détecteur qu'il ne peut placer que de deux façons: soit droit, soit incliné. Or, la mécanique quantique stipule qu'il est impossible de mesurer la polarisation d'un photon à la fois dans une base droite (0° et 90°) et dans une base inclinée (45° et 135°). C'est l'une ou l'autre, il faut choisir. Par conséquent, si le détecteur de B est droit, il ne peut mesurer que les photons polarisés horizontalement ou verticalement. Si le photon arrive "incliné", le détecteur sera incapable de déterminer si sa polarisation était de 45° ou de 135° . Il fournira alors un résultat aléatoire.

Et inversement si le détecteur est incliné. Aussi, à chaque fois qu'A envoie un photon, B choisit la position de son détecteur au hasard; par conséquent, il se trompe en moyenne une fois sur deux. A la fin de la transmission, B envoie à A sur le canal classique la liste de tous les choix qu'il a fait, mais pas le résultat de ses mesures. A lui répond sur le même canal en lui indiquant quels étaient ses bons choix (détecteur droit ou incliné). A et B ne conservent alors que la liste des bonnes mesures.

Il ne leur suffit plus qu'à convenir publiquement que, par exemple, les polarisations de 0° et 45°

représentent des 0, et les autres des 1, pour construire leur clé en binaire avec cette liste.

Pas de droit à l'erreur

Comment un pirate peut-il intercepter la communication sur le canal quantique? Comme B, il mesurera la polarisation du photon, puis renverra à B un photon identique. Toutefois, ce pirate ne pourra pas faire mieux que B, et il se trompera aussi une fois sur deux. Par conséquent, lorsque le pirate aura vu juste, il renverra un "bon" photon à B, mais lorsqu'il se sera trompé, il aura une chance sur deux de renvoyer un photon différent de celui qu'avait envoyé A.

Pour savoir si la communication a été interceptée, B devra envoyer à A, en plus de la liste de ses choix, les premières valeurs de ses mesures. Ces données-là ne seront bien sûr pas utilisées pour calculer la clé. A vérifiera alors ces mesures. Si il constate que B a fait des erreurs qu'il n'aurait pas dû faire, elle en déduira que la communication a été écoutée et la clé ne sera pas utilisée.