LE TEMPS

Physique Samedi3 décembre 2011

La cryptographie quantique passe l'épreuve du temps

Par Pierre-Yves Frei

Cette méthode de codage extrêmement sûre et exploitée par des chercheurs genevois démontre qu'elle est fiable sur le long terme

Le monde de l'infiniment petit, des particules élémentaires, laisse sans voix. Comment peut-il soutenir le monde macroscopique sur ses frêles épaules quand il fonctionne si différemment de lui? On laissera le devoir de la réponse aux philosophes des sciences ou encore aux théoriciens et l'on s'en tiendra à cette affirmation: il n'y a que dans l'univers quantique que l'on trouve le vrai hasard, ce que les spécialistes appellent l'aléatoire absolu.

Certes, les êtres humains sont capables de créer des générateurs aléatoires grâce à des algorithmes mathématiques de leur invention. Mais ces derniers ne sont pas capables de générer ce hasard absolu qui reste l'apanage de l'infiniment petit. Fort de cette constatation, les physiciens tentent depuis le milieu des années 1980 d'utiliser cette qualité quantique dans le domaine de la cryptographie, autrement dit du chiffrement et de la sécurisation de messages envoyés d'un point A à un point B.

Aujourd'hui, cette approche n'est plus seulement théorique. On sait créer des clés secrètes «quantiques» et les utiliser à des fins de cryptographie. Il existe même des applications commerciales. Dans ce domaine, c'est une entreprise genevoise qui occupe la place de leader mondial. ID Quantique, une spin-off du Laboratoire d'optique appliquée (GAP) de l'Université de Genève dirigé par Nicolas Gisin, multiplie les preuves que son système, pour pointu qu'il soit, fonctionne et qu'il peut faire mieux, plus sûr, que les méthodes classiques de codage.

C'est donc une étape importante que cette société, l'Université de Genève et la HES-SO décrivent dans la dernière édition du New Journal of Physics. Les chercheurs ont en effet réussi à maintenir un système de cryptographie quantique en parfait état de fonctionnement pendant plus d'un an et demi. «C'est une étape importante, confie Damien Stucki, physicien chez ID Quantique. Elle démontre la robustesse et la fiabilité de ce système sur un réseau existant, avec des utilisateurs, et non pas dans un petit laboratoire. Cela renforce ses arguments commerciaux.»

Aujourd'hui, quelques banques, qui préfèrent garder l'anonymat, ont déjà recours à la cryptographie quantique pour certaines applications spécifiques. Car même si sa puissance est reconnue, cette méthode de chiffrement connaît ses limites. Elle ne peut pas aujourd'hui s'envisager sur des distances supérieures à 100 kilomètres. Pourquoi cette limite? Essentiellement parce que la méthode de chiffrement repose sur des photons, autrement dit des particules de lumière, que l'on fait circuler dans des fibres optiques. «Nous enregistrons des pertes de signal qui nous limitent en distance aujourd'hui, regrette le professeur Nicolas Gisin. Mais nous préparons une riposte. Plutôt que d'envoyer 5 millions de photons individuels par seconde, nous prévoyons d'en envoyer 600 millions. On multiplie ainsi les chances que certains d'entre eux traversent des distances comme Genève-Bâle.»

Une grande partie de la contribution de ce système tient donc au hasard absolu qui caractérise le monde quantique. Diverses propriétés peuvent caractériser un photon particulier et notamment sa phase. En effet, il faut se souvenir qu'une particule quantique peut être décrite comme une onde, comme une sinusoïde qui se répète. On peut décrire à quel état du cycle un photon se trouve quand on l'observe.

Imaginons maintenant deux acteurs, Bob et Alice, qui entendent communiquer grâce à cette méthode de cryptographie quantique. Le premier génère des paquets de photons et les envoie à Alice qui reçoit ces trains de lumière et les réduit à un seul photon dont la phase est attribuée par un générateur aléatoire quantique. Avant de le renvoyer à Bob. C'est par ces allers-retours que les deux interlocuteurs vont établir leur clé cryptographique et ce n'est que lorsque celle-ci sera reconnue par les deux parties que de l'information pourra être échangée.

«On ne peut pas observer une particule sans changer ses caractéristiques, explique Damien Stucki. Si un espion veut intercepter la communication chiffrée, il doit accéder à la clé cryptographique. Dans ce cas, il doit mesurer les états de phase des photons utilisés pour échanger cette clé. Seulement, en observant ces particules, il perturbe leurs propriétés. Dès lors, Alice et Bob, dont les systèmes ont établi la clé, vont rapidement être alertés par un taux d'erreur anormal sur les phases des photons. Ils se savent alors observés et peuvent interrompre l'échange de la clé et tout cela sans avoir divulgué de l'information car la clé n'en contient aucune.» L'espion a la tâche d'autant moins facile qu'Alice et Bob renouvellent en permanence la clé cryptographique qui les lie.

S'il a prouvé sa fiabilité sur plus de dix-huit mois, ce système est-il inviolable pour autant? Cette question a donné lieu à un large débat quand, en 2009, des chercheurs indépendants, d'ailleurs mandatés par ID Quantique, ont découvert des failles, par ailleurs comblées depuis. L'inviolabilité est donc question de définition. La cryptographie quantique répondrait aux exigences de la sécurité de principe. Elle serait, à ce titre, un modèle sûr, grâce aux propriétés étonnantes des particules qu'elle utilise. Les lois de la physique quantique assureraient donc cette inviolabilité.

Il en irait autrement de la sécurité dite d'implémentation. Celle-ci met en jeu le matériel qui génère les communications cryptées. Les machines sont des artefacts humains, par essence imparfaits. Elles peuvent à ce titre présenter des failles exploitables par des hackers quantiques. «Mais ces derniers n'ont rien à voir avec des hackers normaux qui peuvent détourner des informations sur Internet et les mettre de côté en attendant de découvrir la clé cryptographique, ajoute le professeur Nicolas Gisin à l'origine de nombreux travaux pionniers dans ce domaine. Un espion quantique a non seulement l'obligation de se connecter physiquement sur la ligne mais, en outre, il est condamné à lire les données en temps réel. Impossible de différer leur décryptage.»

Les photons font donc bonne garde. Mais ils ne doivent pas se reposer sur leurs lauriers quantiques pour autant.