Clés inviolables

Autor(en): **Dessibourg, Olivier**

Objekttyp: **Article**

Zeitschrift: **Horizons : le magazine suisse de la recherche scientifique**

Band (Jahr): **22 (2010)**

Heft 85

PDF erstellt am: **16.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-971085

Clés inviolables

Pour transmettre des messages codés, un nouveau système de cryptage mise sur des photons plutôt que sur des chiffres. La communication ne pourra ainsi pas être interceptée sans que cela se remarque.

PAR OLIVIER DESSIBOURG

James Bond le confirmera: un bon espion est celui qui parvient à prendre connaissance d'un message sans que l'émetteur et le destinataire sachent qu'il a été lu. Toutefois, les héritiers modernes de l'agent 007 peineront à faire leur métier, en informatique du moins. Car un mode de cryptage inédit se profile depuis une décennie: la cryptographie quantique. Physicien de l'Université de Genève (UniGE), Grégoire Ribordy a cofondé la société ID Quantique à Carouge pour commercialiser cette technologie révolutionnaire.

A ce jour, les systèmes de cryptage utilisent des «clés» pour coder des messages binaires formés de 0 et 1. Or, pour que les entités qui communiquent puissent les lire, ces clés, aussi numériques, doivent être échangées. Avec le risque d'être interceptées et décryptées.

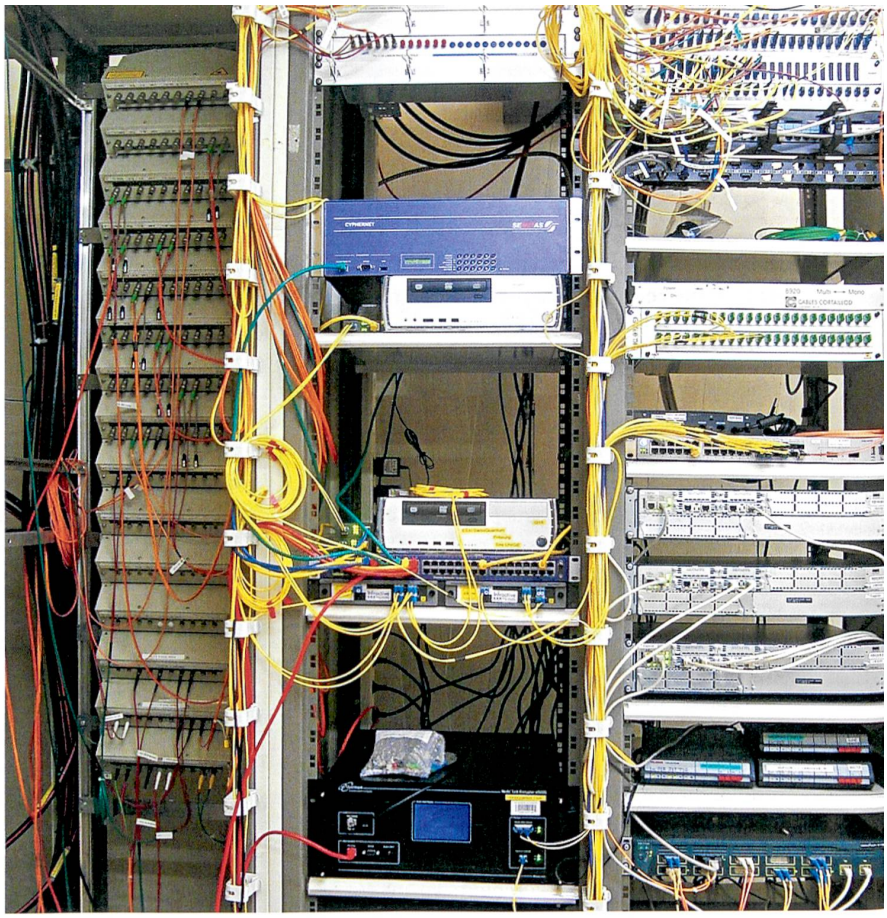
Collier de photons

C'est là que les physiciens de l'UniGE, à l'origine sous l'impulsion du professeur Nicolas Gisin, entrent en scène: au lieu d'utiliser des chiffres, ils recourent à des photons. Ces particules de lumière, lorsqu'on les fait passer à travers des filtres, peuvent être «orientées» de manière à porter une information correspondant au 0 ou au 1. Répéter la démarche à l'envi permet de créer une clé sous la forme d'un collier de photons. Ce train de lumière peut être envoyé entre deux interlocuteurs reliés par fibre optique, avec une sécurité quasi parfaite: «Selon le principe physique dit ‹de Heisenberg›, les particules ne peuvent être mesurées sans que leur configuration soit perturbée», justifie Grégoire Ribordy. Autrement dit, si un espion tente d'intercepter la communication, les interlocuteurs le remarquent aussitôt et peuvent réagir.

Le physicien en convient: «Au fur et à mesure que nous développons ces systèmes, nous sommes revenus de l'idée qu'ils sont sûrs à 100%. Plutôt que parler de ‹sécurité de technologie›, il faut assurer une ‹sécurité d'implémentation›. Car au-delà du modèle idéal, sa concrétisation fait toujours appel à des composants électroniques et optiques. Or si ceux-ci sont optimalisés, la sécurité est supérieure à celle d'un système de cryptage classique.»

Dans ce marché émergent, ID Quantique a deux firmes compétitrices, l'américaine MagiQ et la française Smart Quantum, même si pour Grégoire Ribordy les concurrents principaux restent les encodeurs classiques. Où se situe la start-up suisse? «Devant! Nous avons déjà testé nos systèmes en situation réelle, lors de votations genevoises en 2007. Nous sommes les seuls à être certifiés pour le marché depuis la fin 2009. Et surtout, nous développons notre technologie dans le cadre d'un réseau fonctionnel depuis un an.»

Baptisé SwissQuantum, celui-ci est coordonné par l'UniGE et soutenu par le Fonds national suisse. «Un des objectifs est d'accroître les distances sur lesquelles les données cryptées sont échangées, précise le scientifique. A savoir 100 km sur le terrain et 250 km en laboratoire. Au-delà, les photons se perdent... Pour atteindre les 500 km, il nous faudra des ‹répétiteurs quantiques›, des relais relançant la lumière codée. Cette technologie est actuellement étudiée par les physiciens de l'UniGE, et nous nourrissons mutuellement nos réflexions au sein du Pôle de recherche national Quantum Photonics. C'est donc profitable pour tout le monde!» ■



Boîte noire d'un nouveau type. Celle qui se trouve en bas au milieu de l'armoire électrique contient un système de cryptographie quantique. C'est de là que des photons sont envoyés entre deux interlocuteurs reliés par fibre optique.
Photo: idquantique.com