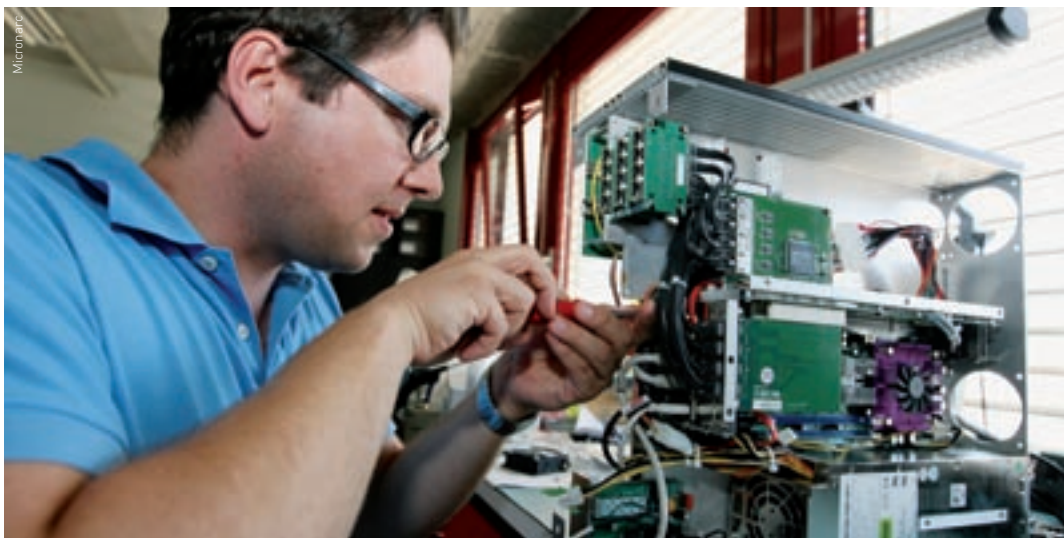


# La cryptographie quantique enfin maîtrisée

Halte aux hackers ! L'entreprise genevoise id Quantique dissèque les rayons lumineux pour créer des clefs secrètes basées sur la cryptographie quantique. Ce procédé désormais maîtrisé est destiné à améliorer la sécurité des réseaux de fibres optiques avec une fiabilité quasi absolue.



id Quantique a d'abord développé un prototype qui a été testé sur le réseau de fibres optiques de Swisscom. Puis, l'appareil a permis d'échanger une clé de cryptage entre deux stations connectées chacune à un PC par un port USB.

«La cryptographie quantique, c'est fiable et sûr». Cette affirmation émane non seulement de la société id Quantique, spécialisée dans la conception et la fabrication d'instruments optiques et photoniques de sécurité et de réseau, mais également du professeur Nicolas Gisin, du Groupe de physique appliquée de l'Université de Genève (UNIGE). Explications : la cryptographie conventionnelle, science qui constitue l'ensemble des techniques permettant de garantir la confidentialité et l'intégrité des échanges d'informations, ne date pas d'hier. Il y a près de deux mille ans, Jules César l'utilisait déjà et cela s'est perpétré jusqu'à nos jours avec les Prix Nobel d'Einstein sur le photon en 1921. Jusqu'à récemment, elle est restée confinée aux domaines militaires et diplomatiques. Avec le développement des télécoms ces vingt-cinq dernières années, la cryptographie est en quelque sorte entrée dans les mœurs, comme par exemple dans les applications de télébanking.

Nos précieuses données sont ainsi chiffrées puis déchiffrées au moyen d'un algorithme. Jusqu'ici, rien de révolutionnaire, d'autant plus qu'un malin espion peut quand même happer au vol le message ainsi brouillé et l'interpréter. «C'est comme entre deux joueurs de tennis. L'un envoie le message en lançant la balle, l'autre l'intercepte correctement sur sa raquette... ou sur son ordinateur. Seulement voilà, un spectateur mal veillant peut à tout moment apprivoiser la balle au vol», vulgarise avec humour, Grégoire Ribordy, directeur d'id Quantique à Genève.

## Bulle de savon insaisissable

La cryptographie quantique permet quant à elle de garantir une sécurité bien plus accrue, car elle est basée sur les lois de la physique quantique. La suite de nos explications : de nos jours, les systèmes modernes de communication échangent les informations au moyen d'impulsions lumineuses voyageant sur des réseaux de fibres optiques. Or, pour chaque bit, une impulsion

est émise et transmise via la fibre optique à un récepteur qui la détecte et la transforme en signal électronique. En cryptographie quantique, le même principe est suivi, sauf que les impulsions sont constituées d'un unique photon. Ce dernier représente une quantité d'énergie minuscule. En lisant cet article, vos yeux en détectent des milliards à chaque seconde, ce qui constitue un système quantique élémentaire. En particulier, il n'est pas possible de casser le photon en deux. Ainsi, un espion ne peut pas prendre un demi-photon, tout en laissant l'autre moitié poursuivre sa route. Si le hacker veut intercepter le bit échangé, il lui faut détecter le photon et donc interrompre la communication. «Pour en revenir à nos deux joueurs de tennis, c'est comme si la balle était remplacée par une... bulle de savon», compare Grégoire Ribordy. Effectivement, bien maligne serait la personne qui pourrait happer une telle bulle sans la détruire. Voilà pour la théorie. En pratique, id Quantique a tout

d'abord développé un prototype qui a été testé sur le réseau de fibres optiques de Swisscom. L'appareil a permis d'échanger une clé de cryptage entre deux stations connectées chacune à un PC par un port USB. Concrètement, la première caractéristique importante d'un système de cryptographie quantique est le débit de la clé. Celui-ci va de quelques centaines à quelques milliers de bits par seconde, suivant la distance. Cette valeur est basse par rapport au débit des systèmes de télécommunication actuels. Il s'agit toutefois du prix à payer en échange d'une sécurité absolue par les lois de la physique quantique. Deuxièmement, la distance de transmission joue aussi un rôle important. Bien que les fibres optiques soient constituées de verre de très haute qualité, elles ne sont pas parfaitement transparentes. Il arrive ainsi qu'un photon soit absorbé lors de sa propagation et n'atteigne pas l'extrémité de la fibre optique. Dans les systèmes de télécommunication conventionnels, des répéteurs sont utilisés pour régénérer le signal. Ils sont espacés d'environ 80 km et amplifient le signal optique. En cryptographie quantique, il n'est pas possible d'utiliser de tels répéteurs. Tout comme les espions, ils corrompent la transmission et introduisent des erreurs et le débit décroît avec la distance. En résumé, plus la distance devient grande, plus le nombre de photon transmis devient faible pour permettre l'établissement d'une clé.

## Des progrès déjà en 2004 avec l'archivage électronique

Pour faire davantage connaître son savoir-faire, l'entreprise genevoise avait assuré en 2004 le premier archivage de données



Nœud du réseau SwissQuantum situé à l'Université de Genève.

sans faille grâce à la cryptographie quantique. id Quantique était associée pour la circonstance à l'UNIGE ainsi qu'à VTX Deckpoint, une autre société genevoise active dans les technologies de l'information (accès internet, hébergement, sécurité et applications ASP). En mars dernier, dans le cadre du projet SwissQuantum, id Quantique et l'UNIGE ont déployé un réseau pilote dédié à la recherche, au développement, à des démonstrations et activités de formation dans le domaine des communications quantiques (lire encadré). Mais au cours des derniers mois, plusieurs articles mettant en cause la sécurité de la cryptographie quantique sont parus dans la presse non spécialisée. «Il est important de rappeler que les vulnérabilités qui y étaient présentées n'ont pas trait au principe de la cryptographie quantique, mais à certaines implémentations connexes. La présence de failles dans une implémentation est un problème qui concerne tous les systèmes de sécurité, qu'ils soient basés sur la cryptographie classique ou quantique», considère Grégoire Ribordy.

Toujours est-il que des systèmes de sécurisation des réseaux basés sur les principes d'échange de la mécanique quantique ne sont plus très loin de devenir une réalité. Selon la plate-forme web Techno-science.net, des chercheurs britanniques ont réalisé un saut de géant dans les ordres


de grandeur des performances de la cryptographie quantique. L'équipe a démontré que des clés quantiques pouvaient être envoyées le long d'une fibre optique de 20 kilomètres avec un débit supérieur à 1 Mbit/s. Cette performance pourrait permettre à des utilisateurs de communiquer avec une sécurité totale à travers les réseaux informatiques. Technologiquement, cette discipline est suffisamment mûre pour la commercialiser à grande échelle afin de sécuriser toutes les transactions (voix, données, vidéos, etc.), raison pour laquelle id Quantique déploie ses premiers systèmes pour essayer de convaincre non seulement les instituts bancaires, les centres d'archivages, mais aussi les bâtiments gouvernementaux ou toute firme désireuse de protéger encore davantage ses réseaux.

#### Un Swiss Technology Award en 2004

id Quantique est une société anonyme non cotée en bourse dont le siège est à Genève. Elle a été créée en octobre 2001 par quatre chercheurs de l'Université de Genève et a l'ambition de devenir le leader dans le domaine de la sécurisation des communications au moyen de la photonique quantique. L'entreprise genevoise a développé le premier système commercial de cryptographie quantique, ainsi que le premier générateur quantique de nombres aléatoires. Les

produits de la société visent le marché des applications cryptographiques de haute sécurité et ont le potentiel d'augmenter de façon drastique la confidentialité des communications numériques, en résolvant les problèmes de la création et de l'échange de clés cryptographiques.

La société a été soutenue dès sa fondation par le réseau CCSO, ainsi que par l'initiative CTI Startup, qui lui a décerné son «CTI-Startup label» en juin 2004. Fin 2003, id Quantique a levé un million d'euros auprès du fond de capital risque i2i, basé au Luxembourg. La société a été distinguée en novembre 2001 lors des European Innovation Awards décernés par le Wall Street Journal Europe. Elle a aussi reçu les prix Technologie Standort Schweiz et de Vigier

en 2002 et Swiss Technology Award en 2004. id Quantique est l'un des partenaires du projet Secoqc, l'initiative européenne pour la recherche et le développement dans le domaine de la cryptographie quantique. La société emploie actuellement une quinzaine de collaborateurs. Par ailleurs, id Quantique vient d'annoncer qu'elle va collaborer avec Siemens IT Solutions and Services (Hollande), l'un des principaux intégrateurs mondiaux pour la commercialisation de ses produits de chiffrement, avec et sans distribution quantique de clef. (micronarc) 

Info :  
[www.idquantique.com](http://www.idquantique.com)  
[www.swissquantum.com](http://www.swissquantum.com)  
[www.micronarc.ch](http://www.micronarc.ch)

## en filigrane

### Le premier réseau quantique durable

En mars dernier, dans le cadre du projet SwissQuantum, l'Université de Genève (UNIGE) et ses partenaires ont déployé un réseau quantique pilote. Il est aujourd'hui mis en œuvre et restera opérationnel durant plusieurs mois pour servir à la recherche, au développement, à des démonstrations et à des activités de formation dans le domaine des communications quantiques. SwissQuantum est un projet lancé lors des élections fédérales d'octobre 2007, qui consistait à sécuriser, par cryptage quantique, un lien critique existant entre le lieu du dépouillement et le centre de calcul de l'Etat de Genève. Ce procédé est désormais utilisé pour les élections genevoises : il a notamment servi pour la Constituante en automne 2008 et servira en octobre prochain à l'occasion des élections cantonales. Or, un nouveau réseau pilote de cryptographie quantique, déployé dès aujourd'hui par l'UNIGE, sera, lui, opérationnel durant plusieurs mois. Il servira pour des activités de recherche, de développement, de démonstration et de formation dans le domaine des communications quantiques. Technologie exploitant les lois de la physique quantique pour garantir la confidentialité des communications transmises au travers de réseaux optiques, la cryptographie quantique fait l'objet de travaux de recherche depuis une quinzaine d'années. Jusqu'à présent, les efforts des spécialistes se sont concentrés sur les applications dites «point à point». Si quelques réseaux quantiques comportant plus de deux nœuds ont déjà été déployés (aux Etats-Unis, en Europe, en Afrique du Sud et en Chine), leur utilisation n'a jamais dépassé quelques semaines et relevait de démonstrations plus ou moins artificielles.

Le réseau SwissQuantum comporte trois nœuds situés dans la région genevoise : à l'UNIGE, à l'Ecole d'ingénieur-e-s de Genève et au CERN. Ces nœuds forment un triangle et sont connectés par des fibres optiques conventionnelles mises à disposition par le Centre des technologies de l'information de l'Etat de Genève. Le réseau est notamment sollicité pour sécuriser une liaison à haute vitesse (10 gigabits) entre le CERN et l'UNIGE. Il revient à l'Ecole d'ingénieur-e-s de Genève de tester et de valider les performances du réseau, ceci de manière indépendante. D'autres services cryptographiques sont aussi disponibles sur le réseau.