La cryptographie quantique en bref

Le groupe du prof. Nicolas Gisin, de la Faculté des sciences de l'Université de Genève (UNIGE), a développé la cryptographie quantique à partir du milieu des années 1990. Cette technologie permet avant tout de sécuriser les communications sur les réseaux de fibres optiques.

Pour bien exposer le principe de la cryptographie quantique, le recours à une illustration simplifiée s'avère utile. L'échange de messages entre un expéditeur et un destinataire au moyen d'un système de communication conventionnel peut être comparé à un match de tennis. L'expéditeur du message prend une balle de tennis et y inscrit le message qu'il souhaite faire parvenir à son partenaire. Il lui envoie alors cette balle. Le destinataire l'attrape et lit le message. Dans cette situation, rien n'empêche une tierce personne placée entre les deux joueurs d'attraper la balle de tennis avec un filet à papillons, de prendre connaissance du message, puis de la renvoyer au destinataire. Et les deux joueurs ne remarquent pas que leur communication est interceptée.

Toutefois, si, au lieu d'utiliser des balles de tennis, les joueurs utilisent des bulles de savon, une interception devient impossible. L'individu touchant la bulle de savon la fait instantanément éclater, interrompant, par la même occasion, la communication.

En pratique, il est clair que les réseaux de communication modernes n'utilisent pas des balles de tennis, mais plutôt des impulsions lumineuses voyageant le long de fibres optiques. Ces impulsions sont constituées d'un grand nombre de particules de lumière appelées photons. Un espion peut intercepter ces impulsions en en prélevant un petit nombre. Dans un système de cryptographique quantique, on réduit le nombre de photons par impulsion au minimum: un seul photon. Objet microscopique, un photon est extrêmement fragile. Si un individu le touche, il le perturbe, ce qui a pour conséquence de révéler son intervention. Les lois de la physique quantique stipulent en effet qu'il n'est pas possible d'observer un objet quantique sans le modifier (principe d'incertitude d'Heisenberg).

La cryptographie quantique développée à l'UNIGE et portée au stade industriel par *id Quantique* repose sur ces principes.