La cryptographie est à réinventer

EXPO L'art de l'écriture secrète résistera-t-il à l'avènement de l'ordinateur quantique ?

▶ Une exposition sur la cryptographie se tient jusqu'en mai 2018 au Mundaneum à Mons.

▶ Les méthodes de protection des données actuelles seront obsolètes lorsque l'ordinateur quantique verra le jour.

Top secret ! » C'est le nom de l'exposition qui a ouvert ses portes ce mardi au Mundaneum à Mons, mettant la cryptographie à l'honneur. La quoi ? La science du secret. C'est l'ensemble des techniques qui permettent d'encoder une information de manière à pouvoir vérifier son authenticité et à en contrôler l'accès. Passeport, carte bancaire, carte d'identité, paiement en ligne, vote électronique, objets connectés, la cryptographie fait partie de notre quotidien. Mais les techniques d'aujourd'hui ne sont en rien celles du monde de demain.

Si elle est notre amie, car c'est d'elle que viendront les futures clés de cryptage, la recherche en physique quantique est également une menace pour notre société connectée. En effet, la possibilité de parvenir à construire l'ordinateur quantique croît de jour en jour. Or, les capacités de calculs démentiels de cet engin décrypteraient rapidement les messages chiffrés par les meilleurs systèmes utilisés aujourd'hui. Et par là, rendraient caduques les méthodes de cryptage actuelles.

Vous êtes vous jamais demandé comment vos transactions bancaires sur internet étaient protégées ? La méthode la plus couramment utilisée se nomme « chiffrement RSA », acronyme révélant les initiales de ses trois inventeurs en 1977. Son principe repose sur une clé publique et une clé privée.

Cette machine à crypter les dépêches était utilisée par l'agence de presse Havas dans les années 20 et 30. © D.R.

Pour payer, vous introduisez différents numéros repris sur votre carte de crédit. Lorsqu'ils sont envoyés au destinataire, ces numéros sont chiffrés en utilisant la clé publique de ce dernier. Si celle-ci est connue de tous, la clé privée est uniquement connue du destinataire. Et elle seule permet de déchiffrer les numéros bancaires envoyés. Vos données sont donc a priori protégées.

Sauf que cette clé privée n'est pas arbitraire. Elle est constituée de deux nombres premiers, dont la multiplication donne la clé publique. Or cette dernière est un très grand nombre. De sorte que si sa valeur est connue, parvenir à identifier les deux nombres premiers dont elle est issue est très complexe. Trop complexe pour nos ordinateurs actuels. Mais pas pour l'ordinateur quantique. Cette opération de factorisation, il la fera sans la moindre difficulté.

L'existence de cette épée de Damoclès est connue depuis 1994 et les travaux du mathématicien Peter Shor. Depuis, c'est la course folle. Des scientifiques mettent toute leur énergie à faire naître l'ordinateur quantique pendant que d'autres tentent d'inventer des systèmes de cryptage que celui-ci ne pourra pas briser.

Ces approches post-quantiques ont des noms barbares : des chercheurs s'arrachent les cheveux sur la cryptographie multivariable, à base de hachage, de codes correcteurs ou encore de réseaux.

Passeport, carte bancaire, carte d'identité, paiement en ligne, vote électronique… : la cryptographie fait partie de notre quotidien

Mais la « cryptographie quantique », ainsi nommée, n'est-elle pas sur les rails ? Si, mais elle ne serait pas suffisante pour contrer les capacités de décryptage du futur ordinateur quantique. Notamment, à cause de l'absence de clé publique.

En effet, en cryptographie quantique, une clé commune de déchiffrement est construite entre l'expéditeur et le destinataire. Elle est une ribambelle de bits représentés par des photons lancés dans de la fibre optique tendue entre eux deux. Chaque photon est polarisé selon une certaine direction afin de porter la valeur 0 ou 1 d'un bit. Quand un espion intercepte ces photons, il bloque leur polarisation, révélant ainsi son acte malfaisant à l'expéditeur et au destinataire qui changent alors de clé.

Ce système, bien que marginal, existe déjà aux USA. La société Battelle Memorial Institute a ainsi créé un réseau de fibre optique de plus d'une dizaine de kilomètres entre deux de ses sites. Et ce, pour échanger des informations confidentielles. ■

LÆTITIA THEUNIS

Exposition « Top Secret ! », du mardi 10 octobre au dimanche 20 mai 2018 au Mundaneum, 76 rue de Nimy à Mons.

L'INVENTEUR

Alan Turing, l'homme qui a « cassé » Enigma

L'essor de la cryptographie, on le doit à l'Anglais Alan Turing (1912-2012) et à l'Américain Claude Shannon (1916-2016) *« Ils ont façonné d'une manière indélébile notre monde informatisé et numérique. Et ce, en contribuant aux progrès nécessaires pour gagner la Deuxième Guerre mondiale*, explique Jean-Jacques Quisquater, spécialiste international de la cryptographie, professeur émérite de l'UCL et commissaire scientifique de l'exposition « Top secret ! ». *Ils ont ainsi participé à la protection des messages confidentiels venant des commandements alliés, inventant au passage si pas en tout, en majeure partie, la technologie qui a conduit au smartphone, au CD, aux codes secrets très sûrs. Ils ont aussi contribué à casser les codes allemands, y compris de la fameuse machine Enigma, dont un exemplaire original est présenté à l'exposition. »*

L.TH.