# Chiffrement : la machine Enigma de l'ère quantique voit le jour

La machine Enigma quantique existe. Des chercheurs de l'université de Rochester (Etat de New York) et du NIST (National Institute of Standards and Technology), associés à d'autres équipes de recherche américaines, sont parvenus à mettre au point la première machine de chiffrement quantique. Celle-ci est capable d'envoyer des messages codés, exploitant une clef plus courte que le message lui-même.

Cette expérience découle des travaux de physiciens au cours des 10 dernières années. Ceux-ci ont montré que les propriétés quantiques permettaient d'envoyer un message parfaitement sécurisé via une clef significativement plus courte que le message à proprement parler. Avec la physique classique, pour résister aux assauts d'un adversaire ayant des capacités de calcul infinies, la clef doit être au moins aussi longue que le message lui-même pour garantir que le code restera inviolé (selon une loi publiée en 1949 par le mathématicien et ingénieur Claude Shannon).

## Opération quantique aléatoire

La machine à chiffrer quantique fonctionne via l'encodage de l'information dans un photon et via l'altération de l'état de ce dernier par une opération aléatoire. Pour restaurer l'information, il faut appliquer l'opération inverse. C'est cette séquence d'opérations de transformation qui est stockée dans la clef, que doivent posséder l'émetteur et le récepteur. Mais, contrairement au procédé classique consistant à ajouter un nombre aléatoire à chaque bit, ce mécanisme permet de conserver une taille de clef réduite autorisant, selon les chercheurs, l'envoi de la prochaine clef avec le message lui-même.

L'appareil mis au point par les chercheurs consiste en un canon à photons. Le flux de particules passe au travers d'un masque, un modulateur de lumière, qui permet de greffer l'information à l'onde des photons et d'ajouter une opération codant ces données et empêchant leur déchiffrement par un tiers. « *Nous avons démontré ce phénomène avec un prototype enfermant 6 bits par photon (incluant le message, la prochaine clef de chiffrement et des bits de correction d'erreurs) tout en utilisant une clef secrète inférieure à 6 bits par particule et en demeurant parfaitement sûrs par rapport à la théorie de l'information* », explique l'équipe de recherche. Lors de ses expériences, cette dernière a transmis 420 paquets de 63 photos.

## Complémentaire à la distribution quantique de clefs

Autrement dit, les huit chercheurs ayant participé à ces travaux ont bâti l'équivalent de la machine Enigma (le nom de l'appareil utilisé par les nazis pour envoyer leurs messages codés) de l'ère quantique. Rappelons que le code de la machine Enigma de l'Allemagne nazie avait été cassé par les alliés, qui avaient regroupé leurs meilleurs spécialistes à Bletchley Park, notamment le mathématicien anglais Alan Turing.

Les chercheurs notent que leur invention peut être couplée à la technique de distribution quantique de clefs, permettant à deux parties d'échanger une clef secrète sur des canaux de communication standards (via la détection de toute tentative d'espionnage). La machine Enigma quantique faisant alors figure de complément naturel à ce principe d'échange de clefs. Un assemblage qui, sur le papier, permettrait de bâtir de vrais mécanismes de chiffrement quantique de bout en bout.

**A lire aussi :**

L'ordinateur quantique va rendre tout le chiffrement obsolète

IBM met l'ordinateur quantique à la portée de tous, en mode Cloud

Un ordinateur quantique casseur de clé de chiffrement

**crédit photo © Pavel Ignatov / Shutterstock**