La cryptographie quantique ou la distribution quantique de clés

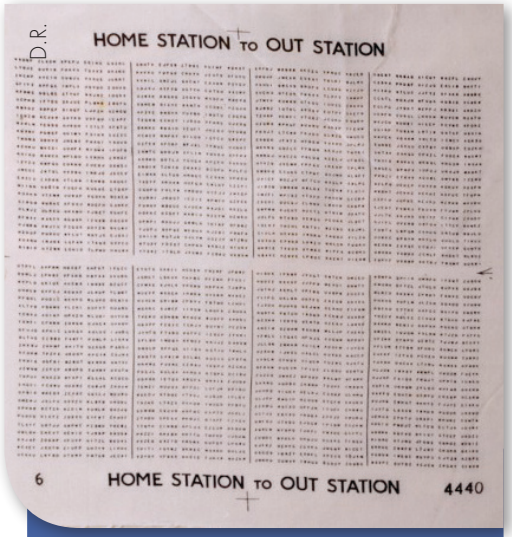
Contrairement à son nom, la cryptographie quantique n'est pas de la cryptographie, car elle n'est pas une méthode de cryptage d'un message en utilisant la mécanique quantique. On devrait plus correctement la nommer « distribution quantique de clés » comme c'est le cas en anglais. Il s'agit en effet d'un ensemble de protocoles permettant de distribuer une clé de chiffrement entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information.

Un des problèmes principaux dans le domaine de la cryptographie est d'une part de chiffrer l'information à transmettre, et d'autre part de partager avec le destinataire la méthode et la clé pour le déchiffrement du message. Le point faible est très souvent la transmission de cette clé. On peut la chiffrer par une autre technique, mais on ne fait que déplacer le problème. Cette autre technique utilisant très probablement une autre clé qu'il faudra bien transmettre...

Ici, la physique quantique offre une solution élégante pour partager une clé entre deux personnes grâce à l'impossibilité pour un espion de dupliquer les informations transmises sans se faire repérer.

Le phénomène d'intrication quantique a été découvert au niveau théorique par Einstein et Schrödinger dans les années 1930. Dans le transport de clés «quantiques» l'information est transportée par les photons, ces composants élémentaires de la lumière. Chaque photon peut être polarisé, c'est-à-dire que l'on impose une direction à son champ électrique.

La distribution quantique de clés



One Time Pad, feuillet microfilmé d'un agent du SOE

Lorsque deux personnes veulent communiquer secrètement (on appelle généralement l'émettrice «Alice» et le récepteur «Bob» l'espionne étant appelée «Eve») elles s'envoient des messages codés. Pour les décrypter, il faut que les deux personnes disposent de la « clé » qui permettra de les déchiffrer. Au départ, seule Alice la détient. Et il ne faut surtout pas qu'elle soit interceptée quand elle est envoyée à Bob. C'est là que la cryptographie quantique intervient. Alice envoie la clé sous forme de photons émis un par un dans une fibre optique, une prouesse technologique particulièrement difficile. Bob réceptionne ces photons et mesure leurs propriétés. Ce sont elles qui vont lui permettre de reconstituer la clé. Pour s'en emparer, Eve doit elle aussi observer ces photons sans laisser de trace suspecte. Or la

physique quantique explique qu'il est impossible d'observer un photon sans en modifier les propriétés. C'est le célèbre principe d'incertitude d'Heisenberg. En d'autres termes, Alice et Bob peuvent, en s'échangeant des informations par un canal standard, détecter immédiatement toute tentative d'espionnage : la cryptologie quantique est théoriquement inviolable.

Patrice Lefort-Lavauzelle
Président de l'Association des entreprises partenaires de la Défense et membre du Comité de Liaison Défense (CLD) du MEDEF

Un peu d'humour…

Une méthode de chiffrement parfaitement sûre existe-t-elle ?

Une méthode parfaitement sûre est une méthode telle que, l'adversaire interceptant le message, même ayant à sa disposition une puissance de calcul infinie, ne peut pas retrouver la moindre information concernant le message en clair à partir du message chiffré.

Une telle méthode théoriquement parfaite existe : Le « masque jetable » (One Time Pad, OTP) également appelé chiffre de Vernam, utilisé notamment par les membres du Special Operations Executive (SOE) durant la Seconde Guerre mondiale. Ce dispositif de chiffrement est le seul qui soit théoriquement impossible à casser. Sa clé répond à trois impératifs :

- Etre aussi longue que le texte à chiffrer.
- Etre parfaitement aléatoire.
- N'être utilisée que pour chiffrer un seul message, puis être immédiatement détruite.

L'intérêt considérable de cette méthode de chiffrement est que si les trois règles ci-dessus sont respectées strictement, le système offre une sécurité théorique absolue.

Ce procédé impose néanmoins quelques contraintes. La première est la longueur et le nombre des clés nécessaires (surtout s'il y a plusieurs correspondants) avec le problème de leur transmission, de leur stockage et de leur identification. Ensuite générer des clés réellement aléatoires nécessite des moyens complexes (pour la petite histoire, durant la Guerre froide, les soviétiques employaient des «lanceurs de dés» : leur travail consistait à lancer des dés toute la journée et à noter le résultat…). Enfin, garantir l'utilisation unique de chaque clé, même à des années d'intervalle, pose des problèmes importants d'organisation.

La seule méthode véritablement sûre pour transmettre des clés est le transport physique, typiquement dans une valise diplomatique sous bonne escorte, ou alors... la distribution quantique. Un procédé utilisé par la Defense Advanced Research Projects Agency (DARPA) américaine, théoriquement parfaitement sûre mais comportant des limites contraignantes concernant la distance maximale et le débit.

La distribution quantique de clés est-elle finalement si fiable ?

Le protocole quantique de transmission de la clé n'est peut-être pas aussi inviolable que l'on pensait. Un groupe de recherche norvégien a présenté une faille dans ce protocole utilisable pour récupérer intégralement la clé sans que ni l'expéditeur, ni le destinataire, ne soient au courant

Les chercheurs utilisent les caractéristiques d'un détecteur de photons. Celui-ci peut être rendu aveugle s'il est noyé sous un flux important de photons. Il devient ainsi totalement insensible aux photons envoyés un par un. Le détecteur peut être déclenché à nouveau si un flux plus brillant encore lui est envoyé. Ainsi, il est possible d'intercepter les photons envoyés par l'expéditeur et mesurer la clé en utilisant la même configuration de détecteur que le destinataire.

La solution pour contrer cette action serait de mesurer l'intensité du flux de photons, sous réserve bien entendu de ne pas perturber la transmission de la clé.

PLL