CAS D'APPLICATION

Comment la cryptographie quantique fonctionne-t-elle ?

L'affaire de la NSA a de nouveau catapulté le sujet de la protection des données et, plus spécifiquement, d'échange de données au cœur de l'actualité des médias et du grand public. Comment empêcher que des données puissent être interceptées par un tiers ? La solution à ce problème se trouve dans la cryptographie : le message doit être codé. Cependant, cette mesure de chiffrement comporte également quelques risques. Que se passe--il si la clé d'échange est elle-même interceptée ? C'est précisément là où la cryptographie quantique entre en jeu.

L'idée fondamentale sur laquelle repose la notion de distribution de clé quantique (*Quantum Key Distribution* - QKD) est d'employer des photons uniques au lieu de paquets entiers de photons. De cette façon une oreille indiscrète (écoute clandestine désignée sous le nom d'« Ève » dans la mécanique quantique) ne peut pas simplement détourner les photons qui sont envoyés de la personne A à la personne B (désignée respectivement sous le nom de « Alice » et de « Bob, », dans la mécanique quantique). Ève devrait détecter et puis copier les photons pour empêcher que l'interception soit détectée par Bob. C'est précisément ce que la mécanique quantique rend impossible (ce qu'on appelle le théorème de non-clonage).
Le schéma 1 dépeint à quoi la génération de clé pour des données de codage et de décodage peut ressembler. Ce protocole désigné par BB84 (développé par Bennett et Brassard en 1984) emploie la polarisation des photons comme moyen de génération d'une séquence de clé. Alice sélectionne l'un des quatre états de polarisation – H (horizontal), V (vertical), +45°, et -45° – et envoie un tel photon à Bob. Elle doit d'abord indiquer quelle valeur de bit les deux états de polarisation arrangés orthogonalement ont : 0 ou 1. Dans notre exemple, H correspond à 0, V correspond à 1, 45° correspondent à 0, et -45° correspondent à 1. Si Bob reçoit un tel photon, il décide soit de mesurer sur la base H/V ou 45°/-45° et note finalement l'état de polarisation (et ainsi la valeur de bit) du photon. Bob communique avec Alice dans le sens classique, non sécurisé et ils comparent leur sélection de base. Cette information, qui est inutile à Ève parce qu'elle ne connaît pas les résultats précis, est suffisante à Alice et Bob pour déterminer quelles valeurs de bits ils peuvent utiliser pour leur clé. Un développement ultérieur du protocole BB84 utilise des photons liés, qui sont fortement corrélés dans leurs propriétés, et qui sont envoyés d'une source unique à Alice et à Bob simultanément. Une telle source a été développée, par exemple, par l'équipe expérimentale des physiciens du groupe de photonique du prof. Weihs à l'université d'Innsbruck : une source de Sagnac pulsée de photons de polarisation liée. Ici on emploie un cristal non linéaire qui produit deux photons à une longueur d'onde de 808 nm de plus basse énergie à partir d'un photon unique de plus de haute énergie à 404 nm. Les photons sont détectés utilisant deux SPADs (*Single Photon Counting Module*) de type Count de Laser Components.
Aussi sûres que soient ces méthodes dans la théorie, dans la pratique il y a en réalité beaucoup de risques d'erreurs. La plus importante source d'erreur réside dans la qualité des détecteurs de photons simples qu'Alice et Bob utilisent. Dans la théorie, les détecteurs disponibles sont parfaits, identiques, et ont une efficacité de détection de 100 % ; cependant, dans la pratique, ce n'est jamais le cas. C'est précisément cette différence dans l'efficacité de détection de deux détecteurs que les pirates en informatique quantique utilisent pour accéder à la clé de chiffrement. Une méthode alternative aveugle le SPAD, à l'aide d'une impulsion lumineuse, et utilise ce temps d'aveuglement du détecteur pour intercepter l'information. Grâce à l'identification des sources d'erreurs exploitées par les pirates en informatique quantique, des groupes de recherche ont pu travailler sur des approches pour proposer des solutions à ces problèmes et développer des versions du protocole QKD selon des méthodes de mesures indépendantes du dispositif.
L'industrie peut également contribuer à rendre les méthodes plus efficaces et précises. L'échange constant entre la recherche et l'industrie est ainsi extrêmement important ●

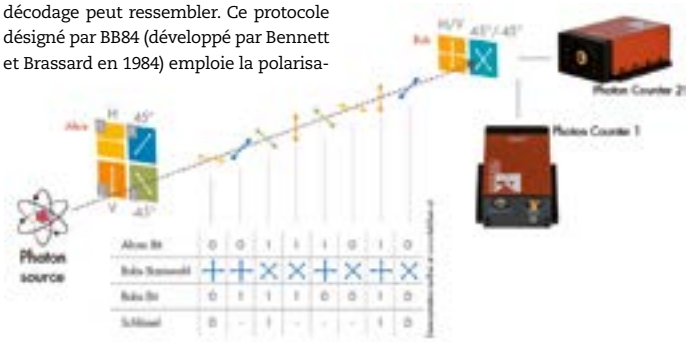

Schéma 1 (source : www.teilchen.at)

+ SUR LE WEB
www.lasercomponents.fr

France
Laser Components S.A.S.
Tel: +33 1 39 59 52 25
Fax: +33 1 39 59 53 50
info@lasercomponents.fr
www.lasercomponents.fr