LASER COMPONENTS®

Comment Fonctionne la Cryptographie Quantique

Champs d'Application des Modules COUNT®

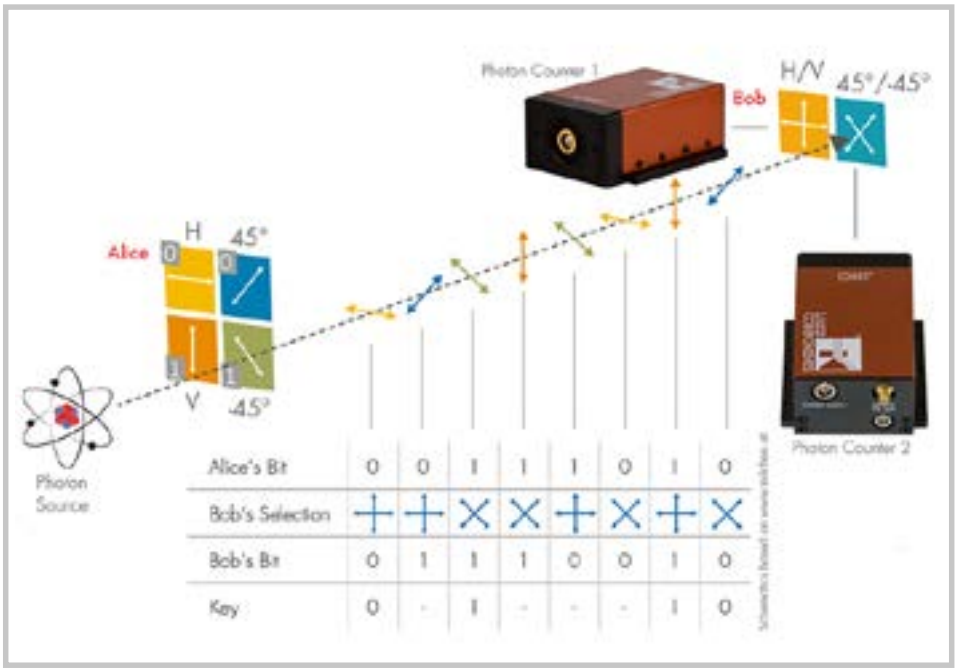
La sécurité des données et l'échange de données sont des sujets d'une importance croissante. Comment empêcher que des données soient interceptées par un tiers? La solution réside dans la cryptographie : Le message doit être codé. Mais que se passe-t-il si l'échange de clés est intercepté? C'est là qu'intervient la cryptographie quantique.

L'idée fondamentale de la distribution de clés quantiques (QKD) est d'utiliser des photons uniques au lieu de paquets entiers de photons. De cette façon, un écouteur (appelé „Eve" en mécanique quantique) ne peut pas simplement détourner les photons qui sont envoyés de la personne A vers la personne B (appelés respectivement „Alice" et „Bob" en mécanique quantique). Eve devrait copier puis détecter les photons pour empêcher l'interception d'être détectée par Bob. C'est précisément ce que la mécanique quantique rend impossible (le „théorème de non clonage").

La figure 1 (page suivante) montre à quoi peut ressembler la génération de clés pour le codage et le décodage des données. Ce protocole appelé BB84 (développé par Bennett et Brassard en 1984) utilise la polarisation des photons comme moyen de générer une séquence 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 la valeur binaire des deux états de polarisation disposés orthogonalement : 0 ou 1. Dans notre exemple, H correspond à 0, V correspond à 1, 45° correspond à 0, et -45° correspond à 1. Si Bob reçoit un tel photon, il décide de mesurer sur la base de H/V ou de 45°/-45° et note finalement l'état de polarisation (et donc la valeur du bit) du photon. Bob communique avec Alice au sens classique du terme, et ils comparent leurs sélections de base. Cette information, qui n'est d'aucune utilité pour Eve car elle ne connaît pas les résultats exacts, suffit à Alice et Bob pour déterminer les valeurs binaires qu'ils peuvent utiliser pour leur clé[1].

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

Figure 1: Schéma d'échanges de clés quantiques entre Alice et Bob



Un autre développement du protocole BB84 utilise des photons intriqués, dont les propriétés sont fortement corrélées, qui sont envoyés d'une source unique à Alice et Bob simultanément. Une telle source a été développée, par exemple, par les physiciens expérimentaux du groupe de photonique du professeur Weihs à l'université d'Innsbruck : une source Sagnac pulsée de photons liés en polarisation[2]. On utilise ici un cristal non linéaire qui produit deux photons de faible énergie à une longueur d'onde de 808 nm à partir d'un photon de plus forte énergie à 404 nm. Les photons sont détectés à l'aide de deux "COUNT" SPADs de LASER COMPONENTS.

Aussi sûres que ces méthodes soient en théorie, en pratique, il y a beaucoup de marge d'erreur. Les sources d'erreur les plus importantes sont les détecteurs de photons uniques qu'utilisent Alice et Bob. En théorie, les détecteurs disponibles sont parfaits, identiques, et ont une efficacité de détection de 100% ; cependant, en pratique, ce n'est jamais le cas. C'est précisément cet écart dans l'efficacité de détection de deux détecteurs que les pirates quantiques utilisent pour accéder à la clé[3].

Une autre méthode consiste à „aveugler" les SPAD à l'aide d'une impulsion lumineuse et à utiliser le „temps mort" du détecteur pour intercepter les informations[4].

Grâce à l'identification des sources d'erreur par les pirates quantiques, les groupes de recherche ont pu travailler sur des approches pour résoudre ces problèmes et développer une version „indépendante des unités de mesure" du QKD[5]. L'industrie peut également contribuer à rendre les méthodes plus efficaces et plus précises. L'échange constant entre la recherche et l'industrie est donc extrêmement important.

[1] http://www.weltderphysik.de/gebiet/technik/quanten-technik/quanten-kryptographie/

[2] http://www.uibk.ac.at/exphys/photonik/people/parametric-downconversion.html

[3] http://arxiv.org/abs/quant-ph/0702262

[4] http://arxiv.org/pdf/1008.4593v2.pdf

[5] http://arxiv.org/abs/1109.1473

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