TeraXion

An indie Semiconductor Company

ARTICLE

Distribution de clés quantiques en communications optiques

Auteurs: Guillaume Brochu[1], Marc-André Laliberté[2]

1. Chercheur, TeraXion
2. Gestionnaire de ligne de produits, Communications optiques, TeraXion.

Surmonter les défis techniques que pose la DQC

La distribution quantique de clés (DQC) dans le contexte des communications quantiques est une méthode de communication sécurisée qui permet à deux parties de produire des clés secrètes partagées qui sont utilisées par la suite pour crypter et décrypter des messages. Reposant sur les principes de la mécanique quantique, l'action de mesurer un système quantique crée des anomalies détectables, permettant de repérer un espion.

À l'heure où le gouvernement, les banques, le secteur médical et d'autres secteurs réglementés sont en pleine transformation numérique, la DQC est un outil important pour améliorer la sécurité des communications sur les réseaux à fibres optiques en renforçant le cryptage classique du trafic Internet et d'autres canaux de communication. En effet, les efforts massifs de recherche et de développement déployés à l'échelle mondiale sur les ordinateurs quantiques et leur capacité théorique à percer les algorithmes de chiffrement classiques constituent une menace réelle pour nos données critiques protégées par ces algorithmes, lesquelles peuvent être stockées au moment de la transmission et déchiffrées ultérieurement.

Bon nombre des chefs de file sur le marché mondial des communications investissent dans la recherche et le développement de systèmes de communications quantiques. Les premiers pionniers ont abordé la DQC avec un schéma de distribution « préparation et mesure » en utilisant des protocoles tels que BB84, ou ses variantes apparentées. Il s'agit de méthodes permettant de communiquer en toute sécurité une clé privée d'une partie à une autre dans un canal quantique dédié en exploitant le principe de superposition à l'aide de photons [1-5]. En revanche, un autre schéma repose sur l'intrication quantique qui consiste à coder les clés dans des paires de photons intriqués répartis entre les deux parties (protocoles tels que E91 ou BBM92) [6,7].

La recherche sur la DQC et d'autres technologies quantiques s'accélère rapidement dans le monde entier, et de nouvelles approches pour cette technologie sont désormais envisagées. Ces récents systèmes utilisent des protocoles tels que la DQC à champ double (Twin-field QKD/TF-QKD) avec des lasers à faible bruit verrouillés par des boucles à verrouillage de phase, ou des schémas de DQC à variables continues (CV-QKD) qui nécessitent généralement des lasers à faible bruit et à spectre étroit [8,9].

DQC avec impulsions atténuées

Les systèmes basés sur des schémas de DQC appelés « préparation et mesure » sont les plus courants dans les mises en application pratiques actuelles et, bien que les recherches récentes proposent encore des modèles de systèmes uniques, ils partagent certains principes de base communs.

Dans tous les schémas, Alice envoie à Bob des impulsions de photons polarisés atténués au niveau du quasi-monophoton, tandis qu'Ève, l'espionne, tente de les intercepter pour récupérer des renseignements sur la clé secrète. La figure 1 présente une description simplifiée du système à fibres optiques requis pour la DQC utilisant des impulsions atténuées.

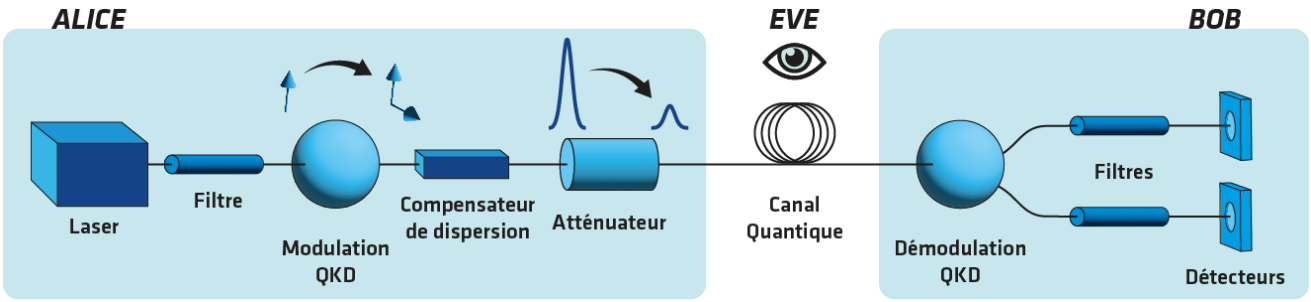

Figure 1. Description simplifiée d'un système de DQC à impulsions atténuées sur fibre optique.

Un laser monomode est modulé pour produire un train d'impulsions qui est ensuite multiplexé en polarisation. Les qubits (ou bits quantiques, l'unité de base des renseignements quantiques) de la clé secrète sont codés dans l'état de phase et de polarisation des impulsions. Avant de quitter la boîte de l'émetteur du côté d'Alice, le train d'impulsions modulées est fortement atténué de manière à l'amener au niveau du photon quasi unique, de sorte que si Ève essaie de capter certaines des impulsions, celles-ci ne seraient pas récupérables par Bob et ne pourraient donc pas être utilisées pour créer la clé secrète. Du côté du récepteur (Bob), le démodulateur de DQC traite le signal reçu qui est transmis à deux détecteurs de photons uniques.

Les dispositifs de DQC améliorent les performances

La modulation et la démodulation de la DQC nécessitent généralement des interféromètres Mach-Zehnder asymétriques, des modulateurs de phase, des séparateurs et des combinateurs de polarisation, ainsi que des générateurs de nombres aléatoires quantiques. De plus, des composants optiques tels que des compensateurs de dispersion et des filtres spectraux sont parfois nécessaires pour améliorer les performances du système. Il convient de noter que le protocole de DQC utilisé et les sous-systèmes optiques associés sont plus compliqués que cette description simpliste (Fig.1), utilisée pour illustrer le rôle et l'importance des composants optiques, tels que les compensateurs de dispersion, les filtres à bande large et étroite et les lasers à faible bruit.

La réduction des pertes excessives est de première importance sur le canal quantique et dans la boîte de réception du côté de Bob, car tout photon perdu doit, selon le protocole de DQC, être considéré comme s'il avait été mesuré par Ève, ce qui réduit le taux de transmission des clés sécurisées utilisables.

Compensation de dispersion chromatique

Au niveau quantique, la dispersion chromatique élargit la distribution statistique du moment d'arrivée des photons aux détecteurs. Si la dispersion chromatique est trop importante, les photons peuvent manquer la fenêtre temporelle de détection, ce qui constitue une anomalie qui perturbe le transfert des clés secrètes

comme le ferait un affaiblissement optique. Par conséquent, lorsque l'on augmente la longueur des fibres pour le canal quantique, l'effet néfaste de l'affaiblissement et de la dispersion optiques s'accumule. Un compensateur de dispersion chromatique est généralement nécessaire pour les distances supérieures à 50 km. En général, le compensateur de dispersion est inséré avant l'atténuateur dans le boîtier de l'émetteur, du côté d'Alice.

Filtres à bande large et étroite

Outre l'affaiblissement et la dispersion, la diffusion non linéaire des photons du canal régulier adjacent, c'est-à-dire lorsque le canal quantique se trouve dans la même fibre que celle utilisée pour la transmission de données par multiplexage en longueur d'onde dense (DWDM) à une puissance optique plus élevée, ainsi que d'autres sources de bruit comme l'émission spontanée du laser, peut provoquer de fausses détections sur les détecteurs de photons uniques. Comme le taux de rejet des démultiplexeurs DWDM typiques n'est souvent pas suffisant, il peut être nécessaire d'utiliser des filtres à haut taux de rejet, à bande étroite et à faible perte en amont des détecteurs de photons uniques ou ailleurs dans le montage optique.

Les solutions de TeraXion pour la DQC

Au fil des années, TeraXion a développé plusieurs technologies et produits homologués qui pourraient répondre aux défis actuels et futurs des fabricants de systèmes de DQC :

Compensateurs de dispersion à faible perte

Le ClearSpectrum™ DCML de TeraXion gère la dispersion chromatique et couvre l'ensemble de la bande C pour améliorer les signaux de DQC sur de longues distances. Offrant une perte d'insertion inférieure à 3 dB pour des distances allant jusqu'à 200 km avec un seul module, ces compensateurs réduisent également les effets non linéaires intracanaux et intercanaux et présentent très peu de latence.

Filtres passe-bande étroits

Les solutions de filtrage optique avancées TFN et les filtres statiques réduisent l'effet néfaste de la dispersion non linéaire et d'autres sources de bruit optique dans le système de DQC. La DQC au moyen d'impulsions atténuées nécessite généralement des filtres à bande passante ayant une isolation spectrale élevée et une largeur de bande d'environ 2 à 20 GHz qui est déterminée par la fréquence de répétition des impulsions. Selon la bande passante requise et les autres défis liés à l'application, un module accordable en fréquence ou athermique peut être utilisé pour améliorer les performances du filtre et stabiliser sa longueur d'onde centrale. Ceci est particulièrement important lors de l'encodage d'information quantique dans les bandes latérales de fréquence d'un état cohérent atténué.

Filtres passe-bande ultra-étroits

Grâce à leur bande passante variant de 50 MHz à 500 MHz, les filtres UNF de TeraXion sont bien adaptés aux systèmes de DQC utilisant une source de photons intriqués. Ils peuvent, par exemple, être utilisés pour optimiser la bande passante à la suite du processus de conversion paramétrique spontanée (SPDC).

Lasers à faible bruit

Les composants de détection optique comme les lasers PureSpectrum™ de TeraXion offrent un contrôle précis de la rétroaction, un fonctionnement à bruit ultrafaible (largeur spectrale jusqu'à 20 kHz) et une stabilité supérieure de la longueur d'onde.

Les composants disponibles sur le marché permettent de réduire les coûts de démonstration et de faire progresser les systèmes jusqu'au point de la commercialisation. TeraXion souhaite établir des partenariats avec les fabricants de systèmes afin de faire évoluer la technologie avec eux. La gamme de composants de communications quantiques de TeraXion soutient l'avancement des technologies quantiques, de la recherche et du développement jusqu'à la commercialisation complète.

Que vous utilisiez des sources à photons uniques, des impulsions atténuées, des photons intriqués, la DQC à variables continues, la DQC à champ double ou une nouvelle approche, nos ingénieurs se feront un plaisir de discuter des défis que pose votre système.

Références

[1] YUAN, Z. L., DIXON, A. R., DYNES, J. F., et al. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. Applied Physics Letters, 2008, vol. 92, no 20, p. 201104 https://doi.org/10.1063/1.2931070

[2] ERAERDS P., WALENTA N., LEGRÉ M., et al. Quantum key distribution and 1 Gbps data encryption over a single fibre. New Journal of Physics, 2010, vol. 12, no 6, p. 063027 https://doi.org/10.1088/1367-2630/12/6/063027

[3] BOARON A., BOSO G., RUSCA D., et al. Secure quantum key distribution over 421 km of optical fiber. Physical review letters, 2018, vol. 121, no 19, p. 190502 https://doi.org/10.1103/PhysRevLett.121.190502

[4] MLEJNEK, Michal, KALITEEVSKIY, Nikolay A., et NOLAN, Daniel A. Modeling high quantum bit rate QKD systems over optical fiber. In : Quantum Technologies 2018. SPIE, 2018. p. 122-131 https://doi.org/10.1117/12.2306875

[5] CHEN, Yu-Ao, ZHANG, Qiang, CHEN, Teng-Yun, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 2021, vol. 589, no 7841, p. 214-219 https://doi.org/10.1038/s41586-020-03093-8

[6] TITTEL W., Brendel J., Zbinden H., and Gisin N. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. Physical Review Letters, 2000, vol. 84, pp. 4737 https://doi.org/10.1103/PhysRevLett.84.4737

[7] KAISER Florian, ISSAUTIER, Amandine, NGAH, Lutfi A., et al. A versatile source of polarization entangled photons for quantum network applications. Laser Physics Letters, 2013, vol. 10, no 4, p. 045202.CV-QKD https://doi.org/10.1088/1612-2011/10/4/045202

[8] PITTALUGA, Mirko, MINDER, Mariella, LUCAMARINI, Marco, et al.600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics, 2021, vol. 15, no 7, p. 530-535. https://doi.org/10.1038/s41566-021-00811-0

[9] HUANG, Duan, HUANG, Peng, LIN, Dakai, et al. High-speed continuous-variable quantum key distribution without sending a local oscillator. Optics letters, 2015, vol. 40, no 16, p. 3695-3698 https://doi.org/10.1364/OL.40.003695

TeraXion
An indie Semiconductor Company

teraxion.com

2716 rue Einstein
Québec City, Québec, CANADA G1P 4S8
+1 (877) 658-8372 / ultrafast@teraxion.com