Distribution d'intrication dans des canaux standards télécoms pour la cryptographie quantique haut débit

Djeylan Aktas[1], Bruno Fedrici[1,2], Laurent Labonté[1], and Sébastien Tanzilli[1]

[1] *Laboratoire de Physique de la Matière Condensée, Université Nice Sophia Antipolis, UMR CNRS 7336, Parc Valrose, 06108 NICE CEDEX, France*
[2] *Université Claude Bernard Lyon 1, 43 Boulevard du 11 Novembre 1918, 69100 Villeurbanne, France*

labonte@unice.fr

RÉSUMÉ

Nous proposons une association innovante entre la cryptographie quantique et le domaine des télécommunications dans le but de mettre en place un réseau de communication sécurisée répondant aux exigences de débit et de distances actuelles. Nous montrons que la combinaison de ces deux technologies permet de dépasser l'état de l'art tout en préservant la sécurité absolue des transactions des données.

MOTS-CLEFS : *télécoms; filtre à réseaux de Bragg; communication quantique; cryptographie.*

1. INTRODUCTION

En ce jour où la confidentialité des données transmises est un enjeu crucial de notre société, la cryptographie quantique (CQ) vient apporter des solutions dont la sécurité inconditionnelle repose sur les principes de la Physique Quantique, qui permet de révéler toute tentative d'espionnage. Si les concepts de la CQ sont aujourd'hui parfaitement maitrisés, les performances des protocoles sont limitées en terme de débit et de distance d'échange, principalement à cause de deux raisons. La CQ nécessite l'utilisation de signaux à très faible puissance, et d'autre part la copie du signal à transmettre est interdite, à l'instar des communications classiques. Cependant grâce aux propriétés exclusives qu'offrent la Physique Quantique, il est possible aujourd'hui de contourner ces contraintes expérimentales et d'envisager le déploiement pratique d'un réseau de communications quantiques. Parmi ces ressources, nous pouvons citer l'exemple de l'intrication de paires de photons ou encore la téléportation d'états quantiques [1-2]. En parallèle de ces développements, l'industrie des télécoms a bénéficié d'une grande effervescence durant ces 20 dernières années, et jouit aujourd'hui d'une grande maturité en proposant des composants dont les caractéristiques sont ajustables à la demande et les performances extrêmement intéressantes.

Nous proposons une association prometteuse entre la CQ et le domaine des télécoms, en exploitant les corrélations spectrales de paires de photons intriqués en énergie-temps dans des paires de canaux télécoms, visant ainsi à multiplier le débit par le nombre de paires de canaux envisagés. La conjugaison innovante de ces 2 approches complémentaires a pour but l'échange de données dont la sécurité est absolue dans un réseau de communication télécom long de plus de 100km.

La solution proposée est déclinée, dans le cadre de ces travaux, à un protocole de CQ de type « Eckert 92 » dont l'observable est la phase [3]. Notons que la solution développée dans ces travaux peut être transposée à bien d'autres protocoles et observables (polarisation, fréquence).

2. PRINCIPE DE LA STRATÉGIE ET DISPOSITIF EXPÉRIMENTAL

Comme cela est montré à la figure 1, notre dispositif est composé de 3 blocs :

- La source de paires de photons est composé d'un laser continu à 770 nm qui vient exciter un milieu (2). Par fluorescence paramétrique, un photon de pompe donne naissance à un couple

de photons (signal et idler) corrélés en temps et en énergie. L'accord de phase est centré autour de 1539.77 nm (canal 47 dans la grille ITU). L'efficacité du processus est de 1.10^{-6}. Un spectre typique de largeur 4 THz est montré à la figure 2.a.

- Un système de filtrage composé de filtres de Bragg joue un double rôle, celui de séparer de manière déterministe les paires de photon, mais aussi de filtrer avec un fort taux de réjection la pompe (>90 dB) tout en maintenant des pertes très faibles (< 0.2 dB).
- Le système d'analyse entièrement fibré (interféromètre de Michelson) présent chez les deux partenaires (appelés communément Alice et Bob) de l'observable envisagé (la phase), puis des démultiplexeurs en longueur d'ondes (DWDM) dont les canaux de largeur 100 GHz correspondent à la grille ITU.

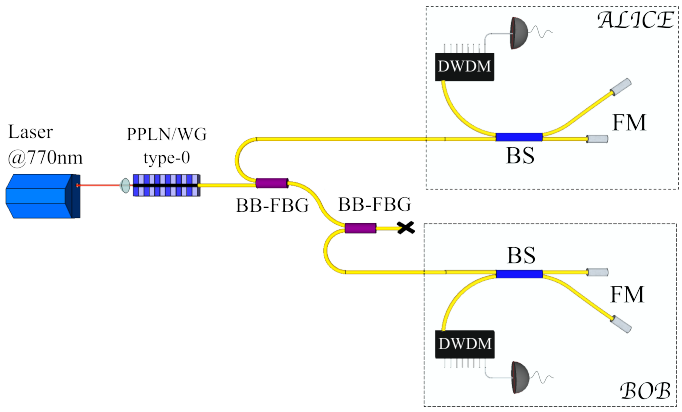

Fig. 1 : Dispositif expérimental. Guide dans un cristal Niobate de Lithium (PPLN/WG), Démultiplexeur de longueur d'onde (DWDM), coupleur 50/50 (BS), miroir de Faraday (FM)

Chaque paire de photons corrélés en énergie et portant la clef de chiffrement à Alice et Bob est séparée puis se propage dans les interféromètres de Michelson stabilisé en température, et enfin emprunte une paire de canaux télécoms symétriques par rapport à la longueur d'onde centrale du spectre (voir figure 2.a). Les détecteurs placés en bout de canaux appairés sont des photodiodes à avalanche. Les protocoles de CQ à paires de photons sont basés sur des corrélations non-locales qui se manifestent par des figures d'interférence entre les deux détecteurs disposés chez Alice et Bob. La figure d'interférence ainsi obtenue constitue la figure de mérite du protocole et sa visibilité constitue un marqueur indiquant la qualité du montage et son potentiel à distribuer des clefs secrètes.

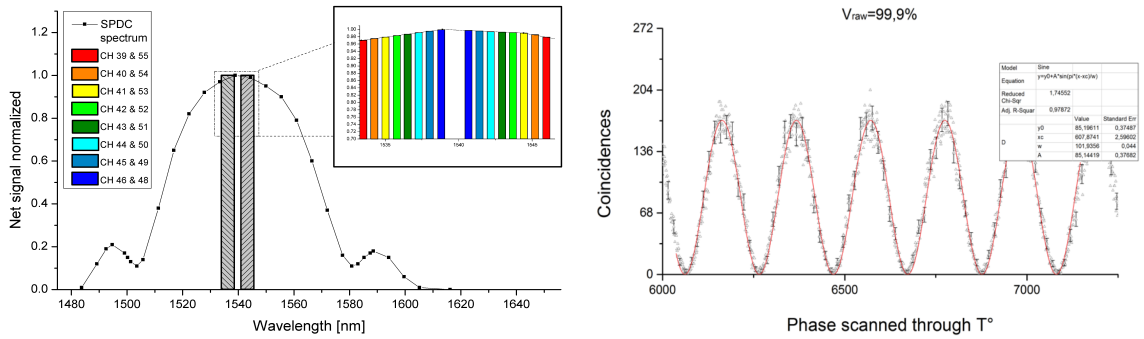

Fig. 2 : (a) Exemple de spectre de la source de paires de photons (b) Interférence entre deux paires de canaux.

3. CARACTÉRISATIONS ET POTENTIEL

Nous avons voulu vérifié dans un premier temps la visibilité des interférences des 8 voies. Pour se faire, nous avons placé successivement les deux APDs sur les 8 paires des DWDMs. Nous avons fait varier la phase d'un des interféromètres de telle manière à observer des interférences. Un résultat typique est représenté à la figure 2.b. La visibilité brute est de 99.9%. Pour les 7 autres voies, nous avons obtenu des visibilités au dessus de 99.5%. Ces visibilités proches de 100 % sont de bons indicateurs de la pureté de l'état produit et de la qualité du dispositif expérimental.

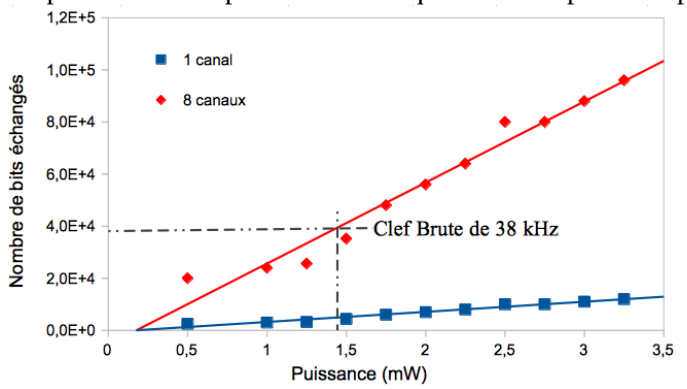

Fig. 3 : Taux de clefs échangées en fonction de la puissance.

Un paramètre crucial à la confidentialité de l'échange est le niveau de puissance mise en jeu qui est proportionnel au nombre de bits échangés. Mais il ne doit pas être trop élevé sous peine d'altérer le niveau de sécurité. Nous avons choisi une puissance de travail de 1.4 mW ce qui correspond à une visibilité de 82%. A ce niveau de puissance, nous sommes en mesure d'échanger un taux de bits égal à 38 kbits/sec comme le montre la figure 3 qui montre le débit de la liaison en fonction de la puissance pour un canal puis pour la somme des 8 canaux.

Ce résultat est extrêmement prometteur puisqu'il se situe au dessus de l'état de l'art dans les CQ. Nous pouvons citer un article de référence qui obtient un débit de 0.5 kbits/sec [4].

Un challenge important à relever est le déploiement de notre solution le long de tronçon de fibre de ligne télécoms. Nous avons déjà commencé à relever ce défi en introduisant 2 tronçons de 50 km de fibre optique couplés à leur module de compensation de dispersion chromatique (DCF). La prochaine étape de notre travail est d'étudier la distribution du taux de coïncidences entre ces deux partenaires distants. Les 1ères estimations de débit sont de 200 bits/sec, ce qui serait une performance à ce jour jamais atteinte avec ce type de protocole.

CONCLUSION

Nous avons montré le potentiel d'une solution astucieuse de déployer un réseau de CQ répondant aux exigences modernes de débit et de distance, basée sur l'exploitation de la bande passante d'une source de paires de photons dans laquelle une multitude de canaux fins télécoms viennent desservir deux utilisateurs distants.

REMERCIEMENT

Nous tenons à remercier le groupe Prysmian pour le prêt des bobines de fibre de ligne ainsi que les modules de DCF associés.

RÉFÉRENCES

[1] Gisin et al, Phys. Rev. Lett. **84 (**2000)
[2] Bennett et al, Phys. Rev. Lett. **70 (**1993)
[3] Ekert et al, Phys. Rev. Lett. **67 (**1991)
[4] Takesue et al , Opt. Expr. **18** (2010)