



Conférence à Télécom Paris le Jeudi 7 Décembre à 14h, amphithéâtre Emeraude

Eleni DIAMANTI

E. L. Ginzton Laboratory, Stanford University
et Laboratoire Charles Fabry de l'Institut d'Optique, Orsay

Sécurité et réalisation de systèmes de distribution de clés quantiques utilisant un protocole de phases différentielles

Résumé : La distribution de clés quantiques permet à deux parties de partager une clé de manière sûre, en accord avec les lois de la physique quantique. Le protocole le plus utilisé, Bennett-Brassard 1984 (BB84), est vulnérable aux attaques dites "photon-number splitting" (PNS), qui limitent sévèrement la distance de distribution dans le cas pratique d'une implémentation avec des pulsations de lasers très atténuées. Dans l'expérience que je vais décrire, nous proposons une solution pratique et efficace à ce problème en utilisant un nouveau protocole, basé sur le codage d'information dans les phases différentielles des pulsations cohérentes très atténuées. Nous avons également développé une analyse de sécurité pour ce protocole et démontré qu'il est robuste face à tout type d'attaque individuelle et en particulier face aux attaques PNS. De plus, nous avons construit un détecteur de photons uniques à une longueur d'onde de 1550 nm, qui combine la conversion de fréquences dans un guide d'ondes de niobate de lithium périodiquement polarisé avec la détection par une photodiode d'avalanche de silicium (Si APD). Ce détecteur présente des caractéristiques plus favorables pour les expériences de cryptographie quantique que les InGaAs/InP APDs qui sont utilisés d'habitude. En utilisant le protocole des phases différentielles ainsi que les nouveaux détecteurs de photons uniques, nous avons réalisé une expérience fonctionnant à 1 GHz, qui nous permet de générer une clé sûre à un débit de 0.5 Mbit/s sur une distance de 10 km et 170 bit/s sur une distance de 100 km de fibre optique. Je vais également décrire une expérience fonctionnant à 10 GHz, avec laquelle nous avons testé les limites de notre dispositif.

Lieu *Télécom Paris (Ecole Nationale Supérieure des Télécommunications)*
46 rue Barrault, 75013 Paris

Métro Ligne 6, Corvisart ; Ligne 7, Tolbiac.

Bus lignes 62 (Vergniaud), 21 (Daviel) ou 67 (Bobillot)

LTCI, Laboratoire Traitement et Communication de l'Information
UMR 5141, Unité Mixte de Recherche CNRS - GET/Télécom Paris