Résumé

Les réseaux et systèmes de télécommunications mondiaux fondent aujourd'hui leur confidentialité sur la cryptographie classique, qui repose sur des hypothèses mathématiques fragiles. La distribution quantique de clef (QKD) est aujourd'hui la seule façon connue pour distribuer des clefs avec une sécurité inconditionnelle. Ce travail de thèse contribue à combler de manière pluridisciplinaire et polyvalente le gap entre les limites physiques fondamentales et l'implémentation expérimentale, en termes de vitesse, fiabilité et robustesse.

Dans un premier temps, nous avons donc proposé une implémentation du protocole BB84 utilisant les états de phase cohérents. Le récepteur homodyne a été conçu de manière à compenser les fluctuations de phase et de polarisation dans les interféromètres, ainsi que dans le reste du canal de propagation.

Ensuite, nous avons mis en place un dispositif expérimental de système QKD à la longueur d'onde 1550 nm, avec une modulation QPSK fonctionnant avec un trajet et un sens de parcours uniques, dans une fibre optique mono-mode. Les deux schémas de détection: le comptage de photons (PC) et la détection homodyne équilibrée (BHD) ont été mis en œuvre.

Enfin, nous avons effectué des comparaisons théoriques et expérimentales de ces deux récepteurs. Le récepteur BHD a été élaboré avec une décision à double seuil. La mise en œuvre d'un tel processus accepte des mesures non-conclusives, et réduit l'efficacité de génération des clés, mais reste encore bien meilleur que celle des PCs à 1550 nm. Nous avons également prouvé que ce système est robust sous la plupart des attaques potentielles.

Abstract

Nowadays the information security and privacy of the telecommunications Networks are based on the classical cryptography, which relies on the fragile mathematical assumptions. The quantum key distribution (QKD) is presently the only known way to distribute keys with unconditional security. This thesis aims to apply a multidisciplinary versatile approach to fill the gap between the fundamental physical limits and the experimental system implementations, in terms of speed, reliability and robustness.

First of all, we proposed a BB84 protocol implementation using coherent phase states. The homodyne receiver was designed to compensate the phase and polarization fluctuations in the interferometers, as well as in the rest of the propagation channel.

Then we established an experimental one-way QKD system operating at 1550 nm Telecom wavelength in a single mode fiber link, with QPSK modulation. Both the photon counting detection (PC) and the balanced homodyne detection (BHD) schemes have been implemented.

Finally, we conducted theoretical and experimental comparisons of these two receivers. The BHD receiver has been improved with a dual-threshold post-decision. The implementation of such a process accepts non-conclusive measurements, and reduced key generation efficiency, but its permanence remains still better than the PC receiver at 1550 nm. We also proved that this system is robust under most common potential attacks.