Proposition de recherche doctorale

Communications quantiques cohérentes et cryptographie quantique

Mots clés :

- **Directeur de thèse** : ROMAIN ALLEAUME
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire Traitement et Communication de l'Information
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Dans le cadre de la thèse on étudiera la question du partage d'une référence de phase dans les communications quantiques cohérentes, i.e. la synchronisation de la phase du signal avec une référence de phase en réception (et également appelés « oscillateur local »). Un oscillateur local est en effet typiquement nécessaire pour réaliser un protocole de distribution quantique de clé à variable continue, qui fait intervenir une détection cohérente homodyne [FDDVTG09]. Les implementations actuelles [FDDVTG09, DemoSequre12] fonctionnent en transmettant l'oscillateur local sur le canal quantique, mais ne permettent pas totalement de garantir qu'il est de confiance. Ceci ouvre la voie à d'éventuelles attaques de type side-channel, comme il peut en exister pour les systems de cryptographie quantique à variables discrètes [Makarov11]. Une façon nette de parer à ce problème est de transmettre la reference de phase de façon quantique, et d'inclure ainsi cet aspect dans l'analyse de sécurité. En parallèle avec le travail théorique, on réalisera expérimentalement un protocole de "quantum optical phase locked loop", i.e une boucle de vérouillage de la phase reposant sur la détection (dans un premier temps avec une détection homodyne) des états quantiques appartenant au code que l'on aura défini. La base de ce travail passera par la mise au point d'une boucle à vérouillage de phase adaptée aux caractéristiques (notamment de bande passante) d'une detection homodyne impulsionnelle limitée au bruit de photon. [FDDVTG09] S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri and P Grangier, Field test of a continuous-variable quantum key distribution prototype, New Journal of Physics 11 (2009) 045023 [Makarov11] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. 2, 349 (2011).

Résumé du projet de recherche (Langue 2)

- communications quantiques compatibles avec architectures optiques cohérentes récentes - application à la mise en oeuvre de communications quantiques reposant sur des codes super-additifs