Spécialité de Master « Optique, Matière, Plasmas »

Stage de recherche (4 mois minimum, à partir de début mars 2010)

Proposition de stage pour l'année 2009-2010 (ne pas dépasser 1 page)

Date de la proposition : 29 octobre 2009

Responsable du stage / *internship supervisor*

Nom / *name* : Diamanti — Prénom / *first name* : Eleni

Tél : 0145817114 — Fax : 0145817158

Courriel / *mail* : eleni.diamanti@telecom-paristech.fr

Nom du Laboratoire / *laboratory name :* Laboratoire Traitement et Communication de l'Information (LTCI)

Code d'identification : UMR 5141 — Organisme : CNRS – Télécom ParisTech

Site Internet / *web site* : http://www.ltci.enst.fr

Adresse / *address* : 46 rue Barrault, 75013 Paris

Lieu du stage / *internship place*: Télécom ParisTech

Titre du stage / *internship title* : **Étude des canaux cachés dans des systèmes de cryptographie quantique**

Résumé / *summary*

Le travail de l'équipe Information Quantique de Télécom ParisTech se situe dans le domaine du traitement de l'information quantique. Ce domaine offre la perspective de communications futures de meilleure qualité et de plus grande sécurité. Dans les récentes années, une de ses applications les plus importantes, la distribution quantique de clés, a connu des progrès importants qui ont mené au développement de systèmes commerciaux et à l'implémentation du premier réseau de cryptographie quantique télécom en 2008, dans le cadre d'un grand projet européen dans lequel notre équipe était fortement impliquée.

La sécurité inconditionnelle de protocoles de distribution quantique de clés, c'est-à-dire leur sécurité contre un espion possédant des ressources infinies, est en principe prouvée. En pratique, cependant, celle-ci dépend du modèle choisi pour décrire les composants physiques qui constituent le système implémenté. Si le système n'est pas parfaitement décrit par ce modèle, alors de l'information secrète peut être perdue au profit de l'espion. Ce type de perte est dénommé « canal caché ». L'apparition des canaux cachés est en général liée à des composants photoniques, tels que des sources ou des détecteurs, imparfaits et non fiables. Elle peut également découler des hypothèses faites à l'étape de la correction d'erreurs du protocole, notamment l'hypothèse courante de la taille infinie de la clé. Heureusement, une fois identifiées et modélisées, les attaques d'espionnage liées aux canaux cachés peuvent être éliminées grâce aux lois de la physique, nous permettant ainsi de regagner une sécurité absolue.

Dans ce stage, nous proposons d'étudier les canaux cachés dans des systèmes pratiques de cryptographie quantique, et en particulier dans un système de distribution quantique de clés à variables continues développé en collaboration avec l'équipe Optique Quantique du Laboratoire Charles Fabry de l'Institut d'Optique, utilisé dans le premier réseau de cryptographie quantique, et actuellement en fonction dans notre laboratoire. Le but sera d'identifier des canaux cachés spécifiques à ce système, de les relier aux imperfections du système, et de proposer des contremesures pour chaque faille identifiée. Le sujet comportera une partie théorique mais il est principalement expérimental. Le stage pourra se poursuivre par une thèse au cours de laquelle seront développés des systèmes perfectionnés et seront étudiées des nouvelles preuves de sécurité adaptées à l'existence des canaux cachés dans les implémentations pratiques.

Toutes les rubriques ci-dessous doivent obligatoirement être remplies

Ce stage pourra-t-il se prolonger en thèse ? *Possibility of a PhD* ? : Oui

Si oui, financement de thèse envisagé / *financial support for the PhD* : Ministère, DGA, Commission Européenne

Lasers et Matière	X	Physique des Plasmas	
Optique de la science à la technologie	X	Lumière, Matière : Mesures Extrêmes	

*Fiche à transmettre (fichier pdf **obligatoirement**) sur le site http://stages.master-omp.fr*