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

Date de la proposition :14 octobre 2009

Responsable du stage */internship supervisor*			
Nom/*name* :	Gallion	Prénom/*first name*	Philippe
Tél :(33) 1 45 81 77 02		Fax : (33) 1 45 89 00 20	
Courriel/*mail* :	gallion@enst.fr		
Nom du Laboratoire / *Laboratory name* :	Telecom ParisTech		
Code d'identification:	Organisme : CNRS	LTCI, UMR 3141	
Site Internet/*web site* :	http://perso.telecom-paristech.fr/~gallion/	http://www.telecom-paristech.fr/	
Adresse/ *address* :	46, rue Barrault 75634 PARIS CEDEX 13		
Lieu du stage/ *Internship place*:	46, rue Barrault 75634 PARIS CEDEX 13		

Sécurité de la distribution quantique de clef par modulation de phase et détection homodyne

Contexte scientifique :

La distribution quantique de clef (QKD) est aujourd'hui la seule manière connue de distribuer des clefs de cryptographie avec une sécurité inconditionnelle. La sécurité quantique résulte en premier lieu de l'impossibilité de dupliquer les signaux reçus, principe de non-clonage, ou d'en distraire une partie significative sans signer son intervention par une modification importante du taux d'erreur des signaux reçus.

La sécurité repose en second lieu sur le caractère destructif ou perturbateur de toute observation et sur les erreurs résultant d'observations incompatibles d'un même objet quantique. La compatibilité de la QKD avec les réseaux optiques ne conservant pas la polarisation, impose l'utilisation d'une modulation de phase pour laquelle une détection homodyne s'avère mieux adaptée que les compteurs de photons, compte tenu, notamment, de leur faible rendement quantique et des effets thermiques très important aux longueurs d'onde des télécommunications et de leur rapidité trop faible en regard des débits de clef souhaités. L'utilisation d'une décision à seuil multiple permet de plus l'optimisation du taux de génération de clef. La récupération de phase alors nécessaire à la réception est soumise aux limites fondamentales imposées par les incertitudes quantiques. Elle impose des techniques spécifiques pour lesquelles le gain en sécurité reste largement à explorer d'autant qu'en l'absence de source à un photon unique, l'utilisation actuelle d'impulsions cohérentes atténuées au niveau quantique rend les systèmes homodynes eux aussi vulnérables aux attaques de type PNS (Photon Number Splitting).

La cryptographie quantique quitte aujourd'hui les promesses de la physique du siècle dernier pour celui la mise en œuvre. Elle doit faire ses preuves avec la réalité technologique et composer dans un contexte inter disciplinaire très riche incluant les communications numériques, les communications optiques, la théorie de l'information, le traitement électronique du signal et l'informatique.

Travail proposé :

Il s'agit de travailler sur une plateforme réelle de cryptographie quantique en cours de développement dans une un équipe fédérant ces différentes compétences et impliquée dans différents projets comme le projet « High bit-rate and versatile Quantum NETwork, (HQNET) » de l'Agence Nationale de la Recherche (ANR) par exemple.

Envoyer un curriculum vitae, une lettre de motivation et des lettres de recommandation à Philippe GALLION

Ce stage pourra-t-il se prolonger en thèse Oui

Si oui, financement de thèse envisagé : Bourse du Ministère ou ANR

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