Spécialité de Master « Optique, Matière, Plasmas »

Proposition de stage pour l'année 2011-2012

Date de la proposition : 7 novembre 2011

Responsable du stage / *internship supervisor*:

Nom / *Gallion* Prénom/ *Philippe*:

Tél : 0145817702 Fax :

Courriel / *mail*: gallion@enst.fr

Nom du Laboratoire / *laboratory name*:

Code d'identification : Organisme : TELECOM ParisTech et CNRS LTCI

Site Internet / *web site*: http://perso.telecom-paristech.fr/~gallion/

Adresse / *address:*

Lieu du stage / *internship place*: 46, rue Barrault - 75634 PARIS CEDEX 13

Titre du stage / Sécurité de la distribution quantique de clef par modulation de phase et détection homodyne

Résumé / *summary*

La sécurité des communications quantiques est traditionnellement considérée comme seulement limitée que par les principes de base de la physique et non, comme pour la sécurité classique, simplement en termes de ressources dont Eve pourrait disposer de manière réaliste.
Une sécurité inconditionnelle de la couche quantique n'est pas suffisante pour parvenir à une sécurité de bout en bout, jusqu'à la couche application. Par exemple les circuits classiques de l'électronique intégrée sont très vulnérables aux attaques dites de canaux cachés, généralement consistant en l'observation, la perturbation ou la manipulation de la couche physique de traitement, pouvant facilement s'effondrer la sécurité coûteuse de la couche quantique.
Pour conserver un rôle crédible dans les systèmes de communication sécurisés, la sécurité quantique doit aujourd'hui trouver un moyen de l'infiltration progressive des systèmes de sécurité classique. Elle doit également être inclue dans une approche de sécurité de bout en bout et doit préciser sa compatibilité avec les technologies de fibre optique et des systèmes.

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 (Dark counts) très important aux longueurs d'onde des télécommunications et de leur rapidité trop faible en regard des débits de clef souhaités. De plus en l'absence de source à un photon unique, l'utilisation actuelle d'impulsions cohérentes atténuées au niveau quantique rend les systèmes très vulnérables aux attaques de type PNS (Photon Number Splitting).
L'utilisation d'une détection homodyne, associée à d'une décision à seuils multiples permet l'optimisation du taux final de génération de clef par un compromis entre le taux d'erreur intrinsèque et le taux d'abandons de décisions. Des impulsions fortes multiplexées temporellement permettent simultanément la distribution d'horloge, un gain de mélange et La récupération de phase relative ; Cette dernière impose des techniques spécifiques pour lesquelles l'impacte sur la sécurité reste largement à explorer en liaison avec le type de source utilisé et la cohérence de phase éventuelle entre impulsions signal successives.

Bien que les limites de sécurité des systèmes quantiques ait été largement étudiée dans les pires situations, comme sous l'attaque puissante du fractionnement nombre de photons, certains aspects fondamentaux, en relation avec le rôle de la phase optique en tant que fournisseur supplémentaire de sécurité, ou comme un éventuel paramètre attaque, restent à être, et sera étudiée.

Il s'agit de travailler sur une plateforme réelle de cryptographie quantique en cours de développement dans une équipe fédérant ces différentes compétences et impliquée dans différents projets

Ce sujet est en collaboration avec différentes start-up innovantes dont Secure-IC.
Collaborations prévue le CICESE et te TECH de Monterey au Mexique.

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***: A l'étude**

Lasers et matière		Lumière, Matière : Mesures Extrêmes	
Optique de la science à la technologie	**X**	Plasmas : de l'espace au laboratoire	