UNIVERSITE PIERRE & MARIE CURIE
LA SCIENCE A PARIS

Institut Formation Doctorale

FICHE DESCRIPTIVE D'UN MODULE DE FORMATION

11-E130-02	LES COMMUNICATIONS QUANTIQUES

Les communications quantiques
PROCHAINE SESSION : 24, 31 mai, 7, 14 et 21 juin 2007 (5 demi-journées)

Séminaire / Conférence Sensibilisation		Organisation : ED 130 EDITE
Durée : 2.5 jours		Contact email : jwona.fagot@telecom-paris.fr
1 sessions/ an	25 places/session	Recommandé en ☒ 1re ☒ 2e ☒ 3e année

Objectifs

Ce séminaire peut être vu comme une sérieuse introduction à certaines applications de la physique quantique aux communications informatiques et plus spécialement à sécurisation des réseaux. Il fait appel à des principes de physique quantique qui seront rappeler et expliciter sans justification. Il fait aussi appel à la théorie de l'information de Shannon dont les éléments nécessaires seront également expliqués en cours.

Contenu

Utiliser des canaux quantiques pour communiquer peut induire des propriétés étonnantes et des plus précieuses. Ce séminaire présente quelques protocoles utilisant ces canaux quantiques. Le protocole quantique majeur est l'échange quantique de clé (QKD : Quantum Key Distribution) que nous décrirons après avoir établi les bases de son utilité. Ce protocole permet à deux utilisateurs distants d'établir une clé de chiffrement aléatoire en étant certains de la confidentialité de cette clé, quelle que soit l'ingéniosité et quelle que soit l'investissement technologique d'un espion. Nous verrons en détail le principal algorithme de QKD nommé BB84. Les taux d'erreur dans les appareillages quantiques rendent nécessaires plusieurs étapes algorithmiques fort intéressantes. Nous mentionnerons les autres protocoles ainsi que l'état de l'art en matière de réalisations techniques pour la communication par fibre optique et pour la communication par laser à l'air libre. Nous verrons différentes possibilités d'utilisation de la QKD pour construire des réseaux quantiques. Nous étudierons également l'état de l'art des protocoles d'authentification, d'Oblivious Tranfert et de Bit Commitment ; ces derniers permettront, lorsque ces réseaux fonctionneront, de mettre au point des systèmes de vote électronique totalement confidentiels et fiables ou bien des systèmes d'enchères boursières. Dans ce cours, nous utiliserons la théorie de l'information de Shannon, ainsi que des résultats et des calculs quantiques.

- Rappel de cryptographie symétrique et asymétrique
- Chiffre de Vernam et propriétés puis Principe de BB84
- Les différentes étapes algorithmiques et stratégie d'attaques
- TD sur les autres protocoles de QKD
- Authentification
- Bit commitment et Oblivious transferts
- Les réseaux quantiques à base de QKD

Responsable pédagogique / Formateurs

Intervenant : Patrick BELLOT. Professeur dans le département Informatique et réseaux de l'Ecole Nationale Supérieure des Télécommunications. Il participe avec son équipe, aux travaux de recherche du projet européen Secoqc visant à la réalisation d'un réseau Internet sécurisé par la cryptographie quantique.

Pour en savoir plus : http://www.edite-de-paris.com.fr/Formation/Formation.html

Date de mise à jour de la fiche (mois/année) : octobre 2006