FFCNCERC 2 520 € 3 jour(s)
ERXCS23

[Formation] Cryptographie et communications quantiques

OBJECTIFS

- Lister les principes de la cryptographie quantique
- Expliquer les différentes étapes et les principes de la distribution quantique de clé
- Étudier le lien entre cryptographie quantique et intrication
- Utiliser des systèmes de cryptographie quantique industriels déployés et/ou au laboratoire à travers des démonstrations
- Expliquer les principes des réseaux quantiques de type Quantum Internet, et les applications de la cryptographie quantique
- Identifier l'impact des technologies quantiques sur la cryptographie et la nécessité d'une cryptographie post-quantique

PROGRAMME

Cryptographie quantique

- Principes de la cryptographie quantique (non-clonage, monnaie quantique)
- Protocole QKD et exemple du protocole BB84
- Attaque et Sécurité d'un protocole QKD, exercices

Cryptographie quantique et intrication

- Inégalités de Bell, Protocole EPR
- Démonstration expérimentale de violation des inégalités de Bell
- Mise en œuvre expérimentale de systèmes de communications quantiques, encodage à variables discrètes (DV) ou continues (CV)

Distribution Quantique de clé (QKD) : technologies, systèmes

- Communications optiques, communications quantiques : éléments clés d'un système de communication

NOUVEAU ATELIER RÉALISABLE À DISTANCE AVANCÉ

DATES ET LIEUX

Du 17/03/2025 au 19/03/2025 à Paris
Du 24/09/2025 au 26/09/2025 à Paris

PUBLIC / PREREQUIS

Toute personne (ingénieur, technicien, scientifique, etc.) souhaitant comprendre les notions de base et mieux appréhender les principes et les enjeux applicatifs des communications et de la cryptographie quantiques.

Des bases d'algèbre linéaire (espace vectoriel, produit scalaire, projecteur, etc.) sont nécessaires.

COORDINATEURS

Romain Alléaume

Romain Alléaume (ENS Ulm 98, TP 2003, PhD Sorbonne U 2004) est Professeur à Telecom Paris. Ses recherches portent sur la cryptographie et les communications quantiques, ainsi que le traitement quantique de l'information. Auteur de plus de 50 articles et 3 brevets dans le domaine de la distribution quantique de clés (QKD) il co-fonda la start-up SeQureNet en 2008, qui mis sur le marché le premier système de cryptographie quantique à variables continues (CV-QKD). Il coordonne la participation d'IP Paris aux projets européens QSNP et FranceQCI, pour lesquel il membre du comité exécutif. Il

- Systèmes QKD : technologies, performance
- Panorama des développements industriels de systèmes QKD

Réseaux QKD et applications

- Démonstration d'un système industriel de QKD, détection d'une attaque
- Réseaux de distribution quantique de clé : état de l'art, vision industrielle
- Cas d'usage de la QKD pour la sécurisation des réseaux

Internet Quantique

- Vision et application d'un Internet Quantique
- Téléportation et Répéteur Quantiques
- Protocoles de cryptographies quantiques au-delà de la QKD
- Application (TD) : simulations numériques de réseaux quantiques avec NetSquid

Cryptographie dans un monde quantique

- Menaces induites par l'ordinateur quantique sur la cryptographie actuelle
- Introduction à la Cryptographie Post-Quantique
- Hybridation de la QKD et de la cryptographie post-quantique

Synthèse et conclusion

est aussi responsable de l'équipe-projet Inria-IP Paris QURIOSITY.

Eleni Diamanti

Eleni Diamanti (PhD Stanford 2006, postdoc Marie Curie IOGS) est directrice de recherche au CNRS au LIP6-Sorbonne Université à Paris. Ses sujets de recherche portent sur le développement des ressources photoniques et des applications, notamment en cryptographie, pour les réseaux de communication quantique. Elle est lauréate d'une bourse du European Research Council, directrice du Paris Centre for Quantum Technologies et membre du comité exécutif des projets Européens QSNP et FranceQCI. Elle est également cofondatrice et conseillère scientifique de la société Welinq qui développe des solutions d'interconnexion quantique.

MODALITES PEDAGOGIQUES

Cours et exercices d'application. Travaux pratiques. Illustrations technologiques récentes.

La formation comporte un voyage apprenant à travers les principaux laboratoires d'informatique quantique d'île de France : Telecom Paris (Palaiseau), Orange innovation (Chatillon) et Sorbonne Université (Paris).