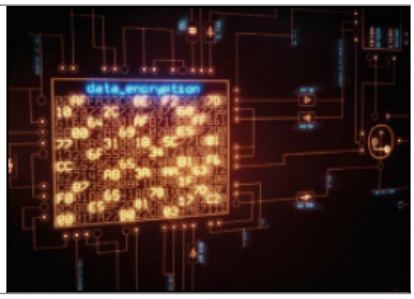
INSTITUT d'OPTIQUE GRADUATE SCHOOL | Continuing Education
Formation Continue

QC4 | Comprendre la cryptographie post-quantique



NIVEAU : INTERMÉDIAIRE

Publics : Professionnels et entreprises qui cherchent à se préparer aux défis posés par les ordinateurs quantiques émergents.

Prérequis : Connaissances générales en mathématiques et en algorithmique

Responsable(s) pédagogique(s) : Philippe GABORIT - Professeur à l'Université de Limoges

Langue de la formation : Français

Capacité maximum : 12

Prix : 1400€ HT - **Durée :** 2 jours - 14 h

Contexte

Alors que les ordinateurs quantiques deviennent une réalité technologique, ils menacent les bases mêmes des systèmes cryptographiques classiques.

Ce stage offre une première immersion dans l'univers de la cryptographie post-quantique, en explorant à la fois les fondements théoriques et les enjeux concrets de cette transition.

Objectifs

- Déterminer les principes fondamentaux de la cryptographie post-quantique
- Identifier les concepts de base des ordinateurs quantiques et leur impact sur la sécurité
- Décrire les défis et les opportunités de la cryptographie post-quantique dans un contexte pratique
- Estimer les implications de la cryptographie post-quantique pour la sécurité informatique à long terme
- Reconnaître les différents types de cryptographie post-quantique

Prochaines sessions

- 10 décembre 2026 au 11 décembre 2026 - Bordeaux/distanciel

QC4 | Comprendre la cryptographie post-quantique

Thèmes abordés

Ordinateur quantique et ses problématiques
Réseaux Euclidiens
Codes correcteurs d'erreurs
Schémas basés sur les signatures
Standardisation NIST

Le programme

Introduction
- Présentation de la cryptographie post-quantique
- Processus de standardisation
- Les différentes familles de cryptosystèmes post-quantiques

Réseaux Euclidiens
- Définitions
- Schémas de chiffrement et de signature
- Schémas standardisés

Codes correcteurs d'erreurs
- Définitions
- Schémas de chiffrement et de signature

Signatures basées sur le MPC in the head
- Définitions
- Quelques schémas proposés pour standardisation

Autres familles de schémas
- Signatures basées sur les fonctions de hachage
- Isogénies

Méthodologie et évaluation

Questionnaire de positionnement
Exposés et exercices sur ordinateur
Démonstrations interactives
QCM en fin de formation

Formation Continue de l'Institut d'Optique - 2 av. Augustin Fresnel, 91127 Palaiseau. Tél . : +33 1 6453 3236 - fc.institutoptique.fr
PARIS-SACLAY - SAINT-ETIENNE - BORDEAUX