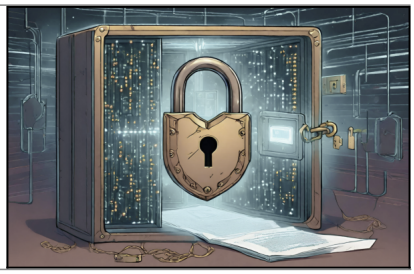
INSTITUT d'OPTIQUE GRADUATE SCHOOL | Continuing Education
Formation Continue

QC4 | Comprendre la cryptographie post-quantique



Nouvelle Formation

NIVEAU : ADVANCED

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 : French

Capacité maximum : 12

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

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

Dates et lieu des prochaines sessions

- 24 march 2025 au 25 march 2025 - Limoges

Thèmes abordés

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

QC4 | Comprendre la cryptographie post-quantique

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