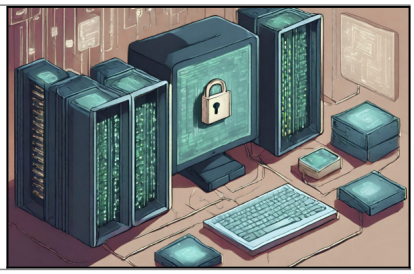
INSTITUT d'OPTIQUE GRADUATE SCHOOL | Continuing Education
Formation Continue

QC8 | Cryptographie basée sur les codes



Nouvelle formation

NIVEAU : AVANCÉ
Publics : Toute personne ou entreprise qui cherche à se préparer à la transition cryptographique à venir.
Prérequis : De bonnes notions en mathématiques, en algèbre et en algorithmique
Responsable(s) pédagogique(s) : Philippe GABORIT - Professeur à l'Université de Limoges
Langue de la formation : Français
Capacité maximum : 12
Prix : 1900€ HT - **Durée :** 3 jours

Contexte

La cryptographie post-quantique basée sur les codes constitue l'une des approches les plus prometteuses face aux menaces que feront peser les ordinateurs quantiques sur les systèmes actuels.

Ce stage permet de comprendre les principes fondamentaux de cette approche.

Objectifs

- Déterminer les principes fondamentaux de la cryptographie post-quantique basée sur les codes
- Identifier les différents schémas en métrique de Hamming (chiffrement, signature)
- Décrire les différents schémas basés sur la métrique rang
- Évaluer les développements futurs en cryptographie post-quantique
- Distinguer comment ces schémas s'inscrivent dans le processus de standardisation du NIST

Prochaines sessions

- 22 avril 2025 au 24 avril 2025 - Limoges

QC8 | Cryptographie basée sur les codes

Thèmes abordés

Théorie des codes correcteurs d'erreurs
Métrique de Hamming et schémas associés
Métrique Rang et schémas associés
Codes et MPC in the head

Le programme

Introduction
- Théorie des codes correcteurs d'erreurs
- Métrique de Hamming
- Métrique rang

Métrique de Hamming
- Schémas de chiffrement
- Schémas de signature
- Présentation des candidats au processus de standardisation

Métrique rang
- Schémas de chiffrement
- Schémas de signature
- Présentation des candidats au processus de standardisation

Codes et MPC in the head
- Présentation des candidats au processus de standardisation

Méthodologie et évaluation

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