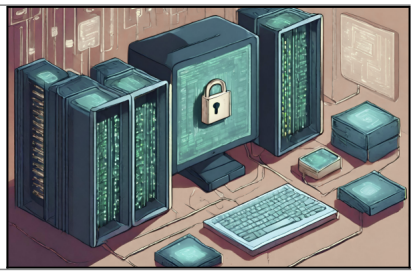
# QC8 | Cryptographie basée sur les codes



**Nouvelle Formation**

NIVEAU : SPECIALIZED
**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 :** French
**Capacité maximum :** 12
**Prix :** 1900€ HT - **Durée :** 3 jours

## 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

## Dates et lieu des prochaines sessions

- 22 april 2025 au 24 april 2025 - Limoges

## 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

# QC8 | Cryptographie basée sur les codes

## 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



*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*