Xavier LEROY

CHAIRE SCIENCES DU LOGICIEL

Le calcul sécurisé : calculer sur des données chiffrées ou privées

6 nov. > 18 déc. 2025

COLLÈGE DE FRANCE
1530

Thomas Römer
Administrateur du Collège de France
11, place Marcelin-Berthelot, 75005 Paris
www.college-de-france.fr

Année académique
2025/2026

Cours & Séminaires

Amphithéâtre Mireille Delmas-Marty.
Les cours auront lieu les jeudis, de 9 h 30 à 11 h.
Ils seront suivis par les séminaires de 11 h 15 à 12 h 15.
Les cours et séminaires sont gratuits, en accès libre, sans inscription préalable.

6 novembre 2025

COURS - **Sécuriser le calcul : introduction et étude de cas**

13 novembre 2025

COURS - **Chiffrement totalement homomorphe : calculer sur des données chiffrées (1)**

SÉMINAIRE - **Pierrick Gaudry** (CNRS)
Outils cryptographiques pour le vote électronique

20 novembre 2025

COURS - **Chiffrement totalement homomorphe : calculer sur des données chiffrées (2)**

SÉMINAIRE - **Damien Stehlé** (CryptoLab)
Chiffrement totalement homomorphe CKKS

27 novembre 2025

COURS - **Calcul multipartite sécurisé : partager des secrets**

SÉMINAIRE - **Ilaria Chillotti** (DESILO Inc)
Chiffrement totalement homomorphe : panorama, applications et nouvelles directions

4 décembre 2025

COURS - **Calcul multipartite sécurisé : circuits brouillés et transfert inconscient**

SÉMINAIRE - **Geoffroy Couteau** (CNRS)
Calcul sécurisé et aléa corrélé, de la théorie à la pratique

11 décembre 2025

COURS - **Calcul vérifiable et preuves zero-knowledge**

SÉMINAIRE - **Michele Orrù** (CNRS)
Des preuves zero-knowledge à l'anonymat en ligne

18 décembre 2025

COURS - **Sécuriser le calcul : nouvelles directions et conclusions**

SÉMINAIRE - **David Pointcheval** (Cosmian)
Le chiffrement fonctionnel : agréger des données sensibles

Illustration : *Machine à voter NEDAP ESF1*, France.