



From
09
SEP.
2024
to
13
SEP.
2024

09h00
-
19h00

2024-T3 POST-QUANTUM ALGEBRAIC CRYPTOGRAPHY

Introductory summer school on Post-quantum algebraic cryptography

IES Cargèse, Corsica

INSCRIPTION

Post-quantum algebraic cryptography

Introductory summer school at Institut d'Etudes Scientifiques, Cargèse (Corsica)

September 9 to 13, 2024

Organisers: Delaram Kahrobaei, Ludovic Perret

Topics: Lattice Based, Code-based, Multivariate-based, Group-based, Isogeny-based
Primitives, QKD, Quantum Algorithms

URL of the page: <https://www.ihp.fr/en/events/introductory-summer-school-post-quantum-algebraic-cryptography>

Speakers:

- Luca De Feo (IBM, Switzerland): Isogeny-based Cryptography
- Pierre-Alain Fouque (University of Rennes, France): Lattice-based Cryptography
- Thomas Debris Alazard (INRIA)
- Delaram Kahrobaei (New York, USA, York, UK): Group-based Cryptography
- Kristin Lauter (Meta AI, USA): AI for PQC
- Ludovic Perret (Sorbonne, Paris, France): Multivariate-based Cryptography
- Timothy Spiller (York, UK): QKD



INSTITUT HENRI POINCARÉ

Sorbonne Université / CNRS
11 rue Pierre et Marie Curie
75231 Paris Cedex 05

TIMETABLE

The institute:

- Monday to Friday from 8:30am to 6pm,
- closed on public holidays.

The museum - Maison Poincaré :

- Monday, Tuesday, Thursday and Friday from 9:30am to 5:30pm,
- Saturday from 10am to 6pm,
- closed on Wednesday and Sunday.

URL of the page: <https://www.ihp.fr/en/events/introductory-summer-school-post-quantum-algebraic-cryptography>