ISOGENY-BASED CRYPTOGRAPHY

JANUARY 13 TO FEBRUARY 28, 2026

PROGRAM THEME:

Isogeny-based cryptography is a young post-quantum field built on the hardness of computing isogenies between supersingular elliptic curves. Its assumptions enable advanced protocols such as ring signatures, oblivious PRFs, and oblivious transfer. SQI sign, notable for its small keys and signatures, is a leading candidate in NIST's second post-quantum signature competition, though slower than its rivals. The field is highly interdisciplinary, combining deep mathematics, theoretical computer science, and practical engineering.

PROGRAM COORDINATORS:

Péter Kutas (Eötvös Loránd University and University of Birmingham)
Carlos Cid (OIST)
Steven Galbraith (University of Auckland)
Jonathan Komada Eriksen (KU Leuven)
Tanja Lange (Eindhoven University of Technology)
Chloe Martindale (University of Bristol)
Tomoki Moriya (Mitsubishi Electric)
Hiroshi Onuki (University of Tokyo)
Tsuyoshi Takagi (University of Tokyo)

2/09-2/13 2026
SCHOOL: "Introduction to Isogeny-based Cryptography"

Program website

VENUE: Visiting Program area L5EF03 and seminar rooms around OIST

OIST OKINAWA INSTITUTE OF SCIENCE AND TECHNOLOGY