INSALATE DI MATEMATICA

Post-quantum cryptography from elliptic-curve isogenies

17/12/2025

Gioella Lorenzon

Katholieke Universiteit Leuven

IN THIS TALK

How do we communicate securely in a digitised world, and with quantum computers threatening to break many of today's cryptographic schemes? One promising answer comes from elliptic-curve isogenies. In this talk we will introduce post-quantum cryptography, and focus on a branch called isogeny-based cryptography, which relies on hard problems related to maps between elliptic curves. In particular, we will delve into cryptographic group actions and their instantiation via (oriented) isogenies.

🔑words: post-quantum cryptography, elliptic-curve isogenies, group actions, orientations

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Dipartimento di Matematica e Applicazioni

"Obvious" is the most dangerous word in mathematics.
(Eric Temple Bell)

U9 - 15

4:45 pm (CET)

Insalate.di.matematica