Roma Tre

Dipartimento di Matematica e Fisica
Segreteria per la Ricerca

SEMINARIO di CRITTOGRAFIA

Valerio ARDIZIO

(KU Leuven, COSIC)

TOWARDS AN ISOGENY-BASED PROTOCOL FOR MORE EFFICIENT PASSWORD-AUTHENTICATED KEY EXCHANGE (PAKE)

---

9 Febbraio 2026

ore 14.30

Lungotevere Dante 376

AULA M3

Abstract: After introducing fundamental concepts within the realm of isogeny-based cryptography, together with mentioning basic ideas and security requirements necessary for understanding Password-Authenticated Key Exchange (PAKE) protocols, the focus will shift to the intersection of isogeny-based cryptography and PAKE protocols. We will explore both provably secure instantiations and vulnerable constructions and I will conclude by presenting the core ideas behind my current joint work-in-progress with Dr. De Feo and Dr. Basso, which aims to construct a provably secure PAKE protocol using bin-SIDH as the underlying key exchange mechanism.

per informazioni: Dr. Nicoletta Falcone (nicoletta.falcone@uniroma3.it)