Roma Tre

Dipartimento di Matematica e Fisica
Segreteria per la Ricerca

SEMINARIO di CRITTOGRAFIA

Massimiliano SALA

(Università di Trento)

On polynomial systems, mysterious solutions and complexity theory

20 Novembre 2026

ore 11.30

Largo San Leonardo Murialdo 1 - Edificio C

AULA C006

Abstract: Among square quadratic systems over F_2, those with exactly one solution outnumber those with none — by one part in 2^n, at every n, the opposite of the linear case. We give an explicit $O(n^3)$ injection from most solution-free systems to uniquely solvable ones, and read it against coNP, DP, NP and the planted-MQ assumption of post-quantum cryptography.

per informazioni: Prof Marco Pedicini (marco.pedicini@uniroma3.it)