Roma Tre

Dipartimento di Matematica e Fisica
Segreteria per la Ricerca

SEMINARIO di CRITTOGRAFIA

Jonathan Fuchs

(Radboud University)

Key-Then-Hash: Universal Hashing from Public Functions

Lunedì 16 Novembre 2026

ore 15.00

Largo San Leonardo Murialdo 1 - Edificio C

AULA C006

Abstract: Universal hashing is a standard tool for extending keyed functions on fixed-length inputs to variable-length messages, notably in message authentication. It can provide efficient compression with information-theoretic bounds on collision probabilities.

This talk presents the key-then-hash approach to constructing universal hash functions from public functions. We will first consider constructions based on public permutations and explain how their concrete properties yield universality guarantees without relying on an ideal-permutation model. We will then generalize these techniques to non-invertible public functions, examining which properties are needed to preserve these guarantees.

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