Roma Tre

Dipartimento di Matematica e Fisica
Segreteria per la Ricerca

SEMINARIO di CRITTOGRAFIA

Daniele Friolo

(Roma Tre University)

Anamorphic Cryptography and Secret Sharing

Lunedì 30 Novembre 2026

ore 15.00

Largo San Leonardo Murialdo 1 - Edificio C

AULA C006

Abstract: Anamorphic Encryption (Persiano, Phan and Yung, Eurocrypt '22) allows private communication in a challenging setting where encryption is severely controlled by a central authority (henceforth the dictator) who can demand the users to surrender their secret keys. Anamorphic Signatures (AS) (Kutylowski, Persiano, Phan, Yung, Zawada, Crypto '23) face the even more restrictive world where only authentication is allowed but users still want to send secret messages despite the repressive control of the dictator holding their signing key. Several constructions have been proposed so far, but they all come with some limitations.

In this talk, I will introduce the main ideas behind Anamorphic Encryption and Signatures and present my recent work on Anamorphic Secret Sharing Signatures (ASSS), a new flexible setting where digital signatures are used to covertly embed secret shares which t out of N designated receivers can combine to recover a covert secret. We formalize this new primitive together with new robustness, forward secrecy, and private unforgeability notions and we give a construction for Schnorr-like signatures overcoming the limitations of previous constructions. ASSS additionally imply (regular single-receiver) AS, but two signatures (instead of one) are needed to recover the covert message.

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