SEMINARIO DI GEOMETRIA E ALGEBRA

UNIBA - POLIBA

Mercoledì 11 Marzo 2026 - Ore 15:00
Dipartimento di Matematica UniBa, aula XI, primo piano.

Alessio Meneghetti
(Università di Bari)

Post-Quantum Cryptography and Computationally-Hard Algebraic Problems

Abstract. Post-Quantum Cryptography is a branch of public-key Cryptography focused on schemes capable of withstanding quantum attacks: classic cryptography, which is largely based on algebraic methods involving discrete logarithms and factorization of large integers, is vulnerable against quantum computers due to Shor's methods relying on the quantum version of the Discrete Fourier Transform.

After a brief overview of post-quantum cryptography with some notable examples we discuss the underlying computationally-hard algebraic problems, presenting in particular the Syndrome Decoding Problem (SDP), the Multivariate Quadratic Problem (MQ), and the Linear Equivalence Problem (LEP). We conclude by discussing some recent results on the link between them, presenting an isomorphism between SDP and MQ and some famous conjectures.

https://sites.google.com/view/sga-poliuniba/home-page