Ministero dell'Università e della Ricerca

PRIN
PROGETTI DI RICERCA DI RILEVANTE INTERESSE NAZIONALE

UNIVERSITÀ DI TRENTO

CODICE PROGETTO

2022RFAZCJ

Algebraic methods in Cryptanalysis

OBIETTIVO PRINCIPALE DELL'OPERAZIONE

Disseminazione dei risultati intermedi ottenuti durante il primo anno di attività del progetto e ulteriore stimolazione delle interazioni tra le unità di ricerca.

Politecnico di Torino

UNIVERSITÀ DEGLI STUDI DI MILANO

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Algebraic Methods in Cryptanalysis
Convegno progetto PRIN

2 Febbraio 2026 – 10:00
Dipartimento di Scienze Matematiche
Politecnico di Torino, Aula Buzano

Invited speakers

Lorenzo Campioni, Università dell'Aquila

Giuseppe D'Alconzo, Politecnico di Torino

Roberto La Scala, Università di Bari

Pietro Mercuri, Università di Trento

Lorenzo Romano, Politecnico di Torino

Giulia Salvatori, Politecnico di Torino

Matilda Urani, Politecnico di Torino

Irene Villa, Università di Trento

Andrea Visconti, Università di Milano

Organizers: Danilo Bazzanella, Nadir Murru, Carlo Sanna

Contacts: danilo.bazzanella@polito.it, nadir.murru@unitn.it,

carlo.sanna@polito.it

Program

9:30 **Roberto La Scala** – Oracle-based multistep strategy for solving polynomial systems over finite fields and algebraic cryptanalysis of the Aradi cipher

9:50 **Giulia Salvatori** - An attack to RSA via continued fractions and quadratic forms

10:10 **Matilda Urani** – Accurate BGV parameters selection

10:30, **Pietro Mercuri, Lorenzo Romano** – Cryptanalysis with the Hidden Subgroup Polynomial-time reduction and attacks

11:00 Coffee Break

11:30 **Andrea Visconti** – Algebraic tools and their applications in cryptanlysis

11:50 **Irene Villa** - Construction and cryptanalysis of a multivariate CCZ scheme

12:10 **Lorenzo Campioni** – Geometric characterization of maximal unrefinable partitions via the Keith-Nath transformation

12:30 **Giuseppe D'Alconzo** – Rethinking the relaxed permuted kernel problem: a new formulation and algebraic attacks

12:50 Lunch

14:30 **Workshops**

18:00 End of conference