CIFRIS25 *September 11th and 12th 2025*

PROGRAM TIMES & SPEAKER DETAILS

SEPTEMBER 11th 2025 - FIRST DAY

Università Roma Tre - Dip.to Ingegneria - Via Vito Volterra 62

9.00 - 9.30	Registration and badge
9.30 - 9.45	Welcome speech: **Prof. M. Sala, Prof. M. Pedicini, Rappresentante ACN**
9.45-10.00	INSTITUTIONAL ROUND TABLE Moderatore: **Rappresentante ACN** - Banca d'Italia - Polizia Postale
10.00-10.15	Presentazione De Cifris: **Roberto Civino**
10.15.10.45	PARTNERS **- DataKrypto** **- E4 Computer Engineering** **- ForkBomb** **- Random Power**
10.45-11.00	*coffee break*
11.00-12.00	INVITED SPEAKER: LUDOVIC PERRET
12.00-13.00	SYMMETRIC CRYPTOGRAPHY AND CODING THEORY Roberto La Scala, Università di Bari Oracle-Based Multistep Strategy for Solving Polynomial Systems Over Finite Fields and Algebraic Cryptanalysis of the Aradi Cipher Francesco Ghiandoni, Università di Perugia AG Codes for Secure and Private Information Retrieval Alessio Caminata, Università di Genova Construction and cryptanalysis of a multivariate CCZ scheme a.k.a. do not bring your Pesto to Switzerland!
13.00-14.00	*lunch break*

Participation in the CIFRIS25 Conference is **free** and open to all De Cifris members and to everyone

CIFRIS25 *September 11th and 12th 2025*

14.00-15.20

APPLIED CRYPTOGRAPHY

Daniele Venturi, Università di Roma, La Sapienza
Evolving Secret Sharing

Marco Rinaudo, Telsy S.p.A.
The critical role of acceleration in fully homomorphic encryption

Barbara Masucci, Università di Salerno
Design and Analysis of Distributed Schemes for Anonymous Access Control

Antonio Tortora, Università della Campania "Luigi Vanvitelli"
Using Homomorphic Encryption for Inner-Product Functional Encryption

15.20-15.40 coffee break

15.40-17.00

POST-QUANTUM CRYPTOGRAPHY

Michele Battagliola, Università Politecnica delle Marche
Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures

Giuseppe D'Alconzo, Politecnico di Torino
Towards Post-Quantum Multi-Signatures from Group Action Assumptions

Alessandro Barenghi, Politecnico di Milano
Moving to a Post-Quantum World: Challenges in Engineering and Deploying Quantum Resistant Cryptography

Walter Tiberti, Università dell'Aquila
Post-Quantum Cryptography in Intra-Vehicle Networks

Click here for
REGISTRATION

Participation in the CIFRIS25 Conference is **free** and open to all De Cifris members and to everyone

CIFRIS25 *September 11th and 12th 2025*

PROGRAM TIMES & SPEAKER DETAILS

SEPTEMBER 12th 2025 - SECOND DAY

Università Roma Tre - Dip.to di Matematica e Fisica - Largo San Murialdo 1

10.00 - 11.00

ROOM "M1"

TOPICS IN APPLIED CRYPTOGRAPHY (TAC)

Francesco Stocco, Telsy
QKD (Re)Initialization via PQC: An Industrial Security-Usability Trade-off

Massimo Caccia, Random Power s.r.l. & University of Insubria
Quantum Root-of-Trust: Post-Quantum Security for Industrial IoT

Carlo Brunetta, Independent researcher
Verifiable Computation Outsourcing via Contracts over Blockchain Transactions

11.00 - 11.30 *coffee break*

11.30 - 13.00

Invited talk: Peter Rønne, Université du Luxembourg
Transparent Verification in E-Voting

Laura Mattiuz, Cybersecurity Center, FBK
A Review of Post-Quantum e-Voting

Lorenzo Rovida, University of Milano-Bicocca, DISCo
Exploring blind signatures under FHE by combining GBFV and HAWK

10.00 - 11.00

ROOM "M2"

NUMBER THEORY AND CRYPTOGRAPHY

Dimitry Koshelev, Lleida University
Endomorphisms for Faster Cryptography on Elliptic Curves of Moderate CM Discriminants

Pietro Mercuri, Università di Trento
High order elements in finite fields arising from recursive towers

11.00 - 11.30 *coffee break*

11.30 - 13.00

Lorenzo Romano, Politecnico di Torino
One Reduction To Rule Them All. The Hidden Subgroup Problem and its role among post-quantum cryptographic assumptions

Andrea Sanguineti, Università di Genova
Algebraic modelings of the Supersingular Isogeny Problem

Alessandro Zaccagnini, Università di Parma
Integer Factorization

Participation in the CIFRIS25 Conference is **free** and open to all De Cifris members and to everyone

CIFRIS25 *September 11th and 12th 2025*

10.00 - 11.00

ROOM “M3”

SYMMETRIC CRYPTOGRAPHY AND CODING THEORY

Enrico Piccione, Universitetet i Bergen
Recent advancements on TI without on-line randomness

George Petrides
Decomposing Permutation Polynomials for More Efficient Hardware Implementations

11.00 - 11.30 *coffee break*

11.30 - 13.00

Rocco Brunelli, Università RomaTre
Generic Partial Decryption as Feature Engineering for Neural Distinguishers

Alessandro Neri, Università di Napoli
Coding Theory Meets Convex Geometry: The Etzion-Silberstein Conjecture

Paolo Santonastaso, Politecnico di Bari
Optimal Rank-Metric Codes from Skew Polynomial Rings: Constructions and a Welch–Berlekamp Like Algorithm

13.00 - 14.00 *lunch break*

14.00 - 15.30

ROOM “M1”

RECENT ADVANCES IN POST-QUANTUM CRYPTOGRAPHY

Invited talk: Paolo Santini, Università Politecnica delle Marche
Riding a BIKE with failures (without falling down too many times)

Rahmi El Mechri, Università Politecnica delle Marche
SPECK: Signature from Permutation Equivalence of Codes and Kernel

15.30 - 16.00 *coffee break*

16.00 - 17.00

Rosa Fera, Università di Cassino e del Lazio meridionale
Hilbert series and degrees of regularity of Oil & Vinegar and Mixed quadratic systems

Wissam Ghantous, University of Central Florida
Cycles in the generalized supersingular L-isogeny graph

Martina Vigorito, EPITA Paris
On the Security of MQ-based ZKPoK in the Multi-Instance Setting

17.00 - 18.00

A JOURNEY INTO BITCOIN’S CRYPTOGRAPHY

Participation in the CIFRIS25 Conference is **free** and open to all De Cifris members and to everyone

CIFRIS25 *September 11th and 12th 2025*

14.30 - 15.30	**ROOM "M2"** HISTORY OF CRYPTOGRAPHY
15.30 - 16.00	*coffee break*
16.00 - 17.00	QUANTUM RANDOM NUMBER GENERATORS & CRYPTOGRAPHY
14.30 - 15.30	**ROOM "M3"** PROTOCOLS, PRIVACY AND SECURITY IN DIGITAL IDENTITY
15.30 - 16.00	*coffee break*
16.00 - 17.00	PROTOCOLS, PRIVACY AND SECURITY IN DIGITAL IDENTITY

Click here for
REGISTRATION

Participation in the CIFRIS25 Conference is **free** and open to all De Cifris members and to everyone