

# CIFRIS26

October 5, 2026

Roma Tre University

# PROGRAMME

# Aula Magna

## 08:30-09:00 Registrazione e consegna badge

La sessione di apertura è introdotta da **Germana Zuffanti**  
(Divisione comunicazione e rapporti istituzionali, ACN)

## 09:00-09:15 Saluti

Prof. **Massimiliano Fiorucci** (Rettore, Univ. Roma Tre)  
Amm. **Luigi Schinelli** (Capo Servizio Crittografia, ACN)  
Prof. **Massimiliano Sala** (Presidente De Cifris)

## 09:15-09:30 Le attività di De Cifris

**Marco Pedicini** (Direttore Scientifico De Cifris)

## 09:30-09:45 • Keynote

**Santo Mirabelli** (Polizia Postale)  
*Crittografia: la sfida dell'accesso legittimo ai dati nell'era delle comunicazioni cifrate*

## 09:45-10:15 De Cifris Partners

09:45-09:50 **Andrea Gelpi** – coordinatore di De Cifris Partners  
09:50-09:55 **Francesco Barbaro** (BANCOMAT S.p.A.)  
09:55-10:00 **Federico Lombardi** (Conio S.r.l.)  
10:00-10:05 **Mirko Frighetto** (DataKrypto S.r.l.)  
10:05-10:10 **Massimo Caccia** (Random Power S.r.l.)  
10:10-10:15 **Tiziana Liberati** (E4 Computer Engineering S.p.A.)

## 10:15-11:00 Panel ACN

Moderata: **Roberto Civino**  
(Divisione Algoritmi e Applicazioni Crittografiche, ACN)  
Costruire la filiera crittografica nazionale, dalla ricerca all'industria  
**Marco Baldi** (UNIVPM)  
**Francesca Galli** (Segreteria Tecnica, MUR)  
**Marco Mangiulli** (Capo Ricerca e Sviluppo, ARUBA S.p.A.)

## Chairs

Alessandro Casale (ACN)  
Marco Pedicini (Università Roma Tre)  
Massimiliano Sala (De Cifris)

## Event coordination

cifris26@decifris.it (Valentina)

## 11:30-15:45 Scientific Sessions

**Session I chair:** Roberto La Scala (U. Bari)

11:30-12:00 **Marco Macchetti** (Qualcomm Wireless GmbH)  
*The challenges of securing PQC on embedded systems*

12:00-12:30 **Christopher Battarbee** (University of Edinburgh)  
*The Rise and Fall of Semidirect Product Cryptography in Finite Groups*

12:30-13:00 **Elena Andreeva** (TU Wien)  
*Expanding Primitives, Expanding Possibilities in Symmetric Cryptography*

13:00-14:00 Lunch Break

**Session II chair:** Alessandro Neri (U. Federico II, Napoli)

14:00-14:30 **Violetta Weger** (TUM)  
*Where Does Code-Based Cryptography Stand, and What Will the Future Bring?*

14:30-15:00 **Léo Perrin** (Inria)  
*The Cambrian Explosion of Symmetric Techniques for Advanced Protocols*

15:00-15:30 **Paola de Perthuis** (CWI)  
*Recent advances in module-lattice reduction models*

15:30-15:45 Coffee break

15:45-17:15 **Workshops** (parallel sessions)

17:15-17:30 Coffee break

17:30-19:00 **Workshops** (parallel sessions)



# Roma Tre



DE COMPONENTIS CIFRIS  
ASSOCIAZIONE per la CRITTOGRAFIA

# CIFRIS26

October 5, 2026

Roma Tre University

## PQ Recent Advances in Post-Quantum Cryptography Aula Magna

15:45–16:30 **Ilaria Zappatore** (University of Limoges)

*Decoding Gabidulin codes and their generalizations with application to constant-time RQC*

16:30–17:15 **Guido Lido** (Roma Tor Vergata)

*A generalisation of SQLSign*

17:15–17:30 Coffee break

17:30–18:15 **Laura Mattiuz** (Università Politecnica delle Marche)

*On the Hardness of Finding Permutation Automorphisms of Linear Codes*

18:15–19:00 **Edoardo Signorini** (European Commission JRC)

*Efficient Straight-Line Extractable NIZKPs for Cryptographic Group Actions*

### Comitato organizzatore:

Marco Baldi (Università Politecnica delle Marche), Alessio Caminata (Università degli Studi di Genova), Annamaria Iezzi (Université Grenoble Alpes), Alessio Meneghetti (Università degli Studi di Bari), Edoardo Persichetti (Florida Atlantic University), Federico Pintore (Università degli Studi di Trento).

### Event coordination

cifris26@decifris.it (Valentina)



# Roma Tre



# CIFRIS26

October 5, 2026

Roma Tre University

## TAC TOPICS IN APPLIED CRYPTOGRAPHY Hall C

16:15-16:45 **Andrea Gangemi** (ShunyaXifra)

*On Delegation of Verifiable Presentations from mdoc and BBS Credentials*

16:45-17:15 **Simone Dutto** (ACN)

*The cost of quantum resistance: comparing classical and post-quantum cryptography*

17:15-17:30 Coffee break

17:30-18:00 **Alessandro Barenghi** (Politecnico di Milano)

*Tough cookies in the PQC migration: where current standards will have a hard time chewing*

18:00-18:30 **Alessandra Dolmeta** (Politecnico di Torino)

*Beyond the Algorithm: Hardware/Software Design for Post-Quantum Cryptography*

### Comitato organizzatore:

Riccardo Longo (chair) Fondazione Bruno Kessler, Center for Cybersecurity

Veronica Cristiano - Telsy

Marco Pedicini - Università Roma Tre

Silvio Ranise - FBK Center for Cybersecurity; University of Trento, Department of Mathematics

Alessandro Tomasi - Fondazione Bruno Kessler, Center for Cybersecurity

Stefano Berlato - Fondazione Bruno Kessler, Center for Cybersecurity

Chiara Spadafora - Swiss Post

<https://aleph.fbk.eu/events/TAC2026>

### Chair locale:

Silvia Onofri (Scuola Normale Superiore)

### Event coordination

cifris26@decifris.it (Valentina)



# Roma Tre



DE COMPONENTIS CIFRIS  
ASSOCIAZIONE per la CRITTOGRAFIA

# CIFRIS26

October 5, 2026

Roma Tre University

## SYMM Symmetric and Code Based Cryptography Piazza Telematica Aula 2

15:45-16:30 **André Schrottenloher** (Inria Rennes)

Recent advances in quantum algorithms for cryptanalysis

16:30-17:15 **Valentino Smaldore** (U. Padova)

Three-weight rank-metric codes and regular fat linear sets

17:15-17:30 Coffee break

17:30-18:15 **Emanuele Bellini** (TII)

Automated Cryptanalysis in Symmetric Cryptography: CLAASP Features and Tool Comparison

18:15-19:00 **Roberto Civino** (ACN)

Circle-Linear Cryptanalysis: Bibrace Characters and Weak-Key Linear Distinguishers for

### Comitato Organizzatore

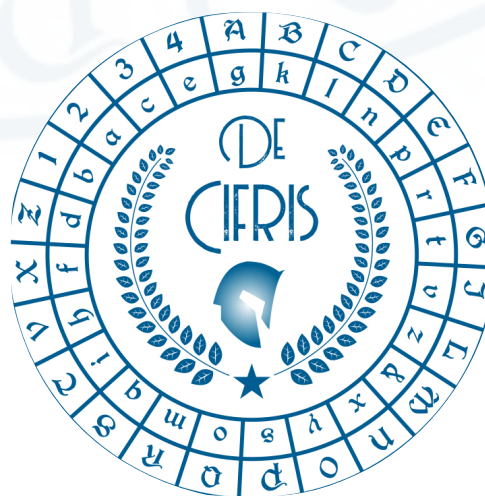
Roberto La Scala (Università di Bari)

Marco Calderini (Università di Trento)

Ferdinando Zullo (Università della Campania)



**Roma Tre**



# CIFRIS26

October 5, 2026

# OPENdams WORKSHOP Aula 3 bis

15:45–16:05 **Silvia Onofri** (Scuola Normale Superiore, Pisa)  
Quantum Private Queries in Entanglement Routing Protocols

16:05–16:25 **Gabriele Radici** (Uni. Trento)  
Binary Quadratic Systems and their relation to complexity theory

16:25–16:45 **Leonardo Errati** (Politecnico di Torino)  
Canonical Liftings: Beyond Signature Compression

16:45–17:00 **Ester Diago** et al. (Uni. Trento)  
A blockchain-based quiz game

17:15–17:30 Coffee break

17:30–17:50 **Tiziana Liberati** (E4 Computer Engineering)  
GPU Acceleration of Learning With Errors KEMs Using OpenACC for Post-Quantum Cryptography

17:50–18:10 **Aurora Pistocchio** et al. (Uni. Trento)  
Quantum Risks in Public Blockchains: Exposure, Readiness, and Migration Strategies

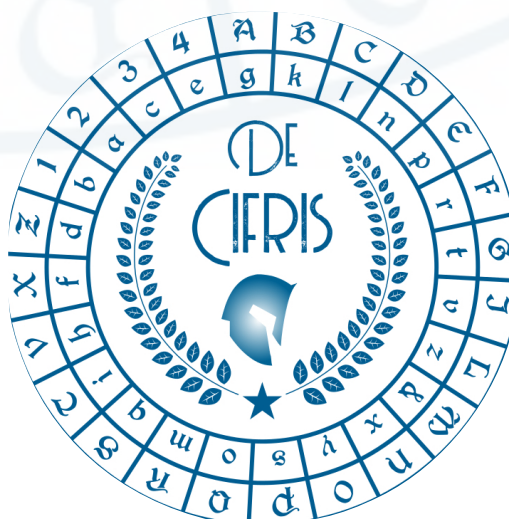
18:10–18:30 **Lorenzo Viganò** (Uni. Trento)  
Sparkle+ and its Security Claims

18:30–18:45 **Edoardo Barbieri** et al. (Uni. Trento)  
Scalable and verifiable off-chain gaming tournaments on the XRP Ledger via Zero-Knowledge proofs

**Chair:** Massimo Caccia (*Random Power*).



## Roma Tre



DE COMPONENTIS CIFRIS  
ASSOCIAZIONE per la CRITTOGRAFIA

# CIFRIS26

October 5, 2026

Roma Tre University

## NT NUMBER THEORY CRYPTOGRAPHY dams Aula 5

17:30-18:10 **Daan van Gent** (Leiden University)  
*Attacks on module lattices using (Galois) symmetries*

18:10-18:25 **Alessandro Cobbe** (Universität der Bundeswehr München)  
*The Rabin cryptosystem over number fields*

18:25-18:40 **Nadir Murru** (Università di Trento)  
*Norms and Embeddings in Fully Homomorphic Encryption*

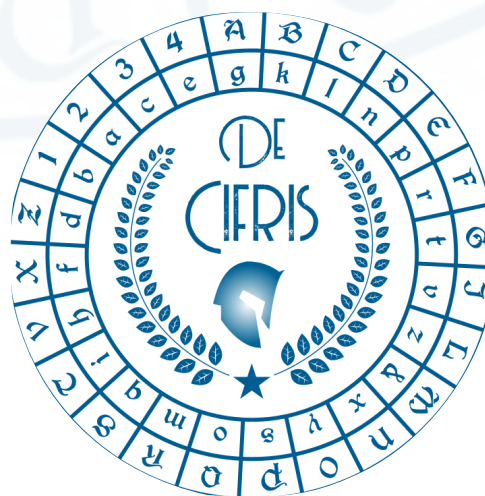
18:40-18:55 **Francesco Sica** (Florida Atlantic University)  
*Improvements to Multi-Scalar Multiplication for Zero-Knowledge Arguments*

### Comitato Organizzatore

- Andrea Gangemi (ShunyaXifra)
- Pietro Mercuri (Università di Trento)



**Roma Tre**



# CIFRIS26

October 5, 2026

Roma Tre University

Il convegno si svolge presso il **Rettorato** in via Ostiense 133B:  
**Aula Magna** (Tower **A**, 2nd Floor)  
**Hall C** (Tower **C**, hall)  
**Aula 2** (Building **D** – Piazza Telematica – 1st floor).

E presso il **DAMS** in via Ostiense 139:  
**Aula 3bis** (al piano rialzato – **OPEN** workshop)  
**Aula 5** (al piano rialzato – **NT** workshop)



Roma Tre

