POLITECNICO DI TORINO
Repository ISTITUZIONALE

Introduction to CIFRIS24 ACTA

Original
Introduction to CIFRIS24 ACTA / Cavicchioni, G., De Feo, L., Errati, L., Masucci, B., Sala, M.. - ELETTRONICO. - 5:(2025), pp. 2-3. [10.69091/koine/vol-5-I00]

Availability:
This version is available at: 11583/3001487 since: 2025-07-03T17:56:40Z

Publisher:
De Cifris Press

Published
DOI:10.69091/koine/vol-5-I00

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

26 November 2026

Introduction to CIFRIS24 ACTA

Con questo volume la nostra collana *De Cifris Koine*, inaugurata con gli atti di Cifris23, compie un anno. Questa edizione raccoglie gli atti di Cifris24, il nostro secondo congresso nazionale, tenutosi a Roma dal 25 al 27 settembre 2024 presso il *Centro Donato Menichella* di Banca d'Italia.
Nella tradizione della precedente edizione, Cifris24 ha offerto una grande occasione di avvicinamento tra discipline distanti con il comune interesse per la crittografia e la sicurezza delle informazioni. Ampio spazio è stato riservato al dialogo tra mondo della ricerca e industria, con particolare attenzione alle sfide emergenti in materia di sicurezza.

La sessione istituzionale si è aperta con gli interventi di Alessandra Perrazzelli, Massimiliano Sala e Marco Pedicini. Abbiamo visto i temi più attuali in campo istituzionale presentati all'interno di una tavola rotonda tra rappresentanti dell'Arma dei Carabinieri, dell'Agenzia per la Cybersicurezza Nazionale (ACN), della Guardia di Finanza e del Ministero degli Interni, moderata da Luigi Bellomarini.
La componente industriale della comunità De Cifris ha mostrato vivo interesse e presentato le proprie iniziative.

La sessione scientifica è stata coordinata dai due chair del comitato scientifico Luca De Feo e Barbara Masucci, che hanno assicurato la qualità e il rigore degli interventi. I temi principali, di dimostrato interesse istituzionale e industriale, sono stati: funzioni booleane, protocolli zero-knowledge, crittografia post-quantistica e quantum-safe, crittografia a chiave pubblica, con risultati sia teorici sia applicati. Quattro prestigiosi invited speaker hanno accresciuto la risonanza dell'evento in ambito scientifico. La varietà nazionale ed internazionale dei sedici interventi e dei loro contenuti dimostrano il crescente interesse italiano per la crittografia.

Accanto alle sessioni scientifiche, Cifris24 ha ospitato una ricca varietà di workshop tematici, con importanti momenti di approfondimento su argomenti specifici. Importanti novità sono state le prime edizioni di

- **QCifris** - Quantum Cifris,
- **FCiR** - Financial Cryptography in Rome
- **CodeMath**, Coding Theory and Discrete Mathematics
- **CPSID**, Cryptography Protocols and Security in Digital Identity

completate da riedizioni di

- **CifrisCloud**, Cryptography for the Cloud
- **NTC**, Number Theory and Cryptography
- **ReAdPQC**, Recent Advances in Post-Quantum Cryptography
- **SymCrypt**, Symmetric Cryptography and Boolean functions
- **TAC**, Topics in Applied Cryptography

Desideriamo ringraziare tutti i relatori e i partecipanti per il loro prezioso contributo, che ha reso possibile la realizzazione di un'edizione ricca di contenuti e spunti di riflessione per la comunità scientifica e professionale.

Febbraio 2025

Giulia Cavicchioni
Luca De Feo
Leonardo Errati
Barbara Masucci
Massimiliano Sala