

DE CIFRIS KOINE
Book Series
Volume III

ERUDITORUM ACTA 2024

DE CIFRIS KOINE

Series Editorial Board

Editor-in-Chief

Massimiliano Sala,
De Componendis Cifris, Presidente

Managing editor

Antonino Ali,
Università di Trento, Professore

Editors

Gianira Nicoletta Alfarano,
KU Leuven, Researcher

Elena Berardini,
Université de Bordeaux, Chaire de Professeur Junior

Martino Borello,
Université Paris 8, Maître de Conférences

Alessio Caminata,
Università di Genova, Ricercatore

Michela Ceria,
Politecnico di Bari, Ricercatrice

Michele Ciampi,
The University of Edinburgh, Chancellor's Fellow

Roberto Civino,
Università dell'Aquila, Ricercatore

Veronica Cristiano,
Telsy SpA, Cryptographer

Daniele Friolo,
Università di Roma "La Sapienza", Ricercatore

Tommaso Gagliardoni,
Kudelski Security, Cryptographer and Scientist

Giovanni Giuseppe Grimaldi,
Università di Napoli Federico II, Ricercatore

Annamaria Iezzi,
Université Grenoble Alpes, Maîtresse de Conférences

Michela Iezzi,
Banca d'Italia, Ricercatrice

Carla Mascia,
HIT - Hub Innovazione Trentino, Ricercatrice

Carmine Monetta,
Università di Salerno, Ricercatore

Andrea Monti,
Università di Chieti, Docente

Marco Moraglio,
Università dell'Insubria, Ricercatore

Nadir Murru,
Università di Trento, Professore

Giancarlo Rinaldo,
Università di Messina, Ricercatore

Francesco Romeo,
Università di Cassino e del Lazio Meridionale, Ricercatore

Carlo Sanna,
Politecnico di Torino, Ricercatore

Paolo Santini,
Università Politecnica delle Marche, Ricercatore

Lea Terracini,
Università di Torino, Professoressa

Marco Timpanella,
Università di Perugia, Ricercatore

Ilaria Zappatore,
Université de Limoges, Maîtresse de Conférences

DE CIFRIS KOINE

Book Series

De Cifris Koine è una collana editoriale curata da De Cifris Press, marchio dell'associazione nazionale De Componendis Cifris dedicata allo studio e alla divulgazione della crittografia e delle discipline correlate.

Questa collana rappresenta un punto di riferimento per la comunità crittografica italiana, offrendo una panoramica delle ricerche e delle innovazioni nel campo. Attraverso la pubblicazione degli atti di conferenze e workshop, De Cifris Koine fornisce non solo approfondimenti scientifici, ma anche contributi divulgativi, mettendo in luce i progressi e le attività dei principali esponenti in questo ambito.

La serie abbraccia un ampio spettro di argomenti, estendendosi oltre la crittografia stessa per includere le sue molteplici applicazioni e intersezioni con altre discipline. Tra queste, si annoverano la teoria dei codici, vari rami della matematica come l'algebra, la teoria dei numeri e la geometria, l'informatica con un focus particolare sulla cybersecurity e sull'informatica teorica, nonché l'ingegneria elettrica, le telecomunicazioni, la storia e gli aspetti legali legati alla crittografia.

Gli articoli pubblicati in questa collana sono accettati in tre lingue: italiano, inglese e francese.

La periodicità della pubblicazione è trimestrale.

De Cifris Koine is a book series published by De Cifris Press, publishing house of the national association De Componendis Cifris, whose activities focus on cryptography and related topics. De Cifris Koine volumes form the voice of the Italian cryptographic community, as they collect communications from both scientific and educational events and summaries of papers of its members and of their activities. In particular, De Cifris Koine hosts conference and workshop proceedings, including short abstracts.

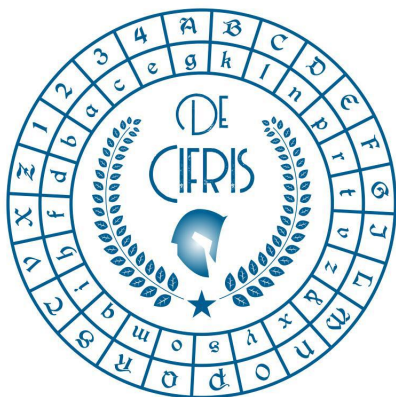
Topics covered in De Cifris Koine volumes relate to cryptography and its applications to and connections with other disciplines, as for example coding theory, maths (mainly algebra, number theory and geometry), computer science (mainly cyber security and theoretical computer science), electronic engineering, telecommunication engineering, history of cryptography and law. Accepted articles are either in Italian, English or French. Volumes are published quarterly.

La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

Cette collection est une référence importante pour la communauté cryptographique italienne, offrant une vue d'ensemble de la recherche et des innovations dans ce domaine. Grâce à la publication d'actes de conférences et de groupes de travail (workshops), la De Cifris Koine fournit non seulement des contributions scientifiques académiques, mais aussi des contributions à destination du grand public, mettant en lumière les progrès et les activités des principaux acteurs et des principales actrices du domaine.

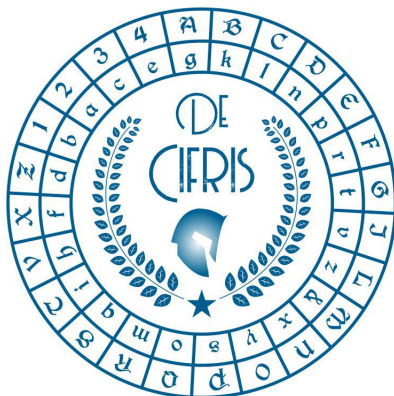
Les articles de cette collection couvrent un large éventail de sujets allant de la cryptographie à ses nombreuses applications et intersections avec d'autres disciplines. On y retrouve notamment la théorie des codes, diverses branches des mathématiques telles que l'algèbre, la théorie des nombres et la géométrie, l'informatique, avec un accent sur la sécurité informatique et l'informatique théorique, ainsi que le génie électrique, les télécommunications et les aspects juridiques de la cryptographie. Les articles soumis à la De Cifris Koine sont acceptés en italien, anglais et français. La fréquence de publication est trimestrielle.

ERUDITORUM ACTA 2024



Edited by:

- *Antonino Ali*,
Università di Trento, Italy.
- *Massimiliano Sala*,
Università di Trento, Italy.



Pubblicazione trimestrale di proprietà dell'associazione nazionale di crittografia
De Componendis Cifris

Autorizzazione del Tribunale di Milano in data 23 - 02 - 2024

Num. R.G. 1315/2024 Num. Reg. Stampa 22

ISSN 3034-9796 - ISBN 979-12-81863-02-6

I diritti d'autore sono riservati.

L'uso di fotocopie di documenti conservati dall'Archivio di Stato di Venezia è stato concesso con suo Nulla Osta dal protocollo ASVe 3269/2024.

Editore: De Componendis Cifris APS.

Marchio Editoriale: De Cifris Press.

Direttore responsabile: Massimiliano Sala

Redazione: Antonino Ali, Nadir Murru

Luogo di pubblicazione: Via Gianfranco Zuretti 34 - 20125 Milano

e-mail: editorial@decifris.it

Stampa in proprio

Numero 3 - Pubblicato il 01 - 09 - 2024

PREFACE

Questo volume, raccogliendo i contributi presentati durante il nostro convegno "*De Cifris Eruditorum 2024*", offre un'analisi multidisciplinare della crittografia, tracciando il suo percorso storico ed esplorando, da un punto di vista giuridico, le sue attuali applicazioni e implicazioni.

I tre interventi storici toccano sia l'età classica, sia il Medio Evo, sia il Rinascimento. I due contributi giuridici si concentrano sulla cyber security e sul delicato equilibrio tra il rispetto dei diritti fondamentali e la necessità di sicurezza.

This volume contains all talks given at our conference "*De Cifris Eruditorum 2024*". It offers a multidisciplinary approach to cryptography, starting from its historical evolution and arriving at exploring its current applications from a legal point of view.

The three historical talks touch on the cryptographic evolution in the classical age, in the Middle Ages and in the Renaissance.

The two talks by legal experts focus on cyber security and the difficult balance between fundamental rights and security needs.

Ce volume, rassemblant les contributions présentées lors de notre conférence "*De Cifris Eruditorum 2024*", offre une analyse multidisciplinaire de la cryptographie, retraçant son parcours historique et explorant, d'un point de vue juridique, ses applications et implications actuelles.

Les trois interventions historiques couvrent l'âge classique, le Moyen Âge et la Renaissance. Les deux contributions juridiques se concentrent sur la cyber sécurité et sur le délicat équilibre entre le respect des droits fondamentaux et la nécessité de sécurité.

Massimiliano Sala & Antonino Ali
Editor in Chief & Managing Editor
De Cifris Koine

Indice

| | |
|--|----|
| Introduzione a Eruditorum ACTA 2024 | 2 |
| <i>Antonino Ali and Massimiliano Sala</i> | |
| Franceschi - Partenio, una disputa crittografica nel Rinascimento | 5 |
| <i>Paolo Bonavoglia</i> | |
| Scrivere per nascondere, leggere per scoprire. Le origini della crittografia | 24 |
| <i>Marco Moraglio</i> | |
| Epigrafi cifrate nelle chiese antiche | 35 |
| <i>Cosimo Palma</i> | |
| Il nuovo framework giuridico cyber dell'Italia. La crittografia come strumento di cybersicurezza e per l'autonomia strategica nazionale | 52 |
| <i>Marcello Albergoni</i> | |
| Human Rights Implications of Encryption Backdoors | 59 |
| <i>Antonino Ali</i> | |