

DE CIFRIS KOINE
Book Series
Volume I

CIFRIS23 ACTA

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 Edimburgh, 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.

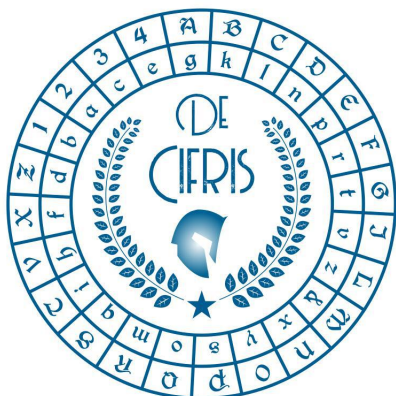
La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

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. Par exemple, 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.

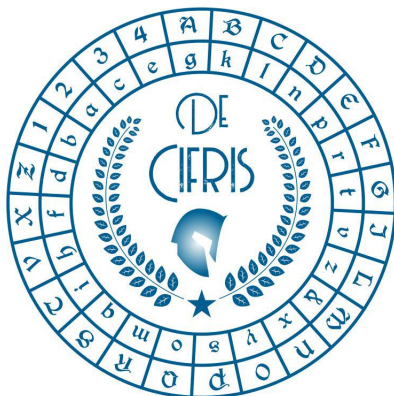
CIFRIS23 ACTA

Official Proceedings of the 2023 Congress of *De Componendis Cifris*



Edited by:

- *Daniele Friolo*,
Università di Roma "La Sapienza", Italy
- *Roberto Civino*,
Università dell'Aquila, Italy
- *Michele Ciampi*,
The University of Edinburgh, United Kingdom
- *Sihem Mesnager*,
University of Paris VIII, France
- *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 979-12-81863-00-2

I diritti d'autore sono riservati.

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 1 - Pubblicato il 30 - 04 - 2024

PREFACE

Il primo volume della collana De Cifris Koine segna l'apertura di un nuovo capitolo per la nostra associazione ed è dedicato agli atti del primo congresso nazionale di crittografia, CIFRIS23. Questa iniziativa rappresenta un importante punto di svolta, evidenziando il dinamismo e l'impegno della comunità crittografica italiana. La selezione dei lavori in questo volume, e più in generale nelle prossime edizioni della collana, riflette non solo l'eccellenza e la diversità della ricerca crittografica nel nostro Paese, ma anche il sostenuto interesse delle istituzioni e del settore aziendale. Questa attenzione conferma la crittografia come elemento centrale nelle strategie di sicurezza e nell'innovazione tecnologica. Con il lancio di questa collana, ci proponiamo di creare una risorsa preziosa per gli esperti del settore, fornendo una panoramica aggiornata e stimolante di un campo in costante evoluzione.

The first volume of the De Cifris Koine series marks the opening of a new chapter for our association and is dedicated to the proceedings of the first national cryptographic congress, CIFRIS23. This initiative represents an important turning point, highlighting the dynamism and commitment of the Italian cryptographic community. The selection of papers in this volume, and more generally in future editions of the series, reflects not only the excellence and diversity of cryptographic research in our country, but also the sustained interest of institutions and the corporate sector. This attention confirms cryptography as a central element in security strategies and technological innovation. With the launch of this series, we aim to create a valuable resource for experts in the field, providing an up-to-date and stimulating overview of a constantly evolving field.

Le premier volume de la série De Cifris Koine marque l'ouverture d'un nouveau chapitre pour notre association et est consacré aux actes du premier congrès national de cryptographie, CIFRIS23. Cette initiative représente un moment important, qui souligne le dynamisme et l'engagement de la communauté cryptographique italienne. La sélection des articles dans ce volume, et plus généralement dans les éditions futures de la série, reflète non seulement l'excellence et la diversité de la recherche cryptographique dans notre pays, mais aussi l'intérêt soutenu des institutions et du secteur des entreprises. Cette attention confirme que la cryptographie est un élément central des stratégies de sécurité et de l'innovation technologique. Avec le lancement de cette série, nous visons à créer une ressource précieuse pour les experts dans le domaine, en fournissant une vue d'ensemble actualisée et stimulante d'un domaine en constante évolution.

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

Table of Contents

Part I Introduction to CIFRIS23 ACTA

Part II Institutional Session

Round Table with representatives of government's Departments and other Italian public-law institutions	8
<i>Francesca Medda</i>	
Cryptography and its applications in the Italian scenario	17
<i>Massimo Giulietti</i>	
La visione di De Cifris: partnership con le aziende leader	19
<i>Antonino Ali</i>	
La crittografia nelle comunicazioni sicure: l'esperienza BV TECH	22
<i>Vincenzo Mafra</i>	
Telsy e l'indipendenza tecnologica nel campo della crittografia	26
<i>Speech of Guglielmo Morgari</i>	

Part III Scientific Session

Number theory and cryptography

KEYNOTE: MPC in the head for isomorphisms and group action	32
<i>Antoine Joux</i>	
Efficiency of SIDH-based signatures (yes, SIDH)	34
<i>Wissam Ghantous, Federico Pintore and Mattia Veroni</i>	
The group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$	36
<i>Massimiliano Sala and Daniele Taufer</i>	

Between theory and practice

FPGA And Software Acceleration of Multi-Scalar Multiplication: CycloneMSM	40
<i>Kaveh Aasaraai, Emanuele Cesena, Rahul Maganti, Nicolas Stalder, and Javier Varela</i>	
On Linear Codes with Random Multiplier Vectors and the Maximum Trace Dimension Property	41
<i>Márton Erdélyi, Pál Hegedüs, Sándor Z. Kiss, and Gábor P. Nagy</i>	
On a generalization of the Deligne-Lustzig curve of Suzuki type and application to AG codes	43
<i>Marco Timpanella</i>	
On the Black-Box Impossibility of Multi-Designated Verifiers Signature Schemes from Ring Signature Schemes	45
<i>Kyosuke Yamashita and Keisuke Hara</i>	

Boolean functions and symmetric cryptography

KEYNOTE: Threshold Implementations: Securing Implementations of Symmetric-Key Algorithms	49
<i>Keynote by Svetla Nikova</i>	
Differential experiments using parallel alternative operations	52
<i>Marco Calderini, Roberto Civino, and Riccardo Invernizzi</i>	
Automatic Boomerang Attacks Search on Rijndael	55
<i>Marine Minier, Loïc Rouquette, and Christine Solnon</i>	

Cloud encryption

Searchable Encryption with randomized ciphertext and randomized keyword search	58
<i>Marco Calderini, Riccardo Longo, Massimiliano Sala, and Irene Villa</i>	
Cryptanalysis of a privacy-preserving authentication scheme	61
<i>Sigurd Eskeland</i>	
mRLWE-CP-ABE: a revocable CP-ABE for post-quantum cryptography	64
<i>Marco Cianfriglia, Elia Onofri*, and Marco Pedicini</i>	

Part IV Workshops

Synthetic data and finance

Organizer: Francesca Medda

CBDCs, Digital Currencies and Assets Tokenization: opportunities and risks

Organizers: Andrea Bracciali and Davide Carboni

Introduction to CBDCs Workshop	70
<i>Daniel Broby</i>	
Crypto assets' value and investor protection	73
<i>Gianfranco Trovatore</i>	
What consensus mechanism will be used for Central Bank Digital Currencies (CBDCs)?	75
<i>Vincenzo Vespri and Filippo Zatti</i>	
CBDCs: A new generation of digital cash	78
<i>Guneet Kaur and Andrea Bracciali</i>	

Recent Advances in Post-Quantum Cryptography

Organizers: Marco Baldi, Giulio Codogni, Elisa Gorla, Roberto La Scala, Alessio Meneghetti, Emanuela Orsini, Gerardo Pelosi, Edoardo Persichetti and Federico Pintore

Introduction to PQ Workshop	83
<i>Marco Baldi, Giulio Codogni, Elisa Gorla, Roberto La Scala, Alessio Meneghetti, Emanuela Orsini, Gerardo Pelosi, Edoardo Persichetti, and Federico Pintore</i>	
SQISIGN	85
<i>Luca De Feo</i>	
No one should learn from these errors: surveying fault attack resistance of post quantum cryptosystems	88
<i>Alessandro Barenghì</i>	
MCE and MEDS: From Group Actions to Signatures	91
<i>Krijn Reijnders</i>	

Signatures from Five-Pass Zero-Knowledge Protocols and the Curious Case of CROSS	94
<i>Paolo Santini</i>	

Topics in Applied Cryptography

Organizers: Silvio Ranise, Alessandro Tomasi, D’Intino Andrea and Roio Denis

Introduction to TAC Workshop	98
<i>Silvio Ranise and Alessandro Tomasi</i>	
Royal Rumbles in Cryptography: the NIST PQC Competition	100
<i>Marco Baldi</i>	
The Zencode Whitepaper	102
<i>Denis Roio</i>	
Multiparty Class Group Encryption and Applications to E-Voting	105
<i>Michele Battaqliola, Giuseppe D’Alconzo, Andrea Gangemi, and Chiara Spadafora</i>	
Vote App: Verifiable and Coercion-Resistant I-Voting	107
<i>Riccardo Longo, Chiara Spadafora, and Francesco Antonio Marino</i>	
OpenABE Bindings for Kotlin	110
<i>Stefano Berlato, Roberto Carbone, and Silvio Ranise</i>	
Cryptographic Enforcement of Attribute-based Access Control Policies	113
<i>Stefano Berlato, Alessandro Colombo, Roberto Carbone, and Silvio Ranise</i>	

Privacy-preserving Machine Learning Workshop

Organizers: Marco Pedicini and Michela Iezzi

Introduction to Privacy-Preserving ML Workshop	117
•	
Privacy Preserving Machine Learning with TFHE	118
<i>Andrei Stoian</i>	
PPML: Machine learning on data you cannot see	119
<i>Valerio Maggio</i>	

New trends in Group-Based Cryptography

Organizers: Norberto Gavioli, Carmine Monetta and Marialaura Noce

Introduction to Group-based Workshop	122
<i>Norberto Gavioli, Carmine Monetta, and Marialaura Noce</i>	
The Impact of the Semidirect Discrete Logarithm Problem (SDLP) in Post-quantum Cryptography PQC	124
<i>Delaram Kahrobaei</i>	
Some results on the groups generated by round functions	127
<i>Riccardo Aragona</i>	
A method to cryptanalyze (Simultaneous) Conjugacy Search Problem in certain Metabelian Platform Groups	130
<i>Martina Vigorito</i>	
Linearization of hard problems via right-angled Artin groups	133
<i>Ramón Flores, Delaram Kahrobaei, and Thomas Koberda</i>	
A “smart” application of homomorphic encryption	135
<i>Antonio Tortora</i>	

La visione di De Cifris: partnership con le aziende leader

Antonino Ali

Membro del Collegio dei probiviri e del Comitato Scientifico di De Componendis Cifris
antonino.ali@unitn.it

In questa sessione del Congresso, discuteremo la collaborazione tra la nostra associazione, e il settore privato. In qualità di membro della De Cifris - Società Italiana di Crittografia, e in veste di esperto legale specializzato in regolamentazione e controllo dell'uso della crittografia, intendo delineare la missione e gli obiettivi principali della De Cifris. Questi riflettono la nostra visione e le nostre aspirazioni, tenendo conto della recente costituzione dell'associazione.

Un obiettivo cardine dell'associazione, come esplicitato nell'articolo 4, paragrafi 1-2, dello Statuto, è esplorare le potenzialità della crittografia a vantaggio del nostro Paese. Da tempo, la nostra associazione si dedica alla promozione e allo sviluppo della crittografia avanzata, favorendo la ricerca di eccellenza, l'innovazione e la formazione di professionisti nel campo della sicurezza informatica. L'integrazione ottimale delle competenze nazionali in materia di crittografia rientra tra gli obiettivi primari dell'Associazione.

L'apertura dell'associazione al mondo privato aziendale costituisce un passo significativo per rafforzare la sicurezza informatica e l'innovazione tecnologica complessive. Questa collaborazione pubblico-privata facilita lo scambio di conoscenze e competenze, un elemento cruciale in un settore in rapida evoluzione come quello della sicurezza digitale. Le imprese private apportano esperienza pratica e soluzioni innovative, che possono essere integrate nelle strategie di sicurezza a livello nazionale e internazionale.

Inoltre, l'inclusione del settore privato nell'associazione stimola la ricerca e lo sviluppo in tecnologie crittografiche avanzate, promuovendo maggiore sicurezza dei dati e privacy per aziende e consumatori. Questa sinergia tra diversi settori può accelerare il progresso verso sistemi crittografici più robusti, a beneficio dell'intera società nella lotta contro le minacce informatiche e nella protezione delle informazioni sensibili.

De Cifris mira a stabilire partnership con aziende leader nel campo della crittografia e a creare sinergie tra università, ricerca e industria. Queste collaborazioni strategiche possono accelerare lo sviluppo di prodotti, servizi e piattaforme crittografiche di spicco, contribuendo significativamente alla sicurezza e allo sviluppo tecnologico del nostro Paese. Riteniamo essenziale la collaborazione tra competenze

crittografiche nazionali per il futuro della nostra sicurezza digitale e dello sviluppo tecnologico.

Questo Congresso segna un momento fondamentale per avviare e rafforzare collaborazioni tra il settore pubblico e quello privato nel campo della crittografia, un passo decisivo per consolidare la posizione del nostro Stato in un contesto globale sempre più interconnesso e digitalizzato. De Cifris, nel suo regolamento, prevede specifiche modalità per permettere a enti pubblici e aziende private di aderire, definendo chiaramente le linee guida per sponsorizzazioni e partnership.

Uno degli obiettivi primari di De Cifris è promuovere attivamente lo studio e la ricerca nel settore crittografico in Italia, abbracciando sia gli aspetti teorici che quelli applicativi. Questo si traduce in un impegno costante per facilitare collaborazioni sinergiche tra università, istituzioni e imprese, creando un ecosistema fertile per l'innovazione e lo sviluppo. In aggiunta, l'associazione offre corsi di formazione e specializzazione, rivolti a imprese di varie dimensioni, per diffondere le competenze crittografiche e rispondere alle esigenze del mercato.

L'Associazione De Cifris, per il raggiungimento dei suoi scopi sociali e per lo svolgimento delle attività menzionate, è aperta a collaborazioni con le istituzioni pubbliche italiane ed europee, così come con entità private di diverse tipologie e forme. Questo include la partecipazione attiva nella stesura di politiche e normative tecniche, un ruolo che sottolinea l'importanza e l'influenza di De Cifris nel panorama crittografico nazionale e internazionale. Con questi sforzi, l'associazione mira a costruire un ponte solido tra vari settori, favorendo un avanzamento tecnologico e scientifico condiviso e orientato al futuro.

Dalle presentazioni dell'Ing. Vincenzo Mafrika di BVTECH e del dott. Guglielmo Morgari di TELSYP emergono temi chiave che intrecciano gli aspetti classici e strategici della crittografia nel contesto della sovranità tecnologica.

L'intervento dell'Ing. Mafrika mette in luce l'esperienza di BV Tech nel campo della crittografia per le comunicazioni sicure, sottolineando l'importanza tradizionale della crittografia nel garantire comunicazioni sicure, proteggere dati sensibili e supportare infrastrutture critiche. Questo approccio classico alla crittografia è essenziale per mantenere un tessuto digitale sicuro e affidabile.

Dall'altra parte, il dott. Morgari, intervenendo per TELSYP, evidenzia il ruolo strategico della crittografia nel raggiungimento della sovranità tecnologica nazionale. La sua presentazione si concentra sull'importanza di possedere e controllare le tecnologie crittografiche, fondamentali per preservare l'indipendenza e l'autonomia tecnologica di uno Stato. Qui, la crittografia trascende la sua funzione di mera misura di sicurezza, assumendo il ruolo di pilastro per la protezione dell'indipendenza tecnologica.

Il contributo congiunto dei rappresentanti di queste società private, con cui la nostra associazione collabora, mette in evidenza la funzione multipla di questa disciplina in un panorama tecnologico avanzato e interconnesso. Da un lato, essa agisce come baluardo nella protezione delle comunicazioni e dei dati, un ruolo vitale per

la sicurezza quotidiana delle informazioni in un'era in cui i dati rappresentano una risorsa cruciale. Dall'altro, assume un significato strategico più ampio nel rafforzare l'autonomia tecnologica e la sovranità di uno Stato. In questo ambito, diventa essenziale per mantenere il controllo sulle proprie risorse tecnologiche e per garantire l'indipendenza nazionale in settori chiave come l'informazione e la tecnologia.

Pertanto, la crittografia emerge come elemento essenziale non solo per la difesa delle informazioni sensibili e la protezione della privacy individuale e collettiva, ma anche come fattore chiave per l'affermazione e il mantenimento dell'indipendenza tecnologica. L'efficacia su questi due livelli complementari sottolinea l'importanza crescente della disciplina nell'era digitale, evidenziando il suo ruolo centrale nella strategia di sicurezza e sovranità tecnologica.