DE CIFRIS KOINE
Book Series
Volume I

CIFRIS23 ACTA

DE CIFRIS KOINE
Series Editorial Board

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.

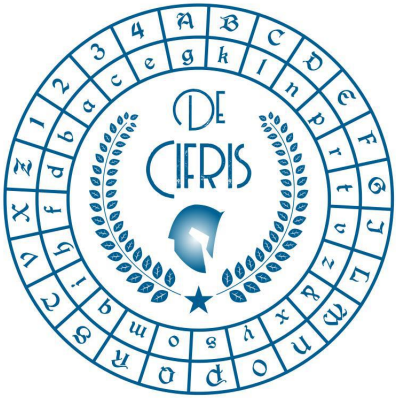
La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

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 publique, 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.

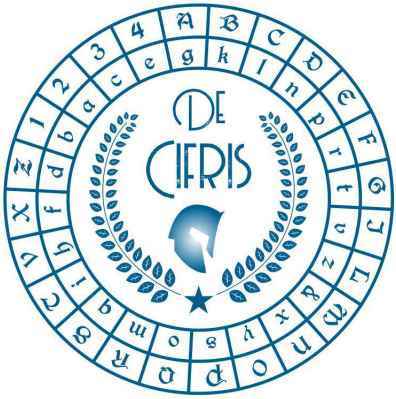
CIFRIS23 ACTA

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 Edimburgh, 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

Editore: De Componendis Cifris APS.
Marchio Editoriale: De Cifris Press.
Direttore responsabile: Massimiliano Sala
Redazione: Antonino Alì, 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 Alì
Editor in Chief & Managing Editor
De Cifris Koine

Table of Contents

Between theory and practice

Boolean functions and symmetric cryptography

Cloud encryption

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

Recent Advances in Post-Quantum Cryptography
Organizers: Marco Baldi, Giulio Codogni, Elisa Gorla, Roberto La Scala, Alessio Meneghetti, Emmanuela Orsini, Gerardo Pelosi, Edoardo Persichetti and Federico Pintore

Topics in Applied Cryptography

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

Privacy-preserving Machine Learning Workshop

Organizers: Marco Pedicini and Michela Iezzi

New trends in Group-Based Cryptography

Organizers: Norberto Gavioli, Carmine Monetta and Marialaura Noce

La visione di De Cifris: partnership con le aziende leader

Antonino Alì

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 Mafrica di BVTECH e del dott. Guglielmo Morgari di TELSY emergono temi chiave che intrecciano gli aspetti classici e strategici della crittografia nel contesto della sovranità tecnologica.

L'intervento dell'Ing. Mafrica 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 TELSY, 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.