

COLLECTIO CIPHRARUM

Book Series

3

Editor in Chief

Massimiliano SALA
Università degli Studi di Trento

Scientific Committee

Carlo BLUNDO
Università degli Studi di Salerno

Robert COULTER
University of Delaware

Alfredo DE SANTIS
Università degli Studi di Salerno

Eric FILIOL
University Higher School of Economics of Moscow

Massimo GIULIETTI
Università degli Studi di Perugia

Tor HELLESETH
University of Bergen

Gabor KORCHMAROS
Università degli Studi della Basilicata

Sihem MESNAGER
Université Vincennes–Saint–Denis (Paris 8)

Francesco PAPPALARDI
Università degli Studi Roma Tre

Ivan VISCONTI
Università degli Studi di Salerno

Founder

Michele ELIA
Politecnico di Torino

COLLECTIO CIPHRARUM

Book Series

OP	a	b	c	d	e	f	g	h	i	l	m	
	x	y	z	n	o	p	q	r	r	f	t	u
QR	a	b	c	d	e	f	g	h	i	l	m	
	q	r	f	t	u	x	y	z	n	o	p	
ST	a	b	c	d	e	f	g	h	i	l	m	
	p	q	r	f	t	u	x	y	z	n	o	
VX	a	b	c	d	e	f	g	h	i	l	m	
	u	x	y	z	n	o	p	q	r	f	t	
YZ	a	b	c	d	e	f	g	h	i	l	m	
	o	p	q	r	f	t	u	x	y	z	n	

The method is capable of dispatching with accuracy every kind of urgent messages, but in practice it requires care and exact attention.

(POLYBIUS 150 BC)

La collana *Collectio CiphRARum* pubblica atti di convegni e workshop in crittografia e argomenti affini, inclusi cicli di seminari di ampia durata. La collana ospita con preferenza non esclusiva atti di convegni in Italia o organizzati congiuntamente da sedi italiane e straniere. Di norma ogni volume ospita tra dieci e venti interventi, in formato di extended abstract ciascuno in lingua inglese, più eventuali survey tematici dietro invito degli editor. Gli abstract possono anche riassumere risultati già pubblicati in altre sedi. Tutti i contributi sono referati in maniera anonima da esperti internazionali. Gli organizzatori di un workshop sono invitati a proporre la pubblicazione degli atti nella *Collectio CiphRARum* contattando il Board.

The book series *Collectio CiphRARum* presents proceedings papers of talks given at workshops/conferences in Cryptography and related matters, including talks given at organized seminar series. *Collectio CiphRARum* has a keen interest in workshops/conferences that are either held in Italy or co-organized by at least one Italian research institution. A book will usually contain ten to twenty extended abstracts, sketching research that June be published in another publication venue, plus invited surveys, which are meant to be published exclusively here. All papers are refereed by anonymous international experts. Any organizer of a workshop/conference, falling in the book series scope, is invited to contact the Editorial Board for proposing a new volume.

CRYPTOGRAPHY AND CODING THEORY CONFERENCE 2021

edited by

ROBERTO GUGLIELMO MORGARI, MARIA TOTA, FERDINANDO ZULLO

preface by

MASSIMILIANO SALA

Contributions of

GIANIRA ALFARANO, AMIR HAMZAH ABD GHAFAR, DAVIDE BACCO, MARCO BALDI
CHRISTOPHER BATTARBEE, ELENA BERARDINI, MATTEO BOCCHI, MARTINO BORELLO
ALESSANDRO BUDRONI, MARCO CALDERINI, ALESSIO CAMINATA, ISAAC CANALES MARTÍNEZ
GIUSEPPE COTARDO, ADRIANO GAIBOTTI, PAOLO GASTI, WISSAM GHANTOUS, MASSIMO GIULIETTI
EMANUELE GIUNTA, HEIDE GLUESING-LUERSSEN, ELISA GORLA, ANNAMARIA IEZZI, NICCOLÒ IZZO
RELINDE JURRIUS, WRYA K. KADIR, LEYLA İŞİK, STEFANO LIA, MICHAEL LODI, GIOVANNI LONGOBARDI
JONATHAN MANNAERT, CAROLA MANOLINO, SIHEM MESNAGER, ANDREA MOLINO, PAOLA MORANDO
MIGUEL ÁNGEL NAVARRO PÉREZ, FRANCESCO PAVESE, MARCO PEDICINI, EDOARDO PERSICHETTI
ENRICO PICCIONE, FEDERICO PINTORE, JOACHIM ROSENTHAL, MASSIMILIANO SALA
ALEXANDER SALTUARI, PAOLO SANTONASTASO, MANUELA SAPONARO, MARCO TIMPANELLA
MATTEO TORRE, IVAN VISCONTI, ILARIA ZAPPATORE, GIOVANNI ZINI



aracne



ISBN
979-12-5994-981-3

FIRST EDITION
ROMA 9 JUNE 2022

Contents

Part I Introduction

- 15 Preface
Massimiliano Sala
- 17 Cryptography and Coding Theory for the community
*Norberto Gavioli, Guglielmo Morgari,
Maria Tota, Ferdinando Zullo*

Part II Abstracts Scientific session - Invited speakers

- 23 Degrees of regularity
Alessio Caminata
- 25 A general theory of supports and generalized weights for
linear codes
Elisa Gorla
- 27 q -Analogues in codes and related combinatorics
Relinde Jurrius
- 29 “Readers digest of” 17-year achievements on Boolean and
vectorial functions and open problems
Sihem Mesnager
- 31 The work of Michele Elia on continued fractions and factor-
ing
Joachim Rosenthal

Part III
Abstracts Scientific session

- 35 Partial key exposure attack on RSA using Dickman's function
*Amir Hamzah A. Ghafar**, *Muhammad Rezal K. Ariffin*
- 37 Riemann–Roch spaces and algebraic geometry codes
Simon Abeldard, *Yves Aubry*, *Elena Berardini**, *Alain Couvreur*,
Fabien Herbaut, *Grégoire Lecerf*, *Marc Perret*
- 39 Roos-like bound for skew-cyclic codes in Hamming and (sum-)rank metric
*Gianira N. Alfarano**, *F. Javier Lobillo*,
Alessandro Neri, *Antonia Wachter-Zeh*
- 41 Bruhat–Tits trees as a cryptanalytic tool for isogeny-based cryptography
Laia Amorós, *Annamaria Iezzi**, *Kristin Lauter*,
Chloe Martindale, *Jana Sotáková*
- 43 LESS-FM: fine-tuning signatures from the code equivalence problem
Alessandro Barenghi, *Jean-François Biasse*,
*Edoardo Persichetti**, *Paolo Santini*
- 45 On existence of certain APN functions over $\mathbb{F}_{2^{3m}}$
Daniele Bartoli, *Marco Calderini**,
Olga Polverino and *Ferdinando Zullo*
- 47 Cryptanalysis of semidirect product key exchange using matrices over non-commutative rings
*Christopher Battarbee**, *Delaram Kahrobaei*, *Siamak F. Shahandashti*
- 49 On short minimal codes and related combinatorial structures
Martino Borello
- 51 Explicit formulas for hashing into \mathbb{G}_2 on BLS pairing-friendly curves
Alessandro Budroni, *Federico Pintore**

- 53 A new trapdoor construction for LWE
*Alessandro Budroni**, *Igor Semaev*
- 55 Multivariate correlation attacks and the cryptanalysis of LFSR-based stream ciphers
*Isaac A. Canales-Martínez**, *Igor Semaev*
- 57 On interactive oracle proofs for Boolean R1CS statements
Ignacio Cascudo, *Emanuele Giunta**
- 59 Small complete caps in $\text{PG}(4n + 1, q)$
Antonio Cossidente, *Bence Csajbók*,
Giuseppe Marino, *Francesco Pavese**
- 61 Codes for the binary asymmetric channel
*Giuseppe Cotardo**, *Alberto Ravagnani*
- 63 On the non-existence of Cameron-Liebler sets of k -spaces in $\text{PG}(n, q)$
Jan De Beule, *Jonathan Mannaert**, *Leo Storme*
- 65 Loops, multi-edges and collisions in supersingular isogeny graphs
Wissam Gbantous
- 67 PIR codes from combinatorial structures
Massimo Giulietti, *Arianna Sabatini*, *Marco Timpanella**
- 69 An algorithm-based fault tolerant technique for solving polynomial linear systems
Eleonora Guerrini, *Romain Lebreton*, *Ilaria Zappatore**
- 71 Independent spaces of q -polymatroids
*Heide Gluesing-Luerssen**, *Benjamin Jany*
- 73 On the index of the Diffie-Hellman mapping
*Leyla Işık**, *Arne Winterhof*
- 75 On interpolation-based decoding of MRD codes
*Wrya K. Kadir**, *Chunlei Li*, *Ferdinando Zullo*

- 77 AG codes from \mathbb{F}_q -rational points of the GK maximal curve
*Stefano Lia**, *Marco Timpanella*
- 79 Partially scattered linearized polynomials, linear sets and rank metric codes
*Giovanni Longobardi**, *Corrado Zanella*
- 81 Optimum distance flag codes and Singer groups
*Miguel Ángel Navarro-Pérez**, *Xaro Soler-Escrivà*
- 83 Algebraic attack on the WG-PRNG
Enrico Piccione
- 85 On a class of linear square MRD codes
Olga Polverino, *Marco Timpanella*,
*Giovanni Zini**, *Ferdinando Zullo*
- 87 On the list decodability of rank-metric codes
*Paolo Santonastaso**, *Ferdinando Zullo*

Part IV

Abstracts Corporate research session

- 91 Compute express link security
Paolo Amato, *Danilo Caraccio*, *Niccolò Izzo**
- 93 Quantum key distribution for telecom applications
*Davide Bacco**, *Ilaria Vagniluca*,
Tommaso Occhipinti, *Alessandro Zavatta*
- 95 Hash-based post-quantum signature verifications on 32-bit microcontrollers
Matteo Bocchi, *Adriano Gaibotti*
- 97 Cryptography for electronic locks in security doors
Luca De Robertis, *Giuseppe Leotta*, *Andrea Molino**
- 99 Keyless: a privacy-preserving biometric authentication system
Paolo Gasti