COLLECTIO CIPHRARUM

Book Series

3

COLLECTIO CIPHRARUM

Book Series

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 IŞIK, 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 III
Abstracts Scientific session