

# ALGEBRA FOR CRYPTOGRAPHY

edited by

**RICCARDO ARAGONA  
NORBERTO GAVIOLI  
FILIPPO MIGNOSI**

preface by

**MASSIMILIANO SALA**

OP a b c d e f g h i l m  
x y z n o p q 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

COLLECTIO CIPHRARUM N. 1  
PROCEEDINGS OF CRYPTOGRAPHIC CONFERENCES AND WORKSHOPS

## ALGEBRA FOR CRYPTOGRAPHY

In this volume we report talks given at the workshop "Algebra for Cryptography", held at L'Aquila in 2019. Young and talented speakers covered a wide range of algebraic methods of cryptographic interest, such as group theory, elliptic curves and Boolean functions. The talks reported here will nicely introduce the reader to such research lines, who will get a general idea of the connection between Algebra and Cryptography.

*Contributions of* Martino BORELLO, Marco CALDERINI, Roberto CIVINO, Ilaria COLAZZO, Francesca DALLA VOLTA, Luciano MAINO, Alessio MENEGHETTI, Nadir MURRU, Federico PINTORE, Maria TOTA, Giovanni ZINI.



### RICCARDO ARAGONA

Born in Rome in 1980, he is a researcher at the DISIM of the University of L'Aquila, on issues relating to groups of permutations and symmetric cryptography. After graduating in Mathematics at the "Sapienza" University of Rome, he obtained a doctorate in Mathematics at the "Tor Vergata" University of Rome in co-tutorship with the Northeastern University of Boston. After 9 years of research grants at the "Sapienza" and the University of Trento, he arrived in L'Aquila in 2018.



### NORBERTO GAVIOLI

Born in Varese in 1964, he obtained a doctorate in Mathematics from the University of Trento and has been an associate professor of Algebra at the University of L'Aquila since 2000. His research mainly concerns finite  $p$ -groups,  $p$  groups, modular Lie algebras, applications of group theory to symmetric cryptography. He is coordinator of the Cryptography and Codes group of the Italian Mathematical Union, participates in the national initiative De Componendis Cifris.



### FILIPPO MIGNOSI

Born in Palermo in 1963, he is full professor of Computer Science at the University of L'Aquila. After a degree in Mathematics with a thesis in number theory, he received a doctorate in 1991 in "Fundamental Computer Science" at the University of Paris and two years later a doctorate in Mathematics in Italy. He currently deals with algorithm theory, Deep Learning, information theory and cryptography, combinatorics and discrete mathematics.

# ALGEBRA FOR CRYPTOGRAPHY

edited by

**RICCARDO ARAGONA, NORBERTO GAVIOLI, FILIPPO MIGNOSI**

preface by

**MASSIMILIANO SALA**

*Contributions of*

**MARTINO BORELLO, MARCO CALDERINI, ROBERTO CIVINO  
ILARIA COLAZZO, FRANCESCA DALLA VOLTA, LUCIANO MAINO  
ALESSIO MENEGHETTI, NADIR MURRU, FEDERICO PINTORE  
MARIA TOTA, GIOVANNI ZINI**



# Collectio CiphRARum N °1