Foreword

Edgar Martínez-Moro · Josep M. Miret ·
Luis Ramiro Piñeiro

Published online: 26 July 2018
© Springer Nature Switzerland AG 2018

This volume includes survey papers, as well as new contributions, related with the courses of the CIMPA Research School “Mathematical models for security applications” held in Havana, Cuba, from August 29th to September 9th 2016. The School was dedicated to the memory of Emeritus Professor Mirka Miller who suggested that it be held in Havana and who made important contributions to many of the topics which were discussed.

The School was a meeting point for researchers from several Universities in Central America and Europe, who are working in Coding Theory, Cryptography and other security-related applications of Mathematics. Its goal was to introduce the participants to selected topics of Mathematics with direct applications in privacy and security issues, giving motivating examples and open problems.

The papers selected are gathered into three categories. (i) *Security of statistical databases*. Nowadays personal records are usually kept in a computerised database. The security of statistical database problem is to allow researchers to obtain as many statistics based on subpopulations of the database without compromising any particular record. Possible uses of combinatorics of finite sets and other mathematical tools to deal with security problems are examined. (ii) *Discrete logarithm cryptography*. The use of digital technologies in the daily tasks has changed our habits in the so-called e-society. Nevertheless, the introduction of these technologies requires ensuring privacy and security of digital devices and services. Subsequently, public key cryptosystems based on discrete logarithm problem have increased, especially elliptic curve cryptosystems since they guarantee the same security with smaller key lengths. Some aspects to consider in order to obtain cryptographically good elliptic curves or to achieve efficient implementations of index-calculus algorithms are presented. (iii) *Codes and cryptographic tools*. Error-correcting codes are used to achieve a reliable transmission of information through noisy channels. Some of their most recent leading topics are pointed out. Boolean functions, which have connections to cryptography and coding theory, are also considered and recent progress in their construction by algebraic means are reported.

We would like to thank the members of the Organizing and Scientific Committees for all their tasks and support: Valentina Badia, Edy T. Baskoro, Josep Domingo-Ferrer, Jorge Estrada, Pablo Freyre, Carlos M. Legón and Hebert

E. Martínez-Moro
Univ. Valladolid, Valladolid, Spain

J. M. Miret (✉)
Univ. Lleida, Lleida, Spain
e-mail: miret@matematica.udl.cat

L. R. Piñeiro
Univ. La Habana, Havana, Cuba

Pérez-Rosés. We also appreciate the assistance in evaluating the quality of submitted papers provided by additional referees.

We would also like to thank the International Center for Pure and Applied Mathematics (CIMPA) for the support provided, especially to Jeanick Allanic, Claude Cibils and Christian Mauduit for all their help. Thanks as well to the Cuban Society of Mathematics and Computer Science and the Mathematics Department at University of Lleida, Spain, for collaborating in the financial support. And many thanks to the Mathematics Faculty at the Universidad de La Habana, Cuba, for the hospitality and the welcoming atmosphere they created.

Finally, we are very grateful to all the lecturers for the courses and talks given, which were very interesting and attractive to both graduate students and researchers, providing them with an appropriate background on these topics and stimulating further research. And thanks to all the participants for attending the CIMPA School and learning new techniques and methods with enthusiasm, allowing us to share a enjoyable stay in Havana strengthening our collaborations.

List of participants

- Pedro Enrique Albalade, Universidad de La Habana, Cuba
- Valentina Badía, Universidad de La Habana, Cuba
- Adrian Balmore Valencia, Mercantil Banco Universal, Venezuela
- Antonio Bolufé Röhler, Universidad de La Habana, Cuba
- Mijaíl Borges Quintana, Universidad de Oriente, Cuba
- Ernesto A. Borrego Rodríguez Universidad de La Habana, Cuba
- Gustavo Andrés Cabaña, Inst. de Matemática Aplicada del Litoral (IMAL), Argentina
- Daniel Idelfonso Cervantes, CINVESTAV-IPN, México México
- Yakeline Chávez, MININT, Cuba
- Joan-Josep Climent, Universitat d'Alacant, Spain
- Reynier Antonio de la Cruz, Universidad de La Habana, Cuba
- Ernesto Domínguez Fiallo, Universidad de La Habana, Cuba
- Dayme Almeida Echevarria, Universidad de La Habana, Cuba
- Pablo Freyre Arozarena, Universidad de La Habana, Cuba
- Javier Hernán García, Universidad de los Andes, Colombia
- Ricard Garra, Universitat de Lleida, Spain
- Felipe González Casabianca Universidad de los Andes Colombia
- Alexei González Dopico, Universidad de La Habana, Cuba
- Carlos M. Legón Pérez, Universidad de La Habana, Cuba
- Evaristo José Madarro, Universidad Central de Las Villas, Cuba
- Ismel Martínez, Universidad de La Habana, Cuba
- Edgar Martínez-Moro, Universidad de Valladolid, Spain
- Ariadna Miranda, MININT, Cuba
- Josep M. Miret, Univ. Lleida, Spain
- Gabriella Akemi Miyamoto, State University of Campinas, Brazil
- Horacio Navarro, Inst. de Matemática Aplicada del Litoral (IMAL), Argentina
- José Eduardo Ochoa, Inst. Politecnico Nacional, México
- José Ángel Ornella, Universidad de Oriente, Cuba
- Adrián Alfonso Peñate, Universidad de La Habana, Cuba
- Hebert Pérez Rosés, Universitat de Lleida, Spain
- Luis Ramiro Piñero, Universidad de La Habana, Cuba
- Emily Carolina Piñero, Experian Soluciones V, Venezuela
- Francisco Rodríguez-Henríquez, CINVESTAV, México
- Joe Ryan, University of Newcastle, Australia
- Julián Salas, Universitat Rovira i Virgili, Spain
- Rubén Sánchez Acosta, Universidad de La Habana, Cuba
- José de Jesús Serrano, Inst. Politécnico Nacional, México
- Anier Soria Lorente, Universidad de Granma, Cuba
- Dania Tamayo, Universidad de La Habana, Cuba
- Gustavo Torres, Universidad de Oriente, Cuba

Fig. 1 At Alma Mater, Universidad de La Habana

Fig. 2 At Mathematics Faculty, Universidad de La Habana