Editorial

María Isabel González Vasco[1] and Gretchen L. Matthews[2]

[1]Departmento de Matemáticas, Universidad Carlos III de Madrid, Spain
[2]Department of Mathematics, Virginia Tech, U.S.A.

MathCrypt 2023 is the fifth in a workshop series started in 2018 with the ambition of becoming a regular annual venue for mathematicians to exchange ideas and present new results on different aspects of mathematical cryptography. Created as a discussion and dissemination forum for mathematicians working in cryptography, Mathcrypt was held in 2018, 2019, 2021, and 2022. This year's edition was held on August 19th, 2023, in Santa Barbara, California, immediately before Crypto 2023.

While mathematicians are used to sharing results informally at conferences and publishing final versions in journals, cryptography follows the computer science tradition of having peer-reviewed conference proceedings as the primary means of dissemination. This difference in publication dynamics is a significant obstacle for those working in mathematical cryptography, as partial results related to the hardness of mathematical assumptions used in cryptography or new ideas for the use of different mathematical tools in this field may not find their place in a traditional cryptographic venue. In contrast, MathCrypt welcomes research introducing new assumptions that can be used to construct or improve cryptographic schemes, proposing new attacks on cryptographic assumptions (even if they are not currently viable but have future promise), as well as implementation improvements for cryptographic schemes and attacks.

In this volume of *Mathematical Cryptology*, the works presented as full papers in the fifth edition of MathCrypt are collected. For this year's edition, we had the privilege to serve along with many distinguished colleagues on the organizing committee, which worked hard to put together an inspiring program: Jung Hee Cheon (Seoul National University), Vanesa Daza (Universitat Pompeu Fabra), Mingjie Chen (University of Birmingham), Philippe Gaborit (Université de Limoges), Nicolas Gama (Université de Versailles), David Jao (University of Waterloo), Jason LeGrow (Virginia Tech), Travis Morrison (Virginia Tech), Ludovic Perret (Sorbonne), Edoardo Persichetti (Florida Atlantic University), Angela Robinson (NIST), Rainer Steinwandt (University of Alabama at Huntsville) and Mehdi Tibouchi (École Normale Superieure). After a peer-review process, five papers were accepted as full contributions, which comprise this volume. In addition, six short contributions were accepted for presentation at the workshop.

We are grateful to everyone who made MathCrypt 2023 possible: the authors, presenters, chairs, and all the researchers who submitted their work. Special thanks to the Crypto 2023 organization team for supporting MathCrypt as an affiliated event. We look forward to many more editions of MathCrypt to come with new, exciting results and ideas.

María Isabel González Vasco
Gretchen L. Matthews