Editorial

Katherine E. Stange[1] and Rainer Steinwandt[2]

[1]Department of Mathematics, University of Colorado Boulder, U.S.A.
[2]Department of Mathematical Sciences, University of Alabama in Huntsville, U.S.A.

The MathCrypt Workshop series was conceived in 2017 in order to encourage more mathematicians and computational number theorists to propose and work on hard problems in cryptography. This *Mathematical Cryptology* volume accompanies the fourth edition of the workshop, held on August 14th, 2022 in Santa Barbara, California, right before Crypto 2022. Previous editions were held in 2018, 2019, and 2021.

MathCrypt addresses a gap in the publishing culture between mathematics and computer science. Whereas mathematicians recognize peer-reviewed journal publications as the standard, computer scientists often publish in peer-reviewed conference proceedings as their premier venue. The latter involves an accelerated calendar marked by submission deadlines, conference presentations, and proceedings volumes, to which mathematicians are less accustomed. The aim of MathCrypt was to create a regular annual venue for mathematicians to contribute to and collaborate with the cryptographic research community in the computer science model, but with the valued partnership of a peer-reviewed journal for publishing.

Mathematical cryptography is at a crucial juncture, as we search for and vet possible replacements for our current hardness assumptions and cryptographic systems that are impacted by efficient quantum algorithms. Mathematical cryptanalysis is fundamental for refining and establishing trust in new constructions, but it is a high-risk endeavor. Partial results can be difficult to find a venue for, but are crucial to our understanding of the hardness of underlying assumptions. Even certain failed attacks can provide deep insight. Attacks on parameters outside proposed parameters can introduce new ideas that may lead to more complete breaks, or may illustrate, justify, and confirm the selected parameters. MathCrypt aims to provide a much-needed venue for these works, to encourage the vetting of new cryptographic assumptions.

MathCrypt also welcomes the proposal of new cryptographic schemes and new ideas for hard cryptographic problems. The generation of new ideas for future cryptography is essential, and yet this research may be challenging to publish in a traditional venue—evaluating and refining a new cryptographic system may take much longer than a single review cycle of a few short weeks: its true value may only be revealed through a trail of follow-up work.

For this year's edition, we had the privilege to serve along with a number of distinguished colleagues on the organzing committee, and we are grateful they made this year's MathCrypt possible: Jung Hee Cheon (Seoul National University), Nicolas Gama (Université de Versailles), David Jao (University of Waterloo), Kristin Lauter (FAIR Labs North America at Meta), Travis Morrison (Virginia Tech), Edoardo Persichetti (Florida Atlantic University), and Mehdi Tibouchi (École Normale Superieure). After a peer-review process, six papers were accepted and presented in a one-day workshop preceeding Crypto 2022, along with one short paper. The final versions of the full papers comprise this issue.

We are grateful to the authors, presenters, and all submitters to MathCrypt 2022. A special thank you goes to the other members of the organizing committee who worked hard on evaluating submissions and putting together a final program full of exciting results. Thank you to the organizing team of Crypto 2022, who supported MathCrypt as an affiliated event, and provided all necessary infrastructure to run this workshop smoothly as a successful hybrid event. We appreciate everyone who joined us in Santa Barbara or online, and we look forward to many future years of MathCrypt.

Katherine E. Stange
Rainer Steinwandt