NUMBER-THEORETIC METHODS IN CRYPTOLOGY
BANACH CENTER PUBLICATIONS, VOLUME 126
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2023

PREFACE

This volume contains a collection of papers presented at the NuTMiC 21 conference. The conference was held at Adam Mickiewicz University, Poznań, Poland in August 2022. Note that the event was postponed by a year due to the covid pandemic. It was the third edition of the series of conferences whose theme is the Number-Theoretic Methods in Cryptology. The first edition was held at the University of Warsaw in September 2017 and the second edition was held at the Paris-Sorbonne University in June 2019.

Besides the well-established connections between number theory and cryptology, such as primality testing, factorisation, elliptic curves and lattices, the conference endeavoured to forge new ones that would benefit both fields. The main goal of the conference was to gather researchers working in all areas of number theory and cryptology as well as in the intersection of the two fields. The conference was an excellent avenue for the presentation of new research results and ideas. The presentations have covered a wide range of topics, including: EC based cryptographic algorithms, encryption schemes, lattice based and isogeny based algorithms and digital signatures, reductions between various computational problems, computational approaches to the Riemann hypothesis and high rank elliptic curves. Investigation of deep mathematical ideas and their application to cryptology has a great potential to improve both the efficiency and security of cryptographic algorithms and protocols.

The proceedings include eight peer-reviewed papers and three invited talks, which were not refereed. The papers cover the following topics: elliptic curve L-functions with applications to encryption and oracle factoring algorithms, isogeny based and Pell cubics based cryptosystems, lattice and isogeny based algorithms, efficient constructions of supersingular elliptic curves and isogeny based cryptography, computational approach to the Riemann hypothesis, high rank elliptic curves with given torsion group, oracle factoring with the aid of elliptic/hyperelliptic curves and the malleability of factorization problem.

We wish to thank the Program Committee members and the reviewers for their time and effort. We also thank the local organisers who made the conference a success. We express our deep appreciation to the authors for their contributions. Last but not least, we highly appreciate the support the conference received from the Faculty of Mathematics and Informatics of Adam Mickiewicz University in Poznań, and from Banach Center, Institute of Mathematics, PAS for publishing the conference proceedings.

October, 2023 *Maciej Grześkowiak, Josef Pieprzyk and Jacek Pomykała*