

## Preface

These are the proceedings of WAIFI 2016, the 6th International Workshop on the Arithmetic of Finite Fields, held in Ghent, Belgium, during July 13–15, 2016. The five previous editions of this workshop were held in Madrid, Spain (WAIFI 2007), Siena, Italy (WAIFI 2008), Istanbul, Turkey (WAIFI 2010), Bochum, Germany (WAIFI 2012), and Gebze, Turkey (WAIFI 2014). Springer has published all previous volumes of the WAIFI proceedings in the LNCS series.

Since 2008, WAIFI has been held every even year, bringing together mathematicians, computer scientists, engineers, and physicists who conduct research in different areas of finite field arithmetic.

The program consisted of three invited talks and 17 contributed papers. The invited speakers were Swastik Kopparty (Rutgers University, USA), Simeon Ball (Universitat Politècnica de Catalunya, Spain) and Razvan Barbulescu (CNRS, Paris 6 and 7, France). The papers supporting the two last invited talks were also included in the proceedings. The contributed talks were selected from 38 submissions, each of which was assigned to at least three committee members or external reviewers chosen by the members. Additionally, the Program Committee had a significant online discussion phase for several days. Three additional presentations were made during the workshop but are not part of these proceedings.

We are very grateful to the members of the Program Committee for their dedication, professionalism, and careful work with the review and selection process. We also sincerely thank the external reviewers who contributed with their special expertise to review papers for this workshop.

We deeply thank the general co-chairs, Vincent Rijmen and Leo Storme, for their support of the Program Committee and their hard work in leading the overall organization of the workshop helped by the Organizing Committee. We would also like to sincerely thank members of the Steering Committee of the workshop series for their constant support and encouragement in our efforts to create a stimulating scientific program leading to this volume. Furthermore, we thank Jean-Jacques Quisquater for his valuable help in publicity and we are also very grateful to José Luis Imaña and Jan de Beule for diligently maintaining the workshop website. As with the previous volumes, Springer agreed to publish the revised and expanded versions of the WAIFI 2016 papers as an LNCS volume. We thank Alfred Hoffman and Anna Kramer from Springer for making this possible.

The submission and selection of papers were done using the EasyChair conference management system. Hence, thank you EasyChair! We would also like to acknowledge the Foundation Compositio Mathematica and FWO for being sponsors of the workshop.

Finally, but most importantly, we deeply thank all the authors who submitted their papers to the workshop and the participants all over the world who chose to honor us with their attendance.

February 2017

Sylvain Duquesne  
Svetla Petkova-Nikova

Arithmetic of Finite Fields

6th International Workshop, WAIFI 2016, Ghent,  
Belgium, July 13-15, 2016, Revised Selected Papers  
duquesne, S.; Nikova, S. (Eds.)

2016, XII, 277 p. 12 illus., Softcover

ISBN: 978-3-319-55226-2