Lecture Notes in Computer Science 11321

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

More information about this series at http://www.springer.com/series/7407

Lilya Budaghyan
Francisco Rodríguez-Henríquez (Eds.)

Arithmetic of Finite Fields

7th International Workshop, WAIFI 2018
Bergen, Norway, June 14–16, 2018
Revised Selected Papers

Springer

Editors
Lilya Budaghyan
Department of Informatics
University of Bergen
Bergen, Norway

Francisco Rodríguez-Henríquez
Centro de Investigación y de Estudios
Avanzados del Instituto Politécnico
Nacional
Mexico, Mexico

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-05152-5 ISBN 978-3-030-05153-2 (eBook)
https://doi.org/10.1007/978-3-030-05153-2

Library of Congress Control Number: 2018962540

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

These are the proceedings of WAIFI 2018, the 7th International Workshop on the Arithmetic of Finite Fields, held in Bergen, Norway, during June 14–16, 2016. The six previous editions of this workshop were held in Madrid, Spain (WAIFI 2007), Siena, Italy (WAIFI 2008), Istanbul, Turkey (WAIFI 2010), Bochum, Germany (WAIFI 2012), Gebze, Turkey (WAIFI 2014), and Ghent, Belgium (WAIFI 2016). 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 six invited talks and 14 contributed papers. The invited speakers were Simon Blackburn (Royal Holloway University of London, UK), Anwar Hasan (University of Waterloo, Canada), Daniel Panario (Carleton University, Canada), Daniel Katz (California State University, USA), Ferruh Özbudak (Middle East Technical University, Turkey), and Benjamin Smith (Inria, France). The papers supporting the three last invited talks were also included in the proceedings. The contributed talks were selected from 26 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. Two of the papers were selected for the best paper award: "On Symmetry and Differential Properties of Generalized Boolean Functions" by Thor Martinsen, Wilfried Medil, Alexander Pott, Pantelimon Stanica, and "A New Family of Pairing-Friendly Elliptic Curves" by Michael Scott and Aurore Guillevic.

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, Lilya Budaghyan and Tor Helleseth, 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 are very grateful to José Luis Imaña for his valuable help in publicity and 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 from Springer for making this possible. We would like to acknowledge that the submission and selection of papers were done using the EasyChair conference management system. We would also like to thank Bergen Research Foundation for sponsoring the workshop. Finally, but most importantly, we deeply thank all the authors who submitted their papers to the workshop and the participants from all over the world who chose to honor us with their attendance.

June 2018

Lilya Budaghyan
Francisco Rodríguez-Henríquez

Organization

International Workshop on the Arithmetic of Finite Fields

Bergen, Norway
June 14–16, 2018

Organized by
University of Bergen

Steering Committee

Claude Carlet	University of Paris 8, France
Anwar Hasan	University of Waterloo, Canada
José Luis Imaña	Complutense University of Madrid, Spain
Çetin Kaya Koç	University of California Santa Barbara, USA
Sihem Mesnager	University of Paris 8, France
Ferruh Özbudak	Middle East Technical University, Turkey
Christof Paar	Ruhr-Universität Bochum, Germany
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Erkay Savas	Sabanci University, Turkey
Berk Sunar	Worcester Polytechnic Institute, USA
Gustavo Sutter	Autonomous University of Madrid, Spain

General Chairs

Lilya Budaghyan	University of Bergen, Norway
Tor Helleseth	University of Bergen, Norway

Program Chairs

Lilya Budaghyan	University of Bergen, Norway
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, México

Program Committee

Diego F. Aranha	University of Campinas, Brazil
Daniel Augot	Inria, France
Angela Barbero	University of Valladolid, Spain
Marco Calderini	University of Bergen, Norway
Claude Carlet	University of Paris 8, France
Craig Costello	Microsoft Research, USA

Robert Coulter	University of Delaware, USA
Luca De Feo	Université Paris Saclay, UVSQ and Inria, France
Cunsheng Ding	Hong Kong University of Science and Technology, SAR China
Huseyin Hisil	Yasar University, Turkey
Koray Karabina	Florida Atlantic University, USA
Alla Levina	ITMO University, Russia
Chunlei Li	University of Bergen, Norway
Nian Li	Hubei University, China
Oleg Logachev	Moscow State University, Russia
Florian Luca	Wits University, South Africa
Matthew Parker	University of Bergen, Norway
Léo Perrin	Inria, France
Arash Reyhani-Masoleh	Western University, Canada
Igor Semaev	University of Bergen, Norway
Max Sala	University of Trento, Italy
Erkay Savas	Sabanci University, Turkey
Patrick Solé	Télécom ParisTech, France
Natalia Tokareva	Novosibirsk State University, Russia
Øyvind Ytrehus	Simula, Norway

Additional Reviewers

Daniele Bartoli	University of Perugia, Italy
Massimo Giulietti	University of Perugia, Italy
Bernhard Heim	German University of Technology, Oman
Brandon Langenberg	PQSecure Technologies, USA
Michael Naehrig	Microsoft Research, USA
Erdinc Ozturk	Sabanci University, Turkey
Federico Pintore	University of Oxford, UK
Joost Renes	University of Nijmegen, The Netherlands
Éric Schost	University of Waterloo, Canada
Deng Tang	Southwest Jiaotong University, China
Frederik Vercauteren	Katholieke Universiteit Leuven, Belgium
Vanessa Vitse	Université de Grenoble I, France
Arne Winterhof	Österreichische Akademie der Wissenschaften, Austria

Organizing Committee

Marco Calderini	University of Bergen, Norway
Nikolay Kaleyski	University of Bergen, Norway
Chunlei Li	University of Bergen, Norway

Sponsoring Institutions

Bergen Research Foundation

Contents

Invited Talk 1

Pre- and Post-quantum Diffie–Hellman from Groups, Actions, and Isogenies 3
Benjamin Smith

Elliptic Curves

A New Family of Pairing-Friendly Elliptic Curves 43
Michael Scott and Aurore Guillevic

Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields 58
Momonari Kudo and Shushi Harashita

Fast Computation of Isomorphisms Between Finite Fields Using Elliptic Curves 74
Anand Kumar Narayanan

Invited Talk 2

Construction of Some Codes Suitable for Both Side Channel and Fault Injection Attacks 95
Claude Carlet, Cem Güneri, Sihem Mesnager, and Ferruh Özbudak

Hardware Implementations

On Hardware Implementation of Tang-Maitra Boolean Functions 111
Mustafa Khairallah, Anupam Chattopadhyay, Bimal Mandal, and Subhamoy Maitra

Rapid Hardware Design for Cryptographic Modules with Filtering Structures over Small Finite Fields 128
Nusa Zidaric, Mark Aagaard, and Guang Gong

Invited Talk 3

Sequences with Low Correlation 149
Daniel J. Katz

Arithmetic and Applications of Finite Fields

Vector-Valued Modular Forms on Finite Upper Half Planes 175
Yoshinori Hamahata

Normal Basis Exhaustive Search: 10 Years Later 188
L. Moura, D. Panario, and D. Thomson

On Symmetry and Differential Properties of Generalized Boolean Functions. 207
Thor Martinsen, Wilfried Meidl, Alexander Pott, and Pantelimon Stănică

Characterizations of Partially Bent and Plateaued Functions over Finite Fields 224
Sihem Mesnager, Ferruh Özbudak, and Ahmet Sınak

Codes of Length Two Correcting Single Errors of Limited Size II. 242
Torleiv Kløve

Fractional Jumps: Complete Characterisation and an Explicit Infinite Family 250
Federico Amadio Guidi and Giacomo Micheli

Some Sextics of Genera Five and Seven Attaining the Serre Bound 264
Motoko Qiu Kawakita

Cryptography

Direct Constructions of (Involutory) MDS Matrices from Block Vandermonde and Cauchy-Like Matrices 275
Qiuping Li, Baofeng Wu, and Zhuojun Liu

Exploiting Preprocessing for Quantum Search to Break Parameters for $\mathcal{MQ}$ Cryptosystems 291
Benjamin Pring

Author Index 309