Lecture Notes in Computer Science **9061**

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

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

Çetin Kaya Koç · Sihem Mesnager
Erkay Savaş (Eds.)

Arithmetic of Finite Fields

5th International Workshop, WAIFI 2014
Gebze, Turkey, September 27−28, 2014
Revised Selected Papers

Springer

Editors
Çetin Kaya Koç
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA
USA

Erkay Savaş
Sabancı University
Istanbul
Turkey

Sihem Mesnager
University of Paris VIII
Paris
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-16276-8 ISBN 978-3-319-16277-5 (eBook)
DOI 10.1007/978-3-319-16277-5

Library of Congress Control Number: 2015932669

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the revised and expanded versions of the papers presented at the 5th International Workshop on the Arithmetic of Finite Fields (WAIFI). The workshop was held in Gebze, Turkey, during September 27–28, 2014.

The final program contained three invited and nine contributed papers, which are all found in this volume. The contributed papers were selected from 17 submissions using a careful refereeing process. At least three and in most cases four referees reviewed each paper. The final decisions were taken only after a clear position could be clarified through additional reviews and comments.

We are very grateful and express our thanks to the Program Committee Chairs, the Program Committee Members, and also to the external reviewers for their great work of reviewing. Their help and cooperation was essential, especially due to the short amount of time available to conduct the reviewing task.

The Program Committee invited Claude Carlet, Ferruh Özbudak, and Francisco Rodríguez-Henríquez to speak on topics of their choice, as related to the WAIFI 2014. We thank them for having accepted. Their contributions provided a valuable framing for the contributed papers.

The Steering Committee also thanks the General Chair, Çetin Kaya Koç, and the Program Co-chairs, Sihem Mesnager and Erkay Savaş for the rigorous work. Furthermore, the Committee thanks Jean-Jacques Quisquater and José Luis Imaña for their valuable help in publicity and web page matters.

Springer has published all previous volumes of the WAIFI Proceedings:

- Ferruh Özbudak and Francisco Rodríguez-Henríquez (Eds.): Arithmetic of Finite Fields, 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16–19, 2012. Springer, LNCS Volume 7369.
- M. Anwar Hasan and Tor Helleseth (Eds.): Arithmetic of Finite Fields, 3rd International Workshop, WAIFI 2010, Istanbul, Turkey, June 27–30, 2010. Springer, LNCS Volume 6087.
- Joachim von zur Gathen, José Luis Imaña, and Çetin Kaya Koç (Eds.): Arithmetic of Finite Fields, 2nd International Workshop, WAIFI 2008, Siena, Italy, July 6–9, 2008. Springer, LNCS Volume 5130.
- Claude Carlet and Berk Sunar (Eds.): Arithmetic of Finite Fields, 1st International Workshop, WAIFI 2007, Madrid, Spain, June 21–22, 2007. Springer, LNCS Volume 4547.

As with the previous volumes, Springer agreed to publish the revised and expanded versions of the WAIFI 2014 papers as an LNCS volume. We thank Alfred Hoffman and Ronan Nugent from Springer for making this possible.

September 2014

Çetin Kaya Koç
Sihem Mesnager
Erkay Savaş

Organization

Committees

Steering Committee

Claude Carlet	University of Paris VIII, France
Jean-Pierre Deschamps	Rovira i Virgili University, Spain
José Luis Imaña	Complutense University of Madrid, Spain
Çetin Kaya Koç	University of California, Santa Barbara, USA
Ferruh Özbudak	Middle East Technical University, Turkey
Christof Paar	Ruhr University Bochum, Germany
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Berk Sunar	Worcester Polytechnic Institute, USA
Gustavo Sutter	Autonomous University of Madrid, Spain

General Chair

Çetin Kaya Koç	University of California, Santa Barbara, USA

Program Chairs

Sihem Mesnager	University of Paris VIII, France
Erkay Savaş	Sabancı University, Turkey

Publicity Chair

Jean-Jacques Quisquater	Université catholique de Louvain, Belgium

Local Arrangements Chairs

Şükran Külekçi	Tübitak BİLGEM, Turkey
Mehmet Sabır Kiraz	Tübitak BİLGEM, Turkey

Program Committee

Daniel Augot	Inria and LIX, France
Lejla Batina	Radboud University Nijmegen, The Netherlands
Luca Breveglieri	Politecnico di Milano, Italy
Claude Carlet	University of Paris VIII, France
Murat Cenk	Middle East Technical University, Turkey
Gérard Cohen	Télécom ParisTech, France
Philippe Gaborit	University of Limoges, France
Pierrick Gaudry	CNRS, Nancy, France
Tor Helleseth	University of Bergen, Norway

Hüseyin Hışıl	Yaşar University, Turkey
Mehran Mozaffari Kermani	Rochester Institute of Technology, USA
Alexander Kholosha	University of Bergen, Norway
Gregor Leander	Ruhr University Bochum, Germany
Julio López	University of Campinas, Brazil
Wilfried Meidl	Sabancı University, Turkey
Sihem Mesnager	University of Paris VIII, France
Christophe Negre	Université de Perpignan, France
Harald Niederreiter	RICAM, Austrian Academy of Sciences, Austria
Erdinç Öztürk	Istanbul Commerce University, Turkey
Alexander Pott	Otto-von-Guericke University, Germany
Arash Reyhani-Masoleh	University of Western Ontario, Canada
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Erkay Savaş	Sabancı University, Turkey
Zülfükar Saygı	TOBB Ekonomi ve Teknoloji Üniversitesi, Turkey
Kai-Uwe Schmidt	Otto-von-Guericke University, Germany
Leo Storme	Ghent University, Belgium
Jean-Pierre Tillich	Inria-Rocquencourt, France

Additional Reviewers

Çetin Kaya Koç	University of California, Santa Barbara, USA
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium

Contents

Third Invited Talk

Coding Theory and Code-Based Cryptography