

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Ferruh Özbudak  
Francisco Rodríguez-Henríquez (Eds.)

# Arithmetic of Finite Fields

4th International Workshop, WAIFI 2012  
Bochum, Germany, July 16-19, 2012  
Proceedings

## Volume Editors

Ferruh Özbudak  
Middle East Technical University  
Institute of Applied Mathematics  
Ankara, Turkey  
E-mail: ozbudak@metu.edu.tr

Francisco Rodríguez-Henríquez  
Centro de Investigación y de Estudios  
Avanzados del Instituto Politécnico Nacional (CINVESTAV-IPN)  
Departamento de Computación  
Av. IPN No. 2508, Col. San Pedro Zacatenco, Mexico, D.F. 07360, Mexico  
E-mail: francisco@cs.cinvestav.mx

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-31661-6 e-ISBN 978-3-642-31662-3  
DOI 10.1007/978-3-642-31662-3  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012940985

CR Subject Classification (1998): I.1, G.2, E.3, K.6.5, D.4.6, F.2.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

These are the proceedings of WAIFI 2012, the 4th International Workshop on the Arithmetic of Finite Fields, held in Bochum, Germany, during July 16–19, 2012. The three previous editions of this workshop were held in Madrid, Spain (WAIFI 2007), Siena, Italy (WAIFI 2008), and Istanbul, Turkey (WAIFI 2010). 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. WAIFI 2012 was organized by the Ruhr-Universität Bochum, Germany, in cooperation with the International Association for Cryptologic Research (IACR). The General Chair of the conference was Christopher Wolf.

The program consisted of four invited talks and 13 contributed papers. The invited speakers were Shay Gueron (University of Haifa, Israel), Florian Hess (Universität Oldenburg, Germany), Alexander Pott (Universität Magdeburg, Germany), and Emmanuel Thome (INRIA, France). The papers supporting the four invited talks were also included in the proceedings. The contributed talks were selected from 29 submissions each of which was assigned to at least three committee members. Additionally, the Program Committee had a significant online discussion phase for several days.

We are very grateful to the Program Committee members and to the external reviewers for their dedication and professionalism. Special thanks go out to Christopher Wolf, the General Chair, for his hard work in leading the overall organization and dealing with various local arrangements with meticulous care. We would also like to thank Jean-Jacques Quisquater and Çetin Kaya Koç, who helped us to negotiate the publication of WAIFI 2012 proceedings as a volume of *Lecture Notes in Computer Science*. We are also very grateful to José Luis Imaña for diligently maintaining the workshop website. We heartily thank the members of the Steering Committee of the workshop series for their constant support and encouragement.

The submission and selection of papers were done using the EasyChair conference management system. Hence, thank you EasyChair! 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.

July 2012

Ferruh Özbudak  
Francisco Rodríguez-Henríquez

# WAIFI 2012

International Workshop on the Arithmetic of Finite Fields

Bochum, Germany

July 16–19, 2012

*Organized by*

Ruhr-Universität Bochum

*In cooperation with*

The International Association for Cryptologic Research (IACR)

## Steering Committee

Claude Carlet	University of Paris 8, France
Jean-Pierre Deschamps	University Rovira i Virgili, Spain
José Luis Imaña	Complutense University of Madrid, Spain
Çetin Kaya Koç	University of California Santa Barbara, USA
Christof Paar	Ruhr-Universität Bochum, Germany
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Berk Sunar	Worcester Polytechnic Institute, USA
Gustavo Sutter	Autonomous University of Madrid, Spain

## General Chair

Christopher Wolf	Ruhr-Universität Bochum, Germany
------------------	----------------------------------

## Program Chairs

Ferruh Özbudak	Middle East Technical University, Turkey
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, México

## Local Organizing Committee

Marina Efimenko	Ruhr-Universität Bochum, Germany
Sebastian Uellenbeck	Ruhr-Universität Bochum, Germany
Christian Walter	Ruhr-Universität Bochum, Germany

## Program Committee

Jean-Claude Bajard	LIP6 CNRS/Université Pierre et Marie Curie, France
Stephane Ballet	Institut de Mathématiques de Luminy, France
Jean-Luc Beuchat	University of Tsukuba, Japan
Luca Breveglieri	Politecnico di Milano, Italy
Debrup Chakraborty	CINVESTAV-IPN, Mexico
Ricardo Dahab	University of Campinas, Brazil
Jérémie Detrey	INRIA, France
Haining Fan	Tsinghua University, China
Olav Geil	Aalborg University, Denmark
Guang Gong	University of Waterloo, Canada
Jorge Guajardo	Robert Bosch LLC, USA
Anwar Hasan	University of Waterloo, Canada
Tor Helleseth	University of Bergen, Norway
José L. Imaña	Complutense University of Madrid, Spain
Koray Karabina	University of Waterloo, Canada
Alexander Kholosha	University of Bergen, Norway
Tanja Lange	Technical University of Eindhoven, The Netherlands
Ivan Landjev	Bulgarian Academy of Sciences, Bulgaria
Julio López	University of Campinas, Brazil
Edgar Martínez-Moro	University of Valladolid, Spain
Gary Mullen	Pennsylvania State University, USA
Harald Niederreiter	Austrian Academy of Sciences, Austria
Arash Reyhani-Masoleh	University of Western Ontario, Canada
Erkay Savaş	Sabancı University, Turkey
Peter Schwabe	Academia Sinica, Taiwan
Igor Semaev	University of Bergen, Norway
Patrick Solé	Télécom ParisTech, France and AbdelAziz University, Saudi Arabia
Arne Winterhof	Austrian Academy of Sciences, Austria

## External Reviewers

Diego Aranha	Stéphane Louboutin
Jean-Philippe Aumasson	Cuauhtemoc Mancillas-López
Selçuk Baktır	Marc Mouffron
Razvan Barbulescu	Mehran Mozaffari-Kermani
Daniel Bernstein	Christophe Negre
Alessandro Barengi	Matthew Parker
Qi Chai	Gerardo Pelosi
Fernando Hernando	Christiane Peters
Hans Hüttl	Thomas Plantard

Damien Robert  
Robert Rolland  
Sumanta Sarkar

Reza Sohizadeh  
Zilong Wang  
Yang Yang

## **Sponsoring Institutions**

Ruhr-Universität Bochum, Germany  
Mercator Foundation, Essen, Germany

# Table of Contents

## Invited Talk 1

Generalised Jacobians in Cryptography and Coding Theory . . . . .	1
<i>Florian Hess</i>	

## Coding Theory and Code-Based Cryptography

The Weight Distribution of a Family of Reducible Cyclic Codes . . . . .	16
<i>Gerardo Vega and Carlos A. Vázquez</i>	
A New Method for Constructing Small-Bias Spaces from Hermitian Codes . . . . .	29
<i>Olav Geil, Stefano Martin, and Ryutaroh Matsumoto</i>	
An Improved Threshold Ring Signature Scheme Based on Error Correcting Codes . . . . .	45
<i>Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Gerhard Hoffmann, and Pascal Véron</i>	

## Invited Talk 2

Sequences and Functions Derived from Projective Planes and Their Difference Sets . . . . .	64
<i>Alexander Pott, Qi Wang, and Yue Zhou</i>	

## Boolean Functions

On Formally Self-dual Boolean Functions in 2, 4 and 6 Variables . . . . .	81
<i>Lin Sok and Patrick Solé</i>	
On the Algebraic Normal Form and Walsh Spectrum of Symmetric Functions over Finite Rings . . . . .	92
<i>Boris Batteux</i>	
Verification of Restricted EA-Equivalence for Vectorial Boolean Functions . . . . .	108
<i>Lilya Budaghyan and Oleksandr Kazymyrov</i>	



### Invited Talk 3

Software Implementation of Modular Exponentiation, Using Advanced Vector Instructions Architectures .....	119
<i>Shay Gueron and Vlad Krasnov</i>	

### Finite Field Arithmetic

Efficient Multiplication over Extension Fields .....	136
<i>Nadia El Mrabet and Nicolas Gama</i>	
$\text{GF}(2^m)$ Finite-Field Multipliers with Reduced Activity Variations .....	152
<i>Danuta Pamula and Arnaud Tisserand</i>	
Finding Optimal Formulae for Bilinear Maps .....	168
<i>Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals, and Paul Zimmermann</i>	

### Equations and Functions

Solving Binary Linear Equation Systems over the Rationals and Binaries .....	187
<i>Benedikt Driessen and Christof Paar</i>	
Hashing with Elliptic Curve $L$ -Functions .....	196
<i>Sami Omar, Raouf Ouni, and Saber Bouanani</i>	

### Invited Talk 4

Square Root Algorithms for the Number Field Sieve .....	208
<i>Emmanuel Thomé</i>	

### Polynomial Factorization and Permutation Polynomial

Improving the Berlekamp Algorithm for Binomials $x^n - a$ .....	225
<i>Ryuichi Harasawa, Yutaka Sueyoshi, and Aichi Kudo</i>	
On Some Permutation Binomials of the Form $x^{\frac{2^n-1}{k}+1} + ax$ over $\mathbb{F}_{2^n}$ : Existence and Count .....	236
<i>Sumanta Sarkar, Srimanta Bhattacharya, and Ayça Çeşmelioglu</i>	

Author Index .....	247
--------------------	-----