Lecture Notes in Computer Science 6087

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 of Computer Science, Saarbruecken, Germany

M. Anwar Hasan Tor Helleseth (Eds.)

Arithmetic of Finite Fields

Third International Workshop, WAIFI 2010
Istanbul, Turkey, June 27-30, 2010
Proceedings

Springer

Volume Editors

M. Anwar Hasan
University of Waterloo, Department of Electrical and Computer Engineering
Waterloo, Ontario N2L 3G1, Canada
E-mail: ahasan@uwaterloo.ca

Tor Helleseth
University of Bergen, Department of Informatics, HIB
PB 7803, 5020, Bergen, Norway
E-mail: tor.helleseth@ii.uib.no

Library of Congress Control Number: 2010928209

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

ISSN 0302-9743
ISBN-10 3-642-13796-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13796-9 Springer Berlin Heidelberg New York

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

These are the proceedings of WAIFI 2010, the Third International Workshop on the Arithmetic of Finite Fields, held in Istanbul, Turkey, during June 27-30, 2010. The first workshop, WAIFI 2007, was held in Madrid, Spain, and then WAIFI 2008 was held in Siena, Italy. In 2008, the workshop series was made biannual and it is now being held every even year, bringing together mathematicians, computer scientists, engineers and physicists who are doing research on various aspects of finite field arithmetic.

This year the workshop received 33 submissions, each of which was reviewed by at least three reviewers who were either members of the Program Committee of the workshop or external reviewers chosen by the members. Once the review phase was over, the Program Committee had online discussions over a period of several days. In the end, a total of 15 papers representing both theoretical and practical aspects of finite field arithmetic were accepted for presentation. These accepted papers are part of these proceedings. In addition to the presentations of these papers, we were fortunate to have three invited talks given by P. Vijay Kumar, Alfred Menezes and Henning Stichtenoth. The papers, which the invited talks were based on, are also part of the 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 General Co-chairs Çetin Kaya Koç and Ferruh Özbudak for their support of the Program Committee and their hard work in leading the overall organization of the workshop and holding it in the historic city of Istanbul– a joint European Capital of Culture for year 2010. We are also very grateful to José Luis Imaña for diligently maintaining the workshop website, and to Claude Carlet for making workshop announcements. Our very special thanks go to Murat Cenk, Gökay Saldamli and Zülfükar Saygi for dealing with various local arrangements with a lot of care.

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 the proceedings of WAIFI 2010. Special thanks go to Jean-Jacques Quisquater for making arrangements with Springer to publish the proceedings as a volume of *Lecture Notes in Computer Science*.

The process of paper submission, review and online discussion was carried out using the EasyChair conference management system, which we found to be very useful. The system was also used for dealing with final versions of the accepted and invited papers and towards the preparation of the proceedings. So, thank

you EasyChair! We would also like to acknowledge Istanbul Şehir University for being a sponsor of the workshop.

Finally, but most importantly, we deeply thank the authors from all over the world who submitted their papers to the workshop. It was their hard work and endeavor to advance the field of knowledge that made the workshop a stimulating forum. We also thank the participants of the workshop for making it a very successful event.

June 2010

M. Anwar Hasan
Tor Helleseth

Organization

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, & Istanbul Şehir University, Turkey
Christof Paar	Ruhr University of Bochum, Germany
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Berk Sunar	Worcester Polytechnic Institute, USA
Gustavo Sutter	Autonomous University of Madrid, Spain

Executive Committee

General Co-chairs

Çetin Kaya Koç	University of California Santa Barbara, USA, & Istanbul Şehir University, Turkey
Ferruh Özbudak	Middle East Technical University, Turkey

Program Co-chairs

M. Anwar Hasan	University of Waterloo, Canada
Tor Helleseth	University of Bergen, Norway

Financial, Local Arrangements Chairs

Murat Cenk	Middle East Technical University, Turkey
Gökay Saldamli	Boğaziçi University, Turkey
Zülfükar Saygi	TOBB ETU, Turkey

Publicity Chair

Claude Carlet	University of Paris 8, France

Program Committee

Daniel Augot	INRIA, France
Roberto Avanzi	Ruhr-University Bochum, Germany
Jean-Claude Bajard	LIP6 CNRS/Université Pierre et Marie Curie, France
Luca Breveglieri	Politecnico di Milano, Italy
Stephen Cohen	University of Glasgow, Scotland, UK

Cunsheng Ding	Hong Kong University of Science and Technology, China
Serdar Erdem	Gebze Institute of Technology, Turkey
Haining Fan	Tsinghua University, China
Olav Geil	Aalborg University, Denmark
Guang Gong	University of Waterloo, Canada
Jorge Guajardo	Philips Research, The Netherlands
Darrel Hankerson	Auburn University, USA
M. Anwar Hasan	University of Waterloo, Canada
Tor Helleseth	University of Bergen, Norway
José Luis Imaña	Complutense University of Madrid, Spain
Alexander Kholosha	University of Bergen, Norway
P. Vijay Kumar	Indian Institute of Science, Bangalore, India
Tanja Lange	Technical University of Eindhoven, The Netherlands
Julio López	UNICAMP, Brazil
Gary McGuire	University College Dublin, Ireland
Eiji Okamoto	University of Tsukuba, Japan
Alexander Pott	University of Magdeburg, Germany
Francisco Rodríguez-Henríquez	Cinvestav, Mexico
Erkay Savas	Sabanci University, Turkey
Igor Semaev	University of Bergen, Norway
Patrick Solé	Télécom ParisTech, France

External Reviewers

Selcuk Baktir
Daniel J. Bernstein
Jean-Luc Beuchat
Lilya Budaghyan
Stanislav Bulygin
Ricardo Dahab
Jean-Pierre Deschamps
Xinxin Fan
Fung-Wei Fu
Conrado Gouvêa
Honggang Hu
Yiyuan Luo
Subhamoy Maitra
Ryutaroh Matsumoto
Wilfried Meidl
Hiroyoshi Morita
Carlos Munuera
Harald Niederreiter
Gerardo Pelosi
Massimiliano Sala
Nazar Abbas Saqib
Sumanta Sarkar
Peter Schwabe
Arnaud Tisserand
Arne Winterhof
Bo-Yin Yang

Sponsoring Institution

Istanbul Şehir University, Turkey

Table of Contents

Invited Talk 1

Recursive Towers of Function Fields over Finite Fields 1
Henning Stichtenoth

Efficient Finite Field Arithmetic

High-Performance Modular Multiplication on the Cell Processor 7
Joppe W. Bos

A Modified Low Complexity Digit-Level Gaussian Normal Basis Multiplier 25
Reza Azarderakhsh and Arash Reyhani-Masoleh

Type-II Optimal Polynomial Bases 41
Daniel J. Bernstein and Tanja Lange

Pseudo-random Numbers and Sequences

Pseudorandom Vector Sequences Derived from Triangular Polynomial Systems with Constant Multipliers 62
Alina Ostafe

Structure of Pseudorandom Numbers Derived from Fermat Quotients . . . 73
Zhixiong Chen, Alina Ostafe, and Arne Winterhof

Boolean Functions

Distribution of Boolean Functions According to the Second-Order Nonlinearity 86
Stéphanie Dib

Hyper-bent Boolean Functions with Multiple Trace Terms 97
Sihem Mesnager

Invited Talk 2

On the Efficiency and Security of Pairing-Based Protocols in the Type 1 and Type 4 Settings 114
Sanjit Chatterjee, Darrel Hankerson, and Alfred Menezes

Functions, Equations and Modular Multiplication

Switching Construction of Planar Functions on Finite Fields 135
Alexander Pott and Yue Zhou

Solving Equation Systems by Agreeing and Learning 151
Thorsten Ernst Schilling and Håvard Raddum

Speeding Up Bipartite Modular Multiplication 166
Miroslav Knežević, Frederik Vercauteren, and Ingrid Verbauwhede

Finite Field Arithmetic for Pairing Based Cryptography

Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography 180
Naomi Benger and Michael Scott

Delaying Mismatched Field Multiplications in Pairing Computations ... 196
Craig Costello, Colin Boyd, Juan Manuel Gonzalez Nieto, and Kenneth Koon-Ho Wong

Invited Talk 3

Regenerating Codes for Distributed Storage Networks 215
Nihar B. Shah, K.V. Rashmi, P. Vijay Kumar, and Kannan Ramchandran

Finite Fields, Cryptography and Coding

On Rationality of the Intersection Points of a Line with a Plane Quartic 224
Roger Oyono and Christophe Ritzenthaler

Reflections about a Single Checksum 238
Ulrich Tamm

Efficient Time-Area Scalable ECC Processor Using μ-Coding Technique 250
Mohamed N. Hassan and Mohammed Benaissa

Author Index 269