

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Claude Carlet Berk Sunar (Eds.)

Arithmetic of Finite Fields

First International Workshop, WAIFI 2007
Madrid, Spain, June 2007
Proceedings

Volume Editors

Claude Carlet

Université Paris 8, Département de mathématiques
2, rue de la Liberté; 93526 - SAINT-DENIS Cedex 02, France
E-mail: claude.carlet@inria.fr

Berk Sunar

Worcester Polytechnic Institute
100 Institute Road, Worcester, MA 01609, USA
E-mail: sunar@wpi.edu

Library of Congress Control Number: 2007928526

CR Subject Classification (1998): E.4, I.1, E.3, G.2, F.2

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

ISSN 0302-9743

ISBN-10 3-540-73073-7 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-73073-6 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12077106 06/3180 5 4 3 2 1 0

Preface

These are the proceedings of WAIFI 2007. The conference was held in Madrid, Spain, during June 21–22, 2007. We are very grateful to the Program Committee members and to the external reviewers for their hard work! The conference received 94 submissions out of which 27 were finally selected for presentation. Each paper was refereed by at least two reviewers, and at least by three in the case of papers (co)-authored by Program Committee members. All final decisions were taken only after a clear position was clarified through additional reviews and comments. The Committee also invited Harald Niederreiter and Richard E. Blahut to speak on topics of their choice and we thank them for having accepted.

Special compliments go out to José L. Imaña, the general Co-chair and local organizer of WAIFI 2007, who brought the workshop to beautiful Madrid, Spain. WAIFI 2007 was organized by the department Computer Architecture of Facultad de Informática of the Universidad Complutense, in Madrid. We also would like to thank the General Co-chair Çetin K. Koç for his guidance. Finally, we would like to thank the Steering Committee for providing us with this wonderful opportunity.

The submission and selection of papers were done using the iChair software, developed at EPFL by Thomas Baignères and Matthieu Finiasz. Many thanks for their kind assistance! We also thank Gunnar Gaubatz for his precious help in this matter.

June 2007

Claude Carlet
Berk Sunar

Organization

Steering Committee

Jean-Pierre Deschamps	University Rovira i Virgili, Spain
José L. Imaña	Complutense University of Madrid, Spain
Çetin K. Koç	Oregon State University, USA
Christof Paar	Ruhr University of Bochum, Germany
Jean-Jacques Quisquater	Université Katholique de Louvain, Belgium
Berk Sunar	Worcester Polytechnic Institute, USA
Gustavo Sutter	Autonomous University of Madrid, Spain

Executive Committee

General Co-chairs

José L. Imaña	Complutense University of Madrid, Spain
Çetin K. Koç	Oregon State University, USA

Program Co-chairs

Claude Carlet	University of Paris 8, France
Berk Sunar	Worcester Polytechnic Institute, USA

Financial, Local Arrangements Chairs

Luis Piñuel	Complutense University of Madrid, Spain
Manuel Prieto	Complutense University of Madrid, Spain

Publicity Chair

Gustavo Sutter	Autonomous University of Madrid, Spain
----------------	--

Program Committee

Jean-Claude Bajard	CNRS-LIRMM in Montpellier, France
Ian F. Blake	University of Toronto, Canada
Marc Daumas	CNRS-LIRMM in Perpignan, France
Jean-Pierre Deschamps	University Rovira i Virgili, Spain
Josep Domingo-Ferrer	University Rovira i Virgili, Spain
Philippe Gaborit	University of Limoges, France
Joachim von zur Gathen	B-IT, University of Bonn, Germany
Pierrick Gaudry	LORIA-INRIA, France
Guang Gong	University of Waterloo, Canada
Jorge Guajardo	Philips Research, Netherlands
Anwar Hasan	University of Waterloo, Canada

Çetin K. Koç	Oregon State University, USA
Tanja Lange	Technische Universiteit Eindhoven, Netherlands
Julio López	UNICAMP, Brazil
Gary Mullen	Pennsylvania State University, USA
Harald Niederreiter	National University of Singapore, Singapore
Ferruh Ozbudak	Middle East Technical University, Turkey
Erkay Savaş	Sabancı University, Turkey
Igor Shparlinski	Macquarie University, Australia
Horacio Tapia-Recillas	UAM-Iztapalapa, D.F., Mexico
Apostol Vourdas	University of Bradford, UK

Referees

O. Ahmadi	M. Finiasz	A. Martínez-Ballesté
J. Aragonés	D. Freeman	N. Méloni
R.M. Avanzi	T. GÜdü	Y. Nawaz
O. Barenys	C. Güneri	C. Negre
I. Barenys	K. Gupta	T.B. Pedersen
L. Batina	G. Hanrot	M.N. Plasencia
D.J. Bernstein	F. Hess	D. Pointcheval
P. Birkner	K. Horadam	T. Plantard
M. Cenk	L. Imbert	C. Ritzenthaler
J. Chung	S. Jiang	G. Saldamli
V. Daza	T. Kerins	Z. Saygı
C. Ding	D. Kohel	F. Sebe
A. Doğanaksoy	G. Kömürcü	B. Schoenmakers
N. Ebeid	G. Kyureghyan	A. Tisserand
N. El Mrabet	G. Leander	F. Vercauteren
H. Fan	J. Lutz	W. Willems

Sponsoring Institutions

Real Sociedad Matemática Española, Spain.

Ministerio de Educación y Ciencia, Spain.

Facultad de Informática de la Universidad Complutense de Madrid, Spain.

ArTeCs: Architecture and Technology of Computing Systems Group,

Universidad Complutense de Madrid, Spain.

Universidad Complutense de Madrid, Spain.

Table of Contents

Structures in Finite Fields

Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields	1
<i>Robert W. Fitzgerald and Joseph L. Yucas</i>	
Some Notes on d -Form Functions with Difference-Balanced Property . . .	11
<i>Tongjiang Yan, Xiaoni Du, Enjian Bai, and Guozhen Xiao</i>	
A Note on Modular Forms on Finite Upper Half Planes	18
<i>Yoshinori Hamahata</i>	

Efficient Implementation and Architectures

A Coprocessor for the Final Exponentiation of the η_T Pairing in Characteristic Three	25
<i>Jean-Luc Beuchat, Nicolas Brisebarre, Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto</i>	
VLSI Implementation of a Functional Unit to Accelerate ECC and AES on 32-Bit Processors	40
<i>Stefan Tillich and Johann Großschädl</i>	
Efficient Multiplication Using Type 2 Optimal Normal Bases	55
<i>Joachim von zur Gathen, Amin Shokrollahi, and Jamshid Shokrollahi</i>	

Efficient Finite Field Arithmetic

Effects of Optimizations for Software Implementations of Small Binary Field Arithmetic	69
<i>Roberto Avanzi and Nicolas Thériault</i>	
Software Implementation of Arithmetic in \mathbb{F}_{3^m}	85
<i>Omran Ahmadi, Darrel Hankerson, and Alfred Menezes</i>	
Complexity Reduction of Constant Matrix Computations over the Binary Field	103
<i>Oscar Gustafsson and Mikael Olofsson</i>	
Towards Optimal Toom-Cook Multiplication for Univariate and Multivariate Polynomials in Characteristic 2 and 0	116
<i>Marco Bodrato</i>	

Classification and Construction of Mappings over Finite Fields

A Construction of Differentially 4-Uniform Functions from Commutative Semifields of Characteristic 2	134
<i>Nobuo Nakagawa and Satoshi Yoshiara</i>	
Complete Mapping Polynomials over Finite Field F_{16}	147
<i>Yuan Yuan, Yan Tong, and Huanguo Zhang</i>	
On the Classification of 4 Bit S-Boxes	159
<i>G. Leander and A. Poschmann</i>	
The Simplest Method for Constructing APN Polynomials EA-Inequivalent to Power Functions	177
<i>Lilya Budaghyan</i>	

Curve Algebra

New Point Addition Formulae for ECC Applications	189
<i>Nicolas Meloni</i>	
Explicit Formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation	202
<i>Stefan Erickson, Michael J. Jacobson Jr., Ning Shang, Shuo Shen, and Andreas Stein</i>	
The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic	219
<i>Reza Rezaeian Farashahi and Ruud Pellikaan</i>	

Cryptography

On Kabatianskii-Krouk-Smeets Signatures	237
<i>Pierre-Louis Cayrel, Ayoub Otmani, and Damien Vergnaud</i>	
Self-certified Signatures Based on Discrete Logarithms	252
<i>Zuhua Shao</i>	
Attacking the Filter Generator over $GF(2^m)$	264
<i>Sondre Rønjom and Tor Helleseth</i>	

Codes

Cyclic Additive and Quantum Stabilizer Codes	276
<i>Jürgen Bierbrauer</i>	

Determining the Number of One-Weight Cyclic Codes When Length and Dimension Are Given	284
<i>Gerardo Vega</i>	
Error Correcting Codes from Quasi-Hadamard Matrices	294
<i>V. Álvarez, J.A. Armario, M.D. Frau, E. Martín, and A. Osuna</i>	
Fast Computations of Gröbner Bases and Blind Recognitions of Convolutional Codes	303
<i>Peizhong Lu and Yan Zou</i>	
Discrete Structures	
A Twin for Euler's ϕ Function in $\mathbb{F}_2[X]$	318
<i>R. Durán Díaz, J. Muñoz Masqué, and A. Peinado Domínguez</i>	
Discrete Phase-Space Structures and Mutually Unbiased Bases	333
<i>A.B. Klimov, J.L. Romero, G. Björk, and L.L. Sánchez-Soto</i>	
Some Novel Results of p -Adic Component of Primitive Sequences over $Z/(p^d)$	346
<i>Yuewen Tang and Dongyang Long</i>	
Author Index	355