Lecture Notes in Computer Science 4547

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

Claude Carlet Berk Sunar (Eds.)

Arithmetic of Finite Fields

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

Springer

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

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	Sabanci 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

Efficient Implementation and Architectures

Efficient Finite Field Arithmetic

Classification and Construction of Mappings over Finite Fields

Curve Algebra

Cryptography

Codes

Discrete Structures