Lecture Notes in Computer Science 5130

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

Joachim von zur Gathen
José Luis Imaña
Çetin Kaya Koç (Eds.)

Arithmetic of Finite Fields

2nd International Workshop, WAIFI 2008
Siena, Italy, July 6–9, 2008
Proceedings

Springer

Volume Editors

Joachim von zur Gathen
B-IT, Universität Bonn
Dahlmannstr. 2
53113 Bonn, Germany
E-mail: gathen@bit.uni-bonn.de

José Luis Imaña
Complutense University
28040 Madrid, Spain
E-mail: jluimana@dacya.ucm.es

Çetin Kaya Koç
Istanbul Chamber of Commerce
34112 Istanbul, Turkey,
E-mail: koc@cryptocode.net

Library of Congress Control Number: 2008929536

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 3-540-69498-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-69498-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12323364 06/3180 5 4 3 2 1 0

Preface

These are the proceedings of WAIFI 2008, the second workshop on the Arithmetic of Finite Fields, that was held in Siena, Italy, July 6-9, 2008. The first workshop, WAIFI 2007, which was held in Madrid (Spain), was received quite enthusiastically by mathematicians, computer scientists, engineers and physicists who are performing research on finite field arithmetic. We believe that there is a need for a workshop series bridging the gap between the mathematical theory of finite fields and their hardware/software implementations and technical applications. We hope that the WAIFI workshop series, which from now on will be held on even years, will help to fill this gap.

There were 34 submissions to WAIFI 2008, of which the Program Committee selected 16 for presentation. Each submission was reviewed by at least three reviewers. Our thanks go to the Program Committee members for their many contributions and hard work. We are also grateful to the external reviewers listed below for their expertise and assistance in the deliberations. In addition to the contributions appearing in these proceedings, the workshop program included an invited lecture given by Amin Shokrollahi.

Special compliments go out to Enrico Martinelli, General Co-chair, and to Roberto Giorgi and Sandro Bartolini, local organizers of WAIFI 2008, who brought the workshop to Siena, one of the most beautiful cities of Tuscany, Italy. WAIFI 2008 was organized by the Dipartimento di Ingegneria dell'Informazione of the University of Siena, Italy.

The submission and selection of papers were done using the iChair software, developed at EPFL by Thomas Baignères and Matthieu Finiasz. We also thank Deniz Karakoyunlu for his help in this matter.

July 2008

Joachim von zur Gathen
José Luis Imaña
Çetin Kaya Koç

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	Oregon State University, USA
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

José Luis Imaña	Complutense University of Madrid, Spain
Enrico Martinelli	University of Siena, Italy

Program Co-chairs

Joachim von zur Gathen	B-IT, University of Bonn, Germany
Çetin Kaya Koç	Oregon State University, USA

Financial, Local Arrangements Chairs

Sandro Bartolini	University of Siena, Italy
Roberto Giorgi	University of Siena, Italy

Publicity Chair

Claude Carlet	University of Paris 8, France

Program Committee

Omran Ahmadi	University of Waterloo, Canada
Daniel Augot	INRIA-Rocquencourt, France
Jean-Claude Bajard	University of Montpellier II, France
Luca Breveglieri	Politecnico di Milano, Italy
Stephen Cohen	University of Glasgow, UK
Ricardo Dahab	Universidade Estadual de Campinas, Brazil
Gianluca Dini	University of Pisa, Italy
Serdar Erdem	Gebze Institute of Technology, Turkey
Joachim von zur Gathen	B-IT, University of Bonn, Germany

Elisa Gorla	University of Zürich, Switzerland
Dirk Hachenberger	University of Augsburg, Germany
Anwar Hasan	University of Waterloo, Canada
Marc Joye	Thomson R&D, France
Çetin Kaya Koç	Oregon State University, USA
Arjen Lenstra	EPFL, Switzerland
Peter Montgomery	Microsoft Research, USA
Ferruh Özbudak	Middle East Technical University, Turkey
Francesco Pappalardi	University of Rome 3, Italy
Francisco Rodríguez-Henríquez	Cinvestav, Mexico
René Schoof	University of Rome 2, Italy
Éric Schost	University of Western Ontario, Canada
Jamshid Shokrollahi	Ruhr University Bochum, Germany
Berk Sunar	Worcester Polytechnic Institute, USA
Chris Umans	California Institute of Technology, USA
Colin Walter	Comodo Research Lab, UK

Referees

A. Barenghi	D. Karakoyunlu	A. Reyhani-Masoleh
L. Batina	A. Karlov	M. Roetteler
A. Canteaut	S. Khazaei	G. Saldamlı
C. Carlet	C. Lauradoux	J. Sarinay
P. Charpin	D. Loebenberger	S. Sarkar
N. Courtois	M. Macchetti	E. Savas
J. Detrey	W. Marnane	O. Schütze
L. El Aimani	F. Morain	I. Shparlinski
H. Fan	C. Negre	M. Stam
S. Fischer	M. Nüsken	R. Venkatesan
F. Fontein	S. Paul	J. Zumbrägel
P. Gaborit	G. Pelosi	
M. Kaihara	T. Plantard	

Sponsoring Institutions

Microsoft Research.
CINECA - Inter University Computing Centre, Italy
University of Siena, Italy

Table of Contents

Structures in Finite Fields

Efficient Finite Field Arithmetic

Efficient Implementation and Architectures

Classification and Construction of Mappings over Finite Fields

Codes and Cryptography