Lecture Notes in Computer Science 5130

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
   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
Gerhard Weikum
   Max-Planck Institute of Computer Science, Saarbruecken, Germany
Arithmetic of Finite Fields

2nd International Workshop, WAIFI 2008
Siena, Italy, July 6–9, 2008
Proceedings
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
Jean-Pierre Deschamps
José Luis Imaña
Çetin Kaya Koç
Christof Paar
Jean-Jacques Quisquater
Berk Sunar
Gustavo Sutter

University of Paris 8, France
University Rovira i Virgili, Spain
Complutense University of Madrid, Spain
Oregon State University, USA
Ruhr University of Bochum, Germany
Université catholique de Louvain, Belgium
Worcester Polytechnic Institute, USA
Autonomous University of Madrid, Spain

Executive Committee

General Co-chairs
José Luis Imaña
Enrico Martinelli

Complutense University of Madrid, Spain
University of Siena, Italy

Program Co-chairs
Joachim von zur Gathen
Çetin Kaya Koç

B-IT, University of Bonn, Germany
Oregon State University, USA

Financial, Local Arrangements Chairs
Sandro Bartolini
Roberto Giorgi

University of Siena, Italy
University of Siena, Italy

Publicity Chair
Claude Carlet

University of Paris 8, France

Program Committee

Omran Ahmadi
Daniel Augot
Jean-Claude Bajard
Luca Breveglieri
Stephen Cohen
Ricardo Dahab
Gianluca Dini
Serdar Erdem
Joachim von zur Gathen

University of Waterloo, Canada
INRIA-Rocquencourt, France
University of Montpellier II, France
Politecnico di Milano, Italy
University of Glasgow, UK
Universidade Estadual de Campinas, Brazil
University of Pisa, Italy
Gebze Institute of Technology, Turkey
B-IT, University of Bonn, Germany
VIII Organization

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

- Interpolation of the Double Discrete Logarithm ........................................ 1  
  *Gerasimos C. Meletiou and Arne Winterhof*

- Finite Dedekind Sums ................................................................. 11  
  *Yoshinori Hamahata*

- Transitive q-Ary Functions over Finite Fields or Finite Sets: Counts, Properties and Applications .................................................. 19  
  *Marc Mouffron*

### Efficient Finite Field Arithmetic

- Fast Point Multiplication on Elliptic Curves without Precomputation .......... 36  
  *Marc Joye*

- Optimal Extension Field Inversion in the Frequency Domain .................... 47  
  *Selçuk Baktır and Berk Sunar*

- Efficient Finite Fields in the Maxima Computer Algebra System .............. 62  
  *Fabrizio Caruso, Jacopo D’Aurizio, and Alasdair McAndrew*

### Efficient Implementation and Architectures

- Modular Reduction in GF($2^n$) without Pre-computational Phase ........... 77  
  *M. Knežević, K. Sakiyama, J. Fan, and I. Verbauwhede*

- Subquadratic Space Complexity Multiplication over Binary Fields with Dickson Polynomial Representation ............................................ 88  
  *M. Anwar Hasan and Christophe Negre*

- Digit-Serial Structures for the Shifted Polynomial Basis Multiplication over Binary Extension Fields .................................................. 103  
  *Arash Hariri and Arash Reyhani-Masoleh*

### Classification and Construction of Mappings over Finite Fields

- Some Theorems on Planar Mappings ................................................ 117  
  *Gohar M. Kyureghyan and Alexander Pott*
Classifying 8-Bit to 8-Bit S-Boxes Based on Power Mappings from the
Point of DDT and LAT Distributions ........................................... 123

Bora Aslan, M. Tolga Sakalli, and Ercan Bulus

EA and CCZ Equivalence of Functions over $GF(2^n)$ ..................... 134

K.J. Horadam

**Codes and Cryptography**

On the Number of Two-Weight Cyclic Codes with Composite
Parity-Check Polynomials ............................................................. 144

Gerardo Vega

On Field Size and Success Probability in Network Coding ............ 157

Olav Geil, Ryutaroh Matsumoto, and Casper Thomsen

Montgomery Ladder for All Genus 2 Curves in Characteristic 2 .... 174

Sylvain Duquesne

On Cryptographically Significant Mappings over $GF(2^n)$ .......... 189

Enes Pasalic

**Author Index** ........................................................................... 205