Lecture Notes in Computer Science 5527

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

Maria Bras-Amorós Tom Høholdt (Eds.)

Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes

18th International Symposium, AAECC-18
Tarragona, Spain, June 8-12, 2009
Proceedings

Springer

Volume Editors

Maria Bras-Amorós
Universitat Rovira i Virgili
Departament d'Enginyeria Informàtica i Matemàtiques
Avinguda Països Catalans, 26, 43007 Tarragona, Catalonia, Spain,
E-mail: maria.bras@urv.cat

Tom Høholdt
The Technical University of Denmark
Department of Mathematics
Building 303, 2800 Lyngby, Denmark,
E-mail: tom@mat.dtu.dk

Library of Congress Control Number: Applied for

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 3-642-02180-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-02180-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12690084 06/3180 5 4 3 2 1 0

Preface

The AAECC symposia series was started in 1983 by Alain Poli (Toulouse), who, together with R. Desq, D. Lazard and P. Camion, organized the first conference. Originally the acronym AAECC stood for "Applied Algebra and Error-Correcting Codes." Over the years its meaning has shifted to "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes," reflecting the growing importance of complexity, particularly for decoding algorithms. During the AAECC-12 symposium the Conference Committee decided to enforce the theory and practice of the coding side as well as the cryptographic aspects. Algebra was conserved, as in the past, but slightly more oriented to algebraic geometry codes, finite fields, complexity, polynomials, and graphs. The main topics for AAECC-18 were algebra, algebraic computation, codes and algebra, codes and combinatorics, modulation and codes, sequences, and cryptography.

The invited speakers of this edition were Iwan Duursma, Henning Stichtenoth, and Fernando Torres. We would like to express our deep regret for the loss of Professor Ralf Kötter, who recently passed away and could not be our fourth invited speaker.

Except for AAECC-1 (Discrete Mathematics 56, 1985) and AAECC-7 (Discrete Applied Mathematics 33, 1991), the proceedings of all the symposia have been published in Springer's *Lecture Notes in Computer Science* (Vols. 228, 229, 307, 356, 357, 508, 539, 673, 948, 1255, 1719, 2227, 2643, 3857, 4851).

It is a policy of AAECC to maintain a high scientific standard, comparable to that of a journal. This was made possible thanks to the many referees involved. Each submitted paper was evaluated by at least two international researchers. AAECC-18 received and refereed 50 submissions. Of these, 22 were selected for publication in these proceedings as regular papers and 7 were selected as extended abstracts.

The symposium was organized by Maria Bras-Amorós and Tom Høholdt, with the help of Jesús Manjón, Glòria Pujol, Jordi Castellà, Antoni Martínez, and Xavier Fernández under the umbrella of the CRISES group for Cryptography and Statistical Secrecy, at the Universitat Rovira i Virgili, led by Josep Domingo-Ferrer.

It was sponsored by the Catalan Government, the UNESCO Chair in Data Privacy located at Universitat Rovira i Virgili, and the Spanish Network on Mathematics of Information Society.

We would like to dedicate these proceedings to the memory of our colleague Ralf Kötter.

June 2009

Maria Bras-Amorós
Tom Høholdt

Applied Algebra, Algebraic Algorithms, and Error Correcting Codes - AAECC-18

General Chair

Maria Bras-Amorós	Universitat Rovira i Virgili, Catalonia, Spain

Co-chair

Tom Høholdt	Technical University of Denmark

Program Committee

Jacques Calmet	University of Karlsruhe, Germany
Claude Carlet	University of Paris 8, France
Gerard D. Cohen	Ecole Nationale Supérieure des Télécommunications, France
Cunsheng Ding	Hong Kong University of Science and Technology, China
Gui-Liang Feng	University of Southwestern Louisiana, USA
Marc Giusti	Ecole Polytechnique, France
Guang Gong	University of Waterloo, Canada
Joos Heintz	University of Buenos Aires, Argentina and University of Cantabria, Spain
Kathy Horadam	RMIT University, Australia
Hideki Imai	University of Tokyo, Japan
Navin Kashyap	Queen's University, Canada
Shu Lin	University of California, USA
Oscar Moreno	University of Puerto Rico
Wai Ho Mow	Southwest Jiaotong University, China
Harald Niederreiter	National University of Singapore
Michael E. O'Sullivan	San Diego State University, USA
Ferruh Ozbudak	Middle East Technical University, Turkey
Udaya Parampalli	University of Melbourne, Australia
Alain Poli	University P. Sabatier, France
S. Sandeep Pradhan	University of Michigan at Ann Arbor, USA
Asha Rao	Royal Melbourne Institute of Technology, Australia
Shojiro Sakata	Technical University of Denmark
Hong-Yeop Song	Yonsei University, Korea
Chaoping Xing	Nanyang Technological University, Singapore

Organizing Committee

Jesús Manjón	Universitat Rovira i Virgili, Catalonia, Spain
Glòria Pujol	Universitat Rovira i Virgili, Catalonia, Spain
Jordi Castellà-Roca	Universitat Rovira i Virgili, Catalonia, Spain
Antoni Martínez-Ballesté	Universitat Rovira i Virgili, Catalonia, Spain
Xavier Fernández	Universitat Rovira i Virgili, Catalonia, Spain

Table of Contents

Codes

Cryptography

Algebra

Extended Abstracts