Lecture Notes in Computer Science 3969

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

Øyvind Ytrehus (Ed.)

Coding and Cryptography

International Workshop, WCC 2005
Bergen, Norway, March 14-18, 2005
Revised Selected Papers

Springer

Volume Editor

Øyvind Ytrehus
University of Bergen
Department of Informatics
N-5020 Bergen, Norway
E-mail: oyvind@ii.uib.no

Library of Congress Control Number: 2006927431

CR Subject Classification (1998): E.3-4, G.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-35481-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-35481-9 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 2006

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11779360 06/3142 5 4 3 2 1 0

Preface

This volume contains refereed papers devoted to coding and cryptography. These papers are the full versions of a selection of the best extended abstracts accepted for presentation at the International Workshop on Coding and Cryptography (WCC 2005) held in Bergen, Norway, March 14–18, 2005. Each of the 118 extended abstracts originally submitted to the workshop were reviewed by at least two members of the Program Committee. As a result of this screening process, 58 papers were selected for presentation, of which 52 were eventually presented at the workshop together with four invited talks.

The authors of the presented papers were in turn invited to submit full versions of their papers to the full proceedings. Each of the full-version submissions were once again thoroughly examined and commented upon by at least two reviewers. This volume is the end result of this long process.

I am grateful to the reviewers who contributed to guaranteeing the high standards of this volume, and who are named on the next pages. It was a pleasure for me to work with my program co-chair Pascale Charpin, whose experienced advice I have further benefited greatly from during the preparation of this volume. Discussions with Tor Helleseth and Ángela Barbero were also useful in putting the volume together. Finally, I would like to thank all the authors and all the other participants of the WCC 2005 for making it in every sense a highly enjoyable event.

March 2006 Øyvind Ytrehus

Organization

WCC 2005 was organized by the Selmer Center at the Department of Informatics, University of Bergen, Norway, in cooperation with INRIA Rocquencourt.

Conference Chair	Tor Helleseth (University of Bergen, Norway)
Program Co-chairs	Pascale Charpin (INRIA Rocquencourt, France)
	Øyvind Ytrehus (University of Bergen, Norway)
Program Committee	
	D. Augot (INRIA Rocquencourt, France)
	C. Carlet (Université Paris VIII, France)
	P. Charpin (**Co-chair**, INRIA Rocquencourt, France)
	C. Ding (Hong Kong University of Science and Technology, China)
	H. Dobbertin (University of Bochum, Germany)
	S. Dodunekov (Institute of Mathematics, Sofia, Bulgaria)
	I. Dumer (UC Riverside, USA)
	G. Gong (University of Waterloo, Canada)
	T. Helleseth (University of Bergen, Norway)
	I. Honkala (University of Turku, Finland)
	T. Hholdt (DTU, Denmark)
	T. Johansson (Lund University, Sweden)
	G. Kabatianski (IPIT, Moscow, Russia)
	T. Lange (University of Bochum, Germany)
	J. Massey (Lund University, Sweden)
	M. Mihaljevic (Serbian Acad. of Sciences and Art, Serbia and Montenegro)
	K. Nyberg (Nokia, Finland)
	M.G. Parker (University of Bergen, Norway)
	K. Paterson (Royal Holloway, UK)
	I. Semaev (University of Bergen, Norway)
	N. Sendrier (INRIA, France)
	D. Stinson (University of Waterloo, Canada)
	H. van Tilborg (Eindhoven University of Technology, The Netherlands)
	S. Vladuts (Université de Marseille, France)
	Ø. Ytrehus (**Co-chair**, University of Bergen, Norway)
	G. Zémor (ENST, France)
	V. Zinoviev (IPIT, Moscow, Russia)

Other Referees for WCC 2005

In addition to the members of the Program Committee, the following were also involved as reviewers in the WCC 2005 review process:

Alexei Ashikhmin
Roberto M. Avanzi
Leonid Bassalygo
Peter Beelen
Raghav Bhaskar
Peter Boyvalenkov
Dario Catalano
Yang Cui
Ernst M. Gabidulin
Philippe Gaborit
Clemens Heuberger
Claude-Pierre Jeannerod
Shaoquan Jiang
Ellen Jochemsz
Antoine Joux
Alexander Kholosha
Emil Kolev
Kristine Lally
Ivan Landjev
Vladimir Levenshtein
Simon Litsyn
Pierre Loidreau
Nikolai Manev
Marine Minier
Thomas Mittelholzer
Kiril Morozov
Wakaha Ogata
Kalle Ranto
Petri Rosendahl
Berry Schonemakers
SoongHan Shin
Andrey Sidorenko
Faina Solov'eva
Jeremy Thorpe
Jean-Pierre Tillich
Jing Ying
Nam Yul Yu

Sponsoring Institutions

The Selmer Center, University of Bergen
The Norwegian Research Council (NFR)

Table of Contents

Second Support Weights for Binary Self-dual Codes
Keisuke Shiromoto 1

On Codes Correcting Symmetric Rank Errors
Nina I. Pilipchuk, Ernst M. Gabidulin 14

Error and Erasure Correction of Interleaved Reed–Solomon Codes
Georg Schmidt, Vladimir R. Sidorenko, Martin Bossert 22

A Welch–Berlekamp Like Algorithm for Decoding Gabidulin Codes
Pierre Loidreau 36

On the Weights of Binary Irreducible Cyclic Codes
Yves Aubry, Philippe Langevin 46

3-Designs from Z_4-Goethals-Like Codes and Variants of Cyclotomic Polynomials
Jyrki Lahtonen, Kalle Ranto, Roope Vehkalahti 55

Space-Time Code Designs Based on the Generalized Binary Rank Criterion with Applications to Cooperative Diversity
A. Roger Hammons Jr. 69

Geometric Conditions for the Extendability of Ternary Linear Codes
Tatsuya Maruta, Kei Okamoto 85

On the Design of Codes for DNA Computing
Olgica Milenkovic, Navin Kashyap 100

Open Problems Related to Algebraic Attacks on Stream Ciphers
Anne Canteaut 120

On the Non-linearity and Sparsity of Boolean Functions Related to the Discrete Logarithm in Finite Fields of Characteristic Two
Nina Brandstätter, Tanja Lange, Arne Winterhof 135

Interpolation of Functions Related to the Integer Factoring Problem
Clemens Adelmann, Arne Winterhof 144

On Degrees of Polynomial Interpolations Related to Elliptic Curve Cryptography
Takakazu Satoh 155

Finding Good Differential Patterns for Attacks on SHA-1
Krystian Matusiewicz, Josef Pieprzyk 164

Extending Gibson's Attacks on the GPT Cryptosystem
Raphael Overbeck 178

Reduction of Conjugacy Problem in Braid Groups, Using Two Garside Structures
Maffre Samuel 189

A New Key Assignment Scheme for Access Control in a Complete Tree Hierarchy
Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci 202

Multi-Dimensional Hash Chains and Application to Micropayment Schemes
Quan Son Nguyen 218

On the Affine Transformations of HFE-Cryptosystems and Systems with Branches
Patrick Felke 229

Dimension of the Linearization Equations of the Matsumoto-Imai Cryptosystems
Adama Diene, Jintai Ding, Jason E. Gower, Timothy J. Hodges, Zhijun Yin 242

RSA-Based Secret Handshakes
Damien Vergnaud 252

On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Codes
Ventzislav Nikov, Svetla Nikova 275

ID-Based Series-Parallel Multisignature Schemes for Multi-Messages from Bilinear Maps
Lihua Wang, Eiji Okamoto, Ying Miao, Takeshi Okamoto, Hiroshi Doi 291

A New Public-Key Cryptosystem Based on the Problem of Reconstructing *p*–Polynomials
Cédric Faure, Pierre Loidreau 304

On the Wagner–Magyarik Cryptosystem
Françoise Levy-dit-Vehel, Ludovic Perret 316

Constructions of Complementary Sequences for Power-Controlled OFDM Transmission
Kai-Uwe Schmidt, Adolf Finger 330

A Novel Method for Constructing Almost Perfect Polyphase Sequences
Xiangyong Zeng, Lei Hu, Qingchong Liu 346

Linear Filtering of Nonlinear Shift-Register Sequences
Berndt M. Gammel, Rainer Göttfert 354

Realizations from Decimation Hadamard Transform for Special Classes of Binary Sequences with Two-Level Autocorrelation
Nam Yul Yu, Guang Gong 371

Frequency/Time Hopping Sequences with Large Linear Complexities
Yun-Pyo Hong, Hong-Yeop Song 386

One and Two-Variable Interlace Polynomials: A Spectral Interpretation
Constanza Riera, Matthew G. Parker 397

Improved Bounds on Weil Sums over Galois Rings and Homogeneous Weights
San Ling, Ferruh Özbudak 412

Locally Invertible Multivariate Polynomial Matrices
Ruben G. Lobo, Donald L. Bitzer, Mladen A. Vouk 427

Author Index 443