

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

Yeow Meng Chee Chao Li San Ling
Huaxiong Wang Chaoping Xing (Eds.)

Coding and Cryptology

Second International Workshop, IWCC 2009
Zhangjiajie, China, June 1-5, 2009
Proceedings

Volume Editors

Yeow Meng Chee
San Ling
Huaxiong Wang
Chaoping Xing

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371

E-mail: {ymchee; lingsan; hxwang; xingcp}@ntu.edu.sg

Chao Li
National University of Defense Technology,
410073 Changsha Hunan, China

E-mail: lichao_nudt@sina.com

Library of Congress Control Number: Applied for

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 3-642-01813-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-01813-8 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12674015 06/3180 5 4 3 2 1 0

Preface

The biennial International Workshop on Coding and Cryptology (IWCC) aims to bring together many of the world's greatest minds in coding and cryptology to share ideas and exchange knowledge related to advancements in coding and cryptology, amidst an informal setting conducive for interaction and collaboration.

It is well known that fascinating connections exist between coding and cryptology. Therefore this workshop series was organized to facilitate a fruitful interaction and stimulating discourse among experts from these two areas.

The inaugural IWCC was held at Wuyi Mountain, Fujian Province, China, during June 11-15, 2007 and attracted over 80 participants. Following this success, the second IWCC was held June 1-5, 2009 at Zhangjiajie, Hunan Province, China. Zhangjiajie is one of the most scenic areas in China.

The proceedings of this workshop consist of 21 technical papers, covering a wide range of topics in coding and cryptology, as well as related fields such as combinatorics. All papers, except one, are contributed by the invited speakers of the workshop and each paper has been carefully reviewed. We are grateful to the external reviewers for their help, which has greatly strengthened the quality of the proceedings.

IWCC 2009 was co-organized by the National University of Defense Technology (NUDT), China and Nanyang Technological University (NTU), Singapore. We acknowledge with gratitude the financial support from NUDT.

We would like to express our thanks to Springer for making it possible for the proceedings to be published in the *Lecture Notes in Computer Science series*. We also thank Zhe-xian Wan for his great encouragement and constant support for this workshop series. We are also grateful to the staff and students from both NUDT and NTU for the administrative and technical support they have rendered to the conference and the proceedings. Special thanks go to Longjiang Qu for taking care of the website of the workshop, and Yang Ding for assistance on matters related to L^AT_EX.

Yeow Meng Chee
Chao Li
San Ling
Huaxiong Wang
Chaoping Xing

Organization

Chair of Organizing Committee

Zhe-xian Wan Academy of Mathematics and System Sciences, CAS, China

Organizing Committee

Yeow Meng Chee	Nanyang Technological University, Singapore
Chao Li	National University of Defense Technology, China
San Ling	Nanyang Technological University, Singapore
Huaxiong Wang	Nanyang Technological University, Singapore
Zhengming Wang	National University of Defense Technology, China
Chaoping Xing	Nanyang Technological University, Singapore
Jianming Zhu	National University of Defense Technology, China

Table of Contents

An Infinite Class of Balanced Vectorial Boolean Functions with Optimum Algebraic Immunity and Good Nonlinearity	1
<i>Claude Carlet and Keqin Feng</i>	
Separation and Witnesses	12
<i>Gérard Cohen</i>	
Binary Covering Arrays and Existentially Closed Graphs	22
<i>Charles J. Colbourn and Gerzson Kéri</i>	
A Class of Three-Weight and Four-Weight Codes	34
<i>Cunsheng Ding</i>	
Equal-Weight Fingerprinting Codes	43
<i>Ilya Dumer</i>	
Problems on Two-Dimensional Synchronization Patterns	52
<i>Tuvi Etzion</i>	
A New Client-to-Client Password-Authenticated Key Agreement Protocol	63
<i>Deng-Guo Feng and Jing Xu</i>	
Elliptic Twin Prime Conjecture	77
<i>John B. Friedlander and Igor E. Shparlinski</i>	
Hunting for Curves with Many Points	82
<i>Gerard van der Geer</i>	
List Decoding of Binary Codes—A Brief Survey of Some Recent Results	97
<i>Venkatesan Guruswami</i>	
Recent Developments in Low-Density Parity-Check Codes	107
<i>Wen-Ching Winnie Li, Min Lu, and Chenying Wang</i>	
On the Applicability of Combinatorial Designs to Key Predistribution for Wireless Sensor Networks	124
<i>Keith M. Martin</i>	
On Weierstrass Semigroups of Some Triples on Norm-Trace Curves	146
<i>Gretchen L. Matthews</i>	
ERINDALE: A Polynomial Based Hashing Algorithm	157
<i>V. Kumar Murty and Nikolajs Volkovs</i>	

A Survey of Algebraic Unitary Codes	171
<i>Frédérique Oggier</i>	
New Family of Non-Cartesian Perfect Authentication Codes	188
<i>Dingyi Pei</i>	
On the Impossibility of Strong Encryption Over \aleph_0	202
<i>Raphael C.-W. Phan and Serge Vaudenay</i>	
Minimum Distance between Bent and Resilient Boolean Functions	219
<i>Longjiang Qu and Chao Li</i>	
Unconditionally Secure Approximate Message Authentication	233
<i>Dongvu Tonien, Reihaneh Safavi-Naini, Peter Nickolas, and Yvo Desmedt</i>	
Multiplexing Realizations of the Decimation-Hadamard Transform of Two-Level Autocorrelation Sequences	248
<i>Nam Yul Yu and Guang Gong</i>	
On Cayley Graphs, Surface Codes, and the Limits of Homological Coding for Quantum Error Correction	259
<i>Gilles Zémor</i>	
Author Index	275