Progress in Computer Science and Applied Logic

Coding, Cryptography and Combinatorics

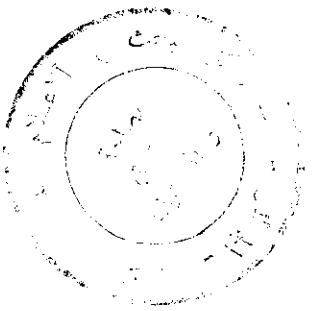
Keqin Feng
Harald Niederreiter
Chaoping Xing
Editors

Birkhäuser

Progress in Computer Science and Applied Logic
Volume 23

Coding, Cryptography and Combinatorics

Keqin Feng
Harald Niederreiter
Chaoping Xing
Editors



Birkhäuser Verlag
Basel · Boston · Berlin

Editors:

Keqin Feng
Department of Mathematical Sciences
Tsinghua University
Beijing 100084
China
kqfeng@math.hkbu.edu.hk
kfeng@math.tsinghua.edu.cn

Harald Niederreiter
Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543
Republic of Singapore
nied@math.nus.edu.sg

Chaoping Xing
Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543
Republic of Singapore
matxcp@nus.edu.sg

2000 Mathematics Subject Classification 11G18, 11G20, 11T71, 94A55, 94A60, 94A62, 94B05, 94B35, 94B60, 94B65

A CIP catalogue record for this book is available from the Library of Congress, Washington D.C., USA

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

ISBN 3-7643-2429-5 Birkhäuser Verlag, Basel – Boston – Berlin

Printed on acid-free paper produced of chlorine-free pulp. TCF ∞
Printed in Germany
ISBN 3-7643-2429-5

9 8 7 6 5 4 3 2 1

www.birkhauser.ch

Table of Contents

Preface vii

Invited Papers

Claude Carlet
On the Secondary Constructions of Resilient and Bent Functions 3

Tadao Kasami
Adaptive Recursive MLD Algorithm Based on Parallel Concatenation Decomposition for Binary Linear Codes 29

Wen-Ching Winnie Li
Modularity of Asymptotically Optimal Towers of Function Fields 51

Peizhong Lu and Lianzhen Huang
A New Correlation Attack on LFSR Sequences with High Error Tolerance 67

Amin Shokrollahi
LDPC Codes: An Introduction 85

Contributed Papers

Jintai Ding and Dieter Schmidt
The New Implementation Schemes of the TTM Cryptosystem Are Not Secure 113

Elona Erez and Meir Feder
The Capacity Region of Broadcast Networks with Two Receivers 129

Fang-Wei Fu, San Ling and Chaoping Xing
Constructions of Nonbinary Codes Correcting t-Symmetric Errors and Detecting All Unidirectional Errors: Magnitude Error Criterion 139

Aline Gouget
On the Propagation Criterion of Boolean Functions 153

Tor Helleseth, Jyrki Lahtonen and Petri Rosendahl
On Certain Equations over Finite Fields and Cross-Correlations of m-Sequences 169

Françoise Levy-dit-Vehel and Ludovic Perret
A Polly Cracker System Based on Satisfiability 177

Jing Li
Combinatorially Designed LDPC Codes Using Zech Logarithms and Congruential Sequences 193

Lei Li and Shoulun Long
New Constructions of Constant-Weight Codes 209

San Ling and Patrick Solé
Good Self-Dual Quasi-Cyclic Codes over $\mathbf{F}_q$, q Odd 223

Wilfried Meidl
Linear Complexity and k-Error Linear Complexity for p^n-Periodic Sequences 227

Jean-Francis Michon, Pierre Valarcher and Jean-Baptiste Yunès
HFE and BDDs: A Practical Attempt at Cryptanalysis 237

Harald Niederreiter
Digital Nets and Coding Theory 247

Harald Niederreiter and Ferruh Özbudak
Constructive Asymptotic Codes with an Improvement on the Tsfasman-Vlăduţ-Zink and Xing Bounds 259

Josef Pieprzyk and Huaxiong Wang
Malleability Attacks on Multi-Party Key Agreement Protocols 277

Charles C. Pinter
Combinatorial Tableaux in Isoperimetry 289

Yuansheng Tang
On the Error Exponents of Reliability-Order-Based Decoding Algorithms for Linear Block Codes 303

Xiaojian Tian and Cunsheng Ding
A Construction of Authentication Codes with Secrecy 319

Hitoshi Tokushige, Jun Asatani, Marc P.C. Fossorier and Tadao Kasami
Selection Method of Test Patterns in Soft-Input and Output Iterative Bounded Distance Decoding Algorithm 331

Yejing Wang, Luke McAven and Reihaneh Safavi-Naini
Deletion Correcting Using Generalised Reed-Solomon Codes 345

Arne Winterhof
A Note on the Linear Complexity Profile of the Discrete Logarithm in Finite Fields 359

Huapeng Wu, M. Anwar Hasan and Ian F. Blake
Speeding Up RSA and Elliptic Curve Systems by Choosing Suitable Moduli 369

Gang Yao, Feng Bao and Robert H. Deng
Security Analysis of Three Oblivious Transfer Protocols 385

Gang Yao, Guilin Wang and Yong Wang
An Improved Identification Scheme 397