

Table of Contents

Coding and Applications

Recent Developments in Array Error-Control Codes	1
<i>Patrick Guy Farrell</i>	
High Rate Convolutional Codes with Optimal Cycle Weights	4
<i>Eirik Rosnes and Øyvind Ytrehus</i>	
A Multifunctional Turbo-Based Receiver Using Partial Unit Memory Codes	24
<i>Lina Fagoonee and Bahram Honary</i>	
Commitment Capacity of Discrete Memoryless Channels	35
<i>Andreas Winter, Anderson C.A. Nascimento, and Hideki Imai</i>	
Separating and Intersecting Properties of BCH and Kasami Codes	52
<i>Hans Georg Schaathun and Tor Helleseeth</i>	

Applications of Coding in Cryptography

Analysis and Design of Modern Stream Ciphers	66
<i>Thomas Johansson</i>	
Improved Fast Correlation Attack Using Low Rate Codes	67
<i>Håvard Molland, John Erik Mathiassen, and Tor Helleseeth</i>	
On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions	82
<i>Yuri Borissov, An Braeken, Svetla Nikova, and Bart Preneel</i>	
Degree Optimized Resilient Boolean Functions from Maiorana-McFarland Class	93
<i>Enes Pasalic</i>	
Differential Uniformity for Arrays	115
<i>K.J. Horadam</i>	

Cryptography

Uses and Abuses of Cryptography	125
<i>Richard Walton</i>	
A Designer's Guide to KEMs	133
<i>Alexander W. Dent</i>	

VIII Table of Contents

A General Construction of IND-CCA2 Secure Public Key Encryption	152
<i>Eike Kiltz and John Malone-Lee</i>	
Efficient Key Updating Signature Schemes Based on IBS	167
<i>Dae Hyun Yum and Pil Joong Lee</i>	
Periodic Sequences with Maximal Linear Complexity and Almost	
Maximal k -Error Linear Complexity	183
<i>Harald Niederreiter and Igor E. Shparlinski</i>	

Cryptanalysis

Estimates for Discrete Logarithm Computations in Finite Fields of	
Small Characteristic	190
<i>Robert Granger</i>	
Resolving Large Prime(s) Variants for Discrete	
Logarithm Computation	207
<i>A.J. Holt and J.H. Davenport</i>	
Computing the $M = UU^t$ Integer Matrix Decomposition	223
<i>Katharina Geißler and Nigel P. Smart</i>	
Cryptanalysis of the Public Key Cryptosystem Based on the Word	
Problem on the Grigorchuk Groups	234
<i>George Petrides</i>	
More Detail for a Combined Timing and Power Attack against	
Implementations of RSA	245
<i>Werner Schindler and Colin D. Walter</i>	
Predicting the Inversive Generator	264
<i>Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and</i> <i>Igor E. Shparlinski</i>	
A Stochastic Model and Its Analysis for a Physical Random	
Number Generator Presented At CHES 2002	276
<i>Werner Schindler</i>	
Analysis of Double Block Length Hash Functions	290
<i>Mitsuhiro Hattori, Shoichi Hirose, and Susumu Yoshida</i>	

Network Security and Protocols

Cryptography in Wireless Standards (Invited Paper)	303
<i>Valtteri Niemi</i>	
On the Correctness of Security Proofs for the 3GPP Confidentiality and	
Integrity Algorithms	306
<i>Tetsu Iwata and Kaoru Kurosawa</i>	

A General Attack Model on Hash-Based Client Puzzles	319
<i>Geraint Price</i>	
Tripartite Authenticated Key Agreement Protocols from Pairings	332
<i>Sattam S. Al-Riyami and Kenneth G. Paterson</i>	
Remote User Authentication Using Public Information.....	360
<i>Chris J. Mitchell</i>	
Mental Poker Revisited	370
<i>Adam Barnett and Nigel P. Smart</i>	
Author Index	385

Cryptography and Coding

9th IMA International Conference, Cirencester, UK,

December 16-18, 2003, Proceedings

Paterson, K.G. (Ed.)

2003, X, 390 p., Softcover

ISBN: 978-3-540-20663-7