

Table of Contents

A Statistical Decoding Algorithm for General Linear Block Codes	1
<i>A. Al Jabri</i>	
On the Undetected Error Probability for Shortened Hamming Codes on Channels with Memory	9
<i>Christoph Lange, Andreas Ahrens</i>	
The Complete Weight Enumerator for Codes over $\mathcal{M}_{n \times s}(\mathbb{F}_q)$	20
<i>Irfan Siap</i>	
Further Improvement of Kumar-Rajagopalan-Sahai Coding Constructions for Blacklisting Problem	27
<i>Maki Yoshida, Toru Fujiwara</i>	
A Simple Soft-Input/Soft-Output Decoder for Hamming Codes	38
<i>Simon Hirst, Bahram Honary</i>	
A Technique with an Information-Theoretic Basis for Protecting Secret Data from Differential Power Attacks	44
<i>Manfred von Willich</i>	
Key Recovery Attacks on MACs Based on Properties of Cryptographic APIs	63
<i>Karl Brincat, Chris J. Mitchell</i>	
The Exact Security of ECIES in the Generic Group Model	73
<i>N.P. Smart</i>	
A New Ultrafast Stream Cipher Design: COS Ciphers	85
<i>Eric Filiol, Caroline Fontaine</i>	
On Rabin-Type Signatures	99
<i>Marc Joye, Jean-Jacques Quisquater</i>	
Strong Adaptive Chosen-Ciphertext Attacks with Memory Dump (or: The Importance of the Order of Decryption and Validation)	114
<i>Seungjoo Kim, Jung Hee Cheon, Marc Joye, Seongan Lim, Masahiro Mambo, Dongho Won, Yuliang Zheng</i>	
Majority-Logic-Decodable Cyclic Arithmetic-Modular AN-Codes in 1, 2, and L Steps	128
<i>F. Javier Galán-Simón, Edgar Martínez-Moro, Juan G. Tena-Ayuso</i>	
Almost-Certainly Runlength-Limiting Codes	138
<i>David J.C. MacKay</i>	

Weight vs. Magnetization Enumerator for Gallager Codes	148
<i>Jort van Mourik, David Saad, Yoshiyuki Kabashima</i>	
Graph Configurations and Decoding Performance	158
<i>J.T. Paire, P. Coulton, P.G. Farrell</i>	
A Line Code Construction for the Adder Channel with Rates Higher than Time-Sharing	166
<i>P. Benachour, P.G. Farrell, Bahram Honary</i>	
The Synthesis of TD-Sequences and Their Application to Multi-functional Communication Systems	176
<i>Ahmed Al-Dabbagh, Michael Darnell</i>	
Improvement of the Delsarte Bound for τ -Designs in Finite Polynomial Metric Spaces	191
<i>Svetla Nikova, Ventzislav Nikov</i>	
Statistical Properties of Digital Piecewise Linear Chaotic Maps and Their Roles in Cryptography and Pseudo-Random Coding	205
<i>Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, Yuanlong Cai</i>	
The Wide Trail Design Strategy	222
<i>Joan Daemen, Vincent Rijmen</i>	
Undetachable Threshold Signatures	239
<i>Niklas Borselius, Chris J. Mitchell, Aaron Wilson</i>	
Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection / Correction Strategies	245
<i>Werner Schindler, François Koeune, Jean-Jacques Quisquater</i>	
Key Recovery Scheme Interoperability – A Protocol for Mechanism Negotiation	268
<i>Konstantinos Rantos, Chris J. Mitchell</i>	
Unconditionally Secure Key Agreement Protocol	277
<i>Cyril Prissette</i>	
An Efficient Stream Cipher Alpha1 for Mobile and Wireless Devices	294
<i>N. Komninos, Bahram Honary, Michael Darnell</i>	
Investigation of Linear Codes Possessing Some Extra Properties	301
<i>Viktoriya Masol</i>	
Statistical Physics of Low Density Parity Check Error Correcting Codes ..	307
<i>David Saad, Yoshiyuki Kabashima, Tatsuto Murayama, Renato Vicente</i>	
Generating Large Instances of the Gong-Harn Cryptosystem	317
<i>Kenneth J. Giuliani, Guang Gong</i>	

Lattice Attacks on RSA-Encrypted IP and TCP	329
<i>P.A. Crouch, J.H. Davenport</i>	
Spectrally Bounded Sequences, Codes, and States: Graph Constructions and Entanglement	339
<i>Matthew G. Parker</i>	
Attacking the Affine Parts of SFLASH	355
<i>Willi Geiselmann, Rainer Steinwandt, Thomas Beth</i>	
An Identity Based Encryption Scheme Based on Quadratic Residues	360
<i>Clifford Cocks</i>	
Another Way of Doing RSA Cryptography in Hardware.....	364
<i>Lejla Batina, Geeke Muurling</i>	
Distinguishing TEA from a Random Permutation: Reduced Round Versions of TEA Do Not Have the SAC or Do Not Generate Random Numbers	374
<i>Julio César Hernández, José María Sierra, Arturo Ribagorda, Benjamín Ramos, J.C. Mex-Perera</i>	
A New Search Pattern in Multiple Residue Method (MRM) and Its Importance in the Cryptanalysis of the RSA.....	378
<i>Seyed J. Tabatabaian, Sam Ikeshiro, Murat Gumussoy, Mungal S. Dhanda</i>	
A New Undeniable Signature Scheme Using Smart Cards	387
<i>Lee Jongkook, Ryu Shiryong, Kim Jeungseop, Yoo Keeyoung</i>	
Non-binary Block Inseparable Errors Control Codes	395
<i>Alexandr Y. Lev, Yuliy A. Lev, Vyacheslav N. Okhrymenko</i>	
Cryptanalysis of Nonlinear Filter Generators with {0, 1}-Metric Viterbi Decoding.....	402
<i>Sabine Leveiller, Joseph Boutros, Philippe Guillot, Gilles Zémor</i>	
Author Index	415



<http://www.springer.com/978-3-540-43026-1>

Cryptography and Coding

8th IMA International Conference Cirencester, UK,

December 17-19, 2001 Proceedings

Honary, B. (Ed.)

2001, IX, 419 p., Softcover

ISBN: 978-3-540-43026-1