

Contents

Applications of Exponential Sums in Communications Theory	1
<i>K.G. Paterson</i>	
Some Applications of Bounds for Designs to the Cryptography	25
<i>S. Nikova and V. Nikov</i>	
Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions	35
<i>E. Pasalic and T. Johansson</i>	
Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics	45
<i>E. Martínez-Moro, F.J. Galán-Simón, M.A. Borges-Trenard, and M. Borges-Quintana</i>	
A New Method for Generating Sets of Orthogonal Sequences for a Synchronous CDMA System	56
<i>H. Donelan and T. O'Farrell</i>	
New Self-Dual Codes over $GF(5)$	63
<i>S. Georgiou and C. Koukouvinos</i>	
Designs, Intersecting Families, and Weight of Boolean Functions	70
<i>E. Fiol</i>	
Coding Applications in Satellite Communication Systems	81
<i>S. McGrath</i>	
A Unified Code	84
<i>X. Liu, P. Farrell, and C. Boyd</i>	
Enhanced Image Coding for Noisy Channels	94
<i>P. Chippendale, C. Tanriover, and B. Honary</i>	
Perfectly Secure Authorization and Passive Identification for an Error Tolerant Biometric System	104
<i>G.I. Davida and Y. Frankel</i>	

An Encoding Scheme for Dual Level Access to Broadcasting Networks	114
<i>T. Amornraksa, D.R.B. Burgess, and P. Sweeney</i>	
Photograph Signatures for the Protection of Identification Documents	119
<i>B. Bellamy, J.S. Mason, and M. Ellis</i>	
An Overview of the Isoperimetric Method in Coding Theory	129
<i>J.-P. Tillich and G. Zémor</i>	
Rectangular Basis of a Linear Code	135
<i>J. Maucher, V. Sidorenko, and M. Bossert</i>	
Graph Decoding of Array Error-Correcting Codes	144
<i>P.G. Farrell and S.H. Razavi</i>	
Catastrophicity Test for Time-Varying Convolutional Encoders	153
<i>C. O'Donoghue and C. Burkley</i>	
Low Complexity Soft-Decision Sequential Decoding Using Hybrid Permutation for Reed-Solomon Codes	163
<i>M.-s. Oh and P. Sweeney</i>	
On Efficient Decoding of Alternant Codes over a Commutative Ring	173
<i>G.H. Norton and A. Sălăgean</i>	
Reduced Complexity Sliding Window BCJR Decoding Algorithms for Turbo Codes	179
<i>J. Gwak, S.K. Shin, and H.-M. Kim</i>	
Advanced Encryption Standard (AES) - An Update	185
<i>L.R. Knudsen</i>	
The Piling-Up Lemma and Dependent Random Variables	186
<i>Z. Kukorelly</i>	
A Cryptographic Application of Weil Descent	191
<i>S.D. Galbraith and N.P. Smart</i>	
Edit Probability Correlation Attack on the Bilateral Stop/Go Generator	201
<i>R. Menicocci and J.Dj. Golić</i>	

Look-Up Table Based Large Finite Field Multiplication in Memory Constrained Cryptosystems	213
<i>M.A. Hasan</i>	
On the Combined Fermat/Lucas Probable Prime Test	222
<i>S. Müller</i>	
On the Cryptanalysis of Nonlinear Sequences	236
<i>S.W. Golomb</i>	
Securing Aeronautical Telecommunications	243
<i>S. Blake-Wilson</i>	
Tensor-Based Trapdoors for CVP and Their Application to Public Key Cryptography	244
<i>R. Fischlin and J.-P. Seifert</i>	
Delegated Decryption	258
<i>Y. Mu, V. Varadharajan, and K.Q. Nguyen</i>	
Fast and Space-Efficient Adaptive Arithmetic Coding	270
<i>B. Ryabko and A. Fionov</i>	
Robust Protocol for Generating Shared RSA Parameters	280
<i>A.M. Barmawi, S. Takada, and N. Doi</i>	
Some Soft-Decision Decoding Algorithms for Reed-Solomon Codes	290
<i>S. Wesemeyer, P. Sweeney, and D.R.B. Burgess</i>	
Weaknesses in Shared RSA Key Generation Protocols	300
<i>S.R. Blackburn, S. Blake-Wilson, M. Burmester, and S.D. Galbraith</i>	
Digital Signature with Message Recovery and Authenticated Encryption (Signcryption) - A Comparison	307
<i>C.Y. Yeun</i>	
Index	313



<http://www.springer.com/978-3-540-66887-9>

Cryptography and Coding

7th IMA International Conference, Cirencester, UK,

December 20-22, 1999 Proceedings

Walker, M. (Ed.)

1999, X, 352 p., Softcover

ISBN: 978-3-540-66887-9