Contents

Applications of Exponential Sums in Communications Theory 1
K.G. Paterson

Some Applications of Bounds for Designs to the Cryptography 25
S. Nikova and V. Nikov

Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions 35
E. Pasalic and T. Johansson

Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics 45
E. Martínez-Moro, F.J. Galán-Simón, M.A. Borges-Trenard, and M. Borges-Quintana

A New Method for Generating Sets of Orthogonal Sequences for a Synchronous CDMA System 56
H. Donelan and T. O'Farrell

New Self-Dual Codes over GF(5) 63
S. Georgiou and C. Koukouvinos

Designs, Intersecting Families, and Weight of Boolean Functions 70
E. Filiol

Coding Applications in Satellite Communication Systems 81
S. McGrath

A Unified Code 84
X. Liu, P. Farrell, and C. Boyd

Enhanced Image Coding for Noisy Channels 94
P. Chippendale, C. Tanriover, and B. Honary

Perfectly Secure Authorization and Passive Identification for an Error Tolerant Biometric System 104
G.I. Davida and Y. Frankel

An Encoding Scheme for Dual Level Access to Broadcasting Networks 114
T. Amornraksa, D.R.B. Burgess, and P. Sweeney

Photograph Signatures for the Protection of Identification Documents 119
B. Bellamy, J.S. Mason, and M. Ellis

An Overview of the Isoperimetric Method in Coding Theory 129
J.-P. Tillich and G. Zémor

Rectangular Basis of a Linear Code 135
J. Maucher, V. Sidorenko, and M. Bossert

Graph Decoding of Array Error-Correcting Codes 144
P.G. Farrell and S.H. Razavi

Catastrophicity Test for Time-Varying Convolutional Encoders 153
C. O'Donoghue and C. Burkley

Low Complexity Soft-Decision Sequential Decoding Using Hybrid Permutation for Reed-Solomon Codes 163
M.-s. Oh and P. Sweeney

On Efficient Decoding of Alternant Codes over a Commutative Ring 173
G.H. Norton and A. Sălăgean

Reduced Complexity Sliding Window BCJR Decoding Algorithms for Turbo Codes 179
J. Gwak, S.K. Shin, and H.-M. Kim

Advanced Encryption Standard (AES) - An Update 185
L.R. Knudsen

The Piling-Up Lemma and Dependent Random Variables 186
Z. Kukorelly

A Cryptographic Application of Weil Descent 191
S.D. Galbraith and N.P. Smart

Edit Probability Correlation Attack on the Bilateral Stop/Go Generator 201
R. Menicocci and J.Dj. Golić

Look-Up Table Based Large Finite Field Multiplication in Memory Constrained Cryptosystems 213
M.A. Hasan

On the Combined Fermat/Lucas Probable Prime Test 222
S. Müller

On the Cryptanalysis of Nonlinear Sequences 236
S.W. Golomb

Securing Aeronautical Telecommunications 243
S. Blake-Wilson

Tensor-Based Trapdoors for CVP and Their Application to Public Key Cryptography 244
R. Fischlin and J.-P. Seifert

Delegated Decryption 258
Y. Mu, V. Varadharajan, and K.Q. Nguyen

Fast and Space-Efficient Adaptive Arithmetic Coding 270
B. Ryabko and A. Fionov

Robust Protocol for Generating Shared RSA Parameters 280
A.M. Barmawi, S. Takada, and N. Doi

Some Soft-Decision Decoding Algorithms for Reed-Solomon Codes 290
S. Wesemeyer, P. Sweeney, and D.R.B. Burgess

Weaknesses in Shared RSA Key Generation Protocols 300
S.R. Blackburn, S. Blake-Wilson, M. Burmester, and S.D. Galbraith

Digital Signature with Message Recovery and Authenticated Encryption (Signcryption) - A Comparison 307
C.Y. Yeun

Index 313