

CONTENTS

Keeping Secrets a Personal Matter or the Exponential Security System by T. Beth	1
Review of Coding Techniques for Parallel Asynchronous Communications by M. Blaum and J. Bruck	11
Multisignatures Revisited by C. Boyd	21
Coding Schemes for Two-dimensional Position Sensing by J. Burns and C. J. Mitchell	31
Design of Orthogonal Sequences: A Geometric Approach by A. G. Burr	67
Using Genetic Algorithms to Search for Binary Sequences with Large Merit Factor by W. Crompton and N. M. Stephens	83
Orientable Sequences by Z.-D. Dai, K. M. Martin, M. J. B. Robshaw and P. R. Wild	97
Improved Bounds for the Rabin Primality Test by I. Damgård and P. Landrock	117
Multi-Functionality and its Application in Digital Communication System Design by M. Darnell and B. Honary	129
An In-Band CDMA System Employing Sequence Segment Keying by M. Darnell and T. E. Miller	151
A New Approach to the Design of Codes for the Binary Adder Channel by V. C. da Rocha, Jr and J. L. Massey	179
Duality and Normal Basis Multiplication by W. Geiselmann and D. Gollmann	187
Transformation Matrices of Clock-controlled Shift Registers by D. Gollmann	197

Minimisation of Error Multiplication for M-ary Signals by B. Honary and G. Markarian	211
Cryptanalysis of LOKI by L. Ramkilde Knudsen	223
Finding the Position of a Subarray in a Pseudo-Random Array by S. Lloyd and J. Burns	237
Untrustworthy Participants in Perfect Secret Sharing Schemes by K. M. Martin	255
Randomness Properties of Two Chaotic Mappings by A. McGrail	265
Recurrent Sequences Modulo Prime Powers by R. G. E. Pinch	297
Digital Signatures: RSA or El Gamal? by F. Piper and N. Stephens	311
Error Control Codes with In-band Spectral Nulls by A. Popplewell and J. J. O'Reilly	321
On Encoding and Decoding of the Codes from Hermitian Curves by B.-Z. Shen	337
The Genetic Code by R. J. Slater	359
On the Construction of Majority-Logic Decodable Group Codes by K.-H. Zimmermann	367