

CONTENTS

Preface	v
Organizing Committees	vii
Fuzzy Identity-based Encryption: New and Efficient Schemes <i>J. Baek, W. Susilo and J. Zhou</i>	1
A Functional View of Upper Bounds on Codes <i>A. Barg and D. Nogin</i>	15
A Method of Construction of Balanced Functions with Optimum Algebraic Immunity <i>C. Carlet</i>	25
Enumeration of a Class of Sequences Generated by Inversions <i>A. Çeşemlioğlu, W. Meidl and A. Topuzoğlu</i>	44
A Critical Look at Cryptographic Hash Function Literature <i>S. Contini, R. Steinfeld, J. Pieprzyk and K. Matusiewicz</i>	58
Scalable Optimal Test Patterns for Crosstalk-induced Faults on Deep Submicron Global Interconnects <i>Y. M. Chee and C. J. Colbourn</i>	80
An Improved Distinguisher for Dragon <i>J. Y. Cho and J. Pieprzyk</i>	91
Constructing Perfect Hash Families Using a Greedy Algorithm <i>C. J. Colbourn</i>	109
Two-Weight Codes Punctured from Irreducible Cyclic Codes	119

C. Ding, J. Luo and H. Niederreiter

On the Joint Linear Complexity of Linear Recurring Multisequences	125
<i>F. Fu, H. Niederreiter and F. Özbudak</i>	
Research on P2P Worn Detection Based on Information Correlation-PWDIC	143
<i>H. Hu, J. Zhang, F. Xiao and B. Liu</i>	
On the Relation among Various Security Models for Certificateless Cryptography	154
<i>Q. Huang and D. S. Wong</i>	
Distance-Preserving Mappings	171
<i>T. Kløve</i>	
Single Cycle Invertible Function and its Cryptographic Applications	183
<i>C. Li, B. Sun and Q. Dai</i>	
Concurrent Signatures without a Conventional Keystone	196
<i>Y. Mu, D. S. Wong, L. Chen, W. Susilo and Q. Wu</i>	
Authentication Codes in the Query Model	214
<i>R. Safavi-Naini, D. Tonien and P. R. Wild</i>	
Collision in the DSA Function	226
<i>I. E. Shparlinski and R. Steinfeld</i>	
The Current Status in Design of Efficient Provably Secure Cryptographic Pseudorandom Generators	233
<i>R. Steinfeld</i>	
The Successive Minima Profile of Multisequences	256
<i>L. Wang and H. Niederreiter</i>	
A Construction of Optimal Sets of FH Sequences	268
<i>J. Yin</i>	
Author Index	277