

Table of Contents

A Signature Scheme with Efficient Proof of Validity	1
<i>Masayuki Abe and Miyako Ohkubo</i>	
Secret-Sharing Schemes: A Survey.....	11
<i>Amos Beimel</i>	
Lattice Codes for the Gaussian Wiretap Channel.....	47
<i>Jean-Claude Belfiore, Frédérique Oggier, and Patrick Solé</i>	
List Decoding for Binary Goppa Codes	62
<i>Daniel J. Bernstein</i>	
Faster 2-Regular Information-Set Decoding.....	81
<i>Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe</i>	
Ideal Secret Sharing Schemes for Useful Multipartite Access Structures	99
<i>Oriol Farràs and Carles Padró</i>	
Loiss: A Byte-Oriented Stream Cipher	109
<i>Dengguo Feng, Xiutao Feng, Wentao Zhang, Xiubin Fan, and Chuankun Wu</i>	
Secure Message Transmission by Public Discussion: A Brief Survey	126
<i>Juan Garay, Clint Givens, and Rafail Ostrovsky</i>	
Variations on Encoding Circuits for Stabilizer Quantum Codes.....	142
<i>Markus Grassl</i>	
Algorithms for the Shortest and Closest Lattice Vector Problems.....	159
<i>Guillaume Hanrot, Xavier Pujol, and Damien Stehlé</i>	
An Experiment of Number Field Sieve over $GF(p)$ of Low Hamming Weight Characteristic	191
<i>Kenichiro Hayasaka and Tsuyoshi Takagi</i>	
The Minimum Distance of Graph Codes	201
<i>Tom Høholdt and Jørn Justesen</i>	
Local Duality and the Discrete Logarithm Problem.....	213
<i>Ming-Deh Huang</i>	
On the Effects of Pirate Evolution on the Design of Digital Content Distribution Systems	223
<i>Aggelos Kiayias</i>	

VIII Table of Contents

Arithmetic of Split Kummer Surfaces: Montgomery Endomorphism of Edwards Products	238
<i>David Kohel</i>	
A New Family of Quadriphase Sequences with Low Correlation	246
<i>Jie Li, Xiangyong Zeng, and Lei Hu</i>	
On the Link of Some Semi-bent Functions with Kloosterman Sums	263
<i>Sihem Mesnager and Gérard Cohen</i>	
Locally Decodable Codes: A Brief Survey	273
<i>Sergey Yekhanin</i>	
On Relationship of Computational Diffie-Hellman Problem and Computational Square-Root Exponent Problem	283
<i>Fanguo Zhang and Ping Wang</i>	
Author Index	295