

Table of Contents

Cryptanalysis of Multivariate Systems

Properties of the Discrete Differential with Cryptographic Applications.....	1
<i>Daniel Smith-Tone</i>	
Growth of the Ideal Generated by a Quadratic Boolean Function.....	13
<i>Jintai Ding, Timothy J. Hodges, and Victoria Kruglov</i>	
Mutant Zhuang-Zi Algorithm.....	28
<i>Jintai Ding and Dieter S. Schmidt</i>	
Cryptanalysis of Two Quartic Encryption Schemes and One Improved MFE Scheme.....	41
<i>Weimei Cao, Xiuyun Nie, Lei Hu, Xiling Tang, and Jintai Ding</i>	

Cryptanalysis of Code-Based Systems

Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes.....	61
<i>Christian Wieschebrink</i>	
Grover vs. McEliece.....	73
<i>Daniel J. Bernstein</i>	
Information-Set Decoding for Linear Codes over $\mathbf{F}_q$	81
<i>Christiane Peters</i>	
A Timing Attack against the Secret Permutation in the McEliece PKC.....	95
<i>Falko Strenzke</i>	
Practical Power Analysis Attacks on Software Implementations of McEliece.....	108
<i>Stefan Heyse, Amir Moradi, and Christof Paar</i>	

Design of Encryption Schemes

Key Exchange and Encryption Schemes Based on Non-commutative Skew Polynomials.....	126
<i>Delphine Boucher, Philippe Gaborit, Willi Geiselmann, Olivier Ruatta, and Felix Ulmer</i>	

Designing a Rank Metric Based McEliece Cryptosystem	142
<i>Pierre Loidreau</i>	
Secure Variants of the Square Encryption Scheme	153
<i>Crystal Lee Clough and Jintai Ding</i>	
Low-Reiter: Niederreiter Encryption Scheme for Embedded Microcontrollers	165
<i>Stefan Heyse</i>	

Design of Signature Schemes

Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles	182
<i>Markus Rückert</i>	
Proposal of a Signature Scheme Based on STS Trapdoor	201
<i>Shigeo Tsujii, Masahito Gotaishi, Kohtaro Tadaki, and Ryo Fujita</i>	
Selecting Parameters for the Rainbow Signature Scheme	218
<i>Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann</i>	
Author Index	241