

Table of Contents

General Fault Attacks on Multivariate Public Key Cryptosystems	1
<i>Yasufumi Hashimoto, Tsuyoshi Takagi, and Kouichi Sakurai</i>	
Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies	19
<i>David Jao and Luca De Feo</i>	
Full Cryptanalysis of the Chen Identification Protocol	35
<i>Philippe Gaborit, Julien Schrek, and Gilles Zémor</i>	
Decoding One Out of Many	51
<i>Nicolas Sendrier</i>	
On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack	68
<i>Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari</i>	
Roots of Square: Cryptanalysis of Double-Layer Square and Square+ . . .	83
<i>Enrico Thomae and Christopher Wolf</i>	
An Efficient Attack on All Concrete KKS Proposals	98
<i>Ayoub Otmani and Jean-Pierre Tillich</i>	
XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions	117
<i>Johannes Buchmann, Erik Dahmen, and Andreas Hülsing</i>	
On the Differential Security of Multivariate Public Key Cryptosystems	130
<i>Daniel Smith-Tone</i>	
Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices	143
<i>Stefan Heyse</i>	
Efficient Threshold Encryption from Lossy Trapdoor Functions	163
<i>Xiang Xie, Rui Xue, and Rui Zhang</i>	
Monoidic Codes in Cryptography	179
<i>Paulo S.L.M. Barreto, Richard Lindner, and Rafael Misoczki</i>	
Simplified High-Speed High-Distance List Decoding for Alternant Codes	200
<i>Daniel J. Bernstein</i>	

Statistical Decoding of Codes over $\mathbb{F}_q$	217
<i>Robert Niebuhr</i>	
High-Speed Hardware Implementation of Rainbow Signature on FPGAs	228
<i>Shaohua Tang, Haibo Yi, Jintai Ding, Huan Chen, and Guomin Chen</i>	
Wild McEliece Incognito	244
<i>Daniel J. Bernstein, Tanja Lange, and Christiane Peters</i>	
A New Spin on Quantum Cryptography: Avoiding Trapdoors and Embracing Public Keys	255
<i>Lawrence M. Ioannou and Michele Mosca</i>	
A Security Analysis of Uniformly-Layered Rainbow: Revisiting Sato-Araki's Non-commutative Approach to Ong-Schnorr-Shamir Signature towards PostQuantum Paradigm	275
<i>Takanori Yasuda and Kouichi Sakurai</i>	
Author Index	295