

Table of Contents

Encryption

Broadcast Encryption with Multiple Trust Authorities	1
<i>Kent D. Boklan, Alexander W. Dent, and Christopher A. Seaman</i>	
Security of Sequential Multiple Encryption	20
<i>Atsushi Fujioka, Yoshiaki Okamoto, and Taichi Saito</i>	
Mediated Traceable Anonymous Encryption	40
<i>Malika Izabachène, David Pointcheval, and Damien Vergnaud</i>	

Elliptic Curves

Starfish on Strike	61
<i>Daniel J. Bernstein, Peter Birkner, and Tanja Lange</i>	
Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves	81
<i>Pierre-Alain Fouque and Mehdi Tibouchi</i>	

Implementation of Pairings

Fixed Argument Pairings	92
<i>Craig Costello and Douglas Stebila</i>	
New Software Speed Records for Cryptographic Pairings	109
<i>Michael Naehrig, Ruben Niederhagen, and Peter Schwabe</i>	

Implementation of Cryptographic Algorithms

Accelerating Lattice Reduction with FPGAs	124
<i>Jérémie Detrey, Guillaume Hanrot, Xavier Pujol, and Damien Stehlé</i>	
Efficient Software Implementation of Binary Field Arithmetic Using Vector Instruction Sets	144
<i>Diego F. Aranha, Julio López, and Darrel Hankerson</i>	

Cryptographic Protocols and Foundations

Communication Optimal Multi-valued Asynchronous Broadcast Protocol	162
<i>Arpita Patra and C. Pandu Rangan</i>	

On the Impossibility of Batch Update for Cryptographic Accumulators	178
<i>Philippe Camacho and Alejandro Hevia</i>	
On the Round Complexity of Zero-Knowledge Proofs Based on One-Way Permutations	189
<i>S. Dov Gordon, Hoeteck Wee, David Xiao, and Arkady Yerukhimovich</i>	
Cryptanalysis of Symmetric Primitives	
Message Recovery and Pseudo-preimage Attacks on the Compression Function of Hamsi-256	205
<i>Çağdaş Çalık and Meltem Sönmez Turan</i>	
Generic Attacks on Misty Schemes	222
<i>Valérie Nachev, Jacques Patarin, and Joana Treger</i>	
Post-Quantum Cryptography	
Cryptanalysis of the Hidden Matrix Cryptosystem	241
<i>Jean-Charles Faugère, Antoine Joux, Ludovic Perret, and Joana Treger</i>	
A Lattice-Based Threshold Ring Signature Scheme	255
<i>Pierre-Louis Cayrel, Richard Lindner, Markus Rückert, and Rosemberg Silva</i>	
Side-Channel Attacks	
Defeating Any Secret Cryptography with SCARE Attacks	273
<i>Sylvain Guilley, Laurent Sauvage, Julien Micolod, Denis Réal, and Frédéric Valette</i>	
How Leaky Is an Extractor?	294
<i>François-Xavier Standaert</i>	
Combined Implementation Attack Resistant Exponentiation	305
<i>Jörn-Marc Schmidt, Michael Tunstall, Roberto Avanzi, Ilya Kizhvatov, Timo Kasper, and David Oswald</i>	
Author Index	323