

Table of Contents

Protocols

Secure Outsourced Computation	1
<i>Jake Loftus and Nigel P. Smart</i>	
Fully Simulatable Quantum-Secure Coin-Flipping and Applications	21
<i>Carolin Lunemann and Jesper Buus Nielsen</i>	
Efficient and Secure Generalized Pattern Matching via Fast Fourier Transform	41
<i>Damien Vergnaud</i>	
Identification Schemes from Key Encapsulation Mechanisms	59
<i>Hiroaki Anada and Seiko Arita</i>	

Cryptanalysis

Attacking Bivium and Trivium with the Characteristic Set Method	77
<i>Zhenyu Huang and Dongdai Lin</i>	
Improved Cryptanalysis of the Multi-Prime Φ -Hiding Assumption	92
<i>Mathias Herrmann</i>	
FPGA Implementation of a Statistical Saturation Attack against PRESENT	100
<i>Stéphanie Kerckhof, Baudoin Collard, and François-Xavier Standaert</i>	
Collisions of MMO-MD5 and Their Impact on Original MD5	117
<i>Yu Sasaki</i>	

Secret-Key Cryptography

Really Fast Syndrome-Based Hashing	134
<i>Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe</i>	
Montgomery's Trick and Fast Implementation of Masked AES	153
<i>Laurie Genelle, Emmanuel Prouff, and Michaël Quisquater</i>	

Efficient Implementations

Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation	170
<i>Michael Hutter, Marc Joye, and Yannick Sierra</i>	
Efficient Multiplication in Finite Field Extensions of Degree 5	188
<i>Nadia El Mrabet, Aurore Guillevic, and Sorina Ionica</i>	

Cryptographic Schemes

Achieving Optimal Anonymity in Transferable E-Cash with a Judge	206
<i>Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré</i>	
Revocable Attribute-Based Signatures with Adaptive Security in the Standard Model	224
<i>Alex Escala, Javier Herranz, and Paz Morillo</i>	

Algorithmic Problems

Using the Inhomogeneous Simultaneous Approximation Problem for Cryptographic Design	242
<i>Frederik Armknecht, Carsten Elsner, and Martin Schmidt</i>	
Analyzing Standards for RSA Integers	260
<i>Daniel Loebenberger and Michael Nüsken</i>	

Elliptic Curves

Hashing into Hessian Curves	278
<i>Reza Rezaeian Farashahi</i>	
On Randomness Extraction in Elliptic Curves	290
<i>Abdoul Aziz Ciss and Djiby Sow</i>	

Fault Analysis

Fault Analysis of Grain-128 by Targeting NFSR	298
<i>Sandip Karmakar and Dipanwita Roy Chowdhury</i>	
Differential Fault Analysis of Sosemanuk	316
<i>Yaser Esmaeili Salehani, Aleksandar Kircanski, and Amr Youssef</i>	
An Improved Differential Fault Analysis on AES-256	332
<i>Subidh Ali and Debdeep Mukhopadhyay</i>	

Security Proofs

Benaloh's Dense Probabilistic Encryption Revisited	348
<i>Laurent Fousse, Pascal Lafourcade, and Mohamed Alnuaimi</i>	
On the Security of the Winternitz One-Time Signature Scheme	363
<i>Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Hülsing, and Markus Rückert</i>	

Invited Talks

Efficient Zero-Knowledge Proofs (Abstract)	379
<i>Jens Groth</i>	
Some Key Techniques on Pairing Vector Spaces	380
<i>Tatsuaki Okamoto and Katsuyuki Takashima</i>	
The NIST SHA-3 Competition: A Perspective on the Final Year	383
<i>Bart Preneel</i>	
Author Index	387