

Table of Contents

Post-Quantum Cryptology

Secure Parameters for SWIFFT	1
<i>Johannes Buchmann and Richard Lindner</i>	
FSBday: Implementing Wagner's Generalized Birthday Attack against the SHA-3 Round-1 Candidate FSB	18
<i>Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen, Christiane Peters, and Peter Schwabe</i>	

Key Agreement Protocols

Reusing Static Keys in Key Agreement Protocols	39
<i>Sanjit Chatterjee, Alfred Menezes, and Berkant Ustaoglu</i>	
A Study of Two-Party Certificateless Authenticated Key-Agreement Protocols	57
<i>Colleen Swanson and David Jao</i>	

Side Channel Attacks

Fault Analysis of Rabbit: Toward a Secret Key Leakage	72
<i>Alexandre Berzati, Cécile Canovas-Dumas, and Louis Goubin</i>	
On Physical Obfuscation of Cryptographic Algorithms	88
<i>Julien Bringer, Hervé Chabanne, and Thomas Icart</i>	
Cache Timing Attacks on Clefia	104
<i>Chester Rebeiro, Debdeep Mukhopadhyay, Junko Takahashi, and Toshinori Fukunaga</i>	

Symmetric Cryptology

Software Oriented Stream Ciphers Based upon FCSRs in Diversified Mode	119
<i>Thierry P. Berger, Marine Minier, and Benjamin Pousse</i>	
On the Symmetric Negabent Boolean Functions	136
<i>Sumanta Sarkar</i>	
Improved Meet-in-the-Middle Attacks on AES	144
<i>Hüseyin Demirci, İhsan Taşkın, Mustafa Çoban, and Adnan Baysal</i>	

Hash Functions

Related-Key Rectangle Attack of the Full HAS-160 Encryption Mode... 157
Orr Dunkelman, Ewan Fleischmann, Michael Gorski, and Stefan Lucks

Second Preimage Attack on SHAMATA-512 169
Kota Ideguchi and Dai Watanabe

Towards Secure and Practical MACs for Body Sensor Networks 182
Zheng Gong, Pieter Hartel, Svetla Nikova, and Bo Zhu

Indifferentiability Characterization of Hash Functions and Optimal
Bounds of Popular Domain Extensions..... 199
Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi

A Distinguisher for the Compression Function of SIMD-512 219
Florian Mendel and Tomislav Nad

Number Theoretic Cryptology

Sampling from Signed Quadratic Residues: RSA Group Is Pseudofree... 233
Mahabir Prasad Jhanwar and Rana Barua

Software Implementation of Pairing-Based Cryptography on Sensor
Networks Using the MSP430 Microcontroller 248
Conrado Porto Lopes Gouvêa and Julio López

A New Hard-Core Predicate of Paillier’s Trapdoor Function 263
Dong Su and Kewei Lv

Lightweight Cryptology

Private Interrogation of Devices via Identification Codes 272
Julien Bringer, Hervé Chabanne, Gérard Cohen, and Bruno Kindarji

RFID Distance Bounding Multistate Enhancement 290
Gildas Avoine, Christian Floerkemeier, and Benjamin Martin

Two Attacks against the F_f RFID Protocol 308
Olivier Billet and Kaoutar Elkhiyaoui

Signature Protocols

Efficient Constructions of Signcryption Schemes and Signcryption
Composability 321
Takahiro Matsuda, Kanta Matsuura, and Jacob C.N. Schuldt

On Generic Constructions of Designated Confirmer Signatures: The “Encryption of a Signature” Paradigm Revisited	343
<i>Laila El Aimani</i>	
Verifiably Encrypted Signatures from RSA without NIZKs	363
<i>Markus Rückert</i>	
Identity Based Aggregate Signcryption Schemes	378
<i>S. Sharmila Deva Selvi, S. Sree Vivek, J. Shriram, S. Kalaivani, and C. Pandu Rangan</i>	
Multiparty Computation	
Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience	398
<i>Arpita Patra, Ashish Choudhary, and C. Pandu Rangan</i>	
Non-committing Encryptions Based on Oblivious Naor-Pinkas Cryptosystems	418
<i>Huafei Zhu and Feng Bao</i>	
Oblivious Multi-variate Polynomial Evaluation	430
<i>Gérald Gavin and Marine Minier</i>	
Author Index	443