

Table of Contents

Invited Papers

How to Compute on Encrypted Data	1
<i>Vinod Vaikuntanathan</i>	
From Multiple Encryption to Knapsacks – Efficient Dissection of Composite Problems	16
<i>Orr Dunkelman</i>	
Using the Cloud to Determine Key Strengths	17
<i>Thorsten Kleinjung, Arjen K. Lenstra, Dan Page, and Nigel P. Smart</i>	

Protocol

A Unified Characterization of Completeness and Triviality for Secure Function Evaluation	40
<i>Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek</i>	
On the Non-malleability of the Fiat-Shamir Transform	60
<i>Sebastian Faust, Markulf Kohlweiss, Giorgia Azzurra Marson, and Daniele Venturi</i>	
Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84	80
<i>Arpita Maitra and Goutam Paul</i>	
On-Line/Off-Line Leakage Resilient Secure Computation Protocols	100
<i>Chaya Ganesh, Vipul Goyal, and Satya Lokam</i>	

Side Channel

Leakage Squeezing of Order Two	120
<i>Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Maghrebi</i>	
ROSETTA for Single Trace Analysis: Recovery Of Secret Exponent by Triangular Trace Analysis	140
<i>Christophe Clavier, Benoit Feix, Georges Gagnerot, Christophe Giraud, Mylène Roussellet, and Vincent Verneuil</i>	

Hash Functions and Stream Cipher

Collision Attack on the Hamsi-256 Compression Function 156
Mario Lamberger, Florian Mendel, and Vincent Rijmen

Generalized Iterated Hash Functions Revisited: New Complexity Bounds
for Multicollision Attacks 172
Tuomas Kortelainen, Ari Vesanen, and Juha Kortelainen

A Differential Fault Attack on the Grain Family under Reasonable
Assumptions 191
Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar

Cryptanalysis of Pseudo-random Generators Based on Vectorial
FCSRs 209
Thierry P. Berger and Marine Minier

Cryptanalysis of Block Ciphers

Faster Chosen-Key Distinguishers on Reduced-Round AES 225
Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean

The Higher-Order Meet-in-the-Middle Attack and Its Application to
the Camellia Block Cipher (Extended Abstract) 244
Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic

Double-SP Is Weaker Than Single-SP: Rebound Attacks on Feistel
Ciphers with Several Rounds 265
Yu Sasaki

Automatic Search of Truncated Impossible Differentials for
Word-Oriented Block Ciphers 283
Shengbao Wu and Mingsheng Wang

Time Memory Trade-Off

High-Speed Parallel Implementations of the Rainbow Method in a
Heterogeneous System 303
*Jung Woo Kim, Jungjoo Seo, Jin Hong, Kunsoo Park, and
Sung-Ryul Kim*

Computing Small Discrete Logarithms Faster 317
Daniel J. Bernstein and Tanja Lange

Hardware

Embedded Syndrome-Based Hashing 339
Ingo von Maurich and Tim Güneysu

Compact Hardware Implementations of the Block Ciphers mCrypton, NOEKEON, and SEA	358
<i>Thomas Plos, Christoph Dobraunig, Markus Hofinger, Alexander Oprisnik, Christoph Wiesmeier, and Johannes Wiesmeier</i>	

Elliptic Curve

Efficient Arithmetic on Elliptic Curves in Characteristic 2	378
<i>David Kohel</i>	
A New Model of Binary Elliptic Curves	399
<i>Hongfeng Wu, Chunming Tang, and Rongquan Feng</i>	
Analysis of Optimum Pairing Products at High Security Levels	412
<i>Xusheng Zhang and Dongdai Lin</i>	
Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian	431
<i>Robert Drylo</i>	

Digital Signature

Faster Batch Forgery Identification	454
<i>Daniel J. Bernstein, Jeroen Doumen, Tanja Lange, and Jan-Jaap Oosterwijk</i>	
Implementing CFS	474
<i>Gregory Landais and Nicolas Sendrier</i>	

Symmetric Key Design and Provable Security

SipHash: A Fast Short-Input PRF	489
<i>Jean-Philippe Aumasson and Daniel J. Bernstein</i>	
A Novel Permutation-Based Hash Mode of Operation FP and the Hash Function SAMOSA	509
<i>Souradyuti Paul, Ekawat Homsirikamol, and Kris Gaj</i>	
Resistance against Adaptive Plaintext-Ciphertext Iterated Distinguishers	528
<i>Asli Bay, Atefeh Mashatan, and Serge Vaudenay</i>	
Sufficient Conditions on Padding Schemes of Sponge Construction and Sponge-Based Authenticated-Encryption Scheme	545
<i>Donghoon Chang</i>	

Author Index	565
--------------------	-----