

Table of Contents

Hash Attacks

Rotational Rebound Attacks on Reduced Skein	1
<i>Dmitry Khovratovich, Ivica Nikolić, and Christian Rechberger</i>	
Finding Second Preimages of Short Messages for Hamsi-256	20
<i>Thomas Fuhr</i>	
Non-full-active Super-Sbox Analysis: Applications to ECHO and Grøstl	38
<i>Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta</i>	
Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2	56
<i>Jian Guo, San Ling, Christian Rechberger, and Huaxiong Wang</i>	
Collision Attacks against the Knudsen-Preneel Compression Functions	76
<i>Onur Özen and Martijn Stam</i>	

Symmetric-Key Cryptosystems

Improved Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions	94
<i>Emmanuel Volte, Valérie Nachez, and Jacques Patarin</i>	
The World Is Not Enough: Another Look on Second-Order DPA	112
<i>François-Xavier Standaert, Nicolas Veyrat-Charvillon, Elisabeth Oswald, Benedikt Gierlichs, Marcel Medwed, Markus Kasper, and Stefan Mangard</i>	

Block and Stream Ciphers

Conditional Differential Cryptanalysis of NLFSR-Based Cryptosystems	130
<i>Simon Knellwolf, Willi Meier, and María Naya-Plasencia</i>	
A Byte-Based Guess and Determine Attack on SOSEMANUK	146
<i>Xiutao Feng, Jun Liu, Zhaocun Zhou, Chuankun Wu, and Dengguo Feng</i>	
Improved Single-Key Attacks on 8-Round AES-192 and AES-256	158
<i>Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	

Protocols

Constant-Size Commitments to Polynomials and Their Applications 177
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg

Computationally Secure Pattern Matching in the Presence of Malicious
Adversaries 195
Carmit Hazay and Tomas Toft

Linear-Complexity Private Set Intersection Protocols Secure in
Malicious Model 213
Emiliano De Cristofaro, Jihye Kim, and Gene Tsudik

Key Exchange

Generic Compilers for Authenticated Key Exchange 232
Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk

A Forward-Secure Symmetric-Key Derivation Protocol: How to Improve
Classical DUKPT 250
Eric Brier and Thomas Peyrin

Foundation

Efficient String-Commitment from Weak Bit-Commitment 268
Kai-Min Chung, Feng-Hao Liu, Chi-Jen Lu, and Bo-Yin Yang

On the Static Diffie-Hellman Problem on Elliptic Curves over Extension
Fields 283
Robert Granger

Random Oracles with(out) Programmability 303
*Marc Fischlin, Anja Lehmann, Thomas Ristenpart,
Thomas Shrimpton, Martijn Stam, and Stefano Tessaro*

Zero-Knowledge

Short Pairing-Based Non-interactive Zero-Knowledge Arguments 321
Jens Groth

Short Non-interactive Zero-Knowledge Proofs 341
Jens Groth

Optimistic Concurrent Zero Knowledge 359
Alon Rosen and abhi shelat

Lattice-Based Cryptography

Faster Fully Homomorphic Encryption	377
<i>Damien Stehlé and Ron Steinfeld</i>	
A Group Signature Scheme from Lattice Assumptions	395
<i>S. Dov Gordon, Jonathan Katz, and Vinod Vaikuntanathan</i>	
Lattice-Based Blind Signatures	413
<i>Markus Rückert</i>	

Secure Communication and Computation

The Round Complexity of Verifiable Secret Sharing: The Statistical Case	431
<i>Ranjit Kumaresan, Arpita Patra, and C. Pandu Rangan</i>	
General Perfectly Secure Message Transmission Using Linear Codes	448
<i>Qiushi Yang and Yvo Desmedt</i>	
On Invertible Sampling and Adaptive Security	466
<i>Yuval Ishai, Abishek Kumarasubramanian, Claudio Orlandi, and Amit Sahai</i>	
Multiparty Computation for Modulo Reduction without Bit-Decomposition and a Generalization to Bit-Decomposition	483
<i>Chao Ning and Qiuliang Xu</i>	

Models, Notions, and Assumptions

A Closer Look at Anonymity and Robustness in Encryption Schemes ...	501
<i>Payman Mohassel</i>	
Limitations on Transformations from Composite-Order to Prime-Order Groups: The Case of Round-Optimal Blind Signatures	519
<i>Sarah Meiklejohn, Hovav Shacham, and David Mandell Freeman</i>	
The Semi-Generic Group Model and Applications to Pairing-Based Cryptography	539
<i>Tibor Jager and Andy Rupp</i>	

Public-Key Encryption

The Degree of Regularity of HFE Systems	557
<i>Vivien Dubois and Nicolas Gama</i>	
Structured Encryption and Controlled Disclosure	577
<i>Melissa Chase and Seny Kamara</i>	

Leakage Resilient ElGamal Encryption 595
 Eike Kiltz and Krzysztof Pietrzak

Efficient Public-Key Cryptography in the Presence of Key Leakage 613
 *Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and
 Daniel Wichs*

Author Index 633