

Contents – Part I

Provable Security for Symmetric Cryptography

Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security	3
<i>Viet Tung Hoang and Stefano Tessaro</i>	
Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers.	33
<i>Thomas Peyrin and Yannick Seurin</i>	
XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees.	64
<i>Bart Mennink</i>	
Indifferentiability of 8-Round Feistel Networks.	95
<i>Yuanxi Dai and John Steinberger</i>	
EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC.	121
<i>Benoît Cogliati and Yannick Seurin</i>	

Asymmetric Cryptography and Cryptanalysis I

A Subfield Lattice Attack on Overstretched NTRU Assumptions: Cryptanalysis of Some FHE and Graded Encoding Schemes.	153
<i>Martin Albrecht, Shi Bai, and Léoucas</i>	
A Practical Cryptanalysis of the Algebraic Eraser	179
<i>Adi Ben-Zvi, Simon R. Blackburn, and Boaz Tsaban</i>	
Lattice-Based Fully Dynamic Multi-key FHE with Short Ciphertexts.	190
<i>Zvika Brakerski and Renen Perlman</i>	
Cryptography with Auxiliary Input and Trapdoor from Constant-Noise LPN	214
<i>Yu Yu and Jiang Zhang</i>	

Cryptography in Theory and Practice

The Multi-user Security of Authenticated Encryption: AES-GCM in TLS 1.3.	247
<i>Mihir Bellare and Björn Tackmann</i>	

A Modular Treatment of Cryptographic APIs: The Symmetric-Key Case	277
<i>Thomas Shrimpton, Martijn Stam, and Bogdan Warinschi</i>	

Encryption Switching Protocols	308
<i>Geoffroy Couteau, Thomas Peters, and David Pointcheval</i>	

Compromised Systems

Message Transmission with Reverse Firewalls—Secure Communication on Corrupted Machines	341
<i>Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz</i>	

Big-Key Symmetric Encryption: Resisting Key Exfiltration	373
<i>Mihir Bellare, Daniel Kane, and Phillip Rogaway</i>	

Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results	403
<i>Jean Paul Degabriele, Kenneth G. Paterson, Jacob C.N. Schuldt, and Joanne Woodage</i>	

Symmetric Cryptanalysis

A 2^{70} Attack on the Full MISTY1	435
<i>Achiya Bar-On and Nathan Keller</i>	

Cryptanalysis of the FLIP Family of Stream Ciphers	457
<i>Sébastien Duval, Virginie Lallemand, and Yann Rotella</i>	

Crypto 2016 Award Papers

The Magic of ELF's	479
<i>Mark Zhandry</i>	

Breaking the Circuit Size Barrier for Secure Computation Under DDH	509
<i>Elette Boyle, Niv Gilboa, and Yuval Ishai</i>	

Algorithmic Number Theory

Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case	543
<i>Taechan Kim and Razvan Barbulescu</i>	

Efficient Algorithms for Supersingular Isogeny Diffie-Hellman	572
<i>Craig Costello, Patrick Longa, and Michael Naehrig</i>	

Symmetric Primitives

New Insights on AES-Like SPN Ciphers	605
<i>Bing Sun, Meicheng Liu, Jian Guo, Longjiang Qu, and Vincent Rijmen</i>	
Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices . . .	625
<i>Christof Beierle, Thorsten Kranz, and Gregor Leander</i>	
Another View of the Division Property	654
<i>Christina Boura and Anne Canteaut</i>	
Author Index	683