

Contents – Part I

Lattice-Based Cryptography

Sieving for Shortest Vectors in Lattices Using Angular Locality-Sensitive Hashing	3
<i>Thijs Laarhoven</i>	
Coded-BKW: Solving LWE Using Lattice Codes	23
<i>Qian Guo, Thomas Johansson, and Paul Stankovski</i>	
An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices	43
<i>Paul Kirchner and Pierre-Alain Fouque</i>	
Provably Weak Instances of Ring-LWE	63
<i>Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange</i>	

Cryptanalytic Insights

Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis	95
<i>Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda Alkhzaimi, and Chao Li</i>	
On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure.	116
<i>Alex Biryukov and Léo Perrin</i>	
Capacity and Data Complexity in Multidimensional Linear Attack	141
<i>Jialin Huang, Serge Vaudenay, Xuejia Lai, and Kaisa Nyberg</i>	
Observations on the SIMON Block Cipher Family	161
<i>Stefan Kölbl, Gregor Leander, and Tyge Tiessen</i>	

Modes and Constructions

Tweaking Even-Mansour Ciphers	189
<i>Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin</i>	
Multi-key Security: The Even-Mansour Construction Revisited	209
<i>Nicky Mouha and Atul Luykx</i>	

Reproducible Circularly-Secure Bit Encryption: Applications
and Realizations 224
Mohammad Hajiabadi and Bruce M. Kapron

Multilinear Maps and IO

Zeroizing Without Low-Level Zeroes: New MMAP Attacks
and Their Limitations 247
*Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrede Lepoint,
Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai,
and Mehdi Tibouchi*

New Multilinear Maps Over the Integers 267
Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi

Constant-Round Concurrent Zero-Knowledge from Indistinguishability
Obfuscation 287
Kai-Min Chung, Huijia Lin, and Rafael Pass

Indistinguishability Obfuscation from Compact Functional Encryption 308
Prabhanjan Ananth and Abhishek Jain

Pseudorandomness

Efficient Pseudorandom Functions via On-the-Fly Adaptation 329
Nico Döttling and Dominique Schröder

The Iterated Random Permutation Problem with Applications
to Cascade Encryption 351
Brice Minaud and Yannick Seurin

The Exact PRF Security of Truncation: Tight Bounds for Keyed Sponges
and Truncated CBC 368
Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro

An Algebraic Framework for Pseudorandom Functions and Applications
to Related-Key Security 388
Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue

Block Cipher Cryptanalysis

Integral Cryptanalysis on Full MISTY1 413
Yosuke Todo

New Attacks on Feistel Structures with Improved Memory Complexities 433
Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir

Known-Key Distinguisher on Full PRESENT	455
<i>Céline Blondeau, Thomas Peyrin, and Lei Wang</i>	
Key-Recovery Attack on the ASASA Cryptosystem with Expanding S-Boxes.	475
<i>Henri Gilbert, Jérôme Plût, and Joana Treger</i>	
Integrity	
Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance . . .	493
<i>Viet Tung Hoang, Reza Reyhanitabar, Phillip Rogaway, and Damian Vizár</i>	
Relational Hash: Probabilistic Hash for Verifying Relations, Secure Against Forgery and More	518
<i>Avradip Mandal and Arnab Roy</i>	
Explicit Non-malleable Codes Against Bit-Wise Tampering and Permutations.	538
<i>Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran</i>	
Assumptions	
Cryptanalysis of the Co-ACD Assumption	561
<i>Pierre-Alain Fouque, Moon Sung Lee, Tancrede Lepoint, and Mehdi Tibouchi</i>	
Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP	581
<i>Ming-Deh A. Huang, Michiel Kisters, and Sze Ling Yeo</i>	
A Quasipolynomial Reduction for Generalized Selective Decryption on Trees	601
<i>Georg Fuchsbauer, Zahra Jafargholi, and Krzysztof Pietrzak</i>	
Hash Functions and Stream Cipher Cryptanalysis	
Practical Free-Start Collision Attacks on 76-step SHA-1	623
<i>Pierre Karpman, Thomas Peyrin, and Marc Stevens</i>	
Fast Correlation Attacks over Extension Fields, Large-Unit Linear Approximation and Cryptanalysis of SNOW 2.0	643
<i>Bin Zhang, Chao Xu, and Willi Meier</i>	
Cryptanalysis of Full Sprout	663
<i>Virginie Lallemand and Maria Naya-Plasencia</i>	

Higher-Order Differential Meet-in-the-middle Preimage Attacks on SHA-1 and BLAKE.	683
<i>Thomas Espitau, Pierre-Alain Fouque, and Pierre Karpman</i>	
Implementations	
Decaf: Eliminating Cofactors Through Point Compression	705
<i>Mike Hamburg</i>	
Actively Secure OT Extension with Optimal Overhead	724
<i>Marcel Keller, Emmanuela Orsini, and Peter Scholl</i>	
Algebraic Decomposition for Probing Security	742
<i>Claude Carlet, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche</i>	
Consolidating Masking Schemes	764
<i>Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
Author Index	785

Contents – Part II

Multiparty Computation I

A Simpler Variant of Universally Composable Security for Standard Multiparty Computation	3
<i>Ran Canetti, Asaf Cohen, and Yehuda Lindell</i>	
Concurrent Secure Computation via Non-Black Box Simulation	23
<i>Vipul Goyal, Divya Gupta, and Amit Sahai</i>	
Concurrent Secure Computation with Optimal Query Complexity	43
<i>Ran Canetti, Vipul Goyal, and Abhishek Jain</i>	
Constant-Round MPC with Fairness and Guarantee of Output Delivery	63
<i>S. Dov Gordon, Feng-Hao Liu, and Elaine Shi</i>	

Zero-Knowledge

Statistical Concurrent Non-malleable Zero-Knowledge from One-Way Functions	85
<i>Susumu Kiyoshima</i>	
Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting	107
<i>Fabrice Benhamouda, Geoffroy Couteau, David Pointcheval, and Hoeteck Wee</i>	
Impossibility of Black-Box Simulation Against Leakage Attacks	130
<i>Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti</i>	
Efficient Zero-Knowledge Proofs of Non-algebraic Statements with Sublinear Amortized Cost	150
<i>Zhangxiang Hu, Payman Mohassel, and Mike Rosulek</i>	

Theory

Parallel Hashing via List Recoverability	173
<i>Iftach Haitner, Yuval Ishai, Eran Omri, and Ronen Shaltiel</i>	
Cryptography with One-Way Communication	191
<i>Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai</i>	

(Almost) Optimal Constructions of UOWHFs from 1-to-1, Regular One-Way Functions and Beyond.	209
<i>Yu Yu, Dawu Gu, Xiangxue Li, and Jian Weng</i>	

Signatures

Practical Round-Optimal Blind Signatures in the Standard Model	233
<i>Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig</i>	
Programmable Hash Functions Go Private: Constructions and Applications to (Homomorphic) Signatures with Shorter Public Keys.	254
<i>Dario Catalano, Dario Fiore, and Luca Nizzardo</i>	
Structure-Preserving Signatures from Standard Assumptions, Revisited	275
<i>Eike Kiltz, Jiaxin Pan, and Hoeteck Wee</i>	
Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions	296
<i>Benoît Libert, Thomas Peters, and Moti Yung</i>	

Multiparty Computation II

Efficient Constant Round Multi-party Computation Combining BMR and SPDZ	319
<i>Yehuda Lindell, Benny Pinkas, Nigel P. Smart, and Avishay Yanai</i>	
Round-Optimal Black-Box Two-Party Computation.	339
<i>Rafail Ostrovsky, Silas Richelson, and Alessandra Scafuro</i>	
Secure Computation with Minimal Interaction, Revisited	359
<i>Yuval Ishai, Ranjit Kumaresan, Eyal Kushilevitz, and Anat Paskin-Cherniavsky</i>	
PoW-Based Distributed Cryptography with No Trusted Setup.	379
<i>Marcin Andrychowicz and Stefan Dziembowski</i>	

Non-signaling and Information-Theoretic Crypto

Multi-prover Commitments Against Non-signaling Attacks.	403
<i>Serge Fehr and Max Fillinger</i>	
Arguments of Proximity [Extended Abstract]	422
<i>Yael Tauman Kalai and Ron D. Rothblum</i>	
Distributions Attaining Secret Key at a Rate of the Conditional Mutual Information	443
<i>Eric Chitambar, Benjamin Fortescue, and Min-Hsiu Hsieh</i>	

Privacy with Imperfect Randomness	463
<i>Yevgeniy Dodis and Yanqing Yao</i>	
Attribute-Based Encryption	
Communication Complexity of Conditional Disclosure of Secrets and Attribute-Based Encryption	485
<i>Romain Gay, Iordanis Kerenidis, and Hoeteck Wee</i>	
Predicate Encryption for Circuits from LWE	503
<i>Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee</i>	
Bilinear Entropy Expansion from the Decisional Linear Assumption	524
<i>Lucas Kowalczyk and Allison Bishop Lewko</i>	
New Primitives	
Data Is a Stream: Security of Stream-Based Channels	545
<i>Marc Fischlin, Felix Günther, Giorgia Azzurra Marson, and Kenneth G. Paterson</i>	
Bloom Filters in Adversarial Environments	565
<i>Moni Naor and Eylon Yogev</i>	
Proofs of Space	585
<i>Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak</i>	
Fully Homomorphic/Functional Encryption	
Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity	609
<i>Anne Broadbent and Stacey Jeffery</i>	
Multi-identity and Multi-key Leveled FHE from Learning with Errors	630
<i>Michael Clear and Ciarán McGoldrick</i>	
From Selective to Adaptive Security in Functional Encryption	657
<i>Prabhanjan Ananth, Zvika Brakerski, Gil Segev, and Vinod Vaikuntanathan</i>	
A Punctured Programming Approach to Adaptively Secure Functional Encryption	678
<i>Brent Waters</i>	
Multiparty Computation III	
Secure Computation from Leaky Correlated Randomness	701
<i>Divya Gupta, Yuval Ishai, Hemanta K. Maji, and Amit Sahai</i>	

Efficient Multi-party Computation: From Passive to Active Security
via Secure SIMD Circuits 721
 Daniel Genkin, Yuval Ishai, and Antigoni Polychroniadou

Large-Scale Secure Computation: Multi-party Computation for (Parallel)
RAM Programs. 742
 Elette Boyle, Kai-Min Chung, and Rafael Pass

Incoercible Multi-party Computation and Universally Composable
Receipt-Free Voting 763
 Joël Alwen, Rafail Ostrovsky, Hong-Sheng Zhou, and Vassilis Zikas

Author Index 781