

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
Céline Blondeau, Thomas Peyrin, and Lei Wang

Key-Recovery Attack on the ASASA Cryptosystem with Expanding
S-Boxes. 475
Henri Gilbert, Jérôme Plût, and Joana Treger

Integrity

Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance . . . 493
*Viet Tung Hoang, Reza Reyhanitabar, Phillip Rogaway,
and Damian Vizár*

Relational Hash: Probabilistic Hash for Verifying Relations, Secure
Against Forgery and More 518
Avradip Mandal and Arnab Roy

Explicit Non-malleable Codes Against Bit-Wise Tampering
and Permutations. 538
*Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey,
and Manoj Prabhakaran*

Assumptions

Cryptanalysis of the Co-ACD Assumption 561
*Pierre-Alain Fouque, Moon Sung Lee, Tancrede Lepoint,
and Mehdi Tibouchi*

Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP 581
Ming-Deh A. Huang, Michiel Koster, and Sze Ling Ye

A Quasipolynomial Reduction for Generalized Selective Decryption
on Trees 601
Georg Fuchsbauer, Zahra Jafarholi, and Krzysztof Pietrzak

Hash Functions and Stream Cipher Cryptanalysis

Practical Free-Start Collision Attacks on 76-step SHA-1 623
Pierre Karpman, Thomas Peyrin, and Marc Stevens

Fast Correlation Attacks over Extension Fields, Large-Unit Linear
Approximation and Cryptanalysis of SNOW 2.0 643
Bin Zhang, Chao Xu, and Willi Meier

Cryptanalysis of Full Sprout 663
Virginie Lallemand and Maria Naya-Plasencia

Higher-Order Differential Meet-in-the-middle Preimage Attacks on SHA-1
and BLAKE. 683
Thomas Espitau, Pierre-Alain Fouque, and Pierre Karpman

Implementations

Decaf: Eliminating Cofactors Through Point Compression 705
Mike Hamburg

Actively Secure OT Extension with Optimal Overhead 724
Marcel Keller, Emmanuela Orsini, and Peter Scholl

Algebraic Decomposition for Probing Security 742
Claude Carlet, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche

Consolidating Masking Schemes. 764
*Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs,
and Ingrid Verbauwhede*

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
Yu Yu, Dawu Gu, Xiangxue Li, and Jian Weng

Signatures

Practical Round-Optimal Blind Signatures in the Standard Model 233
Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig

Programmable Hash Functions Go Private: Constructions and Applications to (Homomorphic) Signatures with Shorter Public Keys. 254
Dario Catalano, Dario Fiore, and Luca Nizzardo

Structure-Preserving Signatures from Standard Assumptions, Revisited 275
Eike Kiltz, Jiaxin Pan, and Hoeteck Wee

Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions 296
Benoît Libert, Thomas Peters, and Moti Yung

Multiparty Computation II

Efficient Constant Round Multi-party Computation Combining BMR and SPDZ 319
Yehuda Lindell, Benny Pinkas, Nigel P. Smart, and Avishay Yanai

Round-Optimal Black-Box Two-Party Computation. 339
Rafail Ostrovsky, Silas Richelson, and Alessandra Scafuro

Secure Computation with Minimal Interaction, Revisited 359
Yuval Ishai, Ranjit Kumaresan, Eyal Kushilevitz, and Anat Paskin-Cherniavsky

PoW-Based Distributed Cryptography with No Trusted Setup. 379
Marcin Andrychowicz and Stefan Dziembowski

Non-signaling and Information-Theoretic Crypto

Multi-prover Commitments Against Non-signaling Attacks. 403
Serge Fehr and Max Fillinger

Arguments of Proximity [Extended Abstract] 422
Yael Tauman Kalai and Ron D. Rothblum

Distributions Attaining Secret Key at a Rate of the Conditional Mutual Information 443
Eric Chitambar, Benjamin Fortescue, and Min-Hsiu Hsieh

Privacy with Imperfect Randomness 463
Yevgeniy Dodis and Yanqing Yao

Attribute-Based Encryption

Communication Complexity of Conditional Disclosure of Secrets
and Attribute-Based Encryption 485
Romain Gay, Iordanis Kerenidis, and Hoeteck Wee

Predicate Encryption for Circuits from LWE 503
Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee

Bilinear Entropy Expansion from the Decisional Linear Assumption 524
Lucas Kowalczyk and Allison Bishop Lewko

New Primitives

Data Is a Stream: Security of Stream-Based Channels 545
*Marc Fischlin, Felix Günther, Giorgia Azzurra Marson,
and Kenneth G. Paterson*

Bloom Filters in Adversarial Environments 565
Moni Naor and Eylon Yosev

Proofs of Space 585
*Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov,
and Krzysztof Pietrzak*

Fully Homomorphic/Functional Encryption

Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity 609
Anne Broadbent and Stacey Jeffery

Multi-identity and Multi-key Leveled FHE from Learning with Errors 630
Michael Clear and Ciarán McGoldrick

From Selective to Adaptive Security in Functional Encryption 657
*Prabhanjan Ananth, Zvika Brakerski, Gil Segev,
and Vinod Vaikuntanathan*

A Punctured Programming Approach to Adaptively Secure Functional
Encryption 678
Brent Waters

Multiparty Computation III

Secure Computation from Leaky Correlated Randomness 701
Divya Gupta, Yuval Ishai, Hemanta K. Maji, and Amit Sahai

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



<http://www.springer.com/978-3-662-47988-9>

Advances in Cryptology -- CRYPTO 2015
35th Annual Cryptology Conference, Santa Barbara, CA,
USA, August 16-20, 2015, Proceedings, Part I
Gennaro, R.; Robshaw, M. (Eds.)
2015, XVIII, 787 p. 108 illus., Softcover
ISBN: 978-3-662-47988-9