

Contents – Part III

Memory Hard Functions

Depth-Robust Graphs and Their Cumulative Memory Complexity.	3
<i>Joël Alwen, Jeremiah Blocki, and Krzysztof Pietrzak</i>	
Script Is Maximally Memory-Hard	33
<i>Joël Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, and Stefano Tessaro</i>	

Symmetric-Key Constructions

Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts	65
<i>Gorjan Alagic and Alexander Russell</i>	
Boolean Searchable Symmetric Encryption with Worst-Case Sub-linear Complexity	94
<i>Seny Kamara and Tarik Moataz</i>	

Obfuscation I

Patchable Indistinguishability Obfuscation: $i\mathcal{O}$ for Evolving Software	127
<i>Prabhanjan Ananth, Abhishek Jain, and Amit Sahai</i>	
Breaking the Sub-Exponential Barrier in Obfustopia	156
<i>Sanjam Garg, Omkant Pandey, Akshayaram Srinivasan, and Mark Zhandry</i>	

Symmetric Cryptanalysis II

New Impossible Differential Search Tool from Design and Cryptanalysis Aspects: Revealing Structural Properties of Several Ciphers	185
<i>Yu Sasaki and Yosuke Todo</i>	
New Collision Attacks on Round-Reduced Keccak	216
<i>Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo</i>	

Obfuscation II

Lattice-Based SNARGs and Their Application to More Efficient Obfuscation	247
<i>Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu</i>	

Cryptanalyses of Candidate Branching Program Obfuscators.	278
<i>Yilei Chen, Craig Gentry, and Shai Halevi</i>	

Quantum Cryptography

Quantum Authentication and Encryption with Key Recycling: Or: How to Re-use a One-Time Pad Even if $P = NP$ — Safely & Feasibly	311
<i>Serge Fehr and Louis Salvail</i>	
Quantum Authentication with Key Recycling	339
<i>Christopher Portmann</i>	
Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol for NP Secure Against Quantum Adversaries	369
<i>André Chailloux and Anthony Leverrier</i>	

Multiparty Computation III

Faster Secure Two-Party Computation in the Single-Execution Setting.	399
<i>Xiao Wang, Alex J. Malozemoff, and Jonathan Katz</i>	
Non-interactive Secure 2PC in the Offline/Online and Batch Settings	425
<i>Payman Mohassel and Mike Rosulek</i>	
Hashing Garbled Circuits for Free.	456
<i>Xiong Fan, Chaya Ganesh, and Vladimir Kolesnikov</i>	

Public-Key Encryption and Key-Exchange

Adaptive Partitioning.	489
<i>Dennis Hofheinz</i>	
0-RTT Key Exchange with Full Forward Secrecy	519
<i>Felix Günther, Britta Hale, Tibor Jager, and Sebastian Lauer</i>	

Multiparty Computation IV

Computational Integrity with a Public Random String from Quasi-Linear PCPs	551
<i>Eli Ben-Sasson, Iddo Bentov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, and Madars Virza</i>	

Ad Hoc PSM Protocols: Secure Computation Without Coordination	580
<i>Amos Beimel, Yuval Ishai, and Eyal Kushilevitz</i>	
Topology-Hiding Computation Beyond Logarithmic Diameter	609
<i>Adi Akavia and Tal Moran</i>	
Author Index	639

Contents – Part I

Lattice Attacks and Constructions I

Revisiting Lattice Attacks on Overstretched NTRU Parameters	3
<i>Paul Kirchner and Pierre-Alain Fouque</i>	
Short Generators Without Quantum Computers: The Case of Multiquadratics.	27
<i>Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal</i>	
Computing Generator in Cyclotomic Integer Rings: A Subfield Algorithm for the Principal Ideal Problem in $L_{ AK }(\frac{1}{2})$ and Application to the Cryptanalysis of a FHE Scheme.	60
<i>Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre G��lin, and Paul Kirchner</i>	

Obfuscation and Functional Encryption

Robust Transforming Combiners from Indistinguishability Obfuscation to Functional Encryption	91
<i>Prabhanjan Ananth, Aayush Jain, and Amit Sahai</i>	
From Minicrypt to Obfustopia via Private-Key Functional Encryption	122
<i>Ilan Komargodski and Gil Segev</i>	
Projective Arithmetic Functional Encryption and Indistinguishability Obfuscation from Degree-5 Multilinear Maps	152
<i>Prabhanjan Ananth and Amit Sahai</i>	

Discrete Logarithm

Computation of a 768-Bit Prime Field Discrete Logarithm	185
<i>Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, and Colin Stahlke</i>	
A Kilobit Hidden SNFS Discrete Logarithm Computation	202
<i>Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thom��</i>	

Multiparty Computation I

Improved Private Set Intersection Against Malicious Adversaries	235
<i>Peter Rindal and Mike Rosulek</i>	

Formal Abstractions for Attested Execution Secure Processors	260
<i>Rafael Pass, Elaine Shi, and Florian Tramèr</i>	

Lattice Attacks and Constructions II

One-Shot Verifiable Encryption from Lattices.	293
<i>Vadim Lyubashevsky and Gregory Neven</i>	
Short Stickelberger Class Relations and Application to Ideal-SVP.	324
<i>Ronald Cramer, Léo Ducas, and Benjamin Wesolowski</i>	

Universal Composability

Concurrently Composable Security with Shielded Super-Polynomial Simulators	351
<i>Brandon Broadnax, Nico Döttling, Gunnar Hartung, Jörn Müller-Quade, and Matthias Nagel</i>	
Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs	382
<i>Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, and Ivan Visconti</i>	

Lattice Attacks and Constructions III

Private Puncturable PRFs from Standard Lattice Assumptions.	415
<i>Dan Boneh, Sam Kim, and Hart Montgomery</i>	
Constraint-Hiding Constrained PRFs for NC ¹ from LWE.	446
<i>Ran Canetti and Yilei Chen</i>	

Zero Knowledge I

Amortized Complexity of Zero-Knowledge Proofs Revisited: Achieving Linear Soundness Slack	479
<i>Ronald Cramer, Ivan Damgård, Chaoping Xing, and Chen Yuan</i>	
Sublinear Zero-Knowledge Arguments for RAM Programs.	501
<i>Payman Mohassel, Mike Rosulek, and Alessandra Scafuro</i>	

Side-Channel Attacks and Countermeasures

Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model.	535
<i>Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub</i>	

How Fast Can Higher-Order Masking Be in Software?	567
<i>Dahmun Goudarzi and Matthieu Rivain</i>	

Functional Encryption I

Multi-input Inner-Product Functional Encryption from Pairings.	601
<i>Michel Abdalla, Romain Gay, Mariana Raykova, and Hoeteck Wee</i>	
Simplifying Design and Analysis of Complex Predicate Encryption Schemes	627
<i>Shashank Agrawal and Melissa Chase</i>	

Elliptic Curves

Twisted μ_4 -Normal Form for Elliptic Curves	659
<i>David Kohel</i>	
Efficient Compression of SIDH Public Keys.	679
<i>Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik</i>	

Author Index	707
-------------------------------	-----

Contents – Part II

Functional Encryption II

On Removing Graded Encodings from Functional Encryption.	3
<i>Nir Bitansky, Huijia Lin, and Omer Paneth</i>	
Functional Encryption: Deterministic to Randomized Functions from Simple Assumptions	30
<i>Shashank Agrawal and David J. Wu</i>	

Lattice Attacks and Constructions IV

Random Sampling Revisited: Lattice Enumeration with Discrete Pruning	65
<i>Yoshinori Aono and Phong Q. Nguyen</i>	
On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HELib and SEAL.	103
<i>Martin R. Albrecht</i>	
Small CRT-Exponent RSA Revisited.	130
<i>Atsushi Takayasu, Yao Lu, and Liqiang Peng</i>	

Multiparty Computation II

Group-Based Secure Computation: Optimizing Rounds, Communication, and Computation.	163
<i>Elette Boyle, Niv Gilboa, and Yuval Ishai</i>	
On the Exact Round Complexity of Self-composable Two-Party Computation.	194
<i>Sanjam Garg, Susumu Kiyoshima, and Omkant Pandey</i>	
High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority	225
<i>Jun Furukawa, Yehuda Lindell, Ariel Nof, and Or Weinstein</i>	

Symmetric Cryptanalysis I

Conditional Cube Attack on Reduced-Round Keccak Sponge Function	259
<i>Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, and Jingyuan Zhao</i>	

A New Structural-Differential Property of 5-Round AES	289
<i>Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom</i>	

Zero Knowledge II

Removing the Strong RSA Assumption from Arguments over the Integers. . .	321
<i>Geoffroy Couteau, Thomas Peters, and David Pointcheval</i>	
Magic Adversaries Versus Individual Reduction: Science Wins Either Way.	351
<i>Yi Deng</i>	

Provable Security for Symmetric Cryptography I

The Multi-user Security of Double Encryption	381
<i>Viet Tung Hoang and Stefano Tessaro</i>	
Public-Seed Pseudorandom Permutations	412
<i>Pratik Soni and Stefano Tessaro</i>	

Security Models I

Cryptography with Updates	445
<i>Prabhanjan Ananth, Aloni Cohen, and Abhishek Jain</i>	
Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited	473
<i>Yevgeniy Dodis, Siyao Guo, and Jonathan Katz</i>	

Provable Security for Symmetric Cryptography II

Modifying an Enciphering Scheme After Deployment	499
<i>Paul Grubbs, Thomas Ristenpart, and Yuval Yarom</i>	
Separating Semantic and Circular Security for Symmetric-Key Bit Encryption from the Learning with Errors Assumption.	528
<i>Rishab Goyal, Venkata Koppula, and Brent Waters</i>	

Security Models II

Toward Fine-Grained Blackbox Separations Between Semantic and Circular-Security Notions.	561
<i>Mohammad Hajiabadi and Bruce M. Kapron</i>	
A Note on Perfect Correctness by Derandomization.	592
<i>Nir Bitansky and Vinod Vaikuntanathan</i>	

Blockchain

Decentralized Anonymous Micropayments	609
<i>Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Miao, Ian Miers, and Pratyush Mishra</i>	
Analysis of the Blockchain Protocol in Asynchronous Networks	643
<i>Rafael Pass, Lior Seeman, and Abhi Shelat</i>	
Author Index	675

Advances in Cryptology - EUROCRYPT 2017
36th Annual International Conference on the Theory
and Applications of Cryptographic Techniques, Paris,
France, April 30 - May 4, 2017, Proceedings, Part III
Coron, J.-S.; Nielsen, J.B. (Eds.)
2017, XXI, 641 p. 54 illus., Softcover
ISBN: 978-3-319-56616-0