Contents – Part II

Functional Encryption II

On Removing Graded Encodings from Functional Encryption. .............. 3
                Nir Bitansky, Huijia Lin, and Omer Paneth

Functional Encryption: Deterministic to Randomized Functions
from Simple Assumptions ................................................. 30
                Shashank Agrawal and David J. Wu

Lattice Attacks and Constructions IV

Random Sampling Revisited: Lattice Enumeration with Discrete Pruning . . . 65
                Yoshinori Aono and Phong Q. Nguyen

On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices
in HElib and SEAL. .......................................................... 103
                Martin R. Albrecht

Small CRT-Exponent RSA Revisited. ..................................... 130
                Atsushi Takayasu, Yao Lu, and Liqiang Peng

Multiparty Computation II

Group-Based Secure Computation: Optimizing Rounds, Communication,
and Computation. .......................................................... 163
                Elette Boyle, Niv Gilboa, and Yuval Ishai

On the Exact Round Complexity of Self-composable
Two-Party Computation .................................................... 194
                Sanjam Garg, Susumu Kiyoshima, and Omkant Pandey

High-Throughput Secure Three-Party Computation for Malicious
Adversaries and an Honest Majority ..................................... 225
                Jun Furukawa, Yehuda Lindell, Ariel Nof, and Or Weinstein

Symmetric Cryptanalysis I

Conditional Cube Attack on Reduced-Round Keccak Sponge Function . . . . 259
                Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang,
                and Jingyuan Zhao
A New Structural-Differential Property of 5-Round AES

Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom

289

Zero Knowledge II

Removing the Strong RSA Assumption from Arguments over the Integers.

Geoffroy Couteau, Thomas Peters, and David Pointcheval

321

Magic Adversaries Versus Individual Reduction:
Science Wins Either Way.

Yi Deng

351

Provable Security for Symmetric Cryptography I

The Multi-user Security of Double Encryption

Viet Tung Hoang and Stefano Tessaro

381

Public-Seed Pseudorandom Permutations

Pratik Soni and Stefano Tessaro

412

Security Models I

Cryptography with Updates

Prabhanjan Ananth, Aloni Cohen, and Abhishek Jain

445

Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited

Yevgeniy Dodis, Siyao Guo, and Jonathan Katz

473

Provable Security for Symmetric Cryptography II

Modifying an Enciphering Scheme After Deployment

Paul Grubbs, Thomas Ristenpart, and Yuval Yarom

499

Separating Semantic and Circular Security for Symmetric-Key Bit Encryption from the Learning with Errors Assumption.

Rishab Goyal, Venkata Koppula, and Brent Waters

528

Security Models II

Toward Fine-Grained Blackbox Separations Between Semantic and Circular-Security Notions

Mohammad Hajiabadi and Bruce M. Kapron

561

A Note on Perfect Correctness by Derandomization.

Nir Bitansky and Vinod Vaikuntanathan

592
Blockchain

Decentralized Anonymous Micropayments .......................... 609
  Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Miao,
  Ian Miers, and Pratyush Mishra

Analysis of the Blockchain Protocol in Asynchronous Networks .... 643
  Rafael Pass, Lior Seeman, and Abhi Shelat

Author Index .......................................................... 675
Contents – Part III

Memory Hard Functions

Depth-Robust Graphs and Their Cumulative Memory Complexity
Joël Alwen, Jeremiah Blocki, and Krzysztof Pietrzak

Scrypt Is Maximally Memory-Hard
Joël Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, and Stefano Tessaro

Symmetric-Key Constructions

Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts
Gorjan Alagic and Alexander Russell

Boolean Searchable Symmetric Encryption with Worst-Case Sub-linear Complexity
Seny Kamara and Tarik Moataz

Obfuscation I

Patchable Indistinguishability Obfuscation: iO for Evolving Software
Prabhanjan Ananth, Abhishek Jain, and Amit Sahai

Breaking the Sub-Exponential Barrier in Obfustopia
Sanjam Garg, Omkant Pandey, Akshayaram Srinivasan, and Mark Zhandry

Symmetric Cryptanalysis II

New Impossible Differential Search Tool from Design and Cryptanalysis Aspects: Revealing Structural Properties of Several Ciphers
Yu Sasaki and Yosuke Todo

New Collision Attacks on Round-Reduced Keccak
Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo

Obfuscation II

Lattice-Based SNARGs and Their Application to More Efficient Obfuscation
Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu
Cryptanalyses of Candidate Branching Program Obfuscators. 278
Yilei Chen, Craig Gentry, and Shai Halevi

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
Serge Fehr and Louis Salvail

Quantum Authentication with Key Recycling 339
Christopher Portmann

Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol
for $NP$ Secure Against Quantum Adversaries 369
André Chailloux and Anthony Leverrier

Multiparty Computation III
Faster Secure Two-Party Computation in the Single-Execution Setting. 399
Xiao Wang, Alex J. Malozemoff, and Jonathan Katz

Non-interactive Secure 2PC in the Offline/Online and Batch Settings 425
Payman Mohassel and Mike Rosulek

Hashing Garbled Circuits for Free 456
Xiong Fan, Chaya Ganesh, and Vladimir Kolesnikov

Public-Key Encryption and Key-Exchange
Adaptive Partitioning 489
Dennis Hofheinz

0-RTT Key Exchange with Full Forward Secrecy 519
Felix Günther, Britta Hale, Tibor Jager, and Sebastian Lauer

Multiparty Computation IV
Computational Integrity with a Public Random String
from Quasi-Linear PCPs 551
Eli Ben-Sasson, Iddo Bentov, Alessandro Chiesa, Ariel Gabizon,
Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev,
Mark Silberstein, Eran Tromer, and Madars Virza
Ad Hoc PSM Protocols: Secure Computation Without Coordination .............. 580
Amos Beimel, Yuval Ishai, and Eyal Kushilevitz

Topology-Hiding Computation Beyond Logarithmic Diameter ................. 609
Adi Akavia and Tal Moran

Author Index ............................................................... 639
Contents – Part I

Lattice Attacks and Constructions I

Revisiting Lattice Attacks on Overstretched NTRU Parameters .................. 3
Paul Kirchner and Pierre-Alain Fouque

Short Generators Without Quantum Computers:
The Case of Multiquadratics.......................................................... 27
Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal

Computing Generator in Cyclotomic Integer Rings: A Subfield Algorithm for the Principal Ideal Problem in \( L_{JK}(\frac{1}{2}) \) and Application to the Cryptanalysis of a FHE Scheme. .................... 60
Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin, and Paul Kirchner

Obfuscation and Functional Encryption

Robust Transforming Combiners from Indistinguishability Obfuscation to Functional Encryption ............................................. 91
Prabhanjan Ananth, Aayush Jain, and Amit Sahai

From Minicrypt to Obfustopia via Private-Key Functional Encryption ..... 122
Ilan Komargodski and Gil Segev

Projective Arithmetic Functional Encryption and Indistinguishability Obfuscation from Degree-5 Multilinear Maps ......................... 152
Prabhanjan Ananth and Amit Sahai

Discrete Logarithm

Computation of a 768-Bit Prime Field Discrete Logarithm .................... 185
Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, and Colin Stahlke

A Kilobit Hidden SNFS Discrete Logarithm Computation ...................... 202
Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé

Multiparty Computation I

Improved Private Set Intersection Against Malicious Adversaries ............ 235
Peter Rindal and Mike Rosulek
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Formal Abstractions for Attested Execution Secure Processors</td>
<td>260</td>
</tr>
<tr>
<td></td>
<td><em>Rafael Pass, Elaine Shi, and Florian Tramèr</em></td>
<td></td>
</tr>
<tr>
<td>Lattice Attacks and Constructions II</td>
<td>One-Shot Verifiable Encryption from Lattices.</td>
<td>293</td>
</tr>
<tr>
<td></td>
<td><em>Vadim Lyubashevsky and Gregory Neven</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Short Stickelberger Class Relations and Application to Ideal-SVP</td>
<td>324</td>
</tr>
<tr>
<td></td>
<td><em>Ronald Cramer, Léo Ducas, and Benjamin Wesolowski</em></td>
<td></td>
</tr>
<tr>
<td>Universal Composability</td>
<td>Concurrently Composable Security with Shielded Super-Polynomial Simulators</td>
<td>351</td>
</tr>
<tr>
<td></td>
<td><em>Brandon Broadnax, Nico Döttling, Gunnar Hartung, Jörn Müller-Quade, and Matthias Nagel</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs</td>
<td>382</td>
</tr>
<tr>
<td></td>
<td><em>Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, and Ivan Visconti</em></td>
<td></td>
</tr>
<tr>
<td>Lattice Attacks and Constructions III</td>
<td>Private Puncturable PRFs from Standard Lattice Assumptions.</td>
<td>415</td>
</tr>
<tr>
<td></td>
<td><em>Dan Boneh, Sam Kim, and Hart Montgomery</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraint-Hiding Constrained PRFs for NC$^1$ from LWE</td>
<td>446</td>
</tr>
<tr>
<td></td>
<td><em>Ran Canetti and Yilei Chen</em></td>
<td></td>
</tr>
<tr>
<td>Zero Knowledge I</td>
<td>Amortized Complexity of Zero-Knowledge Proofs Revisited: Achieving Linear Soundness Slack</td>
<td>479</td>
</tr>
<tr>
<td></td>
<td><em>Ronald Cramer, Ivan Damgård, Chaoping Xing, and Chen Yuan</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sublinear Zero-Knowledge Arguments for RAM Programs</td>
<td>501</td>
</tr>
<tr>
<td></td>
<td><em>Payman Mohassel, Mike Rosulek, and Alessandra Scafuro</em></td>
<td></td>
</tr>
<tr>
<td>Side-Channel Attacks and Countermeasures</td>
<td>Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model</td>
<td>535</td>
</tr>
<tr>
<td></td>
<td><em>Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub</em></td>
<td></td>
</tr>
</tbody>
</table>
Dahmun Goudarzi and Matthieu Rivain

Functional Encryption I

Multi-input Inner-Product Functional Encryption from Pairings .......... 601
Michel Abdalla, Romain Gay, Mariana Raykova, and Hoeteck Wee

Simplifying Design and Analysis of Complex Predicate
Encryption Schemes .................................................. 627
Shashank Agrawal and Melissa Chase

Elliptic Curves

Twisted $\mu_4$-Normal Form for Elliptic Curves ....................... 659
David Kohel

Efficient Compression of SIDH Public Keys ......................... 679
Craig Costello, David Jao, Patrick Longa, Michael Naehrig,
Joost Renes, and David Urbanik

Author Index ......................................................... 707
Advances in Cryptology - EUROCRYPT 2017
Coron, J.-S.; Nielsen, J.B. (Eds.)
2017, XXI, 677 p. 66 illus., Softcover
ISBN: 978-3-319-56613-9