Contents – Part II

Functional Encryption II

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

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

Lattice Attacks and Constructions IV

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

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

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

Multiparty Computation II

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

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

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

Symmetric Cryptanalysis I

Conditional Cube Attack on Reduced-Round Keccak Sponge Function
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

Zero Knowledge II

Removing the Strong RSA Assumption from Arguments over the Integers.

Geoffroy Couteau, Thomas Peters, and David Pointcheval

Magic Adversaries Versus Individual Reduction:

Science Wins Either Way.

Yi Deng

Provable Security for Symmetric Cryptography I

The Multi-user Security of Double Encryption

Viet Tung Hoang and Stefano Tessaro

Public-Seed Pseudorandom Permutations

Pratik Soni and Stefano Tessaro

Security Models I

Cryptography with Updates

Prabhanjan Ananth, Aloni Cohen, and Abhishek Jain

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

Yevgeniy Dodis, Siyao Guo, and Jonathan Katz

Provable Security for Symmetric Cryptography II

Modifying an Enciphering Scheme After Deployment

Paul Grubbs, Thomas Ristenpart, and Yuval Yarom

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

Rishab Goyal, Venkata Koppula, and Brent Waters

Security Models II

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

Mohammad Hajiabadi and Bruce M. Kapron

A Note on Perfect Correctness by Derandomization.
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*
  
  3

- **Scrypt Is Maximally Memory-Hard.**
  
  *Joël Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, and Stefano Tessaro*
  
  33

### Symmetric-Key Constructions

- **Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts.**
  
  *Gorjan Alagic and Alexander Russell*
  
  65

- **Boolean Searchable Symmetric Encryption with Worst-Case Sub-linear Complexity.**
  
  *Seny Kamara and Tarik Moataz*
  
  94

### Obfuscation I

- **Patchable Indistinguishability Obfuscation: $iO$ for Evolving Software.**
  
  *Prabhanjan Ananth, Abhishek Jain, and Amit Sahai*
  
  127

- **Breaking the Sub-Exponential Barrier in Obfustopia.**
  
  *Sanjam Garg, Omkant Pandey, Akshayaram Srinivasan, and Mark Zhandry*
  
  156

### Symmetric Cryptanalysis II

- **New Impossible Differential Search Tool from Design and Cryptanalysis Aspects: Revealing Structural Properties of Several Ciphers.**
  
  *Yu Sasaki and Yosuke Todo*
  
  185

- **New Collision Attacks on Round-Reduced Keccak.**
  
  *Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo*
  
  216

### Obfuscation II

- **Lattice-Based SNARGs and Their Application to More Efficient Obfuscation.**
  
  *Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu*
  
  247
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptanalyses of Candidate Branching Program Obfuscators.</td>
<td>278</td>
</tr>
<tr>
<td><em>Yilei Chen, Craig Gentry, and Shai Halevi</em></td>
<td></td>
</tr>
<tr>
<td><strong>Quantum Cryptography</strong></td>
<td></td>
</tr>
<tr>
<td>Quantum Authentication and Encryption with Key Recycling:</td>
<td>311</td>
</tr>
<tr>
<td>Or: How to Re-use a One-Time Pad Even if ( P = NP ) —</td>
<td></td>
</tr>
<tr>
<td>Safely &amp; Feasibly</td>
<td></td>
</tr>
<tr>
<td><em>Serge Fehr and Louis Salvail</em></td>
<td></td>
</tr>
<tr>
<td>Quantum Authentication with Key Recycling</td>
<td>339</td>
</tr>
<tr>
<td><em>Christopher Portmann</em></td>
<td></td>
</tr>
<tr>
<td>Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol</td>
<td>369</td>
</tr>
<tr>
<td>for ( NP ) Secure Against Quantum Adversaries</td>
<td></td>
</tr>
<tr>
<td><em>André Chailloux and Anthony Leverrier</em></td>
<td></td>
</tr>
<tr>
<td><strong>Multiparty Computation III</strong></td>
<td></td>
</tr>
<tr>
<td>Faster Secure Two-Party Computation in the Single-Execution Setting.</td>
<td>399</td>
</tr>
<tr>
<td><em>Xiao Wang, Alex J. Malozemoff, and Jonathan Katz</em></td>
<td></td>
</tr>
<tr>
<td>Non-interactive Secure 2PC in the Offline/Online and Batch Settings</td>
<td>425</td>
</tr>
<tr>
<td><em>Payman Mohassel and Mike Rosulek</em></td>
<td></td>
</tr>
<tr>
<td>Hashing Garbled Circuits for Free</td>
<td>456</td>
</tr>
<tr>
<td><em>Xiong Fan, Chaya Ganesh, and Vladimir Kolesnikov</em></td>
<td></td>
</tr>
<tr>
<td><strong>Public-Key Encryption and Key-Exchange</strong></td>
<td></td>
</tr>
<tr>
<td>Adaptive Partitioning</td>
<td>489</td>
</tr>
<tr>
<td><em>Dennis Hofheinz</em></td>
<td></td>
</tr>
<tr>
<td>0-RTT Key Exchange with Full Forward Secrecy</td>
<td>519</td>
</tr>
<tr>
<td><em>Felix Günther, Britta Hale, Tibor Jager, and Sebastian Lauer</em></td>
<td></td>
</tr>
<tr>
<td><strong>Multiparty Computation IV</strong></td>
<td></td>
</tr>
<tr>
<td>Computational Integrity with a Public Random String</td>
<td>551</td>
</tr>
<tr>
<td>from Quasi-Linear PCPs</td>
<td></td>
</tr>
<tr>
<td><em>Eli Ben-Sasson, Iddo Bentov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, and Madars Virza</em></td>
<td></td>
</tr>
</tbody>
</table>
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 $\mathbb{L}_{[\mathbb{A}\mathbb{K}]}(\frac{1}{2})$ 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
Formal Abstractions for Attested Execution Secure Processors  ............ 260
   Rafael Pass, Elaine Shi, and Florian Tramèr

Lattice Attacks and Constructions II

One-Shot Verifiable Encryption from Lattices  ........ ................. 293
   Vadim Lyubashevsky and Gregory Neven

Short Stickelberger Class Relations and Application to Ideal-SVP  .... 324
   Ronald Cramer, Léo Ducas, and Benjamin Wesolowski

Universal Composability

Concurrently Composable Security with Shielded Super-Polynomial Simulators  ..................... 351
   Brandon Broadnax, Nico Döttling, Gunnar Hartung, Jörn Müller-Quade, and Matthias Nagel

Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs  .... 382
   Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, and Ivan Visconti

Lattice Attacks and Constructions III

Private Puncturable PRFs from Standard Lattice Assumptions  ........ 415
   Dan Boneh, Sam Kim, and Hart Montgomery

Constraint-Hiding Constrained PRFs for NC$^1$ from LWE  ........ 446
   Ran Canetti and Yilei Chen

Zero Knowledge I

Amortized Complexity of Zero-Knowledge Proofs Revisited: Achieving Linear Soundness Slack  .................... 479
   Ronald Cramer, Ivan Damgård, Chaoping Xing, and Chen Yuan

Sublinear Zero-Knowledge Arguments for RAM Programs  ........ 501
   Payman Mohassel, Mike Rosulek, and Alessandra Scafuro

Side-Channel Attacks and Countermeasures

Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model  ........ ......... 535
   Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Fast Can Higher-Order Masking Be in Software?</td>
<td>567</td>
</tr>
<tr>
<td>Dahmum Goudarzi and Matthieu Rivain</td>
<td></td>
</tr>
<tr>
<td><strong>Functional Encryption I</strong></td>
<td></td>
</tr>
<tr>
<td>Multi-input Inner-Product Functional Encryption from Pairings</td>
<td>601</td>
</tr>
<tr>
<td>Michel Abdalla, Romain Gay, Mariana Raykova, and Hoeteck Wee</td>
<td></td>
</tr>
<tr>
<td>Simplifying Design and Analysis of Complex Predicate Encryption Schemes</td>
<td>627</td>
</tr>
<tr>
<td>Shashank Agrawal and Melissa Chase</td>
<td></td>
</tr>
<tr>
<td><strong>Elliptic Curves</strong></td>
<td></td>
</tr>
<tr>
<td>Twisted $\mu_4$-Normal Form for Elliptic Curves</td>
<td>659</td>
</tr>
<tr>
<td>David Kohel</td>
<td></td>
</tr>
<tr>
<td>Efficient Compression of SIDH Public Keys</td>
<td>679</td>
</tr>
<tr>
<td>Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>707</td>
</tr>
</tbody>
</table>
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