Contents – Part II, Track I

Signatures

Universal Signature Aggregators ................................................. 3  
Susan Hohenberger, Venkata Koppula, and Brent Waters

Fully Structure-Preserving Signatures and Shrinking Commitments .......... 35  
Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi

Zero-Knowledge Proofs

Disjunctions for Hash Proof Systems: New Constructions and Applications .................................................. 69  
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval

Quasi-Adaptive NIZK for Linear Subspaces Revisited ....................... 101  
Eike Kiltz and Hoeteck Wee

Leakage-Resilient Cryptography

Leakage-Resilient Circuits Revisited – Optimal Number of Computing Components Without Leak-Free Hardware ........................................... 131  
Dana Dachman-Soled, Feng-Hao Liu, and Hong-Sheng Zhou

Noisy Leakage Revisited ............................................................. 159  
Stefan Dziembowski, Sebastian Faust, and Maciej Skorski

Garbled Circuits

Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge ............................................................. 191  
Tore Kasper Frederiksen, Jesper Buus Nielsen, and Claudio Orlandi

Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits Using Half Gates ....................................................... 220  
Samee Zahur, Mike Rosulek, and David Evans
Crypto Currencies

One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin

*Jens Groth and Markulf Kohlweiss*

The Bitcoin Backbone Protocol: Analysis and Applications

*Juan Garay, Aggelos Kiayias, and Nikos Leonardos*

Secret Sharing

Linear Secret Sharing Schemes from Error Correcting Codes

*Ronald Cramer, Ivan Bjerre Damgård, Nico Döttling, Serge Fehr, and Gabriele Spini*

Function Secret Sharing

*Elette Boyle, Niv Gilboa, and Yuval Ishai*

Outsourcing Computations

Cluster Computing in Zero Knowledge

*Alessandro Chiesa, Eran Tromer, and Madars Virza*

Hosting Services on an Untrusted Cloud

*Dan Boneh, Divya Gupta, Ilya Mironov, and Amit Sahai*

Obfuscation and E-Voting

How to Obfuscate Programs Directly

*Joe Zimmerman*

End-to-End Verifiable Elections in the Standard Model

*Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang*

Multi-party Computations

Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data

*Shashank Agrawal, Shweta Agrawal, and Manoj Prabhakaran*

Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World

*Melissa Chase, Rafail Ostrovsky, and Ivan Visconti*
## Encryption

Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation .................................................. 563  
**Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, and Joe Zimmerman**

Improved Dual System ABE in Prime-Order Groups via Predicate Encodings .......................................................... 595  
**Jie Chen, Romain Gay, and Hoeteck Wee**

## Resistant Protocols

Resisting Randomness Subversion: Fast Deterministic and Hedged Public-Key Encryption in the Standard Model ......................... 627  
**Mihir Bellare and Viet Tung Hoang**

Cryptographic Reverse Firewalls .................................................. 657  
**Ilya Mironov and Noah Stephens-Davidowitz**

## Key Exchange

Mind the Gap: Modular Machine-Checked Proofs of One-Round Key Exchange Protocols .................................................. 689  
**Gilles Barthe, Juan Manuel Crespo, Yassine Lakhnech, and Benedikt Schmidt**

Authenticated Key Exchange from Ideal Lattices .......................... 719  
**Jiang Zhang, Zhenfeng Zhang, Jintai Ding, Michael Snook, and Özgür Dagdelen**

## Quantum Cryptography

Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model .......................................................... 755  
**Dominique Unruh**

Privacy Amplification in the Isolated Qubits Model ......................... 785  
**Yi-Kai Liu**

## Discrete Logarithms

Generic Hardness of the Multiple Discrete Logarithm Problem ............. 817  
**Aaram Yun**

## Author Index

.......................................................... 837
Contents – Part I, Track R

Best Paper
Cryptanalysis of the Multilinear Map over the Integers .......................... 3
Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé

Honorable Mentions
Robust Authenticated-Encryption AEZ and the Problem That It Solves .... 15
Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway

On the Behaviors of Affine Equivalent Sboxes Regarding Differential
and Linear Attacks ......................................................... 45
Anne Canteaut and Joëlle Roué

Random Number Generators
A Provable-Security Analysis of Intel’s Secure Key RNG ........................ 77
Thomas Shrimpton and R. Seth Terashima

A Formal Treatment of Backdoored Pseudorandom Generators ............ 101
Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels, and Thomas Ristenpart

Number Field Sieve
Improving NFS for the Discrete Logarithm Problem in Non-prime
Finite Fields ......................................................................... 129
Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain

The Multiple Number Field Sieve with Conjugation and Generalized
Joux-Lercier Methods .......................................................... 156
Cécile Pierrot

Algorithmic Cryptanalysis
Better Algorithms for LWE and LWR ....................................... 173
Alexandre Duc, Florian Tramèr, and Serge Vaudenay
On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes .................................................. 203
Alexander May and Ilya Ozerov

Symmetric Cryptanalysis I

Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE ......................... 231
Itai Dinur

A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro .................................. 254
Gregor Leander, Brice Minaud, and Sondre Rønjom

Symmetric Cryptanalysis II

Structural Evaluation by Generalized Integral Property .................. 287
Yosuke Todo

Cryptanalysis of SP Networks with Partial Non-Linear Layers .......... 315
Achiya Bar-On, Itai Dinur, Orr Dunkelman, Virginie Lallemand, Nathan Keller, and Boaz Tsaban

Hash Functions

The Sum Can Be Weaker Than Each Part .................................. 345
Gaëtan Leurent and Lei Wang

SPHINCS: Practical Stateless Hash-Based Signatures .................. 368
Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O’Hearn

Evaluating Implementations

Making Masking Security Proofs Concrete: Or How to Evaluate the Security of Any Leaking Device .............................. 401
Alexandre Duc, Sebastian Faust, and François-Xavier Standaert

Ciphers for MPC and FHE .................................................. 430
Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner
Masking

Verified Proofs of Higher-Order Masking
Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub

Inner Product Masking Revisited
Josep Balasch, Sebastian Faust, and Benedikt Gierlichs

Fully Homomorphic Encryption I

Fully Homomorphic Encryption over the Integers Revisited
Jung Hee Cheon and Damien Stehlé

(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces
Koji Nuida and Kaoru Kurosawa

Related-Key Attacks

KDM-CCA Security from RKA Secure Authenticated Encryption
Xianhui Lu, Bao Li, and Dingding Jia

On the Provable Security of the Iterated Even-Mansour Cipher Against Related-Key and Chosen-Key Attacks
Benoît Cogliati and Yannick Seurin

Fully Homomorphic Encryption II

FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second
Léo Ducas and Daniele Micciancio

Bootstrapping for HElib
Shai Halevi and Victor Shoup

Efficient Two-Party Protocols

More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries
Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner

How to Efficiently Evaluate RAM Programs with Malicious Security
Arash Afshar, Zhangxiang Hu, Payman Mohassel, and Mike Rosulek
## Symmetric Cryptanalysis III

Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function ................................................................. 733  
*Itai Dinur, Paweł Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michał Straus*

Twisted Polynomials and Forgery Attacks on GCM ............................. 762  
*Mohamed Ahmed Abdelraheem, Peter Beelen, Andrey Bogdanov, and Elmar Tischhauser*

## Lattices

Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices .... 789  
*Vadim Lyubashevsky and Thomas Prest*

## Author Index

................................................................. 817