

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
<i>Alexander May and Ilya Ozerov</i>	

Symmetric Cryptanalysis I

Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE	231
<i>Itai Dinur</i>	

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

Symmetric Cryptanalysis II

Structural Evaluation by Generalized Integral Property	287
<i>Yosuke Todo</i>	

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

Hash Functions

The Sum Can Be Weaker Than Each Part	345
<i>Gaëtan Leurent and Lei Wang</i>	

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

Evaluating Implementations

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

Ciphers for MPC and FHE.	430
<i>Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner</i>	

Masking

Verified Proofs of Higher-Order Masking	457
<i>Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub</i>	
Inner Product Masking Revisited	486
<i>Josep Balasch, Sebastian Faust, and Benedikt Gierlichs</i>	

Fully Homomorphic Encryption I

Fully Homomorphic Encryption over the Integers Revisited	513
<i>Jung Hee Cheon and Damien Stehlé</i>	
(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces	537
<i>Koji Nuida and Kaoru Kurosawa</i>	

Related-Key Attacks

KDM-CCA Security from RKA Secure Authenticated Encryption	559
<i>Xianhui Lu, Bao Li, and Dingding Jia</i>	
On the Provable Security of the Iterated Even-Mansour Cipher Against Related-Key and Chosen-Key Attacks	584
<i>Benoît Cogliati and Yannick Seurin</i>	

Fully Homomorphic Encryption II

FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second . . .	617
<i>Léo Ducas and Daniele Micciancio</i>	
Bootstrapping for HElib	641
<i>Shai Halevi and Victor Shoup</i>	

Efficient Two-Party Protocols

More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries	673
<i>Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner</i>	
How to Efficiently Evaluate RAM Programs with Malicious Security	702
<i>Arash Afshar, Zhangxiang Hu, Payman Mohassel, and Mike Rosulek</i>	

Symmetric Cryptanalysis III

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

Twisted Polynomials and Forgery Attacks on GCM	762
<i>Mohamed Ahmed Abdelraheem, Peter Beelen, Andrey Bogdanov, and Elmar Tischhauser</i>	

Lattices

Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices	789
<i>Vadim Lyubashevsky and Thomas Prest</i>	

Author Index	817
-------------------------------	-----

Contents – Part II, Track I

Signatures

Universal Signature Aggregators.	3
<i>Susan Hohenberger, Venkata Koppula, and Brent Waters</i>	
Fully Structure-Preserving Signatures and Shrinking Commitments.	35
<i>Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi</i>	

Zero-Knowledge Proofs

Disjunctions for Hash Proof Systems: New Constructions and Applications.	69
<i>Michel Abdalla, Fabrice Benhamouda, and David Pointcheval</i>	
Quasi-Adaptive NIZK for Linear Subspaces Revisited	101
<i>Eike Kiltz and Hoeteck Wee</i>	

Leakage-Resilient Cryptography

Leakage-Resilient Circuits Revisited – Optimal Number of Computing Components Without Leak-Free Hardware.	131
<i>Dana Dachman-Soled, Feng-Hao Liu, and Hong-Sheng Zhou</i>	
Noisy Leakage Revisited	159
<i>Stefan Dziembowski, Sebastian Faust, and Maciej Skorski</i>	

Garbled Circuits

Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge.	191
<i>Tore Kasper Frederiksen, Jesper Buus Nielsen, and Claudio Orlandi</i>	
Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits Using Half Gates	220
<i>Samee Zahur, Mike Rosulek, and David Evans</i>	

Crypto Currencies

One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin	253
<i>Jens Groth and Markulf Kohlweiss</i>	

The Bitcoin Backbone Protocol: Analysis and Applications	281
<i>Juan Garay, Aggelos Kiayias, and Nikos Leonardos</i>	

Secret Sharing

Linear Secret Sharing Schemes from Error Correcting Codes and Universal Hash Functions	313
<i>Ronald Cramer, Ivan Bjerre Damgård, Nico Döttling, Serge Fehr, and Gabriele Spini</i>	

Function Secret Sharing.	337
<i>Elette Boyle, Niv Gilboa, and Yuval Ishai</i>	

Outsourcing Computations

Cluster Computing in Zero Knowledge	371
<i>Alessandro Chiesa, Eran Tromer, and Madars Virza</i>	

Hosting Services on an Untrusted Cloud	404
<i>Dan Boneh, Divya Gupta, Ilya Mironov, and Amit Sahai</i>	

Obfuscation and E-Voting

How to Obfuscate Programs Directly	439
<i>Joe Zimmerman</i>	

End-to-End Verifiable Elections in the Standard Model.	468
<i>Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang</i>	

Multi-party Computations

Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data	501
<i>Shashank Agrawal, Shweta Agrawal, and Manoj Prabhakaran</i>	

Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World	532
<i>Melissa Chase, Rafail Ostrovsky, and Ivan Visconti</i>	

Encryption

Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation	563
<i>Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, and Joe Zimmerman</i>	
Improved Dual System ABE in Prime-Order Groups via Predicate Encodings	595
<i>Jie Chen, Romain Gay, and Hoeteck Wee</i>	

Resistant Protocols

Resisting Randomness Subversion: Fast Deterministic and Hedged Public-Key Encryption in the Standard Model	627
<i>Mihir Bellare and Viet Tung Hoang</i>	
Cryptographic Reverse Firewalls	657
<i>Ilya Mironov and Noah Stephens-Davidowitz</i>	

Key Exchange

Mind the Gap: Modular Machine-Checked Proofs of One-Round Key Exchange Protocols	689
<i>Gilles Barthe, Juan Manuel Crespo, Yassine Lakhnech, and Benedikt Schmidt</i>	
Authenticated Key Exchange from Ideal Lattices	719
<i>Jiang Zhang, Zhenfeng Zhang, Jintai Ding, Michael Snook, and Özgür Dagdelen</i>	

Quantum Cryptography

Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model	755
<i>Dominique Unruh</i>	
Privacy Amplification in the Isolated Qubits Model	785
<i>Yi-Kai Liu</i>	

Discrete Logarithms

Generic Hardness of the Multiple Discrete Logarithm Problem	817
<i>Aaram Yun</i>	

Author Index	837
------------------------	-----