

Contents – Part II

Asiacrypt 2016 Award Papers

| | |
|---|----|
| Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64 | 3 |
| <i>Yosuke Todo, Gregor Leander, and Yu Sasaki</i> | |
| Cliptography: Clipping the Power of Kleptographic Attacks | 34 |
| <i>Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou</i> | |

Zero Knowledge

| | |
|--|-----|
| Zero-Knowledge Accumulators and Set Algebra | 67 |
| <i>Esha Ghosh, Olga Ohrimenko, Dimitrios Papadopoulos, Roberto Tamassia, and Nikos Triandopoulos</i> | |
| Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption | 101 |
| <i>Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang</i> | |

Post Quantum Cryptography

| | |
|---|-----|
| From 5-Pass \mathcal{MQ} -Based Identification to \mathcal{MQ} -Based Signatures | 135 |
| <i>Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe</i> | |
| Collapse-Binding Quantum Commitments Without Random Oracles | 166 |
| <i>Dominique Unruh</i> | |
| Digital Signatures Based on the Hardness of Ideal Lattice Problems in All Rings | 196 |
| <i>Vadim Lyubashevsky</i> | |

Provable Security

| | |
|--|-----|
| Adaptive Oblivious Transfer and Generalization | 217 |
| <i>Olivier Blazy, Céline Chevalier, and Paul Germouty</i> | |
| Selective Opening Security from Simulatable Data Encapsulation | 248 |
| <i>Felix Heuer and Bertram Poettering</i> | |

Selective-Opening Security in the Presence of Randomness Failures 278
Viet Tung Hoang, Jonathan Katz, Adam O’Neill, and Mohammad Zaheri

Efficient KDM-CCA Secure Public-Key Encryption
for Polynomial Functions 307
Shuai Han, Shengli Liu, and Lin Lyu

Structure-Preserving Smooth Projective Hashing 339
Olivier Blazy and Céline Chevalier

Digital Signature

Signature Schemes with Efficient Protocols and Dynamic Group Signatures
from Lattice Assumptions 373
*Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen,
and Huaxiong Wang*

Towards Tightly Secure Lattice Short Signature and Id-Based Encryption . . . 404
Xavier Boyen and Qinyi Li

From Identification to Signatures, Tightly: A Framework and Generic
Transforms 435
Mihir Bellare, Bertram Poettering, and Douglas Stebila

How to Obtain Fully Structure-Preserving (Automorphic) Signatures
from Structure-Preserving Ones. 465
*Yuyu Wang, Zongyang Zhang, Takahiro Matsuda, Goichiro Hanaoka,
and Keisuke Tanaka*

Functional and Homomorphic Cryptography

Multi-key Homomorphic Authenticators. 499
Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, and Elena Pagnin

Multi-input Functional Encryption with Unbounded-Message Security 531
Vipul Goyal, Aayush Jain, and Adam O’Neill

Verifiable Functional Encryption. 557
Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai

ABE and IBE

Dual System Encryption Framework in Prime-Order Groups
via Computational Pair Encodings. 591
Nuttapong Attrapadung

Efficient IBE with Tight Reduction to Standard Assumption
in the Multi-challenge Setting 624
Junqing Gong, Xiaolei Dong, Jie Chen, and Zhenfu Cao

Déjà Q All Over Again: Tighter and Broader Reductions
of q -Type Assumptions 655
Melissa Chase, Mary Maller, and Sarah Meiklejohn

Partitioning via Non-linear Polynomial Functions: More Compact IBES
from Ideal Lattices and Bilinear Maps 682
Shuichi Katsumata and Shota Yamada

Foundation

How to Generate and Use Universal Samplers 715
*Dennis Hofheinz, Tibor Jager, Dakshita Khurana, Amit Sahai,
Brent Waters, and Mark Zhandry*

Iterated Random Oracle: A Universal Approach for Finding Loss
in Security Reduction 745
*Fuchun Guo, Willy Susilo, Yi Mu, Rongmao Chen, Jianchang Lai,
and Guomin Yang*

NIZKs with an Untrusted CRS: Security in the Face of Parameter
Subversion 777
Mihir Bellare, Georg Fuchsbauer, and Alessandra Scafuro

Cryptographic Protocol

Universal Composition with Responsive Environments 807
*Jan Camenisch, Robert R. Enderlein, Stephan Krenn, Ralf Küsters,
and Daniel Rausch*

A Shuffle Argument Secure in the Generic Model. 841
Prastudy Fauzi, Helger Lipmaa, and Michał Zajac

Efficient Public-Key Distance Bounding Protocol 873
Handan Kılınç and Serge Vaudenay

Indistinguishable Proofs of Work or Knowledge 902
*Foteini Baldimtsi, Aggelos Kiayias, Thomas Zacharias,
and Bingsheng Zhang*

Multi-party Computation

Size-Hiding Computation for Multiple Parties 937
*Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka,
and Eiji Okamoto*

How to Circumvent the Two-Ciphertext Lower Bound for Linear
Garbling Schemes 967
Carmen Kempka, Ryo Kikuchi, and Koutarou Suzuki

Constant-Round Asynchronous Multi-Party Computation Based
on One-Way Functions 998
Sandro Coretti, Juan Garay, Martin Hirt, and Vassilis Zikas

Reactive Garbling: Foundation, Instantiation, Application. 1022
Jesper Buus Nielsen and Samuel Ranellucci

Author Index 1053

Contents – Part I

Asiacrypt 2016 Best Paper

| | |
|---|---|
| Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds | 3 |
| <i>Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène</i> | |

Mathematical Analysis I

| | |
|--|----|
| A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm | 37 |
| <i>Palash Sarkar and Shashank Singh</i> | |
| On the Security of Supersingular Isogeny Cryptosystems | 63 |
| <i>Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti</i> | |

AES and White-Box

| | |
|--|-----|
| Simpira v2: A Family of Efficient Permutations Using the AES Round Function | 95 |
| <i>Shay Gueron and Nicky Mouha</i> | |
| Towards Practical Whitebox Cryptography: Optimizing Efficiency and Space Hardness. | 126 |
| <i>Andrey Bogdanov, Takanori Isobe, and Elmar Tischhauser</i> | |
| Efficient and Provable White-Box Primitives | 159 |
| <i>Pierre-Alain Fouque, Pierre Karpman, Paul Kirchner, and Brice Minaud</i> | |

Hash Function

| | |
|---|-----|
| MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity | 191 |
| <i>Martin Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen</i> | |
| Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks. | 220 |
| <i>Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter</i> | |

| | |
|--|-----|
| Linear Structures: Applications to Cryptanalysis of Round-Reduced KECCAK | 249 |
| <i>Jian Guo, Meicheng Liu, and Ling Song</i> | |
| Randomness | |
| When Are Fuzzy Extractors Possible? | 277 |
| <i>Benjamin Fuller, Leonid Reyzin, and Adam Smith</i> | |
| More Powerful and Reliable Second-Level Statistical Randomness Tests for NIST SP 800-22 | 307 |
| <i>Shuangyi Zhu, Yuan Ma, Jingqiang Lin, Jia Zhuang, and Jiwu Jing</i> | |
| Authenticated Encryption | |
| Trick or Tweak: On the (In)security of OTR’s Tweaks | 333 |
| <i>Raphael Bost and Olivier Sanders</i> | |
| Universal Forgery and Key Recovery Attacks on ELMd Authenticated Encryption Algorithm | 354 |
| <i>Asli Bay, Oğuzhan Ersoy, and Ferhat Karakoç</i> | |
| Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes | 369 |
| <i>Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Victor Lomné, and Florian Mendel</i> | |
| Authenticated Encryption with Variable Stretch | 396 |
| <i>Reza Reyhanitabar, Serge Vaudenay, and Damian Vizár</i> | |
| Block Cipher I | |
| Salvaging Weak Security Bounds for Blockcipher-Based Constructions | 429 |
| <i>Thomas Shrimpton and R. Seth Terashima</i> | |
| How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers. | 455 |
| <i>Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu</i> | |
| Design Strategies for ARX with Provable Bounds: SPARX and LAX | 484 |
| <i>Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov</i> | |
| SCA and Leakage Resilience I | |
| Side-Channel Analysis Protection and Low-Latency in Action: – Case Study of PRINCE and Midori – | 517 |
| <i>Amir Moradi and Tobias Schneider</i> | |

Characterisation and Estimation of the Key Rank Distribution
in the Context of Side Channel Evaluations 548
Daniel P. Martin, Luke Mather, Elisabeth Oswald, and Martijn Stam

Taylor Expansion of Maximum Likelihood Attacks for Masked
and Shuffled Implementations. 573
*Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Olivier Rioul,
François-Xavier Standaert, and Yannick Tégli*

Unknown-Input Attacks in the Parallel Setting: Improving the Security
of the CHES 2012 Leakage-Resilient PRF 602
*Marcel Medwed, François-Xavier Standaert, Venzislav Nikov,
and Martin Feldhofer*

Block Cipher II

A New Algorithm for the Unbalanced Meet-in-the-Middle Problem. 627
Ivica Nikolić and Yu Sasaki

Applying MILP Method to Searching Integral Distinguishers Based
on Division Property for 6 Lightweight Block Ciphers. 648
Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin

Reverse Cycle Walking and Its Applications. 679
Sarah Miracle and Scott Yilek

Mathematical Analysis II

Optimization of LPN Solving Algorithms 703
Sonia Bogos and Serge Vaudenay

The Kernel Matrix Diffie-Hellman Assumption. 729
Paz Morillo, Carla Ràfols, and Jorge L. Villar

Cryptographic Applications of Capacity Theory: On the Optimality
of Coppersmith’s Method for Univariate Polynomials 759
Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr

A Key Recovery Attack on MDPC with CCA Security
Using Decoding Errors 789
Qian Guo, Thomas Johansson, and Paul Stankovski

SCA and Leakage Resilience II

A Tale of Two Shares: Why Two-Share Threshold Implementation Seems
Worthwhile—and Why It Is Not. 819
Cong Chen, Mohammad Farmani, and Thomas Eisenbarth

Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions. 844
Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, Fuchun Guo, and Mingwu Zhang

Efficient Public-Key Cryptography with Bounded Leakage and Tamper Resilience. 877
Antonio Faonio and Daniele Venturi

Public-Key Cryptosystems Resilient to Continuous Tampering and Leakage of Arbitrary Functions 908
Eiichiro Fujisaki and Keita Xagawa

Author Index 939



<http://www.springer.com/978-3-662-53889-0>

Advances in Cryptology - ASIACRYPT 2016
22nd International Conference on the Theory and
Application of Cryptology and Information Security,
Hanoi, Vietnam, December 4-8, 2016, Proceedings,
Part II

Cheon, J.H.; Takagi, T. (Eds.)

2016, XXIV, 1055 p. 198 illus., Softcover

ISBN: 978-3-662-53889-0