

## 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
<i>Viet Tung Hoang, Jonathan Katz, Adam O'Neill, and Mohammad Zaheri</i>	

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

Structure-Preserving Smooth Projective Hashing . . . . .	339
<i>Olivier Blazy and Céline Chevalier</i>	

## Digital Signature

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

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

From Identification to Signatures, Tightly: A Framework and Generic Transforms . . . . .	435
<i>Mihir Bellare, Bertram Poettering, and Douglas Stebila</i>	

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

## Functional and Homomorphic Cryptography

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

Multi-input Functional Encryption with Unbounded-Message Security . . . . .	531
<i>Vipul Goyal, Aayush Jain, and Adam O'Neill</i>	

Verifiable Functional Encryption. . . . .	557
<i>Saikrishna Badrinarayanan, Vipul Goyal, Aayush Jain, and Amit Sahai</i>	

## ABE and IBE

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

Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting . . . . .	624
<i>Junqing Gong, Xiaolei Dong, Jie Chen, and Zhenfu Cao</i>	
Déjà Q All Over Again: Tighter and Broader Reductions of $q$ -Type Assumptions . . . . .	655
<i>Melissa Chase, Mary Maller, and Sarah Meiklejohn</i>	
Partitioning via Non-linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps . . . . .	682
<i>Shuichi Katsumata and Shota Yamada</i>	
<b>Foundation</b>	
How to Generate and Use Universal Samplers . . . . .	715
<i>Dennis Hofheinz, Tibor Jager, Dakshita Khurana, Amit Sahai, Brent Waters, and Mark Zhandry</i>	
Iterated Random Oracle: A Universal Approach for Finding Loss in Security Reduction . . . . .	745
<i>Fuchun Guo, Willy Susilo, Yi Mu, Rongmao Chen, Jianchang Lai, and Guomin Yang</i>	
NIZKs with an Untrusted CRS: Security in the Face of Parameter Subversion . . . . .	777
<i>Mihir Bellare, Georg Fuchsbauer, and Alessandra Scafuro</i>	
<b>Cryptographic Protocol</b>	
Universal Composition with Responsive Environments . . . . .	807
<i>Jan Camenisch, Robert R. Enderlein, Stephan Krenn, Ralf Küsters, and Daniel Rausch</i>	
A Shuffle Argument Secure in the Generic Model. . . . .	841
<i>Prastudy Fauzi, Helger Lipmaa, and Michał Zając</i>	
Efficient Public-Key Distance Bounding Protocol . . . . .	873
<i>Handan Kılınç and Serge Vaudenay</i>	
Indistinguishable Proofs of Work or Knowledge . . . . .	902
<i>Foteini Baldimtsi, Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang</i>	
<b>Multi-party Computation</b>	
Size-Hiding Computation for Multiple Parties . . . . .	937
<i>Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto</i>	

How to Circumvent the Two-Ciphertext Lower Bound for Linear Garbling Schemes . . . . .	967
<i>Carmen Kempka, Ryo Kikuchi, and Koutarou Suzuki</i>	
Constant-Round Asynchronous Multi-Party Computation Based on One-Way Functions . . . . .	998
<i>Sandro Coretti, Juan Garay, Martin Hirt, and Vassilis Zikas</i>	
Reactive Garbling: Foundation, Instantiation, Application. . . . .	1022
<i>Jesper Buus Nielsen and Samuel Ranellucci</i>	
<b>Author Index</b> . . . . .	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>Aslı 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
<i>Daniel P. Martin, Luke Mather, Elisabeth Oswald, and Martijn Stam</i>	
Taylor Expansion of Maximum Likelihood Attacks for Masked and Shuffled Implementations. . . . .	573
<i>Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Olivier Rioul, François-Xavier Standaert, and Yannick Tégli</i>	
Unknown-Input Attacks in the Parallel Setting: Improving the Security of the CHES 2012 Leakage-Resilient PRF . . . . .	602
<i>Marcel Medwed, François-Xavier Standaert, Ventsislav Nikov, and Martin Feldhofer</i>	
<b>Block Cipher II</b>	
A New Algorithm for the Unbalanced Meet-in-the-Middle Problem. . . . .	627
<i>Ivica Nikolić and Yu Sasaki</i>	
Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers. . . . .	648
<i>Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin</i>	
Reverse Cycle Walking and Its Applications. . . . .	679
<i>Sarah Miracle and Scott Yilek</i>	
<b>Mathematical Analysis II</b>	
Optimization of LPN Solving Algorithms . . . . .	703
<i>Sonia Bogos and Serge Vaudenay</i>	
The Kernel Matrix Diffie-Hellman Assumption. . . . .	729
<i>Paz Morillo, Carla Ràfols, and Jorge L. Villar</i>	
Cryptographic Applications of Capacity Theory: On the Optimality of Coppersmith’s Method for Univariate Polynomials . . . . .	759
<i>Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr</i>	
A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors . . . . .	789
<i>Qian Guo, Thomas Johansson, and Paul Stankovski</i>	
<b>SCA and Leakage Resilience II</b>	
A Tale of Two Shares: Why Two-Share Threshold Implementation Seems Worthwhile—and Why It Is Not. . . . .	819
<i>Cong Chen, Mohammad Farmani, and Thomas Eisenbarth</i>	

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**



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