

Contents – Part I

Best Paper

Improved Security Proofs in Lattice-Based Cryptography: Using the Rényi Divergence Rather Than the Statistical Distance	3
<i>Shi Bai, Adeline Langlois, Tancrede Lepoint, Damien Stehlé, and Ron Steinfeld</i>	

Indistinguishability Obfuscation

Multi-input Functional Encryption for Unbounded Arity Functions	27
<i>Saikrishna Badrinarayanan, Divya Gupta, Abhishek Jain, and Amit Sahai</i>	
Multi-party Key Exchange for Unbounded Parties from Indistinguishability Obfuscation	52
<i>Dakshita Khurana, Vanishree Rao, and Amit Sahai</i>	

PRFs and Hashes

Adaptively Secure Puncturable Pseudorandom Functions in the Standard Model	79
<i>Susan Hohenberger, Venkata Koppula, and Brent Waters</i>	
Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security	103
<i>Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue</i>	
New Realizations of Somewhere Statistically Binding Hashing and Positional Accumulators	121
<i>Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters, and Daniel Wichs</i>	

Discrete Logarithms and Number Theory

Computing Individual Discrete Logarithms Faster in $GF(p^n)$ with the NFS-DL Algorithm	149
<i>Aurore Guillevic</i>	
Multiple Discrete Logarithm Problems with Auxiliary Inputs	174
<i>Taechan Kim</i>	
Solving Linear Equations Modulo Unknown Divisors: Revisited	189
<i>Yao Lu, Rui Zhang, Liqiang Peng, and Dongdai Lin</i>	

Four \mathbb{Q} : Four-Dimensional Decompositions on a \mathbb{Q} -curve over the Mersenne Prime	214
<i>Craig Costello and Patrick Longa</i>	

Signatures

Efficient Fully Structure-Preserving Signatures for Large Messages	239
<i>Jens Groth</i>	
A Provably Secure Group Signature Scheme from Code-Based Assumptions.	260
<i>Martianus Frederic Ezerman, Hyung Tae Lee, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Type 2 Structure-Preserving Signature Schemes Revisited	286
<i>Sanjit Chatterjee and Alfred Menezes</i>	
Design Principles for HFEv- Based Multivariate Signature Schemes	311
<i>Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding</i>	

Multiparty Computation I

Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness	337
<i>Dana Dachman-Soled, Chang Liu, Charalampos Papamanthou, Elaine Shi, and Uzi Vishkin</i>	
Three-Party ORAM for Secure Computation.	360
<i>Sky Faber, Stanislaw Jarecki, Sotirios Kentros, and Boyang Wei</i>	
On Cut-and-Choose Oblivious Transfer and Its Variants	386
<i>Vladimir Kolesnikov and Ranjit Kumaresan</i>	

Public Key Encryption

An Asymptotically Optimal Method for Converting Bit Encryption to Multi-Bit Encryption	415
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	
Selective Opening Security for Receivers	443
<i>Carmit Hazay, Arpita Patra, and Bogdan Warinschi</i>	
Function-Hiding Inner Product Encryption	470
<i>Allison Bishop, Abhishek Jain, and Lucas Kowalczyk</i>	

ABE and IBE

Idealizing Identity-Based Encryption	495
<i>Dennis Hofheinz, Christian Matt, and Ueli Maurer</i>	
A Framework for Identity-Based Encryption with Almost Tight Security	521
<i>Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada</i>	
Riding on Asymmetry: Efficient ABE for Branching Programs	550
<i>Sergey Gorbunov and Dhinakaran Vinayagamurthy</i>	
Conversions Among Several Classes of Predicate Encryption and Applications to ABE with Various Compactness Tradeoffs.	575
<i>Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada</i>	

Zero-Knowledge

QA-NIZK Arguments in Asymmetric Groups: New Tools and New Constructions	605
<i>Alonso González, Alejandro Hevia, and Carla Ràfols</i>	
Dual-System Simulation-Soundness with Applications to UC-PAKE and More	630
<i>Charanjit S. Jutla and Arnab Roy</i>	
Secret Sharing and Statistical Zero Knowledge	656
<i>Vinod Vaikuntanathan and Prashant Nalini Vasudevan</i>	
Compactly Hiding Linear Spans: Tightly Secure Constant-Size Simulation-Sound QA-NIZK Proofs and Applications	681
<i>Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung</i>	

Multiparty Computation II

A Unified Approach to MPC with Preprocessing Using OT	711
<i>Tore Kasper Frederiksen, Marcel Keller, Emmanuela Orsini, and Peter Scholl</i>	
Secure Computation from Millionaire	736
<i>Abhi Shelat and Muthuramakrishnan Venkitasubramaniam</i>	
Garbling Scheme for Formulas with Constant Size of Garbled Gates	758
<i>Carmen Kempka, Ryo Kikuchi, Susumu Kiyoshima, and Koutarou Suzuki</i>	
Card-Based Cryptographic Protocols Using a Minimal Number of Cards	783
<i>Alexander Koch, Stefan Walzer, and Kevin Härtel</i>	

Author Index	809
-------------------------------	-----

Contents – Part II

Attacks on ASASA

Key-Recovery Attacks on ASASA	3
<i>Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman</i>	

Number Field Sieve

The Tower Number Field Sieve	31
<i>Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung</i>	

Hashes and MACs

On the Impact of Known-Key Attacks on Hash Functions	59
<i>Bart Mennink and Bart Preneel</i>	
Generic Security of NMAC and HMAC with Input Whitening	85
<i>Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro</i>	

Symmetric Encryption

On the Optimality of Non-Linear Computations of Length-Preserving Encryption Schemes	113
<i>Mridul Nandi</i>	
Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing	134
<i>Benoît Cogliati and Yannick Seurin</i>	
An Inverse-Free Single-Keyed Tweakable Enciphering Scheme.	159
<i>Ritam Bhaumik and Mridul Nandi</i>	

Foundations

On Black-Box Complexity of Universally Composable Security in the CRS Model.	183
<i>Carmit Hazay and Muthuramakrishnan Venkatasubramanian</i>	
Public Verifiability in the Covert Model (Almost) for Free.	210
<i>Vladimir Kolesnikov and Alex J. Malozemoff</i>	

Limits of Extractability Assumptions with Distributional Auxiliary Input	236
<i>Elette Boyle and Rafael Pass</i>	
Composable and Modular Anonymous Credentials: Definitions and Practical Constructions.	262
<i>Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, and Markulf Kohlweiss</i>	
Side-Channel Attacks	
ASCA, SASCA and DPA with Enumeration: Which One Beats the Other and When?.	291
<i>Vincent Grosso and François-Xavier Standaert</i>	
Counting Keys in Parallel After a Side Channel Attack	313
<i>Daniel P. Martin, Jonathan F. O’Connell, Elisabeth Oswald, and Martijn Stam</i>	
A Unified Metric for Quantifying Information Leakage of Cryptographic Devices Under Power Analysis Attacks	338
<i>Liwei Zhang, A. Adam Ding, Yunsi Fei, and Pei Luo</i>	
How Secure is AES Under Leakage	361
<i>Andrey Bogdanov and Takanori Isobe</i>	
Design of Block Ciphers	
A Synthetic Indifferentiability Analysis of Interleaved Double-Key Even-Mansour Ciphers.	389
<i>Chun Guo and Dongdai Lin</i>	
Midori: A Block Cipher for Low Energy	411
<i>Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni</i>	
Optimally Secure Block Ciphers from Ideal Primitives.	437
<i>Stefano Tessaro</i>	
Authenticated Encryption	
Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption	465
<i>Bart Mennink, Reza Reyhanitabar, and Damian Vizár</i>	
Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates.	490
<i>Christoph Dobraunig, Maria Eichlseder, and Florian Mendel</i>	

Collision Attacks Against CAESAR Candidates: Forgery and Key-Recovery Against AEZ and Marble	510
<i>Thomas Fuhr, Gaëtan Leurent, and Valentin Suder</i>	

Symmetric Analysis

Optimized Interpolation Attacks on LowMC.	535
<i>Itai Dinur, Yunwen Liu, Willi Meier, and Qingju Wang</i>	
Another Tradeoff Attack on Sprout-Like Stream Ciphers	561
<i>Bin Zhang and Xinxin Gong</i>	
Reverse-Engineering of the Cryptanalytic Attack Used in the Flame Super-Malware	586
<i>Max Fillinger and Marc Stevens</i>	
Analysis of SHA-512/224 and SHA-512/256	612
<i>Christoph Dobraunig, Maria Eichlseder, and Florian Mendel</i>	

Cryptanalysis

Tradeoff Cryptanalysis of Memory-Hard Functions	633
<i>Alex Biryukov and Dmitry Khovratovich</i>	
Property Preserving Symmetric Encryption Revisited.	658
<i>Sanjit Chatterjee and M. Prem Laxman Das</i>	
Refinements of the k -tree Algorithm for the Generalized Birthday Problem. . . .	683
<i>Ivica Nikolić and Yu Sasaki</i>	
How to Sequentialize Independent Parallel Attacks?: Biased Distributions Have a Phase Transition.	704
<i>Sonia Bogos and Serge Vaudenay</i>	

Privacy and Lattices

Pure Differential Privacy for Rectangle Queries via Private Partitions	735
<i>Cynthia Dwork, Moni Naor, Omer Reingold, and Guy N. Rothblum</i>	
Implementing Candidate Graded Encoding Schemes from Ideal Lattices	752
<i>Martin R. Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois</i>	
New Circular Security Counterexamples from Decision Linear and Learning with Errors	776
<i>Allison Bishop, Susan Hohenberger, and Brent Waters</i>	

Author Index	801
-------------------------------	-----

Advances in Cryptology -- ASIACRYPT 2015
21st International Conference on the Theory and
Application of Cryptology and Information
Security, Auckland, New Zealand, November 29 --
December 3, 2015, Proceedings, Part I
Iwata, T.; Cheon, J.H. (Eds.)
2015, XXV, 810 p. 93 illus., Softcover
ISBN: 978-3-662-48796-9