Contents – Part I

Best Paper

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

Indistinguishability Obfuscation

Multi-input Functional Encryption for Unbounded Arity Functions ............. 27
   Saikrishna Badrinarayanan, Divya Gupta, Abhishek Jain, and Amit Sahai

Multi-party Key Exchange for Unbounded Parties from Indistinguishability Obfuscation ................................................................. 52
   Dakshita Khurana, Vanishree Rao, and Amit Sahai

PRFs and Hashes

Adaptively Secure Puncturable Pseudorandom Functions in the Standard Model .......................................................... 79
   Susan Hohenberger, Venkata Koppula, and Brent Waters

Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security ................................................. 103
   Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue

New Realizations of Somewhere Statistically Binding Hashing and Positional Accumulators .................................................. 121
   Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters, and Daniel Wichs

Discrete Logarithms and Number Theory

Computing Individual Discrete Logarithms Faster in $GF(p^n)$ with the NFS-DL Algorithm .......................................................... 149
   Aurore Guillevic

Multiple Discrete Logarithm Problems with Auxiliary Inputs .................. 174
   Taechan Kim

Solving Linear Equations Modulo Unknown Divisors: Revisited ............. 189
   Yao Lu, Rui Zhang, Liqiang Peng, and Dongdai Lin
FourQ: Four-Dimensional Decompositions on a $\mathbb{Q}$-curve over the Mersenne Prime .................................................. 214
   Craig Costello and Patrick Longa

Signatures

Efficient Fully Structure-Preserving Signatures for Large Messages .......... 239
   Jens Groth

A Provably Secure Group Signature Scheme from Code-Based Assumptions .......................................................... 260
   Martianus Frederic Ezerman, Hyung Tae Lee, San Ling, Khoa Nguyen,
   and Huaxiong Wang

Type 2 Structure-Preserving Signature Schemes Revisited .................... 286
   Sanjit Chatterjee and Alfred Menezes

Design Principles for HFEv- Based Multivariate Signature Schemes ........ 311
   Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao,
   and Jintai Ding

Multiparty Computation I

Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness .......................................................... 337
   Dana Dachman-Soled, Chang Liu, Charalampos Papamanthou,
   Elaine Shi, and Uzi Vishkin

Three-Party ORAM for Secure Computation .................................. 360
   Sky Faber, Stanislaw Jarecki, Sotirios Kentros, and Boyang Wei

On Cut-and-Choose Oblivious Transfer and Its Variants .................... 386
   Vladimir Kolesnikov and Ranjit Kumaresan

Public Key Encryption

An Asymptotically Optimal Method for Converting Bit Encryption to Multi-Bit Encryption ........................................... 415
   Takahiro Matsuda and Goichiro Hanaoka

Selective Opening Security for Receivers .................................... 443
   Carmit Hazay, Arpita Patra, and Bogdan Warinschi

Function-Hiding Inner Product Encryption .................................. 470
   Allison Bishop, Abhishek Jain, and Lucas Kowalczyk
ABE and IBE

Idealizing Identity-Based Encryption ........................................... 495
   Dennis Hofheinz, Christian Matt, and Ueli Maurer

A Framework for Identity-Based Encryption with Almost Tight Security .... 521
   Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada

Riding on Asymmetry: Efficient ABE for Branching Programs ............... 550
   Sergey Gorbunov and Dhinakaran Vinayagamurthy

Conversions Among Several Classes of Predicate Encryption
   and Applications to ABE with Various Compactness Tradeoffs ............ 575
   Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada

Zero-Knowledge

QA-NIZK Arguments in Asymmetric Groups: New Tools
   and New Constructions ...................................................... 605
   Alonso González, Alejandro Hevia, and Carla Ràfols

Dual-System Simulation-Soundness with Applications to UC-PAKE
   and More ................................................................. 630
   Charanjit S. Jutla and Arnab Roy

Secret Sharing and Statistical Zero Knowledge .................................. 656
   Vinod Vaikuntanathan and Prashant Nalini Vasudevan

Compactly Hiding Linear Spans: Tightly Secure Constant-Size
Simulation-Sound QA-NIZK Proofs and Applications .......................... 681
   Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung

Multiparty Computation II

A Unified Approach to MPC with Preprocessing Using OT .................... 711
   Tore Kasper Frederiksen, Marcel Keller, Emmanuela Orsini,
   and Peter Scholl

Secure Computation from Millionaire .......................................... 736
   Abhi Shelat and Muthuramakrishnan Venkitasubramaniam

Garbling Scheme for Formulas with Constant Size of Garbled Gates ....... 758
   Carmen Kempka, Ryo Kikuchi, Susumu Kiyoshima,
   and Koutarou Suzuki

Card-Based Cryptographic Protocols Using a Minimal Number of Cards .... 783
   Alexander Koch, Stefan Walzer, and Kevin Härtel

Author Index .................................................................................. 809
## Contents – Part II

### Attacks on ASASA

Key-Recovery Attacks on ASASA ............................................. 3  
*Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman*

### Number Field Sieve

The Tower Number Field Sieve ............................................. 31  
*Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung*

### Hashes and MACs

On the Impact of Known-Key Attacks on Hash Functions .............. 59  
*Bart Mennink and Bart Preneel*

Generic Security of NMAC and HMAC with Input Whitening ........... 85  
*Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro*

### Symmetric Encryption

On the Optimality of Non-Linear Computations of Length-Preserving Encryption Schemes ............................................. 113  
*Mridul Nandi*

Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing ................................. 134  
*Benoît Cogliati and Yannick Seurin*

An Inverse-Free Single-Keyed Tweakable Enciphering Scheme .......... 159  
*Ritam Bhaumik and Mridul Nandi*

### Foundations

On Black-Box Complexity of Universally Composable Security in the CRS Model ......................................................... 183  
*Carmit Hazay and Muthuramakrishnan Venkitasubramaniam*

Public Verifiability in the Covert Model (Almost) for Free ............. 210  
*Vladimir Kolesnikov and Alex J. Malozemoff*
Limits of Extractability Assumptions with Distributional Auxiliary Input .......................... 236

_Elette Boyle and Rafael Pass_

Composable and Modular Anonymous Credentials: Definitions and Practical Constructions ................................................. 262

_Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, and Markulf Kohlweiss_

**Side-Channel Attacks**

ASCA, SASCA and DPA with Enumeration: Which One Beats the Other and When? .................................................................................................................. 291

_Vincent Grosso and François-Xavier Standaert_

Counting Keys in Parallel After a Side Channel Attack ........................................................................................................... 313

_Daniel P. Martin, Jonathan F. O’Connell, Elisabeth Oswald, and Martijn Stam_

A Unified Metric for Quantifying Information Leakage of Cryptographic Devices Under Power Analysis Attacks .................................................................................................................. 338

_Liwei Zhang, A. Adam Ding, Yunsi Fei, and Pei Luo_

How Secure is AES Under Leakage ......................................................................................................................... 361

_Andrey Bogdanov and Takanori Isobe_

**Design of Block Ciphers**

A Synthetic Indifferentiability Analysis of Interleaved Double-Key Even-Mansour Ciphers ......................................................................................................................... 389

_Chun Guo and Dongdai Lin_

Midori: A Block Cipher for Low Energy ......................................................................................................................... 411

_Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni_

Optimally Secure Block Ciphers from Ideal Primitives ........................................................................................................... 437

_Stefano Tessaro_

**Authenticated Encryption**

Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption ......................................................................................................................... 465

_Bart Mennink, Reza Reyhanitabar, and Damian Vizár_

Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates ......................................................................................................................... 490

_Christoph Dobraunig, Maria Eichlseder, and Florian Mendel_
Collision Attacks Against CAESAR Candidates: Forgery and Key-Recovery Against AEZ and Marble ........................................ 510
Thomas Fuhr, Gaëtan Leurent, and Valentin Suder

Symmetric Analysis

Optimized Interpolation Attacks on LowMC. ........................................ 535
Itai Dinur, Yunwen Liu, Willi Meier, and Qingju Wang

Another Tradeoff Attack on Sprout-Like Stream Ciphers ................. 561
Bin Zhang and Xinxin Gong

Reverse-Engineering of the Cryptanalytic Attack Used in the Flame Super-Malware .............................................................. 586
Max Fillinger and Marc Stevens

Analysis of SHA-512/224 and SHA-512/256 ........................................ 612
Christoph Dobraunig, Maria Eichlseder, and Florian Mendel

Cryptanalysis

Tradeoff Cryptanalysis of Memory-Hard Functions ...................... 633
Alex Biryukov and Dmitry Khovratovich

Property Preserving Symmetric Encryption Revisited .................... 658
Sanjit Chatterjee and M. Prem Laxman Das

Refinements of the $k$-tree Algorithm for the Generalized Birthday Problem. . . 683
Ivica Nikolić and Yu Sasaki

How to Sequentialize Independent Parallel Attacks?: Biased Distributions Have a Phase Transition ...................................................... 704
Sonia Bogos and Serge Vaudenay

Privacy and Lattices

Pure Differential Privacy for Rectangle Queries via Private Partitions ...... 735
Cynthia Dwork, Moni Naor, Omer Reingold, and Guy N. Rothblum

Implementing Candidate Graded Encoding Schemes from Ideal Lattices .... 752
Martin R. Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois

New Circular Security Counterexamples from Decision Linear and Learning with Errors ...................................................... 776
Allison Bishop, Susan Hohenberger, and Brent Waters

Author Index ................................................................. 801