

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
<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