

Contents – Part I

Cryptanalysis

LP Solutions of Vectorial Integer Subset Sums – Cryptanalysis of Galbraith’s Binary Matrix LWE	3
<i>Gottfried Herold and Alexander May</i>	
Improved Algorithms for the Approximate k -List Problem in Euclidean Norm	16
<i>Gottfried Herold and Elena Kirshanova</i>	
Zeroizing Attacks on Indistinguishability Obfuscation over CLT13	41
<i>Jean-Sébastien Coron, Moon Sung Lee, Tancrede Lepoint, and Mehdi Tibouchi</i>	

Protocols

Cut Down the Tree to Achieve Constant Complexity in Divisible E-cash	61
<i>David Pointcheval, Olivier Sanders, and Jacques Traoré</i>	
Asymptotically Tight Bounds for Composing ORAM with PIR	91
<i>Ittai Abraham, Christopher W. Fletcher, Kartik Nayak, Benny Pinkas, and Ling Ren</i>	
Predictable Arguments of Knowledge	121
<i>Antonio Faonio, Jesper Buus Nielsen, and Daniele Venturi</i>	
Removing Erasures with Explainable Hash Proof Systems	151
<i>Michel Abdalla, Fabrice Benhamouda, and David Pointcheval</i>	
Scalable Multi-party Private Set-Intersection	175
<i>Carmit Hazay and Muthuramakrishnan Venkitasubramaniam</i>	

Encryption Schemes

Tightly Secure IBE Under Constant-Size Master Public Key	207
<i>Jie Chen, Junqing Gong, and Jian Weng</i>	
Separating IND-CPA and Circular Security for Unbounded Length Key Cycles	232
<i>Rishab Goyal, Venkata Koppula, and Brent Waters</i>	

Structure-Preserving Chosen-Ciphertext Security with Shorter
Verifiable Ciphertexts 247
Benoît Libert, Thomas Peters, and Chen Qian

Leakage-Resilient and Non-Malleable Codes

Non-malleable Codes with Split-State Refresh 279
Antonio Faonio and Jesper Buus Nielsen

Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable
and Updatable Non-malleable Codes 310
Dana Dachman-Soled, Mukul Kulkarni, and Aria Shahverdi

Fully Leakage-Resilient Codes 333
Antonio Faonio and Jesper Buus Nielsen

Number Theory and Diffie-Hellman

On the Bit Security of Elliptic Curve Diffie–Hellman 361
Barak Shani

Extended Tower Number Field Sieve with Application to Finite Fields
of Arbitrary Composite Extension Degree 388
Taechan Kim and Jinhyuck Jeong

Provably Secure NTRU Instances over Prime Cyclotomic Rings 409
Yang Yu, Guangwu Xu, and Xiaoyun Wang

Equivalences and Black-Box Separations of Matrix Diffie-Hellman
Problems 435
Jorge L. Villar

Author Index 465

Contents – Part II

Encryption with Access Control

Dual System Framework in Multilinear Settings and Applications to Fully Secure (Compact) ABE for Unbounded-Size Circuits.	3
<i>Nuttapong Attrapadung</i>	
CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions.	36
<i>Fabrice Benhamouda, Florian Bourse, and Helger Lipmaa</i>	
Bounded-Collusion Attribute-Based Encryption from Minimal Assumptions	67
<i>Gene Itkis, Emily Shen, Mayank Varia, David Wilson, and Arkady Yerukhimovich</i>	
Access Control Encryption for Equality, Comparison, and More	88
<i>Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, and Claudio Orlandi</i>	

Special Signatures

Deterring Certificate Subversion: Efficient Double-Authentication-Preventing Signatures	121
<i>Mihir Bellare, Bertram Poettering, and Douglas Stebila</i>	
Chameleon-Hashes with Ephemeral Trapdoors: And Applications to Invisible Sanitizable Signatures.	152
<i>Jan Camenisch, David Derler, Stephan Krenn, Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig</i>	
Improved Structure Preserving Signatures Under Standard Bilinear Assumptions.	183
<i>Charanjit S. Jutla and Arnab Roy</i>	

Fully Homomorphic Encryption

Chosen-Ciphertext Secure Fully Homomorphic Encryption.	213
<i>Ran Canetti, Srinivasan Raghuraman, Silas Richelson, and Vinod Vaikuntanathan</i>	
Circuit-Private Multi-key FHE	241
<i>Wutichai Chongchitmate and Rafail Ostrovsky</i>	

FHE over the Integers: Decomposed and Batched in the Post-Quantum Regime	271
<i>Daniel Benarroch, Zvika Brakerski, and Tancrede Lepoint</i>	

Real-World Schemes

Ceremonies for End-to-End Verifiable Elections	305
<i>Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang</i>	
A Modular Security Analysis of EAP and IEEE 802.11	335
<i>Chris Brzuska and Håkon Jacobsen</i>	

Multiparty Computation

On the Computational Overhead of MPC with Dishonest Majority	369
<i>Jesper Buus Nielsen and Samuel Ranellucci</i>	
Better Two-Round Adaptive Multi-party Computation	396
<i>Ran Canetti, Oxana Poburinnaya, and Muthuramakrishnan Venkitasubramaniam</i>	
Constant Round Adaptively Secure Protocols in the Tamper-Proof Hardware Model	428
<i>Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam</i>	

Primitives

Constrained Pseudorandom Functions for Unconstrained Inputs Revisited: Achieving Verifiability and Key Delegation	463
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
Constraining Pseudorandom Functions Privately	494
<i>Dan Boneh, Kevin Lewi, and David J. Wu</i>	
Universal Samplers with Fast Verification	525
<i>Venkata Koppula, Andrew Poelstra, and Brent Waters</i>	

Author Index	555
-------------------------------	-----

Public-Key Cryptography – PKC 2017

20th IACR International Conference on Practice and
Theory in Public-Key Cryptography, Amsterdam, The
Netherlands, March 28-31, 2017, Proceedings, Part I
Fehr, S. (Ed.)

2017, XIV, 466 p. 32 illus., Softcover

ISBN: 978-3-662-54364-1