

Contents – Part II

Cryptanalysis

Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields	3
<i>Christophe Petit, Michiel Kisters, and Ange Messeng</i>	
Degenerate Curve Attacks: Extending Invalid Curve Attacks to Edwards Curves and Other Models.	19
<i>Samuel Neves and Mehdi Tibouchi</i>	
Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryptography with Weak Pseudorandomness	36
<i>Fabrice Benhamouda, Céline Chevalier, Adrian Thillard, and Damien Vergnaud</i>	
How to Generalize RSA Cryptanalyses	67
<i>Atsushi Takayasu and Noboru Kunihiro</i>	

Leakage-Resilient and Circularly Secure Encryption

Leakage-Resilient Public-Key Encryption from Obfuscation	101
<i>Dana Dachman-Soled, S. Dov Gordon, Feng-Hao Liu, Adam O'Neill, and Hong-Sheng Zhou</i>	
On Generic Constructions of Circularly-Secure, Leakage-Resilient Public-Key Encryption Schemes	129
<i>Mohammad Hajiabadi, Bruce M. Kapron, and Venkatesh Srinivasan</i>	
KDM-Security via Homomorphic Smooth Projective Hashing.	159
<i>Hoeteck Wee</i>	

Protocols

Asynchronous Secure Multiparty Computation in Constant Time	183
<i>Ran Cohen</i>	
Adaptively Secure Multi-Party Computation from LWE (via Equivocal FHE).	208
<i>Ivan Damgård, Antigoni Polychroniadou, and Vanishree Rao</i>	
Universally Composable Direct Anonymous Attestation.	234
<i>Jan Camenisch, Manu Drijvers, and Anja Lehmann</i>	

Universally Composable Authentication and Key-Exchange with Global PKI	265
<i>Ran Canetti, Daniel Shahaf, and Margarita Vald</i>	
Very-Efficient Simulatable Flipping of Many Coins into a Well: (and a New Universally-Composable Commitment Scheme)	297
<i>Luís T.A.N. Brandão</i>	
Robust Secret Sharing Schemes Against Local Adversaries	327
<i>Allison Bishop and Valerio Pastro</i>	
Primitives	
Reducing Depth in Constrained PRFs: From Bit-Fixing to NC ¹	359
<i>Nishanth Chandran, Srinivasan Raghuraman, and Dhinakaran Vinayagamurthy</i>	
Non-Malleable Functions and Their Applications	386
<i>Yu Chen, Baodong Qin, Jiang Zhang, Yi Deng, and Sherman S.M. Chow</i>	
On Public Key Encryption from Noisy Codewords	417
<i>Eli Ben-Sasson, Iddo Ben-Tov, Ivan Damgård, Yuval Ishai, and Noga Ron-Zewi</i>	
Indistinguishability Obfuscation with Non-trivial Efficiency	447
<i>Huijia Lin, Rafael Pass, Karn Seth, and Sidharth Telang</i>	
Author Index	463

Contents – Part I

CCA Security

Trading Plaintext-Awareness for Simulatability to Achieve Chosen Ciphertext Security	3
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	
Chosen-Ciphertext Security from Subset Sum	35
<i>Sebastian Faust, Daniel Masny, and Daniele Venturi</i>	
On the Hardness of Proving CCA-Security of Signed ElGamal	47
<i>David Bernhard, Marc Fischlin, and Bogdan Warinschi</i>	
CCA-Secure Keyed-Fully Homomorphic Encryption	70
<i>Junzuo Lai, Robert H. Deng, Changshe Ma, Kouichi Sakurai, and Jian Weng</i>	
On the Key Dependent Message Security of the Fujisaki-Okamoto Constructions	99
<i>Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	

Functional Encryption

Extended Nested Dual System Groups, Revisited	133
<i>Junqing Gong, Jie Chen, Xiaolei Dong, Zhenfu Cao, and Shaohua Tang</i>	
Functional Encryption for Inner Product with Full Function Privacy	164
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
Deniable Functional Encryption	196
<i>Angelo De Caro, Vincenzo Iovino, and Adam O'Neill</i>	

Identity-Based Encryption

Identity-Based Cryptosystems and Quadratic Residuosity	225
<i>Marc Joye</i>	
Identity-Based Hierarchical Key-Insulated Encryption Without Random Oracles	255
<i>Yohei Watanabe and Junji Shikata</i>	

Signatures

Attribute-Based Signatures for Circuits from Bilinear Map	283
<i>Yusuke Sakai, Nuttapong Attrapadung, and Goichiro Hanaoka</i>	
Efficient Unlinkable Sanitizable Signatures from Signatures with Re-randomizable Keys	301
<i>Nils Fleischhacker, Johannes Krupp, Giulio Malavolta, Jonas Schneider, Dominique Schröder, and Mark Simkin</i>	
Fault-Tolerant Aggregate Signatures	331
<i>Gunnar Hartung, Björn Kaidel, Alexander Koch, Jessica Koch, and Andy Rupp</i>	
Delegatable Functional Signatures	357
<i>Michael Backes, Sebastian Meiser, and Dominique Schröder</i>	
Mitigating Multi-target Attacks in Hash-Based Signatures	387
<i>Andreas Hülsing, Joost Rijneveld, and Fang Song</i>	
Nearly Optimal Verifiable Data Streaming	417
<i>Johannes Krupp, Dominique Schröder, Mark Simkin, Dario Fiore, Giuseppe Ateniese, and Stefan Nuernberger</i>	
ARMed SPHINCS: Computing a 41 KB Signature in 16 KB of RAM	446
<i>Andreas Hülsing, Joost Rijneveld, and Peter Schwabe</i>	
Author Index	471

Public-Key Cryptography – PKC 2016

19th IACR International Conference on Practice and
Theory in Public-Key Cryptography, Taipei, Taiwan,
March 6-9, 2016, Proceedings, Part II

Cheng, C.-M.; Chung, K.-M.; Persiano, G.; Yang, B.-Y.
(Eds.)

2016, XIV, 464 p. 51 illus. in color., Softcover

ISBN: 978-3-662-49386-1