

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