

Table of Contents

Leakage

Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability (or: Quadratic Residuosity Strikes Back)	1
<i>Zvika Brakerski and Shafi Goldwasser</i>	
Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks	21
<i>Yevgeniy Dodis and Krzysztof Pietrzak</i>	
Protecting Cryptographic Keys against Continual Leakage	41
<i>Ali Juma and Yevgeniy Vahlis</i>	
Securing Computation against Continuous Leakage	59
<i>Shafi Goldwasser and Guy N. Rothblum</i>	

Lattice

An Efficient and Parallel Gaussian Sampler for Lattices	80
<i>Chris Peikert</i>	
Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE	98
<i>Shweta Agrawal, Dan Boneh, and Xavier Boyen</i>	

Homomorphic Encryption

Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness	116
<i>Craig Gentry</i>	
Additively Homomorphic Encryption with d -Operand Multiplications ...	138
<i>Carlos Aguilar Melchor, Philippe Gaborit, and Javier Herranz</i>	
i -Hop Homomorphic Encryption and Rerandomizable Yao Circuits	155
<i>Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan</i>	

Theory and Applications

Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography	173
<i>Vipul Goyal, Yuval Ishai, Mohammad Mahmoody, and Amit Sahai</i>	

Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption	191
<i>Tatsuaki Okamoto and Katsuyuki Takashima</i>	

Structure-Preserving Signatures and Commitments to Group Elements	209
<i>Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo</i>	

Efficient Indifferentiable Hashing into Ordinary Elliptic Curves	237
<i>Eric Brier, Jean-Sébastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi</i>	

Key Exchange, OAEP/RSA, CCA

Credential Authenticated Identification and Key Exchange	255
<i>Jan Camenisch, Nathalie Casati, Thomas Gross, and Victor Shoup</i>	

Password-Authenticated Session-Key Generation on the Internet in the Plain Model	277
<i>Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky</i>	

Instantiability of RSA-OAEP under Chosen-Plaintext Attack	295
<i>Eike Kiltz, Adam O'Neill, and Adam Smith</i>	

Efficient Chosen-Ciphertext Security via Extractable Hash Proofs	314
<i>Hoeteck Wee</i>	

Attacks

Factorization of a 768-Bit RSA Modulus	333
<i>Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann</i>	

Correcting Errors in RSA Private Keys	351
<i>Wilko Henecka, Alexander May, and Alexander Meurer</i>	

Improved Differential Attacks for ECHO and Grøstl	370
<i>Thomas Peyrin</i>	

A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony	393
<i>Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	

Composition

Universally Composable Incoercibility	411
<i>Dominique Unruh and Jörn Müller-Quade</i>	
Concurrent Non-Malleable Zero Knowledge Proofs	429
<i>Huijia Lin, Rafael Pass, Wei-Lung Dustin Tseng, and Muthuramakrishnan Venkitasubramaniam</i>	
Equivalence of Uniform Key Agreement and Composition Insecurity	447
<i>Chongwon Cho, Chen-Kuei Lee, and Rafail Ostrovsky</i>	

Computation Delegation and Obfuscation

Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers	465
<i>Rosario Gennaro, Craig Gentry, and Bryan Parno</i>	
Improved Delegation of Computation Using Fully Homomorphic Encryption	483
<i>Kai-Min Chung, Yael Kalai, and Salil Vadhan</i>	
Oblivious RAM Revisited	502
<i>Benny Pinkas and Tzachy Reinman</i>	
On Strong Simulation and Composable Point Obfuscation	520
<i>Nir Bitansky and Ran Canetti</i>	

Multiparty Computation

Protocols for Multiparty Coin Toss with Dishonest Majority	538
<i>Amos Beimel, Eran Omri, and Ilan Orlov</i>	
Multiparty Computation for Dishonest Majority: From Passive to Active Security at Low Cost	558
<i>Ivan Damgård and Claudio Orlandi</i>	
Secure Multiparty Computation with Minimal Interaction	577
<i>Yuval Ishai, Eyal Kushilevitz, and Anat Paskin-Cherniavsky</i>	
A Zero-One Law for Cryptographic Complexity with Respect to Computational UC Security	595
<i>Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek</i>	

Pseudorandomness

On Generalized Feistel Networks	613
<i>Viet Tung Hoang and Phillip Rogaway</i>	

Cryptographic Extraction and Key Derivation: The HKDF Scheme	631
<i>Hugo Krawczyk</i>	
Time Space Tradeoffs for Attacks against One-Way Functions and PRGs	649
<i>Anindya De, Luca Trevisan, and Madhur Tulsiani</i>	
Pseudorandom Functions and Permutations Provably Secure against Related-Key Attacks	666
<i>Mihir Bellare and David Cash</i>	
 Quantum	
Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries	685
<i>Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail</i>	
On the Efficiency of Classical and Quantum Oblivious Transfer Reductions	707
<i>Severin Winkler and Jürg Wullschleger</i>	
Sampling in a Quantum Population, and Applications	724
<i>Niek J. Bouman and Serge Fehr</i>	
Author Index	743