Table of Contents

Cryptography from Lattices

Deterministic Public Key Encryption and Identity-Based Encryption from Lattices in the Auxiliary-Input Setting 1
Xiang Xie, Rui Xue, and Rui Zhang

Ring Switching in BGV-Style Homomorphic Encryption 19
Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart

Zero-Knowledge Proofs with Low Amortized Communication from Lattice Assumptions 38
Ivan Damgård and Adriana López-Alt

Fully Anonymous Attribute Tokens from Lattices 57
Jan Camenisch, Gregory Neven, and Markus Rückert

Signature Schemes

Efficient Structure-Preserving Signature Scheme from Standard Assumptions 76
Jan Camenisch, Maria Dubovitskaya, and Kristiyan Haralambiev

Compact Round-Optimal Partially-Blind Signatures 95
Olivier Blazy, David Pointcheval, and Damien Vergnaud

History-Free Sequential Aggregate Signatures 113
Marc Fischlin, Anja Lehmann, and Dominique Schröder

A New Hash-and-Sign Approach and Structure-Preserving Signatures from DLIN 131
Melissa Chase and Markulf Kohlweiss

Encryption Schemes I

Blackbox Construction of a More Than Non-Malleable CCA1 Encryption Scheme from Plaintext Awareness 149
Steven Myers, Mona Sergi, and abhi shelat

Decentralized Dynamic Broadcast Encryption 166
Duong Hieu Phan, David Pointcheval, and Mario Strefler

Time-Specific Encryption from Forward-Secure Encryption 184
Kohei Kasamatsu, Takahiro Matsuda, Keita Emura, Nuttapong Attrapadung, Goichiro Hanaoka, and Hideki Imai

Efficient Two-Party and Multi-Party Computation

Improved Secure Two-Party Computation via Information-Theoretic Garbled Circuits 205
Vladimir Kolesnikov and Ranjit Kumaresan

5PM: Secure Pattern Matching 222
Joshua Baron, Karim El Defrawy, Kirill Minkovich, Rafail Ostrovsky, and Eric Tressler

Implementing AES via an Actively/Covertly Secure Dishonest-Majority MPC Protocol 241
Ivan Damgård, Marcel Keller, Enrique Larraia, Christian Miles, and Nigel P. Smart

Security in the UC Framework

On the Centrality of Off-Line E-Cash to Concrete Partial Information Games 264
Seung Geol Choi, Dana Dachman-Soled, and Moti Yung

Universally Composable Security with Local Adversaries 281
Ran Canetti and Margarita Vald

Cryptanalysis

On the Strength Comparison of the ECDLP and the IFP 302
Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, and Tetsuya Izu

New Attacks for Knapsack Based Cryptosystems 326
Gottfried Herold and Alexander Meurer

Multiple Differential Cryptanalysis Using LLR and χ^2 Statistics 343
Céline Blondeau, Benoît Gérard, and Kaisa Nyberg

Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-commutative Rings 361
Enrico Thomae

Encryption Schemes II

Homomorphic Encryption for Multiplications and Pairing Evaluation ... 374
Guilhem Castagnos and Fabien Laguillaumie

Publicly Verifiable Ciphertexts ... 393
Juan Manuel González Nieto, Mark Manulis, Bertram Poettering, Jothi Rangasamy, and Douglas Stebila

Public-Key Encryption with Lazy Parties ... 411
Kenji Yasunaga

Efficient Constructions

Probabilistically Correct Secure Arithmetic Computation for Modular Conversion, Zero Test, Comparison, MOD and Exponentiation ... 426
Ching-Hua Yu and Bo-Yin Yang

MAC Aggregation with Message Multiplicity ... 445
Vladimir Kolesnikov

Efficiency Limitations of Σ-Protocols for Group Homomorphisms Revisited ... 461
Björn Terelius and Douglas Wikström

A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument ... 477
Helger Lipmaa and Bingsheng Zhang

Protocols and Combiners

Active Security in Multiparty Computation over Black-Box Groups ... 503
Yvo Desmedt, Josef Pieprzyk, and Ron Steinfeld

Hash Combiners for Second Pre-image Resistance, Target Collision Resistance and Pre-image Resistance Have Long Output ... 522
Arno Mittelbach

Human Perfectly Secure Message Transmission Protocols and Their Applications ... 540
Stelios Erotokritou and Yvo Desmedt

Oblivious Transfer with Hidden Access Control from Attribute-Based Encryption ... 559
Jan Camenisch, Maria Dubovitskaya, Robert R. Enderlein, and Gregory Neven

Author Index ... 581