Table of Contents

Cryptosystems I

On Ideal Lattices and Learning with Errors over Rings 1
Vadim Lyubashevsky, Chris Peikert, and Oded Regev

Fully Homomorphic Encryption over the Integers 24
Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan

Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups 44
David Mandell Freeman

Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption 62
Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters

Obfuscation and Side Channel Security

Secure Obfuscation for Encrypted Signatures 92
Satoshi Hada

Public-Key Encryption in the Bounded-Retrieval Model 113
Joël Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish, and Daniel Wichs

Protecting Circuits from Leakage: The Computationally-Bounded and Noisy Cases 135
Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan

2-Party Protocols

Partial Fairness in Secure Two-Party Computation 157
S. Dov Gordon and Jonathan Katz

Secure Message Transmission with Small Public Discussion 177
Juan Garay, Clint Givens, and Rafail Ostrovsky

On the Impossibility of Three-Move Blind Signature Schemes 197
Marc Fischlin and Dominique Schröder

Efficient Device-Independent Quantum Key Distribution 216
Esther Hänggi, Renato Renner, and Stefan Wolf

Cryptanalysis

New Generic Algorithms for Hard Knapsacks 235
Nick Howgrave-Graham and Antoine Joux

Lattice Enumeration Using Extreme Pruning 257
Nicolas Gama, Phong Q. Nguyen, and Oded Regev

Algebraic Cryptanalysis of McEliece Variants with Compact Keys 279
Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich

Key Recovery Attacks of Practical Complexity on AES-256 Variants with Up to 10 Rounds 299
Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir

2010 IACR Distinguished Lecture

Cryptography between Wonderland and Underland 320
Moti Yung

Automated Tools and Formal Methods

Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others 322
Alex Biryukov and Ivica Nikolić

Plaintext-Dependent Decryption: A Formal Security Treatment of SSH-CTR 345
Kenneth G. Paterson and Gaven J. Watson

Computational Soundness, Co-induction, and Encryption Cycles 362
Daniele Micciancio

Models and Proofs

Encryption Schemes Secure against Chosen-Ciphertext Selective Opening Attacks 381
Serge Fehr, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee

Cryptographic Agility and Its Relation to Circular Encryption 403
Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash

Bounded Key-Dependent Message Security 423
Boaz Barak, Iftach Haitner, Dennis Hofheinz, and Yuval Ishai

Multiparty Protocols

Perfectly Secure Multiparty Computation and the Computational Overhead of Cryptography 445
Ivan Damgård, Yuval Ishai, and Mikkel Krøigaard

Adaptively Secure Broadcast 466
Martin Hirt and Vassilis Zikas

Universally Composable Quantum Multi-party Computation 486
Dominique Unruh

Cryptosystems II

A Simple BGN-Type Cryptosystem from LWE 506
Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan

Bonsai Trees, or How to Delegate a Lattice Basis 523
David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert

Efficient Lattice (H)IBE in the Standard Model 553
Shweta Agrawal, Dan Boneh, and Xavier Boyen

Hash and MAC

Multi-property-preserving Domain Extension Using Polynomial-Based Modes of Operation 573
Jooyoung Lee and John Steinberger

Stam's Collision Resistance Conjecture 597
John Steinberger

Universal One-Way Hash Functions via Inaccessible Entropy 616
Iftach Haitner, Thomas Holenstein, Omer Reingold, Salil Vadhan, and Hoeteck Wee

Foundational Primitives

Constant-Round Non-malleable Commitments from Sub-exponential One-Way Functions 638
Rafael Pass and Hoeteck Wee

Constructing Verifiable Random Functions with Large Input Spaces 656
Susan Hohenberger and Brent Waters

Adaptive Trapdoor Functions and Chosen-Ciphertext Security 673
Eike Kiltz, Payman Mohassel, and Adam O'Neill

Author Index 693