Table of Contents

Private Computation

Efficient Private Matching and Set Intersection 1
Michael J. Freedman, Kobbi Nissim, and Benny Pinkas

Positive Results and Techniques for Obfuscation 20
Benjamin Lynn, Manoj Prabhakaran, and Amit Sahai

Secure Computation of the k^{th}-Ranked Element 40
Gagan Aggarwal, Nina Mishra, and Benny Pinkas

Signatures I

Short Signatures Without Random Oracles 56
Dan Boneh and Xavier Boyen

Sequential Aggregate Signatures from Trapdoor Permutations 74
Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham

Unconditional Security

On the Key-Uncertainty of Quantum Ciphers and the Computational Security of One-Way Quantum Transmission 91
Ivan Damgård, Thomas Pedersen, and Louis Salvail

The Exact Price for Unconditionally Secure Asymmetric Cryptography .. 109
Renato Renner and Stefan Wolf

On Generating the Initial Key in the Bounded-Storage Model 126
Stefan Dziembowski and Ueli Maurer

Distributed Cryptography

Practical Large-Scale Distributed Key Generation 138
John Canny and Stephen Sorkin

Optimal Communication Complexity of Generic Multicast Key Distribution 153
Daniele Micciancio and Saurabh Panjwani

Foundations I

An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem 171
Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio

Black-Box Composition Does Not Imply Adaptive Security 189
Steven Myers

Identity-Based Encryption

Chosen-Ciphertext Security from Identity-Based Encryption 207
Ran Canetti, Shai Halevi, and Jonathan Katz

Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles 223
Dan Boneh and Xavier Boyen

Elliptic Curves

Construction of Secure Random Curves of Genus 2 over Prime Fields 239
Pierrick Gaudry and Éric Schost

Projective Coordinates Leak 257
David Naccache, Nigel P. Smart, and Jacques Stern

Signatures II

Security Proofs for Identity-Based Identification and Signature Schemes . . 268
Mihir Bellare, Chanathip Namprempre, and Gregory Neven

Concurrent Signatures 287
Liqun Chen, Caroline Kudla, and Kenneth G. Paterson

The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures 306
Tal Malkin, Satoshi Obana, and Moti Yung

Public-Key Cryptography

Public-Key Steganography 323
Luis von Ahn and Nicholas J. Hopper

Immunizing Encryption Schemes from Decryption Errors 342
Cynthia Dwork, Moni Naor, and Omer Reingold

Secure Hashed Diffie-Hellman over Non-DDH Groups 361
Rosario Gennaro, Hugo Krawczyk, and Tal Rabin

Foundations II

On Simulation-Sound Trapdoor Commitments 382
Philip MacKenzie and Ke Yang

Hash Function Balance and Its Impact on Birthday Attacks 401
Mihir Bellare and Tadayoshi Kohno

Multiparty Computation

Multi-party Computation with Hybrid Security 419
Matthias Fitzi, Thomas Holenstein, and Jürg Wullschleger

On the Hardness of Information-Theoretic Multiparty Computation 439
Yuval Ishai and Eyal Kushilevitz

Dining Cryptographers Revisited 456
Philippe Golle and Ari Juels

Cryptanalysis

Algebraic Attacks and Decomposition of Boolean Functions 474
Willi Meier, Enes Pasalic, and Claude Carlet

Finding Small Roots of Bivariate Integer Polynomial Equations Revisited 492
Jean-Sébastien Coron

New Applications

Public Key Encryption with Keyword Search 506
Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano

Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data 523
Yevgeniy Dodis, Leonid Reyzin, and Adam Smith

Algorithms and Implementation

Merkle Tree Traversal in Log Space and Time 541
Michael Szydlo

Can We Trust Cryptographic Software? Cryptographic Flaws in GNU Privacy Guard v1.2.3 555
Phong Q. Nguyen

Anonymity

Traceable Signatures 571
Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung

Handcuffing Big Brother: an Abuse-Resilient Transaction Escrow Scheme 590
Stanislaw Jarecki and Vitaly Shmatikov

Anonymous Identification in *Ad Hoc* Groups 609
Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup

Author Index 627