Public-Key Cryptanalysis I
On the Security of RSA Padding p. 1
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization p. 19
The Hardness of the Hidden Subset Sum Problem and Its Cryptographic Implications p. 31
Invited Lecture
Information-Theoretic Cryptography p. 47
Secure Communication and Computation
Information Theoretically Secure Communication in the Limited Storage Space Model p. 65
The All-or-Nothing Nature of Two-Party Secure Computation p. 80
Distributed Cryptography
Adaptive Security for Threshold Cryptosystems p. 98
Two Party RSA Key Generation p. 116
Robust Distributed Multiplication without Interaction p. 130
A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting p. 148
Secret-Key Cryptography
Truncated Differentials and Skipjack p. 165
Fast Correlation Attacks Based on Turbo Code Techniques p. 181
Highly Nonlinear Resilient Functions Optimizing Siegenthaler's Inequality p. 198
Message Authentication Codes
UMAC: Fast and Secure Message Authentication p. 216
Square Hash: Fast Message Authentication via Optimized Universal Hash Functions p. 234
Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions p. 252
Stateless Evaluation of Pseudorandom Functions: Security Beyond the Birthday Barrier p. 270
Public-Key Cryptanalysis II
Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97 p. 288
Weakness in Quaternion Signatures p. 305
Cryptanalysis of "2R" Schemes p. 315
Factoring N = p p. 326
Traitor Tracing
An Efficient Public Key Traitor Tracing Scheme p. 338
Dynamic Traitor Tracing p. 354
Efficient Methods for Integrating Traceability and Broadcast Encryption p. 372
Differential Power Analysis
Differential Power Analysis p. 388
Towards Sound Approaches to Counteract Power-Analysis Attacks p. 398
Signature Schemes
Separability and Efficiency for Generic Group Signature Schemes p. 413
A Forward-Secure Digital Signature Scheme p. 431
Abuse-Free Optimistic Contract Signing p. 449
Zero Knowledge
Can Statistical Zero Knowledge Be Made Non-interactive? or On the Relationship of SZK p. 467
and NiSZK
On Concurrent Zero-Knowledge with Pre-processing p. 485
Asymmetric Encryption
On the Security Properties of OAEP as an All-or-Nothing Transform p. 503
Non-malleable Encryption: Equivalence between Two Notions, and an
Indistinguishability-Based Characterization p. 519
Secure Integration of Asymmetric and Symmetric Encryption Schemes p. 537
Electronic Cash
Auditable, Anonymous Electronic Cash p. 555
Protocols and Broadcasting
Oblivious Transfer with Adaptive Queries p. 573
Compressing Cryptographic Resources p. 591
Coding Constructions for Blacklisting Problems without Computational Assumptions p. 609
An Information Theoretic Analysis of Rooted-Tree Based Secure Multicast Key
Distribution Schemes p. 624
Author Index p. 639
Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.