Hash Attacks
Rotational Rebound Attacks on Reduced Skein p. 1
Finding Second Preimages of Short Messages for Hamsi-256 p. 20
Non-full-active Super-Sbox Analysis: Applications to ECHO and Grøstl p. 38
Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2 p. 56
Collision Attacks against the Knudsen-Preneel Compression Functions p. 76
Symmetric-Key Cryptosystems
Improved Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions p. 94
The World Is Not Enough: Another Look on Second-Order DPA p. 112
Block and Stream Ciphers
Conditional Differential Cryptanalysis of NLFSR-Based Cryptosystems p. 130
A Byte-Based Guess and Determine Attack on SOSEMANUK p. 146
Improved Single-Key Attacks on 8-Round AES-192 and AES-256 p. 158
Protocols
Constant-Size Commitments to Polynomials and Their Applications p. 177
Computationally Secure Pattern Matching in the Presence of Malicious Adversaries p. 195
Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model p. 213
Key Exchange
Generic Compilers for Authenticated Key Exchange p. 232
A Forward-Secure Symmetric-Key Derivation Protocol: How to Improve Classical DUKPT p. 250

Foundation
Efficient String-Commitment from Weak Bit-Commitment p. 268
On the Static Diffie-Hellman Problem on Elliptic Curves over Extension Fields p. 283
Random Oracles with(out) Programmability p. 303
Zero-Knowledge
Short Pairing-Based Non-interactive Zero-Knowledge Arguments p. 321
Short Non-interactive Zero-Knowledge Proofs p. 341
Optimistic Concurrent Zero-Knowledge p. 359
Lattice-Based Cryptography
Faster Fully Homomorphic Encryption p. 377
A Group Signature Scheme from Lattice Assumptions p. 395
Lattice-Based Blind Signatures p. 413
Secure Communication and Computation
The Round Complexity of Verifiable Secret Sharing: The Statistical Case p. 431
General Perfectly Secure Message Transmission Using Linear Codes p. 448
On Invertible Sampling and Adaptive Security p. 466
Multiparty Computation for Modulo Reduction without Bit-Decomposition and a Generalization to Bit-Decomposition p. 483
Models, Notions, and Assumptions
A Closer Look at Anonymity and Robustness in Encryption Schemes p. 501

Limitations on Transformations from Composite-Order to Prime-Order Groups: The Case of Round-Optimal Blind Signatures p. 519
The Semi-Generic Group Model and Applications to Pairing-Based Cryptography p. 539
Public-Key Encryption
The Degree of Regularity of HFE Systems p. 557
Structured Encryption and Controlled Disclosure p. 577
Leakage Resilient ElGamal Encryption p. 595
Efficient Public-Key Cryptography in the Presence of Key Leakage p. 613
Author Index p. 633