Discrete-log-based signatures may not be equivalent to discrete log p. 1
Do all elliptic curves of the same order have the same difficulty of discrete log? p. 21
Adapting density attacks to low-weight knapsacks p. 41
Efficient and secure elliptic curve point multiplication using double-base chains p. 59
Upper bounds on the communication complexity of optimally resilient cryptographic multiparty computation p. 79
Graph-decomposition-based frameworks for subset-cover broadcast encryption and efficient instantiations p. 100
Revealing additional information in two-party computations p. 121
Gate evaluation secret sharing and secure one-round two-party computation p. 136
Parallel multi-party computation from linear multi-secret sharing schemes p. 156
Updatable zero-knowledge databases p. 174
Simple and tight bounds for information reconciliation and privacy amplification p. 199
Quantum anonymous transmissions p. 217
Privacy-preserving graph algorithms in the semi-honest model p. 236
Spreading alerts quietly and the subgroup escape problem p. 253
A sender verifiable mix-net and a new proof of a shuffle p. 273
Universally anonymizable public-key encryption p. 293
Fast computation of large distributions and its cryptographic applications p. 313
An analysis of the XSL algorithm p. 333
New applications of time memory data tradeoffs p. 353
Linear cryptanalysis of the TSC family of stream ciphers p. 373
A practical attack on the fixed RC4 in the WEP mode p. 395
A near-practical attack against B mode of HBB p. 412
New improvements of Davies-Murphy cryptanalysis p. 425
A related-key rectangle attack on the full KASUMI p. 443
Some attacks against a double length hash proposal p. 462
A failure-friendly design principle for hash functions p. 474
Identity-based hierarchical strongly key-insulated encryption and its application p. 495
Efficient and provably-secure identity-based signatures and signcryption from bilinear maps p. 515
Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps p. 533
Modular security proofs for key agreement protocols p. 549
A simple threshold authenticated key exchange from short secrets p. 566
Examining indistinguishability-based proof models for key establishment protocols p. 585
Server-aided verification : theory and practice p. 605
Errors in computational complexity proofs for protocols p. 624

Universal designated verifier signature proof (or how to efficiently prove knowledge of a signature) p. 644

Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs p. 662

Universally convertible directed signatures p. 682