The first experimental cryptanalysis of the Data Encryption Standard p. 1
Linear cryptanalysis of the Fast Data Encipherment Algorithm p. 12
Differential-linear cryptanalysis p. 17
Linear cryptanalysis using multiple approximations p. 26
Hashing with $\text{SL}_{2}$ p. 40
Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks p. 50
Cryptographic protocols based on discrete logarithms in real-quadratic orders p. 56
Designated confirmer signatures and public-key encryption are equivalent p. 61
Directed acyclic graphs, one-way functions and digital signatures p. 75
An identity-based signature scheme with bounded life-span p. 83
More flexible exponentiation with precomputation p. 95
A parallel permutation multiplier for a PGM crypto-chip p. 108
Cryptographic randomness from air turbulence in disk drives p. 114
Cryptanalysis of the Gemmell and Naor multiround authentication protocol p. 121
LFSR-based hashing and authentication p. 129
New bound on authentication code with arbitration p. 140
Multi-secret sharing schemes p. 150
Designing identification schemes with keys of short size p. 164
Proofs of partial knowledge and simplified design of witness hiding protocols p. 174
Language dependent secure bit commitment p. 188
On the length of cryptographic hash-values used in identification schemes p. 202
Incremental cryptography: the case of hashing and signing p. 216
An efficient existentially unforgeable signature scheme and its applications p. 234
Bounds for resilient functions and orthogonal arrays p. 247
Tracing traitors p. 257
Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms p. 271
Fast generation of provable primes using search in arithmetic progressions p. 282
Attack on the cryptographic scheme NIKS-TAS p. 294
On the risk of opening distributed keys p. 308
Cryptanalysis of cryptosystems based on remote chaos replication p. 318
A Fourier transform approach to the linear complexity of nonlinearly filtered sequences p. 332
The security of cipher block chaining p. 341
A chosen plaintext attack of the 16-round Khufu cryptosystem p. 359
Ciphertext only attack for one-way function of the MAP using one ciphertext p. 369
Pitfalls in designing substitution boxes p. 383
A randomness-rounds tradeoff in private computation p. 397
Secure voting using partially compatible homomorphisms p. 411
Maintaining security in the presence of transient faults p. 425
Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.