Trends and challenges for securer cryptography in practice p. 1
Distinguishing attacks on T-functions p. 2
Introducing a new variant of fast algebraic attacks and minimizing their successive data complexity p. 16
Equivalent keys in HFE, C*, and variations p. 33
A new structural attack for GPT and variants p. 50
A family of fast syndrome based cryptographic hash functions p. 64
Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing p. 84
Identity based delegation network p. 99
On session key construction in provably-secure key establishment protocols p. 116
On the security of probabilistic multisignature schemes and their optimality p. 132
Efficient secure group signatures with dynamic joins and keeping anonymity against group managers p. 151
An analysis of double base number systems and a sublinear scalar multiplication algorithm p. 171
Power analysis by exploiting chosen message and internal collisions - vulnerability of checking mechanism for RSA-decryption p. 183
Optimization of the MOVA undeniable signature scheme p. 196
Questionable encryption and its applications p. 210
Twin RSA p. 222
Security of two-party identity-based key agreement p. 229
Related-key differential attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b p. 244
Advanced slide attacks revisited: realigning slide on DES p. 263
New multiset attacks on Rijndael with large blocks p. 277
Homomorphic cryptosystems based on subgroup membership problems p. 314

Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.