Cryptanalysis of two signature schemes based on bilinear pairings in CISC '05
Identity-based key-insulated signature with secure key-updates
Efficient intrusion-resilient signatures without random oracles
New constructions of large binary sequences family with low correlation
On the rate of coincidence of two clock-controlled combiners
Designing power analysis resistant and high performance block cipher coprocessor using WDDL and wave-pipelining
OPMAC : one-key Poly1305 MAC
A general construction of tweakable block ciphers and different modes of operations
Dynamic threshold and cheater resistance for shamir secret sharing scheme
Efficient short signcryption scheme with public verifiability
A revocation scheme preserving privacy
Deterministic packet marking with link signatures for IP traceback
Survey and taxonomy of feature selection algorithms in intrusion detection system
A network security policy model and its realization mechanism
Packet marking based cooperative attack response service for effectively handling suspicious traffic
A verifiable formal specification for RBAC model with constraints of separation of duty
Design and implementation of fast access control that supports the separation of duty
A practical alternative to domain and type enforcement integrity formal models
Return address randomization scheme for annuling data-injection buffer overflow attacks
Application and evaluation of Bayesian filter for Chinese spam
Batch decryption of encrypted short messages and its application on concurrent SSL handshakes
An enterprise security management, system as a Web-based application service for small/medium businesses
Obtaining asymptotic fingerprint codes through a new analysis of the Boneh-Shaw codes

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