AES
Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds p. 1
Implementation of the AES-128 on Virtex-5 FPGAs p. 16
Analysis of RFID Protocols
Weaknesses in a Recent Ultra-Lightweight RFID Authentication Protocol p. 27
Differential Cryptanalysis of Reduced-Round PRESENT p. 40
Invited Talk
The Psychology of Security p. 50
Cryptographic Protocols
An (Almost) Constant-Effort Solution-Verification Proof-of-Work Protocol Based on Merkle Trees p. 80
Robust Threshold Schemes Based on the Chinese Remainder Theorem p. 94
An Authentication Protocol with Encrypted Biometric Data p. 109
Authentication
Authenticated Encryption Mode for Beyond the Birthday Bound Security p. 125
Cryptanalysis of the TRMS Signature Scheme of PKC'05 p. 143
Public-Key Cryptography
New Definition of Density on Knapsack Cryptosystems p. 156
Another Generalization of Wiener's Attack on RSA p. 174
An Adaptation of the NICE Cryptosystem to Real Quadratic Orders p. 191
Pseudorandomness
A Proof of Security in O(2^{n}) for the Benes Scheme p. 209
Analysis of Stream Ciphers
Yet Another Attack on Vest p. 221
Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers p. 236
Correlated Keystreams in MOUSTIQUE p. 246
Stream Ciphers Using a Random Update Function: Study of the Entropy of the Inner State p. 258
Analysis of Grain's Initialization Algorithm p. 276
Hash Functions
Password Recovery on Challenge and Response: Impossible Differential Attack on Hash Function p. 290
How (Not) to Efficiently Dither Blockcipher-Based Hash Functions? p. 308
Broadcast Encryption
Attribute-Based Broadcast Encryption Scheme Made Efficient p. 325
Lower Bounds for Subset Cover Based Broadcast Encryption p. 343
Invited Talk
A Brief History of Provably-Secure Public-Key Encryption p. 357
Implementation
On Compressible Pairings and Their Computation p. 371
Twisted Edwards Curves p. 389
Efficient Multiplication in $\mathbb{F}[\mathbb{Z}^{m}]$, $m \geq 1$ and $5 \leq l \leq 18$ p. 406

Author Index p. 415

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