Malicious Code on Java Card Smartcards: Attacks and Countermeasures p. 1
Static Program Analysis for Java Card Applets p. 17
On Practical Information Flow Policies for Java-Enabled Multiapplication Smart Cards p. 32
New Differential Fault Analysis on AES Key Schedule: Two Faults Are Enough p. 48
DSA Signature Scheme Immune to the Fault Cryptanalysis p. 61
A Black Hen Lays White Eggs: Bipartite Multiplier Out of Montgomery One for On-Line RSA Verification p. 74
Ultra-Lightweight Implementations for Smart Devices - Security for 1000 Gate Equivalents p. 89
Fast Hash-Based Signatures on Constrained Devices p. 104
Fraud Detection and Prevention in Smart Card Based Environments Using Artificial Intelligence p. 118
The Trusted Execution Module: Commodity General-Purpose Trusted Computing p. 133
Management of Multiple Cards in NFC-Devices p. 149
Coupon Recalculation for the GPS Authentication Scheme p. 162
Provably Secure Grouping-Proofs for RFID Tags p. 176
Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices p. 191
A Practical DPA Countermeasure with BDD Architecture p. 206
SCARE of an Unknown Hardware Feistel Implementation p. 218
Evaluation of Java Card Performance p. 228
Application of Network Smart Cards to Citizens Identification Systems p. 241
SmartPRO: A Smart Card Based Digital Content Protection for Professional Workflow p. 255
A Practical Attack on the MIFARE Classic p. 267
A Chemical Memory Snapshot p. 283
Recent Advances in Electronic Cash Design p. 290
Author Index p. 295
Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.