《Information Security》

图书基本信息

书名：《Information Security and Cryptology - ICISC 2004信息安全与密码术 - ICISC 2004》

13位ISBN编号：9783540262268

10位ISBN编号：3540262261

出版时间：2005-07-21

出版社：Springer

作者：Park, Choonsik; Chee, Seongtaek;

页数：490

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《Information Security》

内容概要

This book constitutes the thoroughly refereed postproceedings of the 7th International Conference on Information Security and Cryptology, ICISC 2004, held in Seoul, Korea in December 2004. The 34 revised full papers presented have gone through two rounds of reviewing and improvement and were selected from 194 submissions. The papers are organized in topical sections on block ciphers and stream ciphers, public key cryptosystems, PKI and related implementations, digital signatures, elliptic curve cryptosystems, provable security and primitives, network security, steganography, and biometrics.

《Information Security》

书籍目录

Invited Talks Security by, and for, Converged Mobile Devices Security for Ubiquitous ComputingBlock Cipher and Stream Cipher Algebraic Attacks on Combiners with Memory and Several Outputs New Method for Bounding the Maximum Differential Probability for SPNs and ARIA Dragon: A Fast Word Based Stream CipherPublic Key Cryptosystem An Efficient and Verifiable Solution to the Millionaire Problem All in the XL Family: Theory and Practice Efficient Broadcast Encryption Using Multiple Interpolation Methods On Private Scalar Product Computation for Privacy-Preserving Data MiningPKI and Related Implementation Separable Implicit Certificate Revocation Fractional Windows Revisited: Improved Signed-Digit Representations for Efficient Exponentiation Improvement on Ha-Moon Randomized Exponentiation Algorithm Efficient Computation of Tate Pairing in Projective Coordinate over General Characteristic FieldsDigital Signature On Subliminal Channels in Deterministic Signature Schemes Threshold Entrusted Undeniable Signature On the Security Models of (Threshold) Ring Signature Schemes Identity Based Threshold Ring Signature Batch Verifications with ID-Based SignaturesElliptic Curve Cryptosystem A Method for Distinguishing the Two Candidate Elliptic Curves in CM Method Generating Prime Order Elliptic Curves: Difficulties and Efficiency Considerations……Network SecurityStegangraphyBiometricsAuthor Index

《Information Security》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com