

<<Information Security>>

图书基本信息

书名：<<Information Security and Cryptology - ICISC 2000: Third International Conference, Seoul, Korea, December 8-9, 2000, Proceedings (平装)>>

13位ISBN编号：9783540417828

10位ISBN编号：3540417826

出版时间：2000-12

出版时间：1 (2001年4月1日)

作者：Dongho Won

页数：260

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：<http://www.tushu007.com>

<<Information Security>>

内容概要

Book Description This book constitutes the thoroughly refereed post-proceedings of the Third International Conference on Information Security and Cryptology, ICISC 2000, held in Seoul, Korea, in December 2000.

The 20 revised full papers presented were carefully reviewed and selected from a total of 56 submissions. Among the topics addressed are cryptanalysis, elliptic curve cryptography, cryptographic protocols, block ciphers, hash functions, multi-party protocols, digital signatures, E-commerce, anonymous auction systems, finite field polynomials, anonymous fingerprinting, network security, and security evaluation systems.

书籍目录

A Note on the Higher Order Differential Attack of Block Ciphers with Two-Block Structures
On the Strength of KASUMI without FL Functions against Higher Order Differential Attack
On MISTY1 Higher Order Differential Cryptanalysis
Difference Distribution Attack on DONUT and Improved DONUT
New Results on Correlation Immunity
Elliptic Curves and Resilient Functions
Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction
Characterization of Elliptic Curve Traces under FR-Reduction
A Multi-party Optimistic Non-repudiation Protocol
Secure Matchmaking Protocol
An Improved Scheme of the Gennaro-Krawczyk-Rabin Undeniable Signature System Based on RSA
Efficient and Secure Member Deletion in Group Signature Schemes
An Efficient and Practical Scheme for Privacy Protection in the E-Commerce of Digital Goods
An Internet Anonymous Auction Scheme
Efficient Sealed-Bid Auction Using Hash Chain
Micropayments for Wireless Communications
Cryptographic Applications of Sparse Polynomials over Finite Rings
Efficient Anonymous Fingerprinting of Electronic Information with Improved Automatic Identification of Redistributors
Hash to the Rescue: Space Minimization for PKI Directories
A Design of the Security Evaluation System for Decision Support in the Enterprise Network Security Management
Author Index

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:<http://www.tushu007.com>