

<<信息安全与密码术>>

图书基本信息

书名：<<信息安全与密码术>>

13位ISBN编号：9783540491125

10位ISBN编号：3540491120

出版时间：2006-12

出版时间：湖南文艺出版社

作者：Rhee, Min Surp; Lee, Byoungcheon;

页数：358

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>

## <<信息安全与密码术>>

### 内容概要

This book constitutes the refereed proceedings of the 9th International Conference on Information Security and Cryptology, ICISC 2006, held in Busan, Korea in November/December 2006. The 26 revised full papers presented together with two invited talks have gone through two rounds of reviewing and improvement and were selected from 129 submissions. The papers are organized in topical sections on hash functions, block and stream ciphers, efficient implementation and hardware, network security and access control, mobile communications security, forensics, copyright protection, biometrics, public key cryptosystems, and digital signatures.

书籍目录

Invited Talks RFID Privacy Based on Public-Key Cryptography Generic Attacks on Symmetric Ciphers Hash Functions - Improved Collision Attack on the Hash Function Proposed at PKC'98 Hashing with Polynomials Birthday Paradox for Multi-collisions Block and Stream Ciphers New Variant of the Self-Shrinking Generator and Its Cryptographic Properties On Constructing of a  $32 \times 32$  Binary Matrix as a Diffusion Layer for a 256-Bit Block Cipher On Algebraic Immunity and Annihilators Efficient Implementation and Hardware High-Speed RSA Crypto-processor with Radix-4 Modular Multiplication and Chinese Remainder Theorem A High-Speed Square Root Algorithm in Extension Fields The Smallest ARIA Module with 16-Bit Architecture A Simpler Sieving Device: Combining ECM and TWIRL Network Security and Access Control Janus: A Two-Sided Analytical Model for Multi-Stage Coordinated Attacks A Time-Frame Based Trust Model for P2P Systems Spatial Context in Role-Based Access Control Mobile Communications Security An Efficient Scheme for Detecting Malicious Nodes in Mobile Ad Hoc Networks Mobile RFID Applications and Security Challenges Forensics An Efficient Forensic Evidence Collection Scheme of Host Infringement at the Occurrence Time Copyright Protection A Copy Protection Technique Using Multi-level Error Coding ..... Biometrics Hash Functions- Public Key Cryptosystems Digital Signatures 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>