

<<信息安全及密码术Informatio>>

图书基本信息

书名：<<信息安全及密码术Information security and cryptology>>

13位ISBN编号：9783540496083

10位ISBN编号：3540496084

出版时间：2006-12

出版时间：Springer-Verlag New York Inc

作者：Lipmaa, Helger (EDT)/ Yung, Moti (EDT)/ Lin, Donghai (EDT)

页数：303

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>

内容概要

This book constitutes the refereed proceedings of the Second SKLOIS (State Key Laboratory of Information Security) Conference on Information Security and Cryptology, Inscrypt 2006 (formerly CISC), held in Beijing, China in November/December 2006. The 23 revised full papers presented were carefully reviewed and selected from 225 submissions. The papers are organized in topical sections on digital signature schemes, sequences and stream ciphers, symmetric-key cryptography, cryptographic schemes, network security, access control, computer and applications security, as well as Web and media security.

书籍目录

Digital Signature Schemes Cryptanalysis of Two Signature Schemes Based on Bilinear Pairings in CISC '05
Identity-Based Key-Insulated Signature with Secure Key-Updates Efficient Intrusion-Resilient Signatures
Without Random Oracles Sequences and Stream Ciphers New Constructions of Large Binary Sequences Family
with Low Correlation On the Rate of Coincidence of Two Clock-Controlled Combiners Symmetric-Key
Cryptography Designing Power Analysis Resistant and High Performance Block Cipher Coprocessor Using
WDDL and Wave-Pipelining OPMAC: One-Key Poly1305 MAC A General Construction of Tweakable Block
Ciphers and Different Modes of Operations Cryptographic Schemes Dynamic Threshold and Cheater Resistance
for Shamir Secret Sharing Scheme Efficient Short Signcryption Scheme with Public Verifiability A Revocation
Scheme Preserving Privacy Network Security Deterministic Packet Marking with Link Signatures for IP
Traceback Survey and Taxonomy of Feature Selection Algorithms in Intrusion Detection System A Network
Security Policy Model and Its Realization Mechanism Packet Marking Based Cooperative Attack Response
Service for Effectively Handling Suspicious Traffic Access Control A Verifiable Formal Specification for RBAC
Model with Constraints of Separation of Duty Design and Implementation of Fast Access Control That Supports
the Separation of Duty Computer and Applications Security A Practical Alternative to Domain and Type
Enforcement Integrity Formal Models Return Address Randomization Scheme for Annuling Data-Injection
Buffer Overflow Attacks Application and Evaluation of Bayesian Filter for Chinese Spam Web and Media
Security 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>