

图书基本信息

书名：<<密码术与网络安全/会议录 Cryptology and network security>>

13位ISBN编号：9783540494621

10位ISBN编号：3540494626

出版时间：2006-12

出版时间：Springer-Verlag New York Inc

作者：Pointcheval, David (EDT)/ Mu, Yi (EDT)/ Chen, Kefei (EDT)

页数：380

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 5th International Conference on Cryptology and Network Security, CANS 2006, held in Suzhou, China in December 2006. The 26 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 148 submissions. The papers are organized in topical sections on encryption, key exchange, authentication and signatures, proxy signatures, cryptanalysis, implementation, steganalysis and watermarking, boolean functions and stream ciphers, intrusion detection, as well as disponibility and reliability.

书籍目录

Encryption Concrete Chosen-Ciphertext Secure Encryption from Subgroup Membership Problems Efficient Identity-Based Encryption with Tight Security Reduction Key Exchange A Diffie-Hellman Key Exchange Protocol Without Random Oracles Authenticated Group Key Agreement for Multicast Authenticated and Communication Efficient Group Key Agreement for Clustered Ad Hoc Networks Authentication and Signatures Efficient Mutual Data Authentication Using Manually Authenticated Strings Achieving Multicast Stream Authentication Using MDS Codes Shorter Verifier-Local Revocation Group Signatures from Bilinear Maps Proxy Signatures Security Model of Proxy-Multi Signature Schemes Efficient ID-Based One-Time Proxy Signature and Its Application in E-Cheque Cryptanalysis Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binary Fields Improved Collision Attack on Reduced Round Camellia Stealing Secrets with SSL/TLS and SSH Kleptographic Attacks Implementation Bitslice Implementation of AES A Fast Algorithm for Determining the Linear Complexity of Periodic Sequences over GF(3) Steganalysis and Watermarking Steganalysis Based on Differential Statistics Watermarking Essential Data Structures for Copyright Protection Boolean Functions and Stream Ciphers A Note of Perfect Nonlinear Functions Chaotic Keystream Generator Using Coupled NDFs with Parameter Perturbing Intrusion Detection Disponibility and Reliability 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>