第一图书网, tushu007.com

<<应用密码学与网络安全 ACNS 200>>

图书基本信息

书名：<<应用密码学与网络安全 ACNS 2006/会议录 LNCS-3989>>

13位ISBN编号：9783540347033

10位ISBN编号：3540347038

出版时间：2006-7-11

出版时间：Springer

作者：Zhou, Jianying (EDT)/ Yung, Moti (EDT)/ Bao, Feng (EDT)

页数：488

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 4th International Conference on Applied Cryptography and Network Security, ACNS 2006, held in Singapore in June 2006.　The 33 revised full papers presented were carefully reviewed and selected from 218 submissions. The papers are organized in topical sections on intrusion detection and avoidance, cryptographic applications, DoS attacks and countermeasures, key management, cryptanalysis, security of limited devices, cryptography, authentication and Web security, ad-hoc and sensor network security, cryptographic constructions, and security and privacy.

书籍目录

Intrusion Avoidance and Detection Adaptive Detection of Local Scanners Probabilistic Proof of an Algorithm to Compute TCP Packet Round-Time for Intrusion Detection DSO:Dependable Signing OverlayCryptographic Applications Do Broken Hash Functions Affect the Security of Time-Stamping Schemes? A Handy Multi-coupon System An Efficient Single-Key Pirates Tracing Scheme Using Cover-Free FamiliesDoS:Attacks and Countermeasures Efficient Memory Bound Puzzles Pattern Databases Effect of Malicious Synchronization Misusing Unstructured P2P Systems to Perfrom DoS Attacks:The Network That Never ForgetsKey Management Password Based Server Aided Key Exchange Secure Password-Based Authenticated Group Key Agreement for Data-Sharing Peer-to-Peer Networks Stateful SuBset CoverCryptanalysis The Rainbow Attack on Stream Ciphers Based on Maiouana-McFarland Functions Breaking a New Instance of TTM Cryptosystems   Cpyptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange Using Different PasswordsSecurity of Limited Devices   An AES Smart Card Implementation Resistant to Power Analysis Attacks Physical Security Bounds Against Tampering Flexible Exponentiation with Resistance to Side Channel AttacksCryptography An Improved Poly1305 MAC ……Authentication and Web SecurityAd Hoc and Sensor Network SecurityCryptogtaphic ConstructionsSecurity and PrivacyAuthor Index

第一图书网, tushu007.com

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