《Information and Comm》

图书基本信息

书名：《Information and Communications Security信息及通信安全》

13位ISBN编号：9783540309345

10位ISBN编号：3540309349

出版时间：2006-1

出版社：1 (2006年1月9日)

作者：Sihan Qing

页数：492

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Information and Comm》

内容概要

This book constitutes the refereed proceedings of the 7th International Conference on Information and Communications Security, ICICS 2005, held in Beijing, China in December 2005. The 40 revised full papers presented were carefully reviewed and selected from 235 submissions. The papers are organized in topical sections on fair exchange, digital signatures, cryptographic protocols, cryptanalysis, network security, applied cryptography, key management, access control, applications, watermarking, and system security.

《Information and Comm》

书籍目录

Fair Exchange An Evenhanded Certified Email System for Contract Signing Efficient ID-Based Optimistic Fair Exchange with Provable Security On the Quest for Impartiality: Design and Analysis of a Fair Non-repudiation Protocol Generic, Optimistic, and Efficient Schemes for Fair Certified Email DeliveryDigital Signatures I Cryptanalysis of a Forward Secure Blind Signature Scheme with Provable Security On Delegatability of Four Designated Verifier Signatures PIATS: A Partially Sanitizable Signature SchemeCryptographic Protocols Ciphertext Comparison, a New Solution to the Millionaire Problem Private Itemset Support Counting Visual Cryptographic Protocols Using the Trusted Initializer\ Admissible Interference by Typing for Cryptographic ProtocolsCryptanalysis On the Security Bounds of CMC, EME, EME+ and EME* Modes of Operation On the Security of Encryption Modes of MD4, MD5 and HAVAL Cryptanalysis of PASS II and MiniPass Simple Power Analysis on Fast Modular Reduction with NIST Recommended Elliptic CurvesDigital Signatures II Asymmetric Concurrent Signatures Generic Construction of (Identity-Based) Perfect Concurrent Signature, Sequential Aggregate Signatures Working over Independent Homomorphic Trapdoor One-Way Permutation DomainsNetwork Security Session Table Architecture for Defending SYN Flood Attack A Behavior-Based Ingress Pate-Limiting Mechanism Against DoS/DDoS Attacks Port Scan Behavior Diagnosis by Clustering … …Applied Cryptography Key ManagementAccess Control Applications Watermarking System SecurityAuthor 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:www.tushu000.com