

<<Security in Communic>>

图书基本信息

书名：<<Security in Communication Networks通信网络中的安全>>

13位ISBN编号：9783540243014

10位ISBN编号：3540243011

出版时间：2005-3

出版时间：北京燕山出版社

作者：Blundo, Carlo; Cimato, Stelvio;

页数：379

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>

<<Security in Communic>>

内容概要

This book constitutes the thoroughly refereed postproceedings of the 4th International Conference on Security in Communication Networks, SCN 2004, held in Amalfi, Italy in September 2004. The 25 revised full papers presented together with an invited paper were carefully selected during two rounds of reviewing and improvement. The papers are organized in topical sections on reduction of security and primitives, digital signature schemes, anonymity and privacy, authentication and identification, zero knowledge, public key cryptosystems, distributed cryptography, cryptanalysis of public key crypto systems, cryptanalysis, email security, and key distribution and feedback shift registers.

书籍目录

Invited Talk ECRYPT: The Cryptographic Research Challenges for the Next Decade
 Reduction of Security/Primitives Relationships Between Diffie-Hellman and "Index Oracles"
 On the Security Notions for Public-Key Encryption Schemes
 Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel
 Signature Schemes A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs
 Group Signatures with Separate and Distributed Authorities
 Threshold Cryptography for Mobile Ad Hoc Networks
 Anonymity and Privacy Designated Verifier Signatures: Anonymity and Efficient Construction from Any Bilinear Map
 Group Signatures: Better Efficiency and New Theoretical Aspects
 Efficient Blind Signatures Without Random Oracles
 Authentication and Identification Minimalist Cryptography for Low-Cost RFID Tags
 On the Key Exposure Problem in Chameleon Hashes
 Zero Knowledge Identity-Based Zero Knowledge Public Key Cryptosystems
 A Robust Multisignatures Scheme with Applications to Acknowledgment Aggregation
 Efficient Key Encapsulation to Multiple Parties
 Improved Signcryption from q -Diffie-Hellman Problems
 Distributed Cryptography Colored Visual Cryptography Without Color Darkening
 On the Size of Monotone Span Programs
 Universally Composable DKG with Linear Number of Exponentiations
 Cryptanalysis of Public Key Cryptosystems
 An Algebraic Approach to NTRU ($q=2n$) via Witt Vectors and Overdetermined Systems of Nonlinear Equations

 Email Security Key Distribution and Feedback Shift Registers
 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>