

# 《网络用安全与密码术》

## 图书基本信息

书名：《网络用安全与密码术》

13位ISBN编号：9783540380801

10位ISBN编号：3540380809

出版时间：2006-12

出版社：Springer-Verlag New York Inc

作者：De Prisco, Roberto (EDT)/ Yung, Moti (EDT)

页数：364

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](http://www.tushu000.com)

# 《网络用安全与密码术》

## 内容概要

This book constitutes the refereed proceedings of the 5th International Conference on Security and Cryptology for Networks, SCN 2006, held in Maiori, Italy in September 2006. The 24 revised full papers presented together with the abstract of an invited talk were carefully revised and selected from 81 submissions. The papers are organized in topical sections on distributed systems security, signature schemes variants, block cipher analysis, anonymity and e-commerce, public key encryption and key exchange, secret sharing, symmetric key cryptanalysis and randomness, applied authentication, and public key related cryptanalysis.

# 《网络用安全与密码术》

## 书籍目录

Distributed Systems Security: Foundations   Edge Eavesdropping Games   Universally Composable Simultaneous BroadcastSignature Schemes Variants   Relations Among Security Notions for Undeniable Signature Schemes.  
Concurrent Blind Signatures Without Random Oracles   Universal Designated Verifier Signatures Without Random Oracles or Non-black Box AssumptionsBlock Ciphers Analysis   Understanding Two-Round Differentials in AES   Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b.   Anonymity and E-Commerce   Constant-Size Dynamic k-TAA   On Secure Orders in the Presence of Faults   Balancing Accountability and Privacy Using E-CashPublic Key Encryption and Key Exchange   About the Security of MTI/C0 and MQV   Chosen-Ciphertext Secure Threshold Identity-Based Key Encapsulation Without Random Oracles   A New Key Exchange Protocol Based on MQV Assuming Public ComputationsSecret Sharing   Ideal Secret Sharing Schemes Whose Minimal Qualified Subsets Have at Most Three Participants   Cheating Immune (2, n)-Threshold Visual Secret Sharing   Rational Secret Sharing, RevisitedSymmetric Key Cryptanalysis and Randomness   On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1  
Distinguishing Stream Ciphers with Convolutional Filters   On Statistical Testing of Random Numbers GeneratorsApplied Authentication   Lightweight Email Signatures   Shoehorning Security into the EPC Tag Standard.....Public Key Related CryptanalysisInvited TalkAuthor Index

# 《网络安全与密码术》

## 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](http://www.tushu000.com)