

<<金融密码术与数据安全>>

图书基本信息

书名：<<金融密码术与数据安全>>

13位ISBN编号：9783540462552

10位ISBN编号：3540462554

出版时间：2006-12

出版商：Springer-Verlag New York Inc

作者：Di Crescenzo, Giovanni (EDT)/ Rubin, Avi (EDT)

页数：325

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>

<<金融密码术与数据安全>>

内容概要

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and Societies, LNCS has grown into the most comprehensive computer science research forum available. The scope of LNCS, including its sub series LNAI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes - Proceedings (published in time for the respective conference) - Post-proceedings (consisting of thoroughly revised final full papers) -research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.)

书籍目录

Authentication and Fraud Detection Phoolproof Phishing Prevention A Protocol for Secure Public Instant Messaging Using Automated Banking Certificates to Detect Unauthorised Financial Transactions Privacy
Privacy in Encrypted Content Distribution Using Private Broadcast Encryption A Private Stable Matching Algorithm Private Policy Negotiation Reputation and Mix-Nets Uncheatable Reputation for Distributed Computation Markets An Efficient Publicly Verifiable Mix-Net for Long Inputs Auditable Privacy: On Tamper-Evident Mix Networks Short Papers A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation Defeating Malicious Servers in a Blind Signatures Based Voting System Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng Credit Transfer for Market-Based Infrastructure A Note on Chosen-Basis Decisional Diffie-Hellman Assumptions Cryptanalysis of a Partially Blind Signature Scheme or How to Make Conditional Financial Cryptography A Generic Construction for Token-Controlled Public Key Encryption Timed-Release and Key-Insulated Public Key Encryption Conditional Encrypted Mapping and Comparing Encrypted Numbers Revisiting Oblivious Signature-Based Envelopes Payment Systems Provably Secure Electronic Cash Based on Blind Multisignature Schemes Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings..... Efficient Protocols Author Index

<<金融密码术与数据安全>>

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>