

# 《信息和通信安全》

## 图书基本信息

书名：《信息和通信安全》

13位ISBN编号：9787030152442

10位ISBN编号：7030152441

出版时间：2005-4

出版社：科学出版社

作者：杨波，韩臻编

页数：396

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)

# 《信息和通信安全》

## 内容概要

本书为第四届中国信息和通信安全学术会议论文集，收录论文73篇，内容涉及信息和通信安全的各个领域，包括密码学、网络安全、信息隐藏与数字水印、电子商务安全等。

本书可供从事信息安全、密码学、计算机、通信、数字等专业的科技人员和高等院校相关专业的师生阅读、参考。

## 书籍目录

密码学 一种完整的非对称公钥叛逆者追踪方案 Jacobi序列的pattern分布 多输出函数的相关度及其一点应用 多值钟控“停走”生成器的概率模型 广义  $\chi^2$ -相关免疫布尔向量函数 基于圈积的多级密钥分享方案 SHACAL-2算法分析 New Proxy Blind Signature and Proxy Ring Signature Schemes form Bilinear Pairings Znp上广义部分Bent函数的密码学性质  $d=9$  Hamilton阵列编码实现与密码特性分析 逻辑化方法的分析改进及其与串空间方法的比较 广播信道下动态会议密钥管理 点包含问题的秘密信息识别与安全多方计算 A New Identification and Key Agreement Protocol Achieving User Anonymity for Distributed Networks Break and Repair the Proxy Blind Signature Scheme Based on DLP 基于线性多项式重构的快速相关攻击算法研究 一种新的不经意的基于数字签名的电子信封 Cryptanalysis on Two Blind Signature Schemes 可扩展双域椭圆曲线密码协处理器的设计与实现 无符号三元联合稀疏形式表示 A New Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key Transformation between Hessian-form and Weierstrass-form of Elliptic Curve 关于有限域 $GF(2^m)$ 上最优正规基的乘法矩阵的计算 一种快速求解降次函数的新算法 理想安全曲线基点选取算法的设计 消息认证码的研究现状 安全协议的可视化分析和设计研究 一类布尔函数的Walsh谱分解式及其应用 一类细胞自动机的状态研究  $GF(2)$ 上线性函数支数达到最大的充要条件 Cryptanalysis of REESSE1 Digital Signature Algorithm A Class of the Weak Generalized Self-shrinking Generators 密码算法的FPGA实现 基于双线性映射的ID-代理签名与指定验证者代理签名 关于完全非线性函数的一些研究 Study on the Differential Uniform of S-boxes Verifiably Committed Signatures Based On Discrete Logarithm短文 改进的求和生成器的密码分析 A New Theorem of the Quadratic Residuosity Problem 破译6轮Rijndael算法全部密钥的最新结果 Two Improved Proxy Signature Schemes for Mobile Communication 一个分组密码的工作模式及其安全性分析 Further Analysis on Some Signature Schemes with Message Recovery(Extended Abstract) DNA计算在密码领域中应用的探讨 基于对的组密钥协商协议及其分析 A New Type of Proxy . Blind Signature : Multi-proxy Blind Multi-signature Scheme 一种高效的群签名方案 多输出函数的自相关函数特征和线性结构网络安全 基于身份的AAA认证在移动IP中的应用 Security Comes to SNMP The Study of the IDSS Based on Agent A Single Sign-on Solution Based on PKI and PMI 安全协议中拒绝服务攻击的防范及分析 P2P网络中基于级别的访问控制 A Complete Policy Lifecycle Model for Policy-Based Security Management of Information Systems Secure Multicast Communication in Ad Hoc Networks The Analysis of Bluetooth Monitor Subsystem Power Consumption Grid Node Computing Pool Security Analysis Based on Knowledge Base SDSI中名字证书链的分布式发现 基于移动代理的网络入侵预警框架 A Novel Approach to Intrusion Detection Based on SVD and SVM短文 信息和通信网络结构的鲁棒性与脆弱性研究——复杂网络视角的网络安全研究进展 基于库函数调用的入侵检测技术研究 缓冲区溢出攻击代码的分析研究 WALSG : A Solution to Web Application Level Security AHP在信息系统风险评估中的应用研究 基于异构平台的入侵容忍COTS服务器设计与实现 A Study of Secure Routing Technology for Ad Hoc Networks信息隐藏与数字水印 改进的隐写术安全性度量 基于椭圆曲线的数字签名水印方案研究与设计 广义E1Gamal签名中窄带阈下信道的可实现容量及其构造方案电子商务安全 A Electronic Cash System with Several Banks 一种无关联的可分电子票据方案

# 《信息和通信安全》

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