

<<密码学进展>>

图书基本信息

书名：<<密码学进展>>

13位ISBN编号：9787030132178

10位ISBN编号：7030132173

出版时间：2004-4

出版时间：科学出版社

作者：陈克非 李祥

页数：474

字数：702000

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>

<<密码学进展>>

内容概要

本书是2004年在无锡召开的第八届中国密码学学术会议论文集。

书中共收集密码学各个分支的研究论文73篇，主要内容包括序列密码、分组密码、公钥密码、非传统密码、数字签名、秘密共享、多方计算、密码协议、信息隐藏、代数、信息论与编码、网络安全与系统安全、密码应用等。

本书可供从事密码学、数学和计算机通信专业的科技人员以及高等院校相关专业的师生参考。

<<密码学进展>>

书籍目录

序列密码 On the Statistical Properties and Linear Span of FCSR Sequences WOPS:A Family of Word-oriented PSGs 一类可加线性流密码的密钥疑义度率及其应用 一种改进的基于后验概率判决的快速相关攻击算法 蓝牙组合生成器的相关性分析 The Editing Generator-An Extension 分组密码 Trace Representations of Coordinates of Finite Field Elements and Their Cryptographic Applications DES类密码S盒的演化设计策略 一类广义Feistel密码的差分分析 一类S盒密码学性质的研究 对低轮Safer++256的积分密码分析 公钥密码、秘密共享、多方计算 Ring Identification Schemes 一种适合椭圆曲线密码的快速标量乘法对算法 基于身份的密钥封装机制 公开可验证的门限签名方案 A Study of Secure Multi-party Scientific Computation Problem 安全的门限秘密共享方案 线性多密钥共享 The Combined Use of FAPKC does not Compromise the Security An Efficient Verifiable Secret Sharing Scheme 构造有限域上具有给定阶点的椭圆曲线非传统密码 Quantum Identity Authentication Without Lost of Quantum Channel 一种基于Petri网的分组密码体制 热流密码体制的一种非齐次半线性模型的加、解密实现 基于热流密码体制的加、解密实现及相关分析 混沌动力系统临界点理论及应用研究 一类单参数混沌系统的追踪控制与保密通信数字签名 An Efficient Group Signature from Gap Diffie-Hellman Groups A Transitive Signature Schemes Provably Secure Against Adaptive Chosen-message Attack Improved Scheme of the Forgeable Self-certified Signature t-out-of-n Ring Signatures from Discrete Logarithm Public Keys Cryptanalysis of Two Signature Schemes 基于DSA的两种盲签名体制 可使用异型密钥的多重签名和多潜信道 一个完善的强Key-insulated签名方案 Equivalent Private Key Attack on a Signature Scheme Based on Error-correcting Codes 传递签名及其应用的研究 对修改的ElGamal数字签名的密码分析 一种高效安全的群签名成员删除方案密码协议 Analysis on the Secrecy of the Password-only Key Exchange Protocol Using Item- node Graph Model Convenient, Secure E-payment Protocol with Optional Encryption A New Approach to Prevent Blackmailing in E-cash Efficient Protocols of Secure Electronic Coupons 一种新颖的基于RSA密码体制的最优化公平交换协议 基于GNY逻辑的无线移动网络密码协议的安全性分析 理想在协议分析中的进一步应用 一个改进的Kerberos鉴别协议的设计与分析 三方密码协议运行模式分析法 一种新型群组通信的密钥协商协议 基于有穷自动机模型的电子商务协议的公平性分析信息隐藏 Steganography by Communication Protocols 基于视觉掩蔽值的稳健水印认证算法 一种基于QR分解的脆弱水印算法代数、信息论与编码 Bounded One-way Functions and Its Properties k-1阶相关免疫布尔函数的“最优k元逼近”问题 Bent函数的演化设计 完善保密密码体制的条件与设计 HAVAL标准中布尔函数的分析与改进 基于条件熵匿名模型的优化 准最佳二进阵列 Optimal Maximal Prefix Codes for Data Compression and Encryption 代数次数为2的p值广义Bent函数的标准型及其在多维护广义Bent函数构造中的应用网络安全与系统安全 An Implementation of Cryptosystems Based on Tate Pairing A Model of Secure Dynamic ad-hoc Mobile Networks 基于安全类型系统的访问控制模型 无线局域网密钥安全管理方案研究 Efficient Key Agreements in ad-hoc Networks 一种动态安全的密文数据库检索方法密码应用 F上椭圆曲线协处理器的FPGA有效实现 Java大整数类在概率素数测试中的BUG及分析 有限自动机单钥密码的一种IC卡实现及对合的选择 Hardware Implementation Aspects of Modular Exponentiations Extended Abstract 一种新的SIP SSO机制

<<密码学进展>>

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>