

<<密码学进展>>

图书基本信息

书名：<<密码学进展>>

13位ISBN编号：9787811047424

10位ISBN编号：781104742X

出版时间：2007-10

出版时间：西南交通大学出版社

作者：何大可

页数：353

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2007年10月在成都召开的中国密码学会2007年会论文集。

书中收录了涉及密码学若干分支的研究论文54篇。

主要内容包括：序列密码与分组密码、公钥密码、HASH函数与数字签名、密码协议、量子密码、密码实现与应用等。

本书可供从事密码学、信息安全、通信与信息系统、计算机应用技术等专业的科技人员和高等院校师生参考。

<<密码学进展>>

书籍目录

序列密码与分组密码 Algebraic Immunity Hierarchy of Boolean Functions Joint Linear Complexity of
 Multiple Linear Recurring Sequences 周期为 $2N$ 的二元序列的 K -错线性复杂度的期望值 $Z/(2E)$ 上本原
 序列的模压缩序列的唯一性 Q -LFSR的分类研究 Two Criteria on the Key Schedule of Block Ciphers 基
 于蚁群算法搜索分组密码的线性逼近公钥密码 A New Form of an Elliptic Curve Authenticated
 Certificateless public key encryption without pairing Efficient fully secure hierarchical identity based encryption
 without random oracles Efficient chosen-Ciphertext secure certificateless threshold key encapsulation mechanism
 适用于ATE对实现的椭圆曲线的构造 利用双基链计算超椭圆曲线除子标量乘 环 ZN 上圆锥曲线
 的RSA密码的短私钥攻击的注记 圆锥曲线与素性判定 基于滑动窗口技术的有限域 $GF(2N)$ 乘法算法
 杂凑函数与数字签名 Cryptanalysis of au et al.'s hierarchical identity-based signature scheme Short signature
 from ElGamal Encryption and Its Application to Scalable Broadcast Cryptanalysis and Improvement of two proxy
 signature schemes 无证书广义指定验证者签名方案 标准模型下T门限强壮的组签名方案 关于“基于
 离散对数问题的盲数字签名改进方案”的注记 一个前向安全的基于身份的多代理多签密方案 提高
 抗碰撞能力的HASH函数新框架密码协议 Towards optimal t-out-of-n oblivious transfers Extensible belief
 multisets for wireless security protocol analysis 保护隐私的联合求解线性方程组 一个多安全群组密钥协商
 协议的安全性注记 “FFGG”协议的设计与分析 A KEY Management protocol with robust continuity
 for sensor networks Needham-schroeder共享密钥协议的重新设计量子密码密码实现与应用短文附件

<<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>