第一图书网, tushu007.com

<<超椭圆曲线密码体制的理论与实现>>

图书基本信息

书名：<<超椭圆曲线密码体制的理论与实现>>

13位ISBN编号：9787802076235

10位ISBN编号：7802076234

出版时间：2006-7

出版时间：经济管理出版社

作者：肖如良

页数：176

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

内容概要

本书介绍了近几年来作者在超椭圆曲线密码体制的理论及其实现上的成果。
全书共分八章，主要介绍了超椭圆曲线密码体制的算法数论基础、超椭圆曲线的密码学体系、除子群运算的核心算法、从ECC的技术标准到超椭圆曲线密码体制的实现技术，同时也对超椭圆曲线密码体制与ECC及RSA在安全强度、复杂度以及实现上进行了比较。
　本书可以作为信息安全，密码学、计算机科学与技术等专业的大学生和研究生的教学参考书，也可供从事相关专业的教学、科研和工程人员参考。

书籍目录

第一章 绪论 1.1 计算机网络和信息系统的安全 1.2 PKI基础设施 1.3 基于PKI的安全解决方案 1.4 公钥密码的发展 I.5 椭圆曲线密码体制 1.6 超椭圆曲线密码体制的研究背景、意义及现状 1.7 本书的主要工作 第二章 超椭圆曲线密码学算法数论基础 2.1 算法数论基础理论 2.2 超椭圆曲线的有关定义及基本性质 2.3 除子 2.4 主除子及Jacobian商群 2.5 Jacobian商群的基数 2.6 Frobenius自同态 2.7 超椭圆曲线密码体制的安全性条件及商群的构造方法 本章小结第三章 超椭圆曲线密码体制的理论研究 3.1 除子的明文嵌入方法FPI 3.2 FPI明文嵌入方法的分析 3.3 明文嵌入方法FPI的实验结果分析 3.4 基于FPI的超椭圆曲线的密码学体系 本章小结第四章 超椭圆曲线上除子群运算的核心算法 4.1 主要的数据结构 4.2 参数的表示 4.3 超椭圆曲线密码引擎的核心问题——标量乘法的解决方案 本章小结第五章 从ECC的技术标准到HECC的实现 5.1有限域的算法约定 5.2 Jacobian商群的算法约定 5.3 数据类型及其转换的算法约定 5.4 超椭圆曲线密码体制的参数约定 5.5 超椭圆曲线密码体制的可供参考的曲线约定 5.6 超椭圆曲线密码体制结合SSL协议的应用 5.7 椭圆曲线密码体制结合SET协议的双重数字签名 本章小结第六章 超椭圆曲线密码体制的关键实现技术 6.1概述 6.2 HECC的数据类型转换 6.3 HECC实现的基本思想 6.4 HECC实现的关键类的设计 6.5 HECC的密钥类的设计 6.6 HECC的辅助类的设计 6.7 综合加密类IESEngine的设计 6.8 综合加密系统HECIES的实现流程 本章小结第七章 超椭圆曲线密码体制HECC的评价 7.1 HECC与ECC、RSA在同等安全强度下的比较 7.2 HECC与ECC在复杂度上的比较 7.3 HECC与ECC在实现上的比较 本章小结第八章 超椭圆曲线密码体制的应用以及进一步的工作 8.1 超椭圆曲线密码体制的应用 8.2 进一步的工作 本章小结参考文献后记

第一图书网, tushu007.com

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