第一图书网, tushu007.com

# <<椭圆曲线密码体系研究>>

## 图书基本信息

书名：<<椭圆曲线密码体系研究>>

13位ISBN编号：9787560938585

10位ISBN编号：7560938582

出版时间：2006-10

出版时间：华中科技大学出版社

作者：肖攸安

页数：248

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

椭圆曲线密码体系是当前信息安全领域的研究热点之一，本书在分析和研究椭圆曲线密码学的最新研究成果的基础上，分7章总结了作者在该领域所完成的一系列的研究工作。
其中，第1章从网络信息安全现状出发，分析了所面临的安全威胁，归纳了人们所提出的安全需求，给出了相应的解决方案，引出了椭圆曲线公钥密码体系。
第2章主要介绍和讨论了在本书中所要用到的椭圆曲线密码体系的基本数学理论基础和相关的背景知识。
第3章在介绍有限域上的离散椭圆曲线的基础上，深入讨论了椭圆曲线有限群上的椭圆曲线离散对数问题，归纳了安全椭圆曲线选取准则。
第4章研究了椭圆曲线有限群阶的计算问题，深入研究了SEA数点算法。
第5章根据安全通信的需要，在讨论通信协议安全性问题的基础上，研究和分析了作者所设计的可用于椭圆曲线密码体系的密钥生成、密钥协商、密钥分配、信息加密、数字签名等多种安全高效的密码方案。
第6章和第7章深入研究了椭圆曲线密码体系实现中的若干关键技术，给出了典型方案的具体实现算法和实验结果。
　　本书适用于信息、计算机及相关专业的博士、硕士研究生和高年级本科生，也可作为信息安全领域的研究人员和专业技术人员的参考书。

# <<椭圆曲线密码体系研究>>

## 书籍目录

第1章 绪论　1.1 网络信息安全　1.2 安全威胁和安全需求　1.2.1 被动攻击　1.2.2 主动攻击　1.2.3 安全需求　1.3 解决方案　1.4 公钥密码编码学第2章 椭圆曲线数学基础　2.1 群　2.2 环　2.3 域　2.4 有限域　2.5 椭圆曲线　2.6 椭圆曲线的分类　2.7 椭圆曲线上点的群运算法则　2.8 自同态环第3章 椭圆曲线离散对数　3.1 有限域上的离散椭圆曲线　3.2 椭圆曲线离散对数问题　3.3 一般椭圆曲线上的离散对数问题的求解　3.3.1 大步小步算法　3.3.2 Pohlig-Hellman演化类算法　3.3.3 Pollard- ρ 概率类算法　3.3.4 Index算法和Xedni算法　3.4 特殊椭圆曲线上的离散对数问题的求解　3.5 安全椭圆曲线第4章 椭圆曲线有限群阶的计算　4.1 Schoof算法　4.2 SEA算法　4.3 模多项式及其实现　4.4 Elkies算法及其实现　4.5 Atkin算法及其实现　4.6 SEA算法的最后步骤　4.7 SEA算法的实现第5章 椭圆曲线密码体系　5.1 密码协议及其安全性　5.1.1 密码协议分析的前提　5.1.2 密码协议分析的方法　5.2 密钥的管理　5.2.1 用户基本密钥的生成　5.2.2 密钥协商方案　5.2.3 XKDS密钥分配方案　5.3 数据加密　5.4 数字签名　5.4.1 XECDS普通数字签名方案　5.4.2 加密与签名　5.4.3 盲数字签名方案　5.4.4 代理数字签名方案　5.4.5 XECLPDS受控代理数字签名方案　5.4.6 其他数字签名方案第6章 椭圆曲线密码体系的若干关键技术　6.1 寻找安全椭圆曲线　6.2 基点的选取　6.3 基本群运算的实现　6.4 椭圆曲线有限群上的数乘运算第7章 椭圆曲线密码体系的实践　7.1 任意长度安全真随机密钥的生成　7.2 XKAS密钥协商方案　7.3 XKDS密钥分配方案　7.4 数据加密算法　7.5 XECDS数字签名方案参考文献

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