

<<椭圆曲线公钥密码导引>>

图书基本信息

书名：<<椭圆曲线公钥密码导引>>

13位ISBN编号：9787030173607

10位ISBN编号：7030173600

出版时间：2006-10

出版单位：科学出版社

作者：祝跃飞、张亚娟

页数：246

字数：298000

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>

## <<椭圆曲线公钥密码导引>>

### 内容概要

椭圆曲线是一门古老而内容丰富的数学分支，ECC理论涉及了许多深奥的椭圆曲线算数理论，要系统地详细地讲授ECC理论需要较深的数学基础。

本书的目的是在交换代数的基础上系统阐述ECC理论，为有志于从事该方向研究的人员提供一本系统全面的基础性教材。

本书围绕ECC的理论和实践分三部分：第一部分介绍椭圆曲线的算术理论，主要是有限域上椭圆曲线的相关理论；第二部分为ECC的密码理论，重点论述了有限域上椭圆曲线的求阶算法，椭圆曲线上的离散对数求解算法和椭圆曲线公钥密码体制，椭圆曲线的素性证明和大数分解算法；第三部分为椭圆曲线公钥密码的有效实现，重点论述椭圆曲线公钥密码体制中的关键算子；标量乘法和双标量乘法的快速实现。

本书可以作为信息安全和密码学专业研究生的教材，也可供相关的研究人员参考。

## &lt;&lt;椭圆曲线公钥密码导引&gt;&gt;

## 书籍目录

前言第1章 椭圆曲线 1.1 概述 1.2 仿射平面曲线 1.3 仿射Weierstrass方程 1.4 椭圆曲线  
 1.5 除子 (divisor) 习题第2章 有限域上的椭圆曲线 2.1 有理映射和同种 2.2 同种的次数  
 2.3  $K(E)$  的导数 2.4 可分性 2.5  $E[m]$  的群结构 2.6 可除多项式 2.7 Weil对 2.8 Itasse  
 定理 2.9 群结构 2.10 Weil定理 2.11 扭曲线 2.12 超奇异曲线 习题二第3章 椭圆曲线离  
 散对数问题 3.1 Shanks的小步大步算法 3.2 Pollard  $p$ 算法 3.3 Pohlig—Hellman算法 3.4  
 Index Calculus算法 3.5 椭圆曲线离散对数问题 3.5.1 MOV算法 3.5.2 阶为 $p$ 的椭圆曲线  
 3.6 椭圆曲线公钥密码 3.6.1 安全参数的选取 3.6.2 Diffie-Hellman密钥交换协议 3.6.3  
 ElGamal加密体制 3.6.4 ECDSA 习题三第4章 椭圆曲线求阶算法 4.1 Schoof算法 4.2  
 Elkies素数 4.3 同种映射和模多项式 4.4 Atkin素数 4.5 Schoof-Elkies—Atkin算法 4.6 Satoh  
 算法 4.7 AGM算法第5章 椭圆曲线大数分解算法 5.1 Pollai-d  $p-1$ 算法 5.2 模 $n$ 约化 5.3  
 Lenstra算法 5.4 时间复杂度第6章 椭圆曲线素性判定算法 6.1 带复乘的椭圆曲线 6.2  
 Goldwasser—Kilian测试 6.3 Atkin测试第7章 椭圆曲线密码的快速实现 7.1 点加 $P+Q$ 和倍点 $2P$   
 7.1.1 投射坐标 7.1.2 椭圆曲线 $y^2=X^3+ax+b$  7.1.3 椭圆曲线 $y^2+xy=x^3+ax^2+b$  7.2 标量  
 乘法 $kP$  7.2.1 动点的标量乘法 7.2.2 定点的标量乘法 7.3 双标量乘法 $kP+2Q$  7.3.1 JSF  
 7.3.2 JSF3 7.4 Koblitz曲线参考文献《现代数学基础丛书》已出版书目

<<椭圆曲线公钥密码导引>>

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>