

<<椭圆曲线及其在密码学中的应用>>

图书基本信息

书名：<<椭圆曲线及其在密码学中的应用>>

13位ISBN编号：9787030200341

10位ISBN编号：7030200349

出版时间：2007-12

出版时间：科学

作者：吴铤 董军武 王明强

页数：172

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>

## <<椭圆曲线及其在密码学中的应用>>

### 内容概要

本书以介绍椭圆曲线在密码学中的应用为目标，用浅显易懂的语言全面讲述了椭圆曲线公钥密码的相关知识，包括公钥密码学概述、有限域上椭圆曲线的算术理论、椭圆曲线上离散对数的求解算法以及有限域上椭圆曲线的求解算法等。

本书最突出的特点在于只利用近世代数等基础知识来揭示椭圆曲线内在的代数和几何结构，所以特别适合作为研究生和高年级本科生等初学者了解、掌握椭圆曲线公钥密码理论的入门书籍，也可供相关研究人员参考。

## <<椭圆曲线及其在密码学中的应用>>

### 书籍目录

译者的话 序言 前言 第1章 公钥密码算法 1.1 私钥密码学与公钥密码学 1.2 Diffie—Hellman密钥交换协议 1.3 ELGAMAL密码体制 1.4 签名方案 1.5 标准 第2章 椭圆曲线上的群运算 2.1 仿射平面曲线 2.2 仿射椭圆曲线 2.3 变量变换与标准形式 2.4 奇异性 2.5 局部环 $OP(E)$  2.6 射影平面曲线 2.7 射影椭圆曲线 2.8 除子 2.9 直线 2.10 Picard群 2.11 群法则 第3章 有限域上的椭圆曲线 3.1 有理映射和自同态 3.2 分歧指数与次数 3.3  $K(E)$ 上的导数 3.4 可分性 3.5  $m$ 扭点 3.6 除子多项式 3.7 Weil对 3.8 Hasse定理 3.9 Weil定理 3.10 挠曲线 3.11 超奇异曲线 3.12 群结构 第4章 离散对数问题 4.1 Shanks's大步小步法 4.2 Pollard's  $\rho$ 算法 4.3 Pohlig—Hellman方法 4.4 指标计算法 4.5 椭圆曲线离散对数问题 第5章 椭圆曲线上点数的计算 5.1 大步—小步算法 5.2 Schoof算法 5.3 Elkies素数 5.4 同种映射和模多项式 5.5 Atkin素数 5.6 SEA算法 参考文献 符号表 中英文对照索引

<<椭圆曲线及其在密码学中的应用>>

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>