

《椭圆曲线密码算法导引》

图书基本信息

书名：《椭圆曲线密码算法导引》

13位ISBN编号：9787302169888

10位ISBN编号：7302169888

出版时间：2008-5

出版社：清华大学出版社

作者：卢开澄,卢华明

页数：113

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《椭圆曲线密码算法导引》

内容概要

《椭圆曲线密码算法导引》分为两个部分，共6章。第一部分是数学基础，介绍与椭圆曲线算法有关的数论、群论与有限域理论；第二部分是椭圆曲线有效算法，讨论椭圆曲线公钥密码及其实用算法。《椭圆曲线密码算法导引》语言精练，结构合理，内容丰富，立论严谨，适合作为计算机专业高年级学生和研究生的教材，也可供科技工作者参考。

《椭圆曲线密码算法导引》

书籍目录

第一部分 数学基础第1章 数论简介1.1 基本概念1.2 同余式1.3 Euler函数1.4 Euler定理、Fermat定理1.5 一元一次同余方程1.6 中国剩余定理1.7 平方剩余与非平方剩余第2章 群论2.1 群的概念2.2 置换群2.3 群的基本性质2.4 若干概念2.4.1 阶2.4.2 子群2.4.3 循环群2.5 陪集2.6 群的同构与同态2.7 群的置换表示2.8 正规子群和商群2.9 交换群第3章 有限域3.1 定义3.2 有限域的特征与元素的阶3.3 n 的阶3.4 本原元素3.5 极小多项式3.6 不可化约多项式3.7 有限域的性质3.8 x^n-x 的因式分解3.9 同构3.10 迹和范3.11 一般二次方程求解问题第二部分 椭圆曲线密码有效算法第4章 椭圆曲线4.1 Weierstrass方程4.2 判别式与结式4.3 椭圆曲线上的加法法则4.4 射影平面4.5 有限域上的椭圆曲线4.6 $\text{char}(K)=2$ 加法法则4.7 $(P+Q)+R=P+(Q+R)$ 与椭圆曲线上的Abel群4.8 Mordell-Weil定理4.8.1 有理点的高度4.8.2 若干等式4.8.3 关于高度 $H(P)$ 的几个不等式4.8.4 Mordell-Weil定理证明4.8.5 群 $E(Q)$ 的有限生成4.9 Lutz-Nazell定理4.10 Hasse定理第5章 椭圆曲线公钥密码介绍5.1 传统密码5.2 RSA公钥密码与数字签名5.3 椭圆曲线密钥互换协议5.4 椭圆曲线ElGamael公钥第6章 椭圆曲线密码若干实用算法6.1 概论6.2 如何确定椭圆曲线6.3 $\#E(GF(2^n))$ 的计算6.4 $GF(2^m)$ 上算术问题6.5 求 P 点阶的算法6.6 求 kP 的算法6.7 NAF6.8 复合域6.9 Weil定理6.10 快速求逆的算法6.11 复合域的求逆6.12 若干 $2kP$ 型公式参考文献

《椭圆曲线密码算法导引》

编辑推荐

椭圆曲线原属抽象数学“代数几何学”的一个分支，自从Koblitz等人提出用来构造公钥密码以来，获得了快速发展。椭圆曲线密码算法作为“计算机密码学”的续篇，可以为非数学专业的人士在椭圆曲线与“密码”之间搭起一座桥梁。本书分为两个部分。第一部分是数学基础，介绍与椭圆曲线算法有关的数论、群论与有限域理论；第二部分是椭圆曲线有效算法，讨论椭圆曲线公钥密码及其实用算法。本书适合作为计算机专业高年级学生和研究生的教材，也可供科技工作者参考。

《椭圆曲线密码算法导引》

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：www.tushu111.com