

<<椭圆与超椭圆曲线公钥密码的理论与实现>>

图书基本信息

书名：<<椭圆与超椭圆曲线公钥密码的理论与实现>>

13位ISBN编号：9787030173584

10位ISBN编号：7030173589

出版时间：2006-12

出版时间：科学出版社

作者：王学理

页数：478

字数：586000

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>

<<椭圆与超椭圆曲线公钥密码的理论与实现>>

内容概要

本书论述了椭圆与超椭圆曲线公钥密码学的基本理论及实现，其中包括：椭圆曲线公钥密码体制介绍，椭圆和超椭圆曲线的基本理论，定义在有限域上椭圆和超椭圆曲线的有理点的计数，椭圆和超椭圆曲线上的离散对数，椭圆和超椭圆曲线离散对数的初等攻击方法、指标攻击方法、代数几何攻击方法及代数数论攻击方法。

本书的特点之一，内容涉及面广，在有限的篇幅内，包含了必要的预备知识和较完备的数学证明，尽可能形成一个完整的体系；特点之二，用较为系统和统一的方法总结了大部分有限域上椭圆和超椭圆曲线有理点的有效计数方法；特点之三，用系统的数学方法讲述了椭圆和超椭圆曲线离散对数攻击的主要有效方法；特点之四，我们总是从算法数论的角度进行论述，对每个重要的理论结果，总是尽可能给出其可编程的实际算法。

本书的部分较初等的内容曾多次在中国科学院研究生院信息安全重点实验室及广州大学和湖南大学作为研究生教材使用。

本书可作为信息安全、数论及相关专业的研究人员、高等学校的教师和高年级学生的参考书，其部分内容也可做为信息安全、数论等专业的研究生的教材使用。

书籍目录

第一部分 椭圆曲线密码体制	第一章 椭圆曲线密码体制	1.1 有限域上的椭圆曲线	1.2 椭圆曲线公钥密码体制	1.3 基于双线性对的密码方案	第二部分 提升到整体域上的点数计算算法
第二章 复数域上的椭圆曲线	2.1 Weierstrass函数和椭圆曲线	2.2 椭圆曲线的同构	2.3 同种椭圆曲线	2.4 除子多项式	2.5 模多项式
第三章 一般域上的椭圆曲线	3.1 椭圆曲线的群结构	3.2 除子类群	3.3 同种映射	3.4 Tate模和Weil对	3.5 有限域上的椭圆曲线
3.6 p挠元点和自同态环	第四章 复乘理论与算法	4.1 椭圆曲线的复乘理论	4.2 利用复乘生成椭圆曲线	4.3 算法综述	第五章 椭圆曲线的SEA算法
5.1 算法的概述	5.2 等价模多项式	5.3 计算同种曲线	5.4 计算除子多项式的因子	5.5 Atkin算法	5.6 计算tmodln
5.7 算法汇总	第三部分 提升到局部域上的点数计算算法	第六章 p-adic数	6.1 p-adic数的引入	6.2 赋值	6.3 完备化
6.4 Hensel引理	第七章 椭圆曲线的形式群	7.1 在无穷远点展开	7.2 形式群	第八章 局部域上的椭圆曲线	8.1 极小Weierstrass方程
8.2 约化映射及其性质	8.3 有限阶点	8.4 坐标赋值有限的点集	第九章 Satoh方法的理论基础	9.1 引论	9.2 多项式的因子的提升
9.3 典范提升的构造	9.4 应用到点数的计算	第十章 Satoh的算法及其实现	10.1 局部域及其上一些算法的实现	10.2 Frobenius同态及典范提升	10.3 提升的算法
10.4 计算迹	第十一章 Mestre的AGM算法	11.1 典范提升的j不变量的计算	11.2 计算Frobenius映射的迹	11.3 范数的快速算法	11.4 改进的AGM算法
11.5 改进的Satoh算法	第十二章 Harley算法	12.1 广义牛顿算法	12.2 提升域多项式与Harley算法	第十三章 Kedlaya算法	13.1 de Rham复形与上同调
13.2 上同调空间的基	13.3 Frobenius提升	13.4 算法综述	13.5 推广到Superelliptic曲线	第十四章 F2上超椭圆曲线的Kedlaya算法	14.1 F2上超椭圆曲线的上同调
14.2 算法综述	第四部分 椭圆曲线密码体制的攻击方法	第十五章 椭圆曲线离散对数的初等攻击	15.1 椭圆曲线公钥密码	15.2 小步一大步法	15.3 家袋鼠和野袋鼠
15.4 MOV约化	15.5 Flt, 约化	15.6 SSSA约化	15.7 有限域上离散对数的计算	第十六章 超椭圆曲线离散对数的指标计算法	16.1 超椭圆曲线的Jacobian
16.2 虚2次代数函数域	16.3 小亏格超椭圆曲线离散对数的指标计算方法	16.4 大亏格超椭圆曲线离散对数的指标计算方法	第十七章 椭圆曲线离散对数的代数几何攻击方法	17.1 Weil下降与Weil攻击	17.2 特征2的GHS攻击
17.3 奇特征	17.4 Weil限制与低次扩域上的椭圆曲线离散对数攻击	第十八章 离散对数的代数数论攻击方法	18.1 Brauer群和Galois上同调	18.2 Brauer群及有限域中的离散对数问题-	18.3 不变量映射的局部计算
18.4 不变量映射的整体计算	18.5 数域筛法	18.6 函数域筛法	18.7 (超)椭圆曲线离散对数, Tate对和Brauer群	第五部分 椭圆曲线密码体制的实现	第十九章 椭圆曲线的倍点计算
19.1 基域和曲线的选择	19.2 椭圆曲线上点的表示和运算	19.3 椭圆曲线的倍点运算	19.4 Frobenius展开	参考文献索引	《现代数学基础丛书》已出版书目

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>