<<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

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。

<<椭圆与超椭圆曲线公钥密码的理论与实现>>

书籍目录

版权说明