<<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

出版时间：清华大学出版社

作者：卢开澄,卢华明

页数：113

<<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

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