<<椭圆曲线公钥密码导引>>

图书基本信息

书名：<<椭圆曲线公钥密码导引>>

13位ISBN编号：9787030173607

10位ISBN编号：7030173600

出版时间：2006-10

出版时间：科学出版社

作者：祝跃飞、张亚娟

页数：246

字数：298000

<<椭圆曲线公钥密码导引>>

内容概要

椭圆曲线是一门古老而内容丰富的数学分支，ECC理论涉及了许多深奥的椭圆曲线算数理论，要系统详细地讲授ECC理论需要较深的数学基础。
本书的目的是在交换代数的基础上系统阐述ECC理论，为有志于从事该方向研究的人员提供一本系统全面的基础性教材。
本书围绕ECC的理论和实践分三部分：第一部分介绍椭圆曲线的算术理论，主要是有限域上椭圆曲线的相关理论；第二部分为ECC的密码理论，重点论述了有限域上椭圆曲线的求阶算法，椭圆曲线上的离散对数求解算法和椭圆曲线公钥密码体制，椭圆曲线的素性证明和大数分解算法；第三部分为椭圆曲线公钥密码的有效实现，重点论述椭圆曲线公钥密码体制中的关键算子；标量乘法和双标量乘法的快速实现。
本书可以作为信息安全和密码学专业研究生的教材，也可供相关的研究人员参考。

<<椭圆曲线公钥密码导引>>

书籍目录

<<椭圆曲线公钥密码导引>>

版权说明