<<椭圆曲线及其在密码学中的应用>>

图书基本信息

书名：<<椭圆曲线及其在密码学中的应用>>

13位ISBN编号：9787030200341

10位ISBN编号：7030200349

出版时间：2007-12

出版时间：科学

作者：吴铤 董军武 王明强

页数：172

<<椭圆曲线及其在密码学中的应用>>

内容概要

本书以介绍椭圆曲线在密码学中的应用为目标，用浅显易懂的语言全面讲述了椭圆曲线公钥密码的相关知识，包括公钥密码学概述、有限域上椭圆曲线的算术理论、椭圆曲线上离散对数的求解算法以及有限域上椭圆曲线的求解算法等。

本书最突出的特点在于只利用近世代数等基础知识来揭示椭圆曲线内在的代数和几何结构，所以特别适合作为研究生和高年级本科生等初学者了解、掌握椭圆曲线公钥密码理论的入门书籍，也可供相关研究人员参考。

<<椭圆曲线及其在密码学中的应用>>

书籍目录

<<椭圆曲线及其在密码学中的应用>>

版权说明