《超椭圆曲线密码体制的理论与实现》

图书基本信息

书名：《超椭圆曲线密码体制的理论与实现》

13位ISBN编号：9787802076235

10位ISBN编号：7802076234

出版时间：2006-7

出版社：经济管理出版社

作者：肖如良

页数：176

《超椭圆曲线密码体制的理论与实现》

内容概要

本书介绍了近几年来作者在超椭圆曲线密码体制的理论及其实现上的成果。全书共分八章，主要介绍了超椭圆曲线密码体制的算法数论基础、超椭圆曲线的密码学体系、除子群运算的核心算法、从ECC的技术标准到超椭圆曲线密码体制的实现技术，同时也对超椭圆曲线密码体制与ECC及RSA在安全强度、复杂度以及实现上进行了比较。

本书可以作为信息安全，密码学、计算机科学与技术等专业的大学生和研究生的教学参考书，也可供从事相关专业的教学、科研和工程人员参考。

《超椭圆曲线密码体制的理论与实现》

书籍目录

《超椭圆曲线密码体制的理论与实现》