<<椭圆曲线密码快速算法理论>>

图书基本信息

书名：<<椭圆曲线密码快速算法理论>>

13位ISBN编号：9787115289438

10位ISBN编号：7115289433

出版时间：2012-10

出版时间：人民邮电出版社

作者：丁勇

页数：166

字数：245000

<<椭圆曲线密码快速算法理论>>

内容概要

《椭圆曲线密码快速算法理论》以作者及其研究组多年的研究成果为主体，结合国内外专家及学者在椭圆曲线密码快速算法方面的代表性成果，系统论述了这一领域的主要研究内容。
本书分为两个部分，共7章。
第一部分(第1、2章)讲述了研究椭圆曲线密码体制所需的基础知识及椭圆曲线上点的计算；第二部分(第3～7章)讲述了椭圆曲线密码的快速算法及其分析，主要包括非邻接形式(NAF)的改进形式，基于最大公约数(GCD)算法的高速带模除法，基于多基表示的快速算法，基于双基数链的Tate对优化算法。
《椭圆曲线密码快速算法理论》既可以作为密码学、信息安全、计算机科学等相关专业的研究生教学参考书，也可作为教师和相关科研人员的参考书。

<<椭圆曲线密码快速算法理论>>

书籍目录

<<椭圆曲线密码快速算法理论>>

编辑推荐

涉及具体技术算法细节及相关程序多年研究积累，反映该领域最新成果作者多年密码学和信息安全研究经验

<<椭圆曲线密码快速算法理论>>

版权说明