计算机工程　2007 33 (06): 98-100　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

Maple在椭圆曲线密码体制中的应用

库俊华，游　林，王升国

(海南师范大学数学系组合与信息科学实验室，海口 571158)

收稿日期　修回日期　网络版发布日期 2007-3-9　接受日期

摘要　Maple是功能强大的符号处理和数值分析工具，作为强大的交互式计算软件，Maple提供了强大的编程接口和工具包来帮助完成复杂的编程工作。利用Maple编程求出椭圆曲线上有理点，用Maple实现椭圆曲线上两点的加法、点的数乘运算及求某个基点阶数的算法，利用Maple实现椭圆曲线密码体制的加密及解密。相比C语言，Maple语言更接近于平时说话的语法。同时，Maple语言可以方便地转化成C语言。效率分析表明，对于数学公式比较多的程序，用Maple要比C语言简洁很多，这为编程带来了方便。

关键词　Maple　椭圆曲线　椭圆曲线密码体制

分类号

DOI:

对应的英文版文章：2007-6-059

通讯作者:

作者个人主页: 库俊华;游　林;王升国