数值计算与计算机应用 2005, 26(1) 74-80 DOI: ISSN: 1000-3266 CN: 11-2124/TP

本期目录 | 下期目录 | 过刊浏览 | 高级检索 [打印本页] [关闭]

论文

一种改进的冗余序列算法在椭圆曲线密码体制中的实现

郝林,李彤,柳青

云南大学信息学院;云南大学软件学院;云南大学软件学院 昆明 650091 ;昆明 650091 ;昆明 650091

摘要：

为了提高椭圆曲线上点的数乘的运算效率,本文提出了椭圆曲线离散对数(ECDLP)上一种改进的快速冗余算法.算法就文献提出的任一大的正整数的二进制冗余序列,给出了新的消除了序列转换中不必要的步骤的构建方法,从而使得大数倍乘中加运算得以大大减少.分析表明,新算法的效率较基本算法有明显提高.

关键词：

A BETTER REDUNDANT BINARY ALGORITHM FOR THE ELLIPTIC CURVES CRYPTOSYSTEM

Hao Lin (School of Information Science and Engineering, Yunnan University, Kunming 650091) Li Tong Liu Qing (School of Software. Yunnan University, Kunming 650091)

Abstract:

For the operational efficiency on the numerical multiplication of points on elliptic curves to be heighten, in this paper, a better fast redundant binary algorithm for the elliptic curves discrete logarithm problem (ECDLP) is presented. A new binary redundant representation which is necessity and suitability to transformation for a very large integer is defined. This algorithm has obtained the speed improvement as compared with the essential one which was presented in the paper by decreasing the addition computing steps.

Keywords:

收稿日期 修回日期 网络版发布日期

DOI:

基金项目:

通讯作者:

作者简介:

本刊中的类似文章

扩展功能

本文信息

Supporting info

PDF(250KB)

[HTML全文](0KB)

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

本文关键词相关文章

本文作者相关文章

PubMed