电子与信息学报 2003 25 (2): 275-278 ISSN: 1009-5896 CN: 11-4494/TN

研究简报

椭圆曲线密码体制中点的数乘的一种快速算法

①郝林, 罗平②

①云南大学计算机科学与工程系,昆明,650091;②清华大学计算机科学与技术系,北京,100084

收稿日期 2001-5-28 修回日期 2002-1-18 网络版发布日期 2008-7-11 接受日期

摘要
该文基于椭圆曲线密码体制, 提出了椭圆曲线上点的数乘的一种快速算法. 该算法通过引入2^k进制序列, 缩短了乘数的相应序列长度, 从而大大减少了点的数乘中的加法运算次数, 并且分析了k的最佳选取, 使得我们提出的算法比通常点的数乘算法效率提高了60%以上。

关键词 椭圆曲线 快速算法 密码学

分类号 TN918.1

A fast algorithm for the point multiplication in elliptic curve cryptosystems

①Hao Lin, Luo Ping②

①Dept. of Computer Science and Engineering Yunnan University Kunmin 650091 China;
②Dept. of Computer Science and Technology Tsinghua University Beijing 100084 China

Abstract
In this paper, a new fast algorithm for the numerical multiplication of the points on elliptic curves is presented. By introducing 2k sequence representation for number, the length of numerical multiplication is shortened, so that the number of addition operation on elliptic curves is decreased greatly. Moreover, the optimal choice of k is analyzed and the efficiency of the algorithm presented is improved about 60.

Key words Elliptic curve Fast algorithm Cryptography

DOI:

通讯作者

作者个人主页 ①郝林; 罗平②