计算机工程与应用 2010 46 (6): 112-115 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于Montgomery的分段并行标量乘快速算法

赵 耿[1，2]，彭程培[1，2]，李晓东[1]，张 栋[1，2]

1.北京电子科技学院，北京 100070
2.西安电子科技大学 通信工程学院，西安 710071

收稿日期 2008-9-25 修回日期 2009-4-1 网络版发布日期 2010-2-23 接受日期

摘要 在椭圆曲线二进制域上，Montgomery算法利用在计算kP过程中只需计算x坐标，在最后才恢复y坐标的特性，使该算法的计算量更少。在此基础上提出基于Montgomery的分段并行标量乘算法来更进一步提高算法的效率，经分析，将整数标量分两段并行计算，算法效率可提高约25%，将其分三段时其效率可提高约37%。通过编程实现验证了新算法的效率确实有明显提高，新算法对椭圆曲线标量乘快速实现有实际意义。

关键词 椭圆曲线 标量乘 Montgomery方法

分类号 TP309.7

Subsection simultaneous fast scalar multiplication algorithm based on Montgomery algorithm

ZHAO Geng[1，2]，PENG Cheng-pei[1，2]，LI Xiao-dong[1]，ZHANG Dong[1，2]

1.Beijing Electronic Science and Technology Institute，Beijing 100070，China
2.College of Communication Engineering，Xidian University，Xi’an 710071，China

Abstract

In the elliptic curve binary field，it needs less computation amount for that the Montgomery algorithm only computes the x coordinate in the whole course and gets the y coordinate in the last step.A new computational algorithm based on the Montgomery subsection method is proposed to enhance the efficiency further for computer kP，the computation amount decreases 25% for the new algorithm of two subsection and 37% for the new algorithm of three subsection compared with the original algorithm.The efficiency of the new algorithm is proved to be improved by the program implementation.The new algorithm possesses good performance on elliptic curve scalar multiplication.

Key words elliptic curve scalar multiplication Montgomery algorithm

DOI: 10.3778/j.issn.1002-8331.2010.06.032

通讯作者 赵 耿 chengpei0232@163.com