北京航空航天大学学报 » 2011, Vol. 37 » Issue (11) :1451-1455 DOI:

基于预计算和周期性的ECC标量乘法算法

张晓强[1], 朱贵良[2], 王卫苹[2], 王蒙蒙[2]*

1. 北京航空航天大学 软件开发环境国家重点实验室, 北京 100191;
2. 华北水利水电学院 信息工程学院, 郑州 450011

Scalar multiplication algorithm of ECC based on precomputation and periodicity

Zhang Xiaoqiang[1], Zhu Guiliang[2], Wang Weiping[2], Wang Mengmeng[2]*

1. State Key Lab of Software Development Environment, Beijing University of Aeronautics and Astronautics, Beijing 100191, China;
2. Department of Information Engineering, North China University of Water Conservancy and Electric Power, Zhengzhou 450011, China

摘要 在研究二进制、带符号的二进制(NAF,Non-Adjacent Form)等常见标量乘法算法的基础上,结合椭圆曲线基点的周期特性和预计算倍点序列方式,提出了一种新的标量乘法算法,并给出了新算法的详细步骤.点的周期性和系数决定了直接进行标量乘法运算还是转化为求其逆元,预计算倍点序列方式避免了椭圆曲线密码体制(ECC,Elliptic Curve Cryptosystem)加解密过程中大量的重复运算.为验证算法的正确性,采用密钥长度为192 bit椭圆曲线,给出了一个具体实例.实例结果和算法分析表明:与二进制和NAF算法相比,新算法虽占用了一些存储空间,但省去了倍点运算的时间开销,同时减少了点加的运算次数,极大地提高了标量乘法运算的效率.该算法的提出对完善ECC理论和加快ECC在实际中的应用具有重要意义.

关键词: 椭圆曲线密码体制 二进制算法 带符号的二进制算法 标量乘法 预计算 周期性

Abstract: Based on the binary method, non-adjacent form (NAF) method, etc., a new scalar multiplication algorithm was proposed, which uses the periodicity of based point and the precomputation mean. Meanwhile, the steps of new algorithm were given. The periodicity of based point and the coefficient of scalar multiplication determine performing the operation of scalar multiplication directly or computing its inverse element. The precomputation mean can void a quantity of repeat computation during the encryption and decryption processes of elliptic curve cryptosystem (ECC). To verify the correctness of new algorithm, a concrete experiment was offered with an elliptic curve, whose key length is 192 bit. The experimental results and algorithm analyses show that comparing with binary and NAF methods, although the new algorithm requires a little extra space to store precomputed points, it does not need the operation of point doublings and reduces the operation times of point addition. Therefore, the new algorithm can improve the efficiency of scalar multiplication sharply. The research achievement is significant for completing the theory of ECC and accelerating its application in practice.

Keywords: elliptic curve cryptosystem(ECC) binary method non-adjacent form(NAF) method scalar multiplication precomputation periodicity

Received 2010-07-02;

About author: 张晓强(1983-),男,河南内黄人,博士生,grayqiang@163.com.

引用本文:

张晓强, 朱贵良, 王卫苹, 王蒙蒙.基于预计算和周期性的ECC标量乘法算法[J] 北京航空航天大学学报, 2011,V37(11): 1451-1455

Zhang Xiaoqiang, Zhu Guiliang, Wang Weiping, Wang Mengmeng.Scalar multiplication algorithm of ECC based on precomputation and periodicity[J] JOURNAL OF BEIJING UNIVERSITY OF AERONAUTICS AND A, 2011,V37(11): 1451-1455

链接本文:

http://bhxb.buaa.edu.cn//CN/ 或 http://bhxb.buaa.edu.cn//CN/Y2011/V37/I11/1451