计算机工程与应用 2009 45 (22): 71-72 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

方幂模快速计算的二进制分组查表法

董付国[1]，厉玉蓉[1，2]，杜 萍[1]

1.山东工商学院 计算机科学与技术学院，山东 烟台 264005
2.山东大学 计算机科学与技术学院，济南 250100

收稿日期 2008-10-7 修回日期 2008-12-22 网络版发布日期 接受日期

摘要 在方幂模的二进制快速算法基础上，进一步改写方幂模计算表达式，设计了一种基于查表法的二进制快速算法。算法将指数的二进制形式进行分组，提前计算并记忆一个二进制分组中首位为1其他位任意变化的所有情况下的方幂模结果，然后遍历指数的二进制形式，按照算法规则直接平方或连续多次平方后与事先记忆的值相乘，已经记忆的值不需要重复计算，从而减少了大量的乘法运算。算法分析和实验结果证明，基于查表法的方幂模二进制快速算法比二进制算法减少了乘法次数，尤其指数二进制形式中有大量1连续出现或相对连续出现（同一分组内有两位以上为1）的情况下算法效率比二进制算法有大幅度提高。

关键词 RSA算法 方幂模 二进制算法 二进制分组查表法

分类号

Binary partition table searching method for fast computation of modular exponentiation

DONG Fu-guo[1]，LI Yu-rong [1，2]，DU Ping[1]

1.School of Computer Science and Technology，Shandong Institute of Business and Technology，Yantai，Shandong 264005，China
2.School of Computer Science and Technology，Shandong University，Jinan 250100，China

Abstract

This paper studies binary algorithm of modular exponentiation，modifies the computing formula，and designs a novel fast algorithm of modular exponentiation based on binary partition table searching method.This algorithm divides the binary of exponent into many blocks，computes and stores modular exponentiation values of all cases of a binary block，whose first bit is 1 and other bits vary freely.Then traverses all binary bits from the most right to the most left，computes the square or square and product of according value stored beforehand，according to algorithm rules.Because the stored value need not compute again，the times of product can be reduced a lot.Algorithm analysis and experiment results show that this algorithm is more efficient compared to binary algorithm of modular exponentiation，especially when a lot of 1s appear continuously，and can be divided into the same block.

Key words RSA algorithm modular exponentiation binary algorithm binary partition table search algorithm

DOI: 10.3778/j.issn.1002-8331.2009.22.024

通讯作者 董付国 dongfuguo2005@126.com