计算机工程与应用 2007 43 (20): 52-55 ISSN: 1002-8331 CN: 11-2127/TP

学术探讨

Montgomery模乘算法的改进及其应用

王红霞[1]，王金荣[2,3]，赵宪生[1]

1.成都理工大学 信息工程学院，成都610059
2.杭州师范学院 信息工程学院，杭州 310018
3.浙江大学 计算机科学与技术学院，杭州 310027

收稿日期 修回日期 网络版发布日期 2007-6-29 接受日期

摘要 Montgomery算法是目前最适合于通用处理器软件实现的大整数模乘算法。1996年，Koc总结了该算法的五种实现方法：SOS、CIOS、FIOS、FIPS和CIHS，并指出CIOS方法综合性能较优。首先深入分析了FIOS实现方法，并通过消除进位传递和减少循环控制等手段，提出了一种改进方法IFIOS。然后将该方法应用于模幂计算，给出了基于滑动窗口技术的Montgomery模幂算法。最后理论分析和实验结果表明，该改进将FIOS的执行速度提高了约54%，与目前常用的CIOS方法相比，亦有较大的优势。

关键词 RSA DSA Montgomery模乘算法

分类号

Improved montgomery multiplication algorithm and its application

WANG Hong-xia[1]，Wang Jin-rong[2,3]，ZHAO Xian-sheng[1]

1.College of Information Engineering，Chengdu University of Technology，Chengdu 610059，China
2.College of Information Engineering，Hangzhou Teacher’s College，Hangzhou 310018，China
3.College of Computer Science，Zhejiang University，Hangzhou 310027，China

Abstract

Montgomery multiplication algorithm is best suited for fast software implementation on standard CPU architectures.In 1996，Koc has summarized its five implementations，such as SOS，CIOS，FIOS，FIPS，CIHS，and points out that the CIOS has the most efficient of all methods.Firstly，this article analyzes the FIOS method in-depth and provides an improved method of FIOS by eliminating carry propagation and decreasing the number of iteration.Second，it also puts this new method to compute modular exponentiation and gives a Montgomery modular exponentiation algorithm based on slidsing window techniques.According to this analysis and experimentation，the new method improves in its efficiency with about 54% by comparison with FIOS，and it also exceeds the CIOS which is common used method of Montgomery multiplication algorithm.

Key words RSA DSA Montgomery multiplication algorithm

DOI:

通讯作者 王红霞