计算机应用 2006 26 (12): 2928-2930 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

# RSA密码算法的一种新的快速软件实现方法

贺毅朝[1]; 张建勋[1]; 王彦祺[1]; 田俊峰[2,3]

石家庄经济学院信息工程系[1]

河北大学 数学与计算机学院[2]

收稿日期 2006-6-20 修回日期 网络版发布日期 2006-12-25 接受日期

摘要 在介绍标准RSA密码系统的基础上，利用计算近似最短加法链算法给出了软件实现模幂运算的一种改进方法；基于求解孙子定理的混合基数计算算法(MRC)改进了RSA的解密方法；最后，结合快速有效的素数测试方法提出了一种能够快速软件实现RSA密码算法的新方法，并分析比较了各相关算法的计算效率。实验结果表明：利用该方法实现的RSA密码软件系统，可使加、解密运算速度平均提高6～10倍。

Abstract Based on introducing standard RSA crytsystem, we advanced an improved method of the software implementation of module power operation using approximate algorithm of calculation shortest addition chains, and improved decryption method of RSA on the basement of Mixed-Radix Conversion (MRC) which is to solve Chinese Remainder Theorem (CRT). Finally, combined with rapid effective prime testing method, a new algorithm that can rapid software implementation RSA cryptsystem was proposed, and it has also been analyzed and compared to other related algorithms. Experimental results show that operation velocity of encryption and decryption operation can be increased 6 to 10 times on average by using the new method.

关键词 PKC算法 RSA算法 最短加法链 孙子定理 混合基数计算算法

Key words Public Key Cryptosystem (PKC) algorithm;RSA algorithm;shortest addition chains;Chinese remainder theorem;Mixed Radix Conversion (MRC)

分类号

**DOI:**

通讯作者:
贺毅朝 heyichao@sjzue.edu.cn

作者个人主页: 贺毅朝 张建勋 王彦祺 田俊峰