Montgomery 算法在 RSA 中的应用及其优化

王琴琴，陈相宁

（南京大学 电子科学与工程系，江苏 南京 210093）

摘　要：Montgomery算法作为一种快速模乘算法，常被应用于RSA、ElGamal等公钥密码算法的基本运算。对RSA和Montgomery算法进行简要的介绍和分析，并阐述了普通的Montgomery算法在RSA中的应用的思路和步骤。最常用的传统算法选取参数 r 为2的幂，基数为2，通过对普通算法的思路和步骤的分析，讨论改变其中参数 r 和基数的选择来减少乘方的模乘法数，并同时应用Dussé快速算法，从而达到大大提高运算速度的目的。

关键词：RSA；Montgomery算法；模乘；Dussé快速算法

中图分类号：TP301.6　　**文献标识码**：A　　**文章编号**：1673－629X(2007)06－0145－02

Optimization and Application of Montgomery Algorithm in RSA

WANG Qin-qin, CHEN Xiang-ning

(Electronics Science and Engineering College, Nanjing Univ., Nanjing 210093, China)

Abstract: *Montgomery algorithm is a fast modular multiplication algorithm and is widely used in the base operation of public－key cryptography algorithms such as RSA and ElGamal. Firstly, the algorithm of RSA and Montgomery are simply introduced and analyzed. Method and calcutive steps of normal application of Montgomery algorithm in RSA are expatiated also. Algorithm in most conmmon use chooses parameter r to power of 2 and the base to 2. Via analyzing the method and calcutive steps of normal algorithm, discusses changing the numerical value of parameter r and the base and use the fast algorithm of Dussé in the meantime, to advance the calcutive velocity a lot.*

Key words: RSA; *montgomery algorithm*; *modular multiplication*; *fast algorithm of Dussé*

1　RSA 算法简述

随着信息技术的飞速发展，网络通信中的身份认证和信息安全传输问题正逐渐受到人们的关注和重视。数字签名、验证和密钥交换都离不开RSA、ElGamal等公钥密码体制算法。RSA算法是第一个既能用于数据加密也能用于数字签名的算法。它易于理解和操作，也很流行。算法的名字以发明者的名字命名：Ron Rivest, Adi Shamir 和 Leonard Adleman。它经历了各种攻击，至今未被完全攻破。

RSA的最重要特色在于双密钥，它们有特殊的数学形式。RSA的一对密钥有三个基本参数：模 n，公钥 b 和私钥 a[1]。n 和 b 是公开的，发送信息方用私钥 a 加密消息，接受方用公钥 b 能得到解密后的信息，从而确定发送信息方的身份，这就构成了签名机制。对方用公钥将要发送的信息加密，只有拥有私钥的一方才能将信息解密。

设消息数为 M，C 为加密后的密文，则 $M^b \bmod n = C$，$C^a \bmod n = M$[2]。

在RSA中最耗时的计算工作就是加解密时的大数模乘运算。Montgomery算法作为一种快速且有效的大数模乘算法，得到了广泛的研究和应用。

最常用的传统算法选取参数 r 为2的幂。文中主要讨论通过选择基数来减少乘方的模乘法数，并同时应用Dussé快速算法，从而达到提高运算速度的目的。

2　Montgomery 算法分析

2.1　Montgomery 约化描述及分析

P. Montgomery 于1985年在《MONT》中发表了Montgomery模约化方法，用于 $t \cdot r^{-1} \bmod n$ 的快速计算[3]。

【定理】　设 n 和 r 为互素的整数，r^{-1} 为 r 模 n 的乘法逆，n^{-1} 为 n 模 r 的乘法逆（即满足 $r \cdot r^{-1} \bmod n = 1$，$n \cdot n^{-1} \bmod r = 1$），定义 $n' = -n^{-1} \bmod r$，$m = t \cdot n' \bmod r$。对整数 t 成立：$(t + m \cdot n)/r = t \cdot r^{-1} \bmod n$。

这一计算模 n 约化的原理称为Montgomery约化。

收稿日期：2006－09－21

作者简介：王琴琴（1984－），女，湖南祁东人，硕士研究生，研究方向为网络信息安全研究；陈相宁，副教授，主要从事网络信息安全研究与教学。

通过选择 r 为基数 N 的幂，即 N^s，可以简单地把 $t + m \cdot n$ 右移 s 比特从而得到 $t + m \cdot n$ 模 r 的约化，这个计算要比运算复杂的带余除法要简单得多，这是 Montgomery 的意义所在。

2.2 Montgomery 乘法

Montgomery 乘法计算 $a \cdot b \bmod n$，是对 Montgomery 约化的应用。应用 Montgomery 约化时，应该选择合适的 $r = N^s > 0, N^{s-1} \leqslant n < N^s$，将模 n 的计算转换到完全剩余系，这是预处理的理论依据[4]。

应用 Montgomery 约化计算 $a \cdot b \bmod n$，步骤如下：

(1) $a' \leftarrow a \cdot r \bmod n, b' \leftarrow b \cdot r \bmod n$；

(2) $t \leftarrow a' \cdot b'$；

(3) 利用 Montgomery 约化计算 $t' = t \cdot r^{-1} \bmod n$；

(4) $u \leftarrow t' \cdot r^{-1} \bmod n$；

(5) 若 $u \geqslant n$，输出 $u - n$，否则输出 u。

可以看出，Montgomery 乘法就是将经过预处理后的变量的乘积代入 Montgomery 约化 $t \cdot r^{-1} \bmod n$ 的变量 t 中。

在上面的步骤中，步骤(1)的预处理的计算是非常费时的，甚至比直接计算模乘还增加了计算费用，因此用 Montgomery 约化计算单个乘积不值得。但在计算模乘方时，耗时的预计算只出现了一次，总的降低了运算消耗。

3 Montgomery 算法在 RSA 中的应用及其改进

3.1 普通算法

应用 Montgomery 算法计算模乘方时，以加密过程计算 $M^b \bmod n$ 为例，通常取基数为 2[5]，将 b 以二进制表示 $b = \sum_{i=0}^{l} b_i \cdot 2^i$，需要 $l + 1$ 次乘法就能完成运算，计算步骤如下：

(1) $M' \leftarrow M \cdot r \bmod n, r' \rightarrow r \bmod n$；

(2) $i \leftarrow l$；

(3) 用 Montgomery 算法计算 $r' = r' \cdot r' \cdot r^{-1} \bmod n$；

(4) 若 $b_i \neq 0$，则用 Montgomery 算法计算 $r' = M' \cdot r' \cdot r^{-1} \bmod n$；

(5) $i \leftarrow i - 1$，若 $i \leqslant 0$ 转到 (3)；

(6) 做后期处理，用 Montgomery 算法计算 $u = r' \cdot r^{-1} \bmod n$；

(7) 若 $u \geqslant n$，输出 $u - n$，否则输出 u。

很明显，所需的乘法的次数依赖指数 6 的位数，因此依赖基数 N 的选择。考虑选择 $N > 2$，乘方的运算次数可以相应减少。依照这样的推论，N 取得越大越好，但事实上，改变基数要增加预运算。因此，N 需要合理选择。

3.2 改进算法

预计算所需内存大小取决于基数的选择[6]。基数为 N，则需预计算 $M^2 \bmod n, M^3 \bmod n, \cdots, M^{N-1} \bmod n$，并将结果存储，进行了 $N - 2$ 次乘法，这需要较大的内存。若改进取 $N = 2^k$，则仅需预计算 $M^3 \bmod n$，$M^5 \bmod n, \cdots, M^{2^k-1} \bmod n$ 并进行存储，只进行了 $N/2$ 次乘法，节省了一半内存。

同时，在应用 Montgomery 算法时，考虑采用 Dussé 快速算法[7]：用 $n'_0 = n' \bmod N$ 代替 n'，$m = \sum_{i=0}^{s-1} m_i N^i$，$r = N^s$（其中 $N = 2^k$），Montgomery 算法改进为：

(1) $n'_0 \leftarrow n' \bmod N$；

(2) $i \leftarrow 0$；

(3) $m_i = t_i \cdot n_0' \bmod r$；

(4) $t = t + m_i n N^i$；

(5) $i \leftarrow i + 1$，若 $i \leqslant s - 1$，则返回步骤 (3)；

(6) $u = t/r$；

(7) 若 $u \geqslant n$，输出 $u - n$，否则输出 u。

将 b 以 N 进制表示为 $b = \sum_{i=0}^{q} b_i \cdot N^i$（其中 $N = 2^k$），优化改进后计算 $M^b \bmod n$ 步骤如下：

(1) $M' \leftarrow M \cdot r \bmod n, r' \leftarrow r \bmod n$；

(2) $i \leftarrow q$；

(3) 用 Dussé 改进算法计算 $r' = r'^N \cdot r^{-1} \bmod n$；

(4) 若 $b_i \neq 0$，则用 Dussé 改进算法计算 $r' = M'^{b_i} \cdot r' \cdot r^{-1} \bmod n$；

(5) $i \leftarrow i - 1$，若 $i \leqslant 0$，转到 (3)；

(6) 若 $u \geqslant n$，输出 $u - n$，否则输出 u。

在改进过程中，实现将数字以 N 进制表示的算法毫无困难[8]，鉴于篇幅不再详述。

4 结束语

Montgomery 算法作为一种高效的模乘算法，得到了广泛的应用。文章系统地分析了该算法的原理及通过选择基数来减少乘方的模乘法数，同时应用 Dussé 快速算法，利用这些改进可以使算法性能得到大幅提升。

参考文献：

[1] Lu Jun - ming, Lin Zheng - hui. A new RSA cryptosystem

（下转第 150 页）

用的原理、易用性、准确性等等。在作出决策时，扫描工具的可用性是最重要也是最基本的，但是扫描过程的可控性和扫描结果分析的准确性同样不容忽视。常见的扫描工具如表 1 所示。

表 1 常见扫描工具

工具类型	名称	平台	特点介绍
ping 扫描	Hping2	Unix/Linux	能自定义发送 ICMP/UDP/TCP 包到目标地址并且显示响应信息
	icmpush& icmpquery	Unix/Linux	可以完全定制 ICMP 包的结构以及种类
	Pinger	Windows	速度很快，能同时发送多个 ICMP ECHO REQUEST 并且显示响应信息
端口扫描	Fport	Windows	能扫描目标主机上所有打开的 TCP/UDP 端口，并显示端口所属的进程
	SuperScan	Windows	能进行 TCP 全连接扫描、ping 扫描，并且可以解析域名
OS 探测	XProbe2	Unix/Linux	基于 ICMP 协议，通过与配套的签名数据库进行模糊匹配来确定 OS 类型
	THC－Amap	Unix/Linux	通过分析端口响应的应用程序指纹数据来确定应用程序及服务
弱点扫描	Whisker	Unix/Linux	能扫描出大量的 HTTP 服务器弱点，并且可以扩充其程序库，创建自己的 HTTP 扫描器
	Nessus	Unix/Linux	应用了多线程和基于插件的技术，速度快，并可以对扫描出的弱点提出解决方案
	GFI LANguard	Windows	对目标主机可以作出较完整的安全测试，并生成可自定义的安全报告
防火墙规则探测	Firewalk	Unix/Linux	分析 IP 包的响应，从而测定网关的 ACL 并且绘制出网络拓扑图

3 结 论

一般而言，扫描者并不是孤立地、单纯地使用某种扫描技术，而是综合地应用一系列的扫描方法。而如果大范围地进行某种扫描，反复高速地发出特定的连接请求，所造成的结果就是目标主机上存在大量等待的 TCP 连接，目标网络中充斥着许多无用的数据包，最终网络拥塞，主机无法正常使用，这正是 DoS 的表现。因此若要防范网络扫描以及可能的 DoS 攻击，要做到以下三点：

(1) 在防火墙及过滤设备上采用严格的过滤规则，禁止扫描的数据包进入系统。

(2) 主机系统除了必要的网络服务外，禁止其它的网络应用程序。

(3) 对于只对内开放的网络服务，更改其提供服务的端口[7]。

此外，网络扫描时发送的数据或多或少都会含有扫描者自身相关信息，从而也可以抓取扫描时的数据包，对扫描者进行反向追踪，这也是一个值得研究的方向。

参考文献：

[1] Stevens W R. TCP/IP 详解卷一：协议[M]. 北京：机械工业出版社，2000：50－60.

[2] Afkin O. Network Scanning Techniques－Understanding how it is done [EB/OL]. 1999－11－01[2005－06－11]. http://www.sys－security.com.

[3] Fyodor. The Art of Port Scanning[EB/OL]. 1997－09－06 [2005－11－12]. http://www.insecure.org/nmap/nmap_doc.html.

[4] 王 灏，王换招. 端口扫描与反扫描技术[J]. 微机发展，2001，11(5)：60－63.

[5] Fyodor. Remote OS detection via TCP/IP stack Fingerprinting[EB/OL]. 1998－10－18[2006－02－01]. http://insecure.org/nmap/nmap－fingerprinting－article.txt.

[6] 洪 宏，张玉清，胡予濮，等. 网络安全扫描技术研究[J]. 计算机工程，2004，30(10)：54－56.

[7] 丁常福，方 敏，徐 亮. 端口扫描技术及防御分析[J]. 微机发展，2003，13(6)：7－12.

(上接第 146 页)

hardware implementation based on Montgomery's algorithm [J]. Journal of Shanghai Jiaotong University，2002，E－7(1)：46－49.

[2] Rivest R L，Shamir A，Adleman L M. A Method for Obtaining Digital Signatures and Public－key Cryptosystems[J]. Communication of the ACM，1978，21(2)：120－126.

[3] Montgomery P L. Modular multiplication without trial division [J]. Mathematics of Computation，1985，44(170)：519－521.

[4] 王金荣，陈 勤，丁 宏. 大数模乘算法的分析与研究[J]. 计算机工程与应用，2004，40(24)：70－72.

[5] Welschenbach M. Kryptographie in C and C＋＋ weite, überarbeitete und erweiterte Auflage[M]. 北京：电子工业出版社，2003：54－80.

[6] 孔凡玉，于 佳，李大兴. 一种改进的 Montgomery 模乘快速算法[J]. 计算机工程，2005(8)：1－3.

[7] Dusse S R，Jr Kaliski B S. A Cryptographic Library for the Motorola DSP56000[C]// Advances in Cryptology－ EUROCRYPT 90. [s.l.]：Springer－Verlag，1990：230－244.

[8] Walter C D. Montgomery Exponentiation Needs No Final Subtractions[J]. Electronic Letters，1999，35(21)：1831－1832.