Journal of Computer Applications
计算机应用,2013,33(5):1374 - 1377
ISSN 1001-9081
CODEN JYIIDU
2013-05-01
http://www.joca.cn

文章编号:1001 - 9081(2013)05 - 1374 - 04
doi:10.3724/SP.J.1087.2013.01374

四素数 RSA 数字签名算法的研究与实现

肖振久[1,2],胡　驰[1*],陈　虹[1]
(1.辽宁工程技术大学 软件学院,辽宁 葫芦岛 125105;　2.中国传媒大学 计算机学院,北京 100024)
(*通信作者电子邮箱 hcshrhh001@163.com)

摘　要:RSA 算法中模数和运算效率之间一直存在矛盾,目前一些认证机构已采用模数为 2 048 bit 的 RSA 签名方法,这必然会影响签名效率。针对这一问题,提出四素数 CRT-RSA 签名算法,并使用安全杂凑函数 SHA512 来生成消息摘要,采用中国剩余定理结合 Montgomery 模乘来优化大数的模幂运算。通过安全性分析和仿真实验表明,该签名算法能抵抗一些常见攻击,并且在签名效率方面具有一定优势。

关键词:RSA 密码算法;四素数;中国剩余定理;蒙哥马利算法;杂凑函数;数字签名
中图分类号:TP309.7　　**文献标志码**:A

Research and implementation of four-prime RSA digital signature algorithm

XIAO Zhenjiu[1,2], HU Chi[1*], CHEN Hong[1]
(1. *College of Software, Liaoning Technical University, Huludao Liaoning* 125105, *China*;
2. *School of Computer, Communication University of China, Beijing* 100024, *China*)

Abstract: In order to improve the operation efficiency of big module RSA (Rivest-Shamir-Adleman) signature algorithm, four prime Chinese Remainder Theorem (CRT)-RSA digital signature was suggested in this paper. The Hash function SHA512 was used to produce message digest, and CRT combining with Montgomery algorithm was applied to optimize large number modular exponentiation. The security analysis and experiment show that the new algorithm can resist some common attacks, and it has some advantages in signature efficiency.

Key words: RSA encryption algorithm; four prime; Chinese remainder theorem; Montgomery algorithm; Hash function; digital signature

0　引言

随着网络和通信技术的发展,在给人们带来益处的同时,也带来了安全隐患。由于传输过程中存在数据被通信双方之外的第三方伪造或篡改的可能,通信双方无法验证数据来源,就很有可能出现一方抵赖的情况,此时就要求保证传输信息的不可否认性。数字签名就是通信双方在网上交换信息时,基于公钥密码体制来防止伪造和欺骗的一种身份认证技术。在所有公钥密码体制中,应用最为广泛的是 RSA(Rivest-Shamir-Adleman)密码算法[1],它的特点是安全性高,易于实现,即可用来加密数据,又能用于身份认证。因此,RSA 签名[2]是一种最常用的数字签名方法。

然而,RSA 算法中的大数的模幂运算比较费时,这一直是制约着 RSA 发展的瓶颈。早期,人们建议使用较小的加密指数或解密指数以加快加密或解密(签名)等基本运算,但是,1990 年 Wiener[3]提出当私钥 d 小于模数 $N^{1/4}$ 时,RSA 密码系统是不安全的,其分析方法本质是利用了连分数中 Legendre 定理;随后 1999 年,Boneh 和 Durfee[4]把弱密钥 d 的上界提高到 $d < N^{0.292}$。因此,出于安全性考虑,目前 RSA 密码系统的模数为 1 024 bit 到 2 048 bit,如此庞大的模数,其运算效率必然受到影响。针对这一问题,很多学者提出了不同的优化算法,比如基于乘同余对称特性和指数 2^k 次方组合优化算法、加法链方法、滑动窗口法和模重复平方算法等[5],这些都是从运算操作的角度去优化;国外还提出了许多从结构上改进的算法,比如 Batch RSA、Mprime RSA、Mpower RSA 和 Rebalanced RSA[6]。这些方法都在一定程度上提高了算法运算效率,其中效果比较显著的是利用中国剩余定理(Chinese Remainder Theorem,CRT)进行解密或签名[7]。本文把融入中国剩余定理的 RSA 算法叫作 CRT-RSA(Chinese Remainder Theorem-Rivest Shamir Adleman)算法。已证明,若不考虑中国剩余定理的计算代价,双素数 CRT-RSA 在运算效率上是传统 RSA 算法的 4 倍;若考虑中国剩余定理的计算代价,双素数 CRT-RSA 在运算速度上分别是原算法的 3.32 倍(模为 1 024 比特)和 3.47 倍(模为 2 048 比特)[8]。这个速度虽令人满意,却存在安全隐患,文献[9]指出传统双素数 CRT-RSA 签名算法容易遭受出错攻击,攻击者能够利用错误的签名来分解模数 N。

本文针对目前一些认证机构采用模数为 2 048 bit 的 RSA 密码系统,比如电子商务中的安全电子交易协议(Secure Electronic Transaction,SET)协议采用的模数为 2 048 bit RSA 签名算法,从安全性和运算效率方面考虑,提出一种四素数 CRT-RSA 数字签名算法。

1　四素数 RSA 算法基本原理

文献[6]中提到一种 Mprime 多素数 RSA 密码算法,本文借鉴这种思想,在传统双素数 RSA 密码算法基础上,把素数

收稿日期:2012-11-15;**修回日期**:2012-12-18。
基金项目:国家自然科学基金资助项目(61103199);北京市自然科学基金资助项目(4112052)。
作者简介:肖振久(1968 -),男,内蒙古宁城人,副教授,博士,主要研究方向:网络与信息安全、数字版权管理;　胡驰(1988 -),男,湖北武汉人,硕士研究生,主要研究方向:数据加密、数字签名;　陈虹(1967 -),女,辽宁阜新人,副教授,硕士,主要研究方向:网络安全。

个数取为 4,算法依然成立,其描述如下:

1)随机选取 4 个不同的大素数 p,q,r 和 s,计算 $n = pqrs$, $\varphi(n) = (p-1)(q-1)(r-1)(s-1)$。

2)取加密密钥 $e = 65537$,计算出私钥 d,满足 $de \equiv 1 \bmod \varphi(n)$。

3)加密解密过程与传统算法一样,仍为:

加密算法　$c = E(m) \equiv m^e \bmod n$

解密算法　$m = D(c) \equiv c^d \bmod n$

下面,本文从数论的角度来证明算法的正确性。

证明　假设明文为 m,密文 c,密钥 (d,n),公钥 (e,n)。由加密解密过程有:$D(c) \equiv c^d \bmod n \equiv (m^e)^d \bmod n \equiv m^{ed} \bmod n$,又因为 $de \equiv 1 \bmod \varphi(n)$,所以 $de \equiv 1 + k\varphi(n)$,其中 k 为正整数,代入上式得 $D(c) \equiv m^{1+\varphi(n)} \bmod n$,若 $\gcd(m,n) = 1$,根据欧拉定理有:$m^{\varphi(n)} \equiv 1 \bmod n$,故有 $m^{1+\varphi(n)} \equiv m \bmod n$;若 $\gcd(m,n) \neq 1$,由于 $n = pqrs$,故 (m,n) 中必含 p,q,r,s 之一,或者 pq,pr,ps,qr 之一,或者 pqr,prs,qrs 之一。由于这几种情况类似,这里只给出 $\gcd(m,n)$ 包含 p,q,r,s 之一的证明过程:若 $\gcd(m,n) = p, m = cp, 1 \leqslant c < qrs$,由欧拉定理得:$m^{\varphi(q)} \equiv 1 \bmod q, m^{\varphi(r)} \equiv 1 \bmod r, m^{\varphi(s)} \equiv 1 \bmod s$,因此,

对任意 k 恒有 $m^{k(q-1)} \equiv 1 \bmod q$,

$m^{k(q-1)(r-1)(s-1)(p-1)} \equiv 1 \bmod q$,就有

$m^{k(q-1)(r-1)(s-1)(p-1)} \equiv 1 + hq$,得出

$m^{k\varphi(n)} \equiv 1 + hq$,因为 $m = cp$,因此得出 $m^{k\varphi(n)+1} \equiv m + cphq$,已知 p,q,r,s 都是素数,故 $\gcd(p,qrs) = 1, \gcd(m, qrs) = 1$,推出 $m^{\varphi(qrs)} \equiv 1 \bmod qrs$,对任意 k,总有

$m^{k(q-1)(r-1)(s-1)} \equiv 1 \bmod qrs$,所以

$m^{k(q-1)(r-1)(s-1)(p-1)} \equiv 1 \bmod qrs$,即

$m^{k\varphi(n)} \equiv 1 + hqrs$,又因为 $m = cp$,所以

$m^{k\varphi(n)+1} \equiv m + chpqrs$,这就证明了

$m^{k\varphi(n)+1} \equiv m \bmod n$,其他同理可证均成立。

2　四素数 RSA 算法在数字签名中的应用

首先简单介绍一下杂凑函数,它是指将任意长度的消息映射成某一固定长度消息的一种函数,一般用于消息完整性检测和认证。它是一种单项散列函数,也就是说给定一个消息 M,用杂凑函数 H,生成消息摘要 $D = H(M)$,这个计算很容易,但反推 M 却很难。把杂凑函数运用到数字签名中,一方面是为了提高签名速度,因为,如果直接对消息签名,当消息很长时需要对其分组,再对每组消息用 RSA 签名,这样签名效率相当低;另一方面,可以不泄漏要签名的消息,这适用于一些特殊的签名场景[10]。本文中用的是一种安全性非常高的杂凑函数 SHA512[11](Secure Hash Algorithm),再结合四素数 RSA 算法,其签名过程如下:

1)用户 A 将要发送的消息 M 通过杂凑函数 H,产生消息摘要 $D = H(M)$;

2)用户 A 用私钥 d 对消息摘要进行签名 $S = D^d \bmod n$;

3)用户 A 将消息 M 和签名 S 一同发送给用户 B;

4)用户 B 接受到消息和签名后用 A 的公钥解密签名 S 得到 D,再用杂凑函数计算一次消息摘要 D',判断 D' 是否等于 D。若相同,则说明消息确实来自于 A,并且在传输途中没有被篡改;否则,很有可能消息不是来自于 A。

运用以上的签名方法,如果用户 A 想否认曾经发送消息 M 给用户 B,用户 B 只需把 A 的公钥和签名 S 一并出示给公证方,通过正确的计算方法就能证实用户 A 确实发送了消息 M;如果用户 B 伪造了一个消息 M',由于他不知道用户 A 的私钥,也就无法出示正确的签名给公证方。这样一来,通信双方都必须真实地反映通信情况,有效地防止了一方抵赖的情况发生。

3　签名过程优化

3.1　Montgomery 模指数算法

Montgomery 模指数算法是 Montgomery 模乘结合指数算法来求大数模幂运算的一种方法[12],Montgomery 模乘是一种将除法运算改为移位运算从而简化两数模乘的算法。这里,本文运用文献[12]中一种改进的 Montgomery 模乘——CIOS(Coarsely Integrated Operand Scanning)模乘法。设整数 $m = (m_{n-1}\cdots m_1 m_0)_b$($b$ 为进制数),$x = (x_{n-1}\cdots x_1 x_0)_b$, $y = (y_{n-1}\cdots y_1 y_0)_b$, $\gcd(m,b) = 1, R = b^n$, $m' = -m^{-1} \bmod b$(m^{-1} 为 m 模 b 的乘法逆元),其算法描述如下:

1)$A = 0$;

2)对 i 从 0 到 $n-1$ 执行:$A = A + x_i y, u_i = a_0 m \bmod b$, $A = (A + u_i m)/b$;

3)如果 $A \geqslant m$,则 $A = A - m$;

4)返回 $A = xyR^{-1} \bmod m$。

再定义函数 $mont(u,v)$ 为 $uvR^{-1} \bmod m$,用上述 CIOS 算法进行计算,然后再结合指数算法,便可得到 $x^e \bmod m$ 的计算方法,其中 x 为整数,$1 \leqslant x < m, e = (e_t\cdots e_1 e_0)_2, e_t = 1$,算法描述如下:

1)$x' = mont(x, R^2 \bmod m), A = R \bmod m$;

2)对 i 从 t 到 0 执行:$A = mont(A,A)$,若 $e_i = 1$ 则 $A = mont(A,x')$;

3)$A = mont(A,1)$;

4)返回 $A = x^e \bmod m$。

经分析知,如果仅仅是求模乘运算,Montgomery 模乘并不能有速度上的提高,因为算法在预处理时还是要用到一般的模运算和模逆运算,但如果是模幂运算,其中含有 $(3 \lg e)/2$ 次模乘运算,这些预处理只需一次就能进行多次没有除法的 Montgomery 模乘运算,这将大幅度提高模幂运算的速度。

3.2　中国剩余定理

中国剩余定理又叫孙子定理,是中国古代求解一次同余式组的方法,也是数论中一个重要的定理。令 r 个整数 $m_1, m_2, \cdots, m_r$ 两两互素,$a_1, a_2, \cdots, a_r$ 是任意 r 个整数,则同余方程组 $x \equiv a_i \bmod m_i (1 \leqslant i \leqslant r)$ 的模 $M = m_1 m_2 \cdots m_r$ 有唯一解,其表达式为:

$$x = \sum_{i=1}^{r} a_i M_i y_i \pmod M$$

其中:$M_i = M/m_i$, $y_i M_i \equiv 1 \bmod m_i$, $1 \leqslant i \leqslant r$。

可见,中国剩余定理能够把高位宽大数的模幂运算转换为低位宽相对较小的数的模幂运算。

3.3　中国剩余定理的应用

运用中国剩余定理,对消息摘要 D 的数字签名可转换为以下运算过程:

1)计算 $m_p = D \bmod p$, $m_q = D \bmod q, m_r = D \bmod r$, $m_s = D \bmod s$;

2)计算 $d_p = d \bmod (p-1), d_q = d \bmod (q-1), d_r = d \bmod (r-1)$, $d_s = d \bmod (s-1)$;

3)计算 $M_1 = m_p^{d_p} \bmod p, M_2 = m_q^{d_q} \bmod q, M_3 = m_r^{d_r} \bmod r$, $M_4 = m_s^{d_s} \bmod s$;

4)计算 $S = (M_1 (qrs)^{p-1} + M_2 (prs)^{q-1} + M_3 (pqs)^{r-1} +$

$M_4(pqr)^{s-1})\bmod n$,即得出签名 S。

在上述计算过程中,先把传统的签名算法 $S = D^d \bmod n$ 转换为求解四个同余式:$S \equiv D^d \bmod p$,$S \equiv D^d \bmod q$,$S \equiv D^d \bmod r$ 和 $S \equiv D^d \bmod s$,再利用中国剩余定理进行求解。在求乘法逆元时,本文没有用扩展欧几里得算法,而是运用了费马小定理:对任何不被素数 p 整除的整数 A,恒有 $A^{p-1} \equiv 1 \bmod p$,可得 $A^{-1} \equiv A^{p-2} \bmod p$,巧妙地通过一个多项式运算来代替其中一个逆元的求解,进一步提高了运算效率。

4 安全性分析

目前,对 RSA 签名系统的攻击一般有直接对模数 N 进行分解攻击、RSA 的选择密文攻击以及对签名算法中的杂凑函数进行攻击。出错攻击是一种专门针对利用中国剩余定理进行签名的攻击方法,文献[3]中提到的连分数攻击也是对 CRT-RSA 潜在的威胁。下面,本文分别考察这几种攻击方法对四素数 CRT-RSA 签名算法的攻击情况。

4.1 对模数 N 分解攻击

直接对模数 N 进行分解是 RSA 签名攻击方法中最直接也是最困难的方法。若模数 N 被成功分解,则攻击者可以计算出私钥 d,从而可以冒充私钥持有者对任意的信息进行签名。然而,目前为止在数学上没有学者提出一个在多项式时间内分解大数 N 的有效算法,并且根据研究表明,在 100 万次每秒的计算机上,对 512 bit(二进制)的大数分解需要 8 个月时间,若大数达到 1 024 bit 时,被分解时间对信息保密来说是安全的。当模数达到 2 048 bit 时,可以认为是绝对安全的。

4.2 选择密文攻击

选择密文攻击是攻击者对 RSA 等公钥算法最常用的攻击,其攻击方法可分为明文破译、骗取仲裁签名和伪造合法签名。本文重点讨论后两者。

4.2.1 骗取仲裁签名

在有仲裁情况下,若攻击者有一非法消息 x 想让仲裁 T 签名,则他可任选一数 N,计算 $y \equiv N^e \bmod n$(e 是 T 的公钥),然后计算 $M = yx$ 发送给 T,T 将签名的结果 $M^d \bmod n$ 发送给攻击者,则有:$(M^d \bmod n)N^{-1} \equiv (yx)^d N^{-1} \equiv (x^d y^d N^{-1}) \equiv x^d N N^{-1} \equiv x^d \bmod n$,攻击者成功骗取 T 对 x 的签名。

4.2.2 伪造合法签名

攻击者可利用自己伪造的两个合法消息 x_1 和 x_2 来拼凑出所需要的 $x_3 \equiv (x_1 x_2) \bmod n$。攻击者如果得到用户 U 对 x_1 和 x_2 的签名 $x_1^d \bmod n$ 和 $x_2^d \bmod n$ 就可以计算出 x_3 的签名:$x_3^d \equiv ((x_1^d \bmod n)(x_2^d \bmod n)) \bmod n$。

由于本文的签名算法并不是对消息直接签名,而是运用杂凑函数先对消息进行压缩处理,再对消息摘要进行签名,由杂凑函数的不可逆性和随机性知,当给定一个 D,很难找到一个消息 M,使得 $H(M) = D$,从这个意义上来说,给攻击者造成了极大的难度,以上攻击方法趋于不可行。在实际应用过程中,为了安全起见,应该拒绝对随机的陌生文档签名。

4.3 对杂凑函数攻击

另一种攻击方法则是对签名算法中的杂凑函数进行攻击。攻击者通常利用生日攻击、穷举攻击和密码分析攻击等[13]方法找到杂凑函数的一对或多对“碰撞”,即找到两个不同的消息 M_1 和 M_2,使得 $H(M_1) = H(M_2)$。这样一来,合法用户便能否认自己的签名。

本文采用的杂凑函数是 SHA512,允许输入报文的最大长度是 2^{128} bit,并产生一个 512 bit 的定长报文摘要,攻击者要找出其“碰撞”的时间复杂度为 2^{256},以目前的计算条件来讲是不可能的。根据文献[13]的结论表明,SHA512 的安全性比 MD5、SHA-1 等要高,更能抵抗生日攻击,并能抵御已知密码分析攻击。

4.4 出错攻击

文献[9]指出,用传统双素数 RSA 算法对明文 M 进行签名时,容易遭受出错攻击。签名方用自己的私钥计算 $C = M^d \bmod n$,使用中国剩余定理,C 可通过 $C_p = M^d \bmod p$,$C_q = M^d \bmod q$ 有效计算出来。假设错误发生在 C_p 时,也就是说计算了一个错误的值 $C_p' \neq C_p$,而 C_q 被正确计算出来,C_p' 和 C_q 就联合产生了一个错误的签名 C',这样一来有如下性质:$q = \gcd(C'^e - M \bmod n, n)$。

证明 根据中国剩余定理有 $C' = C_p'(q^{-1} \bmod p)q + C_q(p^{-1} \bmod q)p \pmod n$,所以

$$
\begin{aligned}
(C'^e - M \bmod n) \bmod q &= ((C_p'(q^{-1} \bmod p)q)^e + \cdots + \\
&(C_q(p^{-1} \bmod q)p)^e - M \bmod n) \bmod q = \\
&((C_q(p^{-1} \bmod q))^e - M \bmod n) \bmod q = \\
&(C^e - M) \bmod q = 0
\end{aligned}
$$

而 C' 是一个错误的签名,所以 $(C'^e - M \bmod n) \bmod p \neq 0$,因而性质成立。

由以上证明过程知,在四素数 CRT-RSA 签名过程中,若 C_p 出错,$\gcd(C'^e - M \bmod N, N)$ 求得的是另外三个素数 q,r 和 s 的乘积,并不能求得某一个素因子,也就无法分解模数 N,因此,四素数 CRT-RSA 签名能抵抗出错攻击。

4.5 连分数攻击

4.5.1 连分数

一个连分数可以表示成

$$
q_0 + \cfrac{a_1}{q_1 + \cfrac{a_2}{q_2 + \cfrac{a_3}{\cdots + \cfrac{a_m}{q_m}}}}
$$

它经常被用于有理数或者无理数的逼近,数论中将 $a_1 = 1$ 的情况称为狭义连分数。

定理 1 连分数收敛定理。若 $\frac{b}{a}$ 满足 $\left|\alpha - \frac{a}{b}\right| < \frac{1}{(2b^2)}$,则 $\frac{b}{s}$ 为 α 的连分数展开式的一个收敛因子,即 $\frac{a}{b} = \frac{P_m}{Q_m}$,有 $a = P_m$,$b = Q_m$,其中 $\frac{P_m}{Q_m}$ 为 α 的收敛子序列。

文献[3]中,作者根据定理 1,通过展开一个已知的正有理数 f' 的第 i 级连分数,逼近所求的分数 f 的值,提出了连分数攻击算法。

定理 2 设 f' 是小于 f 的一个近似估算值,有 $f' = f(1 - \delta)$,$\delta \geqslant 0$,当 m 是偶数且展开式 $\langle q_0, q_1, \cdots, q_m - 1\rangle < f' \leqslant \langle q_0, q_1, \cdots, q_m\rangle$;当 m 是奇数且 $\langle q_0, q_1, \cdots, q_m + 1\rangle < f' \leqslant \langle q_0, q_1, \cdots, q_m\rangle$,那么连分数算法是有效的。

也就是说,连分数算法是否成功依赖于 f' 和 f 之间的差值百分比 δ 的大小。

定理 3 当 $\delta < \frac{1}{(3/2)n_m d_m}$ 时,用连分数算法可以找到 f,

其中 n_m 和 d_m 分别是 f 的分子和分母。

4.5.2　利用连分数攻击 CRT-RSA

在文献[3]的末尾,作者提出了开放性问题,即是否存在对小解密指数 CRT-RSA 的攻击,下面,本文从数论的角度来证明连分数攻击对四素数 CRT-RSA 是无效的。

证明　由 $ed \equiv 1 \bmod \varphi(n)$ 可得 $ed_p \equiv 1 \bmod (p-1)$,那么 $ed_p = k(p-1)+1$,其中 k 为正整数。两边同时除以 $pqrsd_p$,得到 $\frac{e}{pqrs} = \frac{k}{d_p}\left(\frac{p-1}{pqrs} + \frac{1}{kpqrs}\right)$。根据定理 2,令 $\frac{e}{pqrs} = \frac{k}{d_p}(1-\delta)$,而 $n = pqrs$,得到 $\delta = 1 - \frac{p-1}{n} - \frac{1}{kn}$。根据定理 3,要通过连分数算法找出 k 和 d_p 需要满足 $\delta < \frac{1}{(3/2)n_m d_m}$,即 $kd_p < \frac{2n}{3(n-p+1-1/k)}$,由于 n 和 p 都是大素数,所以分母中的 $1-1/k$ 可忽略,再同时除以 n 可得:$kd_p < \frac{2}{3}\cdot\frac{1}{1-1/qrs} \approx \frac{2}{3}$,那么 k 必须小于 1,这与 k 为正整数相矛盾,所以无法找到满足 $\delta < \frac{1}{(3/2)n_m d_m}$ 的情况,攻击无效。

5　仿真实验及比较分析

本次实验的硬件环境为:Pentium4 CPU 3.00 GHz,1.5 GB 内存,80 GB 硬盘;操作系统为:Windows XP;开发工具:Visual C ++6.0。本文基于 C ++ 构建了一个较为完善的大数库,采用无符号长整型数组从低位到高位存储大数,也就是说,把一个大数用 2^{32} 进制表示,这样可以最大限度减少基本运算中循环的次数,提高运算效率。然后用文献[14]中一种新的快速产生大素数的方法随机生成两个 1 024 bit 素数和四个 512 bit 素数,分别用传统双素数签名算法和文中的算法对三个 512 bit 消息摘要进行签名并记录其耗时情况,这里要说明的是,本文的实验程序考虑了中国剩余定理的计算代价,实验结果如表 1 所示。

表 1　三种签名算法耗时情况　　s

算法	第一次	第二次	第三次	平均耗时
传统双素数签名	3.432	3.621	3.568	3.541
双素数 CRT-RSA 签名	0.996	1.107	1.059	1.054
四素数 CRT-RSA 签名	0.311	0.338	0.329	0.326

从表 1 中可以看出,双素数 CRT-RSA 签名效率是传统算法的 3.36 倍,与理论值 3.47 相接近。而采用 Montgomery 模指数算法和中国剩余定理进行的优化的四素数签名算法,其效率是传统算法的 10.86 倍,是双素数 CRT-RSA 的 3.23 倍,这足以说明四素数 CRT-RSA 签名在签名效率方面确实有一定提高。

6　结语

近年来,许多加密技术和大量安全协议都采用了 RSA 算法,在一些对安全性要求比较高的认证机构中,甚至采用了模数为 2 048 bit 的 RSA 签名算法,这对于本来运算效率就不太高的 RSA 算法来说无疑是一个巨大的挑战。本文针对这一问题提出了四素数 CRT-RSA 签名算法,结合了 Montgomery 模指数算法和中国剩余定理对签名过程加以优化,最后在 VC6.0 的开发环境中进行了仿真实验,对几种签名效率做了比较分析,实验结果证实了四素数 CRT-RSA 签名算法在签名效率方面的优越性。

参考文献:

[1] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public key cryptosystems[J]. Communications of the Association for Computer Machinery, 1978, 21(2): 120 – 126.

[2] CAO YINGYU, FU CHONG. An efficient Implementation of RSA digital signature algorithm[C]// 2008 International Conference on Intelligent Computation Technology and Automation. Piscataway: IEEE Press, 2008: 100 – 103.

[3] WIENER M J. Cryptanalysis of short RSA secret exponents[J]. IEEE Transactions on Information Theory, 1990, 36(3): 553 – 558.

[4] BONEH D, DURFEE G. Cryptanalysis of RSA with private key d less than $N^{0.292}$[J]. IEEE Information Theory Society, 2000, 46(4): 1339 – 1349.

[5] 贺克英. 改进的 RSA 算法实现研究[D]. 成都: 电子科技大学, 2010.

[6] PAIXAO C A M. An efficient variant of the RSA cryptosystem[EB/OL]. [2010 – 10 – 02]. http:// www. ime. usp. br/ ~ capaixao/paper. pdf.

[7] 刘承彬, 耿也, 舒奎, 等. 有关中国剩余定理在多个素数的 RSA 解密运算中的加速公示的论证以及加速效率的估算[J]. 大连工业大学学报, 2012, 31(5): 372 – 375.

[8] 杨波. 现代密码学[M]. 北京: 清华大学出版社, 2007.

[9] 费晓飞, 胡捍英. CRT-RSA 算法安全性分析[J]. 微计算机信息, 2009, 25(3): 36 – 38.

[10] 陈月荣. 数字签名技术在电子商务中的应用[D]. 淮北: 淮北师范大学, 2011.

[11] STALLINGS W. Cryprography and network security principles and practice[M]. 5th ed. 北京: 电子工业出版社, 2011.

[12] 王安. RSA 公钥密钥算法的快速实现[D]. 济南: 山东大学, 2008.

[13] 刘美, 王玉柱, 何定养, 等. SHA-512 算法及基于生日攻击的安全性分析[J]. 后勤工程学院学报, 2010, 26(3): 92 – 96.

[14] COUVEIGNES J M, EZOME T, LERCIER R. A faster pseudo-primality test[J]. Rendiconti del Circolo Matematico di Palermo, 2012, 61(2): 261 – 278.

(上接第 1366 页)

[11] ZHU Z S, LU G H, CHEN Y, *et al*. Botnet research survey[C]// COMPSAC'08: 2008 32nd Annual IEEE International Computer Software and Applications Conference. Washington, DC: IEEE Computer Society, 2008: 967 – 972.

[12] ZHUGE J, HAN X, YE Z, *et al*. Discover and track botnets[C]// Proceeedings of the Chinese Symposium on Network and Information Security. New York: ACM, 2005: 183 – 189.

[13] DOUCEUR J. The sybil attack [C]// Proceedings of the 1st International Workshop on Peer-to-Peer Systems. Berlin: Springer, 2002: 251 – 260.

[14] STONE B, COVA M, CAVALLARO L, *et al*. Your botnet is my botnet: analysis of a botnet takeover[EB/OL]. [2012 – 08 – 12]. http://www. csd. uoc. gr/ ~ hy558/papers/torpig. pdf.

[15] CERTICOM . Press release : Certicom announces elliptic curve cryptosystem (ECC) challenge winner[R/OL]. [2012 – 10 – 01]. http://www. certicom. com/2002-press-releases/38-2002-press-releases/340.