

## 一种新的多用户接收 RSA 加密方案

李晓峰, 卢建朱

(暨南大学 计算机科学系, 广东 广州 510630)

(jnulxf@163.com)

**摘 要:**根据 RSA 加密系统和多密钥原理,提出了一种多用户接收的 RSA 加密方案。该方案允许每个用户都采用相同的小公钥,发送者可根据要发送的用户数通过引入随机数  $r$  对加密密钥进行放大,每个接收者用两个小密钥对密文进行解密。这既提高了 RSA 的加密速度,又可抵御对 RSA 的低指数攻击和重发攻击,还可实现发送者识别。

**关键词:** RSA; 多用户接收; 重发攻击; 低指数攻击; 发送者识别; 多密钥

**中图分类号:** TP393.08 **文献标识码:** A

## New encryption scheme of RSA with multi-recipient

LI Xiao-feng, LU Jian-zhu

(Department of Computer Science, Jinan University, Guangzhou Guangdong 510632, China)

**Abstract:** According to the protocol of RSA and the multi-private key theory, a new encryption scheme of RSA with multi-recipient was presented. This protocol allowed each recipient using the same public key during the encryption process and the sender using a random number to enlarge the public key following the number of recipients. Each recipient decrypted the cryptograph by two small public key. Therefore, the encryption speed of RSA was raised while withstanding the low exponent attack and multi-sending attack. Furthermore, this protocol was provided with the function of recipient identification.

**Key words:** RSA; multi-recipient; multi-sending attack; low exponent attack; recipient identification; multi-private key

### 0 引言

RSA 密钥体制<sup>[1]</sup>是 Rivest, Shair 和 Adleman 于 1977 年提出的最具有代表性的公钥算法,被广泛应用于各个领域。但随着网络技术和应用及计算机性能的不断提高,使 RSA 算法面临着巨大的挑战,并对 RSA 算法的应用提出了许多新的要求。更有效算法的出现和计算机计算速度的提高使 RSA 公钥系统的密钥长度不断增加以抵御攻击<sup>[2]</sup>。但 RSA 算法进行大数模幂运算的速度较慢,从而制约了该算法的应用。在实际应用中通常选用费马序列中的数 3 或 65 537 作为加密密钥  $e$ ,以提高 RSA 算法的加密与验证的速度。然而,当小指数 RSA 算法应用于多用户接收时,存在着一些问题。例如,当发送者向多个用户发送信息  $m$ ,根据获取的密文利用中国剩余定理可推出明文信息,即达到低指数攻击。同样地, RSA 算法在多用户接收中存在着重发攻击的安全问题。

本文提出了一种安全的、具有广泛应用前景的多用户接收 RSA 加密方案。方案在发送信息  $m$  中引入随机数  $r$  并根据接收信息的用户数对小公钥  $e$  进行放大,从而避免重发攻击和小指数攻击。该 RSA 算法对单个用户来说为小公钥加密协议,具有实现速度快的优点,同时又能避免重发、小指数等攻击。此外,该算法还可用于发送者识别的多用户接收领域。

### 1 多用户接收 RSA 加密方案

该算法建议 RSA 加密系统使用小公钥  $e = 3$ 。加密系统可分为初始化、加密和解密三个过程。

#### 1.1 初始化阶段

假设 RSA 公钥系统中有  $M$  个用户  $\{u_i\}_{i=1}^M$ 。每个用户  $u_i$  选择两个互异的大素数  $\bar{p}_i, \bar{q}_i$ 。令  $p_i = 2\bar{p}_i + 1, q_i = 2\bar{q}_i + 1$  且使  $p_i, q_i$  都是素数。计算  $n_i = p_i q_i$ ,并将  $n_i$  公开。在本系统中使用小公钥  $e_i = 3, \varphi(n_i) = (p_i - 1)(q_i - 1) = 4\bar{p}_i \bar{q}_i$ ,显然  $\gcd(e_i, \varphi(n_i)) = 1$ 。由公式  $e_i d_i \equiv 1 \pmod{\varphi(n_i)}$  得到用户  $u_i$  的解密密钥  $d_i$ ,用户  $u_i$  将  $d_i$  秘密保存,将  $\bar{p}_i, \bar{q}_i$  销毁。

#### 1.2 加密阶段

信息发送者向  $t$  个接收用户  $\{u_i\}_{i=1}^t$  发送信息  $m$ ,发送者的加密过程如下:

- 1) 选取一个随机小素数  $r$ ,使得  $r > \frac{\sqrt{t}}{2}$ ,其中  $t$  为接收用户数。
- 2) 选择两个互异的大素数  $P, Q$ ,计算  $T = PQ$ ,并满足  $\gcd(r, (P-1)(Q-1)) = 1$ ,由公式  $r r^{-1} \equiv 1 \pmod{\varphi(T)}$  计算  $r$  的逆元。
- 3) 计算模数  $N, N = n_1 n_2 \cdots n_t$ 。
- 4) 对明文进行加密。

收稿日期:2005-01-01;修订日期:2005-03-16

基金项目:国家自然科学基金资助项目(60173038, 69873020);广东省自然科学基金资助项目(010421, 000759)

作者简介:李晓峰(1978-),男,黑龙江海林人,硕士研究生,主要研究方向:计算机网络与安全;卢建朱(1965-),男,湖南郴州人,副教授,博士,主要研究方向:多媒体中的数据处理和通信技术、计算机网络与安全。

当  $m' > n_{\min}$  或  $m > T(n_{\min} = \min\{n_1, n_2, \dots, n_t\})$  时, 将  $m$  分成若干个信息单元  $\{m_j\}_{j=1}^p$ , 使  $0 < m_j < n_{\min}$  并且  $0 < m_j < T$ , 再对每一个信息单元加密。

$$C_j = (m_j)^e \bmod N \quad (j = 1, 2, \dots, p)$$

5) 将密文组合  $(C_1, C_2, \dots, C_p, r^{-1}, T)$  通过广播方式发送给  $t$  个接收用户。

### 1.3 解密阶段

接收用户  $u_i (i = 1, 2, \dots, t)$  接到密文后, 按如下步骤解密, 获取原文信息  $m$ :

1) 根据收到的公共密文计算用户  $u_i$  的密文:

$$C_{ij} = C_j \bmod n_i \quad (j = 1, 2, \dots, p)$$

2) 解密,  $\bar{m}_j = C_{ij}^{d_i} \bmod n_i$ ,

$$m_j = \bar{m}_j^{r^{-1}} \bmod T \quad (j = 1, 2, \dots, p)$$

3) 将  $m_j (1 < j < p)$  串接得到信息  $m$ ,  $m = m_1 \parallel m_2 \parallel \dots \parallel m_p$ 。

注: 若应用中  $n_{\min}$  较小, 则信息  $m$  的分块信息单元会较多, 增加了运算次数。可选择的解决方案是将加密公式改为  $C_j = (m_j' \bmod T)^e \bmod N (j = 1, 2, \dots, p)$ , 原加密方案需满足的条件  $r > \frac{\sqrt{t}}{2}, m_j' < n_{\min}$  改为满足条件  $T < n_{\min}$  即可。这就避免了信息单元分块过小的问题。可证明此可选方案与原方案具有同样的功能, 且同样可以避免各类攻击。

## 2 该算法的发送者识别应用

该算法的调整方案还可用于发送者识别的多用户接收 RSA 加密领域。

初始化阶段与上述方案相同。

在加密阶段发送者选择小素数  $ID$  作为发送者的身份识别信息, 使得  $rID > \frac{\sqrt{t}}{2}, \gcd(rID, (P-1)(Q-1)) = 1$ 。由公式  $(rID)^{-1} = (rID) \bmod T$  计算  $(rID)^{-1}$  并将其公开, 发送者秘密保存  $ID$ 。加密阶段用  $rID$  取代  $r$  对原文进行加密, 将加密得到的密文组合  $(C_1, C_2, \dots, C_p, (rID)^{-1}, T)$  发送给接收用户。

解密阶段, 若接收用户用  $d_i$  和接收到的  $(rID)^{-1}$  计算出正确的原文信息  $m$  后, 将接收到的  $(rID)^{-1}$  和发送者公开的  $(rID)^{-1}$  进行比较, 如果一致则证明信息由  $ID$  的持有者发送, 从而实现发送者识别。

## 3 新方案的安全性分析及效率分析

### 3.1 安全性分析

本文提出的加密认证方案是基于 RSA 加密算法的大数因子分解问题, 攻击者要想从用户  $i$  公开的公钥  $e_i$  得到私钥  $d_i$ , 就必须先求出  $d_i$ , 而由  $e_i$  求  $d_i$  面临大整数因子分解难的问题, 文献[3]分析指出这相当于要攻破 RSA 体系。

1) 该协议能抵御低指数攻击

由文献[4]可知, 若收方数  $t > E(E+1)/2$  时, 要解密原文信息  $m$  只需多项式时间, 所以要抵御低指数攻击必须满足条件  $t \leq E(E+1)/2$ , 则有  $3r(3r+1) \geq 2t$ , 解方程得  $r \geq \frac{\sqrt{1+8t}-1}{6}$ 。协议中  $r > \frac{\sqrt{t}}{2} > \frac{\sqrt{1+8t}-1}{6}$ , 所以能抵御低指

数攻击。

2) 协议能抵御重发攻击

加密过程中引入随机数  $r$ , 使每次加密过程的加密密钥  $E = re$  不同, 即  $C_p = m'^{re} \bmod N, C_q = m'^{re} \bmod N$ , 从而使同一消息接收者每次接收的密文  $C$  都不同, 可抵御重发攻击, 增加了系统的安全性。

3) 发送者识别功能

若攻击者伪装向接受者发送信息就必须知道发送者  $ID$ , 而由  $ID^{-1}$  求  $ID$  面临大数分解问题。真正的  $ID$  持有者可以对原文进行加密, 接收者通过解密信息的正确性和解密密钥的一致性可以判断发送者身份。此外对发送者识别功能进一步改进可以具有数字签名的特性。

### 3.2 效率分析

本协议与传统的 RSA 加密系统不同, 用户只有一个加密密钥, 但解密密钥由两个短密钥组成, 大大加快了解密的速度[5]。

加密过程中采用  $E = re$  作为加密密钥, 其中  $e = 3, r$  为随机小素数, 通过接收信息用户数来最终确定加密密钥的大小, 不用做大数乘法。计算模数  $N$  所需要的  $t$  次乘法和随机选取小素数  $r$  的计算成本是可以忽略的。

解密过程中使用两个小密钥。传统 RSA 在用基本 BR 算法计算时所用时间复杂度为  $O(\log d \log^2 n)$ [1], 当  $d$  很大与  $n$  同数量级时, 复杂度可以认为是  $O(\log^3 n)$ 。这样, 两个解密密钥对改善传统 RSA 计算效率是显而易见的。在效率上提高的倍数为:  $\alpha = \frac{(\log n)^3}{s(\log(n/s))^3} = s^2$ , 其中  $s$  为解密密钥个数。

当密钥个数  $s = 2$  时, 效率大约是传统计算方法的 4 倍。

分析表明, 本协议在满足同时向多个用户发送信息的同时, 在运算速度和安全性方面比一般的小公钥 RSA 加密系统要好。

### 参考文献:

- [1] RIVEST RL, SHAMIR A, ADLEMAN L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.
- [2] LENSTRA AK, VERHEUL ER. Selecting cryptographic key sizes [J]. Journal of Cryptology, 2001, 14(4): 255-293.
- [3] PAIXAO CAM. An efficient variant of the RSA cryptosystem [D]. Institute of Mathematics and Statistics, University of Sao Paulo, Brazil, 2003.
- [4] KNUTH DE. The art of computer programming, Vol. 2: Seminumerical algorithms [M]. Addison Wesley, 1981.
- [5] BONEH D, SHACHAM H. Fast Variants of RSA [R]. RSA Laboratories Cryptobytes, 2002.
- [6] SCHNEIER B. Application cryptography-protocols, algorithms, and source code in C (Second Edition) [M]. Beijing: Machine Press, 2001.
- [7] JOYE M, PAILLIER P. How to use RSA; or How to Improve the Efficiency of RSA Without Loosing its Security [A]. 2002 Information Security Solutions Europe Conference (ISSE2002) [C]. Paris, France, 2002.