基于 RSA 密码体制的门限代理签名

蒋 瀚[1)] 徐秋亮[1)] 周永彬[2)]

[1)](山东大学(南校区)计算机科学与技术学院 济南 250061)

[2)](中国科学院软件研究所信息安全国家重点实验室 北京 100080)

摘 要 在一个(t,n)门限代理签名体制中,原始签名者可以将他的签名权利以门限的方式委托给 n 个代理签名者,至少 t 个代理签名者合作,可以产生相应的代理签名,而任何少于 t 个代理签名者则不能.目前已经有很多基于离散对数问题的门限代理签名方案,但是并没有出现一个真正意义上的基于 RSA 密码体制的门限代理签名方案.鉴于 RSA 在理论及应用中的重要性,基于 RSA 构造门限代理签名体制是必要的.文中借助于 RSA 秘密共享的思想,构造了一个安全、有效的 RSA 门限代理签名方案.在文中的方案中,没有使用可信权威,所有的秘密参数都是由参与者分布式产生的.

关键词 RSA;代理签名;门限;门限代理签名

中图法分类号 TP309

Threshold Proxy Signature Scheme Based on RSA Cryptosystems

JIANG Han[1)] XU Qiu-Liang[1)] ZHOU Yong-Bin[2)]

[1)](*School of Computer Science and Technology, Shandong University, Jinan* 250061)

[2)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080)

Abstract In a (t,n) threshold proxy signature scheme, the original signer delegates the power of signing messages to a designated proxy group of n members. Any t or more proxy signers of the group can cooperatively issue a proxy signature on behalf of the original signer, but $(t-1)$ or less proxy signers cannot. Previously, all of the proposed threshold proxy signature schemes have been based on the discrete logarithm problem, and there has not a RSA-based scheme. However, it is necessary to build a RSA-based threshold proxy signature scheme because of the importance of RSA system. Using the Threshold-RSA method, the authors construct a secure RSA-based threshold proxy signature scheme. In the scheme, a Trust Authority(TA) is not needed and all of the secret parameters are generated in a distributed way.

Keywords RSA; proxy signature; threshold; threshold proxy signature

1 引 言

代理签名方案最早是由 Mambo 等人提出的[1],在一个代理签名方案中,代理签名者可以代表原始签名者产生有效的签名.Kim 与 Zhang 等人分别独立地构造了最初的门限代理签名方案[2-3].在一个(t,n)门限代理签名方案中,原始签名者的签名能力被赋予 n 个代理签名者,使其中 t 或更多个代理签名者合作能产生有效的代理签名.此后,出现了大量门限代理签名方案的研究[4-11].

在现有的门限代理签名方案中,绝大部分都是

收稿日期:2004-12-30;修改稿收到日期:2006-09-25.本课题得到国家自然科学基金(60373026)及山东省自然科学基金(Y2003G02)资助.**蒋 瀚**,男,1974 年生,博士研究生,研究方向为信息安全.**徐秋亮**(通信作者),男,1960 年生,博士,教授,博士生导师,研究领域为密码学与信息安全.E-mail: xql@sdu.edu.cn.**周永彬**,男,1973 年生,博士,副研究员,主要研究方向为应用密码学、网络与信息安全理论与技术.

基于离散对数问题的，只有 Hwang 等人提出了一个基于 RSA 的门限代理签名方案[8]，而 Wang 等人则指出了文献[8]的方案不能满足门限代理签名方案的基本特性[9]，实际上是一个失败的方案，并指出构建一个安全有效的基于 RSA 的门限代理签名方案仍然是一个有待解决的问题. 因此，到目前为止没有一个真正意义上的基于 RSA 的门限代理签名方案. 基于 RSA 构造门限代理签名方案的主要困难是模数 N 的素因子、$\varphi(N)$ 等必须保密，任何人(包括原始签名人)均不可知道. 因而所有秘密必须分布式产生.

2000 年 Shoup 构建了一个较为有效的 RSA 门限签名方案[12]，但在他的方案中，存在庄家(Dealer)，由庄家产生 RSA 的各参数，然后以门限的方式将私钥共享. 如果要在代理签名方案中使用这种方式，则庄家的角色只能由原始签名人或者一个系统权威来担当，则他们就具有了伪造的能力. 因此这种方式也不适合于门限代理签名方案.

Boneh 与 Franklin 在文献[13]中描述了如何分布式地产生 RSA 的模与私钥的协议. 文献[12-17]都致力于门限 RSA 机制的研究并得出了成果. 我们基于这些成果，构建了一个基于 RSA 的门限代理签名方案，这个方案满足代理签名的不可伪造性、原始签名者密钥的私密性，是一个真正意义上的基于 RSA 的门限代理签名方案，解决了 Wang 等人提出的问题[9]. 同时我们用程序对本文方案进行了模拟实现.

2 基于 RSA 的门限代理签名方案

我们的基于 RSA 的门限代理签名方案由以下 5 个过程构成：

(1) 模数 N 的产生. 所有的代理签名者分布式地产生模数 N，使 N 为两个大素数的乘积.

(2) 公钥 e 的产生. 原始签名者选取候选公钥 e，与代理签名者合作进行筛选，$\gcd(e,\varphi(N))=1$.

(3) 私钥 d 的产生与共享. 所有的代理签名者分布式地产生私钥 d 的秘密共享份额.

(4) 代理签名的产生. t 个代理签名者分别产生自己的子代理签名，然后将所有的子代理签名组合成代理签名.

(5) 代理签名的验证. 验证者使用公共信息验证代理签名.

2.1 公共参数

记原始签名者为 U_o，代理签名者的集合为 $PG=\{U_i \mid 1\le i\le n\}$，$i=1,2,\cdots,n$. 实际的代理签名产生者集合为 ASG，为了符号的简洁，不失一般性，设 $ASG=\{U_i \mid 1\le i\le t\}$. $h(\cdot)$ 为一安全散列函数.

2.2 模数 N 的产生

本节的目的是分布式生成一个 RSA 的模 $N=pq$，其中 p,q 都是大素数且对任何人保密，事实上，p,q 不能显式出现.

2.2.1 生成候选 N 值

对于即将产生的 N，设定其长度为 b 比特，并选取素数 $P>N$. 在实际应用中，b 一般选取 512，1024 或 2048，这里不妨设其为偶数.

(1) 代理签名者 $U_i\in PG$ 随机选取 p_i，$q_i\in[\lceil(2^{(b-2)/2}/n)\rceil,\lfloor(2^{b/2}-1)/n\rfloor]$(该范围的确定旨在保证 N 是两个长度为 $b/2$ 比特的大素数的乘积，见下面的命题 1). 令 $l=\lfloor(n-1)/2\rfloor$. 对所有的 $i=1,2,\cdots,n$，用户 $U_i\in PG$ 随机选取两个次数为 l 的多项式 $f_i,g_i\in Z_P[x]$，满足 $f_i(0)=p_i$，$g_i(0)=q_i$. 另外，随机选取一个次数为 $2l$ 的多项式 $h_i\in Z_P[x]$，满足 $h_i(0)=0$.

(2) 对所有的 $i=1,2,\cdots,n$，用户 $U_i\in PG$ 计算：$p_{i,j}=f_i(j)$，$q_{i,j}=g_i(j)$，$h_{i,j}=h_i(j)$，$j=1,2,\cdots,n$. 然后，秘密发送三元组 $\langle p_{i,j},q_{i,j},h_{i,j}\rangle$ 给 U_j.

(3) U_i 接收到所有其他用户秘密发送过来的三元组 $\langle p_{j,i},q_{j,i},h_{j,i}\rangle$，$j=1,2,\cdots,n$，计算 $N_i=(\sum_{j=1}^{n}p_{j,i})\cdot(\sum_{j=1}^{n}q_{j,i})+\sum_{j=1}^{n}h_{j,i} \bmod P$，然后对所有的用户广播 N_i.

(4) 记 $\alpha(x)=(\sum_{j=1}^{n}f_j(x))\cdot(\sum_{j=1}^{n}g_j(x))+\sum_{j=1}^{n}h_j(x) \bmod P$. 显然 $\alpha(i)=N_i$，并且 $\alpha(x)$ 的次数为 $2l\le n-1$.

记 $p=\sum_{i=1}^{n}p_i$，$q=\sum_{i=1}^{n}q_i$，则 $N=\alpha(0)=\sum_{i=1}^{n}p_i\cdot\sum_{i=1}^{n}q_i=pq$. 而每个用户掌握所有的总共 n 个 $\alpha(i)$ 值，使用拉格朗日插值，可以恢复出 $\alpha(x)$，从而得到 $N=\alpha(0) \bmod P$. 由于 $P>N$，因此所有用户都可以得到正确的 N. 该步骤中，p,q 并未显式出现，对任何人都是不可见的，所有用户得到的仅是 N 和 N_i.

命题 1. 以上算法中，$p=\sum_{i=1}^{n}p_i$，$q=\sum_{i=1}^{n}q_i$ 的长度为 $b/2$ 比特，从而 N 的长度正是所设定的 b 比特.

证明. 由步(1)中 p_i,q_i 的取值范围知

$$2^{(b/2)-1}=(2^{(b-2)/2}/n)\cdot n\leq p_{\min}\cdot n<\sum_{i=1}^{n}p_i<$$
$$p_{\max}\cdot n<((2^{b/2}-1)/n)\cdot n<2^{b/2}-1,$$

因此，$p=\sum_{i=1}^{n}p_i$ 的二进制长度为 $b/2$ 比特. 同理，$q=\sum_{i=1}^{n}q_i$ 的二进制长度也为 $b/2$ 比特. 证毕.

2.2.2　检测 N 是否为两个素数的乘积

以下步骤用于判断 N 是否为两个素数的乘积，相关原理参见文献[14].

(1) PG 首先在内部协商一个公开的随机数 $g\in Z_N^*$.

(2) 用户执行一个 Fermat 检测. 用户 U_1 计算 $v_1\equiv g^{N+p_1+q_1+1} \bmod N$，对于 $i=2,3,\cdots,n$，用户 U_i 计算 $v_i\equiv h^{p_i+q_i} \bmod N$. 用户之间交换 v_i 值.

(3) 验证 $v_1\overset{?}{\equiv}\prod_{i=2}^{n}v_i \bmod N$. 如果等式不成立，则 N 不是两个素数的乘积，返回 2.2.1 节，重新计算一个新的 N 值. 若等式成立则 N 是两个素数的乘积.

注：上述检测是一个 Fermat 检测，用于检测一个数是否为两个大整数的乘积. 实际上它检测的是 $g^{N+p+q+1}\overset{?}{\equiv}1 \bmod N$.

当 N 已经通过上述检测，被确信是两个素数的乘积后，由 N 的构造过程知 $N=pq$，其中 $p=\sum p_i$，$q=\sum q_i$. 由整数分解的唯一性，p,q 是素数，且由命题 1 知 p,q 的长度均为 $b/2$ 比特，因而，N 是两个大素数的乘积.

以上给出了分布式构造 $N=pq$ 的一个方法. 如需 p,q 是安全素数，可采用 Pierre-Alain 等人给出的分布式构造 $N=pq$ 的方法，其中 $p=2p'+1,q=2q'+1$，这时计算量会相应增加[17].

2.2.3　$\varphi(N)$的共享

代理签名者 U_1，记 $\varphi_1(N)=N-p_1-q_1+1$，对 $2\leq i\leq n$，代理签名者 U_i 记 $\varphi_i(N)=-p_i-q_i$，则

$$\varphi(N)=N-p-q+1=\sum_{i=1}^{n}\varphi_i(N) \tag{1}$$

$\varphi_i(N),i=1,2,\cdots,N$，可以看作 $\varphi(N)$在代理签名者中的共享份额.

2.3　公钥 e 的产生

记 m_w 为原始签名人的授权书，其中包括原始签名人身份、各个代理签名人身份、门限值 t、代理权限、代理时限等信息. 原始签名人与代理签名人共同执行下列步骤生成代理签名公钥 e，使 $\gcd(e,\varphi(N))=1$. 如果在 2.2 节生成 N 时采用了 Pierre-Alain 的方法[17]，即当 p,q 是安全素数时，该条件是显然成立的，该步可以省略.

(1) 原始签名人随机选取候选公钥 e，并公开.

(2) 对所有的 $i=1,2,\cdots,n$，代理签名者 U_i 计算 $c_i=\varphi_i(N)+ek_i$，其中 k_i 是随机数. 代理签名者将 c_i 发送给原始签名人 U_o.

(3) U_o 收到所有的 c_i 后，计算 $c=\sum_{i=1}^{n}c_i$，并利用欧几里德算法计算最大公因数 $\gcd(e,c)$，如果 $\gcd(e,c)=1$，则接受 e 为代理签名公钥；否则，返回步(1).

事实上，因为 $c=\sum_{i=1}^{n}c_i=\sum_{i=1}^{n}\varphi_i(N)+e\sum_{i=1}^{n}k_i=\varphi(N)+e\sum_{i=1}^{n}k_i$，记 $K=\sum_{i=1}^{n}k_i$，则 $c=\varphi(N)+Ke$. 而 $\gcd(e,\varphi(N))=\gcd(e,(\varphi(N)+Ke))=\gcd(e,c)$，所以通过以上步骤，在原始签名人在不知道 $\varphi(N)$ 的情况下，可以产生一个与 $\varphi(N)$互素的 e，从而作为代理签名公钥.

产生代理签名公钥之后，原始签名人对代理签名公钥与授权书签名，该签名消息记为 σ_w.

2.4　私钥 d 的产生与共享

对于在 2.2 节生成的模数 N，对应的每个代理签名者 U_i 持有私钥 (p,q) 的秘密共享份额 (p_i,q_i). 本节要求对于 2.3 节由原始签名者规定的公钥 e，在代理签名者中分布式地产生与之对应的私钥 d，使

$$ed\equiv 1 \mod\varphi(N) \tag{2}$$

但 d 不能显式出现，其对任何人不可见.

令 $x=-\varphi^{-1}(N) \bmod e$，则 $x\varphi(N)=-1 \bmod e$，因而，$x\varphi(N)+1$ 可被 e 整除，取 $d=(x\varphi(N)+1)/e$，则 d 是整数，且 $ed=x\varphi(N)+1$，从而式(2)成立. 于是问题转化为分布式产生 $x=-\varphi^{-1}(N) \bmod e$ 的问题.

以下步骤，利用上面原理在代理签名者中分布式地生成并共享 RSA 密钥 d.

(1) 代理签名者 U_i 随机取值 $r_i\in Z_e$.

(2) 利用 2.2.1 节的步骤，代理签名者分布式地计算

$$\psi=\sum r_i\cdot\sum\varphi_i(N) \bmod e \tag{3}$$

如果 ψ 对于模 e 是不可逆的，则返回步(1).

(3) 每个代理签名者 U_i 独立计算 $\xi_i=r_i\psi^{-1} \bmod e$. 则由式(3)得

$$\sum \xi_i \equiv (\sum r_i)\psi^{-1} \equiv \varphi^{-1}(N) \bmod e \qquad (4)$$

所以，代理签名者以 ξ_i 为份额共享了 $\varphi^{-1}(N) \bmod e$.

(4) PG 在内部协商一个素数 $P' > 2Ne$. 将 $0 \leq \xi_i < e$ 视为 $Z_{P'}$ 的元素.

(5) 令 $l = \lfloor (t-1)/2 \rfloor$. 对所有的 $i = 1, 2, \cdots, n$，用户 U_i 随机选取两个次数为 l 的多项式 f_i', $g_i' \in Z_{P'}$，满足 $f_i'(0) = -\xi_i$, $g_i'(0) = \varphi_i(N)$. 另外，对于 $i = 2, 3, \cdots, n$，用户 U_i 随机选取一个次数为 $2l$ 的多项式 $h_i' \in Z_{P'}$，满足 $h_i'(0) = 0$，而对于 U_1，随机选取一个次数为 $2l$ 的多项式 $h_1' \in Z_{P'}$，满足 $h_1'(0) = 1$.

(6) 对所有的 $i = 1, 2, \cdots, n$，用户 U_i 计算：$\xi_{i,j} = f_i'(j)$, $\varphi_{i,j} = g_i'(j)$, $h_{i,j}' = h_i'(j)$, $j = 1, 2, \cdots, n$. 然后，将三元组 $\langle \xi_{i,j}, \varphi_{i,j}, h_{i,j}' \rangle$ 秘密发送给 U_j.

(7) 接收到所有其他用户发送过来的信息 $\langle \xi_{j,i}, \varphi_{j,i}, h_{j,i}' \rangle$, $j = 1, 2, \cdots, n$, $j \neq i$，用户 U_i 计算 $T_i = (\sum_{j=1}^{n} \xi_{j,i})(\sum_{j=1}^{n} \varphi_{j,i}) + \sum_{j=1}^{n} h_{j,i}' \bmod P'$，则每个代理签名者的私钥共享份额为 T_i.

命题 2. 任何 t 个代理签名者合作，可利用持有的私钥份额构造出私钥 d.

证明. 为使符号简洁，不妨设代理签名者 $U_1, U_2, \cdots, U_t$ 合作.

记 $$T(x) = (\sum_{j=1}^{n} f_j'(x)) \cdot (\sum_{j=1}^{n} g_j'(x)) + \sum_{j=1}^{n} h_j'(x) \bmod P'.$$

显然 $T(i) = T_i$，并且 $T(x)$ 的次数为 $t-1 = 2l$. 所以 t 个代理签名者使用拉格朗日插值，可以恢复出 $T(0)$：

$$T(0) = \sum_{i=1}^{t} \left(\prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-j}{i-j} \right) \cdot T_i \bmod P',$$

又 $$T(0) = (\sum_{j=1}^{n} f_j'(0)) \cdot (\sum_{j=1}^{n} g_j'(0)) + \sum_{j=1}^{n} h_j'(0) \bmod P'$$

$$= (\sum_{j=1}^{n} (-\xi_j)) \cdot (\sum_{j=1}^{n} \varphi_j(N)) \bmod P' + 1,$$

从而由式(4)和式(1)，得

$$T(0) = (-\varphi^{-1}(N) \bmod e) \cdot \varphi(N) + 1 \bmod P',$$

从而由 d 的选取方法，

$$\frac{T(0)}{e} = \frac{(-\varphi^{-1}(N) \bmod e)\varphi(N) + 1}{e} = d.$$ 证毕.

注：该命题的意义仅在于，指出 t 个代理签名者合作可重构秘密密钥 d，在执行生成代理签名的步骤时，并不真正重构密钥 d，而是每个代理签名的实际参与者分别生成部分签名，最后由部分签名组合成代理签名. 整个过程中不泄漏任何秘密.

2.5 代理签名的产生

在本节，不失一般性，假设实际的代理签名生成者集合 $ASG = \{U_i \mid 1 \leq i \leq t\}$，在这些成员合作产生代理签名的过程中，要求其中一个充当代理签名的组合者，不妨设为 U_1.

(1) 部分代理签名的产生

除 U_1 外，每个代理签名者 $U_i \in ASG$ 利用其秘密份额 T_i, $2 \leq i \leq t$，计算自己的部分代理签名为 $\sigma_i = h(m)^{s_i} \bmod N$，其中，$s_i = \lfloor \lambda_i / e \rfloor$，$\lambda_i = \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-j}{i-j} \cdot T_i \bmod P'$，秘密发送给 U_1.

(2) 部分代理签名的组合

U_1 计算 $\sigma_1 = h(m)^{s_1} \bmod N$，其中，$s_1 = \lfloor \lambda_1 / e \rfloor$，$\lambda_1 = \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-j}{i-j} \cdot T_1 \bmod P'$.

$$\sigma' = \sigma_1 \sigma_2 \cdots \sigma_t \bmod N.$$

由于在取整过程中可能损失小数，σ' 一般不是一个有效的代理签名，但取整过程只进行了 t 次，引起的指数的减小不超过 t，故只需不超过 t 次验证可得到有效签名.

算法 1.

For $k = 0$ to $t-1$

1. $\sigma' = \sigma' h(m) \bmod N$.
2. 验证 $h(m) = (\sigma')^e \bmod N$，如果成立，则令 $\sigma = \sigma'$，跳出循环.

Next

σ 为最终的代理签名.

命题 3. 上述 σ 为有效的代理签名，即满足 $\sigma^e \equiv h(m) \bmod N$.

证明.

$$\begin{aligned} s_1 + s_2 + \cdots + s_t &= \sum_{i=1}^{t} \lfloor \lambda_i / e \rfloor \\ &= \sum_{i=1}^{t} \left\lfloor \left(\prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-j}{i-j} \cdot T_i \bmod P' \right) \Big/ e \right\rfloor \\ &\geq \sum_{i=1}^{t} \left(\left(\prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-j}{i-j} \cdot T_i \bmod P' \right) \Big/ e - 1 \right) \\ &= \left(\sum_{i=1}^{t} \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-j}{i-j} \cdot T_i \bmod P' \right) \Big/ e - t \\ &= T(0)/e - t \\ &= d - t. \end{aligned}$$

类似地，$s_1 + s_2 + \cdots + s_t \leq d$. 即 $s_1 + s_2 + \cdots + s_t =$

$d-k$，$0\leq k\leq t$，于是，

$$\sigma'=\sigma_1\sigma_2\cdots\sigma_t\equiv h(m)^{s_1}h(m)^{s_2}\cdots h(m)^{s_t}$$
$$\equiv h(m)^{(s_1+s_2+\cdots s_t)}\bmod N=h(m)^{d-k}\bmod N,$$

因而，算法 1 必在某一步能够验证成立，输出正确代理签名.　　证毕.

2.6　代理签名的验证

(1) 验证者首先验证原始签名人对授权书 m_w 和代理签名公钥 e 的签名 σ_w.

(2) 使用代理签名公钥验证代理签名 σ：$\sigma^e\stackrel{?}{=}h(m)\bmod N$.

3　安全性分析

在这个方案中，可能存在的安全隐患共有原始签名人密钥的泄漏、原始签名人伪造代理签名、代理签名人合谋伪造有效的非法代理签名.

对于原始签名人密钥泄漏的问题，由于在本方案中原始签名人的私钥仅用于对授权书与代理签名公钥的签名，没有参与交互，所以显然无泄漏可能.

对于原始签名人伪造代理签名，由于公钥中原始签名人只知道公钥 N，e，所以抵抗其伪造代理签名的安全性强度等价于 RSA 体制.

对于代理签名人合谋伪造代理签名，我们有如下命题.

命题 4.　如果大整数分解问题是难解的，则至少 t 个代理签名人合作才能产生合法的代理签名. 攻击本方案的难度相当于攻击 RSA 或 Shamir 门限方案.

证明.　攻击本方案可采用两种方法：攻击 RSA 或从该方案的协议中非法获得秘密参数. 下面讨论第二种方法，即从方案的建立中获取代理签名私钥 (p,q,d).

由 2.2.1 节，私钥 $p=\sum_{i=1}^{n}p_i$，$q=\sum_{i=1}^{n}q_i$，其中 p_i，q_i 分别为用户自己独立产生的私钥共享份额. 同时所有用户通过一个 (n,n) 的 shamir 门限方案共享公钥 $N=pq$，每个人的公钥共享份额为 p_iq_i. 因此对 p,q 的获取有两种途径：(1) 分解大整数 N；(2) 攻破 shamir(n,n) 门限方案，即当至少 n 个代理签名人共同合谋时才能够恢复出代理签名私钥 p,q，从而能够伪造代理签名.

由 2.4 节 d 的产生过程知，任何少于 t 人的群体，不管是否是签名方案的参与者，要想求出私钥 d 需要求出 $\varphi(N)=(p-1)(q-1)$ 与 $-\varphi^{-1}(N)\bmod e$. 而 $\varphi(N)$，$-\varphi^{-1}(N)\bmod e$ 是通过一个 shamir(t,n) 门限方案共享的，因此，非法获得 d 的难度等价于攻破 shamir(t,n) 门限方案的难度，即当至少 t 个代理签名人合作时才能够恢复出代理签名私钥 d，从而能够产生代理签名.

总之，至少 t 个代理签名人合作，才能够产生代理签名.　　证毕.

4　效率分析

4.1　代理签名生成与验证中的运算

为了生成部分代理签名，用户 U_2 至 U_t 各进行一次 RSA 签名，用户 U_1 以某种概率分布计算 1 至 t 次 RSA 签名与验证，其计算量的数学期望为 $t/2$ 次. 所以总的生成部分签名的花费为 $(t-1+t/2)=(3t/2-1)$ 次 RSA 签名运算与 $t/2$ 次 RSA 验证运算.

代理签名的验证过程只需要两次 RSA 签名验证的计算.

4.2　方案建立过程中的运算

考虑代理签名的实际背景，比如，一个总经理可能授权其公司中的部门经理作为其代理签名者群体. 一般而言，一个原始签名人的代理签名者群体不可能太大，即方案中的 n 和 t 一般不会太大.

方案建立过程主要是三个步骤：模数 N 的建立；公钥 e 的建立；私钥 d 的建立.

1) 模数 N 的建立

(1) 候选 N 值建立时，每个用户都需进行：(i) $3(n-1)$ 次的模幂运算；(ii) 一次拉格朗日插值计算. 因共有 n 个代理签名者，总的计算量为 n 倍的上述计算.

(2) 为了检测 N 是否为两个素数的乘积，需要一次 Jacobi 符号的计算，同时每个用户还需要进行两次的模幂运算，总共为 $2n$ 次的模幂运算.

由于 p_i，q_i 分别由用户自己独立随机产生，且由命题 1 $p=\sum_{i=1}^{n}p_i$，$q=\sum_{i=1}^{n}q_i$ 的长度为 $b/2$ 比特，故 p,q 可视为区间 $[2^{b/2-1},2^{b/2}-1]$ 内具有均匀概率分布的随机整数.

由数论中的素数定理，$\pi(x)\sim x/\ln x$，即当整数 x 足够大时，不超过 x 的素数的个数约为 $x/\ln x$ 个. 故 $[2^{b/2-1},2^{b/2}-1]$ 内的素数个数约为

$$\pi(2^{b/2})-\pi(2^{b/2}-1)\approx\frac{2^{b/2}}{(b/2)\ln 2}-\frac{2^{b/2-1}}{(b/2-1)\ln 2}$$
$$\approx\frac{2^{b/2-1}}{(b/2)\ln 2},$$

因而，p,q 为素数的概率为 $(\pi(2^{b/2})-\pi(2^{b/2}-1))/(2^{b/2}-2^{b/2-1})\approx 1/((b/2)\ln 2)$，得到一个满足要求的 N，即使 p,q 同时为素数，期望检测次数为 $((b/2)\ln 2)^2$.

2）公钥 e 的建立

每个候选 e 值的建立需要（当 p,q 为安全素数时，该步可省）：

（1）每个代理签名者进行一次模乘运算.

（2）原始签名者进行一次欧几里德算法.

3）私钥 d 的建立

在私钥 d 的建立过程中，每个成员需要进行两次同 2.2.1 节的秘密共享算法，即（i）$3(n-1)$ 次的模幂运算；（ii）一次拉格朗日插值计算.

由以上的讨论知，本方案在建立的过程中需要的计算量较大. 然而在 t,n 较小的实际情况下，是可以容忍的. 同时，这些计算只需要在系统建立时进行一次，而在方案的使用过程中，代理签名的产生与验证则只需要有限几次 RSA 运算，计算量与现有的基于离散对数的门限代理签名体制相当，有比较高的效率. 因此我们的方案是实用的.

5 结 语

本文的主要贡献在于构造了一个真正意义上的基于 RSA 的门限代理签名方案，解决了 Wang 等人提出的公开问题[9]. 在我们的方案中，代理签名的私钥完全是分布式产生的，任何少于 t 个代理签名者都无法产生合法的代理签名，而原始签名者也不能伪造代理签名. 在效率分析中知，方案在系统建立时需要较大计算量，这主要是由分布式产生 RSA 模数 N，但需保证不向任何人（包括原始签名人）暴露其素因子所花费的. 减低方案建立时的计算量是一个仍然需要研究的问题.

参 考 文 献

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation//Proceedings of the 3rd ACM Conference on Computer and Communications Security. New Delhi, 1996: 48-57

[2] Kim S, Park S, Won D. Proxy signatures, revisited//Han Y, Okamoto T, Qing S. Information and Communications Security. LNCS 1334. Berlin: Springer-Verlag, 1997: 223-232

[3] Zhang K. Threshold proxy signature schemes//Okamoto E, Davida G, Mambo M. Proceedings of the Information Security. Berlin: Springer-Verlag, 1998: 191-197

[4] Sun H M, Lee N Y, Hwang T. Threshold proxy signatures. IEE Proceedings Computes and Digital Technique, 1999, 146(5): 259-263

[5] Sun H M. An efficient nonrepudiable threshold proxy signature scheme with known signers. Computer Communications, 1999, 22(8): 717-722

[6] Hwang M S, Lin I C, Lu E J L. A secure nonrepudiable threshold proxy signature scheme with known signers. International Journal of Informatica, 2000, 11(2): 1-8

[7] Hsu C L, Wu T S, Wu T C. New nonrepudiable threshold proxy signature scheme with known signers. Journal of Systems and Software, 2001, 58(2): 119-124

[8] Hwang M S, Lu E J L, Lin I C. A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem. IEEE Transactions on Knowledge and Data Engineering, 2003, 15(6): 1552-1560

[9] Wang G L, Feng B, Zhou J Y, Deng Robert H. Comments on "A Practical (t,n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem". IEEE Transactions on Knowledge and Data Engineering, 2004, 16(10): 1309-1311

[10] Li Ji-Guo, Cao Zhen-Fu. Improvement of a threshold proxy signature scheme. Journal of Computer Research and Development, 2002, 39(11): 1513-1518(in Chinese)
(李继国，曹珍富. 一个门限代理签名方案的改进. 计算机研究与发展, 2002, 39(11): 1513-1518)

[11] Li Ji-Guo, Cao Zhen-Fu, Li Jian-Zhong, Zhang Yi-Chen. Present situation and progress of proxy signature. Journal of China Institute of Communications, 2003, 24(10): 114-124 (in Chinese)
(李继国，曹珍富，李建中，张亦辰. 代理签名的现状与进展. 通信学报, 2003, 24(10): 114-124)

[12] Shoup V. Practical threshold signatures//Preneel B. Advances in Cryptology: EUROCRYPT′2000. LNCS 1807. Berlin: Springer-Verlag, 2000: 208-220

[13] Boneh D, Franklin M. Efficient generation of shared RSA keys//Kaliski B. Advances in Cryptology: CRYPT′97, LNCS 1294. Berlin: Springer-Verlag, 1997: 425-439

[14] Malkin M, Wu T, Boneh D. Experimenting with shared generation of RSA keys//Proceedings of the Internet Society′s Symposium on Network and Distributed System Security. San Diego, 1999: 43-56

[15] Catalano D, Gennaro R, Halevi S. Computing inverses over a shared secret modulus//Preneel B. Advances in Cryptology: Eurocrypt′00. LNCS 1807. Berlin: Springer-Verlag, 2000: 190-206

[16] Damgard I, Koprowski M. Practical threshold RSA signatures without a trusted dealer//Pfitzmann B. Advances in Cryptology: Eurocrypt′01. LNCS 2045. Berlin: Springer-Verlag, 2001: 152-165

[17] Fouque P A, Stern J. Fully distributed threshold RSA under standard assumptions//Boyd C. Advances in Cryptology: ASIACRYPT′01. LNCS 2048. Berlin: Springer-Verlag, 2001: 310-330

JIANG Han, born in 1974, Ph. D. candidate. His main research area is information security.

XU Qiu-Liang, born in 1960, Ph. D., professor, Ph. D. supervisor. His main research interests include information security and cryptology.

ZHOU Yong-Bin, born in 1973, Ph. D., associate professor. His main research interests include applied cryptology, network and information security.

Background

This paper is supported by the National Natural Science Foundation of China (No. 60373026). The main task of the project is designing and analyzing the digital signature schemes, especially the forward-secure signatures, proxy signatures and the threshold signatures. The authors have made much research on various related signatures, which is published on important journals, such as Chinese Journal of Computers, Applied Mathematics and Computation, etc. The scheme proposed in this paper is an important part of the project.

This paper researches a special kind of digital signature schemes——threshold proxy signature schemes based on RSA cryptosystems. A lot of threshold proxy signature schemes are proposed in resent years. But all of them are based on the discrete logarithm problem. There has not a RSA-based scheme by now for there are essential difficulties in sharing a RSA private key among n players. This paper gives a method to construct a secure RSA-based threshold proxy signature scheme. In the scheme, a Trust Authority (TA) is not needed and all of the secret parameters are generated in a distributed way.