一个安全的门限代理签名方案

王晓明[①] 张 震[①] 符方伟[②]
[①](暨南大学计算机系 广州 510632)
[②](南开大学数学科学学院 天津 300071)

摘 要 针对现有的门限代理签名方案中所存在的合谋攻击，提出了一个安全的门限代理签名方案。合谋攻击是指在不知道任何有效的门限代理签名的情况下，恶意代理成员人数大于或等于门限值时，他们能合谋重新构造代理群的秘密多项式函数，得到代理群的秘密参数，从而可以伪造其他代理成员的代理签名。提出的新方案不仅能满足门限代理签名的性质，而且能抵抗合谋攻击。另外，该方案能根据原始签名人的需要，撤消代理签名人的代理签名权。

关键词 密码学，数字签名，门限代理签名，合谋攻击
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1009-5896(2006)07-1308-04

A Secure Threshold Proxy Signature Scheme

Wang Xiao-ming[①] Zhang Zhen[①] Fu Fang-wei[②]
[①](*Department of Computer Science, Jinan University, Guangzhou* 510632, *China*)
[②](*School of Mathematics Science, Nankai University, Tianjin* 300071, *China*)

Abstract A secure threshold proxy signature scheme is proposed aiming at conspiracy attack, that is, any t (t is threshold value) or more malicious proxy signatures may work together to reconstruct the secret polynomial of the proxy group and derive the secret keys of other members in the proxy group, consequently they can impersonate some other proxy signers to generate a valid threshold proxy signature. The new scheme can not only satisfy the properties of the threshold proxy signature, but also withstand the conspiracy attack. Furthermore, the proxy signer's proxy signing capability can be revoked if the original signer needs.

Key words Cryptography, Digital signature, Threshold proxy signature, Conspiracy attack

1 引言

门限代理签名是一个很重要的数字签名，近年来人们对门限代理签名进行了广泛的研究。目前，已经有许多门限代理签名方案[1-7]被提出。但这些方案都存在以下问题：(1)合谋攻击。文献[1－7]的方案中存在合谋攻击，即在不知道任何有效的门限代理签名的情况下，恶意代理成员人数大于或等于门限值时，他们能合谋重新构造代理群的秘密多项式函数，得到代理群的秘密参数，从而可以伪造其他代理成员的代理签名。在Hsu等人提出的门限代理签名方案[7]中，产生代理签名时需要代理签名人的私钥，因此恶意代理签名人因没有其他代理签名人的私钥不能伪造其他代理签名人的代理签名。但仍然存在着恶意代理签名人的人数大于或等于门限值时，他们能合谋重新构造代理群的秘密多项式函数，从而得到代理群的秘密参数的不安全因素。另外，在Hsu等人的方案中，原始签名人能根据代理签名辨认出代理签名人的身份，这对原始签名人是非常有用的，因为原始签名人能对代理签名人的代理签名进行监督，防止代理签名人滥用他们的代理签名权。但是，在有些实际情况下，尽管代理签名人忠实地行使着原始签名人委托给自己的代理签名权利，代理签名人仍然不愿意原始签名人能根据代理签名确定代理签名人的身份。例如，电子选举、电子支付等。(2)在文献[1－7]的方案中，一旦原始签名人将签名权委托给代理签名人，那么代理签名人就具有对这个签名权的永久代理，这对原始签名人是很不利的。原始签名人希望代理签名人在某一段时间内具有代理签名权，当这段有效期过后，就收回代理签名权。

针对以上问题，本文提出了一个安全的门限代理签名方案。方案不仅能满足门限代理签名的性质，而且也能抵抗以上提到的合谋攻击；根据代理签名不能辨认代理签名人身份；在原始签名人需要时，可收回代理签名权。

2 Kim 等人的门限代理签名方案及其弱点

2.1 Kim等人的门限代理签名方案[1]

设p, q是两个大素数，且$q \mid (p-1)$，g是GF(p)中阶为q的生成元。原始签名人的私钥为 $x_0 \in Z_q^*$，公钥为 $y_0 = g^{x_0} \bmod p$ (y_0 由CA公证过)。h是安全的单向Hash函数。m_w是授权消息，主要包含原始签名人和代理签名人的身份，代理签名的范围等。P_0代表原始签名人，$G_P = \{P_1, P_2, \cdots, P_n\}$为$n$成员的代理群。

2004-11-19 收到，2005-05-19 改回

(1)子密钥生成过程　代理群 $G_P=\{P_1,P_2,\cdots,P_n\}$ 应用Pedersen的秘密分享方案[8]产生每个代理人的子密钥和公共信息如下：

代理群的秘密多项式：

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1} \bmod q \tag{1}$$

每个代理签名人 $P_i\in G_P$ 的子密钥为：$s_i=f(i)=a_0+a_1i+\cdots+a_{i-1}i^{t-1} \bmod q$，其中 $a_i\in Z_q^*$ $(i=1,2\cdots,t-1)$；代理群的公共信息为：$y_G=g^{a_0} \bmod p$, $A_j=g^{a_j} \bmod p$, $j=1,2,\cdots,t-1$。

(2)签名权的委托过程　当原始签名人P_0同意将签名权委托给代理签名人时，原始签名人和每个代理签名人 $P_i\in G_P$ 一起完成以下步骤：

步骤 1　P_0选取随机数 $k\in Z_q^*$，计算 $K=g^k \bmod p$，$e=h(m_w\|K)$, $\sigma=ex_0+k \bmod q$。

步骤 2　P_0首先选择一个秘密多项式

$$f'(x)=\sigma+b_1x+\cdots+b_{t-1}x^{t-1} \bmod q \tag{2}$$

其中 $b_j\in Z_q^*$ $(j=1,2,\cdots,t-1)$，然后计算 $B_j=g^{b_j} \bmod p$ $(j=1,2,\cdots,t-1)$, $\sigma_i=f'(i)$ $(i=1,2,\cdots,n)$,最后秘密送 σ_i 给每个代理签名人 $P_i\in G_P$，公布 (B_j,m_w,K)。

步骤 3　每个 $P_i\in G_P$ 收到 σ_i 后，验证 $g^{\sigma_i}=y_0^{h(m_w\|k)}K\cdot\prod_{j=1}^{t-1}B_j^{i^j} \bmod p$。如果等式成立，每个 P_i 计算 $\sigma_i^{'}=\sigma_i+s_ih(m_w\|K) \bmod q$，$\sigma_i^{'}$ 为代理签名人的代理密钥。

(3)代理签名的产生　设 m 为待签名的消息，$G_t=\{P_1,P_2,\cdots,P_t\}$ 为 t 个代理签名人，他们将代表代理群对消息签名，代理签名产生如下：

步骤 1　$G_t=\{P_1,P_2,\cdots,P_t\}$ 应用Pedersen的秘密分享方案[8]产生每个代理人 $P_i\in G_t$ 的秘密影子和公共信息如下：

代理群 G_t 的秘密多项式：

$$f''(x)=c_0+c_1x+\cdots+c_{t-1}x^{t-1} \bmod q \tag{3}$$

其中 $c_i\in Z_q^*$ $(i=1,2,\cdots,t-1)$；

代理签名人 $P_i\in G_t$ 的秘密影子：$s_i'=f''(i)=c_0+c_1i+\cdots+c_{i-1}i^{t-1} \bmod q$；

公共信息为 $y=g^{c_0} \bmod p$, $C_j=g^{c_j} \bmod p$, $j=1,2,\cdots,t-1$。

步骤 2　每个 $P_i\in G_t$ 计算 $e'=h(y\|m)$, $\gamma_i=s_i'+\sigma_i'e' \bmod q$，秘密送 γ_i 给每个代理签名人 $P_i\in G_t(j=1,2,\cdots,t,\ j\neq i)$。

步骤 3　P_i 收到 $\gamma_i(j=1,2,\cdots,t,j\neq i)$ 后，P_i 验证每个 γ_i 的有效性，即

$$g^{\gamma_i}=\left(y\prod_{i=1}^{t-1}C_i^{j^i}\right)\cdot\left[y_0^{h(m_w\|K)}K\prod_{i=1}^{t-1}B_i^{j^i}\left(y_G\prod_{i=1}^{t-1}A_i^{j^i}\right)^{h(m_w\|K)}\right]^{h(y\|m)} \bmod p$$

如等式成立，γ_i 是有效的。

步骤 4　每个 $P_i\in G_t$ 利用 γ_i 和 Langrange 公式计算

$$T=c_0+\sigma e'=f''(0)+f'(0)e' \bmod q$$

则对消息 m 的代理签名为 (m,T,e',K,m_w)。

(4)代理签名的验证过程　收到代理签名 (m,T,e',K,m_w) 后，首先计算 $y'=g^T(y_0^{h(m_w\|K)}K)^{-e'} \bmod p$，然后验证 $e'=h(y'\|m)$，如等式成立，则代理签名 (m,T,e',K,m_w) 是有效。

2.2　Kim 等人方案的弱点

Kim 等人方案不能抵抗合谋攻击。任意 t 个恶意代理签名人，如 $S_T=\{P_1,P_2,\cdots,P_t\}$，工作在一起能重新构造代理群的秘密多项式 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1} \bmod q$ (见(1)式)。

t 个恶意代理签名人互相泄露他们的子密钥 s_i，并计算

$$f(x)=\sum_{i=1}^{t-1}s_i\prod_{j=1,j\neq i}^{t}\frac{0-j}{i-j} \bmod q$$

于是，这些恶意代理签名人就很容易地获得其他代理签名人的子密钥 $s_l(l\in G_P,l\in S_T)$。

同理，利用恶意代理签名人的代理密钥 $\sigma_i(i=1,2,\cdots,t)$ 和秘密参数 s_i'，他们也能重新构造代理群的秘密多项式 $f'(x)$ (见式 2)和 $f''(x)$ (见式 3)，从而得到其他代理签名人的秘密参数 $\sigma_j(\sigma_j=f'(j))$，$s_j'(s_j'=f''(j))$，$c_0(c_0=f''(0))$ 和原始签名人的委托签名 $\sigma(\sigma=f'(0))$。最终他们得到了其他代理签名人的代理密钥 $\sigma_j'=\sigma_j+s_jh(m_w\|K)$。

因此，这些恶意的代理签名人使用 $(\sigma,\sigma_j,s_j,s_j',c_0)$ 能伪造其他代理签名人的代理签名。

3　安全的门限代理签名方案

设系统有一个可信中心(TC)，TC负责选择系统参数和代理群的秘密参数。P_0为原始签名人，$G_P=\{P_1,P_2,\cdots,P_m\}$ 为m成员的代理群。在G_p中，有一个叫管理人(GP)，GP负责验证代理群成员的个人代理签名的有效性，并把这些有效的个人代理签名合成为代理签名，整个方案包括以下几个部分。

3.1　系统参数

令 $n=p_1p_2=(2qp_1'+1)(2qp_2'+1)$，其中 p_1,p_2,p_1',p_2',q 都为安全的大素数。阶为 q 的元素 g (即 $g^q=1 \bmod n$)。$\mathrm{ID}_o\in Z_q^*$ 为原始签名人P_o的身份标志，x_o 和 $y_o=g^{x_o} \bmod n$ 分别为P_o的私钥和公钥(y_o 由CA公证过)。设 d 是TC的私钥，e 是TC的公钥(e 由CA公证过)，这里 (e,d) 满足 $\gcd(e,\phi(n))=1$，$ed=1 \bmod \phi(n)$，$\phi(n)=(p_1-1)(p_2-1)$。$\mathrm{ID}_i\in Z_q^*$ 为每个代理签名人的身份标志。$h(\cdot)$ 为安全的单向Hash函数。m_w 是授权消息，主要包含原始签名人和代理签名人的身份，代理签名的范围等。

TC 首先选择秘密参数 k_G 作为代理群的私钥，计算 $y_G=g^{k_G} \bmod n$ 为代理群的公钥(y_G 由 CA 公证过)。然后选择秘密多项式:

$$f(x)=k_G+a_1x+\cdots+a_mx^m \bmod q \tag{4}$$

其中 $a_i\in Z_q^*$ $(i=1,2\cdots,m)$，并计算每个代理签名人 $(P_i\in G_P)$ 的子密钥 $z_i=f(\mathrm{ID}_i)$ $(i=1,2,\cdots,m)$ 和公共信息:

$$A_K = g^{a_i} \bmod n,\ (k=1,2,\cdots,m),$$
$$U_j = g^{f(w_j)L_j d} \bmod n,\ (j=1,2,\cdots,m+1-t) \tag{5}$$

其中 $L_j = \prod_{l=1,l\neq j}^{m+1-t} \frac{-w_l}{w_j - w_l}$，$(w_1, w_2, \cdots, w_m)$为 TC 选择的公共参数。

最后，TC 分别秘密送 z_i 给每个 $P_i \in G_P$，并公布所有 (A_k, U_j)。

3.3 代理权的委托过程

当原始签名人P_o同意将签名权委托给代理群时，原始签名人和代理群中的每个代理签名人 $P_i \in G_P$ 一起完成以下步骤：

(1)P_o选取随机数 $\varepsilon \in Z_q^*$，计算

$$\left.\begin{aligned} u &= g^{\varepsilon} \bmod n, \\ \sigma &= \varepsilon + x_o h(m_w \| u \| y_G \| y_o) \bmod q \end{aligned}\right\} \tag{6}$$

然后随机选择一个秘密多项式:

$$f'(x) = \sigma + c_1 x + \cdots + c_m x^m \bmod q \tag{7}$$

其中 $c_i \in Z_q^*$ $(i=1,2,\cdots,m)$，并计算

$$\left.\begin{aligned} b_i &= f'(\mathrm{ID}_i) \bmod q\ (i=1,2,\cdots,m), \\ C_k &= g^{c_k} \bmod n\ (k=1,2,\cdots,m) \\ B_j &= g^{f'(w_j)L_j} \bmod n\ (j=1,2,\cdots,m+1-t) \end{aligned}\right\} \tag{8}$$

最后，分别秘密送 b_i 给每个 $P_i \in G_P$，公布所有 (C_k, B_j, u, m_w)。

(2) 收到 b_i 后，每个 $P_i \in G_P$ 验证

$$g^{b_i} = u y_0^{h(m_w \| u \| y_G \| y_o)} \prod_{j=1}^{m} C_j^{\mathrm{ID}_i^j} \bmod n$$

如等式成立，P_i 计算 $\gamma_i = eb_i + z_i h(m_w \| u \| y_G \| y_o) \bmod q$ 作为他的代理子密钥。

3.4 代理签名的产生过程

设 $G_P = \{P_1, P_2, \cdots, P_m\}$ 中 t 个代理签名人 $G_t = \{P_1, P_2, \cdots, P_t\}$ 为消息 m 签名。代理签名产生过程如下：

(1)每个 $P_i \in G_t$ 选择随机数 $\beta_i, \delta_i \in Z_q^*$，计算 $r_i = g^{\beta_i} \delta_i^e \bmod n$，送 r_i 给代理群的管理人 GP。

(2) GP 收到所有的 r_i 后，计算

$$R = \prod_{i=1}^{t} r_i \bmod n \tag{9}$$

送 R 给每个 $P_i \in G_t$。

(3)每个 $P_i \in G_t$ 选择随机数 $\alpha \in Z_q^*$，计算

$$\left.\begin{aligned} V &= \left(\prod_{j=1}^{m+1-t} U_j^{L_j'}\right)^{h(m_w \| u \| y_G \| y_o)} \left(\prod_{j=1}^{m+1-t} B_j^{L_j'}\right) \bmod n \\ c &= h(R \| m) \\ s_{i1} &= \beta_i - \gamma_i L_i c + \alpha_i e \bmod q \\ s_{i2} &= \delta_i g^{-\alpha_i} V^{-c} \bmod n \end{aligned}\right\} \tag{10}$$

送 (s_{i1}, s_{i2}, c) 给 GP，其中 $L_i' = \prod_{l=1}^{t} \frac{\mathrm{ID}_l}{w_j - \mathrm{ID}_l}$，$L_i = \prod_{l=1,l\neq i}^{t} \frac{\mathrm{ID}_l}{\mathrm{ID}_i - \mathrm{ID}_l} \prod_{l=1}^{m+1-t} \frac{-w_l}{\mathrm{ID}_i - w_l}$。

(4)收到所有 (s_{i1}, s_{i2}, c) 后，GP 首先计算

$$V = \left(\prod_{j=1}^{m+1-t} U_j^{L_j'}\right)^{h(m_w \| u \| y_G \| y_o)} \left(\prod_{j=1}^{m+1-t} B_j^{L_j'}\right) \bmod n$$

然后验证

$$g^{s_{i1}} s_{i2}^e = r_i \left\{ \left[\left(u y_o^{h(m_w \| u \| y_G \| y_o)} \prod_{j=1}^{m} C_j^{\mathrm{ID}_i^j} \right)^e \cdot \left(y_G \prod_{j=1}^{m} A_j^{\mathrm{ID}_i^j} \right)^{h(m_w \| u \| y_G \| y_o)} \right]^{L_i} V^e \right\}^{-c} \bmod n \tag{11}$$

如果等式成立，GP 计算

$$\left.\begin{aligned} s_1 &= \sum_{i=1}^{t} s_{i1} \bmod q \\ s_2 &= \left(\prod_{i=1}^{t} s_{i2}\right) V^{c(t-1)} \bmod n \end{aligned}\right\} \tag{12}$$

则消息 m 的代理签名为 (s_1, s_2, c, u, m_w, m)。

3.5 代理签名的验证过程

当收到代理签名 (s_1, s_2, c, u, m_w, m) 时，签名接收者首先计算

$$R' = [(u y_o^{h(m_w \| u \| y_G \| y_o)})^e y_G^{h(m_w \| u \| y_G \| y_o)}]^c g^{s_1} s_2^e \bmod n \tag{13}$$

然后验证

$$c = h(R' \| m) \tag{14}$$

如等式成立，代理签名 (s_1, s_2, c, u, m_w, m) 有效。

3.6 收回代理签名权

如果原始签名人P_o需要收回代理签名人的代理签名权，则P_o送与P_i相对应的 g^{b_i} 给GP。当收到代理签名人的个人代理签名 $(s_{i1}, s_{i2}, c, u, r_i)$ 时，GP 首先判断等式

$$g^{s_{i1}} s_{i2}^e = r_i \left\{ \left[g^{eb_i} \left(y_G \prod_{j=1}^{m} A_j^{\mathrm{ID}_i^j} \right)^{h(m_w \| u \| y_G \| y_o)} \right]^{L_i} V^e \right\}^{-c} \bmod n$$

是否成立，如果等式成立，则P_i是P_o要收回代理权的代理签名人。因此，P_i的个人代理签名无效。于是原始签名人P_o就收回了他委托给代理签名人P_i的代理签名权。

3.7 安全性分析

(1) GP 通过验证式(11)是否成立来确认代理签名人的个人代理签名 (s_{i1}, s_{i2}) 是否有效。

证明 根据式(4) – 式(10)得

$$\begin{aligned} g^{s_{i1}} s_{i2}^e &= g^{\beta_i} g^{-\gamma_i L_i c} g^{\alpha_i e} \delta_i^e g^{-\alpha_i e} V^{-ec} \\ &= r_i (g^{eb_i} g^{z_i h(m_w \| u \| y_G \| y_o)})^{-L_i c} V^{-ec} \\ &= r_i \left\{ \left[\left(u y_o^{h(m_w \| u \| y_G \| y_o)} \prod_{j=1}^{m} C_j^{\mathrm{ID}_i^j} \right)^e \cdot \left(y_G \prod_{j=1}^{m} A_j^{\mathrm{ID}_i^j} \right)^{h(m_w \| u \| y_G \| y_o)} \right]^{L_i} V^e \right\}^{-c} \bmod n \end{aligned}$$

Q.E.D

(2) 签名验证人通过验证式(14)是否成立来确认门限代理签名是否有效。

证明　令 $h=h(m_w\|u\|y_G\|y_o)$。根据式(5)，式(8)，式(9)，式(12),(13)和 $L_j=\prod_{l=1,l\neq j}^{m+1-t}\frac{-w_l}{w_j-w_l}$，$L_i=\prod_{l=1,l\neq i}^{t}\frac{\mathrm{ID}_l}{\mathrm{ID}_i-\mathrm{ID}_l}\cdot\prod_{l=1}^{m+1-t}\frac{-w_l}{\mathrm{ID}_i-w_l}$，$L_i'=\prod_{l=1}^{t}\frac{\mathrm{ID}_l}{w_j-\mathrm{ID}_l}$ 得

$$\begin{aligned}
R'&=[(uy_o^h)^e y_G^h]^c g^{\sum_{i=1}^t s_{i1}}\left(\prod_{i=1}^t s_{i2}^e\right)V^{c(t-1)e}\\
&=[(uy_o^h)^e y_G^h]^c\left(\prod_{i=1}^t g^{\beta_i\delta_i^e}\right)g^{-\sum_{i=1}^t\gamma_i L_i c}V^{-ce}\\
&=[(uy_o^h)^e y_G^h]^c Rg^{-\sum_{i=1}^t(eb_i L_i c+z_i hL_i c)}V^{-ce}\\
&=[(uy_o^h)^e y_G^h]^c Rg^{-\sum_{i=1}^t f'(\mathrm{ID}_i)L_i ce}g^{-\sum_{i=1}^t f(\mathrm{ID}_i)L_i ch}\\
&\cdot\left(\prod_{j=1}^{m+1-t}U_j^{L_j'}\right)^{-hce}\left(\prod_{j=1}^{m+1-t}B_j^{L_j'}\right)^{-ce}\\
&=[(uy_o^h)^e y_G^h]^c R\left(g^{\sum_{i=1}^t f'(\mathrm{ID}_i)L_i+\sum_{j=1}^{m+1-t}f'(w_j)L_jL_j'}\right)^{-ce}\\
&\cdot\left(g^{\sum_{i=1}^t f(\mathrm{ID}_i)L_i+\sum_{j=1}^{m+1-t}f(w_j)L_jL_j'}\right)^{-ch}\\
&=[(uy_o^h)^e y_G^h]^c R[(uy_o^h)^e y_G^h]^{-c}\\
&=R \bmod n
\end{aligned}$$

又根据式(10)和上述方程，我们有

$$c=h(R\|m)=h(R'\|m)\qquad \text{Q.E.D}$$

(3)原始签名人不能伪造门限代理签名。因为原始签名人不知道代理签名人的秘密参数 z_i，而 z_i 是由代理群的秘密参数 k_G (见式(4))和 $z_i=f(\mathrm{ID}_i)$ 确定的，并且在验证门限代理签名时需要 $y_G=g^{k_G} \bmod n$。同理，因为不知道代理群的秘密参数 b_i，GP 也不能伪造门限代理签名。b_i 取决于原始签名人的秘密参数 x_o (见式(6)－式(8))，验证门限代理签名时需要 $y_o=g^{x_o} \bmod n$。

(4) 合谋攻击。致使 G_P 中 m 个恶意群成员合谋，他们也不能重新构造代理群的秘密多项式函数 $f(x)$。因为要构造 m 阶的多项式，就必须有 $m+1$ 秘密参数 $z_i=f(\mathrm{ID}_i)$，然而 m 个恶意代理群成员合谋也只有 m 个秘密参数 $z_i=f(\mathrm{ID}_i)$，所以他们也不能重新构造代理群的秘密多项式函数 $f(x)$。如恶意群成员企图从 $U_j=g^{f(w_j)L_j d} \bmod n$ 求 $f(w_j)$，则这是解离散对数的问题。

同理，恶意的代理签名人也不能构造秘密多项式 $f'(x)$ 和 $f''(x)$。因此，本方案能抵抗合谋攻击，克服了文献[1－7]方案中的缺点。

(5)本方案能抵抗伪造攻击。从 3.5 节知，门限代理签名的验证方程为

$$R'=[(uy_o^{h(m_w\|u\|y_G\|y_o)})^e y_G^{h(m_w\|u\|y_G\|y_o)}]^c g^{s_1}s_2^e \bmod n$$

令 $F_s=uy_o^{h(m_w\|u\|y_G\|y_o)}$，$F_p=y_G^{h(m_w\|u\|y_G\|y_o)}$，把上式重写为

$$R'=(F_s^e F_p)^{-h(R\|m)}g^{s_1}s_2^e \bmod n \qquad (15)$$

显然，F_s 取决于参数 (u,m_w,y_G,y_o)，F_p 取决于参数 (u,m_w,y_o)，(y_G,y_o) 是由CA 公证过的。假定 (s_1,R,m,F_s,F_p)，如不知道密钥 d，那么是很难找到一个满足式(15)的 s_2。如假定 (s_2,R,m,F_s,F_p)，则在离散对数问题的假设下，也无法找出 s_1 能满足式(15)。又如假定 (s_2,s_1,m,F_s,F_p)，则在安全的单向Hash函数的假设下，也不能找到一个R满足式(15)。如给定 (u,m_w)，我们就能计算满足式(15)的F_s和F_p，然而在离散对数的问题和单向Hash函数的假设下，是无法找到一个 (u,m_w) 能满足式 $F_s=uy_o^{h(m_w\|u\|y_G\|y_o)}$ 和 $F_p=y_G^{h(m_w\|u\|y_G\|y_o)}$ 的。

(6)未被委托的群体是不能假冒一个合法的代理群产生有效的门限代理签名。因为，未被委托的群体不知道代理群的秘密参数 k_G。k_G 是由 TC 秘密选择的，而验证代理签名时需要 $y_G=g^{k_G} \bmod n$ (y_G 是 CA 验证过的)。另外，原始签名人需要对 y_G 进行签名(见式(6))。

4　结束语

本文指出了 Kim 等人方案的不安全因素，即遭受合谋攻击。基于离散对数和大数分解的困难性，构造了一个能抵抗合谋攻击的安全门限代理签名方案。同时也分析了一切可能的攻击，得到了在离散对数和大数分解困难性的假设下，本方案是安全的结论。另外，方案还具有在原始签名人需要时，可收回代理签名权的特性。

参 考 文 献

[1] Kim S, Park S, Won D. Proxy signature, revisited. ICICS'97, Lecture Notes in Computer Science, Springer,Berlin,1997, 1334: 223－232.

[2] Zhang K. Threshold proxy signature scheme. 1997 Information Security Workshop, Tokyo, Japan, September, 1997: 191－197.

[3] Sun H M. An efficient nonrepudiable threshold proxy signature scheme with known signers. *Computer Communication.*1997, 22 (8):717－722.

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

[5] Sun, H M Lee, N Y Hwang. T. Threshold proxy signatures. *IEE Proc- Computers and Digital Techniques*, 1999, 146(5): 259－263.

[6] 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 (9): 119－124.

[7] Lee N Y, Hwang T, Wang C H. On Zhang's nonrepudiable proxy signatures. ACISP'98, Lecture Notes in Computer Science, Springer, Berlin, 1998: 414－422.

[8] Pedersen. Distributed provers with applications to undeniable signatures. Proc. Eurocrypt'91, Lecture Notes in Computer Science, Sprinter, Berlin, 1991, 547: 221－238.

王晓明:　女, 1960 年生, 教授, 研究方向为信息安全、 密码学、计算机网络安全等.

张　震:　男，1975 年生, 助教, 研究方向为信息安全、计算机网络等.

符方伟:　男，1963 年生, 教授, 研究方向为信息安全、密码学等.