指定验证人的(*t*,*n*)门限代理签名方案*

王晓明[1+], 符方伟[2]

[1](暨南大学 计算机系,广东 广州 510632)

[2](南开大学 数学科学学院,天津 300071)

A (*t*,*n*) Threshold Proxy Signature Scheme with Specified Verifiers

WANG Xiao-Ming[1+], FU Fang-Wei[2]

[1](Department of Computer, Ji'nan University, Guangzhou 510632, China)

[2](School of Mathematics Science, Nankai University, Tianjin 300071, China)

+ Corresponding author: Phn: +86-20-85220781, Fax: +86-20-85228335, E-mail: wxmsq@eyou.com, http://www.jnu.edu.cn

Received 2003-09-26;Accepted 2004-01-06

Wang XM, Fu FW. A (*t*,*n*) threshold proxy signature scheme with specified verifiers. *Journal of Software*, 2005,16(6):1190−1196. DOI: 10.1360/jos161190

Abstract: The concept of specified verifiers is first introduced into the threshold proxy signature, and a (*t*,*n*) threshold proxy signature scheme with the specified verifiers is proposed. In the proposed scheme, any t or more proxy signers can sign a message on behalf of an original signer for the specified verifiers, and only the specified verifiers together are able to verify the validity of the proxy signature. In ordinary (*t*,*n*) proxy threshold signature schemes, anyone can verify the validity of the proxy signature. In some applications, however, it is required that a proxy signature could be verified only by the specified verifiers together, that is, no a verifier can gain an advantage of the knowledge of the validity of the proxy signature before the other verifiers know its validity (e.g. tenders, bits). Furthermore, the proposed scheme can also revoke the proxy signature right of the proxy signers delegated by the original signer if original signer needs.

Keywords: digital signature; threshold proxy signature; signature for specified verifiers

摘要: 将指定验证人概念引入门限代理签名,提出了一个指定验证人的(*t*,*n*)门限代理签名方案.该方案不仅实现了门限代理签名,而且还能实现只有指定验证人一起才能验证门限代理签名的特性.在普通的门限代理签名方案中,任何人都能验证门限代理签名的有效性.然而,在某些情况下,只希望指定的验证人一起才能验证门限代理签名.这在实际中是需要的,如电子商务中的电子投标等.另外,该方案还具有在原始签名人需要时,收回某个代理签名人代理权的特性.

关键词: 数字签名;门限代理签名;指定验证人签名

* Supported by the National Natural Science Foundation of China under Grant No.60172060 (国家自然科学基金); the Natural Science Foundation of Guangdong Province of China (广州省自然科学基金); the Natural Science Foundation of Ji'nan University of China (暨南大学自然科学基金)

作者简介: **王晓明**(1960－),女,重庆人,博士,教授,主要研究领域为计算机网络安全,现代密码学;**符方伟**(1963－),男,教授,博士生导师,主要研究领域为信息论,计算机网络安全,现代密码学,编码理论.

中图法分类号: TP309 文献标识码:A

在代理签名方案中引入秘密分存就形成了门限代理签名方案.(*t*,*n*)门限代理签名就是将一个代理签名密钥分成 *n* 份子代理签名密钥,*n* 个代理签名人分别拥有各自的子代理密钥.各代理签名人利用自己的分存子代理密钥所签署的签名叫做部分代理签名.当部分代理签名的个数大于或等于 *t* 时,这些部分代理签名按着某种方式结合,产生了有效的门限代理签名.门限代理签名的目的是当原始签名人因公务或身体健康等原因不能行使签名权利时,将签名权委托给其他人替自己行使签名权.门限代理签名在许多领域都有重要的应用,如电子商务中 CA 证书的签发,电子支票的分发等.在普通的门限代理签名方案[1−5]中,任何人都能验证门限代理签名的有效性.然而,在某些情况下,并不希望任何人都能验证门限代理签名,而只有指定的验证人一起才能验证门限代理签名.这在实际中是需要的,如电子商务中的电子投标等.1996 年,Laih 等人提出了指定验证人的多重数字签名方案[6],实现了只有指定验证人一起才能验证多重数字签名的特性.然而,文献[7]指出 Laih 的方案是不安全的,即验证群中的特别验证者 Clerk 能单独验证多重数字签名.

针对如何将指定验证人这一概念引入门限代理签名中,如何克服 Laih 等人方案中的 Clerk 能单独验证多重数字签名的缺点.针对这些问题,本文提出了一个指定验证人的门限代理签名方案.该方案不仅实现了代理签名,指定验证人一起才能验证门限代理签名的特性,而且克服了 Laih 等人的指定验证人的多重数字签名方案中的 Clerk 能单独验证多重数字签名的缺点.另外,已有的代理签名方案不具有收回代理权的特性.本方案能在原始签名人需要时,收回给某个代理签名人的代理权.

1 Laih 等人的方案[6]

1.1 密钥产生阶段

设 $G_s=\{U_{s1},U_{s2},\ldots,U_{sn}\}$ 为有 n 签名人的群,$G_v=\{U_{v1},U_{v2},\ldots,U_{vm}\}$ 为有 m 验证人的群.在每个群里都有一个特别成员(clerk),G_s 的 Clerk 为 U_{sc},G_v 的 Clerk 为 U_{vc}.可信中心选择两个大素数 p 和 q,且 $q|(p-1)$,一个阶为 q 的生成元 $g\in Z_p$.每个 $U_{si}\in G_s$ 的私钥为 $s_i\in Z_q^*$,公钥为 $Y_{si}=g^{-s_i} \bmod p$.每个 $U_{vj}\in G_v$ 的私钥为 $v_j\in Z_q^*$,公钥为 $Y_{vj}=g^{-v_j} \bmod p$,G_s 的公钥为 $Y'_s=\prod_{i=1}^{n} g^{-s_i} \bmod p$,G_v 的公钥为 $Y'_v=\prod_{j=1}^{m} g^{-v_j} \bmod p$.

1.2 多重数字签名的产生

设待签名消息为 m,为了完成对 m 的签名,群 G_s 中所有签名人需要执行以下步骤:

(1) 每个 $U_{si}\in G_s$ 选择一个随机数 $1<r_i<q$,计算 $x_i=(Y'_v)^{r_i} \bmod p$,并送 x_i 给 U_{sc}.

(2) U_{sc} 计算 $x=\prod_{i=1}^{n} x_i \bmod p$,并对 G_s 中所有签名人广播 x.

(3) 每个 U_{si} 计算 $e=h(x\,\|\,m)$ 和 $w_i=r_i+es_i \bmod q$,然后送 w_i 给 U_{sc}.

(4) 收到所有 $w_i(i=1,2,\ldots,n)$后,U_{sc} 计算 $e=h(x\,\|\,m)$ 和 $w=\prod_{i=1}^{n} w_i \bmod q$,则多重数字签名为(e,w,m).

1.3 多重数字签名的验证

为了完成对多重数字签名(e,w,m)的验证,G_v 中所有验证人一起完成以下步骤:

(1) 每个 $U_{vj}\in G_v$ 计算

$$x_j=[g^w(Y'_s)^e]^{-v_j} \bmod p \tag{1}$$

并送 x_j 给 U_{vc}.

(2) U_{vc} 计算

$$x=\prod_{j=1}^{m} x_j \bmod p \tag{2}$$

并对 G_v 的所有验证人广播 x.

(3) 每个 U_{vj} 验证 $e=h(x \| m)$,如等式成立,则(e,w,m)是有效的多重数字签名.

2 文献[7]对 Laih 等人方案的攻击

文献[7]指出,Laih 等人的方案是不安全的,因为验证群 G_v 的 CLerk 能单独验证多重数字签名.由式(1)和式(2)得

$$\left.\begin{aligned} x=\prod_{j=1}^{m}[g^{w}(Y_s')^{e}]^{-v_j}=(Y_v')^{w}(Y_s')^{-e\sum_{j=1}^{m}v_j} \bmod p \\ (Y_s')^{-\sum_{j=1}^{m}v_j}=[x(Y_v')^{-w}]^{e^{-1}} \bmod p \end{aligned}\right\} \tag{3}$$

如 U_{vc} 曾协助 G_v 验证过一次签名(e,w),则他就拥有 x,那么 U_{vc} 就能利用式(3)计算出 $(Y_s')^{-\sum_{j=1}^{m}v_j}$,从此他就能单独验证所有 G_s 的签名了.例如,现有一个 G_s 对信息 $\tilde{m}$ 的签名$(\tilde{e},\tilde{w})$,U_{vc} 首先计算 $\tilde{x}=(Y_v')^{\tilde{w}}\{[x(Y_v')^{-w}]^{e^{-1}}\}^{\tilde{e}} \bmod p$,然后验证 $\tilde{e}=h(\tilde{x} \| \tilde{m})$.若等式成立,则签名$(\tilde{e},\tilde{w})$有效.因此,$U_{vc}$ 能单独验证多重数字签名.

3 本文提出的指定验证人的(t,n)门限代理签名方案

设 u_o 是一个原始签名人,$G_p=\{u_{p1},u_{p2},\ldots,u_{pn}\}$为有 n 代理签名人的群,$G_v=\{u_{v1},u_{v2},\ldots,u_{vm}\}$为指定验证人的群.在每个群里都有一个管理人,群 G_p 的管理人为 GP,主要负责系统的初始化,验证部分代理签名,结合部分代理签名产生代理签名.群 G_v 的管理人为 GV,主要帮助指定验证人验证代理签名.另外,假定 $P=\{u_{p1},u_{p2},\ldots,u_{pt}\}(t\le n)$代表 G_s 对信息 M 进行签名.

3.1 初始化

系统初始化需要以下几个步骤:

(1) GP 首先选择两个大素数 p 和 q,且 $q \mid (p-1)$,一个阶为 q 的元素 g(即 $g^q=1 \bmod p$),一个安全的单向 Hash 函数 h,然后公布 p,q,g,h.

(2) 原始签名人 u_o,代理签名人 u_{pi} 和指定验证人 u_{vj} 的密钥分别是 $\rho_o,k_i,v_j \in Z_q^*$ $(i=1,2,\ldots,n,j=1,2,\ldots,m)$,公钥为 $Y_o=g^{\rho_o} \bmod p$, $y_i=g^{k_i} \bmod p$ $(i=1,2,\ldots,n)$, $y_{vj}=g^{v_j} \bmod p$ $(j=1,2,\ldots,m)$, 公钥都经过 CA(certificate authority)验证过.

(3) $ID_i(i=1,2,\ldots,n)$为代理签名人 u_{pi} 的身份标识.

(4) 代理群 G_p 的密钥是 $k_G \in Z_q^*$,公钥为 $Y_G=g^{k_G} \bmod p$,指定验证群 G_v 的公钥为 $Y_v=\prod_{j=1}^{m}y_{vj} \bmod p$.

3.2 分存秘密的生成

GP 首先选择一个随机多项式

$$f(x)=k_G+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1} \bmod q \tag{4}$$

其中 $a_i \in Z_q^*$ $(i=1,2,\ldots,t-1)$为随机整数,然后计算

$$z_i=f(ID_i) \bmod q, \quad i=1,2,\ldots,n \tag{5}$$

和相应的参数

$$u_i=g^{z_i} \bmod p, \quad i=1,2,\ldots,n \tag{6}$$

$$w_i=z_i y_i^{k_G} \bmod p, \quad i=1,2,\ldots,n \tag{7}$$

最后,送 w_i 给 u_{pi},并公布 $u_i(i=1,2,\ldots,n)$.

3.3 代理密钥的生成

原始签名人 u_o 委托他的签名权给代理签名人(i=1,2,…,n),u_o 和每个 u_{pi} 需要完成以下步骤:

(1) u_o 首先选择一个随机整数 $\alpha \in Z_q^*$,计算

$$A = g^{\alpha} \mod p \tag{8}$$

$$c = \alpha + \rho_o h(m_w \| A) \mod q \tag{9}$$

其中 m_w 是一个含有门限值、委托签名的有效期、原始签名人和代理签名人身份标志的委托证书.

然后,再选择一个随机多项式

$$f'(x) = c + c_1 x + c_2 x^2 + ... + c_{t-1} x^{t-1} \mod q \tag{10}$$

其中 $c_i \in Z_q^*$ (i=1,2,…,t–1)为随机整数,计算

$$b_i = f'(ID_i) \mod q, \quad i = 1,2,...,n \tag{11}$$

$$D_i = b_i y_i^{\rho_o} \mod p, \quad i = 1,2,...,n \tag{12}$$

最后,送 D_i 给 u_{pi},并公布 $[m_w, A, C_j = g^{c_j} \mod p\ (j = 1,2,...,t-1)$.

(2) 收到 D_i 后,u_{pi} 首先计算

$$z_i = w_i Y_G^{-k_i} \mod p,$$

$$b_i = D_i Y_o^{-k_i} \mod p,$$

然后验证

$$u_i = g^{z_i} \mod p \tag{13}$$

$$g^{b_i} = A Y_o^{h(m_w \| A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} \mod p \tag{14}$$

如果式(13)、式(14)成立,则 u_{pi} 计算

$$\gamma_i = b_i + z_i h(m_w \| A) \mod q \tag{15}$$

作为他的代理密钥.

3.4 代理签名的生成

若代理签名 G_p 中的任意 t 个代理签名人代表原始签名人对信息 M 进行签名,则每个代理签名人 $u_{pi} \in P$ 需要完成以下步骤:

(1) 每个 $u_{pi} \in P$ 选择随机数 $\beta_i, \delta_i \in Z_q^*$,计算

$$d_{i1} = g^{\beta_i} \mod p \tag{16}$$

$$d_{i2} = g^{\delta_i} \mod p \tag{17}$$

$$d_{i3} = Y_v^{\beta_i d_{i2} d_{i1}^{-1} + \delta_i} \mod p \tag{18}$$

送(ID_i,d_{i1},d_{i2},d_{i3})给 GP.

(2) 收到所有(ID_i,d_{i1},d_{i2},d_{i3})(i=1,2,…,t)后,GP 计算

$$R = \prod_{i=1}^{t} d_{i3}^{d_{i1}} \mod p \tag{19}$$

$$\widetilde{S} = \prod_{i=1}^{t} d_{i2}^{d_{i1}} \mod p \tag{20}$$

送 $(R, \widetilde{S})$ 给 P 中的每个代理签名人.

(3) 收到 $(R, \widetilde{S})$ 后,每个 $u_{pi} \in P$ 计算

$$e = h(R \| \widetilde{S} \| M \| PSID) \tag{21}$$

$$s_i = \beta_i d_{i2} + (L_i \gamma_i + k_i) e \mod q \tag{22}$$

送 s_i 给 GP.其中 $L_i = \prod_{j=1, j\neq i}^{t} -ID_j (ID_i - ID_j)^{-1} \mod q$,$PSID$ 是所有代理签名人的身份标志的连接.

(4) GP 计算 $e = h(R \| \widetilde{S} \| M \| PSID)$,验证

$$g^{s_i} = d_{i1}^{d_{i2}} \{[A(Y_o u_i)^{h(m_w \| A)} \prod_{j=1}^{t-1} C_j^{ID_i^j}]^{L_i} y_i\}^e \mod p \tag{23}$$

若式(23)成立,则(s_i,d_{i1},d_{i2},d_{i3})是有效的部分代理签名,GP 计算

$$S = \sum_{i=1}^{t} s_i \mod q \tag{24}$$

则信息 M 的代理签名是 $(S, \widetilde{S}, e, A, m_w, PSID)$.

3.5 代理签名的验证

为了验证信息 M 的代理签名,验证群中所有指定验证人一起完成以下步骤:

(1) 每个 $u_{vj} \in G_v$,计算

$$R_j = \{\widetilde{S} g^S [A(Y_o Y_G)^{h(m_w \| A)} \prod_{i=1}^{t} y_i]^{-e}\}^{v_j} \mod p \tag{25}$$

送 R_j 给 GV.

(2) 收到所有 R_j(j=1,2,…,m),GV 计算

$$R' = \prod_{j=1}^{m} R_j \mod p \tag{26}$$

送 R'给验证群 G_v 中的每个验证人.

(3) 每个 $u_{vj} \in G_v$ 验证

$$e = h(R' \| \widetilde{S} \| M \| PSID) \tag{27}$$

如果式(27)成立,则信息 M 的代理签名是有效的.

3.6 收回代理签名权

如果原始签名人想收回代理签名人 $u_{pi} \in G_p$ 的代理签名权,则送与 u_{pi} 对应的 g^{b_i} 给 GP.

当收到每个代理签名人的部分代理签名(ID_i,d_{i1},d_{i2},d_{i3}),GP 首先取出 g^{b_i} ,然后验证

$$g^{b_i} = A Y_o^{h(m_w \| A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} \mod p \tag{28}$$

如果式(28)成立,则 u_{pi} 是一个被收回代理签名权的代理签名人,因此,u_{pi} 的部分代理签名无效.于是,u_{pi} 的代理权就被收回.

3.7 方案性能的分析

(1) 代理签名人通过验证式(14)是否成立来确认 b_i 的有效性.

证明:根据式(8)~式(11),得到

$$g^{b_i} = g^{f'(ID_i)} = g^c g^{c_1 ID_i + \ldots + c_{t-1} ID_i^{t-1}} = g^\alpha g^{\rho_o h(m_w \| A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} = A Y_o^{h(m_w \| A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} \mod p .$$

(2) GP 能通过验证式(23)是否成立来确认部分代理签名 s_i 的有效性.

证明:根据式(6)、式(14)~式(16)和式(22)得

$$g^{s_i} = g^{\beta_i d_{i2}} g^{(L_i \gamma_i + k_i)e} = d_{i1}^{d_{i2}} g^{[(b_i + z_i h(m_w \| A)) L_i + k_i]e} = d_{i1}^{d_{i2}} \left\{ \left[A(Y_o u_i)^{h(m_w \| A)} \prod_{j=1}^{t-1} C_j^{ID_i^j} \right]^{L_i} y_i \right\}^e \mod p .$$

(3) 签名验证人通过验证式(27)是否成立来确认代理签名的有效性.

证明:根据式(4)、式(5)、式(8)、式(10)、式(11)、式(15)和式(22),得

$$S=\sum_{i=1}^{t}s_i=\sum_{i=1}^{t}\{\beta_i d_{i2}+[L_i(b_i+z_i h(m_w\|A)+k_i]e\}=\left[\sum_{i=1}^{t}\beta_i d_{i2}\right]+\left[c+k_G h(m_w\|A)+\sum_{i=1}^{t}k_i\right]e \mod q,$$

$$g^S=\left(g^{\sum_{i=1}^{t}\beta_i d_{i2}}\right)\left[A(Y_oY_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i\right]^e \mod p,$$

$$\prod_{i=1}^{t}g^{\beta_i d_{i2}}=g^S\left[A(Y_oY_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i\right]^{-e} \mod p,$$

根据式(17)~式(20)、式(25)、式(26)和上式得

$$R'=\prod_{j=1}^{m}R_j=\prod_{j=1}^{m}\{\widetilde{S}g^S[A(Y_oY_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i]^{-e}\}^{v_j}=\prod_{j=1}^{m}(\prod_{i=1}^{t}d_{i2}^{d_{i1}}\prod_{i=1}^{t}g^{\beta_i d_{i2}})^{v_j}=\prod_{j=1}^{m}(\prod_{i=1}^{t}g^{\delta_i d_{i1}}\prod_{i=1}^{t}g^{\beta_i d_{i2}})^{v_j}$$

$$=\prod_{i=1}^{t}(\prod_{j=1}^{m}y_{v_j}^{\delta_i d_{i1}}y_{v_j}^{\beta_i d_{i2}})=\prod_{i=1}^{t}Y_v^{(\delta_i+\beta_i d_{i2}d_{i1}^{-1})d_{i1}}=\prod_{i=1}^{t}d_{i3}^{d_{i1}}=R \mod p.$$

根据式(21)和上式得 $e=h(R\|\widetilde{S}\|M\|PSID)=(R'\|\widetilde{S}\|M\|PSID)$.

(4) 原始签名人不能伪造代理签名.

因为原始签名人无法获得代理签名人的密钥 k_i 和秘密参数 z_i.因此,原始签名人不能伪造代理签名.

(5) 本方案能抵抗伪造攻击.

根据式(19)、式(28)得

$$g^S=\prod_{i=1}^{t}d_{i1}^{d_{i2}}\left[A(Y_oY_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i\right]^{h\left(\prod_{i=1}^{t}d_{i3}^{d_{i1}}\|\widetilde{S}\|M\|PSID\right)} \mod p.$$

令 $Y_P=A(Y_oY_G)^{h(m_w\|A)} \mod p$,则上式可以写为

$$g^S=\prod_{i=1}^{t}d_{i1}^{d_{i2}}\left(Y_P\prod_{i=1}^{t}y_i\right)^{h\left(\prod_{i=1}^{t}d_{i3}^{d_{i1}}\|\widetilde{S}\|M\|PSID\right)} \mod p.$$

假定 $M,PSID,Y_P,d_{i2},d_{i3},\widetilde{S}$ 在离散对数的问题(DLP)和单向 Hash 函数的假设下,无法找出一对(S,d_{i1})满足上式;若假定 $M,PSID,d_{i1},d_{i2},d_{i3},S,\widetilde{S}$,则能找出一个 Y_p 满足上式,然而无法找出 (m_w,A) 使 $Y_P=A(Y_oY_G)^{h(m_w\|A)} \mod p$ 成立.

根据式(25)、式(26)得, $R=R'=\prod_{j=1}^{m}R_j=\prod_{j=1}^{m}\left\{\widetilde{S}g^S\left[A(Y_oY_G)^{h(m_w\|A)}\prod_{i=1}^{t}y_i\right]^{-h(R\|\widetilde{S}\|M\|PSID)}\right\}^{v_j} \mod p$.即使知道 $\sum_{j=1}^{t}v_j$,又知道 M,m_w,A,则在 DLP 和单向 Hash 函数的假定下,也无法找出满足上式的($R,S,\widetilde{S}$),而且从 $y_{v_j}=g^{v_j} \mod p$ 得到 v_j 是离散对数的问题.因此提出的方案能抵抗伪造攻击.

(6) 本方案能抵抗合谋攻击.

代理签名群 G_p 中 t 个恶意代理签名人可能把他们的 z_i 和 b_i 发送给攻击者 U,企图进行合谋攻击.虽然,U 已有 t 个代理签名人的秘密参数 z_i 和 b_i,他能重新构造多项式函数 $f(x),f(x)'$,恢复系统秘密参数 k_G 和 c,于是他就能获得其他代理签名人 u_{pj} 的秘密参数 z_j 和 b_j,也就是说,他能计算出其他人的代理密钥 γ_i,但是他不能冒充其他代理签名人 u_{pj} 产生有效的代理签名.因为他不知道其他代理人 u_{pj} 的密钥 k_j,而在代理签名时要用到 k_j(见式(22)),即在验证代理签名时,必须用代理签名人的公钥 y_j(见式(25)~式(27)),否则,代理签名无效.如果攻击者 U 获得其他代理签名人 u_{pk} 的秘密参数 z_k 和 b_k 后,企图利用自己的私钥 k_t 进行代理签名,那么在验证代理签名时,必须用攻击者 U 的公钥 y_t 来验证,否则验证方程是不成立的.然而,原始签名人在委托他的代理签名权时,已经说明了哪些人拥有代理签名权(见代理密钥生成部分中的 m_w),并且在验证部分代理签名有效性时,要用到代理签名人的身份标志 ID_i 及与 ID_i 相对应的公钥 y_i(见式(23)),而攻击者 U 无法更改 m_w 和 ID_i.那么验证时也就不能用攻击者 U 的公钥 y_t,从而攻击者 U 伪造的代理签名无法通过验证方程(式(23)),因此伪造的代理签名无效.若攻击者

企图根据 $s_j=\beta_j d_{j1}+(L_j\gamma_j+k_j)e \bmod q$ 求出 k_j,但因不知道随机数β_j,而无法求出 k_j.所以,攻击者不能假冒别人产生有效的代理签名.因此,本方案能抵抗合谋攻击.

(7) 验证群中的管理人和验证人都不能单独验证代理签名.

根据式(25)、式(26)得

$$R' = Y_v^S \tilde{S}^{\sum_{j=1}^{m} v_j} \{[A(Y_o Y_G)^{h(m_w \| A)} \prod_{i=1}^{t} y_i]^{-e}\}^{\sum_{j=1}^{m} v_j} \bmod p \tag{29}$$

假定 $e,S,\tilde{S},m_w,A$,如果又能知道 $\tilde{S}^{\sum_{j=1}^{m} v_j}$ 和 $\left\{\left[A(Y_o Y_G)^{h(m_w \| A)} \prod_{i=1}^{t} y_i\right]^{-e}\right\}^{\sum_{j=1}^{m} v_j}$,就能计算出 R',从而能够单独验证代理签名,然而 v_j 是每个指定验证人的密钥,从 $y_{vj} = g^{v_j} \bmod p$ 求 v_j 是离散对数的问题.因此,任何其他人无法知道 v_j.另外,根据式(17),式(20)和式(29)可以写为

$$\left[A(Y_o Y_G)^{h(m_w \| A)} \prod_{i=1}^{t} y_i\right]^{\sum_{j=1}^{m} v_j} = \left[(R')^{-1} Y_v^S Y_v^{\sum_{i=1}^{t} \delta_i d_{i1}}\right]^{e^{-1}} \bmod p.$$

若知道 $Y_v^{\sum_{i=1}^{t} \delta_i d_{i1}}$ 和 R',则能计算出 $\left[A(Y_o Y_G)^{h(m_w \| A)} \prod_{i=1}^{t} y_i\right]^{\sum_{j=1}^{m} v_j}$.然而, δ_i 是由代理签名人 u_{pi} 选的随机数,所以任何人都不能计算出 $Y_v^{\sum_{i=1}^{t} \delta_i d_{i1}}$.因此,指定验证人和 GV 都不能单独验证代理签名.

(8) 本方案不需要安全信道.

建立一个安全信道是很昂贵的,有时也是很困难的.在本方案中,因为每个代理签名人只要用他的密钥就能计算出所需秘密参数.因此,不需要安全信道.

4 结束语

提出一个(*t*,*n*)门限代理签名方案,实现了指定验证人一起才能验证门限代理签名的特性.任何指定验证人和验证群中的管理人 GV 都不能单独验证门限代理签名.在离散对数的问题和单向 Hash 函数的假定下,分析了各种可能的攻击,得出了本方案是安全的结论.另外,本方案还具有收回代理签名权的特性,这是很多代理签名方案都不具备的特性.

References:

[1] Hwang MS, Lu JL, Lin IC. 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.

[2] Sun HM. An efficient nonrepudiable threshold proxy signature scheme with known signers. Computer signature scheme with known signers. Computer Communications, 1999,22(8):712−722.

[3] Hsu CL, Wu TS, Wu TC. Improvements of generalization of threshold signature and authenticated encryption for group communications. Information Processing Letters, 2002,81:41−45.

[4] Hsu CL, Wu TS, Wu TC. New nonrepudiable threshold proxy signature scheme with known signers. The Journal of Systems and Software, 2001,58:119−124.

[5] Zhang K. Threshold proxy signature schemes. In: Information Security Workshop (ISW'97). LNCS 1396, Berlin: Springer-Verlag. 1997. 191−197.

[6] Laih CS, Yen SM. Multisignature for specified group of verifiers. Journal of Information Science and Engineering, 1996,12(1): 282−292.

[7] WH H. Weakness in some multisignature schemes for specified group of verifiers. Information Processing Letters, 2002,83(2):95−99.