

文章编号:1001-9081(2007)05-1058-04

## 基于身份的指定验证人的门限代理签名方案

徐丽娟<sup>1</sup>, 徐秋亮<sup>1</sup>, 郑志华<sup>2</sup>

(1. 山东大学 计算机科学与技术学院, 山东 济南 250061;

2. 山东师范大学 信息科学与工程学院, 山东 济南 250014)

(xulijuan937@sohu.com)

**摘 要:**在基于身份的公钥密码体制下实现了一个指定验证者的门限代理签名方案,该方案的实现基于双线性对。虽然人们对如何提高双线性对的执行效率方面取得了大量的研究成果,但是双线性对运算仍然是基于身份密码机制中最耗时的运算,该方案减少了双线性对的运算需求,从而提高了效率。另外还对此方案进行了相应的安全性分析及安全性证明。

**关键词:**基于身份的签名;双线性对;指定验证者的签名;门限代理签名

**中图分类号:** TP309.7 **文献标识码:** A

## ID-based designated-verifier threshold proxy signature

XU Li-juan<sup>1</sup>, XU Qiu-liang<sup>1</sup>, ZHENG Zhi-hua<sup>2</sup>

(1. School of Computer Science and Technology, Shandong University, Jinan Shandong 250061, China;

2. School of Information Science and Engineering, Shandong Normal University, Jinan Shandong 250014, China)

**Abstract:** An ID-based designated-verifier threshold proxy signature using bilinear pairings was introduced. Though fruitful achievements have been made in enhancing the computation of pairings, the computation of bilinear pairings is still a heavy burden on ID-based cryptography. The computation of bilinear pairings in the ID-based designated-verifier threshold proxy signature was reduced and its efficiency was improved. In addition, a relevant security was analyzed and proved.

**Key words:** ID-based signature; bilinear pairings; designated-verifier signature; threshold proxy signature

## 0 引言

代理签名的概念首先由 Mambo 等于 1996 年引入<sup>[1]</sup>,即原始签名人将其签名能力授权给代理签名人,代理签名人代表原始签名人进行签名。Zhang 和 Kim 等最早提出了门限代理签名方案<sup>[2,3]</sup>, $(t, n)$  门限代理签名就是原始签名人授权  $n$  个代理签名人,使得任意  $t$  或更多的代理签名人可以合作产生对消息的代理签名。在某些情况下,希望只有签名人指定的验证者才能验证门限代理签名。这种签名方式在实际中得到了应用,如电子商务中的电子投标等。

基于身份的加密和签名方案首先由 Shamir 于 1984 年提出<sup>[4]</sup>,该方案的主要思想就是利用用户的身份作为其公钥。简化了基于证书的公钥体制对公钥证书的管理。

## 1 预备知识

### 1.1 双线性对

$G_1$  是阶为素数  $q$  的加法循环群,  $P$  为  $G_1$  中任一生成元,  $G_2$  是与  $G_1$  同阶的乘法循环群。双线性对是指满足以下性质的一个映射  $\hat{e}: G_1 \times G_1 \rightarrow G_2$ :

- 双线性: 对于任意的  $P_1, P_2, Q \in G_1$ , 有  
 $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q) \times \hat{e}(P_2, Q)$

和

$$\hat{e}(Q, P_1 + P_2) = \hat{e}(Q, P_1) \times \hat{e}(Q, P_2)$$

从而对所有的  $P, Q \in G_1, a, b \in \mathbf{Z}_q^*$ , 满足:

$$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$$

- 非退化性: 存在  $P, Q \in G_1$ , 使得  $\hat{e}(P, Q) \neq I_{G_2}$ , 其中  $I_{G_2}$  为群  $G_2$  的单位元。

- 可计算性: 对于任意  $P, Q \in G_1$  存在有效的算法计算  $\hat{e}(P, Q)$ 。

### 1.2 GDH 群

#### 1.2.1 计算 DH 问题

**定义 1** 给定  $(P, aP, bP)$ , 计算  $abP$ , 称为计算 DH 问题 (Computational Diffie-Hellman Problem, CDHP)。其中  $a, b \in \mathbf{Z}_q^*$ 。

一个概率多项式时间 (Probabilistic, Polynomial-Time, PPT) 算法  $A$  在  $G_1$  群内解决 CDHP 的成功概率记为:

$$Succ_{A, G_1}^{CDH}$$

CDH 假设: 对于任何 PPT 算法  $A$ ,  $Succ_{A, G_1}^{CDH}$  可以忽略。

#### 1.2.2 判定 DH 问题

**定义 2** 给定  $(P, aP, bP, cP)$ , 其中  $a, b, c \in \mathbf{Z}_q^*$ , 判定  $cP = abP$ , 称为判定 Diffie-Hellman 问题 (Decisional Diffie-Hellman Problem, DDHP)。

DDHP 在  $G_1$  群上是易解的。

GDH 群 (Gap Diffie-Hellman group): 一个素数阶群  $G_1$  是 GDH 群, 当存在一个有效的 PPT 算法在  $G_1$  上解决 DDHP, 同时不存在 PPT 算法以不可忽略的概率成功解决 CDHP。

## 2 体制的定义

**定义 3** 一个基于身份门限代理签名体制是由一组多项式时间算法组成的算法组 (Setup, Extract, PD, PV, Pshare,

收稿日期: 2006-11-08; 修订日期: 2007-01-22 基金项目: 国家自然科学基金资助项目 (60373026)

作者简介: 徐丽娟 (1981-), 女, 山东济宁人, 硕士, 主要研究方向: 密码学、信息安全; 徐秋亮 (1960-), 男, 教授, 博士生导师, 博士, 主要研究方向: 密码学、信息安全; 郑志华 (1962-), 女, 高级实验师, 硕士, 主要研究方向: 信息安全。

$PSgn, Pver$ , 算法定义如下:

**Setup**: 参数生成算法, 用于生成系统参数。

**Extract**: 私钥生成算法, 用于为参与签名的用户生成密钥对。

**PD**: 授权算法, 用于原始签名人为多个代理签名人生成授权证书。

**PV**: 授权验证算法, 用于验证上算法生成的证书是否合法。

**Pshare**: 代理密钥生成算法, 用于为多个代理签名人生成秘密分享值。

**PSgn**: 指定验证者的门限代理签名算法, 用于产生最终的签名。

**Pver**: 指定验证者的门限代理签名验证算法, 用于验证签名的合法性。

### 3 基于身份指定验证人的门限代理签名

#### 3.1 初始化

##### 3.1.1 参数的生成

$G_1$  是一个素数阶为  $q$  生成元为  $P$  的 GDH 群, 其中  $q > 2^k$ ,  $k$  是安全参数。 $\hat{e}: G_1 \times G_1 \rightarrow G_2$  是双线性对映射。主密钥  $s \in \mathbb{Z}_q^*$ ,  $P_{pub} = sP$ 。hash 函数:

$$H_1: \{0, 1\}^* \rightarrow G_1$$

$$H_2: \{0, 1\}^* \times G_1 \rightarrow G_1$$

$$H_3: \{0, 1\}^* \times G_1 \times G_2 \rightarrow G_1$$

##### 3.1.2 密钥的生成

$P_0$  是原始签名人,  $PS = \{P_1, P_2, \dots, P_n\}$  是  $n$  个代理签名人组成的代理签名群,  $P_v$  是指定验证者, PKG 根据身份信息  $ID_0, ID_i (i = 1, 2, \dots, n), ID_v$  来计算公钥  $Q_0 = H_1(ID_0) \in G_1$ ,  $Q_i = H_1(ID_i) \in G_1$ ,  $Q_v = H_1(ID_v) \in G_1$  和相应私钥  $d_0 = sQ_0 \in G_1$ ,  $d_i = sQ_i \in G_1$ ,  $d_{m_v} = sQ_v \in G_1$ 。

##### 3.2 分存密钥的生成

每个  $P_i \in PS$  随机选择一个  $(t-1)$  阶的多项式

$$f_i(x) = \sum_{l=1}^{t-1} a_{il}x^l + a_{i0} \quad (1)$$

其中  $a_{il} \in \mathbb{Z}_q^*$ , 公开  $A_{il} = a_{il}P (l = 0, 1, \dots, t-1)$ 。

$P_i$  通过安全信道把  $f_i(j)$  给  $P_j (j \neq i)$ 。 $P_j$  接收到  $f_i(j)$  之后验证其有效性

$$f_i(j)P = \sum_{k=0}^{t-1} j^k A_{ik} \quad (2)$$

每个  $P_i$  计算它的秘密共享  $r_i = \sum_{k=1}^n f_k(i)$  并公开  $U_i = r_i P$ 。

##### 3.3 代理密钥的生成

原始签名人  $P_0$  委托他的签名权给代理签名人  $P_i (i = 1, 2, \dots, n)$ ,  $P_0$  和每个  $P_i$  完成以下各步:

$P_0$  使用 Cha-Cheon<sup>[5]</sup> 提出的基于身份的签名方案为  $m_\omega$  进行签名:

选择随机数  $r_\omega \in \mathbb{Z}_q^*$ , 计算  $U_\omega = r_\omega Q_0$ ,  $h_\omega = H_2(m_\omega, U_\omega)$  和  $V_\omega = (r_\omega + h_\omega)d_0$ 。然后  $P_0$  把  $\langle m_\omega, U_\omega, V_\omega \rangle$  发送给  $P_i \in PS$ 。

其中  $m_\omega$  是一个含有门限值、委托签名的有效期、原始签名人、代理签名人以及验证者身份标志的委托证书。

$P_i$  验证原始签名人对  $m_\omega$  签名的有效性: 计算

$$Q_0 = H_1(ID_0) \in G_1$$

$$h_\omega = H_2(m_\omega, U_\omega) \in G_1$$

然后判断

$$\hat{e}(P, V_\omega) = \hat{e}(P_{pub}, U_\omega + h_\omega Q_0) \quad (3)$$

是否成立。如果成立则接受签名, 否则拒绝。

$P_i$  计算  $s_i = d_i + V_\omega$  作为他的代理私钥。然后随机选择  $(t-1)$  阶多项式:

$$g_i(x) = \sum_{l=1}^{t-1} b_{il}x^l + s_i \quad (4)$$

其中系数  $b_{il} \in G_1$ , 公开  $B_{il} = \hat{e}(P, b_{il})$ ,  $l = 1, 2, \dots, t-1$ 。

$P_i \in PS$  可计算出

$$B_{i0} = \hat{e}(P, s_i) = \hat{e}(P_{pub}, U_\omega + h_\omega Q_0 + Q_i) \quad (5)$$

$P_i$  把  $g_i(j) (j \neq i)$  通过安全信道发送给  $P_j$ 。 $P_i$  接收  $g_j(i)$ , 并通过下式验证其有效性:

$$\hat{e}(P, g_j(i)) = \prod_{k=0}^{t-1} B_{jk}^{ik}$$

最后  $P_i$  计算他的代理密钥的分享值为  $skp_i = \sum_{k=1}^n g_k(i)$ ,

公开  $\hat{e}(P, skp_i)$ 。

##### 3.4 代理签名的生成

代理签名群  $PS$  中的任意  $t$  个代理签名人 (设为  $D = \{P_1, P_2, \dots, P_t\}$ ) 代表原始签名人对消息  $m$  ( $m$  与委托证书  $m_\omega$  中所要求签发的消息一致) 进行指定验证者  $P_v$  的代理签名, 每个代理签名人  $P_i \in D (i = 1, 2, \dots, t)$  完成以下步骤:

计算:

$$g_{ID_v} = \hat{e}(Q_v, P_{pub})$$

$$Y_i = g_{ID_v}^{r_i}$$

$$Y = \prod_{i=1}^t Y_i^{\eta_i}, \quad \eta_i = \prod_{j \neq i}^{j \in \{1, 2, \dots, t\}} \frac{j}{j-i}$$

$$U = \sum_{i=1}^t \eta_i U_i, \quad \eta_i = \prod_{j \neq i}^{j \in \{1, 2, \dots, t\}} \frac{j}{j-i}$$

$$H = H_3(m, U, Y)$$

签名过程采用修改的 Cheon 等<sup>[6]</sup> 提出的基于身份的签名方案:

计算:

$$V_i = r_i \left( \sum_{i=1}^t Q_i \right) + H_3(m, U, Y) skp_i$$

$$\sigma_i = (U_i, V_i)$$

为代理签名份额。

指定 clerk 接收到  $V_i$  并通过下式验证其正确性:

$$\hat{e}(P, V_i) = \hat{e}\left(U_i, \sum_{i=1}^t Q_i\right) \hat{e}(P, skp_i)^{\eta_i} \quad (6)$$

如果式(6)成立,  $\sigma_i$  为  $P_i$  对  $m$  的有效代理签名。当  $D$  中所有人对  $m$  的签名都有效时, clerk 计算

$$V = \sum_{i=1}^t \eta_i V_i, \quad \eta_i = \prod_{j \neq i}^{j \in \{1, 2, \dots, t\}} \frac{j}{j-i}$$

对消息  $m$  的代理签名为  $\langle m, U_\omega, m_\omega, (U, V) \rangle$ 。

##### 3.5 代理签名的验证

接收到  $\langle m, U_\omega, m_\omega, (U, V) \rangle$  之后, 指定的验证者需要进行以下各步:

判断  $m$  是否与  $m_\omega$  中的要求一致, 如果不满足  $m_\omega$  中的条件, 则停止, 否则继续进行下一步。

判断  $P_0$  与  $D$  中的代理签名人的身份是否与  $m_\omega$  中所标识的原始签名人和代理签名人的身份相符。如果不符合则停止,

否则进行下一步。

计算:

$Y^* = \hat{e}(d_{ID_V}, U)$  当下式:

$$\hat{e}(P, V) = \hat{e}(U + P_{pub} H_3(m, U, Y^*), \sum_{i=1}^t Q_i) \cdot \hat{e}(P, V_\omega)^{nH_3(m, U, Y^*)} \quad (7)$$

成立时,接受签名。

## 4 方案性能分析

### 4.1 正确性证明

代理签名人通过验证式(3) 是否成立来确定对委托证书  $m_\omega$  的签名  $\langle m_\omega, U_\omega, V_\omega \rangle$  的有效性:

$$\begin{aligned} \hat{e}(P, V_\omega) &= \hat{e}(P, (r_\omega, h_\omega) d_0) \\ &= \hat{e}(P_{pub}, U_\omega + h_\omega Q_0) \end{aligned}$$

Clerk 通过验证式(6) 是否成立来确定部分代理签名  $V_i$  的有效性:

$$\begin{aligned} \hat{e}(P, V_i) &= \hat{e}(P, r_i \left( \sum_{i=1}^t Q_i \right) + H_3(m, U, Y) skp_i) \\ &= \hat{e}(P, r_i \left( \sum_{i=1}^t Q_i \right)) \hat{e}(P, H_3(m, U, Y) skp_i) \\ &= \hat{e}(U_i, \sum_{i=1}^t Q_i) \hat{e}(P, skp_i)^H \end{aligned}$$

指定的验证人通过验证式(7) 是否成立来确定生成的代理签名的有效性:

$$\begin{aligned} \hat{e}(P, V) &= \hat{e}(P, \sum_{i=1}^t \eta_i V_i) \\ &= \hat{e}(U, \sum_{i=1}^t Q_i) \hat{e}(P, \sum_{i=1}^t \eta_i skp_i H_3(m, U, \prod_{i=1}^t Y_i^{\eta_i})) \\ &= \hat{e}(U, \sum_{i=1}^t Q_i) \cdot \hat{e}(P, \left( \sum_{i=1}^t d_i + nV_\omega \right) H_3(m, U, \prod_{i=1}^t g_{ID_V}^{\eta_i r_i})) \\ &= \hat{e}(U, \sum_{i=1}^t Q_i) \cdot \hat{e}(P, \left( \sum_{i=1}^t d_i + nV_\omega \right) H_3(m, U, \prod_{i=1}^t \hat{e}(d_{ID_V}, \eta_i U_i))) \\ &= \hat{e}(U, \sum_{i=1}^t Q_i) \cdot \hat{e}(P, \left( \sum_{i=1}^t d_i + nV_\omega \right) H_3(m, U, \hat{e}(d_{ID_V}, U))) \\ &= \hat{e}(U + P_{pub} H_3(m, U, Y^*), \sum_{i=1}^t Q_i) \cdot \hat{e}(P, V_\omega)^{nH_3(m, U, Y^*)} \end{aligned}$$

### 4.2 安全性分析

· 不可伪造性。本文所提出的方案中,授权证书的签发采用了 Cha-Cheon 签名体制,该签名已被证明在随机预言模型下能抵抗基于适应性选择消息和固定 ID 的存在性伪造攻击(EF-fID-CMA)。即本文所提方案中,攻击者无法伪造授权证书。本方案签名过程采用修改的 Cheon 等<sup>[6]</sup> 提出的基于身份的签名方案,该方案在随机预言模型下已被证明是安全的。本文的修改并不影响原方案的安全性,即本文所提方案攻击者无法伪造代理签名。不能通过假冒被指定验证者的身份来获得验证签名的权利,正如不能伪造代理签名的原因一样。所以本方案具有不可伪造性。

· 可区分性。委托证书  $m_\omega$  里包含了所有代理签名人以及原始签名人的身份信息,而且代理签名等式的验证过程中都需要原始签名人以及参与签名的代理签名人的公钥。因此本方案能满足可区分性。

· 不可否认性。代理签名的验证等式里包含了委托证书以及代理签名人的公钥,因此一旦代理签名人为原始签名人产生了代理签名就不能否认这个签名。

· 限制验证性。仅仅是原始签名人指定的验证者  $P_V$  才能验证代理签名群产生的代理签名,因为如果敌手在不知道验证人  $P_V$  的私钥  $d_{ID_V}$  的情况下计算  $Y^*$  就相当于从  $U_i$  中计算出  $r_i$ ,这是离散对数难解问题。

### 4.3 安全性证明

#### 4.3.1 安全性模型

以形式化的语言描述,称基于身份的指定验证者的门限代理签名体制是适应性选择消息和固定 ID 的攻击下存在性不可伪造的(EF-fID-CMA),如果对任意的概率多项式时间的攻击者  $A$ , 在下面的试验中获得非零返回值的概率是可以忽略的。

定义 4 试验  $Exp_{IDT\_PS,A}^{fID-CMA}(k): IDT\_PS = (Setup, Extract, Sshare, PD, PV, Pshare, PSgn, Pver)$  是基于身份指定验证者的门限代理签名体制,攻击者为  $A$ ,安全参数  $k$ ,  $fID\_CMA$  是适应性选择消息和固定 ID 攻击,定义试验  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$ :

(1) 运行  $Setup$ , 输入  $1^k$ , 把生成的系统参数  $para$  给  $A$ 。

(2) 令  $C_{list} \leftarrow \emptyset; D_{list} \leftarrow \emptyset; G_{list} \leftarrow \emptyset; S_{list} \leftarrow \emptyset$ 。

(3)  $A$  在输入  $para$  的情况下,以任意次序做任意次以下操作或询问:

1) 询问  $Extract(\cdot)$  随机预言机,输入身份  $ID_i$ , 得到相应私钥  $d_i$ , 令  $C_{list} = C_{list} \cup \{(ID_i, d_i)\}$ ;

2) 询问  $PD(\cdot)$  随机预言机,若  $A$  得到  $proxy_{p0 \rightarrow PS} \leftarrow PD(ID_i, m_\omega)$ , 令  $D_{list} = D_{list} \cup \{(ID_i, m_\omega, proxy_{p0 \rightarrow PS})\}$ ;

3)  $Pshare$  操作,请求生成代理签名人  $ID_j$  的代理密钥的分享值  $skp_j$ , 设原始签名人的身份为  $ID_i$ , 若  $A$  得到

$$skp_j \leftarrow Pshare(ID_j, proxy_{p0 \rightarrow PS}, ID_i)$$

则令

$$G_{list} = G_{list} \cup \{(ID_j, proxy_{p0 \rightarrow PS}, skp_j, ID_i)\};$$

4) 询问  $PSgn(\cdot)$  随机预言机,设  $ID_k$  为指定验证者的身份。若  $A$  得到

$$(m, \tau) \leftarrow PSgn(m, ID_k, skp_j, proxy_{p0 \rightarrow PS})$$

令

$$S_{list} = S_{list} \cup \{(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j)\}$$

(4)  $A$  输出  $(ID_i, m_\omega, proxy_{p0 \rightarrow PS})$  或  $(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j)$ 。

(5) 若  $A$  的输出结果满足下面条件之一,则攻击成功:

1) 输出为  $(ID_i, m_\omega, proxy_{p0 \rightarrow PS})$ , 满足  $PV(proxy_{p0 \rightarrow PS}, ID_i) = 1, (ID_i, \cdot) \notin C_{list}$ , 且  $(ID_i, m_\omega, proxy_{p0 \rightarrow PS}) \notin D_{list}$ , 则成功伪造了一个委托签名,  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$  返回值 1。

2) 输出为  $(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j)$ , 设授权者身份  $ID_i$ , 代理者身份  $ID_j$ , 指定验证者身份  $ID_k$ 。满足  $Pver(ID_i, m, \tau, ID_k, ID_j, proxy_{p0 \rightarrow PS}) = 1, (proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j) \notin S_{list}, (ID_i, \cdot) \notin C_{list}, (ID_0, \cdot) \notin C_{list}, (ID_v, \cdot) \notin C_{list}, (ID_j, proxy_{p0 \rightarrow PS}, skp_j, ID_i) \notin G_{list}$ , 成功伪造了一个指定验证者的门限代理签名,  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$  返回值 1。

3) 其他情况  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$  返回值为 0。

定义攻击者  $A$  成功的概率为:

$$Adv_{IDT\_PS,A}^{fID-CMA}(k) = \Pr[Exp_{IDT\_PS,A}^{fID-CMA}(k) = 1]$$

如果  $A$  在时间  $t$  内,对  $Extract(\cdot)$  最多进行  $q_E$  次询问,对  $PD(\cdot)$  最多进行  $q_S$  次询问,对  $PSgn(\cdot)$  最多进行  $q_{PS}$  次询问,  $Adv_{IDT\_PS,A}^{fID-CMA}(k)$  的概率至少为  $\varepsilon$ , 则称  $A(t, q_E, q_S, q_{PS}, \varepsilon) - breaks$  指定验证者的门限代理签名体制。我们称指定验证者的门限代理签名体制是  $(t, q_E, q_S, q_{PS}, \varepsilon) - secure$ , 如果不存在任何攻击者  $(t, q_E, q_S, q_{PS}, \varepsilon) - breaks$  该体制。

#### 4.3.2 安全性证明

**定理 1** 设  $IDT\_PS = (Setup, Extract, Sshare, PD, PV, Pshare, PSgn, Pver)$  为由 Cha-Cheon 签名体制:  $ID\_Sign = \{Setup, Extract, Sgn', Ver'\}^{[5]}$  和修改的 Cheon 等<sup>[6]</sup> 提出的基于身份的签名方案:  $ID\_BSign = \{Setup, Extract, Sgn'', Ver''\}^{[6]}$  演化而来的基于身份指定验证者门限代理签名体制, 如果  $ID\_Sign$  是  $EF-fID-CMA$ , 且  $ID\_BSign$  是  $EF-fID-CMA$ , 则  $IDT\_PS$  是  $EF-fID-CMA$ 。

**证明** 假设存在概率多项式时间的攻击者  $A$ , 执行  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$ , 并以不可忽略的概率  $\varepsilon$  返回值为 1, 由  $A$  可以构造  $ID\_Sign$  的  $fID-CMA$  攻击者  $B$  和  $ID\_BSign$  的  $fID-CMA$  攻击者  $C$ 。

(1) 运行  $Setup$ , 把生成的系统参数  $para$  分别作为  $B$  和  $C$  的输入。

(2) 令  $C_{list} \leftarrow \emptyset; D_{list} \leftarrow \emptyset; G_{list} \leftarrow \emptyset; S_{list} \leftarrow \emptyset$ 。

(3) 将  $para$  作为  $A$  的输入, 运行  $A$  执行  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$ ,  $B$  和  $C$  模拟  $A$  的各种询问如下:

1)  $Extract(\cdot)$  询问, 对询问  $ID_i, B, C$  分别以  $ID_i$  访问自己的  $Extract(\cdot)$  随机预言机, 并把结果作为对  $A$  的应答, 令  $C_{list} = C_{list} \cup \{(ID_i, d_i)\}$ 。

2)  $PD(\cdot)$  询问, 对输入的  $ID_i$  和  $m_\omega$ ,  $B$  以  $ID_i$  和  $m_\omega$  访问  $Sgn'(\cdot)$  随机预言机, 设得到应答为  $\delta$ ,  $B$  以  $proxy_{p0 \rightarrow PS} = (m_\omega, \delta)$  作为对  $A$  的应答令

$$D_{list} = D_{list} \cup \{(ID_i, m_\omega, proxy_{p0 \rightarrow PS})\}$$

3)  $Pshare$  请求生成  $ID_i$  的代理密钥的分享值  $skp_i$  操作, 对输入的  $ID_i$  和  $proxy_{p0 \rightarrow PS}$ , 设  $proxy_{p0 \rightarrow PS} = (m_\omega, \delta)$ , 原始签名人的身份为  $ID_i$ , 若  $Ver'(proxy_{p0 \rightarrow PS}, ID_i) \neq 1$ ,  $B$  应答为  $\perp$ ; 否则,  $C$  以  $m_\omega$  和  $proxy_{p0 \rightarrow PS}$  询问自己的  $Extract(\cdot)$  并采用秘密分享算法产生  $n$  个代理签名者的代理密钥的分享值  $skp_j$ , 把应答  $skp_j$  作为对  $A$  的应答, 令

$$G_{list} = G_{list} \cup \{(ID_j, proxy_{p0 \rightarrow PS}, skp_j, ID_i)\}$$

4)  $PSgn(\cdot)$  询问, 对输入的  $proxy_{p0 \rightarrow PS}, m, ID_k, skp_j (j = 1, 2, \dots, t)$ 。设  $proxy_{p0 \rightarrow PS} = (m_\omega, \delta)$ ,  $B$  以  $m_\omega$  访问  $Sgn'(\cdot)$  随机预言机,  $C$  以  $m$  访问  $Sgn''(\cdot)$ , 设得到的应答为  $\tau$ ,  $C$  以  $(m, \tau)$  作为对  $A$  的应答, 令

$$S_{list} = S_{list} \cup \{(proxy_{p0 \rightarrow PS}, m, \tau, Q_k, skp_j)\}$$

(4) 设  $S'_{list}$  和  $E_{list}^B$  分别表示攻击者  $B$  对  $Sgn'(\cdot)$  和  $B$  的  $Extract(\cdot)$  的所有访问及相应应答所构成的序列,  $S''_{list}$  和  $E_{list}^C$  分别表示攻击者  $C$  对  $Sgn''(\cdot)$  和  $C$  的  $Extract(\cdot)$  的所有访问及相应应答所构成的序列。若  $A$  输出  $(ID_i, m_\omega, proxy_{p0 \rightarrow PS})$ , 满足  $PV(proxy_{p0 \rightarrow PS}, ID_i) = 1$ ,  $(ID_i, \cdot) \notin C_{list}$ , 且  $(ID_i, m_\omega, proxy_{p0 \rightarrow PS}) \notin D_{list}$ , 设  $proxy_{p0 \rightarrow PS} = (m_\omega, \delta)$ , 则  $B$  可输出  $(ID_i, m_\omega, \delta)$  满足  $Ver'((m_\omega, \delta), ID_i) = 1$  且  $(ID_i, m_\omega, \cdot) \notin S'_{list}$ ,  $(ID_i, \cdot) \notin E_{list}^B$ ; 若  $A$  输出  $(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j)$ , 设  $proxy_{p0 \rightarrow PS} = (m_\omega, \delta)$ , 设原始签名人和代理签名者的身份分

别为  $ID_i$  和  $ID_j$ , 指定验证者身份  $ID_k$ , 满足  $Pver(ID_i, m, \tau, ID_k, ID_j, proxy_{p0 \rightarrow PS}) = 1$ ,  $(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j) \notin S_{list}$ ,  $(ID_i, \cdot) \notin C_{list}$ ,  $(ID_j, \cdot) \notin C_{list}$ ,  $(ID_k, \cdot) \notin C_{list}$ ,  $(ID_j, proxy_{p0 \rightarrow PS}, skp_j, ID_i) \notin G_{list}$ , 则  $C$  可输出  $(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j)$ , 满足  $Ver''(proxy_{p0 \rightarrow PS}, m, \tau, ID_k, skp_j) = 1$  且  $(m, m_\omega, \cdot) \notin S''_{list}$ ,  $(m_\omega, proxy_{p0 \rightarrow PS}) \notin E_{list}^C$ ,  $(ID_i, \cdot) \notin E_{list}^C$ ,  $(ID_j, \cdot) \notin E_{list}^C$ ,  $(ID_k, \cdot) \notin E_{list}^C$ 。

综上所述, 若  $A$  执行  $Exp_{IDT\_PS,A}^{fID-CMA}(k)$  以不可忽略的概率  $\varepsilon$  返回值为 1, 则概率

$$Succ_{ID\_Sign}^{fID-CMA}(B) = \Pr[Para \leftarrow Setup(1^k), (ID, m, \delta) \leftarrow B^{Sgn'(\cdot), E(\cdot)}(para); Ver'((m, \delta), ID) = 1 \ \& \ (ID, \cdot, m, \cdot) \notin S'_{list} \ \& \ (ID, \cdot) \notin E_{list}] \geq \varepsilon$$

$$Succ_{ID\_BSign}^{fID-CMA}(C) = \Pr[Para \leftarrow Setup(1^k), (proxy_{p0 \rightarrow PS}, m, \tau, Q_k, skp_j) \leftarrow C^{Sgn''(\cdot), E(\cdot)}(para); Ver''(proxy_{p0 \rightarrow PS}, m, \tau, Q_k, skp_j) = 1 \ \& \ (m, \cdot, m_\omega, \cdot) \notin S''_{list} \ \& \ (m_\omega, \cdot) \notin E_{list}] \geq \varepsilon$$

即本方案在适应性选择消息和固定  $ID$  攻击下是安全的。

#### 4.4 效率分析

基于 Cha-Cheon 提出的基于身份的签名方案<sup>[5]</sup> 构造门限代理签名, 比文献[7]中原始签名人的签名方案在验证时少进行一个双线性对的计算, 由于  $n$  个代理签名人都要验证原始签名人对  $m_\omega$  的签名, 所以本文方案在验证时就减少了  $n$  个双线性对的计算。Clerk 接收到每个代理签名人的部分代理签名  $V_i$ , 对其进行验证时可使用已计算出的公开值  $\hat{e}(P, skp_i)$ , 只需进行两个双线性对的计算。指定的验证人  $P_V$  在对式(7)进行验证时可利用已经被代理签名人计算过的  $\hat{e}(P, V_\omega)$  的值, 同样也是只需自己计算两个双线性对的值即可。

#### 5 结语

本文在文献[7]和[8]的基础上, 提出并实现了在基于身份的公钥密码体制下的指定验证者门限代理签名方案, 该方案中签名的验证式仅仅需要两个对值的计算, 提高了计算效率。

#### 参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy Signature: Delegation of the Power to Sign Messages[J]. IEICE Transaction Fundamentals, 1996, E79-A(9): 1338 - 1353.
- [2] ZHANG K. Threshold Proxy Signature Schemes [A]. Information Security Work-shop (ISW'97) [C]. LNCS, Springer-Verlag, 1997, 1396: 282 - 290.
- [3] KIM S, PARK S, WON D. Proxy Signatures, Revisited[A]. Information and Communications Security (ICICS'97) [C]. LNCS, Springer-Verlag, 1997, 1334: 223 - 232.
- [4] SHAMIR A. Identity - based cryptosystems and signature schemes [A]. Advances in Cryptology (CRYPTO'84) [C]. LNCS, Springer-Verlag, 1984, 0916: 47 - 53.
- [5] CHA JC, CHEON JH. An identity-based signature from gap Diffie-Hellman groups[A]. DESMEDI Y, ed. Public Key Cryptography (PKC'03)[C]. LNCS, Springer-Verlag, 2003, 2567: 18 - 30.
- [6] CHEON J, KIM Y, YOON H. Batch Verifications with ID-based Signatures[A]. Information Security and Cryptology (ICISC'04) [C]. LNCS, Springer-Verlag, 2005, 3506: 233 - 248.
- [7] XU J, ZHANG ZF, FENG DG. Identity Based Threshold Proxy Signature, Report 2004/250[R]. Cryptology ePrint Archive, 2004.
- [8] CAO T, LIN D, XUE R. ID-based designated-verifier proxy signatures[J]. IEEE Proceeding Communications, 2005, 152(6): 989 - 994.