新的标准模型下基于身份的代理签名方案

冀会芳[1] 韩文报[1] 刘连东[2]

(信息工程大学信息工程学院 郑州 450002)[1] (信息工程大学电子技术学院 郑州 450004)[2]

摘 要 代理签名是原始签名者将其签名能力授权给代理签名者,从而代理签名者可以代表原始签名者对指定的消息进行签名。提出了一种新的基于身份的代理签名方案,并在标准模型下证明了方案是适应性选择消息和身份攻击下签名存在性不可伪造的,其安全性基于CDH假设是困难的。与现有标准模型下基于身份的代理签名方案相比,新方案的执行效率更高。

关键词 基于身份密码,代理签名,标准模型,双线性对

中图法分类号 TP309 **文献标识码** A

New Identity-based Proxy Signature in the Standard Model

JI Hui-fang[1] HAN Wen-bao[1] LIU Lian-dong[2]

(Institute of Information Engineering, PLA Information Engineering University, Zhengzhou 450002, China)[1]

(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)[2]

Abstract A proxy signature scheme entity to delegate its signing capability to another allows an original entity (proxy) in such a way that the proxy one can sign messages on behalf of the delegator. A new identity-based proxy signature scheme was proposed. The scheme is existentially unforgeable in the standard model against adaptive chosen message and identity attacks under the Computational Diffie-Hellman assumption. Compared with the known identity-based proxy signature scheme in the standard model, the scheme enjoys less operation.

Keywords Identity based cryptography, Proxy signature, Standard model, Bilinear pairings

1 概述

代理签名是Mambo, Usuda和Okamoto于1996年提出的概念[1],其基本思想是原始签名者将其签名权利授权给代理签名者,此后代理签名者可以代表原始签名者对消息进行签名;根据代理方式的不同,代理签名分为完全代理、部分代理和证书代理签名;根据原始签名者是否知道代理私钥,代理签名又可以分为保护代理者的签名和不保护代理者的签名。目前,保护代理者的证书代理签名是代理签名研究的热点问题。

结合代理签名和基于身份密码,国内外众多学者提出了许多基于身份的代理签名方案,这些方案都是基于双线性对设计的,并且在随机预言模型[6]下被证明是安全的。在这种模型中,任何具体对象都被视作随机对象,如Hash函数被视作一个随机预言返回值。在具体方案中,因为所用的Hash函数都是具体的,这就可能导致在使用过程中出现安全漏洞。因此不需要随机预言模型,即设计在标准模型下可证明安全的基于身份的代理签名方案,同时尽可能少地涉及双线性对运算,是本文研究工作的出发点之一。

2006年,Paterson等基于Waters方案提出一个标准模型下基于身份的签名方案[8]。在此基础上,李明祥等提出一个基于身份的代理签名方案[9]。李继国等给出一个效率更高的基于身份的签名方案[10]。在文献[10]的基础上,本文给出一个基于身份的代理签名方案,本方案在标准模型下是可证明安全的。与文献[9]中的方案相比,本方案的执行效率更高。

2 预备知识

2.1 安全模型

一个基于身份的代理签名方案IBPS={Setup, Extract, PKGen, PSign, Verify}由以下5个概率算法组成:

(1)系统建立(Setup):给定一个安全参数k,PKG生成系统公开参数$Params$和系统主密钥s。

(2)私钥提取(Extract):给定用户身份ID,PKG利用系统主密钥s为之生成私钥S,并通过安全方式发送给用户。

(3)代理密钥生成(PKGen):给定原始签名者ID_A及代理签名者ID_P的私钥S_A和S_P、授权信息W,该信息包含授权对象、范围、期限等信息,算法生成代理密钥K_P。

(4)代理签名(PSign):给定代理密钥K_P和待签名消息M,算法生成代理签名σ。

(5)验证(Verify):给定原始签名者身份ID_A和代理签名者身份ID_P、授权信息W、消息M和代理签名σ,如果σ是有效的代理签名,算法输出1,反之输出0。

到稿日期:2010-09-02 返修日期:2010-11-12 本文受国家973计划项目(2007CB807902),新世纪优秀人才计划项目(NCET-07-0384)和全国优秀博士学位论文作者专项基金(FANEDD-2007B74)资助。

冀会芳(1982—),女,博士生,主要研究方向为密码学和信息安全,E-mail:huifangji@126.com;韩文报(1963—),男,教授,博士生导师,主要研究方向为信息安全和网络密码;刘连东(1979—),男,博士生,讲师,主要研究方向为信息安全。

下面介绍基于身份代理签名方案的不可伪造性。

定义 1 一个基于身份的代理签名方案称作是适应性选择消息和身份攻击下存在性不可伪造的，如果不存在任何多项式有界的攻击者 $\mathcal{F}$ 以 ε 的优势赢得如下定义的游戏：

初始化：挑战者 $\mathcal{C}$ 运行 Setup(1^k)，生成系统公开参数 Params 和主密钥 s。

询问：攻击者 $\mathcal{F}$ 进行至多多项式有界次的以下 3 种询问：

(1) 用户私钥询问：$\mathcal{F}$ 提交一个身份 ID_u 给 $\mathcal{C}$，$\mathcal{C}$ 返回与之对应的私钥 S_u 给 $\mathcal{F}$；

(2) 代理密钥询问：$\mathcal{F}$ 提交原始签名者 ID_A 和代理签名者 ID_P 的私钥 S_A 和 S_P，$\mathcal{C}$ 返回代理密钥 K_P；

(3) 代理签名询问：$\mathcal{F}$ 提交一个原始签名者 ID_A，代理签名者 ID_P、授权信息 W 和消息 M 给 $\mathcal{C}$，$\mathcal{C}$ 返回对消息 M 的代理签名 σ；

伪造：攻击者 $\mathcal{F}$ 输出一个 5 元组 $(ID_A^*, ID_P^*, W^*, M^*, \sigma^*)$，如果满足以下条件：

1) $\mathcal{F}$ 没有对 ID_A^* 或 ID_P^* 进行过用户私钥询问；

2) $\mathcal{F}$ 没有对 (ID_A^*, ID_P^*, W^*) 进行过代理私钥询问；

3) $\mathcal{F}$ 没有对 $(ID_A^*, ID_P^*, W^*, M^*)$ 进行过代理签名询问，则称攻击者 $\mathcal{F}$ 获胜。

攻击者 $\mathcal{F}$ 在游戏中的优势定义为它在游戏中获胜的概率，即 $adv[\mathcal{F}]=\Pr[\mathcal{F}\ wins]$。

2.2 双线性映射

设 G_1 和 G_2 是同为素数 p 阶的循环群。g 是 G_1 的一个随机生成元。映射 $e: G_1 \times G_1 \to G_2$ 称作双线性对，如果该映射具有以下 3 个性质：

(1)双线性性：对任意的 $a, b \in Z_p$，都有 $e(g^a, g^b)=e(g, g)^{ab}$；

(2)非退化性：满足 $e(g, g) \neq 1_{G_2}$；

(3)可计算性：对任意的 $a, b \in Z_p$，存在一个有效的算法计算 $e(g, g)^{ab}$。

2.3 困难假设

CDH 假设(Computational Diffie-Hellman 假设)

挑战者 $\mathcal{C}$ 随机选择 $a, b \in Z_p$ 并输出 (g, g^a, g^b)，攻击者试图输出 $g^{ab} \in G_1$。攻击者有至少 ε 的优势解决 CDH 问题，如果 $\Pr[A(g, g^a, g^b)=g^{ab}] \geqslant \varepsilon$ 成立。如果不存在攻击者以至少 ε 的优势解决上述游戏，则称 ε-CDH 假设成立。

3 基于身份的代理签名方案

下面给出基于身份的代理签名方案的具体构造。这里假设所有的用户身份 ID、授权信息 W 和待签名消息 M 分别是长为 n_u，n_w 和 n_m 的比特串。本方案还可以推广到所有用户身份、授权信息和消息是任意长比特串的情形，只需利用一个抗碰撞的 Hash 函数把所有用户身份、授权信息和消息都映射为长为 n_u，n_w 和 n_m 的比特串。

设 G_1，G_2 和 $e: G_1 \times G_1 \to G_2$ 如上定义，且 g 是 G_1 的随机生成元。记 $a \in_R B$ 为从集合 B 中随机选择元素 a。

系统建立(Setup)：PKG 随机选择 $\alpha \in_R Z_p^*$，计算 $g_1=g^\alpha$，选择 $g_2 \in_R G_1$。选择元素 $u' \in_R Z_p$，$w', m' \in_R G_1$。选择向量 $U=(u_i)_{1 \leqslant i \leqslant n_u}$，$u_i \in_R Z_p$，$1 \leqslant i \leqslant n_u$，$W=(w_i)_{1 \leqslant i \leqslant n_w}$，$w_i \in_R G_1$，$1 \leqslant i \leqslant n_w$，$M=(m_i)_{1 \leqslant i \leqslant n_m}$，$m_i \in_R G_1$，$1 \leqslant i \leqslant n_m$。令 $z_1=e(g_1, g_2)$，$z_2=e(g, g_2)$，定义函数 $F_u(ID)=u'+\sum_{j=1}^{n_u} i_j u_j$，$F_w(W)=w' \prod_{i=1}^{n_w} w_i^{W_i}$，$F_m(M)=m' \prod_{i=1}^{n_m} m_i^{M_i}$，其中 $ID=i_1 i_2 \cdots i_{n_u}$，$W=W_1 W_2 \cdots W_{n_w}$ 和 $M=M_1 M_2 \cdots M_{n_m}$ 分别为长为 n_u，n_w 和 n_m 的比特串。系统参数定义为 $P=(g, g_1, g_2, z_1, z_2, u', U, w', W, m', M)$，主密钥为 g_2^α。

私钥提取(Extract)：给定一个用户身份 ID，PKG 选择 $t \in_R Z_p$，计算用户 ID 的私钥 $S_{ID}=(s_{ID,1}, s_{ID,2})=(g_2^{\alpha+tF_u(ID)}, z_2^t)$，注意选择适当的 t 使得 $\alpha+t \cdot F_u(ID) \neq 0 \bmod p$。用户 ID 通过 $e(g, s_{ID,1})=z_1 \cdot s_{ID,2}^{F_u(ID)}$ 来验证私钥的合法性。若等式成立，则接受 S_{ID} 作为其私钥，否则重新从 PKG 获取密钥。

代理密钥生成(PKGen)：给定一个原始签名者身份 ID_A 和一个授权信息 W(包含授权对象、范围、期限等信息)，ID_A 首先选取 $r_W \in_R Z_p$，生成一个授权证书 $\sigma_W=(\sigma_{W,1}, \sigma_{W,2}, \sigma_{W,3})$，其中 $\sigma_{W,1}=s_{A,1} \cdot F_w(W)^{r_W}$，$\sigma_{W,2}=s_{A,2}$，$\sigma_{W,3}=g^{r_W}$；然后发送$(W, \sigma_W)$给指定的代理签名者 ID_P。ID_P 首先验证 $e(g, \sigma_{W,1})=z_1 \cdot \sigma_{W,2}^{F_u(ID_A)} \cdot e(\sigma_{W,3}, F_w(W))$ 是否成立。若成立，ID_P 选取 $r_W' \in_R Z_p$，计算代理私钥 $K_P=(K_{P,1}, K_{P,2}, K_{P,3}, K_{P,4})$，其中 $K_{P,1}=s_{P,1} \cdot \sigma_{W,1} \cdot F_w(W)^{r_W'}$，$K_{P,2}=\sigma_{W,2}$，$K_{P,3}=s_{P,2}$，$K_{P,4}=\sigma_{W,3} \cdot g^{r_W'}$。

代理签名(PSign)：给定消息 M，代理签名者 ID_P 按照如下步骤生成代理签名：

(1)随机选取 $s \in Z_q^*$，计算 $\sigma_1=K_{P,1} \cdot F_m(M)^s$；

(2)令 $\sigma_2=K_{P,2}$，$\sigma_3=K_{P,3}$，$\sigma_4=K_{P,4}$；

(3)计算 $\sigma_5=g^s$。

返回 $\sigma=(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$作为消息 M 的代理签名。

验证(Verify)：已知 σ 是在原始签名人 ID_A、代理签名人 ID_P 和授权证书 W 下消息 M 的代理签名。验证者计算 $e(g, \sigma_1)=z_1^2 \cdot \sigma_2^{F_u(ID_A)} \cdot \sigma_3^{F_u(ID_P)} \cdot e(\sigma_4, F_w(W)) \cdot e(\sigma_5, F_m(M))$ 是否成立。如果成立，则返回 1，表示 σ 是有效的代理签名，否则返回 0。

正确性：从以下推导很容易得出方案是正确的。

用户私钥生成阶段，

$$e(g, s_{ID,1})=e(g, g_2^{\alpha+tF_u(ID)})=e(g, g_2^\alpha)e(g, g_2^{tF_u(ID)})$$
$$=e(g_1, g_2)e(g, g_2)^{tF_u(ID)}=z_1 \cdot s_{ID,2}^{F_u(ID)}$$

代理密钥生成阶段，

$$e(g, \sigma_{W,1})=e(g, s_{A,1} \cdot F_w(W)^{r_W})$$
$$=e(g, g_2^{\alpha+t_A F_u(ID_A)} \cdot F_w(W)^{r_W})$$
$$=e(g, g_2^\alpha)e(g, g_2^{t_A F_u(ID_A)})e(g, F_w(W)^{r_W})$$
$$=z_1 \cdot \sigma_{W,2}^{F_u(ID_A)} \cdot e(\sigma_{W,3}, F_w(W))$$

验证阶段，

$$e(g, \sigma_1)=e(g, K_{P,1} \cdot F_m(M)^s)$$
$$=e(g, s_{P,1} \cdot \sigma_{W,1} \cdot F_m(M)^s)$$
$$=e(g, g_2^{2\alpha+t_A F_u(ID_A)+t_P F_u(ID_P)} \cdot F_w(W)^{r_W+r_W'} \cdot F_m(M)^s)$$
$$=e(g, g_2^{2\alpha})e(g, g_2^{t_A F_u(ID_A)})e(g, g_2^{t_P F_u(ID_P)})e(g, F_w(W)^{r_W+r_W'})e(g, F_m(M)^s)$$
$$=e(g_1, g_2)^2 e(g, g_2)^{t_A F_u(ID_A)} e(g, g_2)^{t_P F_u(ID_P)} e(g^{r_W+r_W'}, F_w(W))e(g^s, F_m(M))$$
$$=z_1^2 \cdot \sigma_2^{F_u(ID_A)} \cdot \sigma_3^{F_u(ID_P)} \cdot e(\sigma_4, F_w(W)) \cdot e(\sigma_5, F_m(M))$$

4 方案分析

4.1 安全性分析

定理 1 假设存在一个 EUF-IBPS-ACMIA 的攻击者 $\mathcal{F}$，可在时间 t 内以 ε 的优势在定义 1 的游戏中获胜。假设 $\mathcal{F}$ 可

以进行至多 $q_E/q_{PK}/q_{PS}$ 次私钥提取/代理密钥/代理签名询问，则存在一个区分者 $\mathscr{C}$，可在时间 t' 内以 ϵ' 的优势解决 CDH 问题，其中

$$\epsilon'>\frac{\epsilon}{64q_Eq_{PS}(q_{PK}+q_{PS})(n_u+1)(n_w+1)(n_m+1)}$$

$$t'>t+t_eO(1)(q_E+q_{PK}+q_{PS})+t_m(O(1)q_E+O(n_w)q_{PK}+O(n_w+n_m)q_{PS})$$

式中，t_m 表示群中一个乘法运算所需要的时间，t_e 表示一个指数运算所需要的时间。

证明：假设存在 EUF-IBPS-ACMIA 的伪造者 $\mathscr{F}$，可以构造挑战者 $\mathscr{C}$ 解决 CDH 问题。假设 $\mathscr{C}$ 收到一个 CDH 问题实例 (g^a,g^b)，它的目标是计算 g^{ab}。$\mathscr{C}$ 运行 EUF-IBPS-ACMIA 游戏中的攻击者 $\mathscr{F}$，并且扮演其中的挑战者。

系统建立：令 $\tau_u=2q_E,\tau_w=2(q_{PK}+q_{PS}),\tau_m=2q_{PS}$。$\mathscr{C}$ 选取整数 $k_u\in_R\{1,\cdots,n_u\},k_w\in_R\{1,\cdots,n_w\},k_m\in_R\{1,\cdots,n_m\}$，并且 $\tau_u(n_u+1)<p,\tau_w(n_w+1)<p,\tau_m(n_m+1)<p$。选择 $x_u'\in_R Z_{\tau_u}$ 和 $x_{u,i}\in_R Z_{\tau_u}$，$1\leqslant i\leqslant n_u$，选择 $x_w'\in_R Z_{\tau_w}$ 和 $x_{w,j}\in_R Z_{\tau_w}$，$1\leqslant j\leqslant n_w$，选择 $x_m'\in_R Z_{\tau_m}$ 和 $x_{m,j}\in_R Z_{\tau_m}$，$1\leqslant j\leqslant n_m$，选择整数 $y_w'\in_R Z_p$ 和 $y_{w,i}\in_R Z_p$，$1\leqslant i\leqslant n_w$，$y_m'\in_R Z_p$ 和 $y_{m,i}\in_R Z_p$，$1\leqslant i\leqslant n_m$。

为便于分析，分别定义以下函数

$$J_u(ID)=x_u'+\sum_{j=1}^{n_u}i_j\cdot x_{u,j}-k_u\tau_u$$

$J_w(W)=x_w'+\sum_{j=1}^{n_w}W_jx_{w,j}-\tau_wk_w$ 和 $K_w(W)=y_w'+\sum_{j=1}^{n_w}W_jy_{w,j}$

$J_m(M)=x_m'+\sum_{j=1}^{n_m}M_jx_{m,j}-\tau_mk_m$ 和 $K_m(M)=y_m'+\sum_{j=1}^{n_m}M_jy_{m,j}$

$\mathscr{C}$ 设定系统的公开参数为 $g_1=g^a,g_2=g^b,u'=x_u'-k_u\tau_u,u_i=x_{u,i},1\leqslant i\leqslant n_u,w'=g_2^{x_w'-k_w\tau_w}g^{y_w'},w_i=g_2^{x_{w,i}}g^{y_{w,i}}$，$1\leqslant i\leqslant n_w,m'=g_2^{x_m'-k_m\tau_m}g^{y_m'},m_i=g_2^{x_{m,i}}g^{y_{m,i}},1\leqslant i\leqslant n_m$。

对任意的用户身份 ID、授权信息 W 和消息 M，有

$$F_u(ID)=u'+\sum_{j=1}^{n_u}i_ju_j=J_u(ID)$$

$$F_w(W)=w'\prod_{j=1}^{n_w}w_j^{W_j}=g_2^{J_w(W)}g^{K_w(W)}$$

$$F_m(M)=m'\prod_{j=1}^{n_m}m_j^{M_j}=g_2^{J_m(M)}g^{K_m(M)}$$

成立。$\mathscr{C}$ 按照如下方式回答 $\mathscr{F}$ 的询问：

私钥提取询问：给定一个用户身份 ID，若 $J_u(ID)\neq0 \bmod p$，$\mathscr{C}$ 选择 $t\in_R Z_p$，生成用户 ID 的私钥为

$$S_{ID}=(s_{ID,1},s_{ID,2})=(g_1^{-1}(g\cdot g_2)^{t\cdot F_u(ID)},e(gg_2,g^tg_1^{-1/F_u(ID)}))$$

$\mathscr{F}$ 可以按照如下方式验证其私钥的合法性：

$$\begin{aligned}e(g,s_{ID,1})&=e(g,g_1^{-1}(gg_2)^{t\cdot F_u(ID)})\\&=e(g,g_2^a(gg_2)^{t\cdot F_u(ID)-a})\\&=e(g_1,g_2)\cdot e((gg_2)^{F_u(ID)},g^{t-a/F_u(ID)})\\&=z_1\cdot e(gg_2,g^tg_1^{-1/F_u(ID)})^{F_u(ID)}\\&=z_1\cdot s_{ID,2}^{F_u(ID)}\end{aligned}$$

若 $J_u(ID)=0 \bmod p$，则 $\mathscr{C}$ 终止模拟过程，返回一个随机比特。为简便起见，如果 $J_u(ID)=0 \bmod \tau_u$，模拟终止。事实上，据 $\tau_u(n_u+1)<p$，有 $0\leqslant\tau_uk_u<p$ 和 $0\leqslant x_u'+\sum_{j=1}^{n_u}i_jx_{u,j}<p$ 成立，我们有 $-p<J_u(ID)<p$，从而得到如下关系式：$J_u(ID)=0 \bmod p\Rightarrow J_u(ID)=0 \bmod \tau_u$，因此有 $J_u(ID)\neq0 \bmod \tau_u\Rightarrow J_u(ID)\neq0 \bmod p$。

代理密钥询问：给定一个原始签名者身份 ID_A、授权证书 W 和代理者身份 ID_P，如果 $J_w(W)\neq0 \bmod \tau_w$，$\mathscr{C}$ 随机选取 $t_A,t_P,r_W\in Z_p$，生成代理密钥 $K_P=(K_{P,1},K_{P,2},K_{P,3},K_{P,4})$，其中 $K_{P,1}=g_2^{2a+t_AF_u(ID_A)+t_PF_u(ID_P)}F_w(W)^{\tilde{r}_W}$，$K_{P,2}=z_2^{t_A}$，$K_{P,3}=z_2^{t_P}$，$K_{P,4}=g^{r_W}\cdot g_2^{-2/J_w(W)}=g^{\tilde{r}_W}$，其中 $\tilde{r}_W=r_W-2a/J_w(W)$；若 $J_w(W)=0 \bmod \tau_w$，则 $\mathscr{C}$ 终止模拟过程，返回一个随机比特。

代理签名询问：给定一个原始签名者身份 ID_A、代理者身份 ID_P、授权证书 W 和消息 M，如果 $J_w(W)\neq0 \bmod \tau_w$，$\mathscr{C}$ 首先进行 PKGen 询问，得到代理私钥，然后运行 PSign 算法，生成代理签名 σ；否则，如果 $J_m(M)\neq0 \bmod \tau_m$，$\mathscr{C}$ 随机选取 t_A，$t_P,r_W,s\in Z_p$，计算

$$\begin{aligned}\sigma_1&=g_1^{\frac{-2K_m(M)}{J_m(M)}}\cdot g_2^{t_AF_u(ID_A)+t_PF_u(ID_P)}\cdot F_w(W)^{r_W}\cdot F_m(M)^s\\&=g_2^{2a+t_AF_u(ID_A)+t_PF_u(ID_P)}\cdot F_w(W)^{r_W}\cdot F_m(M)^{\tilde{s}}\end{aligned}$$

令 $\sigma_2=z_2^{t_A},\sigma_3=z_2^{t_P},\sigma_4=g^{r_W}$，计算 $\sigma_5=g_1^{-2/J_m(M)}g^s=g^{s-2a/J_m(M)}=g^{\tilde{s}}$，其中 $\tilde{s}=s-2a/J_m(M)$，返回 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$ 作为代理签名；否则 $\mathscr{C}$ 终止模拟过程，返回一个随机比特。

伪造：如果 $\mathscr{C}$ 不终止模拟，则至少以 ϵ 的概率输出 $(ID_A^*,ID_P^*,W^*,M^*,\sigma^*)$，其中 σ^* 是有效的代理签名。如果 $J_u(ID_A^*)=0 \bmod p$ 且 $J_u(ID_P^*)=0 \bmod p$，则 $\mathscr{C}$ 结束模拟；否则，以下分两种情况讨论：

(1) 若 $J_u(ID_P^*)\neq0 \bmod p$ 且 $\mathscr{F}$ 已询问过 ID_P^* 的私钥，但没有询问过 ID_A^* 的私钥。如果 $J_u(ID_A^*)=0 \bmod p\cap J_w(W^*)=0 \bmod p\cap J_m(M^*)=0 \bmod p$，则 $\mathscr{C}$ 计算并输出

$$\begin{aligned}&\sigma_1^*[s_{P,1}^*\cdot(\sigma_4^*)^{K_w(W^*)}\cdot(\sigma_5^*)^{K_m(M^*)}]^{-1}\\&=g_2^{2a+t_P^*F_u(ID_P^*)}\cdot F_w(W^*)^{r_W^*}\cdot F_m(M^*)^s\cdot\\&\quad[g_2^{a+t_P^*F_u(ID_P^*)}\cdot(g^{r_W^*})^{K_w(W^*)}\cdot(g^s)^{K_m(M^*)}]^{-1}\\&=g_2^a=g^{ab}\end{aligned}$$

作为对 CDH 问题的回答。

(2) 若 $J_u(ID_A^*)\neq0 \bmod p$ 且 $\mathscr{F}$ 已询问过 ID_A^* 的私钥，但没有询问过 ID_P^* 的私钥。如果 $J_u(ID_P^*)=0 \bmod p\cap J_w(W^*)=0 \bmod p\cap J_m(M^*)=0 \bmod p$，则 $\mathscr{C}$ 计算并输出

$$\begin{aligned}&\sigma_1^*[s_{A,1}^*\cdot(\sigma_4^*)^{K_w(W^*)}\cdot(\sigma_5^*)^{K_m(M^*)}]^{-1}\\&=g_2^{2a+t_A^*F_u(ID_A^*)}\cdot F_w(W^*)^{r_W^*}\cdot F_m(M^*)^s\cdot\\&\quad[g_2^{a+t_A^*F_u(ID_A^*)}\cdot(g^{r_W^*})^{K_w(W^*)}\cdot(g^s)^{K_m(M^*)}]^{-1}\\&=g_2^a=g^{ab}\end{aligned}$$

作为对 CDH 问题的回答。

下面计算 $\mathscr{C}$ 的成功概率。

$\mathscr{C}$ 的模拟过程不终止，需要满足以下条件：

(1) 私钥提取询问中，任一个身份 ID 都满足 $J_u(ID)\neq0 \bmod \tau_u$；

(2) 所有代理密钥询问中，授权信息 W 满足 $J_w(W)\neq0 \bmod \tau_w$；

(3) 所有代理签名询问中，有 $J_w(W)\neq0 \bmod \tau_w\cup J_m(M)\neq0 \bmod \tau_m$；

(4) $J_u(ID_P^*)=0 \bmod p\cap J_w(W^*)=0 \bmod p\cap J_m(M^*)=0 \bmod p$

或

$J_u(ID_A^*)=0 \bmod p\cap J_w(W^*)=0 \bmod p\cap J_m(M^*)=0$

mod p

成立。

设 $ID_1,\cdots,ID_{q_I}$ 为所有询问中出现过的不含挑战身份的用户身份，显然有 $q_I\leqslant q_E$，$W_1,\cdots,W_{q_{II}}$ 为所有询问中出现的不含挑战授权信息的授权信息，则有 $q_{II}\leqslant q_{PK}+q_{PS}$，$M_1,\cdots,M_{q_{III}}$ 为在所有询问中出现的不含挑战消息的消息，有 $q_{III}\leqslant q_{PS}$，定义以下概率事件

$A_i: J_u(ID_i)\neq 0 \bmod \tau_u, 1\leqslant i\leqslant q_I, A^*: J_u(ID_A^*)=0 \bmod p$

$B_i: J_w(W)\neq 0 \bmod \tau_w, 1\leqslant i\leqslant q_{II}, B^*: J_w(W^*)=0 \bmod p$

$C_i: J_m(M)\neq 0 \bmod \tau_m, 1\leqslant i\leqslant q_{III}, C^*: J_m(M^*)=0 \bmod p$

则 $\mathscr{C}$ 不终止模拟过程的概率为

$$\Pr[\overline{abort}]\geqslant \Pr[\bigcap_{i=1}^{q_I}A_i\cap A^*\cap(\bigcap_{j=1}^{q_{II}}B_j\cap B^*)\cap(\bigcap_{j=1}^{q_{III}}C_j\cap C^*)]$$

由于函数 $J_u(ID)$，$J_w(W)$，$J_m(M)$ 是独立选择的，因而事件 $\bigcap_{i=1}^{q_I}A_i\cap A^*$，$\bigcap_{j=1}^{q_{II}}B_j\cap B^*$ 和 $\bigcap_{j=1}^{q_{III}}C_j\cap C^*$ 相互独立，据 k_u，u'，u_i，$i=1,\cdots,n_u$ 的随机性，有

$$\begin{aligned}\Pr[A^*]&=\Pr[J_u(ID_A^*)=0 \bmod p]\\&=\Pr[J_u(ID_A^*)=0 \bmod p\cap J_u(ID_A^*)=0 \bmod \tau_u]\\&=\Pr[J_u(ID_A^*)=0 \bmod \tau_u]\Pr[J_u(ID_A^*)=0 \bmod p\,|\,J_u(ID_A^*)=0 \bmod \tau_u]\\&=\frac{1}{\tau_u}\frac{1}{n_u+1}\end{aligned}$$

另一方面，对任意的 i，事件 A_i 和 A^* 相互独立，从而有

$$\begin{aligned}\Pr[\bigcap_{i=1}^{q_I}A_i\cap A^*]&=\Pr[A^*]\Pr[\bigcap_{i=1}^{q_I}A_i\,|\,A^*]\\&=\Pr[A^*](1-\Pr[\bigcup_{i=1}^{q_I}\overline{A_i}\,|\,A^*])\\&\geqslant\Pr[A^*](1-\sum_{i=1}^{q_I}\Pr[\overline{A_i}\,|\,A^*])\\&=\frac{1}{\tau_u}\frac{1}{n_u+1}(1-\frac{q_I}{\tau_u})\geqslant\frac{1}{4q_E(n_u+1)}\end{aligned}$$

同理，$\Pr[\bigcap_{j=1}^{q_{II}}B_j\cap B^*]\geqslant\frac{1}{4(q_{PK}+q_{PS})(n_w+1)}$，$\Pr[\bigcap_{j=1}^{q_{III}}C_j\cap C^*]\geqslant\frac{1}{4q_{PS}(n_m+1)}$，则

$$\begin{aligned}\Pr[\overline{abort}]&\geqslant\Pr[\bigcap_{i=1}^{q_I}A_i\cap A^*\cap(\bigcap_{j=1}^{q_{II}}B_j\cap B^*)\cap(\bigcap_{j=1}^{q_{III}}C_j\cap C^*)]\\&\geqslant\frac{1}{64q_Eq_{PS}(q_{PK}+q_{PS})(n_u+1)(n_w+1)(n_m+1)}\end{aligned}$$

由于 $\mathscr{F}$ 的优势为 ε，从而 $\mathscr{C}$ 的成功概率为

$$\varepsilon'\geqslant\varepsilon/64q_Eq_{PS}(q_{PK}+q_{PS})(n_u+1)(n_w+1)(n_m+1)$$

$\mathscr{C}$ 的时间复杂度取决于各个询问中的乘法运算时间 t_m 和指数运算时间 t_e。每个私钥提取询问需要 $O(1)$ 个指数运算和 $O(1)$ 个乘法运算，每个代理密钥询问需要 $O(1)$ 个指数运算和 $O(n_w)$ 个乘法运算，每个代理签名询问需要 $O(1)$ 个指数运算和 $O(n_w+n_m)$ 个乘法运算，因此 $\mathscr{C}$ 的时间复杂度为

$$t'>t+t_eO(1)(q_E+q_{PK}+q_{PS})+t_m(O(1)q_E+O(n_w)q_{PK}+O(n_w+n_m)q_{PS})$$

4.2 效率分析

表1将本文方案的效率和文献[9]中的方案效率进行比较。记 M 为乘法运算，E 为指数运算，P 为对运算，$|G_1|$，$|G_2|$ 表示 G_1，G_2 中元素比特表示的长度。

表1 方案计算量和通信量比较

方案	代理签名计算量	验证阶段计算量	签名长度
文献[9]	$2E+(n_m+1)M$	$(2n_u+n_w+n_m+4)M+5P$	$5\|G_1\|$
本文方案	$2E+(n_m+1)M$	$(n_w+n_m+2)M+3P+2E$	$3\|G_1\|+2\|G_2\|$

由表1可知，本文方案的通信量和文献[9]中方案的通信量相当，计算量在验证阶段比文献[9]中方案减少两个对运算。相对于对运算的时间复杂度，乘法运算和指数运算的时间复杂度可以忽略不计，本文方案验证阶段的效率比文献[9]中的方案提高了近2/5，因而效率较高。

结束语 本文利用 Waters 的方法，基于文献[9]的基于身份代理签名方案，提出一种在标准模型下安全的基于身份的高效代理签名方案，其安全性证明基于 CDH 假设。在实际使用中，可将签名中不变的部分作为系统参数部分公开，这样签名长度可以减小 2/5。本文方案的系统参数可以采用文献[11]中的方法进行改进，以减少系统参数的长度。分析表明，本文方案的通信效率和文献[9]中方案的通信效率相当，而执行效率高于文献[9]中给出的标准模型下可证明安全的基于身份的代理签名方案。

参 考 文 献

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

[2] Shamir A. Identity based cryptosystems and signature schemes [C] // Proceedings of CRYPTO'84. Berlin: Springer-Verlag, 1984: 47-83

[3] Boneh D, Ranklin M. Identity-based encryption from the Weil pairing[C]// Proceedings of CRYPTO'01. Berlin: Springer-Verlag, 2001: 213-229

[4] Zhang F, Kin K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C] // Proceedings of the 8th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2003: 312-323

[5] Xu J, Zhang Z F, Feng D G. ID-based proxy signature using bilinear pairings[C]// Proceedings of the 3rd International Symposium on Parallel and Distributed Processing and Applications. Berlin: Springer-Verlag, 2005: 359-367

[6] Bellare M, Rogaway. Random oracles are practical: a paradigm for designing efficient protocols[C] // Proceedings of the 1st ACM Conference on Computer and Communications Security. New York: ACM, 1993: 62-73

[7] 张跃宇，李晖，王育民. 标准模型下基于身份的环签名方案[J]. 通信学报，2008，29(4)：40-44

[8] Paterson K, Schuldt J. Efficient identity based signatures secure in the standard model[C] // Proceedings of the ACISP. Melbourne, Australia, 2006: 207-222

[9] 李明祥，韩伯涛，朱建勇，等. 在标准模型下安全的基于身份的代理签名方案[J]. 华南理工大学学报：自然科学版，2009，37(5)：118-122

[10] 李继国，姜平进. 标准模型下可证安全的基于身份的高效签名方案[J]. 计算机学报，2009，32(11)：2130-2136

[11] Chatterjee S, Sarkar P. Trading time for space: towards an efficient IBE scheme with short(er) public parameters in the standard model[C]// Proceedings of the ICISC'2005, LNCS 3935. Springer, 2006: 424-440