文章编号: 1001-0920 (2012) 03-0362-07

标准模型下基于身份的代理环签名方案研究

于义科[1,2], 郑雪峰[1], 张清国[1], 张明德[1]

(1. 北京科技大学 信息工程学院，北京 100083；2. 南昌航空大学 信息工程学院，南昌 330063)

摘 要: 现有的基于身份的代理环签名方案的安全性大都是在随机预言模型下证明的, 随机预言机模型将 Hash 函数理想化为一个完全随机模型, 在实际应用中不一定安全. 鉴于此, 提出一个新的基于身份的代理环签名方案. 在标准模型下证明了该方案能够抵抗存在性伪造攻击, 且签名者具有无条件匿名性, 因此具有更好的安全可靠性.

关键词: 代理环签名；基于身份的密码；计算 Diffie-Hellman 问题

中图分类号: TP309 **文献标识码:** A

Research on ID-based proxy ring signature in the standard model

YU Yi-ke[1,2], *ZHENG Xue-feng*[1], *ZHANG Qing-guo*[1], *ZHANG Ming-de*[1]

(1. School of Information Engineering，University of Science and Technology Beijing，Beijing 100083，China; 2. School of Information Engineering，Nanchang Hangkong University，Nanchang 330063，China. Correspondent: YU Yi-ke，E-mail：yyk312@163.com)

Abstract: Existing ID-based proxy ring signature schemes are proved to be secure in the random oracle model(ROM). Hash function is regarded as ideally random model in ROM, which is not secure in the real world. Therefore, a new proxy ring signature scheme is proposed. It is proved in the standard model that the scheme is existentially unforgeable and unconditionally anonymous. So the scheme is more secure and reliable.

Key words: proxy ring signature；identity based cryptography；computational Diffie-Hellman problem

1 引 言

在电子商务和电子政务中, 人们经常需要将自己的签名权委托给代理人, 让代理人代表本人对一些文件进行签名. 这可以通过代理签名[1]来实现, 但在一般的代理签名方案中, 代理人的身份并没有得到保护, 在电子投票、股票交易、电子支票或电子货币的分发等应用中, 人们越来越关注匿名性. 考虑如下场景: 一个原始签名人将其签名权委托给一组代理签名人 (代理组), 组中任何一个代理签名人都能够代表原始签名人执行签名操作, 但实际签名人希望在执行代理签名的同时保持无条件匿名性, 即任何人 (包括原始签名人) 任何时候都不能明确其身份.

目前, 面向群体的匿名签名方案主要有群签名[2]和环签名[3]两个类型. 显然群签名并不适合这种场合, 因为群管理员可以在必要的时候撤销签名者的匿名性. 环签名可看作是一种简化的群签名, 不需要群管理员或群建立过程, 可以实现无条件匿名, 即使攻击者拥有无限的计算能力, 也无法追踪签名人的身份. 环签名的无条件匿名性在对信息需要长期保护的一些特殊环境中较为适用. 近年来, 环签名和基于身份的密码[4]发展迅速, 基于身份的环签名得到了深入研究[5-10]. 文献 [11] 针对上述场景将代理签名和环签名结合起来, 提出了代理环签名的概念, 并在 [5] 基于身份的环签名方案的基础上构造了第 1 个基于身份的代理环签名方案. 自代理环签名的概念提出以来, 人们对其进行了一些研究. [12] 针对 [11] 应用受限和运算量过大的缺点, 提出一种代理人受保护的代理环签名方案, 该方案能有效防止原始签名人对代理签名人签名的伪造, 且减少了双线性对的计算量, 计算效率较高. [13] 指出 [5] 存在计算不一致方面的问题, 并提出了一种新的环签名和代理环签名方案. [14] 提出了一种基于多线性映射的代理环签名方案, 该方案能防止原始签名者冒充代理签名者对消息进行签名, 通过引入多个密钥生成中心防止其中任何一个对消息进行签名.

目前已有的代理环签名方案普遍在随机预言模

收稿日期: 2010-10-03；**修回日期:** 2011-04-02.

基金项目: 国家自然科学基金项目(60803123, 60674054)；南昌航空大学博士启动基金项目(EA201104185).

作者简介: 于义科(1970–), 男, 副教授, 博士, 从事系统控制理论、信息安全等研究；郑雪峰(1951–), 男, 教授, 博士生导师, 从事工业控制、网络安全等研究.

型下可证是安全的, 然而, 随机预言模型将Hash函数作为一个完全随机的理想模型, 在具体应用中无法构造相应的实例, 因此, 设计标准模型下可证安全的代理环签名方案更有实际意义. 本文首先定义了基于身份的代理环签名(IBPRS)的安全模型; 然后在文献[7]提出的基于身份的环签名方案的基础上设计了一个新的基于身份的代理环签名方案; 最后在所定义的安全模型下不使用随机预言即可证明该方案是安全的, 且其安全性基于更一般的计算Diffie-Hellman假设的困难性, 因此, 本文方案比已有方案具有更高的安全性.

2　预备知识

2.1　双线性映射

定义 1 (双线性映射)　设 G 和 G_1 是阶为素数 p 的两个循环群, g 是群 G 的生成元, 则双线性映射 $e: G\times G\to G_1$ 具有如下性质: 1) 双线性: 对于所有的 $u, v\in G$ 和 $a, b\in_R \mathrm{Z}_p^*$, 均有 $e(u^a, v^b)=e(u,v)^{ab}$; 2) 非退化性: $e(g,g)\neq 1$; 3) 可计算性: 存在一个有效的算法计算 $e(u,v)$, 其中 $u, v\in G$.

2.2　复杂性假设

定义 2 (计算Diffie-Hellman(CDH)问题)　已知 G 是阶为素数 p 的循环群, g 是群 G 的生成元, $a, b\in_R \mathrm{Z}_p^*$, $g, g^a, g^b\in G$, 计算 g^{ab}.

如果不存在解决群 G 上CDH问题的概率至少为 ε 且运行时间至多为 t 的算法, 则称 (ε, t)-CDH 假设在群 G 上成立.

3　IBPRS 体制定义

3.1　IBPRS 的形式化定义

1个 $(1,n)$ 代理环签名方案中一般包括4种角色: 1个私钥生成中心(PKG), 1个原始签名人 P_0, 1个代理签名人组 $\{P_1, P_2, \cdots, P_n\}$ 和1个验证人(可以是任何人).

定义 3 (基于身份的代理环签名(**IBPRS**))　1个 $(1,n)$ IBPRS 方案由1组概率多项式算法$\{\mathcal{G}, \mathcal{E}, (\mathcal{D},\mathcal{P}), \mathrm{PRS}, \mathrm{PRV}\}$ 组成, 各成分如下:

1) 系统建立 $(\mathcal{G})$. 该算法由PKG完成, 输入安全参数 1^k, 输出主密钥msk和系统参数Param. PKG保密msk, 公开Param.

2) 私钥生成 $(\mathcal{E})$. 该算法由PKG执行, 输入主密钥msk, 系统参数Param和用户 P_i 的身份 ID_i, 输出用户私钥 d_i, 并通过安全方式发送给该用户.

3) 代理授权 $(\mathcal{D}, \mathcal{P})$. 这是一对在原始签名人和代理签名人之间交互执行的代理授权算法. $\mathcal{D}$ 由原始签名人执行, 算法输入公开参数Param, 授权文件 w 和原始签名人身份 ID_0, 输出授权证书 σ_w, 发送 (w, σ_w) 给代理签名人组的各个成员 P_i; $\mathcal{P}$ 由每个代理签名人 P_i 执行, 算法输入公开参数Param, 原始签名人身份 ID_0, 授权文件 w, 授权证书 σ_w 和代理签名人身份 ID_i, 输出代理签名人 P_i 的代理签名私钥 pk_i.

4) 签名 (PRS). 该算法由代理签名人 P_i 执行, 输入公开参数Param, 授权文件 w, 构成环的代理签名人身份集合 R, 代理签名人 $\mathrm{ID}_\pi(\mathrm{ID}_\pi\in R)$ 的代理签名私钥 pk_π 和签名消息 m, 输出环 R 对于消息 m 的基于身份的 $(1,n)$ 代理环签名 $p\sigma$.

5) 验证 (PRV). 该算法由验证人(可以是任何人)执行, 输入公开参数Param, 授权文件 w, 原始签名人身份 ID_0, 构成环的代理签名人身份集合 R, 签名消息 m 和代理环签名 $p\sigma$, 输出Valid或Invalid.

3.2　IBPRS 的安全要求

基于身份的代理环签名方案满足如下安全要求:

1) 可区分性(Distinguishability). 任何人都可以区别代理签名和标准签名.

2) 可验证性(Verifiability). 根据代理签名, 验证人能确信原始签名人认可代理签名人所做的签名.

3) 可识别性(Identifiability). 根据代理签名, 任何人都可以确定实际代理签名人来自代理签名组.

4) 强不可伪造性(Strong unforgeability). 除了原始签名人可以将其签名权委托给代理人, 任何其他人都不能伪造原始签名人的签名权. 只有指定的代理签名人能代表原始签名人产生有效的代理签名, 而原始签名人和其他没有指定为代理签名人的第3方都不能产生有效的代理签名.

5) 匿名性(Signer ambiguity). 根据代理签名, 任何攻击者(包括原始签名人)都无法确定实际签名者的身份.

6) 防滥用性(Prevention of misuse). 代理签名者的代理签名私钥除了用于产生合法的代理签名外, 不能用于其他目的.

3.3　IBPRS 的安全模型

根据代理环签名的强不可伪造性要求, 可通过一个挑战者 $\mathcal{C}$ 与敌手 $\mathcal{A}$ 之间的游戏来定义基于身份的代理环签名方案在适应性选择消息和选择身份攻击下的不可伪造性(EU-IBPRS-CMIA). 游戏如下所述:

1) 建立. 挑战者 $\mathcal{C}$ 运行方案的系统建立算法 $\mathcal{G}$ 得到系统参数Param和主密钥msk并发送Param给敌手 $\mathcal{A}$, 保存msk.

2) 询问. 敌手 $\mathcal{A}$ 可以适应性地向挑战者 $\mathcal{C}$ 提出多项式次数的询问.

① 私钥询问. $\mathcal{A}$ 可以询问任何身份 ID_i 的私钥 d_i, $\mathcal{C}$ 运行 $\mathcal{E}$ 算法得到 d_i, 并将 d_i 发送给 $\mathcal{A}$.

② 代理授权询问 I. $\mathcal{A}$ 给出授权文件 w, 原始签名人身份 ID_0 和代理签名人身份 ID_i, $\mathcal{A}$ 扮演原始签名人角色 P_0, 运行 $\mathcal{D}$ 算法, 产生授权证书 σ_w, 发送 (w,σ_w) 给 $\mathcal{C}$. $\mathcal{C}$ 运行 $\mathcal{E}$ 算法得到代理签名人的私钥 d_i, 再运行 $\mathcal{P}$ 算法产生代理签名人 P_i 的代理环私钥 pk_i, 发送给 $\mathcal{A}$.

③ 代理授权询问 II. $\mathcal{A}$ 给出授权文件 w, 原始签名人身份 ID_0 和代理签名人身份 ID_i, $\mathcal{A}$ 扮演代理签名人角色 P_i. $\mathcal{C}$ 运行 $\mathcal{E}$ 算法得到原始签名人 P_0 的私钥 d_0, 再运行 $\mathcal{D}$ 算法产生授权证书 σ_w, 输出 (w,σ_w) 给 $\mathcal{A}$.

④ 签名询问. 敌手 $\mathcal{A}$ 选择包含 n 个代理签名人身份的集合 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$, 授权文件 w 和消息 m. $\mathcal{C}$ 运行 PRS 算法得到代理环签名 $p\sigma$, 并将它发送给敌手 $\mathcal{A}$.

3) 伪造. 最后敌手 $\mathcal{A}$ 输出一个伪造, 该伪造可以是下面 2 种情形之一:

① $\mathcal{A}$ 伪造一个原始签名人 ID_0^* 的授权文件 w^* 的授权证书 σ_{w^*}, 如果满足以下 3 个条件, 则该伪造是有效的: a) $(\mathrm{ID}_0^*,w^*,\sigma_{w^*})$ 是 Valid; b) ID_0^* 没有提交用户私钥询问; c) (ID_0^*,w^*) 没有提交代理授权询问.

② $\mathcal{A}$ 伪造一个在 $(\mathrm{ID}_0^*,w^*,m^*,L^*)$ 下的代理环签名 $p\sigma^*$, 若满足以下 4 个条件, 则该伪造是有效的: a) $\mathrm{PRV}(\mathrm{ID}_0^*,m^*,w^*,L^*,p\sigma^*)$ 是 Valid; b) ID_i^* 没有提交用户私钥询问, 其中 $\mathrm{ID}_i^*\in L^*$; c) (ID_0^*,w^*) 没有提交代理授权询问; d) (m^*,w^*,L^*) 没有提交签名询问.

如果 $\mathcal{A}$ 的伪造是有效的, 则 $\mathcal{A}$ 赢得游戏. 敌手 $\mathcal{A}$ 的优势定义为它能赢得上面游戏的概率, 即

$$\mathrm{Adv}_{\mathcal{A}}=\Pr(\mathcal{A}\ \text{succeeds}).$$

定义 4 如果不存在优势至少为 ε, 运行时间至多为 t 的敌手 $\mathcal{A}$, 且用户私钥询问的次数最多为 q_e, 代理授权询问的次数最多为 q_d, 签名询问的次数最多为 q_s, 则该方案是 $(\varepsilon,t,q_e,q_d,q_s)$-EU-IBPRS-CMIA 安全的.

定义 5 如果已知任意包含 n 个代理签名用户的身份集合 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$ 对于任何消息 m 的 $(1,n)$ 代理签名 $p\sigma$, 任何敌手 $\mathcal{A}$ 能够识别实际签名人的优势不会大于随机猜测, 即 $\mathcal{A}$ 输出实际签名人的概率不会大于 $1/n$, 则称一个基于身份的代理环签名方案具有无条件匿名性.

4 IBPRS 方案

4.1 方案描述

设 P_0 是原始签名人, 身份为 ID_0, $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$ 是 n 个代理签名人 $\{P_1,P_2,\cdots,P_n\}$ 的身份组成的集合. 假设 $H_u:\{0,1\}^*\to\{0,1\}^{n_u}$, $H_m:\{0,1\}^*\to\{0,1\}^{n_m}$, $H_w:\{0,1\}^*\to\{0,1\}^{n_w}$ 为 3 个抗碰撞的 Hash 函数, 用于将用户的身份 ID_i, 授权证书 w 和消息 m 转化为长度为 n_u, n_w 和 n_m 的比特串.

4.1.1 系统参数产生算法 $\mathcal{G}$

PKG 选择阶为素数 p 的循环群 G 和 G_1, 生成元 $g\in G$, 随机数 $\alpha\in\mathrm{Z}_p$, $g_2,u',m',w'\in G$; $\hat{U}=(\hat{u}_1,\hat{u}_2,\cdots,\hat{u}_{n_u})\in G^{n_u}$, $\hat{W}=(\hat{w}_1,\hat{w}_2,\cdots,\hat{w}_{n_w})\in G^{n_w}$, $\hat{M}=(\hat{m}_1,\hat{m}_2,\cdots,\hat{m}_{n_m})\in G^{n_m}$. 构造双线性映射 $e:G\times G\to G_1$, 计算 $g_1=g^{\alpha}$; 公开参数为 $\mathrm{Param}=(G,G_1,e,g,g_1,g_2,u',\hat{U},w',\hat{W},m',\hat{M})$, 主密钥为 $\mathrm{msk}=g_2^{\alpha}$.

4.1.2 用户私钥产生算法 $\mathcal{E}$

已知用户 P_j 的身份 ID_j, 令 $u_j=H_u(\mathrm{ID}_j)$, $\mathcal{U}_{P_j}\subseteq\{1,2,\cdots,n_u\}$ 为 $u_j[i]=1$ 的序号 i 的集合. PKG 随机选择 $r_{P_j}\in\mathrm{Z}_p$, 并计算

$$d_j=(g_2^{\alpha}(U_j)^{r_{P_j}},g^{r_{P_j}})=(D_j^{(1)},D_j^{(2)}),\tag{1}$$

其中 $U_j=u'\prod_{i\in\mathcal{U}_{P_j}}\hat{u}_i$. 则 d_j 为身份为 ID_j 的私钥, 并将 d_j 秘密发送给用户 P_j.

4.1.3 代理授权协议 $(\mathcal{D},\mathcal{P})$

$\mathcal{D}$ 表示如下: 已知授权文件 w, 其包含了代理关系的描述, 如原始签名人的身份信息、每个代理签名人的身份信息和签名消息的限制(如类型、期限)等. 令 $w=H_w(w)$, $\mathcal{W}\subseteq\{1,2,\cdots,n_w\}$ 为 $w[j]=1$ 的序号 j 的集合. 原始签名人 P_0 的私钥为 $(D_0^{(1)},D_0^{(2)})$. P_0 随机选择 $r_w\in\mathrm{Z}_p$, 产生授权证书

$$\begin{aligned}\sigma_w=&\Big(D_0^{(1)}\Big(w'\prod_{j\in\mathcal{W}}\hat{w}_j\Big)^{r_w},D_0^{(2)},g^{r_w}\Big)=\\&\Big(g_2^{\alpha}(U_0)^{r_{P_0}}\Big(w'\prod_{j\in\mathcal{W}}\hat{w}_j\Big)^{r_w},g^{r_{P_0}},g^{r_w}\Big)=\\&(\sigma_w^{(1)},\sigma_w^{(2)},\sigma_w^{(3)}).\end{aligned}\tag{2}$$

原始签名人 P_0 发送授权证书 (w,σ_w) 给每个代理签名人 $P_k(k=1,2,\cdots,n)$.

$\mathcal{P}$ 表示如下: 代理签名人 P_k 首先通过验证如下等式判断授权文件 (w,σ_w) 是否有效:

$$e(\sigma_w^{(1)},g)=e(g_1,g_2)e(U_0,\sigma_w^{(2)})e\Big(w'\prod_{j\in\mathcal{W}}\hat{w}_j,\sigma_w^{(3)}\Big).$$

设每个代理签名人 $P_k(k=1,2,\cdots,n)$ 的私钥为 $(D_k^{(1)},D_k^{(2)})$, 若 (w,σ_w) 有效, P_k 选择 $r_{w_k}\in\mathrm{Z}_p$, 计算

$$\begin{aligned}pk_k=&\Big(\sigma_w^{(1)}D_k^{(1)}\Big(w'\prod_{j\in\mathcal{W}}\hat{w}_j\Big)^{r_{w_k}},D_k^{(2)},g^{r_{w_k}}\sigma_w^{(3)}\Big)=\\&(K_k^{(1)},K_k^{(2)},K_k^{(3)},K_k^{(4)}),\end{aligned}\tag{3}$$

则 pk_k 为代理签名人 P_k 代表原始签名人 P_0 签名的代理签名私钥.

4.1.4 签名算法 PRS

设 m 为要签名的消息, $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$

为环签名中所包含的n个代理签名人$\{P_1, P_2, \cdots, P_n\}$身份的列表, 实际的签名者为$P_\pi(\pi = 1, 2, \cdots, n)$, 代理签名私钥为$(K_\pi^{(1)}, K_\pi^{(2)}, K_\pi^{(3)}, K_\pi^{(4)})$, 代表原始签名人$P_0$对消息$m$进行签名. P_π随机选择$r_1, r_2, \cdots, r_n$, $r_m \in Z_p$. 令$m = H_m(L, m)$, $\mathcal{M} \subseteq \{1, 2, \cdots, n_m\}$为$m[l] = 1$的序号$l$的集合, 利用$P_\pi$计算$U_j = u' \prod\limits_{i \in \mathcal{U}_{P_j}} \hat{u}_i$, 其中$j = 1, 2, \cdots, n$, 有

$$p\sigma = \Big(K_\pi^{(1)} \Big(\prod_{j=1}^{n} (U_j)^{r_j}\Big) \Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l\Big)^{r_m}, K_\pi^{(2)}, g^{r_1}, \cdots, g^{r_{\pi-1}}, K_\pi^{(3)}, g^{r_\pi}, g^{r_{\pi+1}}, \cdots, g^{r_n}, K_\pi^{(4)}, g^{r_m}\Big) = (V, R_0, R_1, \cdots, R_n, R_w, R_m), \tag{4}$$

$p\sigma$为代理环签名.

4.1.5 验证算法 PRV

给定所有环成员的身份集$L = \{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$, 消息$m$以及代理环签名$(V, R_0, R_1, \cdots, R_n, R_w, R_m)$, 验证者首先计算

$$w = H_w(w),\ m = H_m(L, m),\ U_j = u' \prod_{i \in \mathcal{U}_{P_j}} \hat{u}_i,$$

其中$j = 0, 1, \cdots, n$; 然后通过如下公式检查代理环签名的合法性:

$$e(V, g) = e(g_1, g_2)^2 \Big(\prod_{j=0}^{n} e(U_j, R_j)\Big) \times e\Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j, R_w\Big) e\Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l, R_m\Big). \tag{5}$$

如果式(5)成立, 则该签名为有效的代理环签名.

4.2 方案正确性

设$(V, R_0, R_1, \cdots, R_n, R_w, R_m)$是身份集$L = \{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$关于消息的$m$代理环签名. 由签名算法可知

$$V = K_\pi^{(1)} \Big(\prod_{j=1}^{n} (U_j)^{r_j}\Big) \Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l\Big)^{r_m}.$$

由代理授权协议可知

$$K_\pi^{(1)} = \sigma_w^{(1)} D_\pi^{(1)} \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_{w_\pi}} = g_2^\alpha (U_0)^{r_{P_0}} \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_w} g_2^\alpha (U_\pi)^{r_{P_\pi}} \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_{w_\pi}},$$

则有

$$V = g_2^{2\alpha} (U_0)^{r_{P_0}} (U_\pi)^{r_{P_\pi}} \Big(\prod_{j=1}^{n} (U_j)^{r_j}\Big) \times \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_w + r_{w_\pi}} \Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l\Big)^{r_m},$$

$$e(V, g) = e\Big(g_2^{2\alpha} (U_0)^{r_{P_0}} (U_\pi)^{r_{P_\pi}} \Big(\prod_{j=1}^{n} (U_j)^{r_j}\Big) \times \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_w + r_{w_\pi}} \Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l\Big)^{r_m}, g\Big) =$$

$$e\Big(g_2^{2\alpha} (U_0)^{r_{P_0}} (U_1)^{r_1} \cdots (U_\pi)^{r_{P_\pi} + r_\pi} \cdots (U_n)^{r_n} \times \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_w + r_{w_\pi}} \Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l\Big)^{r_m}, g\Big) =$$

$$e(g_2^{2\alpha}, g) e(U_0, g)^{r_{P_0}} e(U_1, g)^{r_1} \cdots e(U_\pi, g)^{r_{P_\pi} + r_\pi} \times e(U_n, g)^{r_n} e\Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j, g\Big)^{r_w + r_{w_\pi}} e\Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l, g\Big)^{r_m} =$$

$$e(g_1, g_2)^2 \Big(\prod_{j=0}^{n} e(U_j, R_j)\Big) e\Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j, R_w\Big) \times e\Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l, R_m\Big), \tag{6}$$

因此方案是正确的.

5 安全分析

方案中的代理环签名验证等式包含授权文件、原始签名人和代理签名人集合, 容易看出方案满足可区分性、可验证性、可识别性和不可滥用性等安全性质. 下面证明方案满足匿名性和存在不可伪造性.

5.1 匿名性

定理 1　本文 IBPRS 方案是无条件匿名的.

证明　方案签名$(V, R_0, R_1, \cdots, R_n, R_w, R_m)$中, $\{R_j\}(j = 0, 1, \cdots, \pi-1, \pi+1, \cdots, n)$和$R_m$是随机生成的, 没有提供实际签名者的任何信息. 另外, $R_\pi = g^{r_{P_\pi} + r_\pi}$. 其中: r_{P_π}是由私钥生成中心(与实际签名人独立的)随机生成的, r_π是由实际签名者随机选择的. 因此, R_π的分布是随机的. $R_w = g^{r_w + r_{w_\pi}}$, 其中$r_w$和$r_{w_\pi}$分别由原始签名人和实际签名人随机选择. 因此, R_w的分布也是随机的. 最后考虑

$$V = g_2^{2\alpha} (U_0)^{r_{P_0}} (U_1)^{r_1} \cdots (U_\pi)^{r_{P_\pi} + r_\pi} \cdots (U_n)^{r_n} \Big(w' \prod_{j \in \mathcal{W}} \hat{w}_j\Big)^{r_w + r_{w_\pi}} \Big(m' \prod_{l \in \mathcal{M}} \hat{m}_l\Big)^{r_m}.$$

其中: 指数部分$r_0, r_1, \cdots, r_{P_\pi} + r_\pi, \cdots, r_n, r_w + r_{w_\pi}, r_m$都是随机的, g_2^α是主密钥. 所有参数均没有提供任何有关实际签名人的信息, 对于敌手而言等同于暴力猜测, 因此本文的代理环签名方案是无条件匿名的. □

5.2 存在不可伪造性

定理 2　如果(ε', t')-CDH 困难问题假设在群G上成立, 则 IBPRS 方案是$(\varepsilon, t, q_e, q_d, q_s)$-EU-IBPRS-CMIA 安全的. 其中

$$\varepsilon' \geqslant \varepsilon / (2^{n+6} (q_e + q_d + q_s)^{n+1} (q_d + q_s) q_s \times (n_u + 1)^{n+1} (n_w + 1)(n_m + 1)), \tag{7}$$

$$t' = t + O((q_e n_u + q_d (n_u + n_w) +$$

$$q_s(nn_u+n_w+n_m))\rho+(q_e+q_d+nq_{ps})\tau),\quad(8)$$

ρ 和 τ 分别为群 G 中的乘法和指数运算时间.

证明 设敌手 $\mathcal{A}$ 能以不可忽略的优势攻击上述方案, 则能构造算法 $\mathcal{B}$ 利用 $\mathcal{A}$ 解决 CDH 问题, 从而导致矛盾. 给定 $\mathcal{B}$ 一个 CDH 问题的实例 (g,g^a,g^b), 为了计算 g^{ab}, $\mathcal{B}$ 模仿 $\mathcal{A}$ 的挑战者 $\mathcal{C}$, 具体过程如下:

Step 1 系统建立. $\mathcal{B}$ 设定

$$l_u=2(q_e+q_d+q_s),\ l_w=2(q_d+q_s),\ l_m=2q_s.$$

其中: q_e 是 $\mathcal{A}$ 私钥询问的次数, q_d 是代理指定询问的次数, q_s 是代理签名询问的次数. 选择整数 k_u, k_w 和 k_m, 满足 $0\leqslant k_u\leqslant n_u$, $0\leqslant k_w\leqslant n_w$, $0\leqslant k_m\leqslant n_m$, 并假定 $l_u(n_u+1)<p$, $l_w(n_w+1)<p$, $l_m(n_m+1)<p$. $\mathcal{B}$ 选择 $x'\in_R \mathrm{Z}_{l_u}$ 和长度为 n_u 的向量 $\boldsymbol{X}=(x_i)$, 其中 $x_i\in_R \mathrm{Z}_{l_u}$; 选择 $y'\in_R \mathrm{Z}_{l_w}$ 和长度为 n_w 的向量 $\boldsymbol{Y}=(y_i)$, 其中 $y_i\in_R \mathrm{Z}_{l_w}$; 选择 $z'\in_R \mathrm{Z}_{l_m}$ 和长度为 n_m 的向量 $\boldsymbol{Z}=(z_j)$, 其中 $z_i\in_R \mathrm{Z}_{l_m}$; 选择 $a',b',c'\in_R \mathrm{Z}_p$, 长度为 n_u 的向量 $\boldsymbol{A}=(a_i)$, 长度为 n_w 的向量 $\boldsymbol{B}=(b_j)$ 和长度为 n_m 的向量 $\boldsymbol{C}=(c_k)$, 其中 $a_i,b_j,c_k\in_R \mathrm{Z}_p$.

对于身份 ID_j, $u_j=H_u(\mathrm{ID}_j)$; 对于授权文件 w, $w=H_w(w)$; 对于消息 m 和环成员的身份集 L, $m=H_m(m,L)$. 定义以下函数:

$$F(u_j)=x'+\sum_{i\in\mathcal{U}_j}x_i-l_uk_u,\ J(u_j)=a'+\sum_{i\in\mathcal{U}_j}a_i;$$

$$K(w)=y'_j+\sum_{j\in\mathcal{W}}y_j-l_wk_w,\ L(w)=b'+\sum_{j\in\mathcal{W}}b_j;$$

$$Q(m)=z'+\sum_{k\in\mathcal{M}}z_k-l_mk_m,\ R(m)=c'+\sum_{k\in\mathcal{M}}c_k.$$

算法 $\mathcal{B}$ 构造上述方案中的公开参数为

$$g_1=g^a,\ g_2=g^b;$$

$$u'=g_2^{-l_uk_u+x'}g^{a'},\ u_i=g_2^{x_i}g^{a_i},\ 1\leqslant i\leqslant n_u;$$

$$w'=g_2^{-l_wk_w+y'}g^{b'},\ w_j=g_2^{y_j}g^{b_j},\ 1\leqslant j\leqslant n_w;$$

$$m'=g_2^{-l_mk_m+z'}g^{c'},\ m_k=g_2^{z_k}g^{c_k},\ 1\leqslant k\leqslant n_m.$$

可以看出, 这些参数的分布与一个真正的挑战者所产生的公开参数的分布是一样的, 由此可以得到主密钥为 $g_2^a=g^{ab}$, 同时以下等式也成立:

$$U_j=u'\prod_{i\in\mathcal{U}_j}u_i=g_2^{F(u_j)}g^{J(u_j)},$$

$$w'\prod_{j\in\mathcal{W}}w_j=g_2^{K(w)}g^{L(w)},\ m'\prod_{k\in\mathcal{M}}m_k=g_2^{Q(m)}g^{R(m)}.$$

算法 $\mathcal{B}$ 将公开参数发送给敌手 $\mathcal{A}$.

Step 2 询问. 当敌手 $\mathcal{A}$ 发起私钥询问和签名询问时, 算法 $\mathcal{B}$ 进行如下响应:

1) 用户私钥询问. 对身份为 ID_j 的用户私钥询问, $u_j=H_u(\mathrm{ID}_j)$, 虽然 $\mathcal{B}$ 不知道主密钥, 但在假定 $F(u_j)\neq 0 \bmod l_u$ (根据条件可推出 $F(u_j)\neq 0 \bmod l_u$ 蕴含 $F(u_j)\neq 0 \bmod p$) 的情况下, $\mathcal{B}$ 也能构造其私钥. $\mathcal{B}$ 随机选取 $r_{u_j}\in \mathrm{Z}_p$ 并计算

$$d_{u_j}=(D_j^{(1)},D_j^{(2)})=$$
$$(g_1^{-J(u_j)/F(u_j)}(U_j)^{r_{u_j}},\ g_1^{-1/F(u_j)}g^{r_{u_j}}).\quad(9)$$

令 $\tilde{r}_{u_j}=r_{u_j}-a/F(u_j)$, 可以验证 d_{u_j} 是 ID_j 的有效密钥. 有

$$D_j^{(1)}=g_1^{-J(u_j)/F(u_j)}(U_j)^{r_{u_j}}=$$
$$g_1^{-J(u_j)/F(u_j)}(g_2^{F(u_j)}g^{J(u_j)})^{r_{u_j}}=$$
$$g_2^a(g_2^{F(u_j)}g^{J(u_j)})^{r_{u_j}-a/F(u_j)}=g_2^a(U_j)^{\tilde{r}_{u_j}},$$
$$D_j^{(2)}=g_1^{-1/F(u_j)}g^{r_{u_j}}=g^{r_{u_j}-a/F(u_j)}=g^{\tilde{r}_{u_j}}.\quad(10)$$

如果 $F(u_j)=0 \bmod l_u$, 则上面的计算将无法进行, $\mathcal{B}$ 失败退出.

2) 代理授权询问 I. $\mathcal{A}$ 提交授权文件 w, 原始签名人身份 ID_0 和代理签名人身份 ID_i, $\mathrm{ID}_i\in\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$, $u_0=H_u(\mathrm{ID}_0)$, $w=H_w(w)$, $\mathcal{A}$ 扮演原始签名人角色 P_0, 首先运行算法 $\mathcal{D}$ 产生授权证书

$$\sigma_w=\left(g_2^a(U_0)^{r_{P_0}}\left(w'\prod_{j\in\mathcal{W}}w_j\right)^{r_w},g^{r_{P_0}},g^{r_w}\right),$$

并将 (w,σ_w) 发送给 $\mathcal{B}$. $\mathcal{B}$ 验证 σ_w 的有效性, 如果 σ_w 有效, 则 $\mathcal{B}$ 以下述方法构造代理签名私钥: $u_i=H_u(\mathrm{ID}_i)$. 如果 $F(u_i)\neq 0 \bmod l_u$, 则 $\mathcal{B}$ 先构造 ID_i 的私钥, 然后运行 $\mathcal{P}$ 算法产生 ID_i 的代理签名私钥; 否则, 若在假设 $l_w(n_w+1)<p$ 下蕴含 $K(w)\neq 0 \bmod l_w$, 则 $\mathcal{B}$ 随机选择 $r_{P_i},r_{w_i}\in \mathrm{Z}_p$, 计算代理签名私钥

$$pk_i=$$
$$\left(g_2^a(U_0)^{r_{P_0}}(U_i)^{r_{P_i}}g_1^{-L(w)/K(w)}\times\right.$$
$$\left.\left(w'\prod_{j\in\mathcal{W}}w_j\right)^{r_w+r_{w_i}},\ g^{r_{P_0}},g^{r_{P_i}},g_1^{-1/K(w)}g^{r_w+r_{w_i}}\right)=$$
$$\left(g_2^{2a}(U_0)^{r_{P_0}}(U_i)^{r_{P_i}}\left(w'\prod_{j\in\mathcal{W}}w_j\right)^{r_w+\tilde{r}_{w_i}},\ g^{r_{P_0}},\right.$$
$$\left.g^{r_{P_i}},g^{r_w+\tilde{r}_{w_i}}\right),\quad(11)$$

其中 $\tilde{r}_w=r_w-a/K(w)$; 其他情况 $\mathcal{B}$ 失败退出.

3) 代理授权询问 II. $\mathcal{A}$ 提交授权文件 w, 原始签名人身份 ID_0 和代理签名人身份 ID_i, $\mathrm{ID}_i\in\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$, $\mathcal{A}$ 扮演代理签名人 ID_i, 有 $w=H_w(w)$, $u_0=H_u(\mathrm{ID}_0)$. 如果 $F(u_0)\neq 0 \bmod l_u$, 则 $\mathcal{B}$ 先构造 ID_0 的私钥, 然后运行算法 $\mathcal{D}$ 产生授权证书 σ_w; 否则, 若 $K(w)\neq 0 \bmod l_w$, 则 $\mathcal{B}$ 随机选择 $r_{P_0},r_w\in \mathrm{Z}_p$, 计算

$$\sigma_w=\left(g_1^{-L(w)/K(w)}(U_0)^{r_{P_0}}\left(w'\prod_{j\in\mathcal{W}}w_j\right)^{r_w},\right.$$
$$\left.g^{r_{P_0}},g_1^{-1/K(w)}g^{r_w}\right)=$$
$$\left(g_2^a(U_0)^{r_{P_0}}\left(w'\prod_{j\in\mathcal{W}}w_j\right)^{\tilde{r}_w},g^{r_{P_0}},g^{\tilde{r}_w}\right),\quad(12)$$

其中 $\tilde{r}_w = r_w - a/K(w)$; 其他情况 $\mathcal{B}$ 失败退出.

4) 签名询问. $\mathcal{A}$ 提交授权文件 w, 原始签名人身份 ID_0, 代理签名人身份列表 $L = \{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$ 和消息 m, $u_0 = H_u(\mathrm{ID}_0)$, $w = H_w(w)$, $\mathcal{A}$ 扮演原始签名人角色 P_0, 提交签名询问 (ID_0, L, w, m). 首先运行算法 $\mathcal{D}$ 产生授权证书

$$\sigma_w = \left(g_2^{\alpha}(U_0)^{r_{P_0}}\left(w'\prod_{j\in\mathcal{W}} w_j\right)^{r_w}, g^{r_{P_0}}, g^{r_w}\right), \quad (13)$$

并将 (w, σ_w) 发送给 $\mathcal{B}$. $\mathcal{B}$ 验证 σ_w 的有效性, 如果 σ_w 有效, 则 $\mathcal{B}$ 以下述方法构造部分代理签名: 首先计算 $u_i = H_u(\mathrm{ID}_i)$, $i = 1, 2, \cdots, n$, 如果 $F(u_j) \neq 0 \bmod l_u$ 或 $K(w) \neq 0 \bmod l_w$, 则 $\mathcal{B}$ 先构造 ID_i 的代理签名私钥, 然后运行 PRS 算法产生签名; 否则, 计算 $m = H_m(L, m)$, 如果 $Q(m) \neq 0 \bmod l_m$, 则 $\mathcal{B}$ 随机选择 r_1, $r_2, \cdots, r_n, r_m \in Z_p$, 并计算

$$\begin{aligned}
&p\sigma = \\
&\left(g_2^{a}(U_0)^{r_{P_0}}\left(w'\prod_{k\in\mathcal{W}} w_k\right)^{r_w}\prod_{j}^{n}(U_j)^{r_j}g_1^{-R(m)/Q(m)}\right)\times \\
&\left(m'\prod_{l\in\mathcal{M}} m_l\right)^{r_m}, g^{r_{P_0}}, g^{r_1}, \cdots, g^{r_i}, \cdots, \\
&g^{r_n}, g^{r_w}, g_1^{-1/Q(m)}g^{r_m}\Big) = \\
&\Big(g_2^{2a}(U_0)^{r_{P_0}}\prod_{j}^{n}(U_j)^{r_j}\left(w'\prod_{k\in\mathcal{W}} w_k\right)^{r_w}(m'\prod_{l\in\mathcal{M}} m_l)^{\tilde{r}_m}, \\
&g^{r_{P_0}}, g^{r_1}, \cdots, g^{r_i}, \cdots, g^{r_n}, g^{r_w}, g^{\tilde{r}_m}\Big), \quad (14)
\end{aligned}$$

其中 $\tilde{r}_m = r_m - a/Q(m)$; 其他情况 $\mathcal{B}$ 失败退出.

Step 3　伪造. 如果 $\mathcal{B}$ 能够回答 $\mathcal{A}$ 所有的询问, 则 $\mathcal{B}$ 没有失败退出, 且 $\mathcal{A}$ 能以不可忽略的概率 ε 输出一个有效的伪造, 该伪造可以是下述 2 种情形之一:

1) $\mathcal{A}$ 伪造一个原始签名人 ID_0^* 授权文件 w^* 的授权证书 $\sigma_{w^*} = (\sigma_{w^*}^{(1)}, \sigma_{w^*}^{(2)}, \sigma_{w^*}^{(3)})$, 没有提交 ID_0^* 私钥询问和 (ID_0^*, w^*) 代理授权询问, 有 $u_0^* = H_u(\mathrm{ID}_0^*)$, $w^* = H_w(w^*)$, 如果 $F(u_0^*) = 0 \bmod p$ 且 $Q(w^*) = 0 \bmod p$, 则 $\mathcal{B}$ 计算并输出

$$\begin{aligned}
&\frac{\sigma_{w^*}^{(1)}}{(\sigma_{w^*}^{(2)})^{J(u_0^*)}(\sigma_{w^*}^{(3)})^{R(w^*)}} = \frac{g_2^{a}(U_0)^{r_{P_0}}\left(w'\prod_{k\in\mathcal{W}} w_k\right)^{r_w}}{g^{J(\mathrm{u}_0^*)r_{P_0}}g^{R(\mathrm{w}^*)r_{\mathrm{w}}}} = \\
&\frac{g_2^{a}(g_2^{F(u_0^*)}g^{J(u_0^*)})^{r_{P_0}}(g_2^{Q(w^*)}g^{R(w^*)})^{r_w}}{g^{J(u_0^*)r_{P_0}}g^{R(w^*)r_w}} = g_2^{a} = g^{ab}, \quad (15)
\end{aligned}$$

式 (15) 即为 CDH 问题实例的解; 否则 $\mathcal{B}$ 失败退出.

2) $\mathcal{A}$ 伪造一个在 $(\mathrm{ID}_0^*, w^*, m^*, L^*)$ 下的代理环签名 $p\sigma^* = (V^*, R_0^*, R_1^*, \cdots, R_n^*, R_w^*, R_m^*)$. 其中: $L^* = \{\mathrm{ID}_1^*, \mathrm{ID}_2^*, \cdots, \mathrm{ID}_n^*\}$. $u_j^* = H_u(\mathrm{ID}_j^*)$, $w^* = H_w(w^*)$, $m^* = H_m(m^*, L^*)$, 如果对于所有 $j \in \{0, 1, \cdots, n\}$, 有 $F(u_j^*) = 0 \bmod p$, $K(w^*) = 0 \bmod p$ 且 $Q(m^*) = 0 \bmod p$, 则 $\mathcal{B}$ 计算

$$\begin{aligned}
&V^*/((R_0^*)^{J(u_0^*)}(R_1^*)^{J(u_1^*)}\cdots(R_n^*)^{J(u_n^*)}\times \\
&(R_w^*)^{L(w^*)}(R_m^*)^{R(m^*)}) = \\
&\left(g_2^{2a}(U_0^*)^{r_0}(U_1^*)^{r_1}\cdots(U_n^*)^{r_n}\left(w'\prod_{j\in\mathcal{W}} w_j\right)^{r_w}\times\right. \\
&\left.\left(m'\prod_{l\in\mathcal{M}} m_l\right)^{r_m}\right)\Big/(g^{J(u_0^*)}g^{J(u_1^*)r_1}\cdots \\
&g^{J(u_n^*)r_n}g^{L(w^*)r_w}g^{R(m^*)r_m}) = \\
&g_2^{2a}(g_2^{F(u_0^*)}g^{J(u_0^*)})^{r_0}(g_2^{F(u_1^*)}g^{J(u_1^*)})^{r_1}\cdots \\
&((g_2^{F(u_n^*)}g^{J(u_n^*)})^{r_n}(g_2^{K(w^*)}g^{L(w^*)})^{r_w}(g_2^{Q(m^*)}g^{R(m^*)})^{r_m})/ \\
&(g^{J(u_0^*)r_0}g^{J(u_1^*)r_1}\cdots g^{J(u_n^*)r_n}g^{J(w^*)r_w}g^{R(m^*)r_m}) = \\
&g_2^{2a} = (g^{ab})^2. \quad (16)
\end{aligned}$$

式 (16) 的输出 $(g^{ab})^2$ 即为 CDH 问题实例的解, 可以在多项式时间内求出.

综上所述, 如果存在一个敌手 $\mathcal{A}$ 能够以不可忽略的概率给出一个有效的伪造, 则存在一个算法 $\mathcal{B}$ 能够以不可忽略的概率解决 CDH 问题, 这与 CDH 问题是一个困难问题相矛盾, 故方案是 EU-IBPTPS-CMIA 安全的.

Step 4　概率分析. 通过分析 $\mathcal{B}$ 不放弃游戏的概率来评估 $\mathcal{B}$ 模拟成功的概率. 模拟不中断需要满足如下 5 个条件:

1) 在身份为 ID 的用户私钥询问中 $F(u) \neq 0 \bmod l_u$, 其中 $u = H_u(\mathrm{ID})$;

2) 代理授权询问 I 中 $F(u_j) \neq 0 \bmod l_u$ 或 $K(w) \neq 0 \bmod l_w$, 其中 $w = H_w(w)$;

3) 代理授权询问 II 中 $F(u_0) \neq 0 \bmod l_u$ 或 $K(w) \neq 0 \bmod l_w$;

4) 签名询问中 $F(u_j) \neq 0 \bmod l_u$ 或 $K(w) \neq 0 \bmod l_w$ 或 $Q(m) \neq 0 \bmod l_m$, 其中 $m = H_m(L, m)$;

5) 伪造授权证书满足 $F(u_0^*) = 0 \bmod p$ 和 $Q(w^*) = 0 \bmod p$, 伪造签名满足对于所有 $j \in \{0, 1, \cdots, n\}$, 有 $F(u_j^*) = 0 \bmod p$, $K(w^*) = 0 \bmod p$ 且 $Q(m^*) = 0 \bmod p$.

为了简化对模拟者的分析, 只考虑在该事件上一个子集的概率. 设在用户私钥询问、不包括身份 ID_k^* 的代理授权询问和签名询问中的身份分别为 $\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_{q_I}$, 在包括身份 ID_k^* 而不包括授权文件 w^* 的代理指定询问和签名询问中的授权文件分别为 $W_1, W_2, \cdots, W_{q_W}$, 在包括身份列表 L^* 和授权文件 w^* 的签名询问中的消息为 $M_1, M_2, \cdots, M_{q_M}$. 显然有 $q_I \leqslant q_e + q_d + q_s$, $q_W \leqslant q_d + q_s$, $q_M \leqslant q_s$. 定义事件 A_i, A^*, B_j, B^*, C_l, C^* 分别为

$$A_i : F(u_i) \neq 0 \bmod l_u,\ A^* : F(u_k^*) = 0 \bmod p,$$

$B_j : K(w_j) \neq 0 \bmod l_w,\ B^* : K(w^*) = 0 \bmod p,$

$C_l : Q(m_l) \neq 0 \bmod l_m,\ C^* : Q(m^*) = 0 \bmod p.$

根据以上分析, 算法没有失败退出的概率为

$$\Pr[\neg\text{abort}] \geqslant \Pr\Big[\Big(\bigcap_{i=1}^{q_I} A_i \bigwedge A^*\Big) \bigwedge \Big(\bigcap_{j=1}^{q_W} B_j \bigwedge B^*\Big) \bigwedge \Big(\bigcap_{l=1}^{q_M} C_l \bigwedge C^*\Big)\Big]. \tag{17}$$

可以看出, 事件$\bigcap_{i=1}^{q_I} A_i \bigwedge A^*$, $\bigcap_{j=1}^{q_W} B_j \bigwedge B^*$ 和$\bigcap_{l=1}^{q_M} C_l \bigwedge C^*$ 是相互独立的. 由假设 $l_u(n_u+1) < p$ 可知, $F(u) = 0 \bmod p$ 蕴涵 $F(u) = 0 \bmod l_u$, 可得

$$\Pr[A^*] = \prod_{k=0}^{n} \Pr[F(u_k^*) = 0 \bmod p \bigwedge F(u_k^*) = 0 \bmod l_u] = \prod_{k=0}^{n} \Pr[F(u_k^*) = 0 \bmod l_u] \times \Pr[F(u_k^*) = 0 \bmod p | F(u_k^*) = 0 \bmod l_u] = 1/(l_u^{n+1}(n_u+1)^{n+1}). \tag{18}$$

另外, 对于任意 i, 事件 A_i 和 A^* 相互独立, 且 $\Pr[\neg A_i | A^*] = 1/l_u$, 则有

$$\Pr\Big[\bigcap_{i=1}^{q_I} A_i | A^*\Big] = 1 - \Pr\Big[\bigcup_{i=1}^{q_I} \neg A_i | A^*\Big] \geqslant 1 - \sum_{i=1}^{q_I} \Pr[\neg A_i | A^*] = 1 - q_I/l_u. \tag{19}$$

所以可得到

$$\Pr\Big[\bigcap_{i=1}^{q_I} A_i \bigwedge A^*\Big] = \Pr[A^*] \Pr\Big[\bigcap_{i=1}^{q_I} A_i | A^*\Big] \geqslant \frac{1}{l_u^{n+1}(n_u+1)^{n+1}}\Big(1 - \frac{q_I}{l_u}\Big) \geqslant \frac{1}{l_u^{n+1}(n_u+1)^{n+1}}\Big(1 - \frac{q_e+q_d+q_s}{l_u}\Big). \tag{20}$$

由设定 $l_u = 2(q_e+q_d+q_s)$, 可得

$$\Pr\Big[\bigcap_{i=1}^{q_I} A_i \bigwedge A^*\Big] \geqslant 1/(2^{n+2}(q_e+q_d+q_s)^{n+1}(n_u+1)^{n+1}). \tag{21}$$

类似分析可得

$$\Pr\Big[\bigcap_{j=1}^{q_W} B_j \bigwedge B^*\Big] \geqslant \frac{1}{4(q_d+q_s)(n_w+1)},$$

$$\Pr\Big[\bigcap_{l=1}^{q_M} C_l \bigwedge C^*\Big] \geqslant \frac{1}{4q_s(n_m+1)}. \tag{22}$$

因此有

$$\Pr[\neg\text{abort}] \geqslant \Pr\Big[\bigcap_{i=1}^{q_I} A_i \bigwedge A^* \bigwedge \bigcap_{j=1}^{q_W} B_j \bigwedge B^* \bigcap_{l=1}^{q_M} C_l \bigwedge C^*\Big] \geqslant \frac{1}{2^{n+2}(q_e+q_d+q_s)^{n+1}(n_u+1)^{n+1}} \times \frac{1}{4(q_d+q_s)(n_w+1)} \times \frac{1}{4q_s(n_m+1)} = \frac{1}{2^{n+6}(q_e+q_d+q_s)^{n+1}(q_d+q_s)} \times \frac{1}{q_s(n_u+1)^{n+1}(n_w+1)(n_m+1)}. \tag{23}$$

Step 5 时间复杂度分析. 算法的时间复杂度由用户私钥询问、代理授权询问和签名询问中的乘法运算和指数运算次数决定. 因为在用户私钥询问、代理授权询问和签名询问中的乘法运算次数分别是 $O(n_u)$, $O(n_u+n_w)$ 和 $O(nn_u+n_w+n_m)$, 指数运算次数分别为 $O(1)$, $O(1)$ 和 $O(n)$, 所以算法 $\mathcal{B}$ 的时间复杂度满足式 (8). □

6 结 论

代理环签名是一种重要的且具有特殊性质的签名形式, 能有效解决在代理签名中对于代理签名者身份的匿名保护问题. 现有的基于身份的代理环签名方案的安全性大都是在随机预言模型下证明的, 鉴于此, 本文设计了一个新的基于身份的代理环签名方案, 并在标准模型下证明了方案基于计算性 Diffie-Hellman 困难假设是存在性不可伪造和无条件匿名性的. 相对于随机预言模型下可证安全的方案而言, 本文方案具有更高的安全性. 方案的签名长度和代理环成员数成线性关系, 如何在标准模型下设计签名长度更短的高效安全方案是进一步要研究的内容.

参考文献(References)

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

[2] Chaum D, Heyst V E. Group signatures[C]. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1991, 547: 257-265.

[3] Wang L L, Zhang G Y, Ma C G. A survey of ring signature[J]. Frontiers of Electrical and Electronic Engineering in China, 2008, 3(1): 10-19.

[4] Shamir A. Identity-based cryptosystems and signature schemes[C]. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1985, 196: 47-53.

[5] Zhang F G, Kim K. ID-based blind signature and ring signature from pairings[C]. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2002, 2501: 533-547.

[6] Chow S S M, Lui R W C, Hui L C K, et al. Identity based ring signature: Why, how and what next[C]. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2005, 3545: 144-161.

(下转第373页)