DOI:10.13878/j.cnki.jnuist.2017.05.005

张亦辰[1]　李继国[1]　袁泓[1]

# 无证书代理签名方案

**摘要**

为了避免基于身份密码系统中的密钥托管问题和传统公钥密码的证书管理问题,利用双线性对,提出了一种无证书代理签名方案.基于计算 Diffie-Hellman 困难问题假定,在随机预言模型下证明了方案的安全性.与已有的同类方案的性能进行了比较,结果表明提出的方案在计算代价和通信代价上有一定的优势.

**关键词**

无证书签名;双线性对;代理签名;随机预言模型

**中图分类号** TP309

**文献标志码** A

**收稿日期** 2017-06-25

**资助项目** 国家自然科学基金(61672207, 61272542);江苏省自然科学基金(BK20161511);中央高校基本科研业务费重点培育专项(2016B10114);中美计算机科学研究中心开放课题 (KJR16039)

**作者简介**

张亦辰,女,博士,副教授,研究方向为密码学理论与技术.zyc_718@163.com

1　河海大学 计算机与信息学院,南京,211100

## 0　引言

2003 年,Al-Riyami 等[1]提出无证书公钥密码体制.无证书公钥签名方案不需要公钥证书,解决了传统公钥密码技术中证书管理与认证的问题,在应用中带来极大的便利.无证书公钥密码体制,需要一个可信第三方 KGC.与基于身份的密码体制下的 PKG 不同,KGC 根据用户的身份 ID 为用户生成部分私钥,用户根据 KGC 产生的部分私钥和自己产生的秘密值共同生成私钥,所以 KGC 不知道用户的私钥,解决了基于身份的密钥托管问题.无证书签名一经提出就受到广泛关注,一些无证书签名方案陆续被提出[2-9].文献[2-3]推广了环签名概念,提出了无证书环签名方案.文献[4-5]对几种无证书签名方案的安全性进行分析并提出了相应的改进方案.Yang 等[6]提出了无证书盲签名方案.为了同时实现签名和加密的功能并提高效率,Li 等[8]提出了无证书在线/离线签名方案.最近,Lu 等[9]提出了无证书强密钥隔离签名方案,并在标准模型下证明了方案的安全性.

1996 年,Mambo 等[10]首次提出代理签名的概念,它指当某个签名人因某种原因不能签名时,将签名权委托给他人(称为代理人)替自己行使签名权,并根据授权对代理签名做了分类,即完全授权方案、部分授权方案和证书授权方案.文献[10]中的方案由于代理签名私钥中没有任何代理签名者的认证信息,所以不能满足强不可否认性的特征,即代理签名者能够否认他或她已经生成的代理签名.有鉴于此,根据不可否认性的特征,在文献[11]中,Lee 等把代理签名分为强代理签名和弱代理签名.弱代理签名仅仅表示原始签名者的签名,代理签名者能够对除原始签名者之外的人否认自己生成这个签名;强代理签名表示原始签名者和代理签名者双方共同产生的签名,一旦代理签名者生成一个有效的代理签名,代理签名者不能对任何人(包括原始签名者)否认这个自己生成的签名.

2005 年,Li 等[12]提出了一个无证书代理签名方案(称为 LCS 方案),并声称该方案满足代理签名所要求的安全性质.Yap 等[13]指出 LCS 方案不能抵抗公钥替换攻击.2009 年,张磊等[14]给出了一类无证书签名方案的构造方法.为了改进通信效率,Chen 等[15]提出了可证安全的无证书短代理签名方案,该方案能适应带宽受限的环境.为了处理密钥泄露问题,Li 等[16]提出了一个前向安全的无证书代理签名方案,基于计算 Diffie-Hellman 困难问题假定,在随机预言模型下证明了

方案的安全性.最近,Lu 等[17]提出了一个标准模型下安全的无证书代理签名方案.为了提高方案的性能,本文提出了一种高效的无证书代理签名方案.

## 1 预备知识

### 1.1 双线性对

令 $G_1$ 为加法循环群,阶为大素数 $q$,$G_2$ 为阶为 $q$ 的乘法循环群,$P$ 为 $G_1$ 的生成元.双线性对是指满足下列性质的一个映射 $e:G_1 \times G_1 \rightarrow G_2$.

双线性:对任意的 $P \in G_1, Q \in G_1, a \in Z_q^*, b \in Z_q^*$,有 $e(aP,bQ)=e(P,Q)^{ab}$.

非退化性:存在 $P \in G_1, Q \in G_1$,使得 $e(P,Q) \neq 1$.

可计算性:对任意的 $P \in G_1, Q \in G_1$,存在有效算法计算 $e(P,Q)$.

### 1.2 困难问题

1)离散对数(DL)问题:给定 $P \in G_1, Q \in G_1$,找出整数 $n$,使得 $Q=nP$,如果这样的 $n$ 存在.

2)计算 Diffie-Hellman(CDH)问题:给定三元组 $(P,aP,bP) \in G_1^3, \forall a,b \in Z_p^*$,计算 $abP$.

3)如果任意的概率多项式时间敌手均不能够以一个不可忽略的优势来解决 CDH 问题,则称 CDH 困难性假设是成立的.

## 2 无证书代理签名的定义及安全模型

### 2.1 无证书代理签名定义

无证书代理签名由参数设置、部分私钥生成、秘密值生成、用户密钥生成、公钥生成、代理密钥产生、代理签名、代理签名验证 8 个算法组成.前 2 个算法由 KGC 执行,其他算法由用户执行.算法具体描述如下:

1)参数设置:输入系统安全参数 $k$、输出系统主密钥 *mastre-key*、系统公开参数 *params*.其中系统公开参数 *params* 向系统中的所有用户公开,系统主密钥 *mastre-key* 由 KGC 秘密保存.

2)部分私钥生成:输入系统参数 *params*、用户身份 *ID*、系统主密钥 *mastre-key*,KGC 为用户生成部分私钥 $D_{ID}$.

3)秘密值生成:输入系统参数 *params*、用户身份 *ID*,输出用户的秘密值 $x_{ID}$.

4)用户密钥生成:输入系统参数 *params*、用户身份 *ID*、用户秘密值 $x_{ID}$ 及用户的部分私钥 $D_{ID}$,输出用户的私钥 $S_{ID}$.

5)公钥生成:输入系统参数 *params*、用户身份 *ID*、用户秘密值 $x_{ID}$,输出该用户的公钥 $P_{ID}$.

6)代理密钥产生:输入系统参数 *params*、原始签名人身份 $ID_A$、秘密值 $x_{ID_A}$、部分私钥 $D_{ID_A}$、代理签名人身份 $ID_B$、秘密值 $x_{ID_B}$、部分私钥 $D_{ID_B}$、授权证书 $w$,输出代理密钥 $S_p$.

7)代理签名:输入系统参数 *params*、消息 $m$、原始签名人身份 $ID_A$、代理签名人身份 $ID_B$、代理密钥 $S_p$,输出代理签名 $u$.

8)代理签名验证:输入系统参数 *params*、消息 $m$、原始签名人身份 $ID_A$、代理签名人身份 $ID_B$、代理签名 $u$、原始签名人及代理签名人的公钥 $P_{ID_A}$ 和 $P_{ID_B}$,验证有效时,输出 1,否则输出 0.

### 2.2 安全模型

根据文献[1,4],无证书签名方案中存在两类敌手,即第Ⅰ类敌手与第Ⅱ类敌手.第Ⅰ类敌手不知道系统主密钥,但可以替换任意用户的公钥.第Ⅱ类敌手知道系统主密钥,但是不能替换目标用户的公钥.无证书代理签名方案的安全性可以用挑战者 $C$ 和两类敌手 $A$ 之间的游戏来定义.

**定义 1**(对第Ⅰ类敌手而言):

1)初始化:$C$ 运行系统参数生成算法,输入安全参数 $k$,输出系统主密钥 *mastre-key* 和系统参数 *params*.$C$ 将 *params* 发给 $A$,保存 *mastre-key*.

2)询问:$A$ 适应性地进行公钥询问、部分私钥询问、秘密值询问、公钥替换询问、代理密钥询问及代理签名询问,$C$ 模拟方案中的相应算法做出响应.

3)伪造:最后 $A$ 输出四元组 $(m^*,w^*,h^*,u^*)$,$A$ 赢得该游戏,当且仅当:① $u^*$ 是原始签名人 $ID_A^*$,代理签名人 $ID_B^*$ 对 $m^*$ 的有效代理签名;② $A$ 没有询问过 $ID_A^*$ 和 $ID_B^*$ 的部分私钥;③ $A$ 没有询问过原始签名人 $ID_A^*$ 和代理签名人 $ID_B^*$ 的代理密钥 $S_p$;④ $A$ 没有询问过原始签名人 $ID_A^*$ 和代理签名人 $ID_B^*$ 对消息 $m^*$ 的代理签名.

**定义 2**(对第Ⅱ类敌手而言):

1)初始化:$C$ 运行系统参数生成算法,输入安全参数 $k$,输出系统主密钥 *mastre-key* 和系统参数 *params*.$C$ 将 *mastre-key* 和 *params* 发给 $A$.

2)询问:$A$ 适应性地进行公钥询问、秘密值询问、公钥替换询问、代理密钥询问及代理签名询问,$C$ 模拟方案中的相应算法做出响应.

3)伪造:最后 $A$ 输出四元组 $(m^*,w^*,h^*,u^*)$,$A$ 赢得该游戏,当且仅当:① $u^*$ 是原始签名人 $ID_A^*$,

代理签名人 $ID_B^*$ 对 $m^*$ 的有效代理签名;② $A$ 没有询问过 $ID_A^*$ 和 $ID_B^*$ 的秘密值且没有替换过 $ID_A^*$ 和 $ID_B^*$ 的公钥;③ $A$ 没有询问过原始签名人 $ID_A^*$ 和代理签名人 $ID_B^*$ 的代理密钥 $S_p$;④ $A$ 没有询问过原始签名人 $ID_A^*$ 和代理签名人 $ID_B^*$ 对消息 $m^*$ 的代理签名.

## 3 无证书代理签名方案构造

无证书代理签名方案由下面几个算法组成:

1)参数设置:输入系统安全参数 $k$.$G_1$ 和 $G_2$ 分别是阶为大素数 $q$ 的加法循环群和乘法循环群($q$ 为大素数),$P$ 为 $G_1$ 的生成元,$e:G_1\times G_1\to G_2$ 是双线性映射.$H_1:\{0,1\}^*\to G_1^*$,$H_2:\{0,1\}^*\to G_1^*$,$H_3:\{0,1\}^*\times G_2^*\to Z_q^*$ 是 Hash 函数,其中,$G_1^*=G_1\backslash\{0\}$,$G_2^*=G_2\backslash\{1\}$.KGC 随机选择 $t\in Z_q^*$ 作为主密钥并保存,计算主公钥 $P_{\text{pub}}=tP$,公开系统参数:$params=\{G_1,G_2,e,q,P,P_{\text{pub}},H_1,H_2,H_3\}$.

2)部分私钥生成:原始签名人 $A$ 和代理签名人 $B$ 的身份信息分别为 $ID_A$,$ID_B$,KGC 计算 $Q_{ID_A}=H_1(ID_A)$,$Q_{ID_B}=H_1(ID_B)$,并为其生成部分私钥 $D_{ID_A}=tQ_{ID_A}$,$D_{ID_B}=tQ_{ID_B}$,将 $D_{ID_A}$,$D_{ID_B}$通过安全信道分别发送给 $A$,$B$.$A$,$B$ 通过等式 $e(D_X,P)=e(Q_X,P_{\text{pub}})$ 来验证 $D_X$ 的真实性,其中 $X$ 代表 $ID_A$,$ID_B$.

3)秘密值生成:$A$,$B$ 随机选择 $x_{ID_A},x_{ID_B}\in Z_q^*$,作为各自的秘密值.

4)用户密钥生成:输入原始签名人 $A$ 和代理签名人 $B$ 的身份信息 $ID_A$,$ID_B$,秘密值 $x_{ID_A}$,$x_{ID_B}$,部分私钥 $D_{ID_A}$,$D_{ID_B}$,则 $A$,$B$ 的私钥分别为($D_{ID_A}$,$x_{ID_A}$),($D_{ID_B}$,$x_{ID_B}$).

5)公钥生成:输入系统参数 $params$、原始签名人 $A$ 和代理签名人 $B$ 的身份信息 $ID_A$,$ID_B$,秘密值 $x_{ID_A}$,$x_{ID_B}$,则 $A$,$B$ 分别计算其公钥 $P_{ID_A}=x_{ID_A}P$,$P_{ID_B}=x_{ID_B}P$.

6)代理密钥生成:输入系统参数 $params$、原始签名人 $A$ 和代理签名人 $B$ 的身份信息 $ID_A$,$ID_B$,秘密值 $x_{ID_A}$,$x_{ID_B}$,部分私钥 $D_{ID_A}$,$D_{ID_B}$,原始签名人建立一个用于说明 $A$,$B$ 身份和授权范围期限等内容的授权许可信息 $w$,计算 $w$ 的授权证书 $S_w=x_{ID_A}H_2(ID_A,ID_B,w)+D_{ID_A}$,将($w$,$S_w$)通过安全信道发送给 $B$.代理签名人 $B$ 首先验证等式 $e(S_w,P)=e(H_2(ID_A,ID_B,w),P_{ID_A})e(Q_{ID_A},P_{\text{pub}})$ 是否成立.如果不成立,则终止代理过程;否则计算代理签名密钥 $S_p=S_w+x_{ID_B}H_2(ID_A,ID_B,w)+D_{ID_B}$.

7)代理签名生成:输入系统参数 $params$、消息 $m\in\{0,1\}^*$、原始签名人身份 $ID_A$、代理签名人身份 $ID_B$、代理密钥 $S_p$.代理签名人 $B$ 随机选择 $r\in Z_q^*$,并计算 $R=e(P,P)^r$,$h=H_3(ID_A,ID_B,m,R)$,$u=hS_p+rP$.用户 $B$ 对消息 $m$ 的代理签名为($m$,$w$,$h$,$u$).

8)代理签名的验证:输入系统参数 $params$、原始签名人和代理签名人身份 $ID_A$,$ID_B$,公钥 $P_{ID_A}$,$P_{ID_B}$,验证者收到签名($m$,$w$,$h$,$u$)后,计算:$Q_{ID_A}=H_1(ID_A)$,$Q_{ID_B}=H_1(ID_B)$,$R'=e(u,P)e(H_2(ID_A,ID_B,w),P_{ID_A}+P_{ID_B})^{-h}e(Q_{ID_A}+Q_{ID_B},P_{\text{pub}})^{-h}$,当且仅当 $h=H_3(ID_A,ID_B,m,R')$ 时接受签名;否则,拒绝签名.

## 4 安全性证明

**定理 1** 在随机预言模型下,若存在第Ⅰ类敌手 $A$ 能在多项式时间内,进行最多 $q_{H_i}$ 次 $H_i(i=1,2,3)$ 哈希询问、$q_k$ 次公钥询问、$q_R$ 次公钥替换询问、$q_e$ 次部分私钥询问、$q_{pk}$次代理密钥询问、$q_{ps}$次代理签名询问,以最多 $\varepsilon$ 的概率成功伪造有效代理签名,则存在算法 $C$ 能在多项式时间内以最多 $\varepsilon'\geqslant\varepsilon(1-1/(2^k-q_{H_3}-q_{ps}))^{q_{ps}+1}/\binom{q_{H_1}}{2}$ 的概率解决 CDH 问题.

**证明** 假设挑战者 $C$ 要解决 CDH 困难问题,输入($aP$,$bP$),目标是要计算出 $abP$.证明思路是如果存在第Ⅰ类敌手 $A$,能以不可忽略的概率攻破本方案,则 $C$ 能利用算法 $A$ 解决 CDH 问题,过程如下:

1)参数设置:输入安全参数 $k$,方案中存在 2 个目标用户,原始签名人 $ID_A^*$ 和代理签名人 $ID_B^*$.$C$ 置 $P_{\text{pub}}=aP$,选择系统参数 $params=\{G_1,G_2,e,q,P,P_{\text{pub}},H_1,H_2,H_3\}$,然后 $C$ 将系统参数发给 $A$.将哈希函数 $H_1$,$H_2$,$H_3$ 看作随机预言机.假设 $A$ 每次的询问是不同的.

2)$H_1$ 询问:$C$ 维护一个列表 $H_1^{\text{list}}$,格式为($ID$,$\alpha$,$Q_{ID}$,$D_{ID}$),初始化为空.假设 $A$ 最多做 $q_{H_1}$ 次 $H_1$ 询问,$C$ 在[1,$q_{H_1}$]中随机选择一个值 $l$.当敌手 $A$ 询问 $ID_i$ 时:

① 如果 $ID_i=ID_A^*$,设置 $Q_{ID_A}^*=\lambda bP$,添加($ID_A^*$,$\perp$,$Q_{ID_A}^*$,$\perp$)到 $H_1^{\text{list}}$,返回 $Q_{ID_A}^*$给敌手 $A$.

② 如果 $ID_i=ID_l=ID_B^*$,设置 $Q_{ID_B}^*=bP$,添加($ID_B^*$,$\perp$,$Q_{ID_B}^*$,$\perp$)到 $H_1^{\text{list}}$,返回 $Q_{ID_B}^*$给敌手 $A$.

③ 否则,随机选择 $\alpha_{ID_i}\in Z_q^*$,计算 $Q_{ID_i}=\alpha_{ID_i}P$,$D_{ID}=\alpha_{ID_i}P_{\text{pub}}$,添加($ID_i$,$\alpha_{ID_i}$,$Q_{ID_i}$,$D_{ID_i}$)到 $H_1^{\text{list}}$,返回 $Q_{ID_i}$给敌手 $A$.

3)$H_2$ 询问:$C$ 维护一个列表 $H_2^{\text{list}}$,格式为($ID_i$,$ID_j$,$w$,$\beta_{ij}$,$H_w$),初始化为空.$A$ 询问 $H_2(ID_i,ID_j,w)$ 时,$C$ 随机选择 $\beta_{ij}\in Z_q^*$,计算 $H_w=\beta_{ij}P$,添加($ID_i$,$ID_j$,$w$,$\beta_{ij}$,$H_w$)到 $H_2^{\text{list}}$,返回 $H_w$ 给敌手 $A$.

4)$H_3$ 询问:$C$ 维护一个列表 $H_3^{\text{list}}$,格式为($ID_i$,$ID_j$,$m$,$R$,$h_{ij}$),初始化为空.$A$ 询问 $H_3(ID_i,ID_j,m,R)$ 时,$C$ 随机选择 $h_{ij}\in Z_q^*$,添加($ID_i$,$ID_j$,$m$,$R$,$h_{ij}$)到 $H_3^{\text{list}}$ 中,返回 $h_{ij}$给 $A$.

5)部分私钥询问:若 $ID_i=ID_A^*$,$C$ 终止;若 $ID_j=ID_l=ID_B^*$,$C$ 终止;否则检索 $H_1^{\text{list}}$ 找到($ID_i$,$\alpha_{ID_i}$,$Q_{ID_i}$,$D_{ID_i}$),返回 $D_{ID_i}$给 $A$,如果 $H_1^{\text{list}}$ 列表中不存在,则进行 $H_1$ 询问.

6)公钥询问:$C$ 维护一个列表 $K^{\text{list}}$,格式为($ID$,$x$,$P_{ID}$),初始化为空.$A$ 询问 $ID_i$ 的公钥时,$C$ 检索 $K^{\text{list}}$,如果 $K^{\text{list}}$存在元组($ID_i$,$x_i$,$P_{ID_i}$),返回 $P_{ID_i}$给 $A$.如果不存在,$C$ 随机选择 $x_i\in Z_p^*$,计算 $P_{ID_i}=x_iP$,添加($ID_i$,$x_i$,$P_{ID_i}$)到 $K^{\text{list}}$,返回 $P_{ID_i}$给 $A$.

7)公钥替换询问:假定 $A$ 对身份为 $ID_i$ 用户公钥进行替换询问($ID_i$,$P_{ID_i}'$)时,$C$ 检索 $K^{\text{list}}$列表,并将元组($ID_i$,$x_i$,$P_{ID_i}$)替换为($ID_i$,$\perp$,$P_{ID_i}'$).

8)秘密值询问:当 $A$ 对身份 $ID_i$ 用户的秘密值询问时,$C$ 检索 $K^{\text{list}}$找到($ID_i$,$x_i$,$P_{ID_i}$),若 $x_i=\perp$,表明身份为 $ID_i$ 用户公钥已经被替换,$C$ 无法回答 $A$ 的秘密值询问,返回 $\perp$ 给 $A$,否则返回 $x_i$ 给 $A$.如果 $C$ 检索 $K^{\text{list}}$没有找到相应的项,则 $C$ 随机选择 $x_i\in Z_p^*$,计算 $P_{ID_i}=x_iP$,添加($ID_i$,$x_i$,$P_{ID_i}$)到 $K^{\text{list}}$,返回 $x_i$ 给 $A$.

9)代理密钥询问:当 $A$ 分别对身份 $ID_i$,$ID_j$ 的原始签名人和代理签名人,授权证书为 $w$ 的代理密钥询问时,$C$ 首先计算授权证书签名 $S_w^{ij}=x_{ID_i}H_2(ID_i,ID_j,w)+D_{ID_i}$,然后计算 $S_p^{ij}=S_w^{ij}+x_{ID_j}H_2(ID_i,ID_j,w)+D_{ID_j}=(x_{ID_i}+x_{ID_j})H_2(ID_i,ID_j,w)+(D_{ID_A}+D_{ID_B})$,返回 $S_p^{ij}$ 给 $A$.

10)代理签名询问:当 $A$ 向 $C$ 提交原始签名人的身份 $ID_i$,代理签名人的身份 $ID_j$,授权证书为 $w$,消息为 $m$ 的代理签名询问时,$C$ 随机选择 $h_{ij}\in Z_p^*$,$u\in G_1$,计算 $R=e(u,P)e(H_2(ID_i,ID_j,w),P_{ID_i}+P_{ID_j})^{-h_{ij}}e(Q_{ID_i}+Q_{ID_j},P_{pub})^{-h_{ij}}$,$Q_{ID_i}=H_1(ID_i)$,$Q_{ID_j}=H_1(ID_j)$.设置 $H_3(ID_i,ID_j,m,R)=h_{ij}$,返回($u$,$h_{ij}$)给 $A$.

11)伪造:如果 $C$ 没有终止,$A$ 以至少 $\varepsilon$ 的概率,输出一个目标身份为 $ID_A^*$ 原始签名人,目标身份为 $ID_B^*$ 的代理签名人,授权证书为 $w^*$,消息为 $m^*$ 的有效代理签名为($m^*$,$w^*$,$u^*$,$h_{ij}^*$).若 $ID_B^*\neq ID_l$,$C$ 终止;否则根据 Forking Lemma[18],$C$ 选择不同的哈希函数 $h'$,再次利用敌手 $A$ 的能力,得到另外一个有效的标准签名($m^*$,$w^*$,$u^{*'}$,$h_{ij}^{*'}$),从而 $C$ 得到 2 个有效的伪造,并且有 $R=e(u^*,P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^*}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^*}$,$R=e(u^{*'},P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^{*'}}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^{*'}}$,其中 $H_2(ID_A^*,ID_B^*,w^*)=bP$,以($ID_i^*$,$ID_j^*$,$\beta$,$w^*$,$H_w$)形式存在于 $H_2^{\text{list}}$ 列表中,$Q_{ID_A^*}+Q_{ID_B^*}=(\lambda+1)bP$,从而有 $e(u^*,P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^*}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^*}=e(u^{*'},P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^{*'}}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^{*'}}$.因此 $C$ 可以计算出 CDH 问题的解 $abP=(\lambda+1)(h^*-h^{*'})^{-1}(u^*-u^{*'})-\beta(P_{ID_A^*}+P_{ID_B^*})$.

12)概率计算:假设事件 $E_1$ 代表 $A$ 经过一系列询问后,$C$ 最终没有终止,由于($m^*$,$w^*$,$u^*$,$h_{ij}^*$)是一个有效的代理签名,存在的概率为 $1/(2^k-q_{H_3}-q_{ps})$,$C$ 不终止的概率为$(1-1/(2^k-q_{H_3}-q_{ps}))^{q_{ps}+1}$;事件 $E_2$ 代表 $A$ 成功伪造一个有效的代理签名,则 $\Pr[E_2]=\varepsilon$;事件 $E_3$ 代表 $C$ 选择目标身份($ID_A^*$,$ID_B^*$),则 $\Pr[E_3]=1/\binom{q_{H_1}}{2}$,因此 $C$ 成功解决困难问题的概率为 $\varepsilon'\geqslant\varepsilon(1-1/(2^k-q_{H_3}-q_{ps}))^{q_{ps}+1}/\binom{q_{H_1}}{2}$.

**定理 2** 在随机预言模型下,若存在第Ⅱ类敌手 $A$ 能在多项式时间内,进行最多 $q_{H_i}$次 $H_i(i=1,2,3)$ 哈希询问、$q_k$ 次公钥询问、$q_R$ 次公钥替换询问、$q_{pk}$次代理密钥询问、$q_{ps}$次代理签名询问,以最多 $\varepsilon$ 的概率成功伪造有效代理签名,则存在算法 $C$ 能在多项式时间内以最多 $\varepsilon'\geqslant\varepsilon(1-1/(2^k-q_{H_3}-q_{ps}))^{q_{ps}+1}/\binom{q_k}{2}$ 的概率解决 CDH 问题.

**证明** 挑战者 $C$ 要解决 CDH 困难问题,输入($aP$,$bP$),目标是要计算出 $abP$.如果存在第Ⅱ类敌手 $A$,能以不可忽略的概率攻破本方案,则 $C$ 能利用算法 $A$ 解决 CDH 问题,过程如下:

1)设置:输入安全参数 $k$,方案中存在 2 个目标用户,原始签名人 $ID_A^*$ 和代理签名人 $ID_B^*$.$C$ 随机选择 $s\in Z_p^*$,计算 $P_{\text{pub}}=sP$,将系统参数 $params=\{G_1,G_2,e,q,P,P_{\text{pub}},H_1,H_2,H_3\}$ 发给 $A$,将哈希函数 $H_2$,$H_3$ 看作随机预言机.假设 $A$ 每次的询问不同.

2)公钥询问:$C$ 维护一个列表 $K^{\text{list}}$,格式为($ID$,$x$,$P_{ID}$),初始化为空.$A$ 最多进行 $q_k$ 次公钥询问,在 $C[1,q_k]$中随机选择一个值 $l$,$A$ 询问 $ID_i$ 的公钥时,$C$ 检索 $K^{\text{list}}$,如果 $K^{\text{list}}$存在元组($ID_i$,$x_i$,$P_{ID_i}$),返回 $P_{ID_i}$给 $A$.如

果不存在,当 $ID_i \neq ID_l$ 且 $ID_i \neq ID_A^*$ 时,$C$ 随机选择 $x_i \in Z_p^*$,计算 $P_{ID_i}=x_iP$;当 $ID_i=ID_A^*$ 时,置 $x_i=\perp$,$P_{ID_i}=\gamma aP$;当 $ID_i=ID_l=ID_B^*$ 时,置 $x_i=\perp$,$P_{ID_i}=aP$,最后 $C$ 添加 $(ID_i,x_i,P_{ID_i})$ 到 $K^{\text{list}}$,返回 $P_{ID_i}$ 给 $A$.

3)$H_2$ 询问:$C$ 维护一个列表 $H_2^{\text{list}}$,格式为 $(ID_i,ID_j,w,\beta_{ij},H_w)$,初始化为空.$A$ 询问 $H_2(ID_i,ID_j,w)$ 时,$C$ 首先判断 $ID_i$ 是否等于 $ID_l$,若 $ID_i \neq ID_l$,$C$ 随机选择 $\beta_{ij} \in Z_p^*$,计算 $H_w=\beta_{ij}P$,否则置 $\beta_{ij}=\perp$,$H_w=bP$.最后 $C$ 添加 $(ID_i,ID_j,w,\beta_{ij},H_w)$ 到 $H_2^{\text{list}}$,返回 $H_w$ 给敌手 $A$.

4)$H_3$ 询问:$C$ 维护一个列表 $H_3^{\text{list}}$,格式为 $(ID_i,ID_j,m,R,h_{ij})$,初始化为空.$A$ 询问 $H_3(ID_i,ID_j,m,R)$ 时,$C$ 随机选择 $h_{ij} \in Z_p^*$,添加 $(ID_i,ID_j,m,R,h_{ij})$ 到 $H_3^{\text{list}}$ 中,返回 $h_{ij}$ 给 $A$.

5)秘密值询问:当 $C$ 接收 $A$ 到身份 $ID_i$ 用户的秘密值询问时,若 $ID_i=ID_l$,$C$ 终止;否则 $C$ 检索 $K^{\text{list}}$ 找到 $(ID_i,x_i,P_{ID_i})$,若 $x_i=\perp$,表明身份为 $ID_i$ 用户公钥已经被替换,$C$ 无法回答 $A$ 的秘密值询问,返回 $\perp$ 给 $A$,否则返回 $x_i$ 给 $A$.如果 $C$ 检索 $K^{\text{list}}$ 没有找到相应的项,则 $C$ 随机选择 $x_i \in Z_p^*$,计算 $P_{ID_i}=x_iP$,添加 $(ID_i,x_i,P_{ID_i})$ 到 $K^{\text{list}}$,返回 $x_i$ 给 $A$.

6)公钥替换询问:$C$ 接收到 $A$ 对身份为 $ID_i$ 用户公钥替换询问 $(ID_i,P'_{ID_i})$ 时,若 $ID_i=ID_l$,$C$ 终止;否则,$C$ 检索 $K^{\text{list}}$ 时找到元组 $(ID_i,x_i,P_{ID_i})$,并设置 $x_i=\perp$,$P_{ID_i}=P'_{ID_i}$.

7)代理密钥询问:当 $C$ 接收到 $A$ 对身份为 $ID_i$ 的原始签名人,身份为 $ID_j$ 的代理签名人,授权证书为 $w$,的代理密钥询问时,首先计算 $S_w^{ij}=x_{ID_i}H_2(ID_i,ID_j,w)+D_{ID_i}$,然后计算 $S_p^{ij}=S_w^{ij}+x_{ID_j}H_2(ID_i,ID_j,w)+D_{ID_j}=(x_{ID_i}+x_{ID_j})H_2(ID_i,ID_j,w)+(D_{ID_A}+D_{ID_B})$,返回 $S_p^{ij}$ 给 $A$.

8)代理签名询问:当 $A$ 向 $C$ 提交身份为 $ID_i$ 的原始签名人,身份为 $ID_j$ 的代理签名人,授权证书为 $w$,消息为 $m$ 的代理签名询问时,$C$ 随机选择 $h_{ij} \in Z_p^*$,$u \in G_1$,计算 $R=e(u,P)e(H_2(ID_i,ID_j,w),P_{ID_i}+P_{ID_j})^{-h_{ij}}e(Q_{ID_i}+Q_{ID_j},P_{pub})^{-h_{ij}}$,$Q_{ID_i}=H_1(ID_i)$,$Q_{ID_j}=H_1(ID_j)$.设置 $H_3(ID_i,ID_j,m,R)=h_{ij}$,返回 $(u,h_{ij})$ 给 $A$.

9)伪造:如果 $C$ 没有终止,$A$ 以至少 $\varepsilon$ 的概率,输出一个目标身份为 $ID_A^*$ 原始签名人,目标身份为 $ID_B^*$ 的代理签名人,授权证书为 $w^*$,消息为 $m^*$ 的有效代理签名 $(m^*,w^*,u^*,h_{ij}^*)$.若 $ID_B^* \neq ID_l$,$C$ 终止;否则根据 Forking Lemma[18],$C$ 选择不同的哈希函数 $H_3'$,再次利用敌手 $A$ 的能力,得到另外一个有效的代理签名 $(m^*,w^*,u^{*'},h_{ij}^{*'})$,从而 $C$ 得到 2 个有效的伪造,并且有 $R=e(u^*,P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^*}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^*}$,$R=e(u^{*'},P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^{*'}}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^{*'}}$.其中 $H_2(ID_A^*,ID_B^*,w^*)=bP$,以 $(ID_i^*,ID_j^*,\perp,w^*,bP)$ 形式存在于 $H_2^{\text{list}}$ 列表中,$P_{ID_A^*}+P_{ID_B^*}=(\gamma+1)aP$.于是 $e(u^*,P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^*}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^*}=e(u^{*'},P)e(H_2(ID_A^*,ID_B^*,w^*),P_{ID_A^*}+P_{ID_B^*})^{-h_{ij}^{*'}}e(Q_{ID_A^*}+Q_{ID_B^*},P_{pub})^{-h_{ij}^{*'}}$.因此 $C$ 可以计算出 CDH 问题的解 $abP=(\gamma+1)(h^*-h^{*'})^{-1}(u^*-u^{*'})-s(Q_{ID_A^*}+Q_{ID_B^*})$.

10)概率计算:假设事件 $E_1$ 代表 $A$ 经过一系列询问后,$C$ 最终没有终止,由于 $(m^*,w^*,u^*,h_{ij}^*)$ 是一个有效的代理签名,存在的概率为 $1/(2^k-q_{H_3}-q_{ps})$,$C$ 不终止的概率为 $(1-1/(2^k-q_{H_3}-q_{ps}))^{q_{ps}+1}$;事件 $E_2$ 代表 $A$ 成功伪造一个有效的代理签名,则 $\Pr[E_2]=\varepsilon$;事件 $E_3$ 代表 $C$ 选择目标身份 $(ID_A^*,ID_B^*)$,则 $\Pr[E_3]=1/\binom{q_k}{2}$,因此 $C$ 成功解决困难问题的概率为 $\varepsilon' \geqslant \varepsilon(1-1/(2^k-q_{H_3}-q_{ps}))^{q_{ps}+1}/\binom{q_k}{2}$.

## 5 效率分析

表 1 给出了本方案与文献[19-20]计算代价比较,其中,$e$ 表示双线性对映射;$M_{G_1}$,$E_{G_1}$,$A_{G_1}$ 分别表示 $G_1$ 上的乘法、指数和加法运算;$M_{G_2}$,$E_{G_2}$ 表示 $G_2$ 上的乘法、指数运算;$M_{Z_q^*}$ 表示 $Z_q^*$ 上的乘运算.由于哈希函数计算操作代价很低可以忽略,此处删除了哈希函数计算操作代价的比较.通过分析比较可知,本方案在计算量上略微优于文献[19-20]中的方案.

令 $|G_1|$,$|G_2|$ 分别表示 $G_1$,$G_2$ 中的元素长度,$|Z_q^*|$ 表示 $Z_q^*$ 中的元素长度,$|m|$,$|m_w|$ 分别表示 $m$ 和 $m_w$ 的长度,表 2 给出了几种方案的通信代价比较.分析表明本方案在通信量上,也略优于文献[19-20]方案.

## 6 结束语

基于双线性映射,本文提出了一个高效的无证书代理签名方案.在随机预言模型下,基于计算 Diffie-Hellman 困难问题假设,证明了方案的安全性.计算代价和通信代价分析表明本方案在效率方面优于文献[19-20]的方案,提出的方案在现实生活中有较好的应用前景.

**表 1 计算代价比较**

Table 1 Computation cost comparison

| 方案 | 运算次数 | | | |
|---|---|---|---|---|
| | 代理授权算法 | 签名算法 | 验证算法 | 运算总和 |
| 文献[19] | $3e+2M_{G_1}+3A_{G_1}+2M_{Z_q^*}+M_{G_2}+E_{G_2}$ | $3M_{G_1}+A_{G_1}$ | $4e+A_{G_1}+2E_{G_2}$ | $7e+5M_{G_1}+5A_{G_1}+M_{G_2}+3E_{G_2}+2M_{Z_q^*}$ |
| 文献[20] | $3e+3M_{G_1}+5A_{G_1}+2E_{G_2}$ | $2M_{G_1}+A_{G_1}$ | $4e+2A_{G_1}+M_{G_2}+E_{G_2}$ | $7e+5M_{G_1}+8A_{G_1}+M_{G_2}+3E_{G_2}$ |
| 本文 | $3e+3A_{G_1}+M_{G_2}$ | $e+2M_{G_1}+A_{G_1}+E_{G_2}$ | $3e+2A_{G_1}+2E_{G_2}$ | $7e+2M_{G_1}+6A_{G_1}+M_{G_2}+3E_{G_2}$ |

**表 2 通信代价比较**

Table 2 Communication cost comparison

| 方案 | 通信代价 | |
|---|---|---|
| | 代理签名长度 | 公钥长度 |
| 文献[19] | $\|m\|+2\|G_1\|+\|m_w\|$ | $2\|G_1\|$ |
| 文献[20] | $2\|G_1\|+\|G_2\|+\|m_w\|$ | $2\|G_1\|$ |
| 本文 | $\|m\|+\|G_1\|+\|Z_q^*\|+\|m_w\|$ | $2\|G_1\|$ |

## 参考文献

References

[1] Al-Riyami S S, Paterson K G. Certificateless public key cryptog-raphy[C]// International Conference on the Theory and Application of Cryptology and Information Security, 2003: 452-473

[2] 桑永宣,曾吉文.两种无证书的分布环签名方案[J].电子学报,2008,36(7):1468-1472
SANG Yongxuan, ZENG Jiwen. Two certificateless distributed ring signature schemes[J]. Acta Electronica Sinica, 2008, 36(7): 1468-1472

[3] Zhu L J, Zhang F T. An efficient certificateless ring signature scheme[J]. Wuhan University Journal of Natural Sciences, 2008, 13(5): 567-571

[4] Li J G, Huang X Y, Mu Y, et al. Cryptanalysis and improvement of an efficient certificateless signature scheme[J]. Journal of Communications and Networks, 2008, 10(1): 10-17

[5] 王化群,徐名海,郭显久.几种无证书数字签名方案的安全性分析及改进[J].通信学报,2008,29(5):88-92
WANG Huaqun, XU Minghai, GUO Xianjiu. Cryptanalysis and improvement of several certificateless digital signature schemes[J]. Journal of Communications, 2008, 29(5): 88-92

[6] Yang X Y, Liang Z Y, Wei P, et al. A provably secure certificateless blind signature scheme[C]// International Conference on Information Assurance and Security, 2009: 643-646

[7] 李艳琼,李继国,张亦辰.标准模型下安全的无证书签名方案[J].通信学报,2015,36(4):185-194
LI Yanqiong, LI Jiguo, ZHANG Yichen. Certificateless signature scheme without random oracles[J]. Journal of Communications, 2015, 36(4): 185-194

[8] Li J G, Zhao J J, Zhang Y C. Certificateless online/offline signcryption scheme[J]. Security and Communication Networks, 2015, 8(11): 1979-1990

[9] Lu Y, Zhang Q L, Li J G. An improved certificateless strong key-insulated signature scheme in the standard model[J]. Advances in Mathematics of Communications, 2015, 9(3): 353-373

[10] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegation signing operation[C]// ACM Conference on Computer and Communication Security, 1996: 48-57

[11] Lee B, Kim H, Kim K. Strong proxy signature and its applications[C]// Proceedings of the 2001 Symposium on Cryptography and Information Security, 2001: 603-608

[12] Li X, Chen K, Sun L. Certificateless signature and proxy signature schemes from bilinear pairings[J]. Lithuanian Mathematical Journal, 2005, 45(1): 76-83

[13] Yap W S, Heng S H, Goi B M. Cryptanalysis of some proxy signature schemes without certificates[C]// WISTP 2007, LNCS 4462, Springer-Verlag, 2007: 115-126

[14] 张磊,张福泰.一类无证书签名方案的构造方法[J].计算机学报,2009,32(5):940-945
ZHANG Lei, ZHANG Futai. A method to construct a class of certificateless signature schemes[J]. Chinese Journal of Computers, 2009, 32(5): 940-945

[15] Chen H, Yang Y, Zhang F T. Short certificateless proxy signature scheme with provable security[C]// International Conference on E-Business and E-Government, 2010: 1350-1354

[16] Li J G, Li Y Q, Zhang Y C. Forward secure certificateless proxy signature scheme[C]// Lopez J, Huang X, Sandhu R. NSS 2013, LNCS 7873, 2013: 350-364

[17] Lu Y, Li J G. Provably secure certificateless proxy signature scheme in the standard model[J]. Theoretical Computer Science, 2016, 639: 42-59

[18] Pointcheval D, Stern J. Security proofs for signature schemes[C]// EURPCRYPT 1996, LNCS vol. 1070, 1996: 387-389

[19] 张建中,魏春艳.一种新的无证书代理签名方案[J].计算机工程,2010,10(36):168-172
ZHANG Jianzhong, WEI Chunyan. Novel certificateless proxy signature scheme[J]. Computer Engineering, 2010, 10(36): 168-172

[20] Tso R, Yi X. Certificateless proxy signature and its extension to blind signature[C]// The 4th International Conference on Network and System Security, 2010: 542-547

# Certificateless proxy signature scheme

ZHANG Yichen[1] LI Jiguo[1] YUAN Hong[1]
1 College of Computer and Information,Hohai University,Nanjing 211100

**Abstract** In order to avoid the key escrow problem in identity based cryptosystem and the certificate management problem in traditional public key cryptosystem,we propose a certificateless proxy signature from bilinear pairing. Based on assumption of the computational Diffie-Hellman hardness problem,our scheme is proved secure in random oracle model.Compared with the existing certificateless proxy signature schemes,the proposed scheme has advantage in both computation cost and communication cost.

**Key words** certificateless signature;bilinear pairing;proxy signature;random oracle