一个标准模型下基于身份的高效代理签名方案

于义科[1,2] 郑雪峰[1] 韩晓光[1] 刘行兵[1]
(北京科技大学信息工程学院 北京 100083)[1] (南昌航空大学信息工程学院 南昌 330063)[2]

摘 要 目前对于基于身份的代理签名方案来说,方案的安全性大多是在随机预言模型下证明的,但随机预言机的实现方式可能会导致方案的不安全。相对而言,设计标准模型下的代理签名方案更有实际意义。提出了一种安全、高效的基于身份的代理签名方案,利用双线性对技术对方案的正确性进行了严格证明,并在标准模型下基于CDH困难假设给出了方案安全性的详细证明。与现有的标准模型下安全的基于身份的代理签名方案相比,该方案具有更高的效率。

关键词 基于身份的代理签名,标准模型,基于身份的密码,CDH-问题
中图法分类号 TP393 **文献标识码** A

Efficient ID-based Proxy Signature in the Standard Model

YU Yi-ke[1,2] ZHEN Xue-feng[1] HAN Xiao-guang[1] LIU Xing-bing[1]
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]
(School of Information Engineering, Nanchang HangKong University, Nanchang 330063, China)[2]

Abstract At present, the security of the identity based proxy signature schemes was almost proven in the random oracle model, but for which any implementation of the random oracle results in insecure schemes. It is more practical to design threshold proxy signature scheme in the standard model, compared with the existing ones. This paper presented an secure and efficient ID-based proxy signature scheme (IBPS) in the standard model. The scheme's correctness was exactly proven in terms of bilinear pairing technique and its security analysis and prove was given in detail in the assumption of the computational Diffie-Hellman problem. Compared with the known identity based scheme in the standard model, the scheme enjoys less operation.

Keywords Identity based proxy signature, Standard model, Identity based cryptography, CDH-problem

1984年,Shamir提出基于身份的公钥密码体制[1],以解决传统公钥密码体制中的证书管理问题。在基于身份的密码体制中,使用能标识用户身份的信息作为公钥,例如Email地址或者IP地址。用户的私钥则由可信第三方(PKG)产生。2001年,Boneh和Franklin提出了第一个应用双线性对的安全、实用的基于身份的加密方案[2]。

代理签名的概念[3]是由Mambo,Usuda和Okamoto在1996年提出的。在现实世界里,人们经常需要将自己的签名权委托给可靠的代理人,让代理人代表本人去行使签名权。代理签名方案给出了解决这个问题的一种方法。根据授权的类型,代理签名可分为完全代理签名、部分代理签名和具有证书的代理签名。部分代理签名又可进一步分为不保护代理的部分代理签名和保护代理的部分代理签名。1997年,Kim等人提出了具有证书的部分代理签名的概念[4]。目前保护代理的具有证书的部分代理签名是代理签名的研究热点,一般将这种代理签名简称为代理签名。

代理签名和基于身份的密码体制相结合,形成了基于身份的代理签名。2003年,Zhang等人提出了第一个基于身份的代理签名(IBPS)方案[5],但没有给出安全证明。随后,人们陆续提出了一些基于身份的代理签名方案[6,7],这些方案都是在随机预言模型(Random Oracle Model)下被证明是安全的。随机预言模型作为一种理想化的计算模型,是由Bellare和Rogoway于1993年提出的[8]。由于在随机预言模型下安全的密码方案在实际环境中不一定是安全的[9],因此设计在标准模型(Standard Model)下可证安全的IBPS方案更有现实意义。

2009年,Li和Han等利用Paterson基于身份的签名(IBS)方案[10],提出了一个IBPS方案[11](简称为LH方案),并在标准模型下基于CDH假设证明了方案的安全性,不过方案的效率不是很高。

本文使用Waters方法[12],在Li和Jiang等的IBS方案[13]基础上,对LH方案方案在不改变攻击模型和困难问题假设的前提下加以改进,提出了一个新的IBPS方案。没有使用随机预言模型证明了该方案是安全的,并且它的安全性同

到稿日期:2010-07-01 返修日期:2011-02-20 本文受国家自然科学基金项目(60803123,60674054),北京市重点学科建设项目(XK100080537),北京市重点学科建设项目-计算机系统结构资助。

于义科(1970—),男,博士,副教授,主要研究领域为密码学与信息安全,E-mail:yyk312@163.com;郑雪峰(1951—),男,教授,博士生导师,主要研究领域为网络与信息安全;韩晓光(1982—),男,博士生,主要研究领域为云计算安全;刘行兵(1973—),男,博士生,主要研究领域为无线网络、信息集成。

样是基于 CDH 假设的困难性。方案的通信代价与 LH 方案相当，方案的代理签名算法计算量与 LH 方案相当，方案的验证算法计算量比 LH 方案减小了将近 40%。

1 预备知识

1.1 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，如果映射 $e:G\times G\to G_1$ 具有如下性质：

(1)双线性：对所有的 $u,v\in G$ 和 $a,b\in_R\mathbb{Z}_p^*$，都有 $e(u^a,v^b)=e(u,v)^{ab}$；

(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 $u,v\in G$。

则称该映射为双线性映射。利用有限域中椭圆曲线上的 Weil 对或 Tate 对可以构造这样的双线性映射。

1.2 复杂性假设

定义 1(CDH-问题) 已知 G 是阶为素数 p 的循环群，g 是群 G 的生成元，$a,b\in_R\mathbb{Z}_p^*$，已知 $g,g^a,g^b\in G$，计算 g^{ab}。这就是在 G 上的计算 Diffie-Hellman(CDH)问题。

定义 2((t,ε)-CDH 假设) 如果不存在运行时间至多为 t、解决群 G 上 CDH 问题的概率至少为 ε 的算法，则称(t,ε)-CDH 假设在群 G 上成立。

2 IBPS 体制定义

2.1 IBPS 的形式化定义

定义 3(IBPS 方案)：设基于身份的签名方案为 $IBS=\{\mathcal{G},\varepsilon,\mathcal{S},\mathcal{V}\}$，则基于身份的代理签名(IBPS)方案为 $IBPS=(\mathcal{G},\varepsilon,\mathcal{S},\mathcal{V},(\mathcal{D},\mathcal{P}),\mathcal{PS},\mathcal{PV})$。

(1)系统参数产生算法 $\mathcal{G}$。输入一个安全参数，PKG(Private Key Generation)以此来产生它的系统参数 *params* 和主密钥 *msk*，然后 PKG 将系统参数 *params* 公开、主密钥 *msk* 保密。

(2)用户私钥产生算法 ε。给定身份 *ID*，PKG 利用系统参数 *params* 和主密钥 *msk*，产生身份 *ID* 的私钥 sk_{ID}，且 PKG 能够为所有用户产生私钥，并通过安全信道发送给用户。

(3)普通签名产生算法 $\mathcal{S}$。用户得到私钥 sk_{ID}，先对私钥验证，验证私钥是否由 *PKG* 产生。若验证通过，则用户利用其身份 ID、私钥 sk_{ID}、*PKG* 的系统参数 params 来产生消息 m 的签名 σ。

(4)普通签名验证算法 $\mathcal{V}$。验证者利用 *PKG* 的系统参数 params 和用户身份 ID 验证消息 m 的签名 σ。若签名有效，则输出 1，否则输出 0。

(5)$(\mathcal{D},\mathcal{P})$是代理指定协议。该协议把原始签名人 ID_A 的签名权委托给代理签名人 ID_B。

$\mathcal{D}$：由原始签名人 ID_A 执行，给定原始签名人身份 ID_A、代理签名人身份 ID_B、授权文件 W 和原始签名人私钥 sk_A，产生授权证书 σ_W。其中授权文件 W 包括原始签名人的身份、代理签名人的身份、代理签名的消息空间以及代理签名的有效期等。

$\mathcal{P}$：由代理签名人 ID_B 执行，代理人得到授权文件 W 和授权证书 σ_W，首先验证授权证书是否由原始人产生。若验证通过，则利用原始签名人身份 ID_A、代理签名人身份 ID_B 和代理签名人私钥 sk_B，产生代理签名私钥 *psk*。

(6)代理签名产生算法 $\mathcal{PS}$。代理签名人执行该算法，给定原始签名人身份 ID_A、代理签名人身份 ID_B、授权文件 W、代理签名人代理私钥 *psk* 和消息 m，该算法输出代理签名 $p\sigma$。

(7)代理签名验证算法 $\mathcal{PV}$。验证者执行该算法。给定原始签名人身份 ID_A、代理签名人身份 ID_B、授权文件 W、代理签名 $p\sigma$ 和消息 m，该算法验证代理签名 $p\sigma$ 的合法性。若代理签名有效，则输出 1，否则输出 0。

如果一个基于身份的代理签名方案满足下面两个条件，则这个基于身份的代理签名方案是正确的：

1)对于任意的用户 *ID* 和消息 m 来说，如果 $sk_{ID}\leftarrow\varepsilon(ID,msk)$，则 $\mathcal{V}(ID,m,S(m,sk_{ID}))=1$。

2)对于任意的原始签名人 ID_A、代理签名人 ID_B 和符合授权文件 W 的消息 m 来说，如果 $sk_A\leftarrow\varepsilon(ID_A,msk)$，$sk_B\leftarrow\varepsilon(ID_B,msk)$，$psk\leftarrow[\mathcal{D}](ID_A,ID_B,W,sk_A),\mathcal{P}(ID_A,ID_B,W,sk_B)]$，则 $\mathcal{PV}(ID_A,ID_B,W,m,\mathcal{PS}(ID_A,ID_B,W,m,psk))=1$。

2.2 IBPS 的安全要求

基于身份的代理签名方案应该满足下面的安全要求：

(1)可区分性(Distinguishability)：任何人都可以区别代理签名和普通签名。

(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签的签名。

(3)强可识别性(Strong identifiability)：根据代理签名，任何人都可确定相应的代理签名人的身份。

(4)强不可伪造性(Strong unforgeability)：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人的第三方都不能产生有效的代理签名。

(5)强不可否认性(Strong undeniability)：如果代理签名人代表原始签名人产生了有效的代理签名，他就不能否认他产生的代理签名。

(6)抗滥用性(Prevention of misuse)：代理签名人不能将代理私钥用于除产生有效代理签名外的其他目的。假如代理签名人滥用了代理私钥，则能明确确定代理签名人的责任。

2.3 IBPS 的安全模型

前面提到的这几个安全要求只是代理签名方案的安全目标，而不是代理签名方案的安全模型。根据代理签名的强不可伪造性要求，通过一个挑战者 $\mathcal{C}$ 与敌手 $\mathcal{A}$ 之间的游戏，我们可以定义基于身份的代理签名方案在适应性选择消息和身份攻击下抗存在性伪造(EU-IBPS-CMIA)的安全模型。游戏叙述如下：

(1)准备阶段：挑战者 $\mathcal{C}$ 运行方案的算法 $\mathcal{G}$，得到系统参数 *params* 和主密钥 *msk*，并发送 *params* 给敌手 $\mathcal{A}$，保密 *msk*。然后 $\mathcal{C}$ 产生两个空集合 *pList* 和 *dList*。

(2)询问阶段：敌手 $\mathcal{A}$ 可以适应性地向挑战者 $\mathcal{C}$ 提出以下一定数量的询问。

1)私钥询问：$\mathcal{A}$ 可以询问任何身份 *ID* 的私钥 sk_{ID}，$\mathcal{C}$ 运行 $\varepsilon(msk,ID)$算法得到 sk_{ID}，并将 sk_{ID} 发送给 $\mathcal{A}$；

2)普通签名询问：$\mathcal{A}$ 可以询问任何身份 *ID* 在任何消息 m 上的普通签名，$\mathcal{C}$ 运行 $\varepsilon(msk,ID)$ 算法得到 sk_{ID}，运行 $\mathcal{S}(sk_{ID},m)$算法产生签名 σ，并将 σ 发送给 $\mathcal{A}$。

3)代理授权询问Ⅰ：$\mathcal{A}$ 提交原始签名人身份 ID_A、代理签名人身份 ID_B 和授权文件 W 请求与 $\mathcal{P}(ID_A,ID_B,W,sk_B)$ 交

互，$\mathcal{A}$扮演$\mathcal{D}(ID_A, ID_B, W, sk_A)$角色。$\mathcal{C}$运行$\varepsilon(msk, ID_B)$得到代理签名人的私钥$sk_B$，然后运行$\mathcal{P}(ID_A, ID_B, W, sk_B)$算法产生代理私钥$psk$，发送给$\mathcal{A}$。同时将$(ID_A, ID_B, W)$加入到集合$pList$中。

4)代理授权询问Ⅱ：$\mathcal{A}$提交原始签名人身份ID_A、代理签名人身份ID_B和授权文件W请求与$\mathcal{D}(ID_A, ID_B, W, sk_A)$交互，$\mathcal{A}$扮演$\mathcal{P}(ID_A, ID_B, W, sk_B)$角色。$\mathcal{C}$运行$\varepsilon(msk, ID_A)$算法得到原始签名人的私钥$sk_A$，然后运行$\mathcal{D}(ID_A, ID_B, W, sk_A)$。同时将$(ID_A, ID_B, W)$加入到集合$dList$中。

5)代理签名询问：$\mathcal{A}$提交原始签名人身份ID_A、代理签名人身份ID_B、授权文件W和消息m，询问ID_B代表ID_A在m上的代理签名，并且$\mathcal{A}$扮演原始签名人ID_A。$\mathcal{C}$运行$\varepsilon(msk, ID_B)$得到代理签名人的私钥sk_B，然后运行$\mathcal{P}(ID_A, ID_B, W, sk_B)$算法产生代理私钥$psk$，运行$\mathcal{PS}(ID_A, ID_B, W, psk, m)$算法得到代理签名$p\sigma$，并将它发送给敌手$\mathcal{A}$。

(3)伪造阶段：完成上述询问后，敌手$\mathcal{A}$最后输出一个伪造的签名，这个伪造的签名是下面3种情形之一：

1)$\mathcal{A}$输出一个普通签名(ID^*, m^*, σ^*)，如果满足下面3个条件，则该签名是有效的。

①$\mathcal{V}(ID^*, m^*, \sigma^*)=1$；

②ID^*没有提交用户私钥询问；

③(ID^*, m^*)没有提交普通签名询问。

2)$\mathcal{A}$输出一个代理签名$(ID_A^*, ID_B^*, W^*, p\sigma^*)$，如果满足以下4个条件，则该签名是有效的。

①$\mathcal{PV}(m^*, ID_A{}^*, ID_B{}^*, W^*, p\sigma^*)=1$；

②(ID_B^*)没有提交用户私钥询问；

③$(ID_A^*, ID_B^*, W^*) \notin pList$；

④$(ID_A^*, ID_B^*, W^*, m^*)$没有提交代理签名询问。

3)$\mathcal{A}$输出一个代理签名$(ID_A^*, ID_B^*, W^*, p\sigma^*)$，如果满足以下3个条件，则该签名是有效的。

①$\mathcal{PV}(m^*, ID_A{}^*, ID_B{}^*, W^*, p\sigma^*)=1$；

②(ID_A^*)没有提交用户私钥询问；

③$(ID_A^*, ID_B^*, W^*) \notin dList$。

如果$\mathcal{A}$伪造的签名是有效的，则游戏返回1，否则返回0。

我们把在上面游戏中获胜的敌手$\mathcal{A}$称为EU-IBPS-CMIA敌手，并将敌手$\mathcal{A}$的优势定义为

$$Adv_A^{IBPS}(k)=\Pr[\mathcal{A}\ succeeds]$$

定义4 对于一个IBPS方案来说，如果在上述游戏中不存在优势至少为ε、运行时间至多为t的EU-IBPS-CMIA敌手$\mathcal{A}$，并且敌手$\mathcal{A}$提交用户私钥询问的次数至多为q_e、普通签名询问的次数至多为q_s、代理指定询问的次数至多为q_d、代理签名询问的次数至多为q_{ps}，则称该方案为$(\varepsilon, t, q_e, q_s, q_d, q_{ps})$-EU-IBPS-CMIA安全的。

3 基于身份的高效代理签名方案

根据文献[13]中的基于身份的签名方案构造一个在标准模型下可证安全的基于身份的代理签名方案。

3.1 方案描述

设用户的身份ID、授权文件W和消息m分别是长度为n_u，n_w和n_m的比特串。

(1)系统参数产生算法$\mathcal{G}$。

令G, G_T是阶为素数p的循环群，生成元$g \in G$，双线性映射为$e: G \times G \to G_T$。PKG随机选择$\alpha \in \mathbb{Z}_p$，$g_2 \in G$，计算$g_1 = g^\alpha \in G$。随机选择$u' \in \mathbb{Z}_p$，$w' \in G$，$m' \in G$，n_u维的向量$U_v=(u_i)$，n_w维的向量$W_v=(w_i)$，n_m维的向量$M_v=(m_i)$，其中$u_i \in \mathbb{Z}_p$，$w_i \in G$，$m_i \in G$。令$z_1=e(g_1, g_2)$，$z_2=e(g, g_2)$，则系统公开参数为$params=(p, g, g_1, g_2, u', U_v, w', W_v, m', M_v, z_1, z_2)$，主密钥为$msk=\alpha$。

(2)用户私钥产生算法ε。

已知用户身份ID，令$U \subseteq \{1, 2, \cdots, n_u\}$为$ID[i]=1$的序号$i$的集合。PKG随机选择$r \in \mathbb{Z}_p$，并计算

$$d_{ID}=(d_1, d_2)=(g_2^{\alpha + r(u' + \sum_{i \in U} u_i)}, z_2^r)$$

则d_{ID}是身份为ID的普通签名私钥，将d_{ID}秘密发送给用户ID。

(3)普通签名产生算法$\mathcal{S}$。

用户得到私钥d_{ID}后，先对私钥进行验证：$e(g, d_1)=z_1 \cdot d_2^{(u' + \sum_{i \in U} u_i)}$。若等式成立，则用户可以确认密钥是由PKG产生的；反之，重新向PKG询问密钥。若密钥验证通过，可对消息签名。设m为要签名的消息，令$\mathcal{M} \subseteq \{1, 2, \cdots, n_m\}$为$m[k]=1$的序号$k$的集合，用户$ID$任意选择$r_m \in \mathbb{Z}_p$，并计算

$$\sigma=(d_1 \cdot (m' \prod_{k \in \mathcal{M}} m_k)^{r_m}, d_2, g^{r_m})=(\sigma_1, \sigma_2, \sigma_3)$$

(4)普通签名验证算法$\mathcal{V}$。

通过下面等式验证签名$\sigma=(\sigma_1, \sigma_2, \sigma_3)$的有效性。

$$e(g, \sigma_1)=z_1 \cdot \sigma_2^{(u' + \sum_{i \in U} u_i)} \cdot e(\sigma_3, m' \prod_{k \in \mathcal{M}} m_k)$$

(5)代理指定协议$(\mathcal{D}, \mathcal{P})$。

$\mathcal{D}$：对于授权文件W来说，定义$\mathcal{W} \subseteq \{1, 2, \cdots, n_w\}$为$W[j]=1$的序号$j$的集合。原始签名人$ID_A$的私钥为$(d_{A1}, d_{A2})$，随机选择$r_w \in \mathbb{Z}_p$，并计算

$$\begin{aligned}\sigma_W &=(d_{A1} \cdot (w' \prod_{j \in \mathcal{W}} w_j)^{r_w}, d_{A2}, g^{r_w}) \\ &=(g_2^{\alpha + r_a(u' + \sum_{i \in U_A} u_i)} \cdot (w' \sum_{j \in \mathcal{W}} w_j)^{r_w}, z_2^{r_a}, g^{r_w}) \\ &=(\sigma_{W1}, \sigma_{W2}, \sigma_{W3})\end{aligned}$$

然后原始签名人ID_A发送(W, σ_W)给代理签名人ID_B，其中σ_W是原始签名人ID_A产生的授权证书。

$\mathcal{P}$：代理签名人ID_B通过验证下面等式判断(W, σ_W)是否有效：

$$e(g, \sigma_{W1})=z_1 \cdot \sigma_{W2}^{(u' + \sum_{i \in U_A} u_i)} \cdot e(\sigma_{W3}, w' \prod_{j \in \mathcal{W}} w_j)$$

如果成立，代理签名人随机选择$r_w{}' \in \mathbb{Z}_p$，并计算

$$\begin{aligned}psk &=(\sigma_{W1} \cdot d_{B1} \cdot (w' \prod_{j \in \mathcal{W}} w_j)^{r_w'}, \sigma_{W2}, d_{B2}, \sigma_{W3} \cdot g^{r_w'}) \\ &=(g_2^{\alpha + r_a(u' + \sum_{i \in U_A} u_i)} \cdot g_2^{\alpha + r_b(u' + \sum_{i \in U_B} u_i)} \cdot \\ &\quad (w' \prod_{j \in \mathcal{W}} w_j)^{r_w + r_w'}, z_2^{r_a}, z_2^{r_b}, g^{r_w + r_w'}) \\ &=(g_2^{2\alpha + r_a(u' + \sum_{i \in U_A} u_i) + r_b(u' + \sum_{i \in U_B} u_i)} \cdot (w' \prod_{j \in \mathcal{W}} w_j)^{r_w + r_w'}, \\ &\quad z_2^{r_a}, z_2^{r_b}, g^{r_w + r_w'}) \\ &=(pk_1, pk_2, pk_3, pk_4)\end{aligned}$$

则psk为代理签名人ID_B代表原始签名人ID_A的代理签名私钥。

(6)代理签名产生算法$\mathcal{PS}$。

设m为要签名的消息，ID_B代表原始签名人ID_A对消息m进行代理签名。令$\mathcal{M} \subseteq \{1, 2, \cdots, n_m\}$为$m[k]=1$的序号$k$的集合，代理签名人$ID_B$随机选择$r_m \in \mathbb{Z}_p$，并计算

$$\begin{aligned}p\sigma &=(pk_1 \cdot (m' \prod_{k \in \mathcal{M}} m_k)^{r_m}, pk_2, pk_3, pk_4, g^{r_m}) \\ &=(g_2^{2\alpha + r_a(u' + \sum_{i \in U_A} u_i) + r_b(u' + \sum_{i \in U_B} u_i)} \cdot (w' \prod_{j \in \mathcal{W}} w_j)^{r_w + r_w'} \cdot \\ &\quad (m' \prod_{k \in \mathcal{M}} m_k)^{r_m}, z_2^{r_a}, z_2^{r_b}, g^{r_w + r_w'}, g^{r_m})=(p\sigma_1, p\sigma_2,\end{aligned}$$

$p\sigma_3, p\sigma_4, p\sigma_5)$

最后代理签名人输出代理签名$(ID_A, ID_B, W, p\sigma)$，其中$p\sigma$是用代理私钥psk产生的在消息m上的签名。

(7)代理签名验证算法$\mathcal{PV}$。

代理签名$p\sigma$是代理签名人ID_B代表原始签名人ID_A在消息m上的有效代理签名吗？如果下面的等式成立，则是；否则，不是。

$$e(g, p\sigma_1) = z_1^2 \cdot p\sigma_2^{(u'+\sum_{i\in U_A} u_i)} \cdot p\sigma_3^{(u'+\sum_{i\in U_B} u_i)} \cdot e(w' \prod_{j\in W} w_j, p\sigma_4) \cdot e(m' \prod_{k\in M} m_k, p\sigma_5)$$

3.2 正确性分析

验证者得到代理签名$(ID_A, ID_B, W, p\sigma)$，则有

$$\begin{aligned}
e(g, p\sigma_1) &= e(g, g_2^{2a+r_a(u'+\sum_{i\in U_A} u_i)+r_b(u'+\sum_{i\in U_B} u_i)} \cdot (w' \prod_{j\in W} w_j)^{r_w+r_{w'}} \cdot (m' \prod_{k\in M} m_k)^{r_m}) \\
&= e(g, g_2^{2a+r_a(u'+\sum_{i\in U_A} u_i)+r_b(u'+\sum_{i\in U_B} u_i)}) \cdot e(g, (w' \prod_{j\in W} w_j)^{r_w+r_{w'}}) \cdot e(g, (m' \prod_{k\in M} m_k)^{r_m}) \\
&= e(g, g_2^{2a}) \cdot e(g, g_2^{r_a(u'+\sum_{i\in U_A} u_i)}) \cdot e(g, g_2^{r_b(u'+\sum_{i\in U_B} u_i)}) \cdot e(g, (w' \prod_{j\in W} w_j)^{r_w+r_{w'}}) \cdot e(g, (m' \prod_{k\in M} m_k)^{r_m}) \\
&= e(g_1, g_2)^2 \cdot e(g, g_2)^{r_a \cdot (u'+\sum_{i\in U_A} u_i)} \cdot e(g, g_2)^{r_b \cdot (u'+\sum_{i\in U_B} u_i)} \cdot e(g^{r_w+r_{w'}}, w' \prod_{j\in W} w_j) \cdot e(g^{r_m}, m' \prod_{k\in M} m_k) \\
&= z_1^2 \cdot p\sigma_2^{(u'+\sum_{i\in U_A} u_i)} \cdot p\sigma_3^{(u'+\sum_{i\in U_B} u_i)} \cdot e(p\sigma_4, w' \prod_{j\in W} w_j) \cdot e(p\sigma_5, m' \prod_{k\in M} m_k)
\end{aligned}$$

所以本方案的代理签名验证算法是正确的。

3.3 安全性分析

由于在一个有效的代理签名中包含一个授权文件、原始签名人身份、代理签名人身份，而且在代理签名验证等式中授权文件、原始签名人身份、代理签名人身份必须同时出现，因此很容易看出本代理签名方案满足可区分性、可验证性、强可识别性、强不可否认性和抗滥用性。

下面证明本文方案满足强不可伪造性。

定理 1 若(ε', t')-CDH假定成立，那么上述IBPS方案是$(\varepsilon, t, q_e, q_s, q_d, q_{ps})$-安全的。其中，

$$\varepsilon' = \frac{\varepsilon}{64(q_e+q_s+q_d+q_{ps})(q_d+q_{ps})(q_s+q_{ps})(n_u+1)(n_w+1)(n_m+1)}$$

$$t' = t + O((q_e n_u + q_s(n_u+n_m) + q_d(n_u+n_w) + q_{ps}(n_u+n_w+n_m))\rho + (q_e+q_s+q_{pk}+q_{ps})\tau)$$

式中，ρ和τ分别是在G中的一次乘法运算时间和一次指数运算时间。

证明：假设敌手$\mathcal{A}$能以不可忽略的优势攻击上面的方案，则能构造算法$\mathcal{B}$，$\mathcal{B}$可以利用$\mathcal{A}$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}，$\mathcal{B}$模拟$\mathcal{A}$的挑战者$\mathcal{C}$，具体过程如下：

系统建立：$\mathcal{B}$设定$l_u = 2(q_e+q_s+q_d+q_{ps})$，$l_w = 2(q_d+q_{ps})$，$l_m = 2(q_s+q_{ps})$，其中$q_e$是$\mathcal{A}$私钥询问的次数，$q_s$是$\mathcal{A}$普通签名询问的次数，$q_d$是代理指定询问的次数，$q_{ps}$是代理签名询问的次数。选择整数$k_u$，$k_w$和$k_m$，满足$0 \leqslant k_u \leqslant n_u$，$0 \leqslant k_w \leqslant n_w$和$0 \leqslant k_m \leqslant n_m$，并假定$l_u(n_u+1) < p$，$l_w(n_w+1) < p$和$l_m(n_m+1) < p$。$\mathcal{B}$选择$x' \in_R \mathbb{Z}_{l_u}$及长度为$n_u$的向量$X = (x_i)$，其中$x_i \in_R \mathbb{Z}_{l_u}$；选择$y' \in_R \mathbb{Z}_{l_w}$及长度为$n_w$的向量$Y = (y_i)$，其中$y_i \in_R \mathbb{Z}_{l_w}$；选择$z' \in_R \mathbb{Z}l_m$及长度为$n_m$的向量$Z = (z_j)$，其中$z_j \in_R \mathbb{Z}l_m$。最后$\mathcal{B}$选择$b', c' \in_R \mathbb{Z}_p$，并选择长度为$n_w$的向量$B = (b_j)$和长度为$n_m$的向量$C = (c_k)$，其中$b_j, c_k \in_R \mathbb{Z}_p$。

对于身份ID、授权文件W和消息M，定义以下几个函数。

$$F(ID) = x' + \sum_{i\in U} x_i - l_u k_u$$

$$K(W) = y_j' + \sum_{j\in W} y_j - l_w k_w$$

$$L(W) = b' + \sum_{j\in W} b_j$$

$$Q(M) = z' + \sum_{k\in M} z_k - l_m k_m$$

$$R(M) = c' + \sum_{k\in M} c_k$$

算法$\mathcal{B}$构造上面方案中的公开参数如下：

$g_1 = g^a$，$g_2 = g^b$

$u' = -l_u k_u + x'$，$u_i = x_i$，$1 \leqslant i \leqslant n_u$

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

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

可以看出这些参数的分布与一个真正的挑战者产生的公开参数的分布是一样的。这样可以得到$g_2^a = g_2^a = g^{ab}$，$u' + \sum_{i\in U} u_i = F(ID)$，$w' \prod_{j\in W} w_j = g_2^{K(W)} g^{L(W)}$，$m' \prod_{k\in M} m_k = g_2^{Q(M)} g^{R(M)}$。

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

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的用户私钥询问，虽然$\mathcal{B}$不知道主密钥，但是在假定$F(ID) \neq 0 \bmod p$的情况下，$\mathcal{B}$也能够构造其私钥d_{ID}。即算法$\mathcal{B}$选取$r \in \mathbb{Z}_p$并计算：

$$\begin{aligned}
d_{ID} &= (g_1^{-1}(gg_2)^{r(u'+\sum_{i\in U} u_i)}, e(gg_2, g^r g_1^{-\frac{1}{(u'+\sum_{i\in U} u_i)}})) \\
&= (d_1, d_2)
\end{aligned}$$

算法$\mathcal{B}$将d_{ID}发送给敌手$\mathcal{A}$，$\mathcal{A}$对其进行验证：

$$\begin{aligned}
e(d_1, g) &= (g_1^{-1}(gg_2)^{r(u'+\sum_{i\in U} u_i)}, g) \\
&= e(g_1^{-1}(gg_2)^{rF(ID)}, g) \\
&= e(g_2^a((gg_2)^{F(ID)})^{r-\frac{a}{F(ID)}}, g) \\
&= e(g_2^a, g) \cdot e((gg_2)^{F(ID)})^{r-\frac{a}{F(ID)}}, g) \\
&= e(g_1, g_2) \cdot e((gg_2)^{F(ID)}, g^{r-\frac{a}{F(ID)}}) \\
&= e(g_1, g_2) \cdot e(gg_2, g^r g_1^{-\frac{1}{F(ID)}})^{F(ID)} \\
&= z_1 \cdot d_2^{F(ID)} = z_1 \cdot d_2^{(u'+\sum_{i\in U} u_i)}
\end{aligned}$$

如果$F(ID) = 0 \bmod p$，上面的计算将无法进行，B将失败退出。为了分析模拟算法概率方便，将$F(ID) \neq 0 \bmod l_u$作为伪造成功私钥的条件。

②普通签名询问：考虑在身份ID下对消息M的标准签名询问。不失一般性，假设$\mathcal{A}$没有询问身份ID的密钥。如果$F(ID) \neq 0 \bmod l_u$，算法$\mathcal{B}$首先构造ID的私钥，然后利用$\mathcal{S}$算法产生ID在消息M上的签名；否则，如果$Q(M) \neq 0 \bmod l_m$，$\mathcal{B}$随机选择$r_u, r_m \in \mathbb{Z}_p$构造在身份$ID$在消息$M$上的标准签名：

$$\begin{aligned}
\sigma &= (g_2^{r_u(u'+\sum_{i\in U} u_i)} g_1^{-\frac{R(M)}{Q(M)}} (m' \prod_{k\in M} m_k)^{r_m}, z_2^{r_u}, g^{r_m} g_1^{-\frac{1}{Q(M)}}) \\
&= (g_2^{r_u(u'+\sum_{i\in U} u_i)} g_2^a (m' \prod_{k\in M} m_k)^{r_m'}, z_2^{r_u}, g^{r_m'}) = (\sigma_1, \sigma_2, \sigma_3)
\end{aligned}$$

式中，$r_m'=r_m-\frac{a}{Q(M)}$，很容易验证签名是有效的；否则，如果 $Q(M)=0 \bmod l_m$，则 $\mathcal{B}$ 将失败退出。

③代理授权询问Ⅰ：$\mathcal{A}$ 提交 (ID_A, ID_B, W) 请求与 $\mathcal{P}$ (ID_A, ID_B, d_B) 交互，并且 $\mathcal{A}$ 扮演 $\mathcal{D}(ID_A, ID_B, d_A)$ 的角色。$\mathcal{A}$ 首先运行算法 $\mathcal{D}(ID_A, ID_B, d_A)$ 产生授权证书：

$$\begin{aligned}\sigma_W &=(d_{A1}\cdot(w'\prod_{j\in\mathcal{W}}w_j)^{r_w}, d_{A2}, g^{r_w})\\ &=(g_2^{a+r_a(u'+\sum_{i\in U_A}u_i)}\cdot(w'\prod_{j\in\mathcal{W}}w_j)^{r_w}, z_2^{r_a}, g^{r_w})\\ &=(\sigma_{W1}, \sigma_{W2}, \sigma_{W3})\end{aligned}$$

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 $\mathcal{B}$ 以下面的方法构造代理私钥。如果 $F(ID_B)\neq 0 \bmod l_u$，则 $\mathcal{B}$ 先构造 ID_B 的私钥，然后运行算法 $\mathcal{P}$ 产生代理私钥；否则，如果 $K(W)\neq 0 \bmod l_w$，在假设 $l_w(n_w+1)<p$ 下，这蕴含 $K(W)\neq 0 \bmod p$，则 $\mathcal{B}$ 随机选择 $r_b, r_w'\in Z_p$，并计算

$$\begin{aligned}psk &=(g_2^{a+r_a(u'+\sum_{i\in U_A}u_i)+r_b(u'+\sum_{i\in U_B}u_i)}\cdot g_1^{-\frac{L(W)}{K(W)}}\cdot(w'\prod_{j\in\mathcal{W}}\\ &\quad w_j)^{r_w+r'_w}z_2^{r_a}, z_2^{r_b}, g_1^{-\frac{1}{K(W)}}g^{r_w+r_w'})\\ &=(g_2^{2a+r_a(u'+\sum_{i\in U_A}u_i)+r_b(u'+\sum_{i\in U_B}u_i)}\cdot(w'\prod_{j\in\mathcal{W}}\\ &\quad w_j)^{r_w+r_w'-\frac{a}{K(W)}}, z_2^{r_a}, z_2^{r_b}, g^{r_w+r_w'-\frac{a}{K(W)}})\\ &=(g_2^{2a+r_a(u'+\sum_{i\in U_A}u_i)+r_b(u'+\sum_{i\in U_B}u_i)}\cdot(w'\prod_{j\in\mathcal{W}}w_j)^{r_w+r_w''},\\ &\quad z_2^{r_a}, z_2^{r_b}, g^{r_w+r_w''})\end{aligned}$$

式中，$r_w''=r_w'-\frac{a}{K(W)}$；否则 $\mathcal{B}$ 失败退出。

④代理授权询问Ⅱ：$\mathcal{A}$ 提交 (ID_A, ID_B, W) 请求与 $\mathcal{D}$ (ID_A, ID_B, d_A) 交互，并且 $\mathcal{A}$ 扮演 $\mathcal{P}(ID_A, ID_B, d_B)$ 的角色。如果 $F(ID_A)\neq 0 \bmod l_u$，则 $\mathcal{B}$ 先构造 ID_A 的私钥，然后运行算法 $\mathcal{D}$ 产生授权证书 σ_W；否则，如果 $K(W)\neq 0 \bmod l_w$，则 $\mathcal{B}$ 随机选择 $r_a, r_w\in Z_p$，计算

$$\begin{aligned}\sigma_W &=(g_1^{-\frac{L(W)}{K(W)}}g_2^{r_a(u'\prod_{i\in U_A}u_i)}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w}, z_2^{r_a}, g_1^{-\frac{1}{K(W)}}g^{r_w})\\ &=(g_2^{a+r_a(u'\prod_{i\in U_A}u_i)}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w-\frac{a}{K(W)}}, z_2^{r_a}, g^{r_w-\frac{a}{K(W)}})\\ &=(g_2^{a+r_a(u'\prod_{i\in U_A}u_i)}(w'\prod_{j\in\mathcal{W}}w_j)^{r'_w}, z_2^{r_a}, g^{r_w'})\end{aligned}$$

式中，$r_w'=r_w-\frac{a}{K(W)}$，将 (W, σ_W) 发送给 $\mathcal{A}$；否则 $\mathcal{B}$ 失败退出。

⑤代理签名询问：$\mathcal{A}$ 提交 (ID_A, ID_B, W, M) 询问 ID_B 代表 ID_A 在 M 上的代理签名，并且 $\mathcal{A}$ 代表原始签名人。$\mathcal{A}$ 运行算法 $\mathcal{D}(ID_A, ID_B, d_A)$ 产生授权证书：

$$\begin{aligned}\sigma_W &=(g_2^{a+r_a(u'+\sum_{i\in U_A}u_i)}\cdot(w'\prod_{j\in\mathcal{W}}w_j)^{r_w}, z_2^{r_a}, g^{r_w})\\ &=(\sigma_{W1}, \sigma_{W2}, \sigma_{W3})\end{aligned}$$

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 $\mathcal{B}$ 以下面的方法构造代理签名。如果 $F(ID_B)\neq 0 \bmod l_u \vee K(W)\neq 0 \bmod l_w$，则 $\mathcal{B}$ 先构造 ID_B 代表 ID_A 签名的代理私钥，然后由算法 $\mathcal{PS}$ 产生在 M 上的代理签名；否则，如果 $Q(M)\neq 0 \bmod l_m$，则 $\mathcal{B}$ 随机选择 $r_b, r_w', r_m\in Z_p$，并计算

$$\begin{aligned}p\sigma &=(g_2^{a+r_a(u'\prod_{i\in U_A}u_i)+r_b(u'\prod_{i\in U_B}u_i)}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w+r_w'}\\ &\quad g_1^{-R(M)/Q(M)}(m'\prod_{k\in\mathcal{M}}m_k)^{r_m}, z_2^{r_a}, z_2^{r_b}, g^{r_w+r_w'},\\ &\quad g_1^{-1/Q(M)}g^{r_m})\\ &=(g_2^{2a+r_a(u'\prod_{i\in U_A}u_i)+r_b(u'\prod_{i\in U_B}u_i)}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w+r_w'}(m'\prod_{k\in\mathcal{M}}\\ &\quad m_k)^{r_m-\frac{a}{Q(M)}}, z_2^{r_a}, z_2^{r_b}, g^{r_w+r_w'}, g^{r_m-\frac{a}{Q(M)}})\\ &=(g_2^{2a+r_a(u'\prod_{i\in U_A}u_i)+r_b(u'\prod_{i\in U_B}u_i)}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w+r_w'}(m'\prod_{k\in\mathcal{M}}\\ &\quad m_k)^{r_m'}, z_2^{r_a}, z_2^{r_b}, g^{r_w+r_w'}, g^{r_m'})\end{aligned}$$

式中，$r_m'=r_m-a/Q(M)$；否则 $\mathcal{B}$ 失败退出。

伪造：如果 $\mathcal{B}$ 能够回答 $\mathcal{A}$ 所有的询问，即 $\mathcal{B}$ 没有失败退出，且 $\mathcal{A}$ 能以不可忽略的概率 ε 输出一个有效的签名伪造。这个伪造可以是下面 3 种情形之一：

①在身份 ID^* 和消息 M^* 下的有效伪造普通签名 $\sigma^*=(\sigma_1^*, \sigma_2^*, \sigma_3^*)$。$\mathcal{A}$ 没有提交 ID^* 私钥询问和 (ID^*, M^*) 普通签名询问。如果 $F(ID^*)=0 \bmod p$ 且 $Q(M^*)=0 \bmod p$，则 $\mathcal{B}$ 计算并输出：

$$\frac{\sigma_1^*}{(\sigma_3^*)^{R(M^*)}}=\frac{g_2^{a+r^*(u'\prod_{i\in U^*}u_i)}(m'\prod_{k\in\mathcal{M}}m_k)^{r_m^*}}{g^{R(M^*)\cdot r_m^*}}=g_2^a=g^{ab}$$

上述输出就是 CDH 问题实例的解；否则 $\mathcal{B}$ 失败退出。

②$\mathcal{A}$ 输出一个代理签名 $(ID_A^*, ID_B^*, W^*, p\sigma^*)$，这是敌手 $\mathcal{A}$ 在已知原始签名人 ID_A^* 的私钥而不知道代理签名人 ID_B^* 的私钥时对代理签名的伪造。

如果 $F(ID_B^*)=0 \bmod p, K(W^*)=0 \bmod p$ 且 $Q(M^*)=0 \bmod p$ 则 $\mathcal{B}$，计算并输出

$$\begin{aligned}&\frac{p\sigma_1^*}{d_{A1}^*(p\sigma_3^*)^{L(W^*)}(p\sigma_4^*)^{R(M^*)}}\\ &=\frac{g_2^{(2a+r_a^*(u'\prod_{i\in U_A^*}u_i)+r_b^*(u'\prod_{i\in U_B^*}u_i))}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w+r_w'}(m'\prod_{k\in\mathcal{M}}m_k)^{r_m^*}}{g_2^{(a+r_a^*(u'\prod_{i\in U_A^*}u_i))}g^{L(W^*)(r_w+r_w')}g^{R(M^*)r_m^*}}\\ &=g_2^a=g^{ab}\end{aligned}$$

上述输出就是 CDH 问题实例的解；否则 $\mathcal{B}$ 失败退出。

③$\mathcal{A}$ 输出一个代理签名 $(ID_A^*, ID_B^*, W^*, p\sigma^*)$，这是敌手 $\mathcal{A}$ 在已知代理签名人 ID_B^* 的私钥而不知道原始签名人 ID_A^* 的私钥时对代理签名的伪造。

如果 $F(ID_A^*)=0 \bmod p, K(W^*)=0 \bmod p$ 且 $Q(M^*)=0 \bmod p$，则 $\mathcal{B}$ 计算并输出：

$$\begin{aligned}&\frac{p\sigma_1^*}{(p\sigma_3^*)^{L(W^*)}d_{B1}^*(p\sigma_4^*)^{R(M^*)}}\\ &=\frac{g_2^{(2a+r_a^*(u'\prod_{i\in U_A^*}u_i)+r_b^*(u'\prod_{i\in U_B^*}u_i))}(w'\prod_{j\in\mathcal{W}}w_j)^{r_w+r_w'}(m'\prod_{k\in\mathcal{M}}m_k)^{r_m^*}}{g^{L(W^*)(r_w+r_w')}g_2^{(a+r_b^*(u'\prod_{i\in U_B^*}u_i))}g^{R(M^*)r_m^*}}\\ &=g_2^a=g^{ab}\end{aligned}$$

上述输出就是 CDH 问题实例的解；否则 $\mathcal{B}$ 失败退出。

上面描述了算法 $\mathcal{B}$ 的模拟过程。下面以伪造②为例分析一下算法 $\mathcal{B}$ 解决 CDH 问题的优势和它的运行时间。伪造①和③完全可以类似地进行分析。

概率分析：如果在模拟过程中满足下列条件，则算法 $\mathcal{B}$ 将不会以失败退出而结束。

①用户私钥询问阶段：$F(ID)\neq 0 \bmod l_u$；

②普通签名询问阶段：$F(ID)\neq 0 \bmod l_u$ 或 $Q(M)\neq 0 \bmod l_m$；

③代理授权询问Ⅰ阶段：$F(ID_B)\neq 0 \bmod l_u$ 或者 $K(W)\neq 0 \bmod l_w$；

④代理授权询问Ⅱ阶段：$F(ID_A)\neq 0 \bmod l_u$ 或者 $K(W)\neq 0 \bmod l_w$；

⑤代理签名询问阶段：$F(ID_B)\neq 0 \bmod l_u$ 或者 $K(W)\neq 0 \bmod l_w$ 或 $Q(M)\neq 0 \bmod l_m$；

⑥伪造阶段：$F(ID_B^*)=0 \bmod p$ 和 $K(W^*)=0 \bmod p$ 和 $Q(M^*)=0 \bmod p$。

为了简化对模拟者的分析，我们只考虑在这个事件上的一个子集的概率。设在用户私钥询问以及不包括身份 ID_B^*

的普通签名询问、代理指定询问和代理签名询问中的身份为 $ID_1,\cdots,ID_{q_I}$，在包括身份 ID_B^* 而不包括授权文件 W^* 的代理指定询问和代理签名询问中的授权文件为 $W_1,\cdots,W_{q_W}$，在包括身份 ID_B^* 的普通签名询问以及包括身份 ID_B^* 和授权文件 W^* 的代理签名询问中消息为 $M_1,\cdots,M_{q_M}$。显然有 $q_I\leqslant q_e+q_s+q_d+q_{ps}$，$q_W\leqslant q_d+q_{ps}$，$q_M\leqslant q_s+q_{ps}$。又定义事件 A_i，A^*，B_j，B^*，C_l，C^* 如下：

$A_i:F(ID_i)\neq 0 \bmod l_u$，$A^*:F(ID_B^*)\neq 0 \bmod p$，

$B_j:K(W_j)\neq 0 \bmod l_w$，$B^*:K(W^*)\neq 0 \bmod p$，

$C_l:Q(M_l)\neq 0 \bmod l_m$，$C^*:Q(M^*)\neq 0 \bmod p$，

根据上面的分析，算法没有失败退出的概率为：

$$\Pr[\neg abort]\geqslant\Pr[\bigcap_{i=1}^{q_I}A_i\wedge A^*\wedge\bigcap_{j=1}^{q_W}B_j\wedge B^*\bigcap_{l=1}^{q_M}C_l\wedge C^*]$$

可以看出，事件 $\bigcap_{i=1}^{q_I}A_i\wedge A^*$，$\bigcap_{j=1}^{q_W}B_j\wedge B^*$ 和 $\bigcap_{l=1}^{q_M}C_l\wedge C^*$ 是相互独立的。

由假设 $l_u(n_u+1)<p$ 可知，$F(ID_B^*)=0 \bmod p$ 蕴涵 $F(ID_B^*)=0 \bmod l_u$，可得

$$\begin{aligned}\Pr[A^*]&=\Pr[F(ID_B^*)=0 \bmod p\wedge F(ID_B^*)=0 \bmod l_u]\\&=\Pr[F(ID_B^*)=0 \bmod l_u]\ \Pr[F(ID_B^*)=0 \bmod p\,|\,F(ID_B^*)=0 \bmod l_u]\\&=\frac{1}{l_u(n_u+1)}\end{aligned}$$

另外，对任意 i，事件 A_i 和 A^* 相互独立，且 $\Pr[\neg A_i\,|\,A^*]=\frac{1}{l_u}$，则

$$\begin{aligned}\Pr[\bigcap_{i=1}^{q_I}A_i\,|\,A^*]&=1-\Pr[\bigcup_{i=1}^{q_I}\neg A_i\,|\,A^*]\\&\geqslant 1-\sum_{i=1}^{q_I}\Pr[\neg A_i\,|\,A^*]=1-\frac{q_I}{l_u}\end{aligned}$$

所以可以得到

$$\begin{aligned}\Pr[\bigcap_{i=1}^{q_I}A_i\wedge A^*]&=\Pr[A^*]\Pr[\bigcap_{i=1}^{q_I}A_i\,|\,A^*]\\&\geqslant\frac{1}{l_u(n_u+1)}\left(1-\frac{q_I}{l_u}\right)\\&\geqslant\frac{1}{l_u(n_u+1)}\left(1-\frac{q_e+q_s+q_d+q_{ps}}{l_u}\right)\end{aligned}$$

由设定 $l_u=2(q_e+q_s+q_d+q_{ps})$，可得

$$\Pr[\bigcap_{i=1}^{q_I}A_i\wedge A^*]\geqslant\frac{1}{4(q_e+q_s+q_d+q_{ps})(n_u+1)}$$

同理可得

$$\Pr[\bigcap_{j=1}^{q_W}B_j\wedge B^*]\geqslant\frac{1}{4(q_d+q_{ps})(n_w+1)}$$

$$\Pr[\bigcap_{l=1}^{q_M}C_l\wedge C^*]\geqslant\frac{1}{4(q_s+q_{ps})(n_m+1)}$$

因此，我们有

$$\begin{aligned}\Pr[\neg abort]&\geqslant\Pr[\bigcap_{i=1}^{q_I}A_i\wedge A^*\wedge\bigcap_{j=1}^{q_W}B_j\wedge B^*\bigcap_{l=1}^{q_M}C_l\wedge C^*]\\&\geqslant\frac{1}{4(q_e+q_s+q_d+q_{ps})(n_u+1)}\cdot\frac{1}{4(q_d+q_{ps})(n_w+1)}\cdot\frac{1}{4(q_s+q_{ps})(n_m+1)}\\&=\frac{1}{64(q_e+q_s+q_d+q_{ps})(q_d+q_{ps})(q_s+q_{ps})(n_u+1)(n_w+1)(n_m+1)}\end{aligned}$$

时间复杂度分析：算法的时间复杂度是由用户私钥询问、普通签名询问、代理指定询问和代理签名询问中的乘法运算和指数运算次数决定的。由于在用户私钥询问、普通签名询问、代理指定询问和代理签名询问中的乘法运算次数分别是 $O(n_u)$，$O(n_u+n_w)$，$O(n_u+n_w)$，$O(n_u+n_w+n_m)$，指数运算次数均为 $O(1)$，所以算法 $\mathcal{B}$ 的时间复杂度为：

$$t+O((q_en_u+q_s(n_u+n_m)+q_d(n_u+n_w)+q_{ps}(n_u+n_w+n_m))\rho+(q_e+q_s+q_d+q_{ps})\tau)$$

4 方案比较

在 LH 方案[11]中，由于 $e(g_1,g_2)$ 可以进行预计算，所以在计算验证计算量时，略去这个部分的计算量。本文方案与 LH 方案比较结果如表 1，表 2 所列。

表 1 计算量与通信量比较

方案	代理签名长度	代理签名计算量	验证计算量
LH 方案	5|G|	2Exp	5E
本方案	3|G|+2|G_T|	2Exp	3E

表 2 符号定义

符号	定义
|G|	G 中元素的长度
|G_T|	|G_T| 中元素的长度
Exp	指数运算的计算量
E	e 运算的计算量

由表 1 可以看出，本文方案的验证算法计算量比 LH 方案减小了两个双线性运算 e 的计算量（因为指数运算的计算量相对于 e 运算的计算量可以忽略不计），相对于 LH 方案，验证效率提高了将近 40%。

结束语 代理签名是一种重要的具有特殊性质的签名形式，现有的基于身份的代理签名方案的安全性大多是在随机预言模型下证明的。本文使用 Waters 方法，在 Li 和 Jiang 等的 IBS 方案基础上，基于 LH 方案提出了一个新的 IBPS 方案。证明过程中的攻击模型和困难问题假设均没有改变，这说明本文方案和 LH 方案具有同样的安全性。本文方案的通信代价和代理签名算法计算量和 LH 方案相当，而验证算法的计算量比 LH 方案减少了将近 40%，因此本文方案具有更高的效率。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto 1984. New York: Springer-Verlag, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Proceedings of Crypto 2001. LNCS 2139. London: Springer-Verlag, 2001: 213-229

[3] 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

[4] Kim S, Park S, Won D. Proxy Signatures, Revisited[C]// Proceedings of Information and Communications Security (ICICS97). LNCS 1334. Springer-Verlag, 1997: 223-232

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

[6] Xu J, Zhang Z, Feng D. ID-based proxy signature using bi-linear pairings[C]// Proceedings of the Third International Symposium on Parallel and Distributed Processing and Applications. Berlin/

Heidelberg:Springer-Verlag,2005:359-367

[7] Wu W,Mu Y,Susilo W,et al. Identity-based proxy signature from pairings[C]// Proceedings of the 4th International Conference on Autonomic and Trusted Computing. Berlin/Heidelberg:Springer-Yerlag,2007:22-31

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

[9] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报,2005,16(10):1743-1756

[10] Paterson K G,Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]// Proceedings of the 11th Australasian Conference on Information Security and Privacy. Berlin/Heidelberg:Springer-Vedag,2006:207-222

[11] 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):118-129

[12] Waters B. Efficient identity-based encryption without random oracles[C]// Proceedings of Eurocrypt. Berlin/Heidelberg:Springer-Verlag,2005:114-127

[13] 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):2131-2136

(上接第 132 页)

耗时情况和相应的加速比。从表 3 中可以看出,BEAPORSA 算法加密并行后,在双核平台上可得到 1.95 的平均加速比值。加密方通过并行处理之后很好地处理了解密方转移过来的计算负载,使 Batch RSA 算法的性能得到整体提升。

表 3 改进算法并行加密前和并行加密后的时间和加速比

算法类型	密钥长度(位/bit)					
	1792	2048	2304	2560	2816	3072
BEAPORSA	468	797	984	1309	1685	2157
BEAPPORSA	250	406	500	672	859	1082
加速比	1.87	1.96	1.97	1.95	1.96	1.99

结束语 本文提出的 Batch RSA 改进算法通过利用 Multi-power RSA 算法的优点,并且将解密时的一些计算量转移到加密端的方式来提升 Batch RSA 的解密性能。该算法可以在保证系统安全性的情况下使系统获得很好的加速比。且改进算法易于并行实现,能在多核平台上有效实现,可通过并行处理的方式使加密端的负载大幅度降低和解密端解密性能进一步提升。改进算法充分发挥了当前多核处理器设备的优势,使 Batch RSA 系统的整体性能得到进一步提升。下一步研究的重点是:如何在多核平台上更加有效地结合 OpenMP 和 OpenSSL 库来实现并行的密码系统以及将改进算法应用到安全套接层协议的握手过程中,进一步研究改进算法在该协议中的性能。

参 考 文 献

[1] Rivest R,Shamir A,Aldeman L. A Methoed for Obtaining DigitalSignatures and Public-key Cryptosystems [J]. Communications of the ACM,1978,21(2):120-126

[2] Boneh D,Shacham H. Fast Variants of RSA [R]. RSA Laboratories Cryptobytes,2002

[3] Takagi T. Fast RSA-type cryptosystem modulo pkq [C]// Krawczyk H,eds. CRYPTO,volume 1462 of Lecture Notes in Computer Science. 1998:318-326

[4] Takagi T. A fast RSA-type public-key primitive modulo pkq using Hensel lifting [J]. IEICE Transactions,2004,87(1):94-101

[5] 闵嗣鹤,严士健. 初等数论(第三版)[M]. 北京:高等教育出版社,2003

[6] Matsumoto T,Kato K. Speeding up secret computations with insecure auxiliary device [C]// Proc of the 8th Annual International Crypto Conference on Advances in Cryptology. London:Springer-Verlag,1988:497-506

[7] FIAT A. Batch RSA[C]// Proc of Crypto '89,LNCS435. Berlin:Springer-Verlag,1989:175-185

[8] Shacham H,Boneh D. Improving SSL Handshake Performance via Batching[C]// Proceedings of 2001'RSA. 2001:28-43

[9] Paxson V,Sommer R. An architecture for exploiting multi-core processors to parallelize network intrusion prevention [C]// Proceedings of the IEEE Sarnoff Symposium. 2007:1-7

[10] Timothy G, Beverly A. Patterns for Parallel Programming [M]. Boston,MA:Addison-Wesley,2005

[11] Castelluccia C,Mykletun E,Tsudik G. Improving secure server performance by re-balancing SSL/TLS handshakes [C]// Proc of the 2006 ACM Symposium on Information,Computer and Communications Security. New York:ACM,2006:26-34

[12] Li Yun-fei,Liu Qing,Li Tong. Design and Implementation of an Improved RSA Algorithm [C]// Proc of the 2010 e-Health Networking,Digital Ecosystems and Technologies. Shenzhen,2010:390-393

[13] 李云飞,柳青,郝林,等. 一种有效的 RSA 算法改进方案的研究[J]. 计算机应用,2010,30(9):2393-2397

[14] Cohen H. A Course in Computational Algebraic Number Theory [D]. vol 138 of Graduate Texts in Mathematics. Springer-Verlag,1996

[15] Vuillaume C. Efficiency comparison of several RSA variants [D]. Darmstadt University of Technology,2003

[16] Silverman R,Wagstaff Jr S. A Practical Analysis of the Elliptic Curve Factoring Algorithm [J]. Math. Comp,1993,61(203):445-462

[17] Okamoto E,Peralta R. Faster Factoring of Integers of a Special Form [J]. IEICE Transactionson Fundamentals of Electronics,Communications,and Computer Sciences,1996,79(4):489-493

[18] Boneh D,Durfee G,Howgrave-Graham N. Factoring N=prq for Large r [C]// Proceedings of Crypto '99. vol. 1666 of LNCS. Springer-Verlag,1999:326-337

[19] Lenstra A K, Verheul E R. Selecting cryptographic key sizes [J]. The Journal of the International Association for Cryptologic Research,2001,14(4):255-293

[20] 李云飞,柳青,李彤,等. 基于多核的批处理 RSA 的并行加速方法[J]. 云南大学学报:自然科学版,2011,33(1):22-26

[21] Liu Qing,Li Yun-fei,Li Tong,et al. The Research of the Batch RSA Decryption Performance[J]. Journal of Computational Information Systems,2011,7(3):948-955

[22] Chandra R,Menon R,Dagum L,et al. Parallel Programming in OpenMP [M]. New York:Morgan Kaufmann,2000

[23] Viega J,Messier M,Chandra P. Network Security with OpenSSL[M]. O'Reilly,2002