

## 标准模型下安全基于身份代理签密方案

明 洋, 冯 杰\*, 胡齐俊

(长安大学 信息工程学院, 西安 710064)

(\*通信作者电子邮箱 784852087@qq.com)

**摘 要:** 针对现实中代理签密的安全问题, 提出一种基于 Gu 等(GU K, JIA W J, JIANG C L. Efficient identity-based proxy signature in the standard model. The Computer Journal, 2013; bxt132) 代理签名的标准模型下可证安全的基于身份代理签密方案。代理签密允许原始签密者授权签密能力给代理签密者, 后者能够代表前者生成密文。该方案通过结合基于身份签密和代理签名, 既保持了基于身份签密的优点, 又具有代理签名的功能。分析表明, 基于 Diffie-Hellman 问题假设下, 所提方案满足机密性、不可伪造性。与已知方案相比, 代理密钥生成算法和代理签密算法中各需要 2 个对运算和 1 个对运算, 方案效率更高。

**关键词:** 代理签密; 标准模型; 基于身份; 双线性对

**中图分类号:** TP309.2 **文献标志码:** A

### Secure identity-based proxy signcryption scheme in standard model

MING Yang, FENG Jie\*, HU Qijun

(School of Information Engineering, Chang'an University, Xi'an Shaanxi 710064, China)

**Abstract:** Concerning the proxy signcryption security problem in reality, motivated by Gu's proxy signature scheme (GU K, JIA W J, JIANG C L. Efficient identity-based proxy signature in the standard model. The Computer Journal, 2013; bxt132), a new secure identity-based proxy signcryption scheme in the standard model was proposed. Proxy signcryption allowed that the original signcrypter delegated his authority of signcryption to the proxy signcrypter in such a way that the latter could generate ciphertext on behalf of the former. By combining the functionalities of identity-based signcryption and proxy signature scheme, the new scheme not only had the advantage of identity-based signcryption scheme, but also had the function of proxy signature scheme. Analysis results show that, under the assumption of Diffie-Hellman problem, the proposed scheme is confidential and unforgeable. Compared with the known scheme, the scheme requires 2 pairings computation in proxy key generation and 1 pairing computation in proxy signcryption. So it has higher computational efficiency.

**Key words:** proxy signcryption; standard model; identity-based; bilinear pairing

1996 年, Mambo 等<sup>[1]</sup>提出了代理签名的概念。代理签名方案中, 原始签名者将自己的签名能力授权给代理签名者, 后者代表前者产生一个有效代理签名。接收到某个消息的代理签名后, 验证者通过给定的步骤来验证有效性, 从而确认此消息的签名是原始签名者授权的。2003 年, Boldyreva 等<sup>[2]</sup>首次提出了代理签名的形式化定义和安全模型, 之后大量代理签名方案被提出<sup>[3-6]</sup>。代理签名因其特殊功能广泛应用于移动通信、网络计算和移动代理应用等实际应用中。

1984 年, Shamir<sup>[7]</sup>首次提出了基于身份公钥密码学概念, 简化了传统基于证书公钥密码体制的密钥管理。该密码学概念利用用户身份某些信息(如用户的姓名或者邮箱地址)作为公钥, 进而消除了对用户证书的需求。私钥则是由可信第三方——私钥生成中心(Private Key Generator, PKG)产生。2003 年, Boneh 等<sup>[8]</sup>首次基于双线性对提出了高效的基于身份加密方案。

1997 年, Zheng<sup>[9]</sup>首次提出了签密概念, 其核心是在一个合理的逻辑步骤内同时完成签名和加密功能, 实现了消息既

保密又认证传输及消息存储的目的。2002 年, Beak 等<sup>[10]</sup>提出了签密的安全模型。同年 Malone-Lee<sup>[11]</sup>首次提出了基于身份签密方案。2009 年, Yu 等<sup>[12]</sup>在标准模型下提出了基于身份的签密方案, 文献[13]指出方案[12]不能很好地实现机密性。自从签密思想提出后大量签密方案被提出<sup>[14-17]</sup>, 并广泛应用于电子现金支付系统、安全认证等实际应用中。

1999 年, Gamage 等<sup>[18]</sup>首次提出了代理签密方案, 该方案结合了代理签名和签密的思想, 它将签密的权利授予代理签密者, 然后代理签密者代替原始签密者进行签密。2004 年, Li 等<sup>[19]</sup>首次利用线性对提出了基于身份代理签密方案, 但该方案不具有不可伪造性和前向安全性。2005 年, Wang 等<sup>[20]</sup>利用双线性对提出了基于身份的代理签密方案, 从计算量上证明了该方案比方案[19]具有更高的效率。同年, Wang 等<sup>[21]</sup>提出了高效的基于身份的代理签密方案, 并证明了方案具有前向安全性和公开验证性。2012 年 Swapna 等<sup>[22]</sup>利用双线性对提出了一个高效的基于身份代理签密方案, 并分析了方案的安全需求。

**收稿日期:** 2014-04-16; **修回日期:** 2014-06-23。 **基金项目:** 国家自然科学基金资助项目(61202438); 中国博士后科学基金资助项目(2011M501427); 西安市科技计划项目(CX1258); 中央高校基础研究支持计划资助项目(CHD2012JC047)。

**作者简介:** 明洋(1979-), 男, 陕西榆林人, 副教授, 博士, 主要研究方向: 公钥密码学、可证明安全理论、无线网络安全; 冯杰(1987-), 女, 陕西咸阳人, 硕士研究生, 主要研究方向: 密码学、数字签名; 胡齐俊(1990-), 男, 湖北黄冈人, 硕士研究生, 主要研究方向: 网络信息安全。

本文基于 Gu 等<sup>[23]</sup>的代理签名方案提出标准模型下安全基于身份代理签密方案,基于 Diffie-Hellman 安全假设下,分别证明方案满足机密性和不可伪造性。与已知方案相比,所提方案具有较高的计算效率。

## 1 基础知识

### 1.1 双线性对

令  $G_1, G_2$  是两个  $p$  阶循环群,其中  $p$  为素数,  $g$  是  $G_1$  的生成元。定义双线性映射  $e: G_1 \times G_1 \rightarrow G_2$ , 满足下面性质。

- 1) 双线性性。 $e(g^a, g^b) = e(g, g)^{ab}$ , 对所有的  $a, b \in \mathbb{Z}_p^*$  均成立。
- 2) 非退化性。 $e(g, g) \neq 1$ 。
- 3) 可计算性。存在有效算法计算  $e(g, g)^{ab}$ 。

### 1.2 困难假设

判定性双线性 Diffie-Hellman (Decision Bilinear Diffie-Hellman, DBDH) 问题: 给定  $g, g^a, g^b, g^c \in G_1$  以及  $Z \in G_2$ , 对于未知的  $a, b, c \in \mathbb{Z}_p^*$ , 判断  $Z = e(g, g)^{abc}$  是否成立。

定义算法  $A$  成功解 DBDH 问题的概率为:  $\text{Succ}_A^{\text{DBDH}} = \Pr[1 \leftarrow A(g, g^a, g^b, g^c, e(g, g)^{abc})] - \Pr[1 \leftarrow A(g, g^a, g^b, g^c, Z)]$ , 其中概率的计算是基于  $a, b, c$  在  $\mathbb{Z}_p^*$  上的随机选取,  $Z$  在  $G_2$  上的随机选择以及算法  $A$  的随机选择上。

定义 1 DBDH 假设。对于任意多项式时间算法  $A$ ,  $\text{Succ}_A^{\text{DBDH}}$  是可忽略的。

计算性 Diffie-Hellman (Computational Diffie-Hellman, CDH) 问题: 给定  $g, g^a, g^b \in G_1$ , 对于未知的  $a, b \in \mathbb{Z}_p^*$ , 计算  $g^{ab} \in G_1$ 。

定义算法  $A$  成功解 CDH 问题的概率为:  $\text{Succ}_A^{\text{CDH}} = \Pr[g^{ab} \leftarrow A(g, g^a, g^b)]$ , 其中概率的计算是基于  $a, b$  在  $\mathbb{Z}_p^*$  上的随机选取以及算法  $A$  的随机选择上。

定义 2 CDH 假设。对于任意多项式时间算法  $A$ ,  $\text{Succ}_A^{\text{CDH}}$  是可忽略的。

## 2 代理签密形式化定义和安全模型

### 2.1 形式化定义

基于身份的代理签密方案由以下 6 个算法组成: 系统建立、密钥生成、授权生成、代理密钥生成、代理签密、代理解密。具体如下:

- 1) 系统建立算法。由 PKG 完成, 输入一个安全参数  $1^k$ , 输出主密钥  $s$  和系统公开参数  $params$ 。
- 2) 密钥生成算法。输入系统参数  $params$  和用户身份  $ID_i$ , 输出用户  $i$  的私钥  $s_{ID_i}$ 。
- 3) 授权生成算法。输入  $(params, s_{ID_i}, w)$ , 其中  $w \in (0, 1)^*$  为授权书, 输出代理授权信息  $\delta$ 。
- 4) 代理密钥生成算法。输入  $(params, \delta, s_{ID_i})$ , 输出  $(w, psk)$ , 其中  $psk$  是代理签密密钥。
- 5) 代理签密生成算法。输入  $(params, w, psk, M, ID_B)$ , 其中  $M \in (0, 1)^*$  为签密的消息,  $ID_B$  是接收者的身份, 输出  $(w, \sigma)$ , 其中  $\sigma$  是代理签密密文。
- 6) 代理解密算法。接收者验证签密密文, 输入  $(params, s_{ID_B}, w, \sigma)$ , 其中  $s_{ID_B}$  是接收者  $B$  的私钥。若密文有效, 则输出 1; 否则输出 0。

### 2.2 安全模型

设原始签密者  $O$  的身份为  $ID_O$ , 私钥为  $s_{ID_O}$ , 代理签密者  $P$  的身份为  $ID_P$ , 私钥为  $s_{ID_P}$ , 原始签密者  $O$  将其签密的能力授权给代理签密者  $P$ 。基于身份代理签密方案是代理签名和基于身份签密方案的结合, 安全性必须满足机密性和不可伪造性。

为了说明机密性, 可以通过挑战者  $C$  与攻击者  $A$  之间的游戏定义, 具体如下。

- 1) 系统设置。挑战者  $C$  生成系统参数  $params$  和主密钥  $s$ 。
- 2) 阶段 1。攻击者  $A$  适应地进行以下询问:

私钥提取询问 输入身份  $ID$  给  $C$ ,  $C$  返回身份  $ID$  的私钥  $s_{ID}$  给  $A$ 。

代理密钥询问 给定系统参数  $params$  和用户身份  $ID$  的授权书  $w$ ,  $C$  返回代理签密者的代理签密密钥  $psk$  给  $A$ 。

代理签密询问 给定消息  $m$ 、接收者身份  $ID_B$  和授权书  $w$ ,  $C$  返回代理签密密文  $\sigma$  给  $A$ 。

代理解密询问 给定接收者  $B$  的私钥  $s_{ID_B}$  和代理签密密文  $\sigma$ , 若是有效的签密, 则  $C$  返回  $\sigma$  给  $A$ , 否则返回拒绝。

3) 挑战。完成阶段 1 的询问后,  $A$  输出身份  $\{ID_O, ID_P, ID_B\}$  和两个相等长度的消息  $\{m_0, m_1\}$ ,  $C$  随机选择一个比特  $b \in \{0, 1\}$ , 并运行代理签密算法产生一个密文  $\sigma^*$  返回给  $A$ 。

4) 阶段 2。 $A$  进行如同阶段 1 中的适应性询问, 但  $A$  不能对  $ID_B$  进行私钥提取询问, 并且身份  $ID_B$  不为空。

5) 猜测。最后  $A$  输出比特  $b' \in \{0, 1\}$ , 若  $b = b'$ , 则  $A$  获胜。 $A$  的优势定义为  $\text{adv}[A] = |\Pr[b = b'] - 1/2|$ 。

定义 3 若不存在任何多项式有界的攻击者以不可忽略的优势赢得上述游戏, 则称基于身份代理签密方案是抗适应性选择密文攻击安全的。

不可伪造性分为 2 种情况:

1) 敌手的攻击为原始签密者攻击, 产生授权给  $ID^*$  的代理签密者;

2) 敌手在未得到  $ID^*$  的授权下, 敌手利用控制的用户伪造一个假装  $ID^*$  授权的代理签密密文。

为了说明方案的不可伪造性, 可以通过挑战者  $C$  与攻击者  $A$  之间的游戏定义, 具体如下。

1) 系统设置。挑战者  $C$  生成系统参数  $params$  和用户身份  $ID_1$  (设用户 1 是不被敌手控制的用户) 的私钥  $s_{ID_1}$ , 且发送  $ID_1$  给攻击者  $A$ 。

2) 询问。攻击者  $A$  适应地进行以下询问:

① 代理密钥询问。

情况 1 给定系统参数  $params$  和用户身份  $ID_i$  ( $i$  是敌手控制的用户) 的授权书  $w$ ,  $C$  返回代理签密密钥  $psk$  给  $A$ , 其中  $w$  可能是  $A$  任意伪造产生的。

情况 2 给定系统参数  $params$  和原始签密者的授权书  $w$ ,  $C$  返回代理签密者  $i$  ( $i$  是敌手控制的用户) 的代理签密密钥  $psk$  给  $A$ , 其中  $w$  可能是  $A$  任意伪造产生的。

② 代理签密询问。给定消息  $m$ 、接收者  $B$  的身份  $ID_B$  和授权书  $w$ ,  $C$  返回代理签密密文  $\sigma$  给  $A$ 。

③ 代理解密询问。给定接收者  $B$  的私钥  $s_{ID_B}$  和代理签密密文  $\sigma$ , 若是有效的签密, 则  $C$  返回  $\sigma$  给  $A$ ; 否则返回拒绝。

3) 伪造。



$$(g_2^a g)^{\frac{-a}{2\delta}} \cdot v^s = x_0 \cdot g_2^a \cdot \mu^{r_p \frac{-a}{2\delta}} \cdot v^{s \frac{-a}{2\delta}} = x_0 \cdot g_2^a \cdot \mu^{r_p H(ID_u)} \cdot v^{s H(w)}$$

$$K_{P3} = (g_1^{\frac{-1}{2\delta}} \cdot g^{r_p})^{\frac{1}{H(ID_p)}} = (g^{r_p \frac{-a}{2\delta}})^{\frac{1}{H(ID_p)}} = g^{r_p}$$

$$K_{P4} = (g_1^{\frac{-1}{2\delta}} \cdot g^s)^{\frac{1}{H(w)}} = (g^{s \frac{-a}{2\delta}})^{\frac{1}{H(w)}} = g^{s'}$$

代理签密询问 若  $\ell \cdot H(ID) \neq 0 \bmod p$  且  $\ell \cdot H(ID_p) \neq 0 \bmod p$ , 则  $C$  运行私钥提取询问生成  $ID$  和  $ID_p$  的私钥  $s_{ID}$  和  $s_{ID_p}$ , 之后进行代理密钥询问得到代理密钥  $psk$ , 运行代理签密算法; 否则  $C$  终止。

代理解签密询问 攻击者  $A$  可以对原始签密者身份  $ID_0$ , 代理签密者身份  $ID_p$  和接收者身份  $ID_B$  的密文  $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, N)$  完成代理解签密询问,  $C$  如下操作:

① 计算  $t = H_1(\sigma_1, \sigma_3, \sigma_4, \sigma_5, T, \mu^{H(ID_0)}, \mu^{H(ID_p)}, \mu^{H(ID_B)})$ 。

② 计算  $M' = H_2(g^t)$ 。

③ 验证下面等式是否成立。

$$e(\sigma_6, g) = e(g_1, g_2)^2 e(\mu, \sigma_3^{H(ID_p)} \cdot \sigma_4^{H(ID_0)}) e(v, \sigma_5) e(\sigma, \sigma_1) e(\tau, \sigma_1^{H(M')})$$

若等式不成立,  $C$  拒绝密文; 否则,  $C$  如下操作:

a) 若  $\ell \cdot H(ID_B) \neq 0 \bmod p$ ,  $C$  运行密钥提取询问计算

$$s_{ID_B} = \{x_{B,0}, x_{B,1}\}, \text{返回消息}$$

$$M = H_1(T) \oplus N = H(e(x_{B,1}, \sigma_2) \cdot e(x_{B,0}, \sigma_1)^{-1}) \oplus C$$

b) 若  $\ell \cdot H(ID_B) = 0 \bmod p$ ,  $C$  终止。

3) 挑战。经过多项式有界次的询问后,  $A$  选择身份  $\{ID_A, ID_p, ID_B\}$  和两个相等长度的消息  $\{m_0, m_1\}$ 。若  $\ell \cdot H(ID_B^*) \neq 0 \bmod p$  且  $\lambda \cdot H(M_b^*) \neq 0 \bmod p$ , 则  $C$  终止; 否则  $C$  随机选择一个比特  $b \in \{0, 1\}$ , 定义  $M_b^* = H_2(g^t)$  则  $M_b^*$  构造的密文为  $\sigma^* = (g^c, g^{cH(ID_B^*)}, g^{r_p^*}, g^{r_A^*}, g^{s^*}, K_{P1}^* \cdot \sigma^c, g^{c \cdot H(M_b^*)}, M_b^* \oplus H(Z))$ 。

4) 阶段2。攻击者  $A$  像阶段1进行多项式有界次询问, 但不允许对  $B$  的私钥进行询问和代理解签密询问。

5) 猜测。攻击者  $A$  输出其对  $b$  的猜测  $b'$ , 若  $b' = b$ , 则  $C$  对 DBDH 问题回答1, 即  $Z = e(g, g)^{abc}$ ; 否则回答0。

下面计算  $C$  的成功概率。

若  $C$  不终止模拟。需要满足下面条件:

a)  $C$  能够进行私钥提取询问, 代理签密询问, 代理解签密询问;

b) 挑战中  $\ell \cdot H(ID_B^*) \neq 0 \bmod p$  且  $\lambda \cdot H(M') \neq 0 \bmod p$ 。

定义下述概率事件:

$$A_i: \ell \cdot H(ID_i) \neq 0 \bmod p, i = 1, 2, \dots, q_e;$$

$$B_j: \ell \cdot H(ID_j) \neq 0 \bmod p, j = 1, 2, \dots, q_{pe};$$

$$C_j: \delta \cdot H_{w_j} \neq 0 \bmod p, j = 1, 2, \dots, q_{pe};$$

$$D_k: \ell \cdot H(ID_k) \neq 0 \bmod p, k = 1, 2, \dots, q_{sc};$$

$$E_k: \lambda \cdot H(M_k) \neq 0 \bmod p, k = 1, 2, \dots, q_{sc};$$

$$F_n: \ell \cdot H(ID_n) \neq 0 \bmod p, n = 1, 2, \dots, q_{usc};$$

$$T_n: \lambda \cdot H(M_n) \neq 0 \bmod p, n = 1, 2, \dots, q_{usc};$$

$$E^*: \ell \cdot H(ID_B^*) = 0 \bmod p;$$

$$T^*: \lambda \cdot H(M_b^*) = 0 \bmod p$$

$$\text{算法 } C \text{ 模拟成功的概率为: } P[\overline{\text{abort}}] = \Pr\left(\bigcap_{i=1}^{q_e} A_i \cap \left(\bigcap_{j=1}^{q_{pe}} B_j \cap \left(\bigcap_{k=1}^{q_{sc}} D_k \cap \left(\bigcap_{n=1}^{q_{usc}} F_n \cap \left(\bigcap_{n=1}^{q_{usc}} T_n \cap E^* \cap T^*\right)\right)\right)\right)\right)$$

$$\left(\bigcap_{j=1}^{q_{pe}} B_j \cap \left(\bigcap_{k=1}^{q_{sc}} D_k \cap \left(\bigcap_{n=1}^{q_{usc}} F_n \cap T_n \cap E^* \cap T^*\right)\right)\right)$$

由于事件  $\bigcap_{i=1}^{q_e} A_i, \bigcap_{j=1}^{q_{pe}} B_j, \bigcap_{j=1}^{q_{pe}} C_j, \bigcap_{k=1}^{q_{sc}} D_k, \bigcap_{k=1}^{q_{sc}} E_k, \bigcap_{n=1}^{q_{usc}} F_n, \bigcap_{n=1}^{q_{usc}} T_n$ ,  $E^*$  和  $T^*$  是相互独立的, 从而有:

$$\Pr\left(\bigcap_{i=1}^{q_e} A_i\right) = 1 - \Pr\left(\bigcup_{i=1}^{q_e} \neg A_i\right) = 1 - q_e \cdot \frac{1^k}{1^k \cdot p} = 1 - \frac{q_e}{p},$$

$$\Pr(E^*) = \frac{1^k}{1^k \cdot p} = \frac{1}{p}$$

$$\text{同理: } \Pr\left(\bigcap_{j=1}^{q_{pe}} B_j\right) = 1 - \frac{q_{pe}}{p}, \Pr\left(\bigcap_{j=1}^{q_{pe}} C_j\right) = 1 - \frac{q_{pe}}{p}, \Pr\left(\bigcap_{k=1}^{q_{sc}} D_k\right) =$$

$$1 - \frac{q_{sc}}{p}, \Pr\left(\bigcap_{k=1}^{q_{sc}} E_k\right) = 1 - \frac{q_{sc}}{p}, \Pr\left(\bigcap_{n=1}^{q_{usc}} F_n\right) = 1 - \frac{q_{usc}}{p}, \Pr\left(\bigcap_{n=1}^{q_{usc}} T_n\right) =$$

$$1 - \frac{q_{usc}}{p}, \Pr(T^*) = \frac{1^k}{1^k \cdot p} = \frac{1}{p}$$

综上:

$$P[\overline{\text{abort}}] = \Pr\left(\bigcap_{i=1}^{q_e} A_i \cap \left(\bigcap_{j=1}^{q_{pe}} B_j \cap \left(\bigcap_{k=1}^{q_{sc}} D_k \cap \left(\bigcap_{n=1}^{q_{usc}} F_n \cap \left(\bigcap_{n=1}^{q_{usc}} T_n \cap E^* \cap T^*\right)\right)\right)\right)\right)$$

$$= \Pr\left(\bigcap_{i=1}^{q_e} A_i\right) \cap \Pr\left(\bigcap_{j=1}^{q_{pe}} B_j\right) \cap \Pr\left(\bigcap_{j=1}^{q_{pe}} C_j\right) \cap \Pr\left(\bigcap_{k=1}^{q_{sc}} D_k\right) \cap \Pr\left(\bigcap_{k=1}^{q_{sc}} E_k\right) \cap \Pr\left(\bigcap_{n=1}^{q_{usc}} F_n\right) \cap$$

$$\Pr\left(\bigcap_{n=1}^{q_{usc}} T_n\right) \cap \Pr(E^*) \cap \Pr(T^*) = \left(1 - \frac{q_e}{p}\right) \cdot \left(1 - \frac{q_{pe}}{p}\right)^2 \cdot \left(1 - \frac{q_{sc}}{p}\right)^2 \cdot \left(1 - \frac{q_{usc}}{p}\right)^2 \cdot \left(\frac{1}{p}\right)^2$$

$$\text{所以 } \varepsilon' = \left(1 - \frac{q_e}{p}\right) \cdot \left(1 - \frac{q_{pe}}{p}\right)^2 \cdot \left(1 - \frac{q_{sc}}{p}\right)^2 \cdot \left(1 - \frac{q_{usc}}{p}\right)^2 \cdot \frac{\varepsilon}{p^2}.$$

算法  $C$  的时间等于攻击者  $A$  的时间加上回答  $q_e$  次私钥提取询问的时间,  $q_{pe}$  次代理密钥询问的时间,  $q_{sc}$  次代理签密询问的时间,  $q_{usc}$  次解签密询问的时间, 设指数运算时间为  $t_e$ , 一次双线性对运算时间为  $t_p$ , 因此  $C$  的运行时间为:

$$t' = t + (4q_e + 8q_{pe} + 5q_{sc} + 4q_{usc})t_e + (2q_{sc} + 4q_{usc})t_p$$

定理2 不可伪造性。假设攻击者  $A$  能够在时间  $t$  内,  $q_e$  次密钥询问,  $q_{sc}$  次代理签密询问,  $q_{usc}$  次代理解签密询问后, 能够以不可忽略的概率  $\varepsilon'$  攻破基于身份代理签密方案, 那么存在一个算法以  $\varepsilon' = \left(1 - \frac{q_{pe}}{p}\right)^2 \cdot \left(1 - \frac{q_{sc}}{p}\right)^2 \cdot \left(1 - \frac{q_{usc}}{p}\right)^2 \cdot \frac{\varepsilon}{p^3}$ , 时间  $t' = t + (6q_{pe} + 5q_{sc} + 3q_{usc})t_e + (q_{sc} + 4q_{usc})t_p$  解 CDH 问题。其中  $t_e$  表示指数运算时间,  $t_p$  表示双线性对运算时间。

证明 算法  $C$  收到攻击者  $A$  给定的一个随机实例  $(g, g^a, g^b) \in G_1$  后, 计算  $g^{ab}$ 。算法  $C$  模拟挑战者并与  $A$  之间的交互如下:

1) 系统建立。构造系统参数  $g_1 = g^a, g_2 = g^b$ ; 随机选取  $\ell, \delta, \lambda, \eta \in \mathbb{Z}_p^*$  设置:  $\mu = g_2^\ell \cdot g, v = g_2^\delta \cdot g, \tau = g_2^\lambda \cdot g, \sigma = g^\eta$ ; 并输出系统参数  $params = (G_1, G_2, e, g, g_1, g_2, \mu, v, \tau, \sigma, H, H_1, H_2)$ 。算法  $C$  如下构造私钥  $s_{ID_1}$  (设用户1是不被控制的用户): 随机选取  $r_1 \in \mathbb{Z}_p^*$ , 计算  $x_{1,0} = g_1^{\frac{-1}{\ell}} \cdot \mu^{r_1}$  和  $x_{1,1} = (g_1^{\frac{-1}{\ell}} \cdot g^{r_1})^{\frac{1}{H(ID_1)}}$ , 则算法生成的私钥  $s_{ID_1} = \{x_{1,0}, x_{1,1}\}$  并发送给  $A$ 。

正性: 算法  $C$  模拟成功的概率为:  $P[\overline{\text{abort}}] = \Pr\left(\bigcap_{i=1}^{q_e} A_i \cap \left(\bigcap_{j=1}^{q_{pe}} B_j \cap \left(\bigcap_{k=1}^{q_{sc}} D_k \cap \left(\bigcap_{n=1}^{q_{usc}} F_n \cap \left(\bigcap_{n=1}^{q_{usc}} T_n \cap E^* \cap T^*\right)\right)\right)\right)\right)$



$$x_{1,0} = g_1^{-\frac{1}{\ell}} \cdot \mu^{r_1} = g_2^a \cdot g_2^{-a} \cdot g_1^{-\frac{1}{\ell}} \cdot \mu^{r_1} = g_2^a \cdot (g_2^\ell)^{-\frac{a}{\ell}} g_1^{-\frac{a}{\ell}} \cdot \mu^{r_1} = g_2^a \cdot (\mu)^{-\frac{a}{\ell}} \cdot \mu^{r_1} = g_2^a \cdot (\mu)^{r_1 - \frac{a}{\ell}}$$

$$\text{令 } r'_1 = \left(r_1 - \frac{a}{\ell}\right) \cdot \left(\frac{1}{H(ID)}\right), \text{ 当 } \ell \cdot H(ID) \neq 0 \bmod p$$

时密钥  $s_{ID_1} = \{x_{1,0}, x_{1,1}\} = \{g_2^a \cdot \mu^{r'_1 H(ID)}, g^{r'_1}\}$  是有效的用户私钥。

2) 询问。攻击者  $A$  适应地进行以下询问。

① 代理密钥询问。

情况 1 用户  $i$  是授权人, 将其签密权利授权给用户  $1 \circ A$  进行代理密钥询问,  $C$  作出如下回应:

a) 若  $\ell \cdot H(ID_i) = 0 \bmod p$  或  $\partial \cdot H_w = 0 \bmod p$ , 算法  $C$  终止。

b) 若  $\ell \cdot H(ID_i) \neq 0 \bmod p$  或  $\partial \cdot H_w \neq 0 \bmod p$ ,  $C$  随机选择  $r_i, s \in \mathbb{Z}_p^*$  并计算:  $K_{P1} = x_{1,0} \cdot g_1^{-\frac{1}{2\ell}} \cdot \mu^{r_i} \cdot g_1^{-\frac{1}{2\ell}} \cdot v^s, K_{P2} = x_{1,1}, K_{P3} = (g_1^{-\frac{1}{2\ell}} \cdot g^{r_i})^{\frac{1}{H(ID_i)}}, K_{P4} = (g_1^{-\frac{1}{2\ell}} \cdot g^s)^{\frac{1}{H_w}}$ 。

正确性:

$$\text{令 } r'_i = \left(r_i - \frac{a}{2\ell}\right) \cdot \left(\frac{1}{H(ID_i)}\right), s' = \left(s - \frac{a}{2\partial}\right) \cdot \left(\frac{1}{H_w}\right)$$

$$K_{P1} = x_{1,0} \cdot g_1^{-\frac{1}{2\ell}} \cdot \mu^{r_i} \cdot g_1^{-\frac{1}{2\ell}} \cdot v^s = x_{1,0} \cdot g_2^{\frac{a}{2\ell}} \cdot g_2^{-\frac{a}{2\ell}} \cdot g_1^{-\frac{a}{2\ell}} \cdot g_1^{-\frac{a}{2\ell}} \cdot v^s$$

$$= x_{1,0} \cdot g_2^{\frac{a}{2\ell}} \cdot (g_2^\ell g)^{-\frac{a}{2\ell}} \cdot v^s$$

$$= x_{1,0} \cdot g_2^{\frac{a}{2\ell}} \cdot (g_2^\ell g)^{-\frac{a}{2\ell}} \cdot v^s = x_{1,0} \cdot g_2^{\frac{a}{2\ell}} \cdot \mu^{r'_i - \frac{a}{2\ell}} \cdot v^{s - \frac{a}{2\partial}} = x_{1,0} \cdot g_2^{\frac{a}{2\ell}} \cdot \mu^{r'_i H(ID_i)} \cdot v^{s' H_w}$$

$$K_{P3} = (g_1^{-\frac{1}{2\ell}} \cdot g^{r_i})^{\frac{1}{H(ID_i)}} = (g^{r_i - \frac{a}{2\ell}})^{\frac{1}{H(ID_i)}} = g^{r'_i},$$

$$K_{P4} = (g_1^{-\frac{1}{2\ell}} \cdot g^s)^{\frac{1}{H_w}} = (g^{s - \frac{a}{2\partial}})^{\frac{1}{H_w}} = g^{s'}$$

情况 2 用户  $1$  是授权人, 将其签密权利授权给用户  $i \circ C$

随机选择  $r_i, s \in \mathbb{Z}_p^*$  并计算:  $K_{P1} = x_{1,0} \cdot g_1^{-\frac{1}{2\ell}} \cdot \mu^{r_i} \cdot g_1^{-\frac{1}{2\ell}} \cdot v^s, K_{P2} = x_{1,1}, K_{P3} = (g_1^{-\frac{1}{2\ell}} \cdot g^{r_i})^{\frac{1}{H(ID_i)}}, K_{P4} = (g_1^{-\frac{1}{2\ell}} \cdot g^s)^{\frac{1}{H_w}}$ 。

$$\text{令 } r'_i = \left(r_i - \frac{a}{2\ell}\right) \cdot \left(\frac{1}{H(ID_i)}\right), s' = \left(s - \frac{a}{2\partial}\right) \cdot \left(\frac{1}{H_w}\right), \text{ 则}$$

代理签密密钥为  $psk = (x_{1,0} \cdot g_2^{\frac{a}{2\ell}} \cdot \mu^{r'_i H(ID_i)} \cdot v^{s' H_w}, x_{1,1}, g^{r'_i}, g^{s'})$ 。

若  $\ell \cdot H(ID_i) = 0 \bmod p$  或  $\partial \cdot H_w = 0 \bmod p$ , 算法  $C$  终止; 否则将代理签密密钥  $psk$  发送给  $A$ 。

② 代理签密询问。若  $\ell \cdot H(ID_i) \neq 0 \bmod p$  且  $\ell \cdot H(ID_i) \neq 0 \bmod p$ ,  $A$  进行代理密钥询问产生代理签密密钥  $psk$ , 运行代理签密算法; 否则  $C$  终止。

③ 代理解签密询问。攻击者  $A$  对密文  $\sigma$  完成解签密询问。若  $\ell \cdot H(ID_B) = 0 \bmod p$ ,  $C$  终止; 否则  $C$  运行密钥提取询问计算  $s_{ID_B} = \{x_{B,0}, x_{B,1}\}$ , 计算  $M = H_1(T) \oplus C = H(e(x_{B,1}, \sigma_2) \cdot e(x_{B,0}, \sigma_1)^{-1}) \oplus N$ , 验证方程成立,  $C$  返回  $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, M)$  给  $A$ 。

3) 伪造。若  $C$  能完成以上的询问, 则  $A$  能以不可忽略的概率返回一个有效的签密伪造。这个伪造可以是下面两种情形之一:

情况 1  $A$  输出消息  $M^*$  的有效代理签密密文  $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*, C^*)$ 。

若  $\ell \cdot H(ID^*) \neq 0 \bmod p$  且  $\partial \cdot H_w \neq 0 \bmod p$  且  $\lambda \cdot H(M^*) \neq 0 \bmod p$ , 算法  $C$  终止。

若  $\ell \cdot H(ID^*) = 0 \bmod p$  且  $\partial \cdot H_w = 0 \bmod p$  且  $\lambda \cdot H(M^*) = 0 \bmod p$ , 算法  $C$  计算:

$$\frac{\sigma_6^*}{x_{1,0} \cdot (\sigma_4^*)^{H(ID^*)} \cdot (\sigma_5^*)^{H_w} \cdot (\sigma_1^*)^\eta \cdot (\sigma_1^*)^{H(M^*)}} = \frac{x_{1,0} \cdot g_2^a \cdot \mu^{r^* H(ID^*)} \cdot v^{s^* H_w} \cdot \sigma^{k^*} \cdot \tau^{k^* H(M^*)}}{x_{1,0} \cdot (g^{r^*})^{H(ID^*)} \cdot (g^{s^*})^{H_w} \cdot (g^{k^*})^\eta \cdot (g^{k^*})^{H(M^*)}} = \frac{[x_{1,0} \cdot g_2^a \cdot (g_2^\ell \cdot g)^{r^* H(ID^*)} \cdot (g_2^\partial \cdot g)^{s^* H_w} \cdot (g^\eta)^{k^*} \cdot (g_2^\lambda \cdot g)^{k^* H(M^*)}] \cdot [x_{1,0} \cdot (g^{r^*})^{H(ID^*)} \cdot (g^{s^*})^{H_w} \cdot (g^{k^*})^\eta \cdot (g^{k^*})^{H(M^*)}]^{-1}}{g_2^a} = g^{ab}$$

情况 2  $A$  输出消息  $M^*$  的有效代理签密密文  $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*, C^*)$ 。

若  $\ell \cdot H(ID^*) \neq 0 \bmod p$  且  $\partial \cdot H_w \neq 0 \bmod p$  且  $\lambda \cdot H(M^*) \neq 0 \bmod p$ , 算法  $C$  终止。

若  $\ell \cdot H(ID^*) = 0 \bmod p$  且  $\partial \cdot H_w = 0 \bmod p$  且  $\lambda \cdot H(M^*) = 0 \bmod p$ , 算法  $C$  计算:

$$\frac{\sigma_6^*}{x_{1,0} \cdot (\sigma_4^*)^{H(ID^*)} \cdot (\sigma_5^*)^{H_w} \cdot (\sigma_1^*)^\eta \cdot (\sigma_1^*)^{H(M^*)}} = g^{ab}$$

若  $C$  模拟成功, 则  $C$  可进行询问阶段和伪造阶段, 与定理 1 概率分析相同, 可以得到算法  $C$  模拟的成功概率为:

$$P[\text{abort}] = \left(1 - \frac{q_{pe}}{p}\right)^2 \cdot \left(1 - \frac{q_{sc}}{p}\right)^2 \cdot \left(1 - \frac{q_{usc}}{p}\right)^2 \cdot \frac{1}{p^3}$$

$$\text{所以有 } \varepsilon' = \left(1 - \frac{q_{pe}}{p}\right)^2 \cdot \left(1 - \frac{q_{sc}}{p}\right)^2 \cdot \left(1 - \frac{q_{usc}}{p}\right)^2 \cdot \frac{\varepsilon}{p^3}$$

完成整个运算过程大概所需的时间为  $t' = t + (6q_{pe} + 5q_{sc} + 3q_{usc})t_e + (q_{sc} + 4q_{usc})t_p$ 。

## 5 效率分析

表 1 给出文献[20-21]方案与本文方案效率的比较, 其中:  $E$  表示指数运算,  $P$  表示对运算。

表 1 基于身份代理签密方案效率比较

方案	安全模型	代理密钥生成	代理签密	代理解签密
文献[20]方案	随机预言机模型	2E+3P	2E+2P	3E+3P
文献[21]方案	随机预言机模型	E+3P	2E+2P	4E+8P
本文方案	标准模型	E+2P	3E+P	3E+4P

目前, 对运算是最耗时的运算。从表 1 中可以看出, 在代理密钥生成阶段, 和文献[20-21]相比, 所提方案仅仅需要 2 个对运算, 而文献[20]方案需要 3 个对运算, 文献[21]方案需要 3 个对运算; 在代理签名阶段, 所提方案仅仅需要 1 个对运算, 而文献[20]方案需要 2 个对运算, 文献[21]方案需要 2 个对运算; 代理解签密阶段, 本方案需要 4 个对运算, 少于文献[21]的 8 个对运算, 而高于文献[20]的 3 个对运算, 但是所提方案能够在标准模型下实现安全性, 而文献[20-21]仅仅在随机预言机模型下实现安全性。

## 6 结语

本文结合基于身份签密和代理签名的功能, 基于 Gu 的代理签名方案提出了标准模型下可证安全的基于身份的代理签密方案, 并且对方案的安全性和效率进行了分析。安全分析表明, 方案在 DBDH 和 CDH 问题假设困难的情况下, 该方案是满足安全性的。方案既保证了基于身份的签密优点又具有了代理签名的功能, 与已有方案相比, 本方案具有较高的效率。

## 参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation [C]// Proceedings of the 3rd ACM Conference on Communications Security. New York: ACM, 1996: 48–57.
  - [2] BODYREVA A, PALACIO A, WARINSCHI B. Security proxy signature schemes for delegation of signing rights[EB/OL]. [2014-4-10]. <http://eprint.iacr.org/2003/096.pdf>.
  - [3] SUN Y, XU C, YU Y, *et al.* Strongly unforgeable proxy signature scheme secure in the standard model [J]. Journal of Systems and Software, 2011, 84(9): 1471–1479.
  - [4] OKAMOTO T, INOMATA A, OKAMOTO E. A proposal of short proxy signature using pairing [C]// Proceedings of the International Conference on Information Technology: Coding and Computing. Piscataway: IEEE Press, 2005: 631–635.
  - [5] LU R, CAO Z, DONG X, *et al.* Designated verifier proxy signature scheme from bilinear pairings [C]// Proceedings of the 1st International Multi-Symposiums on Computer and Computational Sciences. Piscataway: IEEE Press, 2006: 40–47.
  - [6] HUANG X Y, MU Y, SUSILO W, *et al.* Short designated verifier proxy signature from pairings [C]// Proceedings of the 2005 Embedded Ubiquitous Computing-EUC 2005 Workshops. Berlin: Springer-Verlag, 2005: 835–844.
  - [7] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO '84—Advances in Cryptology. Berlin: Springer-Verlag, 1984: 47–53.
  - [8] BONEH D, RANKLIN M. Identity-based encryption from the Weil pairing [C]// Proceedings of the 21st Annual International Conference—Advances in Cryptology. Berlin: Springer-Verlag, 2001: 213–229.
  - [9] ZHENG Y. Digital signcryption or how to achieve cost (signature&encryption) << cost (signature) + cost (encryption) [C]// Proceedings of the 17th Annual International Cryptology Conference—Advances in Cryptology. Berlin: Springer-Verlag, 1997: 165–179.
  - [10] BEAK J, STEINFELD R, ZHENG Y. Formal proofs for the security of signcryption [C]// Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems. Berlin: Springer-Verlag, 2002: 81–98.
  - [11] MALONE-LEE J. Identity-based signcryption [EB/OL]. [2014-03-25]. <http://eprint.iacr.org/2002/098.pdf>.
  - [12] YU Y, YANG B, SUN Y, *et al.* Identity based signcryption scheme without random oracles [J]. Computer Standards and Interfaces, 2009, 31(1): 56–62.
  - [13] ZHANG B. Cryptanalysis of an identity based signcryption scheme without random oracles [J]. Journal of Computational Information Systems, 2010, 6(6): 1923–1931.
  - [14] JIN Z, W Q Y, DU H Z. An improved semantically-secure identity-based signcryption scheme in the standard model [J]. Computer & Electrical Engineering, 2010, 36(3): 545–552.
  - [15] LI F, LIAO Y, QIN Z. Analysis of an identity-based signcryption scheme in the standard model [J]. IEICE Transactions on Fundamental of Electronics, Communications and Computer Science, 2011, 94(1): 268–269.
  - [16] LI F, KHURRAM KHAN M, ALGHATHBAR K, *et al.* Identity-based online/offline signcryption for low power devices [J]. Journal of Network and Computer Applications, 2012, 35(1): 340–347.
  - [17] LI F, TKGI T. Secure identity-based signcryption in standard model [J]. Mathematical and Computer Modelling, 2013, 57(11): 2685–2694.
  - [18] GAMAGE C, LEIWO J, ZHENG Y. An efficient scheme for secure message transmission using proxy-signcryption [C]// Proceedings of the 22nd Australasian Computer Science Conference. Berlin: Springer-Verlag, 1999: 18–21.
  - [19] LI X, CHEN K. Identity-based proxy-signcryption scheme from pairing [C]// Proceedings of the 2004 IEEE International Conference on Services Computing. Washington, DC: IEEE Computer Society, 2004: 494–497.
  - [20] WANG Q, CAO Z. Efficient ID-based proxy signature and proxy signcryption from bilinear pairings [C]// Proceedings of the 2005 International Conference on Computational Intelligence and Security. Berlin: Springer-Verlag, 2005: 167–172.
  - [21] WANG M, LI H, LIU Z. Efficient identity based proxy-signcryption schemes with forward security and public verifiability [C]// Proceedings of the 3rd International Conference on Networking and Mobile Computing. Berlin: Springer-Verlag, 2005: 982–991.
  - [22] SWAPNA G, GOPAL P V S S N, GOWRI T, *et al.* An efficient Identity-based proxy signcryption scheme [J]. International Journal of Information and Network Security, 2012, 1(3): 200–206.
  - [23] GU K, JIA W, JIANG C. Efficient identity-based proxy signature in the standard model [J]. The Computer Journal, 2013: bxt132.
- 
- (上接第 2833 页)
- [8] ZABA M R, RADDUM H, HENRICKSEN M, *et al.* Bit-pattern based integral attack [C]// Proceedings of the 2008 15th International Workshop on Fast Software Encryption. Berlin: Springer, 2008: 363–381.
  - [9] KNUDSEN L, WAGNER D. Integral cryptanalysis [C]// Proceedings of the 2002 9th International Workshop on Fast Software Encryption. Berlin: Springer, 2002: 112–127.
  - [10] FERGUSON N, KELSEY J, LUCKS S, *et al.* Improved cryptanalysis of Rijndael [C]// Proceedings of the 1978 7th International Workshop on Fast Software Encryption. Berlin: Springer, 2001: 213–230.
  - [11] LI Y, WU W, ZHANG L. Integral attacks on reduced round ARIA block cipher [C]// Proceedings of the 2010 6th Information Security Practice and Experience Conference. Berlin: Springer, 2010: 19–29.
  - [12] LIU F, JI W, HU L, *et al.* Analysis of the SMS4 block cipher [C]// Proceedings of the 2007 Australasian Conference on Information Security and Privacy. Berlin: Springer, 2007: 158–170.
  - [13] WU W, ZHANG W, FENG D. Integral cryptanalysis of reduced FOX block cipher [C]// Proceedings of the 2005 International Conference on Information Security and Cryptography. Berlin: Springer, 2006: 229–241.
  - [14] ZHANG P, SUN B, LI C. Saturation attack on the block cipher HIGHT [C]// Proceedings of the 2009 8th International Conference on Cryptology and Network Security. Berlin: Springer, 2009: 76–86.
  - [15] LI Y, WU W, ZHANG L, *et al.* Improved integral attacks on reduced round Camellia [EB/OL]. [2014-03-04]. <https://eprint.iacr.org/2011/163>.
  - [16] DUO L, LI C, FENG K. Square like attack on Camellia [C]// Proceedings of the 2007 9th International Conference on Information and Communication Security. Berlin: Springer, 2007: 269–283.