

文章编号:1001-9081(2014)09-2659-05

doi:10.11772/j.issn.1001-9081.2014.09.2659

## 结合在线/离线方法的无证书签密

赵晶晶\*, 赵雪霞, 石岳蓉

(河海大学 计算机与信息学院, 南京 210098)

(\* 通信作者电子邮箱 565474418@qq.com)

**摘要:**作为密码学原语,签密同时具有签名的认证性与加密的机密性。在线/离线签密结合了在线/离线的方法,在已有基础上提高了系统的效率。但目前的在线/离线签密方案大多数都是在基于身份的环境下实现的,都存在密钥托管的安全问题。基于无证书密码体制撤销证书管理及无密钥托管的优点,提出了一种安全的在线/离线的无证书签密方案,满足离线阶段不需要确定接收者身份信息的条件,并在随机预言模型中证明了方案的安全性。

**关键词:**无证书签密; 基于身份密码学; 认证性; 机密性; 在线/离线; 随机预言模型

中图分类号: TP309 文献标志码:A

### Certificateless signcryption with online/offline technique

ZHAO Jingjing\*, ZHAO Xuexia, SHI Yuerong

(College of Computer and Information, Hohai University, Nanjing Jiangsu 210098, China)

**Abstract:** Signcryption as a cryptographic primitive is a splendid combination of signature with authentication and encryption with confidentiality simultaneously. Online/offline signcryption, with the online/offline technique, provides higher efficiency for the system. However, most of the present signcryption schemes are implemented in the identity-based setting in which there exists key escrow problem. Based on the certificateless cryptography system's advantages with revocation of certificate management and without key escrow problem, a secure online/offline certificateless signcryption scheme was proposed. The proposed scheme satisfied the requirement that there is no need to determine the recipient's information in the offline stage. Moreover, its security was proved in the Random Oracle Model (ROM).

**Key words:** certificateless signcryption; identity-based cryptography; authentication; confidentiality; online/offline; Random Oracle Model (ROM)

## 0 引言

在电子商务中,认证性与机密性是最基本也是重要的要求。电子商务不免涉及移动设备与智能卡,然而它们的物理层易受到攻击,因此,一些有效的密码学保护非常必要。但由于这些设备本身存在功率受限的本质,致使设计出代价低的算法显得尤为重要。

Zheng<sup>[1]</sup>第一次提出签密的原语,它同时拥有不可伪造性与机密性,相对于签名与加密的简单结合,具有更少的计算复杂度和更低的通信代价; Malone-Lee<sup>[2]</sup>首次提出基于身份的签密,文献[3-6]提出的方案在效率与安全性方面作出了相应的改进。

An等<sup>[7]</sup>提出在线/离线的签密。在线/离线原语的原则是在线阶段的计算代价尽量小,换言之,大部分复杂的操作,如指数、双线性对操作,应该在离线阶段完成。为提高系统的灵活性,待签密的消息与接收者的身份信息在离线阶段应该是未知的。然而,An等在文献[7]中并未给出在线/离线签密的具体方案,旨在阐述在线/离线签密的安全模型,并给出其通用构造的分析。之后,Zhang等<sup>[8]</sup>给出了具体的在线/离线的签密方案,但是该方案需要额外的对称密钥加密方案才能获得整体方案的机密性。

为解决基于身份密码学内的密钥托管问题,Al-Riyami

等<sup>[9]</sup>提出了无证书密码学系统。无证书签密的概念首先在文献[10]中给出。目前,大部分的无证书签密方案并不安全,如 Selvi 等<sup>[11]</sup>指出了文献[10,12-13]存在的安全性问题。

文献[14]提出了无证书的在线/离线签密,但在其离线阶段接收者的身份是已知的,这不满足文献[15]对在线/离线概念的定义,降低了方案的灵活性,造成其实用性的退化。并且,文献[16]指出文献[14]的方案存在安全性问题,攻击者可以通过窃听消息得到用户的私钥。所以,针对目前方案的不足,本文拟提出一个全新的、可证明安全的在线/离线的无证书签密方案。

## 1 预备知识

### 1.1 双线性映射

令  $\kappa$  为安全参数,  $G, G_T$  分别是以大素数  $q$  为阶的加法群和乘法群,  $g$  是  $G$  的生成元, 若存在映射  $e: G \times G \rightarrow G_T$  满足以下性质, 则此映射为双线性映射:

双线性性 对所有的  $u, v \in G$ , 以及  $a, b \in \mathbf{Z}_q^*$ , 满足  $e(u^a, v^b) = e(u, v)^{ab}$ 。

非退化性  $e(g, g) \neq 1$ 。

可计算性 对任意的  $u, v \in G$ , 存在一个有效的算法计算  $e(u, v)$ 。

收稿日期:2014-03-13;修回日期:2014-05-23。

作者简介:赵晶晶(1990-),女,安徽芜湖人,硕士研究生,主要研究方向:在线/离线签密; 赵雪霞(1989-),女,河南长葛人,硕士研究生,主要研究方向:代理重加密; 石岳蓉(1990-),女,甘肃定西人,硕士研究生,主要研究方向:基于属性的加密。

## 1.2 困难问题

**定义 1**  $l$ -Strong Diffie-Hellman 假设 ( $l$ -SDH)<sup>[17]</sup>。输入  $(l+1)$  元元组  $(g, g^{\alpha}, g^{\alpha^2}, \dots, g^{\alpha^l}) \in G^{l+1}$ , 输出  $(c, g^{1/(\alpha+c)})$ , 其中  $c \in \mathbf{Z}_q^*$ , 如果不存在算法以优势  $\varepsilon$  在时间  $t$  内解决  $G$  群中的  $l$ -SDH 问题, 则  $(t, \varepsilon, l)$ -SDH 假设在  $G$  中成立。

**定义 2**  $l$ -Bilinear Diffie-Hellman Inversion 假设 ( $l$ -BDHI)<sup>[18]</sup>。输入  $(l+1)$  元元组  $(g, g^{\alpha}, g^{\alpha^2}, \dots, g^{\alpha^l}) \in G^{l+1}$ , 输出  $e(g, g)^{1/\alpha} \in G_T$ , 如果不存在算法以优势  $\varepsilon$  在  $t$  时间内解决  $G$  群中的  $l$ -BDHI 问题, 则  $(t, \varepsilon, l)$ -BDHI 假设在  $G$  群中成立。

**定义 3** Computational Diffie-Hellman 假设 (CDH)。输入元组  $(g, g^a, g^b)$ , 输出  $g^{ab}$ , 如果不存在算法以优势  $\varepsilon$  在  $t$  时间内解决  $G$  群中的 CDH 问题, 则  $(t, \varepsilon)$ -CDH 假设在  $G$  群中成立。

## 2 新无证书在线/离线签密方案

1) 系统初始化。输入安全参数  $\kappa$ , 用户私钥生成中心 (Key Generation Center, KGC) 选择以大素数  $q$  为阶的加法群  $G$  和乘法群  $G_T$ , 并以  $g \in G$  作为生成元, 取  $e: G \times G \rightarrow G_T$  为双线性映射; KGC 随机选择  $s \in \mathbf{Z}_q^*$  作为主密钥  $msk$ ; 设  $g_1 = g^s$ ,  $g_2 = g_1^x$  为主公钥; 定义  $M$  为明文空间, 令  $n_M = |M|$ ; 同时, 令  $n_d$  为身份标识符的比特长度; 定义函数:  $H_1: \{0, 1\}^{n_d} \times G \rightarrow \mathbf{Z}_q^*$ ,  $H_2: G \times G \times G_T \times \{0, 1\}^{2n_d} \rightarrow \{0, 1\}^{n_M}$ ,  $H_3: \{0, 1\}^{n_M + 2n_d} \times G \rightarrow G$ 。则  $params = \{G, G_T, q, e, g, g_1, g_2, M, H_1, H_2, H_3\}$  即为系统公共参数。

2) 用户秘密值及公钥生成。用户  $A$  和  $B$  分别随机选取  $x_A, x_B \in \mathbf{Z}_q^*$  作为他们的秘密值, 则他们的公钥分别为  $PK_A = g^{x_A}, PK_B = g^{x_B}$ 。

3) 部分私钥生成。将  $ID_A, ID_B$  分别作为用户  $A, B$  的身份标识符, 则 KGC 计算  $d_A = g^{(s+H_1(ID_A, PK_A))^{-1}}, d_B = g^{(s+H_1(ID_B, PK_B))^{-1}}$  作为他们的部分私钥, 并分别通过安全信道发送给  $A, B$ 。

4) 用户完全私钥生成。用户  $A$  和  $B$  的完全私钥分别为  $(x_A, S_A), (x_B, S_B)$ 。用户可以计算并存储  $g_{ID} = e(g^{H_1(ID, PK_ID)}, g_1, g)$  值, 以供将来使用。

5) 离线签密生成。假设  $A$  为发送者, 在接收者的身份确定与待签密的消息到达以前,  $A$  做一些预计算来减少在线阶段的负担,  $A$  选择  $r, \alpha, \beta, \gamma, \delta, \mu \in \mathbf{Z}_q^*, C_1 = g^r, R = e(g^{H_1(ID_A, PK_A)}, g)^r = g^{rID_A}, T_0 = (g^{\alpha H_1(ID_A, PK_A)} \cdot g_1^{H_1(ID_A, PK_A)+\gamma} \cdot g_2)^r, T_1 = g^{\beta^{-1} H_1(ID_A, PK_A)r}, T_2 = g_1^{\delta^{-1}}, V_1 = g^{-\mu} d_A^{(r+x_A)}$ 。所以  $\sigma' = \langle C_1, r, R, T_0, T_1, T_2, V_1, \alpha, \beta, \gamma, \mu, \delta \rangle$  为离线阶段的密文。

6) 在线签密生成。当接收者的身份确定, 假设为  $B$ , 待签密的消息  $m \in M$  到达之后, 计算  $t_1 = \beta(H_1(ID_B, PK_B) - \alpha) \bmod q, t_2 = \delta(H_1(ID_B, PK_B) - \gamma) \bmod q, U = PK_B, C_2 = H_2(C_1, U, R, ID_A, ID_B) \oplus m, V_2 = g^\mu W, W = H_3(m, ID_A, ID_B, C_2)$ 。所以最终的密文为  $\sigma = \langle C_1, C_2, T_0, T_1, T_2, t_1, t_2, V_1, V_2 \rangle$ 。

7) 解密及验证。 $B$  在接收到密文  $\sigma = \langle C_1, C_2, T_0, T_1, T_2, t_1, t_2, V_1, V_2 \rangle$  以后, 计算  $U = C_1^x, R = e(T_0 T_1^t_1 T_2^t_2, d_B), m = C_2 \oplus H_2(C_1, U, R, ID_A, ID_B), W = H_3(m, ID_A, ID_B, C_2)$ , 然后验证  $e(V_1 V_2, g^{H_1(ID_A, PK_A)} g_1) = e(PK_A, W) e(C_1, W)$  是否成立,

若成立  $B$  接收消息  $m$ , 否则拒绝。

## 3 安全性分析

以上方案所涉及的安全模型参见文献[10]。

### 3.1 保密性证明

**定理 1** 类型 1 攻击下的机密性。在随机模型中, 如果存在对手  $A_1$  以优势  $\varepsilon$  在类型 1 攻击下(攻击者不知道 KGC 的主私钥, 但可以替换系统中任何用户的公钥)成功破坏以上方案的选择密文的不可区分性 (Indistinguishable-Chosen Ciphertext Attack- I , IND-CCA- I ), 则存在一个模拟者  $C$  在多项式时间内, 以至少  $\varepsilon \frac{1}{q_1} \left(1 - q_s \frac{q_s + q_2}{q}\right) \left(1 - \frac{q_d}{q}\right)$  的优势解决  $(l+1)$ -BDHI 的困难问题。其中,  $q_i (i = 1, 2, 3)$  是允许访问随机预言  $H_i (i = 1, 2, 3)$  的最大次数,  $q_s, q_d$  分别代表允许访问签密与解密预言的最大次数; 此处假设  $q_1 = l$ 。

**证明** 假设  $C$  是  $(l+1)$ -BDHI 困难问题的解决者,  $C$  接收到的  $(l+1)$ -BDHI 挑战实例为  $(g, g^a, g^{\alpha^2}, \dots, g^{\alpha^l}, g^{al+1}) \in G^{l+2}$ ,  $C$  以  $A_1$  作为子程序输出  $e(g, g)^{1/\alpha}$ 。 $C$  维持列表  $L_1, L_2, L_3, L_s, L_{ppk}, L_s$  和  $L_d$ , 分别记录  $H_1, H_2, H_3$ 、秘密值、部分私钥、签密和解密的询问, 列表初始化时都为空。 $C$  为  $A_1$  设定的模拟环境如下:

$C$  先随机选择  $\pi \in \{1, 2, \dots, q_1\}, I_\pi \in \mathbf{Z}_q^*, \omega_1, \omega_2, \dots, \omega_{\pi-1}, \omega_{\pi+1}, \dots, \omega_l \in \mathbf{Z}_q^*$ 。对于  $i \in \{1, 2, \dots, l\} \setminus \{\pi\}$ ,  $C$  计算  $I_i = I_\pi - \omega_i$ 。建立一个  $l-1$  次多项式  $f(z) = \prod_{i=1, i \neq \pi}^{l-1} (z + \omega_i) = \sum_{i=0}^{l-1} c_i z^i, c_0, c_1, \dots, c_{l-1} \in \mathbf{Z}_q^*$ 。然后设生成元为  $\hat{g} = g^{\sum_{i=0}^{l-1} c_i \alpha^i} = g^{f(a)}$ 。

对于  $i \in \{1, 2, \dots, l\} \setminus \{\pi\}$ ,  $C$  扩展  $f_i(z) = \frac{f(z)}{z + \omega_i} = \sum_{j=0}^{l-2} d_{i,j} z^j, d_{i,1}, d_{i,2}, \dots, d_{i,l-2} \in \mathbf{Z}_q^*$ , 设  $\tilde{H}_i = g^{\sum_{j=0}^{l-2} d_{i,j} \alpha^j} = g^{f_i(a)} = g^{f(a)/(a+\omega_i)} = \hat{g}^{1/(a+\omega_i)}$ , 计算  $g_1 = \hat{g}^{-a} \hat{g}^{-l\pi} = \hat{g}^{-a-l\pi}, g_2 = \hat{g}^{a^2} \hat{g}^{2l\pi} \hat{g}^{l\pi} = \hat{g}^{(a+l\pi)^2}$ , 其中  $\hat{g}^a = g^{\sum_{i=0}^{l-1} c_i \alpha^i}$ ,  $\hat{g}^{a^2} = g^{\sum_{i=0}^{l-1} c_i \alpha^{2i}}$ , 所以未知的主私钥隐含的设为  $msk = x = -a - I_\pi \in \mathbf{Z}_q^*$ 。对于  $i \in \{1, 2, \dots, l\} \setminus \{\pi\}, (I_i, \tilde{H}_i^{-1}) = (I_i, g^{1/(I_i+\pi)})$ 。

### 阶段 1:

$H_1$  查询: 输入  $(i, ID_i, PK_i)$ ,  $ID_i$  代表第  $i$  次询问的用户,  $PK_i$  为其相应的公钥。若  $i = \pi$ , 停止模拟。当  $i \neq \pi$  时, 如果列表  $L_1$  中已经存在该元组, 返回  $I_i$ ; 否则,  $C$  令  $I_i = H_1(ID_i, PK_i)$  返回给  $A_1$ , 并将元组  $(i, ID_i, PK_i, I_i)$  加到列表  $L_1$  中。

$H_2$  查询: 输入  $(r, C_1, U, R, ID_A, ID_B) (A, B \in \{1, 2, \dots, q_1\})$ ,  $ID_A, ID_B$  分别代表发送者与接收者, 若列表  $L_2$  中存在该元组, 返回相应的哈希值  $h_2 = H_2(C_1, U, R, ID_A, ID_B)$  给  $A_1$ ; 否则,  $C$  随机选择  $h_2 \in \mathbf{Z}_q^*$  返回给对手, 同时将  $(r, C_1, U, R, ID_A, ID_B)$  加到  $L_2$  中。

$H_3$  查询: 输入  $(m, ID_A, ID_B, C_2) (A, B \in \{1, 2, \dots, q_1\})$ , 若  $L_3$  中存在元组与之匹配, 则返回给  $A_1$  相应的值  $W = H_3(m, ID_A, ID_B, C_2)$ ; 否则,  $C$  随机选择  $W \in G$  返回给对手, 并将  $(m, ID_A, ID_B, C_2, W)$  加入  $L_3$  中。

部分私钥询问: 当输入身份  $ID_i (i = \pi)$ ,  $C$  停止; 否则, 返

回 $\tilde{H}_i^{-1} = g^{1/(I_{i+x})}$ 。

秘密值询问:当输入身份 $ID_i$ ,若 $L_x$ 中存在元组 $(i, ID_i, x_i, PK_i)$ ,返回 $x_i$ 给 $A_1$ ;否则, $C$ 选择 $x_i \in_R \mathbf{Z}_q^*$ ,计算 $PK_i = g^{x_i}$ ,将 $(i, ID_i, x_i, PK_i)$ 添加到 $L_x$ ,并返回 $x_i$ 给 $A_1$ 。

公钥询问:输入身份 $ID_i$ ,搜索 $L_x$ ,若存在则返回 $PK_i$ ;否则 $C$ 选择 $x_i \in_R \mathbf{Z}_q^*$ ,计算 $PK_i = g^{x_i}$ ,将 $PK_i$ 返回给对手,在 $L_x$ 中添加 $(i, ID_i, x_i, PK_i)$ 。

公钥替换询问:输入一个合法的公钥 $PK \in G$ 和身份 $ID_i$ ,先检索列表 $L_x$ ,如存在元组 $(i, ID_i, x_i, PK_i)$ ,则将其改为 $(i, ID_i, \perp, PK)$ ;若不存在,则先运行公钥询问,然后将其公钥替换成 $PK$ 。当 $L_x$ 中的相应的公钥被替换时,则 $L_1$ 列表中相应身份的公钥也同样要被替换掉。这种情况下,用户的秘密值需要由对手提供。

签密询问:输入明文 $m$ ,发送方与接收方 $(ID_A, ID_B)$ ,这里需要考虑两种情况,当 $A \neq \pi$ , $C$ 知道 $ID_A$ 的完全私钥,所以能够正确运行签密算法;当 $A = \pi$ , $C$ 的任务就是找到满足等式 $e(V_1 V_2, g^{H_1(ID_A, PK_A)} g_1) = e(PK_A, W) e(C_1, W)$ 的密文 $\sigma = \langle C_1, C_2, T_0, T_1, T_2, t_1, t_2, V_1, V_2 \rangle$ 。则 $C$ 选择 $r, \alpha, \beta, \gamma, \delta, k \in \mathbf{Z}_q^*$ ,计算 $T_0 = (g^{aH_1(ID_A, PK_A)} \cdot g_1^{H_1(ID_A, PK_A)+\gamma} \cdot g_2)^r, T_1 = g^{\beta^{-1}H_1(ID_A, PK_A)r}, T_2 = g_1^{\delta^{-1}}, t_1 = \beta(H_1(ID_B, PK_B) - \alpha) \bmod q, t_2 = \delta(H_1(ID_B, PK_B) - \gamma) \bmod q, U = PK_B$ ,令 $V_1 = PK_A \cdot g^k, V_2 = C_1, W = (g^{H_1(ID_A, PK_A)} \cdot g_1) \cdot g^{-k} = H_3(m, ID_A, ID_B, C_2)$ ,则 $C_3 = m \oplus H_2(C_1, U, R, ID_A, ID_B)$ ,将该密文 $\sigma = \langle C_1, C_2, T_0, T_1, T_2, t_1, t_2, V_1, V_2 \rangle$ 返回给对手,并加到 $L_x$ 中。

解密询问:输入密文 $\sigma = \langle C_1, C_2, T_0, T_1, T_2, t_1, t_2, V_1, V_2 \rangle$ ,接收者身份标识符 $ID_B$ ,当 $B \neq \pi$ 时, $C$ 知道 $ID_B$ 的完全私钥,可以运行解密算法正确解密。否则, $C$ 计算 $U = C_1^{\gamma_B}$ ,在 $L_2$ 搜索 $(\perp, C_1, U, \perp, ID_A, ID_B)$ ( $\perp$ 表示该值未知),若存在则返回其哈希值进行解密 $m = C_2 \oplus H_2(C_1, U, \perp, ID_A, ID_B)$ ;若不存在, $C$ 则返回一个随机值 $h_2 = H_2(C_1, U, \perp, ID_A, ID_B) \in_R \mathbf{Z}_q^*$ 解密,并将 $(\perp, C_1, U, \perp, ID_A, ID_B, h_2)$ 加入 $L_2$ 中。然后验证 $e(V_1 V_2, g^{H_1(ID_A, PK_A)} g_1) = e(PK_A, W) e(C_1, W)$ 是否成立,若成立则返回 $m$ 给对手;否则返回 $\perp$ 。

挑战阶段: $A_1$ 输出 $(m_0, m_1, ID_A, ID_B^*)$ ,如果 $ID_B^* \neq ID_\pi$ , $C$ 停止。否则, $C$ 选择 $t_1^*, t_2^*, \tilde{t}_0, \tilde{t}_1, \tilde{t}_2 \in_R \mathbf{Z}_q^*, C_2^* \in_R \{0, 1\}^n, C_1^*, V_1^*, V_2^* \in_R G$ ,计算 $T_0^* = g^{\tilde{t}_0}, T_1^* = g^{\tilde{t}_1}, T_2^* = g^{\tilde{t}_2}$ ,然后将 $\sigma^* = \langle C_1^*, C_2^*, T_0^*, T_1^*, T_2^*, t_1^*, t_2^*, V_1^*, V_2^* \rangle$ 作为挑战密文发送给 $A_1$ 。令 $\xi = \tilde{t}_0 + t_1^* \tilde{t}_1 + t_2^* \tilde{t}_2$ ,则 $T^* = \hat{g}^{-\xi}$ 。令 $\rho = \frac{\xi}{\alpha(I_A - \alpha - I_\pi)} = -\frac{\xi}{(I_\pi + x)(I_A + x)}$ ,因为 $x = -\alpha - I_\pi$ , $T^* = \hat{g}^{-\xi} = \hat{g}^{-\alpha(I_\pi - \alpha - I_\pi)\rho} = \hat{g}^{(I_\pi + x)(I_A + x)\rho} = \hat{g}^{(I_\pi I_A + (I_\pi + I_A)x + x^2)\rho}$ 。

阶段2:

$A_1$ 继续进行如同阶段1的适应性询问,但不能询问在身份 $(ID_A^*, ID_B^*)$ 条件下的 $\sigma^* = \langle C_1^*, C_2^*, T_0^*, T_1^*, T_2^*, t_1^*, t_2^*, V_1^*, V_2^* \rangle$ 解密询问。

猜测: $A_1$ 不能察觉出 $\sigma^*$ 不是合法的密文,除非向 $H_2$ 发起关于 $R^* = e(\hat{g}^{I_\pi} g_1, \hat{g})^\rho$ 的询问。在猜测过程中, $A_1$ 的观点如上模拟,但是它的输出会被忽视。标准地来说,为表现模拟环境不可区分于真实环境,应该给出成功的 $A_1$ 很大可能会以输入 $R^* = e(\hat{g}^{I_\pi} g_1, \hat{g})^\rho$ 去询问 $H_2$ 的情况。

解决挑战: $C$ 从 $L_2$ 中随机选择元组 $(r, C_1, U, R, ID_A, ID_B)$ ,

$h_2$ ),选中的元组中包含正确的 $R^* = e(\hat{g}^{I_\pi^*} g_1, \hat{g})^\rho = e(g, g)^{-\xi/(I_\pi + x)} = e(g, g)^{f(a)2^{l/\alpha}} (f(z) = \sum_{i=0}^{l-1} c_i z^i, \hat{g} = g^{f(a)})$ 值的概率为 $1/q_2$ 。则 $(l+1)$ -BDHI问题的解可通过以下的过程提取出来:

$$\left( \frac{R^{1/\xi}}{e(g, g)^{\sum_{i=0}^{l-2} c_{i+1} a^i} e(g^{c_0})} \right)^{1/c_0^2} = \left( \frac{e(g, g)^{f(a)2^{l/\alpha}}}{e(g, g)^{[f(a)^2 - (c_1 a + c_2 a^2 + \dots + c_{l-1} a^{l-1})(c_0 + f(a))] / a}} \right)^{1/c_0^2} = e(g, g)^{\frac{2}{c_0^2}(c_0^2 a)} = e(g, g)^{1/a}$$

概率分析:

$C$ 在以下的情况下会模拟失败:

1)  $E_1: A_1$ 未选择 $ID_\pi$ 作为挑战接收者的身份;

2)  $E_2: A_1$ 询问 $ID_\pi$ 的部分私钥;

3)  $E_3$ :在签密询问中由于 $H_2$ 的碰撞而停止;

4)  $E_4: C$ 在游戏过程中拒绝一个合法的密文。

因为 $\Pr[\neg E_1] = 1/q_1$ ,从 $\neg E_1$ 可以推导出 $\neg E_2$ ,可得出 $\Pr[E_3] \leq q_s q_s + q_2)/q, \Pr[E_4] \leq q_d/q$ 。结合起来,得到总体成功的概率为 $\Pr[\neg E_1 \wedge \neg E_3 \wedge \neg E_4] = \frac{1}{q_1} \left(1 - \frac{q_s + q_2}{q}\right) \left(1 - \frac{q_d}{q}\right)$ 。

定理2 类型2攻击下的机密性。在随机模型中,如果存在一个对手 $A_{\text{II}}$ 能以优势 $\varepsilon$ 在类型2的攻击下(攻击者知道KGC的主私钥,但不能替换系统中任意用户的公钥)成功破坏以上方案的选择密文的不可区分性(Indistinguishable-Chosen Ciphertext Attack-II, IND-CCA-II),则存在一个模拟者 $C$ 在多项式时间内,以至少 $\varepsilon \frac{1}{q_s} \left(1 - \frac{q_s + q_2}{q}\right) \left(1 - \frac{q_d}{q}\right)$ 的概率成功解决CDH困难问题。其中, $q_i (i = 1, 2, 3)$ 是允许访问随机预言 $H_i (i = 1, 2, 3)$ 的最大次数, $q_s, q_d$ 分别代表允许访问秘密值、签密与解密预言的最大次数。

证明 假设 $C$ 接收到的CDH挑战实例为 $(g, g^a, g^b)$ , $C$ 以 $A_{\text{II}}$ 作为子程序输出 $g^{ab}$ 。 $C$ 维持列表 $L_1, L_2, L_3, L_x, L_s$ 和 $L_d$ ,分别记录 $H_1, H_2, H_3$ 、秘密值、签密和解密的询问,初始化时每个列表都为空。 $C$ 为 $A_{\text{II}}$ 设定的模拟环境如下, $C$ 先随机选择 $\pi \in \{1, 2, \dots, q_s\}$ :

阶段1:

$H_1$ 查询:输入 $(i, ID_i, PK_i), ID_i$ 表示第*i*次询问的用户身份, $PK_i$ 为其相应的公钥。如果列表 $L_1$ 中已经存在该元组,返回 $I_i$ ;否则, $C$ 选择 $I_i = H_1(ID_i, PK_i) \in_R \mathbf{Z}_q^*$ 返回给 $A_{\text{II}}$ ,并将元组 $(i, ID_i, PK_i, I_i)$ 加到列表 $L_1$ 中。

$H_2$ 查询:同定理1证明。

$H_3$ 查询:同定理1证明。

部分私钥询问:无需此询问,因为 $C$ 知道 $msk$ 的值,可以自行计算。

秘密值询问:当输入身份 $ID_i$ ,当 $i = \pi$ 时,停止模拟。否则,查询 $L_x$ ,存在元组 $(i, ID_i, x_i, PK_i)$ ,返回 $x_i$ 给 $A_{\text{II}}$ ;不存在则 $C$ 选择 $x_i \in_R \mathbf{Z}_q^*$ ,计算 $PK_i = g^{x_i}, (i, ID_i, x_i, PK_i)$ 添加到 $L_x$ ,并

返回给  $A_{\text{II}}$ 。

公钥询问: 输入身份  $ID_i$ , 当  $i = \pi$ , 返回  $PK_{\pi} = g^a$ 。否则, 搜索  $L_s$ , 若存在则返回  $PK_i$ ; 否则  $C$  选择  $x_i \in_R \mathbf{Z}_q^*$ , 计算  $PK_i = g^{x_i}$ , 将  $PK_i$  返回给对手, 在  $L_s$  中添加  $(i, ID_i, x_i, PK_i)$ 。

公钥替换询问: 输入合法的公钥  $PK \in G$  和身份  $ID_i$ , 当  $i = \pi$ , 停止; 否则同定理 1 证明。

签密询问: 同定理 1 证明。

解密询问: 输入  $\sigma = \langle C_1, C_2, T_0, T_1, T_2, t_1, t_2, V_1, V_2 \rangle$ , 接收者身份  $ID_B$ , 当  $B \neq \pi$  时,  $C$  知道接收者的完全私钥, 可以运行解密算法正确解密。否则,  $C$  能利用自己知道  $ID_B$  的部分私钥计算出  $R$ , 在  $L_2$  搜索  $(r, C_1, \perp, R, ID_A, ID_B)$ , 若存在则返回其哈希值进行解密  $m = C_2 \oplus H_2(C_1, \perp, R, ID_A, ID_B)$ ; 若不存在,  $C$  则随机选择哈希值  $h_2 = H_2(C_1, \perp, R, ID_A, ID_B) \in_R \mathbf{Z}_q^*$  解密, 并将  $(\perp, C_1, \perp, R, ID_A, ID_B, h_2)$  加入  $L_2$  中。然后验证  $e(V_1 V_2, g^{H_1(ID_A, PK_A)} g_1) = e(PK_A, W) e(C_1, W)$  是否成立, 若成立则返回  $m$  给对手; 否则返回  $\perp$ 。

挑战阶段:  $A_{\text{I}}$  输出  $(m_0, m_1, ID_A^*, ID_B^*)$ , 如果  $ID_B^* \neq ID_{\pi}$ ,  $C$  停止; 否则,  $C$  选择  $t_1^*, t_2^* \in_R \mathbf{Z}_q^*$ ,  $C_2^* \in_R \{0, 1\}^{nM}$ ,  $T_0^*, T_1^*, T_2^*, V_1^*, V_2^* \in_R G$ , 令  $C_1^* = g^b$ , 然后将  $\sigma^* = \langle C_1^*, C_2^*, T_0^*, T_1^*, t_1^*, t_2^*, V_1^*, V_2^* \rangle$  作为挑战密文发送给  $A_{\text{II}}$ 。

阶段 2:

$A_{\text{II}}$  进行同阶段 1 的适应性询问, 但不能询问  $\sigma^* = \langle C_1^*, C_2^*, T_0^*, T_1^*, T_2^*, t_1^*, t_2^*, V_1^*, V_2^* \rangle$  在身份  $(ID_A^*, ID_B^*)$  条件下的解密询问。

猜测:  $A_{\text{II}}$  不能察觉出  $\sigma^*$  不是合法的密文, 除非向  $H_2$  发起关于  $U^* = g^{ab}$  的询问。在猜测过程中,  $A_{\text{II}}$  的观点如上模拟, 但是它的输出会被忽视。标准地来说, 为表现模拟环境不可区分于真实环境, 应该给出成功的  $A_{\text{II}}$  很大可能会以输入  $U^* = g^{ab}$  去询问  $H_2$  情况。

解决挑战:  $C$  从  $L_2$  中随机选择元组  $(r, C_1, U, R, ID_A, ID_B, h_2)$ , 有  $1/q_2$  的概率, 选中的元组中包含正确的  $U^* = g^{ab}$ 。

概率分析:

在以下情况中会导致  $C$  的模拟过程失败:

1)  $E_1: A_{\text{II}}$  未选择  $ID_{\pi}$  作为挑战接收者的身份;

2)  $E_2: A_{\text{II}}$  询问  $ID_{\pi}$  的秘密值;

3)  $E_3: A_{\text{II}}$  在签密询问中由于  $H_2$  的碰撞而停止;

4)  $E_4: A_{\text{II}}$  在游戏过程中拒绝一个合法的密文。

因为  $\Pr[\neg E_1] = 1/q_x$ , 从  $\neg E_1$  可以推导出  $\neg E_2$ , 可得出  $\Pr[E_3] \leq q_s(q_s + q_2)/q$ ,  $\Pr[E_4] \leq q_d/q$ 。结合起来, 得到总体成功的概率为  $\Pr[\neg E_1 \wedge \neg E_2 \wedge \neg E_3 \wedge \neg E_4] = \frac{1}{q_x} \left(1 - \frac{q_s + q_2}{q}\right) \left(1 - \frac{q_d}{q}\right)$ 。

### 3.2 不可伪造性证明

定理 3 类型 1 攻击下的不可伪造性。在随机模型中, 如果存在一个伪造者  $F_{\text{I}}$  能以概率  $\varepsilon$  在类型 1 的攻击下成功破坏以上方案的选择明文消息的存在不可伪造性 (Existential Unforgeable -Chosen Message Attack- I, EUF-CMA- I), 则存在一个模拟者  $C$  在多项式时间内, 以至少  $\varepsilon \frac{1}{q_1} \left(1 - \frac{q_s + q_3}{q}\right) \left(1 - \frac{q_d}{q}\right)$  的概率成功解决  $(l+1)$ -SDH 困难问题。其中,  $q_i (i = 1, 2, 3)$  是允许访问随机预言  $H_i (i = 1, 2, 3)$  的最大次数,  $q_s, q_x, q_d$  分别代表允许访问秘密值、签密与解密预言的最大次数。

证明 假设  $C$  接收到一个  $(l+1)$ -SDH 挑战  $(g, g^a, g^{a^2}, \dots, g^{a^l}, g^{a^{l+1}})$ ,  $C$  以  $F_{\text{I}}$  作为子程序输出  $(c, g^{1/(c+a)})$ 。 $C$  维持列表  $L_1, L_2, L_3, L_x, L_{ppk}, L_s$  和  $L_d$ , 分别记录  $H_1, H_2, H_3$ 、秘密值、签密和解密的询问, 初始时每个列表都为空。 $C$  为  $F_{\text{I}}$  设定的模拟环境如下:

$C$  先随机选择  $\pi \in \{1, 2, \dots, q_1\}$ ,  $I_{\pi} \in \mathbf{Z}_q^*$ ,  $\omega_1, \omega_2, \dots, \omega_{\pi-1}, \omega_{\pi+1}, \dots, \omega_l \in \mathbf{Z}_q^*$ 。对于  $i \in \{1, 2, \dots, l\} \setminus \{\pi\}$ ,  $C$  计算  $I_i = I_{\pi} - \omega_i$ 。建立一个  $l-1$  次的多项式  $f(z) = \prod_{i=1, i \neq \pi}^l (z + \omega_i)$ , 即  $f(z) = \sum_{i=0}^{l-1} c_i z^i, c_0, c_1, \dots, c_{l-1} \in \mathbf{Z}_q^*$ 。然后设生成元为  $\hat{g} = \sum_{i=0}^{l-1} c_i a^{i+1} = g^{f(a)}$ 。

对于  $i \in \{1, 2, \dots, l\} \setminus \{\pi\}$ ,  $C$  扩展  $f_i(z) = \frac{f(z)}{z + \omega_i} = \sum_{j=0}^{l-2} d_{i,j} z^j, d_{i,1}, d_{i,2}, \dots, d_{i,l-2} \in \mathbf{Z}_q^*$ , 设  $\tilde{H}_i^{-1} = g^{\sum_{j=0}^{l-2} d_{i,j} j^j} = g^{f_i(a)} = g^{f(a)/(a+\omega_i)} = g^{1/(a+\omega_i)}$ , 计算  $g_1 = \hat{g}^a, g_2 = \hat{g}^{a^2}$ , 其中  $\hat{g}^a = \sum_{i=0}^{l-1} c_i a^{i+1}, \hat{g}^{a^2} = g^{\sum_{i=0}^{l-1} c_i a^{i+2}}$ , 所以未知的主私钥隐含的设为  $msk = x = -a - I_{\pi} \in \mathbf{Z}_q^*$ 。对于  $i \in \{1, 2, \dots, l\} \setminus \{\pi\}$ ,  $(I_i, \tilde{H}_i^{-1}) = (\omega_i, g^{1/(a+\omega_i)})$ 。

预言询问: 同定理 1 的阶段 1。

伪造阶段:  $F_{\text{I}}$  输出在  $(ID_A^*, ID_B^*)$  条件下的挑战密文  $\sigma^* = \langle C_1^*, C_2^*, T_0^*, T_1^*, T_2^*, t_1^*, t_2^*, V_1^*, V_2^* \rangle$ , 若  $ID_A^* \neq ID_{\pi}$  停止, 否则  $C$  用  $ID_B^*$  的完全私钥解密得到  $m^*$ 。

解决挑战:  $C$  在  $L_3$  中检索  $(m^*, ID_A^*, ID_B^*, C_2^*)$  的哈希值, 有  $1/q_3$  的概率存在相应的  $W^*$  值, 然后计算  $(\omega_{\pi}, g^{1/(a+\omega_{\pi})}) = (\omega_{\pi}, (V_1^* V_2^*)^{1/(x_A+r)} (W^*)^{-1})$ 。

概率分析:  $C$  成功的概率为  $\varepsilon \frac{1}{q_1} \left(1 - q_s \frac{q_s + q_3}{q}\right) \left(1 - \frac{q_d}{q}\right)$ 。

定理 4 类型 2 攻击下的不可伪造性。在随机模型中, 如果存在一个伪造者  $F_{\text{II}}$  能以概率  $\varepsilon$  在类型 2 的攻击下成功破坏以上方案的选择明文消息的存在不可伪造性 (Existential Unforgeable-Chosen Message Attack- II, EUF-CMA- II), 则存在一个模拟者  $C$  在多项式时间内, 以至少  $\varepsilon \frac{1}{q_x} \left(1 - q_s \frac{q_s + q_3}{q}\right) \left(1 - \frac{q_d}{q}\right)$  的概率成功解决 CDH 困难问题。其中,  $q_i (i = 1, 2, 3)$  是允许访问随机预言  $H_i (i = 1, 2, 3)$  的最大次数,  $q_s, q_x, q_d$  分别代表允许访问秘密值、签密与解密预言的最大次数。

证明 假设  $C$  接收到的 CDH 挑战实例为  $(g, g^a, g^{ab})$ , 以  $F_{\text{II}}$  作为子程序输出  $g^{ab}$ 。 $C$  维持列表  $L_1, L_2, L_3, L_x, L_s$  和  $L_d$ , 分别记录  $H_1, H_2, H_3$ 、秘密值、签密和解密的询问, 开始时每个列表都为空。 $C$  为  $F_{\text{II}}$  设定的模拟环境如下:  $C$  先随机选择  $\pi \in \{1, 2, \dots, q_x\}$ :

预言询问同定理 2。

在伪造阶段, 令  $W^* = H_3(m^*, ID_A^*, ID_B^*, C_2^*) = g^b$ , 则

$$e(g, g)^{ab} = e(V_1^* V_2^*, g^{H_1(ID_{\pi}^*, PK_{\pi}^*)} g_1) e(C_1^*, (W^*)^{-1}), g^{ab} = (V_1^* V_2^*)^{H_1(ID_A^*, PK_A^*) + msk} (W^*)^{-r}.$$

所以其成功的概率为  $\varepsilon \frac{1}{q_x} \left(1 - q_s \frac{q_s + q_3}{q}\right) \left(1 - \frac{q_d}{q}\right)$ 。

## 4 有效性分析

与文献[15]中基于身份的在线/离线签密方案相比,所实现的环境有所不同,无证书密码学系统撤销了繁琐的证书管理过程,解决了基于身份密码学系统存在的密钥托管问题,所以本文方案在一定程度上具有更强的安全性。但是,在效率方面,离线阶段,本文方案都要比文献[15]的方案多一个G或G<sub>T</sub>群中的多点乘运算;在线阶段,G或G<sub>T</sub>群中多1个点乘和1个多点乘运算。同时,密文的长度也相对长一些,所以接下的工作重点就是减小系统的计算代价与通信代价,使系统更高效。

与文献[14]中无证书的在线/离线签密相比,本文方案着重强调离线阶段无需确定接收者的身份信息,做到了在线阶段才给出接收者的身份信息,提高了方案的灵活性与实用性。在离线阶段,文献[14]的方案还有双线性对的操作,而本文方案最复杂的运算就是群中的点乘与多点乘运算。再者,在文献[16]中已经给出了文献[14]的方案存在的安全性问题,攻击者可以直接通过窃听用户发送的密文提取出用户的私钥,这对用户甚至是整个通信系统都是毁灭性的打击。在此,本文方案在安全假设l-SDH、l-BDHI和CDH下是可证明安全的。

## 5 结语

本文结合无证书密码系统与在线/离线签密的优点,提出了全新的无证书的在线/离线签密方案,并在l-SDH、l-BDHI和CDH的安全假设下证明了方案在随机模型中的安全性。利用在线/离线的方法,在线阶段最复杂的运算只有点乘和多点乘运算。同时,为提高方案的灵活性与实用性,在离线阶段无需确定接收者的身份。然而,本文方案的效率方面以及密文的长度有待于作出进一步改进。

### 参考文献:

- [1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption) ≪ (cost (signature) + (encryption)) [C]// CRYPTO'97: Proceedings of the 17th Annual International Cryptology Conference, LNCS 1294. Berlin: Springer-Verlag, 1997: 165 – 179.
- [2] MALONE-LEE J. Identity-based signcryption [EB/OL]. [2014 – 03 – 06]. <http://www.signcryption.org/publications/pdffiles/MaloneLee-eprint2002-098.pdf>.
- [3] BARRETO P S L M, LIBERT B, McCULLAGH N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps [C]// ASIACRYPT 2005: Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 3788. Berlin: Springer-Verlag, 2005: 515 – 532.
- [4] BOYEN X. Multipurpose identity-based signcryption [C]// CRYPTO 2003: Proceedings of the 23rd Annual International Cryptology Conference, LNCS 2729. Berlin: Springer-Verlag, 2003: 383 – 399.
- [5] CHEN L, MALONE-LEE J. Improved identity-based signcryption [C]// PKC 2005: Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography, LNCS 3386. Berlin: Springer-Verlag, 2005: 362 – 379.
- [6] LIBERT B, QUISQUATER J-J. New identity based signcryption schemes from pairings [M]// IACR Cryptology ePrint Archive. [S. l.]: International Association for Cryptologic Research, 2003: 23.
- [7] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption [C]// EUROCRYPT 2002: Proceedings of the 2002 International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 2332. Berlin: Springer-Verlag, 2002: 83 – 107.
- [8] ZHANG F, MU Y, SUSILO W. Reducing security overhead for mobile networks [C]// AINA 2005: Proceedings of the 2005 Advanced Information Networking and Applications. Washington, DC: IEEE Computer Society, 2005, 1: 398 – 403.
- [9] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// ASIACRYPT 2003: Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 2894. Berlin: Springer-Verlag, 2003: 452 – 473.
- [10] BARBOSA M, FARSHIM P. Certificateless signcryption [C]// ASIACCS'08: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2008: 369 – 372.
- [11] SELVI S S D, VIVEK S S, RANGAN C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing [C]// ICISC 2010: Proceedings of the 5th International Conference on Information Security and Cryptology, LNCS 6151. Berlin: Springer-Verlag, 2010: 75 – 92.
- [12] ARANHA D, CASTRO R, LOPEZ J, et al. Efficient certificateless signcryption [J]. Journal of 8o. Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2008: 257 – 258.
- [13] WU C-H, CHEN Z. A new efficient certificateless signcryption scheme [C]// ISISE'08: Proceedings of the 2008 International Symposium on Information Science and Engineering. Piscataway: IEEE, 2008: 661 – 664.
- [14] LUO M, WEN Y, ZHAO H. Efficient certificateless on-line/off-line signcryption scheme [J]. Computer Science, 2010, 37(5): 103 – 106. (罗铭,闻英友,赵宏.高效无证书的在线/离线签密方案[J].计算机科学,2010,37(5):103 – 106.)
- [15] LIU J K, BAEK J, ZHOU J. Online/offline identity-based signcryption revisited [C]// ICISC 2011: Proceedings of the 14th International Conference on Information Security and Cryptology, LNCS 6584. Berlin: Springer-Verlag, 2011: 36 – 51.
- [16] SHI W, KUMAR N, CONG P, et al. On the security of a certificateless online/offline signcryption for Internet of things [J/OL]. Journal of Peer-to-Peer Networking and Applications, [2014 – 01 – 14]. <http://link.springer.com/article/10.1007%2Fs12083-014-0249-3>.
- [17] BONEH D, BOYEN X. Short signatures without random oracles [C]// EUROCRYPT 2004: Proceedings of the 2004 International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3027. Berlin: Springer-Verlag, 2004: 56 – 73.
- [18] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles [C]// EUROCRYPT 2004: Proceedings of the 2004 International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3027. Berlin: Springer-Verlag, 2004: 223 – 238.