无证书密文等值测试签密方案

张玉磊[①] 白巧玲*[①] 马彦丽[②] 闫晨阳[①] 王彩芬[③]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](国网思极飞天(兰州)云数科技有限公司 兰州 730000)

[③](深圳技术大学 深圳 518118)

摘 要：在云计算应用中，确保消息的机密性和不可伪造性，同时判断不同密文对应明文的等价性显得至关重要。具有密文等值测试功能的签密方案可以实现此类安全目标。该文基于无证书公钥密码环境，设计了一个具有密文等值测试功能的无证书签密方案(CLSCET)。首先，提出了无证书密文等值测试签密方案的框架和安全模型，定义了两类具有不同攻击能力的敌手和3类安全目标。然后构造了具体的无证书密文等值测试签密方案，并分析了方案的正确性。最后，基于随机预言模型，证明该文方案满足选择密文攻击下的单向性(OW-CCA)、选择密文攻击下的不可区分性(IND-CCA2)和选择消息攻击下的不可伪造性(EUF-CMA)安全。与现有近似方案相比，该文方案满足IND-CCA2的机密性、EUF-CMA的不可伪造性和OW-CCA的密文单向性。

关键词：密文等值测试；无证书公钥密码；签密；计算Diffie-Hellman问题

中图分类号：TN918.4; TP309 **文献标识码**：A **文章编号**：1009-5896(2021)09-2534-08

DOI: 10.11999/JEIT200805

Certificateless Signcryption with Equality Test

ZHANG Yulei[①] BAI Qiaoling[①] MA Yanli[②] YAN Chenyang[①] WANG Caifen[③]

[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[②](*SGIT-UNI Cloud Data Technology CO.*, *LTD*, *Lanzhou* 730000, *China*)

[③](*Shenzhen University of Technology*, *Shenzhen* 518118, *China*)

Abstract: In cloud computing applications, it is very important to ensure the confidentiality and unforgeability of messages, while judging the equivalence of different ciphertexts to plaintexts. The signcryption scheme with equality test can achieve the above security goals. Based on the certificateless public key cryptography environment, a Certificateless SignCryption scheme with Equality Test (CLSCET) is designed. Firstly, the framework and security model of the certificateless signcryption with equality test scheme are proposed, moreover two types of adversaries with different attack capabilities and three types of security targets are defined. Secondly, a specific certificateless signcryption with equality test scheme is constructed, and the correctness of the scheme is analyzed. Finally, based on the random oracle model, it is proved that the scheme satisfies the security properties of One-Way against Chosen Ciphertext Attack(OW-CCA), INDistinguishability against adaptive Chosen Ciphertext Attack(IND-CCA2) and Existential UnForgeability against adaptive Chosen Message Attack(EUF-CMA). Compared with the existing approximate schemes, the scheme satisfies the confidentiality of IND-CCA2, the unforgeability of EUF-CMA and the one-way ciphertext of OW-CCA.

Key words: Ciphertext equivalence test; Certificateless public key cryptography; Signcryption; Computational Diffie-Hellman(CDH) problem

1 引言

在云计算许多应用中，需要同时保证消息的不可伪造性和机密性。签名技术通常保证消息的不可伪造性，而加密技术保证消息的机密性。1997年，Zheng[1]首次提出签密的概念。签密可以在同一逻辑步骤内对消息进行签名和加密，其计算开销要远远小于签名和加密的计算开销总和。基于多种密码

收稿日期：2020-09-14；改回日期：2021-03-15；网络出版：2021-03-26

*通信作者： 白巧玲 2512106492@qq.com

基金项目：国家自然科学基金(61662069)，甘肃省高等学校科研项目(2017A-003, 2018A-207)

Foundation Items: The National Natural Science Foundation of China (61662069), The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2018A-207)

体制、设计满足不同需求的签密方案是当前密码学研究的热点之一。

1984年，Shamir[2]提出了基于身份的公钥密码体制，解决了传统公钥密码存在的证书管理问题，但是身份公钥密钥存在密钥托管问题。2003年，Al-Riyami等人[3]提出了无证书公钥密码体制，解决了身份密码体制存在的密钥托管问题。2008年，Barbosa等人[4]结合无证书公钥密码和签密的优势，提出了无证书签密原语。同年，Wu等人[5]基于计算Diffie-Hellman困难问题和离散对数困难问题提出了一个无证书签密方案。但是，Barbosa方案和Wu方案的计算效率较低。2011年，王星等人[6]提出了高效的无证书签密方案，该方案的签密算法使用1个双线性对，解签密算法使用了3个双线性对，与已有方案相比，该方案的效率更优。但是，以上方案均基于双线性对构造无证书签密方案，方案的整体效率仍然较低。2017年，周彦伟等人[7]提出了安全的无双线性对的无证书签密方案，该方案具有更高的效率，同时具有公开验证性。2018年，Mandal等人[8]提出了可验证的无证书签密方案，该方案可以有效地抵抗Internet安全协议和应用程序的自动验证攻击。同年Luo等人[9]提出了一个改进的基于标准模型的无证书签密方案，该方案具有更短的密文、更强的安全性和更高的效率。

云计算等应用中不仅需要通过签密保证消息的机密性和不可伪造性，有时还需要检测不同密文对应的明文是否相同。例如，在云加密数据库中，如何在不暴露明文消息的同时，对不同公钥加密的密文数据进行归类是一种非常重要的功能，而密文等值测试技术可以有效地解决该问题。

2010年，Yang等人[10]首次提出了公钥加密等值测试(Public Key Encryption with Equality Test, PKEET)技术，该技术可以判断不同公钥加密的密文是否对应于同一个明文。2016年，Ma[11]提出了基于身份公钥密码的等值测试(Identity-Based Encryption with Equality Test, IBEET)方案，解决了PKEET存在的证书管理问题。2018年，为了解决IBEET密钥托管问题，Qu等人[12]提出了无证书密文等值测试加密(CertificateLess Public Key Encryption with Equality Test, CLPKEET)方案。2020年，张玉磊等人[13]提出了支持关键字搜索的无证书密文等值测试加密方案，该方案可以提供关键字密文搜索功能，但是，不能提供认证功能。

本文基于无证书公钥密码环境，提出了一个具有密文等值测试功能的无证书签密方案，即无证书密文等值测试签密(CertificateLess SignCryption with Equality Test, CLSCET)方案。首先，提出了无证书密文等值测试签密的系统框架和安全模型，定义了两类具有不同攻击能力的敌手和3类安全目标。然后提出了具体的无证书密文等值测试签密方案。最后，在随机预言模型下，证明本方案满足适应性选择密文攻击下的不可区分性(INDistinguishability against adaptive Chosen Ciphertext Attack, IND-CCA2)、适应性选择消息攻击下的不可伪造性(Existential UnForgeability against adaptive Chosen Message Attack, EUF-CMA)和密文单向性(One-Way against Chosen Ciphertext Attack, OW-CCA)。

2　无证书密文等值测试签密系统框架和安全模型

2.1　方案系统框架

无证书密文等值测试签密方案包括密钥生成中心(Key Generation Center, KGC)、数据发送者、数据接收者和云服务器4个实体。系统模型如图1所示。

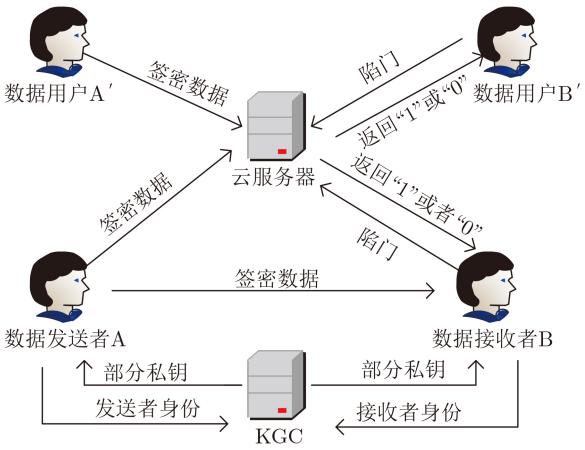

图 1 系统模型图

(1)密钥生成中心(KGC)：生成系统参数、系统主密钥和数据发送者/数据接收者的部分私钥。

(2)数据发送者：数据发送者签密数据并将其发送云服务器和数据接收者。

(3)数据接收者：收到密文数据并对其进行解签密。

(4)云服务器：存储数据发送者上传的密文，云服务器执行密文测试操作。

2.2　安全模型

无证书密文等值测试签密方案中存在A_I和A_{II}两种不同类型的攻击者。A_I敌手可以替换用户的公钥，但不可以访问主密钥，A_{II}敌手可以访问

主密钥，但不可以替换用户的公钥。以下通过挑战者C和攻击者$A \in \{A_I, A_{II}\}$之间的安全游戏来描述机密性、不可伪造性和密文单向性等安全属性。

2.2.1 机密性

游戏1 输入安全参数λ，挑战者C运行系统建立算法和密钥生成算法。当$A = A_I$时, C将系统参数PP发送给A，否则C将系统参数PP和主密钥s发送给A。

询问阶段：当$A = A_I$时，A进行Hash询问、部分私钥询问、公钥询问、私钥询问、替换公钥询问、签密询问、解签密询问和陷门询问，C返回相应值给A，否则A进行Hash询问、公钥询问、私钥询问、签密询问、解签密询问和陷门询问。

挑战阶段：A输出两个等长的消息m_0和m_1, $m_0 \neq m_1$且未被A访问过。目标接收者为j^*，且$j^* \neq t$, C随机选择$b \in \{0,1\}$，返回$\delta^* \leftarrow \text{Signcryption}(\text{SK}_t, \text{PK}_{j^*}, m_b)$作为挑战密文发给A。

猜测阶段：A输出$b' \in \{0,1\}$，当$b' = b$时, A赢得游戏。

2.2.2 不可伪造性

游戏2 输入安全参数λ，挑战者C运行系统建立算法和密钥生成算法。当$A = A_I$时, C将系统参数PP发送给A，否则C将系统参数PP和主密钥s发送给A。

询问阶段：当$A = A_I$时，A进行Hash询问、公钥询问、私钥询问、替换公钥询问、签密询问和解签密询问，C返回相应值给A，否则A进行Hash询问、公钥询问、私钥询问、签密询问和解签密询问。

伪造阶段：A输出发送者身份$i^* (\neq t)$和密文δ^*。如果$\perp \neq \text{Unsigncryption}(\text{PK}_{i^*}, \text{SK}_t, \delta^*)$, A赢得游戏。

2.2.3 单向性

游戏3 输入安全参数λ，挑战者C运行系统建立算法和密钥生成算法。当$A = A_I$时, C将系统参数PP发送给A，否则C将系统参数PP和主密钥s发送给A。

询问阶段：与游戏1中询问阶段相同。

挑战阶段：A输出发送者身份为i^*，且$i^* \neq t$。C随机选取m^*，返回$\delta^* \leftarrow \text{Signcryption}(\text{SK}_{i^*}, \text{PK}_t, m^*)$作为挑战密文发送给A。

猜测阶段：A输出m'，如果$m' = m^*$, A赢得比赛。

3 具体方案

3.1 算法描述

CLSCET方案包括以下算法：

(1)Setup (λ)：输入安全参数λ。

(a) KGC选择两个相同素数阶$(q > 2^k)$的循环群G_1, G_2(P是G_1生成元)和双线性对$e: G_1 \times G_1 \to G_2$。随机选取$s \in Z_q^*$为主密钥，选择抗碰撞Hash函数：$H_1: \{0,1\}^* \times G_1 \to G_1$, $H_2: \{0,1\}^* \times G_1 \times G_2 \times G_1 \to \{0,1\}^*$, $H_3: G_1 \times \{0,1\}^* \to Z_q^*$, $H_4: G_1 \times \{0,1\}^* \to Z_q^*$, $H_5: \{0,1\}^* \to Z_q^*$和$H_6: G_2 \to Z_q^*$。

(b) 设定主公钥$P_{\text{pub}} = sP$，输出系统参数$\text{PP} = (G_1, G_2, q, P, P_{\text{pub}}, e, H_1, H_2, H_3, H_4, H_5, H_6)$。

(2)Public key (PP, x_i)：输入系统参数PP，数据用户的秘密值x_i。

(a) 数据发送者选择随机数$x_A \in Z_q^*$作为自己的秘密值并设置其公钥$\text{PK}_A = x_A P$。

(b) 数据接收者选择随机数$x_B \in Z_q^*$作为自己的秘密值并设置其公钥$\text{PK}_B = x_B P$。

(3) Partial private key $(\text{PP}, s, \text{ID}_i)$：输入系统参数PP，主密钥$s$和数据用户的身份$\text{ID}_i$。

(a) 输入数据发送者身份ID_A, KGC计算$Q_A = H_1(\text{ID}_A, \text{PK}_A)$, $D_A = sQ_A$，然后将部分私钥D_A返回给数据发送者。

(b) 输入数据接收者身份ID_B, KGC计算$Q_B = H_1(\text{ID}_B, \text{PK}_B)$, $D_B = sQ_B$，然后将部分私钥D_B返回给数据接收者。

(4) Private key (PP, x_i, D_i)：输入系统参数PP，数据用户的秘密值x_i和部分私钥D_i。

(a) 设置数据发送者的私钥$\text{SK}_A = (x_A, D_A)$。

(b) 设置数据接收者的私钥$\text{SK}_B = (x_B, D_B)$。

(5) Signcryption$(\text{PP}, M, \text{ID}_A, \text{ID}_B, \text{SK}_A, \text{PK}_B)$：输入系统参数PP，消息$M$，数据发送者的私钥$\text{SK}_A$，数据接收者的公钥$\text{PK}_B$。数据发送者执行以下操作：

(a) 随机选择$r \in Z_q^*$，计算$R = rP$, $\alpha = e(rP_{\text{pub}}, Q_B)$, $T = r\text{PK}_B$。

(b) 计算$h = H_2(\text{ID}_A, \text{ID}_B, R, \alpha, T)$, $C_1 = M \oplus h$。

(c) 计算$w = H_3(R, C_1, \text{ID}_A, \text{ID}_B)$, $u = H_4(R, C_1, \text{ID}_A, \text{ID}_B)$, $V = (wx_A + r)Q_A + uD_A$，其中$C_2 = H_5(M) \cdot H_6[e(\text{PK}_B + P_{\text{pub}}, rQ_B)]$，将密文$\delta = (R, C_1, C_2, V)$发送给数据接收者。

(6) Unsigncryption $(\text{ID}_A, \text{ID}_B, \text{PK}_A, \text{SK}_B, \delta)$：输入数据发送者的公钥$\text{PK}_A$，数据接收者的私钥$\text{SK}_B$，密文$\delta$。数据接收者执行以下操作：

(a) 计算$\alpha = e(R, D_B)$, $T = x_B R$, $h = H_2(\text{ID}_A, \text{ID}_B, R, \alpha, T)$, $M = C_1 \oplus h$。

(b) 计算$w = H_3(R, C_1, \text{ID}_A, \text{ID}_B)$, $u = H_4(R, C_1, \text{ID}_A, \text{ID}_B)$。判断$e(V, P) = e(R + w\text{PK}_A +$

$uP_{\text{pub}}, Q_{\text{A}})$是否相等，若相等返回消息$M$，否则返回符号“$\perp$”。

(7) Trapdoor (SK_{B})：数据接收者随机选择$r' \in Z_q^*$，计算$T_{d_1} = e[R + r'P, x_{\text{B}}H_1(\text{ID}_{\text{B}}, \text{PK}_{\text{B}}) + D_{\text{B}}]$, $T_{d_2} = e[r'P, x_{\text{B}}H_1(\text{ID}_{\text{B}}, \text{PK}_{\text{B}}) + D_{\text{B}}]$，将陷门$T_d = (T_{d_1}, T_{d_2})$发送给云服务器。

(8) Test $(C_{\text{A}}, T_{d_{\text{A}}}, C_{\text{B}}, T_{d_{\text{B}}})$：云服务器收到密文陷门对$(\delta_{\text{A}}, T_{d_{\text{A}}})$和$(\delta_{\text{B}}, T_{d_{\text{B}}})$，计算$E_{\text{A}} = H_6\left(\frac{T_{d_{1,\text{A}}}}{T_{d_{2,\text{A}}}}\right)$, $E_{\text{B}} = H_6\left(\frac{T_{d_{1,\text{B}}}}{T_{d_{2,\text{B}}}}\right)$，判断$\frac{C_{2,\text{A}}}{E_{\text{A}}} = \frac{C_{2,\text{B}}}{E_{\text{B}}}$是否相等，若相等输出“1”，否则输出“0”。

3.2 正确性

当且仅当以下3类等式分别成立，CLSCET方案满足正确性。

(1)加解密的一致性

$$M = C_1 \oplus h = M \oplus h \oplus h = M \tag{1}$$

(2)Unsigncryption算法中验证等式成立

$$\begin{aligned} e(V, P) =& e[(wx_{\text{A}} + r)Q_{\text{A}} + uD_{\text{A}}, P] \\ =& e[(wx_{\text{A}} + r)Q_{\text{A}}, P]\, e(uD_{\text{A}}, P) \\ =& e[(wx_{\text{A}} + r)P, Q_{\text{A}}]\, e(usQ_{\text{A}}, P) \\ =& e[w\text{PK}_{\text{A}} + R, Q_{\text{A}}]\, e(uP_{\text{pub}}, Q_{\text{A}}) \\ =& e(R + w\text{PK}_{\text{A}} + uP_{\text{pub}}, Q_{\text{A}}) \end{aligned} \tag{2}$$

(3)Test算法中验证等式成立

$$\begin{aligned} E_{\text{A}} =& H_6\left(\frac{T_{d_{1,\text{A}}}}{T_{d_{2,\text{A}}}}\right) = H_6[e(R, x_{\text{B}}Q_{\text{B}} + D_{\text{B}})] \\ =& H_6[e(\text{PK}_{\text{B}} + P_{\text{pub}}, rQ_{\text{B}})] \end{aligned} \tag{3}$$

$$\begin{aligned} E_{\text{B}} =& H_6\left(\frac{T_{d_{1,\text{B}}}}{T_{d_{2,\text{B}}}}\right) = H_6[e(R, x_{\text{B}}Q_{\text{B}} + D_{\text{B}})] \\ =& H_6[e(\text{PK}_{\text{B}} + P_{\text{pub}}, rQ_{\text{B}})] \end{aligned} \tag{4}$$

$$\begin{aligned} \frac{C_{2,\text{A}}}{E_{\text{A}}} =& \frac{H_5(M_{\text{A}}).H_6[e(\text{PK}_{\text{B}} + P_{\text{pub}}, rQ_{\text{B}})]}{H_6[e(\text{PK}_{\text{B}} + P_{\text{pub}}, rQ_{\text{B}})]} \\ =& H_5(M_{\text{A}}), \\ \frac{C_{2,\text{B}}}{E_{\text{B}}} =& \frac{H_5(M_{\text{B}}).H_6[e(\text{PK}_{\text{B}} + P_{\text{pub}}, rQ_{\text{B}})]}{H_6[e(\text{PK}_{\text{B}} + P_{\text{pub}}, rQ_{\text{B}})]} \\ =& H_5(M_{\text{B}}) \end{aligned}$$

若$\frac{C_{2,\text{A}}}{E_{\text{A}}} = \frac{C_{2,\text{B}}}{E_{\text{B}}}$，必有$M_{\text{A}} = M_{\text{B}}$。

4 安全性分析

4.1 机密性

定理1 在随机预言模型中，若存在敌手A_{I}以概率ε攻破游戏1，则该方案满足IND-CCA2。

构造一个算法C解决双线性Diffie-Hellman(Bilinear Diffie-Hellman, BDH)困难问题，其中解决问题的概率为$\frac{1}{q_{H_6}}\left(\frac{\varepsilon}{\text{e}(q_{\text{par}} + q_{\text{prv}} + q_T + 1)} - \frac{q_{\text{dsc}}}{q}\right)$。$q_{H_6}$, q_{par}, q_{prv}, q_T和q_{dsc}分别表示H_6询问，部分私钥询问，私钥询问，陷门询问和解签密询问的最大次数，e为自然对数的底。

证明：假设算法C是一个BDH问题的解决者，输入4元组(P, aP, bP, cP)，计算目标为$e(P, P)^{abc}$。C产生系统参数$\text{PP} = (P, H_1, H_2, H_3, H_4, H_5, H_6)$，令$P_{\text{pub}} = aP$, $H_1 - H_6$为随机预言机，PP发送给敌手A_{I}，保留主密钥s，列表L_{H_1}, L_{H_2}, L_{H_3}, L_{H_4}, L_{H_5}, L_{H_6}和公钥询问列表L_{Key}初始为空。

(1)H_1询问：C维护列表L_{H_1}，其中包含元组$[\text{ID}_i, \text{PK}_i, v_i, \text{cn}, Q_i]$。当C收到敌手$\text{A}_{\text{I}}$关于$H_1$的询问时，若$[\text{ID}_i, \text{PK}_i, v_i, \text{cn}, Q_i] \in L_{H_1}$，则返回$Q_i$；否则C随机选择$\text{cn} \in \{0, 1\}$，若$\text{cn} = 0$，返回$v_iP$，否则返回$bv_iP$。

(2)H_2询问：C维护列表L_{H_2}，其中包含元组$[\text{ID}_i, R_i, \alpha_i, T_i, h_i]$。当C收到敌手$\text{A}_{\text{I}}$关于$H_2$的询问时，若$[\text{ID}_i, R_i, \alpha_i, T_i, h_i] \in L_{H_2}$，则返回$h_i$，否则C随机选择$h_i \in \{0, 1\}^*$，添加$[\text{ID}_i, R_i, \alpha_i, T_i, h_i]$到$L_{H_2}$中，返回$h_i$。

(3)H_3询问：C维护列表L_{H_3}，其中包含元组$[R_i, C_i, \text{ID}_i, \text{PK}_i, w_i]$。当C收到敌手$\text{A}_{\text{I}}$关于$H_3$的询问时，若$[R_i, C_i, \text{ID}_i, \text{PK}_i, w_i] \in L_{H_3}$，则返回$w_i$，否则C随机选择$w_i \in Z_q^*$，添加$[R_i, C_i, \text{ID}_i, \text{PK}_i, w_i]$到$L_{H_3}$中，返回$w_i$。

(4)H_4询问：C维护列表L_{H_4}，其中包含元组$[R_i, C_i, \text{ID}_i, u_i]$。当C收到敌手$\text{A}_{\text{I}}$关于$H_4$的询问时，若$[R_i, C_i, \text{ID}_i, u_i] \in L_{H_4}$，则返回$u_i$，否则C随机选择$u_i \in Z_q^*$，添加$[R_i, C_i, \text{ID}_i, u_i]$到$L_{H_4}$中，返回$u_i$。

(5)H_5询问：C维护列表L_{H_5}，其中包含元组$[M, h_5]$。当C收到敌手A_{I}关于H_5的询问时，若$[M, h_5] \in L_{H_5}$，则返回h_5，否则C随机选择$h_5 \in Z_q^*$，添加$[M, h_5]$到L_{H_5}中，返回h_5。

(6)H_6询问：C维护列表L_{H_6}，其中包含元组$[\beta \cdot \eta, h_6]$。当C收到敌手A_{I}关于H_6的询问时，若$[\beta \cdot \eta, h_6] \in L_{H_6}$，则返回$h_6$，否则C随机选择$h_6 \in Z_q^*$，添加$[\beta \cdot \eta, h_6]$到$L_{H_6}$中，返回$h_6$。

(7)公钥询问：当C收到关于ID_i的公钥询问时，操作如下：

(a) 若列表L_{Key}中存在元组$[\text{ID}_i, \text{PK}_i]$，则返回$\text{PK}_i$给敌手$\text{A}_{\text{I}}$。

(b) 否则，C随机选择$\text{cn} \in \{0, 1\}$，令$\Pr[\text{cn} = 0] = \tau$。若$\text{cn} = 0$, C随机选取$x_i \in Z_q^*$，计算$D_i = av_iP$, $\text{SK}_i = (x_i, D_i)$和$\text{PK}_i = x_iP$，添加$[\text{ID}_i, x_i, D_i, \text{SK}_i, \text{PK}_i, 0]$到$L_{\text{Key}}$中，返回$\text{PK}_i$给敌手$\text{A}_{\text{I}}$。若$\text{cn} = 1$，令$\text{PK}_i = x_{\text{know}}P$，其中$x_{\text{know}} \in Z_q^*$，满足$[*, *, *, *, \text{PK}_i] \notin L_{\text{Key}}$；否则，C重新选择$x_{\text{know}}$，添加$[\text{ID}_i, \text{PK}_i, \text{cn}]$到列表$L_{H_1}$和$L_{H_3}$中，返回$\text{PK}_i$给敌手$\text{A}_{\text{I}}$。

(8)部分私钥询问：当C收到关于ID_i的部分私钥询问时，若部分私钥列表中存在元组$[\mathrm{ID}_i, D_i]$，则返回D_i给敌手$\mathrm{A_I}$。否则，C对ID_i进行公钥询问，若$\mathrm{cn}=0$，则返回D_i，否则，C终止模拟。

(9)私钥询问：当C收到关于ID_i的私钥询问时，若私钥列表中存在元组$[\mathrm{ID}_i, \mathrm{SK}_i]$，则返回$\mathrm{SK}_i$给敌手$\mathrm{A_I}$。否则，C对$\mathrm{ID}_i$进行公钥询问，若$\mathrm{cn}=0$，则返回$\mathrm{SK}_i$，否则，C终止模拟。

(10)公钥替换询问：敌手$\mathrm{A_I}$可选择任意一个新公钥PK_i'替换合法用户ID_i的原始公钥PK_i。

(11)签密询问：当C收到敌手$\mathrm{A_I}$关于元组$[\mathrm{ID_S}, \mathrm{ID_R}, m]$(假设$\mathrm{A_I}$已经进行公钥询问)的签密询问时，若$\mathrm{cn}=1$，C查询列表$L_{\mathrm{Key}}$, L_{H_1}, L_{H_2}, L_{H_3}, L_{H_4}, L_{H_5}和L_{H_6}中元组。计算得出$R=rP$, $C_1=m\oplus h_i$, $C_2=h_5\cdot h_6$和$V=(w_i\cdot x_{\mathrm{know}}+r)\,bv_iP+au_ibv_iP$并返回密文$\delta=(R,C_1,C_2,V)$给敌手$\mathrm{A_I}$。否则，C查询列表$L_{\mathrm{Key}}$中元组$[\mathrm{ID}_i, x_i, D_i, \mathrm{SK}_i, \mathrm{PK}_i, \mathrm{cn}]$，运行$\mathrm{Signcryption}(\mathrm{PP}, m, \mathrm{ID_S}, \mathrm{ID_R}, \mathrm{SK_S}, \mathrm{PK_R})$，生成相应的密文$\delta=(R,C_1,C_2,V)$并将其返回给敌手$\mathrm{A_I}$。

(12)解签密询问：当C收到敌手$\mathrm{A_I}$关于元组$[\mathrm{ID_S}, \mathrm{ID_R}, \delta]$的解签密询问时，操作如下：

(a) 若存在且$\mathrm{cn}=0$，C在L_{Key}中查询$[\mathrm{ID}_i, x_i, D_i, \mathrm{SK}_i, \mathrm{PK}_i, \mathrm{cn}]$，运行$\mathrm{Unsigncryption}(\mathrm{PK_S}, \mathrm{SK_R}, \delta)$算法并返回$m$，若输出密文无效，则C输出符号“$\perp$”。

(b) 若存在且$\mathrm{cn}=1$，C在列表L_{H_1}, L_{H_2}, L_{H_3}和L_{H_4}中查询元组$[\mathrm{ID}_i, \mathrm{PK}_i, Q_i]$, $[\mathrm{ID}_i, R_i, \alpha_i, T_i, h_i]$, $[R_i, C_i, \mathrm{ID}_i, \mathrm{PK}_i, w_i]$和$[R_i, C_i, \mathrm{ID}_i, u_i]$，计算$m=C_1\oplus h$。若等式$e(V,P)=e(R+w\mathrm{PK_A}+uP_{\mathrm{pub}}, Q_{\mathrm{A}})$成立，则返回$m$，否则C输出符号“$\perp$”。

(c) 若列表L_{Key}中不存在元组(即公钥被替换)，则C在列表L_{H_1}, L_{H_2}, L_{H_3}和L_{H_4}中查询元组$[\mathrm{ID}_i, \mathrm{PK}_i', Q_i]$，$[\mathrm{ID}_i, R_i, \alpha_i, T_i, h_i]$，$[R_i, C_i, \mathrm{ID}_i, \mathrm{PK}_i', w_i]$和$[R_i, C_i, \mathrm{ID}_i, u_i]$，计算$m=C_1\oplus h$。若等式$e(V,P)=e\left(R+w\mathrm{PK}_{\mathrm{A}}'+uP_{\mathrm{pub}}, Q_{\mathrm{A}}\right)$成立，则返回$m$，否则C输出符号“$\perp$”。

(13)陷门询问：当C收到敌手$\mathrm{A_I}$关于陷门询问时，若$\mathrm{cn}=0$，C在列表L_{Key}中查询$[\mathrm{ID}_i, x_i, D_i, \mathrm{SK}_i, \mathrm{PK}_i, 0]$并返回$\mathrm{Trapdoor}(\mathrm{SK}_i)$的结果给敌手$\mathrm{A_I}$，否则，C终止模拟。

挑战阶段：敌手$\mathrm{A_I}$输出两个身份$\mathrm{ID_S}, \mathrm{ID_R}\in\mathrm{ID}$和两个等长消息$m_0^*$和$m_1^*$。C随机选择$b\in\{0,1\}$，若$\mathrm{cn}=0$，C终止模拟。否则，令$R^*=cP$，计算${C_1}^*=m_b^*\oplus h_i$，$C_2^*=H_5(m_b^*)\cdot H_6[e(x_{\mathrm{know}}P+aP, cbv_i^*P)]$, $V^*=(w_i\cdot x_{\mathrm{know}}+c)\,bv_iP+au_ibv_iP$，发送$\delta^*=(R^*, C_1^*, C_2^*, V^*)$作为挑战密文给敌手$\mathrm{A_I}$。

猜测阶段：敌手$\mathrm{A_I}$输出$b'\in\{0,1\}$。若$b'=b$，则C输出${\eta^*}^{{v_i^*}^{-1}}=e(P,P)^{abc}$作为BDH困难问题的有效解。

分析：如果C在上述游戏中没有停止，则C可以优势ε'解决BDH困难问题。令事件E_1为算法C模拟终止，$\Pr[\neg E_1]=\dfrac{1}{\mathrm{e}(q_{\mathrm{par}}+q_{\mathrm{prv}}+q_T+1)}$；事件$E_2$为解签密失败，$\Pr[E_2]\le-\dfrac{q_{\mathrm{dsc}}}{q}$；事件$E_3$为模拟过程中$\mathrm{A_I}$对$H_6[\mathrm{e}(x_{\mathrm{know}}^*P+aP, cbv_i^*P)]$的询问，$\Pr[E_3]\ge\dfrac{\varepsilon}{\mathrm{e}(q_{\mathrm{par}}+q_{\mathrm{prv}}+q_T+1)}-\dfrac{q_{\mathrm{dsc}}}{q}$。

根据文献[12]可得：$\varepsilon'\ge\dfrac{1}{q_{H_6}}\Pr[E_3]\ge\dfrac{1}{q_{H_6}}\left(\dfrac{\varepsilon}{\mathrm{e}(q_{\mathrm{par}}+q_{\mathrm{prv}}+q_T+1)}-\dfrac{q_{\mathrm{dsc}}}{q}\right)$。证毕

定理2 在随机预言模型中，若存在敌手$\mathrm{A_{II}}$以概率ε攻破游戏1，则该方案满足IND-CCA2。

构造一个算法C解决BDH困难问题，其中解决问题的概率为$\dfrac{1}{q_{H_6}}\left(\dfrac{\varepsilon}{\mathrm{e}(q_{\mathrm{prv}}+q_T+1)}-\dfrac{q_{\mathrm{dsc}}}{q}\right)$。$q_{H_6}$, q_{prv}, q_T和q_{dsc}分别表示H_6询问，私钥询问，陷门询问和解签密询问的最大次数，e为自然对数。

证明：算法构造与定理1相同，系统建立与定理1相似，除了$P_{\mathrm{pub}}=sP$，PP和主密钥s都发送敌手$\mathrm{A_{II}}$。

询问阶段：Hash询问、部分私钥询问、私钥询问、签密询问和陷门询问与定理1相同。

公钥询问：与定理1中相似，除了$\mathrm{cn}=0$时，$D_i=sv_iP$; $\mathrm{cn}=1$时，$\mathrm{PK}_i=aP$。

解签密询问：与定理1中相似，除了公钥被替换的情况。

挑战阶段：与定理1中挑战阶段相同。

猜测阶段：敌手$\mathrm{A_{II}}$输出$b'\in\{0,1\}$。若$b'=b$，则C输出${\beta^*}^{(v_i^*)^{-1}}=e(P,P)^{abc}$作为BDH困难问题的有效解。

分析：与定理1中相似，根据文献[12]可得：$\varepsilon'\ge\dfrac{1}{q_{H_6}}\Pr[E_3]\ge\dfrac{1}{q_{H_6}}\left(\dfrac{\varepsilon}{\mathrm{e}(q_{\mathrm{prv}}+q_T+1)}-\dfrac{q_{\mathrm{dsc}}}{q}\right)$。证毕

4.2 不可伪造性

定理3 随机预言模型中，若存在敌手$\mathrm{A_I}$以概率ε攻破游戏2，则该方案满足EUF-CMA。

构造一个算法C解决计算Diffie-Hellman(Computational Diffie-Hellman, CDH)困难问题，其中解决问题的概率为$\left(1-\dfrac{q_{\mathrm{prv}}}{2^\lambda}\right)\dfrac{1}{\mathrm{e}(q_{\mathrm{prv}}+q_T)}$。$q_{\mathrm{prv}}$和$q_T$分别表示私钥询问和陷门询问的最大次数，$\lambda$为安全参数。

证明：假设算法C是一个CDH困难问题的解决者，输入3元组为(P, aP, bP)，计算目标为abP。系

统建立、Hash询问、公钥询问、私钥询问、公钥替换询问和签密询问与定理1中相同。签名验证询问与定理1中解签密询问相同。

伪造阶段：经过多项式有界次询问后，$\mathrm{A_I}$输出伪造签名$\delta=(R,V,m)$，同时C知道被替换的公钥。若$\mathrm{A_I}$伪造签名成功，其中$P_{\mathrm{pub}}=aP$，$Q^*=bP$，$u^*\neq u^{*'}$，计算$\mathrm{e}(V^*,P)=\mathrm{e}(R^*+w^*\mathrm{PK}_{\mathrm{ID}}^*+u^*P_{\mathrm{pub}},Q^*)$，$\mathrm{e}\left(V^{*'},P\right)=\mathrm{e}\left(R^*+w^*\mathrm{PK}_{\mathrm{ID}}^*+u^{*'}P_{\mathrm{pub}},Q^*\right)$，$\mathrm{e}\left(V^*-V^{*'},P\right)=\mathrm{e}\left[\left(u^*-u^{*'}\right)P_{\mathrm{pub}},Q^*\right]$。则C输出$abP=\left(u^*-u^{*'}\right)^{-1}\left(V^*-V^{*'}\right)$作为CDH困难问题的有效解。

分析：如果C在上述游戏中没有停止，则C可以优势ε'解决CDH困难问题。令事件E_1为敌手未对挑战者身份进行私钥询问，$\Pr[E_1]=1-\frac{q_{\mathrm{prv}}}{2^\lambda}$；事件$E_2$为询问阶段算法C未终止，$\Pr[E_2]=(1-\tau)^{q_{\mathrm{prv}}+q_T}$；事件$E_3$表示伪造阶段敌手伪造合法签名后算法C未终止，则$\Pr[E_3]=\tau$。则模拟过程中算法C不终止的概率为$\Pr[E_1\wedge E_2\wedge E_3]=\left(1-\frac{q_{\mathrm{prv}}}{2^\lambda}\right)(1-\tau)^{q_{\mathrm{prv}}+q_T}\tau$，由于$\tau=\frac{1}{q_{\mathrm{prv}}+q_T+1}$，可得$\varepsilon'\geq\left(1-\frac{q_{\mathrm{prv}}}{2^\lambda}\right)\frac{1}{e\left(q_{\mathrm{prv}}+q_T\right)}$。　证毕

定理4 随机预言模型中，若存在敌手$\mathrm{A_{II}}$以概率ε攻破游戏2，则该方案满足EUF-CMA。

构造一个算法C解决CDH困难问题，其中解决问题的概率为$\left(1-\frac{q_{\mathrm{prv}}}{2^\lambda}\right)\frac{1}{\mathrm{e}\left(q_{\mathrm{prv}}+q_T\right)}$。$q_{\mathrm{prv}}$和$q_T$分别表示私钥询问和陷门询问的最大次数，$\lambda$为安全参数。

证明：算法构造和签名询问与定理3相同。系统建立、Hash询问、部分私钥询问、私钥询问和陷门询问与定理2中相同。签名验证询问与定理3相似，除了公钥被替换的情况。

伪造阶段：与定理3相同，则C输出$abP=\left(w^*-w^{*'}\right)^{-1}\left(V^*-V^{*'}\right)$作为CDH困难问题的有效解。

分析：与定理3中相同。　证毕

4.3 单向性

定理5 在随机预言模型中，若存在敌手$\mathrm{A_I}$以概率ε攻破游戏3，则该方案满足OW-CCA。

构造一个算法C解决BDH困难问题，其中解决问题的概率为$\frac{1}{q_{H_6}}\left(\frac{\varepsilon-\frac{1}{2^\lambda}}{\mathrm{e}\left(q_{\mathrm{par}}+q_{\mathrm{prv}}+1\right)}-\frac{q_{\mathrm{dsc}}}{q}\right)$。$q_{H_6}$，$q_{\mathrm{par}}$，$q_{\mathrm{prv}}$和$q_{\mathrm{dsc}}$分别表示$H_6$询问，部分私钥询问，私钥询问和解签密询问的最大次数。

证明：算法构造、系统建立、Hash询问、公钥询问、私钥询问、公钥替换询问、签密询问、解签密询问和陷门询问与定理1中相同。

挑战阶段：C随机选取m^*，若$\mathrm{cn}=0$，则终止模拟。否则，令$R^*=cP$，计算$C_2^*=H_5(m^*)\cdot H_6[\mathrm{e}(x_{\mathrm{know}}^*P+aP,cbv_i^*P)]$，发送$\delta^*=(R^*,C_1^*,C_2^*,V^*)$作为挑战密文给敌手$\mathrm{A_I}$。

猜测阶段：敌手$\mathrm{A_I}$输出m'。如果$m'=m^*$，则C输出$\eta^{*v_i^{*-1}}=\mathrm{e}(P,P)^{abc}$作为BDH困难问题的有效解。

分析：与定理1中相似，除了$\Pr[\neg E_1]\geq\frac{1}{\mathrm{e}\left(q_{\mathrm{par}}+q_{\mathrm{prv}}+1\right)}$，$\Pr[E_2]\leq-\frac{q_{\mathrm{dsc}}}{q}$，$\Pr[E_3]\geq\frac{1}{q_{H_6}}\left(\frac{\varepsilon-\frac{1}{2^\lambda}}{\mathrm{e}\left(q_{\mathrm{par}}+q_{\mathrm{prv}}+1\right)}-\frac{q_{\mathrm{dsc}}}{q}\right)$。根据文献[12]可得：$\varepsilon'\geq\frac{1}{q_{H_6}}\Pr[E_3]\geq\frac{1}{q_{H_6}}\left(\frac{\varepsilon-\frac{1}{2^\lambda}}{\mathrm{e}\left(q_{\mathrm{par}}+q_{\mathrm{prv}}+1\right)}-\frac{q_{\mathrm{dsc}}}{q}\right)$。　证毕

定理6 在随机预言模型中，若存在敌手$\mathrm{A_{II}}$以概率ε攻破游戏3，则该方案满足OW-CCA。

构造一个算法C解决BDH困难问题，其中解决问题的概率为$\frac{1}{q_{H_6}}\left(\frac{\varepsilon-\frac{1}{2^\lambda}}{\mathrm{e}\left(q_{\mathrm{prv}}+1\right)}-\frac{q_{\mathrm{dsc}}}{q}\right)$。$q_{H_6}$，$q_{\mathrm{prv}}$和$q_{\mathrm{dsc}}$分别表示$H_6$询问、私钥询问和解签密询问的最大次数，$e$为自然对数，$\lambda$为安全参数。

证明：算法构造、系统建立、Hash询问、部分私钥询问、私钥询问、公钥询问、签密询问、解签密询问和陷门询问与定理2中相同。

挑战阶段：与定理5中挑战阶段相同。

猜测阶段：敌手$\mathrm{A_{II}}$输出m'。如果$m'=m^*$，则C输出$\beta^{*(v_i^*)^{-1}}=e(P,P)^{abc}$作为BDH困难问题的有效解。

分析：与定理5中相似，根据文献[12]可得：$\varepsilon'\geq\frac{1}{q_{H_6}}\Pr[E_3]\geq\frac{1}{q_{H_6}}\left(\frac{\varepsilon-\frac{1}{2^\lambda}}{\mathrm{e}\left(q_{\mathrm{prv}}+1\right)}-\frac{q_{\mathrm{dsc}}}{q}\right)$。　证毕

5 效率及性能分析

本节将通过与Qu等人[12]方案和周彦伟等人[7]方案的对比，分析方案的通信开销和性能。

当前，文献[12]方案(Qu方案)具有密文等值测试功能，但不提供不可伪造性；文献[7]方案提供不可伪造性，但不具有密文等值测试功能。本文方案可同时支持密文等值测试性和不可伪造性。令$\boldsymbol{E}$表示双线性对个数，M表示群上点乘计算个数，Q表示群上指数计算个数。由表1可知，本文方案的解签密的效率与文献[7]方案的解密效率相当。但是，由于本文方案增加了密文等值测试功能，方案的签

表 1 计算性能分析

方案	加密(签密)	解密(解签密)	机密性	不可伪造性	密文等值测试性	单向性
Qu等人[12]方案	$3Q+2E$	$2Q+2E$	√	×	√	√
周彦伟等人[7]方案	$2M$	$4M$	√	√	×	×
本文方案	$2M+2E$	$M+E$	√	√	√	√

注：√表示方案具有该属性，×表示方案不具有该属性。

密计算代价略高于文献[7]方案。与文献[12]方案相比，本文方案不仅增加了不可伪造性的属性，而且方案的计算效率更高。

为了更直观地描述方案的效率，本文基于配对密码(Pairing-Based Cryptography, PBC)库[14]对方案进行了实验仿真。实验环境为：华为Magic-Book Pro，处理器Intel(R) Core(TM)i5-8265 UCPU@1.60 GHz 1.80 GHz，内存2 GB和64位Win10操作系统。实验仿真的计算开销对比如图2所示，本文方案的签密算法和解签密算法的效率与文献[7]方案相近，同时明显高于文献[12]方案。

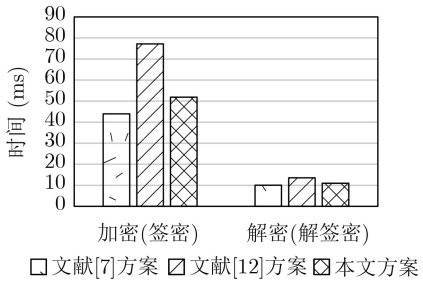

图 2 效率对比

参 考 文 献

[1] ZHENG Y. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)[C]. The 17th Annual International Cryptology Conference, Santa Barbara, USA, 1997: 165-179. doi: 10.1007/BFb0052234.

[2] SHAMIR A. Identity-based Cryptosystems and Signature Schemes[M]. BLAKLEY G R and CHAUM D. Advances in Cryptology. Berlin, Germany, Springer, 1985: 47–53. doi: 10.1007/3-540-39568-7_5.

[3] AL-RIYAMI S S and PATERSON K G. Certificateless public key cryptography[C]. The 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, China, 2003: 452–473. doi: 10.1007/978-3-540-40061-5_29.

[4] BARBOSA M and FARSHIM P. Certificateless signcryption[C]. 2008 ACM Symposium on Information, Computer and Communications Security, Tokyo, Japan, 2008: 369-372. doi: 10.1145/1368310.1368364.

[5] WU Chenhuang and CHEN Zhixiong. A new efficient certificateless signcryption scheme[C]. 2008 International Symposium on Information Science and Engineering, Shanghai, China, 2008: 661-664. doi: 10.1109/ISISE.2008.206.

[6] 王星, 钱海峰. 高效的无证书签密方案[J]. 计算机工程与应用, 2011, 47(20): 62–64. doi: 10.3778/j.issn.1002-8331.2011.20.019.

WANG Xing and QIAN Haifeng. Efficient certificateless signcryption scheme[J]. *Computer Engineering and Applications*, 2011, 47(20): 62–64. doi: 10.3778/j.issn.1002-8331.2011.20.019.

[7] 周彦伟, 杨波, 王青龙. 安全的无双线性映射的无证书签密机制[J]. 软件学报, 2017, 28(10): 2757–2768. doi: 10.13328/j.cnki.jos.005150.

ZHOU Yanwei, YANG Bo, and WANG Qinglong. Secure certificateless signcryption scheme without bilinear pairing[J]. *Journal of Software*, 2017, 28(10): 2757–2768. doi: 10.13328/j.cnki.jos.005150.

[8] MANDAL S, MOHANTY S, and MAJHI B. Universally Verifiable Certificateless Signcryption Scheme for MANET[M]. NATH V. Proceedings of the International Conference on Microelectronics, Computing & Communication Systems. Singapore: Springer, 2018: 77-89. doi: 10.1007/978-981-10-5565-2_7.

[9] LUO Ming and WAN Yuwei. An enhanced certificateless signcryption in the standard model[J]. *Wireless Personal Communications*, 2018, 98(3): 2693–2709. doi: 10.1007/s11277-017-4995-4.

[10] YANG Guomin, TAN C H, HUANG Qiong, *et al*. Probabilistic public key encryption with equality test[C]. Cryptographers' Track at the RSA Conference, San Francisco, USA, 2010: 119–131. doi: 10.1007/978-3-642-11925-5_9.

[11] MA Sha. Identity-based encryption with outsourced equality test in cloud computing[J]. *Information Sciences*, 2016, 328: 389–402. doi: 10.1016/j.ins.2015.08.053.

[12] QU Haipeng, YAN Zhen, LIN Xijun, *et al*. Certificateless public key encryption with equality test[J]. *Information Sciences*, 2018, 462: 76–92. doi: 10.1016/j.ins.2018.06.025.

[13] 张玉磊, 陈文娟, 张永洁, 等. 支持关键字搜索的无证书密文等值测试加密方案[J]. 电子与信息学报, 2020, 42(11): 2713–2719. doi: 10.11999/JEIT190752.
ZHANG Yulei, CHEN Wenjuan, ZHANG Yongjie, *et al*. Certificateless puklic key encryption with equality test of supporting keyword search[J]. *Journal of Electronics & Information Technology*, 2020, 42(11): 2713–2719. doi: 10.11999/JEIT190752.

[14] PBC Library. The pairing-based cryptography library[EB/OL]. http://crypto.stanford.edu/pbc/, 2015.

张玉磊：男，1979年生，博士，副教授，研究方向为密码学与信息安全.

白巧玲：女，1995年生，硕士生，研究方向为网络与信息安全.

马彦丽：女，1992年生，硕士，研究方向为网络与信息安全.

闫晨阳：女，1994年生，硕士生，研究方向为网络与信息安全.

王彩芬：女，1963年生，博士，教授，研究方向为密码学与信息安全.

责任编辑：余　蓉