可证安全的 IDPKC-to-CLPKC 异构签密方案

张玉磊[①] 张灵刚[*①] 王彩芬[①] 马彦丽[①] 张永洁[②]
[①](西北师范大学计算机科学与工程学院 兰州 730070)
[②](甘肃卫生职业学院 兰州 730000)

摘 要：为了保证异构网络中消息的机密性和认证性，该文定义了身份公钥密码 IDPKC 到无证书公钥密码 CLPKC 异构签密模型，并提出具体的 IDPKC-to-CLPKC 异构签密方案。方案中双方密码系统参数相互独立，能够满足实际应用需求。在随机预言模型下，基于 GBDH, CDH 和 q-SDH 困难假设，证明方案满足 IDPKC-to-CLPKC 异构签密的机密性和不可伪造性。同时，该方案满足匿名性，通过密文无法判断发送方和接收方的身份，可以有效保护双方的身份隐私。

关键词：异构签密；匿名性；无证书公钥密码；身份公钥密码
中图分类号： TP309 **文献标识码**：A **文章编号**：1009-5896(2017)09-2127-07
DOI: 10.11999/JEIT170062

Provable Secure IDPKC-to-CLPKC Heterogeneous Signcryption Scheme

ZHANG Yulei[①] ZHANG Linggang[①] WANG Caifen[①] MA Yanli[①] ZHANG Yongjie[②]
[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)
[②](*Gansu Health Vocational College*, *Lanzhou* 730000, *China*)

Abstract: In order to ensure the confidentiality and authentication in different network environments, the security model of IDPKC-to-CLPKC heterogeneous signcryption is defined from IDentity-based Public Key Cryptography (IDPKC) to CertificateLess Public Key Cryptography (CLPKC), and a concrete IDPKC-to-CLPKC heterogeneous signcryption scheme is presented. The system parameters in IDPKC and CLPKC are independent on each other in the scheme, which can meet the practical requirements. Based on the assumptions of Gap Bilinear Diffie-Hellman (GBDH), Computational Diffie-Hellman (CDH) and q-Strong Diffie-Hellman (q-SDH), the scheme is proved to satisfy the confidentiality and unforgeability in the random oracle model. Moreover, the scheme is also proved to satisfy the properties of ciphertext anonymity, which means the attacker can not judge the identities of the sender and the receiver. Therefore, the scheme can effectively protect the privacy of both identities.

Key words: Heterogeneous signcryption; Anonymity; CertificateLess Public Key Cryptography (CLPKC); IDentity-based Public Key Cryptography (IDPKC)

1 引言

异构网络是 5G 通信网络的核心。异构网络中，通信双方一般具有不同的密码系统。为了保证异构网络消息的机密性和不可伪造性，需要研究异构签密(Heterogeneous SignCryption, HSC)问题[1,2]。

2010 年文献[2]提出异构签密原语并构造了传统公钥密码 (Traditional Public Key Cryptography, TPKC)到身份公钥密码(IDentity-based Public Key Cryptography, IDPKC)的 TPKC→IDPKC 异构签密方案，但是该方案只满足签密外部安全性[3]。2011 年，文献[4]提出具有密钥隐私性质并满足内部安全性的 IDPKC→TPKC 异构签密方案。2013 年，文献[5]提出了 IDPKC→TPKC 多接收者异构签密方案。同年，文献[6]提出 TPKC- IDPKC 双向异构签密方案。2016 年，文献[7,8]分别提出从无证书公钥密码(CertificateLess Public Key Cryptography, CLPKC)[9]到 TPKC 的 CLPKC→TPKC 异构签密方案。同年，文献[10]提出用于无线传感器网络 CLPKC→IDPKC 异构签密方案。但是，该方案的双线性对较多，执行效率不高。同时，现有异构签密方案未考虑 IDPKC→CLPKC 异构签密问题。

本文首先定义 IDPKC→CLPKC 异构签密方案的形式化定义和安全模型，然后基于文献[6]设计一

收稿日期：2017-01-18；改回日期：2017-04-13；网络出版：2017-06-14
*通信作者：张灵刚 linggang01@126.com
基金项目：国家自然科学基金(61163038, 61262056)，甘肃省高等学校科研项目(2015B-220, 2013A-014)
Foundation Items: The National Natural Science Foundation of China (61163038, 61262056), The Higher Educational Scientific Research Foundation of Gansu Province (2015B-220, 2013A-014)

个具有匿名性的 IDPKC→CLPKC 异构签密方案。该方案具有以下特点：

(1)随机预言模型下，基于 GBDH(Gap Bilinear Differ-Hellman), CDH(Computational Diffie-Hellman)和 q-SDH(q-Strong Differ-Hellman)困难假设，证明方案满足 IDPKC→CLPKC 异构签密的机密性和不可伪造性。

(2)方案的 IDPKC 和 CLPKC 密码环境使用独立的系统参数，可以满足异构网络实际应用需求。

(3)方案满足匿名性，通过密文无法判断发送方和接收方的身份。

2 IDPKC→CLPKC 异构签密定义及安全模型

2.1 IDPKC→CLPKC 异构签密定义

定义 1 IDPKC→CLPKC 异构签密方案由 5 个算法构成：系统建立算法、密钥生成算法、密钥提取算法、签密算法和解签密算法。

(1)系统建立算法：IDPKC 私钥生成中心(Private Key Generator, PKG)输入安全参数 k_1，输出 IDPKC 主密钥 s_1 和系统参数 Pa_1。PKG 保密 s_1 并公开 Pa_1。CLPKC 密钥生成中心 (Key Generation Center, KGC)输入安全参数 k_2，输出 CLPKC 主密钥 s_2 和系统参数 Pa_2。KGC 保密 s_2 并公开 Pa_2。

(2)密钥生成算法： PKG 输入 Pa_1，s_1 和用户身份 ID_U，生成用户私钥 S_U，ID_U 为用户的公钥。

(3)密钥提取算法：KGC 输入 Pa_2，s_2 和用户身份 ID_U，生成用户的部分私钥 D_U。用户选择秘密值 x_U，产生用户的私钥 $\mathrm{SK}_U=(x_U, D_U)$ 和公钥 PK_U。

(4)签密算法：发送方输入双方系统参数，发送方身份 ID_U 与私钥 S_U、接收方身份 ID_U 与公钥 PK_U 和明文 m，输出密文 δ。

(5)解签密算法：接收方输入双方系统参数，接收方身份 ID_U，公钥 PK_U 及私钥 SK_U 和密文 δ，输出明文 m 或者符号“⊥”。“⊥”表示密文不合法。

2.2 IDPKC→CLPKC 异构签密安全模型

IDPKC→CLPKC 异构签密方案必须满足机密性和不可伪造性，即 CLPKC 适应性选择密文攻击下密文的不可区分性 IND-CCA2(INDistinguishability against Adaptive Chosen Ciphertext Attack)和 IDPKC 适应性选择消息攻击下的存在不可伪造性 EUF-CMA(Existential UnForgeability against adaptive Chosen Messages Attack)。

2.2.1 机密性

定义 2 如果敌手 A_I 和 A_II 赢得游戏 1 和游戏 2 的优势是不可忽略的，那么 IDPKC→CLPKC 方案是 IND-CCA2 安全的。

游戏 1 挑战者 C 和敌手 A_I 之间的 IND-CCA2-Ⅰ交互游戏包括以下 5 个阶段：

初始阶段 C 设置安全参数 k_1 和 k_2。C 执行“系统建立算法”生成 Pa_1 和 Pa_2，返回 IDPKC 主密钥 s_1 给 A_I，保存 s_2。

阶段 1 C 和 A_I 模拟过程中，A_I 能够对以下预言机进行多项式有界次适应性询问。

(1)密钥生成询问：A_I 输入身份 ID_U，C 执行“密钥生成算法”返回 ID_U 的私钥 S_U 给 A_I。

(2)密钥提取询问：A_I 输入身份 ID_U，C 执行“密钥提取算法”返回 ID_U 的部分私钥 D_U，秘密值 x_U，公钥 PK_U 和完全私钥 SK_U 给 A_I。

(3)公钥替换：A_I 选择新的 PK'_U 替换 ID_U 的公钥 PK_U，并将原秘密值 x_U 改为“⊥”。

(4)签密询问：A_I 选择 $(\mathrm{ID}_i, \mathrm{ID}_j, m)$；$C$ 执行“密钥生成算法”和“密钥提取算法”获得发送方 ID_i 的私钥 S_i 和接收方 ID_j 的公钥 PK_j，然后执行“签密算法”返回密文 δ 给 A_I。

(5)解签密询问：A_I 提供密文 δ 和接收方身份 ID_j。如果 ID_j 的公钥没有被替换，那么 C 执行“密钥生成算法”和“密钥提取算法”获得发送方的公钥 Q_i 和接收方的私钥 SK_j，然后执行“解签密算法”返回明文 m 或者“⊥”给 A_I。本文采用弱无证书签密询问[11,12]，如果 ID_j 的公钥被替换，要求提供公钥对应的秘密值。

挑战阶段 A_I 选择两个等长明文 m_0 与 m_1，发送方身份 ID_A 和接收方 ID_B 作为挑战信息。C 执行“密钥生成算法”获得发送者的私钥 S_A，然后随机选择 $\gamma\in\{0,1\}$，执行“签密算法”获得密文 $\delta^*=\mathrm{signcrypt}(\mathrm{ID}_A, S_A, \mathrm{ID}_B, \mathrm{PK}_B, m_\gamma)$。最后返回 δ^* 给 A_I 作为挑战密文。

阶段 2 A_I 和 C 如同“阶段 1”进行问答。A_I 不能询问 ID_B 的部分私钥，但是允许 A_I 询问 ID_A 的私钥：即使 A_I 获得 ID_A 的私钥(发送方的私钥泄露)，A_I 也无法伪造一个合法的密文，即方案满足内部安全性[4]。但是，A_I 不能执行对挑战密文 δ^* 的解签密询问。

猜测阶段 A_I 选择 $\gamma'\in\{0,1\}$。若 $\gamma=\gamma'$，A_I 赢得游戏。定义 A_I 的优势为 $\mathrm{Adv}(A_\mathrm{I})=|\Pr[\gamma'=\gamma]-1/2|$，其中 $\Pr[\gamma'=\gamma]$ 表示 $\gamma'=\gamma$ 的概率。

游戏 2 挑战者 C 和敌手 A_II 之间的 IND-CCA2-Ⅱ交互游戏包括以下 5 个阶段：

初始阶段　C 设置安全参数 k_1 和 k_2。C 执行“系统建立算法”生成 Pa_1 和 Pa_2；将 s_1 和 s_2 返回给 A_{II}。

阶段 1　C 和 A_{II} 模拟过程中，A_{II} 能够对以下预言机进行多项式有界次适应性询问。

(1)密钥生成询问和密钥提取询问过程与游戏 1 基本相同。但是，游戏 2 不允许公钥替换询问。

(2)签密询问：A_{II} 选择 $(\mathrm{ID}_i,\mathrm{ID}_j,m)$。$C$ 执行“密钥生成算法”获得发送方私钥 S_i，执行“密钥提取算法”获得接收方公钥 PK_j，然后调用“签密算法”返回密文 δ 给 A_{II}。

(3)解签密询问：A_{II} 提供密文 δ 和接收方身份 ID_j。C 执行“密钥生成算法”获得发送方公钥 Q_i，执行“密钥提取算法”获得接收方的私钥 SK_j，然后执行“解签密算法”返回明文 m 或者“$\perp$”给 A_{II}。

挑战阶段　A_{II} 选择两个等长明文 m_0 与 m_1，发送方身份 ID_A 和接收方 ID_B 作为挑战信息。要求 A_{II} 没有询问过 ID_B 秘密值。C 选择 $\gamma\in\{0,1\}$，返回 $\delta^*=\mathrm{signcrypt}(\mathrm{ID}_A,S_A,\mathrm{ID}_B,\mathrm{PK}_B,m_\gamma)$ 给 A_{II}。

阶段 2　A_{II} 和 C 如同“阶段 1”进行问答。但是，A_{II} 不能对 ID_B 执行秘密值询问。同时，A_{II} 不能执行对挑战密文 δ^* 的解签密询问。

猜测阶段　A_{II} 选择 $\gamma'\in\{0,1\}$。若 $\gamma=\gamma'$，那么 A_{II} 赢得游戏。定义 A_{II} 的优势为 $\mathrm{Adv}(A_{\mathrm{II}})=|\Pr[\gamma'=\gamma]-1/2|$，其中 $\Pr[\gamma'=\gamma]$ 表示 $\gamma'=\gamma$ 的概率。

2.2.2 不可伪造性

定义 3　如果敌手 F 赢得游戏 3 的优势是不可忽略的，那么称该 IDPKC→CLPKC 异构签密方案是 EUF-CMA 安全的。

游戏 3　挑战者 C 和敌手 F 之间的 EUF-CMA 交互游戏包括以下 3 个阶段：

初始阶段　C 设置安全参数 k_1 和 k_2。C 执行“系统建立算法”生成 Pa_1 和 Pa_2 并返回主密钥 s_2 给 F，保存 s_1。

攻击阶段　F 执行与游戏 1 和游戏 2 相同的多项式有界次询问。

伪造阶段　F 输出 $(\mathrm{ID}_A,\mathrm{ID}_B,\mathrm{PK}_B,\delta^*)$。当以下条件满足时，$F$ 获得胜利。

(1) δ^* 对于 $(\mathrm{ID}_A,\mathrm{ID}_B,\mathrm{PK}_B)$ 合法，即解签密结果不是“$\perp$”。

(2)没有对 $(m^*,\mathrm{ID}_A,\mathrm{ID}_B')$ 执行签密询问（ID_B' 可能与 ID_B 不同）。

(3)没有询问过 ID_A 的私钥。

2.2.3 密文匿名性

定义 4　如果敌手 A 赢得游戏 4 的优势是不可忽略的，那么称该 IDPKC→CLPKC 异构签密方案在适应性选择密文攻击下具有密文匿名性。

游戏 4　挑战者 F 和敌手 A 之间的密文匿名性交互游戏由以下 5 个阶段组成。

初始阶段　F 设置安全参数 k_1 和 k_2。F 执行“密钥生成算法”生成密文发送者两个公钥/私钥 $(Q_{A,0},S_{A,0})$ 和 $(Q_{A,1},S_{A,1})$，并将私钥 $S_{A,0}$ 和 $S_{A,1}$ 发送给 A。F 执行“密钥提取算法”生成密文接收者两个公钥/私钥 $(\mathrm{PK}_{B,0},\mathrm{SK}_{B,0})$ 和 $(\mathrm{PK}_{B,1},\mathrm{SK}_{B,1})$，并将 $\mathrm{PK}_{B,0}$ 和 $\mathrm{PK}_{B,1}$ 发送给 A。

阶段 1　A 执行多项式有界次的签密和解签密询问。

签密询问中，A 提交接收者的公钥 PK_w 和消息 m 给 F。若 PK_w 合法且 $\mathrm{PK}_w\neq\mathrm{PK}_{B,c}$，则 F 执行“签密算法”返回密文 $\delta=\mathrm{signcrypt}(S_{A,c'},\mathrm{PK}_w,m)$ 给 A；否则返回“$\perp$”。

解签密询问中，A 提交一个密文 δ 给 F，F 利用“解签密算法”返回 $\mathrm{unsigncrypt}(Q_{A,c'},\mathrm{SK}_{B,b},\delta)$ 给 A。其中，$c,c'\in\{0,1\}$。

挑战阶段　A 选择消息 m 和发送者的私钥 $S_{A,0}$ 和 $S_{A,1}$。F 选择 $b,b'\in\{0,1\}$，计算 $\delta^*=\mathrm{signcrypt}(S_{A,b'},\mathrm{PK}_{B,b},m)$ 返回给 A 作为挑战密文。

阶段 2　A 和 F 如同“阶段 1”进行问答。但是 A 不能执行有关挑战密文 δ^* 的解签密询问。

猜测阶段　A 输出 $\gamma,\gamma'\in\{0,1\}$。如果 $(\gamma,\gamma')=(b,b')$，那么 A 获得胜利。A 的优势为 $\mathrm{Adv}(A)=\left|\Pr[(\gamma,\gamma')=(b,b')]-1/4\right|$，其中 $\Pr[(\gamma,\gamma')=(b,b')]$ 表示 $(\gamma,\gamma')=(b,b')$ 的概率。

3　本文 IDPKC→CLPKC 异构签密方案

3.1 具体方案

(1)系统建立算法：DPKC 系统中，设 G_{1-1} 是 q_1 阶循环加法群，G_{1-2} 是同阶循环乘法群，$P_1\in G_{1-1}$，$e_1:G_{1-1}\times G_{1-1}\to G_{1-2}$ 为双线性映射。定义 2 个安全 Hash 函数 $H_{1-1}:\{0,1\}^*\to Z_{q_1}^*$，$H_{1-2}:\{0,1\}^*\times G_{1-2}\to Z_{q_1}^*$。随机选取 $s_1\in Z_{q_1}^*$ 作为 IDPKC 主密钥，计算 $P_{\mathrm{pub}_1}=s_1P_1$。设 $g=e_1(P_1,P_1)$。公开系统参数 $\mathrm{Pa}_1=\{G_{1-1},G_{1-2},q_1,g,P_1,P_{\mathrm{pub}_1},e_1,H_{1-1},H_{1-2}\}$，保存主密钥 s_1。

CLPKC 系统中，设 G_{2-1} 是 q_2 阶循环加法群，G_{2-2} 是同阶循环乘法群，$P_2\in G_{2-1}$，$e_2:G_{2-1}\times G_{2-1}\to G_{2-2}$ 为双线性映射。定义 2 个安全 Hash 函数 $H_{2-1}:\{0,1\}^*\to G_{2-1}$，$H_{2-2}:\{0,1\}^*\to\{0,1\}^{l_{G_{2-1}}+l_{\mathrm{ID}}+l_m}$，其中 l_m 表示消息长度，l_{ID} 表示身份长度。随机选取 $s_2\in Z_{q_2}^*$ 作为 CLPKC 主密钥，计算 $P_{\mathrm{pub}_2}=s_2P_2$。公开系统参数 $\mathrm{Pa}_2=\{G_{2-1},G_{2-2},q_2,l_m,l_{\mathrm{ID}},P_2,P_{\mathrm{pub}_2},e_2,H_{2-1},H_{2-2}\}$，保存主密钥 s_2。

(2)密钥生成算法： IDPKC 发送方 Alice 的身份为 $\mathrm{ID}_A \in \{0,1\}^*$，私钥为 $S_A = \dfrac{1}{Q_A + s_1} P_1$，$Q_A = H_{1-1}(\mathrm{ID}_A)$ 为用户公钥。

(3)密钥提取算法： CLPKC 接收方 Bob 的身份为 $\mathrm{ID}_B \in \{0,1\}^*$，部分私钥为 $D_B = s_2 Q_B$，其中 $Q_B = H_{2-1}(\mathrm{ID}_B)$。用户选择 $x_B \in Z_{q_2}^*$ 作为秘密值，其公钥/私钥分别为 $\mathrm{PK}_B = x_B P_2$ 和 $\mathrm{SK}_B = (x_B, D_B)$。

(4)签密算法：发送方 Alice 执行以下步骤：

(a)随机选择 $r_1 \in Z_{q_1}^*$，$r_2 \in Z_{q_2}^*$，计算 $R_1 = g^{r_1}$，$R_2 = r_2 P_2$；

(b)计算 $U = e_2(P_{\mathrm{pub}_2}, Q_B)^{r_2}$ 和 $V = r_2 \mathrm{PK}_B$；

(c)计算 $c = (m \| R_1 \| \mathrm{ID}_A) \oplus H_{2-2}(U, V, R_2)$；

(d)计算 $h = H_{1-2}(m, R_1)$，$W = (r_1 + h) S_A$，则明文 m 的密文为 $\delta = (c, R_2, W)$。

(5)解签密算法：接收方 Bob 收到密文 δ 后，按以下步骤执行：

(a)计算 $U' = e_2(R_2, D_B)$，$V' = x_B R_2$；

(b)计算 $\left(m \| R_1 \| \mathrm{ID}_A\right) = c \oplus H_{2-2}(U', V', R_2)$，$h = H_{1-2}(m, R_1)$，$Q_A = H_{1-1}(\mathrm{ID}_A)$

(c)检查等式 $R_1 = e_1\left(W, P_{\mathrm{pub}_1} + Q_A P_1\right) g^{-h}$ 是否成立。若成立，返回明文 m；否则输出符号“$\perp$”。

3.2 方案正确性

本文方案正确当且仅当以下两类等式成立：

(1)密文能够被正确解密：

$$\begin{aligned} U' &= e_2(R_2, D_B) = e_2(r_2 P_2, s_2 Q_B) = e_2(r_2 s_2 P_2, Q_B) \\ &= e_2\left(P_{\mathrm{pub}_2}, Q_B\right)^{r_2} = U, \\ V' &= x_B R_2 = r_2 x_B P_2 = r_2 \mathrm{PK}_B = V \end{aligned}$$

(2)密文能够被正确验证：

$$\begin{aligned} & e_1\left(W, P_{\mathrm{pub}_1} + Q_A P_1\right) g^{-h} \\ &= e_1\left((r_1 + h)\frac{1}{Q_A + s_1} P_1, s_1 P_1 + Q_A P_1\right) g^{-h} \\ &= e_1(P_1, P_1)^{r_1 + h} g^{-h} = g^{r_1 + h} g^{-h} = g^{r_1} = R_1 \end{aligned}$$

4 安全性证明及效率分析

4.1 机密性

定理 1 在随机预言模型下，假设 GBDH 问题和 CDH 问题困难，则本文方案 IND-CCA2 安全。

引理 1.1 随机预言模型下，如果存在敌手 A_{I} 以 $(q_{H_{2-1}}, q_p, q_u, t, \omega)$ 的优势在游戏 1 中获胜，那么存在一个算法 C 能够以 $\varepsilon/(q_{H_{2-1}} + q_p + q_u)$ 的优势解决 GBDH 困难问题。

引理 1.2 随机预言模型下，如果存在敌手 A_{II} 以 $(q_{H_{2-1}}, q_{\mathrm{sc}}, q_u, t, \varepsilon)$ 的优势在游戏 2 中获胜，那么存在一个算法 C 能够以 $\varepsilon/(q_{H_{2-1}} + q_{\mathrm{sc}} + q_u)$ 的优势解决 CDH 问题。

限于篇幅，略去方案的机密性证明过程。

4.2 不可伪造性

定理 2 随机预言模型下，如果存在敌手 F 以 $(q_{H_{1-1}}, q_{H_{1-2}}, q_s, q_u, t, \varepsilon)$ 的优势在游戏 3 中获胜，那么存在一个算法 C，能够以 $\dfrac{1}{q_{H_{1-1}}}\left(1 - \dfrac{1}{q_{H_{1-1}}}\right)\left(1 - \dfrac{q_s}{2^{k_1}}\right) \cdot \left(1 - \dfrac{1}{q_{H_{1-2}}}\right)\varepsilon$ 的优势解决 q-SDH 问题，其中 k_1 为 IDPKC 安全参数，$q_{H_{1-1}}$，$q_{H_{1-2}}$ 和 q_s 分别表示执行 H_{1-1} 询问、H_{1-2} 询问和签密询问的最大次数。

证明 利用分叉引理[13]证明该方案。C 接收 q-SDH 问题实例 $(P_1, aP_1, a^2 P_1, \cdots, a^{q_1} P_1)$，利用 F 找出一对 $\left(\omega, \dfrac{1}{a + \omega} P_1\right)$。

初始阶段 C 随机选择 $\omega_1, \omega_2, \cdots, \omega_{q_1 - 1} \in Z_{q_1}^*$，选取 G_{1-1} 生成元 G。C 获得 $q_1 - 1$ 对 $\left(\omega_i, \dfrac{1}{a + \omega_i} P_1\right)$，$i \in \{0, 1, \cdots, q_1 - 1\}$。为了获得 $c_0, c_1, \cdots, c_{q_{1-1}} \in Z_{q_1}^*$，展开多项式 $f(z) = \prod_{i=1}^{q_1 - 1}(z + \omega_i) = \sum_{j=0}^{q_1 - 1} c_j z^j$。$C$ 设置 $G = \sum_{j=0}^{q_1 - 1} c_j (a^j P_1) = f(a) P_1$ 和 $P_{\mathrm{pub}_1} = \sum_{j=1}^{q_1} c_{j-1} (a^j P_1) = a f(a) P_1 = aG$。当 $1 \le i \le q_1 - 1$ 时，扩展 $f_i(z) = f(z)/(z + w_i) = \sum_{j=1}^{q_1 - 2} d_j z^j$，计算 $\sum_{i=0}^{q_1 - 2} d_i (a_i P_1) = f_i(a) P_1 = \dfrac{f(a)}{a + w_i} P_1 = \dfrac{1}{a + w_i} G$。则 IDPKC 主密钥为 a (未知)，系统公钥为 $P_{\mathrm{pub}_1} = aG$，C 发送系统参数(包括 G 和 P_{pub_1})给 F。C 执行“系统建立算法”返回 CLPKC 主密钥 $s_2 \in Z_{q_2}^*$、系统公钥 $P_{\mathrm{pub}_2} = s_2 P_2$ 和系统参数给 F。

攻击阶段 C 保持列表 L_{1-1}，L_{1-2}，L_{2-1}，L_{2-2} 和 L_{pk} 分别保存 A_{I} 对询问 H_{1-1}，H_{1-2}，H_{2-1}，H_{2-2} 预言机以及公钥产生的结果。C 随机选择 $l_1 \in \{1, 2, \cdots, lq_{H_{1-1}}\}$ 执行以下询问：

H_{1-1} 询问：当 F 对 H_{1-1} 执行第 i 次询问时，如果 $i = l_1$，那么 C 选取 $\omega_{l_1} \in Z_{q_1}^*$ 并发送给 F；否则，C 返回 ω_i，并将 $(i, \mathrm{ID}_i, \boldsymbol{\omega}_i)$ 保存到 L_{1-1}。

H_{2-1} 询问： C 选择 $r_j \in Z_{q_2}^*$，返回 $Q_j = r_j P_2$ 并将 $(j, \mathrm{ID}_j, r_j, Q_j)$ 保存到 L_{2-1}。

H_{1-2} 询问： C 选取 $t_i \in Z_{q_1}^*$ 发送给 F 并将 (m_i, R_{1_i}, t_i) 保存到 L_{1-2}。

H_{2-2} 询问： C 选择 $h_j \in \{0,1\}^{l_{G_{1-1}} + l_{\mathrm{ID}} + l_m}$ 并将 (U_j, V_j, R_{2_j}, h_j) 保存到 L_{2-2}。

密钥生成询问：F 对新 ID_i 执行询问时，如果 $i=l_1$，那么失败并停止；否则 C 查询 L_{1-1} 获得 $(i,\mathrm{ID}_i,\boldsymbol{\omega}_i)$，并返回 $1/(a+\omega_i)G$ 给 F。

公钥询问：C 选择 $x_j\in Z_{q_2}^*$ 作为秘密值，发送 $\mathrm{PK}_j=x_jP_2$ 给 F 并将 $(\mathrm{ID}_j,\mathrm{PK}_j,x_j)$ 保存到 L_{pk}。

私钥询问：F 询问新 ID_j 的私钥时，C 执行 H_{2-1} 询问获得 $(j,\mathrm{ID}_j,r_j,Q_j)$，查找 L_{pk} 获得 x_j 并发送私钥 $(x_j,r_js_2P_2)$ 给 F。

签密询问：F 提供明文 G_{1-1}、发送方 ID_i 和接收方 ID_j，G_{2-2} 执行以下过程：

(1)如果 $\mathrm{ID}_i\neq\mathrm{ID}_j$，$p_1$ 执行“密钥生成算法”获得 ID_i 的私钥 q_1，再执行“签密算法”完成签密。

(2)如果 ID_i=ID_j，ID_1 选择 ID_2，m，δ，并计算 $R_1=e_1\left(W,P_{\mathrm{pub}_1}+\boldsymbol{\omega}_{l_1}G\right)e_1(G,G)^{-h}$，$R_{2_j}=vP_2$，$U_j=e_2\left(P_{\mathrm{pub}_2},Q_B\right)^v$，$V_j=v\mathrm{PK}_j$，$C$ 执行 H_{2-2} 询问获得 h_j，计算 $c=\left(m\|R_{1_i}\|\mathrm{ID}_i\right)\oplus h_j$。$C$ 检查 L_{1-2} 中是否存在元组 (m,R_1,t_i)。若不存在，则插入元组到 L_{1-2}；否则，C 终止。C 输出密文 $\delta=(c,R_2,W)$ 并发送给 F。

解签密询问：F 提供密文 δ 和接收方 ID_j，C 执行以下过程：

(1)如果 $\mathrm{ID}_j=\mathrm{ID}^*$，$C$ 输出的密文 δ 无效。

(2)如果 $\mathrm{ID}_j\neq\mathrm{ID}^*$，$C$ 首先查询 L_{pk} 获取 ID_j 的秘密值 x_j，然后询问 ID_j 的私钥，计算 $U_j=e_2(R_{2_j},D_j)$ 和 $V_j=x_jR_{2_j}$。C 查询 L_{2-2} 获取 h_j，计算 $\left(m\|R_1\|\mathrm{ID}_i\right)=c\oplus h_j$，完成解签密。

伪造阶段　如果 F 是有效的伪造者，那么可以构造出算法 F'。F' 输出两个密文 $\left((c,\mathrm{ID}_i),h,W\right)$ 和 $\left((c,\mathrm{ID}_i),h',W'\right)$。如果 $\mathrm{ID}_i=\mathrm{ID}_{l_1}$，因为密文有效，所以 $W=(r_1+h)S_{l_1}$，$W'=(r_1+h')S_{l_1}$，其中 $h\neq h'$，则 $S_{l_1}=\dfrac{W-W'}{h-h'}=\dfrac{1}{a+\omega_{l_1}}G$。根据分叉引理，$C$ 输出 $\left(\omega_{l_1},\dfrac{1}{a+\omega_{l_1}}P_1\right)$ 为 q-SDH 问题的解。

根据分叉引理，如果 F 能够以 ε 的优势赢得游戏 3，那么存在算法 C 就能够以 $\dfrac{1}{q_{H_{1-1}}}\left(1-\dfrac{1}{q_{H_{1-1}}}\right)\cdot\left(1-\dfrac{q_s}{2^{k_1}}\right)\left(1-\dfrac{1}{q_{H_{1-2}}}\right)\varepsilon$ 优势解决 q-SDH 问题，其中 k_1 为 IDPKC 系统安全参数。

4.3 匿名性

密文匿名性，即敌手不能从密文中获取发送方和接收方的身份信息[14]。方案中密文涵盖了发送方和接收方的信息，任何第三方都不能从密文中知道收发双发的身份信息，除非第三方有接收方的私钥。

定理 3　随机预言模型下，如果攻击者 A 以 ε 的优势在游戏 4 中获胜，那么存在算法 F 能够以 $\dfrac{4}{3}\left(1-\dfrac{q_u}{2^{k_2}}\right)\varepsilon$ 的优势解决 CDH 问题。其中，q_u 为解签密询问的最大询问次数，k_2 为 CLPKC 安全参数。

证明　假设攻击者 A 能够以不可忽略的优势赢得游戏 4，那么可以构造一个算法 F 解决 CDH 困难问题。给定 CDH 问题实例 (P_2,aP_2,bP_2)，F 的目标是使用 A 解决 CDH 问题，即计算 abP_2。

初始阶段　F 选择 $x,y\in Z_{q_2}^*$，设两个接收者公钥 $\mathrm{PK}_{B,0}=xbP_2$ 和 $\mathrm{PK}_{B,1}$=ybP_2。F 执行“密钥生成算法”，产生 Pa_1 和主密钥 s_1。F 发送 Pa_1，s_1，接收者公钥 $\mathrm{PK}_{B,0}$ 和 $\mathrm{PK}_{B,1}$ 给 A。

阶段 1　F 能够模拟与定理 2 相似的询问。

挑战阶段　A 选择消息 m，两个不同发送者私钥 $S_{A,0}$ 和 $S_{A,1}$ 和接收者公钥 $\mathrm{PK}_{B,0}$ 和 $\mathrm{PK}_{B,1}$，请求 F 返回挑战密文 δ^*=signcrypt$(S_{A,b},\mathrm{PK}_{B,b'},m)$，其中 $b,b'\in\{0,1\}$。F 设置 R_2^*=aP_2，选择 $U^*\in G_{2-2}$，V^*=$a\mathrm{PK}_{B,b'}\in G_{2-1}$，$W^*\in G_{1-1}$ 和 $c^*\in\{0,1\}^{l_m+l_{G_{1-2}}+l_{ID}}$，$F$ 发送 $\delta^*=(c^*,R_2^*,W^*)$ 作为挑战密文给 A。F 选择 $t_i,t_i'\in Z_{q_1}^*$，并将 (m,R_1^*,t_i) 和 (m,R_1^*,t_i') 保存到 L_{1-2} 中。同样地，设定 $H_{2-2}(U^*,R_2^*,\Delta)$ 的值为 $c^*\oplus(m\|R_1^*\|\mathrm{ID}_{A,0})$ 和 $H_{2-2}(U^*,R_2^*,\Delta')$ 值为 $c^*\oplus(m\|R_1^*\|\mathrm{ID}_{A,1})$，并将 (U^*,R_2^*,Δ) 和 (U^*,R_2^*,Δ') 保存到 L_{2-2} 中。其中，“Δ”表示 CDH 问题实例 (P_2,R_2,PK_B) 的一个解。

阶段 2　F 和 A 如同“阶段 1”进行问答。当 A 提交 $(R_2^*,\mathrm{PK}_{B,0},\lambda)$ 询问时，如果等式 $e_2(P_2,\lambda)=e_2(R_2^*,\mathrm{PK}_{B,0})$ 成立，那么 F 输出 x^{-1},λ' 并停止。当 A 提交 $(R_2^*,\mathrm{PK}_{B,1},\lambda)$ 询问时，如果等式 $e_2(P_2,\lambda)=e_2(R_2^*,\mathrm{PK}_{B,1})$ 成立，那么 F 输出 y^{-1},λ' 并停止。如果 A 没有提交这些询问，则 F 随机输出 G_{1-1} 中的一个元素并终止。

猜测阶段　A 随机选择 $\gamma,\gamma'\in\{0,1\}$，F 忽略这个输出。下面分析 F 的优势。

由定理 2 可知 F 从不终止即模拟完美的概率至少为 $\left(1-q_u/2^{k_2}\right)$。定义 E_1 为“A 提交 $(U^*,R_2^*,V_{B,0})$ 或者 $(U^*,R_2^*,V_{B,1})$ 进行 H_{2-2} 询问”事件，则 $\overline{E_1}$ 为 A 没有提交 $(U^*,R_2^*,V_{B,0})$ 或 $(U^*,R_2^*,V_{B,1})$ 进行 H_{2-2} 询问”事件。定义 E_2 为“A 赢得游戏”事件，F 将在事件 E_1 发生的时候解决 CDH 困难问题。

假设 $h_{b,b'}=H_{1-2}(m,R_1^*)$，则 $W_{b,b'}=\dfrac{r_1+h_{b,b'}}{Q_{A,b}+s_1}P_1$。当 $H_{2-2}\left(U^*,R_2^*,\Delta\right)$ 为 $\left(m\|R_1^*\|\mathrm{ID}_{A,b}\right)$=$c^*\oplus H_{2-2}\left(U^*,R_2^*,\mathrm{PK}_{B,b'},V_{B,b'}\right)$ 时，$\delta^*=\left(c^*,R_2^*,W^*\right)$ 才是消息 m 在

私钥$S_{A,b}$和公钥$\mathrm{PK}_{B,b'}$下的密文。如果事件$\overline{E}_1$发生，A没有提交过$\left(U^*,R_2^*,V_{B,b'}\right)$进行询问，那么$A$没有任何优势确定询问的值。因此，$\Pr\left[E_2\left|\overline{E}_1\right.\right]=1/4$。

根据假设有$\Pr[E_2]=1/4+\varepsilon\le\Pr[E_1]+(1/4)(1-\Pr[E_1])$，则$\Pr[E_1]\ge\frac{4}{3}\varepsilon$，最终$\Pr[E_1\wedge E_2]\ge\frac{4}{3}\left(1-\frac{q_u}{2^{k_2}}\right)\varepsilon$。

4.4 效率分析

表 1 比较了本文方案与文献[10]方案的性能，其中，P表示双线性对运算数，e 表示幂运算数。文献[10]方案的运算量为 $6P+1e$；本文方案的运算量为 $4P+2e$，并且，其中 1 个对运算可以作为预运算处理，本文方案的效率更高。同时，本文方案满足密文匿名性，并且考虑了独立的密码系统参数，能够满足实际应用需求。

表 1 方案对比

方案	方向	预运算	签密	解签密	密文匿名
文献[10]	身份-无证书	$0P$	$1P+1e$	$5P+0e$	不满足
本文	无证书-身份	$1P$	$1P+1e$	$2P+1e$	满足

5 结束语

异构网络环境一般采用不同的公钥密码系统。异构签密可以保证异构网络环境消息的机密性和认证性。本文提出了可证安全的 IDPKC→CLPKC 异构签密方案，并且，证明该方案满足 IDPKC→CLPKC 异构签密的机密性、不可伪造性和匿名性。与已有同类方案相比，效率更高。已有的大多数异构签密方案的安全性是基于离散对数和大整数分解等困难假设，但是，它们无法抵抗量子计算机的攻击，因此，有必要研究抵抗量子攻击的异构签密方案[15]。这也将是我们下一步的研究内容。

参 考 文 献

[1] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]. Proceedings of the Cryptology-CRYPTO 1997, California, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[2] SUN Y X and LI H. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. *Science China Information Sciences,* 2010, 53(3): 557–566. doi: 10.1007/ s11432-010-0061-5.

[3] AN J H, DODIS Y, and RABIN T. On the security of joint signature and encryption[C]. Proceedings of the Cryptology-EUROCRYP2002, Berlin, 2002: 83–107. doi: 10.1007/3-540-46035-7_6.

[4] HUANG Q, WONG D S, and YANG G M. Heterogeneous signcryption with key privacy[J]. *Computer Journal*, 2011, 54(4): 525–536. doi: 10.1093/comjnl/bxq095.

[5] FU X T, LI X W, and LIU W. IDPKC-to-TPKI construction of multi-receiver signcryption[C]. Proceedings of the INCoS(5), Washington, USA, 2013: 335–339. doi: 10.1109/INCoS.2013.62.

[6] LI F G, ZHANG H, and TAKAGI T. Efficient signcryption for heterogeneous systems[J]. *IEEE Systems Journal*, 2013, 7(3): 420–429. doi: 10.1109/JSYST.2012.2221897.

[7] LI F G, HAN Y Y, and JIN C H. Practical signcryption for secure communication of wireless sensor networks[J]. *Wireless Personal Communications*, 2016, 89(4): 1–22. doi: 10.1007/s11277-016-3327-4.

[8] 张玉磊, 张灵刚, 张永洁, 等. 匿名 CLPKC-TPKI 异构签密方案[J]. 电子学报, 2016, 44 (10): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

ZHANG Y L, ZHANG L G, ZHANG Y J, *et al*. CLPKC-to-TPKI heterogeneous signcryption scheme with anonymity [J]. *Acta Electronica Sinica*, 2016, 44(10): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

[9] 周彦伟, 杨波, 张文政. 可证安全的高效无证书广义签密方案[J].计算机学报, 2016, 39(3): 543–551. doi: 10.11897/SP.J.1016.2016.00543.

ZHOU Y W, YANG B, and ZHANG W Z. Provably secure and efficient certificateless generalized signcryption[J]. *Chinese Journal of Computers*, 2016, 39(3): 543–551. doi: 10.11897/ SP.J.1016.2016.00543.

[10] LI F G, HAN Y Y, and JIN C H. Practical access control for sensor networks in the context of the Internet of Things[J]. *Computer Communications*, 2016, 89–90: 154–164. doi: 10.1016/j.comcom.2016.03.007.

[11] 张玉磊, 王欢, 李臣意, 等. 可证安全的紧致无证书聚合签密方案[J].电子与信息学报, 2015, 37(12): 2838–2844. doi: 10.11999 /JEIT150407.

ZHANG Y L, WANG H, LI C Y, *et al*. Provable secure and compact certificateless aggregate signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2015, 37(12): 2838–2844. doi: 10.11999/JEIT150407.

[12] BARBOSA M and FARSHIM P. Certificateless signcryption

[C]. Proceedings of ASIACCS 2008, Tokyo, 2008: 369–372. doi: 10.1145/1368310.1368364.

[13] POINTCHEVAL D and STERN J. Security arguments for digital dignatures and blind signatures[J]. *Journal of Cryptology*, 2001, 13(3): 361–396. doi: 10.1007/s001450010003.

[14] LI C K, YANG M, WONG D S, *et al*. An efficient signcryption scheme with key privacy and its extension to ring signcryption[J]. *Journal of Computer Security*, 2010, 18(3): 451–473. doi: 10.3233/JCS-2009-0374.

[15] 路秀华, 温巧燕, 王励成. 格上的异构签密[J]. 电子科技大学学报, 2016, 45(3): 458–462. doi: 10.3969/j.issn.1001-0548.2016.02.025.

LU X H, WEN Q Y, and WANG L C. A lattice-based heterogeneous signcryption[J]. *Journal of University of Electronic Science and Technology of China*, 2016, 45(3): 458–462. doi: 10.3969/j.issn.1001-0548.2016.02.025.

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.

张灵刚： 男，1990 年生，硕士生，研究方向为密码学与信息安全.

王彩芬： 女，1963 年生，博士，教授，博士生导师，研究方向为密码学与信息安全.

马彦丽： 女，1992 年生，硕士生，研究方向为密码学与信息安全.

张永洁： 女，1978 年生，硕士，副教授，研究方向为密码学与信息安全.