异构系统下的双向签密方案

刘景伟*　张俐欢　孙 蓉
(西安电子科技大学综合业务网理论及关键技术国家重点实验室　西安　710071)

摘　要：在过去的研究中，人们通常假设通信双方都处在同一个公钥密码体制环境中，但随着科技的发展和网络的普及，不同的地区可能采用不同的公钥密码体制。为了解决异构系统之间的通信安全问题，该文提出两种在公共密钥基础设施(PKI)和无证书公钥密码体制(CLC)下安全通信的异构签密方案。同时在双线性 Diffie-Hellman 问题(BDHP)和计算性 Diffie-Hellman 问题(CDHP)的难解性下，所提方案在随机预言模型中具有自适应选择密文攻击下的不可区分性(IND-CCA2)和自适应选择消息攻击下的不可伪造性(EUF-CMA)。

关键词：签密；异构系统；选择密文攻击；不可伪造性
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2016)11-2948-06
DOI: 10.11999/JEIT160056

Mutual Signcryption Schemes under Heterogeneous Systems

LIU Jingwei　ZHANG Lihuan　SUN Rong
(*State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: In the past studies, it is generally assumed that both sides of communication are in the same environment of public key cryptography, but with the development of technology and the popularity of the network, different regions may have different public key cryptographies. In order to resolve the communication security problem between heterogeneous systems, two signcryption schemes are proposed, which are used to achieve the communication security between the Public Key Infrastructure (PKI) and CertificatLess public key Cryptography (CLC) under heterogeneous systems. It is proved that the schemes have INDistinguishability against Adaptive Chosen Ciphertext Attacks (IND-CCA2) under Bilinear Diffie-Hellman Problem (BDHP) and Existential UnForgeability against adaptive Chosen Messages Attacks (EUF-CMA) under the Computational Diffie-Hellman Problem (CDHP) in the random oracle model.

Key words: Signcryption; Heterogeneous system; Chosen ciphertext attack; Unforgeability

1　引言

在传统公共密钥基础设施(PKI)系统中，通常存在一个可信认证中心 CA(Certification Authority)，CA 为每一个用户颁发一个与其公钥匹配的公钥证书，实现公钥认证，但这种方法会在证书管理上浪费大量的计算时间和存储空间。为了解决该问题，文献[1]提出了一种基于身份的公钥密码体制 IBC (Identity-Based Cryptosystem)。在 IBC 系统中，用户的私钥是由秘钥生成中心 KGC(Key Generation Center identity-based cryptosystem)生成，KGC 里存放的秘钥则是通过用户的身份生成用户的私钥。这种方法面临着密钥托管的问题。基于该问题，文献[2]提出了无证书公钥密码体制(CLC)。在 CLC 系统中，公钥由用户生成，私钥由用户选择的秘密值和 KGC 产生的部分私钥共同构成。KGC 无法得知用户的完整私钥，因此有效解决了上述的密钥托管问题。

如需同时实现保密性、完整性、认证性和不可否认性，传统的方法是先签署一份邮件，然后对它进行加密，称为“先签名后加密”。1997 年文献[3]首次提出了签密的概念，这个新的密码学原语在一个逻辑步骤内同时实现数字签名和公钥加密的功能，在成本上显著低于传统的先签名后加密方法。2002 年文献[4]提出了正式的签密安全模型。签密在许多应用中都可以发挥优势，如电子商务、移动通信和智能卡等。目前，虽然已经提出了很多基于 PKI

收稿日期：2016-01-13；改回日期：2016-06-09；网络出版：2016-09-01
*通信作者：刘景伟　jwliu@mail.xidian.edu.cn
基金项目：陕西省自然科学基础研究计划 (2016JM6057)，国家科技重大专项(2013ZX03005007)，高等学校学科创新引智计划(B08038)
Foundation Items: The Natural Science Basic Research Plan in Shaanxi Province of China (2016JM6057), The National Science and Technology Major Project of the Ministry of Science and Technology of China (2013ZX03005007), The 111 Project (B08038)

的签密方案[5−8]和基于 CLC 的签密方案[9−15]，但这些方案不能用于异构密码系统间的通信。为了确保异构系统间的安全通信，本文提出了两种异构系统下的签密方案，实现了 PKI 和 CLC 这两个公钥密码系统间的安全通信。

目前已经提出的针对异构通信的签密方案主要有以下几种：2010 年文献[16]提出了一方属于 PKI，另一方属于 IBC 的异构签密机制，但他们的方案只能抵抗外来攻击者，并不能满足不可否认性；2011 年文献[17]提出了发送端属于 PKI，接收端属于 IBC 的异构签密方案，但该方案只允许在 PKI 系统的用户发送消息，在 IBC 系统的用户接收消息，并不能完成双向的安全通信；2013 年文献[18]提出了两个异构签密方案，第 1 个方案是 PKI 中的发送端给基于 IBC 中的接收端发送消息，第 2 个方案是基于 IBC 的发送端给 PKI 中的接收端发送消息。在上述签密方案中，并没有适用于 PKI 和 CLC 异构系统间安全通信的签密方案，因此本文提出了两个适用于 PKI 和 CLC 异构系统间的签密方案 PCHS (PKI-CLC Heterogeneous System)和 CPHS(CLC-PKI Heterogeneous System)。

2　预备知识与安全模型

在本节中简要地描述了文中涉及到的困难性问题，并给出了所提方案对应的安全模型。

2.1 困难性问题

(1)Bilinear Diffie-Hellman(BDH)问题：给定 $(P,aP,bP,cP)(a,b,c\in Z_q^*)$，计算 $w=e(P,P)^{abc}\in G_2$，其中 e 是一个双线性映射，P 是 G_1 的生成元，G_1，G_2 是阶为素数 q 的两个群。

(2)Computational Diffie-Hellman(CDH)问题：给定 $(P,aP,bP)\in G_1,(a,b\in Z_q^*)$，计算 $abP\in G_1$。

2.2 PCHS 安全模型：

本文在其安全模型中考虑两类敌手。第 1 类敌手无法获得 KGC 的主密钥 s，但能够自适应地替换用户的公钥；第 2 类敌手无法替换用户的公钥，但可以获得 KGC 的主密钥 s[19]。

定 义 1　若任何概率时间多项式有界的两类敌手赢得 IND-CCA2 的优势可忽略，则称该方案满足自适应选择密文攻击下的不可区分性。

IND-CCA2-1：初始化：挑战者 $\mathcal{C}$ 产生系统参数 pa 和主密钥 s，保留 s，返回 pa 给敌手 $\mathcal{A}_{\mathrm{I}}$。

阶段 1：$\mathcal{A}_{\mathrm{I}}$ 进行多项式有界次适应性询问。

公钥询问：某用户进行公钥询问，$\mathcal{C}$ 执行相应算法，将 PK 返回。

部分私钥询问：某用户进行部分私钥询问，$\mathcal{C}$ 执行相应算法，将部分私钥 D 返回。

私钥询问：某用户进行私钥询问，$\mathcal{C}$ 从相关的询问列表中找到完整私钥，将 SK 返回。

公钥替换：$\mathcal{A}_{\mathrm{I}}$ 可在规定范围内，任意选择某值对用户公钥进行替换。

签密询问：进行签密询问时，$\mathcal{C}$ 从相关“询问与应答”表中检索 $(\mathrm{SK}_a,\mathrm{PK}_b)$，返回密文 $\sigma\leftarrow\mathrm{Signcrypt}(pa,u_a,u_b,m,\mathrm{SK}_a,\mathrm{PK}_b)$。

解签密询问：进行解签密询问时，$\mathcal{C}$ 从相关“询问应答”表中检索 $(\mathrm{SK}_b,\mathrm{PK}_a)$，返回 $m/\perp\leftarrow\mathrm{Unsigncrypt}(pa,u_a,u_b,m,\mathrm{SK}_b,\mathrm{PK}_a)$。

挑战：在阶段 1 后，$\mathcal{A}_{\mathrm{I}}$ 生成两个相同长度的明文 m_0,m_1 以及希望挑战的接收者的身份 u_b^*，在阶段 1 中 u_b^* 的公钥不能被替换且不能询问 u_b^* 的部分私钥和秘密值。$\mathcal{A}_{\mathrm{I}}$ 从相关“询问与应答”表中找到 $(\mathrm{SK}_a^*,\mathrm{PK}_b^*)$，选择 $\gamma\in\{0,1\}$，计算 $\sigma^*\leftarrow\mathrm{Signcrypt}(pa,u_a^*,u_b^*,m_\gamma,\mathrm{SK}_a^*,\mathrm{PK}_b^*)$。返回挑战密文 σ^*。

阶段 2：$\mathcal{A}_{\mathrm{I}}$ 进行多项式有界次适应性询问，约束条件是：(1) u_b^* 的完整私钥不能被询问；(2) u_b^* 不能是公钥已被替换的那个身份；(3)不能对 u_a^* 和 u_b^* 下的 σ^* 进行解签密询问。

猜测：$\mathcal{A}_{\mathrm{I}}$ 输出一个猜测 γ^*，若 $\gamma^*=\gamma$，$\mathcal{A}_{\mathrm{I}}$ 赢得 IND-CCA2-1。我们定义 $\mathcal{A}_{\mathrm{I}}$ 的获胜优势为 $\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}^{\mathrm{IND\text{-}CCA2-1}}=\left|2\Pr[\gamma^*=\gamma]-1\right|$。

IND-CCA2-2：初始化：挑战者 $\mathcal{C}$ 产生系统参数 pa 和主密钥 s，返回 (pa,s) 给 $\mathcal{A}_{\mathrm{II}}$。

阶段 1，挑战和阶段 2：与上相似。因为 $\mathcal{A}_{\mathrm{II}}$ 知道主密钥 s，但无法进行公钥替换，它能够计算出用户的部分私钥因此无需进行公钥替换和部分私钥询问。

猜测：$\mathcal{A}_{\mathrm{II}}$ 输出一个猜测 γ^*，若 $\gamma^*=\gamma$，$\mathcal{A}_{\mathrm{II}}$ 赢得 IND-CCA2-2。我们定义 $\mathcal{A}_{\mathrm{II}}$ 的获胜优势为 $Adv_{\mathcal{A}_{\mathrm{II}}}^{\mathrm{IND-CCA2-2}}=\left|2\Pr[\gamma^*=\gamma]-1\right|$。

定 义 2　若任何概率时间多项式有界的伪造者赢得 EUF-CMA 的优势是可忽略的，则称方案满足在自适应选择消息攻击下的不可伪造性。

EUF-CMA：初始化：挑战者 $\mathcal{C}$ 产生系统参数 pa 和主密钥 s，保留 s，返回 pa 给敌手 $\mathcal{F}$。

训练：$\mathcal{F}$ 进行适应性多项式有界次询问。

伪造：在上述阶段后，$\mathcal{F}$ 输出一个伪造 (σ^*,u_a^*,u_b^*)。训练期间 u_a^* 的私钥不能被询问。伪造者对发送者 u_a^* 和接收者 u_b^* 下某消息签密询问的应答不能是 σ^*。如果 $\mathrm{Unsigncrypt}(pa,\sigma^*,u_a^*,u_b^*,m_\gamma,\mathrm{SK}_b^*,\mathrm{PK}_a^*)$ 不是符号 $\perp$，$\mathcal{F}$ 赢得 EUF-CMA。

$\mathcal{F}$ 获胜的优势定义为 $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{SUF\text{-}CMA\text{-}1}}=\left|\Pr[\mathrm{win}]\right|$。

CPHS 方案的安全模型与 PCHS 方案类似。

3 具体方案描述

在本节中，我们提出了两个适用于 PKI 和 CLC 异构系统间的签密方案 PCHS 和 CPHS。

令 G_1 和 G_2 分别是素数阶 $\geq 2^{\beta}$ (β 为安全参数) 的加法群和乘法群，P 是 G_1 的一个生成元，$e: G_1 \times G_2 \to G_2$ 是一个双线性映射。KGC 定义 3 个密码学杂凑函数：$H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^n \times \{0,1\}^n \to Z_q^*$，$H_3: G_2 \to \{0,1\}^n$ 和 $H_4: \{0,1\}^n \to \{0,1\}^n$。$n$ 表示要被签密的消息的长度。$\{0,1\}^n$ 表示比特长度为 n 的二进制序列组成集合，Z_q^* 表示有限域 $Z_q = \{0,1,2,\cdots,q-1\}$ 去掉元素零所得到的集合。密钥生成中心随机选择 $s \in Z_q^*$ 作为主控钥，计算系统公钥 $P_{\text{pub}} = sP$。最后，KGC 保密主密钥 s，公布系统参数 $pa\{G_1, G_2, n, e, P, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$。

CLC-KG:

部分私钥提取：算法输入系统参数 pa，主密钥 s 以及用户身份 ID 并执行以下步骤：

计算 $Q = H_1(\text{ID}) \in G_1$；输出部分私钥 $D = sQ \in G_1$。

设置秘密值：算法输入系统参数 pa 和用户身份 ID，随机选择 $x_c \in Z_q^*$ 作为秘密值。

设置私钥：算法输入 pa，用户身份 ID，部分私钥和秘密值，输出 $\text{SK}_c = x_c sQ$ 作为私钥。

设置公钥：算法输入 pa，用户身份 ID 和秘密值，返回 $\text{PK}_c = x_c Q$ 作为公钥。

PKI-KG：

PKI 用户随机选择一个数 $x_p \in Z_q^*$ 为私钥 SK_p，$x_p P$ 作为公钥 PK_p。

PCHS 签密过程：已知明文 m, CLC 系统的公钥 PK_c 和 PKI 系统的私钥 SK_p

(1)选随机数 $k \in Z_q^*$；

(2)计算 $r = H_2(k, m)$，$f = e(P_{\text{pub}}, \text{PK}_c)^r$；

(3)计算 $U_1 = rP$，$U_2 = k + H_3(e(P_{\text{pub}}, \text{PK}_c)^r) = k + H_3(f)$，$U_3 = m + H_4(k)$；

(4)计算 $S = \big(r + \text{SK}_p H_1(m)\big) \bmod n$；

(5)密文是 $\sigma = (S, U_1, U_2, U_3)$。

解签密过程：已知密文 $\sigma = (S, U_1, U_2, U_3)$，CLC 系统的私钥 SK_c 和 PKI 系统的公钥 PK_p。

(1)计算 $k = U_2 - H_3(e(\text{SK}_c, U_1))$；

(2)计算 $m = U_3 - H_4(k)$；

(3)计算 $r = H_2(k, m)$；

(4)$V = SP - H_1(m)\text{PK}_p$。

验证 V 与 $rP(U_1)$ 是否相等：

$$
\begin{aligned}
&H_3\big(e\big(\text{SK}_c, U_1\big)\big) \\
&\quad = H_3\big(e\big(x_c sQ, rP\big)\big) = H_3\big(e\big(x_c Q, sP\big)^r\big) \\
&\quad = H_3\big(e\big(\text{PK}_c, P_{\text{pub}}\big)^r\big) = H_3\big(e\big(P_{\text{pub}}, \text{PK}_c\big)^r\big)
\end{aligned}
$$

即

$$
\begin{aligned}
k &= U_2 + H_3(e(\text{SK}_c, U_1)) \\
V &= SP - H_1(m)\text{PK}_p = \big(r + \text{SK}_p H_1(m)\big)P - x_p P \\
&= rP + x_p H_1(m)P - x_p H_1(m)P = rP = U_1,
\end{aligned}
$$

验证成功。

CPHS：签密过程：已知明文 m，CLC 系统的私钥 SK_c 和 PKI 系统的公钥 PK_p。

(1)选随机数 $k \in Z_q^*$；

(2)计算 $r = H_2(k, m)$　$f = e(P_{\text{pub}}, \text{PK}_p)^r$；

(3)计算 $U_1 = rP$，$U_2 = k + H_3(e(P_{\text{pub}}, \text{PK}_p)^r) = k + H_3(f)$，$U_3 = m + H_4(k)$；

(4)计算 $S = \big(r + H_1(m)\text{SK}_c\big) \bmod n$；

密文是 $\sigma = (S, U_1, U_2, U_3)$。

解签密过程：已知密文 $\sigma = (S, U_1, U_2, U_3)$，CLC 系统的公钥 PK_c 和 PKI 系统的私钥 SK_p。

(1) 计算 $k = U_2 + H_3(e(\text{SK}_p P_{\text{pub}}, U_1))$；

(2) 计算 $m = U_3 + H_4(k)$；

(3) 计算 $r = H_2(k, m)$；

(4) 计算 $V = SP - H_1(m)\text{PK}_c P_{\text{pub}}$。

验证 V 与 $rP(U_1)$ 是否相等：

$$
\begin{aligned}
&H_3\Big(e\big(\text{SK}_p P_{\text{pub}}, U_1\big)\Big) \\
&\quad = H_3\Big(e\big(sx_p P, rP\big)\Big) = H_3\Big(e\big(x_p P, sP\big)^r\Big) \\
&\quad = H_3\Big(e\big(\text{PK}_p, P_{\text{pub}}\big)^r\Big) = H_3\Big(e\big(P_{\text{pub}}, \text{PK}_p\big)^r\Big)
\end{aligned}
$$

即

$$
\begin{aligned}
k &= U_2 + H_3(e(\text{SK}_p P_{\text{pub}}, U_1)) \\
V &= SP - H_1(m)\text{PK}_c P_{\text{pub}} \\
&= (r + \text{SK}_c H_1(m))P - x_c H_1(m) QsP \\
&= rP + x_c H_1(m) QsP - x_c H_1(m) QsP \\
&= rP = U_1,
\end{aligned}
$$

验证成功。

4 安全性证明

在本节中，我们对所提出方案的安全性进行证明。

定理 1(PKI - CLC IND-CCA2-1) 假设存在一个 IND-CCA2-1 敌手 $\mathcal{A}_{\text{I}}$。经过 q_i 询问 $(i = 1,2,3,4)$，q_{e_1} 次 CLC 部分私钥询问，$q_{e_{2c}}$ 次 CLC 私钥询问和 q_{r_c} 次 CLC 公钥替换询问后，能以一个不可忽略的优势 ξ 攻破 PCHS 方案的 IND-CCA2-1 安全性，则存在一个挑战者 $\mathcal{C}$ 能以优势 ξ^* 解决 BDH 问题，这里 ξ^* 为：$\xi(1 - q_{e_1}/q_1)(1 - q_{e_{2c}}/q_1)(1 - q_{r_c}/q_1)(1/q_1 - q_{e_1} - q_{e_{2c}} - q_{r_c})(1/q_3)$。

证明 假设 $\mathcal{C}$ 收到一个 BDH 问题实例 $\langle P, aP, bP, cP\rangle (a, b, c \in Z_q^*)$，该问题的目标是计算出 $\varpi = e(P, P)^{abc} \in G_2$。为完成该目标，在游戏中把 $\mathcal{A}_{\text{I}}$ 作为子程序，$\mathcal{C}$ 作为挑战者与其进行交互；$\mathcal{A}_{\text{I}}$ 询问

以身份 ID_i 作为输入的其它预言机之前都先用身份 ID_i 询问 H_1 预言机。

初始化：$\mathcal{C}$ 运行初始化算法返回系统参数 $pa\{G_1,G_2,n,e,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4\}$ 给 $\mathcal{A}_{\mathrm{I}}$。为避免对 $\mathcal{A}_{\mathrm{I}}$ 的询问的非连续应答，$\mathcal{C}$ 维护起初为空的列表 $\mathrm{L}_1 \sim \mathrm{L}_4$，$\mathrm{LK}_p$ 和 LK_c。

阶段 1：$\mathcal{A}_{\mathrm{I}}$ 执行多项式有界次适应性询问。

H_1 询问：$\mathcal{A}_{\mathrm{I}}$ 选择一系列身份询问相应杂凑值。接收到身份 ID_i 的 H_1 询问时，若 L_1 中含有 (ID_i,Q_i,l_i)，$\mathcal{C}$ 返回 h_i 作为应答；否则，$\mathcal{C}$ 任选整数 $\alpha \in [1,2,\cdots,q_1]$，在不泄露 α 具体数值的情况下，将 ID_α 作为挑战身份发送给 $\mathcal{A}_{\mathrm{I}}$，若收到第 α 次询问，$\mathcal{C}$ 设置 $Q_i = b_1 P$，返回 Q_i，添加 $(\mathrm{ID}_i,Q_i,-)$ 到 L_1. 如果接收到的不是第 α 次询问，选择一个随机数 $l_i \in Z_q^*$，返回 $Q_i = l_i P$，添加 (ID_i,Q_i,l_i) 到 L_1。

H_2 询问：进行 H_2 询问时，比对列表 L_2 中是否存在 (k,m,r)。若存在，返回 r；否则，返回任意的 $r \in Z_q^*$，添加 (k,m,r) 到 L_2。

H_3 询问：进行 H_3 询问时，比对列表 L_3 中是否存在 (f,h_3)。若存在，返回 h_3；否则，返回任意的 $h_3 \in \{0,1\}^n$，添加 (f,h_3) 到 L_3。

H_4 询问：进行 H_4 询问时，比对列表 L_4 中是否存在 (k,h_4)。若存在，返回 h_4；否则，返回任意的 $h_4 \in \{0,1\}^n$，添加 (k,h_4) 到 L_4。

CLC 公钥询问：身份 ID_i 进行公钥询问时，$\mathcal{C}$ 核对 ID_i 和 ID_α。若两者相等，$\mathcal{C}$ 返回公钥 $\mathrm{PK}_i = bP$；若不相等，调用列表 L_1 (ID_i,Q_i,l_i)，任选随机数 $x_i \in Z_q^*$，计算出 $\mathrm{PK}_i = x_i Q_i$，返回公钥 PK_i 并且在 LK_c 中添加 $(\mathrm{ID}_i,-,x_i,Q_i,\mathrm{PK}_i)$。

CLC 部分私钥询问：身份 ID_i 进行部分私钥询问时，$\mathcal{C}$ 核对 ID_i 和 ID_α。若两者相等，$\mathcal{C}$ 放弃游戏；若不相等，$\mathcal{C}$ 调用 H_1 预言机得到 l_i，$d_i = l_i aP$，将 $(\mathrm{ID}_i,d_i,x_i,Q_i,\mathrm{PK}_i)$ 添加到 LK_c 中并返回部分私钥 d_i。

PKI 私钥询问：身份 ID_i 进行私钥询问时，$\mathcal{C}$ 从 LK_p 得到 $(\mathrm{ID}_i,x_i,\mathrm{PK}_i)$，返回 $s_i = x$。

CLC 私钥询问：身份 ID_i 进行私钥询问时，$\mathcal{C}$ 核对 ID_i 和 ID_α。若两者相等，$\mathcal{C}$ 放弃游戏；若不相等，r 从 LK_c 得到 $(\mathrm{ID}_i,d_i,x_i,Q_i,\mathrm{PK}_i)$ 并返回 $s_i = d_i x_i$。

CLC 公钥替换：在规定范围内，$\mathcal{A}_{\mathrm{I}}$ 任选随机数 PK_i^* 把身份 ID_i 的公钥替换为 PK_i。若 ID_i 和 ID_α 相等，$\mathcal{C}$ 放弃游戏；若不相等，将 $(\mathrm{ID}_i,d_i,x_i,Q_i,\mathrm{PK}_i^*)$ 添加到 LK_c 中。

签密：进行签密询问时，$\mathcal{C}$ 核对 $\mathrm{ID}_{发}$ 和 ID_α。若两者相等，$\mathcal{C}$ 运行签密算法并返回结果；否则，$\mathcal{C}$ 从 LK_p 和 LK_c 直接检索到 $(x_p,x_c,Q_c,\mathrm{PK}_c)$，生成密文。

解签密：进行解签密询问时，$\mathcal{C}$ 核对 $\mathrm{ID}_{收}$ 和 ID_α。若两者相等，$\mathcal{C}$ 运行解密算法并返回结果；否则，$\mathcal{C}$ 从 LK_p 和 LK_c 直接检索到 $(x_c,d_c,x_p,\mathrm{PK}_p)$，并做出应答。

挑战：阶段 1 后，$\mathcal{A}_{\mathrm{I}}$ 生成两个相同长度的明文 m_0,m_1 以及希望挑战的接收者的身份 ID_c^*。在阶段 1 中 ID_c^* 的公钥不能被替换且不能询问它的部分私钥和秘密值，若 $\mathrm{ID}_c^* \neq \mathrm{ID}_\alpha$，$\mathcal{C}$ 放弃游戏；否则，$\mathcal{C}$ 从 LK_p 和 LK_c 直接检索到 $(x_p,x_c,Q_c,\mathrm{PK}_c)$ 并计算挑战密文。

阶段 2：$\mathcal{A}_{\mathrm{I}}$ 进行多项式有界次适应性询问，但不能对发送者身份 ID_p^* 和接收者身份 ID_c^* 下的密文 σ^* 进行解签密询问。

猜测：L_3 中储存有 q_3 个杂凑值，$\mathcal{C}$ 从 L_3 中随机等概率地选择 f^*。

输出 $f^* = e(P_{\mathrm{pub}},\mathrm{PK}_c^*)^c = e(aP,bP)^c = e(P,P)^{abc}$ 作为 BDH 问题实例的应答。

概率分析：这一部分讨论 $\mathcal{C}$ 成功解答出 BDH 问题实例 $e(P,P)^{abc}$ 的概率。根据上述的讨论得知，以下 4 种情况会使 $\mathcal{C}$ 放弃游戏：(1) $\mathcal{A}_{\mathrm{I}}$ 以概率 q_{e_1}/q_1 对挑战身份 ID_α 的部分私钥进行询问。(2) $\mathcal{A}_{\mathrm{I}}$ 以概率 $q_{e_{2c}}/q_1$ 对挑战身份 ID_α 的秘密值进行询问。(3) $\mathcal{A}_{\mathrm{I}}$ 以概率 q_{r_c}/q_1 对挑战身份 ID_α 的公钥进行替换。(4)在挑战阶段，$\mathcal{A}_{\mathrm{I}}$ 以概率 $(1-1/q_1-q_{e_1}-q_{e_{2c}}-q_{r_c})$ 选择挑战身份不是 ID_α 的接收者。只有在挑战者不放弃游戏的情况下，才能解决 BDH 问题。于是，$\mathcal{C}$ 不放弃游戏的概率为

$$\left(1-q_{e_1}/q_1\right)\left(1-q_{e_{2c}}/q_1\right)\left(1-q_{r_c}/q_1\right)\left(1/q_1-q_{e_1}-q_{e_{2c}}-q_{r_c}\right)$$

$\mathcal{C}$ 等概率地从 L_3 中任选出 f^* 的概率为 $(1/q_3)$。综上，$\mathcal{C}$ 解决 BDH 问题的优势 ξ^* 为 $\xi\left(1-q_{e_1}/q_1\right)\left(1-q_{e_{2c}}/q_1\right)\left(1-q_{r_c}/q_1\right)\left(1/q_1-q_{e_1}-q_{e_{2c}}-q_{r_c}\right)(1/q_3)$。

证毕

定理 2 (PKI- CLC IND-CCA2-2) 假设存在一个 IND-CCA2-2 敌手 $\mathcal{A}_{\mathrm{II}}$，定义同上，其中 ξ^* 为：$\xi\left(1-q_{e_{2c}}/q_1\right)\left(1/q_1-q_{e_{2c}}\right)\left(1/q_3\right)$。

证明 初始化：阶段 2 与 PKI-CLC IND-CCA2-1 相似，因为第 2 类攻击者知道 KGC 的主密钥，但不具备替换任意用户公钥的能力，所以阶段 1 无需进行公钥替换询问。

概率分析：这一部分讨论 $\mathcal{C}$ 成功解答出 BDH 问题实例 $e(P,P)^{abc}$ 的概率。在阶段 1 中不能询问 ID_c^* 的私钥，并且不能对发送者身份 ID_p^* 和接收者身份 ID_c^* 下的密文 σ^* 进行解签密询问。以下两种情况会使 $\mathcal{C}$ 放弃游戏：

(1) $\mathcal{A}_{\mathrm{II}}$ 以概率 $q_{e_{2c}}/q_1$ 对挑战身份 ID_α 的秘密值进行询问。(2)在挑战阶段，$\mathcal{A}_{\mathrm{II}}$ 以概率 $(1-1/q_1-q_{e_{2c}})$ 选择挑战身份不是 ID_α 的接收者。于是，$\mathcal{C}$ 不放弃游戏的概率为 $\left(1-q_{e_{2c}}/q_1\right)\left(1/q_1-q_{e_{2c}}\right)$。

$\mathcal{C}$ 等概率得从 L_3 中任选出 f^* 的概率为 $(1/q_3)$。综上，$\mathcal{C}$ 解决 BDH 问题的优势 ξ^* 为 $\xi(1-q_{e_{2c}}/q_1)(1/q_1-q_{e_{2c}})(1/q_3)$。 证毕

定理 3 (PKI-CLC EUF-CMA) 假设存在一个 EUF-CMA 伪造者 $\mathcal{F}$，经过 q_i 询问 $(i=1,2,3,4)$，q_{e_1} 次部分私钥询问，$q_{e_{2c}}$ 次 CLC 私钥询问和 q_{r_c} 次 CLC 公钥替换询问后，能以一个不可忽略的优势 ξ 攻破 PCHS 方案的 EUF-CMA 安全性，则存在一个挑战者 $\mathcal{C}$ 能以优势 ξ^* 解决 CDH 问题，这里 ξ^* 为：$\left(\xi-2^{\beta}\right)\left(1-q_{e_{2c}}/q_1\right)\left(1/q_1-q_{e_{2c}}\right)$。

证明 假设 $\mathcal{C}$ 收到一个 CDH 问题的随机实例 $\langle P,aP,bP\rangle\in G_1$，该问题的目标是计算出 $abP\in G_1$。为完成该目标，在游戏中把 $\mathcal{F}$ 作为子程序，$\mathcal{C}$ 作为挑战者与其进行交互。$\mathcal{F}$ 询问以身份 ID_i 作为输入的其它预言机之前都先用身份 ID_i 询问 H_1 预言机。

初始化：$\mathcal{C}$ 运行初始化算法返回系统参数 $pa\{G_1,G_2,n,e,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4\}$ 给 $\mathcal{F}$。为避免对 $\mathcal{F}$ 的询问的非连续应答，$\mathcal{C}$ 维护起初为空的列表 $\mathrm{L}_1\sim\mathrm{L}_4$，$\mathrm{LK}_p$ 和 LK_c。

训练：H_1 询问：$\mathcal{F}$ 选择一系列身份询问相应杂凑值。接收到身份 ID_i 的 H_1 询问时，若 L_1 中含有 (ID_i,Q_i,l_i)，$\mathcal{C}$ 返回 h_i 作为应答；否则，$\mathcal{C}$ 任选整数 $\alpha\in[1,2,\cdots,q_1]$，在不泄露 α 具体数值的情况下，将 ID_α 作为挑战身份发送给 $\mathcal{F}$，若收到第 α 次询问，$\mathcal{C}$ 设置 $Q_i=bP$，返回 Q_i，添加 $(\mathrm{ID}_i,Q_i,-)$ 到 L_1。如果接收到的不是第 α 次询问，选择一个随机数 $l_i\in Z_q^*$，返回 $Q_i=l_iP$，添加 (ID_i,Q_i,l_i) 到 L_1。

H_2~H_4 同 PKI -CLC IND-CCA2-1。

伪造：训练结束后，$\mathcal{F}$ 输出一个伪造 $(\sigma^*,\mathrm{ID}_p^*,\mathrm{ID}_c^*)$。训练期间不能询问 ID_p^* 的私钥，伪造者对发送者 ID_p^* 和接收者 ID_c^* 下的某消息签密询问的应答不能是 σ^*。若 $\mathrm{ID}_p^*\neq\mathrm{ID}_\alpha$，$\mathcal{C}$ 放弃游戏；若相等，$\mathcal{C}$ 调用 H_1, H_2 预言机和 LK_p 得到 $Q_p^*=bP$, r 和 PK_p^*；输出 $abP=(S-r)P_{\mathrm{pub}}\,Q_p^*/\mathrm{PK}_p^*$ 作为应答。

概率分析：讨论 $\mathcal{C}$ 解决 CDH 问题的成功概率。参考定理 1 可得：(1) $\mathcal{F}$ 以概率 $q_{e_{2c}}/q_1$ 对挑战身份 ID_α 的密钥进行询问。(2)在挑战阶段，$\mathcal{F}$ 以概率 $\left(1-1/q_1-q_{e_{2c}}\right)$ 选择挑战身份不是 ID_α 的接收者。于是，$\mathcal{C}$ 不放弃游戏的概率为 $(1-q_{e_{2c}}/q_1)(1/q_1-q_{e_{2c}})$。$\mathcal{F}$ 猜测相关 H_2 预言机相应的哈希值的概率是 $1/2^{\beta}$，因此，$\mathcal{C}$ 解决 BDH 问题的优势 ξ^* 为：$(\xi-2^{\beta})(1-q_{e_{2c}}/q_1)(1/q_1-q_{e_{2c}})$。 证毕

CLC-PKI 的安全性证明与上述方案类似。

5 效率分析

本小节对各异构签密方案的性能进行分析，假设 $|G_1|$=160 b, $|G_2|$=1024 b, $|m|$=160 b, |ID|=160 b。PKI 指该签密方案是在公钥基础设施环境下工作的；IBC 指该签密方案是在基于身份的公钥密码环境下工作的；CLC 指该签密方案是在无证书环境下工作的；箭头代表该方案是异构的签密方案，BP 表示双线性对运算；EXPC 表示幂指数运算；SCM 标量乘运算；密文长度表示通信开销。

从表 1 可以看出，文献[16]虽有较低的计算开销但并不能满足 EUF-CMA 安全性使得该方案存在安全隐患问题；文献[17]虽可以满足安全性但密文长度过大且标量乘运算过多使得所需要的通信开销和计算消耗都变大；文献[18]的通信开销虽小但其标量乘运算较多则计算消耗也随之上升；本文方案的通信开销虽并非最小，但在严格保证了方案的安全性下只需计算两次标量乘具有较低的计算复杂度，可在实际应用中节省更多的时间和精力。在应用方向上，前 3 类方案解决的都是 PKI 和 IBC 系统间的异构安全通信问题，方案则应用在 PKI 和 CLC 系统间，具有创新性。因此综合计算消耗，安全性，通信开销，应用方向等各方面的因素考虑本文方案的性能后，可看出本文方案在整体性能中具有的优越性和创新性。

6 结束语

本文提出了两种异构系统下的签密方案，用于公钥基础设施环境(PKI)和无证书公钥密码环境(CLC)这两个公钥密码系统间的安全通信。这两个方案都只需 2 个线性对运算、2 个标量乘运算和 1

表 1 各签密方案性能对比

方案	方向	计算消耗			安全性		密文长度(bit)
		BP	EXPC	SCM	IND-CCA	EUF-CMA	
文献[16]	PKI→IBC	4	1	2	√	√	640
文献[16]	IBC→PKI	2	1	0	√	–	640
文献[17]	IBC→PKI	2	0	5	√	√	960
文献[17]	IBC→PKI	0	0	6	√	√	960
文献[18]	PKI→IBC	2	2	3	√	√	480
文献[18]	IBC→PKI	2	2	3	√	√	480
PCHS	PKI→CLC	2	1	2	√	√	640
CPHS	CLC→PKI	2	1	2	√	√	640

个幂指数运算，相比于之前提出的方案，具有较低的计算复杂度；同时在双线性 Diffie-Hellman 问题(BDHP)和计算性 Diffie-Hellman 问题(CDHP)的难解性下，所提方案在随机预言模型中具有自适应选择密文攻击下的不可区分性(IND-CCA2)和自适应选择消息攻击下的不可伪造性(EUF-CMA)。这两个方案也可应用于电子商务、网上支付、移动互联和智能卡等领域。

参 考 文 献

[1] SHAMIR A. Identity-based cryptosystem and signature scheme [C]. Proceedings of CRYPTO 84 on Advances in cryptology, New York, NY, USA, 1984, 196: 47–53. doi: 10.1007/3-540-39568-7_5 .

[2] AL-RIYAMI S S and PATERSON K G. Certificateless public key cryptography[C]. 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.

[3] ZHENG Yuliang. 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

[4] BAEK J, STEINFELD R, and ZHENG Yuliang. Formal proofs for the security of signcryption[C]. Proceedings of the Cryptology PKC2002, Paris, France, 2002: 81–98. doi: 10.1007/3-540-45664-3_6.

[5] CH A S, UDDIN N, SHER M, *et al*. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography [J]. *Multimedia Tools and Applications*, 2015, 74(5): 1711–1723. doi: 10.1007/s11042-014-2283-9.

[6] LI C K, YANG G, WONG D S, *et al*. An efficient signcryption scheme with key privacy[C]. Proceedings of the 4th European Public Key Infrastructure Workshop (EuroPKI 2007), Palma de Mallorca, Spain, 2007, 4582: 78–93. doi: 10.1007/978-3-540-73408-6_6.

[7] QIN Bo, WANG Huaqun, WU Qianhong, *et al*. An simultaneous authentication and secrecy in identity-based data upload to cloud[J]. *Cluster Computing*, 2013, 16(4): 845–859. doi: 10.1007/s10586-013-0258-7.

[8] PANG Liaojun, GAO Lu, LI Huixian, *et al*. Anonymous multi-receiver ID-based signcryption scheme[J]. *Information Security*, 2015, 9(3): 193–201. doi: 10.1049/iet-ifs.2014.0360.

[9] BARBOSA M and FARSHIM P. Certificateless signcryption [C]. Proceedings of the ASIACCS2008, New York, USA, 2008: 369–372. doi: 10.1145/1368310.1368364.

[10] 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): 2839–2844. doi: 10.11999/JEIT150407.
ZHANG Yulei, WANG Huan, LI Chenyi, *et al*. Provable secure and compact certificateless aggregate signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2015, 37(12): 2839–2844. doi: 10.11999/JEIT150407.

[11] 孙银霞, 李晖, 李小青. 无证书体制下的多接收者签密密钥封装机制[J]. 电子与信息学报, 2010, 32(9): 2249–2252. doi: 10.3724/SP. J.1146.2009.01260.
SUN Yinxia, LI Hui, and LI Xiaoqing. Certificateless signcryption KEM to multiple recipients[J]. *Journal of Electronics & Information Technology*, 2010, 32(9): 2249–2252. doi: 10.3724/SP.J.1146.2009.01260.

[12] 葛爱军, 陈少真. 具有强安全性的不含双线性对的无证书签名方案[J]. 电子与信息学报, 2010, 32(7): 1766–1768. doi: 10.3724/SP.J.1146.2009.00965.
GE Aijun and CHEN Shaozhen. Strongly secure certificateless signature scheme without pairings[J]. *Journal of Electronics & Information Technology*, 2010, 32(7): 1766–1768. doi: 10.3724/SP.J.1146.2009.00965.

[13] ESLAMI Z and PAKNIAT N. Certificateless aggregate signcryption: security model and a concrete construction secure in the random oracle model[J]. *Journal of King Saud University-Computer and Information Sciences*, 2014, 26(3): 276–286. doi: 10.1016/j.jksuci.2014.03.006.

[14] YIN A and LIANG H. Certificateless hybrid signcryption scheme for secure sommunication of wireless sensor networks [J]. *Wireless Personal Communications*, 2015, 80(3): 1049–1062. doi: 10.1007/s11277-014-2070-y.10.

[15] HAFIZUL ISLAM S K and LI Fagen. Leakage-free and provably secure certificateless signcryption scheme using bilinear pairings[J]. *The Computer Journal*, 2015, 58(10): 2636–2648. doi: 10.1093/comjnl/bxv002.

[16] SUN Yinxia and LI Hui. Eifficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. *Secience China Information Sciences*, 2010, 53(3): 557–566. doi: 10.1007/s11432-010-0061-5.

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

[18] LI Fagen, ZHANG Hui, and TAKAGI T. Efficient signcryption for heterogeneous systems[J]. *IEEE Systems Journal*, 2013, 7(3): 420–429. doi: 1109/JSYST.2012.2221897.

[19] 俞惠芳, 杨波. 可证安全的无证书混合签密[J]. 计算机学报, 2015, 38(4): 805–813. doi: 10.3724/SP.J.1016.2015.00804.
YU Huifang and YANG Bo. Provably secure certificateless hybrid signcryption[J]. *Chinese Journal of Computers*, 2015, 38(4): 805–813. doi: 10.3724/SP.J.1016.2015.00804.

刘景伟：男，1978 年生，博士，副教授，研究方向为信息安全和网络安全.

张俐欢：女，1994 年生，硕士生，研究方向为密码学和信息安全.

孙　蓉：女，1976 年生，博士，副教授，研究方向为信息论与编码理论.