异构双向签密方案的安全性分析和改进

张玉磊* 王 欢 刘文静 王彩芬
(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：异构签密可以保证异构密码系统之间数据的机密性和不可伪造性。2016 年，刘景伟等人提出了传统公钥密码和无证书公钥密码之间的 PCHS 和 CPHS 双向异构签密方案。但是，经过分析，发现 PCHS 方案和 CPHS 方案均不安全。首先描述了第 2 类敌手对两个方案的攻击过程，其次分析了两个方案存在第 2 类敌手攻击的原因，最后对 PCHS 方案和 CPHS 方案进行改进。改进方案克服了原方案的安全性问题，保证了传统公钥密码和无证书公钥密码环境之间数据的安全传输。

关键词：签密；异构系统；KGC 攻击；选择密文攻击；选择消息攻击
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2017)12-3045-06
DOI: 10.11999/JEIT170203

Security Analysis and Improvement of Mutual Signcryption Schemes under Heterogeneous Systems

ZHANG Yulei WANG Huan LIU Wenjing WANG Caifen
(*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Heterogeneous signcryption can be used to guarantee the confidentiality and unforgeability in the different cryptography. In 2016, between traditional public key cryptography and certificateless public key cryptography, the mutual signcryption schemes including PCHS and CPHS were proposed by Liu *et al*. However, via the security analysis, it is shown that the above schemes are not secure. Firstly, the processes of attack performed by the second type of adversary are described. Secondly, the possible reasons why the second type of adversary can perform these attacks are analyzed. In the end, the original schemes are improved. The improved schemes can overcome the security weakness of the original schemes, and can also ensure the security of data transmission between traditional public key cryptographic and certificateless public key cryptography.

Key words: Signcryption; Heterogeneous system; KGC's attack; Chosen cipertext attack; Chosen message attack

1 引言

签密[1]能够在一个逻辑步骤同时实现加密和签名功能，保证数据的机密性和认证性。5G 异构网络环境中，发送方和接收方所属的公钥密码体制可能不同。因此，为了保证异构公钥密码环境的数据机密性和认证性，有必要研究异构签密问题。基于异构签密的优势，研究者们对异构签密进行了广泛的研究[2–8]。

2010 年，文献[2]首次提出异构签密问题，提出了以公钥基础设施 PKI(Public Key Infrastructure)为基础的传统公钥密码体制到身份公钥密码体制 IDPKC(IDentity-based Public Key Cryptographic)的 TPKI→IDPKC 异构签密方案。但是，该方案只满足签密的外部安全性。随后，文献[3]构造了 IDPKC→TPKI 异构签密方案；文献[4]扩展了文献[2]的研究工作，构造了 IDPKC→TPKI 多接收者异构签密方案。但是，以上方案均为单向异构签密方案。为了实现数据的双向安全传输，文献[5]构造了第 1 个双向 TPKI-IDPKC 异构签密方案，该方案满足签密的内部安全性[9]。以上方案仅考虑了 IDPKC 和 TPKI 之间的异构签密问题。为了克服身份公钥密码体制的密钥托管问题[10]，2016 年，文献[6]和文献[7]提出了 CLPKC→TPKI 异构签密方案，但是以上两个方案只具有 CLPKC→TPKI 的单向传输模式。

收稿日期：2017-03-06；改回日期：2017-05-12；网络出版：2017-06-30
*通信作者：张玉磊 zhangyl@nwnu.edu.cn
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)，西北师范大学青年教师科研能力提升计划(NWNU-LKQN-14-7)
Foundation Items: The National Natural Science Foundation of China (61163038, 61262056), The Higher Educational Scientific Research Foundation of Gansu Province of China (2015B-220, 2013A-014), The Young Teachers' Scientific Research Ability Promotion Program of Northwest Normal University (NWNU-LKQN-14-7)

2016 年，刘景伟等人[8]提出了 TPKI-CLPKC 双向异构签密方案，并且，基于随机预言模型，证明 PCHS(TPKI→CLPKC heterogeneous signcryption)方案和 CPHS(CLPKC→TPKI heterogeneous signcryption)方案具有自适应选择密文攻击下的不可区分性和自适应选择消息攻击下的不可伪造性。文献[8]指出，PCHS 方案和 CPHS 方案主要考虑两类敌手：第 1 类敌手 A_{I} 无法获得密钥生成中心 KGC (Key Generation Center)的主密钥，但是，它可以替换用户的公钥；第 2 类敌手 A_{II} 无法替换用户的公钥，但是能够获得 KGC 的主密钥。A_{I} 表现为一般用户，A_{II} 表现为恶意的 KGC。

分析刘景伟等人[8]的 PCHS 方案和 CPHS 方案的安全性，发现两个方案均存在第 2 类敌手攻击，PCHS 方案不满足机密性，CPHS 方案不满足机密性、不可伪造性和正确性。首先，通过具体的攻击过程，指出第 2 类敌手 A_{II} 能够解密 PCHS 方案和 CPHS 方案的密文，两个方案不满足自适应选择密文攻击的不可区分性；A_{II} 完全掌握 CPHS 方案中发送方的私钥，可以对任意消息实现伪造攻击。同时，该方案构造的密文无法通过验证等式。其次，分析 PCHS 方案和 CPHS 方案存在第 2 类攻击的原因，改进私钥生成算法和哈希函数的输入结构，重新设计签密算法，提出了改进的 PCHS 方案和 CPHS 方案。最后，基于随机预言模型，证明改进方案在 TPKI-CLPKC 双向异构密码系统下满足签密内部安全模型的机密性和不可伪造性，可以克服原方案的不足，保证 TPKI 和 CLPKC 异构密码环境数据传输的安全性。

2 刘景伟等人[8]的方案的安全性分析

2.1 方案回顾

刘景伟等人[8]的 PCHS 方案和 CPHS 方案具体包括以下算法：

(1)系统建立算法：令 G_1 和 G_2 分别是素数阶 $\geq 2^{\beta}$ (安全参数为 β)的加法群和乘法群，P 为 G_1 的生成元；$\hat{e}: G_1 \times G_1 \to G_2$ 为双线性映射。KGC 定义 4 个哈希函数：$H_1: \{0,1\}^* \to G_1$，$H_3: G_2 \to \{0,1\}^n$，$H_2: \{0,1\}^n \times \{0,1\}^n \to Z_q^*$，和 $H_4: \{0,1\}^n \to \{0,1\}^n$，其中，$n$ 表示签密消息的长度。KGC 随机选择 $s \in Z_q^*$ 作为系统主密钥，计算系统公钥 $P_{\mathrm{pub}} = sP$。KGC 保密主密钥 s 并发布系统参数 $\{G_1, G_2, n, e, P, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4\}$。

(2)CLPKC-KG(CLPKC 用户密钥建立)：

(a)部分私钥提取算法：KGC 输入系统参数，系统主密钥 s 及用户身份 ID，计算 $Q = H_1(\mathrm{ID})$，输出部分私钥 $D = sQ$。

(b)用户密钥生成算法：用户输入系统参数，随机选择 $x_c \in Z_q^*$ 作为秘密值，生成用户私钥 $\mathrm{SK}_c = x_c sQ_c$ 和公钥 $\mathrm{PK}_c = x_c Q_c$。

(3)PKI-KG(TPKI 用户密钥建立)：TPKI 用户随机选择 $x_p \in Z_q^*$ 作为私钥 SK_p，计算公钥 $\mathrm{PK}_p = x_p P$。

(4)PCHS 签密算法：假定 TPKI 中发送者的公/私钥对为 $(\mathrm{PK}_p, \mathrm{SK}_p)$，CLPKC 中接收者的公钥为 PK_c。发送者执行以下过程：

(a)随机选择 $k \in \{0,1\}^n$，计算 $r = H_2(k,m)$，$f = e\left(P_{\mathrm{pub}}, \mathrm{PK}_c\right)^r$；

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

(c)计算 $S = \left(r + \mathrm{SK}_p H_1(m)\right) \bmod n$，则签密密文为 $\sigma = (S, U_1, U_2, U_3)$。

(5)PCHS 解签密算法：CLPKC 接收者输入私钥 SK_c 和发送者的公钥 PK_p，执行以下过程：

(a)计算 $k = U_2 - H_3\left(e\left(\mathrm{SK}_c, U_1\right)\right), m = U_3 - H_4(k)$；

(b)计算 $r = H_2(k,m)$；$V = \mathrm{SP} - H_1(m)\mathrm{PK}_p$；

(c)验证 V 与 U_1 是否相等，其中 $U_1 = rP$。如果相等，则接受消息 m，否则输出错误符号“⊥”。

(6)CPHS 签密算法：CLPKC 发送者的公/私钥为 $(\mathrm{PK}_c, \mathrm{SK}_c)$，TPKI 接收者的公钥为 PK_p。发送者执行以下过程：

(a)随机选择 $k \in \{0,1\}^n$，计算 $r = H_2(k,m)$，$f = e\left(P_{\mathrm{pub}}, \mathrm{PK}_p\right)^r$；

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

(c)计算 $S = \left(r + H_1(m)\mathrm{SK}_c\right) \bmod n$，则签密后的密文为 $\sigma = (S, U_1, U_2, U_3)$。

(7)CPHS 解签密算法：接收者输入私钥 SK_p 和发送者的公钥 PK_c，执行以下过程：

(a)计算 $k = U_2 + H_3\left(e\left(\mathrm{SK}_p P_{\mathrm{pub}}, U_1\right)\right)$，$m = U_3 + H_4(k)$；

(b)计算 $r = H_2(k,m), V = \mathrm{SP} - H_1(m)\mathrm{PK}_c P_{\mathrm{pub}}$；

(c)验证 V 与 U_1 是否相等，其中 $U_1 = rP$。如果相等，则接受消息 m，否则输出错误符号“⊥”。

2.2 对 PCHS 方案和 CPHS 方案的攻击

PCHS 方案的机密性安全主要依赖于 CLPKC 的主密钥 s，秘密值 x_c，部分私钥 D_c 和随机数 r 等秘密信息。由于 $P_{\mathrm{pub}} = sP$，$\mathrm{PK}_c = x_c Q_c$，$U_1 = rP$，

$D_c = sQ_c$，第 1 类敌手 A_{I}无法直接获得 s， r 和 D_c，否则离散对数困难问题可解。因此，该方案能够抵抗第 1 类敌手 A_{I}的攻击。但是，第 2 类敌手(恶意 KGC)可以解密密文信息。

2.2.1 对 PCHS 方案的攻击　KGC 是 CLPKC 系统的建立者，它了解系统主密钥 s。因此，KGC 可以利用主密钥 s 计算 $e(\mathrm{SK}_c,U_1)=e(x_csQ_c,U_1)=e(\mathrm{PK}_c,U_1)^s$，进而实现攻击。具体攻击过程如下：

(1)捕获签密密文：　KGC 通过窃听等方式获得用户对消息 m 的密文 $\sigma=(S,U_1,U_2,U_3)$。

(2)解密密文：　KGC 首先计算 $k=U_2-H_3(e(\mathrm{SK}_c,U_1))=U_2-H_3(e(x_csQ_c,U_1))=U_2-H_3(e(x_c\cdot Q_c,U_1)^s)=U_2-H_3(e(\mathrm{PK}_c,U_1)^s)$，然后恢复消息 $m=U_3-H_4(k)$。所以，第 2 类敌手能够解密密文 σ，PCHS 方案不满足自适应选择密文攻击的不可区分性。

KGC 也可以通过更简单的方式实现以上攻击：由于 $\mathrm{SK}_c=x_csQ_c=sx_cQ_c=s\mathrm{PK}_c$，所以，KGC 可以获得所有 CLPKC 用户的私钥。因此，第 2 类敌手拥有与用户相同的解密权力，可以对方案所有密文进行解密。

同时，由于 $r=H_2(k,m)\in Z_q^*$, $\mathrm{SK}_p\in Z_q^*$, $H_1\in G_1$，所以，发送方无法计算 $S=(r+\mathrm{SK}_pH_1(m))\bmod n$。因此，由于作者笔误，PCHS 方案无法得到正确的密文。若以新的哈希函数 $H:\{0,1\}^n\to Z_q^*$ 代替 S 表达式中的 $H_1(m)$, PCHS 方案就可以得到正确的密文。

2.2.2 对 CPHS 方案的攻击　CPHS 方案假设 CLPKC 和 TPKI 使用相同的系统参数，TPKI 用户的私钥 $\mathrm{SK}_p\in Z_q^*$，CLPKC 的 KGC 主密钥 $s\in Z_q^*$，TPKI 用户的公钥 $\mathrm{PK}_p\in G_1$，因此，KGC 可以直接计算 $\mathrm{SK}_pP_{\mathrm{pub}}=x_psP=sx_pP\ =s\mathrm{PK}_p$，进而可以解密 CPHS 方案的密文。具体攻击过程如下：

(1)捕获签密密文：　KGC 通过窃听等方式获得用户对消息 m 的密文 $\sigma=(S,U_1,U_2,U_3)$。

(2)解密密文：　KGC 计算 $k=U_2+H_3\left(e\left(\mathrm{SK}_p\,P_{\mathrm{pub}},U_1\right)\right)=U_2+H_3\left(e\left(x_psP,U_1\right)\right)=U_2+H_3\left(e\left(x_pP,U_1\right)^s\right)=U_2+H_3\left(e\left(\mathrm{PK}_p,U_1\right)^s\right)$，然后计算 $m=U_3+H_4(k)$。所以，第 2 类敌手能够解密密文 σ，CPHS 方案不满足自适应选择密文攻击的不可区分性。

由于 CLPKC 用户的私钥格式为 $\mathrm{SK}_c=x_csQ_c=sx_cQ_c=s\mathrm{PK}_c$，KGC 可以获得所有 CLPKC 用户的私钥，因此，KGC 可以对任何消息实现伪造攻击。

与 PCHS 方案相似，CPHS 方案中的 $\mathrm{SK}_c\in Z_q^*$，$r=H_2(k,m)\in Z_q^*$，$H_1\in G_1$，所以，发送方无法计算 $(r+H_1(m)\mathrm{SK}_c)\bmod n$。因此，由于作者笔误，CPHS 方案同样无法得到正确的密文。若以新的哈希函数 $H:\{0,1\}^n\to Z_q^*$ 代替 S 表达式中的 $H_1(m)$，CPHS 方案就可以得到正确的密文。

3　对刘景伟等人[8]方案的改进

根据 2.2 节的分析，第 2 类敌手容易计算 CLPKC 用户的私钥 $\mathrm{SK}_c=s\mathrm{PK}_c$ 和 CPHS 方案中的表达式 $\mathrm{SK}_pP_{\mathrm{pub}}=s\mathrm{PK}_p$，所以，第 2 类敌手可以对 PCHS 方案实施解密攻击，对 CPHS 方案实施解密和任意伪造攻击。因此，必须对文献[8]的 PCHS 方案和 CPHS 方案进行改进。

本文对文献[8]方案的改进主要包括 3 部分。

(1)更改 CLPKC 用户的密钥格式，避免第 2 类敌手 A_{II}能够获得用户的完整私钥：以 $\mathrm{PK}_c=x_cP$ 和 $\mathrm{SK}_c=(x_c,D_c)$ 分别代替原 $\mathrm{PK}_c=x_cQ_c$ 和 $\mathrm{SK}_c=x_cD_c$。

(2)PCHS 方案签密算法中，避免第 2 类敌手能够计算 H_3 哈希函数。以 $H_3(e(P_{\mathrm{pub}},Q_c)^r,r\mathrm{PK}_c)$ 代替 $H_3(e(P_{\mathrm{pub}},\mathrm{PK}_c)^r)$ 哈希函数，即使 KGC 可以获得 $e(P_{\mathrm{pub}},Q_c)^r$，但是，它无法计算 $r\mathrm{PK}_c$，否则 CDH 困难问题可解。因此，第 2 类敌手无法计算 H_3 哈希函数值，进而无法实现解密攻击。

(3)CPHS 方案签密算法中，重新设计签密算法。以 $H_6\left(r\mathrm{PK}_p\right)$ 代替 $H_3\left(e\left(P_{\mathrm{pub}},\mathrm{PK}_p\right)^r\right)$ 哈希函数，以 $S=rQ_c+x_cH_7\left(m\,\|\,U_1\right)+D_c$ 代替 $S=\left(r+H_1(m)\mathrm{SK}_c\right)\bmod n$，增强 CPHS 方案的安全性。

3.1 改进方案

改进的PCHS方案和CPHS方案包括以下算法：

(1)系统建立算法：G_1 和 G_2 分别是素数阶 $\geq 2^\beta$ (安全参数为 β)的加法群和乘法群，P 为 G_1 的生成元；$\hat{e}:G_1\times G_1\to G_2$ 为双线性映射。KGC 定义哈希函数：$H_1:\{0,1\}^*\to G_1, H_2:\{0,1\}^n\times\{0,1\}^n\to Z_q^*$, $H_3:G_2\to\{0,1\}^n$, $H_4:\{0,1\}^n\to\{0,1\}^n, H_5:\{0,1\}^n\to Z_q^*$, $H_6:G_1\to\{0,1\}^n$, $H_7:\{0,1\}^*\to G_1$，其中，n 表示签密消息的长度。KGC 随机选择 $s\in Z_q^*$ 作为系统主密钥，计算系统公钥 $P_{\mathrm{pub}}=sP$。KGC 保密主密钥 s，并发布系统参数 $\{G_1,G_2,n,e,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4,H_5,H_6,H_7\}$。

(2)CLPKC-KG(CLPKC 用户密钥建立)：

(a)部分私钥提取算法：KGC 输入系统参数，主密钥 s 及用户身份 ID_c，计算 $Q_c=H_1(\mathrm{ID}_c)$，输出部分私钥 $D_c=sQ_c$。

(b)用户密钥生成算法：用户随机选择 $x_c\in Z_q^*$ 作为秘密值，生成用户的完整私钥 $\mathrm{SK}_c=(x_c,D_c)$ 和公

钥 $\mathrm{PK}_c = x_c P$ 。

(3)PKI-KG(TPKI 用户密钥建立)：TPKI 用户随机选择 $x_p \in Z_q^*$ 作为私钥 SK_p ，计算公钥 $\mathrm{PK}_p = x_p P$ 。

(4)PCHS 签密算法：假定 TPKI 发送者的公钥/私钥对为 $(\mathrm{PK}_p, \mathrm{SK}_p)$, CLPKC 接收者的公钥为 PK_c 。发送者执行以下过程：

(a)选择随机数 $k \in \{0,1\}^n$ ，计算 $r = H_2(k,m)$, $f = e(P_{\mathrm{pub}}, Q_c)^r$ ；

(b)计算 $U_1 = rP$, $U_2 = k \oplus H_3(f, r\mathrm{PK}_c)$, $U_3 = m \oplus H_4(k)$ ；

(c)计算 $S = (r + \mathrm{SK}_p H_5(m)) \bmod n$ ，则密文是 $\sigma = (S, U_1, U_2, U_3)$ 。

(5)PCHS 解签密算法：CLPKC 接收者输入私钥 SK_c 和 TPKI 发送者的公钥 PK_p ，执行以下过程：

(a)计算 $f = e(D_c, U_1)$, $k = U_2 \oplus H_3(f, x_c U_1)$ ；

(b)计算 $m = U_3 \oplus H_4(k)$, $r = H_2(k,m)$, $V = \mathrm{SP} - H_5(m)\mathrm{PK}_p$ ；

(c)验证 $V = U_1$ 是否成立。如果等式成立，则返回消息 m ，否则返回错误符号“ $\perp$ ”。

(6)CPHS 签密算法：CLPKC 发送者的公钥/私钥对为 $(\mathrm{PK}_c, \mathrm{SK}_c)$, TPKI 接收者的公钥 PK_p 。发送者执行以下过程：

(a)选择随机数 $k \in \{0,1\}^n$ ；计算 $r = H_2(k,m)$, $f = r\mathrm{PK}_p$ ；

(b)计算 $U_1 = rP$, $U_2 = k \oplus H_6(f)$, $U_3 = m \oplus H_4(k)$ ；

(c)计算 $S = rQ_c + x_c H_7(m \,\|\, U_1) + D_c$ 。则密文是 $\sigma = (S, U_1, U_2, U_3)$ 。

(7)CPHS 解签密算法：TPKI 接收者输入私钥 SK_p 和 CLPKC 发送者的公钥 PK_c ，执行以下过程：

(a)计算 $f = \mathrm{SK}_p U_1$, $k = U_2 \oplus H_6(f)$, $m = U_3 \oplus H_4(k)$ ；

(b)验证等式。 $e(P,S) = e(U_1, Q_c) e(\mathrm{PK}_c, H_7(m \,\|\, U_1)) e(P_{\mathrm{pub}}, Q_c)$ 是否成立。如果等式成立，则返回消息 m ，否则返回错误符号“ $\perp$ ”。

3.2 改进的 PCHS 方案的安全性分析

改进 PCHS 方案的目的是提高原方案的机密性，防止第 2 类敌手攻击。因此，以下将证明“改进的 PCHS 方案针对第 2 类攻击者具有自适应选择密文攻击的不可区分性，即 IND-CCA2-A_{II} (INDistinguishability against Adaptive Chosen Ciphertext Attack A_{II})安全。

定理 1 (TPKI-CLPKC-IND-CCA2-A_{II}) 随机预言模型中，假设存在一个 IND-CCA2-A_{II} 敌手能够在 τ 时间内，最多进行 q_p 次 CLPKC 公钥询问，q_e 次 CLPKC 私钥询问和 q_u 次解签密询问，以 ε 的优势赢得 PCHS 游戏，那么存在一个挑战者能以 $\varepsilon' \geq \varepsilon / q_\tau$ 优势解决 CDH 问题，其中，$q_\tau = q_p + q_\varepsilon + 2q_u + 2$ 。

证明 假设 F 输入 CDH 问题实例 (P, aP, bP) ，目标是计算 $abP \in G_1$ 。F 在游戏中充当挑战者，并将 A_{II} 作为子程序。

初始化：F 生成主密钥 $s \in Z_p^*$ 和系统公钥 $P_{\mathrm{pub}} = sP$ ，同时将主密钥 s 和系统参数发给敌手 A_{II}。

阶段 1：A_{II} 发起一系列询问。F 维护初始值为空的列表 $L_1 \sim L_7$, LK_p 和 L_{pk} ，记录 $H_i (1 \leq i \leq 7)$ 预言机和公钥询问信息。

H_1 询问：输入 ID_i ，当 $\mathrm{ID}_i \neq \mathrm{ID}_l$, $l \in \{0,1,2,\cdots,\tau\}$ 时，设置 $Q_i = rP$ ，将 (ID_i, Q_i, r) 存进列表 L_1 中。

$H_k (k = 2,4,5,6,7)$ 询问：对于新的 H_k (k=2,4,5,6,7)询问时，若相关询问在表 L_k 中，直接返回给 A_{II}；否则随机选择一个数返回给 A_{II}，添加相关信息到 $L_k (k = 2,4,5,6,7)$ 。

CLPKC 公钥询问：A_{II} 询问 ID_i 公钥时，如果 $i \neq l$, F 选取新的随机数 $x \in Z_p^*$ ，并计算 $\mathrm{PK}_i = xP$ ，将 $(i, \mathrm{ID}_i, \mathrm{PK}_i, x)$ 存于列表 L_{pk} 中；否则，将 $(l, \mathrm{ID}_l, aP, \perp)$ 存于列表 L_{pk} ，并返回 aP 。

CLPKC 私钥询问：A_{II} 询问 ID_i 私钥，F 运行 CLPKC 公钥询问，并获得 $(i, \mathrm{ID}_i, \mathrm{PK}_i, x)$ ，如果 $i = l$ ，模拟终止。否则，F 运行 H_1 询问得到 $(\mathrm{ID}_i, Q_i, b_i)$ 并返回私钥 (x, rsP) 。

TPKI 私钥询问：A_{II} 询问 ID_j 私钥，F 从 LK_p 得到 $(\mathrm{ID}_j, x_j, \mathrm{PK}_j)$ ，返回 $\mathrm{SK}_j = x_j$ 。

H_3 询问：对于新的 $H_3(f_i, R_i)$ 询问。F执行以下步骤：

(1)检查 $\hat{e}(aP, bP) = \hat{e}(P, R_i)$ 是否成立，如果成立，F 停止且返回 R_i 。

(2)检查列表 L_3 中是否存在 $(f_i, *, h)$ 满足使用 $\hat{e}(U_{1i}, aP) = \hat{e}(P, R_i)$ 。如果 $\mathrm{ID}_i = \mathrm{ID}_l$ 成立，F 返回 h 并用 R_i 代替符号 $*$ 。

(3)如果挑战者执行到这一步，它从 $\{0,1\}^n$ 中随机选择一个 h 并将 (f_i, R_i, h) 插入到列表 L_3 中。

解签密询问：F 接收 A_{II} 发送的密文 $\sigma = (S, U_1, U_2, U_3)$ ，同时核对发送者身份 ID_i 和接收者身份 ID_j ，并执行下面的步骤：

(1)计算 $f = \hat{e}\left(U_1, rP_{\mathrm{pub}}\right)$ 。因为 $Q_j = rP$ ，所以 $f = \hat{e}\left(U_1, rP_{\mathrm{pub}}\right) = \hat{e}\left(U_1, srP\right) = \hat{e}\left(U_1, sQ_j\right) = \hat{e}\left(U_1, D_j\right)$ 。

(2)如果 $\mathrm{ID}_j \neq \mathrm{ID}_l$ ，计算 $R = x_j U_1$ 。通过执行 H_3 询问获得 h_3 , $k = U_2 \oplus h_3$ ；接着执行 H_4 询问获得 $m = U_3 \oplus h_4$ 完成解密过程。

(3)如果 $\mathrm{ID}_j = \mathrm{ID}_l$, F 不能直接计算 R 。此时，

F 搜索列表 L_3，对于不同的 R 寻找 (f_i, R_i, h)，希望等式 $\hat{e}(U_1, aP) = \hat{e}(P, R)$ 成立。如果能找到，说明找到了正确的 R。F 通过执行 H_3 询问获得 h_3，$k = U_2 \oplus h_3$；接着执行 H_4 询问获得 $m = U_3 \oplus h_4$ 完成解密过程。

(4)F 执行到这一步骤时，从 $\{0,1\}^{l_m}$ 中任意选取一个 h，并将 $(*, R_i, h)$ 插入到列表 L_3 中。

(5)执行解签密的验证部分，如果不成立，返回“$\perp$”。

挑战阶段：与 TPKI-CLPKC-IND-CCA2-A_{I} 挑战阶段相同。

阶段 2：A_{II} 像阶段 1 一样进行多项式有界次适应性询问。

猜测：A_{II} 输出一个比特 γ'。因为 L_1 中最多有 q_τ 个元素，且 l 是随机选择的，所以 ID_l 被敌手输出的概率为 $1/q_\tau$。如果该事件发生，除了敌手询问过 $H_3\left(f^*, R^*\right)$，模拟是完美的。因为 Hash 函数 H_3 可以看作是随机预言机，在这个元组不存在于 L_3 的情况下，敌手没有任何优势。反之，F 将在 H_3 询问的步骤(1)中解决 CDH 问题。

改进的CPHS方案的机密性和不可伪造性的证明过程与文献[8]相似，限于篇幅，本文略去改进的CPHS方案的机密性和不可伪造性的证明过程。

4　性能分析

本节分析改进的 CPHS 方案和 PCHS 方案的效率。表 1 描述了改进方案和现有的 TPKI 和 CLPKC 之间异构签密方案的性能，其中，e 和 P 分别表示所需的指数运算和双线性对运算的个数。通过表 1 可以看出，文献[6]和文献[7]的 CLPKC→TPKI 方案需要的双线性对数较少，但是，两个方案只考虑单向通信。文献[8]能够实现 TPKI 和 CLPKC 双向通信，但是 PCHS 方案不满足机密性，CPHS 方案不满足机密性和不可伪造性。本文改进的 PCHS 方案满足 IND-CCA2 安全性，同时具有较高的效率；改进的 CPHS 方案中没有指数运算，增加了 2 个双线对运算，但是提高了原方案的安全性。

5　结束语

本文对刘景伟等人[8]的异构系统下双向签密方案的安全性进行分析，指出 PCHS 方案和 CPHS 方案均存在第 2 类攻击。最后提出了改进的 PCHS 方案和 CPHS 方案。改进方案克服了原方案存在第 2 类攻击的不足，保证了 TPKI 和 CLPKC 异构密码系统之间双向数据的机密性和不可伪造性。改进的 CPHS 方案增加了 2 个双线性对，能否减少双线性对的个数，提高效率，是我们下一步的研究重点。

表 1　TPKI-CLPKC异构签密方案性能比较

方案	方向	预运算	签密	解签密	总运算量	IND-CCA2	EUM-CMA
文献[6]方案	CLPKC→TPKI	$0P$	$0e$+$0P$	$2P$	$2P$	√	√
文献[7]方案	CLPKC→TPKI	$1P$	$1e$	$1e$+$2P$	$2e$+$3P$	√	√
文献[8]PCHS方案	TPKI→CLPKC	$0P$	$1e$+$1P$	$1P$	$1e$+$2P$	×	√
文献[8]CPHS方案	CLPKC→TPKI	$0P$	$1e$+$1P$	$1P$	$1e$+$2P$	×	×
改进的PCHS方案	TPKI→CLPKC	$0P$	$1e$+$1P$	$1P$	$1e$+$2P$	√	√
改进的CPHS方案	CLPKC→TPKI	$0P$	$0e$+$0P$	$4P$	$4P$	√	√

参 考 文 献

[1] LIBERT B and QUISQUATER J J. Improved signcryption from q-Diffie-Hellman problems[C]. International Conference on Security in Communication Networks, Amalfi, Italy, 2004: 220–234. doi: 10.1007/978-3-540-30598-9_16.

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

[4] FU X T, LI X W, and LIU W. IDPKC-to-TPKC construction of multi-receiver signcryption[C]. International Conference on Intelligent Networking and Collaborative Systems (INCoS), Xi'an, China, 2013: 335–339. doi: 10.1109/INCoS.2013.62.

[5] 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.

[6] 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(6): 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(6): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

[7] LI F G, HAN Y N, and JIN C H. Practical signcryption for secure communication of wireless sensor networks[J]. *Wireless Personal Communications*, 2016, 89(4): 1391–1412. doi: 10.1007/s11277-016-3327-4.

[8] 刘景伟, 张俐欢, 孙蓉. 异构系统下的双向签密方案[J]. 电子与信息学报, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT 160056.

LIU J W, ZHANG L H, and SUN R. Mutual signcryption schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT160056.

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

[10] ZHANG L, WU Q H, QIN B, *et al*. Identity-based authenticated asymmetric group key agreement protocol[J]. *Journal of Computer Research & Development*, 2010, 6196(19): 510–519. doi: 10.1007/978-3-642-14031-0_54.

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.

王 欢： 女，1991年生，硕士生，研究方向为信息安全.

刘文静： 女，1994年生，硕士生，研究方向为信息安全.

王彩芬： 女，1963 年生，博士，教授，研究方向为密码学与信息安全.