一种可证安全的PKI和IBC双向匿名异构签密方案的改进

曹素珍 郎晓丽 刘祥震 张玉磊* 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。该文分析了一个传统公钥密码(PKI)和身份密码(IBC)之间的PKI→IBC和IBC→PKI双向匿名异构签密方案的安全性，指出PKI→IBC方案和IBC→PKI方案均不能抵挡敌手攻击，敌手在获取密文前提下均可解密密文。为了增强安全性，该文提出一个改进的PKI→IBC和IBC→PKI方案，并在随机预言模型下基于计算性Diffie-Hellman困难问题和双线性Diffie-Hellman困难问题证明新方案满足机密性与不可伪造性。同时效率分析表明，所提方案具有更高的通信效率。

关键词：异构签密；选择密文攻击；机密性；不可伪造性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)08-1787-06
DOI: 10.11999/JEIT180982

Improvement of a Provably Secure Mutual and Anonymous Heterogeneous Signcryption Scheme Between PKI and IBC

CAO Suzhen LANG Xiaoli LIU Xiangzhen ZHANG Yulei WANG Caifen
(*College of Computer Science and Engineering, Northwest Normal University, Lanzhou* 730070, *China*)

Abstract: Heterogeneous signcryption can ensure the confidentiality and unforgeability of information data between different cryptosystems systems. Security for the traditional Public Key Infrastructure (PKI) and Identity-Based Cryptosystem (IBC) two-way and anonymous heterogeneous signcryption scheme between PKI→IBC and IBC→PKI is analyzed. It is pointed out that PKI→IBC scheme and IBC→PKI scheme can not resist adversary attacks. The ciphertext can be decrypted under the adversary obtaining the ciphertext. To enhance security, a new PKI→IBC and IBC→PKI scheme is proposed, and then confidentiality and unforgeability of the scheme in the random oracle model on the basis of the assumptions of Computational Diffie-Hellman problem and Bilinear Diffie-Hellman problem is proved. The efficiency analysis shows that the new scheme has higher communication efficiency.

Key words: Heterogeneous signcryption; Chosen ciphertext attack; Confidentiality; Unforgeability

1 引言

文献[1]首次提出了区别于传统模式中先签名后加密的签密概念，可以把签名方案的不可伪造性与加密方案的机密性很好结合起来，且计算量小于两者之和。由于，传统公钥基础设施(PKI)与基于身份的密码体制(IBC)在实际应用中有相当重要的地位，因此，众多学者对基于PKI的签密与基于IBC的签密进行了众多的研究[2–7]。

传统签密方案中，消息的发送方与接收方皆来自同一密码体制。但是，在实际应用环境中，跨密码体制通信却越来越普及，因此，文献[8]首次提出了异构签密方案。该方案的发送方来自PKI系统，接收方来自IBC系统，但是该方案不满足消息不可伪造性的安全要求。随后，文献[9]提出了IBC→PKI的异构签密方案，该方案被证明满足内部安全性的要求。文献[10]提出了两个异构签密方案，并给出了具体的形式化定义与安全性模型。文献[11]提出了IBC→CLP(Certificateless Public Key Infrastructure, CLP)在线/离线签密方案，但是该方案在验证等式中用到的双线性对较多从而降低了验证效率。文献[12]提出了异构PKI→CLP签密方案，随后文献[13]指出该方案不满足机密性。文献[14]与文献[15]提出了PKI→IBC的异构签密方案，但是这两个方案只具有单向传输模式。

收稿日期：2018-10-19；改回日期：2019-03-12；网络出版：2019-04-13
*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, 61262057)，甘肃省高等学校科研项目(2017A-003, 2018A-207)
Foundation Items: The National Natural Science Foundation of China (61163038, 61262056, 61262057), The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2018A-207)

2017年，文献[16]提出了公钥基础设施和身份密码体制下匿名双向的异构签密方案，并在随机预言机模型下证明了PKI→IBC方案和IBC→PKI方案在自适应选择消息攻击下的不可伪造性和自适应选择密文攻击下的不可区分性。

对文献[16]中的PKI→IBC和IBC→PKI方案进行安全性分析，发现PKI→IBC方案不满足机密性、不可伪造性和正确性。IBC→PKI方案不满足机密性和正确性。本文通过具体攻击过程，指出敌手总能正确解密密文，所以，文献[16]不满足自适应性选择密文攻击下的不可区分性。同时，PKI→IBC方案和IBC→PKI方案的验证等式均不能通过验证等式的验证，即验证者总是无法接收消息。其次，提出了改进的PKI→IBC方案和IBC→PKI方案，并在随机预言机模型下证明改进方案满足机密性和不可伪造性。

2 文献[16]方案及安全性分析

2.1 方案回顾

限于篇幅，略去对文献[16]方案的描述，具体算法见文献[16]。

2.2 对PKI→IBC和IBC→PKI方案的攻击

文献[16]是PKI→IBC的双向异构签密方案。对于PKI→IBC方案的机密性，主要考虑IBC密码环境中的敌手；对于IBC→PKI方案的机密性，主要考虑PKI密码环境下的敌手。

2.2.1 对PKI→IBC方案的攻击

(1) 机密性：PKI→IBC方案的机密性主要依赖于系统IBC中用户私钥S_B，随机数r。任意敌手A通过计算$e_B(N,S_B)=e_B(XP_B,sQ_B)=e_B(P_{\text{pb}},XQ_B)$，进而实现攻击。具体攻击过程如下。

(a) 获取密文信息：A窃取用户对消息m的密文$\sigma=(X,y)$。

(b) 解密密文：A计算$N=XP_B=rQ_AP_B$, $w_2=e_B(N,S_B)=e_B(XP_B,sQ_B)=e_B(P_{\text{pb}},XQ_B)$，其中$Q_B$为IBC中的用户公钥。恢复消息$Z||Q_A||m=y\oplus H_3^B(w_2)$和$h=H_2^B(X||m)$。

敌手A总是能够破解密文。因此，PKI→IBC方案不满足机密性。

(2) 不可伪造性：PKI→IBC的不可伪造性主要依赖于系统PKI中用户私钥S_A，随机数r。攻击过程如下。

(a) 参数设置：挑战者C通过运行算法系统参数生成，选择$\overline{w}\in Z_q^*$，计算$P_B=\overline{w}P_A$作为群G_1^B的一个生成元。

(b) 查询：敌手A通过签名询问，获取相应签名。

(c) 伪造签名：A随机选取$r'\in Z_q^*$，计算$Z'=(r'+h')S_AP_B=(r'+h')x_A\overline{w}P_A=(r'+h')\overline{w}Q_A$。将$\sigma'=(X',y')$发给IBC中的用户，其中$X'=r'Q_A$。

(d) 验证签名：对伪造的签名进行等式验证$e_A(Z',P_A)=e_A((r'+h')\overline{w}Q_A,P_A)=e_A(X'+h'Q_A,P_B)$，其中$h'=H_2^B(X'||m')$。

所以，敌手A可以成功伪造签密密文。因此，PKI→IBC方案不满足自适应选择消息攻击下的不可伪造性。

(3) 正确性：由于$Z=(r+h)S_AP_B\in G_1^B$是签密者利用私钥进行签名，但是并没有把签名Z发送给IBC系统中的用户，由于作者笔误，IBC系统中的用户无法对等式$e_A(Z,P_A)=e_A(X+hQ_A,P_B)$进行验证；并且$Z\in G_1^B$, $P_A\in G_1^A$，与作者定义的双线性映射不同，所以，PKI→IBC方案中的用户总无法接收消息。

2.2.2 对IBC→PKI方案的攻击

(1) 机密性：IBC→PKI方案的机密性主要依赖于系统PKI中用户的私钥S_A，随机数r。任意敌手A通过等式计算$e_A(N,P_{\text{pb}})^{S_A}=e_A(XP_A,P_{\text{pb}})^{x_A}=e_A(XQ_A,P_{\text{pb}})$，进而实现攻击。

(a) 获取密文信息：A窃取消息m的密文$\sigma=(X,y)$。

(b) 解密密文：A计算$N=XP_A=rQ_BP_A$, $w_2=e_A(N,P_{\text{pb}})^{S_A}=e_A(XP_A,P_{\text{pb}})^{x_A}=e_A(XQ_A,P_{\text{pb}})$。恢复消息$Z||Q_B||m=y\oplus H_3^A(w_2)$和$h=H_2^A(X||m)$。敌手$A$总是能够破解密文。因此，PKI→IBC方案不满足自适应选择密文攻击下的不可区分性。

(2) 正确性：与PKI→IBC方案相似，IBC→PKI方案的签名算法Z没有连同密文σ一起发送给PKI系统下的用户，PKI中的用户总是无法进行验证。

3 对文献[16]的改进

3.1 改进方案

改进的PKI→IBC方案和IBC→PKI方案包括以下算法：

(1) 系统建立算法：输入安全参数k, PKG输出阶为大素数$q(q>2^K)$的循环加法群G_1和循环乘法群G_2，其中P为G_1的生成元。选择$e:G_1\times G_1\to G_2$的一个双线性映射。选择5个安全的抗碰撞散列哈希函数$H_1:\{0,1\}^*\to G_1$, $H_2:\{0,1\}^n\times\{0,1\}^n\to Z_q^*$, $H_3:G_2\to\{0,1\}^n$, $H_4:\{0,1\}^n\to\{0,1\}^n$, $H_5:\{0,1\}^n\to Z_q^*$, $H_6:G_1\to\{0,1\}^n$, $H_7:G_1\to Z_q^*$。随机选择$s\in Z_q^*$作为系统主密钥，计算$P_{\text{pb}}=sP$。

公开系统参数$\mathrm{cp}=\{k, q, n, G_1, G_2, P, e, H_1, H_2, H_3, H_4, H_5, H_6, H_7, P_{\mathrm{pb}}\}$。

(2) 密钥生成(PKI-KG)：用户随机选择$x_A \in Z_q^*$，设置私钥$S_A = x_A$，计算公钥为$Q_A = x_A P$。

(3) 密钥提取(IBC-KG): IBC系统中的用户向PKG提交身份ID, PKG计算私钥为$S_B = sQ_B$并发送给用户，其中$Q_B = H_1(\mathrm{ID})$为公钥。

(4) PKI→IBC签密解签密：

(a) 签密：PKI中的用户输入明文m，私钥S_A和公钥Q_B，并执行以下操作。

①任意选取$k \in \{0,1\}^n$，计算$r = H_2(k, m)$, $f = e(P_{\mathrm{pb}}, Q_B)^{S_A}$。

②计算$U_1 = rP$, $U_2 = k \oplus H_3(f, x_A U_1)$, $U_3 = m \oplus H_4(k)$, $S = (r + x_A H_5(m)) \bmod n$。

③发送$\sigma = (S, U_1, U_2, U_3)$给IBC中的用户。

(b) 解签密：IBC中的用户输入密文σ，公钥Q_A和私钥S_B，并执行以下操作。

①首先计算$f = e(S_B, Q_A)$，其次计算$k = U_2 \oplus H_3(f, x_A U_1)$, $m = U_3 \oplus H_4(k)$, $V = SP - H_5(m)Q_A$。

②验证$V = U_1$，若成立，则接收消息；否则输出错误符号$\perp$。

(c) 正确性分析

$$f = e(S_B, Q_A) = e(sQ_B, x_A P) = e(P_{\mathrm{pb}}, Q_B)^{S_A} \quad (1)$$

$$\begin{aligned} V &= SP - H_5(m)Q_A = rP + x_A P H_5(m) - H_5(m)Q_A \\ &= U_1 + Q_A H_5(m) - H_5(m)Q_A = U_1 \end{aligned} \quad (2)$$

(5) IBC→PKI签密解签密：

(a) 签密：IBC中的用户输入明文m，私钥S_B和公钥Q_A，并执行以下操作。

①选取任意$k \in \{0,1\}^n$，计算$r = H_2(k, m)$, $f = rQ_A$。

②计算$U_1 = rP$, $U_2 = k \oplus H_6(f)$, $U_3 = m \oplus H_4, (k) S = rQ_B + S_B H_7(m, U_1)$。

③发送$\sigma = (S, U_1, U_2, U_3)$给PKI中的用户。

(b) 解签密：PKI中的用户输入密文σ，公钥Q_B和私钥S_A，并执行以下操作。

①计算$f = U_1 S_A$, $k = U_2 \oplus H_6(f)$, $m = U_3 \oplus H_4(k)$ 和计算$h = H_7(f, U_1, x_A U_1)$。

②验证$e(S, P) = e(U_1 + P_{\mathrm{pb}} h, Q_B)$，若成立，则接收消息；否则输出错误符号$\perp$。

(c) 正确性分析

$$f = U_1 S_A = rPx_A = rQ_A \quad (3)$$

$$\begin{aligned} e(S, P) &= e(rQ_B + S_B H_6(m, U_1), P) \\ &= e(rQ_B, P) e(S_B H_6(m, U_1), P) \\ &= e(U_1 + P_{\mathrm{pb}} H_6(m, U_1), Q_B) \end{aligned} \quad (4)$$

3.2 改进的PKI→IBC方案的安全性分析

改进的PKI→IBC方案目的是防止敌手破坏原方案的机密性与不可伪造性。

3.2.1 机密性

定理 1　在随机预言模型下，若敌手A以不可忽略的优势ε赢得PKI→IBC方案游戏，则存在挑战者C就能以$\varepsilon' \geq \varepsilon \left(1 - \frac{1}{q_1}\right)^{q_E} \frac{1}{q_3} \left(1 - \frac{q_U}{2^k}\right)$优势解决CDH问题，则称PKI→IBC方案满足自适应性选择密文攻击下不可区分。其中H_1询问、H_3询问、密钥提取询问与解签密询问的访问次数分别为q_1, q_3, q_E与q_U。

证明　挑战者C输入CDH问题的实例$(P, aP, bP) \in G_1$，目标是计算$abP \in G_1$。

系统建立：C输入安全参数k，设置$P_{\mathrm{pb}} = cP$，并公开系统参数。

阶段1：A进行多次$H_i(1 \leq i \leq 5)$询问，C维护初始为空的表$l_1 \sim l_5$。其中，l_U表示解签密预言机回应结果的列表。

H_1询问：输入ID，若询问的$\mathrm{ID}_i \neq \mathrm{ID}_j$ $j \in \{0, 1, \cdots, \tau\}$时，$C$设置$Q_i = rP$，其中$r \in Z_q^*$，并将$(\mathrm{ID}_i, Q_i, r)$保存到表$l_1$中；否则，$C$终止。

$H_i(i$=2,4,5)询问：若A对H_i进行询问时，C首先查表，若表l_i存在相应的H_i询问，则把相应结果给A；否则，C遵循随机选择$H_2, H_5 \in Z_q^*$, $H_4 \in \{0,1\}^n$的原则，返回随机结果给A。

H_3询问：若A询问H_3时，C检查$e(aP, bP) = e(P, R_i)$，若相等，C返回R_i。若$e(U_{1i}, aP) = e(P, R_i)$且$\mathrm{ID}_i = \mathrm{ID}_j$，则把表$l_3$元组$(f_i, *, h)$中的$h$返回给$A$；否则，随机选择$h \in \{0,1\}^n$给$A$。

密钥提取询问：A询问ID_i的密钥时，C首先查表l_1，若$\mathrm{ID}_i = \mathrm{ID}_j$，则模拟结束；否则，$C$计算$S_i = srP$，并将$S_i$返回给敌手$A$。

签密询问：A对消息m进行签密询问，若$\mathrm{ID}_i \neq \mathrm{ID}_j$, C将按照签密算法进行签密，生成对消息m的签密密文。若$\mathrm{ID}_i = \mathrm{ID}_j$, C通过查表得到h_2, h_3, h_4。得到$r = h_2$，计算$U_1 = h_2 P$, $U_2 = k \oplus h_3$, $U_3 = m \oplus h_4$, $S = (h_2 + S_S h_5) \bmod n$。$C$发送$\sigma$给$A$。

解签密询问：A对密文进行解签密询问时，若$f = e(rP_{\mathrm{pb}}, Q_A) = e(rcP, Q_A) = e(S_B, Q_A)$成立，则计算$R = x_j U_1$。并查询表$l_3$, l_4, l_5获得相应的结果元组(f, h_3), (k, h_4), (m, h_5)。从而得到，$k = U_2 \oplus h_3$, $m = U_3 \oplus h_4$。否则，若$\mathrm{ID}_i = \mathrm{ID}_j$，则模拟结束。

挑战阶段：A选择一个挑战身份ID_i^*和两个等长消息m_0, m_1发送C。若$\mathrm{ID}_i^* \neq \mathrm{ID}_j$，模拟结束；

否则，C选择任意$\zeta\in\{0,1\}$，执行签密算法。最后，C输出密文σ^*。

阶段2：A可以按照阶段1一样进行多项式有限次的询问，但是不能对ID_i^*进行密钥提取询问，也不能对密文σ^*进行解签密询问。

猜测：A输出猜测值ζ'。 证毕

3.2.2 不可伪造性

定理 2 在随机预言模型下，若敌手A以不可忽略的优势ε赢得PKI→IBC方案游戏，则挑战者C能以$\varepsilon'\geq\varepsilon\left(1-\frac{1}{q_1}\right)^{q_E}\left(1-\frac{q_U}{2^k}\right)$优势解决BDH问题，则称PKI→IBC方案满足自适应性选择消息攻击下不可伪造。其中H_1询问、密钥提取询问、解签密询问的访问分别为q_1, q_E, q_U。

证明 挑战者C输入BDH问题的实例$(P, aP, bP)\in G_1$，目标是计算$e(P,P)^{ab}$。

系统建立：C输入安全参数k，设置$P_{\mathrm{pb}}=aP$，并公开系统参数。

H_1询问：输入ID进行H_1询问，若$\mathrm{ID}_i\neq\mathrm{ID}_j$ $j\in\{0,1,\cdots,\tau\}$时，设置$Q_i=\alpha_iP$，其中$\alpha_i\in Z_q^*$，并将$(\mathrm{ID}_i, Q_i, \alpha_i)$保存到表$l_1$中；若$\mathrm{ID}_i=\mathrm{ID}_j$，设置$Q_j=bP$。

$H_i(i=2,4)$询问阶段：同定理1。

H_3询问：若A询问H_3时，C首先检查表l_3是否有相应元组，若存在，则返回相应元组；否则，随机选择$h\in\{0,1\}^n$给A，并保存到表l_3中。

H_5询问阶段：若敌手询问哈希H_5时，C令$H_5(m)=cP$返回给敌手A。

密钥提取询问：A询问ID_i的密钥时，C首先查表l_1，若$\mathrm{ID}_i=\mathrm{ID}_j$，则模拟结束；否则，$C$计算$S_j=bP_{\mathrm{pb}}$，并将$S_i$返回给敌手$A$。

伪造：询问结束后，敌手A输出一个伪造的签名$(\sigma^*,\mathrm{ID}_i^*)$。要求，能询问目标身份的密钥，同时也不能询问任何有关语密文是σ^*的签密。若$\mathrm{ID}_i\neq\mathrm{ID}_i^*$，$C$终止。否则，$A$输出$f^*=e(P_{\mathrm{pb}},Q_B)^{S_A}=e(aP,bP)^{S_A}=e(P,P)^{abS_A}$作为BDH问题一个实例解。 证毕

3.3 改进的IBC→PKI方案的安全性分析

改进的IBC→PKI方案是防止敌手破坏原方案的机密性。

定理 3 在随机预言模型下，若CDH问题困难，证明改进的IBC→PKI方案满足自适应性选择密文攻击下不可区分安全。

证明 挑战者C输入CDH问题的实例$(P, aP, bP)\in G_1$，目标是计算$abP\in G_1$。

系统建立：C输入安全参数k，设置$P_{\mathrm{pb}}=aP$，并公开系统参数。

阶段1：A进行多次哈希询问、签密与解签密询问。

H_1询问：输入ID，若$\mathrm{ID}_i\neq\mathrm{ID}_j$ $j\in\{0,1,\cdots,\tau\}$，C设置$Q_i=rP$，其中$r\in Z_q^*$，并将(ID_i, Q_i, r)保存到表l_1中；否则，C终止。

$H_i(i=4,6)$询问：若A对H_i进行询问时，C首先查表，若表l_i存在相应的H_i询问，则把相应结果给A；否则，C随机选择$h_i\in\{0,1\}^n(i=4,6)$发送给A。

H_7询问：对于每次新的$H_7(f_i, U_i, T_i)$询问，首先检查身份，若$\mathrm{ID}_i=\mathrm{ID}_j$，$C$返回$h_7$并用元组$(f_i, U_i, T_i, h_7)$代替$(*, U_i, T_i, h_7)$。如果满足$H_7(f_i, aP, bP, cP)$，$C$返回$f_i$。检查表$h_7$是否存在$(*, U_i, T_i, h_7)$满足$(f_i, aP, bP, U_i)$，若满足返回$f_i$；否则随机选择给$A$。

密钥提取询问：A询问ID_j的密钥时，C选取$x_j\in Z_q^*$，设置$S_i=x_j$，并将S_i返回给敌手A。

签密询问：C收A选择一个消息m，发送者的私钥S_S，进行签密询问。若$\mathrm{ID}_i\neq\mathrm{ID}_j$，$C$将按照签密算法进行签密，生成对消息$m$的签密密文。若$\mathrm{ID}_i=\mathrm{ID}_j$，$C$通过查表得到$h_2$, h_3, h_4。计算$r=h_2$, $U_1=h_2P$，$U_2=k\oplus h_3$，$U_3=m\oplus h_4$和$S=(h_2+S_Sh_5)\bmod n$。C发送σ给A。

解签密询问：C收到A发送的密文$\sigma=(S, U_1, U_2, U_3)$时，如果$\mathrm{ID}_i=\mathrm{ID}_j$，则模拟结束。若$\mathrm{ID}_i\neq\mathrm{ID}_j$，查询表$l_4$, l_6获得相应的结果元组。$k=U_2\oplus h_6$, $m=U_3\oplus h_4$。

挑战阶段：A选择一个挑战身份ID_i^*和两个等长消息m_0, m_1发送给C。若$\mathrm{ID}_i^*\neq\mathrm{ID}_j$，模拟结束；否则，$C$任意选取$\zeta\in\{0,1\}$，执行签密算法，输出密文$\sigma^*$。

阶段2：A可以按照阶段1一样进行多项式有限次的询问。

猜测：A输出猜测值ζ'。 证毕

4 性能分析

本节首先对改进的PKI→IBC方案和IBC→PKI方案进行效率分析。表1为本文方案与文献[14–16]在通信方向、通信代价及安全性上的比较。其中P为双线性对运算，E为阶乘运算。由表1看出：在通信方向中，本文与文献[16]满足双向性；在安全性上，本文与文献[14, 15]满足通信内部安全性，文献[16]中的PKI→IBC方案既不满足机密性也不满足不可伪造性，IBC→PKI方案不满足机密性；在通信代价上，本文减少了指数运算与双线性对运算。

表 1　PKI→IBC异构签密性能比较

方案	通信方向	签密	解签密	总运算量	机密性	不可伪造性
文献[14]	PKI→IBC	$1E$	$3P$	$1E$+$3P$	√	√
文献[15]	PKI→IBC	$1E$	$3P$	$1E$+$3P$	√	√
文献[16]	PKI→IBC	$1E$+$1P$	$3P$	$1E$+$4P$	×	×
文献[16]	IBC→PKI	$1E$+$1P$	$1E$+$3P$	$2E$+$4P$	×	√
本文方案	PKI→IBC	$1E$+$1P$	$1P$	$1E$+$2P$	√	√
本文方案	IBC→PKI	0	$2P$	$2P$	√	√

因此，本文改进的PKI→IBC方案和IBC→PKI方案在满足机密性与不可伪造性的同时提高了通信效率。

其次，本文利用PBC(Pairing-Based Cryptography library)库对原方案与改进方案进行实验仿真。采用类型为A的椭圆曲线$y^2 = x^3 + x \bmod n$，其生成元$|P| = 512$ bit，大素数$|q| = 1024$ bit。图1，图2，图3，图4分别表示实验1次的计算效率与仿真多次的运算效率。

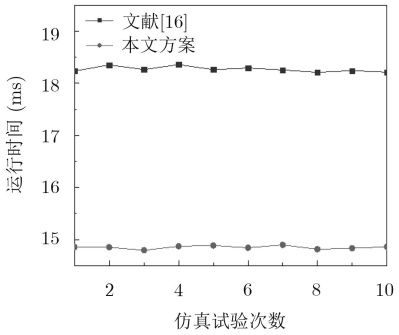

图 1 PKI→IBC签密时间

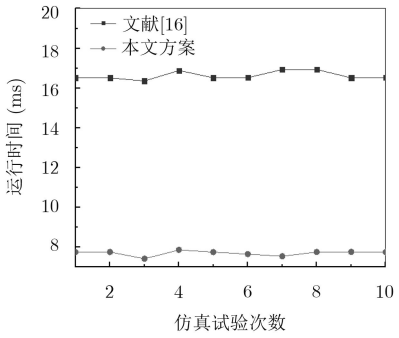

图 2 PKI→IBC解签密时间

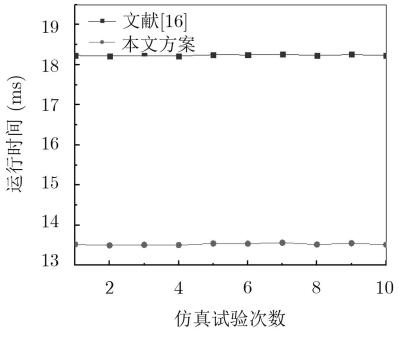

图 3 IBC→PKI签密时间

因此，由仿真实验结果可知，本文改进的PKI→IBC算法与IBC→PKI算法无论是签密时间还是解签密时间都高于文献[16]。

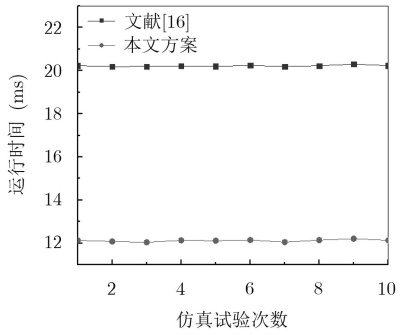

图 4 IBC→PKI解签密时间

5　结束语

本文首先指出文献[16]中提出的PKI→IBC方案与IBC→PKI方案均无法保证密文机密性。随后，提出了改进的PKI→IBC方案和IBC→PKI方案，并在随机预言模型下给出安全证明。最后，在性能分析中，改进的PKI→IBC方案与IBC→PKI方案均减少双线性对运算，提高了通信效率。然而，新方案中的系统参数依然较多，下一步的研究重点是设计更加高效的双向异构签密方案。

参 考 文 献

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

[2] VIVEK S S, SELVI S S D, KOWSALYA S S, *et al*. PKI based Signcryption without pairing: An efficient scheme with tight security reduction[J]. *Journal of Wireless Mobile Networks*, 2012, 3(4): 72–84.

[3] 李发根, 胡予濮, 李刚. 一个高效的基于身份的签密方案[J]. 计算机学报, 2006, 29(9): 1641–1647. doi: 10.3321/j.issn:0254-4164.2006.09.019.

LI Fagen, HU Yupu, and LI Geng. An efficient identity-based Signcryption scheme[J]. *Chinese Journal of Computers*, 2006, 29(9): 1641–1647. doi: 10.3321/j.issn:0254-4164.2006.09.019.

[4] 张宇, 杜瑞颖, 陈晶, 等. 对一个基于身份签密方案的分析与改进[J]. 通信学报, 2015, 36(11): 174–179. doi: 10.11959/j.issn.1000-436x.2015271.

ZHANG Yu, DU Ruiying, CHEN Jing, *et al*. Analysis and improvement of an identity-based Signcryption[J]. *Journal on Communications*, 2015, 36(11): 174–179. doi: 10.11959/j.issn.1000-436x.2015271.

[5] PANG Liaojun, GAO Lu, LI Huixian, *et al*. Anonymous multi-receiver ID-based Signcryption scheme[J]. *IET Information Security*, 2015, 9(3): 194–201. doi: 10.1049/iet-ifs.2014.0360.

[6] NAYAK B. A secure ID-based signcryption scheme based on elliptic curve cryptography[J]. *International Journal of Computational Intelligence Studies*, 2017, 6(2/3): 150–156. doi: 10.1504/IJCISTUDIES.2017.089050.

[7] 杜庆灵. 基于身份的动态群通信签密方案[J]. 信息网络安全, 2017(9): 42–44. doi: 10.3969/j.issn.1671-1122.2017.09.010.

DU Qingling. Identity-based dynamic group communication signcryption scheme[J]. *Netinfo Security*, 2017(9): 42–44. doi: 10.3969/j.issn.1671-1122.2017.09.010.

[8] SUN Yinxia and LI Hui. 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.

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

[10] LI Fagen, ZHANG Hui, and TAKAGI T. Efficient Signcryption for heterogeneous systems[J]. *IEEE Systems Journal*, 2013, 7(3): 420–429. doi: 10.1109/JSYST.2012.2221897.

[11] BENJAMIN K B, ANTHONY P, DZISOOP M D, *et al*. Heterogeneous identity-based to Certificateless online/offline Signcryption[J]. *IJISET- International Journal of Innovative Science, Engineering & Technology*, 2015.

[12] 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/JEIT160056.

LIU Jingwei, ZHANG Lihuan, and SUN Rong. Mutual Signcryption schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT160056.

[13] 张玉磊, 王欢, 刘文静, 等. 异构双向签密方案的安全性分析和改进[J]. 电子与信息学报, 2017, 39(12): 3045–3050. doi: 10.11999/JEIT170203.

ZHANG Yulei, WANG Huan, LIU Wenjing, *et al*. Security analysis and improvement of mutual Signcryption Schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(12): 3045–3050. doi: 10.11999/JEIT170203.

[14] 李臣意, 张玉磊, 张永洁, 等. 高效的TPKC→IDPKC的异构签密方案[J]. 计算机工程与应用, 2018, 54(2): 125–130. doi: 10.3778/j.issn.1002-8331.1606-0281.

LI Chenyi, ZHANG Yulei, ZHANG Yongjie, *et al*. Efficient TPKC→IDPKC heterogeneous Signcryption scheme[J]. *Computer Engineering and Applications*, 2018, 54(2): 125–130. doi: 10.3778/j.issn.1002-8331.1606-0281.

[15] 牛淑芬, 牛灵, 王彩芬, 等. 一种可证安全的异构聚合签密方案[J]. 电子与信息学报, 2017, 39(5): 1213–1218. doi: 10.11999/JEIT160829.

NIU Shufen, NIU Ling, WANG Caifen, *et al*. A provable aggregate Signcryption for heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1213–1218. doi: 10.11999/JEIT160829.

[16] 王彩芬, 刘超, 李亚红, 等. 基于PKI和IBC的双向匿名异构签密方案[J]. 通信学报, 2017, 38(10): 10–17. doi: 10.11959/j.issn.1000-436x.2017194.

WANG Caifen, LIU Chao, LI Yahong, *et al*. Two-way and anonymous heterogeneous Signcryption scheme between PKI and IBC[J]. *Journal on Communications*, 2017, 38(10): 10–17. doi: 10.11959/j.issn.1000-436x.2017194.

曹素珍：女，1976年生，副教授，研究方向为公钥密码学和软件安全.

郎晓丽：女，1993年生，硕士生，研究方向为密码学与信息安全.

刘祥震：男，1991年生，硕士生，研究方向为密码学与信息安全.

张玉磊：男，1979年生，博士，副教授，研究方向为密码学和信息安全.

王彩芬：女，1963年生，博士，教授，研究方向为密码学和信息安全.