研究与开发

一类 PKI-IBC 的双向匿名异构签密方案

冀会芳，刘连东，黄严严，程庆丰
（信息工程大学，河南 郑州 450001）

摘　要：匿名异构签密方案不仅可以实现异构密码环境下用户机密地传递数据，而且提供收发双方用户的隐私保护功能。分析发现，已有的双向匿名异构签密方案不满足消息的保密性，也无法保护发送者的隐私。提出了一个安全的 PKI↔IBC 的 MAHSC（双向匿名异构签密）方案，并分析了其安全性满足消息的保密性、签名的不可伪造性和发送者身份的匿名性。综合效率和安全性分析结果，所提方案具有较好的可行性。

关键词：异构签密；匿名签密；q-Diffie-Hellman 逆问题；双线性 Diffie-Hellman 问题
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000–0801.2020120

A mutual and anonymous heterogeneous signcryption scheme between PKI and IBC

JI Huifang, LIU Liandong, HUANG Yanyan, CHENG Qingfeng
Information Engineering University, Zhengzhou 450001, China

Abstract: Anonymous heterogeneous signcryption scheme can not only transfer data confidentially for users in heterogeneous cryptographic environment, but also provide privacy protection for users of both sending and receiving sides. The security of an anonymous heterogeneous signcryption scheme was analyzed and that it did not satisfy confidentiality and anonymity was pointed out. A new MAHSC (mutual and anonymous heterogeneous signcryption) scheme was proposed. It was analyzed that its security satisfied the confidentiality of messages, the unforgeability of signatures and the anonymity of sender's identity. The results of efficiency and security analysis show that the proposed scheme is feasible.

Key words: heterogeneous signcryption, anonymous signcryption, q-Diffie-Hellman inverse problem, bilinear Diffie-Hellman problem

1　引言

随着信息技术的飞速发展，越来越多的新型信息技术被广泛应用于医疗、农业、教育、交通运输等领域。新型信息技术的广泛应用以及人们对信息安全的需求日益增长，人们对密码技术的

收稿日期：2019–09–30；修回日期：2020–03–20
基金项目：国家自然科学基金资助项目（No.61502527，No.61872449）
Foundation Items: The National Natural Science Foundation of China (No.61502527, No.61872449)

需求不断增加，密码技术也被广泛应用于信息技术的方方面面[1]。为保证用户透明、顺畅地传递信息，跨平台的应用和操作变得越来越频繁。为保证不同密码环境之间的信息安全，异构签密问题应运而生。

自 Sun 等[2]于 2010 年首次提出异构签密的概念以来，国内外学者对异构签密展开了广泛深入的研究。继参考文献[2]中提出从 PKI 到 IBC 的异构签密方案，Huang 等[3]、Li 等[4]和李臣意等[5]分别对从 IBC 到 PKI 的异构签密方案进行了研究。王彩芬等[6]则研究了 PKI 和 IBC 之间的双向异构签密问题，同年，他们还对标准模型下安全的双向异构签密方案[7]进行了研究。

除了 PKI 和 IBC 之间的异构签密问题，学者们对 PKI 和 CLPKC 之间的异构签密问题也展开了研究，张玉磊等[8]提出了 CLPKI 到 PKI 的异构签密方案，同年，刘景伟等[9]提出了 PKI-CLPKC 的双向异构签密方案，张玉磊等[10]还研究了 5G 网络下 TPKC-CLPKC 的异构混合签密方案。

除了基本的异构签密方案，具有特殊性质的异构签密方案也成为学者们关注的重点。牛淑芬等[11]研究了从 PKI 到 IBC 的异构聚合签密问题。同年，Niu 等[12]对 CLPKC 到 IBC 的异构聚合签密方案进行了研究。张玉磊等[13]指出参考文献[12]的方案不满足不可伪造性，并对其进行了改进，进而提出了 PKI 到 CLPKC 之间的异构聚合签密方案[14]。王彩芬等[15]、牛淑芬等[16]、张玉磊等[17]还分别对异构环境下的部分盲签密方案和混合群组签密方案进行了研究。

在分析王彩芬等[6]提出的 PKI 和 IBC 之间双向异构签密方案不满足签密密文机密性的基础上，提出了一个安全的双向异构签密方案，该方案具有两个等价的签密算法，即 PIAHS（PKI→IBC 的匿名异构签密）方案和 IPAHS（IBC→PKI 的匿名异构签密）方案，并对其进行分析。结论表明，所提方案在安全性、计算消耗和通信效率等综合因素下，性能较优。

2 参考文献[6]方案的安全性分析

本文首先对参考文献[6]中双向匿名异构签密方案进行分析。受篇幅所限，本文略去对方案的描述。

2.1 对 PKI 到 IBC 解签密过程的分析

任何人可以通过以下方式解密 PKI 系统中用户向 IBC 系统中用户发送的签密文：

步骤 1 计算 $N = XP_{\text{pub}}$， $w_2 = e_{\text{B}}(N, Q_{\text{B}})$；

步骤 2 计算 $Z \| Q_{\text{A}} \| m = y \oplus H_3^{\text{B}}(w_2)$；

步骤 3 计算 $h = H_2^{\text{B}}(X \| m)$；

步骤 4 验证 $e_{\text{A}}(Z, P_{\text{A}}) = e_{\text{A}}(X + hQ_{\text{A}}, P_{\text{B}})$，若成立，则接受解密结果；否则输出 $\perp$。

2.2 对 IBC 到 PKI 解签密过程的分析

任何人可以通过以下方式解密 IBC 系统中用户向 PKI 系统中用户发送的签密文：

步骤 1 计算 $N = XP_{\text{pub}}$， $w_2 = e_{\text{A}}(N, Q_{\text{A}})$；

步骤 2 计算 $Z \| Q_{\text{B}} \| m = y \oplus H_3^{\text{A}}(w_2)$；

步骤 3 计算 $h = H_2^{\text{A}}(X \| m)$；

步骤 4 验证 $e_{\text{B}}(Z, P_{\text{B}}) = e_{\text{B}}(X + hQ_{\text{B}}, P_{\text{pub}})$，若成立，则接受解密结果；否则输出 $\perp$。

由上述分析可知，任何人都可以利用密文信息对消息进行解密，无须接收者的私钥，因此方案不满足机密性要求，进而也不满足匿名性要求。

3 新的双向匿名异构签密方案

3.1 系统参数生成算法

输入安全参数 k，系统选取两个 q 阶群 G_1 和 G_2， G_1=<P>， e：$G_1 \times G_1 \to G_2$ 是一个双线性映射。PKG 秘密保存 $s \in_R Z_q^*$ 作为系统的主密钥 s，计算 $P_{\text{pub}} = sP$ 作为系统公钥，选取 3 个 Hash 函数：$H_1 : \{0,1\}^{l_1} \to G_1$，$H_2 : \{0,1\}^{l_2+l_m} \to Z_q^*$，$H_3 : G_2 \to \{0,1\}^{2l_2+l_m}$。公开系统参数 params=$\{G_1, G_2, e, P, P_{\text{pub}}, H_i, i = 1,2,3\}$。

3.2　用户密钥生成算法

（1）PKI 系统中用户密钥生成

PKI 系统中用户 A 选取 $x_{\mathrm{A}} \in_R Z_q^*$，并将其私钥置为 $S_{\mathrm{A}} = x_{\mathrm{A}}$，计算用户公钥为 $Q_{\mathrm{A}} = x_{\mathrm{A}}P$。

（2）IBC 系统中用户密钥生成

IBC 中用户递交个人身份信息 $\mathrm{ID_B}$ 给 PKG，PKG 计算 $Q_{\mathrm{B}} = H_1(\mathrm{ID_B})$ 作为用户公钥，计算 $S_{\mathrm{B}} = sQ_{\mathrm{B}} = sH_1(\mathrm{ID_B})$ 作为用户私钥，并将其通过安全信道传送给用户。

下面分别给出 PKI→IBC 系统的异构签密（PKI→IBC heterogeneous signcryption，PIHSC）方案（签密（PISC）和解签密（PIUSC）过程）和 IBC→PKI 系统的异构签密（IBC→PKI heterogeneous signcryption，IPHSC）方案（签密（IPSC）和解签密（IPUSC）过程）的具体描述。

3.3　PIHSC 签密/解签密过程

（1）签密（PISC）

此时发送者 A 是 PKI 中的用户，接收者 B 是 IBC 系统中的用户。

A 利用其私钥 S_{A} 和 B 的公钥 Q_{B}，执行以下步骤对明文 m 进行签密：

步骤 1　随机选取 $r \in Z_q^*$，计算 $X = rQ_{\mathrm{A}}$，$T = rP_{\mathrm{pub}}$；

步骤 2　计算 $h = H_2(X, m)$，$Z = (r+h)S_{\mathrm{A}}$；

步骤 3　计算 $w = e(T, Q_{\mathrm{B}})^{S_{\mathrm{A}}}$，$y = H_3(w) \oplus (Z \| Q_{\mathrm{A}} \| m)$；

步骤 4　发送密文 $\sigma = (X, y)$ 给用户 B。

（2）解签密（PIUSC）

用户 B 输入密文 σ 和私钥 S_{B}，并执行以下步骤对密文进行解密：

步骤 1　计算 $w' = e(X, S_{\mathrm{B}})$；

步骤 2　计算 $Z \| Q_{\mathrm{A}} \| m = y \oplus H_3(w')$；

步骤 3　计算 $h = H_2(X, m)$；

步骤 4　验证 $e(ZP, P_{\mathrm{pub}}) = e(X + hQ_{\mathrm{A}}, P_{\mathrm{pub}})$ 是否成立，若成立，则接受消息 m；否则输出 $\perp$。

（3）正确性分析

验证 1　验证 1 如式（1）所示。

$$\begin{aligned} w' &= e(X, S_{\mathrm{B}}) = e(rQ_{\mathrm{A}}, sQ_{\mathrm{B}}) \\ &= e(rS_{\mathrm{A}}P, sQ_{\mathrm{B}}) = e(rP_{\mathrm{pub}}, Q_{\mathrm{B}})^{S_{\mathrm{A}}} \\ &= e(T, Q_{\mathrm{B}})^{S_{\mathrm{A}}} = w \end{aligned} \tag{1}$$

验证 2　验证 2 如式（2）所示。

$$\begin{aligned} e(ZP, P_{\mathrm{pub}}) &= e((r+h)S_{\mathrm{A}}P, P_{\mathrm{pub}}) \\ &= e(S_{\mathrm{A}}P, (r+h)P_{\mathrm{pub}}) \\ &= e(S_{\mathrm{A}}P, rP_{\mathrm{pub}})e(S_{\mathrm{A}}P, hP_{\mathrm{pub}}) \\ &= e(rQ_{\mathrm{A}}, P_{\mathrm{pub}})e(Q_{\mathrm{A}}, hP_{\mathrm{pub}}) \\ &= e(X + hQ_{\mathrm{A}}, P_{\mathrm{pub}}) \end{aligned} \tag{2}$$

3.4　IPHSC 签密/解签密过程

（1）签密（IPSC）

此时发送者 B 是 IBC 系统中用户，接收者 A 是 PKI 中的用户。

B 利用其私钥 S_{B} 和的 A 公钥 Q_{A}，执行以下步骤对明文 m 进行签密：

步骤 1　随机选取 $r \in Z_q^*$，计算 $X = rQ_{\mathrm{B}}$；

步骤 2　计算 $h = H_2(X, m)$，$Z = (r+h)S_{\mathrm{B}}$；

步骤 3　计算 $w = e(S_{\mathrm{B}}, Q_{\mathrm{A}})^r$，$y = H_3(w) \oplus (Z \| Q_{\mathrm{B}} \| m)$；

步骤 4　发送密文 $\sigma = (X, y)$ 给 PKI 中的用户 A。

（2）解签密（IPUSC）

PKI 中的用户 A 输入密文 σ 和私钥 S_{A}，并执行以下步骤：

步骤 1　计算 $w' = e(X, P_{\mathrm{pub}})^{S_{\mathrm{A}}}$；

步骤 2　计算 $Z \| Q_{\mathrm{B}} \| m = y \oplus H_3(w')$；

步骤 3　计算 $h = H_2(X, m)$；

步骤 4　验证 $e(Z, P) = e(X + hQ_{\mathrm{B}}, P_{\mathrm{pub}})$ 是否成立，若成立，则接受消息 m，否则输出 $\perp$。

（3）正确性分析

验证 3　验证 3 如式（3）所示。

$$\begin{aligned} w' &= e(X, P_{\mathrm{pub}})^{S_{\mathrm{A}}} = e(rQ_{\mathrm{B}}, S_{\mathrm{A}}sP) \\ &= e(rS_{\mathrm{A}}P, sQ_{\mathrm{B}}) = e(Q_{\mathrm{A}}, S_{\mathrm{B}})^r \\ &= w \end{aligned} \tag{3}$$

验证 4 验证 4 如式（4）所示。

$$\begin{aligned} e(Z,P) &= e((r+h)S_{\mathrm{B}},P) = e(Q_{\mathrm{B}},(r+h)P_{\mathrm{pub}}) \\ &= e(Q_{\mathrm{B}},rP_{\mathrm{pub}})e(Q_{\mathrm{B}},hP_{\mathrm{pub}}) \\ &= e(X+hQ_{\mathrm{B}},P_{\mathrm{pub}}) \end{aligned} \quad (4)$$

4 安全性分析和性能分析

本节基于参考文献[6]中定义的安全模型对所提方案的安全性进行分析。

4.1 安全性分析

定理 1 （PIHSC 的 IND-CCA2 安全性）假设存在一个 IND-CCA2 的敌手 A，能以不可忽略的优势 ε 赢得参考文献[6]定义 1 中的游戏，则存在一个挑战者 C 能以不可忽略的优势 ε^* 解决 BDH 问题，其中 $\varepsilon' \geqslant \frac{\varepsilon e}{q_2 q_3}(1-\frac{q_{\mathrm{U}}}{q_1})$，$q_i(i=1,2,3)$ 表示敌手进行 $H_i(i=1,2,3)$ 询问的最多次数，q_{E}、q_{S}、q_{U} 依次表示进行 IBC 私钥提取询问、签密询问和解签密询问的最多次数。

证明 假设 C 收到一个 BDH 问题实例 $(P,aP,bP,cP,h),a,b,c\in Z_q^*$，其目标是利用敌手解决 BDH 问题，即判断 $h=e(P,P)^{abc}$ 是否成立。挑战者 C 按照如下方式与 A 交互进行游戏。

（1）初始阶段

输入安全参数，挑战者 C 精心设置 $\mathrm{params}=\{G_1,G_2,e,P,P_{\mathrm{pub}},H_i,i=1,2,3\}$，其中 $P_{\mathrm{pub}}=cP$。然后 C 运行生成发送者的公私钥对 $(Q_{\mathrm{S}},S_{\mathrm{S}})$，并将其发送给 A。

阶段 1 挑战者 C 在交互过程中维护 5 张初始为空的列表 $L_i(i=1,2,3),L_{\mathrm{S}},L_{\mathrm{U}}$。A 进行多项式次询问。在 A 与 C 的交互过程中，假定 A 对 IBC 中用户 ID_u 首先进行 H_1 询问，且对已执行解签密询问的用户，A 不能再对其进行私钥提取询问。

H_1 询问：进行该询问前，C 选取 $j\in_R\{1,2,\cdots,q_1\}$，在第 i 次询问中，若 $i=j$，则 C 设置 $Q_i=bP$ 并返回，同时添加 $(\mathrm{ID}_i,Q_i,\perp)$ 至列表 L_1 中；若 $i\neq j$，选取 $a_i\in_R Z_q^*$，计算 $Q_i=a_iP$，返回 Q_i 并添加 (ID_i,Q_i,a_i) 至列表 L_1 中。

H_2 询问：进行该询问时，对比表 L_2 中是否存在 $(X\|m,h_2)$，如果存在，返回 h_2；否则 C 选取 $h_2\in_R Z_q^*$，添加 $(X\|m,h_2)$ 至表 L_2 中并返回 h_2。

H_3 询问：进行该询问时，对比表 L_3 中是否存在 (ω,h_3)，如果存在，返回 h_3；否则 C 选取 $h_3\in_R\{0,1\}^{2l_2+l_m}$，添加 (ω,h_3) 至表 L_3 中并返回 h_3。

私钥提取询问：进行该询问时，对于第 i 次询问身份 $\mathrm{ID}_i(1\leqslant i\leqslant q_{\mathrm{E}})$，如果 $\mathrm{ID}_i=\mathrm{ID}_j$，退出模拟，游戏终止；否则 C 计算 $S_i=a_iP_{\mathrm{pub}}$ 并返回给 A。

签密询问：进行该询问时，$\mathcal{A}$ 提交 (m,S_{S},Q_i)，若 $\mathrm{ID}_i\neq\mathrm{ID}_j$，C 利用 PIHSC 中签密算法，得到密文；否则，C 选取 $r'\in_R Z_q^*$ 并计算 $X=r'Q_{\mathrm{S}}$，查表 L_2 得 $h_2=H_2(X,m)$，计算 $Z=(r'+h_2)S_{\mathrm{S}}$，$w=e(T,Q_i)^{S_{\mathrm{S}}}$。若 $(\omega,h_3)\in L_3$，重新选取 r' 进行计算。返回密文 σ 给 A。

解签密询问：进行该询问时，A 提交 $(\sigma,Q_{\mathrm{S}},S_i)$，如果 $\mathrm{ID}_i=\mathrm{ID}_j$，模拟结束；否则 C 计算 $w=e(X,S_i)$，查询 $(X\|m,h_2)\in L_2$ 和 $(\omega,h_3)\in L_3$ 是否成立，最后返回解密结果给 A。

（2）挑战阶段

A 选择两段明文 m_0、m_1 和挑战身份 ID_i^*，并发送给 C。如果 $\mathrm{ID}_i^*\neq\mathrm{ID}_j$，模拟结束；否则 C 选取 $\mu\in_R\{0,1\}$，设置 $X^*=S_{\mathrm{S}}aP$ 和 $w=h$，计算 $y^*=H_3(w)\oplus(Z\|Q_{\mathrm{S}}\|m_\mu)$，最后返回密文 $\sigma^*=(X^*,y^*)$ 给 A。

阶段 2 按照阶段 1 中的步骤，A 执行至多多项式有界次的询问，需满足以下限制条件：不能对挑战身份 ID_i^* 进行私钥提取询问，不能对挑战密文 σ^* 进行解签密询问。

（3）猜测阶段

模拟结束后，A 输出其猜测 μ'，如果 $\mu'=\mu$，输出 $h^{1/S_{\mathrm{S}}}=e(aP,bcP)=e(P,P)^{abc}$ 作为 BDH 问题的解。

在整个模拟过程中，游戏不中止，当且仅当在游戏交互过程中，没有对挑战身份 ID_i^* 进行过私钥提取询问、签密询问和解签密询问，在挑战阶段，对挑战身份 ID_i^* 进行挑战，且 A 对 $w=h$ 进行过 H_3 询问。

若 A 能以概率 ε 赢得上述游戏，则 C 可以概率 ε' 解决 BDH 问题，其中 $\varepsilon' \geqslant \varepsilon(1-\frac{1}{q_1})^{q_S} \cdot \frac{1}{q_2}\frac{1}{q_3}(1-\frac{q_U}{q_1}) \approx \frac{\varepsilon e}{q_2 q_3}(1-\frac{q_U}{q_1})$。

定理 2　（PIHSC 的 EUF-CMA 安全性）假设存在一个 EUF-CMA 的敌手 F，能以不可忽略的优势 ε 赢得参考文献[6]定义 2 中的游戏，则存在一个挑战者 C 能以不可忽略的优势 ε' 解决 q-DHIP 问题，其中 $\varepsilon' \approx \frac{\varepsilon e}{q_2}(1-\frac{q_U}{q_1})$，$q_i(i=1,2,3)$ 表示敌手进行 $H_i(i=1,2,3)$ 询问的最多次数，q_E、q_S、q_U 表示进行 IBC 私钥提取询问、签密询问和解签密询问的最多次数。

证明　假设 C 收到一个 q-DHIP 问题实例 $(P,\alpha P,\alpha^2 P,\cdots,\alpha^q P)$，其目标是计算 $\alpha^{-1}P$。挑战者 C 按照如下方式与 F 交互进行游戏。

（1）初始阶段

挑战者 C 首先输入安全参数，设置 $\mathrm{params}=\{G_1,G_2,e,P,P_{\mathrm{pub}},H_i,i=1,2,3\}$。然后 C 设置 PKI 系统中的用户私钥 $S_S=\alpha^{-1}$。

F 向 C 进行至多 $q_i(i=1,2,3)$ 次 $H_i(i=1,2,3)$ 询问，q_E 次私钥提取询问、q_S 次签密询问和 q_U 次解签密询问，C 按照同定理 1 的方式进行回答。

（2）伪造阶段

如果游戏不中止，则 F 可以概率 ε 对消息 m 生成一个有效的密文 σ，由 Forking 引理，C 可获得关于消息 m 的两个有效签名 (m,h,Z) 和 (m,h',Z')，且满足 $h\neq h'$，由于 $Z=(r+h)S_S$ 和 $Z'=(r+h')S_S$，故可得 $Z-Z'=(h-h')S_S$，即 $S_S P=(Z-Z')(h-h')^{-1}P$。最终 C 输出 $S_S P=\alpha^{-1}P$ 作为 q-DHIP 问题的解。

在整个模拟过程中，游戏不中止，当且仅当在上述询问阶段，没有对挑战身份 ID_j 进行过私钥提取询问，且没有对其进行过与私钥使用相关的询问。因此，如果 A 能概率 ε 赢得该游戏，则 C 可以以概率 ε' 解决 q-DHIP 问题，其中 $\varepsilon' \geqslant \varepsilon(1-\frac{1}{q_1})^{q_S}\frac{1}{q_2}(1-\frac{q_U}{q_1}) \approx \frac{\varepsilon e}{q_2}(1-\frac{q_U}{q_1})$。

定理 3　（PIHSC 的匿名性）假设存在一个敌手 A，能以不可忽略的优势 ε 赢得参考文献[5]定义 3 中的游戏，则存在一个挑战者 C 能以不可忽略的优势 ε' 解决 BDH 问题，其中 $\varepsilon' \geqslant \varepsilon\frac{1}{q_1(q_1+q_S)}\left(1-\frac{q_S}{q_1}\right)\left(1-\frac{q_U}{2^k}\right)$，$q_i(i=1,2,3)$ 表示敌手进行 $H_i(i=1,2,3)$ 询问的最多次数，q_S、q_U 表示进行签密询问和解签密询问的最多次数。

该定理的证明可参见定理 1 的证明过程。

IPHSC 方案的安全性证明过程与上述定理 1~3 的证明过程类似。

4.2　性能分析

本节将本文所提方案的性能与现有异构签密方案的性能进行比较。假设 $|G_1|=|G_2|=160\ \mathrm{bit}$，$|m|=|\mathrm{ID}|=160\ \mathrm{bit}$。表 1 分别给出本文方案在通信消耗、安全性和密文长度上与已有方案的比较。

由表 1 可知，在安全性方面，本文方案与参考文献[8]中方案满足安全性的 3 项要求；在计算消耗方面，本文方案和其他方案相比，对运算数量有所增加；在密文长度方面，除了和参考文献[4]中方案相比，多了一个元素，其他方面和多数方案相当。综合考虑安全性、计算消耗和通信开销等因素，本文方案在整体性能中具有优势。

将本文方案在实验平台（Thinkpad，i5-5200 CPU @2.20 GHz，8 GB 内存）上进行仿真模拟。使用基于 Java 的密码学对运算库（JPBC），采用椭圆曲线 $y^2=x^3+x \bmod n$，$|n|=160$ bit，$|G_1|=|G_2|=160\ \mathrm{bit}$，$|m|=|\mathrm{ID}|=160\ \mathrm{bit}$。实验结果如图 1 所示。

表 1　各异构签密方案性能比较

方案	方向	计算消耗			安全性			密文长度/bit
		mul	exp	pair	IND-CCA	EUF-CMA	匿名性	
参考文献[2]	PKI→IBC	2	1	4	√	√	—	640
参考文献[2]	PKI←IBC	0	1	2	√	√	—	640
参考文献[3]	IBC→PKI	5	0	2	√	√	—	960
参考文献[3]	IBC→PKI	6	0	0	√	√	—	960
参考文献[4]	PKI→IBC	3	2	2	√	√	—	480
参考文献[4]	PKI←IBC	3	2	2	√	√	—	480
参考文献[5]	PKI→IBC	2	1	3	√	√	—	640
参考文献[6]	PKI→IBC	4	1	4	—	√	—	640
参考文献[6]	PKI←IBC	4	1	4	—	√	—	640
参考文献[8]	CLC→PKI	6	0	2	√	√	√	960
参考文献[9]	PKI→CLC	2	1	2	√	√	—	640
参考文献[9]	PKI←CLC	2	1	2	√	√	—	640
本文方案	PKI→IBC	3	1	4	√	√	√	640
本文方案	PKI←IBC	2	2	4	√	√	√	640

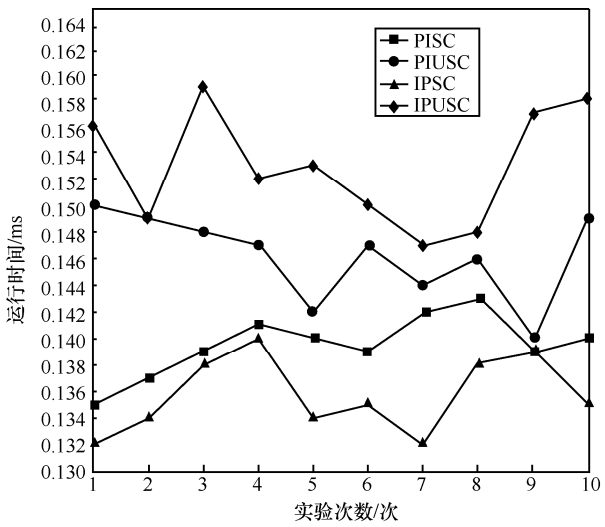

图 1　PKI-IBC 的双向签密/解签密过程

实验模拟了 10 次从 PKI 到 IBC 的签密（PISC）、解签密（PIUSC），从 IBC 到 PKI 的签密（IPSC）、解签密（PIUSC）的时间，4 类操作的平均时间分别为 0.139 5 ms、0.146 2 ms、0.135 7 ms 和 0.152 9 ms，签密时间少于解签密时间的原因在于签密阶段比解签密阶段少两个对运算。从 PKI 到 IBC 的整个签密、解签密平均时间为 0.285 7 ms，从 IBC 到 PKI 的整个签密、解签密平均时间为 0.288 6 ms。从 PKI 到 IBC 的运算时间稍短，主要是因为前者多一个标量乘运算而少一个指数运算，而标量乘运算速度快于指数运算。两个签密总的运算时间短，可以满足实际应用环境中用户对相应时间的要求，方案满足可行性要求。

5　结束语

双向匿名异构签密方案不仅可以解决不同密码环境下用户实现机密、可认证地传递信息的问题，还可以实现通信双方的隐私保护功能，成为

学界研究的热点问题。本文首先分析了参考文献[6]中方案不满足机密性要求，其原因在于任何用户无需接收者的私钥即可解签密得到明文，在此基础上提出了一个新的 PKI↔IBC 的双向匿名异构签密方案，并对方案的安全性和效率进行了分析。和已有方案相比，本文方案在综合考虑安全性、计算消耗和通信开销等因素的前提下，具有优势。如何设计出计算消耗更小、通信开销更低的方案，是下一步研究的重点。

参考文献：

[1] 高健, 陈文彬, 庞建民, 等. 基于组合密钥的智能电网多源数据安全保护[J]. 电信科学, 2020, 36(1): 134-138.
GAO J, CHEN W B, PANG J M, et al. Multi-source date security protection of smart grid based on combination key[J]. Telecommunications Science, 2020, 36(1): 134-138.

[2] SUN Y X, LI H. Efficient signcryption between TPKI and IDPKC and its multi-receiver construction[J]. Science China Information Science, 2010, 53(3): 557-566.

[3] HUANG Q, WONG D S, YANG G M. Heterogeneous signcryption with key privacy[J]. The Computer Journal, 2011, 54(4): 525-536.

[4] LI F G, ZHANG H, TAKAGI T. Efficient signcryption for heterogeneous systems[J]. IEEE Systems Journal, 2013, 7(3): 420-429.

[5] 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.
LI C Y, ZHANG Y L, ZHANG Y J, et al. Efficient TPKC→IDPKC heterogeneous signcryption scheme [J]. CEA, 2018, 54(2): 125-130.

[6] 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.
WANG C F, LIU C, LI Y H, et al. Two-way and anonymous heterogeneous signcryption scheme between PKI and IBC [J]. Journal on Communications, 2017, 38(10): 10-17.

[7] 王彩芬, 李亚红, 张玉磊, 等. 标准模型下高效的异构签密方案[J]. 电子与信息学报, 2017, 39(4): 881-886.
WANG C F, LI Y H, ZHANG Y L, et al. Efficient heterogeneous signcryption scheme in the standard model[J]. Journal of Electronics and Information Technology, 2017, 39(4): 881-886.

[8] 张玉磊, 张灵刚, 张永洁, 等. 匿名 CLPKI-TPKI 异构签密方案[J]. 电子学报, 2016, 10(10): 2432-2439.
ZHANG Y L, ZHANG L G, ZHANG Y J, et al. CP-PKC-to-PKI heterogeneous signcryption scheme with anonymous [J]. Acta Electronica Sinica, 2016, 10(10): 2432-2439.

[9] 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(1): 2948-2953.
LIU J W, ZHANG L H, SUN R. Mutual signcryption schemes under heterogeneous systems [J]. Journal of Electronics and Information Technology, 2016, 38(1): 2948-2953.

[10] 张玉磊, 骆广萍, 王欢, 等. 5G 网络下可证安全的 TPKC-CLPKC 异构混合签密方案[J]. 技术研究, 2019(5): 30-37.
ZHANG Y L, LUO G P, WANG H, et al. TPKC-CLPKC heterogeneous hybrid signcryption scheme under 5G network [J]. Netinfo Security, 2019(5): 30-37.

[11] 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.
NIU S F, NIU L, WANG C F, et al. A provable aggregate signcryption for heterogeneous systems [J]. Journal of Electronics and Information Technology, 2017, 39(5): 1213-1218.

[12] NIU S F, LI Z B, WANG C F. Privacy-preserving multi-party aggregate signcryption for heterogeneous systems[C]//Proceedings of International Conference on Cloud Computing and Security. [S.l.: s.n.], 2017: 216-229.

[13] 张玉磊, 刘祥震, 郎晓丽, 等. 新的具有隐私保护功能的异构聚合签密方案[J]. 电子与信息学报, 2018, 40(12): 3007-3012.
ZHANG Y L, LIU X Z, LANG X L, et al. New privacy preserving aggregate signcryption for heterogeneous systems [J]. Journal of Electronics and Information Technology, 2018, 40(12): 3007-3012.

[14] 张玉磊, 王欢, 刘文静, 等. 可证安全的传统公钥密码-无证书公钥密码异构聚合签密方案[J]. 电子与信息学报, 2018, 40(5): 1079-1086.
ZHANG Y L, WANG H, LIU W J, et al. Provable and secure traditional public key infrastructure- certificateless public key cryptography heterogeneous aggregate signcryption scheme [J]. Journal of Electronics and Information Technology, 2018, 40(5): 1079-1086.

[15] 王彩芬, 许钦百, 刘超, 等. 无证书公钥密码体制-传统公钥基础设施异构环境下部分盲签密方案[J]. 电子与信息学报, 2019, 41(8): 1823-1830..
WANG C F, XU Q B, LIU C, et al. Partial blind signcryption scheme in CLPKC-to-TPKI heterogeneous environment [J]. Journal of Electronics and Information Technology Journal of Electronics and Information Technology, 2019, 41(8): 1823-1830.

[16] 牛淑芬, 杨喜艳, 王彩芬, 等. 基于异构密码系统的混合群

组签密方案[J]. 电子与信息学报, 2019, 41(5): 1180-1186.
NIU S F, YANG X Y, WANG C F, et al. Hybrid group signcryption scheme based on heterogeneous cryptosystem[J]. Journal of Electronics and Information Technology, 2019, 41(5): 1180-1186.

[17] 张玉磊, 刘祥震, 郎晓丽, 等. 一种异构混合群组签密方案的安全性分析与改进[J]. 电子与信息学报, 2019, 41(11): 2708-2714.
ZHANG Y L, LIU X Z, LANG X L, et al. Security analysis and improvements of hybrid group signcryption scheme based on heterogeneous cryptosystem[J]. Journal of Electronics and Information Technology, 2019, 41(11): 2708-2714.

[作者简介]

冀会芳（1982– ），女，博士，信息工程大学讲师，主要研究方向为密码学与信息安全。

刘连东（1979– ），男，信息工程大学讲师，主要研究方向为信息安全。

黄严严（1979– ），女，信息工程大学副编审，主要研究方向为信息安全。

程庆丰（1979– ），男，博士，信息工程大学副教授，主要研究方向为密码学与信息安全。