doi:10.11959/j.issn.1000-436x.2017194

基于 PKI 和 IBC 的双向匿名异构签密方案

王彩芬，刘超，李亚红，牛淑芬，张玉磊
（西北师范大学计算机科学与工程学院，甘肃 兰州 730070）

摘 要：现有的基于传统公钥密码体制（PKI, public key infrastructure）和基于身份的密码体制（IBC, identity-based cryptosystem）之间的异构签密方案都有一定的缺陷，基于此，提出一种新的双向的基于 PKI 和 IBC 的异构签密方案。在随机预言模型中和在基于计算性 Diffie-Hellman 困难问题（CDHP, computational Diffie-Hellman problem）、*q*-Diffie-Hellman 逆问题（*q*-DHIP, *q*-Diffie-Hellman inversion problem）和双线性 Diffie-Hellman 困难问题（BDHP, bilinear Diffie-Hellman problem）的假设下，该方案满足机密性和不可伪造性。同时，该方案还满足密文的无连接性和匿名性。与已有同类异构签密方案对比，该方案不仅实现了签密的双向性，而且在 PKI 和 IBC 生成系统参数时不作限制，更加符合实际的应用环境。模拟实验表明，该方案具有可行性，并且满足用户对系统响应时间的要求。

关键词：异构签密；计算性 Diffie-Hellman 困难问题；双线性 Diffie-Hellman 困难问题；*q*-Diffie-Hellman 逆问题；密文匿名性
中图分类号：TP309.7 **文献标识码**：A

Two-way and anonymous heterogeneous signcryption scheme between PKI and IBC

WANG Cai-fen, LIU Chao, LI Ya-hong, NIU Shu-fen, ZHANG Yu-lei
（School of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China）

Abstract: Exiting heterogeneous signcryption schemes which were between public key infrastructure (PKI) and identity-based cryptosystem (IBC) have some limitations. A new heterogeneous signcryption scheme between PKI and IBC was proposed. In the random oracle mode, the scheme ensured confidentiality and unforgeability on the basis of the assumption of computational Diffie-Hellman problem (CDHP), *q*-Diffie-Hellman inversion problem (*q*-DHIP) and bilinear Diffie-Hellman problem (BDHP). Simultaneously, the proposed scheme guaranteed unconnectedness and anonymity of the ciphertext. Compared with other heterogeneous schemes, the scheme achieved two-way signcryption, and it generated parameters without restrict, which was suitable for actual situations. Simulation tests show that proposed scheme is feasible.

Key words: heterogeneous signcryption, compuatational Diffie-Hellman problem, bilinear Diffie-Hellman problem, *q*-Diffie- Hellman inversion problem, ciphertext anonymit

1 引言

1997 年，Zheng[1]首次提出了签密的概念。与传统的先签名后加密或先加密后签名的方案比较，签密方案不仅可以在一个逻辑步骤里同时完成签名和加密的功能，而且大大减小计算量。同时，签密方案很好地保证了通信过程中消息的机密性、完整性、认证性以及不可伪造性。签密方案提出后被广泛应用在实际环境中，如电子交易、手机通信以及智能卡等。

实际的应用场景，如 5G、云[2]、物联网等复杂的环境，用户分布在不同的密码体制中，而且安全

收稿日期：2017-01-24；**修回日期**：2017-05-17
基金项目：国家自然科学基金资助项目（No.61202395,No.61562077, No.61662069, No.61662071）；甘肃省自然科学基金资助项目（No. 145RJDA325）
Foundation Items: The National Natural Science Foundation of China (No.61202395, No.61562077, No.61662069, No.61662071), The Natural Science Foundation of Gansu Province (No.145RJDA325)

需求方式由普通的端端模式演变为多方通信模式[3]。然而，现有方案大部分是基于同一个密码体制即基于传统公钥密码体制、基于身份的密码体制以及基于无证书密码体制（CLPKI, certificateless public key infrastructure）。虽然部分方案实现了跨域访问机制[4,5]，但实质上这些方案还是基于同一个密码体制。因此，为了满足不同密码体制之间的信息交互，一种新的方法——异构签密方案的提出与研究成为必要。

2010 年，Sun[6]提出了一种双向的基于 PKI 和 IBC 的签密方案。但是提出的方案只给出了外部安全性证明没有满足严格的内部安全性要求。2011 年，Huang[7]提出了一种异构签密方案。但是构造的方案只实现了消息从 IBC 传递到 PKI，没有实现从 PKI 到 IBC 的签密过程。2013 年，Li[8]提出了一种新的异构签密方案，这种方案满足了内部安全性，同时实现了双向的签密过程。但是此方案在文献[9]基于身份的签密方案基础上改进，并没有实现密文的匿名性。2015 年，Benjamin 等[10]提出了一种单向的从 IBC 到 CLPKI 的在线/离线异构签密方案。但是这种方案因为对运算的明显增加而降低了效率同时也没有满足方案的匿名性。2016 年，Zhang[11]提出了从 CLPKI 到 PKI 的异构签密方案，方案实现了系统的参数不同，更加贴近实际的应用环境，而且因为只有 2 个双线性对运算，效率大大提高。

因此，本文提出一种新的基于 PKI 和 IBC 的双向匿名异构签密方案。方案满足了 IND-CCA2、EUF-CMA、内部安全性、密文无连接性和密文匿名性。与上述同类方案相比，PKI 中的用户可以完全使用自己的系统参数生成相应的密钥对，脱离了文献[6~8,10]中必须依赖 PKG 生成参数的限制。模拟实验计算出双向的签密、解签密时间，表明了本文方案在实际应用中的可行性。

2　异构签密方案的定义

一种异构签密方案由以下 5 个算法组成。

系统建立算法。系统输入安全参数 k，然后输出系统的公共参数，包括 PKG 的系统主秘钥和公钥。

PKI 密钥生成算法。PKI 中的用户运行密钥生成算法，生成自己的私钥 sk_A 并将对应的公钥 pk_A 公开。注意，用户的公钥必须被 CA 进行签名绑定。

IBC 密钥提取算法。IBC 中的用户运行密钥提取算法，递交自己的身份 ID 给 PKG。PKG 根据用户的身份 ID 计算出用户的私钥 sk_B 并将私钥 sk_B 通过安全信道发送给用户。用户的公钥 pk_B 可以选用用户的身份 ID。

签密算法。签密算法是一种概率性的算法。发送者首先输入消息 m、发送者的私钥 sk_{s} 和接收者的公钥 pk_{r}，然后运行签密算法输出密文 σ。

解签密算法。解签密算法是一个确定性算法。接收者输入接收到的密文 σ、发送者的公钥 pk_{s} 和接收者的私钥 sk_{r}，然后运行解签密算法输出明文 m 或符号 $\perp$（如果是 σ 不合法的密文）。

为了满足一致性原则，必须要求：如果签密运算能得到 $\sigma = signcrypt(m, sk_{\mathrm{s}}, pk_{\mathrm{r}})$，那么一定可以通过解签密运算得到 $m = unsigncrypt(\sigma, pk_{\mathrm{s}}, sk_{\mathrm{r}})$。

3　具体的异构签密方案

PKI 系统参数生成。系统输入一个安全参数 k_1，G_1^A 和 G_2^A 分别是阶为素数 $q_A (q_A > 2^k)$ 的加法群和循环乘法群，P_A 是群 G_1^A 的生成元，G_1^A、G_2^A 满足双线性映射：$e_A : G_1^A \times G_1^A \to G_2^A$。定义 3 个安全的散列函数：$H_1^A : \{0,1\}^{l_1} \to G_1^A$、$H_2^A : \{0,1\}^{l_1+l_m} \to Z_p^*$、$H_3^A : G_2^A \to \{0,1\}^{l_1+l_2+l_m}$。公开系统参数：$\{G_1^A, G_2^A, e_A, P_A, H_1^A, H_2^A, H_3^A\}$。

IBC 系统参数生成。系统输入一个安全参数 k_2，G_1^B, G_2^B 分别是阶为素数 $q_B (q_B > 2^k)$ 的加法群和循环乘法群，P_B 为群 G_1^B 的生成元，G_1^B、G_2^B 满足双线性映射：$e_A : G_1^B \times G_1^B \to G_2^B$。定义 3 个安全的散列函数：$H_1^B : \{0,1\}^{l_1} \to G_1^B$、$H_2^B : \{0,1\}^{l_1+l_m} \to Z_p^*$、$H_3^B : G_2^B \to \{0,1\}^{l_1+l_2+l_m}$。PKG 随机选取 $s \in Z_q^*$ 作为系统主密钥，计算 $P_{\mathrm{pub}} = sP_B$ 作为系统公钥。公开系统参数 $\{G_1^B, G_2^B, e_B, P_{\mathrm{pub}}, P_B, H_1^B, H_2^B, H_3^B\}$，保留主密钥 s。

PKI 密钥生成。PKI 中的用户随机选取 $x_A \in Z_q^*$，令 $S_A = x_A$ 作为私钥，并计算 $Q_A = x_A P_A$ 作为公钥。

IBC 密钥提取。IBC 中的用户递交 ID_B 给 PKG，并计算 $Q_B = H_1^B(ID_B)$ 作为公钥。PKG 计算 $S_B = sQ_B$ 并通过安全信道发送 S_B 给用户作为用户私钥。

3.1　PKI→IBC 签密解签密过程

1) 签密。PKI 中的用户 A 输入明文 m、私钥 S_A 和公钥 Q_B，并执行以下步骤。

① 随机选取 $r \in Z_q^*$,计算 $X = rQ_A$。

② 计算 $h = H_2^B(X \| m)$, $Z = (r+h)S_A P_B$。

③ 计算 $T = rP_{\text{pub}}P_A$。

④ 计算 $w_1 = e_B(T,Q_B)^{S_A}$, $y = H_3^B(w_1) \oplus (Z \| Q_A \| m)$。

⑤ 发送 $\sigma = (X, y)$ 给 IBC 中的用户 B。

2) 解签密。IBC 中的用户 B 输入密文 σ、公钥 Q_A 和私钥 S_B，并执行以下步骤。

① 计算 $N = XP_B$, $w_2 = e_B(N, S_B)$。

② 计算 $Z \| Q_A \| m = y \oplus H_3^B(w_2)$。

③ 计算 $h = H_2^B(X \| m)$。

④ 验证 $e_A(Z, P_A) = e_A(X + hQ_A, P_B)$，若成立，则接受消息；否则输出错误符号 $\perp$。

3) 正确性分析

验证 1

$$w_2 = e_B(N, S_B) = e_B(rx_A P_A P_B, sH_1^B(ID_B))$$
$$= e_B(rP_{\text{pub}}P_A, Q_B)^{S_A} = e_B(T, Q_B)^{S_A} = w_1$$

验证 2

$$e_A(Z, P_A) = e_A((r+h)S_A P_B, P_A) = e_A(P_B, X + hQ_A)$$

3.2 IBC→PKI 签密解签密过程

1) 签密。IBC 中的用户 B 输入明文 m、私钥 S_B 和公钥 Q_A，并执行以下步骤。

① 随机选取 $r \in Z_q^*$,计算 $X = rQ_B$, $T = rP_B$。

② 计算 $h = H_2^A(X \| m)$, $Z = (r+h)S_B$。

③ 计算 $w_1 = e_A(T,Q_A)^{S_B}$, $y = H_3^A(w_1) \oplus (Z \| Q_B \| m)$。

④ 发送 $\sigma = (X, y)$ 给 PKI 中的用户 A。

2) 解签密。PKI 中的用户 A 输入密文 σ，公钥 Q_B 和私钥 S_A，并执行以下步骤。

① 计算 $N = XP_A$, $w_2 = e_A(N, P_{\text{pub}})^{S_A}$。

② 计算 $Z \| Q_B \| m = y \oplus H_3^A(w_2)$。

③ 计算 $h = H_2^A(X \| m)$。

④ 验证 $e_B(Z, P_B) = e_B(P_{\text{pub}}, X + hQ_B)$，若成立，则接受消息；否则输出错误符号 $\perp$。

3) 正确性分析

验证 3

$$w_2 = e_A(XP_A, P_{\text{pub}})^{S_A} = e_A(rQ_B P_A, x_A sP_B)$$
$$= e_B(rP_B, Q_A)^{S_B} = e_B(N, S_B) = w_1$$

验证 4

$$e_B(Z, P_B) = e_B((r+h)S_A P_A, sP_B) = e_B(P_{\text{pub}}, X + hQ_A)$$

4 安全模型

在整个异构签密交互过程中，分为 2 个过程，简记为 PKI→IBC 和 IBC→PKI。

定义 1 PKI→IBC 的机密性。如果没有任何一个多项式时间有界的敌手以一个不可忽略的优势赢得以下游戏，则称一个异构签密方案在适应性选择密文攻击下具有不可区分性(IND-CCA2)。

1) 初始化阶段。挑战者 $\mathcal{C}$ 使用安全参数 k 进行初始化运算，并将系统参数发送给敌手 $\mathcal{A}$。$\mathcal{C}$ 运行 PKI 公私钥对生成算法生成一对发送者的公私钥对 (Q_s, S_s)，并将 (Q_s, S_s) 发送给 $\mathcal{A}$。

阶段 1 在这个阶段中，$\mathcal{A}$ 可以按照以下步骤进行多次询问。

① 密钥提取询问。$\mathcal{A}$ 选择一个身份 ID_r。$\mathcal{C}$ 运行 IBC 密钥提取算法生成 ID_r 对应的私钥 S_r，并将 S_r 发送给 $\mathcal{A}$。

② 签密询问。$\mathcal{A}$ 输入明文 m，发送者的私钥 S_s 和接收者的公钥 Q_r。$\mathcal{A}$ 将这些参数发送给 $\mathcal{C}$。$\mathcal{C}$ 运行签密算法生成 $\sigma = Signcrypt(m, S_s, Q_r)$，并将 σ 发送给 $\mathcal{A}$。

③ 解签密询问。$\mathcal{A}$ 输入密文 σ，发送者的公钥 Q_s。$\mathcal{C}$ 首次运行 IBC 密钥提取算法生成接收者的私钥 S_r。$\mathcal{C}$ 解签密 3 元组 (σ, Q_s, S_r)，然后将结果发送给 $\mathcal{A}$。如果输出的结果不合法，则输出符号 $\perp$。

2) 挑战阶段。$\mathcal{A}$ 决定什么时候结束阶段 1。$\mathcal{A}$ 产生 2 个等长的明文 m_0、m_1 和一个希望挑战的接收者的身份 ID_r^*。注意：不能在阶段 1 询问 ID_r^* 对应的私钥。$\mathcal{C}$ 输出一个随机的比特 $\beta \in \{0,1\}$，并计算 $\sigma^* = Signcrypt(m_\beta, S_s, ID_r^*)$。最后，$\mathcal{C}$ 将 σ^* 发送给 $\mathcal{A}$。

阶段 2 $\mathcal{A}$ 可以按照阶段 1 的步骤执行多项式时间有界次数的适应性询问。这一阶段，不能对 ID_r^* 进行密钥提取询问也不能对 σ^* 进行解签密询问来获得相应的明文。

3) 猜测阶段。$\mathcal{A}$ 产生一个比特 β'，如果 $\beta' = \beta$，$\mathcal{A}$ 赢得这次游戏。

定义敌手 $\mathcal{A}$ 赢得这个游戏的优势为 $Adv(\mathcal{A}) = |\Pr[\beta' = \beta] - \frac{1}{2}|$。

定义 2 PKI→IBC 的不可伪造性。如果没有任何一个多项式时间有界的敌手以一个不可忽略的优势赢得以下游戏，则称一个异构签密方案在适应性选择消息攻击下具有不可伪造性(EUF-CMA)。

1) 初始化阶段。挑战者 $\mathcal{C}$ 使用安全参数 k 进行初始化运算，并将系统参数和系统主秘钥发送给敌手 $\mathcal{F}$。$\mathcal{C}$ 运行 PKI 公私钥生成算法生成发送者的公私钥对 (Q_s,S_s)，并将 Q_s 发送给 $\mathcal{F}$。

2) 攻击阶段。$\mathcal{F}$ 适应性地执行多项式有界次数的密钥生成询问和解签密询问。在一个签密询问中，发送消息 m 和一个接收者的身份 ID_r 给 $\mathcal{C}$。$\mathcal{C}$ 运行签密算法生成 $\sigma=Signcrypt(m,Q_s,ID_r)$，并将 σ 发送给 $\mathcal{F}$。

3) 伪造阶段。$\mathcal{F}$ 产生一个接收者的身份 ID_r^* 和一个密文 σ^* (不能在签密阶段生成 σ^*)。如果对 σ^* 的解签密询问结果不是错误符号 $\perp$，$\mathcal{F}$ 将赢得这个游戏。

定义 3　PKI→IBC 密文的匿名性。密文的匿名性是指没有第三方可以截取到任何信息帮助其识别密文的发送者或密文的接收者。游戏定义如下所示。

1) 初始阶段。挑战者 $\mathcal{C}$ 使用安全参数 k 并将生成的系统参数发送给敌手 $\mathcal{A}$。

阶段 1　$\mathcal{A}$ 可以按照定义 1 中阶段 1 的方式询问 $\mathcal{C}$。在第一阶段结束时，$\mathcal{A}$ 输出消息 m，2 个发送者的私钥 $\{S_0,S_1\}$ 和 2 个接收者的身份 $\{ID_0,ID_1\}$。$\mathcal{A}$ 不能对任何一个 $\{ID_0,ID_1\}$ 做密钥提取询问。

2) 挑战阶段。$\mathcal{C}$ 随机选择 2 个比特 (b,b_*)，使用发送者的私钥 S_b 和接收者的公钥 ID_{b_*}，输出一个密文 $\sigma=(m,S_b,ID_{b_*})$，并将 σ 发送给 $\mathcal{A}$。

阶段 2　$\mathcal{A}$ 可以像第一阶段一样执行多项式有界次数的适应性询问。注意：不允许提取 $\{ID_0,ID_1\}$ 的私钥，也不允许使用 $\{ID_0,ID_1\}$ 对密文 σ 进行解签密询问。

3) 猜测阶段。$\mathcal{A}$ 产生 2 个比特 (b',b_*')。如果得到 $(b,b_*)=(b',b_*')$，则 $\mathcal{A}$ 赢得游戏。

定义敌手 $\mathcal{A}$ 赢得这场游戏的优势为 $Adv(\mathcal{A})=|\Pr[b=b'\vee b_*=b_*']-\frac{3}{4}|$。

限于篇幅有限，并且 IBC→PKI 的机密性、IBC→PKI 的不可伪造性，以及 IBC→PKI 密文的匿名性分别与定义 1~定义 3 相似，故不作过多叙述。

5　安全分析以及效率分析

5.1　安全性分析

5.1.1　PKI→IBC 的机密性

PKI→IBC 的机密性基于 BDH 困难问题。定理 1 证明了 PKI→IBC 签密方案满足机密性。

定理 1　在随机预言模型下，如果一个 IND-CCA2 敌手 $\mathcal{A}$ 能在时间 t 内，以 ε 的优势赢得定义 1 的游戏（最多能进行 $q_{H_i^B}$ 次 $H_i^B(i=1,2,3)$ 询问、q_s 次签密询问和 q_u 次解签密询问），则存在一个挑战者 $\mathcal{C}$ 能够在 $t'\leqslant t+(2q_s+3q_u)t_e$ 时间内，以 $\varepsilon'\geqslant\dfrac{\varepsilon e}{q_{H_1^B}q_{H_2^B}\left(1-\frac{q_u}{2^k}\right)}$ 的优势解决 BDH 问题，其中，t_e 代表一次双线性对运算所需要的时间。

证明　挑战者 $\mathcal{C}$ 接收一个随机 BDH 问题实例 $<P_B,aP_B,bP_B,cP_B>$，他的目标是计算 $e(P_B,P_B)^{abc}$。在这个游戏中 $\mathcal{A}$ 作为 $\mathcal{C}$ 的子程序。定理 1 的证明如下。

1) 初始阶段。在游戏开始时，$\mathcal{C}$ 首先输入安全参数并且设置系统参数 $\{G_1^A,G_2^A,e_A,P_A,H_1^A,H_2^A,H_3^A,G_1^B\ G_2^B,e_B,P_B,P_{\text{pub}},H_1^B,H_2^B,H_3^B\}$，其中，$P_{\text{pub}}=cP_B$（$\mathcal{C}$ 不知道系统的主密钥 c）。然后，$\mathcal{C}$ 运行 PKI 密钥生成算法生成发送者的公私钥对 (Q_s,S_s) 并将结果发送给 $\mathcal{A}$。

阶段 1　$\mathcal{C}$ 在游戏中维护 5 张表 L_1、L_2、L_3、L_s、L_u，开始时表为空。表 L_1、L_2、L_3 用来保存 $\mathcal{A}$ 对随机预言机 $H_i^B(i=1,2,3)$ 的询问，表 L_s 用来模拟 $\mathcal{A}$ 对签密预言机的询问，L_u 用来模拟 $\mathcal{A}$ 对解签密预言机的询问。$\mathcal{A}$ 对 $\mathcal{C}$ 执行多项式有界次数的询问。为了满足一致性原则，必须满足如下性质：① 在对 ID_u 进行其他询问前，必须先对 ID_u 执行 H_1^B 询问；② 假设每一次询问都不一样；③ $\mathcal{A}$ 不会使用签密询问结果去执行解签密询问；④ 如果 ID_u 已经被用来执行了密钥提取询问，那么敌手不能询问 ID_u 对应的私钥。初始化这些列表按照如下步骤执行。

H_1^B 询问。$\mathcal{C}$ 从 $\{1,2,\cdots,q_{H_1}\}$ 中选择一个随机数 j。在第 i 次询问中，如果 $i=j$，$\mathcal{C}$ 返回 $Q_i=bP_B$ 设置 $ID_i=ID_j$，并将 $(ID_i,Q_i,\perp)$ 添加到表 L_1 中（其中，bP_B 的系数不合法表示为 $\perp$）。如果 $i\neq j$，$\mathcal{C}$ 随机选择 $a_i\in Z_q^*$，计算 $Q_i=a_iP_B$，返回 a_iP_B 并将 (ID_i,Q_i,a_i) 存储在表 L_1 中。

H_2^B 询问。如果 $(X\|m,h_2)$ 在表 L_2 中，返回 h_2；否则，$\mathcal{C}$ 随机选择 $h_2\in Z_p^*$，存储 $(X\|m,h_2)$ 在表 L_2 中，并且将 h_2 返回给 $\mathcal{A}$。

H_3^B 询问。如果 (w,h_3) 在表 L_3 中，返回 L_3；否则，$\mathcal{C}$ 随机选择 $h_3\in\{0,1\}^{l_1+l_2+l_m}$，存储 (w,h_3) 在 L_3 中，

并且将 h_3 返回给 $\mathcal{A}$。

密钥提取询问。$\mathcal{A}$ 对 $ID_i(1\leqslant i\leqslant q_E)$ 进行密钥提取询问。查询元组 (ID_i,Q_i,a_i) 是否在表 L_1 中。如果 $ID_i=ID_j$，模拟结束；否则，$\mathcal{C}$ 计算 $S_i=c(Q_i)=c(a_iP_B)=a_iP_{\text{pub}}$，并将 S_i 返回给 $\mathcal{A}$。

签密询问。$\mathcal{A}$ 选择一个消息 m，发送者的私钥 S_s 和接收者的公钥 Q_i。$\mathcal{A}$ 对 (m,S_s,ID_i) 进行签密询问。如果 $ID_i\neq ID_j$，$\mathcal{C}$ 按照正常签密算法的步骤得到密文。如果 $ID_i=ID_j$，$\mathcal{C}$ 选择 $r'\in Z_p^*$，计算 $X=r'Q_s$，并且通过查表 L_2 得到 $h_2=H_2^B(X\,\|\,m)$。$\mathcal{C}$ 计算 $Z=(r'+h_2)S_rP_B$ 和 $w_1=e_B(T,Q_B)^{S_A}$。如果 (w,h_3) 已经在 L_3 中，$\mathcal{C}$ 重新选择 r'。最后，$\mathcal{C}$ 返回密文 σ 给 $\mathcal{A}$。

解签密询问。$\mathcal{C}$ 收到密文 σ，输入发送者的公钥 Q_s 和接收者的私钥 S_i，对 (σ,Q_s,S_i) 执行解签密询问。如果 $ID_i=ID_j$，模拟结束。如果 $ID_i\neq ID_j$，$\mathcal{C}$ 计算 $w_2=e_B(N,S_{ID_i})$，并查询 $(X\,\|\,m,h_2)$ 和 (w,h_3) 是否在表 L_2 和 L_3 中。最后，$\mathcal{C}$ 返回 m 给 $\mathcal{A}$。

2) 挑战阶段。$\mathcal{A}$ 产生 2 个等长的明文 M_0、M_1 和一个希望挑战的身份 ID_i^*。$\mathcal{A}$ 发送这些信息给 $\mathcal{C}$。如果 $ID_i^*\neq ID_j$，模拟结束。否则，$\mathcal{C}$ 选择 $\mu\in\{0,1\}$，设置 $N^*=aP_B$ 和 $w_2=h$（h 是 BDH 困难问题候选答案），计算 $y^*=H_3^B(w)\oplus(Z\,\|\,Q_s^*\,\|\,m_\mu)$。最后，$\mathcal{C}$ 发送密文 $\sigma^*=(X^*,y^*)$ 给 $\mathcal{A}$。

阶段 2 $\mathcal{A}$ 可以按照阶段 1 中的步骤执行多项式有界次数的询问。$\mathcal{A}$ 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。

3) 猜测阶段。当模拟结束时，$\mathcal{A}$ 输出 μ'。如果 $\mu=\mu'$，输出 $h=e_B(N^*,S_{ID_i})=e(aP_B,cbP_B)=e(P_B,P_B)^{abc}$ 作为 BDH 困难问题的解。否则，$\mathcal{C}$ 不能解决 BDH 困难问题。$\mathcal{C}$ 获胜的概率分析如下。

在密钥提取询问中，$\mathcal{A}$ 没有询问 ID_j 对应的私钥的概率为 $\frac{1}{q_{H_1^B}}$。$\mathcal{A}$ 没有对 ID_j 做密钥提取询问的概率是 $p_1\geqslant(1-\frac{1}{q_{H_1^B}})^{q_E}$。$\mathcal{A}$ 选择 ID_j 作为挑战身份的概率是 $p_2\geqslant\frac{1}{q_{H_1^B}}$。$\mathcal{A}$ 没有询问候选答案 h 的概率是 $p_3\geqslant\frac{1}{q_{H_2^B}}$。$\mathcal{A}$ 没有在解签密阶段因为拒绝一个合法签密结果而退出的概率是 $p_4\geqslant(1-\frac{q_u}{2^k})$。因此，可以得到

$$\varepsilon'=\varepsilon p_1p_2p_3p_4\geqslant\varepsilon\left(1-\frac{1}{q_{H_1^B}}\right)^{q_E}\left(\frac{1}{q_{H_1^B}}\right)\left(\frac{1}{q_{H_2^B}}\right)\left(1-\frac{q_u}{2^k}\right)$$

$$\approx\varepsilon\frac{e}{q_{H_1^B}q_{H_2^B}}\left(1-\frac{q_u}{2^k}\right)$$

在计算 $\mathcal{C}$ 获胜时间时，$\mathcal{C}$ 至多需要一个双线性运算在签密询问中和 3 个双线对运算在解签密询问中。因此，可以得到 $t'\leqslant t+(2q_s+3q_u)t_e$（$t_e$ 代表一次双线性对运算需要的时间，下同）。

5.1.2 PKI→IBC 的不可伪造性

PKI→IBC 的不可伪造性是基于 q-DHIP 困难问题。定理 2 证明了 PKI→IBC 签密方案满足不可伪造性。

定理 2 在随机预言模型下，如果一个 EUF-CMA 敌手 $\mathcal{F}$ 能在时间 t 内，以 ε 的优势赢得定义 2 的游戏(最多能进行 $q_{H_1^B}$ 次 $(H_i^B,i=1,2,3)$ 询问，q_s 次签密询问和 q_u 次解签密询问)，则存在一个挑战者 $\mathcal{C}$ 能够在时间 $t'\leqslant t+q_st_e$ 内，以 $\varepsilon'\geqslant\frac{\varepsilon e}{q_{H_1^B}(1-\frac{q_u}{2^k})}$ 的优势解决 q-DHIP。

挑战者 $\mathcal{C}$ 接收一个随机 q-DHIP 问题实例 $<P_B,\alpha P_B,\alpha^2P_B,\cdots,\alpha^qP_B>$，目标是计算 $\left(\frac{1}{\alpha}\right)P_B$。在这个游戏中 $\mathcal{F}$ 作为 $\mathcal{C}$ 的子程序。以下给出定理 2 的证明。

证明 询问阶段。$\mathcal{F}$ 可以向 $\mathcal{C}$ 提出多项式有界次的散列询问、签密询问和解签密询问，具体过程同定理 1。除此之外，$\mathcal{C}$ 将发送者的私钥 $S_s=\alpha^{-1}$ 发送给 $\mathcal{F}$。

伪造阶段。如果 $\mathcal{C}$ 没有终止，则在没有做过 ID_j 的密钥提取询问和签密询问的条件下，以一个不可忽略的概率 ε 对一个输入消息 m 生成有效签密 σ。由交叉引理可知，通过对 $\mathcal{F}$ 散列重放，$\mathcal{C}$ 可以获得关于消息 m 的 2 个有效签名 (m,h,Z) 和 (m,h',Z')，其中，$h\neq h'$。并且一个合法的签密满足等式 $Z=(r+h)S_{\text{Alice}}P_B$。由此可以构造 2 个等式 $Z=(r+h)S_{\text{Alice}}P_B$ 和 $Z'=(r+h')S_{\text{Alice}}P_B$。两式相减，得 $Z-Z'=(h-h')S_sP_B$，即 $S_sP_B=(Z-Z')(h-h')^{-1}$。最终，$\mathcal{C}$ 可以输出 $S_sP_B=\alpha^{-1}P$ 作为 q-DHIP 问题的解。如下分析 $\mathcal{C}$ 获胜的概率。

在一个密钥提取询问中，没有询问 ID_j 对应的私钥的概率为 $\frac{1}{q_{H_1^B}}$。没有对 ID_j 做密钥提取询问的概率是 $p_1 \geqslant \left(1-\frac{1}{q_{H_1^B}}\right)^{q_E}$。在伪造阶段，$\mathcal{F}$ 选择 ID_j 作为身份的概率是 $p_2 \geqslant \frac{1}{q_{H_1^B}}$。$\mathcal{C}$ 没有在解签密阶段因为拒绝一个合法签密结果而退出的概率是 $p_3 \geqslant \left(1-\frac{q_u}{2^k}\right)$，因此，可以得到

$$\varepsilon' = \varepsilon p_1 p_2 p_3 \geqslant \varepsilon\left(1-\frac{1}{q_{H_1^B}}\right)^{q_E}\left(\frac{1}{q_{H_1^B}}\right)\left(1-\frac{q_u}{2^k}\right) \approx \varepsilon\frac{e}{q_{H_1^B}}\left(1-\frac{q_u}{2^k}\right)$$

在计算 $\mathcal{C}$ 获胜时间时，$\mathcal{C}$ 在解签密询问中至多需要一个双线运算。因此，可以得到 $t' \leqslant t + q_s t_e$。

略去证明过程，只给出解决困难问题的优势概率。

5.1.3　IBC→PKI 的机密性

定理 3　随机预言模型下，如果存在一个敌手 $\mathcal{A}$ 能以 ε 的优势赢得 IBC→PKI 的机密性的游戏（最多能进行 $q_{H_1^B}$ 次 H_1^B 询问、$q_{H_i^A}$ 次 H_i^A (i=2,3)询问、q_s 次签密询问和 q_u 次解签密询问），则存在一个挑战者 $\mathcal{C}$ 能够以 $\varepsilon' \geqslant \frac{\varepsilon e\left(1-\frac{q_u}{2^k}\right)}{q_{H_1^B}(q_{H_2^A}+q_{H_3^A})}$ 的优势解决 BDH 困难问题。

5.1.4　IBC→PKI 的不可伪造性

定理 4　随机预言模型下，如果存在一个敌手 $\mathcal{F}$ 能以 ε 的优势赢得 IBC→PKI 的不可伪造性的游戏（最多能进行 $q_{H_1^B}$ 次 H_1^B 询问、$q_{H_i^A}$ 次 H_i^A (i=2,3) 询问、q_s 次签密询问和 q_u 次解签密询问），则存在一个挑战者 $\mathcal{C}$ 能够以 $\varepsilon' \geqslant \frac{\varepsilon e(1-\frac{q_u}{2^k})}{q_{H_1^B}}$ 的优势解决 CDH 困难问题。

5.1.5　PKI→IBC 和 IBC→PKI 密文的匿名性

定理 5　随机预言模型下，如果存在一个敌手 $\mathcal{A}$ 能以 ε 的优势赢得定义 3 的游戏（最多能进行 $q_{H_i^B}$ 次 $H_i^B(i=1,2,3)$ 询问、q_s 次签密询问和 q_u 次解签密询问），则存在一个挑战者 $\mathcal{C}$ 能够以 $\varepsilon' \geqslant \frac{\left(1-\frac{q_s}{q_{H_1^B}}\right)\left(1-\frac{q_u}{2^k}\right)}{q_{H_1^B}(q_{H_2^B}+q_s)}$ 的优势解决 BDH 困难问题。

定理 6　在随机预言模型下，如果存在一个敌手 $\mathcal{A}$ 能以 ε 的优势赢得 IBC→PKI 密文的匿名性的游戏(最多能进行 $q_{H_1^B}$ 次 H_1^B 询问、$q_{H_i^A}$ 次 $H_i^A(i=2,3)$ 询问、q_s 次签密询问和 q_u 次解签密询问），则存在一个挑战者 $\mathcal{C}$ 能够以 $\varepsilon' \geqslant \frac{\left(1-\frac{q_s}{q_{H_1^B}}\right)\left(1-\frac{q_u}{2^k}\right)}{q_{H_2^A}+q_{H_3^A}+q_s}$ 的优势解决 BDH 困难问题。

5.2　效率分析

从通信量、安全性、通信方向以及密钥和密文长度上来综合评价本文方案。表 1 为本文方案与文献[6~8,11]

表 1　本文方案与文献[6~8,11]中的方案在安全性、通信量以及通信方向上进行比较

方案	安全性					通信量				通信方向
	IND-CCA2	EUF-CMA	内部安全性	密文无连接性	密文匿名性	mul	exp	mod	pair	
SUN-1	是	是	否	否	否	2	1	0	2	PKI→IBC
SUN-2	是	否	否	否	否	0	1	0	2	IBC→PKI
HUANG-1	是	是	是	否	否	5	0	0	2	IBC→PKI
HUANG-2	是	是	是	否	否	6	0	1	0	IBC→PKI
LI-1	是	是	是	否	否	3	2	0	2	PKI→IBC
LI-2	是	是	是	否	否	3	2	0	2	IBC→PKI
ZHANG	是	是	是	是	是	4	0	0	2	CLPKI→IBC
HSC-1	是	是	是	是	是	4	1	0	4	PKI→IBC
HSC-2	是	是	是	是	是	4	2	0	4	IBC→PKI

中的方案进行比较，分别用 SUN-1 和 SUN-2 代表文献[6]中的方案 1 和方案 2，HUANG-1 和 HUANG-2 代表文献[7]中的方案 1 和方案 2，LI-1 和 LI-2 代表文献[8]中的方案 1 和方案 2，ZHANG 代表文献[11]中的方案，HSC-1 和 HSC-2 代表本文方案的 1 和方案 2。为了简便，用 exp 表示 G_2 中的指数运算，用 mul 表示 G_1 中的标量乘法运算，用 pair 表示双线性对运算，mod 表示取摸运算。

假设 $|G_1|=160$ bit，$G_2=160$ bit，$|p|=160$ bit，$|m|=160$ bit，$|ID|=160$ bit。表 2 分别计算出文献[6~8,11]和本文方案的密钥长度以及密文长度。

表 2 本文方案与文献[6~8,11]中的方案在密钥长度、密文长度上的比较

方案	CLPKI/PKI 密钥长度/bit	IBC 密钥长度/bit	密文长度/bit
SUN-1	320	320	640
SUN-2	320	320	640
HUANG-1	320	480	960
HUANG-2	320	480	960
LI-1	320	320	480
LI-2	320	320	480
HSC-1	320	320	320
HSC-2	320	320	320
ZHANG	320	320	800

从表 1 和表 2 综合分析：1) 安全性方面，本文方案仅与文献[11]满足表 1 所列全部安全性要求，安全性高；2) 通信方面，本文方案仅与文献[8]满足通信的双向性；3) 密钥长度、密文长度方面，本文方案有着最小的密钥长度和密文长度，在存储密钥和密文上十分节约空间；4) 通信量方面，本文方案在 pair 有所增加，exp 和 mul 与其他方案比较运算量适中。因此，本文方案在安全性提高的同时，通信量有所增加。

在 2 台处理器是 Intel Core i5，主频是 3.10 GHz 的 4CPU 计算机上进行模拟。同时使用了基于 Java 的密码学对运算库(JPBC)。对运算建立在椭圆曲线 $y^2=x^3+x \bmod q$ 上。设置的参数为 $|q|=154$ bit，$|G_1|=|G_2|=128$ bit，$|Message|=|ID|=1\,024$ bit。

在实验中，模拟了用户 *A* 和用户 *B*，用户 *A* 在 PKI 中，用户 *B* 在 IBC 中。用户 *A* 和用户 *B* 的交互过程，如图 1 所示。

根据图 1 的交互过程，分别画出 PKI→IBC 和 IBC→PKI 的签密、解签密时间图，如图 2 和图 3 所示。从 PKI 到 IBC 的平均签密、解签密时间分别是：0.158 2 s 和 0.146 2 s，从 IBC 到 PKI 的时间分别是：0.086 0 s 和 0.146 6 s。

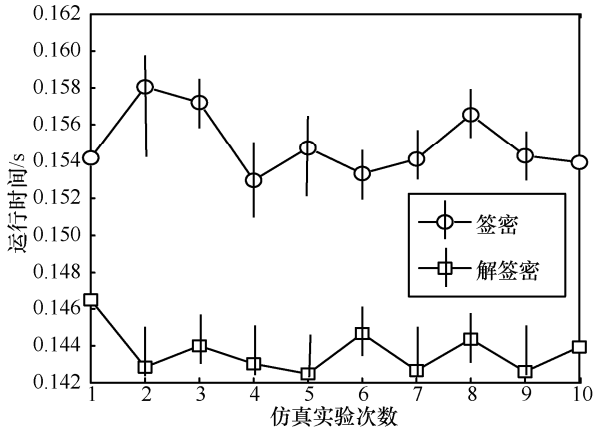

图 2 PKI→IBC 签密、解签密时间

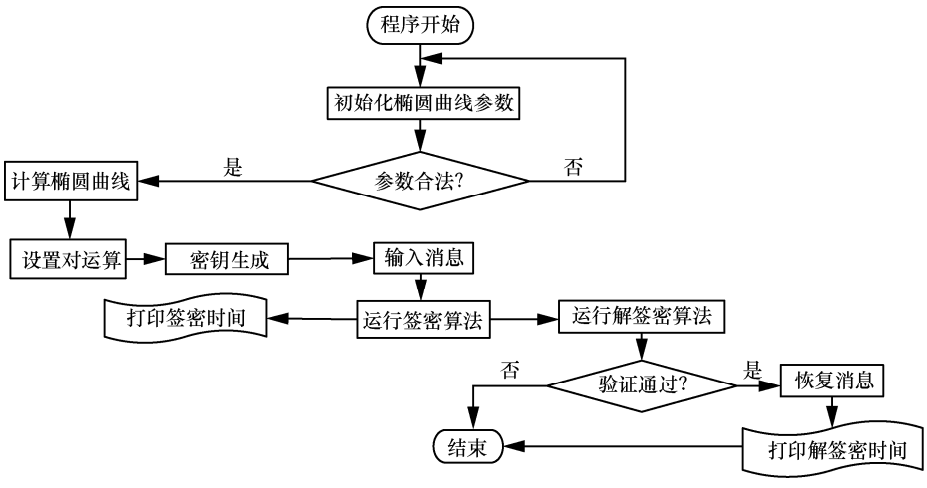

图 1 交互流程

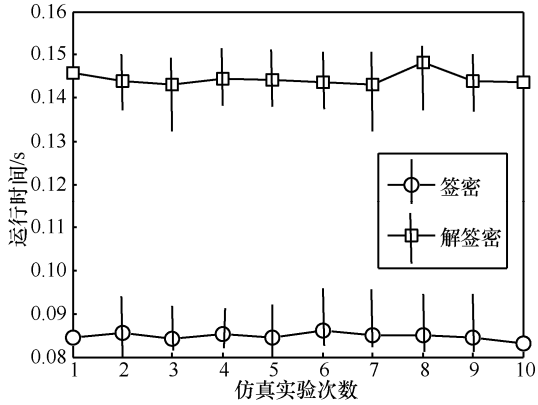

图 3　IBC→PKI 签密、解签密时间

PKI→IBC 和 IBC→PKI 整个签密、解签密平均总时间分别为 0.304 4 s 和 0.232 6 s。IBC→PKI 比 PKI→IBC 时间短的原因是，在签密阶段前者比后者少一个 G_1 上的乘法运算。2 个阶段的签密总时间短，可以满足实际环境中用户对系统响应时间的要求。因此，本文方案满足可行性要求。

6　结束语

本文提出了一个新的基于 PKI 和 IBC 的双向匿名异构签密方案，方案在满足机密性、不可伪造性、完整性以及可验证性的基础上，满足密文的无连接性和匿名性。与已有的方案相比较，本文方案不仅满足了安全性和交互的双向性，而且通信量适中。模拟实验表明，本文方案可以应用在实际环境中，并且满足用户对系统响应时间的需求。

参考文献：

[1] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption)<< cost (signature) + cost(encryption)[C]//International Cryptology Conference on Advances. 1997: 165-179.

[2] LIU Z, WENG J, LI J, et al. Cloud-based electronic health record system supporting fuzzy keyword search[J]. Soft Computing, 2016, 20(8):1-13.

[3] 曹珍富. 密码学的新发展[J].四川大学学报, 2015, 47(1):1-12.
CAO Z F. New development of cryptography[J]. Journal of Sichuan University, 2015, 47(1):1-12.

[4] ZHENG J, GUO X, ZHANG Q, et al. A cross-domain authentication protocol based on ID[J]. International Journal of Computer Science Issues, 2013, 10(1): 264-270.

[5] ZHANG X, LI G, HAN W, et al. A novel ID-based multi-domain handover protocol for mesh points in WMNs[J]. KSII Transactions on Internet & Information Systems, 2015, 9: 2512-2529.

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

[7] HUANG Q. Heterogeneous signcryption with key privacy[J]. Computer Journal, 2011 54 (4): 525-536.

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

[9] BARRETO P, LIBERT B, MCCULLAGH N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[J]. Advances in Cryptology-ASIACRYPT, 2005, 3788: 515-532.

[10] 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.

[11] 张玉磊, 张灵刚, 张永洁, 等. 匿名 CLPKC-TPKI 异构签密方案[J]. 电子与信息学报, 2016, 44(10): 2432-2439.
ZHANG Y L, ZHANG L G, ZHANG Y J, et al. CLPKC-to-TPKC heterogeneous signcryption scheme with anonymity[J]. Acta Electronica Sinica, 2016, 44(10): 2432-2439.

作者简介：

王彩芬（1963-），女，河北安国人，博士，西北师范大学教授、博士生导师，主要研究方向为无线传感器、安全协议与分析、签密、格密码学。

刘超（1989-），男，山东淄博人，西北师范大学硕士生，主要研究方向为网络与信息安全、签密。

李亚红（1985-），女，甘肃定西人，西北师范大学博士生，主要研究方向为信息安全密码学、混淆、格密码学。

牛淑芬（1978-），女，甘肃通渭人，博士，西北师范大学副教授、硕士生导师，主要研究方向为无线传感网络、云计算安全、网络编码。

张玉磊（1979-），男，甘肃靖远人，博士，西北师范大学副教授、硕士生导师，主要研究方向为网络与信息安全、密码学、安全协议分析与设计。