doi:10.11959/j.issn.1000-436x.2015187

基于身份的多接收者匿名签密改进方案

张波[1,2,3]，孙涛[1,2]，于代荣[1,2]

（1. 济南大学 信息科学与工程学院，山东 济南 250022； 2. 山东省网络环境智能计算技术重点实验室，山东 济南 250022；
3. 山东省软件工程重点实验室，山东 济南 250101）

摘 要：对庞等提出的首个考虑发送者和接收者双重匿名性的基于身份的多接收者匿名签密方案进行安全性分析，结果表明该方案不满足选择密文攻击下的密文不可区分性，在现有安全模型下，攻击者可以区分不同消息的签密密文。提出一个在随机预言模型下选定身份安全的改进方案，新方案在 CDH 和 Gap-BDH 困难问题假设下分别满足密文的存在不可伪造性和不可区分性。

关键词：匿名性；多接收者签密；基于身份签密；随机预言

中图分类号：TP309 **文献标识码**：A

Improved identity based multi-receiver anonymous signcryption scheme

ZHANG Bo[1,2,3], SUN Tao[1,2] ,YU Dai-rong[1,2]

(1. School of Information Science and Engineering, University of Jinan, Jinan 250022, China;
2. Shandong Provincial Key Laboratory of Network Based Intelligent Computing, Jinan 250022, China;
3. Shandong Provincial Key Laboratory of Software Engineering, Jinan 250101, China)

Abstract: Recently, Pang, *et al* proposed a novel identity based multi-receiver anonymous signcryption scheme (IBMRASC), which put into consideration both the sender's anonymity and the receiver's anonymity simultaneously. However, the analysis with respect to this scheme indicated that, under existing security models the adversary can distinguish the ciphertexts associated with different plaintexts. Therefore, Pang's approach did not satisfy the requirement of indistinguishability against chosen ciphertext attacks (CCA). An improved scheme which is selective identity secure in the random oracle model was proposed. Under the CDH and Gap-BDH hard problem assumption, the improved scheme is both existentially unforgetable against chosen message attack and indistinguishable against adaptive CCA.

Key words: anonymity; multi-receivers signcryption; identity based signcryption; random oracle

1 引言

保密性、认证性以及不可否认性是开放网络通信过程中需要满足的基本安全目标，可由密码技术中的加密算法和签名算法分别实现。在密码学技术支持下，陆续出现的电子商务平台、移动信息化平台、电子政务专网等系统已经取得了良好的经济效益和社会效益。然而，这些系统在带来无限商机和便利的同时，也面临着新的攻击形式，攻击者可能会试图获取通信双方的身份等敏感信息。而在很多网络应用中，例如 Internet 中的匿名 E-mail、Web 消息浏览与发布、电子支付以及军事、国防等移动通信与计算等，通信双方的身份是应该受到保护的隐私信息。身份信息的私密性也是实体在网络世界中进行某些政治、经济、文化活动的先决条件之一。

收稿日期：2014-10-10；**修回日期**：2015-03-10

基金项目：山东省自然科学基金资助项目(ZR2014FL011, ZR2013FL003)；山东省高等学校科技计划基金资助项目(J13LN21)

Foundation Items: The Natural Science Foundation of Shandong Province(ZR2014FL011, ZR2013FL003); The Higher Educational Science and Technology Program of Shandong Province(J13LN21)

为减低通信和计算代价，1997 年，Zheng[1]提出了被称为“签密（signcryption）”的密码学概念，在单个逻辑步骤内完成加密和签名 2 种操作。因其注重的混合安全目标切合实际应用环境安全需求，签密方案的研究引起了国内外学者的关注，在基于证书、基于身份[2]、无证书等密码架构下的典型方案被先后提出。在数字签密体制中，实体的隐私主要指匿名性。“基于身份”密码体制中的公钥可由用户身份信息进行数学推演得到，这就决定了用户身份与其通信行为的联系紧密而直接。而“匿名性”则要求隐藏用户身份信息，保护用户行为不被攻击者掌握。与传统的基于证书公钥密码体制相比，在基于身份密码架构下对匿名特性的研究更有针对性和挑战性。

环签密是一种能够隐藏发送者身份的密码学方案，在该方案中，发送者可以自主地产生签密环，将自己隐藏在一个用户群组中，因为环中成员可以产生不可区分的签密密文，所以攻击者能够确定信息发送者身份的概率与环中用户个数成反比，从而实现发送者的匿名性。2005 年，Huang 等[3]提出了首个基于身份的环签名和环签密方案，但该方案计算和通信效率都不够高。在此之后，大量基于身份的环签密方案[4~11]被陆续提出。在接收者为多人的应用环境中，目前已知的大多数多接收者签密方案[12~15]均没有考虑接收者匿名的问题，所有授权用户的身份信息及其关联顺序是密文的一部分，密文信息直接暴露接收者身份。为解决接收者隐私保护的问题，2011 年，庞辽军等[16]将签密者身份混淆于一个身份集合中，密文中不包含接收者身份列表，在实现信息发送者匿名性的同时，也实现了接收者身份信息的保密性。庞辽军等的方案（以下简称 PCL 方案）是首个考虑发送者和接收者双重匿名性的方案，具体方案的构造使用了双线性对和拉格朗日插值多项式技术。在 PCL 方案提出后，又陆续出现了多篇具有匿名特性的多接收者签密方案[17~19]。

本文分析后的结果表明：PCL 方案不满足选定身份自适应选择密文攻击下的密文不可区分性，攻击者可以在获得某些签密密文后伪造挑战密文，发起解签密询问，进而对签密密文进行区分。为解决这一问题，本文在文献[20,21]的基础上，提出一个可证明安全的 IBMRASC 具体方案。改进方案的安全性基于计算 Diffie-Hellman（CDH, computational diffie-hellman）困难问题假设和间隙双线性 Diffie-Hellman（Gap-BDH, gap bilinear diffie-hellman）困难问题假设，分别满足选定身份自适应选择密文攻击下的密文不可区分性（IND-sMID-CCA2）和选定身份自适应选择消息攻击下的密文存在不可伪造性（EUF-sID-CMA）。

2 基础知识

2.1 困难问题及困难性假设

设 G_1 和 G_2 分别为 q 阶的循环加法群和乘法群（q 为大素数），P 是群 G_1 的生成元，e 为 G_1 到 G_2 的双线性映射。

1) CDH 问题：已知元素 $a,b\in Z_q^*$ 和元组 $<P,aP,bP>$，计算 abP。

2) 判定双线性 diffie-hellman（DBDH）问题：已知元素 $a,b,c\in Z_q^*, Z\in G_2$ 和元组 $<P,aP,bP,cP,Z>$，判断 $Z=\mathrm{e}(P,P)^{abc}$ 是否成立。

3) 计算双线性 diffie-hellman（CBDH）问题：已知元素 $a,b,c\in Z_q^*$ 和元组 $<P,aP,bP,cP>$，计算 $\mathrm{e}(P,P)^{abc}$。

4) Gap-BDH 问题：假设存在可以解决 DBDH 问题的预言机（输入 $<P,aP,bP,cP,Z>$，其中，$a,b,c\in Z_q^*$，$Z\in G_2$。如果 $Z=\mathrm{e}(P,P)^{abc}$，DBDH 预言机输出 1，此时称元组 $<P,aP,bP,cP,Z>$ 为 DBDH 元组，否则输出 0）。在该预言机的帮助下，已知元素 $a,b,c\in Z_q^*$ 和元组 $<P,aP,bP,cP>$，计算 $\mathrm{e}(P,P)^{abc}$。

定义 1 CDH 困难问题假设算法 A 能够解决 CDH 问题的优势定义为

$$Adv_A^{CDH}=\Pr[A(P,aP,bP)=abP\mid a,b\in Z_p^*]$$

(t,ε) -CDH 困难问题假设是指对于任意概率多项式时间算法，均不能在时间 t 内以不可忽略的优势 ε 解决 CDH 问题。

定义 2 Gap-BDH 困难问题假设算法 A 能够解决 Gap-BDH 问题的优势定义为

$$Adv_A^{Gap-BDH}=\Pr[A(P,aP,bP,cP)=\mathrm{e}(P,P)^{abc}\mid a,b,c\in Z_p^*]$$

(t,q_g,ε) -Gap-BDH 困难问题假设是指对于任意概率多项式时间算法，在发起 q_g 次 DBDH 预言机询问后，均不能在时间 t 内以不可忽略的优势 ε 解决 Gap-BDH 问题。

2.2 IBMRASC 方案的形式化定义

2.2.1 概念模型

IBMRASC 方案由以下 4 个算法构成。

1) Setup:私钥生成中心（PKG, private key generator）使用该算法产生系统参数 *params* 和主密钥 *master-key*。PKG 公开系统参数，秘密持有主密钥。

2) Extract:输入系统参数 *params*，主密钥 *master-key* 和用户身份 ID_u，计算产生用户私钥 $d_u = Extract(params, ID_u, master\text{-}key)$。PKG 使用安全信道将 d_u 发送给用户。PKG 使用该算法对用户进行注册。

3) Anony-signcrypt:输入系统参数 *params*，发送者私钥 d_S，信息接收者身份列表 L' 和明文 M，计算产生密文 $C = Anony\text{-}signcrypt\ (params, M, L', d_S)$。信息发送者使用该算法产生签密密文。

4) De-signcrypt: 输入系统参数 *params*，签密密文 C，接收者私钥 d'_R，如果 C 是合法签密密文，则返回明文消息 $M = De\text{-}signcrypt(params, C, d'_R)$，否则，输出符号 $\perp$。信息接收者使用该算法解密密文。

2.2.2 安全模型

定义 3 密文不可区分性 IBMRASC 方案的密文不可区分性可以由挑战者 B 和攻击者 A 之间进行的游戏定义，过程如下。

建立：B 执行 *Setup* 算法，生成系统参数 *params* 和主密钥 *master-key*，将 *params* 发送给 A，秘密的持有 *master-key*。A 接收到 *params* 后，输出目标身份列表 $L^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$。

第 1 阶段：A 可以向 B 进行多项式次数的询问，询问内容包括如下几方面。

私钥提取询问：A 可以发起对身份信息 ID_u（$ID_u \notin L^*$）的私钥询问，B 运行 *Extract* 算法得到 $d_u = Extract(params, ID_u, master\text{-}key)$，将其返回给 A。

匿名签密询问：A 可以发起对发送者身份 ID_S，接收群组身份 $L' = \{ID'_1, ID'_2, \cdots, ID'_n\}$ 和消息 M 的签密询问。B 计算 $d_S = Extract\ (params, ID_S, master\text{-}key)$ 和 $C = Anony\text{-}Signcrypt\ (params, M, L', d_S)$，并将 C 返回给 A。

解签密询问：A 可以发起对密文 C 和接收者身份 ID'_R 的解签密询问。B 计算 $d'_R = Extract(ID'_R, S, params)$ 并将 $De\text{-}signcrypt(params, C, d'_R)$ 的结果返回给 A。

上述询问的选择是自适应的，即每个询问都可以在前一个询问基础上进行。

挑战：A 选择 2 个等长的消息 M_0 和 M_1 以及他想挑战的签密者身份 ID_S^*，该身份在第 1 阶段没有被用于私钥提取询问。B 选择随机比特 $\gamma \in \{0,1\}$，计算 $C = Anony\text{-}Signcrypt(params, M_\gamma, L^*, d_S^*)$，并将其发送给 A，其中，d_S^* 为身份 ID_S^* 对应的私钥，可由 *Extract* 算法得到。

第 2 阶段：A 可以进行与第 1 阶段相同类型的询问，但不能发起对身份信息 ID_S^* 的私钥提取询问以及对密文 C 在目标列表 $L^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$ 中任何身份下的解签密询问。

猜测：A 输出 $\gamma' \in \{0,1\}$ 作为对 γ 的猜测，如果 $\gamma' = \gamma$，则称 A 赢得游戏。

A 成功的优势定义为 $Adv^{IND-sMID-CCA2} = |\Pr[\gamma' = \gamma] - \frac{1}{2}|$，如果任意概率多项式时间攻击者不能以不可忽略的概率赢得上述挑战—猜测游戏，则称 IBMRASC 方案在选定身份自适应选择密文攻击下具有密文不可区分性（IND-sMID-CCA2）。

定义 4 密文存在不可伪造性 IBMRASC 方案的密文存在不可伪造性定义过程如下。

建立：B 执行 *Setup* 算法，生成系统参数 *params* 和主密钥 *master-key*，将 *params* 发送给 A，秘密的持有 *master-key*。A 收到 *params* 后，输出目标身份 ID_S^*。

询问：如同定义 3 第 1 阶段，A 可以发起多项式次数的自适应询问。

伪造：A 产生元组 (C, L')，其中，C 不能由匿名签密询问得到，且其中的信息发送群组列表 L 中包含目标身份 ID_S^*。如果 A 没有发起过对 L 中任意身份的私钥提取询问，且对接收群组列表 L' 中的所有身份信息对应的私钥 $d'_i (i = 1, 2, \cdots, n)$，解签密的结果 $De\text{-}signcrypt(params, C, d'_i)$ 都是相同的信息 M，则称 A 赢得游戏，也就是说 A 伪造产生了合法的签密密文。

如果任意概率多项式时间攻击者不能以不可忽略的概率赢得上述询问—伪造游戏，则称 IBMRASC 方案在选定身份自适应选择消息攻击下具有密文存在不可伪造性（EUF-sID-CMA）。

3 PCL 方案及安全性分析

3.1 方案简介

Setup：PKG 执行以下过程。

1) G_1 和 G_2 分别是阶为 $q \geqslant 2^l$（l 是作为安全参

数的大整数）的加法群和乘法群，P 是 G_1 的生成元，双线性映射 $\mathrm{e}: G_1 \times G_1 \to G_2$。

2) 定义安全散列函数：$H_1: \{0,1\}^* \to G_1$；$H_2: G_2 \to \{0,1\}^{l_0}$；$H_3: \{0,1\}^{l_0} \times G_1 \to Z_q^*$；$H_4: \{0,1\}^* \to Z_q^*$，其中，$l_0$ 表示明文和密文的长度。

3) 选择随机数 $s_0 \in Z_q^*$ 作为主密钥，计算 $P_{pub} = s_0 P \in G_1$，选择随机数 $P_0 \in G_1^*$，计算 $g = \mathrm{e}(P_{pub}, P_0)$。

4) 公开系统参数 $params = < G_1, G_2, q, \mathrm{e}, P, P_{pub}, P_0, g, H_1, H_2, H_3, H_4 >$，秘密保存主密钥 s_0。

Extract：对用户身份 $ID \in \{0,1\}^*$。PKG 计算用户私钥为 $d_{ID} = s_0 Q_{ID}$，其中，$Q_{ID} = H_1(ID)$ 作为用户公钥。

Anony-signcrypt：设 ID_S 是发送者身份，$L' = \{ID_1', ID_2', \cdots, ID_n'\}$ 是发送者选择的接收群组身份，发送者执行以下过程。

1) 选择用户集 $L = \{ID_1, ID_2, \cdots, ID_m\}$，且 $ID_S \in L$，$L \cap L' = \varnothing$。

2) 选择随机数 $u_i \in Z_q^*$，$i \in \{1,2,\cdots,m\} \setminus \{S\}$，计算 $R_i = u_i P$。

3) 选择随机数 $u_S \in Z_q^*$，计算 $a = \sum_{i=1}^{m} u_i$，$U = aP$，$\sigma = g^a$ 和 $W = H_2(\sigma) \oplus M$。

4) 计算 $h_i = H_3(W, R_i)$，$i \in \{1,2,\cdots,m\} \setminus \{S\}$，令 $R_S = u_S Q_S - \sum_{i=1, i \neq S}^{m} (R_i + h_i Q_i)$，其中，$Q_S$ 是 ID_S 的公钥，令 $R = \{R_1, R_2, \cdots, R_m\}$。

5) 计算 $V = (u_S + h_S) d_S$，其中，$h_S = H_3(W, R_S)$，d_S 是 ID_S 对应私钥。

6) 对 $j = 1,2,\cdots,n$，计算 $x_j = H_4(ID_j')$，$y_j = a(P_0 + Q_j')$，其中，Q_j' 是 ID_j' 的公钥，得到 n 对数：$(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$，构造拉格朗日函数 $F(x)$ 满足等式 $F(x_j) = y_j$ ($j = 1,2,\cdots,n$)。

7) 对于 $j = 1,2,\cdots,n$，计算 $f_j(x) = \prod_{1 \leqslant j \neq j' \leqslant n} \frac{x - x_{j'}'}{x_j - x_{j'}'} = a_{j,1} + a_{j,2} x + \cdots + a_{j,n} x^{n-1}$，其中，$a_{j,1}, a_{j,2}, \cdots, a_{j,n} \in Z_q$。

8) 对于 $j = 1,2,\cdots,n$，计算 $T_j = \sum_{j'=1}^{n} a_{j',j} y_{j'}$，令 $T = \{T_1, T_2, \cdots, T_n\}$。

密文为 $C = < U, V, W, T, R, L >$。

De-signcrypt：不妨设 ID_j' 为信息接收者身份，对密文 $C = < U, V, W, T, R, L >$，解签密过程如下。

验证。

1) 计算 $K = \sum_{i=1}^{m} (R_i + h_i Q_i)$，这里 $h_i = H_3(W, R_i)$，$i = 1,2,\cdots,m$。

2) 如果等式 $\mathrm{e}(V, P) = \mathrm{e}(K, P_{pub})$ 成立，则表示签密者身份确实属于集合 L，否则退出。

判断。

3) 判断等式 $VQ_j' = Kd_j'$ 是否成立，其中，d_j' 是 ID_j' 对应私钥，等式成立则可以对消息进行解密，否则退出。

解密。

4) 计算 $\delta_j = T_1 + x_j T_2 + \cdots + (x_j^{n-1} \bmod q) T_n$，其中，$x_j = H_4(ID_j')$。

5) 计算 $\sigma' = \mathrm{e}(P_{pub}, \delta_j) \mathrm{e}(U, d_j')^{-1}$，$M = H_2(\sigma') \oplus W$。$M$ 则为解签密得到的消息明文。

3.2 安全性分析

该方案并不满足密文的不可区分性，攻击者可以区分不同消息的签密密文，攻击过程如下。

攻击者和挑战者进行定义 3 的游戏，游戏进入挑战阶段，A 选择等长的消息 M_0 和 M_1 以及挑战身份 ID_S^*。

B 随机选择 $\gamma \in \{0,1\}$，对消息 M_γ 进行签密，首先，B 令 $U^* = aP$，$\sigma = Z$，查找 H_1 输出列表获得与 $ID_j''^*$，$i \in \{1,2,\cdots,n\}$ 相对应的 $l_j''^*$，计算出 $y_j^* = l_j''^* U^*$，继而得到 $T_j''^*, j \in \{1,2,\cdots,n\}$。$B$ 最终生成一个目标密文 $C^* = < U^*, V^*, W^*, T^*, R^*, L^* >$，并将 C^* 返回给 A。

攻击者 A 可以发起对信息发送群组和挑战接收群组之外所有用户的私钥提取询问，因此，A 可以选择任意身份 $ID_E \notin (L^* \cup L'^*)$ 并获得该身份对应的私钥 d_E。在获得挑战密文 C^* 后，A 可以按以下步骤区分该密文。

1) 选择一个用户集合 $L = \{ID_1, ID_2, \cdots, ID_m\}$，且 $ID_E \in L$，$L \cap (L^* \cup L'^*) = \varnothing$。

2) 选择随机数 $u_i \in Z_q^*$，$i \in \{1,2,\cdots,m\} \setminus \{E\}$，并计算 $R_i = u_i P$。

3) 选择随机数 $u_E \in Z_q^*$，计算 $R_E = u_E P$。

4) 计算 $h_i = H_3(W^*, R_i)$，$i \in \{1,2,\cdots,m\} \setminus \{E\}$，

令 $R_E = u_E Q_E - \sum_{i=1,i\neq E}^{m}(R_i + h_i Q_i)$，其中，$Q_E$ 是 ID_E 的公钥，令 $R = \{R_1, R_2, \cdots, R_m\}$。

5) 计算 $V = (u_E + h_E)d_E$，其中，$h_E = H_3(W, R_E)$，d_E 是 ID_E 的私钥。

6) 得到新的密文为 $C = <U^*, V, W^*, T^*, R, L>$。

7) 在游戏第 2 阶段，A 发起对 $C = <U^*, V, W^*, T^*, R, L>$，接收者身份 $ID_R^* \in L^*$ 的解签密询问。

8) A 根据挑战者的应答消息与消息 (M_0, M_1) 进行匹配，进而返回 $\gamma' \in \{0,1\}$ 作为猜测，游戏结束。

定理 1　如果挑战者 B 返回的 $C^* = <U^*, V^*, W^*, T^*, R^*, L^*>$ 是对 M_γ 签密密文的完美模拟，则 $C = <U^*, V, W^*, T^*, R, L>$ 同样是对 M_γ 的合法签密密文，攻击者 A 在获得解签密结果后，通过消息匹配以概率 1 赢得游戏。

证明　在解签密算法中解签密者输入 $C = <U^*, V, W^*, T^*, R, L>$，$params$，接收者身份 ID_j' 及其私钥 d_j'，对 C 进行解密，具体过程如下。

验证：计算 $K = \sum_{i=1}^{m}(R_i + h_i Q_i)$，这里 $h_i = H_3(W^*, R_i)$，$i = 1, 2, \cdots, m$。等式 $\mathrm{e}(V, P) = \mathrm{e}(K, P_{pub})$ 成立，这是因为

$$\begin{aligned}\mathrm{e}(V,P) &= \mathrm{e}((u_E + h_E)d_E, P)\\ &= \mathrm{e}(u_E Q_E + h_E Q_E, P_{pub})\\ &= \mathrm{e}(\sum_{i=1,i\neq E}^{m}(R_i + h_i Q_i) + R_E + h_E Q_E, P_{pub})\\ &= \mathrm{e}(\sum_{i=1}^{m}(R_i + h_i Q_i), P_{pub})\\ &= \mathrm{e}(K, P_{pub}) \end{aligned} \quad (1)$$

表明签密者是集合 L 中的成员之一。

解密：计算 $\delta_j = T_1 + x_j T_2 + \cdots + (x_j^{n-1} \bmod q)T_n$，其中，$x_j = H_4(ID_j')$。计算 $\sigma' = \mathrm{e}(P_{pub}, \delta_j)\mathrm{e}(U^*, d_j')^{-1}$，$M_\gamma = H_2(\sigma') \oplus W^*$。

因此，如果 $C^* = <U^*, V^*, W^*, T^*, R^*, L^*>$ 是对 M_γ 签密密文的完美模拟，则 $C = <U^*, V, W^*, T^*, R, L>$ 同样是对 M_γ 的合法签密密文，在得到解签密询问结果并对消息进行匹配后，攻击者 A 以概率 1 赢得游戏。定理证毕。

注：在加法群 G_1 中，PCL 方案判断过程中的运算形式 $VQ_j' = Kd_j'$ 不符合运算规则，因此，此处省略了签密密文 $C = <U^*, V, W^*, T^*, R, L>$ 是否满足该等式的讨论。

4　改进的 IBMRASC 方案

本节给出改进的 IBMRASC 方案，过程如下。

Setup：PKG 执行以下过程。

1) G_1 和 G_2 分别是阶为 $q \geqslant 2^l$（l 是作为安全参数的大整数）的加法群和乘法群，P 是 G_1 的生成元，双线性映射 $\mathrm{e}: G_1 \times G_1 \to G_2$。

2) 定义 4 个单向散列函数：$H_0: \{0,1\}^* \to G_1$；$H_1: G_2 \to Z_q^*$；$H_2: Z_q^* \to \{0,1\}^{l_0}$；

$H_3: \{0,1\}^* \times \{0,1\}^* \times Z_q^* \times \cdots \times Z_q^* \times G_1 \times G_1 \to Z_q^*$，其中，$l_0$ 表示需要处理信息的比特长度。

3) 选择一个随机数 $s_0 \in Z_q^*$ 为主密钥，计算 $P_{pub} = s_0 P \in G_1$。

4) 公开参数 $params = <G_1, G_2, q, \mathrm{e}, P, P_{pub}, H_0, H_1, H_2, H_3>$，秘密保存主密钥 s_0。

Extract：输入参数 $params$, s_0 和用户身份 $ID \in \{0,1\}^*$。PKG 计算用户公钥 $Q_{ID} = H_0(ID)$ 和私钥 $d_{ID} = s_0 Q_{ID}$。

Anony-signcrypt: 设信息发送者身份为 ID_S。输入参数 $params$ 和消息 M，发送者签密过程如下。

1) 选择接收者列表 $L' = \{ID_1', ID_2', \cdots, ID_n'\}$ 以及发送者列表 $L = \{ID_1, ID_2, \cdots, ID_m\}$，满足 $ID_S \in L$，$L \cap L' = \varnothing$。

2) 选择随机数 $r \in Z_q^*$，计算 $U = rP$，$T = rP_{pub}$。

3) 计算 $Q_i' = H_0(ID_i')$，$v_i = H_1(\mathrm{e}(Q_i', T))$，$i = 1, 2, \cdots, n$。

4) 选择随机数 $k \in Z_q^*$，构造多项式 $f(x) = \prod_{i=1}^{n}(x - v_i) + k \bmod q = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$。

5) 计算 $V = (M \| L) \oplus H_2(k)$。

6) 选择随机数 $u_i \in Z_q^*$，$i \in \{1, 2, \cdots, m\} \setminus \{S\}$，并计算 $R_i = u_i P$。

7) 选择随机数 $u_S \in Z_q^*$，计算 $R_S = u_S Q_S - \sum_{i=1,i\neq S}^{m}(R_i + h_i Q_i)$。其中，$Q_S$ 是 ID_S 的公钥，$h_i = H_3(V, L, c_0, c_1, \cdots, c_{n-1}, U, R_i)$，$i \in \{1, 2, \cdots, m\} \setminus \{S\}$。令 $R = \{R_1, R_2, \cdots, R_m\}$。

8) 计算 $\sigma=(u_s+h_s)d_s$，其中，$h_s=H_3(V, L, c_0, c_1,\cdots,c_{n-1},U,R_s)$，$d_s$ 是 ID_s 的私钥。

9) 密文为 $C=<U,V,c_0,c_1,\cdots,c_{n-1},R,L,\sigma>$。

De-signcrypt：输入密文 $C=<U,V,c_0, c_1,\cdots, c_{n-1},R,L,\sigma>$，$params$，接收者身份 ID'_j 及其私钥 d'_j，对 C 进行解密，具体算法如下。

1) 计算 $K=\sum_{i=1}^{m}(R_i+h_iQ)$，其中，$h_i=H_3\ (V,L,c_0, c_1,\cdots,c_{n-1},U,R_i)$，$i=1,2,\cdots,m$。

2) 如果等式 $\mathrm{e}(\sigma,P)=\mathrm{e}(K,P_{pub})$ 成立，则签密者确实为集合 L 中的成员，否则，返回密文不合法并退出。

3) 重构多项式为 $f(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n$，计算 $v'_j=H_1(\mathrm{e}(d'_j,U))$ 以及 $k'=f(v'_j)$。

4) 计算 $M'=V\oplus H_2(k')$，如果 M' 以 L 为后缀，则接受签密密文有效并提取前缀信息 M 作为输出，否则返回符号 $\perp$。

证明 如果 $C=<U,V,c_0,c_1,\cdots,c_{n-1},R,L,\sigma>$ 是由 L 中某成员使用签密算法对明文消息 M 生成的合法签密密文，则接收群组 $L'=\{ID'_1,ID'_2,\cdots,ID'_n\}$ 中的用户可以使用解签密算法获取 M，这是因为

$$\begin{aligned}\mathrm{e}(\sigma,P)&=\mathrm{e}((u_s+h_s)d_s,P)\\&=\mathrm{e}(u_sQ_s+h_sQ_s,P_{pub})\\&=\mathrm{e}(\sum_{i=1,i\neq s}^{m}(R_i+h_iQ_i)+R_s+h_sQ_s,P_{pub})\\&=\mathrm{e}(\sum_{i=1}^{m}(R_i+h_iQ_i),P_{pub})\\&=\mathrm{e}(K,P_{pub})\end{aligned}\tag{2}$$

表明签密密文是由 L 中某成员产生。

$$\begin{aligned}v'_j&=H_1(\mathrm{e}(d'_j,U))\\&=H_1(\mathrm{e}(d'_j,rP))\\&=H_1(\mathrm{e}(Q'_j,rP_{pub}))\\&=H_1(\mathrm{e}(Q'_j,T))\\&=v_j\end{aligned}\tag{3}$$

表明接收群组中成员可以使用自己的私钥重构秘密。

这样，接收群组中成员可获得分享秘密值（明文加密使用的对称密钥）$k'=f(v'_j)=f(v_j)=k$，从而获得明文 $M'=M\,\|\,L=V\oplus H_2(k)$，根据构成规则，成功提取前缀消息 M。

5 安全性及效率分析

安全性分析。下面将在随机预言模型下对方案的安全特性进行证明。

定理 2 密文的不可区分性。如果存在 IND-sMID-CCA2 攻击者 A 能够在时间 t 内，以不可忽略的概率 ε 赢得定义 3 中的游戏，且至多进行 $q_{H_0},q_{H_1},q_{H_2},q_{H_3}$ 次对散列函数 H_0,H_1,H_2,H_3 的询问、q_E 次私钥提取询问、q_{ASC} 次匿名签密询问以及 q_{DSC} 次解签密询问，询问次数总和为 q，则存在能够在时间 $t'<t$ 内以优势 $\varepsilon'\geqslant\varepsilon-\frac{q_{DSC}}{q}$ 解决 Gap-BDH 问题的算法 B。

证明 下面给出算法 B 利用 A 在时间 t' 内以优势 ε' 解决 Gap-BDH 问题的过程。

首先，对 Gap-BDH 问题实例 $<P,aP,bP,cP>$，算法 B 的目标为：在 DBDH 预言机的帮助下计算 $\mathrm{e}(P,P)^{abc}$。B 模拟定义 3 中的挑战者过程如下。

建立 B 设定 $Q=aP$ 以及 $P_{\mathrm{pub}}=bP$，将系统参数 $params=<G_1,G_2,q,e,P,P_{\mathrm{pub}},H_0,H_1,H_2,H_3>$ 发送给 A，在接收到系统参数后，A 选择 n 个目标身份 $L^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$。

H_i，$i=0,1,2,3$，是由 B 控制输出的随机预言机，输出规则如下。

H_0 询问：对身份信息 ID_j，$j\in[1,q_0]$，如果 H_0 输出列表中存在元组 (ID_j,u_j,Q_{IDj})，则返回 Q_{IDj}，否则，进行以下步骤。

1) 选择随机数 $u_j\in Z_q^*$。

2) 如果 $ID_j\in L^*$，则计算 $Q_{IDj}=u_jQ\in G_1$，否则，计算 $Q_{IDj}=u_jP\in G_1$。

3) 将 (ID_j,u_j,Q_{IDj}) 存入 H_0 输出列表，返回 Q_{IDj}。

H_1 询问：向 H_1 输入一个 G_2 中的元素 X_j，$j\in[1,q_1]$ 作为输入，如果 H_1 输出列表中存在 (X_j,x_j)，则返回 x_j，对 $i\in[1,n]$，B 使用 DBDH 预言机检查元组 $<P,Q_{IDi}^*,P_{pub},cP,X_j>$，如果预言机输出为 1，则返回 $(X_j)^{u_i^{-1}}$ 并结束游戏，因为 B 已经获得 $\mathrm{e}(P,P)^{abc}=(X_j)^{u_i^{-1}}$。否则，$B$ 选择随机数 $x_j\in Z_q^*$ 返回并将 (X_j,x_j) 存入 H_1 输出列表。

$H_i(i\in\{2,3\})$ 询问：B 首先查找 $H_i(i\in\{2,3\})$ 输

出列表，如果存在包含询问目标的元组，则返回元组中的输出结果作为应答给 A，否则，B 选择一个恰当的随机元素作为询问结果返回给 A，并将包含询问和结果的元组存入相应的 $H_i(i\in\{2,3\})$输出列表中。

第 1 阶段。A 向 B 进行多项式次数的询问，询问及应答过程如下。

私钥提取询问：A 发起对身份 ID_j $(ID_j\notin L^*)$的私钥询问，B 首先检查 H_0 输出列表中是否已经存在元组(ID_j,u_j,Q_{IDj})，如果存在，则计算 $d_j=u_jP_{pub}$，否则，B 选择随机数 $u_j\in Z_q^*$，计算 $Q_{IDj}=u_jP$ 和 $d_j=u_jP_{pub}$，并将元组(ID_j,u_j,Q_{IDj})存入 H_0 输出列表，将 d_j 返回给 A。

匿名签密询问：A 发起对发送者身份 ID_S，接收群组身份 $L'=\{ID_1',ID_2',\cdots,ID_n'\}$ 和消息 M 的签密询问。B 通过私钥提取询问的应答方式获得身份 ID_S 对应私钥 d_S，计算 C=*Anony-Signcrypt*($params$, M,L',d_S)，在 *Anony-Signcrypt* 算法执行过程中，B 需要完成对 $H_i(i=0,1,2,3)$预言机询问的应答并更新 $H_i(i=0,1,2,3)$预言机输出列表，最终 B 将签密密文 C 发送给 A。

解签密询问：A 发起对签密密文 $C=<U,V,c_0,c_1,\cdots,c_{n-1},R,L,\sigma>$ 和接收者身份 ID_R' 的解签密询问。如果 $ID_R'\notin L^*$，则 B 通过私钥提取询问的应答方式获得身份 ID_R' 对应私钥 d_R'，计算 $M=$ *De-signcrypt*$(C,params,d_R')$，在 De-Signcrypt 算法执行过程中，B 需要完成对 H_i $(i=0,1,2,3)$预言机询问的应答并更新 $H_i(i=0,1,2,3)$预言机输出列表，最终 B 将 M 或符号⊥返回给 A。如果 $ID_R'\in L^*$，B 执行以下步骤。

1) 对 R 中每一个元素 R_i，在 H_3 输出列表中寻找元组 $<V,L,c_0,c_1,\cdots,c_{n-1},U,R_i>$ 是否存在，如果某元组不存在，则 B 返回失败信息并停止游戏。否则，B 可以在 H_3 输出列表中获得 $<V,L,c_0,c_1,\cdots,c_{n-1},U,R_i>$ 对应值 $h_i=\lambda_i$。

2) 计算 $K=\sum_{i=1}^{m}(R_i+h_iQ_i)$，判断等式 $e(\sigma,P)=e(K,P_{pub})$ 是否成立，如果不成立，则 B 返回密文不合法信息并退出。

3) 重构多项式为 $f(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n$。

4) 使用身份 ID_R' 在 H_0 输出列表中查找元组 (ID_R',u_j',Q_{IDj}')，获得 u_j',Q_{IDj}'。

5) 对 $j=1,\cdots,q_{H1}$，在 H_1 输出列表中查找元组 (X_j,x_j)，使用 DBDH 预言机判断 $<P,Q_{IDj}',P_{pub},U,X_j>$ 是否为 DBDH 元组，如果对于某个 j，判断成立，则计算 $k_j=f(x_j)$ 和 $M'=V\oplus H_2(k')$，根据构成规则，返回前缀 M 给 A。否则，返回密文不合法信息并退出。

挑战。A 选择 2 个等长的明文消息 M_0 和 M_1 以及想挑战的签密者身份 ID_S。B 选择随机比特 $\gamma\in\{0,1\}$，并执行以下步骤。

1) 检查列表 H_0 的输出列表中是否存在元组 (ID_S,u_S,Q_{IDS}),如果存在，则计算 $d_S=u_SP_{\text{pub}}$，否则 B 选择随机数 $u_S\in Z_q^*$，计算 $Q_{IDS}=u_SP$ 和 $d_S=u_SP_{pub}$，并将元组 (ID_S,u_S,Q_{IDS}) 插入 H_0 输出列表中。

2) 选择随机数 $r_2\in Z_q^*$，并置 $U=cP$。

3) 选择随机数 $k\in Z_q^*$，$z_i\in Z_q^*$，$i=1,2,\cdots,n$ 构造 n 阶多项式。$f(x)=\prod_{i=1to\,n}(x-z_i)+k(\text{mod}\,q)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x_n$。

4) 计算 $V=(M_\gamma\,\|\,L)\oplus H_2(k)$。

5) 选择随机数 $u_i\in Z_q^*$，$i\in\{1,2,\cdots,m\}\setminus\{S\}$，并计算 $R_i=u_iP$。

6) 选择随机数 $u_S\in Z_q^*$，令 $R_S=u_SQ_S-\sum_{i=1,i\neq S}^{m}(R_i+h_iQ_i)$，其中，$h_i=H_3(V,L,c_0,c_1,\cdots,c_{n-1},U,R_i)$，$i\in\{1,2,\cdots,m\}\setminus\{S\}$，$Q_S$ 是 ID_S 的公钥，令 $R=\{R_1,R_2,\cdots,R_m\}$。

7) 计算 $\sigma=(u_s+h_s)d_s$，其中，$h_s=H_3(V,L,c_0,c_1,\cdots,c_{n-1},U,R_s)$，$d_s$ 是 ID_s 的私钥。

8) 将密文 $C=<U,V,c_0,c_1,\cdots,c_{n-1},R,L,\sigma>$ 返回给 A。

第 2 阶段。A 可以进行和第一阶段相同类型的询问，但是不能发起对身份信息 ID_S 的私钥提取询问以及对密文 C 在目标列表 $L^*=\{ID_1'^*,ID_2'^*,\cdots,ID_n'^*\}$ 中任何身份下的解签密询问。

在上述过程中，B 成功实现了对散列函数 $H_i(i=0,1,2,3)$ 的模拟，另外，在询问过程中，用户的私钥可表示为 $d_j=u_jP_{pub}=u_jbP=bu_jP=bH_0(ID_j)$，假定 b 为 *master-key*，则用户私钥的分布与真实环境中相同，因此，B 的模拟过程是完美的。

猜测。最后，A 输出对 γ 的猜测值 $\gamma'\in\{0,1\}$，A

赢得游戏。

下面分析 B 的优势：A 发起对签密密文 C 和接收者 ID'_R 的解签密询问，如果元组 $<V,L,c_0,c_1,\cdots,c_{n-1},U,R_i>$ 并没有在 H_3 输出列表中出现，就意味着 A 可以不必进行关于 H_3 的询问，而自行猜测出 H_3 的输出，在这种情况下，B 返回失败信息并停止游戏。因为至多有 q_{DSC} 次解签密询问，因此失败概率至多为 $\frac{q_{DSC}}{q}$。如果 A 以不可忽略的概率 ε 赢得 IND-sMID-CCA2 游戏，则意味着 B 在接收到 X_j 作为输入的 H_1 询问时，对 $i=1,\cdots,n$，总会存在 DBDH 元组 (P,QID_i,P_{pub},cP,X_j)。如同在 H_1 询问中一样，B 返回 $\mathrm{e}(P,P)^{abc}=(X_j)^{u_i^{-1}}$，其中 (ID_i,u_i,Q_{IDi}) 来自于 H_0 输出列表。这样，如果存在 IND-sMID-CCA2 攻击者 A 能够以概率 ε 赢得定义 3 中的游戏，则 B 能够以优势 $\varepsilon'\geqslant\varepsilon-\frac{q_{DSC}}{q}$ 解决 Gap-BDH 问题。而且 B 成功解决困难问题是在攻击者成功猜测 γ 之前，所需的计算时间为 $t'<t$。因此，改进方案在选定身份选择密文攻击下满足密文的不可区分性，命题得证。

定理 3 密文的存在不可伪造性 如果存在 EUF-sID-CMA 攻击者 A 能够在时间 t 内，以不可忽略的概率 ε 赢得定义 4 中的游戏，且至多进行 $q_{H_0},q_{H_1},q_{H_2},q_{H_3}$ 次对散列函数 H_0,H_1,H_2,H_3 的询问、q_E 次私钥提取询问、q_{ASC} 次匿名签密询问以及 q_{DSC} 次解签密询问，则存在能够在时间 $t'<2t$ 内以优势 $\varepsilon'=\varepsilon$ 解决 CDH 问题的算法 B。

证明 下面给出算法 B 利用 A 在时间 t' 内以优势 ε' 解决 CDH 问题的过程。

首先，对 CDH 问题实例 $<p,aP,bP>$，算法 B 的目标为计算 abP。B 模拟定义 4 中的挑战者过程如下。

建立。B 设定 $P_{pub}=aP$，将系统参数 $params=<G_1,G_2,q,e,P,P_{pub},H_0,H_1,H_2,H_3>$ 发送给 A，在接收到系统参数后，A 选择目标身份 ID_s^*。

$H_i(i=0,1,2,3)$ 是由 B 控制输出的随机预言机，输出如下。

H_0 询问：向 H_0 输入一个身份 ID_j，$j\in[1,q_0]$，B 检查等式 $ID_j=ID_s^*$ 是否成立，如果成立，则返回 $Q_{IDj}=bP\in G_1$，否则，B 检查 H_0 输出列表中是否存在 (ID_j,u_j,Q_{IDj})，如果存在，则返回 Q_{IDj}，否则，进行以下步骤。

1) 选择随机数 $u_j\in Z_q^*$。

2) 计算 $Q_{IDj}=u_jP\in G_1$。

3) 将 (ID_j,u_j,Q_{IDj}) 存入 H_0 输出列表，返回 Q_{IDj}。

$H_i(i\in\{1,2,3\})$ 询问：B 首先查找 H_i $(i\in\{1,2,3\})$ 输出列表，如果列表中存在包含询问目标的元组，则返回元组中对应元素作为输出结果发送给 A，否则，B 选择一个恰当的随机元素返回给 A，并将包含询问和该随机元素的元组存入相应的 H_i $(i\in\{1,2,3\})$ 输出列表中。

询问。A 向 B 进行多项式次数的询问，询问及应答过程如下。

私钥提取询问：A 发起对身份 ID_j $(ID_j\neq ID_s^*)$ 的私钥询问，B 首先检查 H_0 输出列表中是否已经存在元组 (ID_j,u_j,Q_{IDj})，如果存在，则计算 $d_j=u_jP_{pub}$，否则，B 选择随机数 $u_j\in Z_q^*$，计算 $Q_{IDj}=u_jP$ 和 $d_j=u_jP_{pub}$，并将元组 (ID_j,u_j,Q_{IDj}) 存入 H_0 输出列表，B 返回 d_j 给 A。

匿名签密询问：A 发起对发送者身份 ID_S $(ID_S\neq ID_S^*)$，接收群组身份 $L'=\{ID'_1,ID'_2,\cdots,ID'_n\}$ 和消息 M 的签密询问。B 根据私钥提取询问的应答方式提取身份 ID_S 对应私钥 d_S，计算 $C=Anony\text{-}Signcrypt(params,M,L',d_S)$，在 Anony-Signcrypt 算法执行过程中，B 需要完成对 H_i $(i=0,1,2,3)$ 预言机询问的应答并更新 H_i $(i=0,1,2,3)$ 预言机输出列表，最终 B 将签密密文 C 发送给 A。

解签密询问：A 可以发起对签密密文 C 和接收者 ID'_R 的解签密询问。B 根据私钥提取询问的应答方式提取身份 ID'_R 对应私钥 d'_R，B 计算 $M=De\text{-}signcrypt(C,params,d'_R)$，在 *De-Signcrypt* 算法执行过程中，B 需要完成对 H_i $(i=0,1,2,3)$ 预言机询问的应答并更新 $H_i(i=0,1,2,3)$ 预言机输出列表，最终 B 将 M 或符号 $\perp$ 返回给 A。

在上述过程中，B 成功实现了对散列函数 $H_i(i=0,1,2,3)$ 的模拟，另外，在询问过程中，用户的私钥可表示为 $d_j=u_jP_{pub}=u_jaP=au_jP=aH_0(ID_j)$，假定 a 为 *master-key*，则用户私钥的分布与真实环境中相同，因此，B 的模拟过程是完美的。

伪造。A 产生合法的签密密文(C^*, L^{r*})，其中，$C^* =< U^*, V^*, c_0^*, c_1^*, \cdots, c_{n-1}^*, R^*, L^*, \sigma^* >$ 中信息发送群组 L^* 中包括目标身份 ID_S^*，L^{r*} 为信息接收群组。

根据分叉引理[22]，如果存在这样的攻击者 A 通过上述交互过程可以在时间 t 内产生签密密文，则 B 可以重复攻击者行为，通过控制随机预言机的输出，在时间 $2t$ 内输出签密密文 $C' =< U', V', c_0', c_1', \cdots, c_{n-1}', R', L, \sigma' >$ 和 $C =< U, V, c_0, c_1, \cdots, c_{n-1}, R, L, \sigma >$，其中，$\sigma = (u_s + h_s)d_s$，$\sigma' = (u_s + h_s')d_s$，这样有 $\sigma - \sigma' = (h_S - h_S')d_S$，可计算 $abP = d_s = (\sigma - \sigma')(h_S - h_S')^{-1}$。

因此，改进方案在选定身份选择消息攻击下满足密文的不可伪造性，命题得证。

定理 4　新方案可以保护信息发送者和接收者双方的身份信息，具有两方匿名性。

1) 发送者匿名性：在匿名签密算法中，发送者使用私钥产生的密码操作为产生 $\sigma = (u_s + h_s)d_s$，在解签密阶段，通过验证等式

$$\begin{aligned} \mathrm{e}(\sigma, P) &= \mathrm{e}((u_s + h_s)d_s, P) \\ &= \mathrm{e}(u_s Q_s + h_s Q_s, P_{pub}) \\ &= \mathrm{e}(\sum_{i=1, i\neq s}^{m}(R_i + h_i Q_i) + R_s + h_s Q_s, P_{pub}) \\ &= \mathrm{e}(\sum_{i=1}^{m}(R_i + h_i Q_i), P_{pub}) \\ &= \mathrm{e}(K, P_{pub}) \end{aligned} \tag{4}$$

只能判断签密者是否为 L 中成员，对确定签密者身份没有任何帮助，这是因为

$$\begin{aligned} \sum_{i=1, i\neq s}^{m}(R_i + h_i Q_i) + R_s + h_s Q_s &= \sum_{i=1}^{m}(R_i + h_i Q_i) \\ &= \sum_{i=1, i\neq j}^{m}(R_i + h_i Q_i) + R_j + h_j Q_j \end{aligned} \tag{5}$$

而 $u_i \in Z_q^*$，$i \in \{1, 2, \cdots, m\} \setminus \{S\}$ 和 $u_S \in Z_q^*$ 都是随机选取的整数，因此，L 中任意用户产生该组元素的能力对等。攻击者在获得密文后确定真实签密者身份的概率不大于 $\frac{1}{|L|}$，这就在某种程度上隐藏了签密者身份。

2) 接收者匿名性：密文 $C =< U, V, c_0, c_1, \cdots, c_{n-1}, R, L, \sigma >$ 中不包含接收者身份信息。发送者在签密阶段通过计算 $v_i = H_1(\mathrm{e}(Q_i', T))$，将秘密份额与用户身份进行绑定，在授权接收者接收密文后，通过 $v_j' = H_1(\mathrm{e}(d_j', U))$ 计算各自分享的秘密份额，攻击者（包括其他接收者）无法计算该元素，也就无法将其与接收者身份信息相联系，因此可以隐藏接收者身份。

效率分析　本文选择了新近提出的具有接收者匿名特性的签密方案进行比较，其中文献[17]方案与文献[18]方案仅考虑接收者匿名，并没有考虑发送者匿名问题，PCL 方案与本文提出的改进方案考虑解决发送方与接收方双方匿名问题。表 1 是方案在签密阶段效率、解签密阶段以及密文长度等方面进行的对比。其中 E、M、P、H、R 和 M_P 分别表示指数运算、标量乘运算、对运算、散列函数运算、求逆运算和多项式乘运算，$|G_1|$、$|ID|$、$|Z_q|$ 和 $|M|$ 分别表示各种不同元素的长度，n 是指定接收者的个数。比较过程中考虑了可能进行的预计算。

从表 1 可以看到，在签密阶段，除方案[17]存在一个比较耗时的对运算外，其他 3 个方案差别并不十分明显，而在解签密阶段，本文提出的改进方案比 PCL 方案和文献[18]方案减少了一个对运算和求逆运算，这都是比较耗时的运算类型，考虑到解签密算法需要由多个不同的接收者分别执行，因此新方案在整体效率上有所提高。改进方案在密文长度上有所增加，但相对大规模的明文消息 m 而言，这种增加可以忽略。

6　结束语

本文在基于身份密码架构下对公开信道上信息的安全传输和参与实体的隐私保护技术进行了研究，在单个逻辑步骤中实现消息保密性、认证性的同时，兼顾了参与实体的匿名性。文中分析了目

表 1　效率比较

方案	签密	解签密	密文长度
文献[17]方案	$E+(3n+4)M+P+R+2H+M_p$	$E+(n-1)M+3P+2H+R$	$(n+3)\|G_1\|+\|Z_q\|+\|M\|$
文献[18]方案	$E+(3n+2)M+R+2H+M_p$	$E+(2n-2)M+4P+2H+R$	$(n+2)\|G_1\|+\|ID\|+\|M\|$
PCL 方案	$E+(2m+3n)M+R+(m+1)H+M_p$	$(m+2n)M+4P+2H+R$	$(m+n+2)\|G_1\|+m\|ID\|+\|M\|$
改进方案	$nE+(2m+3)M+(n+3)H+M_p$	$(m+2n-1)M+3P+3H$	$(m+2)\|G_1\|+n\|Z_q\|+2m\|ID\|+\|M\|$

前已有的基于身份多接收者匿名签密具体方案，针对其存在的安全问题做出了改进，新方案在随机预言模型下是可证明安全的，适用于开放环境下面向多用户的敏感信息广播。但在安全模型的定义过程可以看到，本文及 PCL 方案采用的安全模型均是“选定身份（selective-ID）”攻击安全的，即在安全模型定义中，攻击者在进行询问前需要选定攻击目标。相比较“自适应选择身份（adaptive chosen-ID）”攻击而言，“选定身份”是一类稍弱的安全模型，对攻击者能力做了部分限制，因此，自适应选择身份攻击下 IBMRASC 方案的模型定义和具体方案构造仍然是该领域研究的公开问题。

参考文献：

[1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[A]. Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology[C]. London, UK, 1997. 165-179.

[2] SHAMIR A. Identity-based cryptosystem and signature scheme[A]. Proc of CRYPTO 1984[C]. Santa Barbara, California, USA, 1985. 120-126.

[3] HUANG X, SUSILO W, MU Y, *et al*. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[A]. Proc of the 19th International Conference on Advanced Information Networking and Applications[C]. Taipei, China, 2005. 649-654.

[4] YU Y, LI F, XU C, *et al*. An efficient identity-based anonymous signcryption scheme[J]. Wuhan University Journal of Natural Sciences, 2008.13(6): 670-674.

[5] LI F, XIONG H, YU Y. An efficient id-based ring signcryption scheme[A]. Proc of 2008 International Conference on Communications, Circuits and Systems[C]. Shanghai, China, 2008. 483-487.

[6] ZHU Z, ZHANG Y, WANG F. An efficient and provable secure identity based ring signcryption scheme[J]. Computer Standard and Interface, 2008, 31(6): 1092-1097.

[7] LI F, SHIRASE M, TAKAI T. Analysis and improvement of authenticatable ring signcryption scheme[J]. Journal of Shanghai Jiaotong University (Science), 2008,13 (6):679-683.

[8] ZHANG J, GAO S, CHEN H, *et al*. A novel id-based anonymous signcryption scheme[A]. Proc of the Advances in Data and Web Management Joint International Conference[C]. Suzhou, China, 2009.604-610.

[9] ZHANG M, ZHONG Y, YANG B, *et al*. Analysis and improvement of an id-based anonymous signcryption model[A]. Proc of 5th International Conference on Intelligent Computing[C]. Ulsan, South Korea, 2009. 433-442.

[10] SELVI S, VIVEK S, RANGAN C. Identity based ring signcryption schemes revisited[J]. Journal of Math-for Industry. 2011,3: 33-46.

[11] GAURAV S, SUMAN B, ANIL K. An identity-based ring signcryption scheme[A]. IT Convergence and Security 2012, Lecture Notes in Electrical Engineering 215[C]. 2012.151-157.

[12] DUAN S, CAO Z. Efficient and provably secure multi-receiver identity-based signcryption[A]. Proc of the Information Security and Privacy 11th Australasian Conference[C]. Melbourne, Australia, 2006.195-206.

[13] YU Y, YANG B, HUANG X, *et al*. Efficient identity-based signcryption scheme for multiple receivers[A]. Proc of 4th International Conference on Autonomic and Trusted Computing[C]. Hong Kong, China, 2007.13-21.

[14] LAL S, KUSHWAH P. Anonymous ID based signcryption scheme for multiple receivers[EB/OL]. http://eprint.iacr. org/2009/345.2009.

[15] ZHANG B, XU Q. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model[A]. Proc of the 4th International Conference on Information Security and Assurance[C]. Miyazaki, Japan, 2010.15-27.

[16] 庞辽军, 崔静静, 李慧贤, 等. 新的基于身份的多接收者匿名签密方案[J]. 计算机学报, 2011, 34(11): 2104-2113.
PANG L J, CUI J J, LI H X, *et al*. A new multi-receiver ID-based anonymous signcryptionc[J]. Chinese Journal of Computers, 2011, 34(11): 2104-2113.

[17] 李慧贤, 陈绪宝, 巨龙飞, 等. 改进的多接收者签密方案[J]. 计算机研究与发展, 2013, 50(7): 1418-1425.
LI H X, CHEN X B, JU L F, *et al*. Improved multi-receiver signcryption scheme[J]. Journal of Computer Research and Development, 2013, 50(7): 1418-1425.

[18] 庞辽军, 高璐, 裴庆祺, 等. 基于身份公平的匿名多接收者签密方案[J]. 通信学报, 2013, 34(8): 161-168.
PANG L J, GAO L, PEI Q Q, *et al*. Fair and anonymous ID-based multi-receiver signcryption[J]. Journal on Communications, 2013, 34(8): 161-168.

[19] PANG L, LI H, GAO L, *et al*. Completely anonymous multi-recipient signcryption scheme with public verification[J]. PLoS ONE, 2013, 8(5): 63562.

[20] CHOW S, YIU S, HUI L. Efficient identity based ring signature[A]. Proc of ACNS 2005[C]. New York, USA, 2005.499-512.

[21] TSENG Y, HUANG Y, CHANG H. Privacy-preserving multireceiver id-based encryption with provable security[J]. International Journal of Communication Systems of Communication Systems, 2014, 27(7): 1034-1050.

[22] DAVID P, JACQUES S. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology: The Journal of the International Association for Cryptologic Research, 2000, 13(3): 361-396.

作者简介:

张波（1981-），男，山东德州人，济南大学讲师，主要研究方向为密码学与信息安全。

孙涛（1974-），男，山东淄博人，济南大学副教授，主要研究方向为可信计算理论研究与实践。

于代荣（1972-），男，山东济南人，济南大学副教授，主要研究方向为网络安全协议设计与分析。