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

张玉磊 王 欢* 马彦丽 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。分析现有的异构签密方案，发现它们只针对单个消息，无法实现批验证。聚合签密能够把不同用户对多个消息产生的签密密文同时发送给接收者，而且可以提供批量验证，降低验证开销。该文提出一个传统公钥密码-无证书公钥密码异构聚合签密方案，该方案不仅能够保证传统公钥密码(TPKI)和无证书公钥密码(CLPKC)系统间通信的机密性和认证性，而且聚合验证时不需要双线性对。在随机预言模型下，基于间隙双线性 Diffie-Hellman 困难问题、计算 Diffie-Hellman 困难问题和离散对数问题，证明该方案满足自适应性选择密文攻击下的不可区分性和自适应选择消息下的不可伪造性。

关键词：异构签密；聚合签密；间隙双线性 Diffie-Hellman 问题；计算 Diffie-Hellman 问题；离散对数问题
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2018)05-1079-08
DOI: 10.11999/JEIT170712

Provable and Secure Traditional Public Key Infrastructure-certificateless Public Key Cryptography Heterogeneous Aggregate Signcryption Scheme

ZHANG Yulei WANG Huan MA Yanli 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 the unforgeability in the different cryptographies. By analyzing some existing heterogeneous signcryption schemes, it is found that they only deal with a single message and can not achieve batch verification. Aggregation signcryption can not only take n distinct signcryption on n messages signed by n distinct users, but also provide a batch verification and reduce the cost of verification. In this paper, a Traditional Public Key Infrastructure (TPKI)-CertificateLess Public Key Cryptography (CLPKC) heterogeneous aggregation signcryption scheme is proposed, which can ensure the confidentiality and authentication between the TPKI and CLPKC. The scheme does not require bilinear pairings when it is aggregated. It is proved that the scheme has indistinguishability against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen messages attack under gap bilinear Diffie-Hellman and computational Diffie-Hellman problem and Discrete logarithm.

Key words: Heterogeneous signcryption; Aggregation signcryption; Gap bilinear Diffie-Hellman problem; Computational Diffie-Hellman problem; Discrete logarithm problem

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。研究者们结合不同的密码体制环境，提出了相应的签密方案。但在实际应用和 5G 异构网络环境中，发送方和接收方所属的密码体制可能不同。因此，为了保证异构网络环境下异构公钥密码体制之间数据的机密性和认证性，有必要研究异构签密问题[2–8]。

2010 年文献[2]首次提出异构签密的密码原语，并构造了 TPKI(Traditional Public Key Infrastructure) 和 IDPKC(IDentity-based Public Key Cryptography)的双向异构签密方案。但是，该方案只满足签密的外部安全性[9]。随后，文献[4]扩展文献[2]的研究工作，构造了 IDPKC→TPKI 单向多接收者异构签密方案；文献[5]构造了 TPKI-IDPKC 双向异构签密方案。但是以上方案仅考虑了 IDPKC 和 TPKI 之间的异构签密问题。由于

收稿日期：2017-07-19；改回日期：2017-12-26；网络出版：2018-02-05
*通信作者：王欢 1530749678@qq.com
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(2017A-003, 2015B-220)
Foundation Items: The National Natural Science Foundation of China (61163038, 61262056), The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2015B-220)

CLPKC(CertificateLess Public Key Cryptography)可以解决 IDPKC 的密钥托管问题，因此，有必要研究 TPKI 和 CLPKC 之间的异构签密问题。2016 年，文献[6]提出了 CLPKC→TPKI 匿名异构签密方案。该方案可以确保发送方身份的匿名性。同年，文献[7]提出了 TPKI-CLPKC 双向异构签密方案。

聚合签密[10–14]能够把 m 个用户对 m 个消息的签密密文聚合成一个密文，验证者只需要对聚合后的密文进行一次验证，就可以实现对多个用户的认证。2009 年文献[10]首次提出基于身份的聚合签密方案，但该方案不满足公开验证性。2014 年，文献[11]提出了无证书聚合签密方案，但该方案需要同步信息。2015 年文献[12]改进文献[11]的签密算法，改进方案不需要同步信息，且聚合验证密文信息所需要的双线性对个数与用户无关。随着 5G 异构网络的发展，需要面对多方数据的“多对一”传输模式。聚合签密可以实现“多对一”模式的多个用户发送不同数据的机密、聚合传输和批验证。2017 年，文献[14]提出 TPKI→IDPKC 异构聚合签密方案。目前，没有适用于 TPKI 和 CLPKC 异构密码环境的异构聚合签密方案。因此本文提出了一个适用于 TPKI 和 CLPKC 异构系统间的聚合签密(Heterogeneous Aggregate Signcryption TCHGASC)方案。

本文提出的 TCHGASC 方案具有几个特点：

(1)能够在 TPKI 和 CLPKC 密码系统间通信。与已有异构签密方案相比，本文 TCHGASC 方案将聚合与异构签密结合，可以同时对多个消息进行签密验证，效率大大提高。

(2)与已有聚合签密方案相比，TCHGASC 方案验证时不需要双线性对，减少了算法的运算量。

(3)在随机预言模型下，基于间隙双线性 Diffie-Hellman(Gap Bilinear Diffie-Hellman GBDH)和计算 Diffie-Hellman(Computational Diffie-Hellman CDH)困难问题，证明 TCHGASC 方案满足自适应性选择密文攻击下的不可区分性；基于离散对数问题，证明 TCHGASC 方案满足自适应选择消息下的不可伪造性。

2 TCHGASC 方案形式化定义和安全模型

TCHGASC 方案是从 TPKI 到 CLPKC 的聚合签密算法。其中，CA(Certificate Authority)颁发发送者的公私钥，接收者的部分私钥和公钥由 CLPKC 密码系统生成，秘密值由用户自己选择。

2.1 TCHGASC 方案形式化定义

TCHGASC 方案包括以下 7 个算法：

(1)系统建立：输入安全参数 1^k，KGC 输出系统主密钥 s 和系统参数 pa 。

(2)CLPKC-KG 算法：

(a)部分私钥提取：输入用户身份 ID_B，KGC 计算用户的部分私钥 D_B，并发送给用户。

(b)设置密钥：用户选择秘密值 x_B，输出用户私钥 $S_B=(D_B,x_B)$ 和公钥 P_B。

(3)PKI-KG 算法：输入安全参数 1^k，输出发送者的公私钥对 $(\mathrm{pk}_i,\mathrm{sk}_i)$ 。

(4)签密算法：输入消息 m_i，发送者的私钥 sk_i，接收者的身份 ID_B 和公钥 P_B，输出密文 σ_i。

(5)聚合签密算法：输入密文 $\sigma_i(1\le i\le n)$，输出聚合签密密文 σ 。

(6)聚合签密验证算法：输入聚合签密密文 σ，发送者对应的公钥 $\mathrm{pk}_i(1\le i\le n)$，验证聚合密文的合法性。如果合法，输出“是”，否则返回错误符号“$\perp$”。

(7)聚合解签密算法：输入签密密文 σ、发送者的公钥 pk_i、接收者的身份 ID_B 和私钥 SK_B，输出明文 m 或者错误符号“$\perp$”。

2.2 安全模型

TCHGASC 方案安全性考虑机密性和不可伪造性。对于机密性，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，它可以自适应地替换用户的公钥；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。

定义 1 A_{I} 敌手的机密性：若第 1 类敌手能以不可忽略的优势在多项式时间内在游戏中获胜，则称该方案满足自适应性选择密文攻击下的不可区分性(INDistinguishability against Adaptive Chosen Ciphertext Attack A_{I} , IND-CCA2-A_{I})。

初始阶段：$\mathcal{T}$ 运行系统建立算法，将生成的系统参数发送给 A_{I}，保留主密钥 s 。

阶段 1：A_{I} 适应性的执行下列询问。

私钥询问：用户 ID_i 进行私钥询问时，$\mathcal{T}$ 从相关列表中找到完整私钥，并返回。

部分私钥询问：A_{I} 选择一个身份 ID_i，$\mathcal{T}$ 执行相应算法，将 D_i 返回。

公钥询问：用户 ID_i 进行公钥询问时，$\mathcal{T}$ 从相关列表中找到公钥，并返回。

公钥替换：A_{I} 可以在规定范围内，对选择用户的公钥进行替换。

聚合解签密询问：A_{I} 将聚合密文 σ，身份为 $\{\mathrm{ID}_i\}_{i=1}^n$ 的发送者和身份为 ID_R 的接收者提交给 $\mathcal{T}$ 。

$\mathcal{T}$ 检查 σ 的有效性。如果 σ 是一个合法的密文，$\mathcal{T}$ 运行解签密算法，返回 m 或 $\perp$。

挑战：A_{I} 生成两个长度为 n 的消息序列 $M_0^* = \left\{m_{0i}^*\right\}_{i=1}^n$ 和 $M_1^* = \left\{m_{1i}^*\right\}_{i=1}^n$，以及希望挑战的接收者的身份 ID_R。ID_R 不能是公钥已被替换的身份。ID_R 的部分私钥和私钥不能被询问。$\mathcal{T}$ 随机选择 $\gamma \in \{0,1\}$，计算聚合密文 σ^*，将密文 σ^* 发送给 A_{I}。

阶段 2：A_{I} 执行多项式有界的适应性询问。约束条件：(1) ID_R 的私钥不能被询问；(2) ID_R 的公钥不能被替换；(3) A_{I} 不能对密文 σ^* 执行解签密询问。

猜测阶段：A_{I} 输出一个比特 γ'。若 $\gamma' = \gamma$，A_{I} 赢得 IND-CCA2- A_{I}。定义 A_{I} 的优势为 $\mathrm{Adv}(A_{\mathrm{I}}) = \left|\Pr[\gamma' = \gamma] - \frac{1}{2}\right|$。$\Pr[\gamma' = \gamma]$ 表示 $\gamma' = \gamma$ 的概率。

定义 2　A_{II} 敌手的机密性：若第 2 类敌手能以不可忽略的优势在多项式时间内在游戏中获胜，则称该方案满足自适应性选择密文攻击下的不可区分性(INDistinguishability against Adaptive Chosen Ciphertext Attack A_{II}, IND-CCA2 A_{II})。

初始化：$\mathcal{T}$ 运行系统建立算法，将生成的系统参数和主密钥 s 发送给 A_{II}。

阶段 1，阶段 2 和挑战阶段：与定义 1 中相似。但 A_{II} 知道系统主密钥 s，它能够计算出用户的部分私钥。因此，无需进行部分私钥询问和公钥替换。

猜测阶段：A_{II} 输出一个比特 γ'。若 $\gamma' = \gamma$，A_{II} 赢得 IND-CCA2- A_{II}。定义 A_{II} 的优势为 $\mathrm{Adv}(A_{\mathrm{II}}) = \left|\Pr[\gamma' = \gamma] - \frac{1}{2}\right|$。$\Pr[\gamma' = \gamma]$ 表示 $\gamma' = \gamma$ 的概率。

定义 3　不可伪造性：基于异构聚合签密的适应性选择消息攻击由 3 个阶段组成。这是挑战者 F 和敌手 A 之间的游戏。

初始阶段：F 运行系统建立算法，将生成的系统参数、主密钥 s 和发送者公钥 pk_i^* 发送给 A。

攻击阶段：A 适应性地执行下列询问。

(1)私钥询问：A 询问 ID_i 私钥，F 返回 SK_i。

(2)部分私钥询问：A 询问 ID_i 部分私钥，F 返回 D_i。

(3)公钥询问：用户 ID_i 进行公钥询问时，F 从相关列表中找到公钥，并返回。

(4)签密询问：A 提交发送者身份 ID_i、接收者身份 ID_R 和消息 m 给 F。F 将产生的签密密文发送给 A。

伪造阶段：A 输出 $\left(\{\mathrm{ID}_i\}_{i=1}^n, \mathrm{ID}_B, \sigma^*\right)$。如果下面 3 个条件成立，$A$ 赢得此游戏。(1) σ^* 对于 $\{\mathrm{ID}_i\}_{i=1}^n$ 和 ID_B 是合法密文。(2)至少存在一个用户 ID_i^* 和 ID_B 不能进行密钥提取询问。(3)不能执行 m^*，ID_i 或某个接收者 ID_B' 的签密询问。

3　TCHGASC方案

(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 4 个哈希函数：$H_1: \{0,1\}^* \to G_1, H_2: \{0,1\}^n \times \{0,1\}^n \to Z_q^*$，$H_3: G_1 \times G_2 \to \{0,1\}^n$，$H_4: \{0,1\}^* \to Z_q^*$，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 $\left\{G_1, G_2, n, e, P, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4\right\}$。

(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 pa，系统主密钥 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：用户输入系统参数 pa，随机选择 $x_c \in Z_q^*$ 作为秘密值，生成用户私钥 $\mathrm{SK}_c = (x_c, D_c)$ 和公钥 $\mathrm{PK}_c = x_c P$。

(3)PKI-KG(TPKI 用户密钥建立)：TPKI 中的用户随机选择 $x_i \in Z_q^*$ 作为私钥 sk_i，计算公钥 $\mathrm{pk}_i = x_i P$。

(4)签密算法：假定 TPKI 中发送者的公/私钥对为 $(\mathrm{pk}_i, \mathrm{sk}_i)(1 \leq i \leq n)$，CLPKC 中接收者 Bob 的身份和公钥分别为为 ID_B 和 PK_B。发送者执行以下过程：

(a)选择随机数 $k_i \in \{0,1\}^n$，计算 $r_i = H_2(k_i, m_i)$，$U_i = r_i P$；

(b)计算 $T_i = e\left(P_{\mathrm{pub}}, Q_B\right)^{r_i}$，$C_i = m_i \oplus H_3(U_i, T_i, r_i \mathrm{PK}_B)$；

(c)计算 $S_i = \left(r_i + \mathrm{sk}_i H_4(C_i, U_i)\right) \bmod n$，则密文是 $\sigma_i = (S_i, U_i, C_i)$。

(5)聚合签密算法：聚合者输入 pa、消息 m_i 对应的签密密文 $\sigma_i = (S_i, U_i, C_i)$、接收者的身份 ID_B 及接收者公钥 PK_B，其中 $1 \leq i \leq n$。计算 $S = \sum_{i=1}^n S_i$，则聚合签密密文为 $\sigma = (S, U_1, U_2, \cdots, U_n, C_1, C_2, \cdots, C_n)$。

(6)聚合签密验证算法：输入聚合签密密文 σ，发送者对应的公钥 pk_i，验证聚合密文的合法性。如果 $SP = \sum_{i=1}^n U_i + \sum_{i=1}^n H_4(C_i, U_i)\mathrm{pk}_i$ 成立，输出

“真”，否则返回错误符号“$\perp$”。

(7) 聚合解签密算法：CLPKC 中接收者输入私钥 SK_B 和 TPKI 中发送者的公钥 pk_i，执行以下过程：

计算 $T_i = e(D_B, U_i)$，$m_i = C_i \oplus H_3(U_i, T_i, x_B U_i)$，返回消息 m_i。

正确性证明 本文 TCHGASC 方案是正确的，当且仅当异构签密密文 $\sigma_i = (S_i, U_i, C_i)$ 和异构聚合签密密文 $\sigma = (S, U_1, U_2, \cdots, U_n, C_1, C_2, \cdots, C_n)$ 都是按照签密算法得到的。并且以下验证等式成立：

$$\begin{aligned} SP &= \sum_{i=1}^{n} S_i P = \sum_{i=1}^{n} \left(r_i + \mathrm{sk}_i H_4(C_i, U_i)\right) P \\ &= \sum_{i=1}^{n} r_i P + \sum_{i=1}^{n} H_4(C_i, U_i)\,\mathrm{pk}_i \\ &= \sum_{i=1}^{n} U_i + \sum_{i=1}^{n} H_4(C_i, U_i)\,\mathrm{pk}_i \end{aligned}$$

4 安全性分析

4.1 机密性

定理 1 随机预言模型下，假设 GBDH 问题困难，TCHGASC 方案在适应性选择密文攻击下不可区分。

引理 1 随机预言模型下，假设存在一个多项式概率多项式的敌手 A_{I} 能以不可忽略的优势赢得游戏，那么存在一个算法 $\mathcal{T}$ 能以不可忽略的优势解决 GBDH 困难问题。

证明 挑战者 $\mathcal{T}$ 收到一个 GBDH 实例 (P, aP, bP, cP)，敌手 A_{I} 和挑战者 $\mathcal{T}$ 交互如下。

初始阶段：$\mathcal{T}$ 运行系统建立算法，返回系统参数 $\{G_1, G_2, n, e, P, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4\}$ 给 A_{I}，为了回答 A_{I} 的询问，$\mathcal{T}$ 维护初始值为空的列表 $L_1 \sim L_4$，L_{pk} 和 LK_p。其中 $P_{\mathrm{pub}} = aP$。

阶段 1：A_{I} 发起一系列询问。$\mathcal{T}$ 维护初始值为空的列表 $L_1 \sim L_4$，以便用于 A_{I} 对于预言机 H_1, H_2, H_3, H_4 的询问。

H_1 询问：输入 ID_i，当 $i \neq l$ 时，$\mathcal{T}$ 随机选取 $r \in Z_q^*$，设置 $Q_{\mathrm{ID}_i} = rP$。并将 (i, ID_i, r) 添加到表 L_1 中。否则，$\mathcal{T}$ 返回 $H_1(\mathrm{ID}_l) = bP$，将 $(l, \mathrm{ID}_l, \perp)$ 插入列表 L_1 中。

CLPKC 部分私钥询问：A_{I} 询问新的 ID_i 时，$\mathcal{T}$ 运行 H_1 询问，获得 (i, ID_i, r)。如果 $i = l$，模拟终止；否则 $\mathcal{T}$ 返回 $D_i = raP$。

CLPKC 公钥询问：A_{I} 询问新的 ID_i 公钥时，$\mathcal{T}$ 从列表 L_{pk} 搜索 $(\mathrm{ID}_i, \mathrm{PK}_i, x)$ 并发送给 A_{I}。如果不存在，$\mathcal{T}$ 选取新的秘密值 x，计算公钥 PK_i，并返回。将 $(\mathrm{ID}_i, \mathrm{PK}_i, x)$ 存到列表 L_{pk} 中。

CLPKC 私钥询问：A_{I} 询问新的 ID_i 私钥时，$\mathcal{T}$ 运行 H_1 询问获得 (i, ID_i, r)。如果 $i = l$，模拟终止；否则，运行 CLPKC 公钥询问获得 $(\mathrm{ID}_i, \mathrm{PK}_i, x)$，返回私钥 (x, raP)。

CLPKC 公钥替换：当 A_{I} 替换 ID_i 公钥 PK_i 为 PK_i' 时，$\mathcal{T}$ 在 L_{pk} 中用 $(\mathrm{ID}_i, \mathrm{PK}_i', \perp)$ 替换 $(\mathrm{ID}_i, \mathrm{PK}_i, x)$。

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

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

H_3 询问：对于每次新的 $H_3(U_i, T_i, R_i)$ 询问，$\mathcal{T}$ 按照以下步骤执行：

(1)选择 $\{aP, bP, d_i cP, T\}_{i=1}^{n}$ 中的一个元组来询问 DBDH 预言机，如果满足实例，则返回 $T^{d_i^{-1}}$ 作为 GBDH 问题的应答，并停止。其中 $T = e(P, P)^{abc}$。

(2) $\mathcal{T}$ 检查 L_3 中是否存在 $(U_i, *, R_i, h)$ 满足使用 (aP, bP, U_i, T_i) 询问 DBDH 预言机。如果存在，DBDH 预言机返回结果“真”。此时，如果 $\mathrm{ID}_i = \mathrm{ID}_l$，$\mathcal{T}$ 返回 h 并用 (U_i, T_i, R_i, h) 替换 $(U_i, *, R_i, h)$。

(3) 如果 $\mathcal{T}$ 执行到这一步，$\mathcal{T}$ 随机选取 $h \in \{0,1\}^{l_m}$ 并将 (U_i, T_i, R_i, h) 插入到 L_3 中。

聚合解签密询问：对于每次新的询问 $(S, U_1, U_2 \cdots U_n, C_1, \cdots, C_n, \{\mathrm{ID}_i\}_{i=1}^{n}, \mathrm{ID}')$，$\mathcal{T}$ 按以下步骤执行：

(1)执行解签密的验证部分，如果不成立，返回“$\perp$”。

(2)计算 $R = x' U_i$。

(3)对于 $i = 1, \cdots, n$ (我们假定 ID' 的公钥已被替换)，有：

(a)如果 $\mathrm{ID}' \neq \mathrm{ID}_l$，$\mathcal{T}$ 执行以下步骤：

①计算 $T_i = \hat{e}(rU_i, P_{\mathrm{pub}})$，$r$ 可以从列表 L_1 中的 (j, ID', r) 中找到。

②通过执行 H_3 询问获得 h_3，计算 $m_i = C_i \oplus h_3$，完成解密过程。由于 $Q' = r_i P$，因此，

$$\begin{aligned} T_i &= \hat{e}(rU_i, P_{\mathrm{pub}}) = \hat{e}(U_i, rP_{\mathrm{pub}}) = \hat{e}(U_i, arP) \\ &= \hat{e}(U_i, aQ_j) = \hat{e}(U_i, D_j) \end{aligned}$$

(b)如果 $\mathrm{ID}' = \mathrm{ID}_l$，$\mathcal{T}$ 执行以下步骤：

①不能直接计算 T_i。

②$\mathcal{T}$ 执行到这一步骤时，从 $\{0,1\}^{l_m}$ 中任意选取一个 h，并将 $(U_i,*,R_i,h)$ 插入到列表 L_3 中。

挑战阶段：阶段 1 后，$\mathcal{T}$ 生成两个相同长度的明文集合 $m_0^* = \left\{m_{0i}^*\right\}_{i=1}^n$ 与 $m_1^* = \left\{m_{1i}^*\right\}_{i=1}^n$ 和希望挑战的身份 $\left\{\mathrm{ID}_i^*\right\}_{i=1}^n$ 与 ID_R^*。如果 $\mathrm{ID}_R^* \neq \mathrm{ID}_l^*$，$\mathcal{T}$ 失败；否则，$\mathcal{T}$ 根据以下方法构造一个挑战密文。

(1)$\mathcal{T}$ 从 L_{pk} 中获取 $\left\{\mathrm{ID}_i^*\right\}_{i=1}^n$ 的相应公钥 $\left\{\mathrm{PK}_i^*\right\}_{i=1}^n$。

(2) 首先，$\mathcal{T}$ 设置 $\left\{U_i^* = d_i cP\right\}_{i=1}^n$，其中 $\left\{d_i \in Z_q^*\right\}_{i=1}^n$，并随机选取 $\gamma \in \{0,1\}$。然后获得 $\left\{h_{3i}^*\right\}_{i=1}^n$。最后计算 $\left\{C_i^* = m_i \oplus h_{3i}^*\right\}_{i=1}^n$，设置 $\left\{S_i^* = \left(r_i^* + \mathrm{SK}_i H_4\left(m_\gamma, U_i^*\right)\right) \bmod n\right\}_{i=1}^n$。$\mathrm{SK}_i$ 可以从 LK_p 中获得。此时，$\mathcal{T}$ 运行聚合算法，并将结果发送给 A_{I}。

阶段 2：A_{I} 像阶段 1 一样进行多项式有界次适应性询问。

猜测阶段：A_{I} 输出一个比特 γ'。因为有 i 个用户，那么敌手输出身份 ID_l 的概率为 $1/i$。如果 $\mathrm{ID}_R^* = \mathrm{ID}_l$，敌手除了询问过 $\left\{\left(U_i^*, T_i^*, R_i^*\right)\right\}_{i=1}^n$，那么模拟都是完美的。因为 Hash 函数 H_3 可以看作是随机预言机，所以，如果这些元组中的任何一个都不存在于 L_3 中，敌手没有任何优势。反之，$\mathcal{T}$ 将在 H_3 询问的步骤(1)中解决 DBDH 问题。　　证毕

引理 2　随机预言模型下，假设存在一个多项式概率多项式的敌手 A_{II} 能以不可忽略的优势赢得游戏，那么存在一个算法 $\mathcal{T}$ 能以不可忽略的优势解决 CDH 困难问题。

证明　挑战者 $\mathcal{T}$ 收到一个 CDH 实例 (P, aP, bP)，目标是计算 abP。敌手 A_{II} 和挑战者 $\mathcal{T}$ 交互如下。

初始阶段：$\mathcal{T}$ 生成主密钥 $s \in Z_q^*$ 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}。$\mathcal{T}$ 随机选取 $l \leq q_{\mathrm{RP}}$，q_{RP} 是 A_{II} 能够进行公钥询问的最大次数。

阶段 1：A_{II} 发起一系列询问。$\mathcal{T}$ 维护初始值为空的列表 $L_1 \sim L_4$，以便用于 A_{II} 对于预言机 H_1, H_2, H_3, H_4 的询问。还需要维护用于存储公钥信息的列表 L_{pk} 和 LK_p。

H_1 询问：输入 ID_i，如果 i 不重复，$\mathcal{T}$ 随机选取 $r \in Z_q^*$，计算 $Q_i = rP$，并将其返回。同时将 (i, ID_i, r) 添加到列表 L_1。

CLPKC 公钥询问：A_{II} 询问 ID_i 公钥时，如果 $i \neq l$，$\mathcal{T}$ 选取新的随机数 $x \in Z_q^*$，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，$\mathcal{T}$ 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，$\mathcal{T}$ 运行 H_1 询问得到 (i, ID_i, r)，并返回私钥 (x, rsP)。

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

$H_k(k=2,4)$ 询问：对于新的 $H_k(k=2,4)$ 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 $L_k(k=2,4)$。

H_3 询问：对于每次新的 $H_3(U_i, T_i, R_i)$ 询问，$\mathcal{T}$ 按照以下步骤执行：

(1) 对于 $i = 1,2,\cdots,n$，检查 $e(aP, d_i bP) = e(P, R_i)$ 是否成立。如果成立，返回 $d_i^{-1}R$ 并停止。

(2)检查列表 L_3 中是否存在元组 $(U_i, T_i, *, h)$ 满足 $\hat{e}(U_i, aP) = \hat{e}(P, R_i)$。如果 $\mathrm{ID}_i = \mathrm{ID}_l$ 成立，$\mathcal{T}$ 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 (U_i, T_i, R_i, h) 插入到列表 L_3 中。

聚合解签密询问：对于每次新的询问，$\mathcal{T}$ 按以下步骤执行：

(1)执行解签密的验证部分，如果不成立，返回“$\perp$”。

(2)计算 $T_i = \hat{e}\left(U_i, r' P_{\mathrm{pub}}\right)$。$r'$ 可以从 L_1 中获得。因为 $Q' = r'P$，所以 $T_i = \hat{e}\left(U_i, r' P_{\mathrm{pub}}\right) = \hat{e}\left(U_i, sr'P\right) = \hat{e}\left(U_i, sQ'\right) = \hat{e}\left(U_i, D'\right)$。

(3)对于 $i = 1,2,\cdots,n$，有：

如果 $\mathrm{ID}' \neq \mathrm{ID}_l$，$\mathcal{T}$ 按通常的方式完成解签密过程。

如果 $\mathrm{ID}' = \mathrm{ID}_l$，$\mathcal{T}$ 执行以下步骤：

(a)$\mathcal{T}$ 不能直接计算 R。对于不同的 R，$\mathcal{T}$ 搜索列表 L_3 寻找 (U_i, T_i, R_i, h)，希望等式 $\hat{e}(U_i, aP) = \hat{e}(P, R)$ 成立。如果这样的等式成立，说明找到正确的 R。

(b)通过执行 H_3 询问获得 h_3，计算 $m_i = C_i \oplus h_3$ 完成解密过程。

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

挑战阶段：阶段 1 后，$\mathcal{T}$ 生成两个相同长度的明文集合 $m_0^*=\left\{m_{0i}^*\right\}_{i=1}^n$ 与 $m_1^*=\left\{m_{1i}^*\right\}_{i=1}^n$ 和希望挑战的身份 $\left\{\mathrm{ID}_i^*\right\}_{i=1}^n$ 与 ID_R^*。如果 $\mathrm{ID}_R^*\neq\mathrm{ID}_l^*$，$\mathcal{T}$ 失败；否则，$\mathcal{T}$ 根据以下方法构造一个挑战密文。

(1) $\mathcal{T}$ 从 L_{pk} 中获取 $\left\{\mathrm{ID}_i^*\right\}_{i=1}^n$ 的相应公钥 $\left\{\mathrm{PK}_i^*\right\}_{i=1}^n$。

(2) 首先，$\mathcal{T}$ 设置 $\left\{U_i^*=d_ibP\right\}_{i=1}^n$，其中 $\left\{d_i\in Z_q^*\right\}_{i=1}^n$，并随机选取 $\gamma\in\{0,1\}$。然后获得 $\left\{h_{3i}^*\right\}_{i=1}^n$。最后计算 $\left\{C_i^*=m_i\oplus h_{3i}^*\right\}_{i=1}^n$，设置 $\left\{S_i^*=\left(r^*+\mathrm{SK}_iH_5\left(m_\gamma,U_i^*\right)\right)\bmod n\right\}_{i=1}^n$。$\mathrm{SK}_i$ 可以从 LK_p 中获得。此时，$\mathcal{T}$ 运行聚合算法，并将结果发送给 A_{II}。

阶段 2：A_{II} 像阶段 1 一样进行多项式有界次适应性询问。

猜测阶段：A_{II} 输出一个比特 γ'。敌手输出每个用户的概率相同，因为有 i 个用户，输出身份 ID_l 的概率为 $1/i$。如果 $\mathrm{ID}_R^*=\mathrm{ID}_l$，除了敌手询问过 $\left\{\left(U_i^*,T_i^*,R_i^*\right)\right\}_{i=1}^n$，那么模拟都是完美的。因为 Hash 函数 H_3 可以看作是随机预言机，所以，如果这些元组中的任何一个都不存在于 L_3 中，敌手没有任何优势。反之，$\mathcal{T}$ 将在 H_3 询问的步骤(1)中解决 CDH 问题。 证毕

4.2 不可伪造性

定理 2 随机预言模型下，如果存在一个概率多项式伪造者 A 能以不可忽略的优势赢得游戏，那么存在一个算法 F 能以不可忽略的优势解决 DLP (Discrete Logarithm Problem)困难问题。

证明 A 是攻击者，F 是 DLP 问题挑战者。F 给定一个实例 (P,aP)，F 的目的是利用 A 解决 DLP 问题，即计算 a。

初始阶段：F 运行系统初始化算法，将系统参数 pa、主密钥 s 和选定的发送者公钥 $\mathrm{pk}_i^*=aP$ 发送给 A。

攻击阶段：F 维护初始值为空的列表 $L_1\sim L_4$，L_{pk} 和 LK_p。A 适应性地执行下列询问。

H_1 询问：对于新的 H_1 询问时，若相关询问在表 L_1 中，直接返回给 A；否则随机选择一个数返回给 A，添加相关信息到 L_1。

H_2 询问：对于 $L_2=\left(k_i,m_i,h_{2,i}\right)$ 询问，如果曾被询问过，则返回 L_2 给 A；否则返回 $h_{2,i}\in Z_q^*$，并添加到列表 L_2 中。

H_3 询问：F 保持 $L_3=\left(U_i,T_i,W_i,h_{3,i}\right)$，初始为空。如果曾被询问过，则返回 L_3 给 A；否则返回 $h_{3,i}\in\{0,1\}^n$，并添加到列表 L_3 中。

H_4 询问：对于新的 H_4 询问时，若相关询问在 L_4 中，则返回给 A；否则选择 $\eta_i\in Z_q^*$，并将 (C_i,U_i,η_i) 添加到 L_4。

TPKI 私钥询问：A 询问 ID_i 私钥，F 从 LK_p 得到 $(\mathrm{ID}_i,x_i,\mathrm{PK}_i)$。若 $\mathrm{ID}_i\neq\mathrm{ID}_i^*$，返回 $\mathrm{SK}_i=x_i$；否则返回 $\mathrm{SK}_i=a$。

CLPKC 私钥询问：A 询问 ID_j 私钥，F 运行 CLPKC 公钥询问，获得 $\left(j,\mathrm{ID}_j,\mathrm{PK}_j,x\right)$ 并返回私钥。

CLPKC 公钥询问：A 询问 ID_j 公钥时，F 询问 L_{pk} 并返回公钥。

签密阶段：A 对于新的询问 $\left(m_i,\mathrm{ID}_i,\mathrm{ID}_j\right)(1\le i\le n)$，$F$ 操作如下：

(1)随机选择 $t_i,\eta_i\in Z_q^*$，计算 $U_i=t_iP-\eta_i\mathrm{pk}_i$；

(2)计算 $C_i=m_i\oplus h_{3,i}$；

(3)计算 $S_i=t_i\bmod n$；

返回 $\sigma_i=(S_i,U_i,C_i)$ 给 A；

伪造阶段：A 提交 n 个发送者身份 ID_i^* 及对应公钥 pk_i^* 和伪造的聚合密文 $\sigma^*=\left(S^*,U_1^*,U_2^*,\cdots,U_n^*,C_1^*,C_2^*,\cdots,C_n^*\right)$，其中 $(1\le i\le n)$。

在 A 看来，每个序号 i 的概率相同。从多个用户 $\{\mathrm{ID}_i\}(1\le i\le n)$ 选择一个作为目标用户。将 ID_1 选作目标用户，设 A 可以伪造成功。根据分叉引理[15]，对 H_4 询问进行分叉，输出两个聚合密文 $\sigma^*=\left(C_1^*,C_2^*,\cdots,C_n^*,U_1^*,U_2^*,\cdots,U_n^*,S^*\right)$,$\sigma'^*=\left(C_1'^*,C_2'^*,\cdots,C_n'^*,U_1'^*,U_2'^*,\cdots,U_n'^*,S'^*\right)$。对于用户 $(\mathrm{ID}_i)(2\le i\le n)$，使用分叉引理后，$\{U_i\}(2\le i\le n)$ 和 $\left\{H_4\left(C_i,U_i\right)\right\}(2\le i\le n)$ 不变。满足等式：

$$S^*P=S_1^*P+\sum_{i=2}^n S_i^*P,\quad S'^*P=S_1'^*P+\sum_{i=2}^n S_i'^*P$$

因此有：$\left(S^*-S'^*\right)P=S_1^*P-S_1'^*P+\sum_{i=2}^n\left(S_i^*P-S_i'^*P\right)$，$\left(S^*-S'^*\right)P=S_1^*P-S_1'^*P=\left(r_1^*+h_4^*\left(U_1,C_1\right)x_1\right)P-\left(r_1'^*+h_4'^*\left(U_1,C_1\right)x_1\right)P$,$\left(S^*-S'^*\right)\cdot P=\left(h_4^*\left(U_1,C_1\right)x_1-h_4'^*\left(U_1,C_1\right)x_1\right)P=\left(h_4^*\left(U_1,C_1\right)-\right.$

$h_4^{\prime *}(U_1,C_1))x_1P, S^* - S^{\prime *} = \left(h_4^*(U_1,C_1) - h_4^{\prime *}(U_1,C_1)\right)a$ 得 $a = \left(h_4^*(U_1,C_1) - h_4^{\prime *}(U_1,C_1)\right)^{-1}\left(S^* - S^{\prime *}\right)$。即解决了 DLP 问题。　　证毕

5　效率分析

5.1 效率分析

公开文献显示目前没有 TPKI-CLPKC 异构聚合签密方案，因此无法与同类方案进行效率比较。从表 1 可以看出，文献[14]方案是 TPKI-IDPKC 异构聚合签密方案，聚合验证效率为 $2P$。文献[12]方案是目前无证书聚合签密方案中效率最高的。本文方案与文献[14]相比，聚合验证减少了 2 个双线性对；与文献[12]相比，不仅能够应用于异构环境中，而且聚合验证不需要双线性对运算。表中 P 表示双线性对数，n 表示签密用户数。

5.2 仿真实现

为了说明本文提出的方案的执行效率，利用 C 语言和 PBC(Pairing-Based Cryptography)库[16]在 i5-2400@3.1 GHz CPU, 4 GB RAM PC 机上对本文方案进行仿真实现。在仿真过程中，使用 Type A 椭圆曲线，椭圆曲线次数为 2。其中，用户的身份和消息随机生成。

本次仿真分别取 5, 50, 100, 500, 1000, 2000, 2500 个消息，实验结果包括 m 个消息的签密总用时、m 个消息的签密平均用时、TCHGASC 算法验证总用时、TCHGASC 算法验证平均用时、m 个消息的解签密总用时和 m 个消息的解签密平均用时。其中 m 分别取 5, 50, 100, 500, 1000, 2000, 2500。从表 2 和图 1～图 4 可以看出 TCHGASC 算法的各个阶段的计算效率。

表 1 效率对比

方案	密码环境	密文聚合	聚合验证效率	公开验证性
文献[12]方案	CLPKC→CLPKC	是	$4P$	是
文献[14]方案	TPKI→IDPKC	是	$2P$	是
本文方案	TPKI→CLPKC	是	$0P$	是

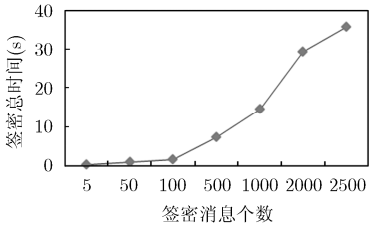

图 1 签密计算效率

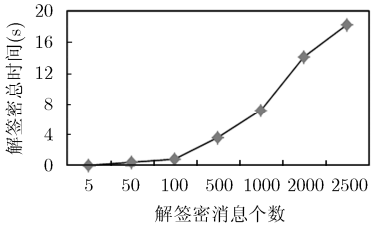

图 2 解签密计算效率

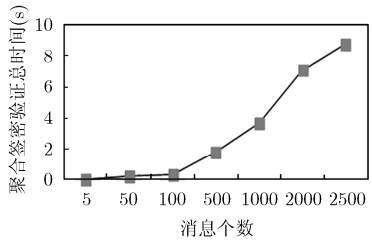

图 3　TCHGASC 验证效率

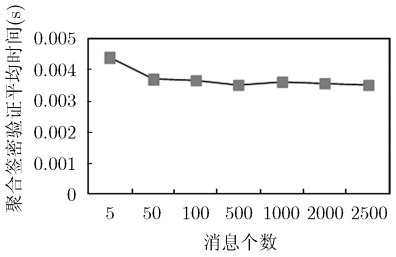

图 4　TCHGASC 验证平均效率

表 2 本文 TCHGASC 方案的计算效率(s)

消息个数(个)	m 个消息签密总时间	m 个消息平均用时	TCHGASC 验证总用时	TCHGASC 验证平均用时	m 个消息解签密用时	m 个消息平均解签密用时
5	0.076577	0.015315	0.022132	0.004426	0.037080	0.007416
50	0.743740	0.014875	0.185723	0.003714	0.367032	0.007341
100	1.456883	0.014569	0.367403	0.003674	0.733901	0.007339
500	7.353371	0.014707	1.756688	0.003513	3.601870	0.007204
1000	14.448123	0.014448	3.601799	0.003602	7.162070	0.007162
2000	29.329224	0.014665	7.150577	0.003575	14.176906	0.007088
2500	35.712263	0.014285	8.764138	0.003506	18.153645	0.007261

6 结束语

本文提出了一个从 TPKI 密码体制到 CLPKC 密码体制的异构聚合签密算法。该算法结合了异构签密和聚合签密的优势。在异构环境下，能够对签密信息进行聚合传输，提高了传输的效率。同时，在验证聚合密文时，不需要双线性对，减少了算法的运算量。所提算法保证了 TPKI 和 CLPKC 异构密码系统之间数据的机密性和不可伪造性。

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 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.

[3] 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.

[4] FU Xiaotong, LI Xiaowei, and LIU Wen. 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 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.

[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(10): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

ZHANG Yulei, ZHANG Linggang, ZHANG Yongjie, *et al*. CLPKC to TPKI heterogeneous signcryption scheme with anonymity[J]. *Acta Electronica Sinica*, 2016, 44(10): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

[7] 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.

[8] LI Fagen, HAN Yanan, and JIN Chunhua. 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.

[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] SELVI S, VIVEK S, SHRIRAM J, *et al*. Identity based aggregate signcryption schemes[C]. International Conference on Cryptology in India, New Delhi, India, 2009: 378–397. doi: 10.1007/978-3-642-10628-6_25.

[11] ESLAMI Z and PAKNIAT N. Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model[J]. *Journal of King Saud University-Computer and Information Sciences*, 2014, 26(3): 276–286.

[12] 张玉磊, 王欢, 李臣意, 等. 可证安全的紧致无证书聚合签密方案[J]. 电子与信息学报, 2015, 37(12): 2838–2844. doi: 10.11999/JEIT150407.

ZHANG Yulei, WANG Huan, LI Chenyi, *et al*. Provable secure and compact certificateless aggregate signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2015, 37(12): 2838–2844. doi: 10.11999/JEIT150407.

[13] 罗敏, 孙腾, 张静茵, 等. 两个无证书聚合签名方案的安全性分析[J]. 电子与信息学报, 2016, 38(10): 2695–2700. doi: 10.11999/JEIT151350.

LUO Min, SUN Teng, ZHANG Jingyin, *et al*. Security analysis on two certificateless aggregate signature schemes[J]. *Journal of Electronics & Information Technology*, 2016, 38(10): 2695–2700. doi: 10.11999/JEIT151350.

[14] 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.

[15] DAVID P and JACQUES S. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396. doi: 10.1007/s001450010003.

[16] The pairing-based cryptography library[OL]. http://crypto.stanford.edu/pbc/,2015.

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，研究方向为密码学与信息安全.

马彦丽： 女，1992 年生，硕士生，研究方向为密码学与信息安全.

刘文静： 女，1994 年生，硕士生，研究方向为密码学与信息安全.

王彩芬： 女，1963 年生，博士，教授，博士生导师，研究方向为密码学与信息安全.