具有内部安全性的常数对无证书聚合签密方案

张永洁[①]　张玉磊*[②]　王彩芬[②]
[①](甘肃卫生职业学院　兰州　730000)
[②](西北师范大学计算机科学与工程学院　兰州　730070)

摘　要：聚合签密不仅能够减少密文的验证计算量，而且能够保证数据的机密性和认证性。该文分析刘等人(2016)提出的无证书聚合签密(CLASC)方案，指出第2类攻击者可以伪造密文，刘方案不满足适应性选择密文攻击的不可区分性和适应性选择消息攻击的不可伪造性。为了提升CLASC方案的安全级别和聚合验证效率，该文提出CLASC的内部安全模型和具有内部安全性的CLASC方案。该方案聚合验证密文只需要3个双线性对，与现有同类方案相比，具有较高的验证效率。基于计算Diffie-Hellman困难假设，证明新方案在随机预言模型下，满足CLASC内部安全模型下的机密性和不可伪造性。

关键词：无证书签密；聚合签密；内部安全性；计算 Diffie-Hellman 困难问题；KGC 攻击
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2018)02-0500-09
DOI: 10.11999/JEIT170419

Certificateless Aggregate Signcryption Scheme with Internal Security and Const Pairings

ZHANG Yongjie[①]　ZHANG Yulei[②]　WANG Caifen[②]
[①](*Gansu Health Vocational College*, *Lanzhou* 730000, *China*)
[②](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Aggregate signcryption can not only reduce the cost of the verification of ciphertexts, but also ensure the confidentiality and authentication. Analyzed Liu *et al*'s CertificateLess Aggregate SignCryption (CLASC) scheme with Const Pairings, it is found that type II adversary, who is the malicious key generator center, could forge the ciphertexts. It means that Liu *et al*'s scheme does not satisfy the indistinguishability under the adaptive chosen ciphertext attacks and unforgeability under the adaptive chosen message attacks. In order to improve the security level and verification efficiency of CLASC scheme, in this paper, the internal secure model of CLASC is defined and a concrete CLASC scheme with this property is presented. As the new scheme only needs 3 bilinear pairingis, it is more efficient than existing CLASC schemes. Based on the assumption of computational Diffie-Hellman, in the random oracle model and the internal security mode of CLASC, the new schems is proved to satisfy the confidentiality, unforgeability and public verification.

Key words: Certificateless signcryption; Aggregate signcryption; Internal security; Computational Diffie-Hellman problem; Attack of Key Generator Center (KGC)

1　引言

1997 年，Zheng[1]提出签密原语。签密能够在一个逻辑步骤内实现加密和签名操作，其效率优于“先签名后加密”方式。2002 年，Baek 等人[2]定义签密安全模型，An 等人[3]提出签密“内部安全”模型：对于机密性，即使发送者的私钥泄露，攻击者也不能从密文中恢复明文；对于不可伪造性，即使接收者的私钥泄露，攻击者也不能伪造密文。签密内部安全模型提升了攻击者的能力，具有更高的安全性。

实际应用中，当签密用户较多时，接收者需要同时验证多个密文。为了提升密文的批验证效率，文献[4]结合聚合签名[5]的优势提出聚合签密概念。2011 年，文献[6]提出第 1 个无证书聚合签密(CertificateLess Aggregate SignCryption, CLASC)方案。随后，文献[7–9]分别提出其它 CLASC 方案。

收稿日期：2017-05-05；改回日期：2017-09-16；网络出版：2017-11-01
*通信作者：张玉磊　zhangyl@nwnu.edu.cn
基金项目：国家自然科学基金(61163038,61262056)，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)

但是，这些方案需要的双线性对个数与用户数线性相关，聚合验证效率较低。为了提高 CLASC 方案的验证效率，文献[10–12]分别提出新的 CLASC 方案。其中，文献[12]方案只需要 3 个双线性对运算，具有较高的验证效率。但是，该方案存在 A_{II} 类攻击，不满足 CLASC 的机密性和不可伪造性。

本文通过构造的攻击算法，证明文献[12]方案存在 A_{II} 类攻击：恶意密钥生成中心可以解密和伪造密文信息。为了提高 CLASC 方案的安全层次和聚合验证效率，本文完善了 CLASC 安全模型，使其具有“内部安全”特性。同时，提出了一个改进的 CLASC 方案。改进方案具有以下特点：

(1)克服了文献[12]方案的安全性问题，可以抵抗无证书聚合签密的 A_{I} 和 A_{II} 两类敌手攻击。

(2)随机预言模型下，基于双线性计算 Diffie-Hellman(Biliner Computational Diffie-Hellman, BDH) 困难问题和计算 Diffie-Hellman (Computational Diffie-Hellman, CDH)困难问题，证明该方案满足签密内部安全模型下的机密性和不可伪造性。

(3)满足公开验证性，第三方可以验证密文的有效性。

(4)聚合验证密文时，方案只需要 3 个双线性对运算。与现有同类方案相比较，具有较高的验证效率。

2　CLASC安全模型

CLASC方案的参与者包括密钥生成中心KGC (Key Generator Center)、用户 u_i、聚合用户 u 和接收用户 u_B。CLASC方案主要包括系统初始化、部分私钥提取、密钥提取、签密、聚合签密、聚合验证和聚合解签密等算法[10]。CLASC方案主要考虑 A_{I} 攻击和 A_{II} 攻击。A_{I} 表现为实现公钥替换攻击的普通用户；A_{II} 表现为恶意KGC。CLASC方案的机密性必须分别考虑 A_{I} 和 A_{II} 适应性选择密文攻击下密文的不可区分性，CLASC方案的不可伪造性必须分别考虑 A_{I} 和 A_{II} 适应性选择消息攻击下的不可伪造性。

2.1 机密性

CLASC 内部安全模型的机密性与文献[8] CLASC 安全模型不同，内部安全模型允许攻击者获得发送方的完整私钥。

游戏 1　假定 C 为挑战者，CLASC 方案针对 A_{I} 的适应性选择密文攻击游戏包括以下阶段。

初始阶段　C 运行“系统初始化”算法，输入安全参数 k，产生系统参数和主密钥 s，计算系统公钥 P_{pub}，保留主密钥 s，发送系统参数和 P_{pub} 给 A_{I}。

阶段 1　A_{I} 对以下预言机执行多项式有界次适应性询问：

(1)Hash 询问：A_{I} 可以询问所有 Hash 预言机，并返回对应 Hash 值。

(2)部分私钥询问：A_{I} 提交用户身份 ID_i，如果列表中存在对应身份信息，则直接返回；否则 C 运行“部分私钥提取”算法，获得并返回部分私钥 D_i 给 A_{I}。

(3)秘密值询问：A_{I} 提交用户身份 ID_i，如果列表中存在对应身份信息，则直接返回；否则 C 运行“密钥提取”算法获得并返回秘密值 x_i 给 A_{I}。

(4)公钥询问：A_{I} 提交用户身份 ID_i，如果列表中存在对应公钥，则直接返回；否则，C 运行“密钥提取”算法，获得并返回对应公钥 P_i 给 A_{I}。

(5)公钥替换询问：A_{I} 提交用户身份 ID_i 和选择的公钥 P_i'，用 P_i' 替换 P_i。

(6)解签密询问：A_{I} 提交聚合密文 δ、发送者身份 ID_i、接收者身份 ID_R，挑战者 C 调用“聚合验证”算法验证密文的有效性。如果密文 δ 有效，挑战者 C 调用“聚合解签密”算法恢复消息 m_i，其中 $1 \le i \le n$。

挑战阶段　A_{I} 决定结束“阶段 1”并进入“挑战阶段”的时机。A_{I} 选择长度相同的消息集合 $\{m_{i0}^*\}$ 和 $\{m_{i1}^*\}$，n 个发送者身份 ID_i 及接收者身份 ID_R 作为挑战信息，并提交给挑战者 C，其中 $1 \le i \le n$。

C 随机选择 $b \in \{0,1\}$，输入消息集合 $\{m_{ib}^*\}$、发送者私钥 $\{S_i\}$ 和接收者公钥 P_R，运行“签密”算法获得签密密文 δ_i^*，运行“聚合签密”算法获得聚合密文 δ^*，最后将 δ^* 返回给 A_{I}，其中 $1 \le i \le n$。

阶段 2　A_{I} 像“阶段 1”一样继续对以上预言机进行多项式有界次地适应性询问，挑战者 C 按照“阶段 1”一样给出相应的反馈。

猜测阶段　A_{I} 选择一个比特 b'，如果 $b' = b$ 并且以下条件成立，则 A_{I} 赢得游戏 1。

(1) A_{I} 不能提交对 ID_R 的“部分私钥询问”。

(2) A_{I} 可以提交对 ID_i $(\mathrm{ID}_i \ne \mathrm{ID}_R)$ 的“部分私钥询问”和“秘密值询问”。

(3)在挑战身份为“发送者 ID_i' 及接收者 ID_R'”条件下的聚合密文 δ^* 没有提交过“解签密询问”询问，其中 $1 \le i \le n$。

定义 1　如果不存在任何多项式有界敌手 A_{I} 在 t 时间内，经过以上预言机询问，以至少 ε 的优势赢得游戏 1，那么 CLASC 方案在适应性选择密文攻击下针对 A_{I} 具有密文不可区分性。

游戏 2 假定 C 为挑战者，CLASC 方案针对 A_{II} 的适应性选择密文攻击游戏包括以下阶段。

初始阶段 C 运行“系统初始化”算法，输入安全参数 k，产生系统参数、主密钥 s 和系统公钥 P_{pub}。C 发送系统参数和主密钥给 A_{II}。

阶段 1 A_{II} 能够对以下预言机执行多项式有界次适应性询问：

(1) 由于 A_{II} 可以直接计算用户的部分私钥，因此，游戏 2 不考虑部分私钥询问。同时，不允许 A_{II} 进行公钥替换询问。

(2) Hash 询问、秘密值询问、公钥询问、解签密询问与游戏 1 基本相似。

挑战阶段 A_{II} 决定结束“阶段 1”并进入“挑战阶段”的时机。A_{II} 选择长度相同的消息明文集合 $\left\{m_{i0}^*\right\}$ 和 $\left\{m_{i1}^*\right\}$，n 个发送者身份 ID_i 及接收者 ID_R 作为挑战信息，并提交这些信息给挑战者 C，其中 $1 \le i \le n$。

C 随机选择 $b \in \{0,1\}$，输入消息集合 $\left\{m_{ib}^*\right\}$、发送者私钥 $\{S_i\}$ 及接收者公钥 P_R，运行“签密”算法获得密文 δ_i^*，运行“聚合签密”算法获得聚合密文 δ^*，最后将 δ^* 返回给 A_{II}，其中 $1 \le i \le n$。

阶段 2 A_{II} 像“阶段 1”一样继续对以上预言机进行多项式有界次地适应性询问，挑战者 C 按照“阶段 1”一样给出相应的反馈。

猜测阶段 A_{II} 选择一个比特 b'，如果 $b' = b$ 并且以下条件成立，那么 A_{II} 赢得游戏 2。

(1) A_{II} 不能提交对 ID_R 的“秘密值询问”。

(2) A_{II} 可以提交对 ID_i $(\text{ID}_i \ne \text{ID}_R)$ 的“秘密值询问”。

(3)在挑战身份为“发送者 ID_i' 及接收者 ID_R'”条件下的聚合密文 δ^* 没有提交过“解签密询问”询问，其中 $1 \le i \le n$。

定义 2 如果不存在任何多项式有界敌手 A_{II} 在 t 时间内，经过以上询问后，以至少 ε 的优势赢得游戏 2，那么 CLASC 方案在适应性选择密文攻击下针对 A_{II} 具有密文不可区分性。

定义 3 如果存在敌手 A_{I} 和 A_{II} 以不可忽略的概率在游戏 1 和游戏 2 中获胜，则 CLASC 方案在适应性选择密文攻击下具有密文不可区分性。

CLASC 内部安全模型的机密性定义允许攻击者获得发送方的完整私钥。即游戏 1 和游戏 2 均允许攻击者 $A \in \{A_{\text{I}}, A_{\text{II}}\}$ 获得发送方的完整私钥。即使发送方私钥泄漏，攻击者 $A \in \{A_{\text{I}}, A_{\text{II}}\}$ 也不能从密文中恢复原始消息。

2.2 不可伪造性

CLASC 内部安全模型的不可伪造性与文献[8] CLASC 安全模型不同，内部安全模型允许攻击者获得接收方的完整私钥。

游戏 3 假定 C 为挑战者，CLASC 方案针对 A_{I} 的适应性选择消息攻击游戏包括以下阶段。

初始阶段 该过程与游戏 1“初始阶段”相同。

攻击阶段 A_{I} 可以执行与游戏 1 相似的预言机询问。

签密询问： A_{I} 提交发送者身份 ID_i 及对应的私钥、接收者身份 ID_R 和消息 m_i，挑战者 C 调用“签密”算法计算 δ_i 并返回给 A_{I}。

伪造阶段 A_{I} 提交消息 m_i^*、发送者身份 ID_i^* 及公钥 P_i^*、接收者身份 ID_R、公钥 P_R 及私钥 S_R 给挑战者 C，C 调用“签密”算法获得密文 δ_i^*，运行“聚合签密”算法获得聚合密文 δ^*，最后将密文 δ^* 返回给 A_{I}，其中 $1 \le i \le n$。

如果以下条件同时成立，则 A_{I} 赢得游戏 3。

(1)对于消息 m_i^*、发送者身份 ID_i^* 及公钥 $P^*{}_i$、接收者身份 ID_R 及公钥 P_R 产生的聚合密文 δ^* 有效，即“聚合验证”算法不会输出 False，其中 $1 \le i \le n$。

(2)至少存在一个用户 ID_i^*，不失一般性，令为 ID_1^*，A_{I} 没有提交过“部分私钥询问”。

(3) A_{I} 没有对 $\left(\text{ID}_1^*, m_1^*, \text{ID}_R\right)$ 执行“签密”询问。

定义 4 如果不存在任何多项式有界敌手 A_{I} 在 t 时间内，经过以上预言机询问后，以至少 ε 的优势赢得游戏 3，那么 CLASC 方案在适应性选择消息攻击下针对 A_{I} 具有存在不可伪造性。

游戏 4 假定 C 为挑战者，CLASC 方案针对 A_{II} 的适应性选择消息攻击游戏包括以下阶段。

初始阶段 该过程与游戏 2“初始阶段”相同。

攻击阶段 A_{II} 可以执行与游戏 2 相似的预言机询问。

签密询问： A_{II} 提交发送者身份 ID_i 及对应的私钥、接收者身份 ID_R 和消息 m_i，挑战者 C 调用“签密”算法计算 δ_i 并返回给 A_{II}。

伪造阶段 A_{II} 提交消息 m_i^*、发送者身份 ID_i^* 及公钥 P_i^*、接收者身份 ID_R、公钥 P_R 及私钥 S_R 给挑战者 C, C 调用“签密”算法获得签密 δ_i^*，运行“聚合签密”算法获得聚合签密 δ^*，最后将聚合密文 δ^* 返回给 A_{II}，其中 $1 \le i \le n$。

如果以下条件同时成立，则 A_{II} 赢得游戏 4。

(1)对于消息 m_i^*、发送者身份 ID_i^* 及公钥 P_i^*、接收者身份 ID_R 及公钥 P_R 产生的聚合密文 δ^* 有效，即“聚合验证”算法不会输出 False，其中 $1 \le i \le n$。

(2)至少存在一个用户 ID_i^*，不失一般性，令为 ID_1^*，A_{II} 没有提交过“秘密值询问”。

(3) A_{II} 没有对 $\left(\mathrm{ID}_1^*, m_1^*, \mathrm{ID}_R\right)$ 执行“签密”询问。

定义 5　如果不存在任何多项式有界敌手 A_{II} 在 t 时间内，经过 Hash 询问、秘密值询问、公钥询问、签密询问和解签密询问后，以至少 ε 的优势赢得游戏 4，那么 CLASC 方案在适应性选择消息攻击下针对 A_{II} 具有存在不可伪造性。

定义 6　如果存在敌手 A_{I} 和 A_{II} 以不可忽略的概率 ε 在游戏 3 和游戏 4 中获胜，则 CLASC 方案在适应性选择消息攻击下具有存在不可伪造性。

CLASC 内部安全模型的不可伪造性定义允许攻击者获得接收方的完整私钥。即游戏 3 和游戏 4 均允许攻击者 $A \in \{A_{\mathrm{I}}, A_{\mathrm{II}}\}$ 获得接收方的完整私钥。即使接收方私钥泄漏，攻击者 $A \in \{A_{\mathrm{I}}, A_{\mathrm{II}}\}$ 也不能伪造有效的密文。

3　文献[12]CLASC方案安全性分析

3.1 文献[12]CLASC 方案

(1)系统初始化：设 k 为安全参数，q 为大素数 ($q \geq 2^k$)。定义阶为 q 的循环加法群 G_1 和循环乘法群 G_2，且生成元 $P \in G_1$。定义双线性映射为 $e: G_1 \times G_1 \to G_2$，哈希函数 $H_1: \{0,1\}^f \times G_1 \to G_1$，$H_2: G_2 \times \{0,1\}^f \to \{0,1\}^{l+f}$, $H_4: G_1 \times \{0,1\}^* \to G_1$, $H_3: \{0,1\}^{l+f} \times G_1 \to G_1$，$l$ 和 f 分别表示消息比特和用户比特长度。KGC 选取 $s \in Z_q^*$ 为主密钥，计算 $P_{\mathrm{pub}} = sP$，发布系统参数 $\left\{G_1, G_2, e, P, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4\right\}$，保存主密钥 s。

(2)用户密钥生成：用户 u_i 选择随机值 $x_i \in Z_q^*$ 作为秘密值，计算公钥 $P_i = x_i P$。

(3)用户部分私钥提取：用户 u_i 提交身份和公钥信息，KGC 计算 $Q_i = H_1(\mathrm{ID}_i, P_i)$, $D_i = sQ_i$，通过安全通道发送 D_i 给用户。用户的公钥为 (P_i, Q_i)，私钥为 (x_i, D_i)。

(4)签密：用户 u_i 发送消息 m_i 给接收用户 u_B，通过以下步骤产生签密密文：

(a)聚合用户 u 随机选择 $r_0 \in Z_q^*$，计算 $R_0 = r_0 P$，广播 R_0。

(b)用户 u_i 收到 R_0 后选择 $r_i \in Z_q^*$，计算 $R_i = r_i P$，$\alpha_i = e\left(r_i P_{\mathrm{pub}}, Q_B\right)$。

(c)计算 $c_i = H_2\left(\alpha_i, \mathrm{ID}_B\right) \oplus \left(m_i \| \mathrm{ID}_i\right)$。

(d)计算 $h_{i1} = H_3\left(\mathrm{ID}_i, m_i, \mathrm{ID}_B\right)$，$h_{i2}=H_4\left(R_0, \Delta\right)$ 和 $v_i = h_{i1} D_i + \left(r_i + x_i\right) h_{i2}$，其中，$\Delta$ 为状态信息。则用户 u_i 发送给 u_B 的消息 m_i 的签密密文为 $\delta_i = (v_i, c_i, R_i)$。

(5)聚合签密：聚合用户 u 收到密文信息 $\delta_i = (v_i, c_i, R_i)$，计算 $V = \sum_{i=1}^{n} v_i$，则聚合密文为 $\delta = \left(\left\{c_i, R_i\right\}_{i=1}^{n}, V\right)$。

(6)聚合解签密：接收用户 u_B 执行以下过程：

(a)计算 $\alpha_i = e\left(R_i, D_B\right)$，计算 $m_i \| \mathrm{ID}_i = c_i \oplus H_2\left(\alpha_i, \mathrm{ID}_B\right)$。

(b)计算 $h_{i1} = H_3\left(\mathrm{ID}_i, m_i, \mathrm{ID}_B\right)$, $h_{i2}=H_4\left(R_0, \Delta\right)$。

(c)验证等式

$$e(V, P) \stackrel{?}{=} e\left(\sum_{i=1}^{n} h_{i1} Q_i, P_{\mathrm{pub}}\right) e\left(\sum_{i=1}^{n}\left(R_i + P_i\right), h_{i2}\right)$$

是否成立，如果成立，则输出消息 m_i，否则密文无效。

3.2 文献[12]CLASC 方案分析

3.2.1 KGC 解密攻击　由于第 2 类敌手 A_{II} (恶意 KGC)了解系统主密钥 s，因此，它可以解密密文信息。KGC 通过以下算法实现解密密文攻击。

(1)KGC 计算用户的部分私钥。KGC 计算接收用户的部分私钥 D_B。

(2)KGC 捕获聚合密文 $\delta = \left(\left\{c_i, R_i\right\}_{i=1}^{n}, V\right)$。

(3)KGC 解密密文。KGC 计算 $\alpha_i^{'} = e\left(R_i, D_B\right)$ 和 $H_2\left(\alpha_i^{'}, \mathrm{ID}_B\right)$，由于 $\alpha_i^{'} = \alpha_i$，因此 KGC 直接计算 $\left(m_i \| \mathrm{ID}_i\right) = C_i \oplus H_2\left(\alpha_i^{'}, \mathrm{ID}_B\right)$ $(1 \leq i \leq n)$ 对密文解密，获得所有用户发送给目标用户的消息。

文献[12]CLASC 方案基于 BDH 困难问题设计“加密环节”，即 $R_i = r_i P$ 等价于 aP，Q_B 等价于 bP，$P_{\mathrm{pub}} = sP$ 等价于 cP，因此，一般用户无法获得 BDH 实例 $(R_i, Q_B, P_{\mathrm{pub}})$ 的解。但是，A_{II} 了解系统主密钥 s(等价于 BDH 问题的 c)，因此，可以获得 BDH 问题的解，进而可以解密文献[12]方案的密文。

3.2.2 KGC 密文伪造攻击　恶意 KGC 不仅可以解密文献[12]方案的密文，而且可以伪造有效的密文。KGC 通过以下算法实现密文伪造攻击。

(1)KGC捕获用户 u_i 对 m_i 的签密密文信息 $\delta_i = (v_i, c_i, R_i)$。

(2)KGC 通过以上“解密攻击”环节获得 $\delta_i = (v_i, c_i, R_i)$ 对应的消息 m_i。

(3)KGC 通过 u_i 的部分私钥和 $h_{i1} = H_3\left(\mathrm{ID}_i, m_i, \mathrm{ID}_B\right) \in Z_q^*$，容易计算固定值 $\left(r_i + x_i\right) h_{i2} = v_i - h_{i1} D_i$。

(4)伪造密文 $\delta_i^* = \left(v_i^*, c_i^*, R_i\right)$。通过 R_i，T 和 D_i，KGC 执行以下过程伪造新消息 m_i^* 的密文。

(a)计算 $\alpha_i = e\left(R_i, D_B\right)$, $c_i^* = H_2\left(\alpha_i, \mathrm{ID}_B\right) \oplus$

$\cdot\left(m_i^* \| \mathrm{ID}_i\right)$。

(b)计算 $h_{i1}^* = H_3\left(\mathrm{ID}_i, m_i^*, \mathrm{ID}_B\right)$, $v_i^* = h_{i1}^* D_i + T$。KGC 伪造消息 m_i^* 的密文为 $\delta_i^* = \left(v_i^*, c_i^*, R_i\right)$。

⑸接收者验证密文 $\delta_i^* = \left(v_i^*, c_i^*, R_i\right)$的合法性。

(a) 计 算 $\alpha_i = e(R_i, D_B)$ ， 计 算 $m_i^* \| \mathrm{ID}_i = c_i^* \oplus H_2\left(\alpha_i, \mathrm{ID}_B\right)$。

(b)判断以下等式是否成立：

$$e\left(v_i^*, P\right) \stackrel{?}{=} e\left(h_{i1} Q_i, P_{\mathrm{pub}}\right) e\left(\left(R_i + P_i\right), h_{i2}\right)$$

由于
$$\begin{aligned} e\left(v_i^*, P\right) &= e\left(h_{i1}^* D_i + T, P\right) \\ &= e\left(h_{i1}^* D_i + \left(r_i + x_i\right) h_{i2}, P\right) \\ &= e\left(h_{i1}^* Q_i, sP\right) e\left(\left(rP_i + x_i P\right), h_{i2}\right) \\ &= e\left(h_{i1} Q_i, P_{\mathrm{pub}}\right) e\left(\left(R_i + P_i\right), h_{i2}\right) \end{aligned}$$

则单个密文验证等式必定成立，KGC 伪造消息 m_i^* 的密文 $\delta_i^* = \left(v_i^*, c_i^*, R_i\right)$成功。

(6)伪造聚合密文。KGC通过以上过程伪造用户 $\left\{u_1, u_2, \cdots, u_n\right\}$ 对 消 息 $\left\{m_1^*, m_2^*, \cdots, m_n^*\right\}$ 的 密 文 $\left\{\delta_i^* = \left(v_i^*, c_i^*, R_i\right)\right\}$。

KGC计算 $v^* = \sum_{i=1}^n v_i^*$ 输出伪造的聚合密文 $\delta^* = \left(\left\{c_i^*, R_i\right\}_{i=1}^n, v^*\right)$。

由于

$$\begin{aligned} e\left(v^*, P\right) &= e\left(\sum_{i=1}^n v_i^*, P\right) \\ &= e\left(\sum_{i=1}^n h_{i1}^* D_i + \left(r_i + x_i\right) h_{i2}, P\right) \\ &= e\left(\sum_{i=1}^n h_{i1}^* D_i + \left(r_i + x_i\right) h_{i2}, P\right) \\ &= e\left(\sum_{i=1}^n h_{i1}^* Q_i, P_{\mathrm{pub}}\right) e\left(\sum_{i=1}^n \left(R_i + P_i\right), h_{i2}\right) \end{aligned}$$

因 此 ， KGC 伪 造 的 聚 合 密 文 $\delta^* = \left(\left\{c_i^*, R_i\right\}_{i=1}^n, v^*\right)$ 合法，KGC单个密文和聚合密文伪造成功。

4 改进的CLASC方案

为了克服文献[12]方案的不足，本文提出改进的 CLASC 方案。方案包括以下算法：

(1)系统初始化：设 k 为安全参数， q 为大素数 $(q \geq 2^k)$。定义阶为 q 的循环加法群 G_1 和循环乘法群 G_2 ， 生成元 $P \in G_1$。 定义双线性映射为 $e: G_1 \times G_1 \to G_2$ ， 哈 希 函 数 $H_0: \{0,1\}^* \to G_1$, $H_1: \{0,1\}^* \to \{0,1\}^{lm}$, $H_2, H_3: \{0,1\}^* \to Z_q^*$, $H_4: \{0,1\}^* \to G_1$， lm 表示消息比特长度。KGC 选取 $s \in Z_q^*$ 为主密钥，计算 $P_{\mathrm{pub}} = sP$ ， 发布系统参数 $\left\{G_1, G_2, e, P, P_{\mathrm{pub}}, H_0, H_1, H_2, H_3, H_4\right\}$， 保存主密钥 s。

(2)用户密钥生成：用户 u_i 选择秘密值 $x_i \in Z_q^*$，公钥为 $P_i = x_i P$。

(3)用户部分私钥提取：用户 u_i 提交身份和公钥信息，KGC 计算 $Q_i = H_0(\mathrm{ID}_i)$， $D_i = sQ_i$， 通过安全通道发送 D_i 给用户。

(4)签密：用户 u_i 发送消息 m_i 给接收用户 u_B， 通过以下步骤产生签密密文：

(a)选择 $r_i \in Z_q^*$，计算 $R_i = r_i P$， $Q_R = H_0\left(\mathrm{ID}_R\right)$ 和 $\omega_i = e\left(P_{\mathrm{pub}}, Q_R\right)^{r_i}$。

(b)计算 $T_i = H_1\left(R_i, \omega_i, r_i P_R, P_R\right)$ 和 $C_i = T_i \oplus m_i$。

(c)计 算 $h_{i2} = H_2\left(R_i, C_i, P_i, P_R\right)$, $h_{i3} = H_3\left(R_i, C_i, P_i, P_R\right)$， $\phi = H_4\left(P_{\mathrm{pub}}\right)$。

(d)计算 $V_i = h_{i2} D_i + h_{i3} x_i \phi + r_i \phi$，输出密文 $\delta_i = \left(R_i, C_i, V_i\right)$。

(5)聚合签密：聚合用户获得密文信息 $\delta_i = \left(R_i, C_i, V_i\right)$ 后， 计 算 $V = \sum_{i=1}^n V_i$ ， 则聚合密文为 $\delta = \left(\left\{C_i, R_i\right\}_{i=1}^n, V\right)$。

(6)聚合验证：接收用户 u_B 验证密文 δ 的合法性。

(a) 计 算 $Q_i = H_0\left(\mathrm{ID}_i\right)$, $\phi = H_4\left(P_{\mathrm{pub}}\right)$, $h_{i2} = H_2\left(R_i, C_i, P_i, P_R\right)$和 $h_{i3} = H_3\left(R_i, C_i, P_i, P_R\right)$。

(b)验证以下等式是否成立，等式成立则输出 True，否则输出 False。

$$e(V, P) \stackrel{?}{=} e\left(\sum_{i=1}^n h_{i2} Q_i, P_{\mathrm{pub}}\right) e\left(\phi, \sum_{i=1}^n h_{i3} P_i + R_i\right)$$

(7)聚合解签密：如果聚合验证算法输出为 $\omega_i = e\left(R_i, D_R\right)$，则接收用户 u_B 通过以下过程恢复消息：

(a)计算 $\omega_i = e\left(R_i, D_R\right)$。

(b) 计 算 $T_i = H_1\left(R_i, \omega_i, x_R R_i, P_R\right)$ 和 $m_i = T_i \oplus C_i$， 其中， $1 \leq i \leq n$。

5 改进方案的性能分析

5.1 正确性

定理 1 CLASC 方案满足正确性。

证明 (1)验证者能够验证密文 $\delta_i = \left(R_i, C_i, V_i\right)$ 的正确性。

$$\begin{aligned}e(V_i,P)&=e\left(h_{i2}D_i+h_{i3}x_i\phi+r_i\phi,P\right)\\&=e\left(h_{i2}D_i,P\right)e\left(h_{i3}x_i\phi,P\right)e\left(r_i\phi,P\right)\\&=e\left(h_{i2}Q_i,P_{\text{pub}}\right)e\left(\phi,h_{i3}P_i+R_i\right)\end{aligned}$$

(2) 验证者能够验证聚合密文 $\delta=\left(\{C_i,R_i\}_{i=1}^n,V\right)$ 的正确性。

$$\begin{aligned}e(V,P)&=e\left(\sum_{i=1}^n V_i,P\right)=e\left(\sum_{i=1}^n h_{i2}D_i,P\right)\\&\quad\cdot\prod_{i=1}^n e\left(\left(h_{i3}x_i+r_i\right)\phi,P\right)\\&=e\left(\sum_{i=1}^n h_{i2}Q_i,P_{\text{pub}}\right)e\left(\phi,\sum_{i=1}^n h_{i3}P_i+R_i\right)\end{aligned}$$

(3)接收者能够正确解密密文 C_i。

由于 $x_RR_i=x_Rr_iP=r_iP_R$ 和 $\omega_i'=e\left(R_i,D_R\right)=e\left(r_iP,sQ_R\right)=e\left(P_{\text{pub}},Q_R\right)^{r_i}=\omega_i$ 成立，只有同时拥有秘密值 x_R 和部分私钥 D_R 的用户才可以正确解密。因此，接收者通过 $T_i'=H_1\left(R_i,\omega_i',x_RR_i,P_R\right)=H_1\left(R_i,\omega_i,r_iP_R,P_R\right)=T_i$ 正确解密 $m_i=H_1\left(R_i,\omega_i',x_RR_i,P_R\right)\oplus C_i$，其中，$1\le i\le n$。　　证毕

5.2 机密性

限于篇幅，略去 CLASC 方案对于敌手 A_{I} 机密性证明过程。以下仅给出针对 A_{II} 敌手的机密性证明过程。

定理 2　随机预言模型下，如果存在一个概率多项式时间敌手 A_{II} 以不可忽略的概率赢得游戏 2，那么存在一个算法 C 能够解决 CDH 困难问题。即假设 CDH 问题困难，改进的 CLASC 方案对于敌手 A_{II} 在适应性选择密文攻击下密文不可区分。

证明　A_{II} 是敌手，C 是 CDH 问题挑战者。C 给定 CDH 问题实例 (P,aP,bP)，目标为计算 abP。

初始阶段　C 设 $P_{\text{pub}}=sP$，s 为系统主密钥，发送系统参数 $\left\{G_1,G_2,e,P,P_{\text{pub}},H_0,H_1,H_2,H_3,H_4\right\}$ 和主密钥 s 给 A_{II}（C 知道主密钥 s）。

阶段 1　C 保持列表 $L_0\sim L_4$ 和 $L=(\text{ID}_i,D_i,x_i,P_i)$ 保存 $H_0\sim H_4$ 预言机询问和密钥询问过程中产生的数据。A_{II} 能够对以下预言机进行询问：

H_0 询问：A_{II} 提交关于 ID_i 的询问，若 $L_0=\{i,\text{ID}_i,\mu_i\}$ 存在相应项，则直接返回 Q_i 值；否则，C 随机选择 $\mu_i\in Z_q^*$，计算 $Q_i=\mu_iP$，增加 (i,ID_i,μ_i) 到列表 L_0 并返回 Q_i 值。

H_1 询问：C 保持列表 $L_1=(R_i,\omega_i,W_i,P_R,T_i)$，初始为空。$C$ 执行以下过程：

(1) C 检查 $e(t_iabP,l_ibP)=e(P,W_i)$ 是否成立，如果成立，则返回 $l_i^{-1}t_i^{-1}W_i$ 并且停止模拟（即 $abP=l_i^{-1}t_i^{-1}W_i$），其中 $R_i=l_ibP$。

(2)如果不成立，则 C 检查 L_1 中是否存在条目 $(R_i,\omega_i,*,P_R,T_i)$ 满足 $e(P_R,l_ibP)=e(P,W_i)$。如果满足等式，并且 $\text{ID}_i=\text{ID}_l$，C 返回 T_i 并且用 W_i 代替*。如果 $\text{ID}_i\ne\text{ID}_l$，$C$ 随机选择 $T_i\in\{0,1\}^{lm}$ 返回，并将 $(R_i,\omega_i,W_i,P_R,T_i)$ 插入到表 L_1。

H_2 询问：A_{II} 提交关于 (R_i,C_i,P_i,P_R) 的询问，若 L_2 已经存在相应项，则直接返回 h_{i2} 值；否则 C 随机选择 $h_{i2}\in Z_q^*$，增加 (R_i,C_i,P_i,P_R) 到表 L_2 并返回 h_{i2} 值。

H_3 询问：A_{II} 提交关于 (R_i,C_i,P_i,P_R) 的询问，若 L_3 已经存在相应项，则直接返回 h_{i3} 值；否则 C 随机选择 $h_{i3}\in Z_q^*$，增加 (R_i,C_i,P_i,P_R) 到表 L_3 并返回 h_{i3} 值。

H_4 询问：A_{II} 提交关于 P_{pub} 的询问，若 L_4 已经存在相应项，则直接返回；否则 C 随机选择 $\theta_i\in Z_q^*$，返回 θ_iP 并将 $(P_{\text{pub}},\theta_i)$ 增加到表 L_4。

公钥询问：A_{II} 提交关于 ID_i 的公钥询问，若 L 存在相应项，则直接返回，否则执行以下过程：

(1)如果 $\text{ID}_i\ne\text{ID}^*$，$C$ 随机选择 $t_i\in Z_q^*$，计算 $P_i=t_iP$，返回 P_i 并将 $(\text{ID}_i,\perp,t_i,P_i)$ 添加到表 L。

(2)如果 $\text{ID}_i=\text{ID}^*$，C 随机选择 $t_i\in Z_q^*$，计算 $P_i=t_iaP$，返回 P_i 并将 $(\text{ID}_i,\perp,\perp,P_i)$ 添加到表 L。

秘密值询问：A_{II} 询问 ID_i 的秘密值时，C 执行“公钥询问”询问，如果 $\text{ID}_i\ne\text{ID}^*$，则返回 t_i；否则 C 不能回答这个询问，模拟终止。

解签密询问：对于每个新的询问 $(R_1,R_2,\cdots,R_n,C_1,C_2,\cdots,C_n,V,\text{ID}_i,\text{ID}')$，$C$ 执行以下步骤：

(1)对于身份 ID_i 和 ID' 询问 H_0 和“公钥询问”预言机，获得 Q_i，Q_i' 和 Q_i,P'，然后 C 执行“聚合验证”算法，如果验证等式不成立返回 False，其中 $1\le i\le n$。

(2)对于 ID' 分以下两种情况：

(a)如果 $\text{ID}_i\ne\text{ID}^*$，$C$ 通过正常算法进行签密。

(b)如果 $\text{ID}_i=\text{ID}^*$，C 执行以下过程：查表 H_0，获得 ID' 的 H_0 值 Q_i，C 可以计算 $\omega_i=e(sQ_i,R_i)$。为了保持一致的询问回答，C 检查 L_1 表，对于不同的 ω_i 寻找条目 (R_i,ω_i,W_i,P,T_i)，满足 $e(R_i,P')=e(P,W_i)$ 等式。如果存在这样的条目，说明找到了正确的 W_i。C 利用对应的 T_i 计算 $m_i=T_i\oplus C_i$ 解密密文。

挑战阶段　A_{II} 决定何时结束“阶段 1”并进入“挑战阶段”。A_{II} 选择两个长度相同的消息集合 $\left\{m_{i0}^*\right\}$ 和 $\left\{m_{i1}^*\right\}$ 及接收者 ID_R^* 作为挑战信息，其中 $1\le i\le n$。

如果 ID_R^* 不是目标身份，那么 C 失败。否则 C 根据下列过程构造挑战密文：

(1)查表 L，获得 ID_i^* 公钥 P_i^*，然后随机选择 $l_i \in Z_q^*$，设置 $R_i^* = l_i bP$。

(2)随机选择 $b' \in \{0,1\}$，计算 $C_i = m_{ib}^* \oplus T_i$。然后计算：$V_i^* = h_{i2}^* D_i^* + h_{i3}^* \theta_i P_i^* + \theta_i R_i^*$。

(3)C 使用聚合算法获得 V^*，并输出 $\left(R_1^*, R_2^*, \cdots, R_n^*, C_1^*, C_2^*, \cdots, C_n^*, V^*\right)$ 给 A_{II}。

根据 CLASC 内部安全模型的机密性定义要求，允许攻击者获得发送方的完整私钥。因此，允许攻击者直接使用发送方的部分私钥和秘密值。

阶段 2 A_{II} 可以继续对以上预言机进行多项式有界次地适应性询问，并给出相应的结果。

猜测阶段 A_{II} 选择一个比特 b''，如果 $b' = b''$，那么敌手 A_{II} 赢得游戏 2。

最后，A_{II} 输出消息集合中一个序号。从敌手的角度考虑，每个序号的概率相同，因此，A_{II} 选择任意一个用户作为目标用户的概率相同。如果 $\mathrm{ID}_R^* = \mathrm{ID}'$，则模拟过程完美，除非 A_{II} 询问 H_1 中与挑战相关的条目 $(R_i, \omega_i, W_i, P', T_i)$。如果 L_1 中不存在以上条目，A_{II} 将没有任何优势。如果 L_1 中存在以上条目，那么，对于给定的输入，C 将以敌手 A_{II} 的优势解决 CDH 困难问题。 证毕

5.3 不可伪造性

限于篇幅，略去 CLASC 方案对于敌手 A_{I} 不可伪造性证明过程。以下仅给出针对 A_{II} 敌手的不可伪造性证明过程。

定理 3 随机预言模型下，如果存在敌手 A_{II} 以不可忽略的概率赢得游戏 4，那么存在一个算法 C 能够在概率多项式时间内以 $\varepsilon' = \dfrac{1}{q_{SV}+n} \cdot \left(1 - \dfrac{1}{q_{SV}+n}\right)^{q_{SV}+n-1} \varepsilon$ 的概率解决 CDH 困难问题。

即假设 CDH 问题困难，则改进的 CLASC 方案对于敌手 A_{II} 在适应性选择消息攻击下密文存在性不可伪造，其中 q_{SV} 为秘密值询问的次数。

证明 A_{II} 是敌手，C 是 CDH 问题挑战者。C 给定 CDH 问题实例 (P, aP, bP)，目标是计算 abP。

初始阶段 C 设 $P_{\mathrm{pub}} = sP$，s 为系统主密钥。发送系统参数和主密钥 s 给 A_{II}。

攻击阶段 C 保持列表 $L_0 \sim L_4$ 和 $L = (\mathrm{ID}_i, x_i, P_i)$ 保存 $H_0 \sim H_4$ 预言机询问和密钥询问过程中产生的数据。A_{II} 能够对以下预言机进行适应性询问：

H_0 询问、H_2 询问和 H_3 询问与定理 2 相似。

H_4 询问：A_{II} 提交关于 P_{pub} 的询问，若 L_4 存在相应项，则直接返回；否则 C 随机选择 $\eta \in Z_q^*$，返回 ηbP 并将 (P_{pub}, η) 增加到表 L_4。

公钥询问：A_{II} 提交关于 ID_i 的公钥询问，若 L 存在相应项，则直接返回，否则执行以下过程：

(1)如果 $\mathrm{ID}_i \neq \mathrm{ID}^*$，$C$ 随机选择 $t_i \in Z_q^*$，计算 $P_i = t_i P$，返回 P_i 并将 $(\mathrm{ID}_i, t_i, P_i)$ 添加到表 L。

(2)如果 $\mathrm{ID}_i = \mathrm{ID}^*$，$C$ 随机选择 $t_i \in Z_q^*$，计算 $P_i = t_i aP$，返回 P_i 并将 $(\mathrm{ID}_i, \perp, P_i)$ 添加到表 L。

秘密值询问：A_{II} 询问 ID_i 的秘密值时，如果 $\mathrm{ID}_i \neq \mathrm{ID}^*$，$C$ 执行“公钥询问”询问，返回 x_i 并添加 $(\mathrm{ID}_i, x_i, P_i)$ 到 L 表；否则 C 不能回答这个询问，模拟终止。

H_1 询问：C 保持列表 $L_1 = (R_i, \omega_i, W_i, P_R, T_i)$，初始为空。$C$ 执行以下过程：

(1)C 测试元组 $(R_i, \omega_i, W_i, P_R, T_i)$ 是否满足等式 $e(l_i bP, P_R) = e(P, W_i)$。等式成立则检查 L_1 中是否存在相应条目 $(R_i, \omega_i, W_i, P_R, T_i)$。

(2)如果 L_1 中存在条目 $(R_i, \omega_i, W_i, P_R, T_i)$，则直接返回 T_i；否则 C 随机选择 $V_i \in \{0,1\}^{lm}$ 返回，并将 $(R_i, \omega_i, W_i, P_R, T_i)$ 插入到表 L_1。

签密询问：对于新的询问 $(m_i, \mathrm{ID}_i, \mathrm{ID}_R)$，如果 $\mathrm{ID}_i \neq \mathrm{ID}^*$，使用正常签密算法获得密文。如果 $\mathrm{ID}_i = \mathrm{ID}^*$，$C$ 执行以下过程：

(1)随机选择 $v \in Z_q^*$，计算 $R_i = vP_i$ 和 $T_i = e(sQ_R, R_i)$。

(2)C 检查表 L_1，寻找条目 $(R_i, \omega_i, W_i, P_R, T_i)$，是否存在等式 $e(R_i, P_R) = e(P, W_i)$。如果等式存在，该类条目存在，C 利用 T_i 计算 $C_i = T_i \oplus m_i$；如果等式不存在，C 随机选择 $T_i \in \{0,1\}^{lm}$，并添加 $(R_i, \omega_i, W_i, P_R, T_i)$ 到列表 L_1。

(3)C 通过表 L_2 和 L_3 获得 h_{i2} 和 h_{i3}，并定义 $\phi = (h_{i3}+v)^{-1} uP$，然后计算 $V_i = h_{i2} D_i + uP_i$，其中 $D_i = sQ_i$ 是部分私钥。最后返回 $\delta_i = (R_i, C_i, V_i)$。显然，签密 δ_i 可以通过验证等式：

$$\begin{aligned} e(V_i, P) &= e(h_{i2} D_i + uP_i, P) = e(h_{i2} D_i, P) e(uP_i, P) \\ &= e(h_{i2} Q_i, sP) e(P_i, uP) \\ &= e(h_{i2} Q_i, sP) e\left(P_i, (h_{i3}+v)\phi\right) \\ &= e\left(h_{i2} Q_i, P_{\mathrm{pub}}\right) e\left(\phi, h_{i3} P_i + vP_i\right) \\ &= e\left(h_{i2} Q_i, P_{\mathrm{pub}}\right) \left(\phi, h_{i3} P_i + R_i\right) \end{aligned}$$

伪造阶段 根据分叉引理[13]，对于消息 m_i^*、身份 ID_i^* 及对应公钥 P_i^*、接收者身份 ID_R^* 及对应公钥 P_R^*，其中 $1 \le i \le n$，重放 A_{II} 签密请求，C 可以获得两个有效的聚合密文 δ^* 和 δ'^*。根据游戏 4 的定义，要求至少存在一个用户 ID_i^*，A_{II} 没有提交过关

于 ID_i^* “秘密值询问”和关于 $\left(\mathrm{ID}_1^*, m_1^*, \mathrm{ID}_R\right)$ 的“签密”询问。

不失一般性，令 $\mathrm{ID}^*=\mathrm{ID}_1^*$。则 $V^*=\sum_{i=2}^{n} V_i^* + V_1^*$，$V'^* = \sum_{i=2}^{n} V_i^* + V_1'^*$，其中，

$$\begin{aligned} V_i^* &= h_{12}^* D_1^* + h_{12}^* x_1^* H_4\left(P_{\mathrm{pub}}\right) + r_1^* H_4\left(P_{\mathrm{pub}}\right) \\ &= h_{12}^* D_1^* + h_{12}^* t_1^* \eta abP + r_1^* H_4\left(P_{\mathrm{pub}}\right) \\ V_1'^* &= h_{12}'^* D_1'^* + h_{12}'^* x_1'^* H_4\left(P_{\mathrm{pub}}\right) + r_1'^* H_4\left(P_{\mathrm{pub}}\right) \\ &= h_{12}'^* D_1^* + h_{12}'^* t_1'^* \eta abP + r_1^* H_4\left(P_{\mathrm{pub}}\right) \end{aligned}$$

C 可以计算 $abP = \eta^{-1}\left(h_{12}^* t_1^* - h_{12}'^* t_1'^*\right)^{-1} \cdot\left(V^* - V'^* + \left(h_{12}^* - h_{12}'^*\right) D_1^*\right)$。因此，$C$ 成功获得 CDH 困难问题的一个实例。与文献[14]相似，C 能够成功解决 CDH 困难问题的优势为 $\varepsilon' = \dfrac{1}{q_{SV}+n} \cdot\left(1-\dfrac{1}{q_{SV}+n}\right)^{q_{SV}+n-1} \varepsilon$，其中 q_{SV} 为秘密值询问的次数。　　证毕

5.4 公开验证性

改进方案支持聚合签密的公开验证。根据“聚合验证算法”的验证等式可知，验证聚合签密密文 $\delta=\left(\left\{C_i, R_i\right\}_{i=1}^{n}, V\right)$ 时不需要任何秘密信息，因此，方案满足公开验证性。

5.5 效率分析

表 1 对比了现有无证书聚合签密方案的安全性、效率和公开验证性，其中，P 表示双线性对数，n 表示用户数。文献[8,9]方案需要的双线性对数与用户数相关，效率较低；文献[10,11]方案需要 4 个双线性对；文献[12]方案需要 3 个双线性对运算，但是，该方案不安全。因此，改进方案具有较高的验证效率。

6 结束语

无证书聚合签密能够对签密信息进行聚合传输和批验证，具有一定的应用需求。分析文献[12]聚合签密方案的安全性，该方案不满足机密性和不可伪造性。A_{II} 不仅能够解密密文，而且可以成功伪造新密文。本文首先分析文献[12]方案的安全性，描述了具体的攻击过程，然后提出了新的 CLASC 方案。新方案满足 CLASC 内部安全模型，同时，具有较高的验证效率。

表 1 无证书聚合签密方案对比

方案	安全性	聚合验证需要的对个数	公开验证性
文献[8]方案	可证安全	$(2n+2)P$	否
文献[9]方案	可证安全	$(2n+2)P$	否
文献[10]方案	可证安全	$4P$	是
文献[11]方案	可证安全	$4P$	是
文献[12]方案	不安全	$3P$	否
本文方案	可证安全	$3P$	是

参 考 文 献

[1] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption)<<cost (signature)+cost (encryption)[C]. Proceedings of the Cryptology-CRYPTO 1997, California, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[2] BAEK J, STEINFELD R, and ZHENG Yu-liang. Formal proofs for the security of signcryption[C]. Proceedings of the Cryptology-PKC2002, Paris, France, 2002: 81–98. doi: 10.1007/s00145-007-0211-0.

[3] AN J H, DODIS Y, and RABIN T. On the security of joint signature and encryption[C]. Proceedings of the Cryptography-EUROCRYPT 2002, Netherlands, 2002: 83–107. doi: 10.1007/3-540-46035-7_6.

[4] SELVI S S D, VIVEK S S, SHRIRAM J, *et al*. Identity based aggregate signcryption schemes[C]. Proceedings of the Cryptology-INDOCRYPT 2009, New Delhi, India, 2009: 378–397. doi: 10.1007/978-3-642-10628-6_25.

[5] 张玉磊, 李臣意, 王彩芬, 等. 无证书聚合签名方案的安全性分析和改进[J]. 电子与信息学报, 2015, 37(8): 1994–1999. doi: 10.11999/JEIT141635.

ZHANG Y L, LI C Y, WANG C F, *et al*. Security analysis and improvements of certificateless aggregate signature schemes[J]. *Journal of Electronics & Information Technology*, 2015, 37(8): 1994–1999. doi: 10.11999/JEIT141635.

[6] LU H J and XIE Q. An efficient certificateless aggregate signcryption scheme from pairings[C]. IEEE Proceedings of International Conference on the Electronics, Communications and Control (ICECC), Ningbo, China, 2011: 132–135. doi: 10.1109/ICECC.2011.6067635.

[7] JIANG Y, LI J P, and XIONG A P. Certificateless aggregate signcryption scheme for wireless sensor network[J]. *International Journal of Advancements in Computing Technology*, 2013, 5(8): 456–463. doi: 10.4156/ijact.vol5.issue8.51.

[8] ESLAMI Z and NASROLLAH P. 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. doi: 10.1016/j.jksuci.2014.03.006.

[9] 刘建华, 毛可飞, 胡俊伟. 基于双线性对的无证书聚合签密方案[J]. 计算机应用, 2016, 36(6): 1558–1562. doi: 10.11772/j.issn.1001-9081.2016.06.1558.
LIU J H, MAO K F, and HU J W. Certificateless aggregate signcryption scheme based on bilinear pairings[J] *Journal of Computer Applications*, 2016, 36(6): 1558–1562. doi: 10.11772/j.issn.1001-9081.2016.06.1558.

[10] 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 Y L, WANG H, LI C Y, *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.

[11] CHEN J Q and REN X X. A privacy protection scheme based on certificateless aggregate signcryption and masking random number in smart grid[C]. The 4th International Conference on Mechanical Materials and Manufacturing Engineering (IC3ME2016), Shenzhen, China, 2016: 10–13. doi: 10.2991/mmme-16.2016.3.

[12] 刘建华, 赵长啸, 毛可飞. 高效的无证书聚合签密方案[J]. 计算机工程与应用, 2016, 52(12): 131–135. doi: 10.3778/j.issn.1002-8331.1510-0193.
LIU J H, ZHAO C X, and MAO K F. Efficient certificateless aggregate signcryption scheme based on XOR[J]. *Computer Engineering and Applications*, 2016, 52(12): 131–135. doi: 10.3778/j.issn.1002-8331.1510-0193.

[13] POINTCHEVAL D and STERN J. Security arguments for digital dignatures and blind signatures[J]. *Journal of Cryptology*, 2001, 13(3): 361–396. doi: 10.1007/s001450010003.

[14] CHENG L, WEN Q Y, JIN Z P, *et al*. Cryptanalysis and improvement of a certificateless aggregate signature scheme [J]. *Information Sciences*, 2015, 295(2): 337–346. doi: 10.1016/j.ins.2014.09.065.

张永洁： 女，1978 年生，硕士，副教授，研究方向为密码学与信息安全.

张玉磊： 男，1979 年生，博士，副教授，研究方向为密码学与信息安全.

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.