doi:10.11959/j.issn.1000-436x.2017152

无线漫游认证中可证安全的无证书聚合签名方案

许芷岩[1,2]，吴黎兵[1]，李莉[3]，何德彪[1,4]

(1. 武汉大学计算机学院，湖北 武汉 430072；2. 湖北第二师范学院计算机学院，湖北 武汉 430205；
3. 武汉大学国际软件学院，湖北 武汉 430072；4. 武汉大学软件工程国家重点实验室，湖北 武汉 430072)

摘 要：无证书聚合签名在实现批验证的同时解决了证书管理和密钥托管问题，在资源受限的无线移动网络中得到广泛应用。首先对一个无线匿名漫游认证方案中的无证书聚合签名进行了安全性分析，指出该方案不能抵抗签名伪造攻击，并提出了一种新的安全高效的无证书聚合签名方案。新方案不需要双线性对操作，在随机预言机模型下证明方案是安全的。与原方案相比，所提方案在提高安全性的同时大大降低了计算开销。

关键词：可证安全；无证书；聚合签名；抗伪造攻击

中图分类号：TP309 **文献标识码**：A

Provably secure certificateless aggregate signature scheme in wireless roaming authentication

XU Zhi-yan[1,2], WU Li-bing[1], LI Li[3], HE De-biao[1,4]

(1. Computer School, Wuhan University, Wuhan 430072, China;
2. College of Computer, Hubei University of Education, Wuhan 430205, China;
3.International School of Software , Wuhan University, Wuhan 430072, China;
4. State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China)

Abstract: Certificateless aggregate signature (CLAS) schemes have been widely applied in resource-constrained wireless mobile networks, because they could not only realize batch validation but also solve the certificate management and key escrow problems. It was shown that a certificateless aggregate signature in an anonymous roaming authentication scheme was vulnerable to the signature forge attack. To address the issue, a new secure and efficient certificateless aggregate signature scheme was presented, which required no bilinear pairing operations. And then the security of the scheme under the ECDLP assumption in the random oracle model was proved. Finally the performance of proposed scheme was evaluated. Compared with the original scheme, the proposal is more secure and the total computational cost is greatly reduced .

Key words: provably secure, certificateless, aggregate signature, resist forgery attack

1 引言

把 n 个签名者对 n 个消息的单个签名通过某种方式聚合成一个签名的过程称为聚合签名（AS）。验证者只需验证聚合签名即可判断聚合前的单个签名是否合法。由于聚合签名能够缩短签名长度、实现批验证、降低验证开销，因此，在需要同时验证多个签名的场景得到广泛应用，尤其适合资源受限的无线移动网络漫游认证过程[1]。

为了避免非授权用户使用漫游服务，在提供服务之前，外地服务器（FAS）首先要验证移动用户（MU）的合法性。在认证过程中，同时可能有大量 MU 向 FAS 发出认证请求信息。如果采用单个签名验证方式分别完成认证过程，将会带来很高的

收稿日期：2016-12-05；修回日期：2017-05-11

基金项目：国家自然科学基金资助项目（No.61501333, No.61572379, No.61472287）；湖北省自然科学基金资助项目（No.2015CFA068）；武汉市科技计划基金资助项目（No.2016060101010047）

Foundation Items: The National Natural Science Foundation of China (No.61501333, No.61572379, No.61472287), The Natural Science Foundation of Hubei Province (No.2015CFA068), Science and Technology Program of Wuhan（No.2016060101010047）

通信和认证开销。为了降低认证过程中的开销，研究者尝试了很多方法，其中，刘丹等[2]采用无证书聚合签名技术实现匿名漫游认证方案。

本文首先对刘丹等提出的 Liu-Shi 方案[2]中的聚合签名技术进行了回顾和安全性分析，指出其不能抵抗单个签名伪造攻击。为了解决签名可伪造问题，提出一个新的无证书聚合签名方案。然后分析了新方案的正确性，并在随机预言机模型下证明了方案的安全性。整个方案没有双线性对操作，在提高安全性的同时降低了计算开销。效率分析表明，本文提出的无证书聚合签名方案更适合资源受限的无线移动网络的漫游认证过程。

2 相关工作

为了更好地实现聚合签名，研究者对其进行了深入的理论研究和应用探讨，基于各种密码技术并结合实际应用场景陆续设计出不同的签名方案。

基于对称密码技术的签名方案[3,4]中，需要通信双方预先进行密钥协商，通信量大，可扩展性较差。基于 PKI 公钥密码技术的方案[5,6]，虽然解决了可扩展性问题，但由于每个用户都需要向证书授权机构（CA）申请一个证书，随着用户量的增加，证书管理成本也随之提升。因此，基于 PKI 的签名方案存在证书管理问题。

基于 ID-PKC 技术的签名方案[7,8]能够解决基于 PKI 的签名方案中存在的证书管理问题。但由于每个用户的私钥是由私钥产生器（PKG）根据用户身份信息产生，PKG 知道每个用户的私钥，因此，基于 ID-PKC 的签名方案存在密钥托管等安全性问题。

Al-Riyami 等[9] 提出了一种无证书的公钥密码技术（CL-PKC）。在 CL-PKC 体制中，用户密钥由部分私钥和秘密值两者共同产生，前者由密钥产生中心（KGC）根据用户身份信息生成，后者由用户自己产生。基于 CL-PKC 的签名方案解决了证书管理问题的同时也解决了密钥托管问题，研究者开始对其进行了大量的理论和应用研究[10~16]。Li 等[11]指出文献[10]提出的无证书签名方案不能抵抗第一类敌手的攻击，并提出改进的方案。针对能获取系统主私钥的第二类敌手（主要考虑恶意 KGC），文献[12]提出了一种安全增强的模型。

Gong 等[13] 将 AS 技术与 CL-PKC 体制相结合，首次提出无证书聚合签名（CLAS）方案，但是没有给出方案的安全性证明。Zhang 等[14]对 CLAS 的概念及安全模型进行了重定义，提出一个新的 CLAS 方案，并证明其能够抵抗自适应消息选择攻击。随后，Horng 等[15]提出了一个满足条件隐私的 CLAS 方案，并声称方案是安全的。但 Li 等[16]指出文献[15]的方案不能抵抗恶意 KGC 的攻击。文献[2]的漫游认证方案中提出了一种 CLAS 方案，但该方案对于安全模型中的 2 类敌手均是可伪造的。

3 Liu-Shi 无证书聚合签名方案及安全性分析

3.1 Liu-Shi 无证书聚合签名方案

Liu-Shi 无证书聚合签名方案[2]由 9 个算法组成，具体方案描述如下。

3.1.1 系统初始化算法

1) 给定一个安全参数 $\lambda \in Z^+$，KGC 选择 q 阶循环群 G_1、G_2，其中，$q > 2^\lambda$；$e: G_1 \times G_1 \to G_2$ 表示双线性映射，P 是 G_1 的生成元。

2) KGC 分别定义 3 个安全散列函数：$H_0, H_1 : \{0,1\}^* \to G_1$，$H_2 : \{0,1\}^* \to Z_q^*$。

3) KGC 随机选择一个数 $s \in Z_q^*$ 作为系统主密钥，并计算 $P_{\text{pub}} = sP$。

4) KGC 秘密保存 s，并公开系统参数 $params = \{\lambda, q, e, G_1, G_2, P, P_{\text{pub}}, H_0, H_1, H_2\}$。

3.1.2 部分私钥提取算法

1) 输入用户 U_i 的身份 ID_i，KGC 计算部分私钥 $D_i = sQ_i$。其中，$Q_i = H_0(ID_i)$。

2) KGC 将 D_i 秘密发送给用户 U_i。

3.1.3 秘密值生成算法

用户 U_i 随机选取 $x_i \in Z_q^*$ 作为其秘密值保存。

3.1.4 私钥生成算法

1) 输入用户 U_i 的部分私钥 D_i 和秘密值 x_i。

2) 令 $sk_{ID_i} = (x_i, D_i)$ 为 U_i 的私钥，秘密保存。

3.1.5 公钥生成算法

1) 给定用户 U_i 的私钥 $sk_{ID_i} = (x_i, D_i)$。

2) 计算 $X_i = x_i P$，并令 X_i 为其公钥。

3.1.6 签名算法

1) 离线签名。在没有收到消息 m_i 之前执行，具体步骤描述如下。

① 给定用户私钥 $sk_{ID_i} = (x_i, D_i)$。

② 签名者选择随机值 $r_i \in Z_q^*$ 和状态信息 Δ。

③ 计算 $R_i = r_i P$，$H = H_1(\Delta)$，$V_i = r_i H$ 和 $S_i =$

$D_i + x_i H$ 。

④ 令 (R_i, V_i, S_i) 为 U_i 对消息 m_i 的离线签名。

2) 在线签名。在收到消息 m_i 之后执行，具体步骤描述如下。

① 给定消息 m_i 及其离线签名 (R_i, V_i, S_i) 。

②分别计算 $h_i = H_2(m_i, ID_i, X_i, \Delta)$ 和 $T_i = V_i + h_i S_i$ 。

③ 令 $\sigma_i = (R_i, T_i)$ 为 U_i 对消息 m_i 的在线签名。

3.1.7 单个签名验证算法

1) 给定用户身份 ID_i 、消息 m_i 及其签名 σ_i 。

2) 验证者计算： $Q_i = H_0(ID_i)$ ， $H = H_1(\Delta)$ 和 $h_i = H_2(m_i, ID_i, X_i, \Delta)$ 。

3) 验证式(1)是否成立。

$$e(P, T_i) = e(P_{\text{pub}}, h_i Q_i) e(H, R_i + h_i X_i) \tag{1}$$

若成立，输出 1；否则输出 0。

3.1.8 聚合签名算法

1) 给定 n 个有效的身份—公钥—消息—签名对 $(ID_i, pk_i, m_i, \sigma_i)$ ，其中， $1 \leqslant i \leqslant n$ 。

2) 聚合者计算

$$R = \sum_{i=1}^{n} R_i \tag{2}$$

$$T = \sum_{i=1}^{n} T_i \tag{3}$$

3) 聚合者输出聚合签名 $\sigma = (R, T)$ 。

3.1.9 聚合签名验证算法

1) 输入系统参数 *params* 、 n 个有效的身份—消息—公钥对 (ID_i, m_i, X_i) 和相应聚合签名 σ 。

2) 对于 $1 \leqslant i \leqslant n$ ，验证者计算 $H = H_1(\Delta)$ 、 $Q_i = H_0(ID_i)$ 和 $h_i = H_2(m_i, ID_i, X_i, \Delta)$ 。

3) 对于聚合签名 $\sigma = (R, T)$ ，验证式(4)是否成立。

$$e(P, T) = e(P_{\text{pub}}, \sum_{i=1}^{n} h_i Q_i) e(H, R + \sum_{i=1}^{n} h_i X_i) \tag{4}$$

若成立，则输出 1；否则输出 0。

3.2 安全分析

本节通过给出对 Liu-Shi 方案[2]具体的攻击过程来展示他们提出的签名方案是可伪造的，整个方案是不安全的。假设敌手 $A \in \{A_1, A_2\}$ ，安全模型参见 5.2.1 节。具体攻击过程如下。

1) 系统参数设置

挑战者 C 通过运行 Setup 算法生成系统参数 *params* 和主私钥 s ，并将 *params* 发送给敌手 A 。

2) 查询

A 通过签名查询，获取 U_i 对消息 m_j 和 m_k 的签名，分别记为 $\sigma_j = (R_j, T_j)$ 和 $\sigma_k = (R_k, T_k)$ 。其中，有

$$\sigma_j = \begin{cases} R_j = r_j P \\ T_j = r_j H + h_j S_j \end{cases} \tag{5}$$

$$\sigma_k = \begin{cases} R_k = r_k P \\ T_k = r_k H + h_k S_k \end{cases} \tag{6}$$

3) 伪造签名

为了伪造 U_i $(1 \leqslant i \leqslant n)$ 对消息 m_l 的签名 $\sigma_l = (R_l, T_l)$ ，敌手 A 进行如下操作。

①由于消息 m_l 、签名者身份 ID_i 、公钥 X_i 和系统状态信息 Δ 均为公开的，所以敌手 A 可计算出 h_l 的值，即有 $h_l = H(m_l, ID_i, X_i, \Delta)$ 。

②敌手 A 令

$$h_l = \delta_j h_j + \delta_k h_k \tag{7}$$

其中， δ_j 、 δ_k 是任意选取的 F_q 域中满足式(7)的 2 个元素。

③敌手 A 伪造用户 U_i 对消息 m_l 的签名 $\sigma_l^* = (R_l^*, T_l^*)$ 如下

$$\sigma_l^* = \begin{cases} R_l^* = \delta_j R_j + \delta_k R_k \\ T_l^* = \delta_j T_j + \delta_k T_k \end{cases} \tag{8}$$

4) 验证签名

容易验证伪造的签名 $\sigma_l^* = (R_l^*, T_l^*)$ 是有效的，具体验证过程如下。

计算 $Q_i = H_0(ID_i)$ 、 $h_l = H_2(m_l, ID_i, X_i, \Delta)$ 和 $H = H_1(\Delta)$ ，将 T_l^* 代入式(1)有

$$\begin{aligned} e(P, T_l^*) &= e(P, \delta_j T_j + \delta_k T_k) \\ &= e(P, \delta_j (r_j H + h_j S_i) + \delta_k (r_k H + h_k S_i)) \\ &= e(P, (\delta_j h_j + \delta_k h_k) s Q_i) \cdot \\ &\quad e(H, (\delta_j r_j + \delta_k r_k) P + (\delta_j h_j + \delta_k h_k) x_i P) \\ &= e(P_{\text{pub}}, h_l Q_i) e(H, R_l^* + h_l X_i) \end{aligned}$$

从以上推导结果可知式(1) 成立，且在攻击过程中敌手 A 既没有替换签名者 U_i 的公钥 X_i ，也没有获取系统主私钥 s ，故 Liu-Shi 方案[2]对于安全模型中的 2 类敌手 A_1 和 A_2 均是可伪造的。

4 新的无证书聚合签名方案

为解决 Liu-Shi 方案[2]中存在的签名可伪造问题，本文提出一种新的 CLAS 方案，该方案无双线

性对操作，由 9 个阶段组成，具体方案描述如下。

4.1 系统初始化阶段

由 KGC 执行 Setup 算法生成相关系统参数的过程。具体步骤描述如下。

1) 选择一个安全参数 $l \in Z^+$，满足 $q > 2^l$。G 是阶为素数 q 的循环加法群，P 是 G 的生成元。

2) 选择随机值 $s \in Z_q^*$ 作为系统主私钥。计算 $P_{\text{pub}} = sP$ 作为系统公钥。

3) 分别定义 3 个散列函数 $f_1 \sim f_3$：$\{0,1\}^* \to Z_q^*$。

4) 秘密保存系统主密钥 s，并公开系统参数 $params = \{l, q, G, P, P_{\text{pub}}, f_1, f_2, f_3\}$。

4.2 部分私钥提取阶段

由 KGC 执行 Part-Private-Key-Extract 算法生成用户部分私钥的过程。具体步骤描述如下

1) 给定用户身份 U_i，随机选择 $\omega_i \in Z_q^*$，计算 $W_i = \omega_i P$ 和 $\alpha_i = f_1(ID_i, W_i)$。

2) 计算部分私钥：$\mu_i = \alpha_i s + \omega_i \bmod q$，并将 μ_i 秘密发送给用户 U_i。

4.3 秘密值生成阶段

由用户 U_i 执行 Secret-Value-Set 算法生成其秘密值的过程。具体步骤描述如下。

1) 输入系统参数 $params$。

2) U_i 随机选择 $x_i \in Z_q^*$ 作为其秘密值保存。

4.4 用户私钥提取阶段

由用户 U_i 执行 User-Private-Key-Extract 算法生成用户私钥的过程。具体步骤描述如下。

1) 输入系统参数 $params$、部分私钥 μ_i 和秘密值 x_i。

2) 令 $sk_i = (x_i, \mu_i)$ 为 U_i 私钥，并秘密保存。

4.5 用户公钥提取阶段

由用户 U_i 执行 User-Public-Key-Extract 算法生成用户公钥的过程。具体步骤描述如下。

1) 输入系统参数 $params$、W_i 和秘密值 x_i。

2) 用户计算 $P_i = x_i P$。

3) 令 $pk_i = (W_i, P_i)$ 为用户 U_i 公钥，并公开。

4.6 单个签名阶段

由签名者 U_i 执行 Offline-Sign 和 Online-Sign 算法生成单个消息签名的过程。

Offline-Sign 算法在没有收到消息 m_i 之前执行，具体步骤描述如下。

1) 输入系统参数 $params$、签名者身份 ID_i 及其密钥对 (pk_i, sk_i)。

2) 随机选择 $r_i \in Z_q^*$。分别计算 $R_i = r_i P$、$\beta_i = f_2(ID_i, P_i, R_i)$ 和 $s_i = \mu_i + \beta_i x_i$。

3) 令 (R_i, s_i) 为 U_i 对消息 m_i 的离线签名。

Online-Sign 算法在收到消息 m_i 之后执行，具体步骤描述如下。

1) 输入系统参数 $params$、离线签名 (R_i, s_i)、消息 m_i 和用户密钥对 (pk_i, sk_i)。

2) 首先计算 $\gamma_i = f_3(m_i, ID_i, P_i)$，然后计算 $t_i = s_i + \gamma_i r_i \bmod q$。

3) 令 $\sigma_i = (R_i, t_i)$ 为 U_i 对 m_i 的在线签名。

4.7 单个签名验证阶段

由验证者执行 Part-Verify 算法验证单个签名合法性的过程。具体步骤描述如下。

1) 输入系统参数 $params$、消息 m_i 及其签名 σ_i。

2) 验证者分别计算 $\alpha_i = f_1(ID_i, W_i)$、$\beta_i = f_2(ID_i, P_i, R_i)$ 和 $\gamma_i = f_3(m_i, ID_i, P_i)$。

3) 验证式(9)是否成立。

$$t_i P = \alpha_i P_{\text{pub}} + W_i + \beta_i P_i + \gamma_i R_i \tag{9}$$

若成立，则输出 1；否则输出 0。

4.8 聚合签名阶段

由聚合者执行 Aggregate-Sign 算法通过特定方式生成聚合签名的过程。具体步骤描述如下。

1) 输入系统参数 $params$、n 个有效的身份—公钥—消息—签名对 $(ID_i, pk_i, m_i, \sigma_i)$。

2) 聚合者计算

$$R = \{R_1, R_2, \cdots, R_n\} \tag{10}$$

$$t = \sum_{i=1}^{n} t_i \tag{11}$$

3) 聚合者输出聚合签名 $\sigma = (R, t)$。

4.9 聚合签名验证阶段

由验证者执行 Aggregate-Verify 算法验证聚合签名合法性的过程。具体步骤描述如下。

1) 输入系统参数 $params$、n 个有效的身份公钥—消息 (ID_i, m_i, X_i) 及相应聚合签名 σ。

2) 对于 $1 \leqslant i \leqslant n$，计算 $\alpha_i = f_1(ID_i, W_i)$、$\beta_i = f_2(ID_i, P_i, R_i)$ 和 $\gamma_i = f_3(m_i, ID_i, P_i)$。

3) 对于聚合签名 $\sigma = (R, t)$，验证式(12)是否成立。

$$tP = \sum_{i=1}^{n} \alpha_i P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i P_i + \sum_{i=1}^{n} \gamma_i R_i \tag{12}$$

若成立，则输出 1；否则输出 0。

5　无证书聚合签名方案分析

5.1　方案正确性

证明　假设通过本文提出的 CLAS 方案得到聚合签名 $\sigma=(R,t)$，将其代入式(12)，正确性验证过程如下

$$\begin{aligned} tP &= \sum_{i=1}^{n} t_i P = \sum_{i=1}^{n} (s_i + \gamma_i r_i) P \\ &= \sum_{i=1}^{n} (\alpha_i s P + \omega_i P + \beta_i x_i P + \gamma_i r_i P) \\ &= \sum_{i=1}^{n} \alpha_i P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i P_i + \sum_{i=1}^{n} \gamma_i R_i \end{aligned}$$

5.2　抗伪造性

将新方案的安全性归约为 ECDLP 困难问题，并在随机预言机模型下证明其满足不可伪造性。

5.2.1　安全模型

CLAS 方案的安全模型中包括 2 类攻击者：A_1 和 A_2。其中，A_1 能够替换用户公钥，但不能获取系统主私钥；A_2 能够获取系统主私钥，但不能进行用户公钥替换，主要指恶意的 KGC。

通过挑战者 C 和 2 类攻击者 A_1 和 A_2 之间的游戏来定义本文提出的 CLAS 方案的安全模型，具体定义详见 Game_1 和 Game_2。

1) Game_1

① 运行系统初始化算法

C 运行 Setup 算法，生成系统参数 *params* 和主私钥 s，并返回 *params* 给 A_1。

② 询问

a) 散列询问。A_1 可以访问 CLAS 方案中定义的散列函数 $f_1 \sim f_3$ 对应的预言机。

b) 部分私钥提取询问。A_1 询问 U_i 的部分私钥，C 运行 User-Private-Key-Extract 算法生成部分私钥 μ_i 返回给 A_1。

c) 秘密值询问。A_1 询问 U_i 的秘密值，如果 U_i 已被执行过公钥替换，则返回 $\perp$；否则，C 运行 Secret-Value-Set 算法生成秘密值 x_i 返回给 A_1。

d) 用户公钥询问。A_1 询问 U_i 的公钥，C 运行 User-Public-Key-Extract 算法生成用户公钥 pk_i 返回给 A_1。

e) 公钥替换询问。A_1 用自己指定的公钥 pk_i' 替换用户 U_i 对应的真实公钥 pk_i。

f) 无证书签名询问。A_1 询问 U_i 对消息 m_i 的签名，C 运行 Part-Verify 算法生成签名 σ_i 并返回给 A_1。

③ 伪造

A_1 经过各种预言机询问之后输出一个 ID_i^* 对消息 m_i^* 的聚合签名 σ^*，其中，$1 \leqslant i \leqslant n$，如满足以下要求，则敌手获胜。

a) ID_i^* 从来没有同时提交过部分私钥询问和公钥替换询问。

b) (ID_i^*, m_i^*) 从来没有提交过签名询问。

2) Game_2

① 运行系统初始化算法

挑战者 C 运行 Setup 算法，将生成的系统参数 *params* 和主私钥 s 均返回给 A_2。

② 询问

$f_1 \sim f_3$ 的散列询问、秘密值询问、公钥询问及签名询问同 Game_1，但不能进行公钥替换询问，且不需要部分私钥询问。

③ 伪造

A_2 经过各种预言机询问之后输出一个 ID_i^* 对消息 m_i^* 的聚合签名 σ^*，其中，$1 \leqslant i \leqslant n$，如满足以下要求，则敌手获胜。

a) ID_i^* 从来没有提交过秘密值询问。

b) (ID_i^*, m_i^*) 从来没有提交过签名询问。

5.2.2　安全证明

定理 1　在随机预言机模型下，若 A_1 能够以不可忽略的概率 ξ 伪造出有效的聚合签名，则挑战者 C 就能以不可忽略的概率解决 ECDLP 问题。

证明　挑战者 C 调用 A_1 在一个多项式时间内解决 ECDLP，假设 $(P, P_1 = aP)$ 是 ECDLP 上的一个实例，C 的目标是计算出 a 的值。

C 运行 Setup 算法完成系统初始化，生成 $params = \{l, q, G_1, P, P_{\text{pub}}, f_1, f_2, f_3\}$ 和 s，并将 *params* 发送给 A_1。

令 $P_{\text{pub}} = P_1$，随机选择用户 ID_I 作为被挑战者身份，A_1 执行如下询问。

1) 散列询问

C 在散列询问的过程中分别维护 3 个与 f_1、f_2、f_3 相对应的列表 f_1^{list}、f_2^{list}、f_3^{list}，均初始化为空。

① f_1 询问。A_1 输入 (ID_i, W_i)，若 f_1^{list} 包括 (ID_i, W_i, α_i)，C 返回 α_i；否则随机选取 $\alpha_i \in Z_q^*$，

返回给 A_1，并添加 (ID_i, W_i, α_i) 到 f_1^{list}。

② f_2 询问。A_1 输入 (ID_i, P_i, R_i)，若 f_2^{list} 包括 $(ID_i, P_i, R_i, \beta_i)$，$C$ 返回 β_i；否则随机选取 $\beta_i \in Z_q^*$ 返回给 A_1，并添加 $(ID_i, P_i, R_i, \beta_i)$ 到 f_2^{list}。

③ f_3 询问。A_1 输入 (m_i, ID_i, P_i)，若 f_3^{list} 包括 $(m_i, ID_i, P_i, \gamma_i)$，$C$ 返回 γ_i；否则随机选取 $\gamma_i \in Z_q^*$ 返回给 A_1，并添加 $(m_i, ID_i, P_i, \gamma_i)$ 到 f_3^{list}。

2) 部分私钥询问

C 维护一个结构为 (ID_i, ω_i, μ_i) 的列表 μ^{list}，初始化为空。A_1 输入 ID_i 并询问其部分私钥，C 首先判断 $ID_i = ID_I$ 是否成立，若成立，输出 $\perp$；否则，C 查找 μ^{list}，若存在 (ID_i, ω_i, μ_i)，则直接返回 μ_i 给 A_1；若不存在，则 C 查找 f_1^{list} 获取 α_i，并选择随机值 $\omega_i \in Z_q^*$，计算 $\mu_i = \alpha_i s + \omega_i \bmod q$ 返回 μ_i 给 A_1，并添加 (ID_i, ω_i, μ_i) 到列表 μ^{list}。

3) 秘密值询问

C 维护一个结构为 (ID_i, x_i) 列表 x^{list}，初始化为空。A_1 输入 ID_i 并询问其秘密值，C 首先判断 $ID_i = ID_I$ 是否成立，若成立，则输出 $\perp$；否则，C 查找 x^{list}，若存在 (ID_i, x_i)，直接返回 x_i 给 A_1；若不存在，C 产生一个随机数 $x_i \in Z_q^*$，返回给 A_1，并添加 (ID_i, x_i) 到列表 x^{list}。

4) 公钥询问

C 维护一个结构为 (ID_i, pk_i) 的列表 pk^{list}，初始化为空。A_1 输入 ID_i 并询问其公钥，C 首先查找 pk^{list}，若存在 (ID_i, pk_i)，直接返回 pk_i 给 A_1；否则，C 查找 x^{list} 获取 x_i，计算 $P_i = x_i P$，令 $pk_i = (W_i, P_i)$ 为 ID_i 对应公钥，返回给 A_1，并添加 (ID_i, pk_i) 到列表 pk^{list}。

5) 公钥替换询问

A_1 输入 (ID_i, pk_i') 发起公钥替换询问，C 将列表 pk^{list} 中对应 (ID_i, pk_i) 替换为 (ID_i, pk_i')。

6) 签名询问

当收到询问 ID_i 对 m_i 签名的消息时，C 随机选取 t_i、α_i、β_i、$\gamma_i \in Z_q^*$，并计算 $R_i = \gamma_i^{-1}(t_i P - \alpha_i P_{\text{pub}} - W_i - \beta_i P_i)$，返回签名 $\sigma_i = (R_i, t_i)$ 给 A_1，并分别添加 α_i、β_i、γ_i 到列表 f_1^{list}、f_2^{list}、f_3^{list}。将 $\sigma_i = (R_i, t_i)$ 代入式(9)，很容易验证式(9)成立。因此，由 C 产生的签名与通过合法方式产生的签名满足不可区分性。

最后，A_1 输出一个有效的 n 个消息—身份对 (m_i, ID_i) 的聚合签名 $\sigma = (R, t)$。C 验证式(12) 是否成立，若不成立则退出。根据伪造引理[17]，A_1 可以输出另外一个有效签名 $\sigma^* = (R, t^*)$，如果通过选择不同的 f_1 重复这个过程，可以得到

$$t^* P = \sum_{i=1}^{n} \alpha_i^* P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i P_i + \sum_{i=1}^{n} \gamma_i R_i \quad (13)$$

由式(12) 和式(13) 可以得到如下推导过程。

$$\begin{aligned} tP - t^* P &= \sum_{i=1}^{n} (t_i - t_i^*) P \\ &= \sum_{i=1}^{n} \alpha_i P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i P_i + \sum_{i=1}^{n} \gamma_i R_i - \\ &\quad \left(\sum_{i=1}^{n} \alpha_i^* P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i P_i + \sum_{i=1}^{n} \gamma_i R_i\right) \\ &= \sum_{i=1}^{n} (\alpha_i - \alpha_i^*) aP \end{aligned}$$

进一步可得出

$$\sum_{i=1}^{n} (t_i - t_i^*) P = \sum_{i=1}^{n} (\alpha_i - \alpha_i^*) aP \quad (14)$$

由式(14)，C 可求出 $a = \sum_{i=1}^{n} (t_i - t_i^*)(\alpha_i - \alpha_i^*)^{-1}$，这与 ECDLP 困难问题假设相矛盾。因此，本文提出的 CLAS 方案能够抵抗随机预言机模型下 A_1 类型敌手的攻击，是不可伪造的。

定理 2 在随机预言机模型下，若 A_2 能够以不可忽略的概率 ξ 伪造出有效的聚合签名，则挑战者 C 就能以不可忽略的概率解决 ECDLP 问题。

证明 挑战者 C 调用 A_1 在一个多项式时间内解决 ECDLP，假设 $(P, P_1 = aP)$ 是 ECDLP 上的一个实例，C 的目标是计算出 a 的值。

C 运行 Setup 算法，生成系统参数 $params = \{l, q, G_1, P, P_{\text{pub}}, f_1, f_2, f_3\}$ 和主私钥 s，并将 $params$ 和 s 发送给 A_2。随机选择用户身份 ID_I 作为被挑战者身份，A_2 执行如下询问。

$f_1 \sim f_3$ 散列询问、秘密值询问、签名询问同定理 1，且没有部分私钥询问和公钥替换询问。

公钥询问 C 维护一个结构为 (ID_i, pk_i) 的列表 pk^{list}，初始化为空。A_2 输入 ID_i 并询问其公钥，C 首先查找 pk^{list}，若存在 (ID_i, pk_i)，则直接返回 pk_i 给 A_2，否则，C 首先判断 $ID_i = ID_I$ 是否成立，若成立，C 令 $P_i = P_1$；若不成立，C 查找 x^{list} 获取 x_i，

计算 $P_i = x_i P$。令 $pk_i = (W_i, P_i)$，返回给 A_2，并添加 (ID_i, pk_i) 到列表 pk^{list}。

最后 A_2 输出一个有效的 n 个消息—身份对 (m_i, ID_i) 的聚合签名 $\sigma = (R, t)$。C 验证等式(12)是否成立，若不成立则退出。根据伪造引理[17]，A_2 可以输出另外一个有效签名 $\sigma^* = (R, t^*)$，如果通过选择不同的 f_2 重复这个过程，可以得到

$$t^* P = \sum_{i=1}^{n} \alpha_i P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i^* P_i + \sum_{i=1}^{n} \gamma_i R_i \quad (15)$$

由式(12)和式(15)可以得到如下推导过程。

$$\begin{aligned} tP - t^* P &= \sum_{i=1}^{n} (t_i - t_i^*) P \\ &= \sum_{i=1}^{n} \alpha_i P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i P_i + \sum_{i=1}^{n} \gamma_i R_i - \\ &\quad \left(\sum_{i=1}^{n} \alpha_i P_{\text{pub}} + \sum_{i=1}^{n} W_i + \sum_{i=1}^{n} \beta_i^* P_i + \sum_{i=1}^{n} \gamma_i R_i \right) \\ &= \sum_{i=1}^{n} (\beta_i - \beta_i^*) aP \end{aligned}$$

进一步可得出

$$\sum_{i=1}^{n} (t_i - t_i^*) P = \sum_{i=1}^{n} (\beta_i - \beta_i^*) aP \quad (16)$$

由式(16)，C 可求出 $a = \sum_{i=1}^{n} (t_i - t_i^*)(\beta_i - \beta_i^*)^{-1}$，这与 ECDLP 困难问题假设相矛盾。因此，本文提出的 CLAS 方案能够抵抗随机预言机模型下 A_2 类型敌手的攻击，是不可伪造的。

6　效率分析

在保证安全性的同时还要考虑协议的计算开销等效率问题。如表 1 所示，分 4 个阶段（单个签名生成、单个签名验证、聚合签名生成及聚合签名验证）对 Liu-Shi 方案[2]和本文方案的计算开销进行详细的对比。容易发现，在保证安全性的同时本文方案具有更高的效率，更适合在资源受限的无线移动网络中使用。其中，$T_{\text{z-sa}}$ 表示 Z_q^* 上的加法运算；$T_{\text{z-sm}}$ 表示 Z_q^* 上的乘法运算；T_{mts} 表示普通散列运算；T_{mtp} 表示散列到点运算；$P_{\text{ecc-pa}}$ 表示椭圆曲线上的点加运算；$P_{\text{ecc-pm}}$ 表示椭圆曲线上的点乘运算；T_{bp} 表示双线性对运算。

7　结束语

聚合签名能够有效降低验证开销。本文首先指出 Liu-Shi 匿名漫游认证方案[2]中提出的签名方法对于安全模型中的 2 类敌手 A_1 和 A_2 均是可伪造的；然后提出了一种新的无证书聚合签名方案，将其安全性归约为 ECDLP 困难问题，并在随机预言机模型下给出安全性证明；最后分析比较了 2 个方案的效率。与 Liu-Shi 方案相比，本文方案在保证安全性的前提下，将计算开销大大降低，提高了验证性能，增强了无证书聚合签名技术在资源受限的无线移动网漫游认证过程中的实用性。

参考文献：

[1] XIONG H, WU Q, CHEN Z. An efficient provably secure certificateless aggregate signature applicable to mobile computation[J]. Control and Cybernetics, 2012, 41(2): 373-391.

[2] 刘丹, 石润华, 张顺, 等. 无线网络中基于无证书聚合签名的高效匿名漫游认证方案[J]. 通信学报, 2016, 37(7): 182-192.
LU D, SHI R H, ZHANG S, et al. Efficient anongmons roaming autbenticotion scheme using certificateless aggregate signature in wireless network[J]. Journal on Communications, 2016, 37(7): 182-192.

[3] JIANG Y, LIN C, SHEN X, et al. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks[J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569-2577.

[4] ZHOU T, XU J. Provable secure authentication protocol with anonymity for roaming service in global mobility networks[J]. Computer Networks, 2011, 55(1): 205-213.

[5] REN K, LOU W, KIM K, et al. A novel privacy preserving authentication and access control scheme for pervasive computing environments[J]. IEEE Transactions on Vehicular Technology, 2006, 55(4): 1373-1384.

[6] KIM J, CHOI S, KIM K, et al. Anonymous authentication protocol for dynamic groups with power-limited devices[C]//Symposium on Cryptography and Information Security (SCIS'03). 2013: 405-410.

表 1　　**计算开销对比**

阶段	Liu-Shi 方案[2]	本文方案
单个签名生成	$T_{\text{mts}} + T_{\text{ecc-pa}} + T_{\text{ecc-pm}}$	$T_{\text{mts}} + T_{\text{z-sa}} + T_{\text{z-sm}}$
单个签名验证	$T_{\text{mts}} + 2T_{\text{mtp}} + 3T_{\text{bp}} + T_{\text{ecc-pa}} + 2T_{\text{ecc-pm}}$	$3T_{\text{mts}} + 3T_{\text{ecc-pa}} + 4T_{\text{ecc-pm}}$
聚合签名生成	$2(n-1)T_{\text{ecc-pa}}$	$(n-1)T_{\text{z-sa}}$
聚合签名验证	$nT_{\text{mts}} + (n+1)T_{\text{mtp}} + 3T_{\text{bp}} + (2n-1)T_{\text{ecc-pa}} + 2nT_{\text{ecc-pm}}$	$3nT_{\text{mts}} + (3n+1)T_{\text{ecc-pm}} + (4n-1)T_{\text{ecc-pa}}$

[7] WAN Z, REN K, PRENEEL B. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks[C]//The lst ACM Conference on Wireless Network Security. ACM, 2008: 62-67.

[8] YANG G, HUANG Q, WONG D S, et al. Universal authentication protocols for anonymous wireless communications[J]. IEEE Transactions on Wireless Communications, 2010, 9(1): 168-174.

[9] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 2003: 452-473.

[10] YAP W S, HENG S H, GOI B M. An efficient certificateless signature scheme[C]//International Conference on Embedded and Ubiquitous Computing. Springer Berlin Heidelberg, 2006: 322-331.

[11] LI J, HUANG X, MU Y, et al. Cryptanalysis and improvement of an efficient certificateless signature scheme[J]. Journal of Communications and Networks, 2008, 10(1): 10-17.

[12] AU M H, MU Y, ChEN J, et al. Malicious KGC attacks in certificateless cryptography[C]//The 2nd ACM Symposium on Information, Computer and Communications Security. ACM, 2007: 302-311.

[13] GONG Z, LONG Y, HONG X, et al. Two certificateless aggregate signatures from bilinear maps[C]//Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on. IEEE, 2007, 3: 188-193.

[14] ZHANG L, ZHANG F. A new certificateless aggregate signature scheme [J]. Computer Communications, 2009, 32(6): 1079-1085.

[15] HORNG S J, TZENG S F, HUANG P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences, 2015, 317: 48-66.

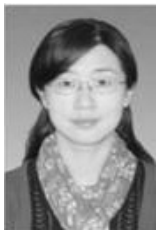
[16] LI J, YUAN H, ZHANG Y. Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Networks, 2015, 317: 48-66.

[17] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

作者简介：

许芷岩（1982-），女，河南周口人，武汉大学博士生，主要研究方向为应用密码学、云存储安全与隐私保护等。

吴黎兵（1972-），男，湖北黄梅人，博士，武汉大学教授、博士生导师，主要研究方向为分布式计算、网络管理等。



李莉（1979-），女，安徽芜湖人，博士，武汉大学副教授、博士生导师，主要研究方向为数据安全、嵌入式安全等。

何德彪（1980-），男，山东阳谷人，博士，武汉大学教授、博士生导师，主要研究方向为应用密码学、安全协议、云计算安全等。