两个无证书聚合签名方案的安全性分析

罗 敏[①] 孙 腾[*①] 张静茵[①] 李 莉[②]
[①](武汉大学计算机学院 武汉 430072)
[②](武汉大学国际软件学院 武汉 430072)

摘 要：张玉磊等人(2015)提出了两种无证书聚合签名方案，并证明其方案在随机预言机模型下是可证明安全的。该文分析张玉磊等人提出的两种方案的安全性，指出了第 1 种方案可以抵抗两类攻击者的攻击；第 2 种方案不能抵抗第 1 类攻击者和第 2 类攻击者的攻击，给出详细的攻击过程，证明攻击者伪造出的签名可以通过验证，分析了第 2 种方案存在伪造攻击的原因，提出了改进的方案。

关键词：公钥密码体制；无证书聚合签名；KGC 被动攻击；计算性 Diffie-Hellman 问题；签名伪造
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2016)10-2695-06
DOI: 10.11999/JEIT151350

Security Analysis on Two Certificateless Aggregate Signature Schemes

LUO Min[①] SUN Teng[①] ZHANG Jingyin[①] LI Li[②]
[①](*Computer School*, *Wuhan University*, *Wuhan* 430072, *China*)
[②](*International School of Software*, *Wuhan University*, *Wuhan* 430072, *China*)

Abstract: Zhang *et al.* (2015) proposed two certificateless aggregate signature schemes, and they demonstrated that both of their schemes are provably secure in the random oracle model. This paper analyzes the security of two schemes proposed by Zhang *et al.* and indicates that the first scheme can resist the attacks by Type 1 and Type 2 adversaries, and the second scheme can not resist the attacks by Type 1 and Type 2 adversaries. The study shows the processes of concrete forgery attacks, and proves the validity of the forged signature by attackers. The reasons of forgery attacks in the second scheme are analyzed, and the modified scheme is proposed.

Key words: Public key cryptography; Certificateless aggregate signature; KGC passive attack; Computational Diffie-Hellman problem; Signature forgery

1 引言

文献[1]提出了公钥密码体制思想，是现代密码学最重要的发明和进展，对于保护网络中的信息安全有着重大意义。在传统的公钥密码体制中，要求存在一个可信的认证中心给每个用户颁发一个证书，用来绑定用户身份和公钥，因此一旦用户量巨大，证书中心需要管理的证书就会剧增，极大地降低了系统的性能。为了缩减证书管理的规模，文献[2]提出了基于用户身份的公钥密码思想，即用户可以选择自己的身份信息(例如学号，邮箱地址，电话号码等)作为公钥，这样就可以有效地解决传统公钥密码体制中的证书管理问题。随着基于身份的公钥密码思想进一步发展，许多基于身份的加密签名方案被提出[3,4]。然而，基于用户身份的签名方案要求存在一个可信的私钥生成中心，用来根据用户身份生成相应的私钥，依次这种公钥密码体制面临着私钥托管问题，即私钥生成中心可以获得所有用户的私钥，从而可以伪造任意用户对任意消息的签名。

为了同时解决传统公钥密码体制中的证书管理和基于用户身份的公钥密码思想中的私钥托管问题，文献[5]提出了无证书公钥密码体制。在这种体制中，私钥生成中心仅仅生成用户的部分私钥，用户再根据私钥生成中心生成的部分私钥和自己选择的秘密值来独立地生成自己的公钥和私钥，这样就同时解决了证书管理和私钥托管两个问题，所以众多满足不同需求的无证书签名方案不断被提出，如文献[6]提出的等级无证书签名方案以及文献[7]提出的无证书群签名方案等等。

随着应用密码学的不断发展，现实中越来越多地要求 n 个签名者对 n 个不同的消息进行签名。传统的数字签名方案随着 n 的不断增大，签名的长度

收稿日期：2015-12-01；改回日期：2016-05-27；网络出版：2016-07-14
*通信作者：孙腾 sunt@whu.edu.cn
基金项目：国家自然科学基金(61402339)
Foundation Item: The National Natural Science Foundation of China (61402339)

和验证工作的复杂度都会不断提升。聚合签名能有效地解决这个问题，减少签名长度，降低签名验证和通信的开销。文献[8]首次提出了聚合签名概念，并给出了基于 BLS 短签名下的构造方案。文献[9]提出基于门限置换的聚合签名方案签名者将签名依次聚合，产生最后的聚合签名。文献[10]将聚合签名与无证书公钥密码机制结合起来，首次提出了无证书聚合签名方案，并给出了两个利用双线性对实现的具体方案。文献[11]提出了一个有效的无证书聚合签名方案，并基于随机预言机模型证明了其安全性。文献[12]提出了一个新型无证书聚合签名方案。文献[13]同样利用双线性对提出了无证书签名方案和无证书聚合签名方案，但文献[14]指出该方案安全性存在问题并给予了改进。

文献[15]基于双线性对提出了一个高效的随机预言机模型下的无证书聚合签名方案，并证明了基于计算性 Diffie-Hellman 假设，该方案在适应性选择消息攻击下是存在性不可伪造的。文献[16]对文献[15]中的无证书聚合签名方案安全性进行深入分析，指出了文献[15]中的方案依旧存在 KGC 被动攻击，并且为了克服原方案存在 KGC 被动攻击的不足，提出了两种改进方案。

本文对文献[16]中张玉磊等人提出的改进方案进行研究和安全性分析，证明了对于无证书聚合签名方案的两类攻击者来说，第 1 种方案可以抵抗两类攻击者的攻击，而第 2 种方案无法抵抗两类攻击者的攻击，一旦攻击者获取到用户对一条消息的合法有效的签名，就能够伪造出用户对其他任意消息的合法有效的签名，即第 2 种方案无法满足弱不可伪造性。

2 背景知识

2.1 双线性对

设 G_1 是由生成元 P 生成的加法群，其阶为大素数 q， G_2 一个乘法群，其阶也为 q。设存在映射 $e: G_1 \times G_1 \to G_2$，该映射满足下列性质：

(1)双线性性：对所有的 $R,Q \in G_1$， $a,b \in Z_q^*$，$e(aR,bQ) = e(R,Q)^{ab}$ 都成立。

(2)非退化性：存在 $R,Q \in G_1$，使得 $e(R,Q) \neq 1$。

(3)可计算性：对于所有的 $R,Q \in G_1$，可以找出有效的算法计算 $e(R,Q)$。

那么就把该映射 e 称为双线性对。

同时，在加法群 G_1 中存在如下假设：

(1)群 G_1 中的计算性 Diffie-Hellman 问题(Computational Diffie-Hellman Problem, CDHP)：对于未知的 $a,b \in Z_q^*$，给定群 G_1 的生成元 P 和 (aP,bP)，没有多项式时间的算法能以不可忽略的概率计算出 $abP \in G_1$，即群 G_1 中的计算性 CDH 问题是困难的。

(2)离散对数问题(Discrete Logarithm Problem, DLP)：对于未知的 $a \in Z_q^*$，给定 G_1 的生成元 P 和 aP，没有多项式时间的算法能以不可忽略的概率计算出 a。

2.2 无证书聚合签名方案

无证书聚合签名方案包括以下 6 个算法：

(1)系统建立算法：输入安全参数 k，由密钥生成中心 KGC 生成系统主密钥 s 和系统参数 pm。

(2)部分私钥生成算法：输入用户身份 ID_i 系统参数 pm 和系统主密钥 s，KGC 计算出用户的部分私钥 D_i，并将 D_i 发送给相应用户。

(3)用户密钥生成算法：用户自己选择秘密值 x_i，输入用户身份 ID_i 和系统参数 pm，生成用户完整私钥 $S_i = (D_i, x_i)$ 以及用户公钥 P_i。

(4)签名算法：输入待签名消息 m_i、用户身份 ID_i、用户完整私钥 S_i 和系统参数 pm，生成用户对消息 m_i 的签名 σ_i。

(5)验证算法：输入消息/签名对 (m_i,σ_i)、用户身份 ID_i、用户公钥 P_i 和系统参数 pm，验证签名是否合法有效。若签名正确，则输出真，否则输出假。

(6)聚合签名生成算法：输入每个用户 ID_i 对于消息 m_i 的签名 σ_i，生成聚合签名 σ，其中 $1 \le i \le n$。

(7)聚合签名验证算法：输入系统参数 pm，消息 m_i，用户公钥 P_i 和聚合签名 σ，验证聚合签名是否合法有效。若聚合签名正确，则输出真，否则输出假，其中 $1 \le i \le n$。

3 文献[16]的无证书聚合签名改进方案回顾

文献[15]提出的具体方案包括以下 6 个算法：

(1)系统建立算法：令安全参数为 k，定义两个循环群 G_1 和 G_2，它们的阶为大素数 q， P 为 G_1 的一个生成元，定义双线性对映射 $e: G_1 \times G_1 \to G_2$。定义哈希函数 $H_1, H_2, H_3: \{0,1\}^* \to G_1, H_4: \{0,1\}^* \to Z_q^*$。KGC 随机选取 $s \in Z_q^*$ 为主密钥，计算 $P_{\mathrm{pub}} = sP$，生成系统参数为 $\{G_1, G_2, e, q, P, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4\}$，KGC 将系统参数公布，秘密保存主密钥 s。

(2)部分私钥生成算法：KGC 计算出 $Q_i = H_1(\mathrm{ID}_i)$, $D_i = sQ_i$，并将 D_i 发送给相应用户。

(3)用户密钥生成算法：用户随机选择秘密值 x_i，生成用户私钥 $S_i = (D_i, x_i)$ 以及用户公钥 $P_i = sP$。

(4)部分签名生成算法：用户运行此算法的具体步骤为：

(a)随机选择 r_i，计算出 $R_i = r_iP$。

(b)计算 $U = H_2(\theta)$, $T=H_3(\theta)$, $h_i=H_4(\theta||\mathrm{ID}_i||m_i||P_i)$。其中 θ 为用户状态信息。

(c)令 $S_i = D_i + x_i(h_iP_{\mathrm{pub}} + U) + r_iT$，则用户 ID_i 对消息 m_i 的签名为 $\sigma_i = (S_i, R_i)$。

(5)聚合签名生成算法：对于每个用户的签名 $\sigma_i = (S_i, R_i)$, $1 \le i \le n$，计算 $S = \sum_{i=1}^{n} S_i$, $R = \sum_{i=1}^{n} R_i$，得到聚合签名 $\sigma = (S, R)$。

(6)聚合签名验证算法：输入身份列表 $\{\mathrm{ID}_i\}$，公钥列表 $\{P_i\}$，状态信息 θ 以及聚合签名 $\sigma = (S, R)$，验证者运行此算法的步骤为：

(a)计算 $Q_i = H_1(\mathrm{ID}_i)$, $U = H_2(\theta)$, $T = H_3(\theta)$, $h_i = H_4(\theta||\mathrm{ID}_i||m_i||P_i)$。

(b)验证下列等式是否成立：$e(S,P) \stackrel{?}{=} e\left(\sum_{i=1}^{n}(Q_i + h_iP_i), P_{\mathrm{pub}}\right) e\left(\sum_{i=1}^{n} P_i, U\right) e(T, R)$ 若成立则输出真，否则输出假。

对于上述方案，密钥生成中心 KGC 能够计算出 $x_iU + r_iT$，并且在哈希函数 H_4 中不存在输入项 R_i，因此 KGC 可以利用 $x_iU + r_iT$ 和 R_i 伪造出用户对任意消息的签名，即上述方案无法抵抗 KGC 被动攻击。为了避免这种情况，文献[16]对文献[15]的方案作出了如下改进。改进方案包括两部分：

(1)将用户状态信息 θ 用 P_{pub} 代替，这样可以减少用户群维护公共状态信息的通信开销。

(2)通过两种方法阻止 KGC 计算出 $x_iU + r_iT$ 的值。

改进方案 1：将元素 R_i 嵌入 H_4 哈希函数，并调整 h_i 在 S_i 中的位置；

改进方案 2：增加哈希函数 H_5，并重新设计 S_i 的生成表达式。

以下仅列出两种方案改进的内容：

(1)改进方案 1：

(a)将元素 R_i 嵌入 H_4 中，即 $h_i=H_4(\mathrm{ID}_i||m_i||P_i||R_i)$。

(b)签名生成算法为：

(i)随机选择 r_i，计算出 $R_i = r_iP$。

(ii)计算 $U = H_2(P_{\mathrm{pub}})$, $T = H_3(P_{\mathrm{pub}})$, $h_i=H_4(\mathrm{ID}_i||m_i||P_i||R_i)$。

(iii)令 $S_i = D_i + h_ix_i(P_{\mathrm{pub}} + U) + r_iT$，则用户 ID_i 对消息 m_i 的签名为 $\sigma_i = (S_i, R_i)$。

(c)聚合签名生成算法：将原方案中生成的聚合签名 $\sigma = (S, R)$ 改为 $\sigma = (S, R_1, R_2, \cdots, R_n)$。

(d)聚合签名验证算法：验证 $\sigma = (S, R_1, R_2, \cdots, R_n)$ 的有效性。

(i)计算 $Q_i=H_1(\mathrm{ID}_i)$, $U=H_2(P_{\mathrm{pub}})$, $T=H_3(P_{\mathrm{pub}})$, $h_i = H_4(\mathrm{ID}_i||m_i||P_i||R_i)$。

(ii)验证等式(1)是否成立：

$$e(S,P) \stackrel{?}{=} e\left(\sum_{i=1}^{n}(Q_i + h_iP_i), P_{\mathrm{pub}}\right) \cdot e\left(U, \sum_{i=1}^{n} h_iP_i\right) e\left(T, \sum_{i=1}^{n} R_i\right) \quad (1)$$

若成立则输出真，否则输出假。

(2)改进方案 2：

(a)增加哈希函数 $H_5:\{0,1\}^* \to Z_q^*$，计算 $k_i = H_5(\mathrm{ID}_i||m_i||P_i)$，其余哈希函数保持不变。

(b)重新设计 S_i 生成表达式，签名生成算法为：

(i)随机选择 r_i，计算出 $R_i = r_iP$。

(ii)计算 $U = H_2(P_{\mathrm{pub}})$, $T=H_3(P_{\mathrm{pub}})$, $h_i=H_4(\mathrm{ID}_i||m_i||P_i)$, $k_i = H_5(\mathrm{ID}_i||m_i||P_i)$。

(iii)令 $S_i = D_i + x_i(h_iP_{\mathrm{pub}} + k_iU) + r_iT$，则用户 ID_i 对消息 m_i 的签名为 $\sigma_i = (S_i, R_i)$。

(c)聚合签名生成算法：与原始方案相同。

(d)聚合签名验证算法：输入身份列表 $\{\mathrm{ID}_i\}$，公钥列表 $\{P_i\}$ 以及聚合签名 $\sigma = (S, R)$，验证者运行此算法的步骤为：

(i)计算 $U = H_2(P_{\mathrm{pub}})$, $T = H_3(P_{\mathrm{pub}})$, $h_i = H_4(\mathrm{ID}_i||m_i||P_i)$ 和 $k_i = H_5(\mathrm{ID}_i||m_i||P_i)$。

(ii)验证等式(2)是否成立：

$$e(S,P) \stackrel{?}{=} e\left(\sum_{i=1}^{n} Q_i + h_iP_i, P_{\mathrm{pub}}\right) e\left(U, \sum_{i=1}^{n} k_iP_i\right) e(T, R) \quad (2)$$

若成立则输出真，否则输出假。

4　文献[16]的改进方案的安全性分析

对于无证书聚合签名方案，一般考虑两类攻击者，A_1 和 A_2。其中 A_1 不能获得系统主密钥 s，但可以进行公钥替换攻击，它模拟的是普通用户；A_2 可以得到系统主密钥，但不允许进行公钥替换攻击，它模拟的是恶意的 KGC。

第 1 类攻击者 A_1 可以进行的预言机询问如下：

(1)用户建立询问：即输入用户身份 ID_i，挑战者 B 运行部分私钥生成算法和用户密钥生成算法计算出用户部分私钥 D_i、秘密值 x_i 和公钥 P_i，B 将 $(\mathrm{ID}_i, D_i, x_i, P_i)$ 保存到列表中，并返回 P_i。

(2)部分私钥询问：即输入用户身份 ID_i，如果 B 保存的列表中有对应身份，则返回 D_i，否则返回空值。

(3)秘密值询问：即输入用户身份 ID_i，如果 B 保存的列表中有对应身份，则返回 x_i，否则返回空值，如果用户公钥被替换，也返回空值。

(4)公钥替换询问：即输入用户身份 ID_i 和攻击者 A_1 选择的公钥 P_i'，如果 B 保存的列表中有对应

身份，则用 $P_i^{'}$ 替换 P_i。

(5)签名询问：即输入用户身份 ID_i，返回对消息 m_i 的签名 σ_i，并且 σ_i 必须通过签名验证算法。

第 2 类攻击者 A_2 由于可以获得主密钥 s，因此不考虑部分私钥询问，也不允许执行公钥替换询问，A_2 可以进行的预言机询问如下：

(1)用户建立询问：即输入用户身份 ID_i，挑战者 B 运行部分私钥生成算法和用户密钥生成算法计算出用户部分私钥 D_i、秘密值 x_i 和公钥 P_i，B 将 $(\mathrm{ID}_i, D_i, x_i, P_i)$ 保存到列表中，并返回 P_i。

(2)秘密值询问：即输入用户身份 ID_i，如果 B 保存的列表中有对应身份，则返回 x_i，否则返回空值，如果用户公钥被替换，也返回空值。

(3)签名询问：即输入用户身份 ID_i，返回对消息 m_i 的签名 σ_i，并且 σ_i 必须通过签名验证算法。

对于无证书聚合签名方案的两种改进方法，文献[16]证明了在随机预言机模型下它们是安全的，但在本节中，我们将通过具体的伪造过程模拟两类攻击者 A_1 和 A_2 在两种改进方案中的攻击能力，分析改进方案是否真正安全。

4.1 攻击者 A_1 对于改进方案 1 的签名伪造过程

由于攻击者 A_1 不知道系统主密钥，但可进行公钥替换攻击，而公钥 $P_i = x_iP$，即 A_1 可获得用户秘密值 x_i，那么 A_1 的攻击过程如下所示：

(1)A_1 通过签名询问，输入用户身份 ID_i，得到用户对消息 m_i 的签名 $\sigma_i = (S_i, R_i)$，其中 $S_i = D_i + h_i x_i(P_{\mathrm{pub}} + U) + r_iT$，$R_i = r_iP$。

(2)令 $W_i = S_i - h_i x_i(P_{\mathrm{pub}} + U) = D_i + r_iT$，即用 W_i 代替 S_i 计算式中未知部分 $D_i + r_iT$，由于 S_i，$h_i = H_4(\mathrm{ID}_i \| m_i \| P_i \| R_i)$，$x_i$，$P_{\mathrm{pub}}$ 和 $U = H_2(P_{\mathrm{pub}})$ 均为 A_1 可以知道的，因此 A_1 就可以利用已获得的签名 $\sigma_i = (S_i, R_i)$ 计算出未知部分 W_i。

(3)对于另一消息 m_i^*，A_1 在伪造签名时需要知道 S_i，R_i，$h_i^* = H_4(\mathrm{ID}_i \| m_i^* \| P_i \| R_i^*)$，$x_i$，$P_{\mathrm{pub}}$ 和 $U = H_2(P_{\mathrm{pub}})$，由于 $R_i^* = r_i^*P$，而 A_1 无法获得用户随机选择的 r_i^*，从而 A_1 无法计算出 $h_i^* = H_4(\mathrm{ID}_i \| m_i^* \| P_i \| R_i^*)$，也就无法伪造出对 m_i^* 的签名。

定理 1 改进方案 1 面对第 1 类敌手 A_1 是安全的。

证明 通过上述分析可以看到，A_1 在伪造签名时必须要计算 h_i^*，而计算 h_i^* 必须获得 R_i^* (不能是 R_i，否则无法通过验证)，因此 h_i^* 是 A_1 无法计算的，从而改进方案 1 面对第 1 类敌手 A_1 是安全的。

4.2 攻击者 A_1 对于改进方案 2 的签名伪造过程

由于攻击者 A_1 不知道系统主密钥，但可进行公钥替换攻击，而公钥 $P_i = x_iP$，即 A_1 可获得用户秘密值 x_i，那么 A_1 可以通过以下过程伪造出用户的合法有效的签名：

(1)A_1 通过签名询问，输入用户身份 ID_i，得到用户对消息 m_i 的签名 $\sigma_i = (S_i, R_i)$，其中 $S_i = D_i + x_i(h_iP_{\mathrm{pub}} + k_iU) + r_iT$，$R_i = r_iP$。

(2)令 $W_i = S_i - x_i(h_iP_{\mathrm{pub}} + k_iU) = D_i + r_iT$，即用 W_i 代替 S_i 计算式中未知部分 $D_i + r_iT$，由于 S_i，$h_i = H_4(\mathrm{ID}_i \| m_i \| P_i)$，$k_i = H_5(\mathrm{ID}_i \| m_i \| P_i)$，$x_i$，$P_{\mathrm{pub}}$ 和 $U = H_2(P_{\mathrm{pub}})$ 均为 A_1 可以知道的，因此 A_1 就可以利用已获得的签名 $\sigma_i = (S_i, R_i)$ 计算出未知部分 W_i。

(3)对于另一消息 m_i^*，A_1 可以利用 S_i，R_i，$h_i^* = H_4(\mathrm{ID}_i \| m_i^* \| P_i)$，$k_i^* = H_5(\mathrm{ID}_i \| m_i^* \| P_i)$，$x_i$，$P_{\mathrm{pub}}$ 和 $U = H_2(P_{\mathrm{pub}})$ 伪造出对 m_i^* 的签名为：$\sigma_i^* = (S_i^*, R_i^*)$，其中 $S_i^* = W_i + x_i(h_i^*P_{\mathrm{pub}} + k_i^*U)$，$R_i^* = R_i$。

定理 2 A_1 通过上述方法伪造出的签名是合法有效的。

证明 我们只需证明最后产生的签名 $\sigma_i^* = (S_i^*, R_i^*)$ 能够通过验证即可。

由于

$$\begin{aligned} e(S_i^*, P) &= e(D_i + r_iT + hi^*x_iP_{\mathrm{pub}} + k_i^*x_iU, P) \\ &= e(O_i, P_{\mathrm{pub}})e(R_i, T)e(h_i^*P_{\mathrm{pub}} + k_i^*U, P_i) \\ &= e(Q_i + h_iP_i, P_{\mathrm{pub}})e(U, k_i^*P_i)e(R_i^*, T) \end{aligned} \tag{3}$$

验证等式成立，因此 A_1 通过上述方法伪造出的签名是合法有效的，通过这个过程，A_1 能够伪造多个用户对多个消息的合法有效的签名，从而 A_1 也可以伪造出合法有效的聚合签名。

4.3 攻击者 A_2 对于改进方案 1 的签名伪造过程

由于攻击者 A_2 不能进行公钥替换攻击，但可获得主密钥 s，同时 $D_i = sQ_i = sH_1(\mathrm{ID}_i)$，因此 A_2 可获得用户部分私钥 D_i，那么 A_2 的攻击过程如下所示：

(1) A_2 通过签名询问，输入用户身份 ID_i，得到用户对消息 m_i 的签名 $\sigma_i = (S_i, R_i)$，其中 $S_i = D_i + h_ix_i(P_{\mathrm{pub}} + U) + r_iT$，$R_i = r_iP$。

(2)令 $W_i = S_i - D_i = h_ix_i(P_{\mathrm{pub}} + U) + r_iT$，即用 W_i 代替 S_i 计算式中未知部分 $h_ix_i(P_{\mathrm{pub}} + U) + r_iT$，对 W_i 进行变形处理，令 $W_i^{'} = W_i/h_i = x_i(P_{\mathrm{pub}} + U) + r_iT/h_i$。

(3) 但对于另一消息 m_i^*，令 $W_i^* = h_i^*W_i^{'} = h_i^*x_i(P_{\mathrm{pub}} + U) + (h_i^*/h_i)\, r_iT$，$A_2$ 在伪造签名时需要知道 S_i，R_i，D_i，$h_i = H_4(\mathrm{ID}_i || m_i || P_i || R_i)$，$h_i^* = H_4(\mathrm{ID}_i || m_i^* || P_i || R_i^*)$，由于 $R_i^* = r_i^*P$，而 A_2 无法获得用户随机选择的 r_i^*，从而 A_2 无法计算出 $h_i^* = H_4(\mathrm{ID}_i || m_i^* || P_i || R_i^*)$，也就无法伪造出对 m_i^* 的签名。

定理 3　改进方案 1 面对第 2 类敌手 A_2 是安全的。

证明　通过上述分析可以看到，A_2 在伪造签名时必须重新构造新的 R_i^*，但是在 R_i^* 的构造中必定要出现 h_i^*，但是要计算 h_i^*，必须获得 R_i^* (不能是 R_i，否则无法通过验证)，因此 h_i^* 是 A_2 无法计算的，从而改进方案 1 面对第 2 类敌手 A_2 是安全的。

4.4 攻击者 A_2 对于改进方案 2 的签名伪造过程

同样由于攻击者 A_2 不能进行公钥替换攻击，但可获得主密钥 s，同时 $D_i = sQ_i = sH_1(\mathrm{ID}_i)$，因此 A_2 可获得用户部分私钥 D_i，那么 A_2 可以通过以下过程伪造出用户的合法有效的签名：

(1) A_2 通过签名询问，输入用户身份 ID_{i1}，得到用户对消息 m_{i1} 的签名 $\sigma_{i1} = (S_{i1}, R_{i1})$，其中 $S_{i1} = D_i + x_i(h_{i1}P_{\mathrm{pub}} + k_{i1}U) + r_{i1}T$，$R_{i1} = r_{i1}P$。

(2) A_2 通过签名询问，输入用户身份 ID_{i2}，得到用户对消息 m_{i2} 的签名 $\sigma_{i2} = (S_{i2}, R_{i2})$，其中 $S_{i2} = D_i + x_i(h_{i2}P_{\mathrm{pub}} + k_{i2}U) + r_{i2}T$，$R_{i2} = r_{i2}P$。

(3) 令 $W_{i1} = S_{i1} - D_i = x_i(h_{i1}P_{\mathrm{pub}} + k_{i1}U) + r_{i1}T$，$W_{i2} = S_{i2} - D_i = x_i(h_{i2}P_{\mathrm{pub}} + k_{i2}U) + r_{i2}T$，即分别用 W_{i1}，W_{i2} 代替 S_{i1}，S_{i2} 计算表达式中未知的部分 $x_i(h_{i1}P_{\mathrm{pub}} + k_{i1}U) + r_{i1}T$ 和 $x_i(h_{i2}P_{\mathrm{pub}} + k_{i2}U) + r_{i2}T$。

(4) 对于另一消息 m_i^*，可以计算出 $h_i^* = H_4(\mathrm{ID}_i||m_i^*||P_i)$，$k_i^* = H_5(\mathrm{ID}_i||m_i^*||P_i)$，可以利用参数 δ_1，δ_2 将 h_i^*，k_i^* 分别表示为 h_{i1}，h_{i2}，k_{i1}，k_{i2} 的线性组合，建立方程组：

$$\left.\begin{aligned}\delta_1 h_{i1} + \delta_2 h_{i2} &= h_i^* \\ \delta_1 k_{i1} + \delta_2 k_{i2} &= k_i^*\end{aligned}\right\} \tag{4}$$

对于上述二元一次方程组，由于 $h_{i1} = H_4(\mathrm{ID}_i||m_{i1}||P_i)$，$k_{i1} = H_5(\mathrm{ID}_i||m_{i1}||P_i)$，$h_{i2} = H_4(\mathrm{ID}_i||m_{i2}||P_i)$，$k_{i2} = H_5(\mathrm{ID}_i||m_{i2}||P_i)$ 都是 A_2 可以知道的，因此根据此方程组可以解出 δ_1，δ_2。

(5) 令 $W_i^* = \delta_1 W_{i1} + \delta_2 W_{i2} = x_i(\delta_1 h_{i1}P_{\mathrm{pub}} + \delta_1 k_{i1}U) + \delta_1 r_{i1}T + x_i(\delta_2 h_{i2}P_{\mathrm{pub}} + \delta_2 k_{i2}U) + \delta_2 r_{i2}T = x_i(h_i^* P_{\mathrm{pub}} + k_i^* U) + (\delta_1 r_{i1} + \delta_2 r_{i2})T$。这样 A_2 就可以利用 A_2 可以知道的 S_i，R_i，D_i，h_{i1}，h_{i2}，k_{i1}，k_{i2}，h_i^*，k_i^* 伪造出对 m_i^* 的签名为：$\sigma_i^* = (S_i^*, R_i^*)$，其中 $S_i^* = D_i + W_i^*$，$R_i^* = \delta_1 R_{i1} + \delta_2 R_{i2}$。

定理 4　A_2 通过上述方法伪造出的签名是合法有效的。

证明　我们只需证明最后产生的签名 $\sigma_i^* = (S_i^*, R_i^*)$ 能够通过验证即可。

由于

$$\begin{aligned} e(S_i^*, P) &= e(D_i + h_i^* x_i P_{\mathrm{pub}} + k_i^* x_i U \\ &\quad + (\delta_1 r_{i1} + \delta_2 r_{i2})T, P) \\ &= e(Q_i, P_{\mathrm{pub}}) e(\delta_1 R_{i1} + \delta_2 R_{i2}, T) \\ &\quad \cdot e(h_i^* P_{\mathrm{pub}} + k_i^* U, P_i) \\ &= e(Q_i + h_i^* P_i, P_{\mathrm{pub}}) e(U, k_i^* P_i) e(R_i^*, T) \end{aligned} \tag{5}$$

验证等式成立，因此 A_2 通过上述方法伪造出的签名是合法有效的，通过这个过程，A_2 能够伪造多个用户对多个消息的合法有效的签名，从而 A_2 也可以伪造出合法有效的聚合签名。

5　原因分析和改进建议

无证书安全模型中的不可伪造性一般分为两种，弱不可伪造性和强不可伪造性。其中弱不可伪造性指的是，对于未进行过签名询问的消息，攻击者无法根据进行过签名询问的其他消息签名对伪造出对其的合法签名；强不可伪造性指的是对于进行过签名询问的消息，攻击者无法伪造出新的合法签名。显然强不可伪造性在无证书安全模型中是更强的安全性要求。

从上述具体的攻击过程可以看出，第 2 类改进方案存在攻击，原因在于攻击者可以实现“弱签名询问”，即攻击者在进行签名询问时，必须要提供他替换的公钥的秘密值，因此两类方案无法满足弱不可伪造性。

我们可以根据改进方案 1 的思想，对改进方案 2 进行进一步改进，使其满足弱不可伪性。即将元素 R_i 嵌入 H_4，H_5 中，即使得 $h_i = H_4(\mathrm{ID}_i||m_i||P_i||R_i)$，$k_i = H_5(\mathrm{ID}_i||m_i||P_i||R_i)$。这样 A_1 在伪造签名时必须计算 h_i^*，k_i^* 的值，而要计算 h_i^*，k_i^*，必须获得 R_i^*，由于 A_1 无法获得 R_i^*，因此 h_i^*，k_i^* 是 A_1 无法计算的，从而改进方案 2 面对第 1 类敌手 A_1 是安全的；而 A_2 在伪造签名时必须重新构造新的 R_i^*，在 R_i^* 的构造中必定要出现 δ_1，δ_2，但是要计算 δ_1，δ_2，必须要知道 h_i^*，k_i^* 的值，而要计算 h_i^*，k_i^*，必须获得 R_i^*，因此 h_i^*，k_i^* 是 A_2 无法计算的，从而改进方案 2 面对第 2 类敌手 A_2 是安全的。

6　结论和效率分析

文献[15]基于双线性对提出了一种具体的无证书聚合签名方案，并在随机预言机模型中证明了其安全性，文献[16]对文献[15]的方案进行了深入分析，证明了此方案中的密钥生成中心 KGC 可以伪造出用户对任意消息的签名，同时为了避免这种情况提出了两种改进方案。我们对这两种改进后的方案进行了分析，通过给出具体的攻击过程，我们证明了

文献[16]的两种方案中，方案 1 面对两类攻击者的攻击时是安全的；方案 2 会被两类攻击者攻击，即两类攻击者可以在方案 2 中伪造出合法有效的签名。

在效率方面，我们将两种最终改进方案与其他同类方案进行了对比，结果如表 1 所示，其中定义 P 为双线性对运算，s 为 G_1 中的标量乘运算，$|G_1|$ 为群 G_1 中的元素长度，n 为签名者的数量，忽略其他耗时较少的普通加法乘法及哈希函数运算。

表 1 无证书聚合签名方案性能比较

方案	签名生成	聚合签名验证	聚合签名长度
文献[11]方案	$3s$	$(n+3)P$	$(n+1)\|G_1\|$
文献[13]方案	$3s$	$4P+2ns$	$(n+1)\|G_1\|$
本文改进方案 1	$4s$	$4P+2ns$	$(n+1)\|G_1\|$
本文改进方案 2	$4s$	$4P+2ns$	$2\|G_1\|$

从表 1 可以看出，在签名生成阶段本文改进方案需要 4 个标量乘运算，虽然比其他两种同类方案多出 1 个标量乘运算，但由于对运算的计算量高于标量乘运算，因此本文改进方案在聚合签名验证阶段运算量小于文献[11]中的方案，和文献[13]中的方案持平。在聚合签名长度方面，本文的改进方案 2 中的聚合签名长度仅为 2 个群 G_1 中的元素长度，而文献[13]中的方案和本文改进方案 1 中的聚合签名长度都与签名者的数量 n 正相关。因此综合考虑，本文的改进方案 2 不仅能满足安全性要求，也有更高的效率，更加适合应用于实际中。

参 考 文 献

[1] DIFFIE W and HELLMAN M E. New directions in cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644–654.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. Advances in Cryptology-CRYPTO'84, Berlin, Springer-Verlag, 1984: 47–53.

[3] 王 竹, 戴一齐, 顺顶锋. 普适安全的基于身份的签名机制. 电子学报, 2011, 39(7): 1613–1617.
WANG Zhu, DAI Yiqi, and YE Dingfeng. Universally composable identity-based signature[J]. *Acta Electronica Sinica*, 2011, 39(7): 1613–1617.

[4] DU Hongzhen and WEN Qiaoyan. An efficient identity-based short signature scheme from bilinear pairings[C]. IEEE Computer Society, Washington D.C., USA: 2007: 725–729.

[5] AL-RIYAMI S S and PATERSON K G. Certificateless public key cryptography[C]. Advances in Cryptology-ASIACRYPT'03, Berlin, Springer-Verlag, 2003: 452–473.

[6] ZHANG Lei, WU Qianhong, JOSEP D F, *et al*. Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security[J]. *Infomation Sciences*, 2014, 272(10): 223–237. doi: 10.1016/j.ins.2014.02.085.

[7] CHEN Hu, ZHU Changjie, and SONG Rushun. Efficient certificateless signature and group signature schemes[J]. *Journal of Computer Research and Development*, 2010, 47(2): 231–237.

[8] BONEN D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[C]. Advances in Cryptology-EUROCRYPT'03, Berlin, Springer-Verlag, 2003: 416–432. doi: 10.1007/3-540-39200-9_26.

[9] LYSYANSKAYA A, MICALI S, REYZIN L, *et al*. Sequential aggregate signatures from trapdoor permutations[C]. Advances in Cryptology-EUROCRYPT'04, Berlin, Springer-Verlag, 2004: 74–90. doi: 10.1007/978-3-540-24676-3_5.

[10] GONG Zheng, LONG Yu, HONG Xuan, *et al*. Two certificateless aggregate signatures from bilinear maps[C]. Proceedings of the IEEE SNPD'07, Qingdao, China: 2007, 3: 188–193. doi: 10.1109/SNPD.2007.132.

[11] ZHANG Lei and ZHANG Futai. A new certificateless aggregate signature scheme[J]. *Computer Communications*, 2009, 32(6): 1079–1085. doi: 10.1016/j.comcom.2008.12.042.

[12] YU Xiuying and HE Dake. New certificateless aggregate signature scheme[J]. *Application Research of Computers*, 2014, 31(8): 2485–2487.

[13] XIONG Hu, GUAN Zhi, CHEN Zhong, *et al*. An efficient certificateless aggregate signature with constant pairing computations[J]. *Information Sciences*, 2013, 219: 225–235. doi: 10.1016/j.ins.2012.07.004.

[14] HE Debiao, TIAN Miaomiao, and CHEN Jianhua. Insecurity of an efficient certificateless aggregate signature with constant pairing computations[J]. *Information Sciences*, 2014, 268: 458–462. doi: 10.1016/j.ins.2013.09.032.

[15] 明洋, 赵祥模, 王育民. 无证书聚合签名方案[J]. 电子科技大学学报, 2014, 43(2): 188–193. doi: 10.3969/j.issn.1001-0548.2014.02.005.
MING Yang, ZHAO Xiangmo, and WANG Yumin. Certificateless aggregate signature scheme[J]. *Journal of University of Electronic Science and Technology of China*, 2014, 43(2): 188–193. doi: 10.3969/j.issn.1001-0548.2014.02.005.

[16] 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 Yulei, LI Chenyi, WANG Caifen, *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.

罗 敏： 男，1974 年生，博士，副教授，研究方向为网络安全与数据挖掘.

孙 腾： 男，1989 年生，硕士，研究方向为密码学与网络安全.

张静茵： 女，1994 年生，硕士，研究方向为密码学与网络安全.

李 莉： 女，1976 年生，博士，副教授，研究方向为网络安全、协议分析和编译技术.