doi:10.11959/j.issn.1000-436x.2017220

新的无证书广义指定验证者聚合签名方案

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：无证书广义指定验证者聚合签名机制不仅能够解决证书管理和密钥托管问题，而且能够实现批验证和保护签名者的隐私。在资源受限的无线移动网络中有广泛应用。首先，对一种指定验证者聚合签名方案进行安全性分析，通过给出 2 种具体攻击方法，指出该方案不满足签名不可伪造性。为了增强安全性，提出一种新的无证书广义指定验证者聚合签名方案，并在随机预言机模型下证明该方案是安全的。与原方案相比，新方案在解决安全缺陷的同时大大降低了计算开销。

关键词：安全分析；指定验证者；无证书聚合签名；抗伪造攻击

中图分类号：TP309 **文献标识码**：A

New certificateless aggregate signature scheme with universal designated verifier

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

(1. School of Computer Science, Wuhan University, Wuhan 430072, China;
2. School of Computer Science, 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 with universal designated verifier had been widely applied in resource-constrained wireless mobile networks, because they could not only solve the problems of the certificate management and private key escrow, but also realize batch validation and the signer's privacy protection. A security analysis for a certificateless aggregate signature scheme with universal designated verifier was firstly provided, and two attack methods to demonstrate that their scheme was forgeable was presented. To enhance security, a new certificateless aggregate signature scheme with universal designated verifier was proposed, and then the security of the scheme in the random oracle model was proved. The performance of our proposed scheme was finally evaluated. Compared with the original scheme, the pvoposed scheme fixes the security flaws and the total computational cost is greatly reduced .

Key words: cryptanalysis, universal designated verifier, certificateless aggregate signature, resist forgery attack

1 引言

在许多实际应用场景中，接收者需要同时验证大量来自不同用户的签名。若分别验证单个签名来完成大量认证授权过程，则接收方将付出很大的计算代价。为了解决上述问题，Boneh 等[1]提出了聚合签名（AS）的概念：把 n 个签名者对 n 个消息的签名通过某种方式聚合起来，形成一个聚合签名。验证者只需验证该聚合签名即可判断聚合之前各签名的合法性。由于聚合签名能够缩减签名长度，

收稿日期：2017-01-09；**修回日期**：2017-04-10
通信作者：吴黎兵，whuwlb@126.com
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), The Science and Technology Program of Wuhan(No.2016060101010047)

实现批验证，降低验证开销，特别适用于解决资源受限的无线移动网络中批量认证问题[2,3]。

文献[4]提出了无证书公钥密码（CL-PKC）体制，该体制解决了证书管理和密钥托管问题。Gong 等[5]将 CL-PKC 与 AS 相结合，首次提出了无证书聚合签名（CLAS）的概念。随后，许多学者开始对 CLAS 进行大量理论研究和应用探讨。Zhang 等[6]对 CLAS 的概念及安全模型进行了重新定义，并提出了一种 CLAS 方案，但该方案不能抵抗恶意 KGC 的攻击。Xiong 等[7]提出了一种无证书聚合签名方案，但 He 等[8]指出该方案不满足不可伪造性。许艳等[9]指出文献[10]中的 CLAS 方案不能抵抗 2 种攻击类型中任何敌手的攻击，并给出了改进方案。

为保护签名者的隐私，Steinfeld 等[11]提出了一种广义指定验证者签名（UDVS）方案。UDVS 方案由签名持有者指定签名验证者，只有被指定的签名验证者才有权限验证签名的有效性。Ming 等[12]将 CL-PKC 体制与 UDVS 相结合，首次提出了无证书广义指定验证者签名的概念。随后，韩亚宁等[13]提出了一种演化的无证书 UDVS 方案，但该方案计算开销较大。

张玉磊等[14]提出一种无证书广义指定验证者聚合签名方案。本文对文献[14]方案进行了详细安全分析之后发现，该方案不能抵抗恶意 KGC 的攻击，签名是可伪造的。为了解决文献[14]方案存在的签名可伪造缺陷，本文提出一种新的无证书广义指定验证者聚合签名（CLASUDV）方案，并在随机预言机模型下证明了方案的安全性。安全比较及性能分析表明，本文方案在解决文献[14]方案的安全缺陷的同时大大降低了计算开销。

2　文献[14]方案及安全性分析

2.1　文献[14]方案

文献[14]方案由无证书聚合签名算法、指定验证者签名算法和指定验证者验证算法组成。

2.1.1　无证书聚合签名算法

q 为大素数，G_1、G_2 是 q 阶加法群和乘法群。P 和 Q 是 G_1 的生成元。$e: G_1 \times G_1 \to G_2$ 是双线性映射。$h_0: \{0,1\}^* \to Z_q^*$，$H_1: \{0,1\}^* \times G_1 \to G_1$，$H_2: \{0,1\}^* \to G_1$，$H_{DV}: \{0,1\}^* \to G_1$ 是方案中定义的 4 个散列函数。

Setup　由 KGC 执行，产生用户秘密值及其公钥，过程如下。

1) KGC 选择一个随机值 $s \in Z_q^*$，计算 $P_{\text{pub}} = sP$。

2) 秘密保存系统主密钥 s，并公布系统参数 $params = \{G_1, G_2, q, e, P, Q, P_{\text{pub}}, h_0, H_1, H_2, H_{DV}\}$。

User-Public-Key-Extract 由 KGC 执行，产生用户秘密值及其公钥，过程如下。

1) 用户 u_i 随机选取 $x_i \in Z_q^*$ 作为其秘密值。

2) 计算 $P_i = x_i P$ 作为其公钥。

User-Private-Key-Extract 由 KGC 和用户共同完成，产生用户完整私钥，过程如下。

1) KGC 计算 $Q_i = H_1(ID_i \| P_i)$ 和 $D_i = sQ_i$，并将 D_i 秘密发送给用户 u_i。

2) 用户 u_i 收到部分私钥 D_i，生成其完整私钥 $S_i = (D_i, x_i)$。

Part-Sign 由用户 u_i $(1 \leqslant i \leqslant n)$ 执行，产生对消息 m_i 的单个签名。过程如下。

1) 随机选取 $r_i \in Z_q^*$，计算 $R_i = r_i P$，$h_i = h_0(ID_i \| m_i \| P_i \| R_i)$ 和 $T = H_2(P_{\text{pub}})$。

2) 计算 $V_i = D_i + h_i r_i T + x_i Q$，令 $\sigma_i = (V_i, R_i)$。

3) u_i 对 m_i 的单个签名，并发送给聚合者。

Part-Verify 由验证者执行，用以验证 u_i 对 m_i 的单个签名的有效性，过程如下。

1)计算 $T = H_2(P_{\text{pub}})$，$Q_i = H_1(ID_i \| P_i)$ 和 $h_i = h_0(ID_i \| m_i \| P_i \| R_i)$。

2) 验证

$$e(V_i, P) = e(Q_i, P_{\text{pub}}) e(T, h_i R_i) e(Q, P_i) \tag{1}$$

若式(1)成立，则接受，否则，退出算法。

Aggregate-Sign 由聚合者执行，将一组单个签名聚合后形成一个聚合签名，过程如下。

1) 输入 u_i 对 m_i 的签名 $\sigma_i = (V_i, R_i)_{1 \leqslant i \leqslant n}$。

2) 对于 $1 \leqslant i \leqslant n$，计算 $h_i = h_0(ID_i \| m_i \| P_i \| R_i)$，然后分别计算 $V = \sum_{i=1}^{n} V_i$ 和 $R = \sum_{i=1}^{n} h_i R_i$。

3) 令 $\sigma = (V, R)$ 为对应聚合签名并输出。

Aggregate-Verify 由验证者执行，验证聚合签名的有效性，过程如下。

1) 给定系统参数 $params$，n 个消息的聚合签名 $\sigma = (V, R)$ 及 $(ID_i, m_i, P_i, \sigma_i)_{1 \leqslant i \leqslant n}$。

2) 计算 $T = H_2(P_{\text{pub}})$，对于 $1 \leqslant i \leqslant n$，分别计算 $Q_i = H_1(ID_i \| P_i)$，并验证

$$e(V,P)=e(\sum_{i=1}^{n}Q_i,P_{\text{pub}})e(T,R)e(Q,\sum_{i=1}^{n}P_i) \quad (2)$$

若式(2)成立，则接受，否则退出算法。

2.1.2 指定验证者签名算法

由签名聚合者（记为 u_A）执行，生成具有指定验证者的聚合签名，过程如下。

1) 给定 *params* 和聚合签名 $\sigma=(V,R)$。

2) 聚合者 u_A 分别计算 $h_{DV}=H_{DV}(x_A P_{DV})$，$\hat{S}=e(V,h_{DV}P_{DV})$ 和 $\hat{R}=h_{DV}R$。

输出指定验证者的聚合签名 $\hat{\sigma}=(\hat{S},\hat{R})$。

2.1.3 指定验证者验证算法

由指定验证者（记为 u_{DV}）执行，验证指定验证者聚合签名 $\hat{\sigma}=(\hat{S},\hat{R})$ 的有效性，过程如下。

1) 输入参数 *params*，$(ID_i,m_i,P_i)_{1\leqslant i\leqslant n}$ 和指定验证者聚合签名 $\hat{\sigma}=(\hat{S},\hat{R})$。

2) 分别计算 $T=H_2(P_{\text{pub}})$、$Q_i=H_1(ID_i\|P_i)$ 和 $h_{DV}=H_{DV}(x_{DV}P_A)$，并验证等式

$$\hat{S}=[e(\sum_{i=1}^{n}Q_i,h_{DV}\cdot P_{\text{pub}})e(T,\hat{R})e(Q,h_{DV}\sum_{i=1}^{n}P_i))]^{x_{DV}} \quad (3)$$

若式(3)成立，则接受，否则，退出算法。

2.2 安全分析

给出 2 种具体攻击方法，展示文献[14]方案中单个签名和聚合签名均是可伪造的，该方案是不安全的。这里主要考虑 CLAS 方案安全模型中恶意 KGC 的攻击，即 $A=A_2$，且满足以下 2 个条件。

1) u_i^* 未提交过秘密值询问。

2) (u_i^*,m_i^*) 未提交过签名询问。

具体攻击过程如下。

2.2.1 单个签名攻击

1) 系统参数设置

攻击者 A 在系统初始化时，首先，选择 G_1 的一个生成元 P，随机数 $\varpi\in Z_q^*$，然后，计算 $Q=\varpi P$ 作为 G_1 的另一个生成元。选择 $s\in Z_q^*$ 作为主私钥，计算 $P_{\text{pub}}=sP$ 作为系统主公钥。发布系统参数 *params*。此时，A 可获取 *params* 和 s。

2) 询问

攻击者 A 随机选取 $r_j'\in Z_q^*$，计算 $R_j'=r_j'P$，通过 h_0 和 H_2 预言机询问分别获取 $T=H_2(P_{\text{pub}})$ 和 $h_j'=h_0(ID_i\|m_j\|P_i\|R_j')$ 的散列值。

3) 伪造签名

由于攻击者 A 为恶意 KGC，故其可获取用户 u_i 的部分私钥 D_i；又因 $Q=\varpi P$，故可求出 $x_iQ=x_i\varpi P=\varpi P_i$。

攻击者 A 依照签名方案伪造用户 u_i 对消 $m_j(j\in[1,n])$ 的签名 σ_j' 为

$$\sigma_j'=\begin{cases}R_j'=r_j'P\\ V_j=D_i+h_j'r_j'T+\varpi P_i\end{cases} \quad (4)$$

4) 验证签名

验证者计算 $T=H_2(P_{\text{pub}})$，$Q_i=H_1(ID_i\|P_i)$ 和 $h_j'=h_0(ID_i\|m_j\|P_i\|R_j')$，把 V_j' 代入式(1)有

$$\begin{aligned}e(V_j',P)&=e(D_i+h_j'r_j'T+\varpi P_i,P)\\&=e(D_i,P)e(h_j'r_j'T,P)e(\varpi P_i,P)\\&=e(Q_i,P_{\text{pub}})e(T,h_j'R_j')e(P_i,Q)\end{aligned} \quad (5)$$

由以上推导可知，伪造的单个签名 σ_j' 是有效的。

2.2.2 聚合签名攻击

1) 系统参数设置

同 2.2.1 节系统参数设置。

2) 询问

攻击者 A 通过 H_2 预言机询问，可获取 $T=H_2(P_{\text{pub}})$ 的散列值。

3) 伪造聚合签名

为了伪造 u_i 对 m_i 的聚合签名 $\sigma=(V,R)$，其中，$1\leqslant i\leqslant n$，攻击者进行以下操作。

同 2.2.1 节步骤 3)伪造签名的步骤。

A 选取随机值 $\gamma\in Z_q^*$，伪造 u_i 对 m_i 的聚合签名 $\sigma'=(V',R')$，其中，$1\leqslant i\leqslant n$，如式(6)所示。

$$\sigma'=\begin{cases}R'=\gamma Q\\ V'=\sum_{i=1}^{n}(D_i+x_iQ)+\gamma T\end{cases} \quad (6)$$

4) 验证签名

验证者首先计算 $Q_i=H_1(ID_i\|P_i)_{1\leqslant i\leqslant n}$ 和 $T=H_2(P_{\text{pub}})$，然后，把 V' 代入式(2)，有

$$\begin{aligned}e(V',P)&=e(\sum_{i=1}^{n}(D_i+x_iQ)+\gamma T,P)\\&=e(\sum_{i=1}^{n}sQ_i,P)e(\sum_{i=1}^{n}x_iP,Q)e(\sum_{i=1}^{n}(\gamma P,T)\\&=e(\sum_{i=1}^{n}Q_i,P_{\text{pub}})e(T,R')e(Q,\sum_{i=1}^{n}P_i)\end{aligned} \quad (7)$$

由以上推导可知伪造的聚合签名 σ' 是有效的。

综上，敌手 A 分别成功伪造了单个签名和聚合签名，因此文献[14]方案是不安全的。

3　新的无证书指定验证者聚合签名方案

为了解决文献[14]方案中的安全缺陷并提高方案的效率，本文提出一种新的 CLASUDV 方案。新方案由无证书聚合签名、指定验证者签名和指定验证者验证 3 个算法组成。

3.1　无证书聚合签名算法

各参数的设置同 2.1.1 节文献[14]方案。

3.1.1　Setup 阶段

同 Zhang-Zhou 方案[14]中 Setup。

3.1.2　User-Public-Key-Extract 阶段

由用户 u_i 执行产生用户公钥，过程如下。

1) 输入系统参数 $params$。

2) 用户 u_i 随机选择 $x_i \in Z_q^*$ 作为秘密值保存。

3) 计算 $P_i = x_i P$ 和 $Q_i = H_1(ID_i \| P_i)$。

4) 令 $pk_i = (P_i, Q_i)$ 为其公钥。

3.1.3　User-Private-Key-Extract 阶段

由 KGC 和用户 u_i 执行产生其私钥，过程如下。

1) 输入系统参数 $params$，秘密值 x_i。

2) 计算 $D_i = sQ_i$。

3) 令 $sk_i = (D_i, x_i)$ 为用户 u_i 的私钥。

3.1.4　Part-Sign 阶段

由用户 u_i 执行产生其对消息 m_i 的单个签名，过程如下。

1) 随机选取 $w_i \in Z_q^*$，计算 $W_i = w_i P$，$\alpha_i = h_0(ID_i \| m_i \| P_i \| W_i)$ 和 $T = H_2(P_{\text{pub}})$；

2) 计算 $V_i = D_i + (\alpha_i w_i + x_i)T$，令 $\sigma_i = (V_i, W_i)$ 为用户 u_i 对消息 m_i 的单个签名，并发送给聚合者。

3.1.5　Part-Verify 阶段

由验证者执行验证 u_i 对消息 m_i 签名的有效性，过程如下。

1) 计算 $T = H_2(P_{\text{pub}})$，$\alpha_i = h_1(ID_i \| m_i \| P_i \| W_i)$

2) 验证

$$e(V_i, P) = e(P_{\text{pub}}, Q_i)e(\alpha_i W_i + P_i, T) \tag{8}$$

若式(8)成立，则接受，否则退出算法。

3.1.6　Aggregate-Sign 阶段

由聚合者执行产生 n 个用户对 n 个消息的聚合签名，过程如下。

1) 输入 u_i 对消息 m_i 的签名 $\sigma_i = (V_i, W_i)_{1 \leqslant i \leqslant n}$。

2) 聚合者计算

$$W = \{W_1, W_2, \cdots, W_n\} \tag{9}$$

$$V = \sum_{i=1}^{n} V_i \tag{10}$$

3) 聚合者输出 u_i 对消息 m_i 的聚合签名 $\sigma = (V, W)$，其中，$1 \leqslant i \leqslant n$。

3.1.7　Aggregate-Verify 阶段

由验证者执行验证聚合签名的有效性，过程如下。

1) 给定参数 $params$、$(ID_i, m_i, P_i, \sigma_i)_{1 \leqslant i \leqslant n}$ 及 n 个消息的聚合签名 $\sigma = (V, W)$。

2) 对于 $1 \leqslant i \leqslant n$，验证者计算：$T = H_2(P_{\text{pub}})$，$Q_i = H_1(ID_i \| P_i)$ 和 $\alpha_i = h_0(ID_i \| m_i \| P_i \| W_i)$，并验证

$$e(V, P) = e(\sum_{i=1}^{n} Q_i, P_{\text{pub}})e(\sum_{i=1}^{n}(\alpha_i W_i + P_i), T) \tag{11}$$

若式(11)成立，则接受，否则，退出算法。

3.2　指定验证者签名算法

由签名聚合者（记为 u_{Agg}）执行，生成具有指定验证者的聚合签名，过程如下。

1) 输入参数 $params$ 和签名 $\sigma = (V, W)$。

2) 分别计算 $\eta_{DV} = H_{DV}(x_{\text{Agg}} \cdot P_{DV})$、$\bar{V} = e(V, \eta_{DV} \cdot P_{DV})$ 和 $\bar{W} = \eta_{DV} \sum_{i=1}^{n} W_i$。

3) 输出指定验证者聚合签名 $\bar{\sigma} = (\bar{V}, \bar{W})$。

3.3　指定验证者验证算法

由指定验证者（记为 u_{DV}）执行，验证指定验证者的聚合签名 $\bar{\sigma} = (\bar{V}, \bar{W})$ 的有效性，过程如下。

1) 输入 $params$，$(ID_i, m_i, P_i)_{1 \leqslant i \leqslant n}$ 和指定验证者的聚合签名 $\bar{\sigma} = (\bar{V}, \bar{W})$。

2) 计算 $\eta_{DV} = H_{DV}(x_{DV} P_{\text{Agg}})$，$\alpha_i = h_1(ID_i \| m_i \| P_i \| W_i)_{1 \leqslant i \leqslant n}$ 和 $T = H_2(P_{\text{pub}})$，并验证

$$\bar{V} = [e(\sum_{i=1}^{n} Q_i, \eta_{DV} P_{\text{pub}})e((\sum_{i=1}^{n} \alpha_i)\bar{W} + \eta_{DV} \sum_{i=1}^{n} P_i), T)]^{x_{DV}} \tag{12}$$

若式(12)成立，则接受，否则退出算法。

4　安全性分析

CLASUDV 方案应满足正确性、不可伪造性、强指定验证性和不可传递性。

4.1　方案正确性

定理 1　本文方案是正确的，当且仅当方案中

涉及的无证书单个签名σ_i、聚合签名σ及具有指定验证者的聚合签名$\bar{\sigma}$是由本文方案中相应算法得到且满足对应验证等式。

证明 假设$\sigma_i=(V_i,W_i)$是由本文单个签名算法产生的u_i对消息m_i签名，代入式(8)，有

$$\begin{aligned}e(V_i,P)&=e(D_i+(\alpha_i w_i+x_i)T,P)\\&=e(Q_i,sP)e((\alpha_i w_i+x_i)P,T)\\&=e(P_{\text{pub}},Q_i)e(\alpha_i W_i+P_i,T)\end{aligned}\tag{13}$$

2) 假设$\sigma=(V,W)$是由本文提出的CLAS算法产生的u_i对消息m_i的聚合签名，其中，$1\leqslant i\leqslant n$，代入式(11)，有

$$\begin{aligned}e(V,P)&=e(\sum_{i=1}^{n}(D_i+(\alpha_i w_i+x_i)T,P)\\&=e(\sum_{i=1}^{n}Q_i,sP)e(\sum_{i=1}^{n}(\alpha_i w_i+x_i)P,T)\\&=e(\sum_{i=1}^{n}Q_i,P_{\text{pub}})e(\sum_{i=1}^{n}(\alpha_i W_i+P_i),T)\end{aligned}\tag{14}$$

假设$\bar{\sigma}=(\bar{V},\bar{W})$是由本文方案产生的指定验证者签名，代入式(12)，有

$$\begin{aligned}\bar{V}&=e(\sum_{i=1}^{n}V_i,\eta_{DV}P_{DV})\\&=e(\sum_{i=1}^{n}(D_i+(\alpha_i w_i+x_i)T),\eta_{DV}x_{DV}P)\\&=[e(\sum_{i=1}^{n}Q_i,\eta_{DV}P_{\text{pub}})e((\sum_{i=1}^{n}\alpha_i)\bar{W}+\eta_{DV}\sum_{i=1}^{n}P_i,T)]^{x_{DV}}\end{aligned}\tag{15}$$

4.2 不可伪造性

包括无证书聚合签名的不可伪造性和指定验证者聚合签名的不可伪造性。安全模型同文献[14]方案。

4.2.1 无证书聚合签名的不可伪造性

将本文方案中CLAS的安全性归约为CDH困难问题。在随机预言模型下证明方案的安全性。

定理2 如果群G_1上的CDH问题是困难的，则本文提出的CLAS方案就能够抵抗A_{I}类敌手的攻击，满足不可伪造性。

证明 假设A_{I}类敌手在随机预言机模型下能以不可忽略概率赢得安全模型中的游戏1，则挑战者C就能以不可忽略的概率解决CDH问题。

初始化 给定CDH问题的一个实例$(P,Q_1=a.P,Q_2=b.P)$，C令$P_{\text{pub}}=Q_1=a.P$，返回系统参数$params$给A_{I}。随机选择ID_{gt}为被挑战者身份。C维护表h_0^{list}，H_1^{list}，H_2^{list}，D^{list}，x^{list}，pk^{list}分别对应h_0、H_1、H_2这3个散列询问，部分私钥，秘密值，公钥询问，各表均初始化为空。

***h_0* 询问** 当A_{I}输入(ID_i,m_i,P_i,W_i)时，C查找h_0^{list}，若存在$(ID_i,m_i,P_i,W_i,\alpha_i)$项，则$C$直接返回$\alpha_i$，否则随机选取$\alpha_i\in Z_q^*$发给$A_{\text{I}}$，并存储$(ID_i,m_i,P_i,W_i,\alpha_i)$项到列表$h_1^{\text{list}}$。

***H_1* 询问** 当A_{I}输入(ID_i,P_i)时，C查找H_1^{list}，若存在$(ID_i,P_i,\vartheta_i,Q_i,\omega_i)$项，则返回$Q_i$；否则$C$随机选取$\vartheta_i\in Z_q^*$和$\omega_i\in\{0,1\}$（其中，$\omega_i=0$的概率为$\zeta=\dfrac{1}{q_{H_1}}$，$\omega_i=1$的概率为$1-\zeta$）。当$\omega_i=0$时，令$Q_i=\vartheta_i P$；当$\omega_i=1$时，令$Q_i=\vartheta_i bP$。返回$Q_i$给$A_{\text{I}}$，并存储$(ID_i,P_i,\vartheta_i,Q_i,\omega_i)$项到列表$H_1^{\text{list}}$。

***H_2* 询问** 当A_{I}输入P_{pub}时，C查找H_2^{list}，若存在$(P_{\text{pub}},\upsilon,T)$项，则$C$返回$T$，否则随机选取$\upsilon\in Z_q^*$，令$T=\upsilon P$并返回给$A_{\text{I}}$，存储$(P_{\text{pub}},\upsilon,T)$项到列表$H_2^{\text{list}}$。

部分私钥询问 当A_{I}询问用户u_i的部分私钥时，C判断ID_i与ID_{gt}是否相等，若相等，则停止模拟输出⊥；否则，C查找D^{list}，若存在(ID_i,D_i)项，返回D_i；若不存在，则C查找H_1^{list}列表，当$\omega_i=1$时退出；当$\omega_i=0$时，计算$D_i=\vartheta_i P_{\text{pub}}=\vartheta_i aP$，$C$存储$(ID_i,D_i)$项到列表$D^{\text{list}}$，并返回$D_i$给$A_{\text{I}}$。

秘密值询问 当A_{I}询问用户u_i的秘密值时，C判断ID_i与ID_{gt}是否相等，若相等，则停止模拟并输出⊥；否则，C查找x^{list}，若存在(ID_i,x_i)项，返回x_i；若不存在，则产生一个随机数$x_i\in Z_q^*$，存储(ID_i,x_i)项到列表x^{list}，并返回x_i给A_{I}。

公钥询问 当A_{I}询问用户u_i公钥时，C查找pk^{list}，若存在(ID_i,pk_i)项，直接返回pk_i，否则，C查找x^{list}获取x_i，计算$P_i=x_i P$，令$pk_i=(P_i,Q_i)$，存储(ID_i,pk_i)项到列表pk^{list}，并返回pk_i给A_{I}。

公钥替换询问 当收到将ID_i公钥替换为pk_i'的消息时，C将(ID_i,pk_i)项替换为(ID_i,pk_i')。

签名询问 当A_{I}询问u_i对m_i签名时，C查找H_1^{list}，若$\omega_i=0$，查找h_0^{list}和H_2^{list}获取α_i和T，C随机选取$W_i\in G_1^*$，并计算$V_i=\vartheta_i P_{\text{pub}}+\alpha_i\upsilon W_i+\upsilon P_i$。$C$返回签名$\sigma_i=(V_i,W_i)$给$A_{\text{I}}$。

伪造　最后，A_{I} 输出与 $(m_i^*, ID_i^*, pk_i^*)_{1\leqslant i\leqslant n}$ 相对应的签名 $\sigma_i^* = (V_i^*, W_i^*)$。若所有 $\omega_i^* = 0$，则退出；否则，只要存在任意 $\omega_i^* = 1$，即可伪造聚合签名。不失一般性，设 $i=1$，C 按照 $\omega_1^* = 1$，$\omega_i^* = 0$（$2\leqslant i\leqslant n$）执行签名过程，进而得到的伪造聚合签名 $\sigma^* = (V^*, W^*)$ 满足验证等式

$$e(V^*, P) = e(\sum_{i=1}^{n} Q_i^*, P_{\mathrm{pub}})e(\sum_{i=1}^{n}\alpha_i W_i^* + P_i^*, T) \quad (16)$$

其中，$Q_i^* = \vartheta_i^* P$ ($2\leqslant i\leqslant n$)；$Q_1^* = \vartheta_1^* bP$，$T = \upsilon P$，$V^* = \sum_{i=1}^{n} V_i^*$，$W^* = \{W_1^*, W_2^*, \cdots, W_n^*\}$，则有

$$\begin{aligned}
&e(V^*, P)\\
&= e(\sum_{i=2}^{n} Q_i^*, P_{\mathrm{pub}})e(\sum_{i=1}^{n}\alpha_i W_i^* + P_i^*, T)e(Q_1^*, P_{\mathrm{pub}})\\
&\Rightarrow e(Q_1^*, P_{\mathrm{pub}})\\
&= e(V^*, P)[e(\sum_{i=2}^{n} Q_i^*, P_{\mathrm{pub}})e(\sum_{i=1}^{n}\alpha_i W_i^* + P_i^*, T)]^{-1}\\
&\Rightarrow abP = \vartheta_1^{*-1}(V^* - \sum_{i=2}^{n}\vartheta_i^* P_{\mathrm{pub}} - \upsilon\sum_{i=1}^{n}(\alpha_i W_i^* + P_i^*))
\end{aligned}$$

由以上推导结果可知，C 解决了 CDH 问题，这与 CDH 困难假设相矛盾。

定理 3　如果群 G_1 上的 CDH 问题是困难的，则本文提出的聚合签名方案就能够抵抗 A_{II} 类敌手的攻击，满足不可伪造性。

证明　若 A_{II} 类敌手在随机预言机模型下能以不可忽略的概率赢得安全模型中的游戏 2，则挑战者 C 就能以不可忽略的概率解决 CDH 问题。

初始化　给定CDH问题的一个实例 $(P, Q_1 = a.P, Q_2 = b.P)$，$C$ 令 $P_{\mathrm{pub}} = \gamma P$，返回参数 *params* 和主私钥 γ 给 A_2。随机选 ID_{gt} 为被挑战者身份。C 维护表 h_0^{list}、H_1^{list}、H_2^{list}、x^{list}、pk^{list} 分别对应 h_0、H_1、H_2 这 3 个散列询问、秘密值询问、公钥询问，各表均初始化为空。

h_0 和 H_1 询问，秘密值询问同定理 2。

***H_2* 询问**　当 A_{II} 输入 P_{pub} 时，C 查找 H_2^{list}，若存在 $(P_{\mathrm{pub}}, \upsilon, T)$ 项，则 C 返回 T，否则，随机选取 $\upsilon\in Z_q^*$，令 $T = \upsilon aP$ 并返回给 A_{II}，存储 $(P_{\mathrm{pub}}, \upsilon, T)$ 到列表 H_2^{list}。

公钥询问　当 A_{II} 询问用户 u_i 公钥时，C 查找 pk^{list}，若存在 (ID_i, pk_i) 项，直接返回 pk_i。否则，当 $\omega_i = 0$ 时，C 查找 x^{list} 获取 x_i，计算 $P_i = x_i P$；当 $\omega_i = 1$ 时，则 C 随机选取 $x_i\in Z_q^*$，计算 $P_i = x_i bP$（$\omega_i = 0$ 的概率为 $\zeta = \dfrac{1}{q_{pk}}$，$\omega_i = 1$ 的概率为 $1-\zeta$）。令 $pk_i = (P_i, Q_i)$，存储 $(ID_i, x_i, pk_i, \omega_i)$ 项到表 pk^{list}，并返回 pk_i 给 A_{II}。

签名询问　当 A_{II} 询问 u_i 对 m_i 签名时，C 查找 h_0^{list}、pk^{list} 和 H_2^{list} 获取 α_i 和 T。若 $\omega_i = 0$，C 随机选 $W_i = w_i P\in G_1^*$，计算 $V_i = \gamma Q_i + \alpha_i \upsilon W_i + \upsilon x_i aP$。$C$ 返回签名 $\sigma_i = (V_i, W_i)$ 给 A_{II}。

伪造　最后 A_{II} 输出与 $(m_i^*, ID_i^*, pk_i^*)_{1\leqslant i\leqslant n}$ 相对应的签名 $\sigma_i^* = (V_i^*, W_i^*)$。若所有的 $\omega_i^* = 0$，则退出；否则，只要存在任意一个 $\omega_i^* = 1$，即可伪造聚合签名。不失一般性，假设 $i=1$，C 按照 $\omega_1^* = 1$，$\omega_i^* = 0$（$2\leqslant i\leqslant n$）执行签名过程，进而得到的伪造的聚合签名 $\sigma^* = (V^*, W^*)$ 满足验证等式

$$e(V^*, P) = e(\sum_{i=1}^{n} Q_i^*, P_{\mathrm{pub}})e(\sum_{i=1}^{n}(\alpha_i W_i^* + P_i^*), T) \quad (17)$$

其中，$Q_i^* = H_1(ID_i^* \| P_i^*)$，$P_1^* = x_1^* bP$，$P_i^* = x_i^* P$ ($2\leqslant i\leqslant n$)，$W^* = \{w_1^* P, w_2^* P, \cdots, w_n^* P\}$，$V^* = \sum_{i=1}^{n} V_i^*$，则有

$$\begin{aligned}
&e(V^*, P)\\
&= e(\sum_{i=1}^{n} Q_i^*, P_{\mathrm{pub}})e(\sum_{i=1}^{n}\alpha_i W_i^* + \sum_{i=2}^{n} P_i^*, T)e(P_1^*, T)\\
&\Rightarrow e(P_1^*, T)\\
&= e(V^*, P)[e(\sum_{i=1}^{n} Q_i^*, P_{\mathrm{pub}})e(\sum_{i=1}^{n}\alpha_i W_i^* + \sum_{i=2}^{n} P_i^*, T)]^{-1}\\
&\Rightarrow abP = (\upsilon x_1^*)^{-1}[V^* - \gamma\sum_{i=1}^{n} Q_i^* - (\sum_{i=1}^{n}\alpha_i w_i^* + \sum_{i=2}^{n} x_i^*)T] \quad (18)
\end{aligned}$$

由以上推导结果可知，C 解决了 CDH 问题，这与 CDH 困难假设相矛盾。

4.2.2　指定验证者聚合签名的不可伪造性

定理 4　若 A_{III} 类敌手在随机预言机模型下能以不可忽略的概率赢得安全模型中的游戏 3，则本文方案在指定验证者身份下和适应性选择消息下满足不可伪造性。

证明　假设攻击者 A_{III} 对消息 $m_i^*(1\leqslant i\leqslant n)$ 伪造的具有指定验证者 u_{DV}^* 的聚合签名为 $\overline{\sigma}^* = (\overline{V}^*, \overline{W}^*)$，且该签名对验证算法是有效的。根据算法可

知，A_{III} 只有通过以下 2 种途径来伪造：获取指定验证者 u_{DV} 的私钥和获取对 $M^*=\{m_i^*\}_{1\leqslant i\leqslant n}$ 伪造的聚合签名。

现对这 2 种途径进行分析。

途径 1 Hash 函数 H_{DV} 的输入只可能是 $x_{\mathrm{Agg}}P_{DV}$ 或 $x_{DV}P_{\mathrm{Agg}}$，令 $\psi=x_{\mathrm{Agg}}P_{DV}=x_{DV}P_{\mathrm{Agg}}$，则已知 ψ 求出 x_{DV} 的困难性相当于解决 ECDLP 问题；又因安全散列满足单向性，即已知 $H_{DV}(\psi)$ 值无法求出 ψ。因此途径 1 不可行。

途径 2 A_{III} 只能通过扮演 A_{I} 或 A_{II} 的角色才有可能获取对消息 $m_i^*(1\leqslant i\leqslant n)$ 伪造的聚合签名，但由定理 2 和定理 3 可知本文方案能够抵抗 A_{I} 或 A_{II} 类敌手的攻击。因此途径 2 也不可行。

4.3 强指定验证性

由式(12)知，只有使用指定验证者的私钥才能验证指定验证者签名 $\bar{\sigma}=(\bar{V},\bar{W})$ 的合法性，而只有 u_{DV} 拥有该私钥 x_{DV}，即只有 u_{DV} 能够验证 $\bar{\sigma}$ 的合法性，因此，方案满足强指定验证性。

4.4 不可传递性

定理 5 指定验证者 u_{DV} 可以通过一定的方法产生一个能满足验证式的签名 σ_{DV}^*，且与按照方案生成的签名 σ_{DV} 不可区分，即满足不可传递性。

证明 u_{DV} 选择 $W_i'\in G_1$，计算 $T=H_2(P_{\mathrm{pub}})$，$\bar{W}'=\eta_{DV}\sum_{i=1}^{n}W_i'$ 和 $\eta_{DV}=H_{DV}(x_{\mathrm{Agg}}P_{DV})$。用上述方式可产生消息 $m_i(1\leqslant i\leqslant n)$ 的一个指定验证者签名的副本 $\bar{\sigma}'=(\bar{V}',\bar{W}')$，且满足验证等式

$$\bar{V}'=[e(\sum_{i=1}^{n}Q_i,\eta_{DV}P_{pub})e((\sum_{i=1}^{n}\alpha_i)\bar{W}'+\eta_{DV}\sum_{i=1}^{n}P_i),T)]^{x_{DV}}$$

因此，由 u_{DV} 产生的签名 $\bar{\sigma}$ 与 $\bar{\sigma}'$ 不可区分，即方案满足不可传递性。

5 安全比较和性能分析

5.1 安全性比较

对本文方案和其他几种聚合签名方案的安全性进行比较分析。其中，A_{I}、A_{II} 分别表示第一、二类攻击者；根据敌手能力不同在，A_{II} 中又分出 3 个等级[15]。其中，B_1、B_2 和 B_3 分别表示一般，较强和超级敌手；◎表示能满足相应属性要求；©表示不能满足相应属性要求；L 表示在安全性较低；H 表示安全性较高。

如表 1 所示，文献[7]方案与文献[14]方案均不能抵抗 A_2 种敌手的攻击，安性较低；文献[9]方案在 A_1 和 A_2 这 2 种敌手的攻击下均可伪造，安全性低；只有本文方案可以抵抗 2 种类型的超级敌手的攻击，安全性较高。

表 1 相关方案安全性对比

方案	A_1				A_2			
	B_1	B_2	B_3	安全性	B_1	B_2	B_3	安全性
文献[7]方案	©	©	◎	H	©	©	©	L
文献[9]方案	©	©	©	L	©	©	©	L
文献[14]方案	©	©	◎	H	©	©	©	L
本文方案	©	©	◎	H	©	©	◎	H

5.2 性能分析

在保证整个方案安全性的同时还要考虑方案的计算开销等效率问题。本文分为系统初始化、用户公钥生成、用户私钥生成、单个签名生成、单个签名验证、聚合签名生成、聚合签名验证、指定签名生成及指定签名验证 9 个阶段，对本文方案和文献[14]方案的计算开销进行比较分析，如表 2 所示。

表 2 计算开销对比

步骤	文献[14]方案开销	本文方案开销
系统初始化	$P_{\mathrm{ecc-pm}}$	$P_{\mathrm{ecc-pm}}$
用户公钥生成	$P_{\mathrm{ecc-pm}}$	$P_{\mathrm{ecc-pm}}+T_{\mathrm{mtp}}$
A_{I} 用户私钥生成	$P_{\mathrm{ecc-pm}}+T_{\mathrm{mtp}}$	$P_{\mathrm{ecc-pm}}$
单个签名生成	$T_{\mathrm{mts}}+T_{\mathrm{mtp}}+2T_{\mathrm{ecc-pa}}+T_{\mathrm{ecc-pm}}+T_{\mathrm{ecc-2pm}}$	$T_{\mathrm{mts}}+T_{\mathrm{mtp}}+T_{\mathrm{ecc-pa}}+2T_{\mathrm{ecc-pm}}$
单个签名验证	$T_{\mathrm{mts}}+2T_{\mathrm{mtp}}+T_{\mathrm{ecc-pm}}+4T_{\mathrm{bp}}$	$T_{\mathrm{mts}}+T_{\mathrm{mtp}}+T_{\mathrm{ecc-pa}}+T_{\mathrm{ecc-pm}}+3T_{\mathrm{bp}}$
聚合签名生成	$nT_{\mathrm{mts}}+nT_{\mathrm{ecc-pm}}+2(n-1)T_{\mathrm{ecc-pa}}$	$(n-1)T_{\mathrm{ecc-pa}}$
聚合签名验证	$2nT_{\mathrm{mtp}}+2(n-1)T_{\mathrm{ecc-pa}}+4T_{\mathrm{bp}}$	$nT_{\mathrm{mts}}+(n+1)T_{\mathrm{mtp}}+3T_{\mathrm{bp}}+(3n-2)T_{\mathrm{ecc-pa}}+nT_{\mathrm{ecc-pm}}$
指定签名生成	$T_{\mathrm{mtp}}+3T_{\mathrm{ecc-pm}}+T_{\mathrm{bp}}$	$T_{\mathrm{mtp}}+(n-1)T_{\mathrm{ecc-pa}}+3T_{\mathrm{ecc-pm}}+T_{\mathrm{bp}}$
指定签名验证	$(n+2)T_{\mathrm{mtp}}+2(n-1)T_{\mathrm{ecc-pa}}+3T_{\mathrm{ecc-pm}}+3T_{\mathrm{bp}}+T_{\mathrm{ecc-exp}}$	$nT_{\mathrm{mtp}}+(2n-1)T_{\mathrm{ecc-pa}}+4T_{\mathrm{bp}}+2T_{\mathrm{ecc-pm}}+2T_{\mathrm{mtp}}+T_{\mathrm{ecc-exp}}$

容易发现，在保证安全性的同时本文方案具有更高的计算效率。其中，T_{mts} 表示普通散列运算；T_{mtp} 表示散列到点运算；$T_{\mathrm{ecc-exp}}$ 表示椭圆曲线上的指数运算；$P_{\mathrm{ecc-pa}}$ 表示椭圆曲线上的点加运算；$P_{\mathrm{ecc-pm}}$ 表示椭圆曲线上的点乘运算；$P_{\mathrm{ecc-2pm}}$ 表示椭圆曲线上的并行执行的 2 个点乘运算；T_{bp} 表示双线性对运算。

6　结束语

广义指定验证者无证书聚合签名在解决证书管理和密钥托管问题的同时保护了签名者的隐私。并且通过缩减签名长度实现了批验证，能有效降低验证开销。本文首先分析了文献[14]的安全性，指出该方案中的签名是可伪造的，并提出了新的方案，在随机预言机模型下证明了新方案的安全性。与文献[14]方案相比，所提方案在解决了原方案的签名可伪造安全缺陷的同时大大降低了计算开销，提高了整个方案的性能，更适合解决资源受限的无线网络中批量认证问题。

参考文献：

[1] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[J]. Lecture Notes in Computer Science, 2003, 2656(1):416-432.

[2] 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.

[3] 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.

[4] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[M]// Advances in Cryptology - ASIACRYPT 2003. Springer Berlin Heidelberg, 2003:452-473.

[5] GONG Z, LONG Y, HONG X, et al. Two Certificateless aggregate signatures from bilinear maps[C]//Eighth Acis International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/distributed Computing. IEEE Computer Society, 2007(3): 188-193.

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

[7] XIONG H, GUAN Z, CHEN Z, et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2013, 219(10): 225-235.

[8] HE D, TIAN M, CHEN J. Insecurity of an efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2014(1), 268: 458-462.

[9] 许艳, 黄刘生, 田苗苗, 等. 一种可证安全的紧致无证书聚合签名方案[J]. 电子学报, 2016, 44(8): 1845-1850.
XU Y, HUANG L S,TIAN M M. A provably secure and compact certificateless aggregate signature scheme[J]. Acta Electronica Sinica,2016, 44(8): 1845-1850.

[10] 杜红珍，黄梅娟，温巧燕．高效的可证明安全的无证书聚合签名方案[J]. 电子学报, 2013, 41(1): 72-76.
DU H Z, HUANG M J,WEN Q Y. Efficient and probably secure certificateless aggregate signature scheme[J]. Acta Electronica Sinica,，, 2013, 41(1): 72-76.

[11] STEINFELD R, BULL L, WANG H, et al. Universal designated verifer signatures[C]//Cryptology-Asiacrypt, 2003: 523 -542.

[12] MING Y, SHEN X, WANG Y M. Certificateless universal designated verifier signature schemes[J]. Journal of China Umiversities of Posts and Telecommunications, 2007, 14(3):85-90.

[13] 韩亚宁, 王彩芬. 无证书广义指定多个验证者有序多重签名[J]. 计算机应用, 2009, 29(6):1643-1645.
HAN Y N, WANG C F. Certificateless universal designated multi-verifiers sequential multi-signature scheme[J]. Journal of Computer Applications, 2009, 29(6): 1643-1645.

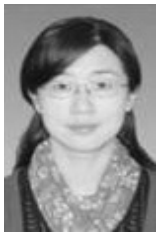
[14] 张玉磊, 周冬瑞, 李臣意,等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2015, 36(2):48-55.
ZHANG Y L, ZHOU D R, LI C Y, et al. Certificateless-based efficient aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2015, 36(2):48-55.

[15] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

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。