doi:10.11959/j.issn.1000-436x.2015033

高效的无证书广义指定验证者聚合签名方案

张玉磊[1]，周冬瑞[1]，李臣意[1]，张永洁[2]，王彩芬[1]
（1. 西北师范大学 计算机科学与工程学院，甘肃 兰州 730070；2. 甘肃卫生职业学院，甘肃 兰州 730000）

摘 要：研究无证书广义指定验证者聚合签名的安全模型，基于双线性映射提出无证书广义指定验证者聚合签名方案。在随机预言模型和计算 Diffie-Hellman 困难问题假设下，证明方案不仅可以抵抗无证书广义指定验证者聚合签名的 3 类伪造攻击，而且满足指定验证性和不可传递性。方案的聚合签名长度和单用户签名长度相当，签名公共验证和指定验证需要的双线性对数固定。

关键词：聚合签名；无证书签名；广义指定验证者；计算 Diffie-Hellman 困难问题
中图分类号：TP309 **文献标识码**：A

Certificateless-based efficient aggregate signature scheme with universal designated verifier

ZHANG Yu-lei[1], ZHOU Dong-rui[1], LI Chen-yi[1], ZHANG Yong-jie[2], WANG Cai-fen[1]
（1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China;
2.Gansu Health Vocational College, Lanzhou 730000, China）

Abstract: The security model of the certificateless aggregate signature scheme with universal designated verifier was studied, and then a certificateless aggregate signature scheme with universal designated verifier using bilinear pairings was proposed. In the random oracle mode, based on the hardness of the computational Diffie-Hellman problem, the new scheme was proved to be secure against three attacks of certificateless aggregate signature scheme with universal designated verifier. Meanwhile, the scheme satisfies properties of strong designated verify and non-transferability. Furthermore, the length of final aggregate signature is equivalent as the length of signal user's signature, it is more efficient than others because the pairing computation is fixed among public verifies and designed verifies.

Key words: aggregate signature; certificateless signature; universal designated verifier; computational Diffie-Hellman problem

1 引言

聚合签名[1]是指通过聚合算法将 n 个签名者对 n 个消息的签名聚合生成一个签名，验证方只需要验证聚合后的签名就可以确信签名是否来自指定的 n 个用户。当 n 个签名者对同一个消息进行签名时，聚合签名就演化为多重签名。聚合签名不仅可以降低验证开销，也可以减少签名长度，在带宽和存储空间受限的环境中有广泛应用[2,3]。

2003 年 AlRiyami 和 Paterson[4]提出无证书公钥密码体制，该体制不仅可以简化传统公钥密码体制中的证书管理问题，还可以避免身份公钥密码体制中的密钥托管问题。鉴于无证书密码体制和聚合签名的优势，许多研究者对无证书聚合签名(CLAS, certificateless aggregate signature)进行了研究[3,5~10]。Gong 等[5]首次定义了 CLAS 安全模型，Zhang[6]完

收稿日期：2014-01-02；**修回日期**：2014-04-08
基金项目：国家自然科学基金资助项目（61163038,61262056,61262057）；甘肃省高等学校科研基金资助项目（2013A-014）；西北师范大学青年教师科研能力提升计划基金资助项目（NWNU-LKQN-12-32）
Foundation Items：The National Natural Science Foundation of China (61163038, 61262056, 61262057); The Higher Educational Scientific Research Foundation of Gansu Province of China (2013A-014); The Young Teachers' Scientific Research Ability Promotion Program of Northwest Normal University (NWNU-LKQN-12-32)

善了无证书聚合签名安全模型。Gong 方案[5]、Zhang 方案[6]和秦方案[7]的聚合签名长度和双线性对数依赖于签名人数。研究者相继提出了更高效的 CLAS 方案[8~10]，其中，Xiong 方案[10]只需要 3 个双线性对运算，但 He 等[11]指出该方案不安全并对方案进行了改进。

广义指定验证者签名(UDVS, universal designated verifier signature)[12]是一种保护签名者隐私的重要方法。它允许签名的持有者指定签名验证者，并且，只有指定验证者可以验证签名的有效性。Ming 等[13]首次提出无证书广义指定验证者签名，韩等[14]首次提出无证书广义指定验证者的多重签名方案（演化的聚合签名方案）。韩方案[14]的签名长度和需要的双线性对数仍然依赖于签名人数。因此，有必要设计双线性对数较少的无证书聚合签名方案和广义指定验证者的无证书聚合签名方案，提高运算效率和通信效率。

本文基于无证书广义指定验证者签名安全模型[13]，对 Xiong 方案的聚合签名算法[10]进行改进，设计高效的具有广义指定验证者的无证书聚合签名 (CLASUDV, certificateless aggregate signature with universal designated verifier)方案，并且，在随机预言模型和计算 Diffie-Hellman 困难(CDH, computational Diffie-Hellman)假设下，证明方案是安全的。与已有方案相比较，方案具有以下优点：聚合签名长度固定，不随签名用户个数的增加而变化；方案满足指定验证性，除指定的验证者外其他用户不能验证聚合签名的有效性；签名的公共验证和指定验证只需要 4 个对运算，具有较高的效率。

2　CLASUDV 方案的定义及安全性要求

广义指定验证者无证书聚合签名(CLASUDV)方案包含 3 部分：无证书聚合签名方案（CLAS）、广义指定验证签名(UD-AS, universal-designated- aggregate-sign)算法和指定验证者验证(UDV-AS, universal-designated-verify-aggregate-sign)算法。方案的参与者有：密钥生成中心(KGC, key generation center)、n 个签名者 $u=\{u_1,\cdots,u_n\}$、签名聚合者 u_A 和指定验证者 u_{DV}，其中，u_A 收集 u_i 对消息 m 的签名 σ_i，生成聚合签名 σ。同时，u_A（或签名持有者）计算指定验证者签名 σ_{DV}，u_{DV} 验证签名 σ_{DV} 的有效性。

2.1　CLAS 方案

定义 1　CLAS 方案[6]包含以下算法：Setup、Partial-Private-Key-Extract、User-Key-Extract、Part-Sign、Part-Verify、Aggregate-Sign 和 Aggregate-Verify。

1) Setup 系统建立算法：KGC 执行。输入安全参数 k，输出系统参数 $Params$ 和系统主密钥 $s\in Z_q^*$。

2) User-Key-Extract 用户密钥生成算法：用户 u_i 执行。选择 $x_i\in Z_q^*$ 作为秘密值，计算用户的公钥 P_i。

3) Partial-Private-Key-Extract 部分私钥生成算法：KGC 执行。输入用户 u_i 的 ID_i、$Params$ 和主密钥 s，返回用户 u_i 的部分私钥 D_i。

4) Part-Sign 部分签名算法：用户 u_i 执行。输入消息 m_i、身份 ID_i、私钥 S_i 和系统参数，输出 u_i 对 m_i 的签名 σ_i，并将 σ_i 发送给签名聚合者 u_A。

5) Part-Verify 部分签名验证算法：若需要验证 u_i 对 m_i 签名 σ_i 的有效性，执行该算法，该算法一般缺省。

6) Aggregate-Sign 聚合算法：由聚合者 u_A 执行，输入系统参数 $Params$、用户 $u=\{u_1,\cdots,u_n\}$ 对应的身份列表 $ID=\{ID_1,\cdots,ID_n\}$、公钥列表 $P=\{P_1,\cdots,P_n\}$、消息列表 $M=\{m_1,\cdots,m_n\}$ 和签名列表 $\sigma=\{\sigma_1,\cdots,\sigma_n\}$，输出消息 $M=\{m_1,\cdots,m_n\}$ 的聚合签名 σ。

7) Aggregate-Verify 聚合签名验证算法：输入系统参数 $Params$、用户 $u=\{u_1,\cdots,u_n\}$ 对应的身份列表 $ID=\{ID_1,\cdots,ID_n\}$、公钥列表 $P=\{P_1,\cdots,P_n\}$、消息列表 $M=\{m_1,\cdots,m_n\}$ 和聚合签名 σ，如果签名正确输出 True，否则输出 False。

2.2　CLASUDV 方案

定义 2　CLASUDV 方案包含 3 类算法：无证书聚合签名方案算法、UD-AS 算法和 UDV-AS 算法。

1) UD-AS 指定验证者聚合签名算法：聚合者 u_A 或聚合签名持有者执行。输入聚合签名 σ，选择指定验证者的身份 ID_{DV} 及对应公钥 P_{DV}，输出广义指定验证者聚合签名 σ_{DV}。

2) UDV-AS 指定验证者聚合验证算法：指定验证者执行。输入系统参数 $Params$、用户 $u=\{u_1,\cdots,u_n\}$ 对应的身份列表 $ID=\{ID_1,\cdots,ID_n\}$、公钥列表 $P=\{P_1,\cdots,P_n\}$、消息列表 $M=\{m_1,\cdots,m_n\}$、验证者的公钥 P_{DV}、私钥 S_{DV} 和签名 σ_{DV}，验证 σ_{DV} 是否有效。如果签名正确输出 True，否则输出 False。

2.3　CLASUDV 方案安全性要求

CLASUDV 方案安全要求主要包括：正确性、不可伪造性、指定验证性和不可传递性。

1) 正确性

按照正确的签名步骤，部分签名、聚合签名和具有指定验证者的聚合签名必须通过相应的签名

验证算法。

2) 强指定验证性

指定验证者验证聚合签名时，必须使用指定验证者的私钥 x_{DV}，因此，除指定的验证者外其他用户不能验证聚合签名的有效性。

3) 不可传递性

指定验证者可以验证聚合签名的有效性，但验证者不能向其他用户证明这一事实。因为验证者可以用自己的私钥生成一个满足“UDV-AS”算法的与 σ_{DV} 不可区分的签名副本 σ'_{DV}。

4) 不可伪造性

对于 CLASUDV 方案的伪造攻击，一般考虑 2 类：一类为适应性选择消息和身份攻击下的存在不可伪造，防止攻击者欺骗指定验证者伪造合法的聚合签名；另一类为无证书指定验证者身份的不可伪造，攻击者用给定的验证者身份 ID^*_{DV} 对于 $M^*=\{m_1^*,\cdots, m_n^*\}$ 伪造一个指定验证者签名 σ^*_{DV}，且 (M^*,σ^*_{DV})通过 UDV-AS 验证算法在计算上不可行。

第一类不可伪造性。第一类攻击主要考虑聚合签名的不可伪造性，攻击者是 A_{I} 和 A_{II}，分别对应 CLAS 方案中适应性选择消息和身份下的一般用户公钥替换攻击和恶意 KGC 攻击。

定义 3 CLASUDV 方案中，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 CLAS 方案在适应性选择消息和身份攻击下不可伪造。

游戏 1 假定 B 为挑战者。B 运行 Setup 算法，产生系统参数 *Params* 和主密钥 s，B 保留 s，发送 *Params* 给 A_{I}。B 与 A_{I} 模拟过程中，A_{I} 可以询问以下预言机。

① 散列询问：A_{I} 可以获得方案中所有散列预言机的访问权，并得到对应的散列值。

② Partial-Private-Key 询问：当 A_{I} 询问 ID_i 的部分私钥时，B 运行“Partial-Private-Key-Extract”算法生成部分私钥 D_i，并返回给 A_{I}。

③ Public-Key 询问：当 A_{I} 询问 ID_i 的公钥时，B 运行“User-Key-Extract”算法产生 P_i 给 A_{I}。

④ Secret-Value 询问：当 A_{I} 询问 ID_i 的秘密值时，B 运行“User-Key-Extract”算法生成 x_i，若用户公钥已被替换，则返回 $\perp$。

⑤ Public-Key-Replace 询问：A_{I} 可以用自己选择的 P'_i 替换 ID_i 的公钥 P_i。

⑥ Part-Sign 询问：A_{I} 可以获得 ID_i 对 m_i 在公钥 P_i 下的签名 σ_i。

基于以上询问，A_{I} 输出用户 $u=\{u_1,\cdots,u_n\}$（身份列表 $ID^*=\{ID_1^*,\cdots,ID_n^*\}$，公钥列表 $P^*=\{P_1^*,\cdots,P_n^*\}$）分别对消息 $M^*=\{m_1^*,\cdots,m_n^*\}$签名的聚合签名 σ^*，并且，如果满足以下条件，则 A_{I} 赢得游戏。

① σ^* 是一个有效的聚合签名，可以通过“Aggregate-Verify”验证。

② 至少存在一个用户 ID_i^*，不失一般性，令为 ID_1^*，没有提交过“Partial-Private-Key”询问。

③ A_I 没有执行对(m_1^*, ID_1^*)的“Part-Sign”询问。

游戏 2 假定 B 为游戏的挑战者。B 运行 Setup 算法，产生系统参数 *Params* 和主密钥 s，发送 *Params* 和 s 给 A_{II}。B 与 A_{II} 模拟过程中，A_{II} 可以询问以下预言机。

① 散列询问、Public-Key 询问、Secret-Value 询问和 Part-Sign 询问：与游戏 1 相同。

② 由于 A_{II} 可以得到主密钥 s，A_{II} 可以生成部分私钥，因此游戏不考虑“Partial-Private-Key”询问，同时 A_{II} 不允许执行“Public-Key-Replace”询问。

基于以上询问，A_{II} 输出用户 $u=\{u_1,\cdots,u_n\}$（身份列表 $ID^*=\{ID_1^*,\cdots,ID_n^*\}$，公钥列表 $P^*=\{P_1^*,\cdots,P_n^*\}$）分别对消息 $M^*=\{m_1^*,\cdots,m_n^*\}$签名的聚合签名 σ^*，并且如果满足以下条件：

a. σ^* 是一个有效的聚合签名，可以通过“Aggregate-Verify”验证；

b. 至少存在一个用户 ID_i^*，不失一般性，令为 ID_1^*没有提交过“Secret-Value”询问”；

c. A_{II} 没有执行对(m_1^*, ID_1^*)的“Part-Sign”询问。

则 A_{II} 赢得游戏。

第二类不可伪造性。第二类攻击主要考虑指定验证者签名的不可伪造性，攻击者为 A_{III}，A_{III} 包含具有不同能力的一般用户和恶意 KGC。

定义 4 CLASUDV 方案中，如果存在敌手 A_{III} 以不可忽略的概率在游戏 3 中获胜，则 CLASUDV 方案在适应性选择消息和指定身份攻击下指定验证者签名不可伪造。

游戏 3 假定 C 为游戏的挑战者。C 运行 Setup 算法，产生系统参数 *Params* 和主密钥 s，C 与 A_{III} 模拟过程中，A_{III} 可以询问以下预言机。

① 散列询问、Public-Key 询问、Secret-Value 询问和 Public-Key-Replace 询问与游戏 1 相同，但是，若 A_{III} 表现为 KGC，则不能进行“Partial-Private-Key”询问和“Public-Key-Replace”询问。

② UD-AS 询问：A_{III} 可以获得对 $M^*=\{m_1^*,\cdots,m_n^*\}$ 指定验证者 ID_{DV}^* 的签名。

基于以上询问，A_{III} 输出对消息 $M^*=\{m_1^*,\cdots,m_n^*\}$ 聚合签名的指定验证者签名 σ_{DV}^*，并且如果满足以下条件：

a. σ_{DV}^* 是一个有效的指定验证者签名，可以通过“UDV-AS”验证；

b. 消息 $M^*=\{m_1^*,\cdots,m_n^*\}$ 之前没有做过 UD-AS 询问；

c. A_{III} 不能对指定验证者 ID_{DV} 做“Secret-Value”询问。

则 A_{III} 赢得游戏。

3　具体的 CLASUDV 方案

令 q 为大素数，选择生成元 $P\in G_1$ 和 $Q\in G_1$，定义阶均为 q 的加法群 G_1 和乘法群 G_2，双线性映射为 $e:G_1\times G_1\to G_2$，定义散列函数 $H_0:\{0,1\}^*\to Z_q^*$，$H_1:\{0,1\}^*\times G_1\to G_1$，$H_2:\{0,1\}^*\to G_1$，$H_{DV}:\{0,1\}^*\to G_1$。

3.1　无证书聚合签名 CLAS 方案

1) Setup：KGC 选择 $s\in Z_q^*$，计算 $P_{\mathrm{pub}}=sP$，发布系统参数 $Params=\{G_1,G_2,e,q,P,Q,P_{\mathrm{Pub}},H_0,H_1,H_2,H_{DV}\}$，保存 s。

2) User-Key-Extract：用户 u_i 选择随机值 $x_i\in Z_q^*$，产生用户的秘密值 x_i；计算公钥 $P_i=x_iP$。

3) Partial-Private-Key-Extract：KGC 计算 $Q_i=H_1(ID_i\|P_i)$，$D_i=sQ_i$，并将 D_i 发送给用户 u_i。用户 u_i 收到部分私钥 D_i，生成用户的私钥 $S_i=(D_i,x_i)$。

4) Part-Sign：用户 $u_i(1\leqslant i\leqslant n)$ 执行以下过程。

① 选择 $r_i\in Z_q^*$，计算 $R_i=r_iP$，$h_i=H_0(ID_i\|m_i\|P_i\|R_i)$ 和 $T=H_2(P_{\mathrm{Pub}})$。

② 计算 $V_i=D_i+h_ir_iT+x_iQ$，输出 u_i 对 m_i 的签名 $\sigma_i=(V_i,R_i)$ 并发送给聚合者 u_A。

5) Part-Verify：若需要验证 u_i 对 m_i 签名 σ_i 的有效性，可以执行该算法，该算法一般缺省。计算 $h_i=H_0(ID_i\|m_i\|P_i\|R_i)$、$Q_i=H_1(ID_i\|P_i)$ 和 $T=H_2(P_{\mathrm{Pub}})$，验证下列等式是否成立

$$e(V_i,P)=e(Q_i,P_{\mathrm{Pub}})e(T,h_iR_i)e(Q,P_i)$$

6) Aggregate-Sign：聚合者 u_A 执行。输入用户 u_i 对不同消息 $m_i(1\leqslant i\leqslant n)$ 的签名 $\{(m_1,\sigma_1=(V_1,R_1)),\cdots,(m_n,\sigma_n=(V_n,R_n))\}$，首先计算 $h_i=H_0(ID_i\|m_i\|P_i\|R_i)$，其中，$1\leqslant i\leqslant n$，然后计算 V 和 R

$$V=\sum_{i=1}^{n}V_i,\quad R=\sum_{i=1}^{n}h_iR_i$$

输出最终聚合签名 $\sigma=(V,R)$。

7) Aggregate-Verify：若需要验证聚合签名 σ 的有效性，可以执行该算法。输入系统参数 $Params$、用户 u_i 对应的身份列表 $ID=\{ID_1,\cdots,ID_n\}$、公钥列表 $P=\{P_1,\cdots,P_n\}$、消息列表 $M=\{m_1,\cdots,m_n\}$ 和签名列表 $\sigma=\{\sigma_1,\cdots,\sigma_n\}$，计算 $Q_i=H_1(ID_i\|P_i)$ $(1\leqslant i\leqslant n)$ 和 $T=H_2(P_{\mathrm{Pub}})$，验证下列等式是否成立

$$e(V,P)\overset{?}{=}e(\sum_{i=1}^{n}Q_i,P_{\mathrm{Pub}})e(T,R)e(Q,\sum_{i=1}^{n}P_i)$$

3.2　指定验证者签名算法和验证者算法

1) UD-AS 算法：签名聚合者 u_A（或签名持有者）指定聚合签名的验证者信息。输入聚合签名 $\sigma=(V,R)$、指定验证者的身份及公钥信息 (ID_{DV},P_{DV}) 和用户 u_A 的公私钥对 (P_A,x_A,D_A)，依次计算：

$$h_{DV}=H_{DV}(x_AP_{DV}),\ \hat{S}=e(V,h_{DV}P_{DV}),\ \hat{R}=h_{DV}R$$

则具有指定验证者的聚合签名为 $\hat{\sigma}=(\hat{S},\hat{R})$。

2) UDV-AS：用户 u_{DV} 验证签名 $\hat{\sigma}$ 的有效性。输入身份列表 $ID=\{ID_1,\cdots,ID_n\}$、公钥列表 $P=\{P_1,\cdots,P_n\}$、消息列表 $M=\{m_1,\cdots,m_n\}$ 和签名 $\hat{\sigma}=(\hat{S},\hat{R})$，执行步骤如下。

① 计算 $T=H_2(P_{\mathrm{Pub}})$，然后依次计算 $Q_i=H_1(ID_i\|P_i)$ 和 $h_{DV}=H_{DV}(x_{DV}P_A)$。

② 验证下列等式是否成立

$$\hat{S}\overset{?}{=}[e(\sum_{i=1}^{n}Q_i,h_{DV}P_{\mathrm{Pub}})e(T,\hat{R})e(Q,h_{DV}\sum_{i=1}^{n}P_i)]^{x_{DV}}$$

3.3　安全性分析

3.3.1　正确性

定理 1　CLASUDV 方案是正确的。

证明　本文 CLASUDV 方案是正确的，当且仅当无证书聚合签名 $\sigma=(V,R)$ 和广义指定验证者无证书聚合签名 $\hat{\sigma}=(\hat{S},\hat{R})$ 是按照签名算法计算得到的，且有 3 类验证等式成立。

1) 每个签名者 u_i 对 m_i 的签名 $\sigma_i=(V_i,R_i)$ $(1\leqslant i\leqslant n)$ 满足“Part-Verify”算法验证等式

$$\begin{aligned}e(V_i,P)&=e(D_i+h_ir_iT+x_iQ,P)\\&=e(D_i,P)e(T,h_ir_iP)e(x_iQ,P)\\&=e(Q_i,P_{\mathrm{Pub}})e(T,h_iR_i)e(Q,P_i)\end{aligned}$$

2) 得到的聚合签名 $\sigma=(V,R)$ 满足“Aggregate-Verify”算法验证等式

$$e(V,P)=e(\sum_{i=1}^{n}V_i,P)=e(\sum_{i=1}^{n}D_i+x_iQ+h_ir_iT,P)$$
$$=e(\sum_{i=1}^{n}D_i,P)e(\sum_{i=1}^{n}h_ir_iT,P)e(\sum_{i=1}^{n}x_iQ,P)$$
$$=e(\sum_{i=1}^{n}Q_i,P_{\text{Pub}})\prod_{i=1}^{n}e(T,h_iR_i)\prod_{i=1}^{n}e(Q,P_i)$$
$$=e(\sum_{i=1}^{n}Q_i,P_{\text{Pub}})e(T,R)e(Q,\sum_{i=1}^{n}P_i)$$

3) 广义指定验证者无证书聚合签名 $\hat{\sigma}=(\hat{S},\hat{R})$ 满足“UDV-AS”算法验证等式

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

3.3.2 强指定验证性

当用户验证指定验证者签名 $\hat{\sigma}=(\hat{S},\hat{R})$ 的有效性时，由验证等式(1)可知，需要使用验证者的私钥，除 u_{DV} 外其他用户不能验证 $\hat{\sigma}=(\hat{S},\hat{R})$ 的有效性，因此，只有指定的验证者可以验证该签名的有效性。

3.3.3 不可伪造性

定理 2 假定 CDH 问题是困难的，证明 CLASUDV 方案在适应性选择消息和身份下的 A_{I} 和 A_{II} 伪造攻击是安全的。

引理 1 随机预言模型下，假定攻击者 A_{I} 在时间 t 内以不可忽略的优势 ε 攻破本文方案，A_{I} 访问 H_1 预言机、Public-Key 预言机、Partial-Private-Key-Extract 预言机、Secret-Value 预言机和 Part-Sign 预言机的执行次数分别为 q_{H1}、q_{PK}、q_{PPK}、q_{SV} 和 q_S，则存在算法 B，在时间 $t'<(t+(q_{H1}+q_{PK}+q_{PPK}+q_{SV}+3q_S+2n+3))t_{SM}+t_{INV}$ 内，以 $\varepsilon'\geqslant\varepsilon\frac{1}{q_{H1}}(1-\frac{1}{q_{H1}})^{n-1+q_{PPK}}$ 的优势得到解决 CDH 问题的一个实例。其中，t_{SM} 和 t_{INV} 分别表示 G_1 群上标量乘法和 Z_q^* 上求逆运算时间。

证明 A_{I} 是攻击者，B 是 CDH 问题挑战者。B 给定 (P,aP,bP)，B 的目标是使用 A_{I} 解决 CDH 问题，即计算 abP。

B 设 $P_{\text{Pub}}=aP$，a 为系统主密钥。选择 $\gamma\in Z_q^*$，计算 $Q=\gamma P$，系统参数为 $Params=\{G_1,G_2,e,q,P,Q,P_{\text{Pub}},H_0,H_1,H_2\}$。$A_{\text{I}}$ 执行以下询问。

H_1 询问：B 保持列表 $L_1=\{ID_i,P_i,a_i,Q_i,c_i\}$，初始为空。$A_{\text{I}}$ 询问 H_1，若 L_1 中存在 ID_i 且 $P_i\neq\perp$，则直接返回 Q_i。否则，B 执行 Public-Key 询问，获得 P_i 值，再选择 $a_i\in Z_q^*$，$c_i\in\{0,1\}$（其中，$c_i=0$ 的概率为 $\xi=\frac{1}{q_{H1}}$，$c_i=1$ 的概率为 $1-\xi$）。若 $c_i=0$，令 $Q_i=a_iP$，增加$(ID_i,P_i,a_i,Q_i,0)$到 L_1 并返回 Q_i 值；否则 c_i=1，计算 $Q_i=a_ibP$，增加$(ID_i,P_i,a_i,Q_i,1)$到 L_1 并返回 Q_i 值。

H_2 询问：B 保持列表 $L_2=\{P_{\text{Pub}},\beta,T\}$，初始为空。$A_{\text{I}}$ 询问 H_2，若 L_2 中存在询问项则直接返回 T，否则，B 选择 $\beta\in Z_q^*$，计算 $T=\beta P$，返回 T 并将(P_{Pub},β,T)增加到 L_2 中。

H_0 询问：B 保持列表 $L_0=\{ID_i,m_i,P_i,R_i,h_i,\eta_i\}$，初始为空。$B$ 收到 A_I 对 ID_i 的 H_0 询问时，若 ID_i 在 L_0 存在且 $P_i\neq\perp$，则直接返回 h_i 值。否则，B 先执行公钥询问，获得 P_i 值，然后选择 $\eta_i\in Z_q^*$，令 $h_i=\eta_i$，增加$(ID_i,m_i,P_i,R_i,h_i,\eta_i)$到 L_0 并返回 h_i 值。

Partial-Private-Key 询问：B 保持列表 $E=\{ID_i,D_i\}$，初始为空。A_{I} 询问 ID_i 的部分私钥时，若 E 中已有相应记录，则直接返回 D_i。否则，A_{I} 执行 H_1 询问，返回(ID_i,P_i,a_i,Q_i,c_i)。若 c_i=1，则终止；否则，计算 $D_i=a_iP_{\text{Pub}}=a_iaP$，返回 D_i 给 A_I，并将(ID_i,D_i)添加到表 E。

Public-Key 询问：B 保持列表 $F=\{ID_i,x_i,P_i,c_i\}$，初始为空。A_{I} 询问 ID_i 的公钥时，若 F 包含询问内容，返回 P_i 给 A_{I}。否则，随机选择 $x_i\in Z_q^*$，计算 $P_i=x_iP$，返回 P_i 给 A_I 将$(ID_i,x_i,P_i,\perp)$添加到 F 表中。

Secret-Value 询问：当 A_{I} 询问 ID_i 的秘密值时，B 查 F 表，若 F 表包含对应 ID_i，检测 x_i 是否为空，如果 $x_i\neq\perp$，则返回对应值，否则 B 执行“Public-Key”询问，保存(ID_i,x_i,P_i)并返回 x_i；若 F 表不包含对应 ID_i，则 B 执行“Public-Key”询问，将$(ID_i,x_i,P_i,\perp)$添加到 F 表中并返回 x_i 值。

Public-Key-Replace 询问：A_{I} 对 ID_i 用新的公钥 P_i' 代替原公钥 P_i。若 F 表中包含身份 ID_i，B 令 $P_i=P_i'$，$x_i=\perp$。若 F 表中未包含身份 ID_i，B 令 $P_i=P_i'$，$x_i=\perp$，并添加到 F 表。

Sign 询问：A_{I} 作 (m_i,ID_i,P_i) 签名询问，B 查表 L_1 获得 (ID_i,P_i,a_i,Q_i,c_i)。若 $c_i=0$，查表 L_0 和 L_2 获得 $(ID_i,m_i,P_i,R_i,h_i,\eta_i)$ 和 T 的值，B 随机选取 $R_i\in G_1$，计算 $V_i=a_iP_{\text{Pub}}+\eta_i\beta R_i+\gamma P_i$，$B$ 返回 $\sigma=(V_i,R_i)$ 给 A_{I}，否则失败退出。

伪造：A_{I} 返回 n 个用户集合 $L^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$，公钥为 $\{P_1^*,P_2^*,\cdots,P_n^*\}$，消息为 $M^*=\{m_1^*,\cdots,m_n^*\}$，伪造的签名 $\sigma_i^*=(V_i^*,R_i^*)$。若所有的 $c_i^*=0$ 则失败退出，否则，只要有一个 $c_i^*=1$ 就可以伪造聚合签名。不失一般性，令 i=1。B 执行 $c_1^*=1$、$c_i^*=0$（$2\leqslant i\leqslant n$）的签名过程得到伪造签名 (V^*,R^*) 必须满足验证等式

$$e(V^*,P)=e(\sum_{i=1}^{n}Q_i^*,P_{\mathrm{Pub}})e(Q,\sum_{i=1}^{n}P_i^*)e(T,R^*)$$

其中，$V^*=\sum_{i=1}^{n}V_i^*$，$R^*=\sum_{i=1}^{n}h_i^*R_i^*$，$Q_i^*=a_i^*P$ $(2\leqslant i\leqslant n)$，$Q_1^*=a_1^*bP$，则有 $e(V^*,P)=[e(\sum_{i=2}^{n}Q_i^*,P_{\mathrm{Pub}})\cdot e(Q,\sum_{i=1}^{n}P_i^*)e(T,R^*)]e(Q_1^*,P_{\mathrm{Pub}})$。

即 $e(Q_1^*,P_{\mathrm{Pub}})$

$$=e(V^*,P)[e(\sum_{i=2}^{n}Q_i^*,P_{\mathrm{Pub}})e(Q,\sum_{i=1}^{n}P_i^*)e(T,R^*)]^{-1}\cdot e(a_1^*bP,aP)$$

$$=e(V^*,P)[e(\sum_{i=2}^{n}a_i^*P,P_{\mathrm{Pub}})e(P,\gamma\sum_{i=1}^{n}P_i^*)e(P,\beta R^*)]^{-1}\cdot$$

$$a_1^*abP=V^*-\sum_{i=2}^{n}a_i^*P_{\mathrm{Pub}}-\gamma\sum_{i=1}^{n}P_i^*-\beta R^*$$

$$abP=a_1^{*-1}(V^*-\sum_{i=2}^{n}a_i^*P_{\mathrm{Pub}}-\gamma\sum_{i=1}^{n}P_i^*-\beta R^*)$$

B 解决 CDH 困难问题。

下面分析 B 成功的概率，首先定义 3 个事件。

1) E_1 为“Partial-Private-Key”询问过程中未退出。

2) E_2 为成功伪造了一个聚合签名 (V^*,R^*)。

3) E_3 为 n 个用户中至少有一个 c^*=1，不失一般性，令 $ID^*=ID_1$。

则有 $Adv_B^{CDH}=\Pr[\mathrm{E}_1\wedge\mathrm{E}_2\wedge\mathrm{E}_3]$

$$=\Pr[\mathrm{E}_1]\Pr[\mathrm{E}_2\,|\,\mathrm{E}_1]\quad\Pr[\mathrm{E}_3\,|\,\mathrm{E}_2\wedge\mathrm{E}_1]$$

如果 E_1 事件发生，则对于某个用户“Partial-Private-Key-Extract”模拟过程中 B 未退出的概率为 $1-\frac{1}{q_{H1}}$。“Partial-Private-Key-Extract”询问至多 q_{PPK} 次，则“Partial-Private-Key”询问过程中未退出的概率至少为 $\left(1-\frac{1}{q_{H1}}\right)^{q_{PPK}}$，即 $\Pr[\mathrm{E}_1]\geqslant\left(1-\frac{1}{q_{H1}}\right)^{q_{PPK}}$。

在 E_1 事件发生的前提下 E_2 事件发生意味着攻击者可以成功伪造一个有效的签名，显然有 $\Pr[\mathrm{E}_2\,|\,\mathrm{E}_1]\geqslant\varepsilon$。

当 E_1 事件和 E_2 事件都发生，并且要求 n 个用户中至少有一个 $c^*=1$（$c_i=0$ 的概率为 $\xi=\frac{1}{q_{H1}}$，$c_i=1$ 的概率为 $1-\xi$），则 E_1 事件和 E_2 事件都发生的前提下，E_3 事件发生的概率至少为 $\xi(1-\xi)^{n-1}$，即 $\Pr[\mathrm{E}_3\,|\,\mathrm{E}_2\wedge\mathrm{E}_1]\geqslant\frac{1}{q_{H1}}\left(1-\frac{1}{q_{H1}}\right)^{n-1}$。

综上概率分析，则有

$$\Pr[\mathrm{E}_1\mathrm{E}_2\mathrm{E}_3]\geqslant\left(1-\frac{1}{q_{H1}}\right)^{q_{PPK}}\varepsilon\frac{1}{q_{H1}}\left(1-\frac{1}{q_{H1}}\right)^{n-1}$$

$$\geqslant\varepsilon\frac{1}{q_{H1}}\left(1-\frac{1}{q_{H1}}\right)^{n-1+q_{PPK}}$$

B 所使用的时间为 $t'<(t+(q_{H1}+q_{PK}+q_{PPK}+q_{SV}+3q_S+2n+3))t_{SM}+t_{INV}$。

引理 2　随机预言模型下，假定攻击者 A_{II} 在时间 t 内以不可忽略的优势 ε 攻破本文方案，A_{II} 访问 H_1 预言机、Public-Key 预言机、Secret-Value 预言机和 Part-Sign 预言机的执行次数分别为 q_{H1}、q_{PK}、q_{SV} 和 q_S，则存在算法 B，在时间 $t'<(t+q_{H1}+q_{PK}+q_{SV}+3q_S+2n+3))t_{SM}+t_{INV}$ 内，以 $\varepsilon'\geqslant\varepsilon\left(1-\frac{1}{q_{PK}}\right)^{q_{SV}}\left(\frac{q_S}{q_S+1}\right)^{q_S}\left(1-\left(\frac{q_{PK}}{q_{PK}+1}\right)^{n}\right)$ 的优势得到解决 CDH 问题的一个实例。

证明　A_{II} 是攻击者，B 是 CDH 问题挑战者。B 给定 (P,aP,bP)，B 的目标是使用 A_{II} 解决 CDH 问题。

B 设 $P_{\mathrm{Pub}}=\lambda P$, λ 为系统主密钥，令 $Q=\gamma aP$。系统参数为 $Params=\{G_1,G_2,e,q,P,P_{\mathrm{Pub}},H_0,H_1,H_2\}$，发送系统参数给 A_{II}。由于 A_{II} 可以获得系统主密钥 λ，所以 A_{II} 可以计算每个用户的部分私钥。A_{II} 执行以下询问。

H_1 询问、H_0 询问、H_2 询问和 Secret-Value 询问同引理 1。

Public-Key 询问：B 保持列表 $F=\{ID_i,x_i,P_i,c_i\}$。A_{II} 询问 ID_i 的公钥时，若 F 包含询问内容，返回 P_i

给 A_{II}。否则，随机选择 $x_i \in Z_q^*$， $c_i \in \{0,1\}$（其中，$c_i=0$ 的概率为 $\xi=\frac{1}{q_{PK}}$，$c_i=1$ 的概率为 $1-\xi$）。若 $c_i=0$，计算 $P_i=l_iP$，返回 P_i 给 A_{II}，并将 (ID_i,x_i,P_i,w_i) 添加到 F 表中若 $c_i=1$，计算 $P_i=x_ibP$，返回 P_i 给 A_{II}，并将 (ID_i,x_i,P_i,c_i) 添加到 F 表中。

Sign 询问：A_{II} 做 (m_i,ID_i,P_i) 签名询问，B 查表 F 和 L_2 获得 (ID_i,x_i,P_i,c_i) 和 $(P_{\mathrm{Pub}},\beta,T)$。若 $c_i=0$，B 随机选取 $R_i\in G_1$，计算 $V_i=\lambda Q_i+\eta_i\beta R_i+\gamma x_ibP$，则签名为 $\sigma=(V_i,R_i)$，B 返回 σ 给 A_{II}，否则，失败退出。

伪造：A_{II} 返回 n 个用户的集合 $L^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$、公钥为 $\{P_1^*,P_2^*,\cdots,P_n^*\}$，签名消息为 $M^*=\{m_1^*,\cdots,m_n^*\}$，伪造的签名 $\sigma_i^*=(V_i^*,R_i^*)$。若所有的 $c_i^*=0$，则失败退出，否则，只要有一个 $c_i^*=1$ 就可以伪造聚合签名。不失一般性，令 i=1。B 执行 $c_1^*=1$、$c_i^*=0$ $(2\leqslant i\leqslant n)$的签名过程得到伪造签名 (V^*,R^*) 必须满足验证等式

$$e(V^*,P)=e(\sum_{i=1}^{n}Q_i^*,P_{\mathrm{Pub}})e(Q,\sum_{i=1}^{n}P_i^*)e(T,R^*)$$

其中，$V^*=\sum_{i=1}^{n}V_i^*$，$R^*=\sum_{i=1}^{n}h_i^*R_i^*$，$Q_i^*=H_1(ID_i^*\|P_i^*)$，$T^*=\beta P$，$P_1^*=x_1^*bP$，$P_i^*=x_i^*P(2\leqslant i\leqslant n)$。

则有下式成立：

$$e(Q,P_1^*)=e(V^*,P)\left(e(\sum_{i=1}^{n}Q_i^*,P_{\mathrm{Pub}})e(Q,\sum_{i=2}^{n}P_i^*)e(T,R^*)\right)^{-1}$$

$$e(\gamma aP,x_1^*bP)=e(V^*,P)$$

$$\left(e(\sum_{i=1}^{n}Q_i^*,\lambda P)e(Q^*,\sum_{i=2}^{n}x_i^*P)e(T,R^*)\right)^{-1}$$

$$=e(V^*,P)\left(e(\sum_{i=1}^{n}\lambda Q_i^*,P)e(\sum_{i=2}^{n}x_i^*Q,P)e(\beta P,R^*)\right)^{-1}$$

$$abP=(\gamma x_1^*)^{-1}(V^*-\sum_{i=1}^{n}\lambda Q_i^*-\sum_{i=2}^{n}x_i^*Q-\beta R^*)$$

B 能够成功计算 abP，B 能够解决 CDH 困难问题。

下面分析 B 成功的概率：定义事件 E_1 为“Secret-Value”和“Sign”询问过程中未退出；E_2 为成功伪造了一个聚合签名 (V^*,R^*)；E_3 为 n 个用户中至少有一个 $c^*=1$，不失一般性，令 $ID^*=ID_1$。

与引理 1 事件概率分析相似，B 成功的概率为

$$\Pr[\mathrm{E}_1\mathrm{E}_2\mathrm{E}_3]\geqslant\left(1-\frac{1}{q_{PPK}}\right)^{q_{SV}+q_S}\varepsilon\frac{1}{q_{PPK}}\left(1-\frac{1}{q_{PPK}}\right)^{n-1}$$

$$\geqslant\varepsilon\frac{1}{q_{PPK}}\left(1-\frac{1}{q_{PPK}}\right)^{n-1+q_{SV}+q_S}$$

定理 3 基于散列函数的单向性，证明 CLASUDV 方案在适应性选择消息和指定验证者身份下的 A_{III} 伪造攻击是安全的。

证明 假设攻击者 A_{III} 对于消息 $M^*=\{m_1^*,\cdots,m_n^*\}$ 伪造的指定验证者 σ_{DV}^* 的签名为 $(M^*,\hat{S}^*,\hat{R}^*)$，该签名能够通过验证算法“UDV-AS”。根据算法，A_{III} 将通过 2 种方式实现伪造：① 获得验证者 ID_{DV} 的私钥 x_{DV}；②获得对 $M^*=\{m_1^*,\cdots,m_n^*\}$ 伪造的聚合签名。

分析方式①不可能：散列函数 H_{DV} 的输入为 x_AP_{DV} 或 $x_{DV}P_A$，令 $Y=x_AP_{DV}=x_{DV}P_A$，则已知 Y 计算 x_{DV} 等价于求解离散对数的困难问题。同时 x_AP_{DV} 或 $x_{DV}P_A$ 作为散列函数 H_{DV} 的输入，由散列函数的单向性可知，通过 H_{DV} 的结果获得 Y 是不可行的。

分析方式②不可能：攻击者 A_{III} 要获得对 $M^*=\{m_1^*,\cdots,m_n^*\}$ 的伪造聚合签名，等价于 A_{III} 扮演 A_{I} 和 A_{II}。定理 1 和定理 2 已分别证明适应性选择消息和身份下的 A_{I} 和 A_{II} 伪造攻击是安全的，因此，方式②不可能。

因此，攻击者 A_{III} 对于 CLASUDV 方案在适应性选择消息和指定验证者身份下的伪造攻击是安全的。

3.3.4 不可传递性

定理 4 指定验证者 u_{DV} 可以模拟一个与无证书聚合签名 σ_{DV} 不可区分的签名副本 σ'_{DV}，并且通过 UDV-AS 算法。

证明 用户 u_{DV} 可以执行“模拟”算法。选择 $R'\in G_1$，计算 $Q_i=H_1(ID_i\|P_i)$，$h_{DV}=H_{DV}(P_{DV})$，$\hat{R}=h_{DV}R'$；计算

$$\hat{S}'=e(\sum_{i=1}^{n}Q_i,x_{DV}h_{DV}P_{\mathrm{Pub}})e(x_{DV}h_{DV}Q,\sum_{i=1}^{n}P_i)e(x_{DV}T,\hat{R})$$

显然，对于消息 $m_i(1\leqslant i\leqslant n)$ 的模拟签名 $\hat{\sigma}'=(\hat{S}',\hat{R})$ 满足验证等式，指定验证者可以产生与签名 $\hat{\sigma}=(\hat{S},\hat{R})$ 不可区分的签名 $\hat{\sigma}'=(\hat{S}',\hat{R}')$。

4 效率分析

本节主要分析无证书聚合签名方案和无证书广义指定验证者聚合签名方案的计算效率，基于双线性

对签名方案中，双线性对的计算最消耗时间，不失一般性，仅考虑最耗时的双线性对(用 P 表示)运算和次耗时的映射到 G_1 群的散列(用 H 表示)运算。设 n 为聚合签名的签名人数，则验证聚合签名时，文献[7]方案需要$(n+2)P$ 运算；文献[8]方案需要 $5P$ 运算；文献[10]方案需要 $3P$ 运算，但该方案不安全；本文无证书聚合签名方案与文献[9]方案都需要 $4P$ 运算；但本文方案少 2 个 H 运算。对比本文无证书广义指定验证者聚合签名方案和文献[14]无证书广义指定验证者多重签名方案（演化的聚合签名）的计算效率，文献[14]需要$(n+2)P$ 运算，本文方案需要 $4P$ 运算。

综合以上分析，本文的无证书聚合签名方案与现有最优的、证明安全的无证书聚合签名方案的效率相当，签名长度固定，不随签名用户数的增加而变化。同时，本文的无证书广义指定验证者聚合签名方案验证签名需要对运算不随用户数的增加而变化，与现有方案相比具有较高的效率。

5　结束语

广义指定验证者聚合签名不仅可以使多个用户、不同消息的签名实现聚合和统一验证，也可以由聚合者（或签名持有者）指定签名的验证者，在一些特殊应用中有重要的作用。本文设计了一个无证书广义指定验证者聚合签名方案，一方面，方案是紧致的，聚合签名长度和对运算个数固定，并且，指定验证者以后的聚合签名方案，运算量没有变化，因此具有较高的效率；另一方面在 CDH 困难假设和随机预言模型下，证明了方案不仅可以抵抗无证书广义指定验证者聚合签名中的 3 类伪造攻击，而且满足指定验证者签名的指定验证性和不可传递性。基于以上优势，该方案可应用于躯体传感器网络和车联网，实现多节点采集数据的聚合传输和指定验证。例如在车联网中，路旁节点(RSU, roadside units)可以把车辆节点发送的各类数据分类聚合，并对不同类的数据指定不同的验证者，然后将各类聚合数据传输给主控设备。这样不仅提高了数据传输效率，而且实现了对不同类数据的验证，具有一定的实际意义。

参考文献：

[1] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[A]. Cryptology- Eurocrypt 2003[C]. Berlin, Springer, 2003.416-432.

[2] CHEN C M, LIN Y H, LIN Y C, *et al*. RCDA: recoverable concealed data aggregation for data integrity in wireless sensor networks[J]. IEEE Transactions on,Parallel and Distributed Systems, 2012, 23(4): 727-734.

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

[4] ALRIYAMI S S, PATERSON K G. Certificateless public key cryptography[A].Cryptology-Asiacrypt 2003[C]. Berlin: Springer, 2003.452- 474.

[5] GONG Z, LONG Y, XIONG H, *et al.* Two certificateless aggregate signatures from bilinear maps[A]. SNPD 2007[C]. IEEE Computer Society, 2007.188-193.

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

[7] 秦艳琳, 吴晓平. 高效的无证书有序多重签名方案[J]. 通信学报, 2013, 34(7): 105-110.
QIN Y L, WU X P. Efficient certificateless sequential multi-signature scheme [J]. Journal on Communications, 2013,34(7):105-110.

[8] ZHANG L, QIN B, WU Q H, *et al*. Efficient many-to-one authentication with certificateless aggregate signatures[J]. Computer Networks, 2010, 54(14) :2482- 2491.

[9] 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 provably-secure certificateless aggregate signature scheme[J]. Acta Electronica Sinica, 2013, 54(14):2482-2491.

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

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

[12] STEINFELD R, BULL L, WANG H, *et al*. Universal designated verifier signatures[A]. Cryptology-Asiacrypt 2003[C]. Berlin, Springer, 2003.523-542.

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

[14] 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.

作者简介：

张玉磊（1979-），男，甘肃靖远人，西北师范大学副教授，主要研究方向为信息安全与密码学。

周冬瑞（1990-），男，河南洛阳人，西北师范大学硕士生，主要研究方向为信息安全与密码学。

李臣意（1989-），男，山东潍坊人，西北师范大学硕士生，主要研究方向为信息安全与密码学。

张永洁（1978-），女，甘肃武都人，甘肃卫生职业学院副教授，主要研究方向为信息安全与密码学。

王彩芬[通信作者]（1963-），女，河北安国人，博士，西北师范大学教授、博士生导师，主要研究方向为密码学和电子商务协议的设计与分析。E-mail: wangcf@nwnu.edu.cn。