无证书聚合签名方案的安全性分析和改进

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

摘 要：该文分析了He等人(2014)提出的无证书签名方案和Ming等人(2014)提出的无证书聚合签名方案的安全性，指出Ming方案存在密钥生成中心(KGC)被动攻击，He方案存在KGC被动攻击和KGC主动攻击。该文描述了KGC对两个方案的攻击过程，分析了两个方案存在KGC攻击的原因，最后对Ming方案提出了两类改进。改进方案不仅克服了原方案的安全性问题，同时也保持了原方案聚合签名长度固定的优势。

关键词：密码学；聚合签名；无证书签名；密钥生成中心攻击；选择消息攻击；计算 Diffie-Hellman 困难问题
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2015)08-1994-06
DOI: 10.11999/JEIT141635

Security Analysis and Improvements of Certificateless Aggregate Signature Schemes

Zhang Yu-lei[①] Li Chen-yi[①] Wang Cai-fen[①] Zhang Yong-jie[②]
[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)
[②](*Gansu Health Vocational College*, *Lanzhou* 730000, *China*)

Abstract: The security of certificateless signature scheme which was proposed by He *et al.* (2014) is analyzed, and the security of the certificateless aggregate signature scheme which was proposed by Ming *et al.* (2014) is analyzed too. It is pointed out that the Key Generation Center (KGC) can realize the passive attacks in the Ming's scheme. It is also pointed out that KGC can realize the passive attack and initiative attack respectively in the Nimg's scheme. The processes of concrete forgery attacks which perfored by KGC are shown, and the possible reasons are analyzed. Finally, two improved Ming's schemes are proposed. The improved schemes not only overcome the security problem of original scheme but also have an advantage that the length of aggregated signature is fixed.

Key words: Cryptography; Aggregate signature; Certificateless signature; Key Generation Center (KGC) attack; Chosen message attack; Computational Diffie-Hellman Hard problem (CDH)

1 引言

无证书公钥密码体制[1–4]能够简化传统公钥密码体制的证书管理问题，同时，也能够避免身份公钥密码体制的密钥托管问题。聚合签名[5]可以降低签名验证和通信开销，也可以减少签名长度。基于无证书公钥密码和聚合签名的优势，无证书聚合签名(CertificateLess Aggregate Signature, CLAS)得到广泛研究[6–12]。

2013年，文献[6]提出了只需要3个双线性对运算的无证书签名方案(CertificateLess Signature, CLS)和CLAS方案。2014年，文献[7]指出文献[6]的CLS方案存在密钥生成中心(Key Generation Center, KGC)伪造攻击，并提出改进的方案。同年，文献[8]也提出了一个高效的CLAS方案。本文对文献[7]和文献[8]方案的安全性进行分析，指出两个方案都存在KGC伪造攻击：文献[8]方案存在KGC被动攻击，文献[7]方案既存在KGC被动攻击，又存在KGC主动攻击。同时，本文分析了两个方案存在KGC被动攻击和主动攻击的原因，并对文献[8]方案进行了两类改进。两类改进方案不仅克服了原方案存在KGC被动攻击的不足，而且具有较低的聚合签名验证开销。同时，第2类改进方案保持了原方案聚合签名长度固定的优势。

2014-12-25 收到，2015-03-23 改回，2015-06-09 网络优先出版
国家自然科学基金(61163038, 61262056, 61262057)，甘肃省高等学校科研项目(2013A-014)和西北师范大学青年教师科研能力提升计划项目(NWNU-LKQN-12-32)资助课题
*通信作者：王彩芬 wangcf@nwnu.edu.cn

2 CLAS方案形式化定义和安全模型

2.1 CLAS 方案形式化定义

CLAS方案一般包括以下算法：

(1)系统建立算法：输入安全参数k, KGC输出系

统主密钥s和系统参数Para。

(2)部分私钥生成算法：输入身份ID_i、系统参数Para和主密钥s，KGC计算用户的部分私钥D_i。

(3)用户密钥生成算法：用户选择秘密值x_i，输入身份ID_i和系统参数Para，输出用户的完整私钥$S_i=(D_i,x_i)$和用户的公钥P_i。

(4)签名算法：输入消息m_i、身份ID_i、私钥S_i及系统参数Para，输出用户对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、公钥P_i及Para，验证签名的有效性。若签名正确，则输出真，否则输出假。

(6)聚合签名生成算法：输入用户u_i对消息m_i的签名σ_i，输出聚合签名σ，其中$1\le i\le n$。

(7)聚合签名验证算法：输入系统参数Para、消息m_i、公钥P_i和聚合签名σ，验证聚合签名σ的有效性。如果聚合签名σ正确，则输出真，否则输出假，其中$1\le i\le n$。

2.2 CLAS方案安全模型

2007年，文献[9]首次定义CLAS方案的安全模型，文献[10]对安全模型进行了完善。CLS方案和CLAS方案一般考虑两类攻击者：A_{I}和A_{II}。A_{I}不能得到系统主密钥，但可以实现公钥替换攻击，一般指普通用户。A_{II}可以得到系统主密钥，但不允许进行公钥替换攻击，一般指KGC。以下描述CLAS方案的安全模型。

游戏1　假定B为挑战者，运行系统建立算法产生系统参数Para和主密钥s。B保留s，发送Para给A_{I}。

B与A_{I}模拟过程中，A_{I}询问以下预言机：

(1)用户建立询问：输入身份ID_i，B运行部分私钥生成算法和用户密钥生成算法获得部分私钥D_i、秘密值x_i和公钥P_i。B存储$(\mathrm{ID}_i,D_i,x_i,P_i)$，返回$P_i$。

(2)部分私钥询问：输入身份ID_i，若列表中存在对应身份，则返回D_i，否则返回空值。

(3)秘密值询问：输入身份ID_i，若列表中存在对应身份，则返回x_i，否则返回空值。若用户公钥被替换，返回空值。

(4)公钥替换询问：输入身份ID_i和A_{I}选择的公钥P_i'，若列表中存在对应身份，则用P_i'替换P_i。

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

基于以上询问，A_{I}输出n个用户$\{u_i\}$在身份$\{\mathrm{ID}_i^*\}$、公钥$\{P_i^*\}$下分别对消息$\{M_i^*\}$的聚合签名σ^*，其中，$1\le i\le n$。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，能够通过聚合验证算法。

(2)至少存在一个用户ID_i^*，不失一般性令为ID_1^*，没有提交过部分私钥询问。

(3)A_{I}没有执行对(m_1^*,ID_1^*)的签名询问。

游戏2　假定B为挑战者。B运行系统建立算法，产生系统参数Para和主密钥s。B发送Para和s给A_{II}。

B与A_{II}模拟过程中，A_{II}可以进行公钥询问、秘密值询问和签名询问。由于A_{II}能够获得主密钥s，因此，不考虑部分私钥询问，也不允许执行公钥替换询问。

基于以上询问，A_{II}输出n个用户$\{u_i\}$在身份$\{\mathrm{ID}_i^*\}$、公钥$\{P_i^*\}$下分别对消息$\{M_i^*\}$签名$\{\sigma_i^*\}$的聚合签名σ^*，其中，$1\le i\le n$。如果满足以下条件，则A_{II}赢得游戏：

(1)σ^*是一个有效的聚合签名，能够通过聚合验证等式。

(2)至少存在一个用户ID_i^*，不失一般性令为ID_1^*，没有提交过秘密值询问。

(3)A_{II}没有执行对(m_1^*,ID_1^*)的签名询问。

定义1　CLAS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，则该方案在适应性选择消息和身份攻击下是不可伪造的。

3　文献[8]方案的安全性分析

本节首先回顾文献[8]方案，然后对该方案进行安全性分析。

3.1 文献[8]方案回顾

文献[8]方案包含以下算法。

(1)系统建立算法。设安全参数为k，q为大素数，生成元$P\in G_1$。定义阶为q的群G_1和G_2，双线性映射$e:\ G_1\times G_1\to G_2$。哈希函数$H_1,H_2,H_3:\{0,1\}^*\to G_1$，$H_4:\{0,1\}^*\to Z_q^*$。KGC选取$s\in Z_q^*$为主密钥，计算$P_{\mathrm{pub}}=sP$，发布系统参数$\mathrm{Para}=\{G_1,G_2,e,q,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4\}$，保存主密钥$s$。

(2)部分私钥生成算法。KGC计算$Q_i=H_1(\mathrm{ID}_i)$，$D_i=sQ_i$，发送D_i给用户u_i。

(3)用户密钥生成算法。用户选择秘密值$x_i\in Z_q^*$，生成用户的私钥$S_i=(D_i,x_i)$和公钥$P_i=x_iP$。

(4)部分签名生成算法。用户执行过程为：

(a)选择$r_i\in Z_q^*$，计算$R_i=r_iP$。

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

(c)计算$S_i=D_i+x_i(h_iP_{\mathrm{pub}}+U)+r_iT$，输出用户$u_i$对$m_i$的签名$\sigma_i=(S_i,R_i)$。($\theta$为用户协商的状态信息)。

(5) 聚合签名生成算法。输入签名$\{\sigma_i=(S_i,R_i)\}$，$1\le i\le n$。计算：$S=\sum_{i=1}^{n}S_i$，$R=\sum_{i=1}^{n}R_i$，输出聚合签名$\sigma=(S,R)$。

(6)聚合签名验证算法。输入身份$\{\mathrm{ID}_i^*\}$、公钥$\{P_i^*\}$、状态信息θ和签名$\sigma=(S,R)$，其中，$1\le i\le n$。验证者执行验证过程为：

(a)计算$Q_i=H_1(\mathrm{ID}_i)$，$U=H_2(\theta)$，$T=H_3(\theta)$，$h_i=H_4(\theta\,||\,\mathrm{ID}_i\,||\,m_i\,||\,P_i)$，$1\le i\le n$。

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

3.2 对文献[8]方案的攻击

分析文献[8]方案，该方案的安全性主要依赖于主密钥s、秘密值x_i、部分私钥D_i和随机值r_i等秘密信息。由于$P_{\mathrm{pub}}=sP$，$P_i=x_iP$，$R_i=r_iP$和$D_i=sQ_i$，一般用户无法获得s，x_i，r_i和D_i的值(否则离散对数困难问题可解)，因此，方案能够抵抗A_{I}攻击。

由于x_i和r_i分别嵌入在元素$P_i\in G_1$和$R_i\in G_1$中，因此KGC无法直接获得x_i和r_i。但是，由于$x_iP_{\mathrm{pub}}=x_isP=sP_i$，因此，KGC能够计算$x_iP_{\mathrm{pub}}$。当KGC捕获用户$u_i$的合法签名$\sigma_i=(S_i,R_i)$，通过$x_iP_{\mathrm{pub}}$和$D_i$能够计算签名表达式$S_i=D_i+x_i(h_iP_{\mathrm{pub}}+U)+r_iT$中的固定值$x_iU+r_iT$，(其中$U=H_2(\theta)$和$T=H_3(\theta)$为固定值)。因为$h_i$的计算与$x_iU+r_iT$无关，并且，$H_4$中不包含$R_i$，因此，KGC利用固定表达式$x_iU+r_iT$、元素$R_i$、固定值$sP_i$和部分私钥$D_i$能够成功伪造用户对新消息$m_i^*$的签名。如果KGC伪造并聚合所有用户的签名，就能够得到伪造的无证书聚合签名。攻击过程为：

(1)捕获签名。KGC通过窃听等方式获得用户对m_i的签名$\sigma_i=(S_i,R_i)$。

(2)计算固定值x_iP_{pub}。KGC容易计算$x_iP_{\mathrm{pub}}=x_isP=sP_i$，其中$P_i$为用户的公钥。

(3)计算固定值x_iU+r_iT。KGC持有所有用户的部分私钥，并且$h_i\in Z_q^*$，因此，KGC能够计算$x_iU+r_iT=S_i-D_i-x_ih_iP_{\mathrm{pub}}=S_i-D_i-h_isP_i$。

(4)伪造签名。KGC利用值R_i，x_iP_{pub}和x_iU+r_iT，容易伪造m_i^*的签名。

(a)计算$h_i^*=H_4(\theta\,||\,\mathrm{ID}_i\,||\,m_i^*\,||\,P_i)$，$\theta$为状态信息。

(b)计算$S_i^*=D_i+h_i^*sP_i+x_iU+r_iT$，则对$m_i^*$的伪造签名为$\sigma_i^*=(S_i^*,R_i)$。

(5)验证消息m_i^*签名$\sigma_i^*=(S_i^*,R_i)$的合法性。

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

(b)判断等式是否成立：$e(S_i^*,P)\stackrel{?}{=}e(Q_i+h_i^*P_i,P_{\mathrm{pub}})e(P_i,U)e(T,R_i)$。

由于$e(S_i^*,P)=e(D_i+h_i^*sP_i+x_iU+r_iT,P)=e(Q_i+h_i^*P_i,P_{\mathrm{pub}})e(P_i,U)e(T,R_i)$签名验证等式成立，KGC伪造用户对新消息的签名成功。

(6)伪造聚合签名。通过以上过程，KGC能够伪造多个用户$\{u_i\}$对多个消息$\{m_i^*\}$的签名$\{m_i^*,\sigma_i^*=(S_i^*,R_i)\}$，$1\le i\le n$，然后计算$S^*=\sum_{i=1}^{n}S_i^*$，$R=\sum_{i=1}^{n}R_i$，输出伪造的聚合签名$\sigma^*=(S^*,R)$。

由于以下验证等式成立，因此，KGC恶意被动攻击成功。

$$\begin{aligned}e(S^*,P)&=e\left(\sum_{i=1}^{n}V_i^*,P\right)\\&=e\left(\sum_{i=1}^{n}\left(D_i+h_i^*sP_i+x_iU+r_iT\right),P\right)\\&=e\left(\sum_{i=1}^{n}(Q_i+h_i^*P),P_{\mathrm{pub}}\right)e\left(\sum_{i=1}^{n}P_i,U\right)e(T,R)\end{aligned}$$

4 文献[7]方案的安全性分析

文献[7]对文献[6]中的CLS方案进行了改进。但是，文献[7]改进方案仍然存在KGC攻击。

4.1 文献[7]方案回顾

文献[7]方案的“部分私钥生成算法”和“用户密钥生成算法”与文献[8]方案算法基本相同，本节仅列出其它算法。

(1)系统建立算法。选择两个生成元P，$Q\in G_1$，哈希函数$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_q^*$。KGC发布系统参数$\mathrm{Para}=\{G_1,G_2,e,q,P,P_{\mathrm{pub}},H_1,H_2\}$。

(2)签名生成算法。用户u_i执行过程为：

(a)选择$r_i\in Z_q^*$，计算$R_i=r_iP$；

(b)计算$h_i=H_2(\text{"0"}\,||\,\mathrm{ID}_i\,||\,m_i\,||\,P_i\,||\,R_i)$和$k_i=(\text{"1"}\,||\,\mathrm{ID}_i\,||\,m_i\,||\,P_i\,||\,R_i)$；

(c)计算$V_i=D_i+h_ir_iP_{\mathrm{pub}}+k_ix_iQ$，输出$u_i$对$m_i$的签名$\sigma_i=(V_i,R_i)$。

(3)签名验证算法。执行以下过程验证签名$\sigma_i=(V_i,R_i)$的合法性：

(a)计算$Q_i=H_1(\mathrm{ID}_i)$，$h_i=H_2(\text{"0"}\,||\mathrm{ID}_i||\,m_i\,||\,P_i\,||\,R_i)$和$k_i=(\text{"1"}\,||\,\mathrm{ID}_i\,||\,m_i\,||\,P_i\,||\,R_i)$；

(b)验证等式是否成立：$e(V_i,P)\stackrel{?}{=}e(Q_i+h_iR_i,P_{\mathrm{pub}})e(k_iP_i,Q)$。

若等式成立则输出真，否则输出假。

4.2 对文献[7]方案的攻击

4.2.1 KGC被动攻击 文献[7]方案与文献[8]方案相似，能够抵抗A_{I}攻击。但是，由于KGC利用主密

钥 s 能够计算 $r_iP_{\text{pub}}=r_isP=sR_i$，并且由于 $V_i=D_i+h_ir_iP_{\text{pub}}+k_ix_iQ$，因此，KGC 通过 r_iP_{pub} 和部分私钥 D_i 能够计算固定值 x_iQ。KGC 利用固定值 x_iQ，r_iP_{pub} 和部分私钥 D_i 能够成功伪造用户 u_i 对任意消息的签名，也可以聚合伪造的单个签名形成伪造的聚合签名。攻击过程如下所述。

(1)捕获签名。KGC通过窃听等方式获得用户 u_i 对 m_i 的签名 $\sigma_i=(V_i,R_i)$。

(2)计算 r_iP_{pub}。由于 KGC 拥有主密钥 s，容易计算 $r_iP_{\text{pub}}=r_isP=sR_i$。

(3)计算固定值 x_iQ。由于 $V_i=D_i+h_isR_i+k_ix_iQ$，同时 $h_i,k_i\in Z_q^*$，则有 $x_iQ=k_i^{-1}(V_i-D_i-h_isR_i)$。

(4)伪造合法签名。由于 $r_iP_{\text{pub}}=r_isP=sR_i$，KGC 任意选择 R_i^*，伪造用户 u_i 对消息 m_i^* 的签名。

(a) 任意选择 $R_i^*\in G_1$，计算 $h_i^*=H_2(\text{"0"}\,||\,\text{ID}_i\,||\,m_i^*\,||\,P_i\,||\,R_i^*)$ 和 $k_i^*=H_2(\text{"1"}\,||\,\text{ID}_i\,||\,m_i^*\,||\,P_i\,||\,R_i^*)$。

(b)计算 $V_i^*=D_i+h_i^*sR_i^*+k_i^*x_iQ$，则 KGC 对 m_i^* 的伪造签名为 $\sigma_i^*=(V_i^*,R_i^*)$。

(5)验证伪造签名 $\sigma_i^*=(V_i^*,R_i^*)$ 的合法性。

(a) 计算 $h_i^*=H_2(\text{"0"}\,||\,\text{ID}_i\,||\,m_i^*\,||\,P_i\,||\,R_i^*)$，$k_i^*=H_2(\text{"1"}\,||\,\text{ID}_i\,||\,m_i^*\,||\,P_i\,||\,R_i^*)$ 和 $Q_i=H_1(\text{ID}_i)$。

(b) 判断签名验证等式是否成立：$e(V_i^*,P)=e(h_i^*R_i^*+Q_i,P_{\text{pub}})e(k_i^*P_i,Q)$。

由于 $e(V_i^*,P)=e(D_i+h_i^*sR_i^*+k_i^*x_iQ,P)=e(sQ_i+h_i^*sR_i^*,P)e(k_i^*Q,x_iP)=e(h_i^*R_i^*+Q_i,P_{\text{pub}})e(k_i^*P_i,Q)$，因此，签名验证等式成立，KGC被动攻击成功。

4.2.2 KGC 主动攻击　文献[11]重新定义了 KGC 的攻击能力，增加了 KGC 主动攻击。KGC 主动攻击是指在系统建立阶段，KGC 选择有利于实现伪造攻击的参数。文献[7]方案不仅存在 KGC 被动攻击，而且存在 KGC 主动攻击。主动攻击过程如下所述。

(1)KGC在系统建立阶段选择特殊的生成元 $Q=tP$，其中 $t\in Z_q^*$。

(2)计算固定值 r_iP_{pub} 和 x_iQ。$r_iP_{\text{pub}}=r_isP=sR_i$，$x_iQ=x_itP=tx_iP=tP_i\,x$。KGC 即使不知道秘密值 x_i 和随机值 r_i，也能够直接计算 r_iP_{pub} 和 x_iQ。

(3)任意伪造签名。选择 $R_i^*\in G_1$，计算 $V_i^*=D_i+h_i^*sR_i^*+k_i^*tP_i$，则 KGC 对 m_i^* 的伪造签名为 $\sigma_i^*=(V_i^*,R_i^*)$。

(4)验证签名的合法性。

由于 $e(V_i^*,P)=e(D_i+h_i^*sR_i^*+k_i^*tP_i,P)=e(D_i+h_i^*sR_i^*,P)e(k_i^*tP_i,P)=e(Q_i+h_i^*R_i^*,P_{\text{pub}})e(k_i^*P_i,Q)$，因此，签名验证等式成立，KGC 主动攻击成功。

5　对文献[8]方案的改进

根据3.2节分析，文献[8]方案中KGC能够计算固定值 x_iU+r_iT，并且由于H_4哈希函数中没有输入项 R_i，KGC利用 R_i 和 x_iU+r_iT 能够伪造用户对任意消息的签名。因此，必须对文献[8]方案进行改进，克服KGC被动攻击。

对文献[8]方案的改进包括两部分：

(1)将 $U=H_2(\theta)$ 和 $T=H_3(\theta)$ 中的 θ 用 P_{pub} 代替，减少用户维护公共状态信息的通信开销。

(2)通过两种方法防止KGC计算 x_iU+r_iT 固定值。一种方法是将元素 R_i 嵌入到H_4哈希函数，并调整 h_i 在 S_i 中的位置。这种改进会增加聚合签名的长度。另一种方法是增加哈希函数H_5，并重新设计 S_i 表达式。这种改进不会增加聚合签名的长度。

5.1 第1类改进方案

以下仅列出改进的内容。

(1)重新定义H_4哈希函数，将元素 R_i 嵌入到H_4中，即 $h_i=H_4(\text{ID}_i\,||\,m_i\,||\,P_i\,||\,R_i)$。

(2)签名生成算法：

(a) 选择 $r_i\in Z_q^*$，计算 $R_i=r_iP$；计算 $U=H_2(P_{\text{pub}})$，$T=H_3(P_{\text{pub}})$，$h_i=H_4(\text{ID}_i\,||\,m_i\,||\,P_i\,||\,R_i)$；

(b)计算 $S_i=D_i+h_ix_i(P_{\text{pub}}+U)+r_iT$，输出签名 $\sigma_i=(S_i,R_i)$。

(3)聚合签名生成算法：输入消息 m_i 的签名 $\{\sigma_i=(S_i,R_i)\}$，$1\le i\le n$，计算：$S=\sum_{i=1}^{n}S_i$，输出聚合签名 $\sigma=(S,R_1,R_2,\cdots,R_n)$。

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

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

(b)验证以下等式是否成立：$e(S,P)\stackrel{?}{=}e\cdot\left(\sum_{i=1}^{n}(Q_i+h_iP_i),P_{\text{Pub}}\right)e\left(U,\sum_{i=1}^{n}h_iP_i\right)e\left(T,\sum_{i=1}^{n}R_i\right)$，若等式成立则输出真，否则输出假。

5.2 第 1 类改进方案性能分析

定理 1　第 1 类改进方案是正确的。

证明　第 1 类改进方案是正确的，当且仅当无证书聚合签名 $\sigma=(S,R_1,R_2,\cdots,R_n)$ 可以通过以下聚合验证等式。

$$\begin{aligned}e(S,P)&=e\left(\sum_{i=1}^{n}S_i,P\right)=e\left(\sum_{i=1}^{n}D_i+h_ix_i(P_{\text{pub}}+U)+r_iT,P\right)\\&=e\left(\sum_{i=1}^{n}(Q_i+h_iP_i),P_{\text{Pub}}\right)\prod_{i=1}^{n}e\left(U,h_iP_i\right)\prod_{i=1}^{n}e\left(T,R_i\right)\\&=e\left(\sum_{i=1}^{n}(Q_i+h_iP_i),P_{\text{Pub}}\right)e\left(U,\sum_{i=1}^{n}h_iP_i\right)e\left(T,\sum_{i=1}^{n}R_i\right)\end{aligned}$$

证毕

定理 2　第 1 类改进方案是安全的。

证明 第1类改进方案的安全性证明过程与原方案的证明过程相似，本节仅列出需要修改的“签名询问”过程和“伪造询问”过程。

(1)定理1中签名询问过程。当B收到A_{I}对$(P_{\mathrm{pub}}, m_i, \mathrm{ID}_i, P_i)$的签名询问时，$B$从表$L_1$~$L_4$中得到对应的值。如果$c_i=1$，$B$选取$R_i\in G_1$，计算$S_i=a_iP_{\mathrm{Pub}}+h_ix_iP_{\mathrm{Pub}}+h_il_iP_i+\beta_iR_i$。如果$c_i=0$，$B$随机选取$r_i,\beta_i\in Z_q^*$，令$T_i=\beta_iP_{\mathrm{pub}}$，计算$R_i=r_iP-\beta_i^{-1}Q_i$，$S_i=r_i\beta_iP_{\mathrm{Pub}}+h_ix_iP_{\mathrm{Pub}}+h_il_iP_i$。返回签名$\sigma=(S_i,R_i)$。

(2)定理1中伪造询问过程。利用以上签名询问，A_{I}获得伪造的聚合签名$\sigma=(S,R_1,R_2,\cdots,R_n)$，要求至少有一个$k\in\{1,\ 2,\cdots,n\}$满足“$A_{\mathrm{I}}$不能对$\mathrm{ID}_k^*$进行部分私钥询问”，并且不能对$(P_{\mathrm{pub}},m_k^*,\mathrm{ID}_k^*,P_k^*)$进行签名询问，令$k$=1。

当B查询表L_1~L_4，获得对应的值。如果$c_1^*\neq 0$，$c_j^*\neq 1(2\le j\le n)$，则B放弃；否则c_1^*=0，c_j^*=1，B可以获得CDH问题的一个实例：$abP=a_1^{*-1}\left(S^*-\beta^*R^*-\sum_{i=1}^n h_i^*l^*P_i^*-h_1^*x_1^*aP-\sum_{i=2}^n(a_i^*+h_i^*x_i^*)aP\right)$。

(3)定理2中签名询问过程。当B收到A_{II}对$(P_{\mathrm{pub}}, m_i, \mathrm{ID}_i, P_i)$进行签名询问时，$B$从表$L_2$~$L_4$和$L$中得到对应值。如果$c_i=1$，$B$已知部分私钥和秘密值，直接使用签名生成算法计算签名$\sigma=(S_i,R_i)$。如果$c_i=1$，B选取$r_i\in Z_q^*$，令$T_i=\beta P_i$，计算$R_i=r_iP-\beta^{-1}h_iH_2(P_{\mathrm{pub}})$，$S_i=r_i\beta_iP_i+sh_iP_i+sH_1(\mathrm{ID}_i)$。$B$返回签名$\sigma=(S_i,R_i)$。

(4)定理2中伪造询问过程。利用以上签名询问，A_{II}获得伪造的聚合签名$\sigma^*=(S^*,R^*)$，要求至少有一个$k\in\{1,2,\cdots,n\}$满足A_{II}不能对ID_k^*进行秘密值询问，并且不能对$(P_{\mathrm{pub}},m_k^*,\mathrm{ID}_k^*,P_k^*)$进行签名询问，不失一般性，令$k=1$。

当B从表L_2~L_4和L中获得对应的值后，检查c_i值。如果$c_1^*\neq 0$，$c_j^*\neq 1(2\le j\le n)$，则B放弃；否则$c_1^*=0$，$c_j^*=1$，B可以获得CDH问题的一个实例：$abP=(x_1^*h_1^*l^*)^{-1}\left(S^*-\sum_{i=1}^n s(Q_i^*+h_i^*P_i^*)-\sum_{i=1}^n\beta^*R_i^*-\sum_{i=2}^n l^*P_i^*\right)$。

第1类改进方案的聚合验证计算开销没有增加，但不足之处是增加了聚合签名的长度，由$2|G_1|$增加为$(n+1)|G_1|$。 证毕

5.3 第 2 类改进方案

第2类改进主要表现在以下几个方面：

(1)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。

(2)修改S_i计算表达式，签名生成算法为：

(a)选择$r_i\in Z_q^*$，计算$R_i=r_iP$；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$k_i=H_5(\mathrm{ID}_i\,||\,m_i\,||\,P_i)$。

(b)计算$S_i=D_i+x_i(h_iP_{\mathrm{pub}}+k_iU)+r_iT$，输出签名$\sigma_i=(S_i,R_i)$。

(3)聚合签名生成算法。输入消息m_i的签名$\{\sigma_i=(S_i,R_i)\}$，$1\le i\le n$。计算：$S=\sum_{i=1}^n S_i$，$R=\sum_{i=1}^n R_i$，输出聚合签名$\sigma=(S,R)$。

(4)聚合验证算法：输入身份列表$\{\mathrm{ID}_i\}$、公钥列表$\{P_i\}$和签名$\sigma=(S,R)$，执行以下验证过程。

(a)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$k_i=H_5(\mathrm{ID}_i\,||\,m_i\,||\,P_i)$。

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

5.4 第 2 类改进方案的性能分析

通过以下聚合验证等式可以证明第 2 类改进方案是正确的。

$$\begin{aligned}e(S,P)&=e\left(\sum_{i=1}^n S_i,P\right)\\&=e\left(\sum_{i=1}^n D_i+x_i(h_iP_{\mathrm{pub}}+k_iU)+r_iT,P\right)\\&=e\left(\sum_{i=1}^n D_i+h_ix_iP_{\mathrm{pub}},P\right)e\left(\sum_{i=1}^n k_ix_iU,P\right)\\&\quad\cdot e\left(\sum_{i=1}^n r_iT,P\right)\\&=e\left(\sum_{i=1}^n(Q_i+h_iP_i),P_{\mathrm{Pub}}\right)e\left(U,\sum_{i=1}^n k_iP_i\right)e(T,R)\end{aligned}$$

第2类改进方案的安全性证明过程与第1类改进方案的证明过程相似，需要修改“签名询问”过程和“伪造询问”过程。第2类改进方案减少了用户维护公共状态信息的通信开销，克服了KGC被动攻击安全性问题，保持签名的聚合验证开销不变，解决了第1类改进方案聚合签名长度与用户人数线性相关的不足。

6 结束语

本文分析文献[7]和文献[8]无证书聚合签名方案的安全性，指出两个方案都存在 KGC 伪造攻击。其中，文献[8]方案存在 KGC 被动攻击，文献[7]方案既存在 KGC 被动攻击，又存在 KGC 主动攻击。同时，分析了 KGC 被动攻击和主动攻击存在的原因，描述了 KGC 对两个方案的伪造攻击过程。最后对文献[8]方案进行了改进，改进方案克服了原方案存在

KGC 被动攻击的不足。运用本文的方法也可以分析文献[13,14]无证书聚合签名方案的安全性，它们同样也存在 KGC 恶意攻击。

基于双线性对的无证书聚合签名方案中，当前最优方案的聚合验证开销是 4 个双线性对，能否减少双线性对个数，提高计算效率，将是设计无证书聚合签名方案需要考虑的问题。

参 考 文 献

[1] Alriyami S S and Paterson K G. Certificateless public key cryptography[C]. Proceedings of the Cryptology-Asiacrypt, Taipei, China, 2003: 452–474.

[2] Liu Jing-wei, Zhang Zong-hua, and Chen Xiao-feng. Certificateless remote anonymous authentication schemes for wireless body area networks[J]. *IEEE Transactions on Parallel & Distributed Systems*, 2014, 25(2): 332–342.

[3] 光焱, 顾纯祥, 祝跃飞, 等. 一种基于 LWE 问题的无证书全同态加密体制[J]. 电子与信息学报, 2013, 35(4): 988–993.
Guang Yan, Gu Chun-xiang, Zhu Yue-fei, *et al.*. Certificateless fully homomorphic encryption based on LWE problem[J]. *Journal of Electronics & Information Technology*, 2013, 35(4): 988–993.

[4] Zhang Lei, Wu Qian-hong, Josep Domingo-Ferrerc, *et al.*. Signatures in hierarchical certificateless cryptography: efficient constructions and provable security[J]. *Information Sciences*, 2014, 272: 223–237.

[5] Boneh D, Gentry C, Lynn B, *et al.*. Aggregate and verifiably encrypted signatures from bilinear maps[C]. Proceedings of the Cryptology-Eurocrypt, Warsaw, Poland, 2003: 416–432.

[6] Xiong Hu, Guan Zhi, Chen Zhong, *et al.*. An efficient certificateless aggregate signature with const pairing computations[J]. *Information Sciences*, 2013, 219: 225–235.

[7] He De-biao, Tian Miao-miao, and Chen Jian-hua. Insecurity of an ef cient certi cateless aggregate signature with constant pairing computations [J]. *Information Sciences*, 2014, 268: 458–462.

[8] 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.
Ming Yang, Zhao Xiang-mo, and Wang Yu-ming. Certificateless aggregate signature scheme[J]. *Journal of University of Electronic Science and Technology of China*, 2014, 43(2): 188–193.

[9] Gong Zheng, Long Yu, Hong Xuan, *et al.*. Two certificateless aggregate signatures from bilinear maps [C]. Proceedings of Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Qingdao, China, 2007: 188–193.

[10] Zhang Lei and Zhang Fu-tai. A new certificateless aggregation signature shceme[J]. *Computer Communications*, 2009, 32(6): 1079–1085.

[11] Au Man-ho, Mu Yi, Chen Jing,*et al.*. Malicious KGC attack in certificateless cryptography[C]. Proceedings of the ASIACCS2007, New York, USA, 2007: 302–311.

[12] 张福泰, 孙银霞, 张磊, 等. 无证书公钥密码体制研究[J]. 软件学报, 2011, 22(6): 1316–1332.
Zhang Fu-tai, Sun Yin-xia, Zhang Lei, *et al.*. Research on certificateless public key cryptography [J]. *Journal of Software*, 2011, 22(6): 1316–1332.

[13] 喻琇瑛, 何大可. 一种新的无证书聚合签名[J]. 计算机应用研究, 2014, 31(8): 2485–2487.
Yu Xiu-ying and He Da-ke. New certificateless aggregate signature scheme [J]. *Application Research of Computers*, 2014, 31(8): 2485–2487.

[14] 侯红霞,张雪锋,董晓丽. 改进的无证书聚合签名方案[J].山东大学学报(理学版), 2013, 48(9): 29–34.
Hou Hong-xia, Zhang Xue-feng, and Dong Xiao-li. Improved certificateless aggregate signature scheme[J]. *Journal of Shandong University* (*Natural Science*), 2013, 48(9): 29–34.

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.

李臣意：　男，1989 年生，硕士，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.

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.