DOI:10.13471/j.cnki.acta.snus.2017.01.013

无证书聚合签名方案的攻击与改进*

杜红珍[1]，温巧燕[2]
（1. 宝鸡文理学院数学与信息科学学院，陕西 宝鸡 721013；
2. 北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘 要：聚合签名因其在物联网中的广泛应用而成为数字签名技术研究的热点。Ming 等（2014）提出了一个高效的无证书聚合签名方案，但 Zhang 等（2015）指出 Ming 方案不能抵抗类型 II 敌手的攻击，并给出了 Ming 方案的 2 种改进。指出 Zhang 等的第二个改进方案是不安全的，通过构造具体的攻击方法，证明了第二个方案无法抵抗类型 II 敌手的攻击。接着基于 Ming 方案构造了一个新的无证书聚合签名方案，在随机预言机模型下证明了新方案是安全的，且方案生成的聚合签名长度是固定的，很适合于物联网应用环境。

关键词：无证书公钥密码；聚合签名；不可伪造性
中图分类号：TP309 **文献标志码**：A **文章编号**：0529－6579（2017）01－0077－08

Attack and improvement of a certificateless aggregate signature scheme

DU Hongzhen[1], *WEN Qiaoyan*[2]
（1. School of Mathematics and Information Science, Baoji University of Arts and Sciences, Baoji 721013, China;
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China）

Abstract: Aggregate signature becomes a hot topic in the digital signature technology researches because of its wide application in the Internet of Things. Ming et al. (2014) proposed an efficient certificateless aggregate signature scheme. But Zhang et al. (2015) showed the scheme is not secure against a Type II adversary, and then they proposed an improvement of Ming's scheme. However, it is pointed out that the improved scheme is still insecure against a Type II adversary by giving specific attacks. Then, based on Ming's scheme, a new certificateless aggregate signature scheme is constructed. The new scheme is provably-secure in the random oracle model and the length of aggregate signature is constant so that it is suitable for the Internet of Things.

Key words: certificateless public key cryptography; aggregate signature; unforgeability

数字签名可以在电子数据传输中提供认证性、完整性和不可否认性等安全服务，是信息安全的核心技术之一。随着新的网络形态及网络服务的出现，研究带有特殊性质的数字签名及其应用成为密码学热点之一[1－4]。聚合签名是一种特殊的数字签名，它被广泛应用于如射频识别（Radio Frequency Identification，RFID）技术、WSN（Wireless Sensor Networks，WSN）数据融合、云计算和分布式系统等诸多领域。无证书聚合签名（Certificateless Aggregate Signature，CLAS）是无证书公钥密码系统

* **收稿日期**：2016－05－06
基金项目：国家自然科学基金（61402015，61402275）；陕西省教育厅专项科研计划项目（15JK1022）；陕西省自然科学基础研究计划项目（2015JM6263）
作者简介：杜红珍（1978 年生），女；**研究方向**：密码学、数字签名；E－mail：hongzhendu@163.com

中的聚合签名。CLAS 与传统基于 PKI 的聚合签名和基于身份的聚合签名相比，它不需要公钥证书的支持，避免了因维护公钥证书带来的巨大的计算、通信与存储成本，同时又不存在密钥托管问题，保护了用户的隐私。所以，研究无证书聚合签名更有理论意义和实际应用价值。

目前对无证书聚合签名研究典型的如文献[3，5－16]。在文献［5］中，Gong 等基于双线性对构造了两个新颖的无证书聚合签名方案，但这两个方案实施因需要大量双线性对运算导致效率低。2009 年，Zhang 等[6]提出了一个新的无证书聚合签名方案，但生成的聚合签名的长度依赖于签名人数，签名验证需计算（$n+3$）个双线性对。2011 年，Xiong 等[7]提出了一个无证书聚合签名方案并应用到移动计算中，但文献［8］指出该方案是可以普遍伪造的。同年，Yanai 等[9]提出了一个无证书有序聚合签名方案。2013 年，杜红珍等人[11]利用双线性对提出一个无证书聚合签名方案，聚合签名的长度可以压缩到 320 bits。同年，Xiong 等[12]提出了一个无证书聚合签名方案，但 He 等[13]和 Cheng 等[14]分别指出 Xiong 方案在类型 II 敌手攻击下是不安全的，同时在文献［14］中，Chen 等还提出了 Xiong 方案的一个改进，但改进方案生成的聚合签名长度随签名人数增加而增长。2014 年，明洋等[15]基于双线性对提出了一个有固定长度的高效的无证书聚合签名方案（简称 Ming 方案），但张玉磊等[16]指出 Ming 方案不能抵抗类型 II 敌手 KGC（Key Generation Center）的被动攻击，接着张玉磊等基于 Ming 方案提出了 2 个改进方案，第一个改进方案经证明是安全的，唯一不足就是生成的聚合签名的长度随签名人数的增加呈线性增长，不适合用于资源受限的无线网络环境，第 2 个改进方案的聚合签名长度是固定的，但作者没有给出安全性证明。本文指出张玉磊的第 2 个改进方案（简称 Zhang 方案）是不安全的，方案仍然不能抵抗 KGC 的被动攻击，最后，本文基于 Ming 方案提出了一个新的有固定长度的无证书聚合签名方案，并在随机预言机模型下证明了新方案是安全的。

1 CLAS 的定义和安全模型

定义 1 一个 CLAS 方案由 KGC，n 个签名用户 $P_i(i=1,2,\cdots,n)$，聚合签名器和验证者构成。方案由以下 6 个算法构成[6]：

-MasterKeyGen：输入安全参数 k，输出系统参数 *params* 和系统主密钥 s。

-PartialKeyGen：输入用户 $P_i(i=1,2,\cdots,n)$ 的的身份符号 ID_i，*params* 和 s，输出 P_i 的部分私钥 d_{IDi}。

-UserKeyGen：由 $P_i(i=1,2,\cdots,n)$ 执行，输入 *params* 和 $P_i(i=1,2,\cdots,n)$ 的 ID_i，输出秘密值 x_i（x_i 由 P_i 选取）和公钥 pk_{IDi}。

-CL-Sign：由 $P_i(i=1,2,\cdots,n)$ 执行（简便起见，本文假设 P_i 要签名的消息为 m_i），输入 *params*，ID_i，d_{IDi}，x_i，pk_{IDi} 和消息 m_i，输出签名 σ_i。

-Aggregate：由聚合签名器执行，输入 n 个有效的身份－消息－公钥－签名对 $(ID_i,m_i,pk_{IDi},\sigma_i)$ $(1\leqslant i\leqslant n)$，输出这 n 个签名 σ_i 的聚合签名 σ。

-AggregateVerify：输入 *params*，n 个有效的身份－消息－签名对 (ID_i,m_i,pk_{IDi}) $(1\leqslant i\leqslant n)$ 及聚合签名 σ，输出该聚合签名有效或无效。

CLAS 的安全模型

CLAS 方案存在两种类型的敌手 A_I 和 A_{II}：1）敌手 A_I：A_I 不知道系统主密钥和目标用户的部分私钥，但可以替换任意用户的公钥，一般 A_I 模拟的是一个恶意的用户。2）敌手 A_{II}：A_{II}知道系统主密钥，但不能替换目标用户的公钥，A_{II}模拟的是一个恶意但被动的 KGC。

定义 2 在 CLAS 方案中，如果存在两类敌手 A_I、A_{II}在以下 Game 中获胜的概率是可以忽略的，则称该 CLAS 方案在适应性选择消息攻击下是存在性不可伪造的。

Game

Game 中涉及一个挑战者 X 和一个敌手 A（$A\in\{A_I,A_{II}\}$），X 输入 k，运行算法 Setup 产生系统主密钥 s 和系统参数 *params*，如果 A 是第一类敌手 A_I，则 X 发送 *params* 给 A，秘密保存 s。如果 A 是第二类敌手 A_{II}，则发送 s 和 *params* 给 A。

A 询问以下预言机：

-Partial-Private-Key-Extract 询问：A 可以询问用户 ID_i 的部分私钥，X 生成部分私钥 d_{IDi}，返回该值给 A。

-Secret-Value 询问：A 可以查询 ID_i 的秘密值，X 返回秘密值 x_i给 A，若 ID_i 的公钥已被替换，则输出“$\perp$”。

-Public-Key 询问：当 A 查询 ID_i 的公钥时，X 产生 ID_i 的公钥 pk_{IDi}，返回给 A。

-Replace-Public-Key 询问：对任意 ID_i，A 能用自己选取的 pk_{IDi}'代替 ID_i 的 pk_{IDi}（该询问仅针对

A_I）。

-CL-Sign 询问：输入消息 m_i，ID_i 和 pk_{IDi}，X 生成签名 σ_i，返回 σ_i 给 A。

最后，$A_{输}$出 1 个有效的消息－身份－公钥－聚合签名（m_i*，ID_i*，$pk_{IDi}*$，$\sigma*$）（$1 \leqslant i \leqslant n$），且满足以下 2 个条件，则 A 获胜：

1）如果 A 是第一类敌手 A_I，至少有一个 $ID_I* \in \{ID_1*, ID_2*, \cdots, ID_n*\}$ 没有既提交给 Replace-Public-Key 预言机又同时提交给 Partial-Private-Key-Extract 预言机。如果 $A = A_{II}$，至少有一个 $ID_I* \in \{ID_1*, ID_2*, \cdots ID_n*\}$ 没有提交 Secret-Value 预言机。

2）（m_I*，ID_I*）没有提交 CL-Sign 询问。

2　Ming 方案及安全性分析

2.1　Ming 方案

该方案[15]由 6 个算法｛MasterKeyGen，PartialKeyGen，UserKeyGen，CL-Sign，Aggregate，AggregateVerify｝构成，具体如下：

-MasterKeyGen：k 为安全参数，G_1 和 G_2 分别为 $q > 2^k$ 阶的循环加法和乘法群，P 是群 G_1 的 1 个生成元，一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$，选随机数 $s \in Z_q*$ 作为系统主密钥，计算 $P_{pub} = sP$。4 个安全 Hash 函数 $H_1, H_2, H_3: \{0,1\}^* \rightarrow G_1$，$H_4: \{0,1\}^* \rightarrow Z_q^*$。则系统公开参数 $params$：$\{G_1, G_2, q, P, e, P_{pub}, H_1, H_2, H_3, H_4\}$。主密钥 s 需秘密保存。

-PartialKeyGen：给定用户 P_i 的身份 ID_i，KGC 计算该用户的部分私钥 $D_i = sQ_i$，其中 $Q_i = H_1(ID_i)$。-UserKeyGen：用户 ID_i 选随机数 $x_i \in \mathbf{Z}_q^*$ 作为秘密值，计算其公钥 $pk_i = x_iP$。

-CL-Sign：给定消息 m_i，部分私钥 D_i，秘密值 x_i，用户身份 ID_i 及公钥 pk_i，签名者随机选取一个状态信息 θ，生成签名如下：

（i）选随机数 $r_i \in \mathbf{Z}_q^*$，计算 $R_i = r_iP$；

（ii）令 $U = H_2(\theta), T = H_3(\theta)$，$h_i = H_4(\theta, m_i, ID_i, pk_i)$；

（iii）计算 $S_i = D_i + x_i(h_iP_{pub} + U) + r_iT$。

则在消息 m_i 上的签名为 $\sigma_i = (R_i, S_i)$。

-Aggregate：给定 n 个消息/签名对 (m_i, σ_i)（$i = 1,2,\cdots,n$），聚合签名器计算 $R = \sum_{i=1}^{n} R_i, S = \sum_{i=1}^{n} S_i$，输出聚合签名 $\sigma = (R, S)$。

-AggregateVerify：输入消息 $m_1, m_2, \cdots m_n$，共同的状态信息 θ 及在这 n 个消息上的聚合签名 $\sigma = (R, S)$，验证者计算如下：

（i）计算 $U = H_2(\theta), T = H_3(\theta)$，$h_i = H_4(\theta, m_i, ID_i, pk_i)$，$Q_i = H_1(ID_i)$，$i = 1,2,\cdots,n$；

（ii）验证等式

$$e(S,P) = e\left(\sum_{i=1}^{n} Q_i + \sum_{i=1}^{n} h_i pk_i, P_{pub}\right) \cdot e\left(U, \sum_{i=1}^{n} pk_i\right) e(T,R)$$

是否成立，如果成立则接受签名，否则签名无效。

2.2　Zhang 等对 Ming 方案的改进

Zhang 等在文献［16］中指出 Ming 方案存在 KGC 的被动攻击，即在 KGC 的攻击下聚合签名是可以普遍伪造的（Zhang 提出的攻击方法详见文献［16］）。接着，Zhang 等对 Ming 方案进行了 2 种改进，经证明第一种改进方案是安全的，但不足是生成的聚合签名的长度由原来的固定长度 $2 \mid G_1 \mid$ 变成了 $(n+1) \mid G_1 \mid$，签名传输代价大大提高，降低了原方案的优势。为了弥补此缺陷，Zhang 等[16]又提出了 Ming 方案的第二种改进（简称 Zhang 方案），下面仅列出 Zhang 方案改变过的算法，其余算法不变。具体描述如下：

-MasterKeyGen：该算法增加了 1 个 Hash 函数 $H_5: \{0,1\}* \rightarrow Z_q^*$，其他参数不变。

-CL-Sign：给定消息 m_i，部分私钥 D_i，秘密值 x_i，用户身份 ID_i 及公钥 pk_i，签名者生成签名如下：

（i）选随机数 $r_i \in \mathbf{Z}_q^*$，计算 $R_i = r_iP$；

（ii）令 $U = H_2(P_{pub}), T = H_3(P_{pub})$，$h_i = H_4(m_i, ID_i, pk_i)$，$k_i = H_5(m_i, ID_i, pk_i)$；

（iii）计算 $S_i = D_i + x_i(h_iP_{pub} + k_iU) + r_iT$，则在消息 m_i 上的签名为 $\sigma_i = (R_i, S_i)$。

-Aggregate：给定 n 个消息/签名对 (m_i, σ_i)（$i = 1,2,\cdots,n$），聚合签名生成器计算 $R = \sum_{i=1}^{n} R_i, S = \sum_{i=1}^{n} S_i$，输出聚合签名 $\sigma = (R, S)$。

-AggregateVerify：输入消息 $m_1, m_2, \cdots, m_n$ 及在这 n 个消息上的聚合签名 $\sigma = (R, S)$，验证者计算如下：

（i）计算 $U = H_2(P_{pub}), T = H_3(P_{pub}), h_i = H_4(m_i, ID_i, pk_i), k_i = H_5(m_i, ID_i, pk_i), Q_i = H_1(ID_i), i = 1,2,\cdots,n$；

（ii）验证等式

$$e(S,P) = e\left(\sum_{i=1}^{n} (Q_i + h_i pk_i), P_{pub}\right) \cdot$$

$$e(U,\sum_{i=1}^{n}k_i\cdot pk_i)e(T,R)$$

是否成立，如果成立则接受签名，否则签名无效。

注 1 Zhang 等通过在 CL-Sign 算法中增加 $k_i = H_5(m_i,ID_i,pk_i)$ 来抵抗 KGC 的攻击，但这种改进仍然不能保证签名方案的安全性，下面我们对 Zhang 方案进行攻击。

2.3 对 Zhang 方案的攻击

本文指出 Zhang 方案不能抵抗 KGC 的攻击，具体攻击如下：

设用户 P_i（$i=1,2,\cdots,n$）的身份/公钥为 ID_i/pk_i，KGC（知道系统主密钥 s 及用户部分私钥 $D_i = sQ_i$）截获用户 P_i 的一个消息/签名对（m_i，$\sigma_i = (R_i,S_i)$）后，计算：

（i）计算 Hash 值 $h_i = H_4(m_i,ID_i,pk_i)$ 和 $k_i = H_5(m_i,ID_i,pk_i)$；

（ii）计算 $w_i = S_i - D_i - h_i\cdot s\cdot pk_i = k_ix_iU + r_iT$；

即 KGC 可以求出值 $k_ix_iU + r_iT$。接下来，KGC 使用该值可以冒充用户 P_i 对任意消息 m_i* 伪造签名如下：

-CL-Sign：

（i）对消息 m_i*，计算

$h_i^* = H_4(m_i^*,ID_i,pk_i)$，$k_i^* = H_5(m_i^*,ID_i,pk_i)$；

（ii）计算 $R_i* = \frac{k_i^*}{k_i}R_i$（$= \frac{k_i^*}{k_i}r_iP$），$w_i* = \frac{k_i^*}{k_i}w_i$，$S_i* = D_i + h_i^*s\cdot pk_i + w_i^*$。

则在消息 m_i* 上的签名为 $\sigma_i* = (R_i*,S_i*)$。

如果 KGC 要伪造 n 个签名人 P_i 在 n 个消息/签名 (m_i*,σ_i*)（$i=1,2,\cdots,n$）上的聚合签名，则计算 $R* = \sum_{i=1}^{n}R_i*$，$S* = \sum_{i=1}^{n}S_i*$，输出聚合签名 $\sigma* = (R*,S*)$。

-AggregateVerify：

给定系统公开参数 *params*，身份/公钥对（ID_i，pk_i），$i=1,2,\cdots,n$，消息/签名对（$(m_1*,m_2*,\cdots,m_n*)$，$\sigma* = (R*,S*)$），验证者计算如下：

（i）计算 $U = H_2(P_{pub})$，$T = H_3(P_{pub})$，$h_i^* = H_4(m_i^*,ID_i,pk_i)$，$k_i^* = H_5(m_i^*,ID_i,pk_i)$，$Q_i = H_1(ID_i)$，$i=1,2,\cdots,n$；

（ii）验证等式

$$e(S*,P) = e(\sum_{i=1}^{n}(Q_i + h_i^*pk_i),P_{pub})\cdot e(U,\sum_{i=1}^{n}k_i^*\cdot pk_i)e(T,R*)$$

是否成立，如果成立则接受签名，否则签名无效。

显然，伪造的聚合签名 $\sigma* = (R*,S*)$ 有效，因为

$$e(S*,P) = e(\sum_{i=1}^{n}S_i*,P) =$$

$$e(\sum_{i=1}^{n}(D_i + h_i^*s\cdot pk_i + w_i^*),P) =$$

$$e(\sum_{i=1}^{n}(Q_i + h_i*pk_i),sP)e(\sum_{i=1}^{n}w_i^*,P) =$$

$$e(\sum_{i=1}^{n}(Q_i + h_i*pk_i),sP)\cdot e(\sum_{i=1}^{n}\frac{k_i^*}{k_i}(k_ix_iU + r_iT),P)) =$$

$$e(\sum_{i=1}^{n}(Q_i + h_i*pk_i),P_{pub})\cdot e(\sum_{i=1}^{n}(k_i^*x_iU + \frac{k_i^*}{k_i}r_iT),P)) =$$

$$e(\sum_{i=1}^{n}(Q_i + h_i^*pk_i),P_{pub})\cdot e(U,\sum_{i=1}^{n}k_i^*\cdot pk_i)e(T,R^*)$$

所以，本文指出 Zhang 方案在类型 II 敌手 KGC 的攻击下仍是不安全的，接下来我们基于 Ming 方案构造了一个新的无证书聚合签名方案，该方案不仅可以抵抗两种类型 I，II 的敌手攻击，且生成的聚合签名长度是固定的。

3 一个新的无证书聚合签名方案

3.1 基本方案

本文方案由算法｛MasterKeyGen，PartialKeyGen，UserKeyGen，CL-Sign，Aggregate，AggregateVerify｝构成，下面仅给出与 Ming 方案中不同的算法：

-CL-Sign：给定消息 m_i，部分私钥 D_i，秘密值 x_i，用户身份 ID_i 及公钥 pk_i，签名者生成签名如下：

（i）选随机数 $r_i\in\mathbf{Z}_q^*$，计算 $R_i = r_iP$；

（ii）计算 $U_i = H_2(m_i,ID_i,pk_i)$，$T = H_3(P_{pub})$，$h_i = H_4(m_i,ID_i,pk_i)$；

（iii）计算 $S_i = h_iD_i + x_iU_i + r_iT$，则在消息 m_i 上的签名为 $\sigma_i = (R_i,S_i)$。

-Aggregate：计算 $R = \sum_{i=1}^{n}R_i$，$S = \sum_{i=1}^{n}S_i$，输出聚合签名 $\sigma = (R,S)$。

-AggregateVerify：输入消息 $m_1,m_2,\cdots,m_n$ 及在这 n 个消息上的聚合签名 $\sigma=(R,S)$，验证者计算如下：

（i）计算 $U_i=H_2(m_i,ID_i,pk_i)$，$T=H_3(P_{pub})$，$h_i=H_4(m_i,ID_i,pk_i)$，$Q_i=H_1(ID_i)$，$i=1,2,\cdots,n$；

（ii）验证等式

$$e(S,P)=e(\sum_{i=1}^{n}h_iQ_i,P_{pub})\cdot\prod_{i=1}^{n}e(U_i,pk_i)e(T,R)$$

是否成立，如果成立则接受签名，否则签名无效。

注 2　为了不增加聚合签名的长度，则在 CL-Sign 算法中就不能将 $R_i=r_iP$ 嵌入到 Hash 函数 H_4 中，但这样又无法阻止 Zhang 或本文提出的攻击，所以只有将消息 m_i 嵌入到 Hash 函数 H_2 中，实质上 $x_iU_i=x_iH_2(m_i,ID_i,pk_i)$ 就是一个 BLS 短签名，KGC 没有用户的秘密值 x_i，自然无法伪造签名，当然考虑到类型 I 敌手的存在，所以签名算法增加了随机数 r_i，做了上述设计。

3.2　新方案的性能分析

3.2.1　安全性

定理 1　在随机预言机模型和计算 Diffie-Hellman 困难假设下，改进 CLAS 方案在适应性选择消息攻击下是存在性不可伪造的（EUF-CLAS-CMA）。

补　计算 Diffie-Hellman 问题（CDH 问题）

给定 P，aP，$bP\in G_1$（a，$b\in Z_q*$ 是未知的随机数），计算 $abP\in G_1$。

定理 1 的证明由下面的引理 1 和引理 2 得出。

引理 1　在随机预言机模型下，假定敌手 A_1 在时间 t 内以不可忽略的优势 ε 攻破了本文方案，记 A_1 访问 H_1 预言机，Partial-Private-Key-Extract 预言机，Public-Key 预言机，CL-Sign 预言机的次数分别为 q_{H_1}，q_E，q_{pk}，q_S，则存在一个算法 X，以 $\varepsilon'\geqslant\varepsilon\left(1-(\frac{q_{H_1}}{q_{H_1}+1})^n\right)\left(\frac{q_{H_1}}{q_{H_1}+1}\right)^{q_E+q_S}$ 的优势，在时间 $t'<t+(q_{H_1}+q_E+q_{pk}+3q_S+2n+2)t_{sm}+t_{inv}$ 内解决 *CDH* 难题，t_{sm}是计算群上 1 个标量乘的时间，t_{inv}是 Z_q* 上 1 个求逆的时间。

证明　设 (aP,bP) 是 G_1 群上 *CDH* 问题的一个任意实例，挑战者 X 将与敌手 A_1 进行以下 Game：

X 定义系统公钥 $P_{pub}=aP$，生成系统参数 params：$\{k,e,G_1,G_2,P,P_{pub},H_1\sim H_4\}$，发送 params 给 A_1，A_1 执行以下查询：

- H_1 查询：X 维护 1 个列表 L_1：(ID_i,Q_i,t_i,c)，当 A_1 查询 $ID_i(1\leqslant i\leqslant q_{H_1})$ 的 Hash 值时，X 调出 L_1，若 L_1 中有数据 (ID_i,Q_i,t_i,c)，则输出 Q_i。否则 X 选随机数 $t_i\in\mathbf{Z}_q^*$，抛掷偏心硬币 $c\in\{0,1\}$（$\Pr[c=0]=\frac{q_{H_1}}{q_{H_1}+1}$，$\Pr[c=1]=\frac{1}{q_{H_1}+1}$），若 $c=0$，定义 $Q_i=t_iP$，否则 $Q_i=t_i(bP)$，添加 (ID_i,Q_i,t_i,c) 到 L_1 中，返回 Q_i 给 A_1。

- H_2，H_4 查询：当 A_1 输入 (m_i,ID_i,pk_i) 查询 $H_2(m_i,ID_i,pk_i)$ 和 $H_4(m_i,ID_i,pk_i)$ 值时，X 调出列表 L_2，若 L_2 中有对应数据 $(m_i,ID_i,pk_i,l_i,l_iP,h_i)$，则输出 l_iP 和 h_i，否则随机选 $l_i,h_i\in\mathbf{Z}_q^*$，定义 $H_2(m_i,ID_i,pk_i)=U_i=l_iP$，$H_4(m_i,ID_i,pk_i)=h_i$，添加 $(m_i,ID_i,pk_i,l_i,l_iP,h_i)$ 到 L_2 中，输出 l_iP 和 h_i。

- H_3 查询：当 A_1 查询 P_{pub} 的 Hash 值时，X 输出以前定义的值。否则选随机数 $j\in\mathbf{Z}_q^*$，定义 $T=H_3(P_{pub})=jP$，输出 T，添加 (P_{pub},j,T) 到 L_3中。

-Partial-Private-Key-Extract 查询：给定 ID_i，X 从 L_1 中调出相应的记录 (ID_i,Q_i,t_i,c)，若 $c=1$，则输出“failure”。否则，计算 $D_i=t_i(aP)$，添加 (ID_i,D_i) 到列表 E^{list} 中，返回 D_i。

-Public-Key 查询：当 A_1 输入用户 ID_i 的公钥，X 随机选 $x_i\in\mathbf{Z}_q^*$，计算 $pk_i=x_iP$，返回 pk_i 给 A_1，添加 (ID_i,x_i,pk_i) 到 pk^{list} 中。

-Secret-Value 查询：当询问 ID_i 的秘密值时，X 调出 pk^{list}，返回以前定义值。否则随机选 $x_i\in\mathbf{Z}_q^*$，计算 $pk_i=x_iP$，返回 x_i 给 A_1，添加 (ID_i,x_i,pk_i) 到 pk^{List}中。如果 ID_i 的公钥被替换，则输出“$\perp$”。

-Replace-Public-Key 查询：当 A_1 输入 (ID_i,pk_i') 时，X 添加 $(ID_i,\perp,pk_i')$ 到 pk^{List}中。

-CL-Sign 查询：当 A_1 输入消息－身份－公钥 (m_i,ID_i,pk_i) 进行签名查询时，X 调出列表 L_1，L_2，L_3，找出相应的记录 (ID_i,Q_i,t_i,c)，$(m_i,ID_i,pk_i,l_i,l_iP,h_i)$ 和 (P_{pub},j,T)，若 $c=0$，X 任选群元素 $R_i\in G_1$，计算 $S_i=h_it_i(aP)+l_ipk_i+jR_i$，返回 (R_i,S_i) 给 A_1，否则 X 停止并输出“failure”。

最后，A_1 停止模拟，输出 1 个有效的在 n（$\leqslant q_{H1}$）个消息－身份－公钥 (m_i*,ID_i*,pk_i*)（$1\leqslant i\leqslant n$）上的聚合签名 $(R*,S*)$。X 调出列表 L_1，找出相应的 n 个记录 $(ID_i*,$

$Q_i*, t_i*, c*)(1 \leqslant i \leqslant n)$，如果这 n 个记录中所有 $c* = 0$ 则失败。否则只要有 1 个 $c* = 1$ 就可以成功计算出 abP 值：

假设是 $(ID_I*, Q_I*, t_I*, c*)$ 中的 $c* = 1$，X 在列表 L_2 中找出 $(m_i^*, ID_i^*, pk_i^*, l_i^*, l_i^* P, h_i^*)$，在列表 L_3 中找出 (P_{pub}, j, T) $(1 \leqslant i \leqslant n)$，根据等式：

$$e(S^*, P) = e(\sum_{i=1}^{n} h_i^* Q_i^*, P_{pub}) \cdot \prod_{i=1}^{n} e(U_i^*, pk_i^*) \cdot e(T, R^*),$$

$$e(S^*, P) = e\Big(\sum_{i=1, i\neq I}^{n} h_i^* t_i^* P + h_I^* t_I^* (bP), aP\Big) \prod_{i=1}^{n} e(l_i^* P, pk_i^*) \cdot e(jP, R^*),$$

$$e(S^*, P) = e\Big(\sum_{i=1, i\neq I}^{n} h_i^* t_i^* P + h_I^* t_I^* (bP), aP\Big) e(P, \sum_{i=1}^{n} l_i^* pk_i^*) \cdot e(jP, R^*)$$

从而可求出

$$abP = (h_I^* t_I^*)^{-1} \cdot \Big(S^* - \sum_{i=1, i\neq I}^{n} h_i^* t_i^* (aP) - \sum_{i=1}^{n} l_i^* pk_i^* - jR^*\Big)$$

X 能求出 abP 值，即解决了 CDH 难题。但目前 CDH 问题是困难的，所以得出本文方案在 A_1 攻击下是安全的。

引理 2 在随机预言机模型下，假定敌手 A_2 在时间 t 内以不可忽略的优势 ε 攻破了本文方案，记 A_2 访问 H_1 预言机，Partial-Private-Key-Extract 预言机，Public-Key 预言机，CL-Sign 预言机的次数分别为 q_{H_1}，q_E，q_{pk}，q_S，则存在一个算法 X，以 $\varepsilon' \geqslant \varepsilon\Big(1 - (\frac{q_{H_1}}{q_{H_1}+1})^n\Big)\Big(\frac{q_{H_1}}{q_{H_1}+1}\Big)^{q_{pk}+q_S}$ 的优势，在时间 $t' < t + (q_{H_1} + q_E + q_{pk} + 2q_S + 2n + 1)t_{sm} + t_{inv}$ 内解决 CDH 问题。

证明 引理 2 的证明与引理 1 的相似，下面仅给出与引理 1 不同的预言机查询。

设 (aP, bP) 是 G_1 群上 *CDH* 问题的一个任意实例，挑战者 X 将与敌手 A_2 进行以下 Game：

X 定义系统公钥 $P_{pub} = sP$，生成系统参数 params：$\{k, e, G_1, G_2, P, P_{pub}, H_1 \sim H_4\}$，发送 params 和系统主密钥 s 给 A_2，A_2 执行以下查询：

$-H_1$ 查询：当 A_2 查询 $ID_i (1 \leqslant i \leqslant q_{H_1})$ 的 Hash 值时，X 调出列表 L_1，若 L_1 中有数据 (ID_i, Q_i, t_i)，则输出 Q_i。否则 X 选随机数 $t_i \in \mathbf{Z}_q^*$，定义 $Q_i = t_i P$，添加 (ID_i, Q_i, t_i) 到 L_1 中，返回 Q_i 给 A_1。

$-H_2$，H_4 查询：当 A_1 输入 (m_i, ID_i, pk_i) 查询 $H_2(m_i, ID_i, pk_i)$ 和 $H_4(m_i, ID_i, pk_i)$ 值时，X 随机选 $l_i, h_i \in \mathbf{Z}_q^*$，定义 $H_2(m_i, ID_i, pk_i) = U_i = l_i(aP)$，$H_4(m_i, ID_i, pk_i) = h_i$，添加 $(m_i, ID_i, pk_i, l_i, l_i(aP), h_i)$ 到 L_2 中，输出 l_i (aP) 和 h_i。

-Public-Key 查询：当询问 ID_i 的秘密值时，X 调出列表 pk^{list}，返回以前定义的秘密值。否则抛掷一个偏心硬币 $c \in \{0, 1\}$ $\Big(\Pr[c=0] = \frac{q_{H_1}}{q_{H_1}+1}, \Pr[c=1] = \frac{1}{q_{H_1}+1}\Big)$，若 $c=0$，随机选 $x_i \in \mathbf{Z}_q^*$，令 $pk_i = x_i P$，否则定义 $pk_i = x_i(bP)$，返回 pk_i 给 A_2，添加 (ID_i, x_i, pk_i, c) 到 pk^{List} 中。

-Secret-Value 查询：当询问 ID_i 的秘密值时，X 调出 pk^{list}，若 $c=0$，返回 x_i，否则输出“⊥”。

-CL-Sign 查询：当 A_2 输入消息 - 身份 - 公钥 (m_i, ID_i, pk_i) 进行签名查询时，X 调出列表 L_1，L_2，L_3 和 pk^{List}，找出相应的记录 (ID_i, Q_i, t_i)，$(m_i, ID_i, pk_i, l_i, l_i(aP), h_i)$，$(P_{pub}, j, T)$，$(ID_i, x_i, pk_i, c)$，若 $c=0$，X 任选群元素 $R_i \in G_1$，计算 $S_i = h_i t_i (sP) + x_i l_i (aP) + jR_i$，返回 (R_i, S_i) 给 A_2，否则 X 停止并输出“failure”。

最后，A_2 停止模拟，输出 1 个有效的在 n $(\leqslant q_{H1})$ 个消息 - 身份 - 公钥 (m_i*, ID_i*, pk_i*) $(1 \leqslant i \leqslant n)$ 上的聚合签名 $(R*, S*)$。X 调出列表 pk^{List}，找出相应的 n 个记录 $(ID_i^*, x_i^*, pk_i^*, c^*)$ $(1 \leqslant i \leqslant n)$，如果这 n 个记录中所有 $c* = 0$ 则失败。否则只要有 1 个 $c* = 1$ 就可以成功计算出 abP 值：

假设是 $(ID_I^*, x_I^*, pk_I^*, c^*)$ 中的 $c* = 1$，X 在列表 L_2 中找出 $(m_i^*, ID_i^*, pk_i^*, l_i^*, l_i^*(aP), h_i^*)$，在列表 L_3 中找出 (P_{pub}, j, T) $(1 \leqslant i \leqslant n)$，根据等式：

$$e(S^*, P) = e(\sum_{i=1}^{n} h_i^* Q_i^*, P_{pub}) \cdot \prod_{i=1}^{n} e(U_i^*, pk_i^*) e(T, R^*),$$

$$e(S^*, P) = e\Big(\sum_{i=1}^{n} h_i^* t_i^* P, sP\Big) \cdot \prod_{i=1, i\neq I}^{n} e(l_i^*(aP), x_i^* P) \cdot e(l_I^*(aP), x_I^*(bP)) \cdot e(jP, R^*)$$

从而可求出

$$abP = (l_I^* x_I^*)^{-1} \cdot \Big(S^* - \sum_{i=1}^{n} h_i^* t_i^* sP - \sum_{i=1, i\neq I}^{n} l_i^* x_i^* (aP) - jR^*\Big)$$

即 X 攻破了 CDH 难题，但是目前 CDH 问题是困难的，所以得出本文方案在 A_2 攻击下是安全的。

3.2.2　*效率分析*　用 p 表示计算 1 个双线性对所需时间，s 表示群 G_1 上 1 个标量乘时间，L 表示群 G_1 上元素的长度。

本文方案生成的聚合签名长度是固定的，即 $2L$，与签名人数无关。而文献［5－6，12，16－17］中的聚合签名长度是（$n+1$）L（n 是签名人数），聚合签名的长度会随着签名人数的增加而膨胀，这些方案不适合用于带宽受限的无线网络环境中。当然本文方案与 Ming 方案相比，为了保证安全性降低了方案计算效率，如聚合签名的验证需要（$n+3$）个双线性对。

在基于双线性对的 CLAS 方案中，如果我们认定有固定长度、固定对运算的 CLAS 方案是高效的，则目前已有的经证明安全的高效的 CLAS 方案就仅仅只有文献［3］中的方案，但这个方案也存在不足：如需要 KGC 为每个签名人分发 2 个部分私钥，还有需要每个签名人维护一个共同的状态信息等。所以，构造安全、高效且不需要额外的增加签名人的私钥的 CLAS 方案是我们以后设计方案的目标。

表 1　CLAS 方案效率比较

Table 1　Efficiency comparison of eleven CLAS schemes

方案	签名开销	验证开销	签名长度	部分私钥长度	安全性
［3］	$5s$	$2ns+5p$	$2L$	$2L$	Yes
［5］－I	$2s$	$(2n+1)\ p$	$(n+1)\ L$	L	No
［5］－II	$3s$	$(n+2)\ p+ns$	$3L$	$2L$	No
［6］	$3s$	$(n+3)\ p$	$(n+1)\ L$	L	Yes
［11］	$4s$	$2ns+4p$	$2L$	L	No
［12］	$3s$	$2ns+3p$	$(n+1)\ L$	L	No
［15］	$4s$	$ns+4p$	$2L$	L	No
［16］－I	$4s$	$2ns+4p$	$(n+1)\ L$	L	Yes
［16］－II	$4s$	$2ns+4p$	$2L$	L	No
［17］	$2s$	$ns+3p$	$(n+1)\ L$	L	Yes
Ours	$4s$	$ns+(n+3)\ p$	$2L$	L	Yes

4　结　论

无证书聚合签名因其压缩和批处理的特性在物联网、分布式系统等领域有广泛的应用，所以研究这种特殊签名很有意义。本文对张玉磊等改进的无证书聚合签名方案进行了安全性分析，指出该方案不能抵抗类型 II 敌手的攻击，最后构造了一个有固定长度的无证书聚合签名方案，并在随机预言机模型下证明了新方案是安全的，以后的工作是进一步深化研究无证书聚合签名体制的构造及安全性证明，为物联网的快速发展提供安全保障。

参考文献：

［1］ LIN X, SUN X, HO P H, et al. GSIS: A secure and privacy preserving protocol for vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3442－3456.

［2］ 王茜，黄林军. 基于交互确认机制的公平电子现金交易协议研究[J]. 中山大学学报(自然科学版),2010, 49(1):9－15.
WANG Q, HUANG L J. Fair e-Cash transaction protocol based on interactive confirmer scheme [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2010, 49(1):9－15.

［3］ ZHANG L, QIN B, WU Q H, et al. Efficient many-to-one authentication with certificateless aggregate signatures [J]. Computer Networks the International Journal of Computer & Telecommunications Networking, 2010, 54(14): 2482－2491.

［4］ 陈兴发,高崇志,姚正安. 安全加密的环签名混淆器[J]. 中山大学学报(自然科学版), 2014, 53(1):8－17.
CHEN X F, GAO C Z, YAO Z A. Secure obfuscation for encrypted ring signatures [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2014, 53(1):8－17.

［5］ GONG Z, LONG Y, HONG X, et al. Two certificateless aggregate signatures from bilinear maps [C]//In Proceedings of IEEE SNPD 2007, 3:188－193.

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

[7] XIONG H, WU Q, CHEN Z. Strong security enabled certificateless aggregate signatures applicable to mobile computation [C]//The Third International Conference on Intelligent Networking and Collaborative Systems, IEEE Computer Society, Washington, 2011: 92 – 99.

[8] MUHAMMAD K K, HE D B. Cryptanalysis of a certificateless aggregate signature scheme for mobile computation [J]. Applied Mathematics & Information Sciences. 2013, 7 (4): 1383 – 1386.

[9] YANAI N, TSO R, MAMBO M, et al. Certificateless ordered sequential aggregate signature Scheme [C]//In Proceedings of the 3rd International Conference on Intelligent Networking and Collaborative Systems 45 (INCoS'11), Fukuoka, Japan, IEEE, 2011: 662 – 667.

[10] CHEN Y C, HORNG G, LIU C L, et al. Efficient certificateless aggregate signature scheme [J]. Journal of Electronic Science and Technology, 2012, 10(3): 209 – 214.

[11] 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, 41(1): 72 – 76.

[12] XIONG H, GUAN Z, CHEN Z, et al. An efficient certificateless aggregate signature with constant pairings computations [J]. Information Sciences, 2013, 219: 225 – 235.

[13] 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: 458 – 462.

[14] CHENG L, WEN Q, ZHANG H, et al. Cryptanalysis and improvement of a certificateless aggregate signature scheme [J]. Information Sciences, 2015, 295: 337 – 346.

[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.
MING Y, ZHAO X M, WANG Y M. Certificateless aggregate signature scheme [J]. Journal of University of Electronic Science and Technology of China, 2014, 43 (2): 188 – 193.

[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.
ZHANG Y L, LI C Y, WANG C F, et al. Security analysis and improvements of certificateless aggregate signature schemes [J]. Journal of Electronics & Information Technology, 2015, 37(8): 1994 – 1999.

[17] SHI J H, SHIANG F T, PO-HSIAN H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks [J]. Information Sciences, 2015, 317: 48 – 66.

(上接第76页)

[9] 郭志荣、易金桥、段文山,等. 一类高维非线性方程(组)自相似解的简易求法[J]. 西北师范大学学报(自然科学版), 2007, 43(2): 33 – 37.
GUO Z R, YI J Q, DUAN W S, et al. A method for finding similarity solution of (2 + 1)-dimensional nonlinear partial differential equation(s) [J]. Journal of Northwest Normal University (Natural Science), 2007, 43(2): 33 – 37.

[10] 赵向青、崔尚斌. 各向异性非线性 Schrödinger 方程的整体可解性[J]. 中山大学学报(自然科学版), 2007, 46(2): 1 – 4.
ZHAO X Q, CUI S B. Global solvability for a non-isotropic nonlinear Schrödinger equation [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2007, 46 (2): 1 – 4.

[11] 黄民海. 四分之一平面域上 Helmholtz 方程组的混合边值问题[J]. 中山大学学报(自然科学版), 2011, 50(5): 7 – 10.
HUANG M H. The mixed boundary-value problem of Helmholtz equation in a quarter-plane [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2011, 50 (5): 7 – 10.

[12] YUEN M W. Rotational and self-similar solutions for the compressible Euler equations in $\mathbf{R}^3$ [J]. Communications in Nonlinear science and Numerical Simulation, 2015, 20 (3): 634 – 640.