doi:10.11959/j.issn.1000-436x.2015196

改进的无证书有序多重签名方案

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：有序多重签名是多个用户按一定顺序对同一消息文件进行的签名和认证。许艳等提出一个在随机预言机模型下可证明安全的无证书有序多重签名方案，该方案生成的多重签名有固定长度，且验证签名的双线性对运算是固定的。指出许艳等的方案在签名验证算法的双线性对计算部分存在不足，并纠正了该缺陷，但纠正后的方案实施效率大大降低。接着提出一个高效的无证书有序多重签名方案，生成的多重签名仅为 1 个群元素，签名的验证仅需 2 个双线性对。

关键词：无证书公钥密码；有序多重签名；随机预言机模型；双线性对

中图分类号：TP309 **文献标识码**：A

Improved certificateless sequential multi-signature scheme

DU Hong-zhen[1], WEN Qiao-yan[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: A sequential multi-signature enabled multiple users to jointly sign a document in order. Xu, *et al* proposed a provably-secure certificateless sequential multi-signature scheme with constant signature length and pairing computations. However, it was shown that the scheme had a drawback in the verifying algorithm, and then it overcame the drawback. But, the efficiency of the corrected scheme was greatly reduced. An efficient certificateless sequential multi-signature scheme is constructed, and the multi-signature generated by proposed scheme consists of one group element and the verification algorithm requires only 2 bilinear pairings.

Key words: certificateless public key cryptography; sequential multi-signature; random oracle model; bilinear pairing

1 引言

无证书公钥密码是 Al-Riyami 等[1]提出的，这是一种性能优良的公钥密码机制，它解决了传统公钥密码中的证书问题，故可以被广泛用于资源受限的无线网络环境，同时又消除了基于身份的公钥密码存在的秘钥托管问题，避免了用户隐私的泄露。目前对无证书公钥密码的研究是密码学界的一个热点。

多重签名(multi-signature)的概念由 Itakura 等[2]提出的，它允许多个签名人对同一个消息进行签名，其最大的优势在于用较低的计算与通信成本实现了同时为多个用户提供完整性、认证性和不可否认服务。在现实中多重签名可分为有序多重签名和无序多重签名。有序多重签名是多个签名人按照某个次序对同一个消息进行签名，如在一个公司中，有一份合同需要董事长、总经理和部门经理共同签名才有效，而总经理只有看到部门经理的签名后才在合同上签名，董事长认可了总经理和部门经理的签名后才愿意签名。多重签名被广泛应用于蜂窝电话、RFID、PDA、传感器等电池寿命、计算能力、

收稿日期：2014-12-23；**修回日期**：2015-08-27

基金项目：国家自然科学基金资助项目(61402015, 61402275)；陕西省教育厅专项科研基金资助项目（15JK1022）；陕西省自然科学基础研究基金资助项目（2015JM6263）；宝鸡文理学院基金资助项目（ZK12042）

Foundation Items: The National Natural Science Foundation of China (61402015, 61402275); The Scientific Research Project of Shaanxi Provincial Education Department (15JK1022); The Basic Research Project of Natural Science in Shaanxi Province (2015JM6263); The Scientific Research Project of Baoji University of Arts and Sciences (ZK12042)

存储空间和带宽受限的无线应用环境。

早期的多重签名方案不能抵抗流氓密钥攻击，直到 2006 年，Bellare 等[3]提出一种新的适用于 PKI 系统的 PPK（plain public key）模型，才较好地解决了这一问题。Wang 等[4]对多重签名的安全性做了研究。Bagherzandi 等 [5]提出一个两轮交互的基于离散对数的多重签名方案，并给出了在 PPK 模型下的安全证明，但该签名计算量大，实施效率低。Ma 等[6]提出一个在 PPK 模型下可证明安全的高效的基于离散对数问题的多重签名方案。于佳卜等[7]研究了标准模型下的前向安全多重签名的安全性模型和构造。2013 年，Kong 等[8]构造了 2 个基于格的多重签名方案，但 2 个方案都是实施效率低，有安全漏洞。第一个高效的基于身份的多重签名方案由 Gentry 等[9]提出，方案使用了双线性对技术，是非交互的，但缺陷是需要所有参与者共享一个新鲜的随机比特串。

无证书多重签名是无证书公钥密码下多个用户对同一个消息进行签名。2008 年，梁红梅等[10]基于双线性对提出了一个无证书多重签名方案，但该方案是可以伪造的，且用户的私钥会泄露。2011 年，张玉磊[11]构造了一个无证书紧致有序多重签名方案。同年，Jin 等[12]提出一个无证书多重代理签名方案，但 Xu 等[13]指出该方案不安全，并提出了一个新的方案。2014 年，Du 等[14]提出一个无证书代理多重签名方案。2013 年，秦艳琳等[15]提出一个可以解决信任连推荐信息认证问题的无证书有序多重签名方案，但许艳等[16]指出该方案不能抵抗敌手的伪造攻击，同时，许艳等基于 He 等[17]的无证书短签名方案构造了一个高效的无证书有序多重签名方案，生成的多重签名仅为一个群元素，签名的验证仅需 2 个双线性对运算。但是本文指出，许艳等方案的签名验证算法有缺陷，即签名的验证并非仅需 2 个双线性对运算，而是需要计算 n+1 个双线性对（n 是签名人数），大量的双线性对运算导致方案实施效率很低。最后，本文在文献[17]的基础上提出了一个改进的无证书有序多重签名方案，该方案的签名长度是固定的，仅为一个群元素，验证签名仅需 2 个双线性对。

2　预备知识

2.1　双线性对和相关数学难题

1) 双线性对

令 l 是一个安全参数，q 是一个 l bit 的素数，G_1 是由 P 生成的阶为 q 的循环加法群，G_2 是有相同阶 q 的循环乘法群。双线性映射 $e: G_1 \times G_1 \to G_2$ 满足下列性质。

双线性性：$\forall P,\ Q \in G_1$，$\forall a,\ b \in Z_q^*$，有 $e(aP,bQ)=e(P,Q)^{ab}$。

这里，$\forall P_1,P_2 \in G_1, e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$，$e(Q,P_1+P_2)=e(Q,P_1)e(Q,P_2)$。

非退化性：$\exists P,Q \in G_1$，使 $e(P,Q) \neq 1$。

易计算性：$\forall P,\ Q \in G_1$，存在有效算法计算 $e(P,Q)$。

2) 计算 Diffie-Hellman (CDH)问题

$\forall\ a,\ b \in Z_q^*$，给定 $P, aP, bP \in G_1$，计算 $abP \in G_1$。

2.2　无证书有序多重签名方案的定义

定义 1　一个无证书有序多重签名方案涉及 n 个用户 $ID_i (1 \leqslant i \leqslant n)$，1 个私钥生成中心 KGC 及 1 个验证者，方案由以下 7 个算法构成[15, 16]。

1) Setup：由 KGC 执行，输入 1 个安全参数 k，输出系统主密钥 s 和系统参数 $params$。

2) Partial-Private-Key-Extract：该算法由 KGC 执行，输入 $params$、s 和身份 ID_i，返回部分私钥 D_i。

3) Set-Secret-Value：由用户 ID_i 执行，选随机数 x_i 作为自己的秘密值。

4) Set-Public-Key：输入 $params$、ID_i 及 x_i，输出用户公钥 P_i。

5) Set-Private-Key: 输入 $params$、ID_i、秘密值 x_i 和部分私钥 D_i，输出 $s_i=(x_i,D_i)$ 作为（完全）私钥。

6) Sign：输入消息 m、$params$、$ID_i (1 \leqslant i \leqslant n)$、公钥 P_i、完全私钥 s_i 及签名顺序 κ，用户 ID_i 验证上一个用户 ID_{i-1} 传来的部分签名 σ_{i-1} 有效后，输出部分签名 σ_i。

7) Verify：输入 m、$params$、$ID_i (1 \leqslant i \leqslant n)$、$P_i$、签名顺序 κ 及完整签名 σ_n，输出“1”或“0”，表示签名有效或无效。

一个无证书有序多重签名方案中存在 2 类敌手，用 $\mathcal{A}$ 和 $\mathcal{F}$ 表示，其中 $\mathcal{A}$ 模拟的是一个 malicious- but-passive KGC，掌握系统主密钥和用户的部分私钥，但不能替换用户的公钥。$\mathcal{F}$ 模拟的是一个 dishonest user，不知道系统主密钥和用户的部分私钥，但可以替换任意用户的公钥。

3 许艳等无证书有序多重签名方案及正确性分析

3.1 许艳等方案介绍

许艳等[16]构造了一个无证书有序多重签名方案，由下面 7 个算法组成。

1) Setup: $(G_1,+),(G_2,\times)$ 分别是 2 个阶为素数 q 的循环群， P 为 G_1 的一个生成元，双线性映射 $e:G_1\times G_1\to G_2$ ， 3 个安全散列函数 $H_0:\{0,1\}^*\times G_1\to Z_q^*$， $H_1:\{0,1\}^*\to Z_q^*$， $H_2:\{0,1\}^*\to G_1$。私钥生成中心 KGC 随机选取 $s\in Z_q^*$ 作为系统主密钥并秘密保存，计算公钥 $P_0=sP$ ，公开系统参数 $params:\{G_1,G_2,q,P,e,P_0,H_0,H_1,H_2\}$。

2) Partial-Private-Key-Extract：给定用户 $N_i(1\leqslant i\leqslant n)$ 身份 ID_i，KGC 计算该用户的部分私钥 (D_i,R_i) 如下。

随机选取 $r_i\in Z_q^*$，计算 $R_i=r_iP,h_i=sH_0(ID_i,R_i)$, $D_i=r_i+h_is$ 。

这里 $h_i=sH_0(ID_i,R_i)$ 应该改为 $h_i=H_0(ID_i,R_i)$。

3) Set-Secret-Value: 选随机数 $x_i\in Z_q^*$ 作为 $N_i(1\leqslant i\leqslant n)$ 的秘密值。

4) Set-Public-Key：$N_i(1\leqslant i\leqslant n)$ 计算公钥 $P_i=x_iP$，并公开 $Pk_i=(P_i,R_i)$ 作为其公钥。

5) Set-Private-Key: $N_i(1\leqslant i\leqslant n)$ 输出数据 $s_i=(x_i,D_i)$ 作为（完全）私钥。

6) Sign：设用户 $N_i(1\leqslant i\leqslant n)$ 将以 $N_1\to N_2\to N_3\to\cdots N_n$ 为签名顺序对推荐信息 m 进行多重签名。

N_1 对 m 签名如下。

(a) N_1 构造 n 位的 0-1 序列 $C_1=(000\cdots001)$，第 n 位为 1，其余位为 0。令 $\kappa=(ID_1,ID_2,\cdots,ID_n)$，计算 $V_1=H_1(ID_1,\kappa,P_1,R_1,P_0)$， $Q_1=H_2(m,ID_1,C_1,P_1,R_1,P_0)$。

(b) 计算 $\sigma_1=Sign_1=(V_1x_1+D_1)Q_1$，则 σ_1 是 N_1 对 m 的部分签名。

用户 N_i 收到 N_{i-1} 发来的的信息/签名$(m,\ \sigma_{i-1})$后，操作如下。

(a)验证 σ_{i-1} 的有效性：N_i 构造 C_j，计算 $V_j=H_j(ID_j,\kappa,P_j,R_j,P_0)$，$1\leqslant j\leqslant i-1$。验证等式 $e(\sigma_{i-1},P)=e(Q_j,\sum_{j=1}^{i-1}(V_jP_j+R_j+h_jP_0))$ 是否成立，如果成立则对(m,σ_{i-1})继续签名如下。

(b)计算 $V_i=H_i(ID_i,\kappa,P_i,R_i,P_0)$， $Q_i=H_2(m,ID_i,C_i,P_i,R_i,P_0)$，其中，$C_i=(000\cdots1000)$ 第 $n-i+1$ 位为 1，其余位为 0。

(c) 计算 $\sigma_i=Sign_i+\sigma_{i-1}=(V_ix_i+D_i)Q_i+\sigma_{i-1}$。则 n 个用户 $N_i(1\leqslant i\leqslant n)$ 对消息 m 的有序多重签名为 $\sigma_n=\sum_{i=1}^{n}Sign_i$。

7) Verify：验证者对传递来的信息/签名数据(m,σ_n)进行验证如下。

(a) 计算 $V_i=H_i(ID_i,\kappa,P_i,R_i,P_0)$， $Q_i=H_2(m,ID_i,C_i,P_i,R_i,P_0)$，$1\leqslant i\leqslant n$。

(b) 验证等式 $e(\sigma_n,P)=e(Q_i,\sum_{i=1}^{n}(V_iP_i+R_i+h_iP_0))$ 是否成立，如果等式成立，则(m,σ_n)有效，否则签名无效。

3.2 许艳等方案的正确性分析

许艳等方案的 Verify 算法中验证签名的等式有错误存在，任何合法用户 $N_i(1\leqslant i\leqslant n)$ 对信息 m 生成的签名都通不过验证，导致整个方案的构造失败。具体分析如下。

1) 整体多重签名验证式

$$e(\sigma_n,P)=e(Q_i,\sum_{i=1}^{n}(V_iP_i+R_i+h_iP_0))$$

存在缺陷，因为

$$\begin{aligned}&e(\sigma_n,P)=e(\sum_{i=1}^{n}Sign_i,P)\\&=e(\sum_{i=1}^{n}(V_ix_i+D_i)Q_i,P)\\&=\prod_{i=1}^{n}e(Q_i,(V_iP_i+R_i+h_iP_0))\\&\neq e(Q_i,\sum_{i=1}^{n}(V_iP_i+R_i+h_iP_0))\end{aligned}$$

2) 第 i 个用户 $N_i(2\leqslant i\leqslant n)$ 对第 $i-1$ 个用户传来的部分多重签名 σ_{i-1} 的有效性需要验证，然而，该验证式存在缺陷，即 $e(\sigma_{i-1},P)=e(Q_j,\sum_{j=1}^{i-1}(V_jP_j+R_j+h_jP_0))$ 存在缺陷，正确的验证等式为

$$e(\sigma_{i-1},P)=\prod_{j=1}^{i-1}e\left(Q_j,V_jP_j+R_j+h_jP_0\right)$$

原因同上。

当然，如果将该方案 Verify 算法中的验证式改正，即分别把

$$e(\sigma_n,P)=e(Q_i,\sum_{i=1}^{n}(V_iP_i+R_i+h_iP_0)),$$

$$e(\sigma_{i-1},P)=e(Q_j,\sum_{j=1}^{i-1}(V_jP_j+R_j+h_jP_0))$$ 改正为

$$e(\sigma_n,P)=\prod_{i=1}^{n}e(Q_i,(V_iP_i+R_i+h_iP_0))$$ 和

$$e(\sigma_{i-1},P)=\prod_{j=1}^{i-1}e(Q_j,V_jP_j+R_j+h_jP_0)$$

则方案正确。但是这样 n 重签名验证算法需要的不是许艳等声称的 2 个双线性对运算，而增长到 n+1 个昂贵的双线性对运算，方案的效率和实用性大大降低。

4　改进的无证书有序多重签名方案

4.1　基本方案

方案由 7 个算法构成，具体构造描述如下。

算法 Setup、Partial-Private-Key-Extract、Set-Secret-Value、Set-Public-Key、Set-Private-Key 与许艳方案对应的算法相同。

1) Sign：设用户 $N_i(1\leqslant i\leqslant n)$ 将以 $N_1\rightarrow N_2\rightarrow N_3\rightarrow\cdots\rightarrow N_n$ 为签名顺序对推荐信息 m 进行多重签名。

N_1 对 m 签名如下。

(a) 令 $\kappa=(ID_1,ID_2,\cdots,ID_n)$（$\kappa$ 标记了 n 个用户的签名顺序 $ID_1\rightarrow ID_2\rightarrow ID_3\rightarrow\cdots\rightarrow ID_n$），计算 $l_1=H_1(ID_1,\kappa,P_1,R_1,m)$，$T=H_2(m,\kappa,P,P_0)$。

(b) 计算 $\sigma_1=Sign_1=(l_1x_1+D_1)T$，则 σ_1 是 N_1 对 m 的部分签名，接着 N_1 把$(m,\ \sigma_1)$发送给用户 N_2。

用户 $N_i(i=2,3,\cdots,n)$ 收到 N_{i-1} 发来的信息/签名$(m,\ \sigma_{i-1})$后，操作如下。

(a) 验证 σ_{i-1} 的有效性：N_i 计算 $l_j=H_1(ID_j,\kappa,P_j,R_j,m)$，$h_j=H_0(ID_j,R_j)$，$1\leqslant j\leqslant i-1$，$T=H_2(m,\kappa,P,P_0)$。验证等式 $e(\sigma_{i-1},P)=e(T,\sum_{j=1}^{i-1}(l_jP_j+R_j+h_jP_0))$ 是否成立。如果成立则对$(m,\ \sigma_{i-1})$继续签名如下。

(b)计算 $l_i=H_1(ID_i,\kappa,P_i,R_i,m)$，$\sigma_i=\sigma_{i-1}+Sign_i=\sigma_{i-1}+(l_ix_i+D_i)T$。

(c) n 个用户 $N_i(1\leqslant i\leqslant n)$ 对信息 m 的有序多重签名为 $\sigma_n=\sum_{i=1}^{n}Sign_i$。

2) Verify：验证者对传递来的信息/签名数据(m,σ_n)进行验证如下。

(a) 计算 $l_i=H_1(ID_i,\kappa,P_i,R_i,m)$，$1\leqslant i\leqslant n$，$T=H_2(m,\kappa,P,P_0)$。

(b) 验证等式 $e(\sigma_n,P)=e(T,\sum_{i=1}^{n}(l_iP_i+\ R_i+h_iP_0))$ 是否成立，如果等式成立，则(m,σ_n)有效，否则签名无效。

方案正确性分析

$$\begin{aligned}e(\sigma_n,P)&=e\left(\sum_{i=1}^{n}(l_ix_i+D_i)T,P\right)\\&=e\left(T,\sum_{i=1}^{n}(l_ix_iP+D_iP)\right)\\&=e\left(T,\sum_{i=1}^{n}(l_iP_i+R_i+h_iP_0)\right)\end{aligned}$$

4.2　方案的安全性分析

定理 1　在随机预言机模型和 CDH 困难假设下，改进的无证书有序多重签名方案在 2 类敌手 $\mathcal{A}$（$\mathcal{A}$ 模拟的是 malicious-but-passive KGC)和 $\mathcal{F}$（$\mathcal{F}$ 模拟的是 dishonest user)适应性选择消息攻击下是存在性不可伪造的。

定理 1 由引理 1 和引理 2 推出。

引理 1　在随机预言机模型和 CDH 困难假设下，改进的无证书有序多重签名方案在敌手 $\mathcal{A}$ 适应性选择消息攻击下是存在性不可伪造的。

证明　已知本文方案有 n 个用户 $N_i(1\leqslant i\leqslant n)$，不妨假设除用户 $N_I\in\{N_1,N_2,\cdots N_n\}$（$N_I$ 的身份 ID_I）以外，其余 n−1 个用户都被敌手 $\mathcal{A}$ 攻破。设 (aP,bP) 是群 G_1 上 CDH 难题的一个任意实例，$\mathcal{C}$ 调用 $\mathcal{A}$ 为子程序，目标是输出值 abP。

$\mathcal{C}$ 运行 Setup 算法，令系统公钥 $P_0=sP$，生成系统参数 $params:\{G_1,G_2,\ q,\ P,\ e,\ P_0,\ H_0,\ H_1,H_2\}$，将系统主密钥 s 及 $params$ 发给 $\mathcal{A}$，$\mathcal{A}$ 执行以下询问。

H_0-询问：当 $\mathcal{A}$ 输入数据（(ID_i,R_i)，$\mathcal{C}$ 调出列表 L_0，若 L_0 中有相应的记录 (ID_i,R_i,h_i)，则输出 h_i。否则 $\mathcal{C}$ 随机选 $h_i\in Z_q^*$，添加 (ID_i,R_i,h_i) 到 L_0 中。返回 h_i 给 $\mathcal{A}$。

H_1-询问：$\mathcal{A}$ 输入 $(ID_i,\kappa,P_i,R_i,m_j)$，$\mathcal{C}$ 调出列表 L_1。若 L_1 中已有相应的记录 $(ID_i,\kappa,P_i,R_i,m_j,l_i)$，返 l_i。否则，任选随机数 $l_i\in Z_q^*$，添加 $(ID_i,\kappa,P_i,R_i,m_j,l_i)$ 到 L_1 中，输出 l_i。

H_2-询问：当 $\mathcal{A}$ 输入 (m_j,κ,P,P_0) 时，$\mathcal{C}$ 返回以前定义的值，否则任选 $v_j\in Z_q^*$，定义 $T_j=v_j(bP)\in G_1$，添加 $(m_j,\kappa,P,P_0,v_j,T_j)$ 到列表 L_2 中，返回 T_j。

Partial-Private-Key-Extract(ID_i)询问：当 $\mathcal{A}$ 询问 ID_i 的部分私钥时，$\mathcal{C}$ 随机选取 $r_i\in Z_q^*$，计算 $R_i=r_iP,D_i=r_i+h_is$，添加 (ID_i,r_i,R_i,D_i) 到部分私钥存储列表 E^{list} 中。返回 (R_i,D_i)。

Set-Secret-Value（ID_i）询问：$\mathcal{A}$ 输入 ID_i，若

$ID_i \neq ID_I$，$\mathcal{C}$ 选随机数 $x_i \in Z_q^*$，计算 $P_i = x_i P$，返回 x_i 给 $\mathcal{A}$。添加 (ID_i, x_i, P_i) 到 P^{list} 中。若 $ID_i = ID_I$，则令 $P_i = aP$，添加 $(ID_i, \perp, P_i)$ 到 P^{list} 中。

Public-Key(ID_i) 询问：当 $\mathcal{A}$ 询问 ID_i 的公钥时，$\mathcal{C}$ 调出列表 E^{list} 和 P^{list}，若 E^{list}，P^{list} 中有相应记录，则输出用户公钥 $PK_i = (R_i, P_i)$，否则执行 Partial-Private-Key-Extract 和 Set-Secret-Value 询问，返回 PK_i。

Sign(ID_i, m_j, PK_i)询问：当 $\mathcal{A}$ 询问身份/公钥为 (ID_i, PK_i) 的用户对信息 m_j 的签名时，若 $ID_i = ID_I$，则 $\mathcal{C}$ 停止模拟，失败退出。否则调出列表 E^{list} 和 P^{list}，找出 ID_i 的部分私钥 (R_i, D_i) 和秘密值 x_i，查询列表 L_1：$(ID_i, \kappa, P_i, R_i, m_j, l_i)$ 和列表 L_2：$(m_j, \kappa, P, P_0, v_j, T_j)$，计算 ID_i 对应的部分签名 $Sign_i = (l_i x_i + D_i)T_j$，返回 $Sign_i$。

最后，$\mathcal{A}$ 停止训练，输出一个有效的关于 n 个用户（ID_i，PK_i）$(1 \leqslant i \leqslant n)$ 在信息 m^* 上的多重签名 σ_n^*，其中身份 $ID_I \in \{ID_1, ID_2, \cdots, ID_n\}$ 没有提交 Set-Secret-Value 预言机，且 σ_n^* 不是由 Sign 预言机生成的。$\mathcal{C}$ 调出列表 L_0：(ID_i, R_i, h_i)，L_1：$(ID_i, \kappa, P_i, R_i, m^*, l_i^*)$，$L_2$：$(m^*, \kappa, P, P_0, v^*, T^*)$，$E^{\text{list}}$：$(ID_i, r_i, R_i, D_i)$，$P^{\text{list}}$：$(ID_i, x_i, P_i)$。因为 σ_n^* 有效，则有验证等式

$$e(\sigma_n^*, P) = e\left(v^*(bP), l_I^*(aP) + \sum_{i=1, i\neq I}^{n} l_i^* x_i P + \sum_{i=1}^{n}(r_i P + h_i s P)\right)$$

成立，从而 $\mathcal{C}$ 计算出

$$abP = (l_I^* v^*)^{-1}\left(\sigma_n^* - \sum_{i=1, i\neq I}^{n} v^* l_i^* x_i (bP) - \sum_{i=1}^{n} v^* r_i (bP) + v^* h_i s(bP)\right)$$

引理 2 在随机预言机模型和 CDH 困难假设下，改进的无证书有序多重签名方案在敌手 $\mathcal{F}$ 的适应性选择消息攻击下是存在性不可伪造的。

证明 $\mathcal{C}$ 运行 Setup 算法，令系统公钥 $P_0 = aP$，生成系统参数 *params* 将其发给 $\mathcal{F}$，$\mathcal{F}$ 执行以下询问。

$H_0 \sim H_2$-Public-Key(ID_i) 询问：与引理 1 中的 $H_0 \sim H_2$-Public-Key(ID_i)预言机问答相同。

Partial-Private-Key-Extract(ID_i)询问：当 $\mathcal{F}$ 询问 ID_i 的部分私钥时，$\mathcal{C}$ 选取随机数 $h_i, D_i \in Z_q^*$，定义 $R_i = D_i P - h_i(aP)$，$h_i = H_0(ID_i, R_i)$，调出列表 L_0，若 L_0 中存在数据 (ID_i, R_i, h_i') 且 $h_i \neq h_i'$，则另选 $h_i, D_i \in Z_q^*$ 使无碰撞存在。最后添加 (ID_i, R_i, h_i) 到 L_0 中，添加 (ID_i, R_i, D_i) 到部分私钥存储列表 E^{list} 中。返回 (R_i, D_i)。

Set-Secret-Value (ID_i)询问：$\mathcal{C}$ 选随机数 $x_i \in Z_q^*$，计算 $P_i = x_i P$,返回 x_i 给 $\mathcal{F}$，添加 (ID_i, x_i, P_i) 到 P^{list} 中。

Replace-Public-Key(ID_i R_i', P_i')询问：$\mathcal{C}$ 替换用户公钥 $PK_i = (R_i, P_i)$ 为 $PK_i' = (R_i', P_i')$。

Sign(ID_i, m_j, PK_i)询问：当 $\mathcal{F}$ 询问身份/公钥为 (ID_i, PK_i) 的用户对信息 m_i 的签名时，$\mathcal{C}$ 调出列表 E^{list} 和 P^{list}，找出 ID_i 对应的 (R_i, D_i) 和秘密值 x_i（如果用户 ID_i 的公钥已被替换则停止模拟），查询列表 L_1：$(ID_i, \kappa, P_i, R_i, m_j, l_i)$ 和列表 L_2：$(m_j, \kappa, P, P_0, v_j, T_j)$，计算 ID_i 对应的部分签名 $Sign_i = (l_i x_i + D_i)T_j$，返回 $Sign_i$。

最后，$\mathcal{F}$ 停止训练，输出一个关于 n 个用户（ID_i，PK_i）$(1 \leqslant i \leqslant n)$ 在信息 m^* 上的多重签名 σ_n^*，其中身份 $ID_I \in \{ID_1, ID_2, \cdots, ID_n\}$ 没有提交 Partial-Private-Key-Extract 预言机，且 σ_n^* 不是由 Sign 预言机生成的。$\mathcal{C}$ 调出列表 L_0，L_1，L_2，E^{list}，P^{list}。若用户 ID_i 的公钥已被替换则失败退出，否则与引理 1 类似，$\mathcal{C}$ 可以计算出 $abP = (h_i v^*)^{-1}(\sigma_n^* - v^* R_I - \sum_{i=1, i\neq I}^{n}(v^* x_i (bP) + v^* h_i (aP)))$。

4.3 方案效率比较

若用 *Sm* 表示群 G_1 上 1 次点标量乘计算，*Pr* 表示 1 个双线性对的计算，$|G_1|$表示群 G_1 上 1 个群元素的长度。通过表 1 可见，改进方案的效率高于(纠错后)许艳等的方案。

表 1 方案效率比较（针对 *n* 个签名人的多重签名）

方案	签名计算量	验证计算量	签名长度
许艳方案	$(2n-1)Sm$	$4nSm+(n+1)Pr$	$\|G_1\|$
本文方案	$(2n-1)Sm$	$4nSm+2Pr$	$\|G_1\|$

5 结束语

有序多重签名方案有着广泛的应用背景。本文指出许艳等的无证书有序多重签名方案在设计验证算法时存在双线性对计算的不足，并针对这一缺陷给出了合理的方案设计。但方案一旦改正效率会大大降低，故在许艳方案基础上又提出一个新的无证书有序

多重签名方案，新方案生成的签名长度是固定的，与签名人数无关，且方案的执行仅需要 2 个双线性对的运算量，效率大大提高，最后在随机预言机模型下证明了新方案是安全的，下一步的研究工作是在标准模型下构造无证书有序多重签名方案。

参考文献：

[1] AL-RIYAMI S, PATERSON K G. Certificateless public key cryptography[A]. Proceedings of ASIACRYPT 2003[C]. Springer-Verlag, 2003. 452-473.

[2] ITAKURA K, NAKAMURA K. A public-key cryptosystem suitable for digital multisignatures[J]. NEC Research and Development, 1983, (71):1-8.

[3] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[A]. 13th ACM Conference on Computer and Communications Security (CCS'06)[C]. Alexandria, USA, 2006.

[4] 王晓峰, 张琛, 王尚平.多重数字签名方案及其安全性证明[J].计算机学报, 2008, 31(1):176-183.
WANG X F, ZHANG C, WANG S P. Digital multi-signature scheme and its security proof[J]. Chinese Journal of Computers, 2008, 31(1):176-183.

[5] BAGHERZANDI A, CHEON J H, JARECKI S. Multisignatures secure under the discrete logarithm assumption and a generalized forking lemma [A]. 15th ACM conference on Computer and communications security (CCS'08)[C]. Alexandria, USA, 2009. 27-31.

[6] MA C, WENG J, LI Y, *et al*. Efficient discrete logarithm based multi-signature scheme in the plain public key model [J]. Designs, Codes and Cryptography, 2010, 54(2):121-133.

[7] 于佳,郝蓉,孔凡玉.标准模型下的前向安全多重签名:安全性模型和构造[J].软件学报, 2010,21(11) : 2920-2932.
YU J, HAO R, KONG F Y. Forward-secure multi-signature in the standard model: security model and construction [J]. Journal of Software, 2010,21(11) : 2920-2932.

[8] FAN Y K, LU H D, JIA Y, *et al*. Lattice-based multi-signature schemes [J]. Applied Mechanics and Materials, 2013, 411-414: 3-6.

[9] BOLDREVA A, GENTRY C, NEILL A. Ordered multisignatures and ID-based sequential aggregate signatures with applications to secure routing[A]. Proc of the 14th ACM Conf on Computer and Communications Security[C]. New York, USA, 2007. 276-285.

[10] 梁红梅, 黄慧, 吴晨煌, 等. 无证书多重签名[J]. 集美大学学报, 2008, 13(2):127-131.
LIANG H M, HUANG H, WU C H, *et al*. Certificateless multi-signature [J]. Journal of Jimei University, 2008，13(2):127-131.

[11] 张玉磊.高效的无证书紧致有序多重签名方案[J].计算机工程, 2011, 37(8): 108-111.
ZHANG Y L. Efficient certificateless compact sequential multi-signature scheme [J]. Computer Engineering, 2011, 37(8): 108-111.

[12] JIN Z P, WEN Q Y. Certificateless multi-proxy signature [J]. Computer Communications, 2011, 34(3): 344-352.

[13] XU J, SUN H X, WEN Q Y, *et al*. Improved certificateless multi-proxy signature [J]. The Journal of China Universities of Posts and Telecommunications, 2012,19(4):94-105.

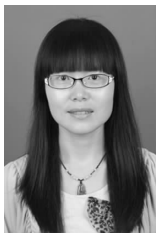
[14] DU H Z, WEN Q Y. Certificateless proxy multi-signature [J]. Information Sciences, 2014, 276:21-30.

[15] 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.

[16] 许艳, 黄刘生, 田苗苗, 等.可证安全的高效无证书有序多重签名方案[J]. 通信学报, 2014,35(11):126-131.
XU Y, HUANG L S, TIAN M M, *et al*. Provably-secure and efficient certificateless sequential multi-signature scheme [J]. Journal on Communications, 2014,35(11):126-131.

[17] HE D B, HUANG B J, CHEN J H. New certificateless short signature scheme[J]. Information Security IET, 2013, 7(2):113-117.

作者简介：



杜红珍（1978-），女，陕西扶风人，宝鸡文理学院副教授，主要研究方向为密码学和物联网安全、数字签名技术。

温巧燕（1959-），女，陕西西安人，北京邮电大学教授、博士生导师，主要研究方向为密码学与信息安全。