doi:10.3969/j.issn.1000-436x.2014.11.014

可证安全的高效无证书有序多重签名方案

许艳[1,2]，黄刘生[1]，田苗苗[1]，仲红[3]

(1. 中国科学技术大学 计算机科学与技术学院，安徽 合肥 230026；
2. 安徽大学 现代教育技术中心，安徽 合肥 230601；3. 安徽大学 计算机科学与技术学院，安徽 合肥 230601)

摘 要：无证书有序多重签名可用于解决信任链推荐信息的认证问题。秦艳琳等提出一个高效的无证书有序多重签名方案，并在随机语言机模型下证明方案的安全性可归约为 CDH（computational Diffie-Hellman）困难问题。对该方案的安全性证明过程进行分析，指出方案难以抵抗伪造攻击：攻击者已知某个多重签名，则可以伪造其他消息的多重签名。随后构造一个更加高效的无证书有序多重签名方案，方案使用更少的双线性对，且只有一个签名消息，占用更小的计算代价和通信代价。最后证明方案在随机预言机模型下具有不可伪造性。

关键词：无证书；多重签名；安全性分析；伪造攻击

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)11-0126-06

Provably secure and efficient certificateless sequential multi-signature scheme in random oracle model

XU Yan[1,2], HUANG Liu-sheng[1], TIAN Miao-miao[1], ZHONG Hong[3]

(1. School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China;
2. Modern Educational and Technology Center, Anhui University, Hefei 230601, China;
3. School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract: Certificate less sequential multi-signature scheme could resolve the problem of authentication of recommendation information transmitted through trust train. Qin yan-lin, *et al* proposed an efficient certificateless sequential multi-signature scheme, and proved the security is based on the fact that computational Diffie-Hellman problem is hard in the random oracle. It is found that Qin's scheme is insecure against the forgery attack after analysing the security proof. If an adversary has obtained the signers' multi-signature, it can forgery the multi-signature for any other message. Then, a more efficient certificateless sequential multi-signature scheme is construced which has lower computation cost and communication cost for using less bilinear pairings and only generating one signature message. Finally, the security proof shows that the proposed scheme can resist the forgery attack under the model of random oracle.

Key words: certificateless; multi-signature; security analysis; forgery attack

1 引言

多重签名是面向群体的签名，多个参与者可对同一个消息进行签名。按照应用环境的不同，可分为有序多重签名和无序多重签名。有序多重签名要求签名者以特定的顺序进行签名，无序多重签名则无顺序要求。1983 年，Itakura 等[1]提出多重签名的概念。文献[2]基于离散对数困难性提出一个多重签名方案。Micali 等[3]首次给出多重签名方案的安全模型。随后一些多重签名方案[4~6]被提出。这些多重签名方案或是基于传统公钥密码体制[1~3]，随着用户增多，会增加 CA 管理证书的负担。文献[4,5]

收稿日期：2014-06-28；**修回日期**：2014-09-20

基金项目：国家自然科学基金资助项目(61202407, 61173188)；中央高校基本科研业务费专项基金资助项目(WK01100s00033)；安徽省高校优秀青年人才基金资助项目(2012SQRL015)；安徽省高校自然科学研究重点基金资助项目(KJ2013A017)

Foundation Items: The National Natural Science Foundation of China (61202407, 61173188); The Fundamental Research Funds for the Central Universities (WK01100s00033); The Special Foundation for Young Scientists of Anhui Province (2012SQRL015); The Educational Commission of Anhui Province (KJ2013A017)

的多重签名方案是基于身份的，不可避免存在着私钥托管问题。这些多重签名方案都不适合大规模分布式的应用环境。

Al-Riyami 等[7]在 2003 年提出无证书公钥密码学，其中用户私钥由 2 部分组成：用户随机选择的秘密值和密钥生成中心(KGC)产生的部分私钥。用户公钥由用户利用秘密值生成。无证书密码体制解决了传统公钥密码体制的证书管理问题和基于身份密码体制的私钥托管问题。近年来已有不少学者对无证书签名进行研究，具有各种属性的无证书签名[8~12]相继被提出。

Zhang 等在文献[13]中对无证书多重签名进行研究，但提出的方案不满足紧致性，签名长度随签名者个数的增加而增加。ISLAM 等[14,15]提出了高效紧致的无证书多重签名方案，但文献[14]提出的方案缺少形式化的安全性证明过程。秦艳琳等在文献[16]中构造的无证书有序多重签名方案满足高效紧致的特点，并在随机预言机模型下证明方案具有不可伪造性，安全性可归约为 CDH 困难问题。然而现在研究发现秦等方案难以抵抗伪造攻击，本文将给出具体攻击方法，并指出其安全性证明过程中的不足：攻击者在伪造签名消息时需要解决 CDH 问题，这在计算上不可行。随后基于 He 等在文献[11]中的无证书短签名方案构造一个更加高效的无证书有序多重签名方案，最终的签名长度与签名者个数无关，仍具有高效紧凑的特点。方案只有一个签名消息比秦等方案[16]占用更小的通信代价，且在验证过程中，比文献[15，16]的方案使用更少的双线性配对。最后证明方案在随机预言机模型下具有不可伪造性。

2　预备知识

2.1　数学困难问题

定义 1　椭圆曲线离散对数（ECDLP）问题：给定 $P,Q\in G$，求 $a\in Z_q^*$ 满足 $Q=aP$ 是困难的。

定义 2　计算 Diffie-Hellman（CDH）问题：给定 $(P,aP,bP)\in G$，$a,b\in Z_q^*$，计算 $abP\in G$ 是困难的。

2.2　无证书有序多重签名方案

无证书有序多重签名方案主要参与者有 KGC，签名者 $N_i(i=1,2,\cdots,n)$ 和验证者 V 。方案由以下 7 个算法构成[16]。

1) 系统参数生成算法：输入安全参数 k，输出系统参数 *Params* 和系统主密钥 s 。

2) 部分私钥提取算法：输入 $N_i(i=1,2,\cdots,n)$ 的唯一的身份标识 ID_i，系统参数 *Params* 和系统主密钥 s 。KGC 验证 ID_i 后，输出 N_i 的部分私钥 D_i 。

3) 秘密值生成算法：输入 $N_i(i=1,2,\cdots,n)$ 的身份标识 ID_i 和系统参数 *Params* 。 N_i 随机选择 x_i 作为秘密值。

4) 公钥生成算法：输入 $N_i(i=1,2,\cdots,n)$ 的身份标识 ID_i，系统参数 *Params* 和 N_i 的秘密值 x_i 。N_i 输出公钥 P_i 。

5) 私钥生成算法：输入 $N_i(i=1,2,\cdots,n)$ 的身份标识 ID_i，系统参数 *Params*，N_i 的部分私钥 D_i 和秘密值 x_i 。 N_i 输出私钥 $s_i=(x_i,D_i)$ 。

6) 签名算法：输入消息 m，$N_i(i=1,2,\cdots,n)$ 的身份标识 ID_i，系统参数 *Params*，N_i 的私钥 s_i 和签名顺序 K 。按照顺序 K，N_i 验证上一签名者的部分签名 σ_{i-1}，如果有效，则输出部分签名 σ_i 。

7) 验证算法：输入消息 m 、完整签名 σ_n 、$N_i(i=1,2,\cdots,n)$ 的身份标识 ID_i 、系统参数 *Params* 、N_i 的公钥 P_i 和签名顺序 K 。输出签名有效或无效。

2.3　无证书有序多重签名方案安全模型

一般无证书有序多重签名方案存在 2 种类型的攻击者。1) 攻击者 A_I：不知道系统主密钥，但可以替换任意签名者的公钥。2) 攻击者 A_{II}：知道系统主密钥，但不能替换签名者的公钥。

无证书有序多重签名方案安全模型[16,17]可以通过挑战者 D 和攻击者 $A\in\{A_I,A_{II}\}$ 之间的攻击游戏来定义。

①系统参数设置：挑战者 D 运行系统参数生成算法，得到系统参数 *Params* 和系统主密钥 s 。D 将 *Params* 发送给攻击者 A 。如果 $A=A_{II}$，则将 *Params* 和 s 发送给 A 。

②询问：假设攻击者 A 攻破 k 个签名者，即 A 知道 k 个签名者的私钥并能伪造他们的部分签名。攻击者 A 为获得未被攻破签名者的部分签名，向挑战者 D 发起一系列的询问，包括用户生成询问、散列询问、部分私钥询问（只适用于攻击者 A_I）、秘密值询问和公钥替换询问，并得到输出。

③伪造：攻击者输出签名者集合 $N_i(i=1,2,\cdots,n)$ 对消息 m^* 的多重签名 σ_n^*，若满足以下条件，则攻击成功。

a) 攻击者 A 未对 m^* 执行部分签名询问。

b) σ_n^* 是签名者 $N_i(i=1,2,\cdots,n)$ 按签名顺序 K 对 m^* 的有效签名。

定义 3 在随机预言机模型下，攻击者 A 已获得 $k(1\leqslant k\leqslant n)$ 个签名者的私钥。当挑战者 D 在多项式时间 t 内，以不小于概率 ε 输出有序多重签名，则称 A 以 $(\varepsilon,t,q_c,q_h,q_{ps},q_{pk},q_{sk},q_s,(n,k))$ 攻破方案。A 至多做 q_c 次生成用户查询，q_h 次散列查询，q_{ps} 次部分私钥查询（仅适用于 $\mathrm{A_I}$），q_{pk} 次公钥替换查询，q_{sk} 次秘密值查询，q_s 次部分签名查询。

定义 4 如果不存在攻击者 A 以 $(\varepsilon,t,q_c,q_h,q_{ps},q_{pk},q_{sk},q_s,(n,k))$ 攻破方案，则称无证书有序多重签名方案在适应性选择消息攻击下是 $(\varepsilon,t,q_c,q_h,q_{ps},q_{pk},q_{sk},q_s,(n,k))$ 不可伪造的。

3 秦艳琳等无证书有序多重签名方案及安全性分析

3.1 秦艳琳等无证书有序多重签名方案

方案由身份信息分别为 ID_i 的 n 个签名者 $N_i(i=1,2,\cdots,n)$，按照顺序 $K:N_1\rightarrow\cdots\rightarrow N_n$ 对消息 m 进行多重签名，最终的签名消息为 $(m,\sigma_n=(S_n,R_n))$。

方案具体的构造过程可参考文献[16]。

方案用到的符号说明：$N_i(i=1,2,\cdots,n)$ 的公钥记为 P_i，私钥 $s_i=(x_i,D_i)$。(S_i',R_i') 是 N_i 对消息 m 的签名，$\sigma_i=(S_i,R_i)$ 是 N_i 对消息 m 的部分签名，其中 $(S_i=\sum_{j=1}^{i-1}S_j',R_i=\prod_{j=1}^{i-1}R_j')$。

3.2 具体攻击方法

本节给出具体的攻击方法。与文献[16]安全性证明过程一样，假设攻击者 A 攻破 $n-1$ 个签名者 $\{N_1,\cdots,N_{k-1},N_{k+1},\cdots,N_n\}$，A 知道他们的完整私钥。但是 A 不能替换 N_k 的公钥，也不知道系统主密钥。攻击过程如下。

1) 系统参数设置：挑战者 D 运行系统参数生成算法，得到系统参数 $Params=\{G,G_T,e,q,P,P_0,g,H_0,H_1,H_2\}$ 和系统主密钥 s。将 $Params$ 发送给攻击者 A。

2) 询问：攻击者进行签名询问，得到 $N_i(i=1,2,\cdots,n)$ 对消息 m 的多重签名 $(m,\sigma_n=(S_n,R_n))$。

3) 伪造：为了伪造 $N_i(i=1,2,\cdots,n)$ 对消息 m^* 的签名，A 做如下操作。

① A 攻破并控制签名者 $\{N_1,\cdots,N_{k-1},N_{k+1},\cdots,N_n\}$，故 A 知道他们对消息 m 的签名 $(S_i',R_i')(i\in[1,n],i\neq k)$。A 计算 $S_k'=S_n-\sum_{i=1,i\neq k}^{n}S_i'$，$R_k'=R_n/\prod_{i=1,i\neq k}^{n}R_i'$。

② 用签名者 $\{N_1,\cdots,N_{k-1}\}$ 的完整私钥对 m^* 进行签名，得到签名 $(m^*,\sigma_{k-1}^*=(S_{k-1}^*,R_{k-1}^*))$。

③ 伪造签名消息 (m^*,σ_k^*)

A 计算 $h_k=H_2(m\|C_k\|ID_k\|P_k)$，$h_k^*=H_2(m^*\|C_k\|ID_k\|P_k)$，随后计算 $S_k'^*=S_k'\frac{h_k^*}{h_k}$，$R_k'^*=R_k'^{\frac{h_k^*}{h_k}}$。令 $S_k^*=S_{k-1}^*+S_k'^*$，$R_k^*=R_{k-1}^*\cdot R_k'^*$，$(m^*,\sigma_k^*=(S_k^*,R_k^*))$ 是攻击者 A 伪造的对消息 m^* 的部分签名。

4) 用签名者 $\{N_{k-1},\cdots,N_n\}$ 的完整私钥对 m^* 进行签名，得到完整签名 $(m^*,\sigma_n^*=(S_n^*,R_n^*))$。

容易验证 $(m^*,\sigma_n^*=(S_n^*,R_n^*))$ 是签名者 $N_i(i=1,2,\cdots,n)$ 对消息 m^* 有效的无证书多重签名，分析如下，验证者首先计算 $h_i^*=H_2(m^*\|C_i\|ID_i\|P_i)$，$1\leqslant i\leqslant n$。然后计算

$$
\begin{aligned}
&e(S_n^*,P)e(\textstyle\sum_{i=1}^{n}h_i^*H_0(ID_i),P_0)\prod_{i=1}^{n}e(P_i,V_i)^{h_i^*}\\
&=e(\textstyle\sum_{i=1}^{n}S_i'^*,P)\prod_{i=1}^{n}[e(H_0(ID_i),P_0)e(P_i,V_i)]^{h_i^*}\\
&=e(\textstyle\sum_{i=1,i\neq k}^{n}S_i'^*,P)\prod_{i=1,i\neq k}^{n}[e(H_0(ID_i),P_0)e(P_i,V_i)]^{h_i^*}\cdot\\
&\quad e(S_k'\cdot\frac{h_k^*}{h_k},P)[e(H_0(ID_k),P_0)e(P_k,V_k)]^{h_k^*}\\
&=e(\textstyle\sum_{i=1,i\neq k}^{n}(r_i^*P-h_i^*(D_i+x_iV_i)),P)\cdot\\
&\quad(\textstyle\prod_{i=1,i\neq k}^{n}[e(H_0(ID_i),P_0)e(P_i,V_i)]^{h_i^*})\cdot\\
&\quad e((r_kP-h_k(D_k+x_kV_k))\frac{h_k^*}{h_k},P)[e(H_0(ID_k),P_0)e(P_k,V_k)]^{h_k^*}\\
&=e(\textstyle\sum_{i=1,i\neq k}^{n}r_i^*P,P)e(r_k\frac{h_k^*}{h_k}P-h_k^*(D_k+x_kV_k),P)\cdot\\
&\quad[e(H_0(ID_k),P_0)e(P_k,V_k)]^{h_k^*}\\
&=\textstyle\prod_{i=1,i\neq k}^{n}e(r_i^*P,P)\cdot e((r_k\frac{h_k^*}{h_k}P,P)\\
&=\textstyle\prod_{i=1,i\neq k}^{n}e(P,P)^{r_i^*}\cdot e((r_kP,P)^{\frac{h_k^*}{h_k}}\\
&=(\textstyle\prod_{i=1,i\neq k}^{n}R_i'^*)\bullet R_k'^*=R_n^*
\end{aligned}
$$

验证等式成立。

文献[16]在安全性证明过程中假设：攻击者 A 已知消息 m^* 的签名 (m^*,S_n^*,R_n^*)，在伪造阶段 A 对 $\overline{m}$ 伪造签名 $(\overline{m},\overline{S}_n^*,\overline{R}_n^*)$，满足 $\overline{R}_n^*=R_n^*$，最后推导得到等式 $abP=(\overline{h_k}-h_k^*)^{-1}(S_n^*-\overline{S_n^*})-\beta_n^*P_n^*$，即解决 CDH 问题。然而伪造签名 $(\overline{m},\overline{S}_n^*,\overline{R}_n^*)$ 在计算上是不

可行的，等价于解决离散对数困难问题：已知 $\overline{R}_n^* = R_n^*$，A 为了伪造签名随机选择 $\overline{r}_i^*(i=1,\cdots,n-1)$，计算 $\overline{R}_i^{*'} = g^{\overline{r}_i^*}(i=1,\cdots,n-1)$，$\overline{R}_n^{*'} = \overline{R}_n^* / (\overline{R}_1^{*'}\cdots\overline{R}_{n-1}^{*'})$，随后 A 计算部分签名 $\overline{S}_i^{*'} = \overline{r}_i^* P - \overline{h}_i^*(D_i + x_i V_i)(i=1,\cdots, n-1)$，然而 A 必须知道 $\overline{r}_n^*$ 才能计算 $\overline{S}_n^{*'} = \overline{r}_n^* P - \overline{h}_n^*(D_n + x_n V_n)$，然而求 $\overline{r}_n^*$ 等价于求解离散对数困难问题，故 A 在证明过程中为求解 CDH 问题使用的等式（2），在计算上很难求出，故文献[16]方案的安全性不能归约到 CDH 问题。在攻击过程中，A 既没收到系统主密钥也没有执行对 N_k 替换公钥询问，故方案无论对任何类型的攻击者 A_I 或 A_{II} 都不具有不可伪造性。

4　可证安全的无证书有序多重签名方案及安全性分析

秦艳琳等提出的无证书有序多重签名方案，N_i 构造签名消息 S_i' 用到的随机数 r_i 可以任意选择。如果攻击者已知某个消息的多重签名，则可以选择 r_i 以满足验证等式从而伪造签名。本文采用 He 等[11]提出的无证书短签名方案构造一个高效的无证书多重签名方案。方案将随机选择的 r_i 固定于部分私钥中，构造签名消息时不采用可以任意选择的随机数。从而攻击者无法按照 3.2 节介绍的方法伪造签名消息。最后将证明方案在随机预言机模型下不可伪造。

4.1　可证安全的无证书有序多重签名方案

1) 系统参数生成算法：令 G、G_T 是 q 阶循环群，q 为素数，P 是 G 的生成元，$e: G\times G \to G_T$ 表示双线性映射。KGC 随机选择 $s \in Z_q^*$，计算 $P_0 = sP$。H_0、H_1、H_2 表示安全的散列函数，$H_0: \{0,1\}^* \times G_1 \to Z_q^*$，$H_1: \{0,1\}^* \to Z_q^*$，$H_2: \{0,1\}^* \to G_1$。公开系统参数 $Params = \{G, G_T, e, q, P, P_0, H_0, H_1, H_2\}$，保密系统主密钥 s。

2) 部分私钥提取算法：输入 $N_i(i=1,2,\cdots,n)$ 的身份 ID_i，KGC 验证 ID_i 后，选择随机数 $r_i \in Z_q^*$，计算 $R_i = r_i P$，$h_i = sH_0(ID_i, R_i)$，$D_i = r_i + h_i s$，将部分私钥 (D_i, R_i) 秘密发送给 N_i。

3) 秘密值生成算法：$N_i(i=1,2,\cdots,n)$ 随机选择 $x_i \in Z_q^*$ 作为秘密值。

4) 公钥生成算法：$N_i(i=1,2,\cdots,n)$ 计算 $P_i = x_i P$，并公开 $PK_i = (P_i, R_i)$ 作为其公钥。

5) 私钥生成算法：$N_i(i=1,2,\cdots,n)$ 输出 $s_i = (x_i, D_i)$ 作为其完整私钥。

6) 签名算法。

①签名者 N_1 对消息 m 进行签名。

a) 计算 $V_1 = H_1(ID_1 \| K \| P_1 \| R_1 \| P_0)$，其中，$K = \{ID_1, ID_2, \cdots, ID_n\}$；$Q_1 = H_2(m \| ID_1 \| C_1 \| P_1 \| R_1 \| P_0)$，其中 C_1 为长度为 n 的 0-1 串，第 n 位为 1，其余位为 0。

b) 计算 $Sign_1 = (V_1 x_1 + D_1)Q_1$。令 $\sigma_1 = Sign_1$ 是 N_1 对 m 的部分签名。

② 签名者 N_i 对 N_{i-1} 发来的签名消息 (m, σ_{i-1}) 进行验证后再签名。

a) 验证：N_i 构造 C_j；计算 $V_j = H_j(ID_j \| K \| P_j \| R_j \| P_0)$，$Q_j = H_2(m \| ID_j \| C_j \| P_j \| R_j \| P_0)$，$1 \leqslant j \leqslant i-1$。验证等式 $e(\sigma_{i-1}, P) = e(Q_j, \sum_{j=1}^{i-1}(V_j P_j + R_j + h_j P_0))$ 是否成立。若成立则对签名消息 (m, σ_{i-1}) 进行签名，否则终止算法。

b) 计算 $V_i = H_i(ID_i \| K \| P_i \| R_i \| P_0)$，$Q_i = H_2(m \| ID_i \| C_i \| P_i \| R_i \| P_0)$，其中 C_i 为长度为 n 的 0-1 串，第 $n-i+1$ 位为 1，其余位为 0。

c) 计算 $Sign_i = (V_i x_i + D_i)Q_i$。令 $\sigma_i = Sign_i + \sigma_{i-1}$ 是 N_i 对 m 的部分签名。

d) 签名者 $N_i(i=1,2,\cdots,n)$ 对消息 m 的完整签名为 (m, σ_n)，其中 $\sigma_n = \sum_{i=1}^n Sign_i$。

7) 验证算法：验证者对签名消息 (m, σ_n) 进行验证。

验证者构造 C_i；计算 $V_i = H_i(ID_i \| K \| P_i \| R_i \| P_0)$，$Q_i = H_2(m \| ID_i \| C_i \| P_i \| R_i \| P_0)$，$1 \leqslant i \leqslant n$。验证等式 $e(\sigma_n, P) = e(Q_i, \sum_{i=1}^n (V_i P_i + R_i + h_i P_0))$ 是否成立。若成立输出为真，表示签名 (m, σ_n) 正确，否则输出为假。

4.2　方案分析

1) 正确性，方案的正确性证明如下。

证明　假设由签名方案得到多重签名 (m, σ_n)，则

$$\begin{aligned} e(\sigma_n, P) &= e(\sum_{i=1}^n Sign_i, P) \\ &= e(\sum_{i=1}^n (V_i x_i + D_i)Q_i, P) \\ &= \prod_{i=1}^n e((V_i x_i + D_i)Q_i, P) \\ &= \prod_{i=1}^n e(Q_i, (V_i P_i + R_i + h_i P_0)) \\ &= e(Q_i, \sum_{i=1}^n (V_i P_i + R_i + h_i P_0)) \end{aligned}$$

2) 抗伪造性，可以证明在随机预言机模型下，针对攻击者 A_I,A_{II}，本方案都是不可伪造的。

定理 1 在随机预言机模型下，如果第 1 类攻击者 A_I 能够以不可忽略的概率伪造出多重签名，则 A_I 能够解决 CDH 问题。

定理 2 在随机预言机模型下，如果第 2 类攻击者 A_{II} 能够以不可忽略的概率伪造出多重签名，则 A_{II} 能够解决 CDH 问题。

证明 不失一般性假设 A_{II} 已攻破 $N_1,\cdots,N_{n-1}$，为伪造多重签名 A_{II} 需要伪造 N_n 的签名。假设存在攻击者 A_{II} 能以不可忽略的概率 ε 攻破改进方案，则挑战者 D 能利用 A_{II} 解决 CDH 问题，即 D 已知 $P_1=aP,P_2=bP$, 最终能输出 abP。D 选择随机数 $s\in Z_n^*$，令 $P_0=sP$，将系统参数和系统主密钥 s 发送给攻击者 A_{II}。A_{II} 执行如下询问，为模拟询问，D 维护表 L_0、L_1、L_2 分别对应对 H_0、H_1、H_2 的询问，表 L_{k1}、L_{k2} 分别对应部分私钥和秘密值的询问。

散列询问。H_0 询问：A_{II} 输入 (ID_i,R_{ID_i})，如果 L_0 包含 (ID_i,R_{ID_i},h_{ID_i})，则 D 返回 h_{ID_i} 给 A_{II}。否则 D 选择随机数 $h_{ID_i}\in Z_q^*$ 返回给 A_{II}，同时将 (ID_i,R_{ID_i},h_{ID_i}) 写入 L_0。H_1 询问：A_{II} 输入 $(ID_i,P_{ID_i},R_{ID_i},P_0)$，如果 L_1 包含 $(ID_i,P_{ID_i},R_{ID_i},P_0,V_{ID_i})$，则 D 返回 V_{ID_i} 给 A_{II}。否则，D 选择随机数 $V_{ID_i}\in Z_q^*$ 返回给 A_{II}，同时将 $(ID_i,P_{ID_i},R_{ID_i},P_0,V_{ID_i})$ 写入 L_1。H_2 询问：A_{II} 输入 $(m_k,ID_i,P_{ID_i},R_{ID_i},P_0)$，如果 L_2 包含 $(m_k,ID_i,P_{ID_i},R_{ID_i},P_0,Q_i,t_i,c_i)$，则 D 返回 Q_i 给 A_{II}。否则，D 选择随机数 $c_i\in\{0,1\}$ 满足 $\Pr[c_i=0]=(1/(q_s+1))$，$t_i\in Z_q^*$，计算 $Q_i=(1-c_i)P_2+t_iP$ 返回给 A_{II}，同时将 $(m_k,ID_i,P_{ID_i},R_{ID_i},P_0,Q_i,t_i,c_i)$ 写入 L_2。

部分私钥询问。A_{II} 询问 ID_i 的部分私钥。D 生成 2 个随机数 $a_{ID_i},b_{ID_i}\in Z_n^*$，令 $r_{ID_i}\leftarrow a_{ID_i}$，$R_{ID_i}\leftarrow a_{ID_i}P$，$h_{ID_i}=H_0(ID_i,R_{ID_i})\leftarrow b_{ID_i}$，计算 $s_{ID_i}=r_{ID_i}+h_{ID_i}s$。最后 D 将 (ID_i,R_{ID_i},h_{ID_i}) 和 (ID_i,s_{ID_i},R_{ID_i}) 分别写入表 L_0 和 L_{k1}。

秘密值询问。A_{II} 询问 ID_i 的秘密值。① $ID_i\neq ID_n$，D 选择随机数 $x_{ID_i}\in Z_n^*$，计算 $P_{ID_i}=x_{ID_i}P$，将 x_{ID_i} 返回给 A_{II} 同时将 (ID_i,x_{ID_i},P_{ID_i}) 写入 L_{k2}。② $ID_i=ID_n$，令 $P_{ID_i}\leftarrow P_1$ 同时将 $(ID_i,\perp,P_{ID_i})$ 写入 L_{k2}。

签名查询。A_{II} 询问 (m_k,ID_i) 的签名。D 在列表 L_{k1},L_{k2} 查找 ID_i 的部分私钥 (ID_i,s_{ID_i},R_{ID_i}) 和秘密值 (ID_i,x_{ID_i},P_{ID_i})。随后 D 执行 H_2 询问得到 $Q_i=H_2(m_k,ID_i,P_{ID_i},R_{ID_i},P_0)$ 对应于表 L_2 中 $(m_k,ID_i,P_{ID_i},R_{ID_i},P_0,Q_i,t_i,c_i)$。① $c_i=0$，D 报错并停止执行。② $c_i=1$，则 $Q_i=t_iP$，D 返回签名 $Sign_{ID_i}=t_i(V_{ID_i}P_{ID_i}+R_{ID_i}+h_{ID_i}P_0)$。

最后 A_{II} 输出一个有效的签名 (ID_n,m_n,σ_n)。D 计算 $Q_n=H_2(m_n,ID_n,P_{ID_n},R_{ID_n},P_0)$，其中，$(P_{ID_n},R_{ID_n})$ 是 ID_n 的原始公钥，随后验证等式 $e(\sigma_n,P)=e(Q_n,(V_{ID_n}P_{ID_n}+R_{ID_n}+h_{ID_n}P_0))\prod_{i=1}^{n-1}e(\sigma_i,P)$ 是否成立。如果等式不成立，则 D 报错并停止执行，否则得到 $e(Sign_n,P)=e(Q_n,(V_{ID_n}P_{ID_n}+R_{ID_n}+h_{ID_n}P_0))$，其中，$(m_n,ID_n,P_{ID_n},R_{ID_n},P_0,Q_n,t_n,c_n)$ 也是表 L_2 中的元素。考虑 $c_n=0$，$Q_n=bP+t_nP$，则 $\sigma_n=(b+t_n)\cdot(V_{ID_n}a+r_{ID_n}+h_{ID_n}s)P$，那么 D 能输出 $abP=(V_{ID_n})^{-1}\cdot(\sigma_n-t_n(V_{ID_n}P_1+R_{ID_n}+h_{ID_n}P_0)-(r_{ID_n}+h_{ID_n}s)P_2)$。所以，如果 A_{II} 能成功伪造合法的多重签名，则挑战者 D 能够解决 CDH 困难问题。

3) 效率分析

将一次双线性运算记为 BP，群 G 的乘法运算记为 M，G_T 上的幂运算记为 E，G_T 上的乘法运算记为 MT。与文献[16]类似，方案运算量不考虑预计算 $V_i=H_i(ID_i\|K\|P_i\|R_i\|P_0)$，$Q_i=H_2(m\|ID_i\|C_i\|P_i\|R_i\|P_0)$ 等。可以看出改进方案最终的多重签名为 σ_n，与单用户签名一样且只有一个签名消息，从表 1 可以看出改进方案的效率略高于原方案，因此比原方案占用更少的计算代价和通信代价，更加高效。同时签名长度不随签名人数的变化而变化，也是紧凑的多重签名方案。

表 1 效率比较

方案	部分签名	部分验证	整体验证
原方案	1M+1E	1BP+1MT	1BP+1MT
改进方案	1M	1BP	1BP

5 结束语

有序多重签名可用于解决信任链推荐信息的认证问题，而无证书密码体制解决了传统公钥密码体制的证书管理和基于身份密码体制的私钥托管问题。秦艳琳等提出了无证书有序多重签名方案，并证明方案

的安全性在随机预言机模型下可归约为 CDH 困难问题。然而本文研究发现秦等的方案难以抵抗伪造攻击且安全性证明存在不足：证明过程需要求解离散对数困难问题，这在计算上不可行。本文基于无证书短签名给出更加高效的无证书有序多重签名方案，并在随机预言机模型下证明方案的安全性。

参考文献：

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

[2] HARDJONO T, ZHENG Y. A practical digital multisignature scheme based on discrete logarithms[A]. Advances in Cryptology-AUSCRYPT'92, LNCS718[C]. Berlin, Springer-Verlag, 1992. 122-132.

[3] MICALI S, OHTA K, REYZIN L. Accountable-Subgroup multisignatures[A]. Pmc of the 8th ACM Conf on Computer and Communications Security[C]. 2001.245-254.

[4] 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.

[5] HARN L, REN J. Efficient identity-based RSA multisignatures[J]. Computers & Security, 2010, 27(3):12-15.

[6] LU S, OSTROVSKY R, SAHAI A, *et al*. Sequential aggregate signatures, multisignatures, and verifiably encrypted signatures without random oracles[J]. Journal of Cryptology, 2013, 26(2):340-373.

[7] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[A]. Proc of Asiacrypt 2003[C]. Springer-Verlag, Berlin, 2003.452-473.

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

[9] TIAN M M, HUANG L S. Cryptanalysis of a certificateless signature scheme without pairings[J]. International Journal of Communication Systems, 2013, 26(11): 1375-1381.

[10] TIAN M M, YANG W, HUANG L S. Cryptanalysis and improvement of a certificateless multi-proxy signature scheme[J]. Fundamenta Informaticae, 2014, 129(4): 365-375.

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

[12] TIAN M M, HUANG L S, YANG W. Practical certificateless short signature scheme[J]. International Journal of Electronic Security and Digital Forensics, 2014, 6(3): 204-218.

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

[14] ISLAM S H, BISWAS G P. Certificateless strong designated verifier multisignature scheme using bilinear pairings[A]. Proceedings of the International Conference on Advances in Computing, Communications and Informatics[C]. Chennai, India, 2012.540-546.

[15] ISLAM S K, BISWAS G P. Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings[J]. Journal of King Saud University-Computer and Information Sciences, 2014, 26(1): 89-97.

[16] 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.

[17] ZHANG Z F, WONG DC S, XU J, *et al*. Certificateless public-key signature: security model and efficient construction[A]. ACNS'06: Proceedings of 4th International Conference on Applied Cryptography and Network Security[C].Berlin, Germany, 2006.

作者简介：

许艳（1981-），女，江苏泗洪人，中国科学技术大学博士生，主要研究方向为信息安全和无线传感网络。

黄刘生（1957-），男，安徽安庆人，中国科学技术大学教授、博士生导师，主要研究方向为无线传感网络、信息安全和分布式计算。

田苗苗（1987-），男，安徽阜阳人，博士，中国科学技术大学博士后，主要研究方向为信息安全和无线传感网络。

仲红（1965-），女，安徽固镇人，博士，安徽大学教授、博士生导师，主要研究方向为信息安全，高性能计算。