doi:10.3969/j.issn.1000-436x.2013.07.012

高效的无证书有序多重签名方案

秦艳琳，吴晓平
（海军工程大学 信息安全系，湖北 武汉 430033）

摘 要：针对分布式环境下信任建模中信任链上推荐信息的认证问题，研究了无证书有序多重签名方案的安全模型，进而基于椭圆曲线密码和双线性映射提出一个无证书有序多重签名方案，并在随机预言机模型下，证明方案的安全性建立在计算 Diffie-Hellman 问题的困难性上。该方案无需证书管理中心，多重签名的长度与单用户的签名长度相当，与签名人数无关，在部分签名阶段不需双线性对运算，在部分签名及整体签名的验证阶段都只需一个双线性对运算，与同类方案相比，具有运行效率上的优势，可方便地应用于大规模分布式环境下信任传播的过程中。

关键词：无证书公钥密码；多重签名；双线性映射；计算 Diffie-Hellman 问题；随机预言机
中图分类号：TP309 **文献标识码：**A **文章编号：**1000-436X(2013)07-0105-06

Efficient certificateless sequential multi-signature scheme

QIN Yan-lin, WU Xiao-ping
(Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: The authentication of recommendation information transmitted through trust train is important for trust model in distributed environment. To solve this problem, the security model for the certificateless sequential multi-signature scheme was studied and then a certificateless sequential multi-signature scheme using elliptic curve cryptography and bilinear pairings was proposed. It is proven in the random oracle that the security of the scheme is based on the fact that the computational Diffie-Hellman problem is hard. Meanwhile, the scheme needs no certificate management center and the length of signature is independent of the number of signers. It needs no bilinear pairing operation in the phase of partial signing, and just needs one each in verification phases of partial signing and integral signing. So it is computationally efficient compared to the existing signature schemes and can be applied conveniently to trust transitivity in large scale distributed environment.

Key words: certificateless cryptography; multi-signature; bilinear pairing; computational Diffie-Hellman problem；random oracle

1 引言

多重数字签名是一种特殊的数字签名方案，指多个用户对同一消息实施签名，根据不同的应用环境，多重签名可分为有序多重签名方案和无序多重签名方案。其中有序多重签名是指各签名者按照特定的顺序依次对消息进行签名；而在无序多重签名方案中各签名者则对消息实施无序的并行签名。

目前，分布式环境下信任建模过程中往往涉及信任传播问题：推荐信息在信任链上进行传递时，如果没有建立有效的认证机制，网络中存在的恶意节点将会对推荐信息进行篡改和伪造，进而影响节点间真实信任关系的建立，因此需要采取数字签名技术确保信息的真实性和完整性。同时，推荐信息传递中使用的签名方式具有以下特点：1）信任链上的网络节点在确认了它前面节点推荐信息的真实性之后，再附加自己的签名，有序多重签名恰好

收稿日期：2012-11-01；修回日期：2013-01-02
基金项目：国家自然科学基金青年基金资助项目(61100042)
Foundation Item: The National Natural Science Foundation of China (project for youth) (61100042)

能够满足此类签名需求；2）基于传统公钥密码体制的有序多重签名方案[1~3]需要证书中心(CA)为用户签发公钥证书，以确保系统中用户公钥的真实性和有效性，而公钥证书库的维护和管理需要消耗大量的计算、存储和通信资源，不适合大规模分布式环境下信任传播的具体应用环境；3）通过基于身份公钥体制构造的多重签名方案[4~7]无需公钥证书，但却存在私钥托管问题。

部分学者提出基于无证书公钥密码的多重签名方案[8~12]，但效率不高或签名长度随签名人数的增加而增长。因此，本文在分析无证书有序多重签名定义及安全模型的基础上，基于文献[13]中的无证书签名方案构造了一种安全、高效的有序多重签名方案。该方案得到的多重签名长度与单个签名者的签名长度相当。同时，部分签名的验证及整体签名的验证除可进行预计算的部分运算外都仅需要一个对运算，具有较高的运算效率，并且在随机预言机模型下，将该方案的安全性归结为计算Diffie-Hellman的困难问题。

2 无证书有序多重签名的定义及安全模型

2.1 无证书有序多重签名的定义

无证书有序多重签名方案主要由密钥生成中心(KGC)、签名用户 $N_i(i=1,2,\cdots,n)$、签名顺序 $?$ 和验证者 V 构成。需要执行7个算法：Setup (系统参数的生成)、Partial-Private-Key-Extract (部分私钥提取)、Set-Secret-Value (秘密值生成)、Set-Public- Key (生成公钥)、Set-Private-Key(生成私钥)、Sign (签名)和 Verify(验证)。

1) Setup：KGC 输入安全参数，生成系统公共参数和主密钥。

2) Partial-Private-Key-Extract：输入用户 $N_i(i=1,2,\cdots,n)$的身份 ID_i，KGC 认证用户身份有效后，输出 N_i 的部分私钥 D_i，并安全传送给 N_i。

3) Set-Secret-Value：N_i 选择随机值 x_i 作为秘密值。

4) Set-Public-Key：N_i 由秘密值计算对应的公开钥。

5) Set-Private-Key：N_i 将自己的完整私钥设为 (x_i,D_i)。

6) Sign：所有的签名者$\{N_1,N_2,\cdots,N_n\}$按照规定顺序 $?$ 执行：签名成员 N_i $(i=2,\cdots,n)$对上一位签名成员的部分签名 s_{i-1} 进行验证；若有效，则使用自己的私钥输出部分签名 s_i。

7) Verify：验证者 V 对签名消息进行验证，以 (m,s_n)、签名顺序 $?$、$N_i(i=1,2,\cdots,n)$的身份 ID_i 及公钥作为算法输入，以一个判定∈{真,假}作为输出，签名有效，当且仅当判定为真。

2.2 无证书有序多重签名的安全模型

本节在文献[1]和文献[14]的基础上提出无证书有序多重签名的安全模型。针对有序多重签名方案的攻击手段主要有以下2种。

1) 随机预言机模型下，敌手能够掌握签名者集合中一部分成员的签名私钥（但无法得到所有签名者私钥）情形下的适应性选择消息伪造签名攻击。

2) 签名成员通过随意交换签名先后顺序进行的攻击。

一般地，在无证书签名方案的安全模型中，存在2种类型的敌手：第一类敌手 A_{I} 和第二类敌手 A_{II}。敌手 A_{I} 可以用自己选择的参数替换任意用户的公钥，但是不能访问到KGC的主密钥；敌手 A_{II} 可以获得系统主密钥，但是无法替换用户的公开钥。

利用CDH挑战者 D 和一个敌手 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$之间的游戏 P 定义无证书有序多重签名在适应性选择消息伪造签名攻击下的安全模型具体如下。

1) 系统参数设置。D 运行 Setup 算法，输出系统公共参数和主密钥。D 将系统公共参数发送给 A。如果 A 是第二类敌手，D 需要将公共参数和主密钥一起发送给 A。

2) 询问。假设 n 个签名成员 $N_1,N_2,\cdots,N_n$ 中有 $k(1\le k<n)$个签名者被敌手 A 控制，即敌手 A 可以获得这 k 个签名成员的签名私钥，从而可以生成这 k 个签名成员的合法部分签名。

A 为得到未被控制签名者的部分签名，执行用户生成询问、散列询问、部分私钥询问(只适用于 A_{I})、秘密值询问和公钥替换询问并得到输出。

3) 伪造。在多项式次提问之后，A 输出一个伪造签名（m^*，$?^*$，s_n^*），满足下列条件。

① s_n^* 是对应于签名顺序 $?^*$ 和用户 $\{N_i\}_{i=1,2,\cdots,n}$ 的公开密钥的合法签名。

② m^* 没有被 A 执行过部分签名询问。

若上述条件全部成立，则 D 输出接受；否则输出拒绝。

定义1 敌手 A 在随机预言机模型下，掌握无证书有序多重签名方案 n 个签名成员中 k $(1\le k<n)$ 个签名者的私钥。称 A 以$(e,q_c,q_h,q_{ps},q_{pk},q_{sk},q_s,(n,k),t)$攻破该方案，当且仅当 D 以超过 e 的

成功概率。最多在时间 t 内在上述游戏中输出接受，其中 A 至多做 q_c 次生成用户询问、q_h 次散列询问、q_{ps} 次部分私钥询问(仅适用于 A_I)、q_{pk} 次公钥替换询问、q_{sk} 次秘密值询问和最多 q_s 次部分签名提问。

定义 2　一个无证书有序多重签名方案在适应性选择消息攻击下是$(e, q_c, q_h, q_{ps}, q_{pk}, q_{sk}, q_s, (n,k), t)$不可伪造的，当且仅当不存在敌手 A 可以$(e, q_c, q_h, q_{ps}, q_{pk}, q_{sk}, q_s, (n,k), t)$攻破该方案。

3　新的无证书有序多重签名方案

本节将基于椭圆曲线密码体制和双线性对设计一种无证书有序多重签名方案，用于大规模分布式环境下推荐信息在信任路径上的安全传递。设某条推荐信任路径上的 n 个节点 $N_i(1\le i\le n)$，按照推荐信息在信任路径上传递的顺序 $N_1? N_2? \cdots ? N_n$ 对推荐节点 N_1 提供的推荐信息 m 进行多重签名，$N_i(1\le i\le n)$的身份信息 $ID_i\in\{0,1\}^*(1\le i\le n)$。具体的签名方案包括以下几个多项式时间算法。

1) Setup Phase：该算法选取正整数 k 作为输入的安全参数，返回系统参数和主密钥。KGC 执行以下步骤。

① 选择由椭圆曲线上的点构成的阶为素数 q 的加法循环群$(G,+)$，和阶为 q 的乘法循环群$(G_T,\cdot)$，双线性映射 $\hat{e}: G\times G? G_T$；

② 选择安全哈希函数 H_0，H_1：$\{0,1\}^*? G^*$，H_2：$\{0,1\}^*? Z_q^*$。选择 $s\in Z_q^*$，G 的一个生成元 P，计算 $P_0=sP$，其中(P_0, s)是系统主公/私钥对，设 $g=\hat{e}(P, P)$，公布系统参数 $O=(G,G_T,\hat{e},q,P,P_0,g,H_0,H_1,H_2)$，对系统主私钥 s 严格保密。

2) Partial-Private-Key-Extract Phase：该算法接受用户 N_i 的身份 ID_i（$1\le i\le n$），系统主私钥 s 及 O 作为输入，产生 N_i 的部分私钥 $D_i=sQ_i=sH_0(ID_i)$，并通过一个秘密信道安全传送给 N_i。

3) Set-Secret-Value Phase：该算法由签名节点 N_i（$1\le i\le n$）运行，将 ID_i（$1\le i\le n$）作为输入，选择一个随机值 $x_i\in Z_q^*$作为 N_i（$1\le i\le n$）的秘密值。

4) Set-Public-Key Phase：N_i（$1\le i\le n$）计算公开密钥 $P_i=x_iP$，把 P_i 对外公开。

5) Set-Private-Key Phase：节点 N_i（$1\le i\le n$）设置(D_i, x_i)作为自己的完整私钥。

6) Sign Phase：设推荐节点 N_1 向请求节点 Re 反馈推荐信息 m，为确保该推荐信息在传递过程中不被篡改，N_1 将首先对 m 进行签名，进而该条信任路径上的中间节点 $N_i(2\le i\le n)$将以 $N_2? \cdots ? N_n$ 为签名顺序对 m 进行多重签名，算法的具体步骤如下。

① 节点 N_1 首先执行以下步骤对推荐信息 m 进行签名。

ⓐ 选择随机数 $r_1\in Z_q^*$，计算 $R_1'=g^{r_1}$；

ⓑ 计算 $V_1=H_1(ID_1\|P_1\|?)$，其中 $?=\{ID_1,ID_2,\cdots,ID_n\}$；

ⓒ 计算 $h_1=H_2(m\|C_1\|ID_1\|P_1)$，其中，$C_1$=(000…001)为 n 位的 0-1 序列，满足第 n 位为 1，其余位为 0；

ⓓ 计算 $S_1'=r_1P-h_1(D_1+x_1V_1)$。

令 $R_1=R_1', S_1=S_1'$，则 $s_1=(S_1,R_1)$ 即为 N_1 对 m 的签名。然后 N_1 将自己签名后的推荐信息$(m,s_1=(S_1,R_1))$发送给信任路径上的下一节点 N_2。

② 节点 N_2 收到 N_1 的签名信息 $s_1=(S_1,R_1)$ 后，首先验证签名的有效性，进而附上自己的签名，具体过程如下：

ⓐ 计算 $V_1=H_1(ID_1\|P_1\|?)$，$h_1=H_2(m\|C_1\|ID_1\|P_1)$，验证等式 $R_1=\hat{e}(S_1,P)[\hat{e}(H_0(ID_1),P_0)\hat{e}(P_1,V_1)]^{h_1}$ 是否成立，若成立则认为 N_1 的签名信息有效，继续下一步；否则认为该推荐信息已被篡改；

ⓑ 选择随机数 $r_2\in Z_q^*$，计算 $R_2'=g^{r_2}$；

ⓒ 计算 $V_2=H_1(ID_2\|P_2\|?)$，$h_2=H_2(m\|C_2\|ID_2\|P_2)$，其中，$C_2$=(000…010)为 n 位的 0-1 序列，满足第 n-1 位为 1，其余位为 0；

ⓓ 计算 $S_2'=r_2P-h_2(D_2+x_2V_2)$；

ⓔ 令 $R_2=R_1\cdot R_2', S_2=S_1+S_2'$，则 $s_2=(S_2,R_2)$ 为 N_2 对 m 的部分签名，N_2 发送签名信息给 N_3。

③ $N_i(3\le i\le n)$在对前面节点传递的签名信息(m,s_{i-1})验证有效后，自己进行签名。具体步骤如下：

ⓐ 由签名的先后顺序构造 C_j，$1\le j\le i$-1；

ⓑ 计算 $V_j=H_1(ID_j\|P_j\|?)$，$h_j=H_2(m\|C_j\|ID_j\|P_j)$，$1\le j\le i$-1，验证 $R_{i-1}=\hat{e}(S_{i-1},P)\hat{e}(\sum_{j=1}^{i-1}h_jH_0(ID_j),P_0)\prod_{j=1}^{i-1}\hat{e}(P_j,V_j)^{h_j}$ 是否成立，若成立则认定前面节点传递的签名信息有效，继续下一步，否则认为该推荐信息在传递过程中已被恶意节点篡改，停止传递；

ⓒ 选择随机数 $r_i \in Z_q^*$，计算 $R_i' = g^{r_i}$；

ⓓ 计算 $V_i=H_1(ID_i\|P_i\|?)$，$h_i = H_2(m \| C_i \| ID_i \| P_i)$，其中，$C_i$=(0…010…0) 为 n 位的 0-1 序列，第 n- i+1 位为 1，其余位为 0；

ⓔ 计算 $S_i' = r_i P - h_i(D_i + x_i V_i)$；

ⓕ 令 $R_i = R_{i-1} \cdot R_i'$，$S_i = S_{i-1} + S_i'$，则 $s_i = (S_i, R_i)$ 为 N_i 对 m 的部分签名，N_i 将附加了自己签名的推荐信息(m,s_i)发送给下一个签名节点，直到 N_n 完成对 m 的部分签名；

ⓖ 推荐信任路径上的节点 $N_1, N_2,\cdots,N_n$ 依次完成对推荐信息 m 的多重签名$(m, s_n = (S_n, R_n))$，其中，$R_n = \prod_{i=1}^{n} R_i'$，$S_n = \sum_{i=1}^{n} S_i'$。

7) Verify Phase：请求节点 Re 在收到由某条信任路径上的各节点对推荐信息的多重签名$(m, s_n = (S_n, R_n))$后，利用信任路径上节点 N_i 的公开密钥 P_i 及身份信息 ID_i，$1 \le i \le n$，执行下列步骤对传递来的签名信息进行验证。

① 由签名的先后顺序构造 C_i，$1 \le i \le n$；

② 计算 $V_i=H_1(ID_i\|P_i\|?)$，$h_i = H_2(m \| C_i \| ID_i \| P_i)$，$1 \le i \le n$。

验证等式 $R_n = \hat{e}(S_n, P)\ \hat{e}(\sum_{i=1}^{n} h_i H_0(ID_i), P_0)\ \prod_{i=1}^{n} \hat{e}(P_i, V_i)^{h_i}$ 是否成立，若成立，则认定通过该条信任路径传递的推荐信息没有被恶意节点篡改；否则舍弃该信息。

下面给出上述有序多重签名方案的正确性证明。

证明 假设有序多重签名$(m, s_n = (S_n, R_n))$是由上述签名方案得到的，则必然满足下列等式：

$$R_n = \hat{e}(S_n, P)\ \hat{e}(\sum_{i=1}^{n} h_i H_0(ID_i), P_0)\ \prod_{i=1}^{n} \hat{e}(P_i, V_i)^{h_i}$$

$$= \hat{e}(\sum_{i=1}^{n} S_i', P)\ \prod_{i=1}^{n} [\hat{e}(H_0(ID_i), P_0)\ \hat{e}(P_i, V_i)]^{h_i}$$

$$= \hat{e}(\sum_{i=1}^{n} [r_i P - h_i(D_i + x_i V_i)], P) \cdot \prod_{i=1}^{n} [\hat{e}(H_0(ID_i), P_0)\ \hat{e}(P_i, V_i)]^{h_i}$$

$$= \prod_{i=1}^{n} \hat{e}(P, P)^{r_i}\ \prod_{i=1}^{n} [\hat{e}(sH_0(ID_i), P)^{-h_i}\ \hat{e}(x_i V_i, P)^{-h_i}] \cdot \prod_{i=1}^{n} [\hat{e}(H_0(ID_i), P_0)\ \hat{e}(P_i, V_i)]^{h_i}$$

$$= \prod_{i=1}^{n} \hat{e}(P, P)^{r_i} = \prod_{i=1}^{n} R_i' = R_n \text{。}$$

另外，信任路径上的节点 $N_i(2 \le i \le n)$收到前一个节点的签名信息(m,s_{i-1})后，验证等式 $R_{i-1} = \hat{e}(S_{i-1}, P)\ \hat{e}(\sum_{j=1}^{i-1} h_j H_0(ID_j), P_0)\ \prod_{j=1}^{i-1} \hat{e}(P_j, V_j)^{h_j}$ 的正确性证明同上。

4 安全性分析

定义 3 Computational Diffie-Hellman(CDH) Problem(计算 Diffie-Hellman 问题)：给定$(P,aP,bP) \in G$，$a,b \in Z_q^*$，在群 G 上计算 abP 是困难的。

定义 4 Elliptic Curve Discrete Logarithm Problem(椭圆曲线离散对数问题)：给定 P，$Q \in G$，计算 $a \in Z_q^*$ 使 $Q=aP$ 是困难的。

在以上定义的 2 类难题的基础上，本文所提多重签名方案在 A_I 是适应性选择消息攻击下第 I 类敌手的情况下是不可伪造的。

定理 1 在随机预言机模型下，若有敌手 A_I 以不可忽略的概率伪造出可以通过验证的有序多重签名，挑战者 D 可利用该敌手的伪造解决一个特定的 CDH 问题。

证明 假设攻击情形对于敌手 A_I 最为有利，他能够控制签名节点集$(N_1,N_2,\cdots,N_n)$中的 n- 1 个节点，但无法控制第 k 个签名节点 N_k。则 A_I 掌握了 n- 1 个签名节点 $N_i(1 \le i \le n, i?k)$的私钥。D 是 CDH 问题挑战者。哈希函数 H_0，H_1，H_2 是随机预言机，给定$\{P,aP,bP\}$，D 期望通过 A_I 伪造签名的过程计算出 abP。为了达到挑战目的，D 需要设置系统参数：$P_0=aP$ 及 $O=(G, G_T, \hat{e}, q, P, P_0, g, H_0, H_1, H_2)$。

D 把设置好的系统参数发送给 A_I。由于 A_I 掌握了签名者 $N_1, N_2,\cdots, N_{k-1}, N_{k+1},\cdots, N_n$ 的签名私钥。所以 A_I 只需通过执行 H_0，H_1，H_2 散列询问、生成用户询问、部分私钥询问、秘密值询问、公钥代替询问和部分签名询问（询问过程与文献[13]类似）得到第 k 个签名成员 N_k 的部分签名，进而 A_I 能以不可忽略的概率在时间 t 内输出一个对于从未被询问过的消息 m^*的合法的有序多重签名 (m^*, S_n^*, R_n^*)。签名过程为 (m^*, S_1^*, R_1^*)？ (m^*, S_2^*, R_2^*)？ …

？（m^*，S_k^*，R_k^*）？…？（m^*，S_n^*，R_n^*）。接下来 D 再次利用 A_{I} 得到在从未被询问过的消息 $\overline{m}$ 上的一个合法的有序多重签名（$\overline{m}$，$\overline{S}_n^*$，$\overline{R}_n^*$）。具体签名过程为（$\overline{m}$，$\overline{S}_1^*$，$\overline{R}_1^*$）？（$\overline{m}$，$\overline{S}_2^*$，$\overline{R}_2^*$）？…？（$\overline{m}$，$\overline{S}_k^*$，$\overline{R}_k^*$）？…？（$\overline{m}$，$\overline{S}_n^*$，$\overline{R}_n^*$）。根据分叉引理[15]，D 以不可忽略的概率得到对于 m^* 的 2 个伪造有序多重签名（m^*，S_n^*，R_n^*）和（m^*，$\overline{S}_n^*$，R_n^*）。则有方程组

$$R_n^* = \hat{e}(S_n^*, P)\ (\prod_{i\neq k}[\hat{e}(H_0(ID_i), P_0)\ \hat{e}(P_i, V_i)]^{h_i^*}) \cdot [\hat{e}(H_0(ID_k^*), P_0)\ \hat{e}(P_k^*, V_k^*)]^{h_k^*} \quad (1)$$

$$R_n^* = \hat{e}(\overline{S}_n^*, P)\ (\prod_{i\neq k}[\hat{e}(H_0(ID_i), P_0)\ \hat{e}(P_i, V_i)]^{h_i^*}) \cdot [\hat{e}(H_0(ID_k^*), P_0)\ \hat{e}(P_k^*, V_k^*)]^{\overline{h}_k^*} \quad (2)$$

其中，$h_k^* \neq \overline{h}_k^*$，由式(1)和式(2)即得

$$\hat{e}(S_n^*, P)\ [\hat{e}(H_0(ID_k^*), P_0)\ \hat{e}(P_k^*, V_k^*)]^{h_k^*} = \hat{e}(\overline{S}_n^*, P)\ [\hat{e}(H_0(ID_k^*), P_0)\ \hat{e}(P_k^*, V_k^*)]^{\overline{h}_k^*}$$

由于 $Q_k^* = bP, V_k^* = b_k^* P$，故可以得到

$$abP = (\overline{h}_k^* - h_k^*)^{-1}(S_n^* - \overline{S}_n^*) - b_k^* P_k^*$$

这样，如果 A_{I} 能成功伪造合法的有序多重签名，D 就可以通过 A_{I} 的伪造过程解决一个特定的 CDH 困难问题，与定义 3 矛盾。

以上讨论了在对攻击者最有利的攻击模型下，即 A_{I} 控制 n-1 个签名节点的情况下，本文所提无证书有序多重签名方案能够抵制适应性选择消息攻击，因此方案的安全性也达到最强。

定理 2　在随机预言机模型下，若有敌手 A_{II} 以不可忽略的概率伪造出可以通过验证的有序多重签名，挑战者 D 可利用该敌手的伪造解决一个特定的 CDH 问题。

证明　设 $P_0 = s'P$，D 将主密钥 s' 与系统参数都发送给 A_{II}。A_{II} 通过散列询问、生成用户询问、秘密值询问、公钥代替询问以及签名询问来得到第 k 个签名成员 N_k 的部分签名，这里 A_{II} 无需进行部分私钥询问，因为 A_{II} 可以获得系统主密钥 s'，进而可以计算出所有用户的部分私钥。其他伪造攻击过程与定理 1 类似，此处略去。

对于签名成员擅自交换签名顺序的攻击，由于方案中的签名成员 $N_i(2\leq i\leq n)$ 进行部分签名时，必须首先使用固定的签名顺序？和 0-1 序列 $C_j(1\leq j\leq i\text{-}1)$ 对前一个签名者的部分签名进行验证并证实有效后，才可以进行当前签名，故能保证多重签名方案的有序性。

5　效率分析

为便于比较，将双线性对运算记为 BP，椭圆曲线 G 上的标量点乘运算记为 SM，G_T 上的乘法运算记为 E。其中，双线性对所消耗的运算时间远高于其他运算。由于方案中所涉及的 $V_i=H_1(ID_i\|P_i\|?)$，$h_i = H_2(m \| C_i \| ID_i \| P_i)$，$(D_i + x_i V_i)$ 等可以进行预计算，对实际应用中整个多重签名方案的运行效率影响不大，因此没有被统计到方案的运算量内。从表 1 可以看出，在本文方案中，部分签名的验证及整体签名的验证都仅需要一个对运算，具有较高的运算效率。并且通过分析本文给出的多重签名算法可知，最终多重签名 $s_n = (S_n, R_n)$ 的长度和单用户签名长度相当，不随签名人数的变化而变化，因此该算法为一个高效的紧致多重签名方案。

表 1　效率比较

方案	部分签名	部分验证	整体验证	是否紧致
文献[8]中的方案	2SM	iBP+(i-1)E	(n+1)BP+nE	否
文献[9]中的方案	2SM	2BP+1E	2BP+1E	是
文献[10]中的方案	4SM	(2i-1)BP+(2i-2)E	(2n+1)BP+2nE	否
文献[11]中的方案	3SM	(2n+1)BP+2SM	2SM+1BP	是
文献[12]中的方案	3E	2BP+1E	2BP+1E	是
本文方案	1SM+1E	1BP+1E	1BP+1E	是

6　结束语

本文研究了无证书有序多重签名的安全模型，利用椭圆曲线密码及双线性对构造了一种无证书有序多重签名方案，并在随机预言机模型下证明其安全性是建立在计算 Diffie-Hellman 问题困难性之上的。该方案签名长度固定，与签名成员人数无关，且部分签名阶段无需双线性对运算，部分签名的验证及整体签名的验证阶段除可进行预计算的部分运算外都仅需要一个对运算，具有较高的工作效率和较低的资源占有率，可以方便地解决大规模分布式环境下信任建模中节点间传递的推荐信息的认证问题。

参考文献：

[1] 王晓峰，张琛，王尚.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. Digital multi-signature scheme and its security proof[J]. Chinese Journal of Computers, 2008, 31(1): 176-183.

[2] **王泽成,斯桃枝,李志斌.改进的带签名者意向的结构化多重签名方案**[J].**计算机应用**, 2008, 28(1):71-73.
WANG Z C, SI Y Z, LI Z B.Improvement of structured multi- signature scheme with signer's intentions[J]. Computer Applications, 2008, 28(1):71-73.

[3] **于佳卜,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 B,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.

[4] **张亚玲,张璟,王晓峰.一个高效的基于身份和** RSA **的紧致多重数字签名方案**[J].**电子与信息学报**, 2008,30(9):2246-2249.
ZHANG Y L, ZHANG J, WANG X F.An efficient identity based compact multi-signature from RSA[J]. Journal of Electronics & Information Technology, 2008, 30(9): 2246-2249.

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

[6] WANG B, YANG X D, YANG G. An identity-based multisignature scheme from the weil pairing[A]. Proceedings of the 2010 International Conference on Computer Design And Applications (ICCDA 2010)[C]. Qinhuangdao, China, 2010.

[7] **张秋璞,叶顶锋.对一个基于身份的多重签密方案的分析和改进**[J].**电子学报**, 2011, 39(12): 2713-2720.
ZHANG Q P,YE D F.Cryptanalysis and improvement of an identity-based multi-signcryption scheme[J]. Chinese Journal of Electronics, 2011, 39(12): 2713-2720.

[8] **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 sequentiaI multi-signature scheme[J]. Computer Applications, 2009, 29(6): 1643-1645.

[9] **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.

[10] **袁玉敏,朱海山,田丽文.无需随机预言的无证书聚合签名方案**[J].**计算机工程与应用**, 2011, 47(7): 103-106.
YUAN Y M, ZHU H S, TIAN L W. Certificateless aggregate signature scheme without random oracles[J].Computer Engineering and Applications, 2011, 47(7): 103-106.

[11] 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.

[12] YANH A, TSD R, MAMBU M, *et al.* Certificateless ordered sequential aggregate signature scheme[A]. 2011 Third International Conference on Intelligent Networking and Collaborative Syste Fukuoka, Japan, 2011.

[13] **陈虎,朱昌杰,宋如顺.高效的无证书签名和群签名方案**[J].**计算机研究与发展**, 2010, 47(2): 231-237.
CHEN H, ZHU C J,SONG R S. Efficient certificateless signature and group signature schemes[J].Journal of Computer Research and Development, 2010, 47(2): 231-237.

[14] 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.

[15] POINTEHEVAL D, STERN J.Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

作者简介：

秦艳琳（1980-），女，河南安阳人，海军工程大学讲师，主要研究方向为动态信任管理理论及网络安全。

吴晓平（1961-），男，山西新绛人，海军工程大学教授、博士生导师，主要研究方向为信息安全及系统工程。