无双线性配对的无证书签名方案

王圣宝[1,2,3]，刘文浩[1]，谢琪[1]

（1. 杭州师范大学 信息科学与工程学院，浙江 杭州 310012；2. 北京邮电大学 网络与交换技术国家重点实验室，北京 100876；
3. 合肥新星应用技术研究所，安徽 合肥 230031）

摘 要：为解决身份基公钥密码体制中的密钥托管问题以及基于传统公钥证书密码体制中的公钥管理过程过于繁琐的问题，Al-Riyami 和 Paterson 提出了无证书公钥密码的概念。在已有的许多无证书签名方案中，在签名产生或者签名的验证过程中都需要双线性配对运算，并且，这些方案的安全性都基于较强的难题假设。提出了一种新的无双线性配对运算的无证书签名方案，并在随机预言机模型下基于较弱的离散对数困难假设证明了它的安全性，而且其效率优于已有方案。

关键词：无证书签名方案；无双线性配对；离散对数；随机预言

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)04-0093-06

Certificateless signature scheme without bilinear pairings

WANG Sheng-bao[1,2,3], LIU Wen-hao[1], XIE Qi[1]

(1. School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310012, China;
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. New Star Institute of Applied Technology, Hefei 230031, China)

Abstract: To solve the key escrow problem inherited in ID-based cryptography and the complex certificate management problem of traditional certification-based public key cryptosystem, Al-Riyami and Paterson proposed the novel concept of certificateless public key cryptography. Almost all existing certificateless signature schemes need bilinear pairings either during signature generation stage or the signature verification stage, and were proven secure only with stronger computational assumptions. A new certificateless signature scheme without pairings was proposed. The scheme is provably secure in the random oracle model (ROM) under the relatively weaker assumption, i.e., the discrete logarithm assumption and is more efficient than the existing schemes.

Key words: certificateless signature scheme; without bilinear pairing; discrete logarithm; random oracle

1 引言

公钥密码学自 1976 年诞生以来，用户的公钥如何才能得到高效认证始终是一个热点研究问题。在基于传统公钥证书的密码方案中，证书的管理过程十分复杂。而在身份基公钥密码体制中不存在公钥证书，但却不可避免地存在密钥托管问题。鉴于此，Al-Riyami 和 Paterson[1]于 2003 年首次提出了

收稿日期：2011-06-08；**修回日期**：2011-12-25

基金项目：国家自然科学基金资助项目（61103209, 61070153）；网络与交换技术国家重点实验室开放基金资助项目（SKLNST-2009-1-13）；安徽省自然科学基金资助项目（10040606Q63）；浙江省自然科学基金资助项目（Z12F020028）

Foundation Items: The National Natural Science Foundation of China (61103209, 61070153); The Open Foundation of State Key Laboratory of Networking and Switching Technology of China (SKLNST-2009-1-13); The Natural Science Foundation of Anhui Province (10040606Q63); The Natural Science Foundation of Zhejiang Province (Z12F020028)

无证书公钥密码学的全新概念。在文献[1]中提出了第一个无证书签名方案，但没有证明其安全性。

近年来，无证书签名方案的研究受到广泛重视，出现了许多新的方案。但是，这些方案或者存在安全漏洞，或者存在计算效率不高的问题。其中，导致计算效率不高的问题主要是因为它们都以双线性配对作为设计工具。2004 年，Yum 等[2]首次提出不使用双线性配对来设计无证书签名方案。然而，Hu 等[3]指出文献[2]中的方案不能抵抗密钥替换攻击，并提出了一个改进的无需双线性配对的无证书签名方案。2005 年，Huang 等[4]提出了针对文献[1]中签名方案的密钥替换攻击，提出了避免此类攻击的改进方案，并详细证明了他们新方案的安全性。同年，Corantla 等[5]提出了一个在 ROM 模型下安全的无证书签名方案，其安全性基于 CDH 假设。该方案中，签名时不需要计算无双线性配对，但在签名的验证过程中则需要 3 次双线性配对运算。2006 年，Cao 等[6]指出 Corantla 等[5]的签名方案仍然不能抵抗密钥替换攻击，并给出一个验证签名需要 4 次双线性配对运算的改进方案。同年，Zhang 等[7]提出了一个无证书签名方案，其签名过程无需双线性配对，但验证过程则需要 4 次双线性配对运算。Choi 等[8]于 2007 年所提出的 2 个方案在签名过程中没有用到双线性配对，但在签名验证过程中至少需要进行 1 次配对运算。2008 年，Duan 等[9]提出了无证书不可否认签名方案，其签名过程需要 2 次双线性配对运算。Liu 等[10]提出了标准模型下安全的无证书签名方案，其验证过程需要进行多达 6 次配对运算。Xiong 等[11]针对 Liu[10]的方案提出了恶意 KGC 攻击，并提出了改进方案，改进方案在验证阶段仍然需要 3 次配对运算。同时，Shim[12]指出了 Xiong 等[11]的方案不能抗密钥替换攻击。2009 年，Yuan 等[13]提出了标准模型下的无证书签名方案，其签名过程无双线性配对运算，验证过程需要 2 次双线性配对运算。Du 等[14]所提出的无证书短签名方案在签名的过程没有用到配对，而且验证过程只需 1 次配对运算。

在各种无证书签名方案的变体类型中，则往往需要更多次数的配对运算。2010 年，Jin 等[15]提出了无证书多重代理签名方案，其签名过程需要 $4n$+4 次配对运算。Guo 等[16]提出了无证书代理重签名方案，其签名过程无需配对运算，但验证过程需要 6 次配对运算。Yang 等[17]给出了无证书可转换加密签名的模型，并提出了具体方案，其签名阶段没有用到配对，而验证阶段需进行 4 次配对运算。2011 年，Zhang 等[18]首次定义了无证书盲签名方案，其签名过程需要进行 2 次配对运算，验证过程需要 3 次配对运算。同年，Yang 等[19]设计了可追踪的无证书门限代理签名方案，其签名过程需进行 $7n$ 次配对运算，而验证阶段要进行 10 次配对运算。

本文提出了无双线性配对运算的高效无证书签名新方案，并基于离散对数（DL, discrete logarithm）困难假设，在随机预言模型（ROM）下证明了所提新方案的安全性。与同类方案相比，本文的新方案具有更好的计算效率。

2 预备知识

2.1 困难问题及假设

离散对数问题（DLP, discrete logarithm problem）：设循环群 G 的阶为 q，P 是它的一个生成元。给定随机元素 $Q \in G$，计算 $a \in Z_q^*$，使其满足 $Q = aP$。

在概率多项式时间内算法 A 在解决 DLP 的优势定义如下：

$$Adv^{DLP}(A) = \Pr[A(P,Q) = a \mid a \in Z_q^*]$$

离散对数假设：对任意概率多项式时间算法 A，$Adv^{DLP}(A)$ 是可以忽略的。

2.2 无证书签名方案

在无证书签名方案中，存在 3 个合法参与者，它们分别是密钥生成中心（KGC）、签名者 ID_i 和验证者 ID_j。一个无证书签名方案由如下 7 个算法构成。

1) 系统建立

输入安全参数 k，输出系统公开参数 *params* 和系统主密钥。然后，公开 *params*，由密钥生成中心（KGC）秘密地保管主密钥。

2) 部分密钥生成

此算法输入给定用户的身份标识 ID_i、系统参数 *params* 和主密钥，KGC 输出身份该用户的部分私钥 D_i，并通过秘密信道将 D_i 返回给用户 ID_i。

3) 秘密值生成

此算法输入用户身份标识 ID_i，系统参数 *params*，输出该用户的秘密值 $x_i \in Z_q^*$。

4) 用户私钥生成

输入用户身份标识 ID_i、系统参数 $params$、用户部分私钥 D_i 及其长期秘密值 x_i，算法输出该用户的私钥 $SK_i=(x_i,D_i)$。

5) 用户公钥生成

输入用户身份标识 ID_i、参数 $params$、部分私钥 D_i 和长期私钥 x_i，输出用户公钥 PK_i。

6) 签名

输入系统参数 $params$、待签名消息 m、签名者用户身份标识 ID_i、其公钥 PK_i 以及签名私钥 SK_i，最终输出该用户针对消息 m 的签名 σ。

7) 验证

输入系统参数 $params$、签名 σ、消息 m、签名者身份标识 ID_i 及其公钥 PK_i，若验证通过，输出 1；否则，输出 0。

2.3 安全模型

本节给出由文献[13]所定义的关于无证书签名方案的形式化安全模型，在该模型中，攻击者被分为 A_{I} 和 A_{II} 两类。

A_{I}：此类攻击者不掌握系统主密钥，但它可以替换合法用户的公钥。

A_{II}：此类攻击者可得到系统主密钥，但是它被禁止替换合法用户的公钥。

定义 1　在 A_{I} 类攻击者攻击下的不可伪造性：在多项式时间内，若 A_{I} 攻击者不能以不可忽略的优势在如下游戏中获胜，则称该无证书签名方案在适应性选择消息攻击下具有不可伪造性 $(EUF-CLSC-CMA)$。

1) 挑战者 C 输入安全参数 k，运行系统建立算法，获得系统主密钥 x 和系统参数 $params$，保密主密钥并将系统参数 $params$ 交给攻击者 A_{I}。

2) 查询阶段，攻击者 A_{I} 执行如下操作。

$Hash$ 查询：A_{I} 可以针对任意输入查询 $Hash$ 值。

部分私钥生成查询：A_{I} 选择一个身份标识 ID，根据参数 $params$ 和系统主密钥 x，C 计算用户部分私钥 D_{ID}，并将其发送给攻击者 A_{I}。

私钥生成查询：攻击者 A_{I} 选择一个身份标识 ID，挑战者 C 根据用户密钥生成算法生成用户 ID 的私钥 SK_{ID}，并将其发送给 A_{I}。

公钥生成查询：攻击者 A_{I} 选择一个用户身份标识 ID，挑战者 C 根据用户公钥生成算法生成该用户的公钥 PK_{ID}，并将其发送给 A_{I}。

用户公钥替换：针对任意身份标识 ID，攻击者 A_{I} 可以选择一个新的公钥来替换原公钥 PK_{ID}。

签名生成查询：攻击者 A_{I} 选择身份标识 ID_i 和明文 m，挑战者 C 对 ID_i 进行私钥生成查询，然后，计算签名 $\sigma=Sign(ID_i,m,SK_i)$，并将 σ 发送给 A_{I}。

3) 签名伪造阶段：攻击者 A_{I} 输出一个四元组 (m^*,σ^*,ID^*,PK^*)。定义 A_{I} 在这个游戏中获胜，当且仅当：

① σ^* 是身份标识为 ID^*，公钥为 PK^* 的用户对消息 m^* 的一个有效无证书签名；

②攻击者 A_{I} 没有查询过身份标识为 ID^* 的用户的部分私钥；

③攻击者 A_{I} 没有查询过身份标识为 ID^*，公钥为 PK^* 的用户对消息 m^* 的签名。

定义 2　在 A_{II} 攻击者攻击下的不可伪造性：若在多项式时间内攻击者 A_{II} 不能以不可忽略的优势在如下游戏中获胜，则称无证书签名方案在适应性选择消息攻击下具有不可伪造性。

1) 建立阶段：挑战者 C 输入安全参数 k，运行“系统参数建立”算法，获得系统主密钥 x 和 $params$，并发送 x 和 $params$ 给攻击者 A_{II}。

2) 查询阶段：攻击者 A_{II} 执行的操作同定义 1 中的阶段 2)。

3) 签名伪造阶段：攻击者 A_{II} 输出一个四元组 (m^*,σ^*,ID^*,PK^*)。定义攻击者 A_{II} 在这个游戏中获胜，当且仅当：

① σ^* 的身份标识为 ID^*，公钥为 PK^* 的用户对 m^* 的一个有效签名；

②攻击者 A_{II} 没有查询过身份标识为 ID^* 用户的长期秘密值 x_i，并且它也没有替换过该用户的公钥；

③攻击者 A_{II} 没有询问过身份标识为 ID^*，公钥为 PK^* 的用户对 m^* 的签名。

定义 3　一个无证书签名方案在适应性选择消息攻击下满足不可伪造的安全属性，当且仅当任何多项式时间攻击者赢得上述 2 个游戏的概率都是可忽略的。

3 新的无证书签名方案

本节给出新提出的无证书签名方案。在本方案中，无论是签名者还是验证者都不需要进行相对费时的双线性配对运算。

1) 系统建立阶段

输入安全参数 k，输出 2 个大素数 p、q，满足

$q \mid p-1$。设 P 为循环群 G_1 中任意一个阶为 q 的生成元。选择安全 *Hash* 函数：$H_1:\{0,1\}^* \times G_1 \to Z_q^*$，$H_2:\{0,1\}^* \to Z_q^*$，KGC 随机选择主密钥 $z \in Z_q^*$，然后计算 $y=zP$，并公开系统参数 (p,q,P,y,H_1,H_2)，保密系统主密钥 z。

2) 用户密钥生成

给定用户身份标识 ID_i，KGC 随机选取 $r_i \in Z_q^*$，然后计算 $R_i=r_iP$，$D_i=r_i+zH_1(ID_i,R_i)$，通过安全信道将 D_i 发给用户。用户将其作为部分私钥，将 $R_i=r_iP$ 作为他的部分公钥。

该用户随机选取 $x_i \in Z_q^*$ 作为其长期私钥，并生成相应私钥 (x_i,D_i)，接着计算 $X_i=x_iP$，生成公钥 (X_i,R_i)。用户可以通过等式 $R_i+H_1(ID_i,R_i)y=D_iP$ 是否成立来判断 KGC 发送的部分私钥是否有效。

3) 签名

假定用户 A 为签名者，随机选择整数 $a \in Z_q^*$，然后计算 $T_A=aP$，$h=H_2(T_A \| X_A \| ID_A \| m)$，$s_1=a/(x_A+D_A+h)$，$s_2=x_A/(x_A+D_A+h)$，从而得到签名 $\sigma=(h,s_1,s_2)$，并将其与部分公钥 R_A 一道传递给用户 B。

4) 签名验证

假定 B 为签名验证者，当收到签名 σ 和 R_A 后，B 计算 $h_1=H_1(ID_A,R_A)$，

$$
\begin{aligned}
&s_1(R_A+X_A+h_1y+hP)=(a/(D_A+x_A+h))\times\\
&(r_AP+x_AP+zh_1P+hP)\\
&=(a/(D_A+x_A+h))\times(D_A+x_A+h)P\\
&=T_A\\
&s_2(R_A+X_A+h_1y+hP)=(x_A/(D_A+x_A+h))\times\\
&(r_AP+x_AP+zh_1P+hP)\\
&=(x_A/(D_A+x_A+h))\times(D_A+x_A+h)P\\
&=X_A。
\end{aligned}
$$

4 安全证明

在随机预言模型下，利用 2.3 节所描述的安全模型，证明前面所提新方案的安全性。

定理 1 （相对 A_1 的不可伪造性）在随机预言模型下，若存在一个 $(EUF-CLSC-CMA)$ 攻击者 A_1 能在多项式时间内以 ε 的优势在定义 1 中的游戏中获胜（假设它最多进行 q_i 次 H_i 查询，其中，$i=1,2$），则存在一个算法 Q 能在多项式时间内以 $\varepsilon/(q_1^2q_2)$ 的优势成功解决离散对数问题。

证明 假设 Q 是一个关于 DLP 问题的有效算法，其输入为 (vP,P)，目标是计算出 v。Q 设置 $y=vP$，然后利用 A_1 作为子程序试图解决 DLP 问题，并且充当 $(EUF-CLSC-CMA)$ 游戏中的挑战者。游戏开始后，挑战者 Q 发送 (p,q,P,y,H_1,H_2) 给攻击者 A_1，并维持列表 $L_1,L_2,L_D,L_{SK},L_{PK},L_S,L_V$ 分别用于跟踪 A_1 对预言机 H_1,H_2、部分私钥提取、私钥提取、公钥提取、签名和验证签名的查询。注意，每个列表最初被设置为空。

H_1 查询：列表 L_1 的格式为 (ID,R,h_1)，当 Q 收到攻击者 A_1 针对 $H_1(ID_i,R_i)$ 的查询时，若 (ID,R,h_1) 已经存在于列表 L_1 中，则返回列表中相应的值给 A_1。否则，挑战者 Q 随机选取 $h_1 \in Z_q^*$，并将 (ID,R,h_1) 加入到列表 L_1 中。

H_2 查询：此列表的格式为 (m,ID,X,T,h_2,c)，假使挑战者 Q 收到 A_1 针对 $H_2(m \| ID \| T \| X)$ 的查询，Q 查找 (m,ID,X,T,h_2) 是否存在于列表 L_2 之中，若存在则返回相应值给 A_1。否则，随机选取 $c \in \{0,1\}$，设 $\Pr[c=1]=\delta$。若 $c=0$，随机选取 $h_2 \in Z_q^*$，并将 h_2 返回给 A_1，然后将 (m,ID,X,T,h_2,c) 加入列表 L_2 中；若 $c=1$，则令 $h_1=\perp$，返回 $\perp$ 给 A_1 表示终止游戏。

部分私钥查询：若 (ID,D,R) 存在于列表 L_D 中，则返回其中相应的值给 A_1。否则，挑战者 Q 随机选择 $D,h_1 \in Z_q^*$，并计算 $R=DP-yh_1$，然后将 (ID,D,R) 加入列表 L_D 中，将 (ID,R,h_1) 加入列表 L_1 中，最后将 (R,D) 返回给攻击者 A_1。

私钥查询：若 (ID,D,x) 在列表 L_{SK} 中存在，则将列表中相应的值返回给 A_1。否则，Q 查找列表 L_D 得到 D，并随机选择 $x \in Z_q^*$，最后将 (ID,D,x) 插入列表 L_{SK}。

公钥查询：若 (ID,R,X) 存在列表 L_{PK} 中，则将列表中相应的值返回给 A_1。否则，Q 先查找列表 L_D 和 L_{SK}，计算 $X=xP$，将 (ID,R,X) 加入列表 L_{PK} 中，并将 (R,X) 返回给 A_1；若在列表 L_D 和 L_{SK} 中不存在，则查找列表 L_2。若 $c=1$，则 Q 随机选取 $r,x \in Z_q^*$，并计算 $R=rP,X=xP$，然后将 (ID,R,X,c) 插入列表 L_{PK}，并返回 (R,X)；若 $c=0$，则运行部

分私钥查询获得 (R,D)，然后 Q 随机选择 $x \in Z_q^*$，并将 (ID,D,x) 插入列表 L_{SK}，接着将 (ID,R,X,c) 插入列表 L_{PK}，并返回 (R,X)。

公钥替换查询：假设签名者的身份标识为 ID，攻击者 A_{I} 可以任意选取一个新的 x' 替换掉原先的 x，并以新的公钥 R' 替换原公钥 R。

签名生成查询：挑战者 Q 在列表 L_{PK} 查找 (ID_B,R_B,X_B,c)。若 $c=1$，则放弃；否则，查找列表 (ID_A,D_A,x_A)，并随机选 $a \in Z_q^*$，计算 $T=aP$，$X=x_AP$，$h_1=H_1(ID_A,R_A)$，$h=H_2(T\|ID_A\|m)$，$s_1=a/(x_A+D_A+h)$ 以及 $s_2=x_A/(x_A+D_A+h)$，最后返回签名 $\sigma=(h,s_1,s_2)$ 给 A_{I}。

验证签名查询：Q 在列表 L_{PK} 查询 ID_A：①若存在且 $c=0$，则在列表 L_1 中查询 (ID_A,R,h_1)，接着计算 $T'=s_1(R_A+X_A+h_1y+hP)$ 和 $X'=s_2(R_A+X_A+h_1y+hP)$；若 $H_2(T'\|X'\|ID_A\|m)=h$ 成立，则输出 1，表示“通过验证”，否则终止模拟游戏；②若存在且 $c=1$，则在列表 L_1 中查找 (ID_A,R_A,h_1)，若存在 $(m,ID_A,T',X',h)\in L_2$，则输出 1，表示“通过验证”，否则终止模拟游戏；③若列表 L_{PK} 中不存在，则表示公钥已被替换，则在列表 L_1 中查找 (ID_A,R_A,h_1)，若发现 $(m,ID_A,T',X',h)\in L_2$，则输出 1，表示“通过验证”，否则终止模拟游戏。

经过多项式次数的上述查询之后，A_{I} 随机选取 $a,s^*\in Z_q^*$，计算 $T=aP$，$h^*=H_2(ID_A\|T\|X\|m)$，$h_1=H_1(ID_A,R_A)$，然后输出对 m 的伪造签名 $\sigma^*=(h^*,s^*)$。注意，挑战者 Q 掌握被攻击者替换掉的公钥。若伪造的签名有效，则 Q 输出 $v=(a-s^*(r_A+x_A+h^*))/h_1s^*$ 作为 DLP 问题的答案；否则，Q 无法解决 DLP 问题。若 A_{I} 对 ID_A 进行过部分私钥或私钥查询，则 Q 失败退出，而 A_{I} 不进行这 2 种查询的概率至少是 $1/q_1^2$；如果 A_{I} 对 T' 进行过 H_2 查询，则 Q 失败退出，而 A_{I} 不进行这种查询的概率大于 $1/q_2$。因此，挑战者 Q 解决 DLP 问题的优势至少为 $\varepsilon/q_1^2q_2$。

定理 2　（相对 A_{II} 攻击下的不可伪造性）。在随机预言模型下，若存在一个 $(EUF-CLSC-CMA)$ 攻击者 A_{II} 能在多项式时间内以优势 ε 在定义 2 中的游戏中获胜（假设攻击者最多进行 q_i 次 H_i 查询，$i=1,2$），则存在一个算法 Q 能在多项式时间内以优势 $\varepsilon/(q_1^2q_2)$ 解决 DLP 问题。

证明　给定一个随机 DLP 问题实例 (p,q,P,aP)，算法 Q 的目标是计算获得 a。同定理 1 的证明，Q 试图以 A_{II} 为子程序解决 DLP 问题，并充当 $(EUF-CLSC-CMA)$ 游戏中的挑战者。游戏开始后，Q 将系统参数 (p,q,P,y,H_1,H_2) 发送给 A_{II}。根据定义，攻击者 A_{II} 掌握系统主私钥 z，但不能进行公钥替换攻击，其他条件及目标同定理 1。

在此攻击游戏中，A_{II} 可以进行定理 1 证明过程中的除验证签名之外的所有查询。

验证签名查询：Q 在列表 L_{PK} 查找 ID_A：①若存在且 $c=0$，则在列表 L_1 中查找 (ID_A,R,h_1')，并计算 $T'=(R_A+X_A+h_1y+hP)s$；若 $H_2(T'\|ID_A\|m)=h$ 成立，则返回“通过”，否则终止游戏模拟；②若存在且 $c=1$，则在 L_1 中查找 (ID_A,R_A,h_1)，若存在 $(m,ID_A,T',X',h)\in L_2$，则返回“通过”，否则终止游戏模拟；③若列表 L_{PK} 中不存在该公钥，则在列表 L_1 中查找，若存在 $(m,ID_A,T',X',h)\in L_2$，则返回“通过”，否则终止游戏模拟。

在游戏的某个阶段，攻击者 A_{II} 随机选取 $a,s^*\in Z_q^*$，并计算 $T=aP$，$h^*=H_2(ID_A\|T\|X\|m)$，$h_1=H_1(ID_A,R_A)$，最后输出对消息 m 的伪造签名 $\sigma^*=(h^*,s^*)$。若伪造签名能通过验证，则挑战者 Q 输出 $r_A=(a-s^*(vh_1+x_A+h^*))/s^*$ 作为 DLP 问题实例的解；否则，Q 不能解决 DLP 问题。若 A_{II} 对 ID_A 进行过部分私钥或私钥查询，则 Q 失败退出。A_{II} 不进行这 2 种查询的概率至少为 $1/q_1^2$；若 A_{II} 对 T' 进行过 H_2 查询，则 Q 失败退出，A_{II} 不进行这种查询的概率大于 $1/q_2$。所以，挑战者 Q 解决 DLP 问题的优势至少为 $\varepsilon/q_1^2q_2$。

5　效率分析

数字签名方案的效率包括签名阶段和验证阶段的计算量以及签名长度等。表 1 将新方案与已有的具有代表性方案的效率进行了比较。其中，P 表示一个双线性配对运算，S 表示群 G_1 中的标量乘法运算，E 表示群 G_2 中的指数运算，H 表示一个散列运算。另外，P_1 表示 G_1 中一个元素的长度，

P_2 表示 G_2 元素的长度，而 Z_1 表示 Z_q^* 中的整数的长度。

表 1 计算量和签名长度的比较

签名方案	签名阶段	验证阶段	长度	安全性
文献[8]中方案 1	2S	2P+2S+1H	$2P_1$	未知
文献[8]中方案 2	1S+1E	1P+2S+1E	$1P_1+1P_2$	未知
文献[7]中方案	3S+2H	4P+3H	$2P_1$	安全
文献[15]中方案	2S+1E	3P+1H	$1P_1+1Z_1$	可证安全
新提方案	1S+1H	2S+1H	$3Z_1$	可证安全

根据文献[20]所给出的分析结果，双线性配对、指数运算与散列运算的计算量分别是标量乘运算的约 21 倍、3 倍及 1 倍。从表 1 可以看到，在签名及其验证签名阶段，只有文献[2,3]中的方案与所提出的新方案一样都没有用到双线性配对。但是，它们已被证明是不安全的。而其他所有方案至少需要进行 1 次双线性配对运算。在本文所提出的新方案中，签名为 $\sigma=(h,s_1,s_2)$。在计算 h 时，签名者需要先计算 $T_A=aP$，即 1 次点乘计算。另外计算 h 时还需进行一次散列操作，即计算 $H_2(T_A\|X_A\|ID_A\|m)$，因此计算量总计为 1S+1H。类似地，可以计算出签名验证阶段所需的计算量，即 2S+1H。新方案的签名长度与表 1 中其他方案相比也具有较大优势。

6 结束语

本文提出了一个新的无双线性配对运算的无证书签名方案。基于离散对数问题假设，在随机预言模型下证明了其安全性。通过分析表明，新方案的计算效率和签名长度都优于已有方案。因此，它更适合应用于计算能力和带宽都受限的场景，例如无线传感器网络和 ad hoc 网络。

参考文献：

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

[2] YUM D H, LEE P J. Generic construction of certificateless signature[A]. In Information Security and Privacy: 9th Australasian Conference, ACISP 2004[C]. Springer-Verlag, 2004. 200-211.

[3] HU B, WONG D, ZHANG Z, *et al*. Key replacement attack against a generic construction of certificateless signature[A]. Proc of 11th Australasian Conference on Information Security and Privacy[C]. Melbourne, Australia, 2006. 235-246.

[4] HUANG X, SUSILO, W, MU Y, ZHANG F. On the security of certificateless signature schemes[A]. Asiacrypt 2003[C]. 2005.13-25.

[5] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme[A]. Proc of CIS'05[C]. Springer-Verlag, 2005. 110-116.

[6] CAO X, PATERSON K G, KOU W. An Attack on a Certificateless Signature Scheme[R]. Cryptology ePrint Archive, 2006.

[7] ZHANG Z, WONG D, XU J, *et al*. Certificateless public-key signature[A]. Security Model and Efficient Construction, ACNS 2006[C]. Springer-Verlag, 2006. 293-308.

[8] CHOI K Y, PARK J H, HWANG J, *et al*. Efficient certificateless signature schemes[A]. Proc of ACNS'07[C]. Springer-Verlag, 2007. 443-458.

[9] DUAN S. Certificateless undeniable signature scheme[J]. Information Sciences, 2008, 178 (3): 742-755.

[10] LIU J, AU M, SUSILO W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model[A]. Proc of ACM 2007 ACM Symposium on Information, Computer and Communications Security[C]. Singapore, 2007. 273- 283.

[11] XIONG H, QIN Z, LI F. An improved certificateless signature scheme secure in the standard model[J]. Funda Info, 2008, 88: 193-206.

[12] SHIM K A. Breaking the short certificateless signature scheme[J]. Information Sciences, 2009, 179 (3): 303-306.

[13] YUAN Y, LI D, TIAN L, ZHU H. Certificateless signature scheme without random oracles[A]. ISA 2009[C]. 2009. 31-40.

[14] DU H, WEN Q. Efficient and provably-secure certificateless short signature scheme from bilinear pairings[J]. Computer Standards and Interfaces, 2009, 31(2): 390-394.

[15] JIN Z, WEN Q. Certificateless multi-proxy signature[J]. Comput Commun, 2011, 34(3): 344-352.

[16] GUO D, WEI P, YU D, *et al*. A certificateiess proxy re-signature scheme[A]. Proc of Computer Science and Information Technology (ICCSIT)[C]. 2010. 157-161.

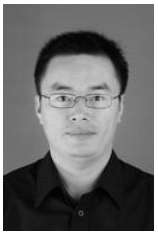
[17] YANG B, XIAO Z, LI S. Certificateiess verifiably encrypted signature scheme[A]. Proc of IC-NIDC[C]. 2010. 783-788.

[18] ZHANG L, ZHANG F, QIN B, *et al*. Provably-secure electronic cash based on certificateless partially-blind signatures[J]. Electron Comm Res, 2011, 10(5): 545-552.

[19] YANG T, XIONG H, HU J. A traceable certificateless threshold proxy signature scheme from bilinear pairings[A]. Proc of APWeb'11[C]. 2011. 376-381.

[20] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. Int J Inf Secur, 2007, 6(4):213-241.

作者简介：



王圣宝（1978-），男，江西鄱阳人，博士，杭州师范大学讲师，主要研究方向为应用密码学与网络信息安全。

刘文浩（1974-），男，湖北孝感人，博士，杭州师范大学讲师，主要研究方向为信息安全研究和无线网络安全。

谢琪（1968-），男，浙江绍兴人，博士后，杭州师范大学教授，主要研究方向为密码学与信息安全。