高效的可证明安全的无证书数字签名方案

何明星，李鹏程，李 虓

(西华大学计算机与软件工程学院 成都 610039)

【摘要】无证书公钥密码体制结合了基于身份和传统PKI公钥密码体制的优势，克服了基于身份公钥密码体制的密钥托管问题及PKI系统的证书管理问题，具有很高的效率。该文提出一个在随机预言机模型下可证明安全的无证书数字签名方案。该方案只需分别在系统初始化阶段、验证阶段预进行一次双线性对运算，而在签名阶段不需要进行计算。计算结果证明该方案比以往的无证书数字签名方案具有更高的计算效率和通信效率，且具有随机预言机模型下的可证明安全性。

关 键 词 双线性对； 无证书数字签名； 可证明安全； 数字签名

中图分类号 TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2015.05.016

Efficient and Provably Secure Certificateless Signature from Bilinear Pairings

HE Ming-xing, LI Peng-cheng, and LI Xiao

(School of Computer and Software Engineering, Xihua University Chengdu 610039)

Abstract Certificateless cryptography aims at combining the advantages of identity based and traditional certificate-based public key cryptography, so as to avoid the key escrow problem inherent in the identity based system and certificate management in public key infrastructure. In this paper, we propose a new efficient certificateless signature scheme and prove its security in the random oracle model. Furthermore, via pre-computing a bilinear pairing in the setup phase, our scheme only needs to compute one pairing in the verify stage. It is more efficient in computation complexity and communication complexity than that of many previous schemes.

Key words bilinear pairing; certificateless signature; provable security; signature

文献[1]首次提出了基于身份的数字签名方案。文献[2]第一次提出双线性对的概念，并利用双线性对构造了一个基于身份的数字签名方案。文献[3]首次构造了一个无证书数字签名方案，该方案也是基于双线性对的，但并没有对该方案进行严格的安全性证明和安全性分析。文献[4]论证了文献[3]的不安全性，容易受到公钥替换攻击，敌手可以假冒用户对任意消息进行伪造签名。文献[5-6]中的方案也不能抵抗公钥替换攻击。此外，经过分析发现文献[6]中用户还可以恢复出SEM拥有的对应于该用户私钥的另一部分私钥，使得该签名方案无仲裁性质。文献[7]构造了一个高效的无证书数字签名方案，它基于离散对数困难性假设，该方案在签名中不需要“双线性对”运算，在验证阶段仅需2次“双线性对”运算。但文献[8]发现文献[7]的方案也不能抵抗公钥替换攻击。文献[9-11]也从不同侧面对安全性和有效性进行了更加深入和广泛的讨论。本文在这些成果基础上提出一个新的在随机预言机模型下可证明安全的无证书数字签名方案，且比以往的无证书数字签名方案具有更高的计算效率和通信效率。

1 无证书数字签名模型

1.1 无证书数字签名

一个无证书数字签名系统由密钥生成中心(key generate center, KGC)、签名者(signaturer)、验证者(verifier)3个合法参与者构成。包含7个多项式时间算法：

1) 系统初始化算法：输入系统安全参数1^k后，返回KGC的主私钥(master secret key,MSK)以及系统全局参数。

2) 部分私钥提取算法：输入用户身份字符串$ID \in \{0,1\}^*$($\{0,1\}^*$表示所有的比特串集合)、系统主私钥MSK及系统公开参数，由KGC返回用户部分私钥D。

3) 设置秘密值算法：用户随机选择一个秘密值

收稿日期：2013－07－21；修回日期：2014－03－01
基金项目：科技部支撑计划(2011BAH26B00)；四川省国际合作项目(2009HH0009)；四川省高校创新团队项目(13TD0005)
作者简介：何明星(1964－)，男，博士，教授，主要从事密码学与信息安全方面的研究.

x，用于生成用户的公钥及私钥。

4) 用户公钥生成算法：用户输入秘密值 x 及系统公开参数后，生成自己的公钥PK。

5) 用户私钥生成算法：用户输入秘密值 x 及由KGC生成的部分私钥 D，返回完整的私钥SK。

6) 签名算法：该算法是概率多项式时间算法。签名发送者在执行算法过程中，输入待签名消息 $m \in M_{\mathrm{CLS}}$、签名发送者身份 ID_S、完整私钥 SK_S 和公钥 PK_S、签名验证方身份 ID_R、全局参数及一些随机数 $r \in R_{\mathrm{CLS}}$。算法执行完毕后，若签名正确则输出消息 $m \in M_{\mathrm{CLS}}$ 对应的签名 $\sigma \in \Sigma_{\mathrm{CLS}}$；否则输出错误标识“⊥”。

7) 签名验证算法：输入签名 $\sigma \in \Sigma_{\mathrm{CLS}}$、签名发送者用户身份 ID_S、公钥 PK_S、签名验证方身份 ID_R 及系统全局参数。算法由签名验证者执行完毕后，若验证签名正确则输出“接受签名”；否则输出错误标识“⊥”。

1.2 无证书数字签名体制的敌手

无证书数字签名体制的敌手[3]分为两类：1) 敌手 A_I 定义为外部的恶意敌手，是主动敌手，不知道系统的主私钥MSK，但拥有替换用户公钥的能力；2) 敌手 A_{II} 是一个诚实但好奇(honest-but- curious)的KGC，是一个被动敌手，拥有系统的主私钥MSK，但不能替换用户的公钥。

在随机预言机模型下，一个无证书数字签名方案的可证明安全性，可通过一个挑战者 C 与敌手 A_I 或者 A_{II} 进行交互来确定。

1.2.1 游戏1(针对敌手 A_I)

1) 系统初始化：挑战者 C 输入系统安全参数 ℓ，运行初始化算法，获取系统主私钥MSK及全局参数，然后将系统全局参数发送给敌手 A_I，并对系统主私钥MSK保密。

2) 攻击阶段：敌手 A_I 可以进行多项式次的交互询问。

① 请求公钥询问 $\mathrm{PK}(\mathrm{ID}_i)$：当敌手 A_I 向挑战者提交一个合法的身份 ID_i 并请求询问该 ID_i 的公钥后，挑战者返回提交 ID_i 相对应的公钥 $\mathrm{PK}(\mathrm{ID}_i)$。

② 替换公钥询问 $\mathrm{PKR}(\mathrm{ID}_i, \mathrm{PK}'_{\mathrm{ID}_i})$：当敌手 A_I 向挑战者提交一个合法的身份 ID_i 以及一个伪造的合符系统格式的公钥 $\mathrm{PK}'_{\mathrm{ID}_i}$ 后，挑战者应该利用提交的伪造公钥 $\mathrm{PK}'_{\mathrm{ID}_i}$ 替换掉敌手提交 ID_i 的当前公钥 $\mathrm{PK}_{\mathrm{ID}_i}$。

③ 秘密值询问 $\mathrm{SV}(\mathrm{ID}_i)$：当敌手 A_I 向挑战者提交一个合法的身份 ID_i 并请求询问该 ID_i 的秘密值 x_i 后，如果该 ID_i 的公钥未被替换，那么挑战者向敌手返回该 ID_i 对应的秘密值 x_{ID_i}；否则模拟失败。

④ 部分私钥提取询问 $\mathrm{PPK}(\mathrm{ID}_i)$：当敌手 A_I 向挑战者提交一个合法的身份 ID_i 并请求询问该 ID_i 的部分私钥后，挑战者返回提交 ID_i 相对应的部分私钥 D_{ID_i}。

⑤ 私钥提取询问 $\mathrm{SK}(\mathrm{ID}_i)$：当敌手 A_I 向挑战者提交一个合法的身份 ID_i 并请求询问该 ID_i 的私钥后，挑战者返回提交 ID_i 相对应的私钥 $\mathrm{SK}_{\mathrm{ID}_i}$，如果该 ID_i 对应的公钥被替换，则模拟失败。

⑥ 签名询问 $\mathrm{Sig}(M_i, \mathrm{ID}_i, \mathrm{PK}_i)$：敌手 A_I 可以对任何用户 ID_i 对消息 M_i 的签名进行询问，挑战者收到一个挑战 $(M_i, \mathrm{ID}_i, \mathrm{PK}_i)$ 后，挑战者 C 对消息 M_i 生成一个签名 σ_i 作于对敌手 A_I 的回答。这里要求对消息 M_i 生成签名 σ_i 对于用户 ID_i 和其对应的公钥 $\mathrm{PK}_{\mathrm{ID}_i}$ 是有效的。

3) 伪造阶段：最后，若敌手 A_I 输出一个元组 $(M^*, \sigma^*, \mathrm{ID}^*, \mathrm{PK}_{\mathrm{ID}^*})$，当且仅当满足以下3个条件，敌手 A_I 获得该游戏的胜利。

① 对于用户 ID^* 和其对应的公钥 $\mathrm{PK}_{\mathrm{ID}^*}$，元组中签名 σ_i 是有效的。

② 敌手 A_I 没有对用户 ID^* 进行过部分私钥提取询问。

③ 敌手 A_I 没有以元组 $(M^*, \mathrm{ID}^*, \mathrm{PK}_{\mathrm{ID}^*})$ 在签名询问中进行交互。

1.2.2 游戏2

与游戏1不同之处：A_{II} 仅有请求公钥询问 $\mathrm{PK}(\mathrm{ID}_i)$、秘密值询问 $\mathrm{SV}(\mathrm{ID}_i)$、私钥提取询问 $\mathrm{SK}(\mathrm{ID}_i)$、签名询问 $\mathrm{Sig}(M_i, \mathrm{ID}_i, \mathrm{PK}_i)$ 的能力。A_{II} 不像 A_I 具有公钥替换的能力 $\mathrm{PKR}(\mathrm{ID}_i, \mathrm{PK}'_{\mathrm{ID}})$：当 A_I 向挑战者提交一个合法的身份 ID_i 及一个伪造的符合系统格式的公钥 $\mathrm{PK}'_{\mathrm{ID}}$ 后，挑战者应利用提交的伪造公钥 $\mathrm{PK}'\mathrm{ID}$ 替换 A_I 提交 ID_i 的当前公钥 $\mathrm{PK}_{\mathrm{ID}_i}$。

2 高效的无证书数字签名方案

2.1 无证书数字签名方案描述

系统初始化算法分为以下5个步骤：

1) KGC首先生成素数 q 阶的加法循环群 G_1 及乘法循环群 G_2，任意选择一个生成元 $P \in G_1$。

2) KGC任意选择 $s \in Z_q^*$ 作为系统主私钥(Z_q^* 表示由 q 决定的乘法群)。

3) KGC计算得到系统主公钥 $P_0 = sP \in G_1$。

4) KGC预计算双线性对 $e(P,P) = g \in G_2$， e 是一个双线性映射。

5) 最后，KGC选择两个密码学安全的Hash函数 $H_1 : \{0,1\}^* \to Z_q^*$ 和 $H_2 : \{0,1\}^* \times 2G_2 \to Z_q^*$（× 表示集合间的笛卡尔积)。

KGC执行完系统初始化算法后，得到系统主私钥 $s \in Z_q^*$、系统主公钥 P_0 及系统全局公开参数 $< G_1, G_2, q, e, P, P_0, g, H_1, H_2 >$。

部分私钥提取算法分为两个步骤：

1) 对每一个用户 U_i，KGC首先计算出身份哈希值 $Q_i = H_1(\mathrm{ID}_i) \in Z_q^* (\mathrm{ID}_i \in \{0,1\}^*)$。

2) KGC计算出用户 U_i 的部分私钥 $D_i = (s + Q_i)^{-1} P \in G_1$。KGC将 D_i 通过安全信道传送给相应的用户 U_i。

设置秘密值算法执行步骤：用户 U_i 随机选择一个秘密值 $x_i \in Z_q^*$。值得注意的是，秘密值 x_i 对用户外的所有人保密，在执行用户公钥生成算法和用户私钥生成算法中所用到的秘密值必须是这里选择的秘密值 x_i。

用户公钥生成算法执行分为两个步骤：

1) 计算得到身份哈希值：

$$Q_i = H_1(\mathrm{ID}_i) \in Z_q^* \quad (\mathrm{ID}_i \in \{0,1\}^*) \tag{1}$$

2) 用户 U_i 计算得到公钥：

$$\mathrm{PK}_i = x_i(P_0 + Q_i P) \in G_1 \tag{2}$$

用户私钥生成算法执行步骤：用户 U_i 获得自己的部分私钥 D_i 和个人秘密值 $x_i \in Z_q^*$ 后得到私钥 $\mathrm{SK}_i =< x_i, D_i > \in (Z_q^*, G_1)$。必须指出，在HLL方案中，用户利用私钥生成算法获得完整的私钥必须在KGC执行完部分私钥提取算法及通过公钥生成算法获得个人秘密值 x_i 后执行。

签名算法执行步骤：假设签名方为Alice，其对应的私钥 $\mathrm{SK}_A =< x_A, D_A >=< x_A, (s + Q_A)^{-1} P >$，相应的公钥 $\mathrm{PK}_A = x_A(P_0 + Q_A P)$。签名验证方为Bob，其对应的私钥 $\mathrm{SK}_B =< x_B, D_B >=< x_B, (s + Q_B)^{-1} P >$，相应的公钥 $\mathrm{PK}_B = x_B(P_0 + Q_B P)$。签名的消息为 M，M对于签名方及验证方均是已知的。具体执行步骤如下：

1) Alice选择一个随机值 $k \in Z_q^*$ 并计算 $R = g^{x_A}$，$T = g^k \in G_2$。

2) Alice计算 $U = H_2(M \| R \| T) \in Z_q^*$。

3) Alice计算得到消息签名 $V = x_A(U^{-1} D_A - P_0 - Q_A P) \in G_1$。

最后，Alice通过公开信道将签名 $\sigma =< R, T, V >$ 发送给Bob。

签名验证算法执行步骤：Bob在接收到Alice发送的签名 $\sigma =< R, T, V >$ 后验证签名。

1) Bob首先计算 $U' = H_2(M \| R \| T) \in Z_q^*$。

2) Bob验证等式：

$$R = e(V + \mathrm{PK}_A, U'(P_0 + Q_A P)) \tag{3}$$

若成立，则接受签名；否则拒绝签名。

2.2　无证书数字签名方案的正确性分析

在一般的数字签名中，签名的原始消息对于签名发送方以及签名验证方均是公开的，所以如果对消息的签名在传输过程中没有被敌手篡改，那么签名验证方在收到签名后，首先计算出正确的 $U' = H_2(M \| R \| T) \in Z_q^*$，有 $U = U' \in Z_q^*$，签名则能通过式(3)的验证，即：

$$e(V + \mathrm{PK}_A, U'(P_0 + Q_A P)) =$$
$$e(x_A(U^{-1} D_A - P_0 - Q_A P) + \mathrm{PK}_A, U'(P_0 + Q_A P)) \tag{4}$$

3　无证书数字签名方案的安全性证明

定理 1　无证书数字签名方案在*k*-CCA困难性假设及随机预言机(Random Oracle)模型下，对敌手 A_I 可抵抗存在性伪造攻击。

证明：挑战者算法 C 首先与敌手 A_I 交互生成*k*-CCA困难问题的实例。

$$P \in G_1, sP \in G_1, (t_0, t_1, \cdots, t_k) \in Z_q^* \tag{5}$$

$$((s + t_1)^{-1} P, (s + t_2)^{-1} P, \cdots, (s + t_k)^{-1} P) \in G_1 \tag{6}$$

初始化阶段：设置 $P_{\mathrm{Pub}} = sP, g = e(P,P)$。值得注意的是系统主私钥 $s \in Z_q^*$ 是保密的。随后 C 随机选择一个指数 $l \in \{1, 2, \cdots, k\}$，这里 $k \leqslant q_{H_1}$。

1) H_1 询问

A_I 可以不重复地对每一个身份 $\mathrm{ID}_i (i \in \{1, 2, \cdots, k\})$ 进行询问：

① 若 $i \neq l$，C向 A_I 返回 $Q_{\mathrm{ID}} = t_i$，并将元组 $(i, \mathrm{ID}, Q_{\mathrm{ID}} = t_i)$ 添加进一个初始化为空的表 L_1；

② 若 $i = l$，则C向 A_I 返回身份值 $Q_{\mathrm{ID}} = t_0$，并将元组 $(i, \mathrm{ID}, Q_{\mathrm{ID}} = t_0)$ 添加进 H_1 哈希询问所维护的表 L_1。

2) H_2 询问

对于 A_I 提起的每一个询问 (M_i, R, T)：

① C首先检查表 L_2，若表中存在一个元组 (M_i, R, T, h_2)，那么C向 A_I 返回相对应的Hash值；

② 否则，C任意选择一个Hash值 $h_2 \in Z_q^*$ 返回给

A_I，并将相应的元组(M_i,R,T,h_2)添加进表L_2；

③ 提取部分私钥询问，A_I就一个身份ID_i向C提起提取部分私钥询问请求；

④ 若$i=l$，C终止该预言机的模拟；

⑤ 若$i\neq l$，C首先查表$L_K=\{i,\mathrm{ID},x_{\mathrm{ID}},D_{\mathrm{ID}},\mathrm{PK}_{\mathrm{ID}}\}$，如果表中存在该$\mathrm{ID}_i$对应的元组，则向$A_I$返回对应的$D_{\mathrm{ID}}=(s+t_i)^{-1}P$；否则，挑战者$C$先以$\mathrm{ID}_i$作一次$H_1$哈希询问，并将元组$(i,\mathrm{ID},Q_{\mathrm{ID}}=t_i)$更新到表$L_1$，然后向$A_I$返回对应ID的部分私钥$D_{\mathrm{ID}}=(s+t_i)^{-1}P$，并将元组$\{i,\mathrm{ID},\perp,D_{\mathrm{ID}},\perp\}$更新到表$L_K$，这里“$\perp$”表示为空。

3) 秘密值询问

当A_I向C以ID_i并提起询问后：

① C首先查表L_K，如果该表中存在一个元组$\{i,\mathrm{ID},x_{\mathrm{ID}},D_{\mathrm{ID}},\mathrm{PK}_{\mathrm{ID}}\}$该$\mathrm{ID}_i$的公钥未被替换，那么$C$向$A_I$返回该ID对应的秘密值$x_{\mathrm{ID}}$，否则输出模拟失败。

② 否则，C先以ID_i作一次H_1哈希询问，并将元组$(i,\mathrm{ID},Q_{\mathrm{ID}}=t_i)$更新到表$L_1$，然后再作一次部分私钥询问并随机选择一个$x_{\mathrm{ID}}\in Z_q^*$，最后向$A_I$返回秘密值$x_{\mathrm{ID}}$并将元组$\{i,\mathrm{ID},x_{\mathrm{ID}},D_{\mathrm{ID}},\mathrm{PK}_{\mathrm{ID}}\}$更新到表$L_K$，元组中插入的公钥$\mathrm{PK}_{\mathrm{ID}}$为$C$成秘密值后利用公钥生成算法获得的。

4) 请求公钥询问

对于A_I的每一个询问ID_i：

① C首先查表L_K，如果该表中存在一个元组$\{i,\mathrm{ID},x_{\mathrm{ID}},D_{\mathrm{ID}},\mathrm{PK}_{\mathrm{ID}}\}$，则返回该ID所对应的公钥$\mathrm{PK}_{\mathrm{ID}}$；

② 否则，C先以ID_i作一次H_1哈希询问，并将元组$(i,\mathrm{ID},Q_{\mathrm{ID}}=t_i)$更新到表$L_1$，然后执行一次秘密值询问，执行公钥生成算法为其生成一个新的公钥对返回给A_I，并将新的元组$\{i,\mathrm{ID},x_{\mathrm{ID}},D_{\mathrm{ID}},\mathrm{PK}_{\mathrm{ID}}\}$添加进该询问维护的表$L_K$。

5) 替换公钥询问

A_I向挑战者提交一个合法的元组$(\mathrm{ID},\mathrm{PK}'_{\mathrm{ID}})$：

① C首先根据ID搜索表L_K，如果表中存在对应ID的元组，则将其内容更新为$\{i,\mathrm{ID},\perp,D_{\mathrm{ID}},\mathrm{PK}'_{\mathrm{ID}}\}$；

② 否则，C先以ID_i作一次H_1哈希询问，并将元组$(i,\mathrm{ID},Q_{\mathrm{ID}}=t_i)$更新到表$L_1$，然后再作一次部分私钥提取，并将新元组$\{i,\mathrm{ID},\perp,D_{\mathrm{ID}},\mathrm{PK}'_{\mathrm{ID}}\}$插入进表$L_K$。$C$并不知道敌手伪造用户公钥所用到的秘密值$x'_{\mathrm{ID}}$。

6) 提取私钥询问

A_I就一个身份ID_i向C起提取私钥询问后：

① 若$i=l$，挑战者终止该预言机的模拟；

② 若$i\neq l$，分两种情况：

第一，挑战者查表L_K，若表中存在该ID对应的元组，但是该用户的公钥已经被替换，挑战者模拟失败；否则返回该用户对应的私钥$\mathrm{SK}_{\mathrm{ID}}=(x_{\mathrm{ID}},D_{\mathrm{ID}})$；

第二，若表L_K中不存在该ID对应的元组，查表L_1，找到该ID对应的身份哈希值Q_{ID}，如果该ID对应元组不存在，则以该ID作一次H_1询问，并将元组$(i,\mathrm{ID},Q_{\mathrm{ID}}=t_i)$更新到表$L_1$，然后执行一次秘密值提取询问，将新元组$\{i,\mathrm{ID},x_{\mathrm{ID}},D_{\mathrm{ID}},\perp\}$插入表$L_K$并向$A_I$返回提交ID私钥$\mathrm{SK}_{\mathrm{ID}}=(x_{\mathrm{ID}},D_{\mathrm{ID}})$。

7) 签名询问

在预言机询问中，A_I提交的询问内容为一个元组$(M_i,\mathrm{ID}_i,\mathrm{PK}_{\mathrm{ID}_i})$，无论该ID公钥是否被替换，$C$均能生成一个合法的签名(通过验证等式)：

① 任意选择两个随机数$r,t\in Z_q^*$，计算得到$R=g^r,T=g^t$；

② 计算$U=H_2(M_i\|R\|T)$；

③ 计算$V=rU^{-1}D_{\mathrm{ID}}-\mathrm{PK}_A$，并将生成的签名$(V,R,T)$返回给$A_I$。

8) 伪造阶段

最后，A_I输出一个成功的伪造元组$(M^*,\sigma^*=(V^*,R^*,T^*),\mathrm{ID}^*,\mathrm{PK}_{\mathrm{ID}^*})$，元组里的签名$\sigma^*$是能通过验证等式的，$\mathrm{ID}^*\neq\mathrm{ID}_l$，若挑战者终止模拟；否则，利用文献[12]中的的攻击方法，C进行重放攻击，生成另一个伪造元组$(M^*,\sigma^*=(V^*,R^*,T^*),\mathrm{ID}^*,\mathrm{PK}_{\mathrm{ID}^*})$，这里要求$A_I$及签名$\sigma^*$需满足：

$$R^*=e(V^*+\mathrm{PK}_{\mathrm{ID}^*},U^{*\prime}(P_0+Q_{\mathrm{ID}^*}P)) \tag{7}$$

$$R^*=e(V^{*\prime}+\mathrm{PK}_{\mathrm{ID}^*},U^{*\prime}(P_0+Q_{\mathrm{ID}^*}P)) \tag{8}$$

最后C则通过两次伪造签名的恒等性$e(V^*+\mathrm{PK}_{\mathrm{ID}^*},U^{*\prime}(P_0+Q_{\mathrm{ID}^*}P))=e(V^{*\prime}+\mathrm{PK}_{\mathrm{ID}^*},U^{*\prime}(P_0+Q_{\mathrm{ID}^*}P))$获得$k$-CCA困难性问题的解$(s+t_0)^{-1}P=D_{\mathrm{ID}^*}=r^{-1}u^{-1}(V^*+\mathrm{PK}_{\mathrm{ID}^*})$。

定理 2 无证书数字签名方案在$k-CCA$困难性假设以及随机预言机模型下，对敌手A_{II}可以抵抗存在性伪造攻击。思路与方法同定理1。

4 无证书数字签名方案的效率分析

表1列举了本文方案与其他无证书数字签名方案在签名以及验证阶段中计算效率和签名规模上的比较。可以看出，本文方案与其他的无证书数字签名方案相比，不但费时的双线性对运算比其他的无

证书数字签名方案少，而且指数运算和计算快速的倍点运算也与其他无证书数字签名方案相当，可见本文方案具有更高的运算效率；另外，本文方案的签名规模也和其他方案大致平衡；最后，在协议的执行过程中，本文方案不需要复杂的运行费时的映射到点(map-to-point)的Hash函数。因此，本文方案是一个高效的无证书数字签名方案。

表1　4个无证书数字签名方案的效率对比

方案	执行算法	双线性对运算	指数运算	倍点运算	签名规模	映射到点Hash函数
文献[3]方案	签名	1	0	2	$\|G_1\|+\|Z_q^*\|$	需要
	验证	4	1	0		
文献[7]方案	签名	0	0	2	$2\|G_1\|$	需要
	验证	2	0	2		
文献[9]方案	签名	0	0	3	$2\|G_1\|$	需要
	验证	4	0	0		
本文方案	签名	0	2	1	$\|G_1\|+2\|G_2\|$	不需要
	验证	1	0	1		

5　结　论

本文提出了一个在随机预言机模型下可证明安全的无证书数字签名方案。方案仅需在系统初始化阶段预计算一次双线性对，在验证阶段计算一次双线性对，而在签名阶段不需要进行双线性对运算，因此本方案比以往一些无证书数字签名方案具有更高的计算效率和通信效率。

参　考　文　献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag, 1984.

[2] SAKAI R, OHGISHI K, KASAHARA M. Cryptosystems based on pairing[C]//Proceedings of Symposium on Cryptography and Information Security. Okinawa, Japan: [s.n.], 2000.

[3] AL-RIYAMI S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology-ASIACRYPT'03. Berlin: Springer-Verlag, 2003.

[4] HUANG Xin-yi, WILLY SUSILO, YI MU, et al. On the security of a certificateless signature scheme from Asiacrypt 2003[C]//4th International Conference on Cryptology and Network Security. Berlin: Springer-Verlag, 2005.

[5] LI X, CHEN K, SUN L. Certificateless signature and proxy signature schemes from bilinear pairings[J]. Lietuvos Matematikos Rinkinys, 2005, 45(1): 76-83.

[6] JU H, KIM D, LEE D, et al. Efficient revocation of security capability in certificateless public key cryptography [C]//Knowledge-Based Intelligent Information and Engineering Systems. Berlin: Springer-Verlag, 2005.

[7] YAP W, HENG S, GOI B. An efficient certificateless signature scheme[C]//Emerging Directions in Embedded and Ubiquitous Computing, EUC Workshops 2006. Berlin: Springer-Verlag, 2006.

[8] ZHANG Zhen-feng, FENG Deng-guo. Key replacement attack on a certificateless signature scheme[EB/OL]. http://eprint.iacr.org/2006/453.

[9] ZHANG Z, XU J, FENG D. Certificateless public-key signature: Security model and efficient construction[C]//Advances in ACNS 2006. Berlin: Springer-Verlag, 2006.

[10] HE D, CHEN J, ZHANG R. An efficient and provably-secure certificateless signature scheme without bilinear pairings[J]. International Journal of Communication Systems, 2012, 25(11): 1432-1442.

[11] HE De-biao, CHEN Yi-tao, CHEN Jian-hua. An efficient certificateless proxy signature scheme without pairing[J]. Mathematical and Computer Modelling, 2013(57): 2510-2518.

编　辑　叶　芳