计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.201200117

一个强安全的无证书签名方案的分析和改进

叶胜男　陈建华
武汉大学数学与统计学院　武汉 430000
(ellaye@whu.edu.cn)

摘　要　无证书公钥密码体制结合了基于身份的密码体制和传统 PKI 公钥密码体制的优势,克服了基于身份的公钥密码体制的密钥托管问题及 PKI 系统的证书管理问题,具有明显的优势。对 Hassouna 等提出的一个强安全无证书签名方案进行安全分析。结果表明,该方案不能验证消息的完整性,存在消息篡改攻击,且方案未使用根据系统主密钥生成的私钥进行签名,所以不是无证书签名方案。在此基础上,提出了一个改进的无证书签名方案,在随机预言机模型下,基于椭圆曲线 Diffie-Hellman 问题假设,证明了该方案可以抵抗第一类强敌手和第二类敌手的攻击,满足存在性不可伪造的安全性。

关键词:无证书签名;双线性对;安全性分析;椭圆曲线 Diffie-Hellman 问题;随机预言机模型
中图法分类号　TN918

Security Analysis and Improvement of Strongly Secure Certificateless Digital Signature Scheme

YE Sheng-nan and CHEN Jian-hua
School of Mathematics and Statistics, Wuhan University, Wuhan 430000, China

Abstract　Certificateless public key cryptosystem combines the advantages of identity-based cryptosystem and traditional PKI public key cryptosystem, overcomes the key escrow problem of identity-based public key cryptosystem and the certificate management problem of PKI system, and has obvious advantages. By analysing the security of a strongly secure certificateless signature scheme proposed by Hassouna, et al, it shows that the scheme cannot resist the attack of falsifying messages and do not use private key generated by system master key to sign. So it is not a certificateless signature scheme. On this basis, an improved certificateless signature scheme is proposed and it proves the scheme can resist the attack of the first class of strong adversaries and the second class of adversaries. In the random oracle model and under the assumption of the Diffie-Hellman problem of the elliptic curve, the improved scheme satisfies the existential forgery.

Keywords　Certificateless signature, Bilinear pairings, Security analysis, Elliptic curve discrete Diffie-Hellman problem, Random oracle model

1　引言

在传统的数字签名方案中,数字证书是根据公钥基础设施(Public Key Infrastructure,PKI)的一套程序和策略颁发的,然后由可信证书机构(Certificate Authority,CA)的私钥签名,起到了将用户身份和公钥安全绑定的作用,以确保其真实性。系统中的每个用户都可以使用其自身的证书,通过加密提供机密性,并通过数字签名提供不可否认性。然而,传统公钥密码学(Public Key Cryptography,PKC)通常存在需要耗费大量时间和精力、发放和管理证书的问题。PKC 对于证书的需要被认为是公钥签名方案部署和管理的主要困难,而基于身份的公钥密码学(Identity Based Public Key Cryptography,ID-PKC)[1]解决了这些问题。在 ID-PKC 中,实体的公钥直接由其身份生成,例如,属于网络主机的 IP 地址或与用户关联的电子邮件地址。私钥被称为密钥生成中心(Key Generation Center,KGC)的可信第三方为实体生成。由于密钥托管问题[1-2],ID-PKC 不能提供真正的不可抵赖性,因此,用户私钥的密钥托管是基于身份的签名方案[3-5]中固有的。

在 2003 年,Riyami 等[6]引入了无证书公钥密码学(Certificateless Public Key Cryptography,CL-PKC)的概念,以克服基于身份的公钥密码学(ID-PKC)的密钥托管限制。在 CL-PKC 中,被称为密钥生成中心(KGC)的可信第三方向用户提供部分私钥。然后,用户将部分私钥与一个 KGC 不知道的秘密值结合起来,以获得他/她的全部私钥。这样,KGC 就不知道用户的私钥。最后,用户将该秘密值与 KGC 的公共参数相结合,以计算自身的公钥。在 Riyami 和 Paterson 等最初的 CL-PKC 方案[6]提出之后,出现了许多无证书密码方案。这些方案包括使用无证书加密[7-10]、无证书签名[11-16]和无证书签密[17-20]。

Hassouna 等[21-22]提出了一个强安全的无证书签名方案,本文对此方案进行了安全性分析,发现该方案存在缺陷。因此在此基础上本文给出了一个改进方案,安全性分析表明在随机预言机模型(Random Oracle Model,ROM)下,改进方案对自适应选择消息攻击是存在性不可伪造的。

到稿日期:2020-12-14　返修日期:2021-05-03
通信作者:陈建华(chenjh_ecc@163.com)

2 预备工作

2.1 双线性对

设G_1，G_2分别是阶为素数q的加法循环群和乘法循环群。P是G_1的生成元。$e:G_1\times G_1\rightarrow G_2$是具有下列性质的双线性对映射。

(1)双线性。对于$Q,W,Z\in G_1$，有$e(Q,W+Z)=e(Q,W)\cdot e(Q,Z)$和$e(Q+W,Z)=e(Q,Z)\cdot e(W,Z)$。

对于$a,b\in Z_q$，有$e(aQ,bW)=e(Q,W)^{ab}=e(abQ,W)$等。

(2)非退化性。存在$P,Q\in G_1$，使得$e(P,Q)\neq 1_{G_2}$。

(3)可计算性。对于任意的$P,Q\in G_1$，存在有效的算法，可以计算$e(P,Q)$。

2.2 数学困难问题

定义 1 计算性 Diffie-Hellman 问题(computational Diffie-Hellman problem)

给定$P,aP,bP\in G_1$($a,b\in Z_q^*$是未知的随机数)，计算$abP\in G_1$。

定义 2 判定双线性 Diffie-Hellman 问题(decisional bilinear Diffie-Hellman problem)

给定$P\in G_1$，$aP,bP,cP\in G_2$($a,b,c\in Z_q^*$是未知的随机数)和$h\in G_r$，判定$h=e(P,Q)^{abc}$是否成立。

2.3 无证书数字签名的定义

(1)系统建立(Set-up)：输入安全参数l，返回系统公共参数$params$和系统主密钥s。这个算法由 KGC 运行。

(2)部分私钥生成(Extract-Partial-Private-Key)：输入$params$、系统主密钥s和用户的身份 ID，输出部分私钥d_{ID}。该算法由 KGC 运行，生成的部分私钥通过安全信道发给相应的用户。

(3)秘密值建立(Set-Secrete-Value)：输入$params$和用户的身份 ID，输出用户的秘密值x_{ID}。该算法由系统中每个用户来执行。秘密值是由系统公共参数$params$和用户的身份 ID 决定的。

(4)私钥建立(Set-Private-Key)：输入$params$，用户的部分私钥d_{ID}和秘密值x_{ID}，输出私钥sk_{ID}。该算法由系统中的每个用户来执行。

(5)公钥建立(Set-Public-Key)：输入$params$和用户的秘密值x_{ID}，输出用户的公钥pk_{ID}。该算法由系统用户执行，且执行完该算法后公开公钥。公钥由系统公共参数$params$和用户的身份信息 ID 共同定义。

(6)签名(CL-Sign)：输入$params$、待签消息m、用户的身份 ID、公钥pk_{ID}以及私钥sk_{ID}，该算法输出签名S。

(7)验证(CL-Verify)：输入$params$、签名人的身份 ID、公钥pk_{ID}、消息m以及签名S。返回“1”说明该签名有效，返回“0”说明该签名无效。

2.4 安全模型

在无证书密码系统中，有两种类型的具备不同能力的敌手A_I，A_{II}。

(1)第一类敌手A_I：攻击者不能获得 KGC 的主密钥和目标用户的部分私钥，但是攻击者能替换目标用户的公钥。此处我们考虑的是由 Huang[23] 提出的强敌手(strong adversary)。强敌手必须提供替换后的公钥所对应的秘密值，才能得到使用替换后的公钥进行验证后的有效签名。

(2)第二类敌手A_{II}：攻击者知道 KGC 的主密钥和用户的部分私钥，但是攻击者不能获得目标用户的秘密值，而且不能替换目标用户的公钥。

定义 3 一个无证书数字签名方案在适应性选择消息攻击下是存在性不可伪造的，如果敌手A_I，A_{II}在以下两个游戏中获胜的概率是可以忽略的。

游戏 1：挑战者C输入安全参数l，运行系统建立算法产生系统主密钥s和系统参数$params$，然后发送$params$给A_I，秘密保存s。

执行下面的询问。

(1)部分私钥询问：当A_I查询用户 ID 的部分私钥时，C通过运行部分私钥算法生成用户 ID 的部分私钥d_{ID}，并将该值返回给A_I。

(2)私钥询问：除了挑战身份ID^*，可以询问其他所有用户 ID 的私钥，C运行私钥算法将私钥sk_{ID}返回给A_I。如果用户 ID 的公钥已被替换，再期望C给出正确答案是不合理的，除非A_I提交新的秘密值给C。

(3)公钥询问：收到询问用户 ID 的公钥时，C运行算法利用秘密值和公钥产生用户的公钥pk_{ID}并返回给A_I。

(4)公钥替换询问：A_I可以用自己选取的公钥pk_{ID}'和对应的秘密值$x_{ID'}$代替用户的公钥pk_{ID}和x_{ID}。将pk_{ID}'设置为该用户的新公钥，将$x_{ID'}$设置为该用户的新秘密值。

(5)签名询问：给定消息m和身份 ID，C用私钥sk_{ID}计算签名S并发送给A_I。如果用户的公钥pk_{ID}已经被替换为pk_{ID}'，C没有对应的秘密值$x_{ID'}$，则在这种情况下签名预言机的输出可能出错。所以，我们要求A_I额外提交新的秘密值$x_{ID'}$给签名预言机。

最后，A_I输出一个相应于挑战身份ID^*和公钥pk_{ID^*}的消息/签名对(m^*,S^*)。如果 CL-Verify$(params,ID^*,m^*,pk_{ID^*},S^*)=1$和以下条件成立：

1)ID^*从来没有被提交给私钥生成预言机；

2)ID^*从来没有既提交给公钥替换预言机又同时提交给部分私钥生成预言机；

3)(ID^*,m^*,pk_{ID^*},S^*)不是由签名预言机得到的。

那么A_I获胜。

游戏 2：挑战者C输入安全参数l，运行系统建立算法产生系统主密钥s和系统参数$params$，然后发送$params$和s给A_{II}。

执行下面的询问。

(1)私钥询问：除了挑战身份ID^*，A_{II}可以查询所有用户 ID 的私钥，C返回私钥sk_{ID}给A_{II}。

(2)要求公钥询问：收到查询用户 ID 的公钥时，C返回该用户的公钥pk_{ID}。

(3)签名询问：给定消息m和身份 ID，C用私钥sk_{ID}计算签名S并发送给A_{II}。

最后，A_{II}输出一个相应于挑战身份ID^*和公钥pk_{ID}的消息/签名对(m^*,S^*)。如果 CL-Verify$(params,ID^*,m^*,pk_{ID^*},S^*)=1$，且满足以下条件：

1)ID^*从来没有被提交给私钥生成预言机；

2)$(ID^*, m^*, pk_{ID^*}, S^*)$不是由签名预言机得到的。

那么A_{II}获胜。

3 回顾 Hassouna 等的安全方案

本节给出由 Hassouna 等[22]提出的无证书签名方案的步骤。

(1)系统建立(由 KGC 运行):设置系统安全参数为 k,KGC 选取阶为 q 的加法循环群 G_1 和乘法循环群 G_2,P 是 G_1 的生成元。双线性对映射 $e: G_1 \times G_1 \rightarrow G_2$。KGC 随机选取 $s \in Z_q^*$ 作为系统主密钥,计算 $P_{pub} = sP$ 为系统公钥。KGC 选择两个安全哈希函数 $H_1: \{0,1\}^* \rightarrow G_1$,$H_2: \{0,1\}^n \rightarrow Z_q^*$。最后 KGC 系统公开参数可表示为 $params = \langle G_1, G_2, e, P, P_{pub}, H_1, H_2, n\rangle$,公开 $params$,保密主密钥 s。

(2)秘密值建立(由用户运行):带有身份 ID_m 的用户 m,随机选取两个秘密值 $x_m, x_m' \in Z_q^*$。然后,用户 m 计算 $X_m = x_m' P$ 并发送给 KGC。所提出的方案强制用户选择强密码通行证、客户端的系统哈希密码 $z_m = H_2(pass)$ 和生成点 $z_m P$,使用哈希值 z_m 作为密钥加密秘密值 x_m 并生成基于密码的加密代码(PEC)作为 $PEC_{z_m}(x_m)$,发送它的副本到 KGC 的公共目录并存储它的副本以及点 $z_m P$。

(3)部分私钥生成(由 KGC 运行):一旦收到由用户 m 计算的 X_m,则 KGC 计算 $Q_m = H_1(ID_m)$,然后生成用户 m 的部分私钥 $D_m = sQ_m$。

(4)公钥建立(由用户运行):用户 m 的身份为 ID_m,计算 $Q_m = H_1(ID_m)$,$Y_m = x_m' Q_m$ 并将 $\langle X_m, Y_m\rangle$ 作为用户的长期公钥 P_m。最后用户 m 发送 Y_m 给 KGC。

(5)私钥建立:用户 m 的私钥为 $S_m = (x_m + z_m) D_m = (x_m + z_m) sQ_m = (x_m + z_m) sH_1(ID_m)$。同时,用户生成秘密项 $Z_m = x_m P$。

(6)签名:用户使用其秘密项 $\{x_m, Z_m\}$ 生成消息 m 的签名,具体如下:

1)签名者选取大的随机整数 $a \in G_2^*$。

2)签名者计算 $MP_m = H_1(m) \in G_1^*$。

3)签名者计算 $MP_{1m} = a x_m MP_m \in G_1^*$

4)签名者计算 $s_m = e(MP_m, Z_m)^{ax_m'} = e(MP_m, P)^{ax_m x_m'}$。

5)签名者发送 $\sigma = (m, MP_{1m}, s_m)$ 作为签名。

(7)验证:验证者收到签名以后,使用用户 m 的公钥 $\langle X_m, Y_m\rangle$ 来验证签名,具体如下:

1)验证者计算 $e(X_m, Q_m) = e(Y_m, P)$,如果等式成立则说明用户 m 的公钥是真实的,否则签名被拒绝。

2)验证者计算 $MP_m' = H_1(m) \in G_1^*$。

3)如果 $MP_{1m} = MP_m'$ 或者 $s_m = e(X_m, H_1(m))$ 成立,则验证者拒绝此签名。

4)验证者计算 $r_m = e(MP_{1m}, X_m)$。

如果等式 $r_m = s_m$,验证者接受签名;否则,拒绝签名。

4 Hassouna 安全方案的安全性分析

通过对上述方案[22]的分析,可以知道该方案存在如下缺陷。

缺陷 1:该方案存在消息篡改攻击,存在一个攻击者 $\mathcal{A}$,其具体攻击如下。

攻击者 $\mathcal{A}$ 将签名者的消息盗取进行篡改或者替换为 m',并随机选取随机整数 $a \in G_2^*$,计算 $MP_m = H_1(m')$,$MP_{1m} = a x_m MP_m$,计算签名 $s_m = e(MP_m, Z_m)^{ax_m'} = e(MP_m, P)^{ax_m x_m'}$。返回签名 $\sigma = (m', MP_{1m}, s_m)$ 给验证者。下面证明由攻击者伪造的签名可以通过验证等式。

$$\begin{aligned} s_m &= e(MP_m, Z_m)^{ax_m'} \\ &= e(MP_m, P)^{ax_m x_m'} \\ &= e(a x_m MP_m, x_m' P) \\ &= e(MP_{1m}, X_m) = r_m \end{aligned}$$

因此,签名可以通过验证等式,即说明攻击者 $\mathcal{A}$ 将签名者的消息篡改或者替换后伪造的签名 $\sigma = (m', MP_{1m}, s_m)$ 是有效的。上述等式很明显是一个恒等式,不管在何种消息下该验证等式都会成立,它无法保证消息的正确性和完整性。即该方案不能抵抗消息的篡改攻击。

缺陷 2:通过对上述方案[22]的签名和验证两步骤分析,可以看出在这两阶段中该方法并未使用用户的私钥,即 KGC 未参与签名和验证。而无证书数字签名方案的核心就是通过 KGC 来解决密钥托管问题。因此,此方案从本质上来说不是无证书签名方案。

5 本文的改进方案

针对上述方案[22]中的缺陷,本文提出一了个可抵抗消息的篡改攻击的无证书签名方案。该方案包括系统建立、秘密值建立、部分私钥生成、公钥建立、私钥建立、签名及验证这 7 个算法。具体描述如下:

(1)系统建立(由 KGC 运行):设置系统安全参数为 k,KGC 选取阶为 q 的加法循环群 G_1 和乘法循环群 G_2,P 是 G_1 的生成元。双线性对映射 $e: G_1 \times G_1 \rightarrow G_2$。KGC 随机选取 $s \in Z_q^*$ 作为系统主密钥,计算 $P_{pub} = sP$ 为系统公钥。KGC 选择 2 个安全哈希函数 $H_1: \{0,1\}^* \rightarrow G_1$(映射到点的哈希函数),$H_2: \{0,1\}^n \rightarrow Z_q^*$(映射到数域的哈希函数)。最后 KGC 系统公开参数可表示为 $params = \langle G_1, G_2, e, P, P_{pub}, H_1, H_2, n\rangle$,公开参数 $params$,保密主密钥 s。

(2)秘密值建立(由用户运行):带有身份 ID_m 的用户 m,随机选取两个秘密值 $x_m, x_m' \in Z_q^*$。然后,用户 m 计算 $X_m = x_m' P$ 并发送给 KGC。

(3)部分私钥生成(由 KGC 运行):收到由用户 m 计算的 X_m,则 KGC 计算 $Q_m = H_1(ID_m)$,然后生成用户 m 的部分私钥 $D_m = sQ_m$。

(4)公钥建立(由用户运行):用户 m 的身份为 ID_m,计算 $Q_m = H_1(ID_m)$,$Y_m = x_m' Q_m$,并将 $\langle X_m, Y_m\rangle$ 作为用户的长期公钥 P_m。最后用户 m 发送 Y_m 给 KGC。

(5)私钥建立:用户 m 计算秘密项 $Z_m = x_m P$,并将 $\langle D_m, Z_m\rangle$ 作为用户的私钥。

(6)签名:当输入一个消息 m 的签名时,用户按以下方式对消息 m 进行签名:

1)签名者选取大的随机整数 $a \in Z_q^*$。

2)签名者计算 $MP_m = H_2(m) \in Z_q^*$。

3)签名者计算 $MP_{1m} = a x_m Q_m \in G_1^*$

4)签名者计算 $s_m = e(MP_m D_m, Z_m)^a = e(Q_m, P)^{as x_m H_2(m)}$。

5)签名者发送 $\sigma = (m, MP_{1m}, s_m)$ 作为签名。

(7)验证：验证者收到签名以后，使用用户 m 的公钥$\langle X_m, Y_m\rangle$来验证签名，具体如下：

1)验证者计算 $e(X_m, Q_m)=e(Y_m, P)$，如果等式成立则说明用户 m 的公钥是真实的，否则签名被拒绝。

2)验证者计算 $MP_m{}'=H_2(m)\in Z_q^*$。

3)验证者计算$r_m=e(MP_{1m}, P_{\text{pub}})^{H_2(m)}$。

4)验证者验证等式$r_m=s_m$。如果等式成立，则签名有效并输出 1；否则输出 0。

6 改进方案的分析

6.1 正确性分析

根据改进方案中的签名验证等式进行如下验证：

$$\begin{aligned}s_m&=e(MP_mD_m, Z_m)^a\\&=e(Q_m, P)^{asx_mH_2(m)}\\&=e(ax_mQ_m, sP)^{H_2(m)}\\&=e(MP_{1m}, P_{\text{pub}})^{H_2(m)}=r_m\end{aligned}$$

因此，本文给出的改进方案是正确的。

6.2 安全性分析

本节分析改进方案的安全性，指出该方案在两种类型的攻击下是安全的。

定理 1 在以 ECDHP 和 BDHP 为数学难解问题假设的随机预言机模型下，改进方案在自适应选择的消息攻击下是存在性不可伪造的。

引理 1 在第一类强敌手A_I攻击下，假设强敌手A_I能够在时间 t 内进行q_H次$H_i(i=1,2)$预言机询问、q_e次部分私钥提取询问、q_{sk}次私钥提取询问、q_{pk}次公钥提取询问、q_s次签名提取询问，则存在一个算法 C 以(ε, t')的优势和时间可以解决 ECDHP 问题。$\varepsilon'<\varepsilon\left(\frac{q_H-1}{q_H}\right)^{q_{sk}+q_s}$，$t'<t+(q_s+q_{pk})t_{sm}+q_st_p$，$t_{sm}$和$t_p$分别是计算$G_1$上的一个标量乘和求一个双线性对的所用时间。

证明：设A_I是此方案的强敌手，即签名的伪造者。假设 C 被赋予了一个挑战：给定$Z_m=x_mP$ 和 abP，在与A_I交互后计算 abx_mP。C 作为挑战者，将与第一类强敌手A_I进行如下交互。

(1)系统建立：C 运行系统算法，选择一个生成元 P，计算$P_{\text{pub}}=sP$，s 是 C 不知道的系统主密钥。在这个游戏中，C 随机选择一个身份ID^*作为挑战 ID，并将 $params=\langle P, P_{\text{pub}}, H_1\rangle$作为公共参数给$A_I$。为了简单起见，我们假设对于任何$ID_i$，在$ID_i$被作为任何查询公钥提取、部分私钥提取、私钥提取和签名标记的输入之前，A_I询问H_1。

(2)H_1预言机询问：C 维护一个由二元组(ID_i, Q_i)组成的列表H_1^{list}，列表初始为空。当A_I用身份ID_i向 C 询问H_1时，如果ID_i已经储存在H_1^{list}中，则 C 将之前相应的值返回给A_I；否则，C 选择一个随机整数 $a\in Z_q^*$，计算$Q_i=aP$，将新元组(ID_i, Q_i)插入列表H_1^{list}中，然后返回给敌手A_I。

(3)H_2预言机询问：C 维护一个由二元组(ID_i, MP_{mi})组成的列表H_2^{list}，列表初始为空。当A_I用身份ID_i向 C 询问H_2时，如果ID_i已经储存在H_2^{list}中，则 C 将之前相应的值返回给A_I；否则，C 选择一个随机整数h_i，将新元组(ID_i, h_i)插入列表H_2^{list}中，然后返回给敌手A_I。

(4)公钥询问：C 维护一个由四元组(ID_i, Q_i, r_i, pk_i)组成的列表pk^{list}，列表初始为空。当敌手A_I输入ID_i询问时，C 检查其是否存在于列表pk^{list}中，如果存在则返回给 A_I；否则，C 从列表H_1^{list}中恢复相应的元组(ID_i, Q_i)并选择一个随机值$r_i\in Z_q^*$，计算$pk_i=\langle X_i, Y_i\rangle=\langle r_iP, r_iQ_i\rangle$返回$pk_i$。然后 C 将(ID_i, Q_i, r_i, pk_i)插入列表pk^{list}。

(5)公钥替换询问：当强敌手A_I输入(ID_i, pk_i)询问时，C 检查是否元组(ID_i, Q_i, r_i, pk_i)存在于列表pk^{list}中，如果存在则 C 计算$pk_i=pk_i{}'$并将$(ID_i, Q_i, r_i{}', pk_i{}')$插入到列表$pk^{\text{list}}$中。这里，我们假设 C 可以从A_I获得对应于替换的$pk_i{}'=\langle r_i{}'P, r_i{}'Q_i\rangle$的替换秘密值$r_i{}'$；否则，$C$ 执行公钥提取生成(ID_i, Q_i, r_i, pk_i)，然后计算$pk_i=pk_i{}'$并将其插入列表pk^{list}中。

(6)私钥询问：C 维护一个由二元组(ID_i, Z_i)组成的列表Z^{list}，列表初始为空。如果列表Z^{list}已经储存(ID_i, Z_i)，则 C 返回此二元组给强敌手A_I；否则，C 调用身份ID_i上的私钥提取预言机并获取值Z_i，将其转发给强敌手A_I并将其插入列表Z^{list}中。

(7)C 维护一个列表sk^{list}，用于对输入ID_i进行查询，如果$ID_i=ID^*$，C 中止并输出“failure”(用E_1表示此事件)。否则，C 选取一个随机数$x_i\in Z_q^*$并进行如下计算：

1)如果E^{list}和pk^{list}已经分别储存相应的元组(ID_i, Q_i, D_i)和(ID_i, Q_i, r_i, pk_i)，则 C 设置$sk_i=x_iD_i$，$Z_i=x_iP$，返回(ID_i, x_i, sk_i, Z_i)给强敌手A_I并将其插入列表sk^{list}中。

2)否则，C 使用身份ID_i对部分私钥询问和公钥询问，然后模拟上述过程，将(ID_i, x_i, sk_i, Z_i)发送给强敌手A_I，并将它们添加到列表sk^{list}中。

(8)签名询问：当 C 接收到一个(ID_i, m_j)的签名询问时，进行如下计算：

1)如果$ID_i=ID^*$，C 中止并输出“failure status”(用E_2表示此事件)。

2)否则，C 从sk^{list}中恢复(ID_i, x_i, sk_i, Z_i)，从pk^{list}中恢复(ID_i, Q_i, pk_i)和H_1^{list}中恢复(m_j, MP)。

3)选取一个随机整数 $a\in Z_q^*$。

4)计算 $MP_1=ax_mQ_m$。

5)计算$s_m=e(MP_mD_m, Z_i)^a$，令(MP_1, s_i)作为身份ID_i在消息m_j上的签名。C 返回(MP_1, s_i)给强敌手A_I作为签名预言机的回应。

最后，强敌手A_I中止模拟并输出一个身份ID^*在消息m^*上的签名 $\sigma=(V^*, S^*)$，此签名满足验证公式$(m^*, ID^*, pk^*, S^*)=1$。C 从pk^{list}中恢复(ID^*, Q^*, pk^*)，从Z^{list}和H_1^{list}中恢复(ID^*, Z)和(m^*, MP^*)，并选取一个随机整数 $a\in Z_q^*$，然后得到$e(V^*, X_i^*)=e(a^*xb^*P, r^*P)=S^*$，$a^*xb^*P=V^*$。

因此，C 可以成功地计算和输出$a^*xb^*P=V^*$作为解决强敌手A_I挑战的方法。挑战者 C 以概率$\varepsilon'<\varepsilon\left(\frac{q_H-1}{q_H}\right)^{q_{sk}+q_s}$和多项式时间$t'<t+(q_s+q_{pk})t_{sm}+q_st_p$解决了$G_1$中的 ECDHP 问题。

引理 2 在第二类强敌手A_{II}攻击下，假设敌手A_{II}能够在时间 t 内进行q_H次H_1预言机询问、q_e次部分私钥提取询问、q_{sk}次私钥提取询问、q_{pk}次公钥提取询问、q_s次签名提取询问，

则存在一个算法 C 以(ε,t')的优势和时间可以解决 BDHP 问题。$\varepsilon'<\varepsilon\left(\frac{q_H-1}{q_H}\right)^{q_e+q_{sk}+q_s}$，$t'<t+(q_s+q_{pk})t_{sm}+q_s t_p$，$t_{sm}$和$t_p$分别是计算$G_1$上的一个标量乘和求一个双线性对的所用时间。

证明：设A_{II}是此方案的敌手，即签名的伪造者。假设 C 被赋予了一个挑战：给定$Z_m=x_mP$，abP 和$X_m=r_mP$，在与A_{II}交互后计算$e(P,P)^{abr_mx_m}$。C 作为挑战者，将与第二类敌手A_{II}进行如下交互。

(1)系统建立：C 运行系统算法，选择一个生成元 P，计算$P_{\text{pub}}=sP$，s 是 C 不知道的系统主密钥。在这个游戏中，C 随机选择一个身份ID^*作为挑战 ID，并将 $params=\langle P,P_{\text{pub}},H_1\rangle$作为公共参数给$A_{II}$。为了简单起见，我们假设对于任何$ID_i$，在$ID_i$被作为任何查询公钥提取、部分私钥提取、私钥提取和签名标记的输入之前，A_{II}询问H_1。

(2)H_1预言机询问：C 维护一个由二元组(ID_i,Q_i)组成的列表H_1^{list}，列表初始为空。当A_{II}用身份ID_i向 C 询问H_1时，如果ID_i已经储存在H_1^{list}中，则 C 将之前相应的值返回给A_{II}；否则，C 选择一个随机整数 $a\in Z_q^*$，计算$Q_i=aP$，将新元组(ID_i,Q_i)插入列表H_1^{list}中，然后返回给敌手A_{II}。

(3)H_2预言机询问：C 维护一个由二元组(ID_i,MP_{mi})组成的列表H_2^{list}，列表初始为空。当A_{II}用身份ID_i向 C 询问H_2时，如果ID_i已经储存在H_2^{list}中，则 C 将之前相应的值返回给A_{II}；否则，C 选择一个随机整数h_i，将新元组(ID_i,h_i)插入列表H_2^{list}中，然后返回给敌手A_{II}。

(4)部分私钥询问：C 维护一个由三元组(ID_i,Q_i,D_i)组成的列表E_1^{list}，列表初始为空。对于任意给定的身份ID_i，C 从列表H_1^{list}中恢复相应的元组(ID_i,Q_i)，如果$ID_i\neq ID^*$，则计算$D_i=sQ_i$返回给敌手A_{II}，并将元组(ID_i,Q_i,D_i)插入列表E_1^{list}中；否则，C 中止并输出“failure”(用E_1表示此事件)。

(5)公钥询问：C 维护一个由四元组(ID_i,Q_i,r_i,pk_i)组成的列表pk^{list}，列表初始为空。当敌手A_{II}输入ID_i询问时，C 检查此四元组是否存在于列表pk^{list}中，如果存在则返回给 A_{II}；否则，C 从列表H_1^{list}中恢复相应的元组(ID_i,Q_i)并选择一个随机值$r_i\in Z_q^*$，计算$pk_i=\langle X_i,Y_i\rangle=\langle r_iP,r_iQ_i\rangle$返回$pk_i$。然后 C 将(ID_i,Q_i,r_i,pk_i)插入列表pk^{list}。

(6)私钥询问：C 维护一个由二元组(ID_i,Z_i)组成的列表Z^{list}，列表初始为空。如果列表Z^{list}已经储存(ID_i,Z_i)，则 C 返回二元组给敌手A_{II}；否则，C 调用身份ID_i上的私钥提取预言机并获取值Z_i，将其转发给敌手A_{II}并将其插入列表Z^{list}中。

C 维护一个列表sk^{list}，用于对输入ID_i进行查询，如果$ID_i=ID^*$，C 中止并输出“failure”(用E_2表示此事件)。否则，C 选取一个随机数$x_i\in Z_q^*$并进行如下计算：

1)如果E^{list}和pk^{list}已经分别储存相应的元组(ID_i,Q_i,D_i)和(ID_i,Q_i,r_i,pk_i)，则 C 设置$sk_i=x_iD_i$，$Z_i=x_iP$，返回(ID_i,x_i,sk_i,Z_i)给敌手A_{II}并将其插入列表sk^{list}中。

2)否则，C 使用身份ID_i对部分私钥询问和公钥询问，然后模拟上述过程，将(ID_i,x_i,sk_i,Z_i)发送给敌手A_{II}，并将它们添加到列表sk^{list}中。

(7)签名询问：当 C 接收到一个(ID_i,m_j)的签名询问时，进行如下计算：

1)如果$ID_i=ID^*$，C 中止并输出“failure status”(用E_3表示此事件)。

2)否则，C 从sk^{list}中恢复(ID_i,x_i,sk_i,Z_i)，从pk^{list}中恢复(ID_i,Q_i,pk_i)和从H_1^{list}中恢复(m_j,MP)。

3)选取一个随机整数 $a\in Z_q^*$。

4)计算 $MP_1=ax_mQ_m$。

5)计算$s_m=e(MP_mD_m,Z_i)^a$和(MP_1,s_i)是身份ID_i在消息m_j上的签名。C 返回(MP_1,s_i)给敌手A_{II}作为签名预言机的回应。

最后，敌手A_{II}中止模拟并输出一个身份ID^*在消息m^*上的签名 $\sigma=(V^*,S^*)$，此签名满足验证公式$(m^*,ID^*,pk^*,S^*)=1$。C 从pk^{list}中恢复(ID^*,Q^*,pk^*)，从Z^{list}和H_1^{list}中恢复(ID^*,Z)和(m^*,MP^*)，并选取一个随机整数$a^*\in Z_q^*$，然后得到$e(V^*,X_i^*)=e(a^*x^*b^*P,rP)=S^*$，$a^*x^*b^*P=S^*$。

因此，C 可以成功地计算和输出$e(P,P)=S^{*1/(x^*b^*)}$作为解决敌手A_{II}挑战的方法。挑战者 C 以概率$\varepsilon'<\varepsilon\left(\frac{q_H-1}{q_H}\right)^{q_e+q_{sk}+q_s}$和多项式时间$t'<t+(q_s+q_{pk})t_{sm}+q_st_p$解决了$G_1$，$G_2$中的 BDHP 问题。

因此，如果攻击者在赢得引理 1 和引理 2 中定义的游戏 I 和游戏 II 方面没有优势，那么所提出的无证书数字签名方案是在随机预言机模型中，对自适应选择性消息攻击是存在性不可伪造的，是基于假设G_1中的 ECDHP 问题和 BDHP 问题是难以解决的。

6.3 效率分析

表 1 列出了本文提出的改进方案与文献[24-27]中方案的比较。表 1 中，B 表示双线性对运算；H 表示 Hash 函数运算；X 表示形如 xQ 的乘法运算；M 表示模幂运算；N 表示模乘运算。

表 1 方案性能比较

Table 1 Performance comparison of different schemes

效率比较	签名方案	验证方案	安全性
文献[24]方案	$3N+2H$	$4B+3H+N$	安全
文献[25]方案	$X+M+B+H$	$B+X+M+H$	安全
文献[26]方案	$6M+3X+H$	$5B+2H+M$	安全
文献[27]方案	$H+M+N$	$3B+H+M+N$	安全
改进后方案	$B+H+2X+M+N$	$3B+H+M$	安全

从表 1 中可以看出，改进后的无证书签名方案与文献[24,26]的方案相比，在签名和验证中计算效率具有优势；与文献[25,27]的方案相比在效率上差异不大。综上所述，改进后的方案效率较高。

结束语 本文分析了 Hassouna 等[22]提出的强安全无证书签名方案，指出了该方案不能抵抗消息篡改攻击，无法保证消息的真实性和完整性，同时，存在由系统主密钥生成的私钥在签名验证中未完全利用的缺陷。针对该方案出现的错误，本文在没有降低执行效率的前提下，对原签名方案进行了改进。安全分析表明，在随机预言机模型中，改进方案对自适应选择性消息攻击是存在性不可伪造的，即是安全的。本文的改进方案在签名和验证过程中都用到了双线性对的计算，使得计算过程复杂且用时长。在今后的研究中，设计算法效率更高且具有强安全的无证书签名方案是进一步研究的重点。

参 考 文 献

[1] SHAMIR A. Identity-Based Cryptosystems and Signature Schemes[C]// Workshop on the Theory & Application of Cryptographic Techniques. Berlin: Springer, 1984.

[2] BARRETO P S L M, KIM H Y, LYNN B, et al. Efficient Algorithms for Pairing-Based Cryptosystems[C]// International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 2002.

[3] BARRETO P, LYNN B, SCOTT M. Constructing Elliptic Curves with Prescribed Embedding Degrees[C]// Springer Berlin Heidelberg. Berlin: Springer, 2003.

[4] BONEH D, LYNN B, SHACHAM H. Short Signatures from the Weil Pairing[C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001.

[5] HESS F. Efficient Identity Based Signature Schemes Based on Pairings[C]// International Workshop on Selected Areas in Cryptography. Berlin: Springer, 2003.

[6] RIYAMI S S, PATERSON K G. Certificateless Public Key Cryptography[C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2003.

[7] DENT A W, BENOÎT L, PATERSON K G. Certificateless encryption schemes strongly secure in the standard model[C]// Public Key Cryptography-PKC 2008, 11th International Workshop on Practice and Theory in Public-Key Cryptography, Barcelona, Spain, 2008. Berlin: Springer, 2008.

[8] VIVEK S S, SELVI S S D, RANGAN C P. CCA2 Secure Certificateless Encryption Schemes Based on RSA[C]// International Conference on Security & Cryptography. IEEE, 2014.

[9] WANG C, HUANG H, TANG Y. An Efficient Certificateless Signature from Pairings[C]// International Symposium on Data. IEEE, 2007.

[10] XIONG H, QIN Z, LI F. An Improved Certificateless Signature Scheme Secure in the Standard Model[J]. Fundamenta Informaticae, 2008, 88(1): 193-206.

[11] ZHANG L, ZHANG F. A New Provably Secure Certificateless Signature Scheme[C]// IEEE International Conference on Communications. IEEE, 2008.

[12] SHIM K A. Forgery Attacks on Two Provably Secure Certificateless Signature Schemes[J]. Information Sciences, 2020, 521: 81-87.

[13] YANG X, PEI X, CHEN G, et al. A Strongly Unforgeable Certificateless Signature Scheme and Its Application in IoT Environments[J]. Sensors, 2019, 19(12): 2692.

[14] HUANG L, ZHOU J, ZHANG G, et al. Certificateless Public Verification for the Outsourced Data Integrity in Cloud Storage [J]. Journal of Circuits, Systems and Computers, 2018, 27(11): 1850181. 1-1850181. 17.

[15] YANG X D, WANG M D, PEI X Z, et al. Security Analysis and Improvement of a Certificateless Signature Scheme in the Standard Model[J]. Acta Electronica Sinica, 2019, 47(9): 1972-1978.

[16] DU H Z, WEN Q Y, ZHANG S S, et al. A new provably secure certificateless signature scheme for Internet of Things[J]. Ad Hoc Networks, 2019, 100: 102074.

[17] YANG X, PEI X, CHEN G, et al. A Strongly Unforgeable Certificateless Signature Scheme and Its Application in IoT Environments[J]. Sensors, 2019, 19(12): 2692.

[18] SELVI S S D, VIVEK S S, RANGAN C P. Certificateless KEM and Hybrid Signcryption Schemes Revisited[C]// International Conference on Information Security Practice and Experience. Berlin: Springer, 2010.

[19] XIE W, ZHANG Z. Certificateless signcryption without pairing [J/OL]. IACR Cryptology ePrint Archive, 2010, 187. https://www. researchgate. net/publication/220336349_Certificateless_Signcryption_without_Pairing.

[20] XIE W, ZHANG Z. Efficient and provably secure certificateless signcryption from bilinear maps[C]// IEEE International Conference on Wireless Communications. IEEE, 2010.

[21] HASSOUNA M, BASHIER E, BARRY B. A Short Certificateless Digital Signature Scheme[C]// International Conference of Digital Information Processing, Data Mining and Wireless Communications. 2015.

[22] HASSOUNA M, BASHIER E, BARRY B. A Strongly Secure Certificateless Digital Signature Scheme in The Random Oracle Model[J]. International Journal of Network Security, 2016, 18(5): 938-945.

[23] HUANG X, MU Y, SUSILO W, et al. Certificateless Signature Revisited[C]// Australasian Conference on Information Security & Privacy. Springer-Verlag, 2007.

[24] ZHANG Z, WONG D S, XU J, et al. Certificateless Public-Key Signature: Security Model and Efficient Construction[C]// International Conference on Applied Cryptography & Network Security. Springer-Verlag, 2006.

[25] CHEN J S, HUANG Z J. Efficient certificbased signature schenle[J]. Computer Engineering Applications, 2012, 48(30): 98-102.

[26] LIU J K, BAEK J, SUSILO W, et al. Certificate-Based Signature Schemes without Pairings or Random Oracles[C]// Information Security, International Conference, Isc, Taipei, Taiwan, September. Berlin: Springer, 2008.

[27] MING Y, WANG Y M. Efficient Certificateless Signature Scheme Based on Bilinear Pairings[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(2): 175-177.

YE Sheng-nan, born in 1996, postgraduate. Her main research interests include cryptography and information security.

CHEN Jian-hua, born in 1964, Ph. D, professor, Ph. D supervisor. His main research interests include cryptography and information security.