doi:10.11959/j.issn.1000-436x.2015060

无证书签密机制的安全性分析与改进

赵振国
(华北水利水电大学 水利学院，河南 郑州 450045)

摘 要：为了解决传统公钥密码体制中的证书管理问题和身份基公钥密码体制中的密钥托管问题，Al-Riyami 和 Paterson 提出了无证书公钥密码体制。最近朱辉等提出了一个不含双线性对运算的无证书签密机制。然而，通过对其进行分析，发现该机制是不安全的（即不能提供保密性和不可伪造性），并给出了具体的攻击方法。为了增强安全性，提出了一个更安全的无证书签密机制，并在随机预言模型下基于离散对数问题和计算性 Diffie-Hellman 问题给出了安全性证明。此外，新机制具有良好的性能，签密算法只需要 4 个模幂运算，解密验证算法只需要 5 个模幂运算。

关键词：签密；无证书；随机预言模型；双线性对
中图分类号：TP309 **文献标识码**：A

Security analysis and improvement of a certificateless signcryption scheme

ZHAO Zhen-guo
(School of Water Conservancy, North China University of Water Resources and Electric Power, Zhengzhou 450045, China)

Abstract: To solve the certificate management problem in the traditional public key cryptography and the key escrow problem in the identity-based public key cryptography, Al-Riyami and Paterson proposed the concept of the certificateless public key cryptography. Recently, Zhu *et al*. proposed a certificateless signcryption without bilinear pairings. However, their scheme was completely insecure against with two concrete attacks. A strongly secure certificateless signcryption without bilinear pairings was also proposed, which was provably secure in the random oracle model under the assumption that the discrete logarithm problem and the computational Diffie-Hellman problems were intractable. Furthermore, the efficiency of the proposed scheme is very high since only four modular exponentiations and five modular exponentiations are needed in the signcryption algoriahm and unsigncryption algorithm separately.

Key words: signcryption; certificateless; random oracle model; bilinear pairing

1 引言

在传统公钥密码中，用户的公钥是通过可信认证中心 CA(certification authority)颁发证书来和户的身份进行绑定。在这样的系统中，大量的存储空间和计算时间被浪费在证书管理上。为了简化证书管理，Shamir 提出了基于身份的公钥密码[1]。在基于身份的公钥密码中，用户的身份(如学号、电子邮件等)就是用户的公钥。因此可以解决传统公钥密码中的证书管理问题。然后，在这种机制中，用户的私钥是由密钥生成中心 KGC (key generation center)通过用户的身份来生成的。密钥中心可以解密任何用户的密文，也可以伪造用户的签名。因此，基于身份的公钥密码面临着密钥

收稿日期：2013-10-29；**修回日期**：2014-02-10
基金项目：“十二五”国家科技支撑计划基金资助项目(2011BAD25B01)；华北水利水电大学高层次人才引进基金资助项目(NCWU201248)；河南省教育厅科学技术重点研究基金资助项目(13A570704)
Foundation Items: The “Twelfth 5-year-plan” Support Plan Projects (2011BAD25B01); The Introduction of High-Level Talents Foundation of North China University of Water Resources and Electric Power (NCWU201248); The Key Technique Program of the Education Department of Henan Province (13A570704)

托管问题。为了解决这个问题，Al-Riyami 等[2]提出了无证书公钥密码。

自从 Al-Riyami 等[2]提出无证书公钥密码以来，无证书签密机制得到了广泛关注和研究。在2008 年，Barbosa 等[3]提出了第 1 个无证书签密机制并在随机预言模型下证明其安全性。然而，Barbosa 等的机制是采用先加密后签名方式，并不能提供不可伪造性。Aranha 等[4]和 Wu 等[5]分别提出了改进的无证书签密机制，并声称机制是可证安全的。Sharmil 等[6]指出上述 2 种机制[4,5]都存在不同程度的安全缺陷。Liu 等[7]提出了第 1 个在标准模型下可证安全的无证书签密机制。然而，Weng 等[8]指出 Liu 等的机制既不能提供保密性，也不能提供不可伪造性。随后，Zhou 等[9]提出了 1 个广义无证书签密，并在随机预言模型下证明其安全性。理论分析[10]和实验结果[11]表明，在达到相同安全强度的条件下，执行 1 次双线性对操作的时间至少是椭圆曲线上点乘运算的 20 倍。因此，无需双线性对运算的无证书签密机制具有更好的性能。最近，Zhu 等[12]提出了 1 个无需双线性对运算的无证书签密机制。同时，Zhu 等在随机预言模型下证明了其安全性。

本文首先指出Zhu等的无需双线性对的无证书签密机制是不安全的，即第 1 类攻击者可以解密密文，也可以伪造密文。为了克服 Zhu 等机制中存在的安全缺陷，本文提出了 1 个改进的无需双线性对的签密机制，并在随机预言模型下证明了其安全性。由于无需双线性对的计算，本文的机制继承了Zhu 等机制的高效性。

2 有关数学难题及其假设

离散对数(DL, discrete logarithm) 问题:设 G 是 1 个阶为 q 的乘法循环， g 是 1 个生成元，对于给定的 1 个元素 g^a，计算 a，其中 $a\in Z_q^*$，是 1 个未知的元素。

设 A 是 1 个多项式算法，定义它解决 DL 问题的优势为

$$\mathrm{Adv}^{DL}(A)=\Pr[A(g^a)=a\mid a\in Z_q^*]$$

DL 假设: 对于任意的多项式算法 A，$\mathrm{Adv}^{DL}(A)$ 是可以忽略的。

计算性 Diffie-Hellman(CDH, computational Diffie-Hellman）问题：设 G 是 1 个阶为 q 的乘法循环，g 是 1 个生成元,对于给定的 2 个元素 g^a 和 g^b，计算 g^{ab}，其中 $a,b\in Z_q^*$，是 2 个未知的元素。

设 A 是 1 个多项式算法，定义它解决 CDH 问题的优势为

$$\mathrm{Adv}^{CDH}(A)=\Pr[A(g^a,g^b)=g^{ab}\mid a,b\in Z_q^*]$$

CDH 假设：对于任意的多项式算法，$\mathrm{Adv}^{CDH}(A)$ 是可以忽略的。

3 Zhu 等的无证书签密机制

1) 系统参数建立算法(setup)

输入安全参数 k，产生 2 个大素数 p、q，且 $q\mid p-1$。g 为循环群 Z_p^* 中 1 个阶为 q 的生成元，选择安全散列函数: $H_1:\{0,1\}^*\times Z_p^*\to Z_q^*$， $H_2:\{0,1\}^n\to Z_q^*$， $H_3:Z_p^*\to\{0,1\}^n$，其中 n 为明文消息比特长度。KGC 随机选择主密钥 $x\in Z_q^*$，计算 $y=g^x$，公开系统参数(p,q,g,y,H_1,H_2,H_3)，保密主密钥 x。

2) 部分密钥生成算法(partial key extract)

给定用户身份 ID_i，KGC 随机选择 $s_i\in Z_q^*$，计算 $w_i=g^{s_i}$， $t_i=s_i+xH_1(ID_i,w_i)$，其中 t_i 作为用户的部分密钥 PS_i， w_i 作为用户的部分公钥 PP_i。

3) 私钥生成算法(private key extract)

给定用户身份 ID_i 和部分密钥 PS_i，用户随机选取 $z_i\in Z_q^*$ 作为秘密值，生成用户私钥 $SK_i=(t_i,z_i)$。

4) 公钥生成(public key extract)

给定用户的身份 ID_i、部分公钥 PP_i 和 z_i，用户计算 $u_i=g^{z_i}$，生成用户公钥 $PK_i=(w_i,u_i)$。

5) 签密算法(sign crypt)

当用户 A 要发送消息 m 给用户 B 时，A 进行以下操作。

① A 随机选取 $r\in Z_q^*$ 并计算 $R=g^r$。

② A 计算 $h_B=H_1(ID_B,w_B)$，$h=H_2(m,R,ID_A)$，$s=\dfrac{r}{z_A+t_A+h}$， $c=H_3((u_Bw_By^{h_B})^r)\oplus m$。

③发送消息 $\sigma=\{h,s,c\}$ 给 B。

6) 解密验证算法(un sign crypt)

① B 计算 $h_B=H_1(ID_B,w_B)$ 并恢复明文 $m=H_3((u_Aw_Ay^{h_A}g^h)^{s(z_B+t_B)})\oplus c$。

②若 $h=H_2(m,(u_Aw_Ay^{h_A}g^h)^s,ID_A)$ 成立，则 B 接受消息 m。

4　Zhu 等机制的安全性分析

Zhu 等在随机预言模型下证明他们的机制是安全的。本章节将通过具体的攻击来证明他们的机制不能满足类型 1 敌人攻击下的保密性和不可伪造性。设用户 A 和 B 分别为发送者和接受者。A 的私钥 $SK_A=\{t_A,z_A\}$，公钥 $PK_A=\{w_A,u_A\}$。B 的私钥 $SK_B=\{t_B,z_B\}$，公钥 $PK_B=\{u_B,w_B\}$。设 $A1$ 是类型 1 的攻击者，则 $A1$ 不知道系统主密钥，但是 $A1$ 可以随时查询用户公钥或替换合法用户的公钥。

1) 保密性

Zhu 等证明他们的机制在面对类型 1 敌人 $A1$ 的攻击时可以提供保密性。然而下面的攻击说明，$A1$ 可以从截获的密文中恢复明文。具体过程如下。

① $A1$ 生成随机数 $b\in Z_q^*$，计算 $h_B=H_1(ID_B,w_B)$，$u'_B=\dfrac{g^b}{w_B y^{h_B}}$，并且利用 u'_B 替换 $PK_B=\{u_B,w_B\}$ 中的 u_B。

② 当用户 A 要发送消息 m 给用户 B 时，A 随机选取 $r\in Z_q^*$ 并计算 $R=g^r$，计算 $h_B=H_1(ID_B,w_B)$，$h=H_2(m,R,ID_A)$，$s=\dfrac{r}{z_A+t_A+h}$，$c=H_3((u'_B\ w_B\ y^{h_B})^r)\oplus m$，并发送消息 $\sigma=\{h,s,c\}$ 给 B。

③ 在截获消息 σ 后，$A1$ 计算 $h_B=H_1(ID_B,w_B)$ 并恢复明文 $m=H_3((v_A w_A y^{h_A} g^h)^{sb})\oplus c$。

定理 1　$A1$ 通过上述方法可以恢复明文。

证明　由于 $A1$ 进行了公钥替换，因此 B 的公钥为：$PK_B=\{u'_B,w_B\}$，其中 $u'_B=\dfrac{g^b}{w_B y^{h_B}}$。因此可以得到

$$(u'_B w_B y^{h_B})^r=(\frac{g^b}{w_B y^{h_B}} w_B y^{h_B})^r=(g^b)^r=g^{br} \quad (1)$$

$$(v_A w_A y^{h_A} g^h)^{sb}=(g^{z_A+t_A+h})^{\frac{r}{z_A+t_A+h}b}=g^{br} \quad (2)$$

所以 $(u'_B w_B y^{h_B})^r$ 和 $(v_A w_A y^{h_A} g^h)^{sb}$ 相等，进而 $H_3((u'_B w_B y^{h_B})^r)$ 和 $H_3((v_A w_A y^{h_A} g^h)^{sb})$ 相等，类型 1 攻击者 $A1$ 可以从截获的消息 σ 恢复明文 m。综上所述，Zhu 等机制不能满足类型 1 敌人攻击下的保密性。

2) 不可伪造性

Zhu 等证明他们的机制在面对类型 1 敌人 $A1$ 的攻击时可以提供不可伪造性。然而下面的攻击说明，$A1$ 可以伪造合法的密文。具体过程如下。

① $A1$ 生成随机数 $a\in Z_q^*$，计算 $h_A=H_1(ID_A,w_A)$，$u'_A=\dfrac{g^a}{w_A y^{h_A}}$，并且利用 u'_B 替换 $PK_A=\{u_A,w_A\}$ 中的 u_A。

② $A1$ 随机选取 $r\in Z_q^*$ 并计算 $R=g^r$，计算 $h_B=H_1(ID_B,w_B)$，$h=H_2(m,R,ID_A)$，$s=\dfrac{r}{a+h}$ 和 $c=H_3((u_B w_B y^{h_B})^r)\oplus m$。最后 $A1$ 发送消息 $\sigma=\{h,s,c\}$ 给 B。

定理 2　$A1$ 通过上述方法产生的密文是合法的。

证明　只需证明产生的密文能够通过解密验证过程即可。由于 $A1$ 进行了公钥替换，因此 A 的公钥为：$PK_A=\{u'_A,w_A\}$，其中 $u'_A=\dfrac{g^a}{w_A y^{h_A}}$。因为

$$(u_B w_B y^{h_B})^r=(g^{z_B+t_B})^r=g^{(z_B+t_B)r} \quad (3)$$

$$(u'_A w_A y^{h_A} g^h)^{s(z_B+t_B)}$$
$$=(\frac{g^a}{w_A y^{h_A}} w_A y^{h_A} g^h)^{\frac{r}{a+h}(z_B+t_B)}$$
$$=(g^{a+h})^{\frac{r}{a+h}(z_B+t_B)}=g^{(z_B+t_B)r} \quad (4)$$

$$(u'_A w_A y^{h_A} g^h)^s=(\frac{g^a}{w_A y^{h_A}} w_A y^{h_A} g^h)^{\frac{r}{a+h}}$$
$$=(g^{a+h})^{\frac{r}{a+h}}=g^r=R \quad (5)$$

因此有 $H_3((u'_A w_A y^{h_A} g^h)^{s(z_B+t_B)})$ 和 $H_3((u_B w_B y^{h_B})^r)$ 相等。当收到消息 σ 后，B 计算 $h_B=H_1(ID_B,w_B)$，恢复明文 $m=H_3((u'_A w_A y^{h_A} g^h)^{s(z_B+t_B)})\oplus c$，并且 $H_2(m,(u_A w_A y^{h_A} g^h)^s,ID_A)$ 和 h 相等显然成立。因此 B 接受消息 m。$A1$ 成功地伪造了 1 组合法密文。综上所述，Zhu 等机制不能满足类型 1 敌人攻击下的不可伪造性。

5　改进的无证书签密机制

从以上分析得知，发送者的密钥为 z_A 和 t_A 的简单线性组合 z_A+t_A；接收者的密钥为 z_B 和 t_B 的简单线性组合 z_B+t_B。$A1$ 利用这种简单的线性关系，通过控制 u_A/u_B 来消除 t_A/t_B 对密文的影响。因此，只要能破坏这种线性关系，就可以抵抗上述攻击。

改进机制也由系统参数建立算法、部分密钥生成算法、私钥生成算法、公钥生成算法、签密算法和解密验证算法组成。其中，前 4 个算法同 Zhu 等机制中的相同。签密算法和解密验证算法如下所述。

1) 签密算法(sign crypt)

当用户 A 要发送消息 m 给用户 B 时，A 进行以下操作。

① A 随机选取 $r\in Z_q^*$ 并计算 $R=g^r$。

② A 计算 $k_A=H_2(ID_A,u_A,w_A,y)$，$h_B=H_1(ID_B,w_B,y)$，$k_B=H_2(ID_B,u_B,w_B,y)$，$T=(u_B^{k_B}w_By^{h_B})^r$，$h=H_3(m,R,T)$，$s=\dfrac{r+h}{k_Az_A+t_A}$ 和 $c=H_4(T)\oplus m$。

③发送消息 $\sigma=\{R,s,c\}$ 给 B。

2) 解密验证算法(un sign crypt)

收到密文 σ 后，B 进行以下操作。

① B 计算 $k_B=H_2(ID_B,u_B,w_B,y)$，$T=R^{k_Bz_B+t_B}$ 并恢复明文 $m=H_3(T)\oplus c$。

② B 计算 $h=H_3(m,R,T)$，$h_A=H_1(ID_A,w_A,y)$，$k_A=H_2(ID_A,u_A,w_A,y)$，$k_B=H_2(ID_B,u_B,w_B,y)$。B 检测等式 $(u_A^{k_A}w_Ay^{h_A})^s=Rg^h$ 是否成立。若成立，B 接受消息 m。

6 安全性证明

1) 保密性

引理 1 如果存在类型 I 的攻击者 $A1$ 能够在概率多项式时间内以不可忽略的优势 ε 在文献[12]的定义 1 的游戏中获胜，则存在挑战者 C 能够在概率多项式时间内以不可忽略的优势解决 CDH 问题。

证明 给定 CDH 问题实例(g^a，g^b)，挑战者 C 的目的是计算 g^{ab}。首先，C 设置系统公钥 $y=g^a$，以 $A1$ 为子程序并充当 CDH 问题的挑战者。C 把系统参数 $\{p,q,g,y,H_1,H_2,H_3,H_4\}$ 发送给 $A1$。C 按照文献[12]的定理 1 的方法来回答 $A1$ 提出的 $H1$ 查询、$H2$ 查询、$H3$ 查询、$H3$ 查询、部分密钥提取查询、私钥提取查询、公钥提取查询、公钥替换查询签密查询和解密验证查询。

经过有界次查询后，$A1$ 随机选择长度相同的明文 m_0、m_1 和系统挑战的 2 个用户身份 ID_A、ID_B。C 选择随机数 $b\in\{0,1\}$，随机选取 $r\in Z_q^*$ 并计算 $R=g^r$，A 计算 $k_A=H_2(ID_A,u_A,w_A,y)$，$h_B=H_1(ID_B,w_B,y)$，$k_B=H_2(ID_B,u_B,w_B,y)$，$T=(u_B^{k_B}w_By^{h_B})^r$，$h=H_3(m_b,R,T)$，$s=\dfrac{r+h}{k_Az_A+t_A}$ 和 $c=H_4(T)\oplus m_b$。最后，C 把密文 $\sigma=\{R,s,c\}$ 返回给 $A1$，这里 C 知道公钥被替换的情况。

经过有界次查询，$A1$ 输出对 b 的判断 b'。如果 $b'=b$，C 计算 $W=\left(\dfrac{(u_A^{k_A}w_Ay^{h_A})^s}{g^h}\right)^{k_Bz_B+t_B}$，并输出 $\left(\dfrac{W}{R^{z_Bk_B+s_B}}\right)^{e^{-1}}=\left(\dfrac{g^{r(z_Bk_B+s_B+ea)}}{g^{r(z_Bk_B+s_B)}}\right)^{e^{-1}}=g^{ra}$ 作为 CDH 问题的答案。否则，C 没有解决 CDH 问题。

若 $A1$ 对 ID_B 执行过部分密钥提取或私钥提取询问，对 R 或 T 执行过 $H3$ 查询或 $H4$ 查询，则 C 将终止仿真。设 q_i 表示 $A1$ 总共进行 Hi 查询的次数，这里 $i=1,2,3,4$。$A1$ 不对 ID_B 进行部分密钥提取查询或私钥提取查询的概率为 $1/q_1^2$。$A1$ 不对 R 或 T 执行过 $H3$ 查询或 $H4$ 查询的概率为 $1/q_3q_4$。因此，C 解决 CDH 问题的优势至少为 $\varepsilon/q_1^2q_3q_4$。

引理 2 如果存在类型Ⅱ的攻击者 $A2$ 能够在概率多项式时间内以不可忽略的优势 ε 在文献[12]的定义 2 的游戏中获胜，则存在挑战者 C 能够在概率多项式时间内以不可忽略的优势解决 CDH 问题。

证明 该引理的证明与引理 1 的证明基本相同。根据引理 1 和引理 2 的结论，可以得到以下定理。

定理 3 在适应性选择密文攻击下，改进的无证书签密机制具有不可区分性。

2) 不可伪造性

引理 3 如果存在类型 I 的攻击者 $A1$ 能够在概率多项式时间内以不可忽略的优势 ε 在文献[12]的定义 3 的游戏中获胜，则存在挑战者 C 能够在概率多项式时间内以不可忽略的优势解决 DL 问题。

证明 给定 DL 问题实例 g^a，挑战者 C 的目的是计算 $a\in Z_q^*$。首先，C 设置系统公钥 $y=g^a$，以 $A1$ 为子程序并充当 CDH 问题的挑战者。C 把系统参数 $\{p,q,g,y,H_1,H_2,H_3,H_4\}$ 发送给 $A1$。C 按照文献[12]的定理 3 的方法来回答 $A1$ 提出的 $H1$ 查询、$H2$ 查询、$H3$ 查询、$H4$ 查询、部分密钥提取查询、私钥提取查询、公钥提取查询、公钥替换查询签密查询和解密验证查询。

经过有界次查询后，$A1$输出 1 个伪造的密文$\sigma=\{R,s,c\}$，这里 C 知道公钥被替换的情况。如果密文是合法的，则等式$(u_A^{k_A}w_A y^{h_A})^s=Rg^h$成立。根据伪造定理[13]可以知道，选择不同的$H_1$、$H_2$、$H_3$、$H_4$，可以得到另外 1 个合法的签名$\sigma'=\{R,s',c'\}$和等式$(u_A^{k'_A}w_A y^{h'_A})^s=Rg^{h'}$。于是可以得到如下 2 个等式

$$(k_A z_A+t_A+ah_A)s=r+h \bmod q \tag{6}$$

$$(k'_A z_A+t_A+ah'_A)s'=r+h' \bmod q \tag{7}$$

在式(6)和式(7)中，仅有a和r 2 个未知量，因此可以通过解方程得到他们的值a^*和r^*。最后，C输出a^*作为 DL 问题的答案。

若$A1$对ID_B执行过部分密钥提取或私钥提取询问，对R或T执行过$H3$查询或$H4$查询，则C将终止仿真。设q_i表示$A1$总共进行 Hi 查询的次数，这里i=1、2、3、4。$A1$不对ID_B进行部分密钥提取查询或私钥提取查询的概率为$1/q_1^2$。采用重放技术[13]产生 2 个或 2 个以上有效密文时，C失败的概率小于$1/9$。因此，C解决 DL 问题的优势至少为$\varepsilon/9q_1^2$。

引理 4　如果存在类型Ⅱ的攻击者$A2$能够在概率多项式时间内以不可忽略的优势ε在文献[12]的定义 4 的游戏中获胜，则存在挑战者 C 能够在概率多项式时间内以不可忽略的优势解决 DL 问题。

证明　该引理的证明与引理 3 的证明基本相同。根据引理 3 和引理 4 的结论，可以得到以下定理。

定理 4　在适应性选择消息攻击下，改进的无证书签密机制具有不可伪造性。

7　性能比较

本章节将对本文提出的签密机制和其他无证书签密机制进行比较。Cao 等[14]给出了 MIRACAL 软件包在 PIV 3 GHz 协处理器和 512 MB 内存的 Windows XP 平台上的执行结果。为了达到 1 024 bit RSA 算法的安全强度，针对基于双线性对的机制，他们使用定义在超奇异曲线$E/F_p: y^2=x^3+3$，其中p是 1 个 512 bit 的素数。针对基于椭圆曲线的机制，他们使用定义在有限域$F_{2^{163}}$上的 Koblitz 曲线$y^2=x^3+ax^2+b$，这里$a=1$并且b是 1 个 163 bit 的素数。不同操作的运行时间如表 1 所示，其中 Pair、SM 和 ME 分别表示双线性对运算，椭圆曲线点乘运算和模幂运算。

表 1　不同操作的运行时间

Pair	SM_Pair	ME
20.01 ms	6.38 ms	11.20 ms

这里把本文无证书签密机制的性能同最新 2 个无证书签密机制 (Zhou 等的机制[9]和 Zhu 等的机制[12])的性能进行比较。同上述 3 种运算的运行时间相比，杂凑函数运算和异或运算的运行时间对整体性能的影响可以忽略不计。这里采用 Cao 等[14]相同的方法，仅把双线性对运算、椭圆曲线点乘运算和模幂运算的运行时间计算在内，具体如表 2 所示。由于没有双线性对运算，Zhu 等的机制和本文的机制具有更好的性能。然而，Zhu 等的机制既不能提供保密性也不能提供不可伪造性。作为 1 种密码机制，安全是第一位的，因此本文的机制更适合实际应用。

表 2　不同签密机制的性能比较

方法	签密运算	解密验证运算
文献[9]	1 SM _ Pair +5 SM + 1 ME ≈63.11 ms	4 SM _ Pair +1 SM + 3 ME ≈120.02 ms
文献[12]	3 ME ≈33.60 ms	4 ME ≈44.80 ms
本文	4 ME ≈44.80 ms	5 ME ≈56.00 ms

8　结束语

本文分析了 Zhu 等提出的无需双线性对的无证书签密机制，指出他们的机制是不安全的，并给出了具体的攻击方法。本文也提出了 1 个改进的无需双线性对的无证书签密机制。该方案具有很强的安全性，本文在随机预言模型下证明了其安全性。该方案继承了 Zhu 等机制的高效性，同时克服了他们机制中存在的安全缺陷。通过对比，本文提出的机制是目前最适合应用的无需双线性对签密机制。

参考文献：

[1] SHAMIRR A. Identity-based cryptosystem and signature scheme[A]. Cryptology-Crypto 1984[C]. Berlin: Springer-Verlag, 1984. 47-53.

[2] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[A]. Cryptology-Asiacrypt 2003[C]. Berlin: Springer-Verlag, 2003.

452-473.

[3] BARBOSA M, FARSHIM P. Certificateless signcryption[A]. Proc of the ACM Symp on Information. Computer and Communications Security (ASIACCS 2008)[C]. 2008. 369-372.

[4] ARANHA D, CASTROO R, LOPEZ J, *et al*. Efficient certificateless signcryption[EB/OL]. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_01_resumo.pdf.

[5] WU C, CHEN Z. A new efficient certificateless signcryption scheme[A]. Proc of the ISISE 2008[C]. Beijing, China, 2008. 661-664.

[6] SHARMILA D, VIVEK S, PANDU R. On the security of certificateless signcryption schemes[EB/OL]. http://eprint. iacr.org/2009/298.

[7] LIU Z, HU Y, ZHANG X, MA H. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(1): 452-464.

[8] WENG J, YAO G, DDENG R. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3): 661-667.

[9] ZHOU C, ZHOU W, DONG X. Provable certificateless generalized signcryption scheme[J]. Designs Codes and Cryptography, 2012,71(2): 1-16.

[10] CHEN L, CHENG Z, SMART N. Identity-based key agreement protocols from pairings[J]. Internal Journal of Information Security, 2007, 6(4):213-241.

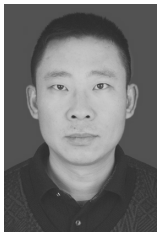
[11] HE H, CHEN J, HU J. An ID-based proxy signature schemes without bilinear pairings[J]. Annals of Telecommunications, 2011, 66(11-12): 657-662.

[12] 朱辉, 李晖, 王育民. 不使用双线性对的无证书签密机制方案[J]. 计算机研究与发展, 2010, 47(9): 1587-1594.
ZHU H, LI H, WANG Y M. Certificateless signcryption scheme without pairing[J]. Journal of Computer Research and Development, 2010, 47(9): 1587-1594.

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

[14] CAO X, KOU W, DU X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges[J]. Information Sciences, 2010, 180(15): 2895-2903.

作者简介：



赵振国（1978-），男，辽宁沈阳人，博士，华北水利水电大学讲师，主要研究方向为大型灌区水资源优化调配软硬件和智慧水利等。