具有强安全性的不含双线性对的无证书签名方案

葛爱军 陈少真
(解放军信息工程大学应用数学系 郑州 450002)

摘 要：该文提出了一种满足强安全性的不需双线性对运算的无证书签名方案，能抵抗适应性选择消息和适应性选择身份的存在性伪造攻击，并且在随机预言模型下基于离散对数难题给出了完整的安全性证明。与现有的绝大多数无证书签名方案都是基于双线性对的不同，该文提出的新方案没有复杂的双线性对运算，具有明显的效率优势。另外，通过对王会歌等人的无证书签名方案进行分析，指出此方案是不安全的，并给出了具体的攻击方法。

关键词：无证书签名；双线性对；离散对数问题；随机预言模型；强安全性
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2010)07-1765-04
DOI: 10.3724/SP.J.1146.2009.00965

Strongly Secure Certificateless Signature Scheme without Pairings

Ge Ai-jun Chen Shao-zhen
(*Department of Applied Mathematics*, *PLA Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: This paper presents a strongly secure certificateless signature scheme without pairings, which is existentially unforgeable against adaptive chosen message and ID attacks. The complete security proof is given under random oracle model, assuming that the discrete logarithm problem is intractable. The scheme is more computationally efficient than others built from pairings，as there is no heavily cost pairing operation in this scheme. In addition, a security analysis is presented for Wang H G's pairing-free certificateless public key signature, and the results show that the scheme is insecure with a concrete attack method.

Key words: Certificateless signature; Bilinear pairing; Discrete logarithm problem; Random oracle model; Strongly secure

1 引言

为了解决基于身份密码体制的密钥托管问题，Al-Riyami[1]等把传统的公钥密码体制与基于身份的密码体制相结合，进而给出了一种新的无证书公钥密码体制。在无证书密码体制中，用户的私钥是由两部分组成的，一部分是由用户自己随机产生的并且秘密保存，另一部分私钥是由 PKG 利用用户的身份信息给出的，这样 PKG 只能产生用户的部分私钥，这也就解决了基于身份密码体制固有的密钥托管问题，从而在无证书签名体制下进行签名可以达到真正的不可伪造性。

随着无证书密码体制的快速发展，许多无证书方案[2–6]被提出，但是这些无证书都是基于椭圆曲线来构造的，导致了昂贵的双线性对运算。鉴于此，本文在现有研究基础上[7,8]，利用 Schnorr 签名的思想，构造了一种新的不需要双线性对的无证书签名方案。因为没有计算代价昂贵的双线性对运算，方案效率要比其他现有的无证书签名方案更高。该方案安全性基于离散对数问题的难解性，并且在 Huang[5]等提出的关于无证书签名的最强攻击类型下都是存在性不可伪造的。

此外，文献[6]将无证书公钥密码体制和没有双线性对的签名体制相结合，提出了一种不依赖于双线性对运算的无证书公钥签名方案，并且声称他们的方案在随机预言模型下是安全的。本文通过分析，指出这种体制是不安全的，攻击者可以计算出签名者的完整私钥，进而可以冒充签名者对任何消息进行伪造签名。

2 预备知识

2.1 无证书签名体制的一般化模型

一个无证书签名体制一般是由如下 4 个多项式时间算法组成：

(1)系统建立算法(Setup)：该算法是由 PKG 完成的概率多项式时间算法，输入安全参数 k，输

2009-07-03 收到，2009-12-01 改回
国家自然科学基金 (60673081)和国家 863 计划项目(2006AA01Z417)资助课题
通信作者：葛爱军 geaijun@163.com

出系统公开参数 params 和主密钥 msk；

(2)密钥生成算法(Key-Extract)：该算法是由 PKG 和用户共同完成的概率多项式时间算法，首先 PKG 利用主密钥 msk 和系统公开参数 params 以及用户的身份 ID，计算出对应该用户的部分私钥 D_{ID} 和部分公钥 P_{ID} 并传送给该用户；然后用户选择一秘密值 s_{ID}，并利用系统公开参数 params，用户的身份 ID，用户的部分私钥 D_{ID}，部分公钥 P_{ID} 及秘密值 s_{ID}，计算出自己的完整私钥 $\mathrm{SK}_{\mathrm{ID}}$ 和完整公钥 $\mathrm{PK}_{\mathrm{ID}}$；

(3)签名算法(Sign)：该算法是由签名用户完成的概率多项式时间算法，输入系统公开参数 params，消息 m，签名用户的私钥 $\mathrm{SK}_{\mathrm{ID}}$，输出对消息 m 的无证书签名 σ；

(4)验证算法(Verify)：该算法是由验证者完成的确定性多项式时间算法，输入系统公开参数 params，消息 m，用户的公钥 $\mathrm{PK}_{\mathrm{ID}}$ 以及对消息 m 的签名 σ，输出判断值“接受”或者“拒绝”。

2.2 无证书签名体制的安全模型

在文献[5]中，根据攻击者的攻击能力，Huang 等人将无证书签名体制的攻击者分为 3 种: Normal Adversary，Strong Adversary，Super Adversary。结合文献[1]和文献[5]，我们给出如下两种攻击类型 A_{I} 和 A_{II}，并且本文所提出的无证书签名方案在最强的攻击类型 Super Type I，Super Type II 下都是存在性不可伪造的。

Super Type I 攻击者 A_{I}：第 2 类攻击者 A_{I} 不知道系统主密钥，但是他可以替换任意用户的公开密钥，在文献[5]中 Super Type I 攻击者 A_{I} 被赋予了最强的攻击能力: 即使对应的公钥已经被替换，A_{I} 仍然可以获得一些可通过验证的消息签名对(不需要 A_{I} 提供对应已经替换了的公钥的秘密值)。在实际应用中，A_{I} 模拟的是除 PKG 之外的攻击者。

Super Type II 攻击者 A_{II}：第 2 类攻击者 A_{II} 已经知道系统主密钥，所以他可以计算出所有用户的部分私钥，但是 A_{II} 不能替换指定用户的公钥。在文献[5]中 Super Type II 攻击者 A_{II} 也被赋予了最强的攻击能力: 即使对应的公钥已经被替换，A_{II} 仍然可以获得一些可通过验证的消息签名对(同样不需要 A_{II} 提供对应已经替换了的公钥的秘密值)。在实际应用中，A_{II} 模拟的是恶意 PKG 的非法攻击。

2.3 复杂性假设

设 p, q 是两个素数且 $q \mid (p-1)$，设 G 是 $\mathbb{Z}_p^*$ 的一个阶为 q 的子群，g 是 G 的生成元，假设 G 中的下列问题是难解的：

(1)离散对数问题(DLP)：给定元素 $\beta \in G$，寻找整数 $a \in \mathbb{Z}_q^*$，使得 $\beta = g^a \pmod p$。

(2)计算 Diffie-Hellman 问题(CDHP)：对 $a, b \in \mathbb{Z}_q^*$，已知 (g, g^a, g^b)，要计算 $g^{ab} \pmod p$。

3 文献[6]的没有双线性对的无证书签名方案及安全性分析

文献[6]中提出了一个不需要双线性对运算的无证书签名方案，该无证书签名方案是基于计算 Diffie-Hellman 问题困难的，本部分将对其进行分析。

3.1 文献[6]的无证书签名方案

首先回顾一下文献[6]中的无证书签名方案，方案描述如下：

(1)系统建立：输入安全参数 k，PKG 产生两个素数 p, q 且 $q \mid (p-1)$，随机选 $\mathbb{Z}_p^*$ 的一个阶为 q 的生成元 g，任意选取主密钥 $x \in \mathbb{Z}_p^*$ 并计算 $y = g^x$，选择 hash 函数 $H_1: \{0,1\}^* \times \mathbb{Z}_p^* \to \mathbb{Z}_q^*$, $H_2: \{0,1\}^* \times \{0,1\}^* \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$。

(2)密钥钥提取：首先 PKG 随机选择 $s \in \mathbb{Z}_p^*$，计算 $w = g^s \pmod p$，$d = s + xH_1(\mathrm{ID}, w)$，返回 $D_{\mathrm{ID}} = d$ 作为用户 ID 的部分私钥，$P_{\mathrm{ID}} = w$ 作为用户 ID 的部分公钥。然后用户 ID 随机选 $z \in \mathbb{Z}_q^*$ 作为秘密值，则用户的私钥 $\mathrm{SK}_{\mathrm{ID}} = (d, z)$，公钥 $\mathrm{PK}_{\mathrm{ID}} = (w, u)$。

(3)签名算法：输入消息 m，签名者 S 首先验证等式 $g^d = wy^{H_1(\mathrm{ID}, w)} \pmod p$ 是否成立，如果不成立，放弃签名，否则计算签名 $\sigma = dH_2(m, \mathrm{ID}, w) + z \pmod q$。

(4)验证算法：验证者接收到对消息 m 的无证书签名 σ 之后，计算 $h_1 = H_1(\mathrm{ID}, w)$，$h_2 = H_2(m, \mathrm{ID}, w)$，计算 g^σ 是否等于 $u(wy^{h_1})^{h_2}$，如果相等则输出“接受”，否则输出“拒绝”。

3.2 对上述方案的安全性分析

假设攻击者收到某签名者 S (其身份为 ID_S)的两个不同签名，不妨设 σ_1 是对消息 m_1 的签名，σ_2 是对消息 m_2 的签名且 $m_1 \neq m_2$，由

$$\sigma_1 = dH_2(m_1, \mathrm{ID}_s, w) + z \pmod q$$
$$\sigma_2 = dH_2(m_2, \mathrm{ID}_s, w) + z \pmod q$$

那么攻击者可以计算出该签名者 S 的完整私钥 $\mathrm{SK}_{\mathrm{ID}_S} = (d, z)$ 如下：

$$d = (\sigma_1 - \sigma_2)/(H_2(m_1, \mathrm{ID}_S, w) - H_2(m_2, \mathrm{ID}_S, w)) \cdot (\mathrm{mod}\, q)$$
$$z = \sigma_1 - ((\sigma_1 - \sigma_2)H_2(m_1, \mathrm{ID}_S, w) / (H_2(m_1, \mathrm{ID}_S, w) - H_2(m_2, \mathrm{ID}_S, w))) (\mathrm{mod}\, q)$$

进而攻击者就可以伪造用户 S 的任意签名。

4 满足强安全性的不含双线性对的无证书签名方案

本节将提出一种满足强安全性的不含双线性对

运算的无证书签名方案，方案是基于离散对数困难问题的，具体如下：

(1)系统建立：输入安全参数 k，PKG 产生两个大素数 p, q 且 $q \mid (p-1)$。随机选 $\mathbb{Z}_p^*$ 的一个阶为 q 的生成元 g，由 g 生成的子群记为 G。PKG 任意选主密钥 $x \in \mathbb{Z}_q^*$ 并计算 $y = g^x \pmod p$。选择 hash 函数: $H_1: \{0,1\}^* \times \mathbb{Z}_p^* \to \mathbb{Z}_q$, $H_2: \{0,1\}^* \times \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \mathbb{Z}_q$, $H_3: \{0,1\}^* \times \{0,1\}^* \times (\mathbb{Z}_p^*)^4 \times \mathbb{Z}_q^* \times \mathbb{Z}_p^* \to \mathbb{Z}_q$。系统公开参数 $\text{params} = \{p, q, g, G, y, H_1, H_2, H_3\}$，主密钥 $\text{msk} = x$。

(2)用户密钥提取：输入用户的身份 ID 后，PKG 首先随机选择 $s_0, s_1 \in \mathbb{Z}_q^*$，然后计算 $p_0 = g^{s_0} \pmod p$，$d_0 = s_0 + xH_1(\text{ID}, p_0) \pmod q$，$p_1 = g^{s_1} \pmod p$，$d_1 = s_1 + xH_2(\text{ID}, p_0, p_1) \pmod q$。PKG 返回用户 ID 的部分私钥 $D_{\text{ID}} = d_0$，用户的部分公钥 $P_{\text{ID}} = (p_0, p_1, d_1)$。用户随机选取 $z \in \mathbb{Z}_q^*$ 并输出 $s_{\text{ID}} = z$ 作为用户的秘密值。输出用户的私钥 $\text{SK}_{\text{ID}} = (D_{\text{ID}}, s_{\text{ID}}) = (d_0, z)$，用户的公钥 $\text{PK}_{\text{ID}} = (P_{\text{ID}}, \mu) = (p_0, p_1, d_1, g^z)$。

(3)签名算法：输入消息 m，签名者 S 完成如下签名：

(a)选择两个随机数 $r, r' \in \mathbb{Z}_q^*$，计算 $c = g^r \pmod p$，$c' = g^{r'} \pmod p$；

(b)令 $u = H_3(m, \text{ID}, c, c', \text{PK}_{\text{ID}})$；

(c)计算 $v = r - uz \pmod q$，$w = r' - ud_0 \pmod q$。

则签名者 S 对消息 m 的签名 $\sigma = (u, v, w)$。

(4)验证算法：给定系统参数 params，签名者的身份 ID 以及对应的公钥 $\text{PK}_{\text{ID}} = (p_0, p_1, d_1, \mu)$，验证者 V 收到对消息 m 的无证书签名 $\sigma = (u, v, w)$ 后，验证如下等式：

$$g^{d_1} = p_1 y^{H_2(\text{ID}, p_0, p_1)} \pmod p$$

$$u = H_3(m, \text{ID}, g^v \mu^u, g^w (p_0 y^{H_1(\text{ID}, p_0)})^u, \text{PK}_{\text{ID}})$$

如果上述两个等式都成立则输出“接受”，否则“拒绝”。

5　方案的安全性分析

方案的正确性显然成立，可以证明该无证书签名方案在攻击类型 Super Type I 和 Super Type II 下都满足存在性不可伪造，而在 Super Type II 攻击下的证明过程与 Super Type I 攻击下的证明类似，篇幅所限，本文只给出在 Super Type I 攻击下的完整证明。

设 A_{I} 是一个 Super Type I 攻击者，给定算法 B 一个离散对数难题实例 $(g, \beta = g^a)$，以下将演示算法 B 如何利用 A_{I} 来求解 a，进而解决离散对数问题。

B 首先运行系统建立算法产生系统参数 $\text{params} = \{p, q, g, G, y, H_1, H_2, H_3\}$，其中主公钥 $y = g^x$，B 返回 params 给 A_{I} 并保密主密钥 x。B 与 A_{I} 进行如下模拟算法：

(1)生成用户请求：假设 A_{I} 最多 q_{CU} 次用户生成请求，B 随机选择 $t \in [1, q_{CU}]$，记 $\text{ID}_t = \text{ID}^*$。对应 A_{I} 的第 i 次用户 ID_i 生成请求，如果 $i \neq t$，则 B 随机选择 $s_0, s_1, e_i, f_i, z_i \in \mathbb{Z}_q^*$，计算 $p_0 = g^{s_0} \pmod p$，$d_0 = s_0 + xe_i \pmod q$，$p_1 = g^{s_1} \pmod p$，$d_1 = s_1 + xf_i \pmod q$，并且 B 添加 $<(\text{ID}_i, p_0), e_i>$ 到列表 L_1（L_1 用来追踪对预言机 H_1 的询问），添加 $<(\text{ID}_i, p_0, p_1), f_i>$ 到列表 L_2（L_2 用来追踪对预言机 H_2 的询问）；如果 $i = t$（此时 $\text{ID}_i = \text{ID}^*$），$B$ 随机选择 $s_1, z_t, f_t \in \mathbb{Z}_q^*$，令 $p_0 = \beta (= g^a)$，$d_0 = "\perp"$，计算 $p_1 = g^{s_1} \pmod p$，$d_1 = s_1 + xf_t \pmod q$，并且 B 添加 $<(\text{ID}^*, p_0, p_1), f_t>$ 到列表 L_2。

最后 B 将 ID_i 密钥信息 $(\text{ID}_i, D_{\text{ID}_i} = (d_0)_{\text{ID}_i}, s_{\text{ID}_i} = z_i, \text{PK}_{\text{ID}_i} = (P_{\text{ID}_i}, \mu_{\text{ID}_i}) = ((p_0)_{\text{ID}_i}, (p_1)_{\text{ID}_i}, (d_1)_{\text{ID}_i}, g^{z_i})$ 添加到密钥列表 L 中。

(2)部分私钥提取询问：A_{I} 询问对应 ID_i 的部分私钥，如果 $\text{ID}_i = \text{ID}^*$，则 B 输出“failure”，模拟失败；否则 B 查表 L 并返回 ID_i 的部分私钥 $(d_0)_{\text{ID}_i}$ 给 A_{I}。

(3)秘密值询问：对应 ID_i 的秘密值，B 查表 L 并返回 s_{ID_i} 给 A_{I}。

(4)公钥替换请求：对 A_{I} 的公钥替换请求 $\{\text{ID}_i, \text{PK}'_{\text{ID}_i} = ((p'_0)_{\text{ID}_i}, (p'_1)_{\text{ID}_i}, (d'_1)_{\text{ID}_i}, \mu'_{\text{ID}_i}\}$，$B$ 首先检查 $g^{(d'_1)_{\text{ID}_i}} = (p'_1)_{\text{ID}_i} \cdot y^{H_2(\text{ID}_i, (p'_0)_{\text{ID}_i}, (p'_1)_{\text{ID}_i})}$，如果等式不成立则 B 拒绝替换；否则 B 将密钥列表 L 中 PK_{ID_i} 替换为 PK'_{ID_i}，注意到密钥列表 L 中对应 ID_i 的私钥未变化。

(5) H_i 询问（$i \in \{1, 2, 3\}$）：A_{I} 可以在任何时间访问随机预言机 H_i，首先 B 维持列表 L_i 来记录对预言机 H_i 的询问及应答。当 A_{I} 询问 H_i 时，如果表 L_i 已经存在该询问值则 B 返回相应的值，否则 B 选一随机数返回给 A_{I}，并且将其添加到相应的列表 L_i 中。

(6)Super-Sign 询问：假设 A_{I} 作出签名询问 (ID_i, m)，若 $\text{ID}_i \neq \text{ID}^*$ 且对应 ID_i 的公钥未被替换时，B 首先查表 L_i 获得相应 ID_i 的私钥 $\text{SK}_{\text{ID}_i} = (D_{\text{ID}_i} = d_0, s_{\text{ID}_i} = z)$，然后随机选择两个随机数 $r, r' \in \mathbb{Z}_q^*$ 并计算 $c = g^r \pmod p$，$c' = g^{r'} \pmod p$；B 随机选 $u \in_R \mathbb{Z}_q^*$ 并令 $u = H_3(m, \text{ID}_i, c, c', \text{PK}_{\text{ID}_i})$，添加 $<(m, \text{ID}_i, c, c', \text{PK}_{\text{ID}_i}), u>$ 到列表 L_3。B 计算 $v = r - uz \pmod q$，$w = r' - ud_0 \pmod q$，B 输出 $\sigma = (u, v, w)$ 作为用户 ID_i 对消息 m 的签名。

否则，若 $\text{ID}_i \neq \text{ID}^*$ 且对应 ID_i 的公钥被替换过

或者 $\mathrm{ID}_i=\mathrm{ID}^*$（$\mathrm{ID}^*$ 的公钥可能被替换过，也可能没有被替换)时，B 虽然未知 ID_i 的完整私钥，但是 B 仍然可以通过如下方法生成 ID_i 的有效签名：B 随机选择 $u,v,w\in\mathbb{Z}_q^*$ 作为用户 ID_i 对消息 m 的签名，并且令 $u=H_3(m,\mathrm{ID}_i,g^v\mu^u,g^w(p_0y^{H_1(\mathrm{ID}_i,p_0)})^u,\mathrm{PK}_{\mathrm{ID}_i})$，$B$ 将 $<(m,\mathrm{ID}_i,g^v\mu^u,g^w(p_0y^{H_1(\mathrm{ID}_i,p_0)})^u,\mathrm{PK}_{\mathrm{ID}_i}),u>$ 添加到列表 L_3。当 A_I 询问对应 H_3 输入为 $(m,\mathrm{ID}_i,g^v\mu^u,g^w(p_0y^{H_1(\mathrm{ID}_i,p_0)})^u,\mathrm{PK}_{\mathrm{ID}_i})$，$B$ 返回一个无碰撞的 u 作为 H_3 的输出并传送给 A_{I}。

模拟结束后，最终 A_{I} 以一个不可忽略的概率输出一有效的签名 $(\mathrm{ID},m,\sigma=(u,v,w))$，如果 $\mathrm{ID}\neq\mathrm{ID}^*$，则算法失败，$B$ 放弃。否则 B 通过充分利用无证书数字签名的一般化 Forking 引理[9]，将上述模拟过程重放两次,可得到两个有效的签名 $\sigma=(u,v,w)$，$\sigma'=(u',v',w')$ 其中 $u\neq u'$，并且有以下等式：$g^w(p_0y^{H_1(\mathrm{ID},p_0)})^u=g^{w'}(p_0y^{H_1(\mathrm{ID},p_0)})^{u'}$。

如果将上式左右两边以 g 为底数各取对数，那么 B 就可以计算出 $a=\log_g\beta=\log_g(p_0)=((w'-w)/(u-u'))-xH_1(\mathrm{ID},\beta)$，进而解决了离散对数问题。

接下来，我们分析 B 解决离散对数问题的成功概率。首先我们指出，A_{I} 利用新的公钥 (p_0',p_1',d_1',μ') 对用户公钥 (p_0,p_1,d_1,μ) 进行替换时，A_{I} 不可能找到另外的 $(p_0',p_1',d_1')\neq(p_0,p_1,d_1)$ 满足 $g^{d_1'}=(p_1')\cdot y^{H_2(\mathrm{ID}_i,p_0',p_1')}$，这是由 Schnorr 签名是存在性不可伪造的来保证的。否则根据文献[10]，已知另外的 (p_0',p_1',d_{11}') 满足 $g^{d_1'}=(p_1')\cdot y^{H_2(\mathrm{ID}_i,p_0',p_1')}$，$B$ 可以在多项式时间内以不可忽视的概率 $\varepsilon\geq 7Q/q$（Q 为 A_{I} 可以访问预言机 H_2 的次数)来解决离散对数问题。故以下的讨论只对公钥 μ 进行替换情况下，B 解决离散对数实例（g，$\beta=g^a$）的成功概率。

假设 A_{I} 在模拟仿真阶段至多进行了 q_{PPK} 次部分私钥提取询问，则 A_{I} 不询问对应 ID^*的部分私钥的概率至少为 $(1-(1/q_{CU}))^{q_{\mathrm{PPK}}}$。又 A_{I} 输出伪造签名 $(\mathrm{ID},m,\sigma=(u,v,w))$ 中 $\mathrm{ID}=\mathrm{ID}^*$ 的概率至少为 $(1/q_{CU})$，设 B 解决该离散对数实例求解 a 的概率为 Adv_B^{DL}，则有

$$\mathrm{Adv}_B^{DL}\geq\frac{1}{q_{CU}}(1-q_{CU})^{q_{\mathrm{PPK}}}\mathrm{Succ}_{A_{\mathrm{I}},\mathrm{super}}^{\mathrm{cma,cida}}$$

其中 $\mathrm{Succ}_{A_{\mathrm{I}},\mathrm{super}}^{\mathrm{cma,cida}}$ 为 A_{I} 在 Super Type I 适应性选择消息选择身份攻击类型下对本文的无证书签名方案的伪造攻击的成功概率。若 $\mathrm{Succ}_{A_{\mathrm{I}},\mathrm{super}}^{\mathrm{cma,cida}}$ 不可忽略，又 q_{CU}，$(1-q_{CU})^{q_{\mathrm{PPK}}}$ 均为常数，故 Adv_B^{DL} 也不可忽略。

6 总结

尽管人们在双线性映射的技术复杂性和如何提高其计算速度方面已做了大量工作，但是双线性对运算仍然是已知最复杂的密码操作。在同等安全级别下(椭圆曲线上 160 bit 的群元素等同于 1024 bit RSA 安全级别)，运行一次双线性对所需的时间约为有限域上指数运算的 10 倍左右[11]。本文提出的不需双线性对运算的无证书签名方案只需 9 个有限域上指数运算，与另外两个无证书签名方案相比(文献[3]需要 4 个双线性对运算，2 个有限域上指数运算，文献[4]需要 2 个双线性对运算，4 个椭圆曲线上的点乘运算)，本文方案虽然在公钥长度及签名长度等有所增加，但是在计算效率方面具有极大的优势。另外，本文方案的安全性基于文献[5]中最强的攻击类型：Super Type I 和 Super Type II 下仍然是存在性不可伪造的，具有更强的安全性。此外，利用本文思想也可以构造一个不含双线性对的无证书签密方案，这也是我们下一步的工作重点。

参 考 文 献

[1] Al-Riyami S S and Paterson K G. Certificateless public key cryptography [C]. ASIACRYPT 2003, LNCS 2894, Berlin: Springer-Verlag, 2003: 452–473.

[2] Barbosa M and Farshim P. Certificateless signcryption [C]. Proceedings of the 2008 ACM symposium on information, computer and communications security, Tokyo, Japan, 2008: 369–372.

[3] Raylin Tso, Xun Yi, and Huang Xin-yi. Efficient and short certificateless signature [C]. CANS 2008, LNCS 5339, Berlin: Springer-Verlag, 2008: 64–79.

[4] Zhang Lei and Zhang Fu-tai. Certificateless signature and blind signature [J]. *Journal of Electronics* (China), 2008, 25(5): 629–636.

[5] Huang Xin-yi, Mu Yi, and Susilo W, *et al*.. Certificateless signature revisited [C]. ACISP 2007, LNCS 4586, Berlin: Springer-Verlag, 2007: 308–322.

[6] 王会歌, 王彩芬, 李泳斌等. 没有 pairing 的无证书公钥签名方案 [J]. 计算机应用, 2008, 28(6): 1395–1397.
Wang H G, Wang C F, and Li Y B, *et al*.. Certificateless public key signature scheme without pairing [J]. *Computer Applications*, 2008, 28(6):1395–1397.

[7] Baek J, Safavi-Naini R, and Susilo W. Certificateless public key encryption without pairing [C]. ISC 2005, LNCS 3650, Berlin: Springer-Verlag, 2005: 134–148.

[8] Sun Yin-xia, Zhang Fu-tai, and Baek J. Strongly secure certificateless public key encryption without pairing [C]. CANS 2007, LNCS 4856, Berlin: Springer-Verlag, 2007: 194–208.

[9] Rafael C and Ricardo D. Two notes on the security of certificateless signature[C]. ProvSec 2007, LNCS 4784, Berlin: Springer-Verlag, 2007: 85–102.

[10] Pointcheval D and Stern J. Security arguments for digital signatures and blind signatures [J]. *Journal of Cryptology*, 2000, 13(3): 361–396.

[11] Miracl. Multiprecision integer and rational arithmetic C/C++library, http://indigo. ie/mscott/.

葛爱军： 男，1985 年生，硕士生，研究方向为数字签名、信息安全.

陈少真： 女，1967 年生，博士，副教授，硕士生导师，研究方向为密码学、信息安全.