可证安全的无证书部分盲签名机制

赵振国

(华北水利水电大学水利学院 郑州 450045)

【摘要】针对现有无证书部分盲签名机制计算复杂度过高的问题，该文设计了一种高效的无证书部分盲签名机制。首先，分析了一个无证书部分盲签名机制的安全性；其次，利用椭圆曲线密码构造一种新的无证书部分盲签名机制；最后，在随机预言模型下证明提出的无证书部分盲签名机制是安全的。分析表明，提出的无证书部分盲签名机制不仅能解决以往机制中存在的安全性缺陷，而且具有更好的性能。

关 键 词 双线性对； 无证书； 部分盲签名； 随机预言模型

中图分类号 TP393.08 **文献标志码** A doi:10.3969/j.issn.1001-0548.2016.05.018

Certificateless Partially-Blind Signature Scheme with Provable Security

ZHAO Zhen-guo

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

Abstract The high computation costs are required in existing certificateless partially-blind signature (CLPBS) schemes. In this paper, we first analyze the security of Shao *et al*.'s CLPBS scheme and then present a new CLPBS scheme based on the elliptic curve cryptography (ECC). The security analysis indicates that the proposed CLPBS scheme is provably secure in the random oracle model. Detailed analysis shows that the proposed CLPBS scheme not only addresses security weaknesses with previous schemes, but also has better performance.

Key words bilinear pairing; certificateless; partially-blind signatures; random oracle model

盲数字签名的概念是由文献[1]提出的，在这种机制中签名者并不知道他所签发消息的具体内容，也不能把签名过程和最终的签名对应起来。因此，盲数字签名可以很好的保护用户隐私，在电子支付、电子投票等领域得到广泛应用。在全盲数字签名中，签名者不知道最终签名的任何信息，这可能导致签名被恶意用户非法使用。为了解决该问题，文献[2]提出了部分盲数字签名的概念。这种机制产生的签名中嵌入了用户和签名者协商好的公共信息，可以很好地解决签名被非法使用的问题。

为了解决传统公钥密码机制中的证书问题，文献[3]提出了基于身份的公钥密码。在公钥密码中，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。在这种机制中，用户的私钥是由私钥生成中心(key generation center, KGC)通过用户的身份来生成的。因此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。为了解决基于身份的公钥密码的密钥托管问题，文献[4]提出了无证书公钥密码机制。自此，科研人员提出了许多无证书密钥协商机制[5-7]和加密机制[8-9]。无证书部分盲签名作为一种非常重要的密码机制得到了广泛关注和研究。文献[10]提出了第一个无证书部分盲签名机制。为改进性能，文献[11-13]分别提出了一种改进的无证书部分盲签名机制。然而，上述无证书部分盲签名机制都需要双线性对运算。理论分析[14]和实验结果[15]表明：在相同安全性的条件下，执行一次双线性对操作的时间至少是椭圆曲线上点乘运算的十余倍。因此，不用双线性对运算的部分盲签名机制具有更好的性能。文献[16]提出了一个无需双线性对运算的无证书部分盲签名机制，同时在随机预言模型下证明了其安全性。

本文将文献[16]中的机制进行安全性分析。通过具体的攻击来证明他们的部分盲签名机制不能提供

收稿日期：2014 – 04 – 18；修回日期：2015 – 09 – 10
基金项目："十二五"国家科技支撑计划(2011BAD25B01)；河南省教育厅科学技术重点研究项目(13A570704)
作者简介：赵振国(1978 –)，男，博士，主要从事大型灌区水资源优化调配软硬件和智慧水利等方面的研究.

不可伪造性。因此，该机制并不能满足应用的需求。为了克服安全缺陷，本文提出了一种新的无证书部分盲签名机制，并在随机预言模型下证明其安全性。

1　有关数学难题及其假设

设 p 和 q 是两大素数。$E(F_p)$ 是定义在有限域 F_p 上的椭圆曲线，G 是由 $E(F_p)$ 上的点构成的阶为 n 的加法群。设 P 是群 G 的基点，定义在椭圆曲线上的离散对数如下所述。

离散对数(discrete logarithm, DL)问题：对于给定 G 中的一个元素 aP，计算 $a\in Z_q^*$，其中a是一个未知的元素。

设 A 是一个多项式算法，定义它解决DL问题的优势为：

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

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

2　形式化安全定义

无证书部分盲签名机制由4个算法组成[16]：系统建立算法、密钥产生算法、签名发布算法和签名验证算法。其中，签名发布算法又包括签名、盲化和去盲3个子算法：

1) 系统建立算法：输入安全参数，输出系统参数和密钥生成中心的主私钥 x。

2) 密钥产生算法：输入系统参数，用户身份 ID_i，KGC生成用户的部分私钥 y_i 和部分公钥 Y_i，用户选择私有秘密 x_i 并生成私钥 S_i 和公钥 P_i。

3) 签名发布算法：输入系统参数，签名者私钥 S_i 和消息 m，签名者和请求者进行交互，依次完成签名、盲化和去盲3个子算法。最后，生成消息的签名 σ。

4) 签名验证算法：输入系统参数、消息 m、签名者身份 ID_i、签名者公钥 P_i 和签名 σ，用户通过该算法验证签名的合法性。

部分盲签名机制的部分盲性是指签名者不能把最终的签名结果和签名实例对应起来。在攻击者 A 的攻击下，部分盲性的形式化定义如下：

1) 挑战者 C 执行系统参数建立算法，生成系统参数和主私钥，并把系统参数返回给攻击者。

2) 挑战者 C 选择随机数 $b\in\{0,1\}$，然后让 A 对消息 (m_b,c) 进行部分盲签名，其中 c 是 C 和 A 之间的协商信息。C 执行去盲操作并把 (m_b,c) 的最终签名发送给 A。

3) A 输出对 b 的猜测 b'。

如果 $b'=b$，则称 A 赢得上述游戏。定义 A 赢得上述游戏的优势为 $\mathrm{Adv}(A)=|2\Pr[b=b']-1|$。

定义 1　无证书部分盲签名机制的部分盲性

如果不存在攻击者 A 能够在概率多项式时间内以不可忽略的优势赢得上述游戏，则称无证书部分盲签名机制满足部分盲性。

在攻击者 $A\in\{A1,A2\}$ 的攻击下，在概率多项式时间内，如果攻击者没有不可忽略的优势在此游戏中获胜，则称无证书部分盲签名机制在适应性选择消息攻击下具有不可伪造性。

在无证书部分盲签名机制的不可伪造安全中，有两种类型的攻击者：类型I攻击者($A1$)和类型II攻击者($A2$)。$A1$ 不知道KGC的主私钥，但他可以使用任意值替换用户的公钥。$A2$ 不能替换用户的公钥，但是他可以获取KGC的主私钥。对于一个攻击者 $A\in\{A1,A2\}$ 来说，他可以进行以下查询：

Hash查询：输入任意消息 M，挑战者 C 把 M 的哈希值返回给 A。

部分密钥查询：输入用户的身份 ID_i，挑战者 C 把对应的部分密钥返回给 A。

私有秘密查询：输入用户的身份 ID_i，挑战者 C 把对应的私有秘密返回给 A。

公钥查询：输入用户的身份 ID_i，挑战者 C 把对应的公钥返回给 A。

公钥替换查询：输入用户的身份 ID_i 和一个新公钥，挑战者 C 利用新公钥替换用户原来的公钥。

签名发布查询：输入消息 m、签名者身份，挑战者 C 生成签名 σ，并把 σ 返回给 A。

在攻击者 $A\in\{A1,A2\}$ 的攻击下，签名机制的不可伪造性定义如下：

1) 挑战者 C 执行系统参数建立算法，生成系统参数和主私钥。C 把系统参数返回给攻击者 A，如果 A 是类型II攻击者，C 把主私钥也返回给 A。

2) 查询阶段，A 执行Hash查询、部分密钥查询、私钥查询、公钥查询、用户公钥替换查询、部分盲签名查询和解密验证查询。如果 A 是类型II攻击者，则 A 能进行用户公钥替换查询。

3) A 在用户身份 ID_i^* 下输入 σ^* 签名。

称 A 赢得此游戏，当且仅当以下条件成立。

1) σ^* 是一个合法的签名。

2) 如果 A 是类型I攻击者，则 A 不能对 ID_i^* 进行过部分密钥查询和私钥查询; 如果 A 是类型II攻击者，则 A 不能对 ID_i^* 进行过私钥查询。

定义 2 无证书部分盲签名机制的不可伪造性

如果不存在攻击者 A 能够在概率多项式时间内以不可忽略的优势赢得上述游戏，则称无证书部分盲签名机制在适应性选择消息攻击下具有不可伪造性。

3 文献[16]中的机制

文献[16]中的无证书盲签名机制分为以下4个步骤：

1) 系统建立算法

输入安全参数 k，KGC产生两大素数 p 和 q 和定义在有限域 F_p 上的椭圆曲线 $E(F_p)$。设 G 是由 $E(F_p)$ 上的点组成的阶为 q 的加法群。KGC选择 G 的一个基点 P 和3个安全Hash函数：$H_1:\{0,1\}^*\times G\to Z_q^*$，$H_2:\{0,1\}^*\times\{0,1\}^*\times G\to Z_q^*$，$H_3:\{0,1\}^*\to Z_q^*$。KGC随机选择主密钥 $s\in Z_q^*$，计算 $P_{\text{pub}}=sP$，公开系统参数 $(p,q,E(F_p),G,P,P_{\text{pub}},H_1,H_2,H_3)$，保密主密钥 s。

2) 密钥产生算法

签名者 i 把他的身份提交给KGC。收到后KGC生成随机数 $y_i\in Z_q^*$，计算 $Y_i=y_iP$、$q_i=H_1(\text{ID}_i,Y_i)$ 和 $d_i=y_i+sq_i$，并把部分私钥 d_i 和部分公钥 Y_i 返回给 i。收到 d_i 和 Y_i 后，i 生成随机数 $x_i\in Z_q^*$ 作为他的私有秘密，计算 $X_i=x_iP$，输出私钥 $S_i=(x_i,d_i)$ 和公钥 $P_i=(X_i,Y_i)$。

3) 签名发布算法

在该算法中，用户和签名者通过执行交互协议来生成消息 m 的部分盲签名，其中 c 是双方共同协商的说明消息。用户和签名者之间的交互协议如下所述。

签名(阶段1)：签名者 i 生成随机数，计算 $R=rP$ 并把 R 发送给用户。

盲化：用户生成两个随机数 $\alpha,\beta\in Z_q^*$，计算 $z=H_3(c)$、$L=\alpha R+\alpha\beta zP$、$h=H_2(m,c,L)$ 和 $u=\alpha^{-1}h+\beta z$，最后把 u 发送给签名者 i。

签名(阶段2)：签名者 i 计算 $z=H_3(c)$、$v=(r+u)/(x_i+d_i+z)$，并把 v 发送给用户。

去盲：用户计算 $w=\alpha v$，输出对消息 (m,c) 的部分盲签名 (L,w)。

4) 签名验证算法

收到对消息 (m,c) 的部分盲签名 (L,w) 后，验证者计算 $q_i=H_1(\text{ID}_i,Y_i)$ 和 $h=H_2(m,c,L)$，并验证等式 $L+hP=w(X_i+Y_i+q_iP_{\text{pub}}+zP)$ 是否成立。如果等式成立，验证者接受签名，否则拒绝签名。

4 文献[16]中机制的安全性分析

文献[16]在随机预言模型下证明所提出的机制是安全的。本文将通过具体的攻击来证明他们的机制不能满足类型Ⅰ攻击者攻击下的不可伪造性。设 i 为签名者，则他的私钥和公钥分别为 $S_i=(x_i,d_i)$ 和 $P_i=(X_i,Y_i)$，其中，$Y_i=y_iP$，$q_i=H_1(\text{ID}_i,Y_i)$，$d_i=y_i+sq_i$，$X_i=x_iP$。

设 $A1$ 是类型Ⅰ的攻击者，则 $A1$ 不知道系统主密钥，但可以随时查询用户公钥或替换合法用户的公钥。$A1$ 可以通过以下4个步骤伪造签名者 i 的签名：

1) $A1$ 生成随机数 $t_i\in Z_q^*$，计算 $z=H_3(c)$ 和 $X_i'=t_iP-(Y_i+q_iP_{\text{pub}}+zP)$。

2) $A1$ 利用 $P_i'=(X_i',Y_i)$ 替换签名者 i 的公钥 $P_i=(X_i,Y_i)$。

3) $A1$ 生成随机数 $l_i\in Z_q^*$，计算 $L=l_iP$、$h=H_2(m,c,L)$ 和 $w=(l_i+h)t_i^{-1}$。

4) $A1$ 输出 (L,w) 作为对消息 (m,c) 的部分盲签名。

因为，$L=l_iP$，$w=(l_i+h)t_i^{-1}$，可以得到：

$$\begin{aligned}&w(X_i'+Y_i+q_iP_{\text{pub}}+zP)=\\&(l_i+h)t_i^{-1}(t_iP-(Y_i+q_iP_{pub}+zP)+\\&Y_i+q_iP_{\text{pub}}+zP)=(l_i+h)t_i^{-1}t_iP=\\&(l_i+h)P=L+hP\end{aligned}\tag{1}$$

因此有 $w(X_i'+Y_i+q_iP_{\text{pub}}+zP)$ 和 $L+hP$ 相等，于是 $A1$ 伪造的签名 (L,w) 可以通过验证者的验证。因此 $A1$ 成功地伪造了一个合法签名。综上所述，文献[16]中的部分盲签名机制不能满足类型Ⅰ攻击者攻击下的不可伪造性。

5 新的无证书部分盲签名机制

新的无证书部分盲签名机制分为以下4个步骤：

1) 系统建立算法

输入安全参数 k，KGC产生两大素数 p 和 q 和定义在有限域 F_p 上的椭圆曲线 $E(F_p)$。设 G 是由 $E(F_p)$ 上的点组成的阶为 q 的加法群。KGC选择 G 的一个基点 P 和3个安全Hash函数：$H_1:\{0,1\}^*\times G\to Z_q^*$，$H_2:\{0,1\}^*\times\{0,1\}^*\times G\to Z_q^*$，$H_3:\{0,1\}^*\times\{0,1\}^*\times G\times G\times G\to Z_q^*$。KGC 随机选择主密钥 $s\in Z_q^*$，计算 $P_{\text{pub}}=sP$，公开系统参数 $(p,q,$

$E(F_p),G,P,P_{\text{pub}},H_1,H_2,H_3$)，保密主密钥 s。

2) 密钥产生算法

签名者 i 把他的身份 ID_i 提交给KGC。收到 ID_i 后，KGC生成随机数 $y_i\in Z_q^*$，计算 $Y_i=y_iP$、$q_i=H_1(\text{ID}_i,Y_i)$ 和 $d_i=y_i+sq_i$，并把部分私钥 d_i 和部分公钥 Y_i 返回给 i。收到 d_i 和 Y_i 后，i 生成随机数 $x_i\in Z_q^*$ 作为他的私有秘密，计算 $X_i=x_iP$，输出私钥 $S_i=(x_i,d_i)$ 和公钥 $P_i=(X_i,Y_i)$。

3) 签名发布算法

在该算法中，用户和签名者通过执行交互协议来生成消息 m 的部分盲签名，其中 c 是双方共同协商的说明消息。用户和签名者之间的交互协议如下所述。

签名(阶段1)：签名者 i 生成随机数 $r\in Z_q^*$，计算 $R=rP$ 并把 R 发送给用户。

盲化：用户生成两个随机数 $\alpha,\beta\in Z_q^*$，计算 $L=\alpha P+\beta R$，$h=H_2(m,c,L)$ 和 $u=h\beta^{-1}$，最后把 u 发送给签名者 i。

签名(阶段2)：签名者计算 $k_i=H_3(c,\text{ID}_i,X_i,Y_i,P_{\text{pub}})$、$v=r-u(k_ix_i+d_i)$，并把 v 发送给用户。

去盲：用户计算 $w=\beta v+\alpha$，输出对消息 (m,c) 的部分盲签名 (h,w)。

4) 签名验证算法

收到对消息 (m,c) 的部分盲签名 (h,w) 后，验证者计算 $q_i=H_1(\text{ID}_i,Y_i)$、$k_i=H_3(c,\text{ID}_i,X_i,Y_i,P_{\text{pub}})$ 和 $T=h(k_iX_i+Y_i+q_iP_{\text{pub}})+wP$，并验证等式 $h=H_2(m,c,T)$ 是否成立。若成立则验证者接受签名，否则拒绝签名。

因为 $L=\alpha P+\beta R$，$h=H_2(m,c,L)$，$u=h\beta^{-1}$，$v=r-u(k_ix_i+d_i)$，$w=\beta v+\alpha$，因此可以得到：

$$T=h(k_iX_i+Y_i+q_iP_{\text{pub}})+wP=$$
$$h(k_iX_i+Y_i+q_iP_{\text{pub}})+(\beta v+\alpha)P=$$
$$h(k_iX_i+Y_i+q_iP_{\text{pub}})=h(k_iX_i+Y_i+q_iP_{\text{pub}})+\beta R-$$
$$h(k_iX_i+Y_i+q_iP_{\text{pub}})+\alpha P=\beta R+\alpha P=L \quad (2)$$
$$h=H_2(m,c,Q)=H_2(m,c,T) \quad (3)$$

因此，本文的签名机制是正确的。

6　安全性证明

定理　1　本文提出的部分盲签名机制满足部分盲性。

证明：在本文的机制中使用了两个盲化因子 $\alpha,\beta\in Z_q^*$，并且这两个盲化因子是随机生成的。另外用户只把盲化后的消息 u 发给了签名者。因为 H_2 是一个安全的哈希函数，因此签名者不能从哈希值 $h=H_2(m,c,L)$ 中恢复消息 m。如果签名 (h,w) 是一个有效的签名，由 $u=h\beta^{-1}$，$w=\beta v+\alpha$，$L=\alpha P+\beta R$ 可以得出存在唯一的 $\beta=hu^{-1}$ 和唯一的 $\alpha=w-hu^{-1}v$ 使得式(2)和式(3)成立。因此，盲化因子 $\alpha,\beta\in Z_q^*$ 在部分盲签名的生成中总是存在的。在定义1涉及的游戏中，由于盲化因子 α 和 β 的存在，攻击者赢得游戏的优势是可以忽略的。因此本文提出的部分盲签名机制满足部分盲性。

定理　2　在适应性选择消息攻击下，改进的无证书部分盲签名机制具有不可伪造性。

上述定理可以由以下两个引理推出。

引理　1　在随机预言模型下，如果存在第Ⅰ类攻击者 $A1$ 能够以不可忽略的概率 ε 伪造出合法的部分盲签名，则存在挑战者 C 能够以不可忽略的概率解决DL问题。

证明：给定DL问题实例 (P,Q)，C 的目的是利用 $A1$ 计算出 $a\in Z_q^*$ 使得 $Q=aP$。首先，C 产生系统参数 $(p,q,E(F_p),G,P,P_{\text{pub}},H_1,H_2,H_3)$，并把它返回给 $A1$，其中 $P_{\text{pub}}=Q$。随后，C 随机选择 ID_I 作为挑战身份，其中 $1\leqslant I\leqslant q_{H_1}$。$q_{H_1}$ 是 $A1$ 进行 H_1 查询的次数。C 按照如下方式回答 $A1$ 的查询。

H1查询：C 维护格式为 (ID_i,Y_i,h_i) 的列表 L_1。收到 $A1$ 对消息 (ID_i,Y_i) 的查询后，C 首次查询 (ID_i,Y_i,h_i) 是否在 L_1 中。如果在 L_1 中，C 把 h_i 返回给 $A1$。否则，C 生成随机数 $h_i\in Z_q^*$，把 (ID_i,Y_i,h_i) 插入到 L_1 中并返回 h_i。

H2查询：C 维护格式为 (m,c,L,h) 的列表 L_2。收到 $A1$ 对消息 (m,c,L,h) 的查询后，C 首次查询在 L_2 中是否存在 (m,c,L,h)。若存在，C 把 h 返回给 $A1$。否则，C 生成随机数 $h\in Z_q^*$，把 (m,c,L,h) 插入到 L_2 中并返回 h。

H3查询：C 维护格式为 $(c,\text{ID}_i,X_i,Y_i,P_{\text{pub}},h)$ 的列表 L_3。收到 $A1$ 对消息 $(c,\text{ID}_i,X_i,Y_i,P_{\text{pub}})$ 的查询后，C 首次查询在 L_3 中 $(c,\text{ID}_i,X_i,Y_i,P_{\text{pub}},h)$ 是否存在。若存在，C 把 h 返回给 $A1$。否则，C 生成随机数 $h\in Z_q^*$，把 $(c,\text{ID}_i,X_i,Y_i,P_{\text{pub}},h)$ 插入到 L_3 中并返回 h。

部分密钥查询：C 维护格式为 (ID_i,d_i,Y_i) 的列表 L_{par}。如果 $\text{ID}_i=\text{ID}_I$，则 C 退出仿真(事件 E_1)，否则 C 查询 (ID_i,d_i,Y_i) 是否在 L_{par} 中。若存在，C 把 d_i 返

回给 $A1$。否则 C 生成两个随机数 $d_i,q_i\in Z_q^*$，计算 $Y_i=d_iP-q_iQ$，把 (ID_i,d_i,Y_i) 和 (ID_i,Y_i,q_i) 分别加入到 L_{par} 和 L_1 中。最后，C 返回 d_i 和 Y_i。

私有秘密查询：C维护格式为 (ID_i,d_i,x_i) 的列表 L_{pri}。C 查询 (ID_i,d_i,x_i) 是否在 L_{pri} 中。若存在，$\mathfrak{C}$ 把 x_i 返回给 $A1$。否则，C 进行部分密钥提取查询得到 d_i，生成随机数 $x_i\in Z_q^*$，把 (ID_i,d_i,x_i) 加入到 L_{pri} 中并返回 x_i。

公钥查询：C 维护格式为 (ID_i,X_i,Y_i) 的列表 L_{pub}。收到 $A1$ 对用户身份 ID_i 的查询后，C 首次查询 (ID_i,X_i,Y_i) 是否在 L_{pub} 中。若存在，C 把 $\mathrm{PK}_i=(X_i,Y_i)$ 返回给 $A1$。否则 C 查询 L_{par} 和 L_{pri}，计算 $X_i=x_iP$，并返回 $\mathrm{PK}_i=(X_i,Y_i)$。若 L_{par} 和 L_{pri} 中不存在相应的记录，且 $\mathrm{ID}_i\neq\mathrm{ID}_I$，$C$ 生成3个随机数 $d_i,h_i,x_i\in Z_q^*$，计算 $X_i=x_iP$，$Y_i=d_iP-h_iQ$，把 (ID_i,d_i,x_i)、(ID_i,d_i,Y_i)、(ID_i,X_i,Y_i) 和 (ID_i,Y_i,h_i) 分别加入到 L_{pri}、L_{par}、L_{pub} 和 L_1 中，并返回 $\mathrm{PK}_i=(X_i,Y_i)$；否则（$\mathrm{ID}_i=\mathrm{ID}_I$）$\mathfrak{C}$ 生成3个随机数 $h_i,x_i,y_i\in Z_q^*$，计算 $X_i=x_iP$，$Y_i=y_iP$，把 $(\mathrm{ID}_i,\perp,x_i)$、$(\mathrm{ID}_i,\perp,Y_i)$、$(\mathrm{ID}_i,X_i,Y_i)$ 和 (ID_i,Y_i,h_i) 分别加入到 L_{pri}、L_{par}、L_{pub} 和 L_1 中，并返回 $\mathrm{PK}_i=(X_i,Y_i)$。

公钥替换查询：收到 $\mathscr{A}1$ 对消息 $(\mathrm{ID}_i,X_i'=x_i'P,Y_i'=y_i'P)$ 的查询后，C 首先查询 (X_i,Y_i) 是否在 L_{pub} 中。若不存在，C 首先执行公钥提取查询。最后，C 利用 X_i' 和 Y_i' 分别替换 X_i 和 Y_i。

签名发布查询：收到 $A1$ 对消息 (ID_i,c,m) 的查询后，C 产生随机数 $h,w\in Z_q^*$，计算 $q_i=H_1(\mathrm{ID}_i,Y_i)$、$k_i=H_3(c,\mathrm{ID}_i,X_i,Y_i,P_{\mathrm{pub}})$ 和 $T=h(k_iX_i+Y_i+q_iP_{\mathrm{pub}})+wP$。$C$ 把 (m,c,T,h) 添加到 L_2 中并输出 (h,w)。

经过有界次查询后，$A1$ 以不可忽略的概率 ε 输出一个对消息 (ID^*,c,m) 的签名 (h_1,w_1)。如果 $\mathrm{ID}^*\neq\mathrm{ID}_I$，则 C 停止仿真(事件 E_2)；否则同时改变 H_1、H_2 和 H_3，由分叉引理可知 $\mathscr{A}1$ 可以在多项式概率事件内生成另外3个有效的签名 (h_2,w_2)、(h_3,w_3) 和 (h_4,w_4)。则可以得到：

$$T=h_j(k_I^jX_I+Y_I+q_I^jP_{\mathrm{pub}})+w_jP\quad j=1,2,3,4 \tag{4}$$

设 $T=tP$，$X_I=x_IP$，$Y_I=y_IP$，则由上述等式可以得到：

$$t=h_j(k_I^jx_I+y_I+q_I^ja)+w_j \bmod q \tag{5}$$

上述方程中有4个未知数，且相互线性独立，因此联立4个方程即可得到 a 的值，即 C 可以解决DL问题。

下面对 C 成功的概率进行分析。从上述模拟过程可以看出，只要 E_1 和 E_2 没有发生，则 C 即可解决DL问题。令 q_{ppk} 表示 $A1$ 进行部分私钥查询的次数。从上述模拟过程可知 $\Pr[\overline{E_1}]\geqslant(1-\frac{1}{q_{H_1}})^{q_{\mathrm{ppk}}}$，$\Pr[A1\text{成功}|\overline{E_1}]\geqslant\varepsilon$，$\Pr[\overline{E_2}|A1\text{成功}\wedge\overline{E_1}]\geqslant\frac{1}{q_{H_1}}$。因此可以得到 C 成功的概率为：

$$\varepsilon'=\Pr[\overline{E_1}\wedge A1\text{成功}\wedge\overline{E_2}]=$$
$$\Pr[\overline{E_1}]\Pr[A1\text{成功}|\overline{E_1}]\Pr[\overline{E_2}\,|\,A1\text{成功}\wedge\overline{E_1}]\geqslant$$
$$\frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{\mathrm{ppk}}}\varepsilon$$

引理 2 在随机预言模型下，如果存在第Ⅰ类攻击者 $A2$ 能够以不可忽略的概率 ε 伪造出合法的部分盲签名，则存在挑战者 C 能够以不可忽略的概率解决DL问题。

证明：给定DL问题实例 (P,Q)，C 的目的是利用 $A2$ 是计算出 $a\in Z_q^*$ 使得 $Q=aP$。首先 C 生成随机数 $s\in Z_q^*$，产生系统参数 $(p,q,E(F_p),G,P,P_{\mathrm{pub}}=sP,H_1,H_2,H_3)$，并把主密钥 s 和系统参数返回给 $A2$。随后，C 随机选择 ID_I 作为挑战身份，其中 $1\leqslant I\leqslant q_{H_1}$，$q_{H_1}$ 是 $A2$ 进行 H_1 查询的次数。C 按照引理1中的方式对H1查询、H2查询、H3查询和签名发布查询进行回答。对于其它查询的回答如下所示。

部分密钥查询：C 维护格式为 (ID_i,d_i,Y_i) 的列表 L_{par}。C 查询 (ID_i,d_i,Y_i) 是否在 L_{par} 中。若存在，C 把 d_i 返回给 $A2$。否则 C 生成两个随机数 $y_i,q_i\in Z_q^*$，计算 $Y_i=y_iP$，$d_i=y_i+sq_i$，把 (ID_i,d_i,Y_i) 和 (ID_i,Y_i,q_i) 分别加入到 L_{par} 和 L_1 中。最后，C 返回 d_i 和 Y_i。

私有秘密查询：C 维护格式为 (ID_i,d_i,x_i) 的列表 L_{pri}。如果 $\mathrm{ID}_i=\mathrm{ID}_I$，则 C 退出仿真(事件 E_1)，否则 C 查询 (ID_i,d_i,x_i) 是否在 L_{pri} 中。若存在，C 把 x_i 返回给 $A2$。否则 C 进行部分密钥提取查询得到 d_i，生成随机数 $x_i\in Z_q^*$，把 (ID_i,d_i,x_i) 加入到 L_{pri} 中并返回 x_i。

公钥查询：C 维护格式为 (ID_i,X_i,Y_i) 的列表 L_{pub}。收到 $A2$ 对用户身份 ID_i 的查询后，C 首次查询 (ID_i,X_i,Y_i) 是否在 L_{pub} 中。若存在，C 把 $\mathrm{PK}_i=(X_i,Y_i)$ 返回给 $A2$。否则 C 查询 L_{par} 和 L_{pri}，计算 $X_i=x_iP$，并返回 $\mathrm{PK}_i=(X_i,Y_i)$。若 L_{par} 和 L_{pri} 中

不存在相应的记录，且 $\mathrm{ID}_i \neq \mathrm{ID}_I$，$C$ 生成3个随机数 $q_i, x_i, y_i \in Z_q^*$，计算 $X_i = x_i P$，$Y_i = y_i P$，$d_i = y_i + sq_i$，把 $(\mathrm{ID}_i, d_i, x_i)$、$(\mathrm{ID}_i, d_i, Y_i)$、$(\mathrm{ID}_i, X_i, Y_i)$ 和 $(\mathrm{ID}_i, Y_i, q_i)$ 分别加入到 L_{pri}、L_{par}、L_{pub} 和 L_1 中，并返回 $\mathrm{PK}_i = (X_i, Y_i)$；否则 $\mathrm{ID}_i = \mathrm{ID}_I$，$C$ 生成两个随机数 $q_i, y_i \in Z_q^*$，计算 $X_i = Q$，$Y_i = y_i P$，$d_i = y_i + sq_i$，把 $(\mathrm{ID}_i, d_i, \perp)$、$(\mathrm{ID}_i, d_i, Y_i)$、$(\mathrm{ID}_i, X_i, Y_i)$ 和 $(\mathrm{ID}_i, Y_i, q_i)$ 分别加入到 L_{pri}、L_{par}、L_{pub} 和 L_1 中，并返回 $\mathrm{PK}_i = (X_i, Y_i)$。

经过有界次查询后，$A2$ 以不可忽略的概率 ε 输出一个对消息 (ID^*, c, m) 的签名 (h_1, w_1)。如果 $\mathrm{ID}^* \neq \mathrm{ID}_I$，则 C 停止仿真(事件 E_2)；否则同时改变 H_1、H_2 和 H_3，由分叉引理可知 $A2$ 可以在多项式概率事件内生成另外一个有效的签名 (h_2, w_2)。则可以得到：

$$T = h_j(k_I X_I + Y_I + q_I P_{\mathrm{pub}}) + w_j P \quad j = 1, 2 \tag{6}$$

设 $T = tP$，则由式(16)可以得到：

$$t = h_j(k_I^j a + y_I + q_I^j s) + w_j \bmod q \tag{7}$$

上述方程中有两个未知数 t 和 a，且相互线性独立，因此联立两个方程即可得到 a 的值，即 C 可以解决DL问题。

下面对 C 成功的概率进行分析。从上述模拟过程可以看出，只要 E_1 和 E_2 没有发生，则 C 即可解决DL问题。令 q_{sv} 表示 $A2$ 进行私有秘密查询的次数。从上述模拟过程可知 $\Pr[\overline{E_1}] \geqslant (1 - \frac{1}{q_{H_1}})^{q_{\mathrm{sv}}}$，$\Pr[A2\text{成功} \mid \overline{E_1}] \geqslant \varepsilon$，$\Pr[\overline{E_2} \mid A2\text{成功} \wedge \overline{E_1}] \geqslant \frac{1}{q_{H_1}}$。因此可以得到 C 成功的概率为：

$$\varepsilon' = \Pr[\overline{E_1} \wedge A2\text{成功} \wedge \overline{E_2}] \geqslant \frac{1}{q_{H_1}}(1 - \frac{1}{q_{H_1}})^{q_{\mathrm{sv}}} \varepsilon$$

7　性能比较

本节把新的无证书部分盲签名机制同文献[16]中的部分盲签名机制进行比较。这里 T_s、T_a 和 T_h 分别表示椭圆曲线点乘、椭圆曲线点加和哈希函数的计算开销。文献[18]在Intel I7-4770协处理器上实现了椭圆曲线密码所需要的各种运算，其中操作系统是Windows 7，时钟频率为3.40 GHz，内存为4 GB。根据实现结果可知：T_s=0.442 ms，T_a=0.001 8 ms，T_h=0.000 1 ms。

表1比较了本文的机制和文献[16]中机制的性能。可看出：执行一次本文的机制的签名算法和文献[16]的机制的签名算法都需要1.328 1 ms；执行一次本文的机制的验证算法需要1.773 6ms；执行一次本文的机制的验证算法需要1.775 5 ms，与文献[16]的机制相比，本文提出的机制具有更好的性能。另外文献[16]的机制不能抵抗第Ⅰ类攻击者的攻击。因此，本文的机制更适合应用的需要。

表1　性能比较

	签名/ms	验证/ms
文献[16]	$3T_s + T_a + 3T_h \approx 1.328\ 1$	$4T_s + 4T_a + 3T_h \approx 1.775\ 5$
本文算法	$3T_s + T_a + 3T_h \approx 1.328\ 1$	$4T_s + 3T_a + 2T_h \approx 1.773\ 6$

8　结束语

文献[16]提出了一个高效的无证书部分盲签名机制，并且在随机预言模型下证明了其安全性。本文通过构造具体的攻击方法来表明他们的机制不能满足保密性和不可伪造性。这些分析表明，文献[16]的机制不能够满足现实应用的需要。同时，本文给出了一个改进的无证书认证机制，并在随机预言模型下证明了它的安全性。

参考文献

[1] CHAUM D. Bind signature for untraceable payments[C]// Advances in Cryptology-Crypto'82. NewYork: Springer-Verlag, 1982: 199-203.

[2] ABE M, FUJISAKI E. How to date blind signatures[C]// Advances in Cryptology-Asiacrypt'96. Kyongju: Springer-Verlag, 1996: 244-251.

[3] SHAMIR A. Identity-based cryptosystem and signature scheme[C]//Advances in Cryptology-Crypto'84. Santa Barbara: Springer-Verlag, 1984: 47-53.

[4] RIYAMI A S, PATERSON K. Certificateless public key cryptography[C]//Advances in Cryptology-Asiacrypt'03. Taiwan, China: Springer-Verlag, 2003: 452-473.

[5] HE D, CHEN Y, CHEN J. A new two-round certificateless authenticated key agreement protocol without bilinear pairings[J]. Mathematical and Computer Modelling, 2011, 54(11): 3143-3152.

[6] HE D, SAHADEO P, CHEN J. An efficient certificateless two-party authenticated key agreement protocol[J]. Computers & Mathematics with Applications, 2012, 64(6): 1914-1926.

[7] SUN H, WEN Q, ZHANG H, et al. A novel pairing-free certificateless authenticated key agreement protocol with provable security[J]. Frontiers of Computer Science, 2013, 7(4): 544-557.

[8] DARIO C. Fully non-interactive onion routing with forward secrecy[J]. International Journal of Information Security, 2013, 12(1): 33-47.

[9] ZHANG G. Fuzzy certificateless identity-based encryption protocol from lattice[J]. Applied Mechanics and Materials, 2013, 380(2): 2262-2266.

[10] ZHANG L, ZHANG F. Certificateless partially blind signatures[C]//1st International Conference on Information Science and Engineering (ICISE). Nanjing: IEEE, 2009: 2883-2886.

[11] ZHANG L, ZHANG F, QIN B, et al. Provably-secure electronic cash based on certificateless partially-blind signatures[J]. Electronic Commerce Research and Applications, 2011, 10(5): 545-552.

[12] LIU J, ZHANG Z, SUN R, et al. Certificateless partially blind signature[C]//26th International Conference on Advanced Information Networking and Applications Workshops (WAINA). Fukuoka: IEEE, 2012: 128-133.

[13] LI F, ZHANG M, TAKAGI T. Identity-based partially blind signature in the standard model for electronic cash[J]. Mathematical and Computer Modelling, 2013, 58(1-2): 196-203.

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

[15] 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.

[16] 邵国金, 薛冰, 陈明. 基于椭圆曲线DLP问题的无证书部分盲签名机制[J]. 四川大学学报: 工程科学版, 2012, 44(1): 112-117.
SHAO Guo-jin, XUE Bing, CHEN Ming. Certificateless partially blind signature scheme based on the elliptic curve discrete logarithm problem[J]. Journal of Sichuan University: Engineering Science Edition, 2012, 44(1): 112-117.

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

[18] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

编 辑 叶 芳