第 25 卷第 3 期　　四川理工学院学报(自然科学版)　　Vol. 25　No. 3
2012 年 6 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Jun. 2012
文章编号:1673-1549(2012)03-0059-05　　DOI:10.3969/j.issn.1673-1549.2012.03.015

高效的和可证明安全的无证书部分盲签名方案

张　勇,郭　琳

(四川职业技术学院计算机科学系,四川　遂宁　629000)

摘　要:为了提高盲签名的签名效率和安全性,学者们提出了多种部分盲签名方案。对其中的两种签名方案分析发现,都存在严重的安全缺陷,其中一种方案存在公钥替换攻击,而另一种方案中不诚实的签名请求者可任意篡改公共协商信息。针对这些安全缺陷,提出了一种新的无证书部分盲签名方案,改进存在的安全缺陷。分析表明,新方案不仅改进了已有方案的安全缺陷,且计算性能更优。

关键词:部分盲签名;无证书;双线性对;公钥替换攻击

中图分类号:TP309　　**文献标识码**:A

Al – Riyamih 等人[1]首次提出了无证书的公钥密码体制,该体制解决了基于身份公钥密码体制中的密钥托管问题,同时又继承了基于身份公钥密码体制的优点,在不使用公钥证书的前提下解决了基于证书公钥系统的证书管理问题。在随后的几年中,国内外研究者广泛关注于无证书的公钥密码体制。

Chaum[2]提出的盲签名概念,与一般数字签名的不同之处在于,签名者不知道他所签发文件的具体内容,并且不能把签名过程与最终所得的签名对应起来,这种特性被称之为盲性。盲签名在具有匿名性要求的领域(如电子支付或匿名的电子选举等)得到了广泛应用。然而在完全盲签名中,最终签名的任何信息都是签名者不知道,这样的签名系统存在不完善性,而且很可能造成签名被非法使用等一系列问题。完全盲签名的这一缺点在部分盲签名[3]中得到了很好的解决,允许在签名中嵌入客户与签名者协商好的公共信息,以便在签名者不知道所签署消息具体内容的情况下更有效的保护签名者的合法权益。

近来,一些研究者提出了无证书的部分盲签名[4-10]。但是,一些方案[5-6]被发现是不安全的[8-9],一些方案[4]的计算开销较高。在改进原有方案的过程中,提出了几种新的无证书部分盲签名方案[7-10]。

本文指出了两种新提出的无证书部分盲签名方案[7-8]的安全缺陷,并且分析发现文献[9]提出的方案也存在与文献[8]方案相同的安全缺陷。在此研究基础上,提出了一种新的方案:无证书部分盲签名。本文方案在随机预言机模型下,被证明是具有安全性的,且计算性能更优。

1　双线性映射与困难问题假设

假设 F_1 和 F_2 分别是素阶为 q 的循环加法群和循环乘法群,定义 $e:F_1 \times F_1 \to F_2$ 为满足以下性质的双线性映射:

双线性性:对于 $\forall(P,Q) \in F_1$ 和 $\forall(a,b) \in Z_q^*$ 有 $e(aP,bQ) = e(P,Q)^{ab}$。

非退化性:存在 $(P,Q) \in F_1$ 满足 $e(P,Q) \neq 1$。

可计算性:对于 $\forall(P,Q) \in F_1$,能有效计算 $e(P,Q)$。

在已经给定的双线性对中主要存在以下的困难问题假设。

CDH(Computational Diffie – Hellman)假设:对于任意未知的 $a,b \in Z_q^*$,给定 $P,aP,bP \in F_1$,不存在概率多项式时间算法能成功计算 abP。

BDH(Bilinear Diffie – Hellman)假设:对于任意未知的 $a,b,c \in Z_q^*$,给定 $(P,aP,bP) \in F_1$,不存在概率多项式时间算法能成功计算 $e(P,P)^{abc}$。

2　两种部分盲签名方案分析

2.1　ZZ 方案分析

ZZ 方案[7]简要描述如下:

收稿日期:2012-04-06

作者简介:张　勇(1970-),男,四川蓬溪人,副教授,硕士,主要从事信息安全与网络数据库开发方面的研究,(E-mail) 517669685@qq.com

Setup:产生并发布系统参数 param = $\{F_l, F_2, e, P, q, Q_{pub}, H_1, H_2, H_3\}$。其中,$F_l$ 是阶为 q 的加法循环群,生成元为 P; F_2 是阶为 q 的乘法循环群;$e: F_l \times F_l \to F_2$ 是双线性映射; $Q_{pub} = sP$ 为 PKG 的公钥,对应的 $s \in Z_q^*$ 是 PKG 的主密钥;$H_1: \{0,1\}^* \times F_l \to F_1$, $H_2: \{0,1\}^* \times F_l \to Z_q^*$ 和 $H_3: \{0,1\}^* \to F_1$ 是安全的散列函数。

KeyGen:签名者 S 将通过随机选择 $s_1 \in Z_q^*$ 产生的 s_1 作为其私有秘密,计算 $Q_1 = s_1 P$,将 Q_1 和 ID_S 发送给 PKG。PKG 计算 $Q_2 = H_1(ID_S, Q_1)$ 和 $S_2 = sQ_2$,将 S_2 通过秘密信道发送给签名者。签名者的私/公钥对为 $SK = (s_1, S_2)$, $PK = (Q_1, Q_2)$。

Issue:用户请求签名者对消息 m 进行部分盲签名的处理,c 是经过双方共同协商,达成一致意见后的说明信息,那么用户和签名者将会执行以下的交互协议:

(1)签名者随机选择 $k \in Z_q^*$,计算 $r = e(Q_2, Q_{pub})^k$,并将 r 发送给用户。

(2)用户选择随机数 $\alpha, \beta \in Z_q^*$,计算 $Q = H_3(c)$, $r' = r^\alpha e(Q_2 + Q, Q_1)^{\alpha\beta}$, $v(= H_2(m \| c, r')$ 和 $v = \alpha^{-1} v(\beta \pmod q)$,然后发送 v 给签名者。

(3)签名者计算 $Q = H_3(c)$ 和 $U = kS_2 vs_1(Q_2 + Q)$,将 U 返回给用户。

(4)用户收到 U 后,计算 $U' = \alpha U$。得到对 (m, c) 的部分盲签名 (U', r')。

Verify:验证者计算 $Q = H_3(c)$ 和 $v' = H_2(m \| c, r')$,验证等式 $r' = e(U', P) e(Q_2 + Q, Q_1)^{v'}$ 是否成立。若等式条件成立就接受该签名,否则该签名将被拒绝。

上述方案实际上就是一种无证书的部分盲签名方案,该方案被其作者称为是安全的,但是经过分析发现该方案由于在签名验证阶段没有使用 PKG 的公钥,因此,存在签名公钥替换攻击。

攻击者选择 $s_1' \in Z_q^*$,计算 $Q_1' = s_1(P, Q_2' = H_1' ID_S, Q_1')$, $S_2' = tQ_2'$(这里,$t \in Z_q^*$ 是攻击者自选的随机数,用以替换 PKG 的私钥),用 (Q_1', Q_2') 替换签名者原有公钥 (Q_1, Q_2)。除了签名者自己,其他任何实体都不能验证出攻击者已经替换了该公钥。在签名的整个过程中,仅在步骤 1) 中使用到了 PKG 的公钥,因此,攻击者用 tP 替换 PKG 公钥,计算 $r = e' Q_2', tP)^k$。由于 k 是签名者选择的随机参数且保密,那么签名请求者无法验证 PKG 公钥已被替换。并且,签名验证者可验证下式成立:

$$
\begin{aligned}
& e(U'P) e(Q_2' + Q, Q_1')^{v'} \\
&= e(\alpha k S_2' \alpha v s_1' Q_2' + Q), P' e(Q_2' + Q, Q_1')^{v'} \\
&= e(\alpha k\, tQ_2' (v' \alpha\beta) s_1' (Q_2' + Q), P) e(Q_2' + Q, Q_1')^{v'} \\
&= e(Q_2' tP)^{\alpha k} e((Q_2' + Q), s_1' P)^{\alpha\beta v'} e(Q_2' + Q, Q_1')^{v'} \\
&= r^\alpha e((Q_2' + Q), Q_1')^{\alpha\beta} = r'
\end{aligned}
$$

众所周知,基于身份(或无证书)的签名方案不再依靠公钥证书验证用户公钥的有效性,而是将 PKG 的公钥参数嵌入到签名算法中以确保系统的安全性。在上述方案中,恶意攻击者可以随意替换 PKG 的公钥而不会被发现,这就使得最基本的安全得不到保障。显而易见,这一方案缺少必要的安全性。

2.2 LDL 方案分析

LDL 部分盲签名方案[8]描述如下。

Setup:系统参数 $param = \{F_l, F_2, e, P, g, q, P_{pub}, H_1, H_2, H_3\}$。其中,$F_l, F_2, P$ 和 e 与前面方案类似;g 是 F_2 的生成元,且 $e(P, P) = g$;$P_{pub} = sP$ 为 PKG 的公钥,对应的 $s \in Z_q^*$ 是 KGC 的主密钥;$H_1: \{0,1\}^* \to Z_q^*$, $H_2: G_l \to Z_q^*$ 和 $H_3: \{0,1\}^* \times F_2 \times F_1 \to Z_q^*$ 是安全的散列函数。

KeyGen:签名者提交其身份 ID_A 给 KGC, KGC 计算 $q_A = H_1(ID_A)$ 和 $D_A = (s + q_A)^{-1} P$ 并返回 D_A 作为 A 的部分私钥。A 随机选择 $x_A \in Z_q^*$ 作为其私有秘密,计算 $Q_A = P_{pub} + q_A P$, $R_A = x_A Q_A$, $y_A = H_2(R_A)$ 和 $SK_A = (x_A + y_A)^{-1}$。其公钥 $PK_A = R_A$。

Issue:用户请求签名者对消息 m 进行部分盲签名,c 是双方共同协商的说明信息,那么用户和签名者执行以下交互协议:

(1)签名者 A 选择随机数 $r \in Z_q^*$,计算 $g_1 = e(P, Q_A)$, $U = g^r$ 和 $V = g_1^r$ 并将 (g_1, U, V) 发送给用户。

(2)用户随机选择 $\alpha, \beta, \lambda \in Z_q^*$,计算 $u = H_1(c)$, $U' = U^\alpha g^{\alpha\beta} g_1^{-\lambda u}$, $V' = V^\alpha g_1^\lambda$, $v = H_3(m, U', PK_A)$ 和 $h = \alpha^{-1} v + \beta$,然后发送 h 给 A。

(3)A 计算 $u = H_1(c)$,和 $W = (r + h) SK_A D_A + ruSK_A P$,将 W 返回给用户。

(4)用户收到 W 后,计算 $W' = \alpha W$。得到对 (m, c) 的部分盲签名 (U', V', W')。

Verify:验证者计算 $q_A = H_1(ID_A)$, $Q_A = P_{pub} + q_A P$, $y_A = H_2(R_A)$, $u = H_1(c)$ 和 $v = H_3(m, U', PK_A)$,验证等式 $e(W', R_A + y_A Q_A) = U' V'^u g^v$ 是否成立。若等式成立则接受签名,否则拒绝。

注意到,验证者在计算 Q_A 时使用了 KGC 的公钥 P_{pub},且 Q_A 作为 A 的基于身份公钥被用于验证签名正确性。因此,该方案有效避免了 ZZ 方案[7]的缺陷。但是,分析发现,不诚实的用户可篡改其与签名者共同协商的信息 c。

令 $t = H_1(c')$,这里,c(为签名请求者私自篡改后的协商信息。签名请求者计算 $V' = V^{\alpha u t^{-1}} g_1^{\lambda u t^{-1}}$,其它计算

不变,最后输出(U',V',W')作为对(m,c')的部分盲签名。这里,由于α和λ是签名请求者私有的随机盲因子,因此,任何实体都不能发现这一不诚实行为。最后,验证者计算$t = H_1(c')$,$v = H_3(m,U',PK_A)$,验证等式。

$$\begin{aligned}
&e(W(,R_A + y_AQ_A) = e(\alpha W,(x_A + y_A)Q_A)\\
&= e(\alpha(r+h)SK_AD_A + \alpha ruSK_AP,(x_A + y_A)Q_A)\\
&= e((\alpha r + v + \alpha\beta)SK_AD_A,(x_A +\\
&y_A)Q_A)e(\alpha ruSK_AP,(x_A + y_A)Q_A)\\
&= e(SK_AD_A,(x_A + y_A)Q_A)^{\alpha r+v+\alpha\beta}e(SK_AP,\\
&(x_A + y_A)Q_A)^{\alpha ru} = g^{\alpha r+v+\alpha\beta}g_1^{\alpha ru}\\
&U'V'^tg^v = U^\alpha g^{\alpha\beta}g_1^{-\lambda u}(V^{\alpha ut^{-1}}g_1^{\lambda ut^{-1}})^tg^v\\
&= g^{\alpha r}g^{\alpha\beta}g_1^{-\lambda u}V^{\alpha u}g_1^{\lambda u}g^v = g^{\alpha r+v+\alpha\beta}g_1^{\alpha ru}
\end{aligned}$$

可见,在验证签名时,验证者不能发现协商信息 c 被替换成了 c'。由于协商信息是对盲消息 m 的说明信息,它被篡改意味着签名请求者可以滥用签名。例如,在电子现金协议中,c 通常用于限定电子钱币的面额和使用期限等,如果 c 可以被自由篡改,将会造成银行的巨大损失。

3　新的无证书部分盲签名方案

Setup:输入安全参数 k,输出系统参数 $params = \{e,F_1,F_2,P,P_0,g,H_1,H_2\}$。其中,$F_1$ 是素数阶为 q 的加法循环群,P 是 F_1 的一个生成元;F_2 是与 F_1 同阶的乘法循环群,$g = e(P,P)$ 为 F_2 的生成元;e: $F_1(F_1 \rightarrow F_2$ 是双线性映射;$P_0 = sP$ 为 KGC 的公钥,$s \in Z_q^*$ 为系统主密钥;$H_1:\{0,1\}^* \rightarrow F_1$,$H_2$: $\{0,1\}^* \rightarrow Z_q^*$ 和 H_3: $\{0,1\}^* \rightarrow Z_q^*$ 为安全的 $Hash$ 函数。

KeyGen:输入签名者身份 ID_S,KGC 计算并输出 ID_S 的部分私钥 $D_S = sQ_S$,其中,$Q_S = H_1(ID_S)$;ID_S 随机选取 $x \in Z_q^*$ 作为其秘密值,其私钥 $S_S = (x,D_S)$ 和公钥 $P_S = xP$。

Issue:用户请求签名者对消息 m 进行部分盲签名的处理,c 是经过双方共同协商,达成一致意见后的说明信息,那么用户和签名者将会执行以下的交互协议。

(1)签名者 ID_s 选择随机数 $r \in Z_q^*$,计算 $R = rQ_S$ 并将 R 发送给用户。

(2)用户随机选择 $\alpha,\beta \in Z_q^*$,计算 $u = H_2(c)$,$U = u^{-1}\alpha(R + \beta Q_S)$,$v = H_3(m,c,ID_s,P_S,U)$ 和 $h = \alpha^{-1}v + \beta$,然后发送 h 给签名者。

(3)签名者计算 $u = H_2(c)$,和 $V = (h + r)(D_S + uxQ_S)$,将 V 返回给用户。

(4)用户收到 V 后,计算 $W = \alpha V$。得到对(m,c)的部分盲签名 (U,W)。

Verify:验证者计算 $Q_S = H_1(ID_S)$,$u = H_2(c)$ 和 $v = H_3(m,c,ID_s,P_S,U)$,验证等式 $e(W,P) = e(vQ_S + uU,P_0 + uP_S)$ 是否成立。若等式成立则接受签名,否则拒绝。

4　分析与比较

4.1　正确性

通过下式可以证明本文无证书部分盲签名方案的正确性。

$$\begin{aligned}
&e(W,P) = e(\alpha V,P)\\
&= e((v + \alpha\beta + \alpha r)(s + ux)Q_S,P)\\
&= e((v + \alpha\beta + \alpha r)Q_S,(s + ux)P)\\
&= e(vQ_S + \alpha(r + \beta)Q_S,sP + uxP)\\
&= e(vQ_S + uU,P_0 + uP_S)
\end{aligned}$$

4.2　部分盲性

在参考文献[2]中有关于部分盲性的定义,本文所提出的部分盲签名方案是满足部分盲特性的。下面是其证明思路:总是有一对唯一的随机盲因子(α,β),存在于任意给定的一个有效的部分盲签名(m,c,U,W)和部分盲签名发布中产生的中间变量(R,v,h,V)中,所以方案满足部分盲性。

定理 1　本文无证书部分盲签名方案满足部分盲性。

证明:对于给定的 (U,W) 和部分盲签名发布中产生的中间变量(R,v,h,V),考虑如下等式。

$$W = \alpha V \tag{1}$$

$$h = \alpha^{-1}v + \beta \tag{2}$$

$$U = u^{-1}\alpha(R + \beta Q_S) \tag{3}$$

根据以上等式可知,一定存在唯一的 $\alpha \in Z_q^*$ 使等式(1)成立;进一步可以通过等式(2)计算出唯一的 β,即 $\beta = h - \alpha^{-1}v$。根据 3.1 节的正确性证明,可得下式成立。

$$e(W,P) = e(vQ_S + uU,P_0 + uP_S)$$

由此可推断出等式(3)也成立。因此,盲因子 α,β 在部分盲签名的生成中总是存在。得证,本方案满足部分盲性。

4.3　不可伪造性

本文考虑无证书体制[1]下的两类敌手 $(Adv \in \{A_I,A_{II}\})$。

A_I 一个来自外部的攻击者,他可以获得部分实体的私钥,可以替换任何实体的部分公钥,但不能获得特定实体的部分私钥和 KGC 的主密钥。A_{II} 是一个恶意但受限的 KGC,他可以获得任何实体的部分私钥和 KGC 的主密钥,但不能获得替换特定实体的公钥以及实体的私有秘钥。

本文采用无证书部分盲签名安全模型来形式化分析新签名方案的不可伪造性。安全模型定义为挑战者 C 和敌手 $A \in \{A_I, A_{II}\}$ 之间的游戏来模拟部分盲签名方案的不可伪造性,包括初始化、查询和伪造三个阶段,详细模型参见文献[10]。

定理 2 如果 CDH 假设成立,本文提出的无证书部分盲签名在 A_I 敌手适应性选择消息攻击下满足不可伪造性。

证明 定理 2 的证明可归结为 A_I 敌手求解 CDH 问题。这里给出一个 CDH 问题实例,演示 C 如何利用 A_I 解决 CDH 问题。首先,令 $P_0 = aP$, C 以 A_I 为子程序并充当游戏中的挑战者。

初始化:C 产生并发送 *params* 给 A_I, 维持初始为空的列表 $L_1, L_2, L_2, L_{PK}, L_{IS}$分别用于跟踪 A_I 对预言机 H_1, H_2, H_3, 公/私钥和签名发布查询。

查询: A_I 自适应地执行多项式时间有界的查询:

H_1 查询:收到$H_1(ID_i)$查询,C首先查询L_1,若(ID_i, Q_i, D_i)已存在,则返回Q_i;否则,如果$ID_i = I$,设置$D_i = \perp$, $Q_i = bP$;否则 C 随机选择 $Q_i \in Z_q^*$,计算 $D_i = sQ_i$,将 (ID_i, Q_i, D_i) 插入 L_1,并返回 Q_i。

H_2 查询: 收到 $H_2(c_i)$ 查询,C 首先查询 L_4,若(c_i, u_i) 已存在,则返回 u_i;否则随机选择 $u_i \in Z_q^*$,将(c_i, u_i) 插入 L_2 返回 u_i。

H_3 查询:收到 $H_3(m_i, c_i, ID_i, P_i, U_i)$ 查询,C 首先查询L_3,若$(m_i, c_i, ID_i, P_i, U_i, v_i)$已存在,则返回$v_i$;否则,$C$随机选择 $v_i \in Z_q^*$,将$(m_i, c_i, ID_i, P_i, U_i, v_i)$ 插入 L_3,并返回 v_i。

部分私钥查询: 当收到对 ID_i 的部分私钥查询时,如果 $ID_i = I$,C 终止模拟;否则 C 执行 $H_1(ID_i)$ 查询并检索 L_1,然后返回 D_i。

私钥查询: 当收到对 ID_i 的私钥查询时,C 查询 L_{PK},若(ID_i, P_i, x_i) 已存在则返回 x_i;否则 C 执行对 ID_i 的公钥查询,并返回 x_i。

公钥查询: 当收到对 ID_i 的公钥查询时,C 首先查询 L_{PK},若(ID_i, P_i, x_i) 在 L_{PK} 中存在,则返回 P_i;否则 C 随机选择$x_i \in Z_q^*$,计算$P_i = x_iP$,将(ID_i, P_i, x_i) 插入L_{PK},返回 P_i。

公钥替换查询: 当收到对 ID_i 的公钥替换查询时,C 用 P_i^* 替换原有 P_i,然后用$(ID_i, P_i^*, \perp)$ 更新 L_{PK}。注意,这里需要 A_I 提供 P_i^*。

签名发布查询: 当收到 $IS(m_i, c_i, ID_i, P_i)$ 查询,如果$ID_i = I$,$m_i = m(\,, c_i = c(\,$,则C终止模拟;否则C查询 L_{IS}, 如果$(m_i, c_i, ID_i, P_i, U_i, W_i)$ 已存在, 则返回(U_i, W_i),否则 C 按下列步骤执行:(1) 如果 $ID_i = I$,随机选择 $W_i, U_i \in F_1$;否则随机选择 $r, \alpha, \beta \in Z_q^*$,计算 $U_i = u_i^{-1}\alpha(rP + \beta Q_i)$ 和 $W_i = (v_i + \alpha\beta + \alpha r)(D_i + u_i x_i Q_i)$;(2) 将$(m_i, c_i, ID_i, P_i, U_i, W_i)$ 插入 L_{IS},返回(U_i, W_i)。

签名验证查询:当收到对 $(U_i, W_i, m_i, c_i, ID_i)$ 的签名验证查询,如果$(m_i, c_i, ID_i, P_i, U_i, W_i)$ 在 L_{IS} 中已存在,则返回成功;否则,若验证签名 $Verify(U_i, W_i, m_i, c_i, ID_i, P_i, P_0) = 1$,C 返回成功,否则返回失败。

伪造:经过上述查询后, A_I 从 L_{IS} 中随机选择 W_i $(i \in [1, q_{is}])$,然后随机选择 $r, \alpha, \beta \in Z_q^*$,计算 $u(\, = H_2(c(\,), U(\, = u(\,^{-1}\alpha(rP + \beta Q_I)$,$v(\, = H_3(m(\,, c(\,, ID_I, P_I, U(\,)$ 和 $h(\, = \alpha^{-1}v(\, + \beta$,输出对$(m(\,, c(\,)$ 的伪造签名 $\sigma(\, = (U(\,, W_i)$。若伪造签名成功,则 C 输出。

$$D_I = abP = \frac{W_i - (v' + \alpha\beta + \alpha r)u' x_I Q_I}{(v' + \alpha\beta + \alpha r)}$$

作为解决 CDH 问题的回答。

若游戏没有被终止,假设 A_I 最多进行 q_i 次 H_i 查询 $(i = 1, 2, 3)$、q_s 次私钥查询、q_p 次公钥替换查询和 q_{is} 次签名发布查询,根据二分引理[11],如果 A_I 以不可忽略的优势 ε 赢得游戏,那么 C 解决 *CDH* 问题的优势: $\tau \leqslant \varepsilon/16q_1q_{is}$。

因此,如果 CDH 假设成立,那么不存在 A_I 敌手攻破本文方案的不可伪造性。证毕。

定理 3 如果 CDH 假设成立,本文提出的无证书部分盲签名在 A_{II} 敌手适应性选择消息攻击下满足不可伪造性。

证明 定理 3 的证明与定理 2 类似。我们给出 A_{II} 敌手面临的 *CDH* 难题:令 $P_I = aP, Q_I = bP$,这里存在 CDH 难题 $V = (h + r)(D_I + ux_IQ_I) = (h + r)(D_I + uabP)$。由于篇幅原因,详细的游戏模拟过程省略。

因此,如果 CDH 假设成立,那么不存在 A_{II} 敌手攻破本文方案的不可伪造性。证毕。

4.4 协商信息不可替换性

本文从签名者替换和签名请求者替换两个方面来分析协商信息不可替换性。

假设协商信息 c 被签名者替换为 c′,那么验证者计算 $u' = H_2(c')$,从而验证。

$$e(vQ_S + u(U, P_0 + u(P_S) \neq e(W, P) \neq e(W(\,, P)$$

这里, $W = \alpha(h + r)(D_S + uxQ_S)$ 为原始签名,$W' = \alpha(h + r)(D_S + u(xQ_S)$ 为替换签名。可见,协商信息 c 被签名者替换后不能通过验证,因此签名者不能替换成功。

假设协商信息 c 被签名者请求者替换为 c',签名请求者计算 $U' = u'^{-1}\alpha(R + \beta Q_S)$,那么验证者计算 $u' = H_2(c')$,从而验证:

$$e(vQ_S + u'U', P_0 + u'P_S) =$$

$e(vQ_S + \alpha(r+\beta)Q_S, sP + u'xP) \neq$

$e(W,P) = e(vQ_S + \alpha(r+\beta)Q_S, sP + uxP)$

可见,协商信息 c 被签名者请求者替换后不能通过验证,因此签名者请求不能替换成功。可证,本文部分盲签名方案满足协商信息不可替换性。

4.5 计算性能分析与比较

表 1 比较了本文方案与其它四种类似方案[7-10]的计算性能。这里,T_p 表示对运算开销,T_s 表示 F_1 中标量乘的计算开销,T_e 表示 F_2 中模指数运算的计算开销,T_h 表示 *map-to- point* 哈希函数的计算开销。根据文献[12],可以得到如下关系:$1T_p \approx 1440t_m$,$1T_s \approx 29t_m$,$1T_e \approx 21t_m$,$1T_h \approx 23t_m$(这里,t_m 表示一个基本计算单元,即整数域上的乘法运算)。

表 1　计算性能比较(单位:次数)

Issue 算法	Verify 算法	总开销	
文献[7]方案	2Tp + 3Te + 3Ts + 2Th	2Tp + 1Te + 2Th	6023tm
文献[8]方案	1Tp + 7Te + 3Ts	1Tp + 2Te + 2Ts	3209tm
文献[9]方案	2Tp + 3Te + 2Ts	2Tp + 2Te	5923tm
文献[10]方案	2Tp + 1Te + 6Ts + 1Th	3Tp + 1Te + 1Th	7462tm
本文方案	7Ts + 1Th	2Tp + 3Ts + 1Th	3013tm

从表 1 中对比看,本文方案的计算性能更优。

5　结束语

针对新近提出的两个无证书部分盲签名方案[7-8],本文指出了这两个部分盲签名方案的安全缺陷。在文献[7]提出的方案中存在签名公钥替换攻击;在文献[8]提出的方案中,恶意用户能非法篡改公共协商信息而不被发现。本文所提出的新的无证书部分盲签名方案,弥补了上述方案存在的缺陷。分析表明,新方案是安全的,且计算性能更优。

参 考 文 献:

[1] Al-Riyami SS,Paterson KG.Certificateless public key cryptography[C].ASIACRYPT 2003,LNCS 2894,Berlin:Springer-Verlag,2003,452-473.

[2] Chaum D.Blind signatures for untraceable payments [C]. Advances in Crypto'82. Plenum, NY, 1982, 199-203.

[3] Abe M,Fujisaki E.How to date blind signatures[C]. Advances in Cryptology-AisaCrypt'96. Heidelberg: Springer-Verlag,1996,244-251.

[4] 苏万力,谭示崇,李艳平,等.无证书部分盲签名[J].吉林大学学报:工学版,2009,39(4):1094-1098.

[5] 荣维坚.无证书部分盲签名方案[J].漳州师范学院学报:自然科学版,2008,21(4):44-47.

[6] 冯 涛,彭 伟,马建峰.安全的无可信 PKG 的部分盲签名方案[J].通信学报,2010,31(1):128-133.

[7] 张小萍,钟 诚.高效无可信私钥生成中心部分盲签名方案[J].计算机应用,2011,31(4):992-995.

[8] 李明祥,杜光辉,罗新方.高效的无证书部分盲签名方案[J].计算机工程与设计,2010,31(22):4817-4819,4892.

[9] 余 丹,杨晓元,黄大威.新的无证书部分盲签名方案[J].计算机应用研究,2010,27(11):4319-4321.

[10] 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, 5(10):545-552.

[11] Pointcheval D,Stern J.Security Arguments for Digital Signatures and Blind Signatures[J].Journal of Cryptology,2000,13(3):361-396.

[12] Shacham H.New Paradigms in Signature Schemes[D]. Stanford:Stanford University,2005.

Efficient and Provable Secure Certificateless Partially-Blind Signature Scheme

ZHANG Yong, *GUO Lin*

(Department of Computer Science, Sichuan Vocational and Technical College, Suining 629000, China)

Abstract: In order to increase efficiency and improve security, mamy no certificate partially blind signature schemes are proposed. Two of them are analyzed to find that both schemes are not secure. One method exists the replacement attack by public keys. But the dishonest signature requester can tamper with the agreed upon information. A new one is proposed to improve the security flaws in the formers. The results show that the new no certificate partially blind signature scheme has not only improved the security flaws, but also has better computing performance.

Key words: partially blind signature; no certificate; bilinear pairing; public key replacement attack