Journal of Computer Applications
计算机应用,2013,33(3):762 -765
ISSN 1001-9081
CODEN JYIIDU
2013-03-01
http://www.joca.cn

文章编号:1001 -9081(2013)03 -0762 -04
doi:10.3724/SP.J.1087.2013.00762

基于身份部分盲签名方案的分析与改进

何俊杰[1*],孙　芳[2],祁传达[1]
(1.信阳师范学院 数学与信息科学学院,河南 信阳 464000;　2.信阳师范学院 计算机与信息技术学院,河南 信阳 464000)
(*通信作者电子邮箱 hejj99@163.com)

摘　要:对李明祥等(李明祥,赵秀明,王洪涛. 对一种部分盲签名方案的安全性分析与改进. 计算机应用,2010,30(10):2687 -2690)提出的一种基于身份的部分盲签名方案进行了安全性分析,指出方案中签名请求者可以非法修改协商信息。为了有效抵抗篡改协商信息攻击,提出一种改进的部分盲签名方案。在随机预言机模型下证明了新方案对自适应选择消息和身份攻击是存在性不可伪造的。与基于身份部分盲签名方案的性能比较显示,新方案具有较高的运算效率。

关键词:盲签名;部分盲签名;双线性对;基于身份;随机预言机模型
中图分类号:TP309　**文献标志码**:A

Cryptanalysis and improvement of ID-based partially blind signature scheme

HE Junjie[1*], SUN Fang[2], QI Chuanda[1]
(1. *College of Mathematics and Information Science, Xinyang Normal University, Xinyang Henan* 464000, *China*;
2. *College of Computer and Information Technology, Xinyang Normal University, Xinyang Henan* 464000, *China*)

Abstract: The cryptanalysis of the ID-based partially blind signature scheme proposed by Li *et al.* (LI M X, ZHAO X M, WANG H T. Security analysis and improvement of a partially blind signature scheme. Journal of Computer Applications, 2010, 30(10): 2687-2690) showed that the signature requester could change the negotiated information illegally. Therefore, an improved partially blind scheme was purposed to resist the tampering negotiated information attacks. The new scheme was proved to be existentially unforgeable against adaptive chosen message and identity attacks in random oracle model. Compared with other ID-based partially blind signature schemes, the new scheme has higher computational efficiency.

Key words: blind signature; partially blind signature; bilinear pairing; ID-based; random oracle model

0　引言

1982 年,Chuam[1]为了实现不可跟踪的支付系统首次提出盲签名的概念。它是签名者和请求者之间的一个双方交互协议,能够让签名者在不知道待签消息的具体内容的情况下对消息进行签名,当盲签名公布后签名者也无法将签名过程与最终公布的签名联系起来。盲签名能够有效地保护签名请求者的隐私,在投票选举、签立遗嘱和现金钞票的电子化中有着广泛的应用。然而由于签名者对所签消息的内容一无所知,很容易造成签名被恶意的请求者非法使用。为了解决盲签名的这一弱点,1996 年,Abe 和 Fujisaki[2]提出了部分盲签名的概念。部分盲签名将待签消息分为两部分:一部分是需要签名的消息,对签名者保持盲性,即签名者不可见;另一部分是签名者与签名请求者事先协商好的公共信息,如对消息的范围、签名的有效期的限定等。部分盲签名方案既可以保护签名请求者的隐私又使得签名者对签名内容是部分可控的,较好地解决了盲签名在匿名性和可控性之间的矛盾。

1984 年,Shamir[3]提出了基于身份公钥密码体制。在基于身份的密码体制中,一般将用户的公开身份信息(如姓名、电话号码、电子邮件地址等)作为用户公钥,或者由用户的身份信息通过一个公开算法(如单向函数)计算出该用户的公钥,而用户私钥则由一个可信第三方——私钥生成中心(Private Key Generator,PKG)统一生成。2001 年,Boneh 等[4]利用双线性对技术提出了第一个基于身份的加密方案。

2005 年,Chow 等[5]结合基于身份公钥密码学和部分盲签名,首次提出了一个基于身份的部分盲签名方案,并证明该方案在随机预言模型下是安全的;Chen 等[6]提出了基于身份的限制性部分盲签名方案;崔巍等[7]基于q-强 Diffie-Hellman 问题提出了更高效的基于身份的限制性部分盲签名方案;但李明祥等[8]指出崔巍方案是不安全的,并给出了一个改进方案。

本文对李明祥等[8]提出的改进方案进行安全性分析,指出该方案也是不安全的,请求者在盲签名发布过程中可以篡改公共信息,使得签名者丧失了对所签消息的可控性。本文提出了一种改进方案,对新方案进行了安全和效率分析。分析表明,新方案在有效抵抗篡改公共消息攻击的同时,满足盲性和不可伪造性等安全性需求;与已有的基于身份的部分盲签名方案相比,所提方案效率较高。

1　预备知识

1.1　双线性映射群

设 G_1、G_2 和 G_T 是阶为素数 p 的循环群,P、Q 分别是 G_1 和 G_2 的生成元。如果(G_1,G_2,G_T)是双线性映射群,则双线性映射 $e:G_1 \times G_2 \rightarrow G_T$ 存在,并满足下面四个条件:

1)双线性性:对于任何 $U \in G_1, V \in G_2, a,b \in \mathbf{Z}_p^*$,有 $e(aU,bV) = e(U,V)^{ab}$。

收稿日期:2012-09-25;**修回日期**:2012-11-19。　**基金项目**:国家自然科学基金资助项目(61272465);河南省自然科学基金资助项目(102102210242, 122400450189);河南省教育厅科学技术研究重点项目(12A520034)。

作者简介:何俊杰(1981 -),男,安徽庐江人,讲师,硕士,CCF 会员,主要研究方向:信息安全;　孙芳(1981 -),女,河南信阳人,讲师,硕士,主要研究方向:信息安全;　祁传达(1965 -),男,河南固始人,教授,博士,主要研究方向:密码理论。

2) 非退化性:存在 $U \in G_1, V \in G_2$,使得 $e(U,V) \neq 1$。

3) 可计算性:对于任何的 $U \in G_1, V \in G_2$,存在一个高效的算法来计算 $e(U,V)$ 的值。

4) 存在有效并可以公开计算的同构映射 $\psi: G_2 \to G_1$,使得 $\psi(Q) = P$。

1.2 困难性假设

1)计算 Diffie-Hellman 问题(Computational Diffie-Hellman Problem,CDHP):设 G_T 是 p 阶循环乘法群,g 是 G_T 的生成元,已知 $g, g^a, g^b, g^c \in G(a,b,c \in \mathbf{Z}_p^*$ 未知),计算 g^{abc}。

2) q-强 Diffie-Hellman 问题(q-Strong Diffie-Hellman Problem, q-SDHP)[9]:设 (G_1, G_2, G_T) 是双线性映射群,ψ 是 G_2 到 G_1 的同构映射,P, Q 分别是 G_1 和 G_2 的生成元,且 $\psi(Q) = P$。已知 $(q+2)$ 元组 $(P, Q, xQ, x^2Q, \cdots, x^qQ)$ ($x \in \mathbf{Z}_p^*$ 未知),输出 $\left(c, \frac{1}{x+c}P\right)$,其中 $c \in \mathbf{Z}_p^*$。

2 李方案[8]回顾

2.1 系统建立

给定安全参数 k,PKG 选择阶为素数 $p(p > 2^k)$ 的双线性映射群 (G_1, G_2, G_T),选择生成元 $Q \in G_2$,构造双线性映射 $e: G_1 \times G_2 \to G_T$ 和同构映射 $\psi: G_2 \to G_1$,计算 $P = \psi(Q) \in G_1$, $g = e(P,Q)$。PKG 随机选择系统主密钥 $s \in \mathbf{Z}_p^*$,计算 $Q_{pub} = sQ \in G_2$ 作为系统公钥。选择哈希函数 $H_1: \{0,1\}^* \to \mathbf{Z}_p^*$ 和 $H_2: \{0,1\}^* \times G_T \to \mathbf{Z}_p^*$, $H_3: \{0,1\}^* \to \mathbf{Z}_p^*$。系统公开参数为 $params = \{G_1, G_2, G_T, p, P, Q, g, e, \psi, Q_{pub}, H_1, H_2, H_3\}$。

2.2 密钥提取

PKG 对身份 ID 生成私钥 $S_{ID} = \frac{1}{H_1(ID)+s}P$。

2.3 发布协议

假设要对消息 m 进行盲签名,c 为请求者与签名者事先协商好的公共信息,则:

1) 签名(阶段 1):签名者随机选择 $x, y \in_R \mathbf{Z}_p^*$,计算 $r = g^x, v = g^y$,并将 (r,v) 发送给请求者。

2) 盲化:请求者随机选择 $\alpha, \beta \in_R \mathbf{Z}_p^*$,计算 $r' = r^{\alpha H_3(c)} g^{\alpha\beta} v^{\alpha}, h = \alpha^{-1} H_2(m,c,r') + \beta$,把 h 发给签名者。

3) 签名(阶段 2):签名者计算 $S = (xH_3(c) + y + h)S_{ID}$,并将 S 发送给请求者。

4) 解盲:请求者计算 $S' = \alpha S$。

最终部分盲签名为 (m,c,r',S')。

2.4 签名验证

如果等式 $e(S', H_1(ID)Q + Q_{pub}) = r' g^{H_2(m,c,r')}$ 成立,则签名是有效的。

3 对李方案[8]的篡改协商信息攻击

通过分析发现李方案[8]不安全,恶意的请求者在盲签名发布过程中可以篡改公共信息。

假设恶意的请求者试图将协商的公共信息 c 篡改为 $\hat{c}$ ($\hat{c} \neq c$)。执行签名发布协议时,请求者收到签名者发送的 (r,v) 后,在盲化阶段,随机选择 $\alpha, \beta \in_R \mathbf{Z}_p^*$,计算 $r' = r^{\alpha H_3(c)} g^{\alpha\beta} v^{\alpha}, \hat{h} = \alpha^{-1} H_2(m,\hat{c},r') + \beta$,把 $\hat{h}$ 发给签名者。之后签名者对 $\hat{h}$ 进行签名,生成 $\hat{S} = (xH_3(c) + y + \hat{h})S_{ID}$;请求者解盲,得到 $\hat{S}' = \alpha\hat{S}$。请求者就可以得到部分盲签名 $(m,\hat{c},r',\hat{S}')$。

事实上,

$$
\begin{aligned}
e(\hat{S}', H_1(ID)Q + Q_{pub}) &= e(\alpha\hat{S}, H_1(ID)Q + sQ) = \\
& e(\alpha(xH_3(c) + y + \hat{h})S_{ID}, (H_1(ID) + s)Q) = \\
& e((\alpha x H_3(c) + \alpha y + \\
& H_2(m,\hat{c},r') + \alpha\beta)(H_1(ID) + s)S_{ID}, Q) = \\
& e((\alpha x H_3(c) + \alpha y + \alpha\beta + H_2(m,\hat{c},r'))P, Q) = \\
& e(P,Q)^{\alpha x H_3(c) + \alpha y + \alpha\beta + H_2(m,\hat{c},r')} = \\
& g^{\alpha x H_3(c)} g^{\alpha y} g^{\alpha\beta} g^{H_2(m,\hat{c},r')} = \\
& r^{\alpha H_3(c)} g^{\alpha\beta} v^{\alpha} g^{H_2(m,\hat{c},r')} = r' g^{H_2(m,\hat{c},r')}
\end{aligned}
$$

说明 $(m,\hat{c},r',\hat{S}')$ 可以通过验证,是有效的部分盲签名。

一方面,在李方案[8]的验证方程 $e(S', H_1(ID)Q + Q_{pub}) = r' g^{H_2(m,c,r')}$ 中,协商信息 c 是以 $H_2(m,c,r')$ 的形式出现的,而 $H_2(m,c,r')$ 由请求者生成,签名者无法区分 h 是由协商的公共信息 c 生成还是由篡改的公共信息 $\hat{c}$($\hat{c} \neq c$) 生成;另一方面,签名方程 $S = (xH_3(c) + y + h)S_{ID}$ 中虽然包含 $H_3(c)$,但是 $H_3(c)$ 被包含在 $r' = r^{\alpha H_3(c)} g^{\alpha\beta} v^{\alpha}$ 中,使得验证方程中不含 $H_3(c)$,验证者无法通过 $H_3(c)$ 验证公共信息 c 的合法性。所以恶意的请求者可以通过上述方法篡改公共信息。

4 对李方案[8]的改进

为了抵抗恶意的请求者的篡改协商信息攻击,对李方案[8]提出了一个改进方案。其中,系统建立和密钥提取阶段与李方案[8]相同(见 2.1 节和 2.2 节)。

1) 发布协议。

假设要对消息 m 进行盲签名,c 为请求者与签名者事先协商好的公共信息。请求者与签名者进行如下交互:

① 承诺:签名者随机选择 $x, y \in_R \mathbf{Z}_p^*$,计算 $r = g^x, v = g^y$,并将 (r,v) 发送给请求者。

② 盲化:请求者随机选择 $\alpha, \beta \in_R \mathbf{Z}_p^*$,计算 $r' = r^{\alpha} g^{\alpha\beta} v^{\alpha H_3^{-1}(c)}, h = \alpha^{-1} H_2(m,c,r') + \beta H_3(c)$,把 h 发给签名者。

③ 签名:签名者计算 $S = (xH_3(c) + y + h)S_{ID}$,并将 S 发送给请求者。

④ 解盲:请求者计算 $S' = \alpha S$。

最终消息 m 的部分盲签名为 (m,c,r',S')。

2) 签名验证。

验证者收到消息 m 的部分盲签名 (m,c,r',S') 后,验证等式 $e(S', H_1(ID)Q + Q_{pub}) = r'^{H_3(c)} g^{H_2(m,c,r')}$ 是否成立。如果成立,则 (m,c,r',S') 为有效的部分盲签名;否则签名无效。

5 改进方案的分析

5.1 安全性分析

5.1.1 正确性

定理 1　改进的基于身份的部分盲签名方案满足正确性。

证明　由于

$$
\begin{aligned}
e(S', H_1(ID)Q + Q_{pub}) &= e(\alpha S, H_1(ID)Q + sQ) = \\
& e(\alpha(xH_3(c) + y + h)(H_1(ID) + s)S_{ID}, Q) = \\
& e(\alpha(xH_3(c) + y + \alpha^{-1}H_2(m,c,r') + \\
& \beta H_3(c))P, Q) = \\
& e(P,Q)^{(\alpha x + \alpha y H_3^{-1}(c) + \alpha\beta)H_3(c) + H_2(m,c,r')} = \\
& g^{(\alpha x + \alpha y H_3^{-1}(c) + \alpha\beta)H_3(c)} g^{H_2(m,c,r')} = \\
& (g^{\alpha x} g^{\alpha y H_3^{-1}(c)} g^{\alpha\beta})^{H_3(c)} g^{H_2(m,c,r')} = \\
& (r^{\alpha} g^{\alpha\beta} v^{\alpha H_3^{-1}(c)})^{H_3(c)} g^{H_2(m,c,r')} = r'^{H_3(c)} g^{H_2(m,c,r')}
\end{aligned}
$$

说明部分盲签名验证过程正确。

5.1.2 不可伪造性

定理 2 在随机预言模型和 q-SDHP 困难的假设下，改进的基于身份的部分盲签名方案对自适应选择消息和身份攻击是存在性不可伪造的。

证明 假设存在一个攻击者 A 以不可忽略的概率成功伪造部分盲签名，下面构造一个算法 B 解决 q-SDHP。

设算法 B 收到 q-SDHP 实例 $(G,H,xH,x^2H,\cdots,x^qH)$，其中 $x \in \mathbf{Z}_p^*$ 未知，B 调用攻击者 A 为子程序计算 $\left(c,\frac{1}{x+c}G\right)$，其中 $c \in \mathbf{Z}_p^*$。

1) 系统设置。算法 B 进行以下操作生成系统公共参数。

①B 随机选择 $w_1,w_2,\cdots,w_{q-1} \in_R \mathbf{Z}_p^*$，生成多项式 $f(z)=\prod_{i=1}^{q-1}(z+w_i)=\sum_{i=0}^{q-1}a_iz^i$，其中 $a_0,a_1,\cdots,a_{q-1} \in \mathbf{Z}_p^*$。

②B 生成 G_2 的生成元 $Q=\sum_{i=0}^{q-1}c_i(x^iH)=f(x)H$ 和 G_1 的生成元 $P=\psi(Q)=\psi(f(x)H)=f(x)\psi(H)=f(x)G$，生成系统公钥 $Q_{\text{pub}}=\sum_{i=0}^{q-1}a_i(x^{i+1}H)=x\sum_{i=0}^{q-1}a_i(x^iH)=xQ \in G_2$，即以 x 模拟系统主密钥，但 B 不知道 x 的值。

③对应任意的 $i(1 \leqslant i \leqslant q-1)$，$B$ 生成多项式 $f_i(z)=\frac{f(z)}{z+w_i}=\sum_{j=0}^{q-2}b_{ij}z^j$，进而计算

$$\sum_{j=0}^{q-2}b_{ij}\psi(x^jH)=\left(\sum_{j=0}^{q-2}b_{ij}x^j\right)\psi(H)=f_i(x)G=\frac{f(x)}{x+w_i}G=\frac{1}{x+w_i}P$$

由此 B 可以得到 $\left(w_i,\frac{1}{x+w_i}P\right)$，$i=1,2,\cdots,q-1$。

2) 询问。B 随机选择 ID^* 作为挑战者的身份，并将 ID^* 和系统公共参数发送给攻击者 A。A 对身份 $ID_i(i=1,2,\cdots,q_1)$ 和消息 $m_i(i=1,2,\cdots,q_S)$ 进行查询。B 需要维护列表 L_1、L_2、L_3、L_S 响应 A 的 H_1 询问、H_2 询问、H_3 询问和签名询问，这些列表初始时是空的。具体交互过程如下：

①H_1 询问：A 关于 $ID_i(1 \leqslant i \leqslant q_1)$ 的每一次询问，B 首先检查列表 L_1。如果在列表 L_1 中已经存在项 (ID_i,ε_i)，B 将 ε_i 返回给 A 作为 ID_i 的 H_1 哈希值。否则，也就是 A 从来没做过 ID_i 的 H_1 询问，如果 $ID_i=ID^*$，则随机选择 $w^* \in_R \mathbf{Z}_p^*$，并将 $\varepsilon_i=w^*$ 返回给 A；如果 $ID_i \neq ID^*$，将 $\varepsilon_i=w_l$ 返回给 A，并将 l 增加 1。B 将 (ID_i,ε_i) 添加到列表 L_1。

②H_2 询问：A 关于 $(m_i,c_i,r'_i)(1 \leqslant i \leqslant q_2)$ 的每一次询问，B 首先检查列表 L_2。如果在列表 L_2 中已经存在项 (m_i,c_i,r'_i,h'_i)，B 将 h'_i 返回给 A 作为 (m_i,c_i,r'_i) 的 H_2 哈希值；否则，随机选取 $h'_i \in_R \mathbf{Z}_p^*$，将 (m_i,c_i,r'_i,h'_i) 添加到列表 L_2，并将 $H_2(m_i,c_i,r'_i)=h'_i$ 返回给 A。

③H_3 询问：A 关于 $c_i(1 \leqslant i \leqslant q_3)$ 的每一次询问，B 首先检查列表 L_3。如果在列表 L_3 中已经存在项 (c_i,ω_i)，B 将 ω_i 返回给 A 作为 c_i 的 H_3 哈希值；否则，随机选取 $\omega_i \in_R \mathbf{Z}_p^*$，将 (c_i,ω_i) 添加到列表 L_3，并将 $H_3(c_i)=\omega_i$ 返回给 A。

④密钥提取询问：对 A 关于 $ID_i(1 \leqslant i \leqslant q_E)$ 的密钥提取询问（假设已经做过关于 ID_i 的 H_1 询问，否则先执行 H_1 询问），B 从列表 L_1 中找出项 (ID_i,ε_i)。如果 $ID_i=ID^*$，B 宣告失败，算法终止；否则，B 计算 $\frac{1}{w_l+x}P=\frac{1}{\varepsilon_i+x}P=S_{ID_i}$，将 S_{ID_i} 返回给 A。

⑤签名询问：任何时候 A 可以选择消息 m、身份 ID 和协商信息 c，对 (ID,m,c) 进行密名询问（假设已经做过关于 ID 的 H_1 询问和关于 c 的 H_3 询问，否则先执行 H_1 询问和 H_3 询问）。B 从列表 L_1 中找出项 (ID,ε)，从列表 L_3 中找出项 (c,ω)；随机选取 $S' \in_R G_1,h' \in_R \mathbf{Z}_p^*$，计算 $r'=(e(S',\varepsilon Q+Q_{\text{pub}})e(P,Q)^{-h'})^{\omega^{-1}}$，如果 (m,c,r',h') 已经在列表 L_2 中，则重新选取 S' 和 h' 并计算 r'；将 (m,c,r',h') 加到列表 L_2 中。B 将 $\sigma=(m,c,r',S')$ 返回给 A。

3) 伪造。如果算法 B 没有终止，则 A 在没有做过 ID^* 的密钥提取询问和 (ID^*,m,c) 的签名询问的条件下，以一个不可忽略的概率对一个输入消息 (m,c)，输出一个身份 ID^* 对应的有效部分盲签名 $\sigma=(m,c,r',S')$。根据 Forking 引理[10]，通过对 A 哈希重放，B 可以获得对消息 (m,c) 的两个有效签名 $(ID^*,m,c,h'_1,\omega_1,r',S'_1)$ 和 $(ID^*,m,c,h'_2,\omega_2,r',S'_2)$，其中 $h'_1 \neq h'_2$。因为有效签名满足

$$r'^{H_3(c)}=e(S',H_1(ID)Q+Q_{\text{pub}})e(P,Q)^{-H_2(m,c,r')}=e(S',H_1(ID)Q+xQ)e(-H_2(m,c,r')P,Q)=e((H_1(ID)+x)S'-H_2(m,c,r')P,Q)$$

所以

$$r'^{\omega_1}=e((w^*+x)S'_1-h'_1P,Q)$$

$$r'^{\omega_2}=e((w^*+x)S'_2-h'_2P,Q)$$

进而

$$r'^{\omega_1\omega_2}=e(\omega_2((w^*+x)S'_1-h'_1P),Q)=e(\omega_1((w^*+x)S'_2-h'_2P),Q)$$

于是

$$\omega_2((w^*+x)S'_1-h'_1P)=\omega_1((w^*+x)S'_2-h'_2P)$$

即

$$(\omega_2h'_1-\omega_1h'_2)P=(w^*+x)(\omega_2S'_1-\omega_1S'_2)$$

所以

$$\frac{1}{w^*+x}P=(\omega_2h'_1-\omega_1h'_2)^{-1}(\omega_2S'_1-\omega_1S'_2)$$

记 $T^*=\frac{1}{w^*+x}P$，B 首先建立多项式 $\frac{f(z)}{z+w^*}=\sum_{j=0}^{q-2}c_jz^j+\frac{c_{-1}}{z+w^*}$，确定出系数 $c_i \in \mathbf{Z}_p^*(i=-1,0,\cdots,q-2)$，然后计算 $\sigma^*=\frac{1}{c_{-1}}\left(T^*-\sum_{i=0}^{q-2}c_i\psi(x^iH)\right)=\frac{1}{x+w^*}G$，最终，输出 $\left(w^*,\frac{1}{x+w^*}G\right)$ 作为 q-SDHP 问题的一个解。

4) 分析。下面分析 B 成功的概率。假设敌手 A 能够在 t 时间内，以 ε 的优势伪造盲签名。

A 没有执行过对 ID^* 的密钥提取询问的概率 $p_1 \geqslant (1-1/q_1)^{q_E}$；$A$ 选择 ID^* 作为伪造阶段的签名者身份的概率 $p_2 \geqslant 1/q_1$。则 X 成功的概率至少为：

$$\varepsilon'=\varepsilon p_1p_2 \geqslant \varepsilon\left(1-\frac{1}{q_1}\right)^{q_E}\left(\frac{1}{q_1}\right) \approx \frac{\varepsilon e}{q_1}$$

在 B 的计算时间方面，每次签名询问最多需要 2 次双线性对运算，所以 $t' \leqslant t+2q_St_e$，其中 t_e 表示计算一次双线性对运算所需要的时间。

5.1.3 盲性

定理 3 改进的基于身份的部分盲签名方案满足盲性。

证明 给定一个有效签名 (m,c,r',S') 和任一组部分盲签名发布过程中签名者保留下来的中间变量 (r,v,h,S)，考虑下列等式

$$r' = r^{\alpha} g^{\alpha\beta} v^{\alpha H_3^{-1}(c)} \tag{1}$$

$$h = \alpha^{-1} H_2(m,c,r') + \beta H_3(c) \tag{2}$$

$$S' = \alpha S \tag{3}$$

其中:$\alpha, \beta \in \mathbf{Z}_p^*$。

由式(3)知存在唯一的 $\alpha \in \mathbf{Z}_p^*$,即 $\alpha = \log_S S'$。进而由式(2)知存在唯一的 $\beta \in \mathbf{Z}_p^*$,即 $\beta = (h - \alpha^{-1} H_2(m,c,r')) H_3^{-1}(c)$。下面说明由式(2) ~ (3)确定的 α、β 满足式(1)。

因为 (m,c,r',S') 是一个有效签名,于是满足验证等式

$$e(S', H_1(ID)Q + Q_{\text{pub}}) = r'^{H_3(c)} g^{H_2(m,c,r')}$$

另一方面,部分盲签名发布过程中的中间变量 (r,v,h,S) 满足

$$S = (xH_3(c) + y + h) S_{ID}$$

于是

$$\begin{aligned} r' &= e(S', H_1(ID)Q + Q_{\text{pub}})^{H_3^{-1}(c)} g^{-H_2(m,c,r')H_3^{-1}(c)} = \\ &\quad e(aS, H_1(ID)Q + sQ)^{H_3^{-1}(c)} g^{-H_2(m,c,r')H_3^{-1}(c)} = \\ &\quad e(\alpha(xH_3(c) + y + h)(H_1(ID) + s) S_{ID}, \\ &\quad Q)^{H_3^{-1}(c)} g^{-H_2(m,c,r')H_3^{-1}(c)} = \\ &\quad e(\alpha(xH_3(c) + y + \alpha^{-1}H_2(m,c,r') + \beta H_3(c)) P, \\ &\quad Q)^{H_3^{-1}(c)} g^{-H_2(m,c,r')H_3^{-1}(c)} = \\ &\quad g^{\alpha(xH_3(c)+y+\alpha^{-1}H_2(m,c,r')+\beta H_3(c))H_3^{-1}(c)} g^{-H_2(m,c,r')H_3^{-1}(c)} = \\ &\quad g^{\alpha x + \alpha y H_3^{-1}(c) + \alpha\beta + H_2(m,c,r')H_3^{-1}(c)} g^{-H_2(m,c,r')H_3^{-1}(c)} = \\ &\quad g^{\alpha x} g^{\alpha\beta} g^{\alpha y H_3^{-1}(c)} = r^{\alpha} g^{\alpha\beta} v^{\alpha H_3^{-1}(c)} \end{aligned}$$

表明由式(2) ~ (3)确定的 α、β 满足式(1)。

因此,盲因子 $\alpha, \beta \in \mathbf{Z}_q^*$ 在有效的部分盲签名和任一组中间结果之间总是存在。所以,即使签名者具有无限的计算能力也不能将公布的部分盲签名与他的签名过程联系起来。也就是说,本文提出的改进方案满足盲性。

5.1.4　防篡改协商信息

一方面,改进方案的验证方程 $e(S', H_1(ID)Q + Q_{\text{pub}}) = r'^{H_3(c)} g^{H_2(m,c,r')}$ 中同时出现了 $H_3(c)$ 和 $H_2(m,c,r')$,验证者可以通过 $H_3(c)$ 和 $H_2(m,c,r')$ 验证公共信息 c 的合法性。假设恶意的签名请求者试图将协商的公共信息 c 篡改为 $\hat{c}$($\hat{c} \neq c$)。请求者无法利用 $\hat{h} = \alpha^{-1} H_2(m,\hat{c},r') + \beta H_3(c)$ 或者 $\hat{h} = \alpha^{-1} H_2(m,\hat{c},r') + \beta H_3(\hat{c})$ 生成能够通过验证的部分盲签名。事实上,

1) 如果请求者仅仅将 $H_2(m,c,r')$ 替换成 $H_2(m,\hat{c},r')$,则最后生成的签名满足

$$e(S', H_1(ID)Q + Q_{\text{pub}}) = r'^{H_3(c)} g^{H_2(m,\hat{c},r')} \neq r'^{H_3(\hat{c})} g^{H_2(m,\hat{c},r')}$$

$(m,\hat{c},r',S')$ 无法通过验证。

2) 如果请求者将 $h = \alpha^{-1} H_2(m,c,r') + \beta H_3(c)$ 替换成 $\hat{h} = \alpha^{-1} H_2(m,\hat{c},r') + \beta H_3(\hat{c})$,则最后生成的签名满足

$$e(S', H_1(ID)Q + Q_{\text{pub}}) = r^{\alpha H_3(c)} g^{\alpha\beta H_3(\hat{c})} v^{\alpha} g^{H_2(m,\hat{c},r')} \neq r'^{H_3(\hat{c})} g^{H_2(m,\hat{c},r')}$$

$(m,\hat{c},r',S')$ 也无法通过验证。

所以恶意的签名请求者无法通过第 3 章的方法篡改公共信息。

5.2　性能分析

将本文方案与 CHOW 方案[5]、李方案[8]、何方案[11]和闫方案[12]进行计算性能方面的比较。主要考虑计算消耗比较大的运算,有双线性对运算、群 G_1 或 G_2 中的标量乘运算、群 G_T 中的幂乘运算和 MapToPoint 哈希运算,分别用 P、M、E 和 H 表示。具体比较数据如表 1 所示。可以看出,本文方案仅使用了 1 次双线性对运算,而且不需要 MapToPoint 哈希运算,计算效率比 CHOW 方案[5]、何方案[11]和闫方案[12]高出很多;比李方案[8]仅仅多了 1 次群 G_T 中的幂乘运算,但克服了可篡改协商信息的缺陷。

表 1　本文方案与其他方案的计算复杂度比较

方案	发布		验证	总运算量
	签名者	请求者		
本文方案	1M+2E	1M+3E	1P+1M+2E	1P+3M+7E
CHOW 方案[5]	4M+1H	6M+1H	3P+1M+2H	3P+11M+4H
李方案[8]	1M+2E	1M+3E	1P+1M+1E	1P+3M+6E
何方案[11]	3M	3M	2P+2M+1H	2P+8M+1H
闫方案[12]	5M+1E	3M +3E	2P+2M+1E	2P+10M+5E

6　结语

本文对李明祥等[8]提出的基于身份的部分盲签名方案进行安全性分析,指出李等方案存在安全缺陷,即请求者在盲签名发布过程中可以篡改事先协商好的公共信息。分析了李方案[8]无法抵抗篡改协商信息攻击的原因,并对其进行了改进。安全性分析表明,改进方案在有效抵抗篡改公共消息攻击的同时,满足盲性并对自适应选择消息和身份攻击是存在性不可伪造的。同时,性能分析表明改进方案是一个效率较高的基于身份的部分盲签名方案。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments [C]// Proceedings of Crypto '82. New York: Plenum Press, 1983: 199 - 203.

[2] ABE M, FUJISAKI E. How to date blind signatures[C]// Proceedings of Asiacrypto '96, LNCS 1163. Berlin: Springer-Verlag, 1996: 244 - 251.

[3] SHAMIR A . Identity - based cryptosystems and signature schemes [C]// Proceedings of Crypto '84. Berlin: Springer-Verlag, 1984: 47 - 53.

[4] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]// Proceedings of Crypto '01, LNCS 2139, Berlin: Springer-Verlag, 2001: 213 - 229.

[5] CHOW S, HUI L, YIU S. Two improved partially blind signature schemes from bilinear pairings[C]// Proceedings of ACISP '05, LNCS 3574. Berlin: Springer-Verlag, 2005: 316 - 328.

[6] CHEN X, ZHANG F, LIU S. ID-based restrictive partially blind signatures and applications[J]. Journal of System and Software, 2007, 80(2): 164 - 171.

[7] 崔巍,辛阳,胡程瑜,等. 高效的基于身份的(受限)部分盲签名[J]. 北京邮电大学学报, 2008, 31(4): 53 - 57.

[8] 李明祥,赵秀明,王洪涛. 对一种部分盲签名方案的安全性分析与改进[J]. 计算机应用, 2010, 30(10): 2687 - 2690.

[9] CACHIN C, CAMENISCH J. Short signatures without random oracles[C]// Proceedings of Eurocrypt '04, LNCS 3027. Berlin: Springer-Verlag, 2004: 56 - 73.

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

[11] 何俊杰,王娟,祁传达. 安全高效的基于身份的部分盲签名方案[J]. 计算机应用, 2012, 32(5): 1388 - 1391.

[12] 闫东升. 一个新的高效的基于身份的部分盲签名方案[J]. 计算机工程与应用, 2008, 44(2): 137 - 139.