文章编号:1000－2367(2016)01－0155－06 DOI:10.16366/j.cnki.1000－2367.2016.01.028

对一个基于身份部分盲签名方案的分析与改进

刘二根[a],周华静[a,b],左黎明[a,b],王 霞[a,b]

(华东交通大学 a.理学院;b.系统工程与密码学研究所,南昌 330013)

摘 要:通过对一个基于身份的部分盲签名方案的分析,指出其存在公共信息被非法篡改的漏洞.针对这一问题,在原方案的基础上进行改进,提出一个新的部分盲签名方案.证明了改进方案的正确性、公共信息不可篡改性和部分盲性,并利用随机预言机模型证明了方案在适应性选择消息和身份攻击下是存在性不可伪造的.

关键词:双线性对;部分盲签名;随机预言机模型;存在性不可伪造

中图分类号:TP309 **文献标志码**:A

为了达到签名的匿名性,1983 年,Chaum[1]第一次提出了盲签名的概念.一个正确的盲签名方案需要满足匿名性和不可追踪性.但是,正是由于盲签名的这种完全匿名性及不可追踪性,容易造成签名的滥用.为了克服这一缺点,文献[2]首次提出部分盲签名的概念.部分盲签名是在盲签名的基础上,在待签名的消息中嵌入用户与签名者事先协商好的公共信息.文献[3]第一次比较详细地定义了部分盲签名的安全模型,给出一个具体的方案,并在随机预言机模型下证明了方案的安全性.文献[4]给出一个基于 RSA 困难问题的部分盲签名方案.文献[5]提出一个基于双线性对的部分盲签名方案.此后,对部分盲签名的研究不断深入.

文献[6]第一次提出基于身份的密码体制,解决了传统公钥证书密码体制下的证书管理问题.文献[7]结合基于身份密码体制和部分盲签名,提出了第一个基于身份的部分盲签名方案.文献[8]提出一个高效的基于身份的限制性部分盲签名方案.文献[9]指出文献[8]中的方案对于篡改公共信息攻击是不安全的,并给出改进方案.文献[10]发现文献[9]中存在同样的攻击,并给出改进方案.

本文通过对文献[10]的研究和分析,发现方案仍存在公共信息被非法篡改的问题.针对这一问题,分析问题存在的原因,并进行改进,提出一个新的部分盲签名方案.

1 预备知识

1.1 双线性对映射

定义 1 设一个素数 p,以 p 为阶的加法循环群 G_1 和乘法循环群 G_2,且存在映射 $e:G_1\times G_1\to G_2$ 满足下面 3 条性质,则称该映射为双线性对映射:

1) 双线性:群 G_1 中的任意两个元素 $P,Q\in G_1$,及任意的 $a,b\in {}_RZ_q^*$,有 $e(aP,bP)=e(P,Q)^{ab}$;

2) 非退化性:存在群 G_1 中的两个元素 $P,Q\in G_1$,使得 $e(P,Q)\neq 1$ 成立;

3) 可计算性:群 G_1 中的任意两个元素 $P,Q\in G_1$,存在有效的多项式时间可以计算出 $e(P,Q)$.

1.2 困难问题

定义 2 q-强 Diffie-Hellman 问题(q-SDHP) 设双线性映射 $e:G_1\times G_2\to G_T$,其中 G_1,G_2 为加法循环群,

收稿日期:2014-11-26;**修回日期**:2015-09-23.

基金项目:国家自然科学基金(11061014;61240025);江西省高校科技落地计划项目(KJLD12067);江西省教育厅科研项目(GJJ13339);华东交通大学校立科研基金项目(11JC04).

第 1 作者简介:刘二根(1965－),男,江西吉安人,华东交通大学教授,研究方向为图论及其应用,E-mail:leg_eg@sina.com.

通信作者:周华静(1991－),女,安徽天长人,华东交通大学硕士研究生,研究方向为密码学与信息安全,E-mail:642578515@qq.com.

G_T 为乘法循环群. φ 是 G_2 到 G_1 的同构映射,P,Q 分别是群 G_1 和群 G_2 的生成元,且 $\varphi(Q)=P$,已知$(P,Q,xQ,x^2Q,\cdots,x^qQ)$,其中 $x\in Z_p^*$ 未知,要求计算$\left(c,\frac{1}{x+c}P\right)$,$c\in Z_p^*$.

2 文献[10]方案分析

2.1 方案回顾

文献[10]给出了一个基于身份的部分盲签名方案,该方案由系统初始化(Setup)、用户密钥提取(UserKeyGen)、签名协议(Sign)及验证(Verify)4 个算法组成,具体描述如下.

1) 系统初始化 输入系统安全参数 1^k,密钥生成中心(KGC)生成阶为 p 的加法循环群 G_1 和 G_2,以及乘法循环群 G_T,其中,$p\leq 2^k$ 为素数. 选择 G_2 的生成元 $Q\in G_2$,作同构映射 $\varphi:G_2\to G_1$,计算 $P=\varphi(Q)\in G_1$,双线性对映射为 $e:G_1\times G_2\to G_T$. KGC 随机选取 $s\in {}_RZ_p^*$,作为系统主私钥,计算 $Q_p=sQ$ 作为系统主公钥,选择安全 Hash 函数:$H_1:\{0,1\}^*\to Z_p^*$,$H_2:\{0,1\}^*\times G_T\to Z_p^*$,$H_3:\{0,1\}^*\to Z_p^*$. 则 $params=\{G_1,G_2,G_T,P,Q,q,e,\varphi,Q_p,H_1,H_2,H_3\}$ 为系统公开参数,公开 $params$,保密 s.

2) 密钥提取 设签名者 A 的身份为 ID_A,KGC 计算签名者的私钥 $S_A=\frac{1}{H_1(ID_A)+s}P$,并通过秘密信道将 S_A 发送给签名者 A.

3) 签名协议 在该算法中需要由签名者和用户进行交互完成. 已知系统公开参数为 $params$,签名者 A 的身份 ID_A,私钥 S_A,消息 $m\in\{0,1\}^*$,c 为用户和签名者事先商量好的公共信息. 作预计算 $g=e(P,Q)$,签名者与用户进行如下交互:

3.1) 承诺 签名者首先随机选取 $x,y\in {}_RZ_p^*$,计算 $r=g^x$,$v=g^y$,将(r,v) 发送给用户;

3.2) 盲化 用户收到(r,v) 后,随机选择 $\alpha,\beta\in {}_RZ_q^*$ 作为盲因子,计算 $r'=r^\alpha g^{\alpha\beta}v^{\alpha H_3^{-1}(c)}$,$h=\alpha^{-1}H_2(m,c,r')+\beta H_3(c)$,并将 h 发送给签名者;

3.3) 签名 签名者在收到 h 后,进行盲签名,计算 $S'=(xH_3(c)+y+h)S_A$,将 S' 发送给用户;

3.4) 解盲 用户在收到盲签名 S' 后,进行解盲,计算 $S=\alpha S'$.

最终得到消息 m 的签名为 $\sigma=(m,c,r',S)$.

4) 验证 验证者收到签名 $\sigma=(m,c,r',S)$ 后,验证等式 $e(S,H_1(ID_A)Q+Q_p)=r'^{H_3(c)}g^{H_2(m,c,r')}$ 是否成立. 如果成立,接受签名,否则,拒绝.

2.2 方案分析

通过对上述方案的研究发现,方案中的公共信息可以被不诚实的用户非法替换,并且签名者和验证者无法察觉.

由于上述方案中,在签名等式中可以提取 $H_3(c)$,因此攻击者只需要在提取出 $H_3(c)$ 后再将 $H_3(c)$ 消去,并嵌入替换后的信息即可. 具体攻击过程如下.

设攻击者 F(即不诚实的用户),试图将事先与签名者 A 商量好的公共信息 c 替换成 $\hat{c}(c\neq\hat{c})$. 攻击者在收到签名者发送的承诺(r,v) 后,将 $\hat{c}$ 嵌入到 h 中,再令 $h^*=H_3^{-1}(c)h$,并发送 h^* 给签名者. 而签名者并不知道攻击者已经篡改了公共信息,因此签名者还是按照原来的公共信息 c 及签名方程进行签名,而攻击者要将篡改后的不合法信息 $\hat{c}$ 嵌入到签名中,需要进行下面交互过程:

1) 签名者 A 随机选取 $x,y\in {}_RZ_p^*$,计算 $r=g^x$,$v=g^y$,将(r,v) 发送给用户 F;

2) 用户随机选取 $\alpha,\beta\in {}_RZ_p^*$,计算 $r'=r^{\alpha H_3(c)}g^{\alpha\beta}v^\alpha$,$h=\alpha^{-1}H_2(m,\hat{c},r')+\beta H_3(\hat{c})$,$h^*=H_3^{-1}(\hat{c})h$ 将 h^* 发送给签名者;

3) 签名者收到 h^* 后,进行盲签名,计算 $S'=(xH_3(c)+y+h^*)S_A$,将 S' 发送给用户;

4) 用户收到 S' 后进行解盲:$S=\alpha H_3(\hat{c})S'$,最终得到消息的签名为 $\sigma=(m,\hat{c},r',S)$;

5) 验证者收到签名 σ 后,对其进行验证,具体过程如下,

$$e(S,H_1(ID_A)Q+Q_p)=e(\alpha H_3(\hat{c})S',H_1(ID_A)Q+Q_p)=e(\alpha H_3(\hat{c})(xH_3(c)+y+h^*)S_A,H_1(ID_A)Q+Q_p)=e(\alpha H_3(\hat{c})(xH_3(c)+y+h^*)S_A,(H_1(ID_A)+s)Q)=$$

$$e(P,Q)^{\alpha H_3(c)(xH_3(c)+y+h^*)} = (g^{\alpha})^{xH_3(c)H_3(c)+yH_3(c)+h} = r^{\alpha H_3(c)H_3(c)} v^{\alpha H_3(c)} g^{\alpha h} =$$
$$r^{\alpha H_3(c)H_3(c)} v^{\alpha H_3(c)} g^{\alpha\beta H_3(c)} g^{H_2(m,c,r')} = r'^{H_3(c)} g^{H_2(m,c,r')}.$$

即被不诚实用户 F 篡改过公共信息并嵌入后的签名可以通过验证等式.

3　方案改进

针对文献[10]中出现的公共信息被篡改的缺陷，在原方案的基础上提出改进方案. 其中系统初始化及密钥提取部分与原方案的相同，只在签名协议和验证部分作如下修改.

1) 签名协议　系统公开参数为 $params$，签名者 A 的身份 ID_A，私钥 S_A，消息 $m \in \{0,1\}^*$，假设 c 为用户和签名者事先商量好的公共信息. 作预计算 $g_1 = e(P,Q)$，$g_2 = e(P,Q_p)$，签名者 A 与用户 B 的交互如下：

1.1) 承诺　签名者 A 随机选取 $x,y \in {}_RZ_q^*$，并计算 $r_1 = g_1^x$，$r_2 = g_2^x$，$v_1 = g_1^y$，$v_2 = g_2^y$，将 (r_1,r_2,v_1,v_2) 发送给用户 B；

1.2) 盲化　用户 B 收到后 (r_1,r_2,v_1,v_2)，随机选择盲因子 $\alpha,\beta \in {}_RZ_p^*$，计算 $r'_1 = r_1^{\alpha} g_1^{\alpha\beta} g_1^{\alpha H_1^{-1}(ID)H_3^{-1}(c)} v_1^{\alpha H_3^{-1}(c)}$，$r'_2 = r_2^{\alpha} g_2^{\alpha\beta} v_2^{\alpha H_3^{-1}(c)}$，$R = r'^{H_1(ID)}_1 r'_2$，$h = \alpha^{-1}H_2(m,c,R) + \beta H_3(c)$，把 h 发送给签名者 A；

1.3) 签名　签名者 A 计算 $V_1 = (xH_3(c) + y + h)P + S_{ID}$，并将 V_1 发送给用户 B；

1.4) 解盲　用户 B 收到盲签名后，进行解盲，计算 $V = \alpha V_1$；

最后得到消息 m 的签名为 $\sigma = (m,c,R,V)$.

2) 验证　验证者收到签名对 $\sigma = (m,c,R;V)$，验证下面等式是否成立：

$$e(V,H_1(ID)Q + Q_p) = R^{H_3(c)} g_1^{H_1(ID)H_2(m,c,R)} g_2^{H_2(m,c,R)},$$

如果等式成立，签名有效，否则，签名无效.

4　改进方案的安全性分析

4.1　正确性

定理 1　改进后的基于身份部分盲签名方案是正确的.

证明

$$e(V,H_1(ID)Q + Q_p) = e(\alpha V_1, H_1(ID)Q + Q_p) = e(\alpha(xH_3(c) + y + h)P +$$
$$\alpha S_{ID}, H_1(ID)Q + Q_p) = e(\alpha(xH_3(c) + y + h)P, H_1(ID)Q + Q_p) e(\alpha S_{ID},$$
$$H_1(ID)Q + Q_p) = e(P,Q)^{\alpha(xH_3(c)+y+h)H_1(ID)} e(P,Q_p)^{\alpha(xH_3(c)+y+h)} e(P,Q)^{\alpha} =$$
$$g_1^{\alpha xH_3(c)H_1(ID)} g_1^{\alpha yH_1(ID)} g_1^{H_2(m,c,R)H_1(ID)} g_1^{\alpha\beta H_3(c)H_1(ID)} g_2^{\alpha xH_3(c)} g_2^{\alpha y} g_2^{H_2(m,c,R)} g_2^{\alpha\beta H_3(c)} g_1^{\alpha} =$$
$$r_1^{\alpha H_3(c)H_1(ID)} v_1^{\alpha H_1(ID)} g_1^{\alpha\beta H_3(c)H_1(ID)} g_1^{H_2(m,c,R)H_1(ID)} r_2^{\alpha H_3(c)} v_2^{\alpha} g_2^{H_2(m,c,R)} g_2^{\alpha\beta H_3(c)} g_1^{\alpha} =$$
$$r'^{H_3(c)H_1(ID)}_1 r'^{H_3(c)}_2 g_1^{H_2(m,c,R)H_1(ID)} g_2^{H_2(m,c,R)} = R^{H_3(c)} g_1^{H_1(ID)H_2(m,c,R)} g_2^{H_2(m,c,R)}.$$

即改进后的方案可以通过验证等式，因此满足正确性.

4.2　公共信息不可篡改

定理 2　改进后的方案可抵抗不诚实用户非法篡改公共信息的攻击.

证明　由于在原方案的签名 $V_1 = (xH_3(c) + y + h)S_A$ 中，不诚实用户可以通过提取 $H_3(c)$ 而嵌入非法公共信息 $\hat{c}$，因此无法抵抗篡改公共信息攻击. 而改进方案中，签名者的签名等式为 $V_1 = (xH_3(c) + y + h)P + S_{ID}$，攻击者无法完整地从该签名等式中提取 $H_3(c)$，因此，无法嵌入非法的公共信息. 即改进后的方案可抵抗篡改公共信息攻击.

4.3　部分盲性

定理 3　改进后的方案满足部分盲性.

证明　只需证明对于方案中任意产生的有效签名对 $\sigma = (m,c,V,S)$ 及签名过程中产生的中间数据 (V_1,h,R)，存在唯一的盲因子 $\alpha,\beta \in Z_p^*$，有下列等式成立：

$$V = \alpha V_1, \tag{1}$$

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

$$R = r'^{H_1(ID)}_1 r'_2. \tag{3}$$

由(1)式可得,$\alpha = \log_{V_1} V$,且由(2)式可得,$\beta = (h - \alpha^{-1} H_2(m,c,r'_1)) H_3^{-1}(c)$,下面证明把由(1)、(2)式得到的 α,β 代入(3)擘式,使得等式成立即可.

因为有效签名对 $\sigma = (m,c,R,V)$,一定能够通过验证等式,即

$$e(V, H_1(ID)Q + Q_p) = R^{H_3(c)} g_1^{H_1(ID)H_2(m,c,R)} g_2^{H_2(m,c,R)}.$$

因此,有:

$$R = e(V, H_1(ID)Q + Q_p)^{H_3^{-1}(c)} g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} = e(\alpha V_1, H_1(ID)Q +$$

$$Q_p)^{H_3^{-1}(c)} g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} = e(\alpha(xH_3(c) + y + h)P + \alpha S_{ID}, H_1(ID)Q +$$

$$Q_p)^{H_3^{-1}(c)} g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} = e(\alpha(xH_3(c) + y + h)P, H_1(ID)Q +$$

$$Q_p)^{H_3^{-1}(c)} g_1^{\alpha H_3^{-1}(c)} g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} = e(P,Q)^{(\alpha x H_3(c) + \alpha y + \alpha h) H_1(ID) H_3^{-1}(c)} \times$$

$$e(P,Q_p)^{(\alpha x H_3(c) + \alpha y + \alpha h) H_3^{-1}(c)} g_1^{\alpha H_3^{-1}(c)} g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} =$$

$$(r_1^{\alpha H_3(c)} v_1^{\alpha} g_1^{H_2(m,c,R)} g_1^{\alpha\beta H_3(c)})^{H_1(ID)H_3^{-1}(c)} (r_2^{\alpha H_3(c)} v_2^{\alpha} g_2^{H_2(m,c,R)} g_2^{\alpha\beta H_3(c)})^{H_3^{-1}(c)} g_1^{\alpha H_3^{-1}(c)} \times$$

$$g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} = r'^{H_1(ID)}_1 r'_2 g_1^{H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{H_2(m,c,R)H_3^{-1}(c)} \times$$

$$g_1^{-H_1(ID)H_2(m,c,R)H_3^{-1}(c)} g_2^{-H_2(m,c,R)H_3^{-1}(c)} = (r_1^{\alpha} g_1^{\alpha\beta} v_1^{\alpha H_3^{-1}(c)} g_1^{\alpha H_1^{-1}(ID)H_3^{-1}(c)})^{H_1(ID)} r_2^{\alpha} g_2^{\alpha\beta} v_2^{\alpha H_3^{-1}(c)} = r'^{H_1(ID)}_1 r'_2.$$

即(3)式成立.因此,对于改进方案中的任意一个有效的签名对及对应的中间变量,可以唯一确定一对盲因子 $\alpha,\beta \in Z_p^*$.所以即使存在具有无限计算能力的攻击者也无法将用户最终得到的消息签名对与签名者的签名过程联系起来.也就是说,改进后的方案具有部分盲性.

4.4 不可伪造性

定理 4 改进的基于身份部分盲签名在基于 q-SDHP 困难问题和随机预言机模型下对适应性选择消息和选择身份攻击具有存在性不可伪造.

类似于文献[10]中,本文基于 q-SDHP 困难问题和随机预言机模型有以下证明.

证明 假设存在一个攻击者 S 能够在多项式有界时间内以不可忽略的概率伪造一个签名并通过验证等式,那么存在一个挑战算法 C 可以解决 q-SDHP 困难问题,问题实例为,已知 $(G, a^0M, aM, a^2M, \cdots, a^qM)$,其中 $a \in Z_p^*$,且未知,则 C 需要计算出 $\left(c, \frac{1}{a+c}G\right)$,其中 $c \in Z_p^*$.C 通过与 S 的交互利用 S 解决困难问题,C 需要维护一些列表来回答 S 的询问,这些列表分别为 L_1, L_2, L_3, L_k, L_s,对应 H_1 询问,H_2 询问,H_3 询问,密钥询问和签名询问,且列表初始时都为空.设 ID^* 为攻击者想要伪造签名的目标用户的身份.

下面具体给出 C 如何利用 S 解决困难问题:

1) 系统设置 算法 C 首先生成系统公开参数:C 随机选取 $b_1, b_2, \cdots, b^{q-1} \in_R Z_p^*$,则多项式 $f(x) = \prod_{i=1}^{q-1}(x + b_i) = \sum_{i=0}^{q-1} t_i x^i, t_0, t_1, \cdots, t_{q-1} \in Z_p^*$.定义循环群 G_1, G_2 的生成元分别为 $P \in G_1, Q \in G_2$,且 $Q = \sum_{i=0}^{q-1} c_i(a^iM) = f(a)M, P = \varphi(Q) = \varphi(f(a)M) = f(a)\varphi(M) = f(a)G$,则系统主公钥为 $Q_p = \sum_{i=0}^{q-1} t_i(a^{i+1}M) = a\sum_{i=0}^{q-1} t_i(a^iM) = aQ$,其中 $Q_p \in G_2$,即用 a 模拟系统主私钥.

设多项式 $f_i(x) = \frac{f(x)}{x + b_i} = \sum_{j=0}^{q-2} w_{ij} x^j$,则有 $\sum_{j=0}^{q-2} w_{ij}\varphi(a^iM) = (\sum_{j=0}^{q-2} w_{ij} a^j)\varphi(M) = \frac{f(a)}{a+b_i}G = \frac{1}{a+b_i}P$,进而可以算出 $\left(b_i, \frac{1}{a+b_i}P\right), 1 \le i \le q-1$.

2) H_1 询问 列表 L_1 中每一项的格式为 (ID_i, h_{1i}),S 向 C 进行用户身份为 ID_i 的 H_1 询问,C 首先查询列表 L_1,如果列表中已经存在 (ID_i, h_{1i}) 的项,直接返回 h_{1i} 给 S;否则,如果 $ID_i = ID^*$ 时,C 随机选取 $b^* \in_R Z_p^*$,将 $h_{1i} = b^*$ 返回给 S;如果 $ID_i \neq ID^*$,将 $h_{1i} = b_i$ 返回给 S,且无论哪种情况,都将 (ID_i, h_{1i}) 添加到列表 L_1.

3) H_2 询问　列表 L_2 中每一项的格式为 (m_i, c_i, R_i, h_{2i})，S 向 C 进行签名消息为 m_i，公共信息为 c_i 的 H_2 询问，C 检查列表，如果列表中已经存在 (m_i, c_i, R_i, h_{2i}) 的项，那么直接返回 h_{2i} 给 S；否则，C 随机选取 $h_{2i} \in {}_RZ_p^*$，返回 h_{2i} 给 S，并将相应的 (m_i, c_i, R_i, h_{2i}) 添加到列表.

4) H_3 询问　列表 L_3 中每一项的格式为 (c_i, h_{3i})，S 向 C 进行公共信息为 c_i 的 H_3 询问，C 检查列表，如果列表中已经存在 (c_i, h_{3i}) 的项，则返回 h_{3i} 给 S；否则，C 随机选取 $h_{3i} \in {}_RZ_p^*$，返回 h_{3i} 给 S，并将 (c_i, h_{3i}) 添加到列表.

5) 密钥提取询问　列表 L_k 中每一项的格式为 (ID_i, S_i)，S 向 C 进行身份为 ID_i 的密钥提取询问，假设在此之前，S 已经进行过 H_1 询问，否则可以先进行 H_1 询问. 如果 $ID_i \neq ID^*$，C 查询列表 L_1，找到 h_{1i}，计算 $S_i = \frac{1}{a+h_{1i}}P$，将 S_i 返回给 S，并将 (ID_i, S_i) 添加到列表 L_k；否则 $ID_i = ID^*$ 时，C 拒绝回答，算法终止.

6) 签名询问　列表 L_s 中每一项的格式为 (m_i, c_i, R_i, V_i)，S 向 C 进行用户身份为 ID_i，签名消息为 m_i，公共信息为 c_i 的签名询问，假设在此之前已经进行过 H_1 询问和 H_3 询问，否则，先进行 H_1 询问和 H_3 询问. C 查询列表 L_1，得到相应的 h_{1i}，查询列表 L_3，得到相应的 h_{3i}，并随机选取 $V_i \in {}_RG_1$，$h_{2i} \in {}_RZ_p^*$，如果 h_{2i} 已经在列表 L_2 中，则重新选取，否则，计算 $R_i = (e(V_i, aQ+Q_p)e(P,Q)^{-h_{2i}})^{h_{3i}^{-1}}$，将 $\sigma = (m_i, c_i, R_i, V_i)$ 返回给攻击者 S，并将 (m_i, c_i, R_i, h_{2i}) 和 (m_i, c_i, R_i, V_i) 分别添加到列表 L_2 和 L_s.

经过上面的询问训练，攻击者 S 可以输出一个关于消息为 m，用户身份为 ID，公共信息为 c 的伪造签名，并且该签名可以通过验证等式，根据分叉引理[11] 可知，通过对哈希函数的重放，可以生成另一个有效的伪造签名，则两个签名分别为 $(ID, m, c, h_{2i}, h_{3i}, R, V)$ 和 $(ID, m, c, h'_{2i}, h'_{3i}, R', V')$，由于签名都是有效的，即都可以通过验证等式. 由于

$$\begin{aligned} R^{H_3(c)} &= e(V, H_1(ID)Q+Q_p)g_1^{-H_1(ID)H_2(m,c,R)}\ g_2^{-H_2(m,c,R)} = e(V, H_1(ID)Q+ \\ &aQ)e(P,Q)^{-H_1(ID)H_2(m,c,R)}e(P,Q_p)^{-H_2(m,c,R)} = e(V, H_1(ID)Q+ \\ &aQ)e(-H_1(ID)H_2(m,c,R)P, Q)e(-H_2(m,c,R)P, aQ) = \\ &e((H_1(ID)+a)V-(H_1(ID)H_2(m,c,R))P, Q), \end{aligned}$$

所以，有：$R^{h_{3i}} = e((b^*+a)V-(b^*h_{2i}+h_{2i})P, Q)$，$R^{h'_{3i}} = e((b^*+a)V'-(b^*h'_{2i}+h'_{2i})P, Q)$.

因此，

$$\begin{aligned} R^{h_{3i}h'_{3i}} &= e(h'_{3i}((b^*+a)V-(b^*h_{2i}+h_{2i})P), Q) = \\ &e(h_{3i}((b^*+a)V'-(b^*h'_{2i}+h'_{2i})P), Q). \end{aligned}$$

于是，$h'_{3i}((b^*+a)V-(b^*h_{2i}+h_{2i})P) = h_{3i}((b^*+a)V'-(b^*h'_{2i}+h'_{2i})P)$，即：$(h'_{3i}(b^*h_{2i}+h_{2i}) - h_{3i}(b^*h'_{2i}+h'_{2i}))P = (b^*+a)(h'_{3i}V - h_{3i}V')$.

所以，可计算出 $\frac{1}{b^*+a}P = (h'_{3i}(b^*h_{2i}+h_{2i}) - h_{3i}(b^*h'_{2i}+h'_{2i}))^{-1}(h'_{3i}V - h_{3i}V')$，多项式 $\frac{f(x)}{x+b^*} = \sum_{i=0}^{q-2}u_ix^i + \frac{u_{-1}}{x+b^*}$，给定系数 $u_i \in {}_RZ_q^*$ $(i=-1,0,1,\cdots,q-2)$，再计算 $\frac{1}{u_{-1}}\left(\frac{1}{b^*+a}P - \sum_{i=0}^{q-2}u_i\varphi(a^iM)\right) = \frac{1}{a+b^*}G$，最后输出 $\left(b^*, \frac{1}{a+b^*}G\right)$，即解决了 q-SDHP.

也就是说，如果一个挑战者 S 能够在多项式时间内通过向挑战算法 C 进行询问训练，以一个不可忽略的概率得到有效的签名，则存在一个多项式时间算法的挑战者 C 能够解决困难问题. 这与困难假设矛盾，因此，改进后的方案是存在性不可伪造的.

5　结束语

本文在文献[10]的基础上提出改进方案，并对方案进行安全性分析. 发现改进后的方案不仅可以抵抗篡改公共信息攻击，还满足部分盲签名的部分盲性. 在随机预言机模型下，证明了方案是基于 q-强 Diffie-Hellman 问题下不可伪造的.

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, LNCS1163. Berlin: Springer-Verlag,1996:244-251.

[3] Abe M, Okamoto T. Provably secure partially blind signatures[C]//Advances in Cryptology-Crypto 2000, LNCS 1880. Berlin: Springer-Verlag,2000:271-286.

[4] Chien H Y, Jan J K, Tseng Y M. RSA-based partially blind signature with low computation[C]//IEEE 8th International Conference on Parallel and Distributed Systems. 2001:385-389.

[5] Zhang F,Safavin R, Susilo W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings[C]//Proceedings of the 4th Internalional Conference on Cryptology. Heidelberg: Springer-Verlag,2003:71-84.

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

[7] Chow S, Hui L, Yiu S. Two improved partially blind signature schemes from bilinear pairings[C]//Proceedings of ACISP'05. Berlin: Springer-Verlag,2005:316-328.

[8] 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.

[9] 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.

[10] 何俊杰,孙 芳,祁传达.基于身份部分盲签名方案的分析与改进[J].计算机应用,2013,33(3):762-765.

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

[12] 文佳骏,左黎明,李 彪.一个高效的无证书代理盲签名方案[J].计算机工程与科学,2014(03):452-457.

[13] 刘二根,周华静,王 霞.一个可证安全的基于证书部分盲签名的改进方案[J].太原理工大学学报,2015,46(5):571-576.

Analysis and Improvement of an ID-based Partially Blind Signature Scheme

LIU Ergen[a], ZHOU Huajing[a,b], ZUO Liming[a,b], WANG Xia[a,b]

(a. School of Science; b. SEC Institute, East China Jiaotong University, Nanchang 330013, China)

Abstract: Based on the analysis of an ID-based partially blind signature, it is pointed out that the public information can be illegally tampered. In order to solve this problem, a new improved partially blind signature scheme should be proposed based on the original scheme. Then prove the correctness, resist public information replace attack, and partial blindness of the improved scheme, also proved the existentially unforgeable against adaptive chosen message and identity attacks under the random oracle.

Keywords: bilinear pairing; partially blind signature; random oracle model; existentially unforgeable