# 一种无证书盲签名方案的分析与改进

刘二根 王 霞* 周华静
(华东交通大学理学院 江西 南昌 330013)
(华东交通大学系统工程与密码学研究所 江西 南昌 330013)

**摘 要** 通过对黄茹芬等提出的无证书盲签名方案进行安全性分析,发现该方案存在公钥替换攻击的漏洞。针对该问题,提出一个能够抵抗公钥替换这一攻击的无证书盲签名方案,而且最终证明了改进的方案在随机预言机模型和 inv-CDH 困难问题假设下对于适应性选择消息攻击是存在性不可伪造的。

**关键词** 盲签名 不可伪造性 随机预言机模型 盲性

**中图分类号** TP309 **文献标识码** A DOI: 10.3969/j.issn.1000-386x.2017.02.056

## ANALYSIS AND IMPROVEMENT OF A CERTIFICATELESS BLIND SIGNATURE SCHEME

Liu Ergen Wang Xia* Zhou Huajing
(*School of Science, East China Jiaotong University, Nanchang 330013, Jiangxi, China*)
(*Institute of System Engineering and Cryptography, East China Jiaotong University, Nanchang 330013, Jiangxi, China*)

**Abstract** After analyzing the security of the blind signature scheme without certificates proposed by Huang Rufen et al, it is found that the scheme cannot resist public key replaced attack. Thus, a modified certificateless blind signature scheme which can resist public key attack is proposed, and the scheme is finally proved to be existentially unforgeable against adaptive chosen message in random oracle model and under inv-CDH complexity assumption.

**Keywords** Blind signature Unforgeability Random oracle model Blindness

## 0 引 言

1982 年,Chaum [1] 首先提出了盲签名这一概念。所谓盲签名,即是签名者虽然对消息签了名,但对他所签消息的内容是 未知的。正是由于这一特点,使得盲签名在电子支付和电子投票中得到广泛的应用。为了解决传统公钥密码体制中公钥证书的存储和管理问题,基于身份的密码体制被 Shamir 等 [2] 提出。在基于身份的密码体制中存在密钥托管这一问题,因为由可信中心 KGC 生成用户私钥。2003 年,无证书公钥密码体制由 Al-Riyami 等 [3] 提出,也相继出现了许多签名和加密方案 [4-6]。在无证书密码体制中,密钥生成中心只产生用户的部分私钥,但却无法知道长期私钥,解决了该体制中的密钥托管这一问题。将盲签名与无证书公钥密码体制相结合可以产生无证书盲签名,由此许多无证书盲签名方案 [7-13] 应运而生。2012 年,黄茹芬等 [14] 提出了一个基于 inv-CDH 问题和 q-SDH 问题的无证书盲签名方案,但通过分析发现其存在公钥替换攻击这一漏洞。本文提出了一个改进的方案,新方案不仅具有盲性,而且证明了在随机预言机模型下是存在性不可伪造的。

## 1 预备知识

### 1.1 双线性映射

设 $G_1$、$G_2$ 分别是由 $P$ 生成的 $p$ 阶加法群和乘法群,$e: G_1 \times G_1 \rightarrow G_2$ 是满足下面 3 个性质的双线性映射:

(1) 双线性: $e(aP,bQ) = e(P,Q)^{ab}$, $\forall P,Q \in$

收稿日期: 2015-09-05。国家自然科学基金项目(11361024,11261019,61472138,61263032)。刘二根,教授,主研领域: 图论及其优化。王霞,硕士生。周华静,硕士生。

$G_1$,$a,b \in Z_p^*$;

(2) 非退化性: 有 $P,Q \in G_1$,使得 $e(P,Q) \neq 1$;

(3) 可计算性: $\forall P,Q \in G_1$,能够计算出 $e(P,Q)$。

### 1.2 逆计算 Diffie-Hellman 困难(inv-CDH)问题

给定 $aP,P \in G$,其中 $a \in Z_p^*$ 未知,计算 $a^{-1}P$。

### 1.3 恶意攻击者模型

在无证书签名方案中,有 2 种类型的攻击者:

(1) 类型 1 的攻击者 $M_1$:无法知道系统主密钥,但可以替换用户公钥;

(2) 类型 2 的攻击者 $M_2$:能够知道系统主密钥,但不能替换用户的公钥。

## 2 文献[14]方案的分析

### 2.1 方案回顾

文献[14]方案包括下面 7 个具体算法:

1) 初始化

选取双线性对: $G_1 \times G_1 \to G_2$,群 $G_1$、$G_2$ 是以 $p$ 为阶加法群、乘法群,群 $G_1$ 的生成元为 $P$,计算 $g = e(P,P)$;选择系统主密钥 $s \in_R Z_p^*$,系统公钥 $P_{\text{pub}} = sP$,选择安全哈希函数 $H_1:\{0,1\}^* \to Z_p^*$ 和 $H_2:\{0,1\}^* \times G_1 \to Z_p^*$,系统公开参数 $params = \{G_1,G_2,e,p,P,P_{\text{pub}},g,H_1,H_2\}$,系统主密钥 $s$ 由 KGC 秘密保存。其中 $A$ 为签名者,$B$ 为用户。

2) 生成部分私钥

输入 $A$ 的身份 $ID$、系统主密钥 $s$ 和系统公开参数 $params$,得到部分私钥 $D_{ID} = \frac{1}{s+Q_{ID}}P$,其中 $Q_{ID} = H_1(ID)$。

3) 秘密值生成

$A$ 选取 $x_{ID} \in_R Z_p^*$ 作为秘密值。

4) 私钥生成

输入 $A$ 的部分私钥 $D_{ID}$ 和秘密值 $x_{ID}$,$A$ 产生自己的私钥 $SK_{ID} = (x_{ID},D_{ID})$。

5) 公钥生成

输入系统公开参数 $params$、秘密值 $x_{ID}$ 和部分私钥 $D_{ID}$,输出 $A$ 的公钥 $PK_{ID} = x_{ID}(P_{\text{pub}} + Q_{ID}P)$。

6) 签名过程

输入系统公开参数 $params$、消息 $m$、$A$ 的身份 $ID$ 和私钥 $SK_{ID}$,具体如下:

(1) 承诺: $A$ 选取 $r \in Z_p^*$,得到 $U = g^r$,把 $U$ 发给 $B$。

(2) 盲化: $B$ 选择 $\alpha,\beta \in_R Z_p^*$ 作为盲化因子,得到 $V = (Ug^{\alpha})^{\beta^{-1}}$,$h' = \beta h + \alpha \bmod p$,其中 $h = H_2(m,V)$,把 $h'$ 发给 $A$。

(3) 签名: $A$ 算出 $S' = \frac{r+h'}{x_{ID}}D_{ID}$,把 $S'$ 发给 $B$。

(4) 解盲: $B$ 得到 $S = \beta^{-1}S'$,关于消息 $m$ 的盲签名为 $\sigma = (S,h)$。

7) 验证

对于给定的消息签名对 $(m,S,h)$、签名者身份 $ID$ 和公钥 $PK_{ID}$,验证等式 $h = H_2(m,e(S,PK_{ID})g^{-h})$ 是不是成立,若成立则接受,不成立则拒绝。

### 2.2 攻击方法

**方法 1** 攻击者 $M$ 获取 $m$ 的一个有效签名 $\sigma = (S,h)$,$M$ 选择 $k \in Z_p^*$,得出 $PK_{ID}^* = kx_{ID}(P_{\text{pub}} + Q_{ID}P)$,把用户公钥 $PK_{ID}$ 替换为 $PK_{ID}^*$,计算 $S^* = k^{-1}S$,则 $\sigma^* = (S^*,h)$ 为身份 $ID$、公钥 $PK_{ID}^*$ 关于消息 $m$ 的有效盲签名。因为:

$$
\begin{aligned}
&H_2(m,e(S^*,PK_{ID}^*)g^{-h})\\
&= H_2(m,e(k^{-1}S,kx_{ID}(P_{\text{pub}} + Q_{ID}P))g^{-h})\\
&= H_2(m,e(k^{-1}\beta^{-1}\frac{r+h'}{x_{ID}}D_{ID},kx_{ID}(s+Q_{ID})P)g^{-h})\\
&= H_2(m,e(k^{-1}\beta^{-1}\frac{r+\beta h+\alpha}{x_{ID}}\frac{1}{s+Q_{ID}}P,kx_{ID}(s+Q_{ID})P)g^{-h})\\
&= H_2(m,e(\beta^{-1}(r+\beta h+\alpha)P,P)g^{-h})\\
&= H_2(m,(Ug^{\alpha})^{\beta^{-1}}) = H_2(m,V)
\end{aligned}
$$

那么,$\sigma^* = (S^*,h)$ 是一个有效的盲签名。

**方法 2** 攻击者随机选择 $\omega \in Z_p^*$,对于任意的消息 $m$,计算 $PK_{ID}^* = \omega P - H_1(ID)P$,用 $PK_{ID}^*$ 代替原有公钥 $PK_{ID}$。具体如下:

1) 承诺: $A$ 选取 $r \in Z_p^*$,得到 $U = g^r$,把 $U$ 发给 $B$。

2) 盲化: $B$ 选择 $\alpha,\beta \in_R Z_p^*$ 为盲化因子,得到 $V = (Ug^{\alpha})^{\beta^{-1}}$,$h' = \beta h + \alpha \bmod p$,其中 $h = H_2(m,V)$,把 $h'$ 发给 $A$。

3) 签名: $A$ 计算 $S' = \frac{r+h'}{\omega - H_1(ID)}P$,把 $S'$ 发给 $B$。

4) 解盲: $B$ 计算 $S^* = \beta^{-1}S'$,消息 $m$ 的盲签名为 $\sigma = (S^*,h)$。

事实上,$\sigma^* = (S^*,h)$ 是一个有效的盲签名。因为:

$$
\begin{aligned}
&H_2(m,e(S^*,PK_{ID}^*)g^{-h})\\
&= H_2(m,e(\beta^{-1}S',\omega P - H_1(ID)P)g^{-h})\\
&= H_2(m,e(\beta^{-1}\frac{r+h'}{\omega - H_1(ID)}P,\omega P - H_1(ID)P)g^{-h})\\
&= H_2(m,e(\beta^{-1}(r+\beta h+\alpha)P,P)g^{-h})\\
&= H_2(m,(Ug^{\alpha})^{\beta^{-1}}) = H_2(m,V)
\end{aligned}
$$

从以上的攻击方法得知，原方案之所以存在公钥替换攻击，是因为没有将用户公钥绑定到部分私钥上。如果用户公钥通过哈希函数绑定到部分私钥中，部分私钥 $D_{ID}$ 是不可伪造的，则不存在公钥替换攻击。

## 3 文献[14]方案的改进

只需要修改文献[14]方案的部分私钥生成算法、公钥生成算法、签名过程和验证算法，其他三个算法保持不变。

1）公钥生成

计算 $X_{ID} = x_{ID}^{-1}P$、$Y_{ID} = x_{ID}^{-1}P_{\text{pub}}$，$PK_{ID} = (X_{ID}, Y_{ID})$ 为签名者的公钥。任何人可以通过验证 $e(X_{ID}, P_{\text{pub}}) = e(Y_{ID}, P)$ 是否成立来判断公钥的有效性。

2）部分私钥生成

将原方案的部分私钥改为 $D_{ID} = \dfrac{1}{1 + sQ_{ID}}P$，其中 $Q_{ID} = H_1(ID, X_{ID}, Y_{ID})$。

3）签名

承诺、盲化和解盲与原方案相同，只需修改签名这一步。

签名：签名者计算 $S' = (r + h')x_{ID}D_{ID}$，把 $S'$ 发给用户。

4）验证

给定消息签名对 $(m, S, h)$、签名者身份 $ID$ 和公钥 $PK_{ID} = (X_{ID}, Y_{ID})$，验证等式 $h = H_2(m, e(S, X_{ID} + Q_{ID}Y_{ID})g^{-h})$ 是不是成立，若成立则接受，否则拒绝。

## 4 安全性分析与效率分析

### 4.1 方案的正确性

**定理 1** 改进的无证书盲签名方案是正确的。

**证明：**

$$\begin{aligned}
h &= H_2(m, e(S, X_{ID} + Q_{ID}Y_{ID})g^{-h}) \\
&= H_2(m, e(\beta^{-1}(r + h')x_{ID}D_{ID}, X_{ID} + Q_{ID}Y_{ID})g^{-h}) \\
&= H_2\left(m, e\left(\beta^{-1}(r + \beta h + \alpha)x_{ID}\frac{1}{1 + sQ_{ID}}P, x_{ID}^{-1}P + Q_{ID}x_{ID}^{-1}P_{\text{pub}}\right)g^{-h}\right) \\
&= H_2(m, e(\beta^{-1}(r + \beta h + \alpha)P, P)g^{-h}) \\
&= H_2(m, (Ug^{\alpha})^{\beta^{-1}}) = H_2(m, V)
\end{aligned}$$

### 4.2 具有盲性

**定理 2** 新方案具有盲性。

**证明：**给一个正确的消息签名对 $(m, S, h)$ 和任意一组盲签名发布过程中产生的视图 $(U, h', S')$，考虑下列等式：

$$S = \beta^{-1}S' \tag{1}$$

$$h' = \beta h + \alpha \bmod p \tag{2}$$

根据式(1)可以确定唯一的 $\beta \in Z_p^*$，其中 $\beta = \log_S S'$。同时，由式(2)可以确定唯一的 $\alpha \in Z_p^*$，$\alpha = h' - h\log_S S'$。因此，该方案具有盲性。

### 4.3 安全性分析

**定理 3** 改进的无证书盲签名方案不存在公钥替换攻击。

**证明：**因为 $D_{ID} = \dfrac{1}{1 + sQ_{ID}}P$，其中 $Q_{ID} = H_1(ID, X_{ID}, Y_{ID})$，那么将签名者的公钥对 $(X_{ID}, Y_{ID})$ 通过哈希函数绑定到部分私钥 $D_{ID}$ 中，部分私钥 $D_{ID}$ 是不可伪造的。因此，该方案不存在公钥替换攻击。

由于类型 2 的攻击更有破坏力，如果攻击成功其影响将是任何用户。本文只证明对类型 2 攻击下是可证安全的，类型 1 的证明过程相似（只是询问过程有些不同）。

**定理 4** 在随机预言机模型和 inv-CDH 困难问题假设下，新方案对攻击者 $M_2$ 在适应性选择消息攻击条件下是存在性不可伪造的。

**证明：**假设 $M_2$ 能以不可忽略的优势成功攻击该新方案，构造一个在概率多项式时间内能够解决 inv-CDH 问题的算法 $B$。

给定 $P, aP \in G_1, a \in Z_p^*$，为了计算 $a^{-1}P$，算法 $B$ 与 $M_2$ 进行交互，回答攻击者 $M_2$ 的 $H_1$、$H_2$ 随机预言询问、部分密钥询问、私钥询问、公钥询问。交互过程如下：

1）系统设置：算法 $B$ 生成系统公开参数 $params = \{G_1, G_2, e, q, P, g, H_1, H_2\}$，并发送系统公开参数和主密钥 $s$ 给攻击者 $M_2$，系统公钥设置为 $P_{\text{pub}} = sP$。列表 $L_1$、$L_2$、$L_P$、$L_{PK}$、$L_{SK}$、$L_S$ 分别用于应对 $M_2$ 对预言机的 $H_1$ 询问、$H_2$ 询问、部分密钥询问、公钥询问、私钥询问、签名询问。$B$ 通过维护表 $L_1$ 来响应 $M_2$ 的 $H_1$ 询问（$M_2$ 至多可以做 $q_{H_1}$ 次 $H_1$ 询问），表 $L_1$ 的表结构为 $(ID_i, X_i, Y_i, h_{1i})$。$B$ 通过维护表 $L_2$ 来响应 $M_2$ 的 $H_2$ 询问（$M_2$ 至多可以做 $q_{H_2}$ 次 $H_2$ 询问），表 $L_2$ 的表结构为 $(m, V, h_{2i})$。$B$ 通过维护表 $L_P$ 来响应 $M_2$ 的部分密钥询问（$M_2$ 至多可以做 $q_p$ 次部分密钥询问），表 $L_P$ 的表结构为 $(ID_i, D_{ID_i})$。$B$ 通过维护表 $L_{SK}$ 来响应 $M_2$ 的私钥询问（$M_2$ 至多可以做 $q_{sk}$ 次私钥询问），表 $L_{SK}$ 的表结构为 $(ID_i, x_{ID_i}, D_{ID_i})$。$B$ 通过维护表 $L_{PK}$ 来响应 $M_2$ 的公钥询问（$M_2$ 至多可以做 $q_{pk}$ 次公钥询问），表 $L_{PK}$ 的表结构为 $(ID_i, x_{ID_i}, X_{ID_i}, Y_{ID_i})$。$B$ 通过维护列表 $L_S$ 来响应 $M_2$ 关于 $(m, ID_i)$ 的签名询问（$M_2$ 至多可以做 $q_s$ 次签名询问），表 $L_S$ 的表结

构为$(m,ID_i,S,h_{2i})$。初始化所有表为空。假设攻击者$M_2$攻击的目标$ID$为$ID^*$,那么不能询问身份$ID^*$的长期私钥,用$a^{-1}$来模拟$ID^*$的长期私钥,对应的公钥为$X_{ID^*}=aP$、$Y_{ID^*}=aP_{pub}$。

2) $H_1$询问: 当$M_2$对$H_1(ID_i,X_i,Y_i)$询问时,若$(ID_i,X_i,Y_i,h_{1i})$在表$L_1$中存在,$B$则返回相应的值$h_{1i}$给$M_2$,否则$B$随机选取$h_{1i}\in Z_q^*$返回给$M_2$,并将$(ID_iX_i,Y_i,h_{1i})$添加到表$L_1$中。

3) $H_2$询问: 当$M_2$对$H_2(m,V)$询问时,若$(m,V)$在表$L_2$中存在,$B$则返回相应的值$h_{2i}$给$M_2$,否则$B$随机选取$h_{2i}\in Z_q^*$返回给$M_2$,并将$(m,V,h_{2i})$添加到表$L_2$中。

4) 公钥询问: 当$B$收到关于$ID_i$的公钥询问时:

(1) 如果$ID_i\neq ID^*$,若$(ID_i,x_{ID_i},X_{ID_i},Y_{ID_i})$在表$L_{PK}$中存在,则返回相应的值$(X_{ID_i}Y_{ID_i})$给$M_2$。若不存在,随机选取$x_i\in Z_p^*$,计算$X_{ID_i}=x_{ID_i}^{-1}P$、$Y_{ID_i}=x_{ID_i}^{-1}P_{pub}$,将$(ID_i,x_{ID_i},X_{ID_i},Y_{ID_i})$添加到表$L_{PK}$中。

(2) 如果$ID_i=ID^*$,用$a^{-1}$来模拟$ID^*$的长期私钥,公钥$X_{ID^*}=aP$、$Y_{ID^*}=aP_{pub}$,将$(ID^*,\perp,X_{ID^*},Y_{ID^*})$添加到表$L_{PK}$中并返回$(X_{ID^*},Y_{ID^*})$给$M_2$。

5) 部分密钥询问: 当$B$收到$M_2$关于$ID_i$部分密钥查询时,若$(ID_i,D_{ID_i})$在表$L_P$中存在,则返回相应的值$D_{ID_i}$给$M_2$,否则$B$先询问表$L_1$提取$h_{1i}$,然后计算$D_{ID_i}=\frac{1}{1+sh_{1i}}P$,将$(ID_i,D_{ID_i})$的值添加到表$L_P$中并返回值$D_{ID_i}$给$M_2$。

6) 私钥询问: 当$B$收到关于$ID_i$的私钥询问时:

(1) 如果$ID_i\neq ID^*$,若$(ID_i,x_{ID_i},D_{ID_i})$在表$L_{SK}$中存在,则返回相应的值$x_{ID_i}$给$M_2$。若不存在,$B$查询表$L_P$得到$D_{ID_i}$,查询表$L_{PK}$得到$x_{ID_i}$,将$(ID_i,x_{ID_i},D_{ID_i})$添加到表$L_{SK}$中并将$x_{ID_i}$返回给$M_2$。若表$L_{SK}$和$L_P$中不存在,随机选择$x_{ID_i}\in Z_p^*$,计算$X_{ID_i}=x_{ID_i}^{-1}P$、$Y_{ID_i}=x_{ID_i}^{-1}P_{pub}$,$B$询问表$L_1$提取$h_{1i}$,然后计算$D_{ID_i}=\frac{1}{1+sh_{1i}}P$,将$(ID_i,x_{ID_i},D_{ID_i})$添加到表$L_{SK}$中并返回$x_{ID_i}$给$M_2$。

(2) 如果$ID_i=ID^*$,算法终止。

7) 签名询问: 当$B$收到关于$(m,ID_i)$的签名询问时:

(1) 如果$ID_i\neq ID^*$,$B$首先询问表$L_1$、$L_{SK}$和$L_{PK}$,然后随机选取$r\in Z_p^*$,计算$U=g^r$,并将公钥对$(X_{ID_i},Y_{ID_i})$和$U$发送给$M_2$。$M_2$选择盲化因子$\alpha,\beta\in Z_p^*$,计算$V=(Ug^{\alpha})^{\beta^{-1}}$,然后查询列表$L_2$,得到$h=H_2(m,V)$,再计算$h'=\beta h+\alpha \bmod p$。$B$计算$S'=(r+h')x_{ID_i}D_{ID_i}$,并将$S'$发送给$M_2$。$M_2$计算$S=\beta^{-1}S'$,输出消息$m$的盲签名$\sigma=(S,h)$,将$(m,ID_i,S,h)$添加到表$L_s$并将签名$\sigma=(S,h)$返回给$M_2$。

(2) 如果$ID_i=ID^*$,$B$首先进行$H_1$询问和公钥询问,得到$Q_{ID^*}$和$(X_{ID^*},Y_{ID^*})$。$B$随机选择$S_i,h_i\in Z_q^*$,若$(m,e(S_i,X_{ID^*}+Q_{ID^*}Y_{ID^*})g^{-h_i},h_{2i})$在表$L_2$中,则重新选取$S_i,h_i\in Z_q^*$,否则令$H_2(m,e(S_i,X_{ID^*}+Q_{ID^*}Y_{ID^*})g^{-h_i})=h_i$,最后将$\sigma=(S_i,h_i)$发送给$M_2$。

若算法$B$没有停止,那么$M_2$在没有询问$ID^*$的私钥和$(ID^*,m^*)$的签名的情况下,能够以一个不可忽略的概率对消息$m^*$输出一个有效的签名$\sigma=(S,h)$。根据分叉引理,对$M_2$哈希重放,$B$可以得到关于$m^*$的两个有效$(ID^*,m^*,S,h)$和$(ID^*,m^*,S',h')$,$h\neq h'$。有效的签名满足: $e(S,X_{ID^*}+h^*Y_{ID^*})g^{-h}=V$,$e(S',X_{ID^*}+h^*Y_{ID^*})g^{-h'}=V$,其中$h^*=H_1(ID^*)$。于是有: $e(S,X_{ID^*}+h^*Y_{ID^*})g^{-h}=e(S',X_{ID^*}+h^*Y_{ID^*})g^{-h'}$。由$h\neq h'$,可以得到: $a^{-1}P=(S-S')(1+h^*s)(h-h')^{-1}$。

因此,在已知$P$、$aP$,其中$a\in Z_p^*$未知的情况下,$B$成功计算出了$a^{-1}P$,inv-CDH 问题得到了解决。新方案对攻击者$M_2$在适应性选择消息攻击条件下的存在性不可伪造是与 inv-CDH 困难问题等价的。

## 5　性能分析

本文预先计算$g=e(P,P)$,并将其作为系统参数公布,解决了对运算比较费时的问题,签名过程不需要对运算,验证过程只需要一次对运算。本文的方案是在文献[14]方案的基础上改进的,改变了签名者的公钥产生过程,部分私钥产生过程中将公钥嵌入到哈希函数中,签名过程中只将$S'=\frac{r+h'}{x_{ID}}D_{ID}$修改为$S'=(r+h')x_{ID}D_{ID}$,验证过程中只修改验证等式$h=H_2(m,e(S,PK_{ID})g^{-h})$为$h=H_2(m,e(S,X_{ID}+Q_{ID}Y_{ID})g^{-h})$。计算复杂度基本没有增加,但是却能够抵抗公钥替换攻击。表 1 为本文提出的方案与文献[14]和文献[12]方案的性能比较。表中的$M$代表点乘运算,$E$代表幂运算,$P$代表双线性对运算。在验证阶段,改进方案的运行时间比文献[14]多了一次点乘运算,计算复杂度明显低于文献[12]中的方案。同时,改进的方案能够抵抗公钥替换攻击。

表 1 本方案与其他方案的性能比较

| 方案 | 签名过程 | 验证过程 | 是否抵抗公钥替换 |
|---|---|---|---|
| 本文方案 | $3E + 4M$ | $1E + 2M + 1P$ | 是 |
| 文献[14] | $3E + 4M$ | $1E + 1M + 1P$ | 否 |
| 文献[12] | $2E + 3M$ | $3E + 4M + 1P$ | 否 |

## 6 结 语

通过对黄茹芬等提出的无证书盲签名方案进行安全性分析，发现该方案不能抵抗公钥替换攻击。由此提出了一个改进的无证书盲签名方案，将签名者的公钥绑定到部分私钥中，有效地解决了原方案中存在的公钥替换攻击的问题，并证明了在随机预言机模型和 inv-CDH 困难问题假设下对于适应性选择消息攻击是存在性不可伪造的。同时该方案是基于无证书密码体制的，克服了证书管理和密钥托管问题。

## 参 考 文 献


[1] Chaum D. Blind signatures for untraceable payments [C] //Advances in Cryptology: Proceedings of Crypto'82, 1983: 199-203.

[2] Shamir A. Identity-based cryptosystems and signatures schemes [C] //Proceedings of Crypto'84 on Advances in Cryptology. New York: Springer-Verlag, 1985: 47-53.

[3] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C] //Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, 2003: 452-473.

[4] Choi K Y, Park J H, Hwang J Y, et al. Efficient certificateless signature schemes [C] //Proceedings of the 5th International Conference on Applied Cryptography and Network Security, 2007: 443-458.

[5] 王圣宝，刘文浩，谢琪. 无双线性配对的无证书签名方案 [J]. 通信学报，2012，33(4)：93-98.

[6] Zhang L, Zhang F. Certificateless signature and blind signature [J]. Journal of Electronics (China), 2008, 25(5): 629-635.

[7] 魏萍，陈海滨，杨晓元. 一个安全无证书的盲签名方案 [J]. 计算机工程与应用，2011，47(5)：96-97.

[8] 杨晓元，梁中银，郭耀，等. 一个高效的无证书盲签名方案 [J]. 南京邮电大学学报(自然科学版)，2009，29(3)：37-42.

[9] 周才学. 三个无证书签名方案的密码学分析与改进 [J]. 计算机工程，2012，38(19)：114-118.

[10] 张玉磊，王彩芬，张永洁，等. 基于双线性对的高效无证书签名方案 [J]. 计算机应用，2009，29(5)：1330-1333.

[11] 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，2014，36(3)：452-457.

[12] 梁红梅，黄振杰. 高效无证书签名方案的安全性分析和改进 [J]. 计算机应用，2010，30(3)：685-687，698.

[13] 何俊杰，王娟，祁传达. 对一个无证书盲签名方案的攻击与改进 [J]. 数学的实践与认识，2014，44(4)：123-128.

[14] 黄茹芬，农强，黄振杰. 一个高效的无证书盲签名方案 [J]. 计算机工程，2013，39(2)：130-136.


(上接第 289 页)


[5] 王卫平，王金辉. 基于 Tag 和协同过滤的混合推荐方法 [J]. 计算机工程，2011，37(14)：34-35.

[6] Xu J, Zheng X, Ding W. Personalized recommendation based on reviews and ratings alleviating the sparsity problem of collaborative filtering [C] //e-Business Engineering (ICEBE), 2012 IEEE Ninth International Conference on, 2012: 9-16.

[7] Yang X G. Collaborative filtering algorithm based on preference of item properties [M]. Foundations of Intelligent Systems. Springer Berlin Heidelberg, 2014: 1143-1149.

[8] 邢春晓，高凤荣，战思南，等. 适应用户兴趣变化的协同过滤推荐算法 [J]. 计算机研究与发展，2007，44(2)：296-301.

[9] 邱璐. 协同过滤算法中的相似度计算与用户兴趣变化问题研究及应用 [D]. 北京：北京邮电大学，2015.

[10] 荣辉桂，火生旭，胡春华，等. 基于用户相似度的协同过滤推荐算法 [J]. 通信学报，2014，35(2)：16-24.

[11] 贾冬艳，张付志. 基于双重邻居选取策略的协同过滤推荐算法 [J]. 计算机研究与发展，2013，50(5)：1076-1084.

[12] 邓晓懿. 移动电子商务个性化服务推荐方法研究 [D]. 大连：大连理工大学，2012.

[13] 韦素云，业宁，吉根林，等. 基于项目类别和兴趣度的协同过滤推荐算法 [J]. 南京大学学报(自然科学版)，2013，49(2)：142-149.

[14] Su H, Lin X, Yan B, et al. The collaborative filtering algorithm with time weight based on mapReduce [M]. Big Data Computing and Communications. Springer International Publishing, 2015.

[15] Yang L, Hu Y. An improved collaborative filtering algorithm based on the constraint model of confidence [J]. Journal of Computational Information Systems, 2015, 11(8): 3001-3009.

[16] 嵇晓声，刘宴兵，罗来明. 协同过滤中基于用户兴趣度的相似性度量方法 [J]. 计算机应用，2010，30(10)：2618-2620.

[17] 于洪，李转运. 基于遗忘曲线的协同过滤推荐算法 [J]. 南京大学学报(自然科学版)，2010，46(5)：520-527.