

# 一种无证书签名方案的分析与改进

史华婷, 万中美

(河海大学理学院, 江苏南京 211100)

**摘要:**无证书公钥密码体制虽然解决了基于身份密码体制中的密钥托管问题,但是当随机预言模型被具体的哈希函数实例化时,将会导致无证书签名方案在现实生活中的不安全。标准模型下的证明为无证书签名方案提供充分的保障。通过两种具体的攻击方法,对李艳琼提出的标准模型下的无证书签名方案进行安全性分析,指出其不能抵抗公钥替换攻击和恶意的KGC攻击。针对存在的安全问题,对原来的无证书签名方案进行改进,并加强方案与公钥、私钥等参数的联系,从而达到安全要求。在标准模型下,基于NGBDH问题和Many-DH问题的困难性假设,改进的无证书签名方案在自适应选择消息攻击下是存在性不可伪造的。与李艳琼提出的方案相比,改进后的无证书签名方案在安全性上有了更高的优势。

**关键词:**无证书签名;标准模型;NGBDH问题;Many-DH问题

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2017)05-0133-05

**doi:**10.3969/j.issn.1673-629X.2017.05.028

## Analysis and Improvement of a Certificateless Signature Scheme

SHI Hua-ting, WAN Zhong-mei

(College of Science, Hohai University, Nanjing 211100, China)

**Abstract:** Although certificateless cryptography solves the key escrow problem in the identity-based public cryptography, a CLS scheme may not be secure in the real world when the random oracles are instantiated by concrete hash functions. The security of certificateless signature scheme can be proved adequately in the standard model. Security analysis has been carried out for Li Yanqiong's CLS scheme by detailed method attack, whose results show that the scheme is not secure against key replacement attacks and malicious KGC attack. In view of the existing secure problems, an improved certificateless signature scheme has been proposed, which enhances the contact with the public key, private key and other parameters, to achieve the safety requirements. Based on the NGBDH problem and Many-DH problem in the standard model, an improved CLS scheme is proved secure against existentially under adaptive chosen message attack. Compared with Li Yanqiong's scheme, the improved CLS scheme has higher advantages in the security.

**Key words:** certificateless signature; standard model; NGBDH problem; Many-DH problem

## 0 引言

为了解决基于身份密码体制<sup>[1]</sup>中的密钥托管问题, Al-Riyami 和 Paterson<sup>[2]</sup>在2003年亚密会议上引入了无证书公钥密码体制的概念。无证书公钥密码体制区别于基于身份密码体制,它需要一个可信密钥生成中心(Key Generation Center, KGC),负责生成用户的部分私钥。在无证书公钥密码体制中,私钥不是由KGC单独生成的,需要用户随机选择一个秘密值和部分私钥组合,才能生成完整的私钥,这就克服了密钥托管问题。

Yum 和 Lee<sup>[3]</sup>在2004年提出了一个由两种属性

构建的无证书签名的通用结构。但是, Hu 和 Wong<sup>[4]</sup>发现该方案是不安全的,其不能抵抗第一类公钥替换攻击,并对其进行了改进。为了提高计算效率, Zhang 等<sup>[5]</sup>提出了一种安全的无证书签名方案。文献[6]给出了一类无证书签名方案的构造方法,并对其进行了安全性证明。文献[7]提出了一种高效的签名方案,但是文献[8]发现其是不安全的,并提出了改进方案。文献[9]对文献[8]在安全性和效率上存在的不足进行改进,提出了不使用双线性对的签名方案。

文献[10]指出,随机预言模型下的可证安全并不是严格意义上的安全,标准模型可以保持随机预言模

收稿日期:2016-05-24

修回日期:2016-09-08

网络出版时间:2017-03-07

基金项目:国家自然科学基金资助项目(61103183)

作者简介:史华婷(1991-),女,硕士,研究方向为密码学理论与技术;万中美,副教授,硕士生导师,研究方向为信息安全、密码学理论与技术。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20170307.0921.048.html>

型中的安全特性。基于以上问题, Liu 等<sup>[11]</sup>在 2007 年亚密会议上提出了第一个标准模型下的无证书签名方案。随后, Xiong<sup>[12]</sup>、Yu<sup>[13]</sup>等又对 Liu 等<sup>[11]</sup>的提出方案进行改进。文献[14]提出了一种标准模型下的无证书短签名方案, 并进行了安全性分析。李艳琼<sup>[15]</sup>根据文献[16]构造了一种新的无证书签名方案, 但是它不能抵抗两类攻击。

针对李艳琼的方案进行了安全分析, 给出了两种具体的攻击方法, 指出其不能抵抗公钥替换攻击和恶意的 KGC 攻击, 并提出了一种改进的无证书签名方案。基于 NGBDH 问题和 Many-DH 问题的困难性假设, 证明改进方案在标准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  $G_1$  是由  $g$  产生的阶为素数  $q$  的乘法循环群,  $G_2$  为同阶乘法循环群。双线性映射  $e: G_1 \times G_1 \rightarrow G_2$ , 满足以下条件:

- (1) 双线性: 对任意  $a, b \in Z_q^*$ , 有  $e(g^a, g^b) = e(g, g)^{ab}$ 。
- (2) 非退化性:  $e(g, g) \neq 1$ 。
- (3) 可计算性: 存在有效的算法计算  $e$ 。

### 1.2 困难性问题

定义 1: NGBDH 问题 (Non pairing-based Generalized Bilinear Diffie-Hellman)。设  $G$  是由  $g$  产生的阶为素数  $q$  的乘法循环群。已知  $(g, g^\alpha, g^\beta)$ ,  $\alpha, \beta \in Z_q^*$ , 求  $(g^{\alpha\beta\gamma}, g^\gamma)$ 。

定义 2: Many-DH 问题 (Many Diffie-Hellman)。设  $G$  是由  $g$  产生的阶为素数  $q$  的乘法循环群。已知  $(g, g^\alpha, g^\beta, g^\gamma, g^{\alpha\beta}, g^{\alpha\gamma}, g^{\beta\gamma})$ ,  $\alpha, \beta, \gamma \in Z_q^*$ , 求  $g^{\alpha\beta\gamma}$ 。

设算法  $C$  解决  $G$  上的 Many-DH 问题的概率  $\varepsilon$  为:

$$\Pr[A(g, g^\alpha, g^\beta, g^\gamma, g^{\alpha\beta}, g^{\alpha\gamma}, g^{\beta\gamma}) = g^{\alpha\beta\gamma}] \geq \varepsilon$$

## 2 李艳琼方案的安全性分析

### 2.1 攻击 1

对方案实施如下恶意的 KGC 攻击:

(1) 在系统参数设置阶段, KGC 任意选取  $a', a_i \in Z_q^*$ , 设  $m' = g^{a'}$ ,  $m_i = g^{a_i}$  ( $i = 1, 2, \dots, n_m$ ), 其他参数正常生成。

(2) 窃听在公钥  $pk_{ID^*}$  下身份  $ID^*$  对消息  $m$  的签名  $\sigma = (V, R_u, R_m)$ , 在相同公钥下 KGC 生成身份  $ID^*$  对任意  $m^*$  的有效签名。

任取  $r \in Z_q^*$ , 则  $V^* = V(R_m)^{-(a'+\sum_{j \in M^*} a_j)} (m' \prod_{j \in M^*} m_j)^r$ ,  $R_u^* = R_u$ ,  $R_m^* = g$ 。其中,  $M = \{j \mid \tilde{m}[j] = 1, 1 \leq j \leq$

$n_m\}$ ,  $M^* = \{j \mid m^*[j] = 1, 1 \leq j \leq n_m\}$  ( $m^* = H_m(m^*)$ ), 且  $F_m(m^*) = m' \prod_{j \in M^*} m_j$ ,  $F_m(\tilde{m}) = g^{(a'+\sum_{j \in M} a_j)}$ 。

因为满足:

$$e(V^*, g) = e(V, g) e((R_m)^{-(a'+\sum_{j \in M} a_j)}, g) e((m' \prod_{j \in M^*} m_j)^r, g) = e(g_2, pk_2) e(g_2, R_u)^{u'+\sum_{i \in U} u_i} e(m' \prod_{j \in M^*} m_j, R_m^*)$$

所以伪造的签名  $\sigma^* = (V^*, R_u^*, R_m^*)$  是有效的, 即该方案不能抵抗恶意的 KGC 攻击。

### 2.2 攻击 2

敌手  $A_1$  用新公钥伪造用户  $ID^*$  的签名:

(1)  $A_1$  任意选取  $x \in Z_q^*$ , 替换用户的公钥为  $pk_{ID^*} = (g^x, g^x, g_2^x)$ 。

(2) 对任意的消息  $m^*$ , 敌手  $A_1$  任意选取  $r_u, r_m \in Z_q^*$ , 计算  $\sigma^* = (g_2^x g_2^{x r_u (u' + \sum_{i \in U} u_i)} (m' \prod_{j \in M^*} m_j)^{r_m}, g^{x r_u}, g^{r_m})$ 。

显然, 伪造的签名  $\sigma^*$  满足验证算法, 所以该方案不能抵抗公钥替换攻击。

## 3 新的无证书签名方案

1) 系统参数设置算法: 给定安全参数  $k$ , KGC 执行以下步骤:

(1) 随机选择两个阶为素数  $q$  的乘法循环群  $G_1, G_2$ ,  $g$  为  $G_1$  的生成元。存在一个双线性映射  $e: G_1 \times G_1 \rightarrow G_2$ 。

(2) 随机选取  $\alpha \in Z_q^*$ ,  $g_2 \in G_1$ , 令  $g_1 = g^\alpha$ , 并设置系统主密钥  $msk = g_2^\alpha$ 。

(3) 随机选取  $u', m_0, m_1, v \in G_1$ , 向量  $U = (u_i) \in G^n$ , 定义两个抗碰撞 Hash 函数  $H_0: \{0, 1\}^* \rightarrow \{0, 1\}^n$ ,  $H: \{0, 1\}^* \times G_1^6 \rightarrow Z_q^*$ 。

(4) 取  $G_1$  中的点  $Q$ , 定义函数  $f(Q)$ , 如果  $Q$  的  $x$  坐标为奇数, 则  $f(Q) = 1$ ; 否则,  $f(Q) = 0$ 。

系统的公开参数为  $params = \{G_1, G_2, e, g, g_1, g_2, u', m_0, m_1, v, U, H_0, H, f\}$ 。

2) 部分私钥生成算法: 对于给定的身份  $ID$ , KGC 首先计算  $H_0(ID)$ ,  $u[i]$  表示  $u = H_0(ID)$  的第  $i$  比特且  $u_{ID} = \{i \mid u[i] = 1, 1 \leq i \leq n\}$ 。KGC 随机选取  $r \in Z_q^*$ , 计算部分私钥  $psk_{ID} = (psk_{ID,1}, psk_{ID,2}) = (g_2^{u' \prod_{i \in u_{ID}} u_i}, g^r)$ 。

3) 用户密钥生成算法: 身份为  $ID$  的用户随机选取  $x_{ID} \in Z_q^*$  为秘密值, 则公钥为  $pk_{ID} = (pk_{ID,1}, pk_{ID,2}) = (g_1^{x_{ID}}, v^{x_{ID}})$ 。

4) 私钥生成算法: 身份为  $ID$  用户随机选择  $r_u \in Z_q^*$ , 并设置私钥为  $sk_{ID} = (psk_{ID,1} F(u)^{r_u}, psk_{ID,2} g^{r_u}) =$

$(sk_{ID,1}, sk_{ID,2})$ 。

5) 签名算法: 用户随机选取  $r_m \in Z_q^*$ , 计算身份为 ID 的用户对消息  $m$  的签名  $V = sk_{ID,1} (pk_{ID,2}^h m_b)^{r_m}$ ,  $R_u = sk_{ID,2}$ ,  $R_m = g^{r_m}$ 。其中,  $b = f(R_u)$ ,  $h = H(m, ID, pk_{ID,2}, R_u, R_m, sk_{ID,2}, g^{r_m}, m_b, v)$ 。

6) 验证算法: 验证者使用 params 和  $pk_{ID}$  对  $(m, \sigma)$  进行验证:

(1) 验证  $e(pk_{ID,1}, pk_{ID,2}) = e(g_1, v)$ ; 若不成立, 则终止。

(2) 计算  $b = f(R_u)$ ,  $h = H(m, ID, pk_{ID,2}, R_u, R_m, m_b, v)$ 。

(3) 若  $e(V, g) = e(g_2, pk_{ID,1}) e(u \prod_{i \in u_{ID}} u_i, R_u) e(pk_{ID,2}^h m_b, R_m)$ 。

## 4 安全模型

无证书签名方案的敌手模型与文献[15]中的类似, 第一类敌手  $A_I$  作为第三方攻击者, 可以替换任意用户的公钥, 但不知道主密钥和部分私钥。第二类敌手  $A_{II}$  作为一个恶意的 KGC, 知道主密钥, 但不可以替换用户的公钥。

下面通过两种游戏定义无证书签名方案的安全模型。

### 4.1 游戏 1

敌手  $A_I$  和挑战者  $C$  之间的游戏如下:

1) 系统参数设置: 输入安全参数  $k$ , KGC 生成 params 和 msk。C 将 params 发送给  $A_I$ , msk 保密。

2) 询问:  $A_I$  进行如下询问:

(1) 部分私钥询问:  $C$  接收到  $A_I$  对身份 ID 的部分私钥的询问, 返回  $psk_{ID}$  给  $A_I$ 。

(2) 公钥询问:  $A_I$  询问身份 ID 的  $pk_{ID}$ ,  $C$  返回  $pk_{ID}$  给  $A_I$ 。

(3) 公钥替换:  $A_I$  给出  $(x'_{ID}, pk'_{ID})$ ,  $C$  将原始的  $(x_{ID}, pk_{ID})$  更新为  $(x'_{ID}, pk'_{ID})$ 。

(4) 私钥询问:  $C$  接收到  $A_I$  对身份 ID 的私钥询问, 返回  $sk_{ID}$  给  $A_I$ 。

(5) 签名询问:  $A_I$  可以询问身份为 ID 的用户对任意消息  $m$  的签名,  $C$  返回签名给  $A_I$ 。

3) 伪造:  $A_I$  输出身份为  $ID^*$  的用户对消息  $m^*$  的签名  $\sigma^*$ 。如果  $A_I$  满足以下条件且  $Verify(params, ID^*, pk_{ID^*}, m^*, \sigma^*) = 1$ , 那么  $A_I$  就赢得了游戏:

(1)  $A_I$  没有发出对  $ID^*$  的部分私钥询问。

(2)  $A_I$  没有发出对  $ID^*$  的私钥询问。

(3)  $A_I$  没有发出对  $(ID^*, m^*)$  的签名询问。

那么, 敌手  $A_I$  赢得游戏 1 的概率定义为  $A_I$  赢得游戏 1 的

概率。

### 4.2 游戏 2

敌手  $A_{II}$  和挑战者  $C$  之间的游戏如下:

1) 系统参数设置: 输入安全参数  $k$ , KGC 生成 params 和 msk, 并将 params、msk 发送给  $A_{II}$ 。

2) 询问:  $A_{II}$  发出和游戏 1 相同的私钥询问、公钥询问、公钥替换询问和签名询问。

3) 伪造:  $A_{II}$  输出身份为  $ID^*$  的用户对消息  $m^*$  的签名  $\sigma^*$ 。如果  $A_{II}$  满足以下条件且  $Verify(params, ID^*, pk_{ID^*}, m^*, \sigma^*) = 1$ , 那么  $A_{II}$  就赢得了游戏。

(1)  $A_{II}$  没有询问过身份  $ID^*$  的私钥。

(2)  $A_{II}$  没有替换身份  $ID^*$  的公钥。

(3)  $A_{II}$  没有询问过身份  $ID^*$  对消息  $m^*$  的签名。

那么,  $A_{II}$  成功的概率定义为  $A_{II}$  赢得游戏 2 的概率。

定义 3: 如果上述两类敌手都能以不可忽略的优势赢得游戏, 那么就称无证书签名方案在适应性选择消息攻击下是存在性不可伪造的。

## 5 安全证明

定理 1: 如果存在一个概率多项式敌手  $A_I$ , 进行最多  $q_{psk}$  次部分私钥询问,  $q_{pk}$  次公钥询问,  $q_{sk}$  次私钥询问,  $q_s$  次签名询问, 以概率  $\varepsilon$  赢得游戏 1, 则存在一个算法  $C$ , 在多项式时间内以  $\varepsilon' \geq \frac{\varepsilon}{8(q_{psk} + q_{sk})(n+1)}$  的概率成功解决 NGBDH 问题。

证明: 输入  $(g, g^a, g^b)$ , 计算  $(g^{ab}, g^c)$ , 利用算法  $C$  解决 NGBDH 问题。C 包含了初始为空的列表  $L = \{ID, psk_{ID}, x_{ID}, pk_{ID}, sk_{ID}\}$ 。

1) 系统参数设置: 令  $l = 2(q_{psk} + q_{sk})$ , 假定  $l(n+1) < q$ 。C 随机选择一个整数  $k$ , 满足  $0 \leq k \leq n$ 。C 随机选择  $x', x_i \in Z_l (1 \leq i \leq n)$ ,  $y', y_i \in Z_q (1 \leq i \leq n)$ ,  $t, c, c_0, c_1 \in Z_q$ 。令  $g_1 = g^a, g_2 = g^b, u' = g_2^{-lk} g^{c'}$ ,  $u_i = g_2^{x_i} g^{y_i} (1 \leq i \leq n)$ ,  $m_0 = g^{c_0}, m_1 = g_2^{c_1} g^{c'}$ ,  $v = g^c$ 。定义两个函数:  $J_u(u) = x' + \sum_{i \in u_{ID}} x_i - lk, K_u(u) = y' + \sum_{i \in u_{ID}} y_i$ , 则  $u' \prod_{i \in u_{ID}} u_i = g_2^{J_u(u)} g^{K_u(u)}$ 。

2) 询问: 在询问阶段, 算法  $C$  回复  $A_I$  的一系列询问。

(1) 部分私钥询问:  $A_I$  询问身份 ID 的  $psk_{ID}$ ,  $C$  检查列表  $L$ , 若存在, 直接返回  $psk_{ID}$  给敌手  $A_I$ 。若不存在,  $C$  检查  $J_u(u) = 0 \bmod q$ : 若  $J_u(u) = 0 \bmod q$ ,  $C$  终止模拟; 若  $J_u(u) \neq 0 \bmod q$ ,  $C$  随机选取  $r \in Z_q$ , 计算部分私钥:

$$psk_{ID} = (g_1^{-\frac{K_u(u)}{J_u(u)}} (u' \prod_{i \in u_{ID}} u_i)^r, g_1^{-\frac{1}{J_u(u)}} g^r) =$$

$$(g_2^\alpha (u' \prod_{i \in u_{ID}} u_i)^{\tilde{r}}, g^{\tilde{r}})$$

其中,  $\tilde{r} = r - \frac{\alpha}{J_u(u)}$ 。

$C$  返回  $\text{psk}_{ID}$  给  $A_1$ , 并将元组添加到  $L$ 。

(2) 公钥询问:  $A_1$  询问身份  $ID$  的公钥,  $C$  检查  $L$ , 若存在, 直接返回  $\text{pk}_{ID}$  给敌手  $A_1$ 。若不存在,  $C$  随机选取  $x_{ID} \in Z_q^*$ , 生成公钥  $\text{pk}_{ID}$ 。 $C$  返回  $(x_{ID}, \text{pk}_{ID})$  给  $A_1$ , 并将元组添加到  $L$ 。

(3) 公钥替换:  $C$  接收到  $A_1$  发出的公钥替换询问, 检查列表  $L$ 。若不存在, 则直接将  $(x'_{ID}, \text{pk}'_{ID})$  存储到  $L$ 。若存在,  $C$  将  $L$  中的  $(x_{ID}, \text{pk}_{ID})$  替换为  $(x'_{ID}, \text{pk}'_{ID})$ 。

(4) 私钥询问:  $C$  接收到  $A_1$  发出的对身份  $ID$  的私钥询问, 检查列表  $L$ 。若存在, 直接返回  $\text{sk}_{ID}$  给敌手  $A_1$ ; 若不存在, 检查  $J_u(u) = 0 \bmod q$ 。如果  $J_u(u) = 0 \bmod q$ ,  $C$  终止模拟; 否则,  $C$  发出部分私钥询问获得身份  $ID$  的  $\text{psk}_{ID}$ , 运行用户密钥生成算法获取  $(x_{ID}, \text{pk}_{ID})$ , 运行私钥生成算法获得  $\text{sk}_{ID}$ 。 $C$  返回元组给  $A_1$  并添加到  $L$ 。

(5) 签名询问:  $A_1$  询问消息  $m$  的签名,  $C$  执行以下步骤:

若  $J_u(u) \neq 0 \bmod q$ ,  $C$  检查  $L$ , 若存在  $(\text{pk}_{ID}, \text{sk}_{ID})$ , 则  $C$  运行签名算法生成消息  $m$  的签名  $\sigma$ , 并返回给  $A_1$ 。

否则,  $C$  选择  $r_1 \in Z_q$ , 使  $f(g^{r_1}) = 1$  (如果  $f(g^{r_1}) = 0$ ,  $C$  再选  $r_1 \in Z_q$ , 使  $f(g^{r_1}) = 1$ )。随后,  $C$  随机选择  $r_m \in Z_q$ , 按如下生成  $\sigma = (V, R_u, R_m)$ :

$$\sigma = (V, R_u, R_m) =$$

$$(g_1^{\frac{ch+c_1x_{ID}}{t}} (u' \prod_{i \in u_{ID}} u_i)^{r_1} (\text{pk}_{ID,2}^h \cdot m_1)^{r_m}, g^{r_1},$$

$$g_1^{\frac{x_{ID}}{t}} g^{r_m}) = (g_1^{\frac{ch+c_1x_{ID}}{t}} (u' \prod_{i \in u_{ID}} u_i)^{r_1} (\text{pk}_{ID,2}^h \cdot m_1)^{r_m})^{\tilde{r}_m}$$

$$(g^{\frac{ch}{x_{ID}}} g_2^{\frac{t}{x_{ID}}} g^{c_1})^{\frac{\alpha x_{ID}}{t}}, g^{r_1}, g^{\tilde{r}_m}) =$$

$$(g_2^{\alpha x_{ID}} (u' \prod_{i \in u_{ID}} u_i)^{r_1} (\text{pk}_{ID,2}^h \cdot m_1)^{\tilde{r}_m}, g^{r_1}, g^{\tilde{r}_m})$$

其中,  $\tilde{r}_m = r_m - \frac{\alpha x_{ID}}{t}$ ,  $h = H(m, ID, \text{pk}_{ID,2}, R_u, R_m,$

$m_b, v)$ ,  $C$  返回  $\sigma$  给  $A_1$ 。

3) 伪造: 若算法  $C$  在上述询问中没有失败退出, 则敌手  $A_1$  成功伪造用户  $ID^*$  对消息  $m^*$  的有效签名。若  $J_u(u^*) \neq 0 \bmod q$  或者  $f(R_u^*) = 1$ ,  $C$  终止。否则, 有:

$$e(V^*, g) = e(g_2, \text{pk}_{ID^*,1}) e(u' \prod_{i \in u_{ID^*}} u_i, R_u^*)$$

$$e(\text{pk}_{ID^*,2}^{h^*}, m_0, R_m^*) = e(g^\beta, g_1^{x_{ID^*}}) e(g^{K_u(u^*)}, R_u^*)$$

$$e(g^{\frac{ch}{x_{ID^*}}}, R_m^*) = e(g, g^{\alpha \beta x_{ID^*}})$$

$$e(g, (R_u^*)^{K_u(u^*)}) e(g, (R_m^*)^{c_0 + \frac{ch^*}{x_{ID^*}}})$$

算法  $C$  输出  $\left( \frac{V^*}{(R_u^*)^{K_u(u^*)} (R_m^*)^{c_0 + \frac{ch^*}{x_{ID^*}}}}, g^{x_{ID^*}} \right)$  作为

NGBDH 问题的解。

4) 概率计算: 算法  $C$  在模拟过程中没有终止, 必须满足以下条件:

(1) 部分私钥询问满足  $J_u(u) \neq 0 \bmod q$ 。

(2) 所有的私钥询问满足  $J_u(u) \neq 0 \bmod q$ 。

(3) 伪造身份  $ID^*$  对消息  $m^*$  的签名  $\sigma^*$  满足  $J_u(u^*) = 0 \bmod q$  和  $f(R_u^*) = 0$ 。

定义 3 个事件  $A^*$ ,  $B^*$ ,  $A_i$ :

$$A^* : J_u(u^*) = 0 \bmod q;$$

$$B^* : f(R_u^*) = 0;$$

$$A_i : J_u(u_i) \neq 0 \bmod l, i = 1, 2, \dots, q_1。$$

由条件  $l(n+1) < q$ ,  $x', x_1, \dots, x_n \in Z_l$ , 得到  $0 \leq l \cdot k < q$ ,  $0 \leq x' + \sum_{i \in u_{ID}} x_i < q$ 。如果  $J_u(u) = 0 \bmod q$ , 则  $J_u(u) = 0 \bmod l$ 。更进一步, 如果  $J_u(u) \neq 0 \bmod l$ , 则  $J_u(u) \neq 0 \bmod q$ 。所以

$$\Pr[A^*] = \Pr[J_u(u^*) = 0 \bmod q \wedge J_u(u^*) =$$

$$0 \bmod l] = \Pr[J_u(u^*) = 0 \bmod l] \cdot$$

$$\Pr[J_u(u^*) = 0 \bmod q \mid J_u(u^*) = 0 \bmod l] =$$

$$\frac{1}{l} \frac{1}{n+1}$$

$$\Pr[\bigwedge_{i=1}^{q_1} A_i \wedge A^*] = \Pr[A^*] \cdot$$

$$\Pr[\bigwedge_{i=1}^{q_1} A_i \mid A^*] \geq \Pr[A^*] \cdot$$

$$(1 - \sum_{i=1}^{q_1} \Pr[\neg A_i \mid A^*]) =$$

$$\frac{1}{l(n+1)} (1 - \frac{q_1}{l}) \geq$$

$$\frac{1}{l(n+1)} (1 - \frac{q_{\text{psk}} + q_{\text{sk}}}{l})$$

另一方面:  $\Pr[B^*] = \frac{1}{2}$ 。因为  $K_u(u)$  和  $r_1$  是独

立选取的, 所以事件  $\bigwedge_{i=1}^{q_1} A_i \wedge A^*$  和事件  $B^*$  是相互独立的, 则算法  $C$  不终止的概率为:

$$\Pr[\neg \text{abort}] \geq \Pr[\bigwedge_{i=1}^{q_1} A_i \wedge A^* \wedge B^*] =$$

$$\Pr[\bigwedge_{i=1}^{q_1} A_i \wedge A^*] \cdot \Pr[B^*] \geq$$

$$\frac{1}{2l(n+1)} \left( 1 - \frac{q_{\text{psk}} + q_{\text{sk}}}{l} \right) =$$

$$\frac{1}{8(q_{\text{psk}} + q_{\text{sk}})(n+1)}$$

因此, 算法  $C$  成功解决 NGBDH 问题的概率为

$$\varepsilon' \geq \frac{\varepsilon}{8(q_{\text{psk}} + q_{\text{sk}})(n+1)}。$$

定理 2: 如果存在一个概率多项式敌手  $A_{II}$ , 进行最多  $q_{\text{pk}}$  次公钥询问,  $q_{\text{sk}}$  次私钥询问,  $q_s$  次签名询问,



以概率  $\varepsilon$  赢得游戏 2。则存在一个算法  $C$ , 在多项式时间内以  $\varepsilon' \geq \frac{\varepsilon}{8q_{sk}(n+1)}$  的概率成功解决 Many-DH 问题。

证明: 输入  $(g, g^\alpha, g^\beta, g^\gamma, g^{\alpha\beta}, g^{\alpha\gamma}, g^{\beta\gamma})$ , 计算  $g^{\alpha\beta\gamma}$ 。利用算法  $C$  解决 Many-DH 问题,  $C$  包含了一个初始为空的列表  $L = \{\text{ID}, x_{\text{ID}}, \text{pk}_{\text{ID}}, \text{sk}_{\text{ID}}\}$ 。

1) 系统参数设置: 令  $l = 2q_{sk}$ , 假定  $l(n+1) < q$ 。 $C$  随机选择一个整数  $k$ , 满足  $0 \leq k \leq n$ 。 $C$  随机选择  $x', x_i \in Z_l (1 \leq i \leq n)$ ,  $y', y_i \in Z_q (1 \leq i \leq n)$ ,  $t, c, c_0, c_1 \in Z_q^*$ 。令  $g_1 = g^\alpha$ ,  $g_2 = g^\beta$ ,  $u' = g_2^{x'-lk} g^\gamma$ ,  $u_i = g_2^{x_i} g^{\gamma_i} (1 \leq i \leq n)$ ,  $m_0 = g^{c_0}$ ,  $m_1 = g_2^t g^{c_1}$ ,  $v = (g^\gamma)^c$ 。

定义两个函数:  $J_u(u) = x' + \sum_{i \in u_{\text{ID}}} x_i - lk$ ,  $K_u(u) = y' + \sum_{i \in u_{\text{ID}}} y_i$ , 则  $u' \prod_{i \in u_{\text{ID}}} u_i = g_2^{J_u(u)} g^{K_u(u)}$ 。 $C$  将 params 和  $\text{msk} = g_2^\alpha = g^{\alpha\beta}$  发送给  $A_{\text{II}}$ 。

2) 询问阶段:  $A_{\text{II}}$  发出以下询问。

(1) 公钥询问:  $A_{\text{II}}$  询问身份 ID 的公钥,  $C$  检查列表  $L$ 。若存在, 直接返回  $\text{pk}_{\text{ID}}$  给敌手  $A_{\text{II}}$ 。若不存在,  $C$  随机选取  $x_{\text{ID}} \in Z_q$ , 计算  $\text{pk}_{\text{ID}} = (\text{pk}_{\text{ID},1}, \text{pk}_{\text{ID},2}) = (g^{\alpha x_{\text{ID}}}, g^{\frac{c}{x_{\text{ID}}}})$  作为身份 ID 的公钥。 $C$  返回  $\text{pk}_{\text{ID}}$  给  $A_{\text{II}}$ , 并将元组添加到  $L$ 。

(2) 私钥询问:  $A_{\text{II}}$  询问身份 ID 的私钥,  $C$  检查列表  $L$ 。若存在, 直接返回  $\text{sk}_{\text{ID}}$  给敌手  $A_{\text{II}}$ 。否则,  $C$  检查  $J_u(u) = 0 \bmod q$ : 若  $J_u(u) = 0 \bmod q$ ,  $C$  终止模拟; 若  $J_u(u) \neq 0 \bmod q$ ,  $C$  随机选取  $r \in Z_q$ , 令

$$\text{sk}_{\text{ID}} = ((g^{\alpha\gamma})^{-\frac{K_u(u)}{J_u(u)}} (u' \prod_{i \in u_{\text{ID}}} u_i)^r, (g^{\alpha\gamma})^{-\frac{x_{\text{ID}}}{J_u(u)}} g^r) = (g_2^{\alpha\gamma x_{\text{ID}}} (u' \prod_{i \in u_{\text{ID}}} u_i)^r, g^r)$$

$$\text{其中, } \tilde{r} = r - \frac{\alpha\gamma x_{\text{ID}}}{J_u(u)}。$$

$C$  返回  $\text{sk}_{\text{ID}}$  给  $A_{\text{II}}$ , 并将元组添加到  $L$ 。

(3) 公钥替换:  $C$  接收到  $A_{\text{II}}$  发出的公钥替换询问, 检查列表  $L$ 。若不存在, 则直接将  $(x'_{\text{ID}}, \text{pk}'_{\text{ID}})$  存储到  $L$  中。若存在,  $C$  将  $L$  中  $(x_{\text{ID}}, \text{pk}_{\text{ID}})$  替换为  $(x'_{\text{ID}}, \text{pk}'_{\text{ID}})$ 。

(4) 签名询问:  $A_{\text{II}}$  询问消息  $m$  的签名,  $C$  执行以下步骤:

若  $J_u(u) \neq 0 \bmod q$ ,  $C$  检查  $L$ , 若  $(\text{pk}_{\text{ID}}, \text{sk}_{\text{ID}})$  存在, 则  $C$  运行签名算法生成消息  $m$  的签名  $\sigma$ , 并返回给  $A_{\text{II}}$ 。否则,  $C$  随机选择  $r_1 \in Z_q$ , 使  $f(g^{r_1}) = 1$  (如果  $f(g^{r_1}) = 0$ ,  $C$  再选  $r_1 \in Z_q$ , 使  $f(g^{r_1}) = 1$ )。随后,  $C$  随机选择  $r_m \in Z_q$ , 按如下生成  $\sigma = (V, R_u, R_m)$ :

$$\sigma = (V, R_u, R_m) = ((g^{\alpha\gamma})^{-\frac{ch+c_1x_{\text{ID}}}{t}} (u' \prod_{i \in u_{\text{ID}}} u_i)^{r_1} (\text{pk}_{\text{ID},2}^h \cdot m_1)^{r_m}, g^{r_1},$$

$$(g^{\alpha\gamma})^{-\frac{x_{\text{ID}}}{t}} g^{r_m}) = (g_2^{\alpha\gamma x_{\text{ID}}} (u' \prod_{i \in u_{\text{ID}}} u_i)^{r_1}$$

$$(\text{pk}_{\text{ID},2}^h \cdot m_1)^{r_m}, g^{r_1}, g^{r_m})$$

其中,  $\tilde{r}_m = r_m - \frac{\alpha\gamma x_{\text{ID}}}{t}$ ,  $h = H(m, \text{ID}, \text{pk}_{\text{ID},2}, R_u, R_m, m_b, v)$ ,  $C$  返回  $\sigma$  给  $A_{\text{II}}$ 。

3) 伪造: 若算法  $C$  在上述询问中没有失败退出, 则敌手  $A_{\text{II}}$  至少以概率  $\varepsilon$  成功伪造用户 ID\* 对消息  $m^*$  的有效签名  $\sigma^*$ 。若  $J_{u^*}(u^*) \neq 0 \bmod q$  或者  $f(R_{u^*}) = 1$ , 则  $C$  终止。否则, 有

$$\begin{aligned} e(V^*, g) &= e(g_2, \text{pk}_{\text{ID}^*}) e(u' \prod_{i \in u_{\text{ID}^*}} u_i, R_{u^*}) e(\text{pk}_{\text{ID}^*,2}^h m_0, R_m^*) = e(g^\beta, \\ &g^{\alpha\gamma x_{\text{ID}^*}}) e(g^{K_{u^*}(u^*)}, R_{u^*}) e(g^{c_0} \cdot g^{\frac{ch}{x_{\text{ID}^*}}}, R_m^*) = \\ &e(g, g^{\alpha\beta\gamma x_{\text{ID}^*}}) e(g, (R_{u^*})^{K_{u^*}(u^*)}) e(g, (R_m^*)^{c_0 + \frac{ch}{x_{\text{ID}^*}}}) \end{aligned}$$

$$\text{算法 } C \text{ 输出 } \left( \frac{V^*}{(R_{u^*})^{K_{u^*}(u^*)} (R_m^*)^{c_0 + \frac{ch}{x_{\text{ID}^*}}}} \right)^{\frac{1}{x_{\text{ID}^*}}} \Rightarrow g^{\alpha\beta\gamma} \text{ 作}$$

为 Many-DH 问题的解。

4) 概率计算: 定理 2 的证明与定理 1 类似, 由此可得算法  $C$  成功解决 Many-DH 问题的概率为  $\varepsilon' \geq$

$$\frac{\varepsilon}{8q_{sk}(n+1)}。$$

## 6 结束语

通过具体的攻击方法, 对李艳琼的方案进行了安全性分析, 指出其不能抵抗公钥替换攻击和恶意的 KGC 攻击。为此, 提出了一种改进的无证书签名方案, 克服了原方案的安全缺陷。基于 NGBDH 问题和 Many-DH 问题, 在标准模型下证明了改进方案的安全性。与原方案相比, 改进方案增强了与公钥、私钥等参数的联系, 具有更强的安全性。在今后的研究中, 构造安全高效的标准模型下的无证书签名方案仍是研究的重点。

## 参考文献:

- [1] Shamir A. Identity-based cryptosystems and signature schemes [C]//Proceedings of the Crypto'84. [s. l.]: [s. n.], 1984: 47-53.
- [2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C]//Proceedings of the Asiacrypt'2003. [s. l.]: [s. n.], 2003: 452-473.
- [3] Yum D H, Lee P J. Generic construction of certificateless encryption [C]//Proceedings of the ACISP'2004. [s. l.]: [s. n.], 2004: 802-811.

(下转第 143 页)

他评估方法,在安全性和准确性方面都有所提高。

## 4 结束语

随着网络技术与应用的快速发展,终端用户行为的复杂性和开放性使得网络安全面临严峻挑战,而对网络终端用户的可信性评估显得尤为重要。结合模糊综合评估理论提出了一种基于模糊综合策略的网络用户行为可信评估方法,采用熵权法来构建用户行为的综合指标权重,并运用模糊算子和加权平均原则保证了评估结果的精确量化。实验结果表明,该评估方法能够在复杂网络环境中对用户行为进行全面、准确和动态的量化评估。结合可信网络连接控制机制,将评估机制扩展到可信网络中将是下一步工作方向。

## 参考文献:

- [1] 林 闯,田立勤,王元卓.可信网络中用户行为可信的研究[J].计算机研究与发展,2008,45(12):2033-2043.
- [2] 田立勤,林 闯.可信网络中一种基于行为信任预测的博弈控制机制[J].计算机学报,2007,30(11):1930-1938.
- [3] 冀铁果,田立勤,胡志兴,等.可信网络中一种基于 AHP 的用户行为评估方法[J].计算机工程与应用,2007,43(19):123-126.
- [4] Xi Zhenyuan, Chen He, Wang Xiaozhong, et al. Evaluation model for computer network information security based on analytic hierarchy process[C]//Intelligent information technology application. [s. l.]:[s. n.],2009:186-189.
- [5] 武小年,周胜源.数据挖掘在用户行为可信研究中的应用[C]//第十一届保密通信与信息安全现状研讨会论文集.厦门:出版地不详,2009.
- [6] 马军煜,赵知劲,叶学义.基于模糊决策分析的可信网络用户行为评估[J].计算机工程,2011,37(13):125-127.
- [7] 吕艳霞,田立勤,孙珊珊.云计算环境下基于 FANP 的用户行为的可信评估与控制分析[J].计算机科学,2013,40(1):132-135.
- [8] Hosseini S B,Shojaee A,Agheli N. A new method for evaluating cloud computing user behavior trust[C]//Proceedings of the 7th information and knowledge technology. [s. l.]:[s. n.],2015:1-6.
- [9] Tian Liqin,Lin Chuang,Ni Yang. Evaluation of user behavior trust in cloud computing[C]//Proceedings of the computer application and system modeling. Taiyuan, Shanxi:[s. n.],2010.
- [10] Li Wen,Ping Lingdi,Lu Kuijun,et al. Trust model of users' behavior in trustworthy internet[C]//Proceedings of the information engineering. Taiyuan, Shanxi:[s. n.],2009:403-406.
- [11] Yang Xiaoqiong,Liu Lianzhong,Zou Rongbo. A statistical user behavior trust evaluation algorithm based on cloud model[C]//Proceedings of the 6th computer science and convergence information technology. Jeju,Seogwipo:[s. n.],2011:598-603.
- [12] Shan Xiaohong,Sun Huamei,Ge Gaoxin. The research of web users' behavior analysis based on Web Log Mining[C]//E-Business and E-Government (ICEE). Shanghai:[s. n.],2011:1-4.
- [13] 陆 悠,罗军舟,李 伟,等.面向网络状态的自适应用户行为评估方法[J].通信学报,2013,34(7):71-80.
- [14] 田 野,彭新光,李宏滨,等.网络用户行为可信性集值统计度量方法[J].小型微型计算机系统,2013,34(10):2354-2357.
- [15] 2005,16(10):1743-1756.
- [11] Liu J K,Au M H,Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model:extended abstract[C]//Proceedings of the ASIACCS'2007. New York:ACM Press,2007:273-283.
- [12] Xiong H,Qin Z G,Li F G. An improved certificateless signature scheme secure in the standard model[J]. Fundamenta Informaticae,2008,88(1-2):193-206.
- [13] Yu Y,Mu Y,Wang G,et al. Improved certificateless signature scheme provably secure in the standard model[J]. IET Information Security,2012,6(2):102-110.
- [14] 魏春艳,蔡晓秋.标准模型下的高效无证书短签名方案[J].计算机工程,2012,38(13):119-121.
- [15] 李艳琼,李继国,张亦辰.标准模型下安全的无证书签名方案[J].通信学报,2015,36(4):185-194.
- [16] 李继国,姜平进.标准模型下可证安全的基于身份的高效的签名方案[J].计算机学报,2009,32(11):2130-2136.
- [10] 冯登国.密码学安全性理论与方法研究[J].软件学报,

(上接第 137 页)