对一个基于离散对数代理盲签名方案的分析与改进*

张瑛瑛[1]，陈 玮[1]，曾吉文[1,2†]

(1. 新疆师范大学 数学科学学院，乌鲁木齐 830054；2. 厦门大学 数学科学学院，福建 厦门 361005)

摘 要： 通过对何俊杰等人提出的一个基于离散对数代理盲签名方案进行分析，从中发现该方案会引起原始签名人的公钥替换攻击。为了解决该方案的安全缺陷，提出了一种新的改进方案。分析表明，改进后的新方案可以抵抗原始签名人的公钥替换攻击，并且在基于离散对数问题下保证了代理盲签名的所有安全性要求，而且提高了效率。

关键词： 数字签名；离散对数；代理盲签名；公钥替换攻击；安全性

中图分类号： TP309 **文献标志码：** A **文章编号：** 1001-3695(2013)11-3390-03

doi:10.3969/j.issn.1001-3695.2013.11.047

Analysis and improvement of proxy blind signature scheme based on DLP

ZHANG Ying-ying[1], CHEN Wei[1], ZENG Ji-wen[1,2†]

(1. *School of Mathematical Sciences, Xinjiang Normal University, Urumqi* 830054, *China*; 2. *School of Mathematical Sciences, Xiamen University, Xiamen Fujian* 361005, *China*)

Abstract: Through the cryptanalysis of a proxy blind signature scheme based on DLP proposed by He Jun-jie, this paper found that this scheme can cause the public replacement attack. To avoid these attacks, this paper proposed a new improved scheme. Analysis result shows that the new improved scheme can resist the original signer's public key replacement attack. It satisfies all the security requirements of proxy blind signature based on the DLP problems and improve the computation efficiency.

Key words: digital signature; discrete logarithm problem; proxy blind signature; public key replacement attack; security

0 引言

代理签名和盲签名是两种非常重要的数字签名类型。1996 年，Mambo 等人[1,2]首次提出了代理签名概念。顾名思义，代理签名是让原始签名者可以将其数字签名权力委托给代理签名者，使其能够代理原始签名者签发指定的数字消息。1982 年，Chaum 在文献[3]中首次提出盲签名方案的概念。盲签名是使用户能将给定的消息让别人签发，而又不泄露任何有关的信息给签名者。

2000 年，Lin 等人[4]将代理签名和盲签名结合，提出了第一个代理盲签名方案，在现实生活中具有非常重要的应用价值，因为它结合了代理签名和盲签名两者的优点。近几年来，多种基于不同体制的代理盲签名方案也被相继提出，如基于身份的代理盲签名方案[5]、无证书的代理盲签名方案[6]、离散对数的代理盲签名方案[7]。

2002 年，Tan 等人[8]提出了一种基于 Schnorr 盲签名的代理盲签名方案，但是 Sun 等人[9]指出该方案存在安全漏洞，容易受到伪造攻击且具有关联性。2005 年，Wang 等人[10]提出一种安全有效的代理盲签名方案。2008 年，李方伟等人在文献[11]中指出该方案并不满足强不可伪造性和不可链接性，任何人都可以伪造代理签名人的密钥，从而冒充代理签名者产生有效的签名，为此提出了改进方案，并且给出了安全性的证明。

2010 年，柳菊霞等人[12]对文献[3]中方案的不可伪造性进行了改进，在此基础上提出了一个新的基于离散对数的代理盲签名方案，声称可以抵抗原始签名人和签名接收者的一般性伪造攻击，同时具有非关联性。但是何俊杰等人[13]指出文献[12]中的方案不满足强不可伪造性和非关联性，并且给出了相应的改进的代理盲签名方案，本文简称为 HSQ 方案。本文对 HSQ 方案进行分析发现，该方案会引起公钥替换攻击。为此对 HSQ 方案进行了改进，改进后的新方案可以抵抗这种攻击。

1 HSQ 的代理盲签名方案回顾

方案的参与者包括原始签名人 A、代理签名人 B、消息拥有者 R、签名验证者。方案描述如下：

1) 系统参数

p、q 为安全大素数，且满足 $q \mid p-1$；$g \in Z_q^*$，且 g 的阶为 q，即 $g^q = 1 \pmod p$。(x_A, y_A)，(x_B, y_B) 分别为原始签名者 A 和代理签名者 B 的公私钥对，其中 $x_A, x_B \in Z_q^*$ 且 $y_A = g^{x_A} \bmod p$，

收稿日期：2013-01-12；修回日期：2012-03-04 基金项目：国家自然科学基金资助项目(11261060)；福建省自然科学基金资助项目(2012J01022)；新疆研究生科研创新资助项目(XJGRI2013130)

作者简介：张瑛瑛(1989-)，女，硕士研究生，主要研究方向为密码学；陈玮(1988-)，男，硕士研究生；曾吉文(1963-)，男(通信作者)，教授，博导，博士，主要研究方向为密码学(jwzeng@xmu.edu.cn)。

$y_B = g^{x_B} \bmod p$,m 为待签名的消息,$H(*)$ 为无碰撞的哈希函数。m_w 是原始签名人 A 将其签名权力委托给代理签名人 B 的授权证书,一般包含原始签名人和代理签名人的身份以及授权期限、可签消息范围等信息。

2) 代理阶段

a) 原始签名者 A 随机选择 $k_A \in Z_q^*$,计算 $r_A = g^{k_A} \bmod p$,$s_A = k_A \cdot H(r_A \| m_w) + x_A \bmod q$。

b) A 把(r_A, s_A)通过安全信道发送给代理签名者 B。

c) B 收到(r_A, s_A)后,首先验证等式 $g^{s_A} = r_A^{H(r_A \| m_w)} y_A \bmod p$ 是否成立,若成立,接受委托并计算 $s' = s_A + x_B \bmod q$,并把 s' 作为其代理签名的私钥。

3) 签名阶段

a) B 随机选择 $k_B \in_R Z_q^*$,计算 $r_B = g^{k_B} \bmod p$,并把(m_w, r_A, r_B)发送给消息拥有者 R。

b) R 收到(m_w, r_A, r_B)后,选择随机数 $a, b, c \in_R Z_q^*$,计算 $r = r_B^c g^a (y_A y_B r_A^{H(r_A \| m_w)})^b \bmod p$,$e = H(r \| m) \bmod q$,$e^* = c^{-1}(b - e) \bmod q$,如果 $r = 0$,重复过程 b),直到 $r \neq 0$,并将 e^* 发送给代理签名者 B。

c) B 收到 e^* 后,计算 $s'' = (k_B + e^* s') \bmod q$,然后将 s'' 发送给消息拥有者 R。

4) 签名提取阶段

消息拥有者 R 收到 s'' 后,计算 $s = (cs'' + a) \bmod q$,这时(m, m_w, s, e, r_A)就是消息 m 的代理盲签名。

5) 签名验证阶段

签名验证者验证等式 $e = H(g^s (y_A y_B r_A^{H(r_A \| m_w)})^e \bmod p \| m) \bmod q$ 是否成立。如果等式成立,则(m, m_w, s, e, r_A)是消息 m 的有效签名;否则,视签名无效。

2　对 HSQ 方案的攻击

HSQ 方案无法抵抗原始签名者 A 的公钥替换攻击,即原始签名者 A 可以替换自己的公钥,进而伪造代理签名人,对消息 m 进行有效的代理盲签名,并声称是由 B 签的,并且原始签名者 A 可以任意改变授权证书 m_w 的内容。

对 HSQ 方案进行公钥替换攻击,具体的攻击方法如下:

a) 根据原始签名者 A 的需要,产生授权证书 m'_w(包括原始签名者 A 和 B 的身份信息、代理签名消息的范围、代理权限等信息)。

b) A 选择随机数 $\overline{k_A} \in Z_q^*$,$\lambda \in Z_q^*$,计算 $\overline{r_A} = g^{\overline{k_A}} \bmod p$。

c) A 计算 $\overline{s'} = \lambda + \overline{k_A} H(\overline{r_A} \| m'_w)$,并用 $\overline{s'}$ 作为代理盲签名的私钥。

d) A 计算 $\overline{y_A} = y_B^{-1} \cdot g^{\lambda} \bmod p$,A 将自己的公钥 y_A 替换成 $\overline{y_A}$。

原始签名者 A 可以用 $\overline{s'}$ 对消息 m 进行有效的签名,第 1 章中的签名阶段就变成:

a) A 随机选择 $\overline{k_B} \in_R Z_q^*$,计算 $\overline{r_B} = g^{\overline{k_B}} \bmod p$,并把$(m'_w, \overline{r_A}, \overline{r_B})$发送给消息拥有者 R。

b) R 收到$(m'_w, \overline{r_A}, \overline{r_B})$后,选择随机数 $a, b, c \in_R Z_q^*$ 计算 $\bar{r} = \overline{r_B}^c g^a (\overline{y_A} y_B \overline{r_A}^{H(\overline{r_A} \| m'_w)})^b \bmod p$,$\bar{e} = H(\bar{r} \| m) \bmod q$,$\overline{e^*} = c^{-1}(b - \bar{e}) \bmod q$,如果 $\bar{r} = 0$,重复 b),直到 $\bar{r} \neq 0$,并将 $\overline{e^*}$ 发送给代理签名者 B。

c) A 收到 $\overline{e^*}$ 后,计算 $\overline{s''} = (\overline{k_B} + \overline{e^*}\,\overline{s'}) \bmod q$,然后将 $\overline{s''}$ 发送给消息拥有者 R,R 收到 $\overline{s''}$ 后,计算 $\bar{s} = (c\,\overline{s''} + a) \bmod q$,这时$(m, m'_w, \bar{s}, \bar{e}, \overline{r_A})$就是消息 m 的代理盲签名。由验证等式可得

$$\bar{e} = H(g^{\bar{s}} (\overline{y_A} y_B \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(g^{c\overline{s''} + a} (y_B^{-1} \cdot g^{\lambda} y_B \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(g^{c(\overline{k_B} + \overline{e^* s'})} + a (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H((g^{\overline{k_B}})^c g^{c\overline{e^* s'}} g^a \cdot (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (g^{\overline{s''}})^{\overline{ce^*}} \cdot (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (g^{\lambda + \overline{k_A} H(\overline{r_A} \| m'_w)})^{\overline{ce^*}} \cdot (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (g^{\lambda} g^{\overline{k_A} H(\overline{r_A} \| m'_w)})^{\overline{ce^*}} \cdot (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\overline{ce^*}} \cdot (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\bar{e}} \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m'_w)})^{\overline{ce^*} + \bar{e}} \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (g^{\lambda} \overline{r_A}^{H(\overline{r_A} \| m_{w'})})^b \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (y_B^{-1} g^{\lambda} y_B \overline{r_A}^{H(\overline{r_A} \| m'_w)})^b \bmod p \| m) \bmod q =$$
$$H(\overline{r_B}^c g^a (\overline{y_A} y_B \overline{r_A}^{H(\overline{r_A} \| m'_w)})^b \bmod p \| m) \bmod q = H(\bar{r} \| m) \bmod q$$

所以,$(m, m'_w, \bar{s}, \bar{e}, \overline{r_A})$是一个有效的代理盲签名,故 HSQ 方案不能抵抗原始签名者 A 的公钥替换攻击。

3　对 HSQ 方案的改进

由以上分析可以看出,$y_A y_B r_A^{H(r_A \| m_w)}$ 是 HSQ 代理盲签名方案中的公钥,进而对其进行少许改进,具体的方法如下:

a) 将 HSQ 方案中步骤 2) 的 a) 中的 s_A 改为 $s_A = k_A \cdot H(r_A \| m_w) + x_A y_A \bmod q$。所以,相应的 c) 中的验证等式变成 $g^{s_A} = r_A^{H(r_A \| m_w)} y_A^{y_A} \bmod p$。相对应的代理盲签名的私钥为 $s' = s_A + x_B \bmod q$,代理盲签名的公钥为 $y_P = g^{s'} \bmod p = r_A^{H(r_A \| m_w)} \cdot y_A^{y_A} y_B \bmod p$。

b) 将 HSQ 方案中步骤 3) 的 b) 中的 r 改为 $r = r_B^c g^a (y_P)^b \bmod p$。所以,HSQ 方案中步骤 5) 即代理盲签名的验证等式修改为 $e = H(g^s (y_P)^e \bmod p \| m) \bmod q$。

4　对改进后方案安全性和效率的分析

4.1　改进后新方案安全性分析

1) 可验证性分析

签名验证者首先验证消息 m 是否满足 m_w 中的约定,再验证代理签名(m, m_w, s, e, r_A)是否满足等式 $e = H(g^s (y_P)^e \bmod p \| m) \bmod q$ 成立。由于 $s' = s_A + x_B \bmod q = k \cdot H(r_A \| m_w) + x_A y_A + x_B \bmod q$,$s'' = (k_B + e^* s') \bmod q$,$r = r_B^c g^a (y_P)^b \bmod p$,$s = (cs'' + a) \bmod q$,$e^* = c^{-1}(b - e) \bmod q$,$y_P = g^{s'} \bmod p = r_A^{H(r_A \| m_w)} y_A^{y_A} y_B \bmod p$。

所以验证性的分析过程具体如下:

$$e = H(g^s (y_P)^e \bmod p \| m) \bmod q =$$
$$H(g^{cs'' + a} (y_P)^e \bmod p \| m) \bmod q =$$
$$H(g^{cs'' + a} (y_P)^e \bmod p \| m) \bmod q =$$
$$H(g^{c(k_B + e^* s')} + a (y_P)^e \bmod p \| m) \bmod q =$$
$$H(r_B^c g^a g^{ce^* s'} (y_P)^e \bmod p \| m) \bmod q =$$

$$H(r_B{}^c g^a (g^{s'})^{ce^*} (y_P)^e \bmod p \| m) \bmod q =$$
$$H(r_B{}^c g^a (y_P)^{b-e} (y_P)^e \bmod p \| m) \bmod q =$$
$$H(r_B{}^c g^a (y_P)^b \bmod p \| m) \bmod q = H(r \| m) \bmod q$$

所以,通过验证的算法是可以得到正确验证的。

2) 不可伪造性

a) 基本的不可伪造性。指的是来自第三方对原始签名人和代理签名人的攻击,即普通伪造者对代理签名的攻击。由于代理签名的私钥 $s' = s_A + x_B \bmod q$,而 $s_A = k_A \cdot H(r_A \| m_w) + x_A y_A \bmod q$。可以看出,代理签名私钥 s' 中包含了 A 的私钥 x_A 和随机数 k_A,也包含了 B 的私钥 x_B。任何一个普通伪造者要想成功伪造有效的代理签名,就必须得到代理签名私钥 s'。普通伪造者要想知道代理签名私钥 s',就必须知道构成代理签名私钥 s' 中所有的数,即知道 (k_A, x_A, x_B)。换句话说,就是普通伪造者要想成功伪造有效的代理签名,就必须知道 (k_A, x_A, x_B)。而本文的 x_A 是 A 的私钥,k_A 是 A 选择的随机数,只有原始签名人 A 一个人知道;同样地,x_B 是 B 的私钥,也只有代理签名者 B 一个人知道。所以普通伪造者是无法通过伪造代理签名私钥 s' 来伪造有效代理签名的。故改进后的方案满足基本的不可伪造性。

b) 代理签名的不可伪造性。指的是原始签名人 A 无法假冒代理签名者 B 生成有效的代理签名。从改进后的方案中可以看出,原始签名人 A 若想假冒代理签名者 B,首先就要构造一个有效的代理盲签名公钥。具体做法如下:原始签名人 A 构造一个 r'_A 满足代理盲签名公钥的等式:

$$y'_P = (r'_A)^{H(r_A' \| m_w')} y_A{}^{y_A} y_B \bmod p$$

从等式中解出 $r'_A = (y'_P \cdot (y_A{}^{y_A} y_B)^{-1})^{(H(r'_A \| m'_w))^{-1}} \bmod p$,而从上式中计算出 r'_A 比求解有限域上离散对数的问题更难。这样原始签名人 A 就无法伪造一个有效的代理盲签名公钥,所以也就无法继续进行代理签名阶段伪造的过程。故改进后的方案满足代理签名的不可伪造性。

c) 公钥的不可伪造性。指的是原始签名人 A 无法通过替换自己的公钥而成功伪造代理签名。与本文对 HSQ 方案攻击的方法类似,若原始签名人 A 选择随机数 $r'_A, s' \in_R Z$,构造一个 y'_A 满足验证等式:

$$y'_P = (r'_A)^{H(r_A' m_w')} (y'_A)^{y'_A} y_B \bmod p = g^{s'} \bmod p$$

从等式中求得 $y'_A = (g^{s'} \cdot ((r'_A)^{H(r'_A \| m'_w)} y_B)^{-1})^{(y'_A)^{-1}} \bmod p$,而从上式中计算出 y'_A 比求解有限域上离散对数的问题更难。所以,原始签名人 A 也就无法实现替换自己的公钥 y_A 为 y'_A。故改进后的方案能抵抗公钥替换攻击。

3) 非关联性

对于一个合法有效的 (m, m_w, s, e, r_A) 和一组代理签名者 B 保留的中间信息 (k_B, r_B, e^*, s''),都存在一组消息拥有者 R 秘密选取的 (a, b, c) 与之相对应。由以上的设计方案可以看出,代理签名者 B 无法求出 (a, b, c),从而代理人就不能通过自己所掌握的中间信息 (k_B, r_B, e^*, s'') 来确定签名是否就是转换为公开后的代理盲签名。故改进后的新方案具有非关联性。

4.2 改进后新方案的效率分析

为方便,令 T_e、T_i、T_m 分别表示模幂、模逆和模乘运算所需的时间。表 1 列举了 HSQ 方案和改进后提出的新方案在计算量上的比较。可以看出,改进后的方案比 HSQ 方案的计算效率更高。

表 1 HSQ 方案与本文提出的新方案计算量的对比

方案	授权阶段	签名阶段	验证阶段	总计
HSQ 方案	$3T_e + 2T_m$	$5T_e + T_i + 6T_m$	$3T_e + 3T_m$	$11T_e + T_i + 11T_m$
本文的新方案	$4T_e + 5T_m$	$4T_e + T_i + 4T_m$	$2T_e + T_m$	$10T_e + T_i + 10T_m$

5 结束语

通过对 HSQ 方案进行分析,本文指出文献[13]的代理盲签名方案在基于离散对数下并不安全,容易引起原始签名人的公钥替换攻击。针对这个缺陷,给出了对该方案的公钥替换攻击的具体方法,并且对其提出了相应的改进方案。改进后的方案在更高的安全性的前提下提高了效率。

参考文献:

[1] MAMBO M, USBDA K, OKAMOTO E. Proxy signatures for delegating signing operation [C] //Proc of the 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996: 48-57.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages [J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 1996, 79(9): 1338-1354.

[3] CHAUM D. Blind signatures for untraceable payments [C] //Advances in Cryptology: Proceedings of Crypto. [S. l.]: Plenum Press, 1982: 199-203.

[4] LIN W D, JAN J K. A security personal learning tools using a proxy blind signature scheme [C] //Proc of International Conference on Chinese Language Computing. 2000: 273-277.

[5] HE De-biao, CHEN Jian-hua, JIN Hu. An ID-based proxy signature schemes without bilinear pairings [J]. Annals of Telecommunications, 2011, 66(11): 657-662.

[6] ZHANG Bo, XU Qiu-liang. Certificateless proxy blind signature scheme from bilinear pairings [C] //Proc of the 2nd International Workshop on Knowledge Discovery and Data Mining. [S. l.]: IEEE Press, 2009: 573-576.

[7] VERMA S, SHARMA B K. A new proxy blind signature scheme based on DLP [J]. International Journal of Information and Network Security, 2012, 1(2): 60-66.

[8] TAN Zuo-wen, LIU Zhuo-jun, TANG Chun-ming. Digital proxy blind signature schemes based on DLP and ECDLP [J]. MM Research Preprints, 2002, 21(7): 212-217.

[9] SUN H M, HSIEH B T, TSENG S M. On the security of some proxy blind signature schemes [J]. Journal of Systems and Software, 2005, 74(3): 297-302.

[10] WANG Shao-bin, HONG Fan, CUI Guo-hua. Secure efficient proxy blind signature schemes based DLP [C] //Proc of the 7th IEEE International Conference on E-Commerce Technology. [S. l.]: IEEE Press, 2005: 452-455.

[11] 李方伟,谭利平,邱成刚. 基于离散对数的代理盲签名 [J]. 电子科技大学学报, 2008, 37(2): 172-174.

[12] 柳菊霞,苏靖枫. 基于离散对数的代理盲签名方案 [J]. 计算机应用, 2010, 30(8): 2167-2169.

[13] 何俊杰,孙芳,祁传达. 一个代理盲签名方案的安全性分析 [J]. 计算机应用研究, 2012, 29(5): 1904-1906.