一个代理盲签名方案的安全性分析*

何俊杰[a]，孙　芳[b]，祁传达[a]
（信阳师范学院 a. 数学与信息科学学院；b. 计算机与信息技术学院，河南 信阳 464000）

摘　要：对柳菊霞等人提出的一种基于离散对数的代理盲签名方案进行了安全性分析，指出方案不满足强不可伪造性和非关联性，为此，提出了一种改进的代理盲签名方案。新方案中，在代理阶段使用授权证书，有效抵抗了原始签名人的伪造攻击；在盲签名阶段增加盲因子，实现了非关联性。分析表明，新方案满足代理盲签名方案的安全性要求，且具有较高的计算效率。

关键词：代理盲签名；离散对数；伪造攻击；非关联性；授权证书
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2012)05-1904-03
doi:10.3969/j.issn.1001-3695.2012.05.081

Cryptanalysis of proxy blind signature scheme

HE Jun-jie[a], SUN Fang[b], QI Chuan-da[a]
(*a. College of Mathematics & Information Science, b. College of Computer & Information Technology, Xinyang Normal University, Xinyang Henan* 464000, *China*)

Abstract: Cryptanalysis of the proxy blind signature scheme based on DLP which was proposed by Liu et al. showed that the scheme didn't satisfy strongly unforgeability and unlinkability. This paper proposed an improved scheme to overcome these security problems. By using authorized certificate in the stage of proxy designation, it effectively resisted the original signer's forgery attacks; by increaseing the number of blind elements in the stage of blind signing, it satisfied the unlinkability of the new shceme. Analysis result shows that the new shceme satisfies the requirements of proxy blind signature scheme and has high calculating efficiency.

Key words: proxy blind signature; discrete logarithm; forgery attack; unlinkability; authorized certificate

数字签名技术作为信息安全领域的一项重要技术，在保证信息完整性、实现网络身份认证和不可否认性等方面都有重要应用。1982 年，Chaum[1] 为了实现不可跟踪的支付系统，首次提出盲签名的概念。一个安全的盲签名方案一般需要满足两条性质：a）盲性，即要求签名人在不知道被签文件的具体内容的情况下对文件进行签名；b）非关联性，即在签名公布后，签名人不能跟踪消息的拥有者。由于盲签名具有盲性和匿名性，能有效地保护用户的隐私，被广泛地应用于匿名电子支付系统、匿名电子投票系统等场合。为适应不同的需求，各种盲签名方案陆续被提出，如群盲签名[2]、部分盲签名[3,4]、基于身份的盲签名[5]等。1996 年，Mambo 等人[6] 首次提出代理签名的概念。在代理签名中，原始签名人可以将其签名的权利授予一个他指定的人或群体，即代理签名人，代理签名人根据原始签名人的意图代替原始签名人行使签名权。一个好的代理签名方案一般需要满足以下安全性要求：a）可验证性，即通过代理签名，验证者能够确信原始签名人确实授权代理签名人对文件进行了有效的签名；b）可区分性，即任何人都可以区分代理签名和一般签名的不同；c）强可识别性，即任何人能够从代理签名中确认代理签名人的身份；d）强不可否认性，即代理签名人不能否认其生成的有效代理签名；e）强不可伪造性，即只有指定的代理签名人能够产生有效的代理签名，原始签名人和任何第三方都不能产生有效的代理签名；f）防滥用性，即代理签名人不能签署未经授权的信息；g）可注销性，即原始签名人可以注销其委托给代理签名人的签名权利。

2000 年，Lin 等人[7] 提出了第一个代理盲签名方案，这种方案既具有盲签名的性质又具有代理签名的性质。2002 年，Tan 等人[8] 在 Schnorr 盲签名的基础上，结合代理签名提出了一种基于离散对数的代理盲签名方案，但 Sun 等人[9] 指出该方案是不安全的，容易受到伪造攻击，且具有关联性。随后，大量基于不同数学难题、具有不同特性的代理盲签名方案被提出[10,11]。2010 年，柳菊霞等人[12] 对 Tan 等人的方案[8] 进行了改进，提出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。

本文对文献[12]所提出的代理盲签名方案进行了安全性分析，指出方案存在以下安全缺陷：a）原始签名人可以伪造代理签名密钥，与消息拥有者交互生成有效的代理盲签名，即方案不满足强不可伪造性；b）签名公布后，代理签名人可以通过保留的相关中间结果对消息拥有者进行跟踪，即方案具有关联性。为此，本文给出了一种改进方案。

1　柳菊霞等人[12]的代理盲签名方案回顾

1.1　系统参数

设 p,q 是两个大素数且满足 $q|(p-1)$；$g\in Z_q^*$，且 g 的阶

收稿日期：2011-09-19；**修回日期**：2011-10-25　　**基金项目**：河南省自然科学基金资助项目(102102210242)；河南省教育厅自然科学基金资助项目(12A520034)

作者简介：何俊杰(1981-)，男，讲师，硕士，主要研究方向为信息安全(hejj99@163.com)；孙芳(1981-)，女，讲师，硕士，主要研究方向为信息安全；祁传达(1965-)，男，教授，硕导，博士，主要研究方向为密码理论.

为 q,即 $g^q \equiv 1 \pmod p$。系统中 A 为原始签名人,B 为代理签名人,R 为消息拥有者;$x_A, x_B \in Z_q^*$ 分别为 A、B 的私钥,相应的公钥分别为 $y_A = g^{x_A} \bmod p$ 和 $y_B = g^{x_B} \bmod p$;m 为待签名的消息;$H(*)$ 为无碰撞的哈希函数。

1.2 代理阶段

a)原始签名人 A 选择随机数 $\bar{k} \in_R Z_q^*$,计算 $\bar{r} = g^{\bar{k}} \bmod p$,$\bar{s} = (x_A \bar{r} + \bar{k}) \bmod q$;

b)A 通过安全信道将$(\bar{r}, \bar{s})$传送给代理签名人 B;

c)B 收到$(\bar{r}, \bar{s})$后,首先验证等式 $g^{\bar{s}} = \bar{r}\, y_A^{\bar{r}} \bmod p$ 是否成立,如果成立,接受委托并计算 $s' = \bar{s} + x_B \bmod q$,并把 s'作为其代理私钥,$y_p = \bar{r}\, y_A^{\bar{r}}\, y_B \bmod p$ 为对应的代理公钥。

1.3 签名阶段

a)B 随机选择 $k \in_R Z_q^*$,计算 $t = g^k \bmod p$,并把$(\bar{r}, t)$发送给消息拥有者 R。

b)R 收到$(\bar{r}, t)$后,选择随机数 $a, b \in_R Z_q^*$,计算 $r = t^t g^a y_p^b \bmod p$,$e = H(r \parallel m) \bmod q$,$e^* = (b - e) \bmod q$。如果 $r = 0$,重复 b),直到 $r \neq 0$,并将 e^* 发送给 B。

c)B 收到 e^* 后,计算 $s'' = (kt + e^* s') \bmod q$,然后将 s''发送给 R。

1.4 签名提取阶段

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

1.5 签名验证阶段

签名验证者验证等式 $e = H(g^s y_p^e \bmod p \parallel m) \bmod q$ 是否成立,如果等式成立,证明(m, s, e)是消息 m 的有效签名;否则,视签名无效。

2 柳菊霞等人[12]的代理盲签名方案的分析

柳菊霞等人在验证方案的正确性后,进一步对方案进行了安全分析,指出方案能够抵抗原始签名人和签名接收者的一般性伪造攻击,且方案具有非关联性。本文对柳菊霞等人提出的方案进行分析,指出方案不具备非关联性,同时原始签名人可以伪造代理签名密钥。

2.1 原始签名人的伪造攻击[13]

不诚实的原始签名人 A 随机选择 $c \in Z_q^*$,计算 $\bar{r} = g^c y_B^{-1} \bmod p$,$\tilde{s}' = (x_A \bar{r} + c) \bmod q$,$\tilde{s}'$就是一个有效的代理签名密钥,相应的公钥为 $\tilde{y}_p = \bar{r}\, y_A^{\bar{r}} y_B \bmod p$。事实上,$\tilde{y}_p = \bar{r}\, y_A^{\bar{r}} y_B \bmod p = g^c y_B^{-1} y_A^{\bar{r}} y_B \bmod p = g^{x_A \bar{r} + c} \bmod p = g^{\tilde{s}'} \bmod p$。原始签名人可以使用上述方法伪造代理签名私钥 $\tilde{s}'$与签名接收者交互作用就可以生成代理盲签名,并声称是由 B 签名的。

2.2 恶意消息拥有者对代理密钥的攻击

在柳菊霞等人的代理盲签名方案中,代理签名人 B 虽然选取的是随机数 k,但在盲签名方程中实际出现的却是 kt,其中 $t = g^k \bmod p$。同时,消息拥有者 R 在盲化消息时,r 的因子 t^t 可以表示成 g^{kt}。B 可以直接将 $k' = kt \bmod q$ 当做消息密钥,把 $g^{k'} \bmod p = g^{kt} \bmod p = t^t \bmod p$ 发送给 R,也能完成签名过程。柳菊霞等人用这种方式处理随机数,期望方案具有非关联性,但实际上这样做不但增加了不必要的计算量,而且降低了签名方案的安全性。

利用 ElGamal 型数字签名方案对两个不同的消息签名时,如果选择了相同的随机数,攻击者就可以计算随机数的值,进而计算出私钥。在柳菊霞等人的代理盲签名方案中,即使代理签名人对不同的消息选取不同的随机数进行签名,也会存在暴露代理密钥的危险。设对两个消息选择不同的随机数 k_1、k_2,满足 $k_1^{k_1} \equiv k_2^{k_2} \pmod p$,即 $g^{k_1 t_1} \equiv g^{k_2 t_2} \pmod p$,其中 $t_i = g^{k_i} \bmod p$ $(i = 1, 2)$,进而可知 $k_1 t_1 \equiv k_2 t_2 \pmod q$。设两盲签名方程分别为 $s''_1 = (k_1 t_1 + e_1^* s') \bmod q$,$s''_2 = (k_2 t_2 + e_2^* s') \bmod q$,两式相减,可得 $s''_1 - s''_2 = (e_1^* - e_2^*) s' \bmod q$,若 $(e_1^* - e_2^*) \neq 0 \bmod q$,则可以计算出代理签名私钥 $s' = (e_1^* - e_2^*)^{-1} (s''_1 - s''_2) \bmod q$。

2.3 方案具有关联性

假设代理签名人 B 保留了所有签名的中间结果。当签名接收者 R 公布签名(m, s, e)后,B 针对每一组中间结果(k, t, e^*, s''),通过等式 $e^* = (b - e) \bmod q$ 和 $s = (a + s'') \bmod q$ 计算出 $b = e^* + e \bmod q$ 和 $a = (s - s'') \bmod q$。验证等式 $e = H(t^t g^a y_p^b \bmod p \parallel m) \bmod q$,若成立,则说明该签名就是选择的$(k, t, e^*, s'')$所对应的代理签名,进而达到跟踪消息 m 的拥有者。因此,方案具有关联性。

3 柳菊霞等人[12]的代理盲签名方案的改进

针对柳菊霞等人代理盲签名方案中存在的安全隐患,本文提出了一个改进方案。改进的代理盲签名方案在代理授权阶段引入授权证书 m_w,以抵抗原始签名人的伪造攻击;在盲签名阶段使用三个随机数进行消息盲化,以达到增强方案的安全性的同时使方案具有非关联性的目的。

3.1 方案描述

3.1.1 系统初始化

$p, q, g, x_A, x_B, y_A, y_B, m, H(*)$ 与 1.1 节相同。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。

3.1.2 代理阶段

a)原始签名人 A 选择随机数 $\bar{k} \in_R Z_q^*$,计算 $\bar{r} = g^{\bar{k}} \bmod p$,$\bar{s} = (\bar{k} \cdot H(\bar{r} \parallel m_w) + x_A) \bmod q$;

b)A 通过安全信道将$(\bar{r}, \bar{s})$传送给代理签名人 B;

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

3.1.3 签名阶段

a)B 随机选择 $k \in_R Z_q^*$,计算 $t = g^k \bmod p$,并把$(m_w, \bar{r}, t)$发送给消息拥有者 R;

b)R 收到$(m_w, \bar{r}, t)$后,选择随机数 $a, b, c \in_R Z_q^*$,计算 $r = t^c g^a (y_A y_B \bar{r}^{H(\bar{r} \parallel m_w)})^b \bmod p$,$e = H(r \parallel m) \bmod q$,$e^* = c^{-1}(b - e) \bmod q$,如果 $r = 0$,重复 b),直到 $r \neq 0$,并将 e^* 发送给 B;

c)B 收到 e^* 后,计算 $s'' = (k + e^* s') \bmod q$,然后将 s''发送给 R。

3.1.4 签名提取阶段

R 收到 s''后,计算 $s = (cs'' + a) \bmod q$,这时$(m, m_w, s, e, \bar{r})$就是消息 m 的代理盲签名。

3.1.5 签名验证阶段

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

$$g^s(y_A y_B \bar{r}^{H(\bar{r}\|m_w)})^e \equiv g^{cs''+a}(g^{x_A}g^{x_B}g^{kH(\bar{r}\|m_w)})^e \equiv$$
$$g^{c(k+e^*s')+a}(y_A y_B \bar{r}^{H(\bar{r}\|m_w)})^e \equiv$$
$$g^{ck}g^a y_p^{e+ce^*} \equiv r^c g^a y_p^b \equiv r(\bmod p)$$

说明验证过程正确。

3.2 方案分析

3.2.1 安全性分析

1)可验证性 签名验证者得到代理盲签名$(m, m_w, s, e, \bar{r})$后,可以通过验证方程 $e = H(g^s(y_A y_B \bar{r}^{H(\bar{r}\|m_w)})^e \bmod p \| m) \bmod q$ 来验证代理盲签名的合法性。

2)可区分性 有效的代理盲签名中包含有授权证书 m_w,任何人都能区分出代理盲签名和一般盲签名的不同。

3)强可识别性 代理盲签名中含有授权证书 m_w,其中包含了代理签名人的身份信息,任何人都可以确定代理签名人的身份。

4)强不可伪造性

a)方案能够有效抵抗第三方的伪造攻击。第三方没有原始签名人和代理签名人的密钥,也没有原始签名人对授权证书 m_w 的签名$(\bar{r}, \tilde{s})$,进而不可能伪造代理签名密钥 s'。盲签名阶段是基于 Schnorr 签名体制设计的,由 Schnorr 签名体制的安全性可知,在没有原始签名人的私钥和代理签名人的私钥的情况下,第三方无法冒充原始签名人生成普通盲签名,也无法冒充代理签名人生成代理盲签名。

b)方案能够抵抗原始签名人的伪造攻击。恶意的原始签名人 A 要想伪造出消息 m 的合法签名,需要构造一个有效的代理签名密钥 $\tilde{s}'$。设原始签名人 A 随机选择 $c \in Z_q^*$,令 $\bar{r} = g^c u \bmod p$,即 $\bar{k} = (c + \log_g u) \bmod q$,则

$$\tilde{s}' = (\bar{k}H(\bar{r}\|m_w) + x_A + x_B) \bmod q =$$
$$((c + \log_g u)H(g^c u\|m_w) + x_A + x_B) \bmod q =$$
$$(cH(g^c u\|m_w) + H(g^c u\|m_w)\log_g u + x_A + x_B) \bmod q$$

为了伪造 $\tilde{s}'$,可以令 $cH(g^c u \| m_w) + x_B \equiv 0 (\bmod q)$ 或 $H(g^c u \| m_w)\log_g u + x_B \equiv 0 (\bmod q)$,即 $y_B g^{cH(g^c u\|m_w)} \equiv 1 (\bmod p)$ 或 $y_B u^{H(g^c u\|m_w)} \equiv 1 (\bmod p)$,想解出 u,会遇到离散对数难题和哈希函数求逆运算。所以原始签名人无法使用 2.1 节的攻击方法伪造代理签名密钥,从而保证了代理签名人的合法权益。

5)强不可否认性 盲签名过程中用到了代理签名的私钥 s',而代理签名的私钥只有代理签名人 B 才能产生,因此代理签名人不可能否认自己产生的代理盲签名。

6)非关联性 假设代理签名人 B 保留了所有签名的中间结果(k, t, e^*, s''),当消息拥有者 R 公布签名$(m, m_w, s, e, \bar{r})$后,B 通过等式 $e^* = c^{-1}(b - e) \bmod q$ 和 $s = (cs'' + a) \bmod q$ 无法计算出三个随机数 a、b、c 及它们的线性组合,也就不能通过 $r = t^c g^a y_p^b \bmod p$ 计算出 r。因此,新方案具有非关联性。

7)防滥用性 授权委托证书 m_w 中包含授权时间和代理的有效期限、可签消息范围等信息,可以限制代理签名人将代理权限用于其他未授权的签名中,防止代理权限的滥用。

8)可注销性 如果原始签名人 A 想收回代理签名人 B 的代理签名权,那么他可以在系统内公布消息,宣布授权证书 m_w 和签名信息 $\bar{r}$ 无效,使得代理签名的验证公钥 $y_A y_B \bar{r}^{H(\bar{r}\|m_w)} \bmod p$ 无效,从而达到注销 B 所拥有的代理密钥 s'的目的。

3.2.2 计算效率分析

令 T_e、T_i 和 T_m 分别表示一次模幂、模逆和模乘运算所需的时间。将新方案与柳菊霞等人[12]的方案和 Tan 等人[8]的方案在计算效率上进行比较,结果如表 1 所示。由于引入了授权证书,使得在盲签名阶段和签名验证阶段,消息拥有者和签名验证者需要分别生成代理签名的公钥 $y_A y_B \bar{r}^{H(\bar{r}\|m_w)} \bmod p$,增加了两次模乘运算和一次模幂运算。可以看出,本文方案比柳菊霞等人方案的时间复杂度稍高,但比 Tan 等人方案的计算效率高很多。

表 1 三个方案的时间复杂度比较

比较项	本文方案	柳菊霞等人[12]的方案	Tan 等人[8]的方案
授权阶段	$3T_e + 2T_m$	$4T_e + 4T_m$	$3T_e + 2T_m$
盲签名阶段	$5T_e + T_i + 6T_m$	$4T_e + 5T_m$	$8T_e + 4T_i + 7T_m$
验证阶段	$3T_e + 3T_m$	$2T_e + T_m$	$3T_e + T_i + 3T_m$
小计	$11T_e + T_i + 11T_m$	$10T_e + 10T_m$	$12T_e + 5T_i + 12T_m$

4 结束语

本文分析了柳菊霞等人提出的改进的代理盲签名方案,指出该方案存在安全隐患,不能应用于电子现金、电子投票等领域。针对该代理盲签名方案存在的不足,提出了一种改进的方案,新方案能够有效地防止原始签名人的一般性伪造攻击,并满足非关联性。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[J]. Advances in Cryptology Proceedings of Crypto,1983,82(3):199-203.

[2] LYSYANSKAYA A, RAMZAN Z. Group blind digital signatures: a scalable solution to electronic cash[C]//Proc of the 2nd International Conferenceon on Financial Cryptography. London: Springer-Verlag,1998:184-197.

[3] ABE M, FUJISAKI E. How to date blind signatures[C]//Proc of Advances in Cryptology-ASIACRYPT. Berlin: Springer-Verlag, 1996:224-251.

[4] ABE M, OKAMOTO T. Provably secure partially blind signatures [C]//Proc of Advances in Cryptology-CRYPTO. Berlin: Springer-Verlag,2000:271-299.

[5] ZHANG Fan-guo, KIM K. ID-based blind signature and ring signature from pairings[C]//Proc of Advances in Cryptology-ASIACRYPT. Berlin: Springer-Verlag,2002:533-547.

[6] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans on Fundamentals, 1996,E79-A(9):1338-1354.

[7] 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. Washington DC: IEEE Computer Society,2000:273-277.

[8] TAN Zuo-wen, LIU Zhou-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. On the security of some proxy signature schemes[EB/OL]. (2003-05-06)[2011-06-05]. http://eprint.iacr.org/2003/068.

[10] 张建中, 王洁, 刘勤喜. 新的代理盲签名方案及其在电子现金中的应用[J]. 计算机应用研究,2009,26(1):347-349.

[11] 何金妮, 辛小龙. 具有消息恢复的代理盲签名[J]. 计算机工程与应用,2010,46(35):112-114.

[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] 傅晓彤, 卢明欣, 肖国镇. 对一类基于离散对数的代理盲签名体制的伪造攻击[J]. 西安电子科技大学学报,2005,32(5):777-780.