第 36 卷 第 8 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.8 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)08—0130—02 文献标识码：A 中图分类号：TN918

多重代理盲签名分析

王国瞻，亢保元，成 林
(中南大学数学科学与计算技术学院，长沙 410075)

摘 要：多重代理盲签名是代理盲签名的延伸，被授权的代理签名者代替多个原始签名者进行签名。采用构造方法，分析一个不需要安全渠道的多重代理盲签名方案的安全性，结果证明其不安全，不满足不可伪造性和不可链接性，不能用于电子商务、电子货币、电子投票等系统。

关键词：代理签名；盲签名；多重代理

Analysis of Multi-proxy Blind Signature

WANG Guo-zhan, KANG Bao-yuan, CHENG Lin
(School of Mathematical Science and Computing Technology, Central South University, Changsha 410075)

【Abstract】A multi-proxy blind signature is an extension of proxy blind signature, which allows the designated proxy signer to generate a signature on behalf of several original signers. The security of a proxy blind multi-signature scheme without a secure channel is analyzed with the method of construction. The results show that this proxy blind signature scheme is not secure. The scheme does not satisfy the properties of unforgeability and unlinkbility. It can not be applied to e-commerce, e-cash and e-voting system.

【Key words】proxy signature; blind signature; multi-proxy

1 概述

文献[1]首次提出盲签名概念，盲签名包括签名者和签名申请者两方。签名者为签名申请者进行签名且不知道消息内容。盲签名方案在很多领域被应用，如电子货币、电子投票等。文献[2]提出代理签名的概念，以代理签名者代替原始签名者进行签名。盲签名和代理签名的结合即代理盲签名。多重代理盲签名是代理盲签名的延伸和扩展，其中有 n 个原始签名者 $A_1, A_2, \cdots, A_n$。每个原始签名者从自己的私钥中产生子密钥 s_i，并把它传给代理签名者 B，B 收到所有有效的 s_i 后，和他自己的私钥一起产生代理签名密钥。代理签名者可以用该代理签名密钥代替原始签名者进行签名。文献[3]提出一个多重代理盲签名方案，并声称该方案满足不可伪造性和不可链接性，本文受文献[4]对文献[5]方案以及文献[5]对文献[6]方案的攻击方式的启发，采用构造方法证明文献[3]方案是不安全的。

2 文献[3]的多重代理签名方案

2.1 初始化阶段

任意选择 2 个大素数 p 和 q，其中，$q|p$-1; $g \in z_p^*$，$g^q \equiv 1 (\mathrm{mod}\ p)$。$A_1, A_2, \cdots, A_n$ 为 n 个原始签名人，B 为代理签名人。每个原始签名人有一个私钥 $x_i \in_R z_q^*$，公钥 $y_i = g^{x_i} (\mathrm{mod}\ p)$。代理签名者有私钥 x_B，公钥 $y_B = g^{x_B} (\mathrm{mod}\ p)$。另外有 3 个安全的哈希函数 $H(\cdot)$, $H_1(\cdot)$, $H_2(\cdot)$。

2.2 代理子密钥产生阶段

每个原始签名人 A_i $(1 \le i \le n)$ 从他的私钥中产生一个代理子密钥 s_i，并经任意渠道把它传给 B，A_i 选择 $k_i \in_R z_q^*$ 并计算 $r_i = g^{k_i} (\mathrm{mod}\ p)$, $s_i = x_i H(m_w, r_i) + k_i (\mathrm{mod}\ q)$。其中，$m_w$ 是所有原始签名人公认的代理授权书，包括代理权限、代理期限、所有原始签名人的公钥等。选择 $k_i' \in_R z_q^*$ 并计算

$$(r_i', c_i, r_i'', s_i') : r_i' = g^{k_i'} (\mathrm{mod}\ p),\ c_i = s_i \cdot r_i' \cdot y_B^{k_i} (\mathrm{mod}\ p)$$

$$r_i'' = H_1(c_i, r_i, r_i'),\ s_i' = k_i' \cdot (r_i'' + x_i)^{-1} (\mathrm{mod}\ q)$$

公布 (r_i, m_w) 并发送 (c_i, r_i'', s_i') 给 B，通过任意渠道，任何人都可以获得 (c_i, r_i'', s_i')，但对本文方案没有影响。

2.3 子密钥验证阶段

在 B 收到 (c_i, r_i'', s_i') 后验证它并重新得到 s_i，先计算

$$r_i' = (y_i \cdot g^{r_i''})^{s_i'} = g^{(r_i''+x_i)s_i'} = g^{(r_i''+x_i)\cdot k_i' \cdot (r_i''+x_i)^{-1}} = g^{k_i'} (\mathrm{mod}\ p)$$

检测等式 $r_i'' = H_1(c_i, r_i, r_i')$ 是否成立。如果成立则认为 (c_i, r_i'', s_i') 是原始签名人 A_i 产生的，否则拒绝。(c_i, r_i'', s_i') 被证明有效后，B 用他的私钥 x_B 重新得到 s_i，即

$$s_i = c_i \cdot r_i'^{-1} \cdot r_i^{-x_B} = s_i \cdot r_i' \cdot y_B^{k_i} \cdot r_i'^{-1} \cdot r_i^{-x_B} = s_i (\mathrm{mod}\ p)$$

通过 $g^{s_i} = r_i \cdot y_i^{H(m_w, r_i)} (\mathrm{mod}\ p)$ 验证 s_i，因为

$$g^{s_i} = r_i \cdot g^{x_i \cdot H(m_w, r_i) + k_i} = r_i \cdot y_i^{H(m_w, r_i)} (\mathrm{mod}\ p)$$

所以如果等式成立则接受 s_i，否则拒绝。

2.4 代理密钥的产生阶段

在 B 接受了 n 个有效的 s_i 之后，产生代理密钥 sk

$$sk = \sum_{i=1}^{n} s_i + x_B (\mathrm{mod}\ q)$$

2.5 签名阶段

代理密钥产生之后，代理签名者 B 可以代替所有原始签

基金项目：国家自然科学基金资助项目(10871205)
作者简介：王国瞻(1984－)，男，硕士，主研方向：密码学，信息安全；亢保元，教授、博士；成 林，硕士
收稿日期：2009-12-27 **E-mail：**wgzcsu2008@yahoo.cn

名人进行签名，假设签名要求者 C 要求代理签名者 B 对消息 m 进行签名，则代理签名者 B 选择 $w_1 \in_R z_q^*$，计算 $x = g^{w_1} (\mathrm{mod}\ p)$，并把 x 传给 C，C 按照代理签名者和所有原始签名者的公钥及所有公布的 r_i 计算

$$\alpha = y_B \prod_{i=1}^{n} (r_i \cdot y_i^{H(m_w, r_i)}) (\mathrm{mod}\ p)$$

C 选择 $w_2, w_3 \in_R z_q^*$，并计算

$$x^* = g^{w_2} \cdot \alpha^{w_3} \cdot x (\mathrm{mod}\ p),\ e^* = H_2(x^*, m),\ e = e^* + w_3 (\mathrm{mod}\ q)$$

把 e 传给 B，B 接受 e 后，计算 $y = w_1 + e \cdot sk (\mathrm{mod}\ q)$，并把 y 传给 C。C 接受 y 后，计算 $y^* = y + w_2 (\mathrm{mod}\ q)$，形成对消息 m 的代理盲签名 (e^*, y^*)。

2.6 代理验证阶段

在代理盲签名 (e^*, y^*) 产生之后，任何人都可以验证该签名。与 C 用相同的方法计算 α，并计算：

$$x^* = g^{y^*} \cdot \alpha^{-e^*} = g^{w_1 + y} \cdot \alpha^{-e^*} = g^{w_1 + w_2 + e \cdot sk} \cdot \alpha^{-e^*} = g^{w_1 + w_2 + w_3 \cdot sk + e^* \cdot sk} \cdot \alpha^{-e^*} = g^{w_1 + w_2} \cdot \alpha^{w_3} \cdot \alpha^{e^*} \cdot \alpha^{-e^*} = g^{w_2} \cdot \alpha^{w_3} \cdot x (\mathrm{mod}\ p)$$

计算 $e'^* = H(x^*, m)$，并且验证 $e'^* = e^*$ 是否成立。如果成立则认为 (e^*, y^*) 是对消息有效的签名，否则拒绝该签名。

3 对文献[3]方案的攻击方案

3.1 原始签名人的伪造方案

不可伪造性是指只有被授权的代理签名者才能产生有效的代理盲签名，其他任何人(包括原始签名人)不能伪造签名。

本节中 (r_i', s_i') 与 2.2 节中 (r_i, s_i) 的每个原始签名人构造的 (r_i', s_i') 无关。所有不诚实的原始签名人一起伪造文献[3]的方案。

每个原始签名人 A_i $(1 \le i \le n)$ 任意选择 $v_i \in z_q^*$，并计算 $r_i' = y_B^{\frac{1}{n}} g^{v_i} (\mathrm{mod}\ p)$，$s_i' = x_i \cdot H(m_w, r_i') + v_i (\mathrm{mod}\ q)$，所以，$g^{s'} = y_i^{H(m_w, r_i')} \cdot r_i' \cdot y_B^{\frac{1}{n}} (\mathrm{mod}\ p)$ 成立。每个原始签名人把 (r_i', s_i') 传给其中的一个 A_1 $(1 \le i \le n)$。例如，原始签名人 A_i $(2 \le i \le n)$ 把 (r_i', s_i') 传给原始签名人 A_1。在 A_1 接收到 $n-1$ 个 (r_i', s_i') 后，与他的 (r_1', s_1') 一起产生代理签名密钥

$$sk' = \sum_{i=1}^{n} s_i'$$

在 sk' 产生之后，A_1 可以代替其他原始签名人进行盲签名。假设 C 要求为消息 m 进行签名，A_1 选择 $w_1 \in_R z_q^*$，计算 $x = g^{w_1} (\mathrm{mod}\ p)$ 并 x 把传给 C。C 计算

$$\alpha = y_B \prod_{i=1}^{n} (r_i' \cdot y_i^{H(m_w, r_i')}) (\mathrm{mod}\ p)$$

签名接受者 C 选择 $w_2, w_3 \in_R z_q^*$，并计算 $x^* = g^{w_2} \cdot \alpha^{w_3} \cdot x (\mathrm{mod}\ p)$，$e^* = H_2(x^*, m)$，$e = e^* + w_3 (\mathrm{mod}\ q)$，把 e 传给 A_1。A_1 接受 e 后，计算 $y = w_1 + e \cdot sk' (\mathrm{mod}\ q)$ 并把 y 传给 C。C 接受 y 后，计算 $y^* = y + w_2 (\mathrm{mod}\ q)$，形成对消息 m 的代理盲签名 (e^*, y^*)。

在签名 (e^*, y^*) 产生后，任何人都可以验证它。采用与 C 相同的方法计算 $\alpha = y_B \prod_{i=1}^{n} (r_i' \cdot y_i^{H(m_w, r_i')}) (\mathrm{mod}\ p)$ 并计算 $x^* = g^{y^*} \cdot \alpha^{-e^*}$。计算 $e'^* = H_2(x^*, m)$，并验证 $e'^* = e^*$ 是否成立。如果成立则认为 (e^*, y^*) 是对消息 m 有效的多重代理盲签名。对其有效性证明如下：

$$g^{sk'} = g^{\sum_{i=1}^{n} s_i'} = g^{\sum_{i=1}^{n} (x_i \cdot H(m_w, r_i') + v_i)} = \prod_{i=1}^{n} y_i^{H(m_w, r_i')} \cdot \prod_{i=1}^{n} g^{v_i} = \prod_{i=1}^{n} y_i^{H(m_w, r_i')} \cdot y_B \cdot \prod_{i=1}^{n} r_i' = y_B \cdot \prod_{i=1}^{n} (y_i^{H(m_w, r_i')} \cdot r_i') = \alpha$$

可得如下等式：

$$x^* = g^{y^*} \cdot \alpha^{-e^*} = g^{y + w_2} \cdot \alpha^{-e^*} = g^{w_1 + w_2 + e \cdot sk'} \cdot \alpha^{-e^*} = g^{w_1 + w_2 + (e^* + w_3) \cdot sk'} \cdot \alpha^{-e^*} = g^{w_2} \cdot \alpha^{w_3} \cdot x (\mathrm{mod}\ p)$$

因此，可得

$$e'^* = H_2(x^*, m) = H_2(g^{y^*} \cdot \alpha^{-e^*}, m) = H_2(g^{w_2} \cdot \alpha^{w_3} \cdot x, m) = e^*$$

可见，等式 $e'^* = e^*$ 成立，即 (e^*, y^*) 是对消息 m 有效的多重代理盲签名，原始签名人的伪造攻击成功，即文献[3]多重代理盲签名不满足不可伪造性。

3.2 对文献[3]方案的链接性攻击

不可链接性是指当最终签名产生后，代理签名者不能把公布的消息和他的签名链接起来。

本节证明文献[3]方案不满足不可链接性，代理签名人可以追踪其签名。在文献[3]方案中，代理签名者保持所有 (w_{1i}, x_i, e_i, y_i)，在签名 (e^*, y^*) 接受者公布后，对所有的 i，代理签名者可以计算 $w_2' = y^* - y_i (\mathrm{mod}\ q),\quad w_3' = e_i - e^* (\mathrm{mod}\ q)$，并验证等式 $e'^* = e^*$ 是否成立。若对于所有 i，等式都成立，则方案满足不可链接性，但

$$g^{y^*} \cdot \alpha^{-e^*} = g^{y_i + w_2'} \cdot \alpha^{-e^*} = g^{w_{1i} + e_i \cdot sk + w_2'} \cdot \alpha^{-e^*} = g^{w_{1i} + (w_3' + e^*) \cdot sk + w_2'} \cdot \alpha^{-e^*} = g^{w_{1i} + w_2'} \cdot \alpha^{w_3'} = x_i \cdot g^{w_2'} \cdot \alpha^{w_3'} \ne x \cdot g^{w_2} \cdot \alpha^{w_3}$$

即等式不是恒成立的。对某个 i，$x_i = x$，$y_i = y$，$w_1 = w_1'$，$w_2 = w_2'$，$e_i = e$，等式 $e'^* = e^*$ 成立。而对于其他 i，等式不成立，即 (w_{1i}, x_i, e_i, y_i) 对于公布的消息 m 是链接的。

4 结束语

本文指出文献[3]多重代理盲签名方案是不安全的，它不满足不可伪造性，不诚实的原始签名人能构造代理签名密钥，从而冒充代理签名人生成有效的代理盲签名。该方案不满足不可链接性，代理签名人可以追踪其签名。

参考文献

[1] Chaum D. Blind Signature for Untraceable Payments[C]//Proc. of Crypto'82. New York, USA: Plenum Press, 1983: 199-203.

[2] Mambo M, Usuda K, Okamoto K. Proxy Signature: Delegation of the Power to Sign Message[J]. IEICE Trans. on Fundamental, 1996, E79-A(9): 1338-1353.

[3] Lu Rongxing, Cao Zhenfu, Zhou Yuan. Proxy Blind Multi-signature Scheme Without a Secure Channel[J]. Applied Mathematics and Cumputation, 2005, 164(1): 179-187.

[4] Wu Lin-Chuan, Yeh Yi-Shiung, Liu Tsann-Shyong. Analysis of Sun et al.'s Linkability Attack on Some Proxy Blind Signature Shemes[J]. System Software, 2006, 79(2): 176-179.

[5] Sun Hungmin, Hsieh B T, Tseng S M. On the Security of Some Proxy Blind Signature Scheme[J]. System Software, 2005, 74(3): 297-302.

[6] Tan Zuowen, Liu Zhuojun, Tang Chunming. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP[J]. MM Research Preprints, 2002, (21): 212-217.

编辑 陈 晖