

文章编号:1001-9081(2009)06-1646-02

代理多重盲签名方案的改进

蔡晓秋¹, 李金周¹, 王天银^{1,2}

(1. 洛阳师范学院 数学科学学院, 河南 洛阳 471022; 2. 北京邮电大学 网络与交换技术国家重点实验室, 北京 100876)

(caixiaoqiu1980@sina.com)

摘要:通过对 LCZ 代理多重盲签名方案的安全性分析,发现任何一个原始签名者都可以冒充代理签名者伪造有效的代理多重盲签名,该方案并不满足强不可伪造性。在 LCZ 方案和 HQL 方案的基础上提出了一种改进方案,改进后的方案有效克服了原方案的安全缺陷,并满足代理多重盲签名的各种要求。

关键词:代理签名;盲签名;多重签名;代理多重盲签名

中图分类号: TP309 **文献标志码:** A

Cryptanalysis of proxy blind multi-signature scheme

CAI Xiao-qiu¹, LI Jin-zhou¹, WANG Tian-yin^{1,2}

(1. School of Mathematical Science, Luoyang Normal University, Luoyang Henan 471022, China;

2. State key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Through the security analysis of LCZ proxy blind multi-signature scheme, it was found that this scheme cannot meet the requirement of strong unforgeability. Any original signer could forge valid proxy blind multi-signatures by impersonating the proxy signer. An improved version was proposed based on LCZ and HQL scheme, which can solve the security problem that exist in LCZ scheme and meet all the requirements of proxy blind multi-signature.

Key words: proxy signature; blind signature; multi-signature; proxy blind multi-signature

0 引言

代理签名在现实生活中有着重要的应用,一提出便受到广泛关注^[1-9]。在实际应用中,有时需要一个代理签名人能够代表多个原始签名人进行代理盲签名,例如多家上市公司委托证券交易所发行一种股票,多家银行委托货币发行部门发行一种货币等。在电子拍卖中,运用代理多重盲签名方案,可以解决竞拍者权力委托、竞拍者身份的匿名性、获胜竞拍者的不可否认性、可公开验证性、竞拍者不可伪装性以及某个竞拍者在不同拍卖中不可关联性问题。

为了解决上述问题,文献[4]给出了一种新的签名体制——代理多重盲签名体制(LCZ 方案)。然而,在 LCZ 方案中,传递代理授权信息时,原始签名人需要对其进行加密;同时,代理签名人在验证代理授权信息时要进行解密,因此,LCZ 方案的计算量较大,而且最后的签名长度随原始签名人的增加而增长。为了解决上述 LCZ 方案的不足之处,文献[6]在 Schnorr 签名方案^[10]的基础上给出了一种新的代理多重盲签名方案(HQL 方案),与 LCZ 方案相比,HQL 方案具有计算量小、效率高和安全性强等优点,而且签名长度不随原始签名人的增加而增长。本文对 LCZ 方案进行了安全性分析,发现在 LCZ 方案中,任何一个原始签名人可以独自冒充代理签名人生成有效的代理多重盲签名,因此,该方案不满足代理签名的强不可伪造性。本文在 LCZ 方案和 HQL 方案的基础上,提出了一种改进方案,并对改进后的方案进行了分析,与 LCZ 方案和 HQL 方案相比,改进后的方案效率更高。

1 LCZ 方案

1.1 初始化阶段

p, q 是大素数,且 $q | p - 1$, g 为 Z_p^* 的阶为 q 的元; $A_i (1 \leq i \leq n)$ 表示原始签名者, B 表示代理签名者, $x_i \in Z_q^*$ 为 A_i 的私钥,对应的公钥为 y_i ,且 $y_i = g^{x_i} \bmod p$, $x_B \in Z_q^*$ 为 B 的私钥,对应的公钥为 y_B ,且 $y_B = g^{x_B} \bmod p$; $H(\cdot)$, $H_1(\cdot)$, $H_2(\cdot)$ 为三个通用安全单向 Hash 函数。

1.2 代理子秘密产生阶段

每个原始签名者 $A_i (1 \leq i \leq n)$ 随机选择 $k_i \in Z_q^*$, 计算: $r_i = g^{k_i} \bmod p$, $s_i = x_i H(m_w, r_i) + k_i \bmod q$, 这里 m_w 表示所有原始签名者协商生成的授权书,它包括代理权限、有效期和所有原始签名者的身份和公钥等信息;接着随机选择 $k'_i \in Z_q^*$, 并计算 $r'_i = g^{k'_i} \bmod p$, $c_i = s_i r'_i y_B^{k_i} \bmod p$, $r''_i = H_1(c_i, r_i, r'_i)$, $s'_i = k'_i (r''_i + x_i)^{-1} \bmod q$;最后公开 (r_i, m_w) , 并将 (c_i, r''_i, s'_i) 发送给代理签名者 B 。

1.3 代理子秘密的验证

代理签名者 B 收到 (c_i, r''_i, s'_i) 后,计算 $r'_i = (y_i g^{r''_i})^{s'_i} = g^{k'_i} \bmod p$, 并验证 $r''_i \stackrel{?}{=} H_1(c_i, r_i, r'_i)$ 是否成立,若成立,则接受 (c_i, r''_i, s'_i) ;接着 B 计算 $s_i = c_i r_i^{-1} r_i^{s'_i} \bmod p$, 并验证 $g^{s_i} \stackrel{?}{=} r_i y_i^{H(m_w, r_i)} \bmod p$ 是否成立,若成立则接受 (c_i, s_i) 。

1.4 代理密钥的产生

代理签名者 B 收到并验证完所有的 (c_i, s_i) 后,计算代理

$$\text{密钥 } sk = \sum_{i=1}^n s_i + x_B \bmod q。$$

收稿日期:2008-12-22;修回日期:2009-02-20。 基金项目:国家 863 计划项目(2006AA01Z419);国家自然科学基金资助项目(60873191);河南省教育厅自然科学基金基础研究计划项目(2008B120005);洛阳师范学院青年基金资助项目(2008-QNJ-012)。

作者简介:蔡晓秋(1980-),女,河南许昌人,讲师,硕士,主要研究方向:数字签名、电子商务;李金周(1962-),男,河南信阳人,讲师,硕士,主要研究方向:数字签名;王天银(1979-),男,河南南阳人,讲师,博士研究生,主要研究方向:信息安全。

1.5 代理签名的产生

假定用户 C 要求代理签名者 B 对消息 m 进行盲签名。

1) 代理签名者 B 随机选择 $w_1 \in_R \mathbf{Z}_q^*$, 计算 $x = g^{w_1} \bmod p$, 并将 x 发送给 C 。

2) 用户 C 根据公开信息计算 $\alpha = y_B \prod_{i=1}^n r_i y_i^{H(m_w, r_i)}$, 然后随机选择 $w_2, w_3 \in_R \mathbf{Z}_q^*$, 计算: $x^* = g^{w_2} \alpha^{w_3} x \bmod p$, $e^* = H_2(x^*, m)$, $e = (e^* + w_3) \bmod q$, 最后将 e 传送给 B 。

3) 收到 e 后, B 计算: $y = w_1 + e \cdot sk \bmod q$, 并将 y 发送给 C 。

4) 收到 y 后, C 计算 $y^* = y + w_2 \bmod q$, 则对消息 m 的签名为 (e^*, y^*) 。

1.6 验证阶段

验证者收到对消息 m 的签名 (e^*, y^*) 后, 计算 $\alpha = y_B \prod_{i=1}^n r_i y_i^{H(m_w, r_i)}$, $x^* = g^{y^*} \alpha^{-e^*} \bmod p$, $e'^* = H_2(x^*, m)$, 验证 $e'^* \stackrel{?}{=} e^*$, 若成立, 则签名有效。

2 LCZ 方案的安全性分析

在 LCZ 方案中, 任何一个原始签名者可以通过伪造有效代理密钥的方式产生对消息 m' 的有效代理多重盲签名。不失一般性, 不妨设原始签名者 A_j 欲对消息 m' 伪造有效签名, 攻击过程如下:

1) 原始签名者 A_j 随机选择 $k_a \in_R \mathbf{Z}_q^*$, 令 $r_a = (y_B \prod_{i \neq j, i=1}^n r_i y_i^{H(m_w, r_i)})^{-1} g^{k_a} \bmod p$, $sk' = k_a + x_j H(m_w, r_a) \bmod q$ 。

2) 在完成 1.3 节的步骤后, 原始签名者 A_j 把 (r_j, m_w) 替换为 (r_a, m_w) 。

3) 原始签名者 A_j 把 sk' 作为代理密钥按照 1.5 节的方法对消息 m' 进行签名, 易知: $g^{sk'} \bmod p = g^{k_a + x_j H(m_w, r_a)} \bmod p = y_B r_a y_j^{H(m_w, r_a)} \prod_{i \neq j, i=1}^n r_i y_i^{H(m_w, r_i)} \bmod p = \alpha'$, 因此 sk' 可以看作代理签名者 B 代表原始签名者 $A_i (1 \leq i \leq n)$ 进行代理签名的代理密钥, 相应的公钥为 α' , 从而原始签名者 A_j 可以利用 sk' 按照 1.5 节的方法成功伪造对消息 m' 的代理多重盲签名。

值得注意的是, 原始签名者 A_j 伪造的代理多重盲签名要想成功通过验证, 关键是他必须把 (r_j, m_w) 更新为 (r_a, m_w) 。然而, 由于 (r_j, m_w) 是由原始签名者 A_j 公开的, 并不经第三方的认证, 从而 A_j 可以成功的更新。

3 改进方案

3.1 初始化阶段

参数 $p, q, g, A_i (1 \leq i \leq n), B, x_i, y_i, x_B, y_B, H(\cdot)$ 的设置同 1.1 节, m_w 也表示授权书, 不同的是它不仅包括代理权限、有效期和原始签名者的标志等信息, 还包括代理签名者的标志。

3.2 代理授权阶段

1) 每个原始签名者 (r_i, s_i) 随机选择 $k_i \in_R \mathbf{Z}_q^*$, 计算 $r_i = g^{k_i} \bmod p$, 并将 r_i 广播给代理签名者 B 和其他原始签名者 $A_k (k \neq i)$ 。

2) A_i 计算 $r_A = \prod_{i=1}^n r_i \bmod p$, $s_i = x_i H(m_w, r_A) + k_i \bmod q$, 并将 s_i 发送给代理签名者 B 。

3) B 收到所有代理授权信息 $(r_i, s_i) (1 \leq i \leq n)$ 后, 计算

$$r_A = \prod_{i=1}^n r_i \bmod p, s_A = \sum_{i=1}^n s_i \bmod q, \text{并验证 } g^{s_A} \stackrel{?}{=} r_A \prod_{i=1}^n y_i^{H(m_w, r_A)} \bmod p, \text{若成立, 计算代理私钥 } x_p = s_A + x_B H(m_w, r_A) \bmod q, \text{其}$$

对应代理公钥为 $y_p = g^{x_p} = r_A (y_B \prod_{i=1}^n y_i)^{H(m_w, r_A)} \bmod p$ 。

3.3 签名生成阶段

假定签名请求者 R 请求代理签名者 B 对消息 m 进行签名:

1) B 随机选择 $k \in_R \mathbf{Z}_q^*$, 计算 $r = g^k \bmod p$, 并把 (r, m_w, r_A) 发给 R 。

2) R 计算 $y_p = r_A (y_B \prod_{i=1}^n y_i)^{H(m_w, r_A)} \bmod p$, 并任选 $\alpha \in_R \mathbf{Z}_q^*, \beta \in_R \mathbf{Z}_q^*$, 计算 $\lambda = r g^\alpha y_p^\beta \bmod p$, $e = H(m, m_w, \lambda) \bmod q$, $\delta = (e - \beta) \bmod q$, 然后将 δ 发送给 B 。

3) B 收到 δ 后计算 $\mu = (k - \delta x_p) \bmod q$, 并将 μ 发送给 R 。

4) R 收到 μ 后, 计算 $s = (\mu + \alpha) \bmod q$ 。

则 $\{m, (m_w, r_A), (e, s)\}$ 就是对文件 m 的签名。

3.4 签名验证阶段

签名验证者收到签名 $\{m, (m_w, r_A), (e, s)\}$ 后, 首先验证文件 m 是否满足代理授权书 m_w 的约定, 若不满足, 则该签名无效; 否则, 接着计算 $y_p = r_A (y_B \prod_{i=1}^n y_i)^{H(m_w, r_A)} \bmod p$, 并验证 $e \stackrel{?}{=} H(m, m_w, g^s y_p^e) \bmod p$, 若等式成立, 则代理多重盲签名 $\{m, (m_w, r_A), (e, s)\}$ 有效, 否则, 该签名无效。

4 对改进方案的分析

4.1 安全性分析

定理 1 即使所有原始签名者 $A_i (1 \leq i \leq n)$ 联合, 他们也不能伪造有效的代理密钥对 (x'_p, y'_p) 。

证明 改进方案的代理密钥对 (x_p, y_p) 满足 $y_p = g^{x_p} = r_A (y_B \prod_{i=1}^n y_i)^{H(m_w, r_A)} \bmod p$, 任何攻击者 (包括所有原始签名者) 要想伪造有效的代理密钥对, 必须找到一组数 (m'_w, r'_A, x'_p) , 使得等式 $g^{x'_p} = r'_A (y_B \prod_{i=1}^n y_i)^{H(m'_w, r'_A)} \bmod p$ 成立, 从而可以将 $(x'_p, y'_p = g^{x'_p} \bmod p)$ 作为代理密钥对冒充代理签名者 B 伪造有效的代理多重盲签名。然而, 这是不可能的, 因为利用等式 $g^{x'_p} = r'_A (y_B \prod_{i=1}^n y_i)^{H(m'_w, r'_A)} \bmod p$ 求解 m'_w, r'_A, x'_p 中任何一个都必须求解离散对数问题, 因此, 即使所有原始签名者 $A_i (1 \leq i \leq n)$ 联合, 他们也不能伪造有效的代理密钥对 (x'_p, y'_p) , 所以改进方案可以抵抗本文提出的攻击。

定理 2 任何人 (包括所有原始签名者) 不能伪造有效的代理多重盲签名。

证明 由定理 1 知: 任何攻击者不能通过伪造有效代理密钥对的方法生成有效的代理多重盲签名, 因此他只能通过伪造满足验证方程 $e' = H(m', m'_w, g^{s'} y_p^{e'}) \bmod p$ 的一组数据 $\{m'_w, r'_A, e', s'\}$ 的方法来生成对消息 m' 的有效代理多重盲签名, 这里 $y_p = r'_A (y_B \prod_{i=1}^n y_i)^{H(m'_w, r'_A)} \bmod p$ 。然而由于 $H(\cdot)$ 是一个安全单向 Hash 函数, 通过验证方程求解 $\{m'_w, r'_A, e', s'\}$ 是不可能的, 因此任何人 (包括所有原始签名者) 不能伪造有效的代理多重盲签名。 (下转第 1658 页)

循环又可分为同枝间接循环和异枝间接循环,如图 6 所示。

直接循环和同枝间接循环会造成程序无限循环,使验证无法终止;异枝间接循环只会造成证明的冗余。

可通过建立一张记录待证目标的证明路径表 (Proving Path Table, PPT) 来消除由直接循环和同枝间接循环导致的无限循环:要证明某个子目标 σ_i 时,首先检查它是否已经在 PPT 中,如果存在,表明已构成无限循环,返回并选择与之匹配的其他公理继续证明;否则将 σ_i 加入到 PPT;当 σ_i 被证明成立后,将其加入到初始化条件中,并从 PPT 中删除 σ_i 及其后面的所有节点。

证明路径表 PPT 的建立可以有效的消除无限循环,保证自动验证的正常终止。

5 结语

本文设计了一个基于 LLT 的时间相关安全协议自动验

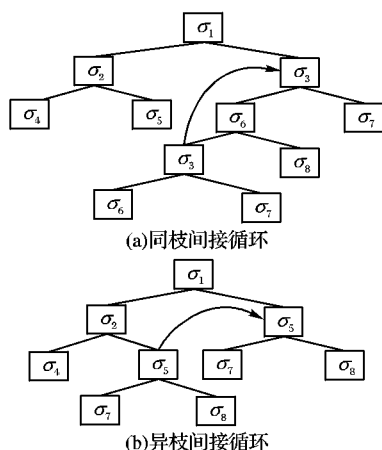


图 6 间接循环示例图

证工具。介绍了工具依赖的逻辑系统 TCPL 以及使用的技术模型,并详细设计了工具实现的相关算法,进行了实例验证;最后分析了工具的正确性和终止性。与当前同类验证工具相比,该工具能够正确、有效地对含有时间因子的协议进行自动分析,总体性能良好。下一步工作是实现反证法的自动化处理,使工具适用于更多、更复杂的情况。

参考文献:

- [1] MONT M C, HARRISON K, SADLER M. The HP time vault service: exploiting IBE for timed release of confidential information [C]// Proceedings of the 12th international conference on World Wide Web. Budapest: ACM Press, 2003: 160 - 169.
- [2] RIVEST R L, SHAMIR A, WAGNER D A. Time-lock puzzles and timed-release cryptographic protocol [R]. Cambridge: MIT Laboratory for Computer Science, 1996.
- [3] HOARE C. Communicating sequential processes [J]. Communications of ACM, 1978, 21(8): 666 - 677.
- [4] 李梦君, 李舟军, 陈火旺. SPVT: 一个有效的安全协议验证工具[J]. 软件学报, 2006, 17(4): 898 - 906.
- [5] 庄庆, 蔡小娟, 董笑菊, 等. 基于 GSPM 的安全协议检验工具[J]. 计算机工程, 2008, 34(17): 130 - 132.
- [6] 苏开乐, 吕关锋, 陈清亮. 基于知识结构的认证协议验证[J]. 中国科学, 2005, 35(4): 337 - 351.
- [7] LEI XIN-FENG, LIU JUN, XIAO JUN-MO. A logic to model time in cryptographic protocols [C]// 2008 International Symposium on Computer Science and Computational Technology. Los Alamitos: IEEE Computer Society, 2008: 399 - 403.
- [8] DOJEN R, COFFEY T. A novel approach to efficient automatic security protocol analysis [J]. ACM Transactions on Information and System, 2005, 8(3): 287 - 311.

(上接第 1647 页)

显然,所提方案满足盲性、不可链接性和代理多重盲签名的其他性质,这里不再赘述。

4.2 效率分析

由于模加法和模乘法的计算量相比模指数运算、模求逆运算和 Hash 运算的计算量来说可以忽略不计,因此本文仅列出模指数运算、模求逆运算和 Hash 运算的计算量的比较。令 E_m 表示模指数运算, I_m 表示模求逆运算, h_m 表示 Hash 运算,表 1 详细列举了 LCZ 方案、HQL 方案和改进方案在代理授权阶段、签名阶段和验证阶段的计算复杂性比较。

表 1 计算复杂性比较

运 算	代理授权阶段			签名阶段			验证阶段		
	LCZ 方案	HQL 方案	改进 方案	LCZ 方案	HQL 方案	改进 方案	LCZ 方案	HQL 方案	改进 方案
E_m	$8n$	$3n + 2$	$n + 1$	$n + 3$	4	4	$n + 2$	5	3
I_m	$2n$	1	0	0	2	0	1	1	0
h_m	$4n$	$n + 1$	$n + 1$	$n + 1$	2	2	$n + 1$	2	2

从表 1 容易看出,改进方案在代理密钥生成阶段、签名阶段和签名验证阶段的计算复杂性比 LCZ 方案和 HQL 方案都低。

另外,同 HQL 方案一样,改进方案的签名长度也不随原始签名人的增加而增长,并且传递代理授权信息时也不需要加密操作。

5 结语

代理多重盲签名具有很大的实际应用价值,可以广泛应用

到电子货币、电子投票、电子拍卖等电子商务领域,并可以解决实际应用中存在的一些问题。本文通过分析发现 LCZ 方案不满足强不可伪造性,并在 LCZ 方案和 HQL 方案的基础上,提出了一种改进方案,改进方案具有更高的安全性和效率。

参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages [J]. IEICE Transactions on Fundamentals, 1996, E79 - A(9): 1338 - 1354.
- [2] SUM H M, LEE N Y, HWANG T. Threshold proxy signatures [J]. IEE Proceedings of Computers & Digital Techniques, 1999, 146 (5): 259 - 263.
- [3] 钱海峰, 曹珍富, 薛庆水. 基于双线性对的新型门限代理签名方案[J]. 中国科学: E 辑, 2004, 34(6): 711 - 720.
- [4] LU R X, CAO Z F, ZHOU Y. Proxy blind multi-signature scheme without a secure channel [J]. Applied Mathematics and Computation, 2005, 164(1): 179 - 187.
- [5] 王天银, 蔡晓秋, 张建中. 对一种门限代理签名方案的密码分析及改进[J]. 计算机应用, 2006, 26(7): 1631 - 1633.
- [6] 胡振鹏, 钱海峰, 李志斌. 一种新的代理多重盲签名方案[J]. 计算机应用, 2007, 27(11): 2718 - 2721.
- [7] 王天银, 蔡晓秋, 张建中. 一种安全有效的代理盲签名方案[J]. 计算机工程, 2007, 33(2): 148 - 149.
- [8] 杨宇光, 温巧燕. 具有门限共享验证的门限代理量子签名方案[J]. 中国科学: G 辑, 2008, 38(7): 834 - 843.
- [9] 樊睿, 王彩芬, 蓝才会, 等. 新的无证书的代理签名方案[J]. 计算机应用, 2008, 28(4): 915 - 917.
- [10] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures [J]. Journal of Cryptology, 2000, 13 (3): 361 - 396.