A New Self-Certified Proxy Multi-Signature Scheme with Message Recovery

ZUO Weiping, LIU Yunfang

College of Mathematics and Information Science, Tianshui Normal College, Tianshui, China

e-mai: *tszwp*108@126.*com*, *lyf*0326@126.*com*

Abstract: Considering the previous proxy signature schemes with message recovery based on the public key systems, a new self-certified proxy multi-signature scheme with message recovery is proposed by using self-certified public key and combining the message recovery signature with the proxy multi-signature. In the scheme, the proxy signer can not only generate a valid proxy multi-signature on behalf of original signer groups, but also the verifier can recover the message from the proxy signature. Compared with the previous schemes, the new scheme can reduce the communication cost, so it is more suitable for signature of short message.

Keywords: self-certified; message recovery; proxy multi-signature

新的自认证消息恢复代理多重签名方案

左为平，刘云芳

天水师范学院数学与信息科学学院，天水，中国，741000

e-mail: tszwp108@126.com, lyf0326@126.com

【摘　要】已有的消息恢复代理签名方案大都是基于公钥密码体制的，结合消息恢复签名和代理多重签名思想，使用自认证公钥技术，提出了一种新的自认证消息恢复代理多重签名方案。新方案不仅可以实现代理多重签名，而且可以实现消息恢复。相比已有方案，新方案可以通过消息恢复功能降低传输消息本身所需的通信开销，因此它更适应于对短消息签名。

【关键词】自认证；消息恢复；代理多重签名

1 引言

在现实世界里，人们经常需要将自己的签名权委托给可靠的代理人，让代理人代表本人去行使这些权利。在电子化的信息社会中，同样也会遇到委托签名的问题。为了解决这个问题，1996年Mambo等人提出了代理签名[1,2]的概念。在一个代理签名中，原始签名人可以把自己的签名权委托给一位代理签名人，让代理签名人代替他生成有效的签名。而代理多重签名[3]是代理签名的一种扩展形式，即一个原始签名团体可以将其签名权委托给一位代理签名人，代理签名人可以代表原始签名团体来进行签名。例如，多个部门同时委托一位代理人在一个文件上签字。由于代理签名在实际生活中有着广泛的应用，因此，对代理签名的研究引起了人们普遍的关注[3-5]。

消息恢复签名[6,7]是指在对消息签名以后，验证人能够从签名中恢复出原消息的一类签名，这类签名的优点是通信量小、通信代价低，适用于对短消息进行签名。由于已有的消息恢复代理签名方案[8,9]大都是基于公钥密码体制的。和公钥密码体制相比，自认证公钥体制[10]具有通信代价低，计算量少，效率高的优点。在自认证公钥密码体制中，用户的公钥由SA（system authority）产生，而相应的私钥由用户自己产生；在验证签名有效性的同时，也验证了公钥的真实性，这些验证可以在逻辑单步内完成，不需要额外的证书。

本文使用自认证公钥技术，结合消息恢复签名和代理多重签名思想，提出了一种新的自认证消息恢复代理多重签名方案。利用该方案，不仅可以实现由一个代理签名人生成代表多个原始签名人的代理签名的目的，而且在传送签名时，没有必要传送消息，因为签名验证人在验证代理多重签名时可以恢复出消息，这就降低了传输消息本身所需的通信开销，因此，它适应于对短消息签名，可广泛应用于移动电子商务等领域。

2 消息恢复的代理多重签名方案

2.1 系统设置

系统权威 SA（system authority）选择两个大素数 p_1 和 q_1，并满足 $p_1=2p'+1$，$q_1=2q'+1$，其中，p' 和 q' 也是大素数。SA 计算 $n=p_1q_1$，并选择一个阶为 $p'q'$ 的生成元 g 和一个单向哈希函数 $h()$。最后，SA 秘密保留 p_1，q_1，p'，q'，公开 n，g，$h()$。

2.2 用户注册

假设 O_1、O_1、…、O_l $(1\le i\le l)$ 表示 l 个原始签名人，对应身份为 ID_i $(1\le i\le l)$；P 表示代理签名人，对应身份为 ID_P；O_i $(1\le i\le l)$、P 随机选择 x_i $(1\le i\le l)$、$x_P\in_R Z_n^*$ 作为各自的私钥，并计算 $u_i=g^{x_i}\bmod n$ $(1\le i\le l)$、$u_P=g^{x_P}\bmod n$，然后将 (u_i,ID_i) $(1\le i\le l)$、(u_P,ID_P) 发送给 SA。SA 收到 (u_i,ID_i) $(1\le i\le l)$、(u_P,ID_P) 后，计算

$$y_i=(u_i-ID_i)^{h(ID_i)^{-1}}\bmod n\ (1\le i\le l)、$$

$$y_P=(u_P-ID_P)^{h(ID_P)^{-1}}\bmod n,$$

并将 y_i $(1\le i\le l)$、y_P 作为 O_i $(1\le i\le l)$、P 的公钥。而公钥 y_i $(1\le i\le l)$、y_P 的有效性可以通过验证等式

$$y_i^{h(ID_i)}+ID_i=g^{x_i}\bmod n\ (1\le i\le l)、$$

$$y_P^{h(ID_P)}+ID_P=g^{x_P}\bmod n$$

是否成立来确认。如果等式成立，则接受，否则拒绝。

2.3 代理授权

每个原始签名人 O_i $(1\le i\le l)$ 随机选择 $k_i\in_R Z_n^*$，计算 $r_i=g^{k_i}\bmod n$，并将 r_i 发送给其他 $l-1$ 个原始签名人，然后计算：

$$r=\prod_{i=1}^{l}r_i,\quad s_i=x_ih(m_w,r)+k_i \tag{1}$$

并将 (m_w,r_i,s_i) 作为代理授权信息发送给代理签名人 P。其中，m_w 是授权证书，主要包含代理签名人 P 的身份，代理权限以及代理签名的有效期等信息。

代理签名人 P 收到每个原始签名人 O_i 的授权信息 (m_w,r_i,s_i) 后，首先计算：$r=\prod_{i=1}^{l}r_i$，然后验证等式：

$$g^{s_i}=r_i(y_i^{h(ID_i)}+ID_i)^{h(m_w,r)}\bmod n\ (1\le i\le l) \tag{2}$$

是否成立。若每个等式都成立，则说明授权合法，代理签名人 P 计算代理签名密钥：

$$s_P=\sum_{i=1}^{l}s_i+x_Ph(m_w,r) \tag{3}$$

2.4 代理签名生成

要生成具有消息恢复功能的代理多重签名，代理签名人 P 首先选择一随机数 $k\in_R Z_n^*$，并计算：

$$R_1=mg^{-kh(m)}\bmod n \tag{4}$$

$$R_2=mg^{-kR_1}\bmod n \tag{5}$$

$$s=kR_1-s_Ph(R_2) \tag{6}$$

则 (m_w,r,R_1,R_2,s) 为代理签名人 P 对消息 m 所作的代理签名。

2.5 消息恢复

验证人收到代理签名 (m_w,r,R_1,R_2,s) 后，首先从代理签名中恢复消息 m。恢复消息 m 的等式如下：

$$m=R_2g^sr^{h(R_2)}[\prod_{i=1}^{l}(y_i^{h(ID_i)}+ID_i)(y_P^{h(ID_P)}+ID_P)]^{h(R_2)h(m_w,r)}\bmod n \tag{7}$$

等式 (7) 的正确性证明：

$$\text{由等式 (5)}\Rightarrow m=R_2g^{kR_1}\bmod n \tag{8}$$

由等式 (6) 和 (8) $\Rightarrow m=R_2g^{s+s_Ph(R_2)}\bmod n$ 由等式 (1)、(2)、(3) 和

$$\Rightarrow m=R_2g^s(g^{\sum_{i=1}^{l}s_i}g^{x_Ph(m_w,r)})^{h(R_2)}\bmod n \tag{9}$$

$$\Rightarrow m=R_2g^s[\prod_{i=1}^{l}[r_i(y_i^{h(ID_i)}+ID_i)^{h(m_w,r)}](y_P^{h(ID_P)}+ID_P)^{h(m_w,r)}]^{h(R_2)}\bmod n$$

$$+(y_P^{h(ID_P)}+ID_P)]^{h(R_2)h(m_w,r)}\bmod n$$

可以看出，在传送代理签名时，没有必要传送消息 m，因为验证人可以从代理签名 (m_w,r,R_1,R_2,s) 中恢复出消息 m。

3 安全性分析

3.1 有效性

在恢复出消息 m 后，验证人利用恢复出的消息 m 验证代理签名 (m_w,r,R_1,R_2,s) 是否有效。验证等式如下：

$$(R_1m^{-1})^{R_1}=(R_2m^{-1})^{h(m)}\bmod n \tag{10}$$

如果等式成立，则说明代理签名有效并接受，否则拒绝。

等式 (10) 的正确性证明：

$$\text{由等式 (4)}\Rightarrow(R_1m^{-1})^{h(m)^{-1}}=g^{-k}\bmod n \tag{11}$$

$$\text{由等式 (5)}\Rightarrow(R_2m^{-1})^{R_1^{-1}}=g^{-k}\bmod n \tag{12}$$

由等式 (11) 和 (12)

$\Rightarrow(R_1m^{-1})^{h(m)^{-1}}=(R_2m^{-1})^{R_1^{-1}}\bmod n$

$\Rightarrow(R_1m^{-1})^{R_1}=(R_2m^{-1})^{h(m)}\bmod n$

从以上分析可以看出，本方案中的代理签名是有效的。

978-1-935068-06-8 © 2009 SciRes.

3.2 不可伪造性

假定攻击者知道 (m,R_1)，攻击者试图通过签名验证等式 $(R_1m^{-1})^{R_1}=(R_2m^{-1})^{h(m)} \bmod n$ 求 R_2，这相当于求解大数分解问题。假定 (m,R_2) 已知，通过上式求 R_1，这是一个非常复杂的数学求解问题，求解的困难性远在求解大数分解问题之上。假定 (m_w,m,r,R_1,R_2) 已知，通过消息恢复等式

$$m=R_2g^sr^{h(R_2)}[\prod_{i=1}^{l}(y_i^{h(ID_i)}+ID_i)$$
$$(y_P^{h(ID_P)}+ID_P)]^{h(R_2)h(m_w,r)} \bmod n$$

求 s，这相当于求解离散对数问题。因此，本方案能抵抗伪造攻击，任何人（包括原始签名人）不能伪造代理签名。

3.3 不可否认性

有效的代理签名 (m_w,r,R_1,R_2,s) 包含授权信息 m_w，而且在签名验证过程中要用到证书 m_w 和代理签名人 P 的公钥，而 P 又无法更改 m_w。因此，只要代理签名人 P 完成了一次代理签名，他就不能否认自己所产生的签名，也就是说，一旦签名完成，P 就不能否认其代理人身份，O_i $(1\le i\le l)$ 也不能否认其授权人身份。

4 结论

自认证公钥体制是一种新的密码体制。本文通过引入自认证公钥体制，并基于数学难解问题，给出了一种不仅可以实现代理多重签名功能，而且还可以实现消息恢复功能的签名方案。分析表明，我们提出的自认证消息恢复代理多重签名方案是安全有效的。该方案适应于对短消息签名，可广泛应用于移动电子商务等领域。

References (参考文献)

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages [J]. IEICE Trans Fundam, 1996, E79-A (9): 1338-1354.

[2] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation [A]. Proceedings of 3rd ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 1996. 48-57.

[3] YI LJ, BAI GQ, XIAO GZ. Proxy multi-signature scheme: a new type of proxy signature scheme [J]. Electronics Letter, 2000, 36 (6): 527-528.

[4] Hsu C, Wu T, He W. New proxy multi-signature scheme [J]. Applied Mathematics and Computation, 2005, 162(3): 1201-1206.

[5] HWANG S J, SHI C H. A simple multi-proxy signature scheme [A]. Proc of 10th National Conference on Information Security [C]. Hualien, Taiwan: ROC, 2000: 134-138.

[6] Nyberg K, Rueppel A R. Message recovery for signature schemes based on the discrete logarithm problem [A]. Advances in Cryptology-Eurocrypt'94, LNCS 950[C]. Berlin: Springer-Verlag, 1994: 175-190.

[7] Zhang Jh, Zou W, Chen D, et al. On the Security of a Digital Signature with Message Recovery Using Self-certified Public Key [J]. Informatica (Slovenia), 2005, 29(3): 243-346.

[8] Zhang Xiaomin, Zhang Jianzhong. Desinated Verifier Proxy Signature Scheme with Message Recovery [J]. Application Research of Computers, 2007,24(7): 131-132(Ch).
张晓敏,张建中.具有消息恢复的指定验证者的代理签名方案[J].计算机应用研究,2007,24(7): 131-132.

[9] Zhang Shaoting, Li Zhihui. Proxy multi-signature scheme with message recovery [J]. Computer Engineering and Applications, 2009,45(5): 108-109(Ch).
张少婷,李志慧.具有消息恢复的代理多重签名方案[J].计算机工程与应用,2009,45(5) : 108-109.

[10] Girault M. Self-certified public keys [A]. Proceedings of Eurocrypt'91, LNCS 434 [C]. Berlin: Springer-Verlag, 1991: 491–497.