文章编号:1001 - 9081(2009)06 - 1640 - 03

一种强多级代理签名方案

陈春华[1],徐秋亮[2],苏 英[1]
(1. 滨州学院 计算机科学技术系,山东 滨州 256600; 2. 山东大学 计算机科学与技术学院,济南 250063)
(chench_h@163.com)

摘 要:为了解决签名权的逐级委托过程中安全性不高、委托过程不容易确认等问题,基于 Schnorr 签名方案构造了一个强多级代理签名方案。新方案通过运用授权证书防止了签名权的滥用。并且该方案不需要第三方的参与,就可以通过验证公式直接确认签名权的转移过程。

关键词:代理签名;多级代理签名;防止滥用
中图分类号: TP309 **文献标志码**:A

Strong multiple grade proxy signature scheme

CHEN Chun-hua[1], XU Qiu-liang[2], SU Ying[1]
(1. *Department of Computer Science and Technology, Binzhou University, Binzhou Shandong* 256600, *China*;
2. *School of Computer Science and Technology, Shandong University, Jinan Shandong* 250063, *China*)

Abstract: To solve the problems of poor security and difficult confirmation in the entrusting process, a new strong multilevel proxy signature scheme is proposed based on the signature scheme of Schnorr. The new scheme prevents from entrusting right abuse by authority certificate, and the transfer process of signed right can be confirmed directly through the formula of verification, without the involvement of the third party.

Key words: proxy signature; multilevel proxy; abuse prevention

0 引言

在现实社会里,人们经常需要将自己的权利委托给可靠的代理人,让代理人代表本人去行使这些权利。在这些可以委托给他人的权利中,包括人们的签名权。在电子化的信息社会中,同样也会遇到签名权的委托问题。文献[1]提出的代理签名方案给出了解决这个问题的一种方法。在代理签名方案中,一个原始签名人可以把数字签名的权利委托给一位或多位代理签名人,让代理签名人代替他生成有效的签名。

在实际应用中,经常会遇到代理签名权需要多级委托的问题,即一个原始者将他的签名权委托给一个或多个代理签名者后,代理签名者有可能会将其签名权继续委托给他人,比如某经理外出度假期间,将一些文件的签名权委托给他的秘书,而在这期间由于某些特殊的原因秘书可能不能去完成对一些文件的签名,这时秘书可将签名权委托给他认为可靠的人。

文献[2]提出了多级代理签名的概念,并指出一多级代理签名方案应满足的 7 个基本要求。在该文献中设计了两个具体的多级代理签名方案,由于这两个方案是以文献[2]中所提出的 7 条基本要求为基础的,所以这两个方案只能满足一些基本的性质,而不满足不可伪造、不可区分以及不可抵赖等性质。

文献[3]设计了一多级代理签名方案,其安全性比文献[2]的方案有了很大的提高。但是经过分析发现,在这一方案中如果一级代理签名人在接到原始签名人的授权后就进行签名,那他所做的就是[MUO96]部分代理签名,可是有研究者已经指出[MUO96]存在着签名权的滥用等安全隐患[4]。另外,文献[3]中指出他们所提出的方案满足身份的可证实性,并指出可以通过逐级确认的方式来确认各级代理者的身份。可是在实际应用中,如果其中的某个或某几个代理人因特殊原因而不能参与验证时,会造成签名权逐级委托的验证无法继续进行。并且通过代理签名的验证过程也不能证明代理权的转移过程,这是因为在文献[3]中的验证公式中,各成员的身份对称,显然无法根据式(1)确认转移过程。

$$v_n = y_0 \cdot y_1^{y_1} \cdot y_2^{y_2} \cdot \cdots \cdot y_n^{n} \cdot K_0^{K_0} \cdot K_1^{K_1} \cdot \cdots \cdot K_{n-1}^{K_{n-1}} \pmod p \quad (1)$$

就此诸多问题,我们结合文献[2,5]提出的强壮的代理签名性质,提出了强壮的多级代理签名的概念,然后根据研究者对文献[5]中的强代理签名方案的代理密钥生成的改进[6]提出一个强壮的多级代理签名方案。新提出的方案可以有效地改进上述签名方案中的一些不足。

1 强壮的多级代理签名的概念

设 A_0 是一个原始签名人,他将自己的数字签名权力委托给了代理签名人 A_1,A_1 又将这个数字签名权力委托给了 A_2,A_2 又委托给了 A_3,……,使得每个 A_i 都可以在一定条件下代表 A_0 生成数字签名。这时,我们称 A_1 是 A_0 的一级代理人,A_2 是 A_0 的二级代理签名人,……,A_i 是 A_0 的 i 级代理签名人,等等。如果 $i < j$,则称 A_i 是 A_j 的上级(代理签名人),或称 A_j 是 A_i 的下级(代理签名人)。称 i 级代理签名人生成的签名为 i 级代理签名。这样的代理签名体制称为多级代理签名体制。而如果一个多级代理签名体制满足以下性质时,我们称其为强壮的多级代理签名体制。

1)强不可伪造性。除原始签名人外,任何人不能够生成有效的原始签名者的普通数字签名,即使多人合谋也不可能;只有每一级被授权的代理签名人才可以产生原始签名人的合

收稿日期:2008 - 12 - 22;**修回日期**:2009 - 02 - 27。 **基金项目**:山东省自然科学基金资助项目(Y2007G37)。

作者简介:陈春华(1967 -),男,山东沾化人,副教授,硕士,主要研究方向:密码学、网络安全; 徐秋亮(1962 -),男,教授,博士生导师,博士,主要研究方向:信息安全; 苏英(1980 -),女,山东滨州人,助教,硕士,主要研究方向:信息安全。

法代理签名,其他任何人(包括原始签名人)都不能产生有效的代理签名。

2)强可鉴别性。任何人都可以由一个代理签名鉴别出代理签名人,并能鉴别出代理权的委托过程。

3)不可抵赖性。一旦代理签名人代表原始签名人产生了一个合法的代理签名,他将不能抵赖这个签名。各级代理签名人包括原始签名人都不能抵赖其委托过程。

4)多级代理签名的可区分性。所有代理签名人生成的代理签名与原始签名人生成的普通数字签名有明显的区别;每一个代理签名人生成的代理签名都与其他各级代理签名人所生成的代理签名有明显的区别。

5)多级代理签名密钥的依赖性。每一代理签名人的代理签名密钥都依赖他上级的签名密钥。

6)防止滥用。代理签名的代理密钥对只能应用于符合授权证书的消息的签名,如果发生滥用,那么代理签名人应负相应的责任。

7)可撤销性。原始签名者可随时收回其下级的代理签名权。

我们将具有上述性质的多级代理签名方案称为强多级代理签名方案。

2　强壮的多级代理签名方案

设 p、q 是大素数,且 $q \mid p-1$,$g \in \mathbf{Z}_p^*$ 并且 $g^q = 1 \pmod p$,p、q、g 对每个用户都是公开的。m_w 是授权证书,$h()$ 是安全的单向哈希函数,Sign() 是签名算法,$Ver()$ 是签名验证算法。

设 $A_0, A_1, \cdots, A_n$ 是 $n+1$ 个用户,A_0 是原始签名者,他们的私钥为 $x_i \in \mathbf{Z}_q^*$ $(i = 0,1,2,\cdots,n)$,公开密钥是 $y_i = g^{x_i} \pmod p$。

2.1　代理授权过程

1)A_0 首先对授权证书进行 Schnorr 签名[7],即选取随机数 $k_0 \in_R \mathbf{Z}_q^*$,然后计算:

$$K_0 = g^{k0} \pmod p \tag{2}$$

$$S_0 = x_0 \cdot h(m_w, K_0) + k_0 \pmod q \tag{3}$$

最后 A_0 发送 (m_w, S_0, K_0) 给 A_1。

2)A_1 首先计算 $h(m_w, K_0)$,然后验证:

$$g^{S_0} \stackrel{?}{\equiv} y_0^{h(m_w,K_0)} \cdot K_0 \pmod p \tag{4}$$

如果不成立,A_1 拒绝接受并要求 A_0 重新发送;如果成立,A_1 随机选择 $k_1 \in_R \mathbf{Z}_q^*$,然后计算:

$$K_1 = g^{k1} \pmod p \tag{5}$$

$$S_1 = S_0 + k_1 \cdot K_1 + x_1 \pmod q \tag{6}$$

最后 A_1 发送 $(m_w, S_1, K_0, K_1, y_0, y_1)$ 给 A_2。

3)A_2 通过

$$g^{S_1} \stackrel{?}{\equiv} y_0^{h(m_w,K_0)} \cdot y_1 \cdot K_0 \cdot K_1^{K_1} \pmod p \tag{7}$$

验证授权的合法性,如果等式成立,A_2 可以确信他所得到的签名权是由 A_0 授权给 A_1,A_1 再授权给自己而来的。接下来,A_2 随机选择 $k_2 \in_R \mathbf{Z}_q^*$,然后计算:

$$K_2 = g^{k2} \pmod p \tag{8}$$

$$S_2 = S_1 + k_2 \cdot K_2 + 2x_2 \pmod q \tag{9}$$

然后 A_2 发送 $(m_w, S_1, K_0, K_1, K_2, y_0, y_1, y_2)$ 给 A_3。

依此类推。

4)A_i 收到 A_{i-1} 送来的 $(m_w, S_{i-1}, K_0, K_1, \cdots, K_{i-1}, y_0, y_1, \cdots, y_{i-1})$ 后,先验证:

$$g^{S_{i-1}} = y_0^{h(m_w,K_0)} \cdot y_1 \cdot y_2^2 \cdot y_3^3 \cdot \cdots \cdot y_{i-1}^{i-1} \cdot K_0 \cdot K_1^{K_1} \cdot \cdots \cdot K_{i-1}^{K_{i-1}} \pmod p \tag{10}$$

如果等式(10)成立,可以确信他的签名权是由 A_0 授权给 A_1,A_1 授权给 $A_2, \cdots, A_{i-1}$ 再权权给自己而来的。接下来,A_i 随机选择 $k_i \in_R \mathbf{Z}_q^*$,然后计算:

$$K_i = g^{ki} \pmod p \tag{11}$$

$$S_i = S_{i-1} + k_i \cdot K_i + i \cdot x_i \pmod q \tag{12}$$

最后 A_i 发送 $(m_w, S_i, K_0, K_1, \cdots, K_i, y_0, y_1, \cdots, y_i)$ 给 A_{i+1}。

依次进行下去。

2.2　代理签名密钥的生成

如果 $A_i (i = 1,2,\cdots,n)$ 想生成代理签名,他在 A_i 收到 A_{i-1} 送来的 $(m_w, S_{i-1}, K_0, K_1, \cdots K_{i-1}, y_0, y_1, \cdots, y_{i-1})$ 后,如果经验证是正确的代理授权(验证方法见 3.1 节),则代理签名密钥对生成过程如下:A_i 计算:

$$x_{pi} = S_{i-1} + x_i \cdot K_0 \pmod q \tag{13}$$

然后以 x_{pi} 作为代理签名私钥,以

$$y_{pi} = g^{x_{pi}} \pmod p \tag{14}$$

作为代理签名公钥。

2.3　代理签名的生成过程

A_i 要代表 A_0 对消息 m 进行签名,首先他判断 $m \stackrel{?}{\in} \{m_w\}$,如果成立,那么他计算:

$$\sigma = \mathrm{Sign}(x_{pi}, m) \tag{15}$$

于是 $(m_w, m, \sigma, K_0, K_1, \cdots, K_i, y_0, y_1, \cdots, y_i)$ 是 A_i 代表 A_0 对消息 m 生成的有效代理签名。

2.4　代理签名的验证

验证人计算 $h(m_w, K_0)$,然后验证:

$$1) m \stackrel{?}{\in} \{m_w\} \tag{16}$$

$$2) y_{pi} = y_0^{h(m_w,K_0)} \cdot y_1 \cdot y_2^2 \cdot y_3^3 \cdot \cdots \cdot y_{i-1}^{i-1} \cdot y_i^{K_0} \cdot K_0 \cdot K_1^{K_1} \cdot \cdots \cdot K_{i-1}^{K_{i-1}} \pmod p \tag{17}$$

$$3) Ver(m, \sigma, y_{pi}) \stackrel{?}{=} \mathrm{True} \tag{18}$$

如果三者都成立,则说明 $(m_w, m, \sigma, K_0, K_1, \cdots, K_i, y_0, y_1, \cdots, y_i)$ 是一有效的代理签名。

3　新提出方案的分析

3.1　方案的正确性

方案的正确性可通过以下证明得到:

$$g^{x_{pi}} = g^{S_{i-1}+x_i \cdot K_0} = y_0^{h(m_w,K_0)} \cdot y_1 \cdot y_2^2 \cdot y_3^3 \cdot \cdots \cdot y_{i-1}^{i-1} \cdot y_i^{K_0} \cdot K_0 \cdot K_1^{K_1} \cdot \cdots \cdot K_{i-1}^{K_{i-1}} \pmod p \tag{19}$$

其中:

$$S_{i-1} = x_0 h(m_w, K_0) + k_0 + k_1 K_1 + x_1 + k_2 K_2 + 2x_2 + \cdots + k_{i-1} K_{i-1} + (i-1) x_{i-1} \pmod p \tag{20}$$

3.2　方案的安全性分析

1)强不可伪造性。由式(1)任何人都不能通过此公式计算求得原始签名人的私钥 x_0,否则,他将面临求解有限域上的离散对数困难问题。

2)强可鉴别性。由式(17)的构成即可鉴别出生成此多级代理签名者为 A_i;同时由式(17)中各成员身份的不对称性可清晰地看出签名权的逐级委托过程为 $A_0 \to A_1 \to \cdots \to A_i$。

3)不可抵赖性。由于代理签名的验证过程中包含了原始签名人的公钥 y_0 和各级代理签名人的公钥 $y_1, y_2, \cdots, y_i$,所以代理签名经验证有效后,A_0 不能抵赖是他将自己的签名权委托了他的下一级,各级代理签名人也不能够抵赖是他们从上一级接过代理签名权同时又将其转移给了他的下一级。同时

由于生成的多级代理签名中包含有签名者的秘密密钥 x_i，所以除了 A_i 外，任何人都不能伪造 A_i 的签名，也就是说 A_i 不能抵赖由他生成的多级代理签名。

4）多级代理签名的可区分性。最终生成的多级代理签名 $(m_w, m, \sigma, K_0, K_1, \cdots, K_i, y_0, y_1, \cdots, y_i)$ 由三部分构成，第一部分 (m_w, m, σ) 是带有证书的数字签名部分，第二部分 $(K_0, K_1, \cdots, K_i)$ 由各级代理签名人计算生成，第三部分 $(y_0, y_1, \cdots, y_i)$ 是各级代理签名人的公钥。因此，很容易将一个多级代理签名与原始签名人的普通数字签名区分开，并且由验证公式知，每一级代理签名人生成的多级代理签名与其他各级代理签名人生成的多级代理签名有明显区别。

5）多级代理签名密钥的依赖性。第 i 级代理签名人的签名密钥 x_{pi} 由 $A_0, A_1, \cdots, A_{i-1}$ 的秘密密钥 $x_0, x_1, \cdots, x_{i-1}$ 和秘密随机数 $k_0, k_1, \cdots, k_{i-1}$ 逐级依次计算生成的，因此每一级代理签名人的代理签名密钥都依赖于他以前的各级代理签名人的签名密钥。

6）防止滥用性。本方案中引入了授权证书，对签名的消息作了限制，因此任何不属于 m_w 的消息都属于非授权消息，如果代理者签署了这样的消息，由于他不能抵赖，故可追究其相应的责任，因此有效地遏制了代理签名的滥用。

7）可撤销性。当原始签名者想撤销多级代理签名时，他只要广播由他签名的 K_0 不再有效的信息就可以了。

3.3 新方案的突出优点

1）验证确认过程高效。通过各级代理签名人身份的不对称，使得验证多级代理签名的同时确认了签名权的转移过程，这样就避免了签名权转移过程的逐级确认这一烦琐的问题，明显提高了验证确认效率。

2）防止滥用。运用授权证书，对签名的消息作了限制，同时由于本方案具有不可抵赖性，有效的防止了代理签名权的滥用。

3）安全性。通过把原始签名人及各中间代理签名人的秘密密钥 $x_0, x_1, \cdots, x_i$ 嵌入到最终的代理签名中，解决了原始签名人与中间各级代理签名人的相互抵赖问题，使原始签名人和各级代理签名人权责清晰，安全性明显提高。

4 结语

本文结合代理签名的性质及多级代理签名的概念提出了强壮的多级代理签名的概念，给出了强壮的多级代理签名的性质，并在最后提出了一种满足强壮的多级代理签名性质的方案。通过分析其安全性表明该方案在防止原始签名人和各级代理签名人之间相互抵赖以及防止签名权的滥用等方面比以往的多级代理签名方案有明显的增强。同时验证过程的效率显著地提高。

参考文献：

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation [C]// Proceedings of 3rd ACM Conference on Computer and Communication Security. New Delhi: ACM Press, 1996: 48 - 57.

[2] 伊丽江. 代理签名体制及其应用研究[D]. 西安: 西安电子科技大学, 2000.

[3] 蔡勉, 康莉. 一种安全的多级代理签名方案[J]. 中国科学院研究生院学报, 2006, 23(5): 653 - 658.

[4] 杨伟强, 徐秋亮. 典型代理签名方案的分析与改进[J]. 计算机工程与应用, 2004, 40(9): 152 - 154.

[5] LEE B, KIM H, KIM K. Strong proxy signature and its application [C]// The 2001 Symposium on Cryptography and Information Security. Oiso: [s. n.], 2001: 603 - 608.

[6] 杨淑娣, 姚正安. 一个改进的强代理签名方案[J]. 计算机应用研究, 2004, 21(8): 119 - 121.

[7] SCHNORR C P. Efficient identification and signatures for smart cards [C]// Crypto 89: Advances in Cryptology, LNCl435. Berlin: Springer-Verlag, 1990: 239 - 252.

(上接第1624页)

比本文方案不仅安全阈值有所提高，而且在MSK方案中攻击者只要捕获不足600个节点就可以控制整个网络，而在本文提出的方案中攻击者要控制整个网络需要捕获800多个节点。

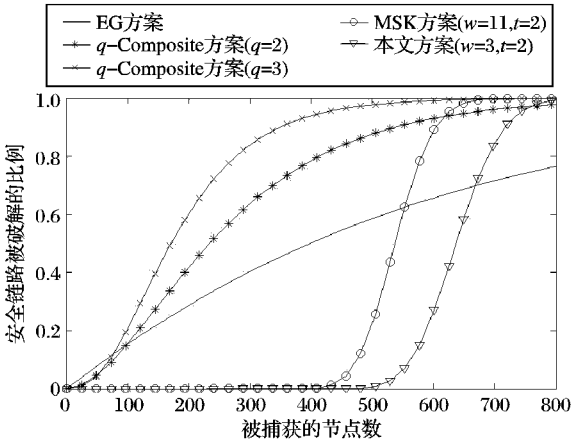

图3 几种方案的性能比较

4 结语

密钥管理是无线传感器网络安全的热点研究问题。本文在对称不完全区组设计和Blom的密钥预分配方案的基础上，提出了一个新的密钥预分配方案，并对其性能进行了详细分析，分析表明，与其他密钥预分配方案相比，本方案具有较好的抵抗攻击的能力。

参考文献：

[1] ESCHENAUER L, GLIGOR V D. A key management scheme for distributed sensor networks [C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. New York: ACM Press, 2002: 41 - 47.

[2] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks [C]// Proceedings of IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 2003: 197 - 205.

[3] BLOM R. An optimal class of symmetric key generation systems [C]// Proceedings of the EUROCRYPT 84 workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques. New York: Springer-Verlag, 1984: 335 - 338.

[4] DU W, DENG J, HAN Y S, *et al*. A pairwise key pre-distribution scheme for wireless sensor networks [J]. ACM Transactions on Information and System Security, 2005, 8(2): 228 - 258.

[5] CAMTEPE S A, YENER B. Combinatorial design of key distribution mechanisms for wireless sensor networks [J]. ACM Transactions on Networking, 2007, 15(2): 346 - 358.