

不可否认的可公开验证的代理多重签密方案

甘元驹, 谢仕义, 付东洋, 郑小平

(广东海洋大学信息学院, 湛江 524088)

摘要: 针对现有的代理签名仅能提供授权的认证而不能提供保密性的弱点, 提出了一种有效的代理多重签密方案。该方案具有如下特点: 原始签名人与代理签密人之间不必使用安全信道; 只有指定的接收者能验证代理签密的有效性; 当代理签名人否认签密时, 接收者可单独将代理签密转换为一般的代理签名。

关键词: 密码学; 代理签密; 不可否认性; 公开验证

Nonrepudiable Proxy Multi-Signcryption Scheme with Public Verifiability

GAN Yuanju, XIE Shiyi, FU Dongyang, ZHENG Xiaoping

(School of Information, Guangdong Ocean University, Zhanjiang 524088)

【Abstract】 Most previous proxy signatures only provide the delegated authenticity and don't provide the confidentiality. An efficient proxy multi-signcryption scheme is presented. The proposed scheme has the following properties: Original signer and proxy signer don't use secure channel; Only the specified recipient can check the validity of the proxy signcryption; When the proxy signer repudiates the signcryption, the recipient can convert this proxy signcryption into an ordinary proxy signature alone.

【Key words】 Cryptography; Proxy signcryption; Nonrepudiable; Public verifiability

1 概述

代理签名是指当某签名人(这里称为原始签名人)因公务或身体健康等原因暂时不能行使签名权力时, 将签名权委派给其它人替自己行使签名权。自1996年Mambo等^[1]提出代理签名方案以来, 由于代理签名在实际应用中起着重要作用, 因此代理签名一提出便受到广泛关注, 国内外学者对其进行了深入的探讨与研究, 提出了各种各样的代理签名方案, 如单一的代理签名、代理多重签名、多重代理多重签名、盲代理签名和门限代理签名等。在现实生活中, 不可否认性是代理签名的重要特点, 如当签名滥用发生时, 权威机构必须确定谁是代理签名的真正签名人。Mambo等^[2]和Kim等^[3]各自提出了具有不可否认的代理签名方案, 但Gan Shi^[4]和Sun Hsieh^[5]分别指出这些的代理签名方案并不具有真正不可否认性的安全缺陷, 并给出相应的改进方案。后来Hsu等^[6]也提出了一种不可否认的门限代理签名方案, 但Yang等^[7]指出该方案同样不安全。由此可见, 不可否认问题是代理签名方案在应用中急需解决的一个关键问题。

针对数字签名仅能提供信息来源认证而不能提供保密性问题, Zheng^[8]组合了数字签名和对称密钥加密算法的功能, 提出一个新型密码学概念称为“签密”(Signcryption)。签密不仅用一步就能提供认证性和保密性, 而且它的计算比传统的先签名后加密更有效。针对代理签名也存在同样的应用要求, Chan Wei^[9]有效地组合了代理签名方案和加密方案, 提出代理签密方案, 扩展了代理签名的概念, 解决了代理签名仅能提供授权的认证而不能提供保密性这一问题, 然而Chan Wei的方案存在以下不足: (1)没有解决代理签名的不可否认性问题; (2)原始签名人和代理签人之间的通信必须使用安全信道; (3)由于只有指定的接收者能解密和验证代理签密的有

效性, 当代理签密者否认签名时, 接收者只能通过交互协议向信任三方证明签名的诚实性, 而不是其它任意验证者。

基于对以上问题的研究, 在文献[4,9~11]的研究基础上, 设计出了一种不可否认的、原始签名人和代理签名人之间的通信不必使用安全信道的可转化的代理多重签密方案。

2 方案描述

2.1 系统初始化

可信任中心选取安全大素数 p, q 满足 $q|p-1$, 一个 $GF(p)$ 中阶为 q 的生成元 g , 一个强单向Hash函数 $h(\cdot)$ 。这些参数是公开的, 系统内每个成员都知道。令 U_1, U_2, \dots, U_n 是 n 个原始签名人, 他们联合请求一个代理签名人UP代表他们对消息 m 签名。其中 U_1, U_2, \dots, U_n 自己的私钥为 $x_{ui} \in Z_q^*$ 以及公钥 $y_{ui} = g^{x_{ui}} \bmod p$ 。代理者 U_p 的私钥为 $x_p \in Z_q^*$ 以及公钥 $y_p = g^{x_p} \bmod p$ 。接收者 U_b 的私钥为 $x_b \in Z_q^*$ 以及公钥 $y_b = g^{x_b} \bmod p$ 。授权信息 mw 包含了原始签名人中每个成员的身份信息和公钥、代理者的身份信息ID和公钥、代理期限、代理权限等。所有的公钥都被CA认证。

2.2 代理签密密钥的生成

Step1 所有的原始签名人 U_i 随机选择一整数 $k_{ui} \in Z_q^*$, 并计算:

$$r_{ui} = g^{k_{ui}} \bmod p \quad (1)$$

基金项目: 国家自然科学基金资助项目(60173041); 广东海洋大学自然科学基金资助项目

作者简介: 甘元驹(1974-), 男, 副教授、硕士, 主研方向: 密码协议分析与信息安全; 谢仕义, 副教授、硕士; 付东洋、郑小平, 讲师、硕士

收稿日期: 2006-02-08 **E-mail:** ganyj@mail.edu.cn

然后将 k_{ui} 广播给其它 $n-1$ 个原始签名人和代理者 U_p 。同样代理者也随机选择一整数 $k_p \in Z_q^*$ ，并计算：

$$r_p = g^{k_p} \bmod p \quad (2)$$

代理者将 r_p 广播给其它 n 个原始签名人。每个原始签名人 U_i 和代理者 U_p 都计算：

$$R = r_p \prod_{i=1}^n r_{ui} \bmod p \quad (3)$$

Step2 每个原始签名人 U_i 计算：

$$e = h(m_w, R, y_p) \quad (4)$$

$$\sigma_i = e y_{ui} x_{ui} + k_{ui} R \bmod p \quad (5)$$

并将 σ_i 通过一般信道发给代理者 U_p 。

Step3 当 U_p 收到所有的 σ_i 后计算：

$$\sigma = e x_p + k_p R + \sum_{i=1}^n \sigma_i \bmod q \quad (6)$$

并且检查如式(7)是否成立：

$$y_\sigma = g^\sigma = R^R (y_p \prod_{i=1}^n y_{ui}^{y_{ui}})^e \bmod p \quad (7)$$

如果成立， U_p 接收 σ 为来自 U_1, U_2, \dots, U_n 的有效代理签密密钥。否则拒绝它并要求重新发送。这里，称 $\{y_\sigma, R\}$ 为代理签密授权证书，因为它不仅包含了 n 个原始签名人同意授权给代理者，同时也包含了代理者同意接收 n 个原始签名者的授权。

2.3 代理签密的生成

假设 U_p 想对一个包含预定义冗余信息^[12] 的消息 m 进行代理签密，首先随机选择一个整数 $k \in Z_q^*$ ，并计算：

$$r_1 = m \cdot y_b^{-k} \bmod p \quad (8)$$

$$r_2 = h(m \parallel r_1 \parallel g^k) \bmod q \quad (9)$$

$$s = k - \sigma r_2 \bmod q \quad (10)$$

消息 m 的代理签密是 $\{r_1, r_2, s\}$ ，然后 U_p 将 $\{r_1, r_2, s\}, m_w, (y_\sigma, R)$ 发送给接收者 U_b 。

2.4 代理签密消息的恢复与验证

Step1 U_b 收到 $\{r_1, r_2, s\}, m_w, (y_\sigma, R)$ 后，先验证授权信息 m_w 是否正确，若正确则计算 $e = h(m_w, R, y_p)$ ，然后根据方程：

$y_\sigma = R^R (y_p \prod_{i=1}^n y_{ui}^{y_{ui}})^e \bmod p$ 验证代理签密授权证书 $\{y_\sigma, R\}$ 是否正确。若不正确，拒绝代理签密 $\{r_1, r_2, s\}$ ，若正确则按方程(11)来恢复消息 m 。

$$m = (g^s y_\sigma^{r_2})^{x_b} \cdot r_1 \bmod p \quad (11)$$

消息恢复式(11)的正确性证明如下：

$$(g^s y_\sigma^{r_2})^{x_b} \cdot r_1 \bmod p = (g^{k - \sigma r_2} y_\sigma^{r_2})^{x_b} \cdot r_1 \bmod p \quad (\text{由式(10)})$$

$$= (g^k y_\sigma^{-\sigma r_2} y_\sigma^{r_2})^{x_b} \cdot r_1 \bmod p = (g^k)^{x_b} \cdot m \cdot y_b^{-k} \bmod p \quad (\text{由式(8)})$$

$$= m \bmod p$$

Step2 U_b 验证恢复的消息 m 是否包含正确的冗余信息。若正确，然后按式(12)验证代理签密的有效性，如果认证式(12)成立，则代理签密是有效的，否则拒绝该代理签密。

$$r_2 = h(m \parallel r_1 \parallel g^s y_\sigma^{r_2}) \bmod q \quad (12)$$

认证式(12)的正确性证明如下：

$$h(m \parallel r_1 \parallel g^s y_\sigma^{r_2}) \bmod q$$

$$= h(m \parallel r_1 \parallel g^{k - \sigma r_2} y_\sigma^{r_2}) \bmod q$$

$$= h(m \parallel r_1 \parallel g^k y_\sigma^{-\sigma r_2} y_\sigma^{r_2}) \bmod q$$

$$= h(m \parallel r_1 \parallel g^k) \bmod q = r_2 \bmod q$$

2.5 代理签密的公开验证

如果以后 U_p 否认对消息 m 的代理签密， U_b 不需代理者 U_p 的合作，就可按下面的方法将代理签密转化为一般的代理签名： U_b 公布所恢复的消息 m 以及 $\{r_1, r_2, s\}, m_w, (y_\sigma, R)$ ，那么任何人都可以通过验证方程：

$$y_\sigma = R^R (y_p \prod_{i=1}^n y_{ui}^{y_{ui}})^{h(m_w, R, y_p)} \bmod p$$

$$r_2 = h(m \parallel r_1 \parallel g^s y_\sigma^{r_2}) \bmod q$$

是否同时成立，来证实代理签密有效性。

3 安全性分析

方案的安全性是基于密码学中两个著名的假设：强单向 Hash 函数的不可逆和求解离散对数的困难性，因而方案在这两个假设下是安全的。下面讨论该方案可能受到的一些攻击：

攻击 1 攻击者在知道 R 的情况下，试图从方程(7)中解出代理密钥 σ ，然而这样的攻击将面临求解离散对数这一难题。攻击者利用代理签密 $\{r_1, r_2, s\}$ 中的 $\{s, r_2\}$ ，试图利用等式 $s = k - \sigma r_2 \bmod q$ 求出 σ ，但方程中包含两个未知变量 k 和 σ ，要想得到 k 的值，攻击者必须解决离散对数难题。因此，攻击者试图通过一些公开信息来计算代理密钥 σ 是不可能的。

攻击 2 代理签密者不可能通过式(5)计算出任何一个原始签名人的私钥 x_{ui} ，因为 k_{ui} 对于代理签密者来说是未知的，且 k_{ui} 受离散对数问题假设保护。另外代理签密者直接利用原始签名人的公钥 y_{ui} 求 x_{ui} 面临求解离散对数问题。

攻击 3 n 个原始签名人合谋也不可能得到代理签密密钥 σ 。因为代理签密密钥 $\sigma = e x_p + k_p R + \sum_{i=1}^n \sigma_i \bmod q$ 中包含有代理者的私钥 x_p 和只有代理者知道的一个随机数 k_p ，要解出 x_p 和 k_p 才能求出 σ ，然而求出 x_p 和 k_p 将是求解离散对数难题。

攻击 4 攻击者不可能从 $\{r_1, r_2, s\}, m_w, (y_\sigma, R)$ 中恢复出消息 m 。从消息 m 的恢复式(11)可知 $m = (g^s y_\sigma^{r_2})^{x_b} \cdot r_1 \bmod p = (y_b^s y_b^{\sigma r_2}) r_1 \bmod p$ ，只有知道代理签密密钥 σ 或 x_b 才能恢复消息，这将是求解离散对数难题。同样，代理签密在没有执行到公开验证阶段，攻击者也不可能验证代理签密，因为攻击者不能得到消息 m 。

攻击 5 攻击者试图伪造代理签密 $\{r_1, r_2, s\}$ 。攻击者将有以下 3 种途径：(1)攻击者先选择 m, r_1, s ，然后确定 r_2 使得 $r_2 = h(m \parallel r_1 \parallel g^s y_\sigma^{r_2}) \bmod q$ ，然而要求出 r_2 ，必须同时解决离散对数难题和强单向 Hash 函数的不可逆难题；(2)攻击者先选择 m, r_1, r_2 ，然后从 $r_2 = h(m \parallel r_1 \parallel g^s y_\sigma^{r_2}) \bmod q$ 求解出 s ，这种方法同样会求解离散对数难题和强单向 Hash 函数的不可逆难题；(3)攻击者先选择 m, r_1, r_2, k ，通过 $s = k - \sigma r_2 \bmod q$ 计算出 s ，然而从上面的攻击 1 可知， σ 是攻击者不能得到的秘密参数，因而也就不能求出 s 。

4 特性分析

4.1 信道分析

本文所提出的方案不需使用安全信道。假设攻击者知道在 n 个原始签名人 U_i 和代理签名人 U_p 之间传递的所有消息。但攻击者不知道也求不出 x_p 和 k_p ，也不可能获得代理签密密钥 σ 。因此不使用安全信道，使本方案的通信成本大大降低。

4.2 不可否认性分析

代理签名人 U_p 不能否认他所生成的代理签密,因在代理签密生成阶段所用的 σ 中包含了代理签名人的密钥信息 x_p ,同时式(7)中包含 U_p 的公钥信息 y_p ,以及授权信息 m_w 中也有 U_p 的身份信息。采用同样的分析可知,原始签名人也不能否认一次成功的代理签密非自己的授权。

4.3 性能分析

从方案的描述过程可知,代理签密授权证书 $\{y_\sigma, R\}$ 以及所生成的代理签密 $\{r_1, r_2, s\}$ 与原始签名人的人数无关,且其长度只与系统 p, q 的长度有关,代理签密授权证书存储空间为 $2|p|(N|N|表示N的长度)$,代理签名的长度为 $|p|+2|q|$ 。在这一点上,与其它的代理多重签名以及可转换的认证加密存储性能相当。

5 结论

针对一些代理签名方案存在的不足,本文提出一个可公开验证的代理多重签密方案。当代理签名人否认他所签的代理签密时,指定的接收者在没有代理签名者的合作下,可将这种代理签密方案转换为一般的代理签名方案,任何验证者都可验证代理签名人的诚实性。方案的通信各方都不需要安全信道。方案的安全性是基于强单向 Hash 函数的不可逆和求解离散对数的困难性。

参考文献

- 1 Mambo M, Usuda K, Okamoto E. Proxy Signatures: Delegation of the Power to Sign Messages[J]. IEICE Trans. on Fundamentals, 1996, E79-A(9): 1338-1354.
- 2 Mambo M, Usuda K, Okamoto E. Proxy Signatures for Delegating Signing Operation[C]. Proc. of the 3rd ACM Conference on Computer

and Communications Security, 1996: 48-57.

- 3 Kim S, Park S, Won D. Proxy Signatures, Revisited[C]. Proc. of Int. Conf. on Information and Communications Security, 1997: 223-232.
- 4 甘元驹, 施荣华. 一种安全有效的代理签名方案[J]. 云南大学学报(自然科学版), 2004, 26(1): 35-37.
- 5 Sun H M, Hsieh B T. Remarks on Two Nonrepudiable Proxy Signature Schemes[C]. Proceedings of the 9th National Conference on Information Security, 1999: 241-246.
- 6 Hsu C L, Wu T S, Wu T C. New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers[J]. The Journal of Systems and Software, 2001, 58(2): 119-124.
- 7 Yang C Y, Tzeng S F, Hwang M S. On the Efficiency of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers[J]. The Journal of Systems and Software, 2004, 73(3): 507-605.
- 8 Zheng Y. Signcryption and Its Applications in Efficient Public Key Solutions[C]. Proceedings of Information Security Workshop, 1997: 291-312.
- 9 Chan W K, Wei V K. A Threshold Proxy Signcryption[C]. Proc. of International Conference on Security and Management, Monte Carlo Resort, Las Vegas, Nevada, USA, 2002: 24-27.
- 10 甘元驹, 黎群辉, 施荣华. 一种追踪接收者的时控代理签名方案[J]. 计算机工程与应用, 2004, 40(10): 140-141.
- 11 甘元驹, 彭银桥. 具有消息链接的可转换的认证加密方案[J]. 浙江大学学报(理学版), 2004, 31(5): 535-537.
- 12 Araki S, Uehara S, Imamura K. The Limited Verifier Signature and Its Application[J]. ICICE Transactions on Fundamentals, 1999, E82-A(1): 63-68.

~~~~~