一个新的可收回代理权的代理盲签名方案

刘文远[①]　佟　凤[①]　王宝文[①]　王亚东[②]
[①](燕山大学信息科学与工程学院　秦皇岛 066004)
[②](哈尔滨工业大学计算机科学与技术学院　哈尔滨 150001)

摘　要：该文针对目前代理签名中普遍存在的代理权撤销难、原始签名人伪造和代理权滥用等问题，提出一个新的可收回代理权的代理盲签名方案。签名阶段将时间戳嵌入到 Abe-Okamoto 部分盲签名中，解决了无可信第三方前提下的代理权撤销问题，并且代理权撤销后，以前产生的有效签名仍然可以得到验证；此外，该方案不仅满足代理签名的基本性质，还避免了代理权滥用、原始签名人伪造和公钥替换攻击。

关键词：代理签名；代理盲签名；可收回代理权；代理权滥用
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2008)10-2468-04

A New Proxy Blind Signature Scheme with Proxy Revocation

Liu Wen-yuan[①]　Tong Feng[①]　Wang Bao-wen[①]　Wang Ya-dong[②]
[①](*Information Science and Engineering Institute*, *Yanshan University*, *Qinhuangdao* 066004, *China*)
[②](*Computer Science and Engineering Institute*, *Harbin Institute of Technology*, *Harbin* 150001, *China*)

Abstract: According to the problems of proxy revocation, original signer's forgery and proxy misuse in proxy signature, a secure proxy blind signature scheme with proxy revocation is proposed. In phase of signature, by embedding non-blind time-stamp in the Abe-Okamoto partially blind signature, the original signer can revoke delegation whenever necessary and all valid proxy signatures generated earlier can longer be verified. Besides having the basic properties of the proxy signature, the new scheme prevents proxy misuse, original signer's forgery and public key substitution attack.

Key words: Proxy signature; Proxy blind signature; Proxy revocation; Proxy misuse

1　引言

代理盲签名作为一种新型的签名方案，一经提出受到国内外学者的广泛关注。2002 年，Tan 等人提出分别基于离散对数问题和椭圆曲线密码体制的代理盲签名方案[1]，随后人们进行许多研究，但是仍然普遍存在代理权撤销难、原始签名人伪造和代理权滥用等问题。目前代理权撤销的方法有两种：(1)改变原始签名人的公钥。但是一旦原始签名人的公钥改变，原始签名人早期产生的签名却不能得到验证；(2)将 r_A (原始签名人产生的代理密钥部分)放到一个公开撤销列表，任何人验证之前都必须确认 r_A 不在公开撤销列表中，但是代理签名人同样可以产生代理签名，并且宣称签名是代理权撤销前产生的，这样在代理权撤销后就很难验证代理签名人以前产生的代理签名的有效性；同时撤销列表也会无限增大[2]。而且现有许多方案的代理权撤销[2, 3]都借助可信第三方，这样增加了额外的成本消耗和系统复杂性。

目前大多数代理盲签名方案都是结合 Schnorr 盲签名，本文采用 Abe-Okamoto 部分盲签名技术[4]保持一个非盲的时间戳，提出一个新的可收回代理权的代理盲签名方案，无需可信第三方，原始签名人便可在需要时撤销代理签名人的代理权，并且代理权撤销后以前产生的有效签名仍可得到验证。新方案中代理签名密钥的设计借鉴了 Mambo 代理签名方案[5, 6]和文献[7]方案，有效地避免了原始签名人伪造和代理权滥用；公开传递参数，减轻了系统负担；利用零知识证明，可以防止公钥替换攻击。

2007-03-26 收到，2007-09-14 改回
国家科技部高新技术计划项目(2005EJ000017)和河北省自然科学基金(F2005000368)资助课题

2　参数设置

(1)设 p 是一个大素数，且 p–1 有大素数因子 q，满足 $q|(p-1)$。小于 p 并与 p 互素的正整数集合和模 p 的乘法运算构成了群 Z_p^*，g 是 Z_p^* 中 q 阶乘法子群的生成元。

(2)$H()$是防冲突的安全单向散列函数。M 是消息。

(3)原始签名人的私钥为 $x_A \in {}_RZ_q^*$，相应的公钥为 $y_A=g^{x_A} \pmod p$；代理签名人的私钥为 $x_B \in {}_RZ_q^*$，相应的公钥为 $y_B = g^{x_B} \pmod p$；代理签名密钥对是 (x_p, y_p)，$y_p= g^{x_p} \pmod p$，其中 x_p 是代理签名私钥，y_p 是代理签名公钥。

(4) m_ω 是具有委托书代理中的证书，包括原始签名人身份信息、代理签名人身份信息、授权范围和代理期限等。

(5)原始签名人要维护一个公开撤销列表，用来存放已撤销代理权的代理签名人的 r_A (原始签名人产生的代理签名密钥部分)。

(6)公钥 y_A 和 y_B 必须在认证中心得到认证。为了防止公钥替换攻击，采用零知识证明来解决，只要签名者注册或修改公钥时，认证中心要求签名者能够证明修改的公钥所对应私钥的知识，那就能够证明公钥是否被修改过[8]。

3　一个新的可收回代理权的代理盲签名方案

目前大部分代理盲签名方案都是基于 Schnorr 盲签名的，而本方案结合 Abe-Okamoto 部分盲签名技术，保持一个非盲的时间戳，在无可信第三方的前提下有效地实现了代理权撤销；代理签名接收人将盲化的消息发送给代理签名人，代理签名人对盲化的消息签名后发送给接收人，接收人对消息去盲后得到代理签名人对消息的真正签名。

3.1 代理签名密钥产生

(1)代理签名人将身份信息发送给原始签名人。

(2)原始签名人安全地随机选择正整数 $k_A \in_R Z_q^*$ 作为秘密值，其中 $k_A \neq x_A$，并计算 $r_A=g^{k_A} \pmod p$，将 r_A 作为提交值。

(3)原始签名人根据提交值 r_A，计算 $h=H(m_\omega,r_A,y_A,y_B)$。然后计算

$$s_A = x_A + k_A \cdot h \pmod q \tag{1}$$

并将代理参数 (m_ω,r_A,s_A) 公开地传递给代理签名人。

(4)代理签名人首先使用原始签名人发送过来的代理参数 (m_ω,r_A,s_A)，计算 $h=H(m_\omega,r_A,y_A,y_B)$，验证式子

$$g^{s_A} = y_A r_A^h \pmod p \tag{2}$$

如果等式成立，代理签名人接受 (m_ω,r_A,s_A) 作为有效代理参数；否则拒绝它，并向原始签名人索要有效的参数或者终止协议。

(5)如果代理签名人确认原始签名人的代理参数 (m_ω, r_A,s_A) 有效，则计算代理签名密钥为

$$x_p = x_B \cdot y_B + s_A \pmod q \tag{3}$$

相应的代理签名公钥为

$$y_p = g^{x_p} = y_B^{y_B} y_A r_A^h \pmod p \tag{4}$$

3.2 代理盲签名产生

(1)代理签名人随机选择数 $u,\ s,\ d \in Z_q^*$，计算 $a = g^u \cdot \pmod p$，$b = g^s T^d \pmod p$。其中实时时间 T=time_stamp 作为时间戳，相当于部分盲签名中的共识信息。将 a, b, m_ω，r_A 和 T 发送给代理签名接收人。

(2)代理签名接收人首先计算 $h=H(m_\omega,r_A,y_A,y_B)$，然后验证式(4)是否成立，如果成立则说明代理签名人是经过原始签名人授权的；然后验证代理签名人的代理权是否有效，需要进行如下工作：一是验证 T 是正确的实时时间；二是验证 T 没有超过 m_ω 中规定的代理期限；三是确定公开撤销列表中没有 r_A；只有同时满足上述 3 个条件才能保证代理签名人的代理权有效。

(3)代理签名接收人验证代理签名人的代理权有效性之后，随机选择数 $t_1,t_2,t_3,t_4 \in Z_q^*$，计算 $\alpha = a g^{t_1} y_p^{t_2} \pmod p$，$\beta = b g^{t_3} T^{t_4} \pmod p$，$\varepsilon = H(\alpha,\beta,T,M)$，$e = \varepsilon - t_2 - t_4 \cdot \pmod q$，然后将 e 发送给代理签名人。

(4)代理签名人计算 $c=e-d \pmod q$，$r=u-c x_p \pmod q$，然后将$(r,\ c,\ s,\ d)$发送给代理签名接收人。

(5)代理签名接收人收到$(r,\ c,\ s,\ d)$后，计算 $\rho=r+t_1 \cdot \pmod q$，$\omega=c+t_2 \pmod q$，$\sigma=s+t_3 \pmod q$，$\delta=d+t_4 \cdot \pmod q$。

(6)最后生成的签名为 $(M,\rho,\omega,\sigma,\delta,r_A,m_\omega,T)$，验证式子

$$\omega+\delta = H(g^\rho y_p^\omega, g^\sigma T^\delta, T, M) \tag{5}$$

如果等式成立则说明签名有效，否则签名无效。

3.3 代理盲签名验证

签名验证人收到签名 $(M,\rho,\omega,\sigma,\delta,r_A,m_\omega,T)$ 后，通过下面步骤验证签名的有效性。

(1)检查 M 是否符合授权书 m_ω 规定的授权范围，若符合进行下一步验证。

(2)核对 r_A 是否在撤销列表中，如果不在则说明代理签名人没有被提前撤销代理权；然后根据时间戳 T，验证 T 是否超过 m_ω 中规定的代理期限，如果没有超过，说明签名是在代理期限内产生的，则进行下一步验证。

(3)根据 r_A，m_ω，计算 $h=H(m_\omega,r_A,y_A,y_B)$，然后验证式(4)是否成立，如果成立则说明代理签名人是经过原始签名人授权的，则进行下一步验证。

(4)根据 $\rho,\omega,\sigma,\delta$, T 验证式(5)是否成立，如果等式成立则说明签名 $(M,\rho,\omega,\sigma,\delta,r_A,m_\omega,T)$ 有效，否则签名无效。

3.4 代理签名权的撤销

正常情况下，代理签名人的代理权会在 m_ω 中规定的代理期限到期后终止。但是如果代理签名人滥用代理权或有其它不法行为，为了体现公平性，原始签名人只在能够提供相应证据并得到有关部门许可的情况下提前撤销代理签名人的代理权，只需把 r_A 放到公开的撤销列表即可。当 r_A 的代理期限终止时，便可将 r_A 从撤销列表中删除，撤销列表不会无限增大，而 r_A 撤销之前产生的代理签名仍可得到验证。因为代理权撤销后代理签名人就不能再产生有效的代理签名，那么产生的签名都可认为是代理权撤销前产生的，这样便解决了代理权撤销问题。

4　安全性分析

分析表明，本文提出的代理盲签名方案满足正确性、强不可伪造性、强不可否认性、强可识别性、可区分性、防止滥用和代理权撤销等性质。

4.1 正确性

代理密钥的产生和代理盲签名的产生阶段需要验证 3 个等式，才能保证签名的正确性和有效性，下面给出式(2), 式

(4), 式(5)的数学证明。

(1)代理签名密钥产生阶段代理签名人通过验证式(2)是否成立来确认原始签名人传递的参数 m_ω, r_A, s_A 是否有效。

证明 $g^{s_A} = g^{x_A + k_A \cdot h} = g^{x_A} g^{k_A \cdot h} = y_A r_A^h \pmod p$

即 $g^{s_A} = y_A r_A^h \pmod p$ 证毕

(2)代理盲签名产生阶段验证人通过验证式(4)是否成立来确认代理签名人是否经过原始签名人授权。

证明

$$y_p = g^{x_p} = g^{x_B \cdot y_B + s_A} = g^{x_B \cdot y_B} g^{s_A} = g^{x_B \cdot y_B} g^{x_A + k_A \cdot h}$$
$$= g^{x_B \cdot y_B} g^{x_A} g^{k_A \cdot h} = y_B^{y_B} y_A r_A^h \pmod p$$

即 $y_p = y_B^{y_B} y_A r_A^h \pmod p$ 证毕

(3)代理盲签名产生阶段通过验证式(5)是否成立来确认产生的代理盲签名是否有效。

证明

$$\omega + \delta = c + t_2 + d + t_4 = e + t_2 + t_4 = (\bmod\ p) g^\rho y_p^\omega$$
$$= g^{r+t_1} y_p^{c+t_2} = g^{u - c \cdot x_p + t_1} y_p^{c+t_2} = g^u g^{-c \cdot x_p} g^{t_1} y_p^{c+t_2}$$
$$= a g^{-c \cdot x_p} g^{t_1}\ y_p^{c+t_2} = a g^{-c \cdot x_p} g^{t_1} g^{x_p (c+t_2)} = a g^{t_1} g^{x_p t_2}$$
$$= a g^{t_1} y_p^{t_2} = \alpha\ (\bmod\ p) g^\sigma T^\delta = g^{s+t_3} T^{d+t_4}$$
$$= g^s T^d g^{t_3} T^{t_4} = b\, g^{t_3} T^{t_4} = \beta (\bmod\ p)$$

则 $H(g^\rho y_p^\omega, g^\rho T^\delta, T, M) = H(\alpha, \beta, T, M)$。因为 $\varepsilon = H(\alpha, \beta, T, M)$，得 $\omega + \delta = \varepsilon = H(\alpha, \beta, T, M) = H(g^\rho y_p^\omega, g^\rho T^\delta, T, M)$。即

$\omega + \delta = \varepsilon = H(g^\rho y_p^\omega, g^\rho T^\delta, T, M)$ 证毕

4.2 强不可伪造性

只有指定的代理签名人能够产生有效代理签名，原始签名人和没有被指定为代理签名人的第三方都不能产生有效代理签名。

(1)伪造者无法根据 y_p 伪造 x_p。因为 $y_p = g^{x_p} = y_B^{y_B} y_A r_A^h \cdot (\bmod\ q)$，而 (r_A, s_A) 是原始签名人对 m_ω 的签名，$m_\omega, r_A, s_A, y_A, y_B$ 是不可更改和伪造的，所以伪造者不可能通过计算 y_p 来伪造 x_p；又已知 y_p 求 x_p 是不可能的，这是基于离散对数问题的。

(2)根据 $x_p = x_B \cdot y_B + s_A$，假如伪造者想要伪造代理签名人的签名，他必须伪造 s_A 和 x_B。根据 $s_A = x_A + k_A \cdot h$，原始签名人的私钥 x_A 和 k_A 对伪造者来说是无法得到的，所以伪造者不可能伪造 s_A；即使原始签名人能够计算出 s_A，但是不知道代理签名人的私钥 x_B，也无法知道 x_p。

(3)利用目前普遍采用的原始签名人伪造方法，先伪造 r_A，再构造代理签名密钥 x_p 的方法(例如文献[7]采用的原始签名人伪造方法)是不可行的，本方案借鉴了 Mambo 方案[5,6]和文献[7]方案的密钥产生，使得不诚实的原始签名人对 r_A 的选择性构造不再能成功地伪造有效的代理签名密钥对。因为由 $y_p = g^{x_p} = y_B^{y_B} y_A r_A^h$ 可知，无法构造出 r_A，使得伪造出来的 x_p 只由 h、x_A、k_A 计算可得，而无需代理签名人的密钥 x_B，因此也就避免了原始签名人伪造。

综上所述，提出的方案不仅能够抵抗普通攻击者的伪造，还可以避免原始签名人伪造，因此具有强不可伪造性。

4.3 强不可否认性

一旦代理签名人代替原始签名人产生了有效的代理签名，他就不能向任何人否认他所签的有效代理签名。

(1)代理签名密钥由代理签名人私钥 x_B 计算得到，任何其他人(包括原始签名人)都不知道代理密钥，只有代理签名人能产生有效代理签名；验证代理签名时需要代理签名人的公钥 y_B，m_ω 中包含代理签名人的身份信息，因此代理签名人无法否认自己产生的代理签名。

(2)代理密钥的产生过程中，代理签名人需要对原始签名人发送过来的代理参数 (m_ω, r_A, s_A) 进行有效性验证，而代理密钥由原始签名人发送的 s_A 计算得到，因此原始签名人不能否认参与了授权过程。

(3)由强不可伪造性可知，任何其它人都不能伪造代理签名，因此一旦产生有效的代理签名，代理签名人就不能向任何人否认他所签的有效代理签名。

4.4 强可识别性

任何人都能够从代理签名中确定代理签名人的身份。因为最终生成代理签名的 m_ω 中包含代理签名人身份信息，任何人都能识别出代理签名人的身份。

4.5 可区分性

由式(4)可知，代理签名的验证过程中需要代理签名人的公钥，原始签名人和代理签名人使用不同结构，因此任何人都可区分代理签名和正常原始签名人的签名。

4.6 防止滥用

(1)防止代理签名权的转移：原始签名人对代理签名人的代理授权信息是 (m_ω, r_A, s_A)，(r_A, s_A) 是原始签名人对 m_ω 的签名，所以 (m_ω, r_A, s_A) 是不可更改的，即一旦原始签名人指定代理签名人，那么由 $y_p = y_B^{y_B} y_A r_A^h$ 可知，y_p 已经确定，除非代理签名人将 x_p 给其他人，否则代理签名人不能利用 (m_ω, r_A, s_A) 再次代理授权。

(2)验证过程中需要能够证明代理签名人身份信息的 m_ω，可以有效地防止代理签名权的滥用。

(3)每次进行消息签名时，都需要对代理签名人的身份信息和代理期限进行有效性验证，并且原始签名人有权在代理人滥用代理权的情况下撤销其代理权，也就有效地约束代理签名人。

4.7 代理签名权的撤销

一旦代理签名人有不法行为，原始签名人只在有合法证据的情况下才能在未到达代理期限时，撤销代理签名人的代理权，这样对原始签名人和代理签名人来说都是公平的。如果代理签名人没有通过代理签名接收人的有效性验证，就不能在代理期限已终止或代理权被撤销之后产生有效签名，这便解决了代理权撤销后无法验证以前签名的问题，因为可以确定产生的签名一定是在代理权撤销前产生的。特别需要指

出的是本方案不需要可信第三方的参与，减轻了系统负担。

5　结束语

本文精心设计了代理签名密钥，并采用Abe-Okamoto部分盲签名技术设计了一个新的可收回代理权的代理盲签名方案。利用签名中嵌入时间戳的方法，在无需可信第三方的前提下有效地解决了普通代理签名方案中代理签名权撤销难的问题，同时有效地防止了代理签名权的滥用、原始签名人伪造和公钥替换攻击；保证了消息的盲化，可应用于对消息有保密性要求的领域。但是由于签名的产生和验证阶段需要验证时间戳的有效性，这对代理签名接收人和验证人都提出了额外的要求，因此其应用范围也受到了一定程度的限制。

参 考 文 献

[1] Tan Z, Liu Z, and Tang C. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP. MM Research Preprints, No.21, MMRC, AMSS, Academia, Sinica, Beijing, 2002, No.21: 212–217.

[2] Lu Eric Jui-Lin, HWang Min-Shiang, and Huang Cheng-Jian. A new proxy signature scheme with revocation. *Applied Mathematics and Computation*, 2005, 161(3): 799–806.

[3] 王晓明，张震，符方伟. 一个安全的门限代理签名方案. 电子与信息学报，2006, 28(7): 1308–1311.
Wang Xiao-ming, Zhang Zhen, and Fu Fang-wei. A secure threshold proxy signature scheme. *Journal of Electronics & Information Technology*, 2006, 28(7): 1308–1311.

[4] Abe M and Okamoto T. Provably secure partially blind signatures. Advances in Cryptology: Crypto' 2000, LNCS, Springer-Verlag, 2000: 271–286.

[5] Mambo M, Usuda K, and Okamoto E. Proxy signatures: delegation of the power to sign messages. *IEICE Trans. Fundamentals*, 1996, E79-A(9): 1338–1354.

[6] Mambo M, Usuda K, and Okamoto E. Proxy signatures for delegating signing operation. Proc. 3rd ACM Conference on Computer and Communications Security, New Delhi: ACM Press, 1996: 48–57.

[7] Wang S H, Wang G L, and Bao F, *et al*.. Cryptanalysis of a proxy-protected proxy signature scheme based on elliptic curve cryptosystem. Vehicular Technology Conference, USA, IEEE 60th 2004: 3240–3243.

[8] 李继国，曹珍富，李建中，等. 代理签名的现状与进展. 通信学报，2003, 24(10): 114–124.
Li Ji-guo, Cao Zhen-fu, and Li Jian-zhong, *et al*.. Present situation and progress of proxy signature. *Journal of China Institute of Communications*, 2003, 24(10): 114–124.

刘文远：　男，1968 年生，教授，博士生导师，研究方向为信息安全、电子商务、智能计算.

佟　凤：　女，1982 年生，硕士生，研究方向为信息安全、密码学、电子商务.

王宝文：　男，1956 年生，副教授，硕士生导师，研究方向为智能计算、企业信息化.