# 一个新的多重代理多重签名方案

祁传达[①②] 王念平[②] 金晨辉[②]
[①](信阳师范学院 数学与信息科学学院 信阳 464000)
[②](解放军信息工程大学 电子技术学院 郑州 450004)

**摘 要** 为克服多重代理签名方案中无法确认谁是真正签名者的弱点，Sun 于 1999 年提出了不可否认的代理签名方案。2000 年 Hwang 等人指出 Sun 的方案不安全，并对 Sun 的方案进行了改进，2004 年 Tzeng, Tan, Yang 各自对 Hwang 等人的方案进行了安全性分析，指出 Hwang 方案容易受到内部伪造攻击。该文通过让原始签名组与代理签名组互动来实现秘密共享和密钥分配的方法，设计了一种新的安全的多重代理、多重签名方案，它能够满足不可否认性和不可伪造性的要求。

**关键词** 数字签名，代理签名，多重代理，多重签名
**中图分类号**：TN918.2 **文章标识码**：A **文章编号**：1009-5896(2006)08-1415-03

# A New Multi-proxy Multi-signature Scheme

Qi Chuan-da[①②] Wang Nian-ping[②] Jin Chen-hui[②]
[①](*College of Mathematics and Information Science, Xinyang Normal University, Xinyang* 464000, *China*)
[②](*Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou* 450004, *China*)

**Abstract** To avoid dispute about who are the actual signers, Sun first proposed a nonrepudiable threshold proxy signature scheme with known signers. Hwang *et al*.(2000) showed that Sun's scheme is insecure and made an improvement on Sun's scheme. Presently, Tzeng, Tan, Yang found that Hwang, *et al*.'s scheme is vulnerable against the conspiracy. This paper used the method of through intercommunion between original signer group and proxy signer group to achieve secret share and distributed keys, designed a new multi-proxy multi-signature scheme. The new scheme fully meets unforgeability and nonrepudiation requirements.

**Key words** Digital signature, Proxy signature, Multi-proxy, Multi-signature

## 1 引言

随着网络的迅速发展，人们迫切需要通过电子设备实现快速、远距离的交易。自 Diffie-Hellman 首次提出公钥密码体制以后，数字签名(也称电子签名)得到了广泛的应用。美国、欧盟分别在 2000 年前后，正式颁布了数字签名法律。《中华人民共和国电子签名法》也于 2005 年 4 月 1 日起正式实施。

Rivest和Shamir等人[1]于 1978 年最早提出数字签名方案，随后许多学者对数字签名进行了大量研究。然而在许多情况下，一个文件有时需要多个人进行签名，有时签名者需要指定别人代替自己签名。Mambo等人[2]于 1996 年首次提出了代理签名方案的概念。所谓代理签名是指原始签名者将签名权委托给可靠的代理人，让代理人代表自己行使签名权。1997 年Kim[3]提出了门限代理签名方案。为克服方案中无法确认谁是真正签名者的弱点，Sun[4]于 1999 年提出了不可否认的代理签名方案。2000 年Hwang [5]指出Sun[4]的方案不安全，并对Sun的方案进行了改进，提出了一个安全的不可否认的代理签名方案。最近，Tzeng[6], Tan[7], Yang[8]均指出Hwang [5]方案容易受到内部攻击，原始签名者可以冒充代理签名组伪造代理签名，并提出了不同的伪造方法。这表明前述这些代理签名方案都不能满足不可否认性和不可伪造性的要求。

本文按照Schnor[9]提出的签名方案的思想，通过原始签名组和代理签名组互动的方式，实现秘密共享和密钥分配，设计了一种新的多重代理、多重签名方案。它能够抵抗内部攻击，满足双方不可否认性和不可伪造性的要求。特别地，当原始签名组成员人数 $l=1$ 时，它就可以作为多重代理签名方案使用；当代理签名组成员人数 $n=1$ 时，它就可以作为代理多重签名方案使用。

## 2 新的多重代理、多重签名方案

在本方案中，有一个由 $l$ 个原始签名者 $O_1,O_2,\cdots,O_l$ 组成的原始签名组和一个由 $n$ 个代理签名者 $P_1,P_2,\cdots,P_n$ 组成的代理签名组。原始签名组全体成员共同授权给代理签名组，要求必须由代理签名组全体成员共同参与，才能代表原始签名组进行代理签名。其委托、签名过程如下：

可信中心选择两个大素数 $p,q$ $\left(2^{1023}<p<2^{1024},\ 2^{159}<q<2^{160}\right)$，且 $q\,|\,p-1$，$g$ 是 $Z_p^*$ 中阶为 $q$ 的生成元，$h(\cdot)$ 是无碰撞的单向 Hash 函数。可信中心公开 $p,q,g,h(\cdot)$。$x_{Oi}$ 是原始签名者 $O_i$ $(i=1,2,\cdots,l)$ 选定的私钥，并公开公钥 $y_{Oi}$ $(y_{Oi}=g^{x_{Oi}} \pmod q)$；$x_{Pj}$ 是代理签名者 $P_j$ $(j=1,2,\cdots,n)$

2005-04-11 收到，2006-03-14 改回
河南省杰出青年科学基金(0312001800)资助课题

选定的私钥，并公开公钥 $y_{Pj}$ ($y_{Pj}=g^{x_{Pj}} \pmod q$)。

以下记 $y_O=\prod_{i=1}^{l}(y_{Oi})^{y_{Oi}}$，$y_P=\prod_{j=1}^{n}(y_{Pj})^{y_{Pj}}$，$m_w$ 表示代理签名授权书，其中包含原始签名者、代理签名组成员的详细信息、授权范围、授权期限等；$m$ 表示待签名的消息。

### 2.1 代理密钥产生阶段

这一阶段为每个代理签名者 $P_j$ ($j=1,2,\cdots,n$) 产生一个部分代理签名密钥对 $(x_j,y_j)$。

(1)每个原始签名者 $O_i(i=1,2,\cdots,l)$ 任选一随机数 $a_i$，计算 $A_i=g^{a_i} \pmod p$ 并广播 $A_i$；每个代理签名者 $P_j(j=1,2,\cdots,n)$ 任选一随机数 $b_j$，计算 $B_j=g^{b_j} \pmod p$ 并广播 $B_j$。

(2)每个签名者(原始签名者和代理签名者)通过计算 $A_i^q\equiv 1 \pmod p (i=1,2,\cdots,l)$，$B_j^q\equiv 1 \pmod p (j=1,2,\cdots,n)$ 是否成立来验证 $A_i$，$B_j$ 的有效性。若 $A_i$，$B_j$ 均有效，继续下一步。

(3)每个原始签名者 $O_i(i=1,2,\cdots,l)$ 计算

$$A=\prod_{i=1}^{l}(A_i)^{A_i} \pmod p,\quad B=\prod_{j=1}^{n}(B_j)^{B_j} \pmod p$$

$$r=A^nB \pmod p,\quad s_i=a_iA_i+x_{Oi}y_{Oi}h(m_w\|r) \pmod q$$

并将 $s_i$ 发送给每个代理签名者 $P_j(j=1,2,\cdots,n)$。

(4)每个代理签名者 $P_j$ ($j=1,2,\cdots,n$) 收到所有的 $s_i(i=1,2,\cdots,l)$ 后，首先按步骤(3)同样的方法计算 $r$，然后验证

$$g^{s_i}\equiv (A_i)^{A_i}(y_{Oi})^{y_{Oi}h(m_w\|r)} \pmod p,\quad i=1,2,\cdots,l \tag{1}$$

是否成立来确认原始签名者中是否存在冒充者。若等式都成立，计算 $s'_j=b_jB_j+x_{Pj}y_{Pj}h(m_w\|r) \pmod q$ 和 $x_j=\sum_{i=1}^{l}s_i+s'_j \pmod q$，并公开 $y_j$ ($y_j=g^{x_j} \pmod p$)。

(5)每个代理签名者 $P_j$ ($j=1,2,\cdots,n$) 收到所有的 $y_i(i\neq j)$ 后，验证

$$y_i\equiv A(B_i)^{B_i}\left[y_O\left(y_{Pi}^{y_{Pi}}\right)\right]^{h(m_w\|r)} \pmod p\ (i\neq j)$$

是否成立来确认代理签名者中是否存在冒充者。若等式都成立，则得到自己的代理密钥对 $(x_j,y_j)$，并记 $Y=(y_1,y_2,\cdots,y_n)$。

### 2.2 代理签名产生阶段

(1)每个代理签名者 $P_j$ ($j=1,2,\cdots,n$) 任选一随机数 $k_j$ 并广播 $K_j$ ($K_j=g^{k_j} \pmod p$)。

(2)每个代理签名者 $P_j$ ($j=1,2,\cdots,n$) 收到所有的 $K_i(i\neq j)$ 后，计算

$$K=\prod_{j=1}^{n}(K_j)^{K_j} \pmod p$$

$$\sigma_j=k_jK_j+x_jy_jh(m\|Y\|K) \pmod q$$

然后将 $(r,Y,K,\sigma_j)$ 发送给签名生成者。

(3)签名生成者计算 $\sigma=\sum_{j=1}^{n}\sigma_j \pmod q$，从而完成对消息 $m$ 的代理签名 $(m,m_w,r,Y,K,\sigma)$。

### 2.3 代理签名验证阶段

签名验证者收到签名 $(m,m_w,r,Y,K,\sigma)$ 后，通过下列步骤验证签名的有效性：

(1)检查消息 $m$ 是否属于授权书 $m_w$ 规定的授权范围，若符合进行下一步。

(2)利用公钥 $y_{Oi}(i=1,2,\cdots,l)$，$y_{Pj}$ 和 $Y=(y_1,y_2,\cdots,y_n)$ 验证

$$\prod_{j=1}^{n}y_j\equiv r(y_O^ny_P)^{h(m_w\|r)} \pmod p \tag{2}$$

是否成立来确认代理签名授权的合法性。若等式成立，进行下一步。

(3)验证

$$g^{\sigma}\equiv K\left[\prod_{j=1}^{n}(y_i)^{y_i}\right]^{h(m\|Y\|K)} \pmod p$$

是否成立来确认代理签名的合法性。若等式成立，则证明代理签名 $(m,m_w,r,Y,K,\sigma)$ 有效。

## 3 安全性分析

本方案的安全性依赖于求解离散对数问题的困难性和 Hash 函数的单向性。

### 3.1 不可伪造性

首先，如果有人想伪造一个授权书 $m_w$ 及对消息 $m$ 的签名 $(m,m_w,r,Y,K,\sigma)$，他必须寻找合适的数 $r,K,\sigma$ 和数组 $Y=(y_1,y_2,\cdots,y_n)$，使得

$$\left.\begin{aligned}\prod_{j=1}^{n}y_j&\equiv r(y_O^ny_P)^{h(m_w\|r)} \pmod p\\ g^{\sigma}&\equiv K\left[\prod_{j=1}^{n}(y_i)^{y_i}\right]^{h(m\|Y\|K)} \pmod p\end{aligned}\right\} \tag{3}$$

成立。若先选定 $r,Y,K$，则他必须通过式(3)计算 $\sigma$，这等价于求解离散对数难题；若先选定 $\sigma$ 和 $r,Y,K$ 中的任意两个，求满足式(3)的另外一个，则他将面对 Hash 函数求逆问题。如果他想利用一个对消息 $m$ 的有效签名 $(m,m_w,r,Y,K,\sigma)$，来伪造一个对 $m'$ 的签名 $(m',m_w,r,Y,K,\sigma')$，他也将面对上述同样问题。

其次，假定有人想冒充某个原始签名者 $O_i$ 参与代理签名授权过程，则在代理签名密钥产生阶段的步骤(4)中，每一个代理签名者都可以识别出来；假定除 $O_i$ 以外的所有原始签名者和全体代理签名者与冒充者恶意串通，来伪造代理密钥 $x_j$ ($j=1,2,\cdots,n$)，由于他们不知道 $O_i$ 的私钥 $x_{Oi}$，所以，要想伪造一个能满足代理签名授权的合法性验证条件(2)的代理密钥，必须选择适当的 $s_l$ 使式(1)满足，这等价于求解离散对数难题。

再次，原始签名者虽然参与了代理密钥的产生过程，但并不知道代理密钥，即使所有的原始签名者联合起来，也不可能伪造签名。若有人冒充或与其他代理签名者及原始签名者恶意串通冒充某个代理签名者 $P_j$ 参与签名过程，它必须选

择适当的 $\sigma'_j$，使得

$$g^{\sigma'_j}\cdot g^{\sum_{i=1,i\neq j}^{n}\sigma_i}\equiv K\left[\prod_{j=1}^{n}(y_i)^{y_i}\right]^{h(m\|Y\|K)}\pmod p$$

成立。这同样面临求解离散对数难题。

### 3.2 不可否认性

代理密钥必须由原始签名者 $l$ 个原始签名者 $O_i(i=1,2,\cdots,l)$ 和 $n$ 个代理签名者 $P_j$ $(j=1,2,\cdots,n)$ 共同参与才能产生，所以每个原始签名者都不能否认自己参与了授权过程，每个代理签名者也不能否认自己参与了授权过程并获得了授权。$r$ 是授权过程的见证，它与授权书 $m_w$ 具有相同的寿命周期。

由于代理签名的产生需要用到所有代理签名者的私钥，缺少代理签名组中的任何一个人，都无法获得有效的代理签名 $(m,m_w,r,Y,K,\sigma)$。所以，每个代理签名者事后都不能否认自己参与了签名过程，否认签名等于宣称自己的私钥泄密。

### 3.3 签名者私钥和代理密钥的安全性

由于在每次代理签名授权过程中，原始签名者和代理签名者的私钥 $x_{Oi}$ 和 $x_{Pj}$ 都是与随机数 $a_i,b_j$ 一起使用的，不同的授权过程选择的随机数也不同。所以，即使经过了多次授权，也不会暴露签名者的私钥。同样，在每次签名过程中，代理密钥 $x_j$ 总是和随机数 $k_j$ 一起使用，不同的签名过程选择的随机数也不同。因而，在一个授权期限内，代理签名的次数再多，也不会危及代理密钥的安全。代理密钥在代理授权期限内可以重复使用。

## 4 结束语

以往的多重代理签名方案的代理密钥的产生都是由原始签名组单方产生，然后再向代理签名组成员进行分配。这样，原始签名组成员合谋就能恢复代理密钥，因而能够很容易伪造签名。

本文提出的多重代理、多重签名方案是通过原始签名组和代理签名组互动的方式，实现秘密共享和密钥分配的，原始签名者虽然参与了代理密钥的产生过程，但并不知道代理密钥，即使所有的原始签名者联合起来，也无法恢复代理密钥。

因此，本文提出的方案比Sun[4]和Hwang[5]的方案更安全，它能够抵抗内部攻击，满足双方不可否认性和不可伪造性的要求。

在本文提出的方案中，当原始签名组成员人数 $l=1$ 时，它就可以作为多重代理签名方案使用；当代理签名组成员人数 $n=1$ 时，它就可以作为代理多重签名方案使用。

## 参 考 文 献


[1] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystem[J]. *Comm. of the ACM*, 1978, 2(2): 120 –146.

[2] Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign message[J]. *IEICE Trans. on Fundam*, 1996, E79-A(9): 1338 –1353.

[3] Kim S J, Park S J, Won D H. Proxy signatures, revisited[A]. Proc. Of the ICICS'1997, Lecture Notes in Computer Science[C], 1997, Vol.1334: 223–232.

[4] Sun H M. An efficient nonrepudiable threshold proxy signature scheme with known signers[J]. *Computer Communications*, 1999, 22(8): 717–722.

[5] Hwang M S, Lin I C, Lu E J L. A secure nonrepudiable threshold proxy signature scheme with known signers[J]. *International Journal of Informatica*, 2000, 11(2): 1–8.

[6] Tzeng S F, Hwang M S, Yang C Y. An improvement of nonrepudiable threshold proxy signature scheme with known signers[J]. *Computers & Security*, 2004, 23: 174 –178.

[7] Tan Z W, Liu Z J. On the security of some nonrepudiable threshold proxy signature scheme with known signers[EB/OL]. http://eprint.iacr.ong/2004/234.

[8] Yang F Y, Jan J K, Jeng W J. Cryptanalysis of a threshold proxy signature scheme with known signers[EB/OL]. http://eprint.iacr.ong/2004/313.

[9] Schnorr C P. Efficient signature generation for smart cards[J]. *Journal of Cryptology*, 1991, 4(30): 161–174.



祁传达：　男，1965 年生，博士生，副教授，主要研究方向为密码理论和信息安全.

王念平：　男，1973 年生，博士生，讲师，主要研究方向为密码理论、应用数学.

金晨辉：　男，1965 年生，教授，博士生导师。主要研究方向为密码学与信息安全.