一种新型的代理签名方案

谷利泽 张 胜 杨义先
(北京邮电大学信息安全中心 北邮国家重点实验室 北京 100876)

摘 要：可识别性是一般代理签名方案的一个特点，即验证者能够从代理签名中确定代理者的身份。在一些特殊的应用中，原始签名者希望在代理签名中隐藏代理签名者身份，验证者无法从代理签名中识别代理者身份，在出现争议时，验证者能通过原始签名者揭示代理者的身份，该文提出的方案能满足这种需求。

关键词：代理签名，可识别性，匿名性，可跟踪性
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2005)09-1463-04

A New Proxy Signature Scheme

Gu Li-ze Zhang Sheng Yang Yi-xian
(*Information Engineering School, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract Identifiability is one of several security requirements of general proxy signature schemes, i.e. a verifier can determine the identity of the corresponding proxy signer from a proxy signature. In special application, the original signer wants to conceal the identity of the corresponding proxy signer in the proxy signature. The verifier can not recognize the identity of the proxy signer from the proxy signature. In the case of a later dispute, the verifier can reveal the real identity of the proxy signer with the help of the original signer from the proxy signature. In the paper, a new proxy signature scheme should satisfy this requirement.

Key words Proxy signature, Identifiability, Anonymity, Traceability

1 引言

代理签名是Mambo等人[1]于1996年第一次提出的，它的主要思想是原始签名者把他的签名权授权给指定的代理者，代理者代表原始签名者行使其签名权，由于实际应用需求不同，人们已经提出许多类型代理签名方案，如强代理签名[2]和弱代理签名、事先指定代理者签名和不事先指定代理者签名[3]、保护代理者签名[4]和非保护代理者签名等等。

新型的代理签名方案不同于以往各类型的代理签名方案[5]，它在代理签名中隐藏代理签名者身份，验证者无法从代理签名中识别代理者身份，在出现争议时，验证者可以通过原始签名者揭示代理签名者的身份。新方案与非保护代理者签名(proxy-unprotected proxy signature)是有区别的，非保护代理者签名是原始签名者对代理签名者的完全信任，它的代理签名不包含代理签名者身份的任何信息。新方案在实际应用中是有需求的，例如为了保密当前本单位人事关系或将来可能人事变化，原始签名者希望对外保密代理签名者身份，又不能完全信赖代理签名者，新方案满足这类需求。其实，本文提出代理签名的一种新划分，即公开代理签名(一般代理签名方案)和匿名代理签名(本文设计的新型代理签名方案)。

2 符号的约定

下面介绍在新方案中使用的符号含义：

p 为大素数(满足安全要求)；g 为域 GF(p) 的本原元；q 为 $p-1$ 的大素数因子，且满足

$$g^q \equiv 1 (\mathrm{mod}\ p)$$

h 为安全的哈希杂凑函数；m 为签名的消息；A 为原始签名者；B 为代理签名者；V 为签名验证者；m_w 是指描述原始签名者 A 授权代理签名者 B 代理权限约定的授权书，包括 A 的标识、B 的代理期限、签名消息范围等内容；x_A 为原始签名者 A 的私钥；y_A 为原始签名者 A 的公钥：

$$y_A = g^{x_A} \bmod p$$

2004-03-28 收到，2004-08-20 改回
国家“973”计划(G1999035804)和国家自然科学基金(60372094，90204017)资助课题

x_B 为代理签名者 B 的私钥； y_B 为代理签名者 B 的公钥：$y_B = g^{x_B} \bmod p$； x_P 为原始签名者 A 和代理签名者 B 共同生成的代理私钥； y_P 为 x_P 相对应的代理公钥：

$$y_P = g^{x_P} \bmod p$$

ID_B 为代理签名者 B 的标识； ID_P 为代理签名者的标识；$\mathrm{Sig}(x,m)$ 为基于离散对数的数字签名算法，参数 x 为签名者私钥，参数 m 为签名的消息，签名返回值为 σ；$\mathrm{Ver}(y,\sigma,m)$ 为与签名算法 Sig 相对应的签名验证算法；参数 y 为签名者公钥，返回值为真或假。

3 方案的模型

这部分中，使用通用方式定义匿名代理签名方案。

3.1 定义

定义1 (匿名代理签名) 假设原始签名者 A 拥有一对密钥对 (x_A,y_A)，代理签名者 B 拥有一对密钥对 (x_B,y_B)，m_w 是代理授权书，$\sigma_A = \mathrm{Sig}(x_A,m_w)$ 是 A 使用他的私钥 x_A 对 m_w 的签名值，σ_B 是 B 使用他的私钥 x_B 生成的自签名值，则匿名代理签名方案由以下第 4 节算法构成：(PKG, PS, PV, PR)。

(1) PKG 是代理密钥对生成算法，它的输入值是 σ_A 和 σ_B，其输出是代理密钥对 (x_P,y_P)，它的实现是由原始签名者 A 和代理签名者 B 经过三轮交互来完成的，其表示形式为

$$(x_P,y_P) \leftarrow \mathrm{PKG}(\sigma_A,\sigma_B)$$

(2) PS是代理签名算法，代理签名者 B 使用代理私钥 x_P 对消息 m 签名，其输入值为 x_P 和 m，输出值是代理签名值 σ_P，其表示形式为

$$\sigma_P \leftarrow \mathrm{PS}(x_P,m)$$

(3) PV是代理签名验证算法，验证者 V 对代理签名进行验证，其输入值为代理签名 (σ_P,m,m_w,y_A)，输出是一个布尔值，要么是真，要么是假，其表示形式为：

$$\mathrm{PV}(\sigma_P,m,m_w,y_P) \stackrel{?}{=} \mathrm{true}$$

(4) PR是揭示代理者身份算法，验证者 V 向原始签名者 A 提交 (σ_P,m_w) (输入值)，原始签名者 A 向验证者 V 返回代理签名者的标识 ID_P，其表示形式为

$$\mathrm{ID}_P \leftarrow \mathrm{PR}(\sigma_P,m_w)$$

3.2 特点

匿名代理签名方案满足以下安全要求：

(1)可验证性：验证者能够验证代理签名的有效性，并且根据代理签名确认这是原始签名者承认的代理签名。

(2)不可伪造性：没有被指定为代理签名的人无法伪造一个代表原始签名者的代理签名，即使原始签名者也不能伪造代理签名。

(3)防止代理权限滥用：代理签名不应超出代理授权书的约定和防止代理权的转移，任何滥用代理权限所带来的后果完全由代理签名者负责。

(4)匿名性：验证者从代理签名中不能确定代理签名者身份。

(5)可跟踪性：原始签名者能识别有效代理签名的代理签名者真实身份。

(6)不可否认性：原始签名者从代理签名中揭示出代理签名者身份，代理签名者不能否认这个代理签名是由自己生成的。

4 新方案的实现

新方案的参加者包括：原始签名者 A、代理签名者 B、签名验证者 V。下面利用离散对数详细描述新方案实现过程：

4.1 代理密钥对的生成 (PKG)

第 1 步 原始签名者 A 通过安全通道向代理签名者 B 发送代理授权书 m_w，B 收到 m_w 后，如果接受代理授权，则秘密计算生成自己的代理密钥 s_B 和 r_1,s_1，其计算过程如下：

$$\begin{aligned} &k_B \in_R Z_q^* \\ &r_B = g^{k_B} \bmod p \\ &s_B = x_B + k_B r_B \bmod q \\ &k_1 \in_R Z_q^* \\ &r_1 = g^{k_1} \bmod p \\ &s_1 = x_B h(r_B,\mathrm{ID}_B,r_1) + k_1 \bmod q \end{aligned}$$

然后，B 把 $(r_B,\mathrm{ID}_B,r_1,s_1)$ 返回给 A，A 验证下面等式：

$$g^{s_1} \stackrel{?}{=} y_B^{h(r_B,ID_B,r_1)} r_1 \bmod p$$

如果等式成立，原始签名者 A 秘密保存 (r_B,y_B,ID_B) 以备日后需要时揭示代理签名者身份，然后计算 $Y_p = y_B r_B^{r_B} \bmod p$ 并把 Y_P 写入 m_w 中。

第 2 步 原始签名者 A 对增添 Y_P 的 m_w 进行数字签名，其计算过程如下：

$$\begin{aligned} &k_A \in_R Z_q^* \\ &r_A = g^{k_A} \bmod p \\ &s_A = x_A h(m_w,r_A) + k_A \bmod q \end{aligned}$$

A 把得到的签名值 (r_A,s_A) 和 m_w 通过安全通道发送给 B，B 验证下面等式：

$$g^{s_A} \stackrel{?}{=} y_A^{h(m_w,r_A)} r_A \bmod p$$

如果等式成立，B 秘密保存 (r_A,s_A,m_w,s_B)。

第 3 步　代理签名者 B 生成代理私钥 x_P，即 $x_P = s_A + s_B \bmod q$。

4.2 代理签名算法(PS)

如果消息 m 符合代理授权书 m_w 的约定，代理签名者 B 利用签名算法 Sig，使用代理私钥 x_P 生成代理签名 σ_P，即 $\sigma_P = \mathrm{Sig}(x_P, m)$，其代理签名值为 $(m, \sigma_P, m_w, r_A, y_A)$。

4.3 代理签名验证算法(PV)

第 1 步　验证者 V 验证消息 m 是否符合代理授权书 m_w 的约定，如果符合，进入第二步，否则认为代理签名 σ_P 无效。

第 2 步　验证者 V 利用代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 计算 $y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p$ (其中 Y_P 从 m_w 中得到)，然后检查等式：$\mathrm{Ver}(y_P, \sigma_P, m) \stackrel{?}{=} \mathrm{true}$ 是否成立，如果成立，代理签名有效，否则无效。

4.4 揭示代理者身份算法 (PR)

第 1 步　验证者 V 向原始签名者 A 提供代理签名 $(m, \sigma_P, m_w, r_A, y_A)$，$A$ 使用代理签名验证算法 PV 验证其代理签名的有效性，若验证有效，进入第二步。

第 2 步　原始签名者 A 从 m_w 中得到 Y_P，然后依此取出在代理密钥对生成阶段保存的 $(r_B, y_B, \mathrm{ID}_B)$，判断等式：$Y_P \stackrel{?}{=} y_B r_B^{r_B} \bmod P$，如果存在 $(r_B, y_B, \mathrm{ID}_P)$ 满足这个等式，则 ID_P 是实现代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 的代理签名者。

5 方案的分析

5.1 可验证性

定理 1　代理签名者 B 使用代理私钥 x_P，代表原始签名者 A 对消息 m 签名，验证者 V 利用代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 计算代理公钥：

$$y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p$$

然后使用 y_P 验证相应的代理签名，那么 $y_P = g^{x_P} \bmod p$。

证明　由于

$$x_P = s_A + s_B \bmod q$$
$$s_A = x_A h(m_w, r_A) + k_A \bmod q$$
$$s_B = x_B + k_B r_B \bmod q$$
$$Y_P = y_B r_B^{r_B} \bmod p$$

所以

$$\begin{aligned} g^{x_P} &= g^{s_A + s_B} \bmod p \\ &= g^{x_A h(m_w, r_A) + k_A + x_B + k_B r_B} \bmod p \\ &= g^{x_A h(m_w, r_A)} g^{k_A} g^{x_B} g^{k_B r_B} \bmod p \\ &= y_A^{h(m_w, r_A)} r_A y_B r_B^{r_B} \bmod p \\ &= y_A^{h(m_w, r_A)} r_A Y_P \bmod p \\ &= y_P \end{aligned}$$

即 $y_P = g^{x_P} \bmod p$ 成立。　证毕

由于代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 包含 y_A，表明这是原始签名者 A 承认的代理签名。

5.2 不可伪造性

(1) 根据 y_P，伪造者无法伪造 x_P。这是因为 $y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p$，而 (r_A, s_A) 是 A 对 m_w 的签名，Y_P 包含在 m_w 中，r_A，s_A，m_w，Y_P 都是不可更改和伪造的，所以伪造者不可能通过计算 y_P 伪造 x_P，又已知 y_P 求 x_P 是离散对数问题。

(2) 根据 $x_P = s_A + s_B \bmod q$，假如伪造者能够伪造代理签名者 B 的代理签名，伪造者必须同时具备以下两个条件：

(a) 伪造 s_A，因为

$$s_A = x_A h(m_w, r_A) + k_A \bmod q$$

而 A 的私钥 x_A 和 k_A 对伪造者都是无法得到的，所以伪造者不可能伪造 s_A。又由于原始签名者 A 和代理签名者 B 之间的交互都是经过安全通道完成的，所以伪造者不可能冒充 B 或直接窃取 s_A。

(b) 伪造 s_B，由于

$$s_B = x_B + k_B r_B \bmod q$$

而 B 的私钥 x_B，k_B 和 r_B 对伪造者都是无法得到的，所以伪造者也不可能伪造 s_B。

所以，根据 $x_P = s_A + s_B \bmod q$，伪造者不可能得到 x_P。

(3) 原始签名者 A 也不可能伪造代理签名者 B 的代理签名，虽然 A 可得到 s_A，却无法得到 s_B，这是因为 $s_B = x_B + k_B r_B \bmod q$，$B$ 的私钥 x_P 和 k_B (虽 A 可知 r_B，但已知 r_B 推出 k_B 是离散对数问题)对于 A 是无法获得的，所以 A 也是不可能得到 x_P。

总之，除了代理签名者 B，任何人都无法伪造 A 的代理签名。

5.3 防止代理权限滥用

防止代理权限滥用其实包含两层含义：

(1) 防止代理权的转移：原始签名者 A 对代理签名者 B 的代理授权信息是 (m_w, r_A, s_A)，(r_A, s_A) 是 A 对 m_w 的签名，所以 r_A，s_A，m_w 都是不可更改的，且 Y_P 包含在 m_w 中，代理公钥:

$$y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p$$

即一旦原始签名者 A 指定代理签名者 B，y_P 就已经确定，除非 B 把 x_P 给他的代理者，否则 B 不能利用 (m_w, r_A, s_A) 再次代理授权。

(2) 防止代理签名者越权：代理签名验证算法 (PV) 的第 1 步就是验证消息 m 是否符合代理授权书 m_w 的约定，如果不符合，那么签名无效，所以 A 可以充分利用代理授权书

m_w有效约束B代理权限范围。

5.4 匿名性、身份确认和不可否认性

验证者V利用代理签名(m,σ_P,m_w,r_A,y_A)计算代理公钥:

$$y_P = y_A^{h(m_w,r_A)} r_A Y_P \bmod p$$

验证这个代理签名，(m,σ_P,m_w,r_A,y_A)没有包含代理签名者身份，虽然已知$Y_p = y_B r_B^{r_B} \bmod P$，但$r_B$对于$V$是无法得到的，已知$Y_p$是无法推出$y_B$的，由此可见，验证者$V$能够验证代理签名的有效性，但并不知代理签名者的身份。

在必要时，在原始签名者A的帮助下，验证者V利用揭示代理者身份的算法(PR)，能够揭示代理签名者的身份。

由上面5.2节的不可伪造性可知，除代理签名者B外任何人(包括原始签名者A)都不能伪造B的代理签名，所以B不能否认由A揭示的代理签名是由自己生成的。

6 结束语

代理签名者往往是原始签名者信得过和器重的人，原始签名者和代理签名者这种紧密关系有时希望对外界保密，新方案就是针对这类需求而设计的，在原有强代理签名方案的基础上增添了匿名代理者身份和可跟踪的特点，为代理签名方案增添新类型方案。

参 考 文 献

[1] Mambo M, Usuda K, Okamoto E. Proxy signature: delegation of the power to sign messages. EICE Trans. Fundamentals, 1996, E79-A:9: 1338 – 1353.

[2] Lee B, Kim H, Kim K. Strong proxy signature and its applications. International Conference on Information and Communication Security, Proc. of SCIS, Japan, 2001: 603 – 608.

[3] Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature Proc. ACISP, Spring-Verlag, 2001, LNCS 1334: 474 – 486.

[4] Shum K, Wei Victor K. A strong proxy signature scheme with proxy signer privacy protection.http://www.computer.org/proceedings/wetice/1748/17480055.pdf, 2002.

[5] Kim S, Park S, Won D. Proxy signature, revisited, International Conference on Information and Communication Security, Proc of ICICS' 97, Berlin, Springer, 1997: 223 – 232.

谷利泽： 男，1965年生，博士生，研究方向为现代密码学及电子商务等.

张 胜： 男，1974年生，博士生，研究方向为密码学、电子商务和网络安全.

杨义先： 男，1961年生，教授，博士生导师，长江学者奖励计划特聘教授、香港中文大学信息工程系访问教授，主要从事现代密码学、编码理论、电子商务等方面的研究工作.