第 36 卷 第 9 期 计 算 机 工 程 2010 年 5 月
Vol.36 No.9 Computer Engineering May 2010
·安全技术· 文章编号：1000—3428(2010)09—0145—02 文献标识码：A 中图分类号：TP309.2

保护代理人身份的多级多重代理签名方案

任 燕，王济荣
(运城学院应用数学系，运城 044000)

摘 要：基于 RSA 签名体制，提出一个可以保护代理人身份的多级多重代理签名方案，利用影子身份产生中心为每个代理人产生一个影子身份，以影子身份为消息签名，确保代理人的身份不被泄露。当代理人滥用职权时，权威机构可以要求影子身份产生中心根据其影子身份追溯代理人的真实身份。安全性分析表明，该方案具有不可否认性、可区分性和不可伪造性。

关键词：代理签名；多级代理签名；多重代理多重签名；代理人身份保护

Multiple Grade and Multi-proxy Signature Scheme Protecting Agent Identity

REN Yan, WANG Ji-rong
(Department of Applied Mathematics, Yuncheng University, Yuncheng 044000)

【Abstract】This paper proposes a multiple grade and multi-proxy signature scheme to protect agents' identity based on RSA signature scheme. The producing center of shadow identity gives every agent a shadow identity to sign for messages, which ensures that agents' identity can not be divulged, and the authority can ask producing center of shadow identity to trace back to the true identity of an agent when he abuses his power. Security analysis shows that the scheme has the properties of non-repudiation and distinguish ability, and it can not be faked up.

【Key words】proxy signature; multiple grade proxy signature; multi-proxy multi-signature; agent identity protection

1 概述

为了解决数字化信息社会中的数字签名权委托问题，文献[1-2]提出了代理签名的概念。然而在某些情况下，代理签名人在得到原始签名人的授权后，由于身体不适或工作繁忙等原因无法亲自签名，需要将签名权力进一步委托，由此，文献[3]提出了多级代理签名的概念，文献[4-5]提出了一些多级代理签名方案。但是现有的多级方案中各级代理人只有一个，因此，代理签名人权利过于集中。文献[6-9]提出多重代理多重签名方案，但多重代理多重签名局限于一级。文献[10]将代理签名分为未对代签名人提供保护的代理签名和对代签名人提供保护的代理签名。本文将多级代理、多重代理多重签名与保护签名人身份相结合，提出了一个保护代理人身份的多级多重代理签名方案。其用影子身份产生中心为每个代理人产生一个影子身份，并用影子身份为消息签名，从而保护代理人的身份不被泄露，但是当某个代理人滥用职权时，权威机构可以要求影子身份产生中心根据其影子身份追溯代理人的真实身份。与现有的方案相比，本方案同时突破了多级代理签名方案中各级代理人只有一个和多重代理签名的“一级”的局限，并可以实现代理人身份保护。

2 保护代理人身份的多级多重代理签名方案

2.1 系统参数设置

可信中心 SA 选择大素数 p, q，其中，$q|p-1$。设 g 是 Z_p^* 中阶为 q 的生成元，PGC 为安全的影子身份产生中心，私钥为 $x_{\mathrm{PGC}} \in Z_q^*$，对应的公钥 $y_{PGC} = g^{x_{\mathrm{PGC}}} \pmod p$。设原始签名人为 $P_0 = P_{01}, P_{02}, \cdots, P_{0n_0}$，私钥为 $x_{P_{0j}} \in Z_q^*$，对应的公钥为 $y_{P_{0j}} = g^{x_{P_{0j}}} \pmod p$ $(j = 1,2,\cdots,n_0)$。对应的 i 级代理为 $P_i = P_{i1}, P_{i2}, \cdots, P_{in_i}$，它们的密钥对分别为 $\left(x_{P_{ij}}, y_{P_{ij}}\right)$ $(j = 1,2,\cdots,n_i)$，满足 $x_{P_{ij}} \in Z_q^*$，$y_{P_{ij}} = g^{x_{P_{ij}}} \pmod p$。原始签名人和一级代理间有授权证书 w_1，它包含对一级代理签名人再授权范围等事项的说明。一级代理签名人对二级代理签名人的授权是否合法要根据 w_1 判断。同理，i-1 级代理签名人与 i 级代理签名人间有授权证书 w_i，包含的内容同上。id_{P_0}，id_{PGC}，id_{P_i} 分别是 P_0，PGC，$P_i (i = 1,2,\cdots,n)$ 的身份。H 为安全单向 hash 函数。

2.2 代理授权过程

代理授权过程分为 2 个阶段。

(1)PGC 为 P_{ij} $(j = 1,2,\cdots n_i)$ 产生影子身份 $n_{P_{ij}}$，公开参数 r_{ij}' 和部分签名私钥 s_{ij}'。具体过程如下：

1) P_{ij} 在 PGC 登记，注册其身份 $id_{P_{ij}}$ $(j = 1,2, \cdots n_i)$。

2)PGC 选择 $r_{ij}' \in Z_q^*$，计算 $n_{P_{ij}} = H(id_{P_{ij}}, r_{ij}')$。

3)PGC 选择 $k_{ij}' \in Z_q^*$，计算 $s_{ij}' = (k_{ij}' + x_{\mathrm{PGC}} H(n_{P_{ij}}, r_{ij}')) \bmod p)$，$r_{ij}'' = g^{k_{ij}'} \bmod p$。然后把 $\left\{n_{P_{ij}}, s_{ij}', r_{ij}'\right\}$ 妥善保存在自己的数据库中，再把 $\left\{n_{P_{ij}}, s_{ij}', r_{ij}'\right\}$ 通过安全信道发送给 P_{ij}，一旦 P_{ij} 做出违法的事，PGC 可以确定其身份。

4) P_{ij} 收到 $\left\{n_{P_{ij}}, s_{ij}', r_{ij}'\right\}$ 后验证 $r_{ij}' y_{\mathrm{PGC}}^{H(n_{P_{ij}}, r_{ij}')} \stackrel{?}{\equiv} g^{s_{ij}'} \bmod p$。若

基金项目：山西省自然科学基金资助项目(2009011005-3)
作者简介：任 燕(1982－)，女，讲师，主研方向：密码学，有限域；王济荣，副教授
收稿日期：2009-11-27 **E-mail：**renyan-2000@163.com

该式成立，P_{ij} 把 $s_{ij}^{'}$ 作为在代理阶段计算代理签名私钥的一部分，$n_{P_{ij}}$ 作为与 $id_{P_{ij}}$ 相联系的影子身份。

(2) P_{i-1} 为 P_i 产生另外一部分签名私钥 $s_{ij}^{''}$，公开参数 t_{ij}。具体过程如下：

1) P_{i-1} 中每个代理人分别选择 $k_{ij}^{''} \in Z_q^*$，计算：

$$t_{ij} = g^{k_{ij}^{''}} (\mathrm{mod}\ p), s_{ij}^{''} = (k_{ij}^{''} + x_{P_{ij}} e)(\mathrm{mod}\ q)$$

$$e = h(w_i, t_{ij})$$

P_{i-1} 把 $\left\{s_{ij}^{''}, w_i, t_{ij}\right\}$ 发送给 P_{ij}。

2) P_{ij} 收到 $\left\{s_{ij}^{''}, w_i, t_{ij}\right\}$ 后先计算 $e = h(w_i, t_{ij})$，再验证：

$$t_i y_{p_{i-1}}^{\ e} \stackrel{?}{\equiv} g^{s_{2i}} \bmod p$$

若该式成立，则接受 P_{i-1} 的授权，并把 $s_{ii}^{''}$ 作为签名私钥的一部分，否则，不接受授权。

2.3 代理签名产生

设 P_i 要签名的消息为 m_i，代理签名产生步骤如下：

(1) P_i 中每个代理人计算 $s_{ij} = (s_{ij}^{''} H(s_{1j}^{'}, id_{P_{ij}}) + s_{1j}^{'} x_{P_{ij}}) (\mathrm{mod}\ q)$ 作为签名私钥。

(2) P_i 中每个代理人计算 $y_{ij} = g^{s_{ij}} (\mathrm{mod}\ p)$ 作为签名公钥。

(3) P_i 中每个代理人随机选择 $\alpha_{ij} \in Z_q^*$，计算 $R_{ij} = g^{\alpha_{ij}} \bmod p$ 并公开 $R_{ij}, n_{P_{ij}}$。

(4) P_i 中每个代理人计算：

$$R_i = \prod_{j=1}^{n_i} R_{ij} (\mathrm{mod}\ p)$$

$$e_{ij} = H(m_1, w_1 \| \cdots \| w_i \| id_{P_{ij}} \| \cdots \| R_i \| n_{P_i})$$

$$S_{ij} = \alpha_{ij} + s_{ij} e_{ij}$$

并公开 R_i, S_{ij}。

(5)签名生成者计算：

$$S_i = \sum_{j=1}^{n_i} S_{ij} (\mathrm{mod}\ q) \quad N_{P_i} = \prod_{j=1}^{n_i} n_{P_{ij}} (\mathrm{mod}\ p)$$

$$Y_i = \prod_{j=1}^{n_i} y_{ij} (\mathrm{mod}\ p)$$

则 P_i 对 m_i 的代理签名为 $\left(S_i, N_{P_i}, R_i, w_1, \cdots, w_i, Y_i, m_i\right)$。

2.4 代理签名验证

接收者收到 $\left(S_i, n_{P_i}, R_i, w_1, \cdots, w_i, m_i\right)$ 后计算

$$e_{ij} = H(m_1, w_1 \| \cdots \| w_i \| id_{P_{ij}} \| \cdots \| R_i \| n_{P_i})$$

验证 $g^{S_i} = R_i Y_i^{e_{ij}} (\mathrm{mod}\ p)$ 是否成立，如果成立，则接受签名。

定理 1 第 i 级代理签名人通过 $r_{ij}^{'} y_{\mathrm{PGC}}^{\ H(n_{P_{ij}}, r_{ij})} \stackrel{?}{\equiv} g^{s_{ij}^{'}} \bmod p$ 及 $t_{ij} y_{P_{i-1,j}}^{\ e} = g^{s_{ij}^{''}} (\mathrm{mod}\ p)$ 验证 P_{i-1} 所发私钥的正确性。

证明：

$$g^{s_{ij}^{'}} = g^{k_{ij}^{'} + x_{\mathrm{PGC}} H(n_{P_{ij}}, r_{ij})} = g^{k_{ij}^{'}} g^{x_{\mathrm{PGC}} H(n_{P_{ij}}, r_{ij})} = r_{ij}^{'} y_{\mathrm{PGC}}^{\ H(n_{P_{ij}}, r_{ij})}$$

$$g^{s_{ij}^{''}} = g^{k_{ij}^{''} + x_{P_{i-1,j}} h(w_1, t_{ij})} = g^{k_{ij}^{''}} g^{x_{P_{i-1,j}} h(w_1, t_{ij})} = t_{ij} y_{P_{i-1,j}}^{\ e} \ (\mathrm{mod}\ p)$$

定理 2 若一级代理签名按上面步骤生成，则签名的合法性可通过等式 $g^{S_i} = R_i y_i^{e_i} (\mathrm{mod}\ p)$ 进行验证。

证明：

$$g^{S_i} = g^{S_{i1} + S_{i2} + \cdots + S_{in_i}} = g^{S_{i1}} g^{S_{i2}} \cdots g^{S_{in_i}} =$$

$$g^{\alpha_{i1} + s_{i1} e_{i1}} g^{\alpha_{i2} + s_{i2} e_{i2}} \cdots g^{\alpha_{in_i} + s_{in_i} e_{in_i}} = g^{\alpha_{i1}} g^{\alpha_{i2}} \cdots g^{\alpha_{in_i}}$$

$$g^{s_{i1} e_{i1}} g^{s_{i2} e_{i2}} \cdots g^{s_{in_i} e_{in_i}} = R_{i1} R_{i2} \cdots R_{in_i} y_{i1}^{\ e_{i1}} y_{i2}^{\ e_{i2}} \cdots y_{in_i}^{\ e_{in_i}} =$$

$$R_i Y_i^{e_{ij}} (\mathrm{mod}\ p)$$

3 安全性分析

本方案具有如下特性：(1)可以保护代理签名人的身份。由代理授权的第(1)阶段可知，安全的影子身份产生中心 PGC 为代理人产生的影子身份可以实现代理人身份保护，基于安全的 hash 函数，任何人不能由代理签名人的影子身份得到他的真实身份，但是当某个代理签名人滥用签名权时，权威中心可以根据其影子身份要求 PGC 在他的数据库中追查出代理人的真实身份。(2)具有强不可否认性和可区分性。在本方案中代理人不能否认自己的签名。在代理签名中，虽然没有代理签名人的身份特征，但有其影子身份 n_{p_i}，n_{p_i} 是与代理人相对应的，且代理人不能伪造影子身份，所以，代理签名人一旦生成代理签名便不能否认。又由于安全 hash 函数的特性，所有代理签名人的影子身份是不同的，因此生成的代理签名是不同的，即可区分的。(3)具有强不可伪造性。首先，任何人无法由原始签名人的公钥获得其私钥，因此，无法伪造原始签名人生成的普通的数字签名。其次，任何人不能由代理人的签名公钥获得其代理签名私钥，而且由代理签名产生阶段(1)可知，即使原始签名人与 PGC 合谋，也无法获取代理签名人的私钥，因此，无法伪造代理签名。

4 结束语

本文基于 RSA 签名体制，提出了一种新的多级多重代理签名方案，不仅可以确保代理人身份不被泄露，当某个代理人滥用职权时，权威机构还可以要求影子身份产生中心根据其影子身份追溯他的真实身份，大大增加了方案的灵活性和实用性。理论分析表明本文的方案是安全的。

参考文献

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages[J]. IEICE Trans. on Fundamentals of Electronics Communications and Computer Sciences, 1996, 79(9): 1338-1354.

[2] Mambo M, Usuda K, Okamoto E. Proxy Signatures for Delegation Signing Operation[C]//Proc. of the 3rd Conference on Computer and Communications Security. New York, USA: ACM Press, 1996.

[3] 伊丽江. 代理签名及应用研究[D]. 西安: 西安电子科技大学, 2000.

[4] 蔡 勉, 康 莉. 一种防抵赖的多级代理签名方案[J]. 北京工业大学学报, 2006, 32(10): 62-67.

[5] 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): 78-80.

[6] 杨迎辉, 孙艳蕊, 袁喜凤, 等. 改进的门限多代理多重共享验证签名方案[J]. 计算机工程, 2008, 34(23): 170-172.

[7] 祁传达, 李 溪, 金晨辉. 基于RSA的门陷多重代理多重签名方案[J]. 计算机工程与设计, 2007, 28(21): 5105-5107.

[8] 施华荣. 一种基于椭圆曲线的多重代理多重签名方案[J]. 计算机应用研究, 2008, 25(4): 1142-1146.

[9] 汪秋国, 施华荣, 江 玲. 新的多重代理多重签名方案[J]. 电子科技大学学报, 2008, 37(5): 712-715.

[10] Shao Zuhua. Proxy Signature Schemes Based on Factoring[J]. Information Processing Letter, 2003, 85(3): 137-143.

编辑 张 帆