

# 一种安全的门限代理签名方案

尚光龙,王天芹,谢 倩

(河南大学 数据与知识工程研究所,河南 开封 475004)

**摘 要:**基于离散对数问题和 RSA 公钥密码体制以及安全的单向函数,提出了一个安全的门限代理签名方案。新方案引入授权文书和时间证书等概念,克服了代理人滥用权力的缺陷,使代理人只能在特定时间内进行次数一定的代理签名;对每个参与者,分配了验证片段,高效解决了参与者的欺诈问题,有效克服了伪造签名攻击和合谋攻击,提高了签名的安全性。分析表明,新方案提高了门限代理签名的安全性,是一个安全可行的具有理论和应用价值的门限代理签名方案。

**关键词:**离散对数问题;RSA 公钥密码体制;门限代理签名

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2008)05-0147-03

## A Secure Threshold Proxy Signature Scheme

SHANG Guang-long, WANG Tian-qin, XIE Qian

(Institute of Data and Knowledge Engineering, Henan University, Kaifeng 475004, China)

**Abstract:** Based on the security of the discrete logarithmic problem, the RSA public-key cryptosystem and the one-way function, proposed a new security enhanced method of a threshold proxy signature scheme. The scheme has the ability for the original signer to control the power of the proxy digital signature by introduction the concepts of authorization-writ and time-certification; To resist the cheat between each participants, the scheme introduces the concept of verifying-share and successfully resists the attacking of circumvention and frame, improves the security of the signature. Analysis shows that it's a feasible and secure threshold proxy signature which has theory and application value.

**Key words:** discrete logarithmic problem; RSA public-key cryptosystem; threshold proxy signature

## 0 引 言

1996年, Mambo, Usuda 和 Okamoto 首先提出了代理签名的概念<sup>[1,2]</sup>, 所谓代理签名就是指一个被指定的代理签名者可以代表原始签名者生成有效的签名。

在代理签名方案中引入秘密分存就形成了门限代理签名方案。自1997年 K Zhang 和 Kim 等人第一次分别提出门限代理签名方案以来<sup>[3,4]</sup>, 学术界提出了很多类似的方案, 其中  $n$  份部分代理签名密钥,  $n$  个代理签名人分别拥有各自的代理密钥; 各代理签名人利用自己流行的是  $(t, n)$  门限代理签名方案。 $(t, n)$  门限代理签名方案就是将一个代理签名子密钥分成分存的子代理密钥所签署的签名叫部分代理签名; 当部分代理签名的个数大于或等于  $t$  时, 这些部分代理签名按着某种方式结合, 产生有效的门限代理签名。

2003年 Yang 等人提出了一个效率很高的门限代理签名方案<sup>[5]</sup>, 随即有人提出该方案有很大的缺陷, 即原始签名人可以伪造代理签名; Xu 等人随后提出了一个可以克服这一缺陷的方案<sup>[6]</sup>, 但明显的是, Xu 的方案未能解决门限方案中常见的参与者欺诈问题, 并且未能很好地解决原始授权人对代理人的签名权限的控制问题, 比如对签名时间和次数的控制, 而这些问题在实际应用中是经常遇到的。鉴于此, 文中利用 RSA 公钥密码体制和离散对数及单向函数的安全性, 基于上述方案, 提出了一个新的安全增强的门限代理签名方案, 有效地解决了参与者欺诈和对代理人权限的控制问题, 并有效地克服了合谋攻击。分析表明, 新提方案具有很高的安全性和实用性, 是一个切实可行的方案。

## 1 一种安全增强的门限代理签名方案

### 1.1 方案初始化

(1) 设  $p, q$  为两个大素数且满足  $q \mid (p-1)$ , 计算  $n = pq$  并公开  $n$ , 选择参数  $e$  和  $d$  使得  $\gcd(e, \Phi(n)) = 1$  和  $ed \equiv 1 \pmod{\Phi(n)}$ , 其中  $\Phi(n) = (p-1)(q-1)$ , 公开  $e$  和  $\Phi(n)$  并保密  $d$ ;

收稿日期: 2007-08-16

基金项目: 国家自然科学基金资助项目(10671056)

作者简介: 尚光龙(1979-), 男, 河南南阳人, 硕士研究生, 主要从事密码学与信息安全研究; 王天芹, 副教授, 博士, 主要从事数论与密码学研究。

(2) 设  $g \in Z_p^*$  为阶为  $q$  的本原元,  $H$  为选定的安全单向函数(如 SHA-1)<sup>[7]</sup>。授权人(原始签名人)  $p_0$  的密钥对为  $(x_0, y_0)$ , 其中  $x_0$  为私钥,  $y_0 = g^{x_0} \bmod p$  为公钥; 代理签名人  $p_1, \dots, p_n$  中  $p_i$  的密钥对为  $(x_i, y_i)$ , 其中  $x_i$  为私钥,  $y_i = g^{x_i} \bmod p$  为公钥; 代理签名人  $p_i$  的身份标识记为  $ID_i$ ;

(3) 为克服参与者  $p_i$  之间的欺诈行为, 引入验证片段  $w_i$ 。

## 1.2 签名权力委托过程

当  $p_0$  打算将签名权委托给  $p_i$  时, 执行如下操作:

(1)  $p_0$  生成用于限制  $p_i$  的授权文书  $A_p$ , 其中包括  $p_i$  的身份标识  $ID_i$ 、委托授权的有效期限、 $p_0$  代表  $p_0$  行使数字签名权力的权限范围、 $p_i$  代表  $p_0$  行使数字签名权力的最大签名次数等内容;

(2)  $p_0$  用私钥  $x_0$  签署  $A_p$ , 得到可限制  $p_i$  的签名权限的授权证书  $C_p$ , 并发送给  $p_i$ ;  $p_i$  接收到授权证书  $C_p$  后, 用  $y_0$  解析出  $ID_i$  并与自己的身份标识进行对比, 若正确, 则接受授权, 否则丢弃;

(3)  $p_0$  选择一个随机数  $k \in Z_q$ , 计算  $K = g^k \bmod p$  和代理签名子密钥

$$\sigma = x_0 H(A_p \| K) + k \bmod q$$

(4)  $p_0$  计算  $w_i = H(\sigma)^d \bmod n$  并将  $\sigma$  和  $w_i$  分别作为签名子密钥和验证片段通过秘密信道分配给签名参与者  $p_i$  保管。

至此,  $p_0$  完成了授权  $p_i$  在指定范围内代表  $p_0$  行使数字签名权力的委托过程。

## 1.3 代理签名生成过程

设  $m$  为待签名消息,  $p_1, \dots, p_i$  为实际的代理签名人, DC 是  $p_1, \dots, p_n$  中的特殊成员, 负责把有效的部分代理签名合成为代理签名。

(1) 每个  $p_i$  秘密选择一个随机数  $k_i \in Z_q^*$  并广播  $r_i = g^{k_i} \bmod p$ , 然后  $p_i$  计算

$$R = \prod_{j=1}^i r_j \bmod p$$

(2)  $p_i$  计算部分代理签名  $s_i = k_i R + (t^{-1} \sigma + x_i H(A_p \| K)) H(R \| ID_i \| m) \bmod q$ 。

(3)  $p_i$  生成请求认证文书, 内容包括  $p_i$  的身份标识  $ID_i$ 、部分代理签名  $s_i$  以及请求  $p_0$  对所签署的  $s_i$  进行认证的消息。

(4)  $p_i$  利用私钥  $x_i$  签署请求认证文书, 得到请求认证信息  $M_Q$  并将其发送给  $p_0$  请求认证。

(5)  $p_0$  收到  $p_i$  提交的  $M_Q$  后, 首先用  $y_i$  验证其完整性和真实性, 若有错误, 则拒绝提供认证服务。

(6)  $p_0$  验证由其设定的最大签名次数以及  $p_i$  已经

代表  $p_0$  行使数字签名权力的签名次数。若在委托授权范围内, 则根据收到  $M_Q$  的时间, 对  $M_Q$  中的  $s_i$  签发时间证书  $T_p$ , 同时修改签名次数信息, 并将  $T_p$  发送给  $p_i$ , 此时  $T_p$  表示  $B$  代表  $A$  对消息  $m$  所签署的部分代理签名  $s_i$  的时间证明。

(7)  $p_i$  收到  $T_p$  后, 形成信息  $M = (m, s_i, C_p, T_p)$  并发送给指定的签名合成者 DC。DC 解析出消息  $m$ 、部分代理签名  $s_i$ 、授权证书  $C_p$  和时间证书  $T_p$ , 并用  $p_0$  的公钥  $y_0$  验证  $T_p$  和  $C_p$  的合法性, 若验证无效, 则  $M$  无效; 若  $M$  有效, 则 DC 通过下式来验证  $s_i$  的有效性:

$$g^{s_i} = r_i^R [(Ky_0^{H(A_p \| K)})^{t^{-1}} y_i^{H(A_p \| K)}]^{H(R \| ID_i \| m)} \bmod p$$

部分签名  $s_i$  的正确性证明如下:

由于

$$s_i = k_i R + (t^{-1} \sigma + x_i H(A_p \| K)) H(R \| ID_i \| m) \bmod q$$

得

$$g^{s_i} = g^{k_i R + (t^{-1} \sigma + x_i H(A_p \| K)) H(R \| ID_i \| m) \bmod q} =$$

$$r_i^R [(Ky_0^{H(A_p \| K)})^{t^{-1}} y_i^{H(A_p \| K)}]^{H(R \| ID_i \| m)} \bmod p$$

故部分签名成立。

(8) 如果每个  $s_i$  都通过验证, 则 DC 通过计算  $S =$

$$\sum_{i=1}^i s_i \bmod q \text{ 形成代理签名 } (m, A_p, K, ID_i, R, S)。$$

## 1.4 代理签名验证过程

验证者接收到  $(m, A_p, K, ID_i, R, S)$  后, 首先计

算  $A = K(y_0 \prod_{i=1}^i y_i)^{H(A_p \| K)} \bmod p$ , 然后验证  $g^S = R^R A^{H(R \| ID_i \| m)} \bmod p$  是否成立即可。

验证过程正确性证明如下:

$$g^S = g^{\sum_{i=1}^i s_i} \bmod p =$$

$$g^{\sum_{i=1}^i k_i R + \sum_{i=1}^i [t^{-1} k + t^{-1} x_0 H(A_p \| K) + x_i H(A_p \| K)] H(R \| ID_i \| m)} \bmod p$$

$$= R^R (Ky_0^{H(A_p \| K)})^{\sum_{i=1}^i y_i^{H(A_p \| K)}}^{H(R \| ID_i \| m)} \bmod p =$$

$$R^R A^{H(R \| ID_i \| m)} \bmod p$$

故代理签名成立。

## 2 方案的安全性分析

为了保证代理签名的安全运作, 一个代理签名方案应该满足方案的基本不可伪造性、代理签名的不可伪造性、代理者身份的可追踪性等。据此, 对本方案的安全性分析如下:

(1) 基本的不可伪造性: 由于离散对数问题的难解性,  $p_i$  无法计算出  $p_0$  的签名私钥  $x_0$ , 因此不可能伪造  $p_0$  的普通数字签名, 并且任何其他攻击者都不能生成  $p_0$  的普通数字签名;

(2)代理签名的不可伪造性:因为  $k_i$  是每个  $p_i$  自己秘密选取的,因此除了  $p_i$  外,任何人都不能伪造  $p_i$  的有效部分代理签名;

(3)代理签名的可跟踪性:由于委托过程是将  $p_i$  的身份  $ID_i$  与  $p_0$  绑定在一起的,因此  $p_0$  可以根据某一有效的代理确定代理签名者的身份,实现对代理签名者的事后监督功能;

(4)代理签名者权力的限制:委托过程和签名过程中, $p_0$  和  $p_i$  以及签名合成者 DC 之间的交互,有效保证了授权证书  $C_p$  和时间证书  $T_p$  的安全性,限制了代理签名者  $p_i$  的权力;

(5)参与者  $p_i$  之间的欺诈检测过程:对于参与者  $p_i$ ,根据上述方案,如果  $w_i^e \equiv H(\sigma)(\text{mod } m)$ ,则  $p_i$  为出示了真正子密钥的合法参与者,否则为内部欺诈者或者外部欺诈者,如果欺诈者  $p_i$  改  $\sigma$  为  $\sigma^*$ ,则他必须计算  $w_i^*$ ,使得

$$w_i^{*e} \equiv H(\sigma)(\text{mod } m)$$

才能通过验证,但是他不知道  $d$ ,所以他能够计算出  $w_i^*$  等价于攻破 RSA 公钥密码体制;如果欺诈者  $p_i$  改  $w_i$  为  $w_i^*$ ,则他必须计算  $\sigma^*$ ,使得

$$H(\sigma^*) \equiv w_i^{*e}(\text{mod } m)$$

在单向函数  $H$  具有足够的安全性时,这也是难以实现的。因此,本方案能有效阻止参与者之间的欺诈,更加有效地克服了伪造签名攻击。

(6)抗合谋攻击:假设  $t-1$  个签名代理人与  $p_1, \dots, p_{t-1}$  与  $p_j$  联合,以让  $p_j$  冒充  $p_i$  签名,但是由于离散对数问题的难解性,他们无法求得  $k_j$  而获得  $x_j$ ,因此不能伪造代理签名。假设  $p_1, \dots, p_{t-1}$  与外部攻击者  $p'$  联合进行内外合谋攻击,但由于  $p'$  并未得到  $p_0$  的签名权力委托,故而不能通过合成者 DC 的认可,也就无法完成签名。因此,本方案能抵抗合谋攻击。

(上接第 146 页)

电信等行业有其特定应用,如信用分析、风险分析、欺诈检测等,是数据仓库的主要市场。在未来大规模定制经济环境下,数据仓库将成为企业获得竞争优势的关键武器。数据仓库的发展趋势主要表现在三个方面:对非结构化数据的处理,实现共享数据、对信息进行打包处理<sup>[8]</sup>。

#### 参考文献:

- [1] 史忠植. 知识工程[M]. 北京:清华大学出版社,1988.
- [2] 王 珊,罗 力. 从数据库到数据仓库[R]. 北京:中国人民大学数据与知识工程研究所,1997:26-28.

### 3 结束语

基于离散对数问题和 RSA 公钥密码体制以及单向函数的安全性,文中提出的新方案除了保持所引文献的优点外,引入了授权文书和时间证书等概念,把代理签名者限制在特定时间和特定次数下代表授权人进行代理签名,有效限制了代理人的签名权力;验证片段的引入,有效阻止了参与者之间的欺诈,克服了合谋攻击和伪造签名攻击。分析表明,新方案满足了数字签名中安全、高效的要求,是一个安全可行的方案,具有较好的理论和应用价值。

#### 参考文献:

- [1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]//Proc 3rd ACM Conference on Computer and Communications Security. [s. l.]: ACM Press, 1996:48-57.
- [2] Mambo M, Usuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Trans Fundam, 1996, E79-A (9):1338-1354.
- [3] Zhang K. Threshold proxy signature schemes[C]//Information Security Wority Workshop. Japan: [s. n.], 1997:191-197.
- [4] Kim S J, Park S J, Won D H. Proxy Signatures[C]//revisited. ICICS' 97, LNCS 1334. [s. l.]: Springer - Verlag, 1997: 223-232.
- [5] Yang C Y, Tzeng S F, Hwang M S. On the efficiency of non-repudiable threshold proxy signatures with known signers[J]. The Journal of Systems and Softwares, 2003, 22 (9): 1-8.
- [6] XU Ying, Liu Huan-ping. An improvement of nonrepudiable (t,n) threshold proxy signature scheme with know signers [J]. Natural Sciences Journal of Harbin Normal University, 2006, 22(2):45-47.
- [7] Stinson D R. 密码学原理与实践[M]. 第2版. 冯登国译. 北京:电子工业出版社, 2003.

- [3] 韩客松,王永成. 文本挖掘数据挖掘和知识管理[J]. 情报学报, 2001(1):45-47.
- [4] 陈文伟,邓 苏. 经验数据发现技术[J]. 计算机世界, 1995 (8):28-30.
- [5] 陈文伟. 决策支持系统及其开发[M]. 第2版. 北京:清华大学出版社, 2000.
- [6] 李德毅. 从数据库中发现知识的策略和方法[J]. 计算机 HJ 界报, 1995(3):22-24.
- [7] 陈文伟,邓 苏. 可视化机器学习研究[J]. 国防科技大学学报, 1995(3):10-12.
- [8] 张维群. 数据挖掘研究和应用的现状和前景[J]. 统计与信息论坛, 2004(1):23-25.