基于离散对数的若干新型代理签名方案

祁 明[1] ,L. Harn[2]
(1. 华南理工大学计算机系,广州 510641;2. 美国密苏里洲立大学计算机系)

摘 要: 本文基于离散对数提出了一个新型代理签名方案和一个代理多重签名方案. 新方案满足如下性质:1. 签名收方验证代理签名与验证原始签名的方式相同;2. 签名收方容易区别代理签名和原始签名,即新方案可以对代理签名者的代理签名权和原始签名权进行有效地分离;3. 原始签名人和代理签名人对其签名不可否认;4. 多个合法签名人可将签名权同时委托给某个人实施代理多重签名.

关键词: 代理签名; 离散对数; 网络安全
中图分类号: TN911.2 **文献标识码**: A **文章编号**: 0372-2112 (2000) 11-0114-02

Some New Proxy Signature Schemes Based on Discrete Logarithms

QI Ming[1] ,L. Harn[2]
(1. *Department of Computer, South China University of Technology, Guangzhou* 510641, *China*;
2. *Computer Science Telecommunication Program, University of Missouri-Kansas City, USA*)

Abstract: A new proxy signature scheme and a proxy multisignature scheme are proposed based on discrete logarithms. These new schemes satisfy following properties:1. the signature receiver is able to verify the proxy signature in similar way to the verification of the original signature. 2. the proxy signature must be distinguishable from the original signature, that is, new schemes can separate proxy signature right from original signature right. 3. the signature schemes are nonrepudiable; in other words, neither the proxy signer nor original signer can deny their signatures. 4. many signers can delegate their signature rights to a certain pepole, so that proxy multisignature can be signed.

Key words: proxy signature; discrete logarithms; network security

1 引言

最近,一种称为代理签名的新型签名方案被提出[1],由于这种签名机制在许多领域都有重要的应用,因此引起了人们的极大兴趣[2~4]. 代理签名的目的是当某签名人(这里称为原始签名人)因公务或身体健康等原因不能行使签名权力时,将签名权委派给其他人替自己行使签名权. 目前已出台的一些代理签名方案仍存在以下问题:

(1) 代理签名方案在验证方程中仅含代理签名者的公钥,从而实际签名权和代理签名权没有实现有效地分离.

(2) 目前授权方程的建立都是采用交互式传递数据的方法,而且不包含代理签名者的身份码. 因此,授权方程的建立既烦琐,又使签名收方不易验证代理签名人的真实性.

(3) 对代理签名而言,如何实现一个人同时受多人之托,进行代理多重签名的问题至今未见研究结果出台.

针对以上三点,本文建立了一个新型代理签名方案和一个代理多重签名方案,解决了上述存在的问题.

2 代理签名方案的基本要求

在一个代理签名方案中,如果假设 A 委托 B 进行代理签名,则此签名方案应满足以下三个最基本的条件:

- 签名收方能够象验证 A 的签名那样验证 B 的签名
- A 的签名和 B 的签名应当完全不同,并且容易区分
- A 和 B 对签名事实不可否认

尽管目前所建立的许多代理签名方案存在各种问题,但基本上都满足上述的基本条件. 由于篇幅所限,本文对已有方案不做介绍.

3 新型代理签名方案

安全参数: P 为大素数, $g \in GF(p)$ 为本原元, f 是单向函数,原始签名人 A 的公钥为 $y_A = g^{x_A} \bmod p$,代理签名人 B 的公钥为 $y_B = g^{x_B} \bmod p$, $x_B \in (1, p-1)$ 且 $(x_B, p-1) = 1$.

授权方程:当 A 打算将签名权委托给 B 时, A 选取随机数 $k \in (1, p-1)$ 并利用 B 的身份码 ID_B 计算 $r = g^k \bmod p$ 和 $s' = rx_A + ID_B k \bmod q$,然后将 (ID_B, r, s') 送 B. B 收到 (ID_B, r, s') 后,先验证 $g^{s'} = y_A^r r^{ID_B} \bmod p$,以确认受委托数据源的可靠性. 确认数据可靠性之后 B 再做如下计算: $s = s' x_B^{-1} \bmod q$,则 (ID_B, r, s) 满足 $y_B^s = y_A^r r^{ID_B} \bmod p$. 上式成立的原因是: $g^{s'} = g^{s' x_B x_B^{-1}} = (g^{x_B})^{s' x_B^{-1}} = y_B^s \bmod p$. 在这里, $y_B^s = y_A^r r^{ID_B} \bmod p$ 被视

收稿日期:1999-10-19;修回日期:2000-06-10
基金项目:广东省自然科学基金(No. 970453)

为授权方程,它建立了 A 和 B 两者公钥之间的内在联系,而这种联系只有在 A 同意转让自己的权力时才可建立. 其中 B 的签名密钥 s 只有 B 自己知道,其他人包括 A 也无法知道.

代理签名:B 利用签名密钥 s(严格地说是利用代理签名密钥)的签名过程是参照文[5]中隐式签名的技巧. 具体签名方法如下:设 m 为待签名消息,f 为单向函数. B 计算 $u = y_B^t \bmod p$ 及 $v = t + sf(m, A) \bmod q$,其中参数 $t \in (1, p-1)$ 为随机数,签名数据为 $c_{A,B} = (m, r, u, v)$.

签名验收:收方收到 $c_{A,B} = (m, r, u, v)$ 后,利用原始签名人 A 和代理签名人 B 的公钥计算:$u' = y_B^v [(y_A^r r^{ID_B})^{-1}]^{f(u,m)} \bmod p$,若 $u' = u$ 成立,则收方接受 B 关于信息 m 的代理签名. 易证明,如果 B 是合法代理人,则上述 $u' = u$ 必定成立,因为

$$\begin{aligned} u' &= y_B^v [(y_A^r r^{ID_B})^{-1}]^{f(u,m)} \bmod p \\ &= y_B^v [(y_B^s)^{-1}]^{f(u,m)} \bmod p \\ &= y_B^{t+sf(u,m)} y_B^{-sf(u,m)} \bmod p = y_B^t \bmod p = u \end{aligned}$$

尽管签名收方在验证签名时同时使用了两种公钥,可以明确原始签名和代理签名的关系,但当收方仍不放心 B 是否是真正的代理人时,可再采用如下交互式方法确认 B 是否知道授权方程 $y_B^s = y_A^r r^{ID_B} \bmod p$ 中的 s:

B $\xrightarrow{(r, y_B, ID_B)}$ 收方

$\xrightarrow{w = y_B^v}$ 选 $v \in (1, p-1)$ 且 $(v, p^{-1}) = 1$

$\xrightarrow{z = w^s}$ $z^{v^{-1}} \stackrel{?}{=} y_A^r r^{ID_B} \bmod p$

签名收方可以确定代理签名人的合法身份及签名的有效性.

性能分析:由于现有的代理签名方案在验证方程中仅含代理签名者的公钥,使得签名收方不易理解所收到的签名究竟是某人自己的真实签名,还是受人之托的代理签名. 新方案克服了这一缺点,因为签名协议使得签名收方在验证时必须同时使用原签名人和代理签名人的公钥,即实际签名权和代理签名权实现了有效地分离.

验证一个代理签名人是否具有签名权,主要是依靠原始签名人和代理签名人之间所建立的授权方程,而目前授权方程的建立都是采用交互式传递数据的方法,而且不包含代理者的身份码. 新方案对此进行了改进,授权方程包含代理签名人的身份码,而且在建立授权方程时,原签名人只需将有关数据直接传给自己所选定的代理人即可,这与人们日常委托他人办事的习惯十分相符.

在确认签名有效性方面,新方案使签名收方可根据实际情况实施一次或两次验证,实现了双重安全保护机制.

原始签名人 A 在给 B 授权时,可将关于 B 的身份码 ID_B 的签名 (ID_B, r, s') 公开地送给 B. 如果除了 B 之外还有 G 通过某种渠道也获得了 (ID_B, r, s'),当 G 想冒充 B 当代理签名人时,G 可能会计算 $s = s' x_G^{-1} \bmod q$,这时得到的授权方程是 $y_G^s = y_A^r r^{ID_B} \bmod p$,而不是 $y_B^s = y_A^r r^{ID_B} \bmod p$. G 若想将授权方程中的 ID_B 改成 ID_G 以得到合法的授权方程时,则会碰到求离散对数的难题. 因此上述方案可抗击假冒代理人事件的发生.

4　代理多重签名方案

多重签名的技术的研究,出现了一些安全且实用的方案[6]. 对于代理签名而言,当多个原始签名人将自己的签名权同时委托给 B 实施代理多重签名的方案目前还未出现. 下面采用类似于上述 3 中的方法构造了实现代理多重签名的方案. 有关安全参数的选取与 3 相同,这里不再赘述.

设 $A_i (i = 1, 2, \cdots, n)$ 是若干原始签名人,每个人的密钥、公钥和秘密参数为 (x_i, y_i, k_i) $(i = 1, 2, \cdots, n)$. 其授权和签名过程如下:

·每个 A_i 计算 $r_i = g^k \bmod p$,并将 r_i 在所有 A_i 中公开,从而每个 A_i 可计算 $r = \prod_{i=1}^{n} r_i \bmod p$,因此 A_i 可计算 $s_i' = rk_i + ID_B x_i \bmod q (i = 1, 2, \cdots, n)$.

·A_i 将 (ID_B, r_i, s_i') 送 $B (i = 1, 2, \cdots, n)$.

·B 将 s_i' 采用 $s_i = s_i' x_B^{-1} \bmod q$ 变成 s_i 得 (ID_B, r_i, s_i),它满足方程 $y_B^s = r_i^r y_i^{ID_B} \bmod p (i = 1, 2, \cdots, n)$.

令 $s = \sum_{i=1}^{n} s_i \bmod q$,$y_G = \prod_{i=1}^{n} y_i \bmod p$($y_G$ 被看成 n 个原始签名人的群公钥),则代理签名的授权方程为 $y_B^s = r^r y_G^{ID_B} \bmod p$,其中 $s = \sum_{i=1}^{n} s_i \bmod q$ 为 B 的代理多重签名密钥.

既然 s 已经获得,其余的签名和验证过程与上述 3 中的方案相同.

5　结束语

代理签名是近年来出现的一种新型签名技术,它的应用非常广泛,如电子商务中 CA 证书的签发,电子支票或电子货币的分发等都涉及代理签名问题. 尽管本文和其它文章建立了一些代理签名的研究结果,但仍有以下问题需要进一步研究和解决:

①如何解决签名权不断转移的"多重代理签名问题"?

②如何利用盲签名、定向签名、零知识签名等特殊签名方案实现代理签名?

参考文献:

[1] M. Mambo, K. Usuda and E. Okamoto. Proxy signitures for delegating signing [A]. In Proc. 3rd ACM Conference on Computer and Communications Security [C], 1996.

[2] K. Zhang. Threshold proxy signature scheme [A]. 1997 Information Security Workshop, Japan, 1977: 101 - 109.

[3] K. Zhang, Nonrepudiable proxy signature scheme [A]. In Proceeding of ACISP '97 [C], 1997: 237 - 239.

[4] N. Lee, T. Hwang and C. Wang. On zhang's nonrepudiable proxy signature scheme [A]. In Proceeding of ACISP '98 [C], 1998: 415 - 422.

[5] 祁明,肖国镇. 加强广义 ElGamal 签名方案的安全性 [J]. 电子学报, 1996, 24(11): 68 - 74.

[6] 祁明,肖国镇. 具有特殊次序的多重签名方案 [J]. 计算机工程, 1997, 23(6): 22 - 24.

作者简介:

祁　明　博士,华南理工大学电子商务学院常务副院长,主要研究信息安全与保密技术.

L. Harn　博士,美国密苏里洲立大学计算机系教授,主要研究密码学及其应用.