代理多重签名:一类新的代理签名方案

伊丽江[1,2,3],白国强[1],肖国镇[1]
(1. 西安电子科技大学综合业务网国家重点实验室,信息安全保密研究所,西安 710071;
2. 山西师范大学数学与计算机系,山西临汾 041000;3. 深圳市中兴通讯股份有限公司,深圳 518004)

摘 要: 在代理签名方案中,代理签名人可以代表原始签名人生成签名. 然而,在已知的各种代理签名方案中,代理签名人生成的每个代理签名都只代表一个原始签名人. 在有些情形,需要一个代理签名能够同时代表多个原始签名人,而已知的代理签名方案都不能满足这个需要. 本文给出一类称为代理多重签名的新代理签名方案. 在这种新方案中,一个代理签名人可以同时代表多个原始签名人在文件上签名.

关键词: 数字签名; 代理签名; 多重签名
中图分类号: TN918.4 **文献标识码**: A **文章编号**: 0372-2112 (2001) 04-0569-02

Proxy Multi-Signature: A New Type of Proxy Signature Schemes

YI Li-jiang[1,2], BAI Guo-qiang[1], XIAO Guo-zhen[1]
(1. *ISN, Information Security and Privacy Instiute, Xidian University, Xi'an* 710071, *China*;
2. *Dept. of Mathematics & Computer, Shan Xi Normal University, Linfen* 041000, *China*)

Abstract: Proxy signature schemes allow a proxy signer to generate a proxy signature on behalf of an original signer. However, since in previous proxy signature schemes a proxy signature is created on behalf of only one original signer, we call these schemes proxy mono-signature schemes. This paper presents a new type of proxy signature schemes called proxy multi-signature schemes in which a proxy signer can generate a proxy signature on behalf of two of more original signers.

Key words: digital signature; proxy signature; multi-signature

1 引言

在现实世界里,人们经常需要将自己的某些权力委托给可靠的代理人,让代理人代表本人去行使这些权利. 在这些可以委托给他人的权力中包括人们的签名权. 例如,某公司的经理需要到外地出差. 为了不影响公司的业务,该经理可以委托一个可靠的助手,让该助手在他出差期间代表他在一些重要文件上签字. 委托签名权力的传统方法是使用印章,因为印章可以在人们之间灵活地传递.

在电子化的信息社会,同样会遇到委托签名权力的问题. 文[1]中提出的代理签名方案给出了解决这个问题的一种方法. 在一个代理签名方案中,一个被指定的代理签名人可以代表原始签名人生成有效的代理签名. 代理签名至少需要满足以下性质:

●不可伪造性. 即除了原始签名人和代理签名人之外,任何其他没有被指定为代理签名人的人都无法伪造一个代表原始签名人的代理签名.

●可验证性. 任何验证签名的人都可以验证代理签名是否有效,并且根据有效的代理签名可以确认原始签名人承认被签名的文件.

目前,人们已经提出了若干不同类型的代理签名方案[1,2]. 但是这些方案中,一个代理签名只能代表一个原始签名人,所以可称这些代理签名为代理单重签名(Proxy mono-signature). 有时,人们需要让一个代理签名能够同时代表多个原始签名人. 例如,如果一个公司将要发布一个涉及到财务部门,工程部门以及行政管理部门的文件. 该文件必须由这些部门联合签名才有效,或者这些部门也可以委托它们都信任的一个代理人同时代替它们在该文件上签字. 对于前一种情况,可以用多重签名方案[3]解决. 而对于后一种情况,即多个部门同时委托一个代理人在一个文件上签名,还没有现成的方案来实现.

本文针对以上问题,提出了一类新的代理签名方案,称之为代理多重签名(Proxy Multi-Signature). 在一个代理多重签名方案中,一个代理签名人可以同时代表多个原始签名人的利益在一个文件上签字.

2 两个代理多重签名方案

设 P 是一个大素数,$2^{511} < P < 2^{512}$,g 是 Z_p^* 的一个生成元.

令 $A_1, \cdots, A_n$ 是 n 个原始签名人. 他们联合请求一个代理

收稿日期:1999-12-27;修回日期:2000-07-18
基金项目:电科院国防预研"九五"重点项目(No. 31.2.1.3);国家重点基础研究发展规划项目(No. G1999035804)

签名人 Bob 代表他们在一个文件 m 上签名. 对任意 $1 \le \forall i \le n$, A_i 有一个公开密钥 V_i 和一个秘密密钥 S_i, 使得 $S_i \in_R Z_{p-1} \setminus \{0\}$, $v_i = g^{s_i} \bmod p$.

2.1 代理多重签名方案 Ⅰ

(1) 子代理密钥的生成: 对任意 $1 \le \forall i \le n$, A_i 随机选择 $k_i \in_R Z_{p-1} \setminus \{0\}$, 计算出 $K_i = g^k \bmod p$ 和 $\sigma_i = S_i + k_i K_i \bmod p - 1$.

(2) 子代理密钥的发送: 对任意 $1 \le \forall i \le n$, A_i 将 (σ_i, K_i) 作为子密钥通过安全信道交给 B.

(3) 子代理密钥的验证: 对任意 $1 \le \forall i \le n$, B 验证等式 $g^{\sigma_i} = V_i K_i^{K_i} \bmod p$ 是否成立. 如果成立, (σ_i, K_i) 就是一个有效的子代理密钥. 否则他拒绝接受这个密钥而请求 A_i 重新发送一个有效的子代理密钥, 或者他终止协议.

(4) 代理密钥的生成: 如果 B 确认所有 (σ_i, K_i) $(1 \le \forall i \le n)$ 都是有效的, 那么他计算出的 $\sigma = \sum_{i=1}^{n} \sigma_i k_i \bmod (p-1)$.

(5) 代理签名的生成: 当 Bob 代表所有原始签名人 $A_1, \cdots, A_n$ 在文件 m 上签名时, 他用 σ 作为普通签名运算中的签名秘密密钥来执行普通的签名运算. 于是生成的代理签名是 $(m, Sign_\sigma(m), K_1, \cdots, K_n)$, 其中 $Sign_\sigma(m)$ 表示用签名方法在密钥 σ 下生成的关于消息 m 的签名.

(6) (代理签名的验证) 验证人在验证以上代理签名时首先计算 $v = v_1^{K_1} \cdots v_n^{K_n} K_1^{K_1^2} \cdots K_n^{K_n^2} \bmod p$, 然后用 v 作为一个新的公钥对 $Sign_\sigma(m)$ 进行普通签名的验证.

2.2 代理多重签名方案 Ⅱ

(1) 子代理密钥的生成: 对任意 $1 \le \forall i \le n$, A_i 随机选择 $k_i \in_R Z_{p-1} \setminus \{0\}$ 并计算 $K_i = g^k \bmod p$. 然后他计算出 $e_i = h(m_w, K_i)$, 这里 $h(*)$ 是某个 Hash 函数. 最后 A_i 计算出 $\sigma_i = e_i s_i + k_i \bmod p - 1$.

(2) 子代理密钥的发送: 对任意 $1 \le \forall i \le n$, A_i 将 (σ_i, K_i, m_w) 通过安全信道交给 B.

(3) 子代理密钥的验证: 对 $1 \le \forall i \le n$, B 验证等式 $e_i = h(m_w, K_i)$ 和 $g^{\sigma_i} = v_i^{e_i} K_i \bmod p$ 来确认 (σ_i, K_i, m_w) 的有效性.

(4) 代理密钥的生成: 如果 B 确认了所有 (σ_i, K_i, m_w) $(1 \le \forall i \le n)$ 的有效性, 那么他计算 $\sigma = \sum_{i=1}^{n} \sigma_i e_i K_i \bmod (p-1)$.

(5) 代理签名的生成: 当 B 代表 $A_1, \cdots, A_n$ 在文件 m 上签名时, 他用 σ 作为签名密钥执行普通的签名运算. 最后 $(m, Sign_\sigma(m), K_1, \cdots, K_n, m_w)$ 便是生成的代理签名.

(6) (代理签名的验证) 验证人在验证代理签名时首先计算 $e_i = h(m_w, K_i)$ $(1 \le \forall i \le n)$ 和 $v = v_1^{e_1^2} \cdots v_n^{e_n^2} K_1^{e_1} \cdots K_n^{e_n} \bmod p$. 然后用 v 作为公钥对 $Sign_\sigma(m)$ 执行普通签名的验证运算.

3 安全性分析

以上两个代理签名方案满足以下性质:

性质 1 代理签名人无法根据子代理密钥计算出任何一个原始签名人的秘密密钥 (分析方法与文[1]同).

性质 2 任何人可以验证代理多重签名的有效性. 在方案 Ⅰ中, 有

$$v = v_1^{K_1} \cdots v_n^{K_n} K_1^{K_1^2} \cdots K_n^{K_n^2} \bmod p = g^{s_1 K_1 + \cdots + s_n K_n + k_1 K_1^2 + \cdots + k_n k_n^2} \bmod p = g^{\sigma_1 K_1 + \cdots + \sigma_n K_n} \bmod p = g^{\sigma} \bmod p$$

在方案 Ⅱ中, 有

$$v = v_1^{e_1^2} \cdots v_n^{e_n^2} K_1^{e_1} \cdots K_n^{e_n} \bmod p = g^{s_1 e_1^2 + \cdots + s_n e_n^2 + k_1 e_1 + \cdots k_n e_n} \bmod p = g^{(s_1 e_1 + k_1) e_1 \cdots + (s_n e_n + k_n) e_n} \bmod p = g^{\sigma} \bmod p$$

于是在这两个方案中, v 都是与 σ 相应的有效的验证公钥.

性质 3 通过有效的代理多重签名, 验证者可以确认每个原始签名人对被签文件都是承认的. 这是因为, 在验证多重代理签名时, 需要用到每个原始签名人的公钥.

性质 4 在没有得到所有原始签名人的子代理密钥的情况下, 任何人都无法生成一个有效的代理多重签名. 例如, 在方案 Ⅰ中, 如果没有得到所有有效的 $\sigma_i (1 \le i \le n)$, 任何人都无法找到一组 $(\sigma, K_1, \cdots, K_n)$, 使它们满足 $g^{\sigma} = v_1^{K_1} \cdots v_n^{K_n} K_1^{K_1^2} \cdots K_n^{K_n^2} \bmod p$. 这是由离散对数问题的困难性决定的.

4 结论

在本文中, 提出了一类新的代理签名方案. 利用这种代理签名方案, 可以有效地实现由一个代理签名人生成代表多个原始签名人的代理签名的目的. 本文认为, 这种新签名方案在电子商务和网络安全通信方面有广泛的应用前景. 特别地利用该方案可以构造具有良好性质的公平交换协议 (另文), 由于篇幅所限, 在此不详细讨论.

参考文献:

[1] M. Mambo, K. Usuda, and E. Okamot. Proxy signatures: Delegation of the power to sign messages [J]. IEICE Trans. Fundamentals, 1996, E79-A(9): 1338 - 1354.

[2] S. Kim, S. Park and D. Won proxy signatures, revisited [A]. Proc. of I-CICS '97, International Conference on Information and Communications Security [C], LNCE, 1334, 1997: 223 - 232.

[3] K. Ohta and t. Okamoto. A digital multisignature scheme based on the Fiat-Shamir scheme [A]. Advances in Cryptology—ASIACRYTP '91 [C]: . 139 - 148.

作者简介:

伊丽江 博士后, 1966 年 7 月出生于山西省襄汾县. 分别于 1988 年和 1993 年获理学学士和理学硕士学位. 2000 年 12 月获西安电子科技大学博士学位, 现在深圳中兴通讯股份有限公司博士后工作站工作. 研究方向为密码学, 研究兴趣包括: 密码学, 网络安全, 电子商务等. email: lijiangyi@263.net

白国强 博士后, 1963 年 11 月出生于陕西. 1984 年获理学学士学位, 1988 年获理学硕士学位. 2000 年 12 月获西安电子科技大学博士学位, 研究方向为密码学, 现在清华大学微电子学研究所做博士后研究.