矢量空间秘密共享-多重签名方案

许春香,董庆宽,肖国镇
(西安电子科技大学综合业务网国家重点实验室信息保密研究所,陕西西安 710071)

摘 要: 本文把矢量空间秘密共享方案与多重签名方案结合起来,提出了一种新的签名方案,即矢量空间秘密共享 - 多重签名方案,并对该方案的安全性进行了分析. 在该方案中,任何参与者的授权子集能容易地产生群签名,而参与者的非授权子集不可能产生有效的群签名,验证者可通过验证方法验证个体签名和群签名的合法性. 该方案能保证一个参与者的授权子集的群签名不能被其他参与者子集所伪造,而且可以跟踪被怀疑的伪造者并将其曝光. 该方案能抵御各种可能的攻击.

关键词: 矢量空间秘密共享方案; 多重签名; 离散对数; 安全性分析
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2003) 01-0048-03

A Vector Space Secret Sharing-Multisignature Scheme

XU Chun-xiang, DONG Qing-kuan, XIAO Guo-zhen
(Institute of Information Security, ISN, Xidian University, Xi'an, Shannxi 710071, China)

Abstract: A new signature scheme, i.e. a vector space secret sharing-multisignature scheme, is proposed based on vector space secret sharing scheme and multisignature scheme. The security of this scheme is analyzed. In this scheme, the group signature can be easily produced if an authorized subset of participants pool their secret shares and it is impossible for them to generate a group signature if an unauthorized subset of participants pool their secret shares. The validity of the partial signature and the group signature can be verified by means of verification equations. A group signature of authorized subset of participants cannot be impersonated by any other set of participants. Moreover the suspected forgery can be traced and the malicious participants can be caught in this scheme. None of several possible attacks can successfully break this scheme.

Key words: vector space secret sharing scheme; multisignature scheme; discrete logarithm; security analysis

1 引言

随着计算机通信网的蓬勃发展,人们希望通过网络来实现快捷、远距离的通信和交易,数字签名方法因此而产生,并开始应用于电子邮递、电子转帐和办公自动化等系统. 传统的数字签名一般由一个人完成签名过程,但在实际当中,有时需要多个人共同签署一个文件,秘密共享签名方案[1,6,9]和多重签名方案[2,4,8]就可用来实现多人共同签名同一文件的愿望.

为了解决数字签名的可跟踪性及确认签名确实来自一个参与者授权子集这两个问题,必须把秘密共享签名方案和多重签名方案结合起来使用,即构造秘密共享-多重签名方案,到目前为止,所构造的秘密共享-多重签名方案都是基于 Shamir (t, n) 门限签名方案,其中 n 为参与者的数目, t 为门限值. 本文先阐述了矢量空间秘密共享方案,然后在假设有一个值得信赖的中心机构的条件下,把矢量空间秘密共享签名方案与多重签名方案结合起来,提出了一种新的方案,即矢量空间秘密共享-多重签名方案,而 (t, n) 门限-多重签名方案[3]是本方案的一个特例. 最后讨论了其安全性,显示该方案能抵御各种可能的攻击. 在该方案中,任何参与者的授权子集能容易地产生群签名,而参与者的非授权子集不可能产生有效的群签名,验证者可通过验证方法验证个体签名和群签名的合法性. 该方案能保证一个授权子集的群签名不能被其他参与者子集所伪造,而且可以跟踪被怀疑的伪造者并将其曝光.

2 矢量空间秘密共享方案

(t, n) 门限方案表明 n 个参与者中任何 t 个将能够重构秘密 k. 更一般的情况是规定参与者的哪些子集能够确定秘密 k,而哪些子集不能确定秘密 k. 设 $P = \{p_1, p_2, \cdots, p_n\}$ 是 n 个参与者的集合, Γ 是 P 的子集的集合,如果在 Γ 中的子集是能够计算秘密 k 的参与者的子集,则称 Γ 为访问结构, Γ 中的子集称为授权子集. Brickell 提出的矢量空间构造[5]是一种针对访问结构构造某些理想方案的方法. $D \in P$ 是可信赖的中心机构. $K = GF(q)$, q 为素数, K^r 表示 K 上所有 r 元构成的矢量空间. 访问结构 Γ 是一个矢量空间访问结构,如果存在函数

收稿日期:2001-03-27;修回日期:2003-08-20
基金项目:国家自然科学基金(No. 60073051);国家 973 项目(No. G1999035804)

$$\psi: P \cup \{D\} \to K^r$$

满足特性

$$\psi(D) = (1,0,\cdots,0) \in \langle \psi(p_i) = (x_{1i}, x_{2i}, \cdots, x_{ri}) : p_i \in A \rangle \Leftrightarrow A \in \Gamma$$

换句话说,矢量 $\psi(D)$ 能表示为集合 $\{\psi(p_i) : p_i \in A\}$ 中的向量的线性组合当且仅当 A 是一个授权子集[5]. 如果 Γ 是这样一个矢量空间访问结构,当对所有 $p \in P$ 有 $S_p = K(S_p$ 表示参与者 p 可能接收到的所有可能子秘密的集合)时,我们能够建立一个理想的秘密共享方案:给定秘密 $k \in K$, D 随机选择 $v_2, \cdots, v_r \in K$,令 $\mathrm{v} = (v_1, v_2, \cdots, v_r)$,其中 $v_1 = k$,显然 $\mathrm{v} \cdot \psi(D) = k$,则分配给第 i 个参与者的子秘密将是 $w_i = \mathrm{v} \cdot \psi(p_i)$,即 $w_i = \sum_{j=1}^{r} v_j x_{ji}$. 函数 ψ 是公开的,授权子集中的参与者利用他们所拥有的子秘密的线性组合计算出秘密 k. 事实上,假设 $A = \{p_1, p_2, \cdots, p_l\}$ 是一个授权子集,则有 $\psi(D) = c_1\psi(p_1) + c_2\psi(p_2) + \cdots + c_l\psi(p_l)$,这里 $c_i \in K$, A 中的参与者能够计算秘密 $k = c_1 w_1 + c_2 w_2 + \cdots + c_l w_l$. 这样构造的方案称为矢量空间秘密共享方案. Shamir 方案即 (t, n) 门限方案是矢量空间秘密共享方案的一个特例,因为只需令 $\psi(p_i) = (1, x_i, x_i^2, \cdots, x_i^{t-1})$,其中 x_i 是 K 中 n 个不同的非零元素[7].

3　矢量空间秘密共享-多重签名方案

假定有一个可信赖的中心机构 D 来分配群体秘密和子秘密.

3.1　群体秘密和子秘密的分配

D 首先选择参数:(1) 一个无碰撞的单向散列函数 H; (2) 素数 p, $2^{511} < p < 2^{512}$; (3) q 是 $p-1$ 的一个素因子, $2^{159} < q < 2^{160}$; (4) $\alpha \equiv h^{(p-1)/q} \bmod p$, $0 < h < p$,且 $h^{(p-1)/q} \bmod p > 1$.

D 选择秘密 k,并随机选择 $v_2, \cdots, v_r \in K$,令 $\mathrm{v} = (v_1, v_2, \cdots, v_r)$,其中 $v_1 = k$,显然有 $\mathrm{v} \cdot \psi(D) = k$,计算 $w_i = \mathrm{v} \cdot \psi(p_i)$, w_i 将用来计算分配给参与者 p_i 的子秘密 u_i. 这里,函数 ψ 是公开的, k、v 以及 w_i 均保持秘密. 假设 $A = \{p_1, p_2, \cdots, p_l\}$ 是一个授权子集,则有 $\psi(D) = c_1\psi(p_1) + c_2\psi(p_2) + \cdots + c_l\psi(p_l)$,这里 $c_i \in K$ 可被任何参与者计算. 此时秘密 $k = c_1 w_1 + c_2 w_2 + \cdots + c_l w_l$. D 计算群体公开密钥 y 和分配给 p_i 的子秘密 u_i 如下:

$$y = \alpha^k \bmod p \quad , \quad u_i = g_i + w_i \bmod q$$

其中 g_i 是一个随机整数且 $0 < g_i < q$. 另外对每一个参与者 p_i, D 还需计算其公开密钥 y_i, z_i:

$$y_i = \alpha^{u_i} \bmod p$$

$$z_i = \alpha^{g_i} \bmod p$$

3.2　参与者个体签名及其验证方法

为了对消息 m 进行群签名,授权子集 $A = \{p_1, p_2, \cdots, p_l\}$ 中的参与者 p_i 随机选择一整数 b_i, $b_i \in [1, q-1]$,并计算公开值 r_i:

$$r_i = \alpha^{b_i} \bmod p$$

每个参与者 p_i, $p_i \in A$,公开 r_i 的值. 一旦有了所有的 r_i, $p_i \in A$ 的值, A 中的每一个参与者 p_i 能计算乘积 R 和散列值 E:

$$R = \prod_{i:p_i \in A} r_i \bmod p \quad , \quad E = H(m, R) \bmod q$$

参与者 p_i 利用他的秘密值 u_i 和 b_i 来计算他的签名 s_i:

$$s_i = c_i \cdot u_i + b_i \cdot E \bmod q$$

A 中的每一个参与者 p_i 将值 $\{m, s_i\}$ 发送给 DC(designated combiner), DC 负责收集和验证每一个个体签名.

DC 利用下式验证 p_i 的签名 $\{m, r_i, s_i\}$:

$$\alpha^{s_i} \stackrel{?}{\equiv} y_i^{c_i \bmod q} \cdot r_i^E \bmod p \qquad (1)$$

若上式成立,则 p_i 的签名 $\{m, r_i, s_i\}$ 有效.

定理 1　若式(1)成立,则 $\{m, r_i, s_i\}$ 是 p_i 的有效签名.

证明　若 $s_i = c_i \cdot u_i + b_i \cdot E \bmod q$,则有

$$\alpha^{s_i} \equiv \alpha^{c_i \cdot u_i \bmod q} \cdot \alpha^{b_i \cdot E \bmod q} \bmod p$$

$$\equiv y_i^{c_i \bmod q} \cdot r_i^E \bmod p$$

因此, $\{m, r_i, s_i\}$ 是 p_i 的有效签名.

3.3　群签名及其验证方法

DC 首先计算:

$$T = \prod_{i:p_i \in A} z_i^{c_i} \bmod p \quad , \quad E = H(m, R) \bmod q$$

授权子集 A 中的每个参与者的签名被验证有效后, DC 计算:

$$S = \sum_{i:p_i \in A} s_i \bmod q$$

这样,验证者可通过下式验证群签名 $\{m, A, R, S\}$:

$$\alpha^S \stackrel{?}{\equiv} y \cdot T \cdot R^E \bmod p \qquad (2)$$

如果上式成立,则群签名 $\{m, A, R, S\}$ 有效.

定理 2　若式(2)成立,则 $\{A, R, S\}$ 是消息 m 的群签名.

证明　因为

$$y \cdot T \cdot R^E \bmod p \equiv T \cdot \alpha^k \cdot R^E \bmod p \equiv T \cdot \alpha_{i:p_i \in A}^{\sum c_i \cdot w_i \bmod q} \cdot R^E \bmod p$$

$$\equiv \alpha_{i:p_i \in A}^{\sum g_i \cdot c_i \bmod q} \cdot \alpha_{i:p_i \in A}^{\sum c_i \cdot w_i \bmod q} \cdot R^E \bmod p$$

$$\equiv \alpha_{i:p_i \in A}^{\sum g_i \cdot C_i + C_i w_i \bmod q} \cdot R^E \bmod p$$

$$\equiv \alpha_{i:p_i \in A}^{\sum c_i \cdot u_i \bmod q} \cdot R^E \bmod P$$

$$\equiv \alpha_{i:p_i \in A}^{\sum c_i \cdot u_i \bmod q} \cdot \alpha_{i:p_i \in A}^{\sum b_i \cdot E \bmod q} \bmod p$$

$$\equiv \alpha_{i:p_i \in A}^{\sum s_i \bmod q} \bmod p \equiv \alpha^S \bmod p$$

故 $\{A, R, S\}$ 是消息 m 的合法群签名.

实际上, (t, n) 门限-多重签名方案[3]是我们提出的方案的特殊情况,因为只需令

$$c_i = \prod_{\substack{j:p_j \in A \\ j \neq i}} \frac{0 - x_j}{x_i - x_j}$$

即可,此时 $|A| = t$.

3.4　安全性分析

根据上面的讨论,我们知道只有授权子集才能产生有效的签名,验证者也很容易验证签名的有效性. 下面我们要讨论这一签名方案的安全性,发现对可能构成威胁的攻击都不能攻破该签名体系.

(1) 从 y 和 y_i 值不能得到群体秘密 k 和子秘密 u_i. 因为要解离散对数问题.

(2) 根据 $s_i = u_i \cdot c_i + b_i \cdot E \bmod q$,不能求得 u_i. 因为对于给定的消息 m,签名方程 $s_i = u_i \cdot c_i + b_i \cdot E \bmod q$ 中有两个未

知数,即 u_i 和 b_i. 如果还有 p_i 对另外一个消息 m 的签名:

$$s_i' = u_i \cdot c_i + b_i' \cdot E' \bmod q$$

这样又增加一个未知数 b_i',可知增加一个方程就增加一个未知数,总之未知数的个数总比方程的个数多出一个. 因此这种攻击不能成功.

(3) 从下面的关系式中不能恢复群体秘密 k:

$$S \equiv \sum_{i:p_i \in A} u_i \cdot c_i + b_i \cdot E \bmod q \equiv k + \sum_{i:p_i \in A} g_i \cdot c_i + \sum_{i:p_i \in A} b_i \cdot E \bmod q$$

因为对于给定的消息 m,上述方程有三个未知数,即 k、$\sum_{i:p_i \in A} g_i \cdot c_i$ 和 $\sum_{i:p_i \in A} b_i$,如果还有对另外一个消息 m 的签名,这样又增加了一个未知数 $\sum_{i:p_i \in A} b_i'$,即每增加一个方程就增加一个未知数,因此未知数的个数总比方程的个数多. 即使授权子集 A 中的参与者联合起来,上述方程也有两个未知数,即 k 和 $\sum_{i:p_i \in A} g_i \cdot c_i$. 增加另外一个授权子集的签名,即增加一个方程,这时又增加一个未知数. 所以,未知数的数目总比方程的数目多. 故这种攻击也不能得逞.

(4) 伪造者不能伪造参与者 p_i 的签名. 假设一个伪造者随机选择一个整数 $b_i' \in [1, q-1]$ 并且公开 $r_i' = \alpha^{b_i'} \bmod p$ 来伪造 p_i 的签名. 乘积值 $R' = \left(\prod_{\substack{j:p_j \in A \\ j \neq i}} r_j\right) r_i' \bmod p$ 由授权子集 A 中的所有参与者共同决定,散列值 $E' = H(m, R')$,在不知道子秘密 u_i 的情况下,很难找到一个合理的值 s_i' 满足

$$\alpha^{s_i'} \equiv y_i^{c \bmod q} \cdot r_i^{E'} \bmod p$$

(5) 一个人不能根据方程 $\alpha^s \equiv y \cdot T \cdot R^E \bmod p$ 伪造一个签名 $\{m, A, R, S\}$. 假设伪造者随机地选择一个整数 R,然后计算散列值 $E = H(m, R) \bmod q$. 显然为了得到整数 S,必须解离散对数问题. 另一方面,如果伪造者随机选择 E 和 S,然后试图确定 R,使其同时满足 $\alpha^s \equiv y \cdot T \cdot R^E \bmod p$ 和方程 $E = H(m, R)$,然而,根据散列函数的性质,这是不可能做到的. 因此这种攻击不能成功.

(6) 参与者集合 P 中的任意多个参与者联合起来不能重构秘密向量 $v = (v_1, v_2, \cdots, v_r)$. 我们知道秘密向量 v 可以根据授权子集中的参与者对应的所有 w_i 来计算. 知道 v 值的任何人能伪造任意子秘密拥有者的签名而不必负任何责任. 因此,在方案中子秘密 u_i 包含了 g_i,而 g_i 值只有可信赖中心机构 D 知道. 一个居心不良的子秘密拥有者 p_i 可以试图从 u_i 中移去 g_i,然而这需要解离散对数问题. 因此,任意多个子秘密拥有者都不能从其子秘密中恢复秘密向量 v,这样就保证了一个参与者的授权子集的群签名不能被任何其他参与者的集合所伪造.

4 结束语

本文在矢量空间秘密共享方案与多重签名方案的基础之上,提出了一新的签名方案,即矢量空间秘密共享-多重签名方案,并对其安全性进行了分析. 在该方案中,群体秘密 k 被分成了 n 个不同的子秘密 $u_1, u_2, \cdots, u_n$,使得任何参与者的授权子集能容易地产生群签名,而参与者的非授权子集不可能产生有效的群签名,且任何人不能从群签名和个体签名中得到群体秘密 k 和子秘密 $u_1, u_2, \cdots, u_n$. 但验证者可通过验证方法验证个体签名和群签名的合法性. 另外,该方案能保证一个授权子集的群签名不能被其他参与者子集所伪造,而且可以跟踪被怀疑的伪造者并将其曝光. 该方案能抵御各种可能的攻击,是一个安全的签名方案.

参考文献:

[1] R Gennaro, S Jarecki, H Krawczyk, T Rabin. Robust threshold DSS signature [A]. Advances in Cryptology-Eurocrypto'96 [C]. Berlin-Heidelberg: Springer-Verlag. 1996. 354 - 371.

[2] K Ohta, T Okamoto. A digital multisignature Scheme based on the Fiat-Shamir scheme [A]. Advances in Cryptology-ASIACRYPT'91 [C]. Fuiyoshida, Japan: Springer-Verlag. 1991. 75 - 79.

[3] Chuan-Ming Li, Tzonelih Hwang, Narn-Yih Lee, Jiun-Jang Tsai. (t, n) threshold-multisignature scheme and generalized-multisignature scheme where suspected forgery implies traceability of adversarial shareholders [J]. Cryptologia. 2000, 24(3): 250 - 268.

[4] T Hardjono, Y Zheng. A practical digital multisignature scheme based on discrete logarithms [A]. Advances in Cryptology-AUSCRYPTO'92 [C]. New York: Springer-Verlag. 1992. 123 - 132.

[5] D R Stinson. Cryptography: Theory and Practice [M]. Florida: CRC Press. 1995: 343 - 350.

[6] Y Desmed, Y Frankel. Shared generation of authenticators and signatures [A]. Advances in Cryptology-Crypto'91 [C]. New York: Springer-Verlag. 1991. 457 - 469.

[7] C Padró, G Sáez. Detection of cheaters in vector space secret sharing schemes [J]. Designs, Codes and Cryptography, 1999, 16(1): 75 - 85.

[8] M Burmester, Y Desmedt, H Doi, M Mambo, E Okamoto, M Tada, Y Yoshifuji. A structured ElGamal-type multisignature scheme [A]. Public Key Cryptography [C]. Victoria, Australia: Springer, 2000. 466 - 483.

[9] R Safavi-Naini, H Wang, K-Y Lam. A new approach to robust threshold RSA signature Schemes [A]. Information Security and Cryptology-ICISC'99 [C]. Seoul, Korea: Springer, 1999. 184 - 196.

作者简介:

许春香 女,1965 年生于湖南宁乡,副教授,博士研究生,主要研究方向为信息安全和密码学. e-mail: chxxu@mail.xidian.edu.cn