矢量空间秘密共享群签名方案

马春波,何大可
(1. 西南交通大学计算机与通信工程学院,四川成都 610031;2. 西南交通大学信息安全与国家计算网格实验室,四川成都 610031)

摘 要: 本文通过引入矢量空间秘密共享技术和阈下通道技术,提出了一种新的群签名方案. 在本签字体制建立后,可以加入或删除成员. 一个部门只有在一定数量成员的参与下,才可以生成有效的群签名. 接收者可以验证签名的有效性,但是不能判断出群签名出自哪一个部门. 当有争端发生时,仲裁者可以"打开"群签名,确定签名的部门. 此签字的公钥长度是独立的."打开"过程通过阈下通道实现.

关键词: 矢量空间秘密共享; 阈下通道; 群签名
中图分类号: TP309. 2 **文献标识码**: A **文章编号**: 0372-2112 (2005) 02-0294-03

Vector Space Secret Sharing Group Signature Scheme

MA Chun-bo, HE Da-ke
(1. *School of Computer and Communications Engineering, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*;
2. *Lab. of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*)

Abstract: Suppose that there are λ departments in a company Ω and any dept. has the right to sign a message on behalf of the company. The group signature made by the dept. should be agreed by the members whose number is over the threshold. The receiver can verify the validity of the signature but can't distinguish which dept. the signature comes from. When the dispute occurs, only the authority can "open" the group signature to distinguish where the signature comes from. Motivated by this consideration, with the combination of vector space secret sharing and subliminal channel technology, a new group signature is presented in this paper. The member can be added or deleted after the scheme founded and the public key length is independent. The "open" process in the presented group signature is realized by subliminal channel.

Key words: vector space secret sharing; subliminal channel; group signature

1 引言

数字签名是认证的重要手段之一,也是现代密码学的主要研究内容之一. 数字签名的主要功能是实现用户对电子形式存放消息的认证. 随着计算机通信网络的发展,数字签名成为了人们在网络上实现快捷、安全的通信和交易的重要手段.

1991 年,Chaum 和 Heyst 首次提出了群签名方案. 在他们的文章中提出了四个实现方案. 在所有的这些方案中,公钥的长度都是和参与者的人数呈线性关系. 文章所提的一些方案还存在别的一些缺陷,比如:在某些方案中,当体制建立后就没有办法增加新的成员;需要"打开"群签名的时候,管理者需要联系所有的成员.

J Camenish 在文献[2]中提出了一种广义群签名方案. 在此方案中,可以方便的加入或删除一个成员. 其缺点是,它的公钥和签名的长度与参与者的人数呈线性关系. 在文献[3]中 J Camenish 和 M Stadler 提出了另外一种群签名方案. 在此方案中,公钥长度和签字的长度都是独立的,并且可以方便的添加和删除成员. 其缺点是它的"打开"的效率非常低. 在此签名中用到了零知识证明技术.

L Chen 和 T Pedersen 在文献[4]中提出了另外两种签名方案. 他们的缺点在于,管理者可能会在某些情况下无法区分签名.

总的来说,群签名应当具有如下特征:

(*a*) 只有组中的成员才能产生有效的群签名.

(*b*) 消息接收者可以验证群签名的有效性,但是不能辨认签名者.

(*c*) 一旦发生争执,仲裁者可以辨别出消息的签名者.

让我们考虑以下问题:假设一个公司 Ω 里有 λ 个部门,每一个部门都可以独立的代表这个公司签字. 只有在一定数量成员的参与下,一个部门才可以生成有效的群签名. 对于接收者来说,它可以验证签名的有效性,但是不能判断出群签名出自哪一个部门. 当有争端发生时,仲裁者可以"打开"群签名,确定签名的部门. 基于此问题,本文通过引入矢量空间秘密共享技术和阈下通道技术,提出了一种新的群签名方案. 在本签字体制建立后,可以加入或删除成员. 此签字的公钥长度是独立的."打开"过程通过阈下通道实现.

2 矢量空间秘密共享

矢量空间秘密共享方法在文献[5]中给出. 对其方法简单描述如下:

收稿日期:2003-10-29;修回日期:2004-08-20
基金项目:西南交通大学博士生创新资金资助

设定 $P \equiv \{p_1, p_2, \cdots, p_n\}$ 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出秘密 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.

矢量空间构造是一种针对访问结构构造某些理想方案的方法. 设 $P \equiv \{p_1, p_2, \cdots, p_n\}$ 是 n 个参与者的集合,Γ 是访问结构,$D \notin P$ 是可信赖的中心机构. $K \equiv GF(q)$,q 为大素数,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 $\phi: P \cup \{D\} \to K^r$ 满足特性:

$$\phi(D) \equiv (1, 0, \cdots, 0) \in \langle \phi(p_i) = (a_{1,i}, a_{2,i}, \cdots, a_{n,i}) : p_i \in A \rangle \Leftrightarrow A \in \Gamma$$

换句话说,矢量 $\phi(D)$ 能表示为集合 $\{\phi(p_i) : p_i \in A\}$ 中的向量的线性组合当且仅当 A 是一个授权子集.

如果 Γ 是这样一个矢量空间访问结构,当对所有 $p \in P$ 有 $S_p \in K(S_p$ 表示参与者 p 可能接收到的所有可能子秘密的集合)时,则能够建立一个理想的秘密共享方案. 给定秘密 $k \in K$,分发者随机选择 $v_2, v_3, \cdots, v_r \in K$,令 $V \equiv (v_1, v_2, \cdots, v_r)$,其中,$v_1 = k$,显然有 $(V, \phi(D)) \equiv k$,则分配给第 i 个参与者的子秘密将是 $w_i \equiv (V, \phi(p_i))$,即 $w_i \equiv \sum_j v_j a_{ji}$. 函数 ϕ 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 $A \equiv \{p_1, p_2, \cdots, p_l\}$ 是一个授权子集,则有 $\phi(D) \equiv c_1\phi(p_1) + c_2\phi(p_2) + \cdots + c_l\phi(p_l)$,这里,$c_i \in K$,$A$ 中的参与者能够计算秘密 $k \equiv c_1 w_1 + c_2 w_2 + \cdots + c_l w_l$. 这样构造的方案称为矢量空间秘密共享方案. 下文中将沿用此处的符号标记.

3　矢量空间秘密共享 —群签名方案

本方案有一个秘密分发者 D 并具有签字功能,可根据参与者提供的 ID,产生相应的签名. 当发生争执时,仲裁者 P 可以确认签名者的身份(ID). 另有 DC(designated combiner_)),负责收集和验证签名. 设 $P \equiv \{p_1, p_2, \cdots, p_n\}$ 是所有的签字者的集合,并有访问结构 $\Omega = \{A_1, A_2, \cdots, A_\lambda\}$,其中,$A_j \subset \Omega$ 是授权子集,$1 \leq j \leq \lambda$.

3.1　初始化

系统具有以下参数:

(1) 两个无碰撞的单项散列函数 H_1, H_2. 其中,H_1 公开,H_2 为 D 和 P 共有的秘密.

(2) 大素数 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 $h^{(p-1)/q} \bmod p > 1$

3.2　群体秘钥和子秘密的产生

D 随机选择秘密 k 和 x 并随机选择 $v_2, v_3, \cdots, v_l \in K$. 令 $V \equiv (v_1, v_2, \cdots, v_l)$,其中,$v_1 \equiv k$. 由以上对矢量空间秘密共享方案的描述,可知:假设 $A_j \equiv \{p_1, p_2, \cdots, p_l\}$ 是一个授权子集,则秘密 $k \equiv c_1 w_1 + c_2 w_2 \cdots c_l w_l$. 这里 $c_i \in K$,可被任何参与者计算. 对 D 来说,k 和向量 V 都应当保密. D 的公钥 y_1, y_2 经如下计算得到:

$$y_1 \equiv \alpha^{k \bmod q} \bmod p \quad y_2 = \alpha^x \bmod p$$

D 除了将子秘密 w_i 分配给参与者 $p_i \in A_j$ 外,还要作如下计算,并公布 η_i, z_i 的值. 其中 $1 \leq i \leq l$

$$u_i = g_i + w_i \bmod q \quad \eta_i = \alpha^{u_i} \bmod p \quad z_i = \alpha^{g_i} \bmod p$$

在这里为 g_i 任意选取的整数,$0 < g_i < q$

3.3　参与者的个体签名的生成及其验证方法

每个参与者 $p_i \in A_j$ 首先通过秘密方式向秘密分发者 D 提交自己的身份信息(ID)并任意选取整数 $b_i \in [1, q-1]$. 计算值 r_i,并公布 r_i 和 ε_i:

$$r_i \equiv \alpha^{b_i \bmod q} \bmod p \quad \varepsilon_i = \alpha^{ID_i} \bmod q$$

对于授权子集 $A_j = \{p_1, p_2, \cdots, p_l\}$,如果每一个参与者都公布了 r 的值,参与者 p_i 可产生单向函数值 E:

$$R \equiv \prod_{i \in A} r_i = \alpha^{\sum_{i \in A} b_i \bmod q} \bmod p$$

$$E \equiv H_1(m, R) \bmod q$$

D 根据参与者 p_i 提交的 ID_i,进行如下计算,并产生对 ID 的签名 $s_{i,2}$:

$$Q_i \equiv H_2(r_i) \bmod q, \quad s_{i,2} \equiv Q_i ID_i + xe \bmod q$$

D 将 $s_{i,2}$ 通过安全信道送给 p_i,并公布 $e_i \equiv (\varepsilon_i)^{Q_i} \bmod q$ 的值. 然后,参与者 p_i 利用他的秘密值 b_i、u_i 来计算他的签名:

$$s_{i,1} = c_i u_i + b_i E e_i \bmod q$$

每一个参与者 p_i 把值 $\{m, s_{i,1}, s_{i,2}, r_i\}$ 发送给 DC(designated combiner_),DC 负责收集和验证每一个签名. DC 利用下式进行签名验证:

$$\alpha^{s_{i,1}} \stackrel{?}{\equiv} (\eta_i)^{c_i \bmod q} (r_i^E)^{\alpha^{s_{i,2}} y_2^{-e_i} \bmod q} \bmod p \qquad (1)$$

定理 1　如果式(1)成立,则 p_i 的签名有效

证明:

$$\alpha^{s_{i,1}} \equiv \alpha^{c_i u_i \bmod q} \alpha^{b_i E e_i \bmod q} \bmod p$$

$$\equiv (\eta_i)^{c_i \bmod q} r_i^{E \alpha^{Q_i ID_i} \bmod p} \bmod p$$

$$\equiv (\eta_i)^{c_i \bmod q} (r_i^E)^{\alpha^{s_{i,2}} y_2^{-e_i \bmod q}} \bmod p$$

证毕

3.4　群体签名的产生及验证

当所有的参与者 $p_i \in A_j$ 提交的签名通过验证后,由 DC 计算:

$$S \equiv \sum_{i \in A} s_{i,1} \bmod q$$

由 DC 生成的群体签名为 $\{m, s_{1,2}, s_{2,2}, \cdots, s_{l,2}, r_1, r_2, \cdots, r_l, S\}$. 为了能验证群签名的正确性,DC 做如下计算,并将其值公布:

$$T \equiv \prod_{i \in A} z_i^{c_i \bmod q} \bmod p$$

接收者将通过下式对群签名进行验证:

$$\alpha^S \stackrel{?}{\equiv} y_1 T \prod_{i \in A} r_i^{E \alpha^{s_{i,2}} (y_2)^{-e_i \bmod q}} \bmod p \qquad (2)$$

定理 2　如果等式(2)成立,则群体签名有效.

证明:

$$\alpha^S \equiv \alpha^{\sum_{i \in A} s_{i,1} \bmod q} \bmod q$$

$$\equiv \alpha^{\sum_{i \in A} c_i w_i \bmod q + \sum_{i \in A} c_i g_i \bmod q + \sum_{i \in A} E b_i e_i \bmod q} \bmod p$$

$$\equiv y_1 T \prod_{i \in A} r_i^{E \alpha^{s_{i,2}} (y_2)^{-e_i \bmod q}} \bmod p$$

证毕.

任何授权子集 $A_j \subset \Omega$ 都可以产生有效的群签名,但是 DC 只能检查群签名的有效性,而不能判断签名来自于哪一个

授权子集.

3.5 身份鉴别

在发生争议的时候,鉴别者 P 可通过拥有的密钥 x 及单向函数 H_2"打开"签名中的 $s_{i,2}$部分,进行身份鉴别,从而判断群签名来自于哪一个授权子集.过程如下:

$$Q_i \mathrm{ID}_i \equiv s_{i,2} - xe_i \mod q$$

其中, $Q_i \equiv H_2(r_i) \mod q$.

在身份鉴别中,本文使用了阈下通道技术.阈下通道技术就是在签字中嵌入额外的一些信息,使得非授权消息接收者只能对签字的正确性进行鉴别,而授权的接收者不但可以对签名进行辨别,还能通过阈下通道得到附加的信息.

本文中,消息接收者 DC 只能对签名进行鉴别,而 P 因为拥有密钥 x 及单向函数 H_2,可以从阈下信道中得到附加的信息,即身份识别码(ID).对于阈下信道,文献[6]进行了较详细的介绍,文献[7]则给出了一个宽带的阈下信道方案.

4 安全性分析

(a)从 y_1, y_2 和 z_i 处得不到 k、x 和 g_i.得到它们的难度等同于求解离散对数的难度.

(b)只有授权子集内的成员可以生成有效的群签名.D 为每一个组内成员 p_i 分配了一个子秘密 w_i.由群签名鉴别式 $\alpha^{\delta} \stackrel{?}{\equiv} y_1 T \prod_{i \in A} \beta_i^{\delta_{i,2}(y_2)^{-e} \bmod q} \bmod p$ 看出, y_1 是由所有的正确的子秘密生成.它可以挫败任何来自授权子集外的假冒攻击.

(c)消息接收者可以验证群签名的有效性,但是不能辨别签名者.消息接收者可以通过(1)式对签名者提供的签名进行鉴别,但是不能分辨签名者.对接收者来说,等式 $s_{i,1} \equiv c_i u_i + b_i E e_i \mod q$ 或 $s_{i,2} \equiv Q_i \mathrm{ID}_i + xe_i \mod q$ 中至少有两个未知数.如果他要攻击 r_i 或 e_i,其难度相当于求解离散对数的难度.

(d)一旦发生争论,从 P 处可以对签名进行身份鉴别.在每一个参与者 p_i 所提交的签名中,等式 $s_{i,2} \equiv Q_i \mathrm{ID}_i + xe_i \mod$ 中的 x 为 P 的密钥,因而, P 可以"打开" $s_{i,2}$,获得关于 ID_i 的知识.此签名方案中,应用了阈下通道的概念.通过 $s_{i,2} \equiv Q_i \mathrm{ID}_i + xe_i \mod q$ 构建了一条阈下通道,传递了消息 ID_i.

(e)授权子集内的参与者任意多个联合都不能重构秘密向量 $V \equiv (v_1, v_2, \cdots, v_l)$.我们知道秘密向量 V 可以根据授权子集中的参与者对应所有的 w_i 来计算.在方案中子秘密 u_i 包含了 g_i,而 g_i 的值只有可信赖的秘密分发中心 D 知道.因此任何 p_i 要从 u_i 中求得 w_i 的难度,等同于求解离散对数的难度.

(f)伪造者不能伪造参与者的签名.假设伪造者随机选择一个整数 $b_i' \in [1, q-1]$,并公开 $r_i' \equiv \alpha^{b_i'} \bmod p$ 来伪造 p_i 的签名.在不知道 k 和 u_i 的情况下,很难找到一个合适的值 $s_{i,1}'$,使它满足:

$$\alpha^{s_{i,1}'} \equiv (\eta)^{c_i \bmod q} (r_i^E) \alpha^{\delta_{i,2} y_2^{-e_i} \bmod q} \mod p$$

(g)授权子集内的参与者任意多个联合,都不能通过 $s_{i,2} \equiv Q_i \mathrm{ID}_i + xe_i \mod q$ 得到秘密 x 和秘密 Q_i.对任何人数的参与者的联合,方程中的未知数始终比人数多.另外,由于 H_2 属于 D 和 P 的秘密,因此,根据单向函数的性质,除 D 和 P 之外的任何人,都不可能通过 $r_i = \alpha^{b_i \bmod q} \bmod p$ 得到 Q_i 得值.

5 结论

本文将矢量空间秘密共享、阈下通道技术及多重签名方案结合在一起,提出了一种新的群签名方案.实现了只有组中的成员才能产生有效的群签名;消息接收者可以验证群签名的有效性,但是不能辨认签名者;一旦发生争执,从消息的群签名权威可以辨认签名者等要求.通过安全性分析,可以看出,本方案是一个安全的签名方案.

参考文献:

[1] CHAUM D, HEYST V E. Group signatures[A]. Processdings of EUROCRYPT'91. Lecture Notes in Computer Science[C]. Berlin: Springer Verlag, 1991. 547: 257 - 265.

[2] CAMENISH J, STADLER M. Efficient group signatures for large groups[A]. Proceedings of CRYPTO'97, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1997. 1296: 410 - 424.

[3] CAMENISH J, STADLER M. A group signature scheme with improved efficiency[A]. Proceedings of ASIACRYPT'98, Lecture Notes in Comrputer Science[C]. Berlin: Springer-Verlag, 1998. 1541: 160 - 174.

[4] CHEN L, PEDERSEN T. New group signature schemes[A]. Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1995. 950: 171 - 181.

[5] PADRO C, SAEZ G. Detection of cheaters in vector space secret sharing schemes[J]. Desings, codes and Cryptography, 1999, 16(1): 75 - 85.

[6] SIMMONS G J. The history of subliminal channels[J]. IEEE Jour. On sel. Areas Comm, 1998, 16(4): 452 - 462.

[7] HARN L, GONG G. Digital signature with a subliminal channels[J]. IEE Proc-Compute Digit Tech, 1997, 144(6): 387 - 389.

作者简介:

马春波 男,1997 年毕业于山东理工大学机械制造专业,获学士学位. 2000 年获桂林电子工业学院自动化专业硕士学位,2002 年起在西南交通大学计算机与通信工程学院攻读博士学位,主要研究领域:密码学,移动通信系统安全,信息系统安全工程. E-mail: cbma@263.net.

何大可 男,西南交通大学计算机安全与通信保密研究所(CSCSI)所长,现任国家高性能计算中心(成都)主任,信息安全与国家计算网格实验室主任,博士生导师,主要研究领域:密码学,移动通信系统安全,信息系统安全工程,并行计算,应用数学.