基于多部秘密共享的存在特权集的门限群签名方案

王天芹
(华北水利水电学院信息工程系 郑州 450011)

摘 要 (t,n)门限群签名是指任意t或更多成员合作生成代表群的有效签名。多部秘密共享是指针对特殊的访问结构实现秘密共享。通过引入多部秘密共享技术,提出一种存在特权集的门限群签名方案。在该方案中,任意成员只需保存一个秘密密钥碎片信息,只有满足条件的成员共同参与才能生成有效的群签名,部分成员合谋不能获得关于群秘密密钥的任何信息。该方案具有"特权集"与"门限"特性、秘密共享的"理想"性、签名的不可伪造性、验证的匿名性与身份的可追查性等良好特性。

关键词 门限群签名,多部秘密共享,多部访问结构,理想秘密共享方案
中图法分类号 TP309 **文献标识码** A

Threshold Group Signature Scheme with Privilege Subsets Based on Multipartite Secret Sharing

WANG Tian-qin
(Department of Information Engineering, North China University of Water Resources and Electric Power, Zhengzhou 450011, China)

Abstract (t,n) threshold group signature scheme enables t out of n signers to sign messages on behalf of the group. Multipartite access structure can be realized by multipartite secret sharing schemes. Based on multipartite secret sharing, this paper presented a threshold group signature scheme with privilege subsets, where each participant shares a single piece of the secret. A valid signature can only be generated under the cooperation of an authorized set. Every unauthorized set can learn nothing about the secret from their shares. Morever, it has the properties of anonymity and traceability.

Keywords Threshold group signature, Multipartite secret sharing, Multipartite access structure, Ideal secret sharing scheme

1 引言与记号

(t,n)门限群签名是指任意t或更多成员合作生成代表群的有效签名。自1991年由Desmedt和Frankel[1]提出以来,门限群签名得到了广泛的研究及应用。在一般的群签名方案中,不管是基于离散对数的[2]或者基于RSA的[3]、不需要可信中心参与的[4]或者需要可信中心参与的[5],各签名者的权限都是相同的,但实际应用中有不同的情形存在[6,7]。文献[6]给出了解决各签名成员权限不相等问题的"存在特权集的门限群签名方案"。在此方案中,分配中心采用"双重"Shamir秘密共享方案在各普通成员之间及各特权成员之间分配秘密密钥碎片,每个特权用户需要保存多个秘密密钥碎片,因此不是理想方案(信息率$\rho\leqslant 1/2$)。

本文借鉴"多部秘密共享"的思想[8],提出一种新的存在特权集的群签名方案(我们这里只考虑存在一个特权集合的情形)。一方面,本方案中所有成员只需保存一个秘密密钥碎片信息,秘密共享的信息率为1,是一个理想方案;另一方面,对于随机选取的系统参数,当基域的阶足够大时,可以保证方案的完善性。

为叙述方便,首先给出本文中所使用的符号与记号:

- $\mathbb{F}$:有限域$GF(p)$,p为大素数;
- $\mathbb{Z}_p$:集合$\{0,1,\cdots,p-1\}$;
- $\mathbb{Z}_q^*$:集合$\{1,2,\cdots,q-1\}$,q为素数。

协议中涉及的主体如下:

- KAC:可信中心,负责系统参数选取及全局密钥的产生与分配;
- SC:签名服务机构,负责单签名的验证及群签名的产生;
- G:n个成员$U_1,U_2,\cdots,U_n$组成的群体;
- V:群签名的验证者。

2 预备知识

(1) 有限域中多项式的零点个数

在本文定理的证明过程中,需要下面关于有限域中多变量多项式零点个数上限的结论。

引理1 设$G(x_1,\cdots,x_k)$是阶为p的有限域$\mathbb{F}$中的非零多项式。假定$\max\{\deg x_i: i=1,\cdots,k\}\leqslant d$,则$G$在$\mathbb{F}^k$中的零点个数$\leqslant kdp^{k-1}$。

(2) 多部访问结构

设U是n个成员的集合,Γ是U的子集的集合,如果在Γ

到稿日期:2010-04-12 返修日期:2010-07-11 本文受国家自然科学基金(素数论若干问题及应用 No. 10671056)资助。
王天芹(1968-),女,博士,教授,主要研究方向为数论、密码学与信息安全,E-mail:wangtq@amss.ac.cn。

中的子集是能够计算出共享秘密的成员子集，则称 Γ 为访问结构。Γ 中的子集称为授权子集，不属于 Γ 的子集称为非授权子集。

将 n 个成员的集合 $U=\{u_1,\cdots,u_n\}$ 划分为 m 个互不相交的子集，即

$$U=\bigcup_{i=1}^{m}C_i \tag{1}$$

对于 U 上的访问结构 Γ，如果 Γ 对于同一个集合 C_i 中的元素不加区分，即 $\forall\pi:U\to U$，s. t. $\pi(C_i)=C_i$，$1\leqslant i\leqslant m$，有

$$V\in\Gamma\Leftrightarrow\pi(V)\in\Gamma$$

则称 Γ 是关于划分(1)的 m-部访问结构。实现访问结构 Γ 的秘密共享方案称为多部秘密共享方案。

(3) 完善秘密共享

一个实现访问结构 Γ 的完善秘密共享方案是在 n 个成员集合中共享一个秘密 S 的方法，它满足下面两条性质：

(a) 任意一个授权子集能够确定 S 的值；

(b) 任意一个非授权子集不能得到有关 S 的任何信息。

(4) 理想秘密共享

对于一个实现访问结构 Γ 的完善秘密共享方案，设秘密密钥集合为 $\mathcal{S}$，密钥碎片集合为 $\mathcal{F}$，成员 u_i 的信息率定义为

$$\rho_i=\frac{\log_2|\mathcal{S}|}{\log_2|\mathcal{F}(u_i)|}$$

其中，$\mathcal{F}(u_i)\subseteq\mathcal{F}$ 表示 u_i 收到的可能密钥碎片的集合。秘密共享方案的信息率定义为

$$\rho=\min\{\rho_i:1\leqslant i\leqslant n\}$$

通常，用信息率来衡量一个秘密共享方案的效率。称 $\rho=1$ 的方案为理想秘密共享方案。

3 存在特权集合的秘密共享方案

设 $U=C_1\cup C_2$，$C_1\cap C_2=\emptyset$，$|C_1|=n_1$，$|C_2|=n-n_1$。考虑访问结构

$$\Gamma=\{V\subseteq U:\exists W\subseteq V,\text{ s. t. }|W\cap C_1|\geqslant t_1\text{ and }|W|=t\} \tag{2}$$

该访问结构对应于特权集为 C_1 的 $(t_1,n_1;t,n)$ 门限访问结构，即只有当 C_1 中至少有 t_1 个成员参与而且参与者总数至少为 t 时才能恢复共享秘密。我们可以构造一个实现该访问结构的理想完善的秘密共享方案。

方案 1　设秘密 $S\in\mathbb{F}$。随机选取 $x_1,x_2\in\mathbb{F}$，$x_1\neq x_2$，两个秘密随机多项式

$$P_1(y)=\sum_{j=0}^{t-1}a_{1,j}y^j\in\mathbb{F}[y]$$

$$P_2(y)=\sum_{j=0}^{t-t_1-1}a_{2,j}y^j\in\mathbb{F}[y]$$

满足

$$\sum_{j=0}^{t-1}a_{1,j}+\sum_{j=0}^{t-t_1-1}a_{2,j}=S$$

令

$$f(x,y)=P_1(y)L_1(x)+P_2(y)L_2(x)=\sum_{i=1}^{2}\sum_{j=0}^{s_i-1}a_{i,j}y^jL_i(x) \tag{3}$$

其中

$$s_1=t,s_2=t-t_1$$

$$L_1(x)=\frac{x-x_2}{x_1-x_2},L_2(x)=\frac{x-x_1}{x_2-x_1}$$

C_i 中每个实体由唯一的点 $(x_i,y_{i,j})$ 来标识，其中 $1\neq y_{i,j}\in\mathbb{F}$ 为随机元素，$y_{i,j}\neq y_{i,k}$，$\forall j\neq k$。$f(x_i,y_{i,j})$ 为其秘密密钥份额；公开函数 f 在 $t-t_1$ 个随机点 (x_i',z_i) 之值为 $f(x_i',z_i)$，$1\leqslant i\leqslant t-t_1$，其中 $x_i'\notin\{x_1,x_2\}$。

显然，方案的信息率 $\rho=1$，是一个理想方案。关于方案的完善性，有以下结论。

引理 2　Γ 中的授权子集能够以概率 $1-Cp^{-1}$ 恢复秘密 S，其中 C 是仅依赖于参数 t 和 t_1 的常数。

证明：设 W 是 Γ 的最小授权子集，$|W\cap C_1|=k_1$，$|W\cap C_2|=k_2$，则有 $k_1+k_2=t$，$k_2\leqslant t-t_1$。

设 $W\cap C_i=\{u_{i,1},\cdots,u_{i,k_i}\}$，$u_{i,j}$ 的标识为点 $(x_i,y_{i,j})$，$k=s_1+s_2-t=t-t_1$。由 W 中实体的公私钥信息及系统的公开参数信息可以得到关于式(3)中未知数 $\{a_{i,j}:i=1,2,0\leqslant j\leqslant s_i-1\}$ 的线性方程组，其系数矩阵为

$$M=\begin{pmatrix}M_1 & 0\\ 0 & M_2\\ H_1 & H_2\end{pmatrix}$$

其中

$$M_i=\begin{pmatrix}1 & y_{i,1} & y_{i,1}^2 & \cdots & y_{i,1}^{s_i-1}\\ 1 & y_{i,2} & y_{i,2}^2 & \cdots & y_{i,2}^{s_i-1}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & y_{i,k_i} & y_{i,k_i}^2 & \cdots & y_{i,k_i}^{s_i-1}\end{pmatrix}$$

$$H_i=\begin{pmatrix}L_i(x_1') & L_i(x_1')z_1 & L_i(x_1')z_1^2 & \cdots & L_i(x_1')z_1^{s_i-1}\\ L_i(x_2') & L_i(x_2')z_2 & L_i(x_2')z_2^2 & \cdots & L_i(x_2')z_2^{s_i-1}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ L_i(x_k') & L_i(x_k')z_k & L_i(x_k')z_k^2 & \cdots & L_i(x_1')z_k^{s_i-1}\end{pmatrix}$$

矩阵 M 为 $2t-t_1$ 阶方阵。如果相应行列式值非 0，则线性方程组有唯一解，从而可以恢复秘密 S。下面讨论 M 的行列式为 0 的概率。

把行列式视为关于变量 $z_1,\cdots,z_k$ 的多项式 $P(z_1,\cdots,z_k)$，其系数依赖于 $L_i(x_j')$，$i=1,2$，$1\leqslant j\leqslant k$ 及 M 中前 t 行所包含的所有 t 阶子式。关于多项式 $P(z_1,\cdots,z_k)$，分两种情况考虑：

(1) $P(z_1,\cdots,z_k)\neq0$

由于 P 中每一个变量的次数 $\leqslant t-1$，由引理 1 知，P 在 $\mathbb{F}^k$ 中的零点个数 $\leqslant k(t-1)p^{k-1}$。又由于 z_j 是 $\mathbb{F}$ 中的随机元素，则 $(z_1,\cdots,z_k)$ 是 P 的零点的概率 $\leqslant k(t-1)p^{k-1}/p^k=k(t-1)p^{-1}$。

(2) $P(z_1,\cdots,z_k)\equiv0$

$P(z_1,\cdots,z_k)\equiv0$ 当且仅当其系数全为 0。P 的系数是关于 $2t-t_1$ 个变量 $y_{i,j}$，$i=1,2$，$0\leqslant j\leqslant s_i-1$，$x_1',\cdots,x_k'$ 的多项式，其中每一个变量的次数 $\leqslant t-1$。由引理 1 知，使所有系数为 0 的变量的个数 $\leqslant(2t-t_1)(t-1)p^{2t-t_1-1}$。又由于 $y_{i,j}$，$i=1,2$，$0\leqslant j\leqslant s_i-1$，$x_1',\cdots,x_k'$ 是 $\mathbb{F}$ 中的随机元素，因此 $P(z_1,\cdots,z_k)\equiv0$ 的概率为 Cp^{-1}，其中 C 是仅依赖于 t 和 t_1 的常数。引理 2 证毕。

引理 3　Γ 的非授权子集不能获得有关秘密 S 的任何信息的概率为 $1-Cp^{-1}$，其中 C 是仅依赖于 t 和 t_1 的常数。

证明：设 V 是 Γ 的非授权子集。不妨假定 $|V|=t-1$，$|V\cap C_i|=k_i\leqslant s_i$，$i=1,2$，则 $k_1+k_2=t-1$。

类似引理 2 的证明，考虑由 V 中实体的公私钥信息及系统的公开参数信息可以得到关于式(3)中未知数 $\{a_{i,j}:i=1,$

$2,0\leqslant j\leqslant s_i-1\}$的线性方程组。矩阵 M 包含 $2t-t_1-1$ 行、$2t-t_1$ 列。在矩阵 M 中增加行向量$(1,\cdots,1)$，得到 $2t-t_1$ 阶方阵 M'。类似引理 2，可以证明矩阵 M' 中行向量线性无关的概率为 $1-Cp^{-1}$，即向量$(1,\cdots,1)$不能被矩阵 M 中的行向量线性表示出的概率为 $1-Cp^{-1}$。也就是说，由 V 中实体的公私钥信息及系统的公开参数信息不能得到有关秘密 S 的任何信息的概率为 $1-Cp^{-1}$。引理 3 证毕。

由引理 2 和引理 3，可以得到下面的结论。

定理 1 方案 1 是实现访问结构 Γ 的完善秘密共享方案的概率为 $1-\varepsilon$，其中 $\varepsilon=\binom{n+1}{t}Cp^{-1}$，$C$ 是仅依赖于参数 t 和 t_1 的常数。

证明：我们只需考虑 Γ 的最小授权子集和最大非授权子集。显然，Γ 的最小授权子集的个数$\leqslant\binom{n}{t}$，而最大非授权子集的个数$\leqslant\binom{n}{t-1}$。而

$$\binom{n}{t}+\binom{n}{t-1}=\binom{n+1}{t}$$

因此，由引理 2 和引理 3 知，方案 1 不是完善的概率$\leqslant\varepsilon=\binom{n+1}{t}Cp^{-1}$，其中 C 是仅依赖于参数 t 和 t_1 的常数。定理 1 证毕。

需要说明，这里的概率是对$\mathbb{F}^2$上的随机点(x,y)进行计算得到的。为了保证方案的完善性，密钥分发者需要对所选取的随机点进行检验，即检验所有的最小授权子集都能够恢复秘密 S，而所有的最大非授权子集都不能得到关于秘密 S 的任何信息。如果检验通过，则相应的秘密共享方案是完善的；否则，需要重新选取随机点进行检验。一般情况下，在实际应用中，n 和 t 相对于 p 来说是很小的值，因此密钥分发者没有必要做上述检验。

由定理 1，可以得到下面的结论。

推论 1 访问结构 Γ 可以由阶为 $p>C\binom{n+1}{t}$ 的有限域 $\mathbb{F}$ 上理想完善的秘密共享方案实现。

4 $(t_1,n_1;t,n)$门限群签名方案

4.1 基本思想

借鉴文献[6]的设计思想，利用成熟的单签名方案，把特权条件要求与秘密共享思想结合起来构造门限群签名方案。与文献[6]不同的是，这里采用“多部秘密共享”技术对秘密密钥进行分割，使方案在满足安全性的前提下具有理想特性。

KAC 负责群密钥与秘密密钥碎片的产生，每个用户得到一个秘密密钥碎片，由 KAC 计算并公开其对应的公开密钥。用户的单签名结果依赖于其所分得的群秘密密钥碎片，SC 负责单签名的验证及群签名的生成。

需要说明，方案中所有公钥的真实性和完整性可以通过使用公钥证书来保证，在此不赘述。

4.2 系统初始化

KAC 执行如下操作：

(1) 选取大素数 p,q，满足 $q|(p-1)$，有限域$\mathbb{Z}_p$中阶为 q 的生成元 g，安全 Hash 函数 h；

(2) 公开 p,q,g,h。

4.3 群密钥与秘密密钥碎片产生

群密钥：KAC 随机选取 $x_1,x_2\in\mathbb{Z}_p,x_1\neq x_2$，两个秘密随机多项式

$$P_1(y)=\sum_{j=0}^{t-1}a_{1,j}y^j\in\mathbb{Z}_p[y]$$

$$P_2(y)=\sum_{j=0}^{t-t_1-1}a_{2,j}y^j\in\mathbb{Z}_p[y]$$

群秘密密钥 $X_G=(\sum_{j=0}^{t-1}a_{1,j}+\sum_{j=0}^{t-t_1-1}a_{2,j})\bmod p\bmod q$，群公开密钥 $Y_G=g^{X_G}\bmod p$；

令

$$f(x,y)=P_1(y)L_1(x)+P_2(y)L_2(x)=\sum_{i=1}^{2}\sum_{j=0}^{s_i-1}a_{i,j}y^jL_i(x)$$

其中

$$s_1=t,s_2=t-t_1$$

$$L_1(x)=\frac{x-x_2}{x_1-x_2},L_2(x)=\frac{x-x_1}{x_2-x_1}$$

公开函数 f 在 $t-t_1$ 个随机点(x_i',z_i)之值 $f(x_i',z_i)$，$1\leqslant i\leqslant t-t_1$，其中 $x_i'\notin\{x_1,x_2\}$。

秘密密钥碎片分发：KAC 对 X_G 采用“分部秘密共享”进行碎片分发。设 $G=C_1\cup C_2,C_1\cap C_2=\varnothing$，其中 C_1 为特权用户集，C_2 为普通用户集。C_i 中每个用户 $u_{i,j}$ 由唯一的点$(x_i,y_{i,j})$来标识，其中 $y_{i,j}\neq1$ 为$\mathbb{Z}_p$中随机元素，$y_{i,j}\neq y_{i,k},\forall j\neq k$。用户 $u_{i,j}$ 的秘密密钥份额为 $\gamma_{i,j}=f(x_i,y_{i,j})\bmod p\bmod q$。由 KAC 公开 $\delta_{i,j}=g^{\gamma_{i,j}}\bmod p$ 作为其公开密钥。

4.4 群签名的产生与验证

给定待签名信息 m，不妨假设只有 t 个成员参加签名，且恰为 $U_1,U_2,\cdots,U_t$，其中有 t_1 个特权用户。假设各成员的身份信息为 $ID_l=(x_l,y_l)$，私钥份额为 γ_l，对应公钥为 δ_l，$1\leqslant l\leqslant t$。

①单签名产生与验证

(1) 每个参与者 $U_l,l=1,2,\cdots,t$ 向 KAC 秘密提交身份信息 ID_l 并秘密随机选取 $k_l\in\mathbb{Z}_q^*$，计算并广播 $r_l=g^{k_l}\bmod p$；

(2) KAC 根据参与者提交的身份信息 $ID_l=(x_l,y_l)$，计算满足等式 $X_G=\sum_{l=1}^{t}c_lf(x_l,y_l)$ 的 c_l 之值，将其秘密传送给 U_l，计算并公开 $s_l'=\delta_l^{c_l}\bmod p$；

(3) 在收到所有 $r_j,j=1,\cdots,t,j\neq l$ 之后，U_l 计算 $r=\prod_{j=1}^{t}r_j\bmod p$；

(4) U_l 计算

$$s_l=(c_l\gamma_lh(m)-k_lr)\bmod q$$

(r_l,s_l)为 U_l 的单签名；

(5) SC 在收到(r_l,s_l)之后，计算并验证以下等式是否成立：

$$g^{s_l}r_l^{r_l}\equiv(s_l')^{h(m)}(\bmod p)\tag{4}$$

若上式成立，则 SC 接受(r_l,s_l)为 U_l 对 m 的单签名。

②群签名的产生与验证

SC 在接收到所有单签名$(r_l,s_l),l=1,2,\cdots,t$ 之后，计算

$$s=\sum_{l=1}^{t}s_l\bmod q,r=\prod_{l=1}^{t}r_l\bmod p$$

(r,s)为对 m 的门限群签名。

(下转第 190 页)

可以提高网页分类的准确率。而且，利用分类规则树存储分类规则，可以使分类效率得到改善。总之，本文所提出的方法一定程度上很好地弥补了现有的关联分类应用于网页分类时在分类精度上的不足，是一种比较好的网页分类方法。

参 考 文 献

[1] 孙建涛，沈抖，陆玉昌，等. 网页分类技术[J]. 清华大学学报：自然科学版，2004，44(4)：65-68

[2] 马金娜，田大钢. 基于支持向量机的中文文本自动分类研究[J]. 系统工程与电子技术，2007，29(3)：475-478

[3] 范焱，郑诚，王清毅，等. 用 Naïve Bayes 方法协调分类 Web 网页[J]. 软件学报，2001，12(9)：1386-1392

[4] 印鉴，谭焕云. 基于 χ^2 统计量的 kNN 文本分类算法[J]. 小型微型计算机系统，2007，28(6)：1094-1097

[5] Liu Bing, Hsu W, Ma Yi-ming. Integrating Classification and Association Rule Mining[C]// ACM International Conference on Knowledge Discovery and Data Mining(SIGKDD'98). 1998：80-86

[6] Li Wen-min, Han Jia-wei, Pei Jian. CMAR：Accurate and Efficient Classifification Based on Multiple Class association Rules [C]// First IEEE International Conference on Data Mining(ICDM'01). 2001：396-376

[7] Guo Yu-qin, Yuan Fang, Liu Hai-bo. Text categorization based on fuzzy classification rules tree[J]. Journal of Southeast University(English Edition)，2008，24(3)：339-342

[8] 王元珍，钱铁云，冯小年. 基于关联规则挖掘的中文文本自动分类[J]. 小型微型计算机系统，2005，26(8)：1380-1383

[9] 邱江涛，唐常杰，乔少杰，等. 基于加权频繁项集的文本分类规则挖掘[J]. 四川大学学报：工程科学版，2008，40(6)：110-114

[10] Cutler M, Shi Yung-ming, Meng Wei-yi. Using the Structure of HTML Documents to Improve Retrieval[C]// Proceeding of the USENIX Symposium on Internet Technologies and Systems Monterey. California，1997：22-33

[11] 董振东，董强. 知网[EB/OL]. http://www.keenage.com，2009

[12] Agrawal R, Imielinski T, Swami A. Mining Association Rules between Sets of Items in Large Databases[C]// Proceeding of the 1993 ACM SIGMOD Conference. Washington DC, USA，1993：207-216

(上接第 152 页)

群签名的验证方程为：

$$g^s r^{r \bmod q} \equiv (Y_G)^{h(m)} \pmod p \tag{5}$$

定理 2 单签名的正确性可以通过式(4)验证。

证明：由单签名的产生过程知，

$g^{s_l} r_l^{r_l} \equiv g^{c_l \gamma_l h(m) - k_l r} \cdot g^{k_l r} \equiv ((\delta_l)^{c_l})^{h(m)} \equiv (s_l')^{h(m)} \pmod p$

因此，单签名满足式(4)。证毕。

定理 3 群签名的正确性可以通过式(5)验证。

证明：由签名过程及定理 2 知，

$$g^s r^r \equiv g^{\sum s_l} (\prod r_l)^r \equiv g^{h(m)\sum c_l \gamma_l - r\sum k_l} \cdot g^{\sum k_l r}$$
$$\equiv (g^{\sum c_l \gamma_l})^{h(m)} \equiv (Y_G)^{h(m)} \pmod p$$

因此，群签名满足式(5)。证毕。

5 分析与讨论

群签名方案具有以下特性：

(1) "特权集"与"门限"特性

由秘密密钥分割过程及定理 1 的证明易见，如果不足 t 个用户参加签名，或者即使有 t 个以上用户参加签名但不满足特权条件，则不能恢复群秘密密钥，从而无法生成有效的群签名。

(2) 秘密共享的"理想"特性

对群秘密密钥分割时，群中任一成员只需保存一个秘密密钥碎片信息，秘密共享的信息率为 1。

(3) 签名的不可伪造性

在基本 ElGamal 签名的安全性假设下，首先除 KAC 之外，任何成员不可能伪造其他成员的单签名，从而任意 $t-1$ 个成员不可能通过伪造其他成员的单签名来伪造群签名；其次，由定理 1 知，任意 $t-1$ 个成员不能得到有关群秘密密钥的任何信息，从而无法直接伪造群签名。因此，本方案可以抵抗任意 $t-1$ 个成员的合谋攻击。

(4) 验证的匿名性与身份的可追查性

验证者 V 利用群公钥可以验证签名的有效性，单签名参与者的身份信息对 V 来说是无法确定的，因此具有签名验证的匿名性；SC 知道签名者身份，如果得到许可，由 SC 追查签名者身份是平凡的。

说明：

(1) 本方案中，将"特权集"的思想嵌入群秘密密钥碎片的产生过程。在实际应用中，为保证方案的安全性，KAC 在进行秘密分割时需要进行检验，以保证秘密共享的完善性。

(2) 与文献[6]中的特权集方案相比较，本方案的优点是具有秘密共享的理想性，缺点是通信代价有所增加(这也是需要进一步解决的问题)。除此之外，二者签名长度、签名和验证的代价都相当。

结束语 本文将"分部秘密共享"技术和"特权集"思想结合在一起，提出了一种存在特权集的门限群签名方案。基于代数中的基本结论，证明了秘密共享方案的安全性。本文方案除了满足一般群签名体制的基本性质之外，还具有"特权集"与"门限"特性、秘密共享的理想性、签名的不可伪造性、验证的匿名性与身份的可追查性等良好特性，在成员存储能力和计算能力受限的场合具有重要的应用价值。

参 考 文 献

[1] Desmedt Y, Frankel Y. Shared generation of autheneicators and signatures[C]// Proceedings of Cryptology-Crypto'91. Berlin：Spring-Verlag，1991：457-469

[2] Harn L. Group-oriented(t,n)-threshold digital signature scheme based on discrete logarithms[J]. IEEE Proceedings of Computers and Digital Techniques，1994，141(5)：307-313

[3] 徐秋亮. 改进门限 RSA 数字签名体制[J]. 计算机学报，2000，23(5)：449-453

[4] 蒋翰，徐秋亮，周永彬. 基于 RSA 密码体制的门限代理签名[J]. 计算机学报，2007，30(2)：241-247

[5] 马春波，何大可. 矢量空间秘密共享群签名方案[J]. 电子学报，2005，33(2)：294-296

[6] 陈伟东，冯登国. 一类存在特权集的门限群签名方案[J]. 软件学报，2005，16(7)：1289-1295

[7] 王天芹. 存在特权集的门限代理群签名方案[J]. 计算机应用研究，2008，25(7)：2146-2147

[8] Farras O, Marti-Farre J, Padro C. Ideal multipartite secret sharing schemes[C]// Lecture Notes in Computer Science 4515. Berlin：Spring-Verlag. 2007：448-465