基于特征值的无可信中心的秘密共享方案研究

张艳硕[①②④] 李文敬*[①④] 赵 耿[①] 王庆瑞[①] 毕 伟[③] 杨 涛[④]

[①](北京电子科技学院 北京 100070)

[②](工业安全与应急技术安徽省重点实验室(合肥工业大学) 合肥 230009)

[③](中思博安科技(北京)有限公司 北京 100195)

[④](公安部第三研究所 上海 201204)

摘 要：利用矩阵特征值的特性，该文提出新的无可信中心的秘密共享方案。该方案无需可信中心的参与，每个参与者提供相同的秘密份额(列向量)，在黑盒子中协同产生各自的秘密份额，从而避免可信中心的权威欺骗。所有参与者提供的列向量组成一个可逆矩阵$\boldsymbol{P}$，可逆矩阵$\boldsymbol{P}$和对角矩阵$\boldsymbol{\Lambda}$生成一个矩阵$\boldsymbol{M}$，并将该矩阵正交化的单位特征向量，作为子密钥分发给各参与者。由于同一个集合的参与者所对应的特征值是相同的，该方案可以有效地防止成员之间的恶意欺诈行为。分析结果表明，该方案是可行的、安全的。

关键词：秘密共享；特征值；可信中心；黑盒子

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2018)11-2752-06

DOI: 10.11999/JEIT180197

Research on Secret Sharing Scheme Without Trusted Center Based on Eigenvalue

ZHANG Yanshuo[①②④] LI Wenjing[①④] ZHAO Geng[①]

WANG Qingrui[①] BI Wei[③] YANG Tao[④]

[①](*Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*)

[②](*Anhui Province Key Laboratory of Industry Safety and Emergency Technology*, *Hefei* 230009, *China*)

[③](*Zsbatech Corporation*, *Beijing* 100195, *China*)

[④](*The Third Research Institute of Ministry of Public Security*, *Shanghai* 201204, *China*)

Abstract: By using the characteristic of matrix eigenvalues, this paper proposes a new secret sharing scheme without trusted center. The scheme does not require a trusted center, and each participant provides the same secret share (column vector) and generates its own secret share in the black box, thus avoiding the authority deception of the trusted center. Reversible matrix $\boldsymbol{P}$ consisting of column vectors provided by all participants,and diagonal matrix $\boldsymbol{\Lambda}$ generate a matrix $\boldsymbol{M}$. Then, the orthogonalized unit eigenvectors of the matrix $\boldsymbol{M}$ is distributed to each participant as a subkey. Because the eigenvalues corresponding to the participants in the same set are the same, this scheme can effectively prevent malicious fraud among members. Analysis results show that the program is feasible and safe.

Key words: Secret sharing; Eigenvalues; Trusted center; Black box

1 引言

秘密共享技术已成为应用密码学中的一项重要技术，它在信息安全存储、传输、以及安全计算中起着非常关键的作用。秘密共享方案最早是Shamir[1]和Blakley[2]分别提出，此后又提出了很多经典的秘密共享方案[3–7]。

传统的秘密共享方案大多都存在一个可信中心，但是由于可信中心负责秘密份额的产生、分配

收稿日期：2018-02-28；改回日期：2018-07-25；网络出版：2018-08-02

*通信作者： 李文敬 2654019946@qq.com

基金项目：国家自然科学基金(61772047)，信息网络安全公安部重点实验室开放基金(C17608)，中国民航信息技术科研基地(CAAC-ITRB-201705)，工业安全与应急技术安徽省重点实验室开放课题资助(ISET201803)

Foundation Items: The National Natural Science Foundation of China (61772047), The Opening Project of Key Laboratory of Information Network Security of Ministry of Public Security (C17608), The Information Technology Research Base of Civil Aviation Administration of China (CAAC-ITRB-201705), Anhui Province Key Laboratory of Industry Safety and Emergency Technology (ISET201803)

以及秘密的恢复，这可能影响系统的安全性、鲁棒性和可用性。针对上述问题，文献[8–12]提出了无中心的秘密共享方案。

本文利用特征值的特点，提出了一个在黑盒子下的无可信中心的秘密共享方案，这是首次从特征值的角度设计的无中心的秘密分享方案。所有的参与者都平等提供秘密份额(列向量)给黑盒子，黑盒子通过判断提供的列矩阵和已存在的向量组的相关性，得到一个由n个n维列向量构成的线性无关向量组，其构成一个n阶方阵，将该方阵作为可逆矩阵，求出对角矩阵的相似矩阵。求出该相似矩阵的特征向量，并将其标准正交化，得到n个正交向量，将该向量作为子密钥分发给各参与者。经分析，该方案是安全的、可行的。

2　特殊门限秘密共享方案

首先以银行为例，3家银行B_1, B_2和B_3共同管理一项基金，基金的使用需要3家银行的执行董事共同商定。其中，银行B_1有3个执行董事，银行B_2有4个执行董事，银行B_3有2个执行董事，每个执行董事的手中都有一把钥匙。在这个例子中，3家银行均只需派出任意一位执行董事，即可决定该基金的使用状况，一共有$3\times4\times2=24$种决定方式。由此，我们定义了一种新的$(n_1+n_2+\cdots+n_t,1+1+\cdots+1)$门限方案。

定义 1　设$B_1,B_2,\cdots,B_t$是t个参与者的集合，且任意两个集合的交集为空集，即$B_f\cap B_g=\Phi$ (Φ为空集，$f\neq g,1\le f\le t,1\le g\le t$)，$|B_i|=n_i(n_1+n_2+\cdots+n_t=n)$。每个集合的参与者都提供一个秘密份额$p_{ij}(1\le i\le t,1\le j\le n_i)$，经过共同商议，生成$n$个子密钥$q_{ij}(1\le i\le t,1\le j\le n_i)$，并将子密钥分发给各集合的参与者。恢复密钥的时候，每个集合均至少出一个人，才可以计算出主密钥k，缺少任何一个集合的参与者都不能计算出该主密钥。

3　前期知识

3.1　数学相关知识

(1)方阵的特征值和特征向量

定义2[13]　设$\boldsymbol{A}$是n阶矩阵，如果数λ和n维非零列向量$\boldsymbol{p}$使关系式

$$\boldsymbol{A}\boldsymbol{p}=\lambda\boldsymbol{p} \tag{1}$$

成立，那么，这样的数λ称为矩阵$\boldsymbol{A}$的特征值，非零向量$\boldsymbol{p}$称为$\boldsymbol{A}$的对应于特征值λ的特征向量。

(2)相似矩阵

定义 3　设矩阵$\boldsymbol{A}$, $\boldsymbol{B}$都是n阶矩阵，若有可逆矩阵$\boldsymbol{P}$，使

$$\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}=\boldsymbol{B} \tag{2}$$

则称$\boldsymbol{B}$是$\boldsymbol{A}$的相似矩阵，可逆矩阵$\boldsymbol{P}$称为把$\boldsymbol{A}$变成$\boldsymbol{B}$的相似变换矩阵。

推论 1　若n阶矩阵$\boldsymbol{A}$与对角矩阵$\boldsymbol{\Lambda}$相似，则存在可逆矩阵$\boldsymbol{P}$，使$\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}=\boldsymbol{\Lambda}=\begin{pmatrix}\lambda_1&&&\\&\lambda_2&&\\&&\ddots&\\&&&\lambda_n\end{pmatrix}$，$\lambda_1,\lambda_2,\cdots,\lambda_n$即是$\boldsymbol{A}$的$n$个特征值。把$\boldsymbol{P}$用其列向量表示为$\boldsymbol{P}=(\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_n)$，于是有：

$$\boldsymbol{p}_i^{-1}\boldsymbol{A}\boldsymbol{p}_i=\lambda_i,\quad i=1,2,\cdots,n \tag{3}$$

$\boldsymbol{P}$的列向量$\boldsymbol{p}_i$就是$\boldsymbol{A}$的对应于λ_i的特征向量。

定理 1　n阶矩阵$\boldsymbol{A}$与对角阵相似(即$\boldsymbol{A}$能对角化)的充分必要条件是$\boldsymbol{A}$有n个线性无关的特征向量。

定理 2　若n阶矩阵$\boldsymbol{A}$与$\boldsymbol{B}$相似，则$\boldsymbol{A}$与$\boldsymbol{B}$的特征值相同。

(3)向量组的线性相关性

定义 4　给定向量组$\boldsymbol{A}:\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$，如果存在不全为零的数$k_1,k_2,\cdots,k_n$，使

$$k_1\boldsymbol{a}_1+k_2\boldsymbol{a}_2+\cdots+k_n\boldsymbol{a}_n=0 \tag{4}$$

则称向量组$\boldsymbol{A}$是线性相关的，否则称它线性无关。

(4)标准正交化：设$\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$是向量空间$\boldsymbol{V}$的一个基，要求$\boldsymbol{V}$的一个标准正交基。这也就是要找一组两两正交的单位向量$\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n$，使$\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n$与$\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$等价。这样一个问题，成为把基$\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$标准正交化。正交化过程如式(5)：

$$\left.\begin{aligned}&\boldsymbol{b}_1=\boldsymbol{a}_1\\&\boldsymbol{b}_2=\boldsymbol{a}_2-\frac{[\boldsymbol{b}_1,\boldsymbol{a}_2]}{[\boldsymbol{b}_1,\boldsymbol{b}_1]}\boldsymbol{b}_1\\&\vdots\\&\boldsymbol{b}_n=\boldsymbol{a}_n-\frac{[\boldsymbol{b}_1,\boldsymbol{a}_n]}{[\boldsymbol{b}_1,\boldsymbol{b}_1]}\boldsymbol{b}_1-\frac{[\boldsymbol{b}_2,\boldsymbol{a}_n]}{[\boldsymbol{b}_2,\boldsymbol{b}_2]}\boldsymbol{b}_2-\cdots\\&\qquad-\frac{[\boldsymbol{b}_{n-1},\boldsymbol{a}_n]}{[\boldsymbol{b}_{n-1},\boldsymbol{b}_{n-1}]}\boldsymbol{b}_{n-1}\end{aligned}\right\} \tag{5}$$

容易验证$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$两两正交，且$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$与$\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$等价。

然后把它们单位化，即取

$$\boldsymbol{e}_1=\frac{1}{\|\boldsymbol{b}_1\|}\boldsymbol{b}_1,\boldsymbol{e}_2=\frac{1}{\|\boldsymbol{b}_2\|}\boldsymbol{b}_2,\cdots,\boldsymbol{e}_n=\frac{1}{\|\boldsymbol{b}_n\|}\boldsymbol{b}_n \tag{6}$$

就是$\boldsymbol{V}$的一个标准正交基。

3.2　黑盒子

(1)黑盒子的定义

定义 5　所谓“黑盒子”，是指从用户的角度来看一个器件或产品时，并不关心其内部构造和原

理，而只关心它的功能及如何使用这些功能[14]。

(2)黑盒子的原理：本方案中的黑盒子需要满足以下功能：

(a)输入一个列向量，黑盒子可以判断该列向量和存储在黑盒子中向量组的线性相关性。本功能的实现根据式(4)设计的。即

$$k_1\boldsymbol{p}_1 + k_2\boldsymbol{p}_2 + \cdots + k_m\boldsymbol{p}_m = 0 \tag{7}$$

其中，$\boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_m$是每次参与者输入的列向量。当新输入的列向量和存储在黑盒子中的向量组线性相关时，黑盒子要求参与者继续输入列向量，直到满足线性无关的条件为止。

(b)输入一个线性无关的向量组，可以将该向量组构成一个可逆的矩阵$\boldsymbol{P}$，根据式(2)将内置的矩阵转化为$\boldsymbol{A}$的相似矩阵，并求出矩阵$\boldsymbol{A}$的特征向量并将其标准正交化。其中，向量组只满足线性无关的条件即可。

(c)输入一个特征向量$\boldsymbol{p}_i$，输出该特征向量对应的特征值λ_i。本功能的实现根据式(3)设计的，即

$$\boldsymbol{p}_i^{-1}\boldsymbol{A}\boldsymbol{p} = \lambda_i$$

其中，$\boldsymbol{p}_i$是参与者输入的子密钥，输出的是该子密钥所对应的特征值。

(3)黑盒子的用法：下面给出程序说明黑盒子在本方案中的用法。

(a)判断线性相关性：

程序：

```
p11=[0  1  0  2]′;
p12=[4  0  0  1]′;
p21=[1  0  3  0]′;
p22=[3  0  0  2]′;
P=[p11 p12 p21 p22]
m=size(P,2)
s=rank(P)
if(m>s)
fprintf('线性相关\n')
else
fprintf('线性不相关\n')
end
```

(b)求出矩阵$\boldsymbol{\Lambda}$的相似矩阵$\boldsymbol{M}$：

程序：

```
diag=[2 0 0 0 ;
      0 2 0 0 ;
      0 0 3 0 ;
      0 0 0 3 ]
format rat
M=P*diag*P^-1
```

(c)求出相似矩阵$\boldsymbol{M}$的特征向量：

程序：[$\boldsymbol{V}$,$\boldsymbol{D}$]=eig($\boldsymbol{M}$)

(d)输入子密钥，输出所对应的特征向量：

程序：

```
p=input('请输入一个子密钥\n')
b=q'*A*q
```

4 无可信中心的秘密共享方案

本节将给出具体方案，该方案可分为3个步骤：参数选取、子秘密生成以及秘密恢复。

4.1 参数选取

本秘密共享系统包含n个参与者。n个参与者构成集合B, B被划分为几个不相交的集合，$B = \bigcup_{i=1}^{t} B_i$，其中$|B_i| = n_i$，$1 \le i \le t$，$n_1 + n_2 + \cdots + n_t = n$，参与者共同选定一个大素数$p$。

首先，每个集合的参与者通过密钥交换协议[15]获得初始信息$s_i(1 \le i \le t)$，然后将结果s_i发送给黑盒子。黑盒子计算$\lambda_i = g^{s_i}(\bmod p)$，其中$g$是黑盒子自动生成的且$g \in Z_p$。

接着，以λ_i为对角元素生成一个对角矩阵

$$\boldsymbol{\Lambda} = \begin{pmatrix} \lambda_1 & & & & & & & \\ & \ddots & & & & & & \\ & & \lambda_1 & & & & & \\ & & & \lambda_2 & & & & \\ & & & & \ddots & & & \\ & & & & & \lambda_2 & & \\ & & & & & & \ddots & \\ & & & & & & & \lambda_t \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\}\lambda_1 \\ \left.\vphantom{\begin{matrix}a\\a\end{matrix}}\right\}\lambda_2 \\ \vdots \\ \left.\vphantom{\begin{matrix}a\\a\end{matrix}}\right\}\lambda_t \end{matrix} \tag{8}$$

其中，λ_1有n_1个，λ_2有n_2个，…，λ_t有n_t个。

然后，选定t个不同的小于p的整数$x_1, x_2, \cdots, x_t$(如选择$1, 2, \cdots, t$)，和生成的λ_i组合成t个数对(x_i,λ_i)。假设主秘密为k，选取$x_0 = 0$组成秘密数对(x_0,k)。(x_0,k)和t个数对(x_i,λ_i)经过Lagrange插值公式生成一个t次多项式：

$$s(x) = k + a_1 x + \cdots + a_t x^t (\bmod p) \tag{9}$$

此时的主秘密为$k = s(0)$。

4.2 子密钥生成

首先，集合B_1的参与者B_{11}生成一个n维的列向量$\boldsymbol{p}_{11}$并提供给黑盒子，黑盒子将其存储在向量组$\boldsymbol{P}$中，此时的向量组为$\boldsymbol{P}:\boldsymbol{p}_{11}$。接着，集合$B_1$中参与者$B_{12}$也生成一个$n$维的列向量$\boldsymbol{p}_{12}$给黑盒子，黑盒子验证$\boldsymbol{p}_{12}$与向量组$\boldsymbol{P}$的线性相关性，若相关，参与者$B_{12}$继续提供列向量，直到满足线性无关的条件为止，此时的向量组为$\boldsymbol{P}:\boldsymbol{p}_{11}, \boldsymbol{p}_{12}$。以此类推，集合$B_1$中的其他参与者也按同样的方式提供列向量给黑盒子，其组成的向量组为$\boldsymbol{P}:\boldsymbol{p}_{11}, \boldsymbol{p}_{12}, \cdots, \boldsymbol{p}_{1n_1}$。

同理，其他集合的参与者也按照集合B_1中参

与者的方式提供n维的列向量给黑盒子。最终，所有集合的参与者提供的列向量组成了一个向量组$\boldsymbol{p}:\boldsymbol{p}_{11},\cdots,\boldsymbol{p}_{1n_1},\cdots,\boldsymbol{p}_{t1},\cdots,\boldsymbol{p}_{tn_t}$，其所构成的矩阵为$\boldsymbol{p}_{n\times \boldsymbol{n}}=(\boldsymbol{p}_{11},\cdots,\boldsymbol{p}_{1n_1},\cdots,\boldsymbol{p}_{t1},\cdots,\boldsymbol{p}_{tn_t})$。

然后，黑盒子利用式(2)计算出矩阵$\boldsymbol{\Lambda}$的相似矩阵$\boldsymbol{M}$，并求出矩阵$\boldsymbol{M}$特征向量并将其标准正交化，得到特征向量向量组$\boldsymbol{Q}:\boldsymbol{q}_{11},\cdots,\boldsymbol{q}_{1n_1},\cdots,\boldsymbol{q}_{t1},\cdots,\boldsymbol{q}_{t,n_t}$。

最后，黑盒子将数对$(x_i,\boldsymbol{q}_{ij})$$(1\le i\le t,1\le j\le n_i)$作为子密钥分发给各集合的参与者，同时也将数对$(x_{-1},s(x_{-1}))$$(x_{-1}\in Z_p$，且与$x_1,x_2,\cdots,x_t$均不相同)发送给每个参与者。

$$\boldsymbol{M}=\boldsymbol{P}\boldsymbol{\Lambda}\boldsymbol{P}^{-1}=(\boldsymbol{p}_{11},\cdots,\boldsymbol{p}_{1n_1},\cdots\boldsymbol{p}_{t1},\cdots,\boldsymbol{p}_{t,n_t})\begin{pmatrix}\lambda_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \lambda_1 & & & & & & \\ & & & \lambda_2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & \lambda_2 & & & \\ & & & & & & \ddots & & \\ & & & & & & & \lambda_t & \\ & & & & & & & & \ddots \\ & & & & & & & & & \lambda_t\end{pmatrix}(\boldsymbol{p}_{11},\cdots,\boldsymbol{p}_{1n_1},\cdots\boldsymbol{p}_{t1},\cdots,\boldsymbol{p}_{t,n_t})^{-1} \tag{10}$$

4.3 秘密恢复

由于门限的特殊性，要求恢复秘密的参与者的人数达到要求，即不少于门限值t，不失一般性，也就是每个参与者集合必须至少出一个人。

假设集合B_1中参与者B_{11}提供子密钥$\boldsymbol{q}_{11}$，集合B_2中参与者B_{21}提供子密钥$\boldsymbol{q}_{21},\cdots$，集合$B_t$中参与者$B_{t1}$提供子密钥$\boldsymbol{q}_{t1}$，他们均将自己的子密钥输入到黑盒子中去，根据式(3)，可以得到特征值$\lambda_1,\lambda_2,\cdots,\lambda_t$。

将(x_{-1},λ_{-1})和t个数对(x_i,λ_i)代入Lagrange插值公式，从而可以得到共享主密钥k：

$$k=s(0)=\sum_{s=1}^{t}\lambda_s\prod_{\substack{j=1\\ j\ne s}}^{t}\frac{-x_j}{x_s-x_j}=\sum_{s=1}^{t}b_s\lambda_s \tag{11}$$

式中，

$$b_s=\prod_{\substack{j=1\\ j\ne s}}^{t}\frac{-x_j}{x_s-x_j} \tag{12}$$

5 方案分析

5.1 正确性

命题 1　任意t个合格成员根据Lagrange插值公式可恢复主秘密k。

分析：在恢复密钥的时候，每个集合都出一个参与者，他们提供子秘密$\boldsymbol{q}_{ij}$给黑盒子，从而得到t个特征值λ_i。把(x_i,λ_i)代入到式(7)中，得到：

$$\left.\begin{aligned}&f(-1)=a_0+a_1\cdot x_{-1}+\cdots+a_t\cdot x_{-1}^t=s(x_{-1})\\&f(x_1)=a_0+a_1\cdot x_1+\cdots+a_t\cdot x_1^t=\lambda_1\\&f(x_2)=a_0+a_1\cdot x_2+\cdots+a_t\cdot x_2^t=\lambda_2\\&\vdots\\&f(x_t)=a_0+a_1\cdot x_t+\cdots+a_t\cdot x_t^t=\lambda_t\end{aligned}\right\} \tag{13}$$

系数矩阵：

$$\boldsymbol{N}=\begin{pmatrix}1 & x_{-1} & \cdots & x_{-1}^t\\ 1 & x_1 & \cdots & x_1^t\\ \vdots & \vdots & \ddots & \vdots\\ 1 & x_t & \cdots & x_t^t\end{pmatrix} \tag{14}$$

$\boldsymbol{N}$可以看成一个的$t\times t$范德蒙矩阵，则它的行列式$\boldsymbol{D}=\prod_{t\ge m>n\ge 1}(x_m-x_n)$。因为$x_1,x_2,\cdots,x_t$互不相等，所以$\boldsymbol{D}\ne 0$。由线性方程组的卡莱姆法则，知方程组只有唯一解，从而可以求出$s(x)$，也就得出共享秘密$k=s(0)$。

5.2 创新性

在子密钥生成的时候，本文方案无需可信中心，秘密份额由全体成员协同产生，每个参与者均提供一个n维列向量给黑盒子。参与者每提供一个n维列向量，都和黑盒子已有的向量组进行线性相关性判断，从而得到n个n维的线性无关的向量组，其构成一个n阶的方阵$\boldsymbol{P}$。然后，根据式(2)得到矩阵$\boldsymbol{M}$，并将$\boldsymbol{M}$的正交特征向量作为子密钥分发给各参与者。

在恢复主密钥的时候，利用相似矩阵的特征值相同的特点，可以得到t个特征值。从而，利用Lagrange插值得到主密钥k。

本方案首次利用相似矩阵的特征值相同的特点设计了一个秘密共享方案，该方案中任何参与者均无法知道主密钥，有效地避免了可信中心的权威欺骗。

5.3 安全性

(1)检验子密钥是否正确

命题 2　参与者可以通过以下数值特征判断子密钥协商过程是否正确：

(a)子密钥的范数为1；

(b)同一集合中的任意两个参与者得到的子密钥满足正交性；

(c)同一集合中的参与者所得到子密钥所对应的特征值相同。

分析：参与者可以将手中的子密钥输入发到黑盒子中验证，若不同时满足以上3个条件，则说明分发过程存在问题。

(2)检测参与者是否诚实

命题 3 在秘密恢复阶段，也可通过下列数值特征检验参与者是否诚实：

(a)子密钥的范数为1；

(b)不同集合参与者得到的子密钥正交性。

分析：参与者可以将手中的子密钥发到黑盒子中验证，若不同时满足以上两个条件，说明参与者存在欺诈行为。

综上所述，对于这个方案的性能分析结果：信息率为1/2，在预防欺诈方面是无条件安全的。

6 方案实例

下面用一个例子说明方案的可行性。

设有B_1，B_2两个集合，集合B_1中有2个参与者B_{11}和B_{12}，集合B_2中有2个参与者B_{21}和B_{22}。试为这2个集合的4个用户分配密钥，并分析重构密钥k的过程。

(1)初始化：首先，利用密钥协商协议，集合B_1和集合B_2中的参与者分别得到协商的结果$s_1=2$和$s_1=15$。黑盒子计算$\lambda_1=6^2(\bmod 17)=2$，$\lambda_2=6^{15}(\bmod 17)=3$，此时生成的$g=6$。黑盒中生成对角矩阵：

$$\boldsymbol{\Lambda}=\begin{pmatrix}2&0&0&0\\0&2&0&0\\0&0&3&0\\0&0&0&3\end{pmatrix} \tag{15}$$

然后，选取数对$(x_0,a_0)=(0,2)$，$(x_1,\lambda_1)=(1,2)$和$(x_2,\lambda_2)=(2,3)$，经过Lagrange插值公式得到$s(x)\equiv 9x^2+8x+2(\bmod 17)$。此时的共享主密钥是$k=2$。

(2)子密钥生成：首先，集合B_1中的参与者B_{11}生成一个4维的列向量$\boldsymbol{p}_{11}=(\,0\quad 1\quad 0\quad 2\,)^{\mathrm{T}}$，提供给黑盒子，此时的向量组为$\boldsymbol{P}:\boldsymbol{p}_{11}$。集合$B_1$中的参与者$B_{12}$再生成一个4维的列向量$\boldsymbol{p}_{12}$提供给黑盒子。黑盒子验证$\boldsymbol{p}_{12}$和向量组$\boldsymbol{P}$之间的线性相关性，若相关，参与者$B_{12}$继续生成列向量，否则，将列向量保存到向量组$\boldsymbol{P}$中。此时的$\boldsymbol{p}_{12}=(\,4\quad 0\quad 0\quad 1\,)^{\mathrm{T}}$满足线性无关的条件，向量组为$\boldsymbol{P}:\boldsymbol{p}_{11},\boldsymbol{p}_{12}$，其构成的矩阵

$$\boldsymbol{P}=(\boldsymbol{p}_{11},\boldsymbol{p}_{12})=\begin{pmatrix}0&1&0&2\\4&0&0&1\end{pmatrix}^{\mathrm{T}} \tag{16}$$

集合B_2的参与者也按同样的方式提供列向量给黑盒子。参与者B_{21}提供的列向量$\boldsymbol{p}_{21}=(\,1\quad 0\quad 3\quad 0\,)^{\mathrm{T}}$，参与者$B_{22}$提供的列向量$\boldsymbol{p}_{22}=(\,3\quad 0\quad 0\quad 2\,)^{\mathrm{T}}$，并分别填入到向量组$\boldsymbol{P}$中，得到$\boldsymbol{P}:\boldsymbol{p}_{11},\boldsymbol{p}_{12},\boldsymbol{p}_{21},\boldsymbol{p}_{22}$，其构成的矩阵

$$\boldsymbol{P}=(\boldsymbol{p}_{11},\boldsymbol{p}_{12},\boldsymbol{p}_{21},\boldsymbol{p}_{22})=\begin{pmatrix}0&4&1&3\\1&0&0&0\\0&0&3&0\\2&1&0&2\end{pmatrix} \tag{17}$$

其次，根据式(2)求得矩阵$\boldsymbol{M}$：

$$\boldsymbol{M}=\boldsymbol{P}^{-1}\boldsymbol{\Lambda}\boldsymbol{P}=\begin{pmatrix}0&1&0&0\\\frac{2}{5}&\frac{6}{5}&-\frac{2}{15}&-\frac{3}{5}\\0&0&\frac{1}{3}&0\\-\frac{1}{5}&-\frac{8}{5}&\frac{1}{15}&\frac{4}{5}\end{pmatrix}\begin{pmatrix}2&0&0&0\\0&2&0&0\\0&0&3&0\\0&0&0&3\end{pmatrix}\begin{pmatrix}0&4&1&3\\1&0&0&0\\0&0&3&0\\2&1&0&2\end{pmatrix}=\begin{pmatrix}2&0&0&0\\-\frac{6}{5}&\frac{7}{5}&-\frac{2}{5}&-\frac{6}{5}\\0&0&3&0\\\frac{8}{5}&\frac{4}{5}&\frac{1}{5}&\frac{18}{5}\end{pmatrix} \tag{18}$$

再次，求出矩阵$\boldsymbol{M}$的特征向量并将其标准正交化，得到向量组$\boldsymbol{Q}:\boldsymbol{q}_{11},\boldsymbol{q}_{12},\boldsymbol{q}_{21},\boldsymbol{q}_{22}$，其所构成的矩阵为

$$\boldsymbol{Q}=(\boldsymbol{q}_{11},\boldsymbol{q}_{12},\boldsymbol{q}_{21},\boldsymbol{q}_{22})=\begin{pmatrix}1&0&0&0\\0&-\frac{4}{5}&0&-\frac{3}{5}\\0&0&1&0\\0&-\frac{3}{5}&0&\frac{4}{5}\end{pmatrix} \tag{19}$$

黑盒子将对角化的矩阵中的列向量作为子密钥分发给参与者，一共得到2组密钥：第1组密钥为：$k_{11}=(x_1,\boldsymbol{q}_{11})$，$k_{12}=(x_1,\boldsymbol{q}_{12})$；第2组密钥为：$k_{21}=(x_2,\boldsymbol{q}_{21})$，$k_{22}=(x_2,\boldsymbol{q}_{22})$。将$k_{11}$，$k_{12}$分别发送给集合$B_1$中参与者$B_{11}$和$B_{12}$，将$k_{21}$和$k_{22}$分发给集合$B_2$中的参与者$B_{21}$和$B_{22}$，同时将数对$(-1,3)$发送给所有参与者。

(3)秘密恢复：假设集合B_1中参与密钥恢复参与者的是B_{11}，集合B_2中参与密钥恢复的参与者是B_{21}。他们将提供的子密钥输入到黑盒中，分别得到$\lambda_1=2$，$\lambda_2=3$。

将(–1, 3)(1, 2), (2, 3)代入式(11)，从而获得共享密钥k：

$$\begin{aligned} k &= \sum_{s=1}^{3}\lambda_s \prod_{\substack{j=1\\ j\neq s}}^{3}\frac{-x_j}{x_s-x_j} = \sum_{s=1}^{3} b_s\lambda_s \\ &= \left[\frac{-1}{(-1)-1}\times\frac{-2}{(-1)-2}\right]\times 3 \\ &\quad + \left[\frac{1}{1-(-1)}\times\frac{-2}{1-2}\right]\times 2 \\ &\quad + \left[\frac{1}{2-(-1)}\times\frac{-1}{2-1}\right]\times 3 \\ &= 1+2-1(\bmod 17) = 2 \end{aligned} \tag{20}$$

7　结束语

本文提出了一种基于特征值的新的无可信中心的秘密共享方案，也是首次从特征值的角度出发设计的秘密共享方案。所有的参与者均提供一个n维的不相关的列向量作为初始子秘密，该子秘密组成一个可逆矩阵，并提供给黑盒子，黑盒子产生一组新的子秘密并分发给参与者。经分析，该方案是安全的，可以作为一种新的秘密共享方案。

参 考 文 献

[1] SHAMIR A. How to share a secret[J]. *Association for Computing Machinery*, 1979, 22(11): 612–613. doi: 10.1145/359168.359176.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C]. IEEE Computer Society, New York, America, 1979: 313–317. doi: 10.1109/AFIPS.1979.98.

[3] YUAN Dazeng, HE Mingxing, ZENG Shengke, *et al*. (t,p)-Threshold point function secret sharing scheme based on polynomial interpolation and its application[C]. IEEE/ACM, International Conference on Utility and Cloud Computing. Texas, USA, 2017: 269–275. doi: 10.1145/2996890.3007871.

[4] SONG Yun, LUO Yu, and WANG Wenhua. Multiparty quantum direct secret sharing of classical information with Bell states and Bell measurements[J]. *International Journal of Theoretical Physics*, 2018, 57(5): 1559–1571. doi: 10.1007/s10773-018-3681-y.

[5] LIU Chengji, LI Zhihui, BAI Chenming, *et al*. Quantum-secret-sharing scheme based on local distinguishability of orthogonal seven-qudit entangled states[J]. *International Journal of Theoretical Physics*, 2018, 57(2): 428–442. doi: 10.1007/s10773-017-3574-5.

[6] WANG Feng , ZHOU Yousheng, and LI Daofeng. Dynamic threshold changeable multi - policy secret sharing scheme[J]. *Security and Communication Networks*, 2016, 8(18): 3653–3658. doi: 10.1002/sec.1288.

[7] BASIT A, KUMAR N C, VENKAIAH V C, *et al*. Multi-stage multi-secret sharing scheme for hierarchical access structure[C]. International Conference on Computing, Communication and Automation. Noida, India, 2017: 556–563. doi: 10.1109/CCAA.2017.8229863.

[8] PILARAM H and EGHLIDOS T. An efficient lattice based multi-stage secret sharing scheme[J]. *IEEE Transactions on Dependable and Secure Computing*, 2017, 14(1): 2–8. doi: 10.1109/TDSC.2015.2432800.

[9] MENG Li, JIA Yu, and HAO Rong. A cellular automata based verifiable multi-secret sharing scheme without a trusted dealer[J]. *Chinese Journal of Electronics*, 2017, 26(2): 313–318. doi: 10.1049/cje.2017.01.026.

[10] WANG Na, FU Junsong, and ZENG Jiwen. Verifiable secret sharing scheme without dealer based on vector space access structures over bilinear groups[J]. *Electronics Letters*, 2018, 54(2): 77–79. doi: 10.1049/el.2017.1840.

[11] 谷婷. 无可信中心可验证可更新的向量空间秘密共享[J]. 科技与创新, 2018(3): 29–33. doi: 10.15913/j.cnki.kjycx.2018.03.029.
GU Ting. No trusted center verifiable updateable vector space secret sharing[J]. *Science and Technology & Innovation*, 2018(3): 29–33. doi: 10.15913/j.cnki.kjycx.2018.03.029.

[12] ESLAMI Z, PAKNIAT N, and NOROOZI M. Hierarchical threshold multi-secret sharing scheme based on birkhoff interpolation and cellular automata[C]. Csi IEEE International Symposium on Computer Architecture and Digital Systems, Tehran, Iran, 2015: 1–6. doi: 10.1109/CADS.2015. 7377795.

[13] 同济大学数学系编. 工程数学线性代数[M]. 北京: 高等教育出版社, 2014: 124–128.
School of Mathematic Sciences, Tongji University. Engineering Mathematics, Linear Algebra[M]. Beijing: Higher Education Press, 2014: 124–128.

[14] 曹尔强, 张沂, 曹晔, 等. “软件黑盒子”文件加锁和加密的一个方法[J]. 长春邮电学院学报, 1991(3): 11–14.
CAO Erqiang, ZHANG Yi, CAO Hua, *et al*. A technique of locking a disk and secreting a whole disk[J]. *Journal of Changchun Post & Telecommunication Institute*, 1991(3): 11–14.

[15] DIFFIE W and HELLMAN M E. New directions in cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644–654. doi: 10.1109/TIT.1976.1055638.

张艳硕：男，1979年生，博士，研究方向为密码理论及其应用.

李文敬：女，1992年生，硕士生，研究方向为信息安全.

赵　耿：男，1964年生，教授，博士后，研究方向为混沌密码理论及其应用、计算机信息安全及保密.

王庆瑞：男，1993年生，硕士生，研究方向为信息安全.

毕　伟：男，1980年生，博士，研究方向为信息安全及区块链技术.

杨　涛：男，1977年生，博士，研究方向为信息安全.