基于特征值的可验证特殊门限秘密共享方案

张艳硕[1,2]，李文敬[1,2]，陈雷[1]，毕伟[3]，杨涛[2]
（1. 北京电子科技学院密码科学与技术，北京 100070；2. 公安部第三研究所，上海 201204；
3. 中思博安科技（北京）有限公司科学研究院，北京 100195）

摘 要：利用 n 阶矩阵的特征方程具有重根的特点，密钥分发者给每一个参与者分发 2 种不同的子密钥，这 2 种子密钥满足线性无关和对应的特征值相等的特性。在子密钥分发和主密钥恢复的过程中，黑盒子通过子密钥的特性来判断参与者活动的真实性，若这 2 种子密钥满足线性无关和特征值相等这 2 个条件，则说明参与者活动是诚实的，否则，可以判定其存在欺诈行为。分析结果表明，该方案是正确的、安全的，且信息率为 $\frac{1}{2}$。

关键词：秘密共享；特征值；可验证；黑盒子
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018143

Verifiable special threshold secret sharing scheme based on eigenvalue

ZHANG Yanshuo[1,2], LI Wenjing[1,2], CHEN Lei[1], BI Wei[3], YANG Tao[2]
1. Department of Cryptography Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China
2. The Third Research Institute of Ministry of Public Security, Shanghai 201204, China
3. Institute of Science, Zsbatech Corporation, Beijing 100195, China

Abstract: Utilizing the characteristic that the characteristic equation of the n-th order matrix have multiple roots, the secret distributor distributes two different sub-keys to each participant, and these two sub-keys satisfy two conditions: linear independent and equality of the corresponding characteristic values. In the process of sub-key distribution and master key recovery, the black box can judge the authenticity of the participants' activities through the characteristics of the sub-keys. If the two sub-keys have satisfied two conditions of linear independence and equal feature values, it can be determined that the participant's activity is honest, otherwise, it can be determined that there exists fraudulent activity. The analysis results show that the scheme is correct, secure, and the information rate is $\frac{1}{2}$.

Key words: secret sharing, eigenvalue, verifiable, 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、传输以及安全计算等环节起着非常关键的作用。在秘密共享技术中最常见的是门限方案，已提出的门限方案有很多种，主要代表为 Shamir[1]的 Lagrange 插值多项式方案、Blakley[2]的矢量方案、Asmuth 等[3]的同余

收稿日期：2018−01−25；**修回日期**：2018−06−22
基金项目：信息网络安全公安部重点实验室开放基金资助项目（No.C17608）；中国民航信息技术科研基金资助项目（No.CAAC-ITRB-201705）；国家自然科学基金资助项目（No.61772047）
Foundation Items: The Opening Project of Key Lab of Information Network Security of Ministry of Public Security (No.C17608) , The Information Technology Research Base of Civil Aviation Administration of China (No.CAAC-ITRB-201705), The National Natural Science Foundation of China (No. 61772047)

类方案及 Karnin 等[4]的矩阵法方案，这些方案已经得到了广泛的研究，但大多没有解决参与者行骗和密钥分发者欺骗的问题。为了解决上述问题，文献[5]提出了可验证秘密共享的思想，并给出了完整的实现方案。文献[6-8]提出了可抵抗恶意欺骗的秘密共享方案。文献[9-13]提出了可抵抗恶意欺骗的多秘密共享方案。

本文在基本 Shamir 门限方案的基础上，利用 n 阶矩阵的特征方程具有重根的特点，提出了一种基于特征值的安全可验证的门限秘密共享方案。本文方案从矩阵特征值的角度出发，设计了一种可验证的秘密共享方案，这是本文方案的主要贡献。经分析证明，该方案是安全的，可以抵抗恶意欺诈。

2 基本 Shamir 门限秘密共享方案

1979 年，Shamir[1]基于多项式的 Lagrange 插值公式提出了一个(n , t)门限方案，称为 Shamir 门限方案或 Lagrange 插值法。Shamir 门限方案的详细介绍如下。

1) 参数选取

设 $GF(p)$是有限域（p 为素数，且 $p>n$），共享密钥为 K。有 n 个参与者，要求重构该共享密钥 K 至少需要 t 个人。

2) 秘密分割

首先，密钥分发者 D 独立随机地选择 t–1 个元素 $a_1, a_2,\cdots, a_{t-1}\in GF(p)$，构造一个 t–1 次多项式为

$$s(x)\equiv K+a_1x+\cdots+a_{t-1}x^{t-1}(\mathrm{mod}\ p) \tag{1}$$

该多项式满足 $s(0)\equiv K \bmod p$ 。

其次，密钥分发者 D 选择 n 个不同的非零元素 $x_i\in GF(p)$，$1\leqslant i\leqslant n$。对于每个非零元素 x_i，分别计算 $y_i\equiv s(x_i)\bmod p$，并将其作为子密钥。

最后，密钥分发者 D 将 n 个数对(x_i, y_i)，$1\leqslant i\leqslant n$，分别秘密传送给参与者 $T_1, T_2,\cdots, T_n$，多项式 $s(x)$则是保密的，可以销毁。

3）秘密恢复

假设 n 个参与者中的任意 t 个（不妨设为 $T_1, T_2,\cdots, T_t$）准备一起恢复密钥 K。

首先，参与者出示他们的子密钥后，得到 t 个点对(x_1, y_1)，(x_2, y_2)，…，(x_t, y_t)。

其次，t 个人计算多项式

$$f(x)\equiv\sum_{k=1}^{t}y_k\prod_{\substack{j=1\\ j\neq k}}^{t}\frac{x-x_j}{x_k-x_j}(\mathrm{mod}\ p) \tag{2}$$

最后，取多项式 $f(x)$的常数项 $f(0)$，即为所求的密钥 K。

3 （$n_1+n_2+\cdots+n_t$, 1+1+…+1）特殊门限秘密共享方案

在给出本文方案之前，我们先看（$m+u$, t+1）门限方案。文献[14]以某银行 3 位出纳和 2 位主任（正、副）开启保险库为例，为防止出现职员监守自盗、遗忘密钥或因职员缺席而打不开保险库等各种问题，银行规定至少有 2 位出纳和 1 位主任在场才能开启保险库，这样共有 3×2=6 种开启方式。本例中，由于出纳与主任的访问权限不同，定义了($m+u$, t+1)门限方案。

定义 1[14] 设 A、B 为 2 个参与者的集合，$A\cap B=\Phi$（Φ 为空集），$|A|=m$，$|B|=u$，t 为门限值且 $t<m$。假设共享密钥为 K，集合 A 中的参与者 A_i 的子秘密为 $k_i(i=1,2,\cdots,m)$，集合 B 中的参与者 B_i 的子秘密为 $k_j(j=1,2,\cdots, u)$。集合 A 中不少于 t 个参与者和 B 中的一个参与者在一起可以恢复密钥 K，而其他任意组合方式都不能恢复密钥 K，称该方案为$(m+u, t+1)$门限共享方案。

在上述方案的基础上，本文提出一种特例。3 家银行 B_1、B_2 和 B_3 共同管理一项基金，基金的使用需要征求 3 家银行执行董事的意见。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 3 个执行董事，每个执行董事都有一把钥匙。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，此时一共有 3×4×3=36 种决定方式。由此，本文定义了一种新的($n_1+n_2+\cdots+n_t$,1+1+…+1)门限秘密共享方案。

定义 2 设 $B_1,B_2,\cdots,B_t$ 是 t 个参与者的集合，任意 2 个集合的交集是空集，即 $B_f\cap B_g=\Phi(1\leqslant f\leqslant t, 1\leqslant g\leqslant t, f\neq g)$, $|B_1|=n_1$, $|B_2|=n_2$, …, $|B_t|=n_t(n_1+n_2+\cdots+n_t=n)$。每个集合的参与者均分得一个子密钥。主密钥恢复阶段，每个集合至少都出一个人，才可以计算出密钥 K，缺少任何一个集合的参与者都不能计算出密钥 K，则称这种方案为$(n_1+n_2+\cdots+n_t$,1+1+…+1)特殊门限秘密共享方案。

4　特殊门限秘密共享方案

4.1　预备知识

4.1.1　方阵的特征值和特征向量

定义 3　设 $\boldsymbol{A}$ 是 n 阶矩阵，如果 λ 和 n 维非零列向量 $\boldsymbol{p}$，使关系式

$$\boldsymbol{A}\boldsymbol{p}=\lambda\boldsymbol{p} \tag{3}$$

成立，那么，这样的 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。

式(3)也可写成

$$(\boldsymbol{A}-\lambda\mathbf{E})\boldsymbol{p}=0 \tag{4}$$

这是 n 个未知数 n 个方程的齐次线性方程组[15]。

4.1.2　对称矩阵的性质

定理 1　设 $\boldsymbol{A}$ 为 n 阶对称矩阵，则必有正交矩阵 $\boldsymbol{p}$，使

$$\boldsymbol{p}^{-1}\boldsymbol{A}\boldsymbol{p}=\boldsymbol{\Lambda}=\begin{pmatrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{pmatrix} \tag{5}$$

其中，$\boldsymbol{\Lambda}$ 是以 $\boldsymbol{A}$ 的 n 个特征值 λ_i（i=1,2,…,n）为对角元的对角矩阵[15]。

推论 1　设 $\boldsymbol{A}$ 为 n 阶对称矩阵，λ 是 $\boldsymbol{A}$ 的特征方程的 l 重根，从而对应的特征值 λ 恰有 l 个线性无关的特征向量[15]。

4.1.3　黑盒子

1) 黑盒子的定义

基于“黑盒子”[16]的含义给出其在本文方案中的定义。

定义 4　黑盒子的内部结构只有其设计者知道，除此之外无人知晓。子密钥生成阶段，密钥分发者 D 输入待分发的主密钥 K、参与者集合的个数 t 和各集合的人数 $n_i(1\leqslant i\leqslant t)$，输出 $2n$ 个子密钥 p_{ij} $(1\leqslant i\leqslant t,1\leqslant j\leqslant 2n_i)$。主密钥恢复阶段，各参与者输入 2 个子密钥 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$，判断是否满足① $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 线性无关；②$\lambda_i=\lambda_{ij}=\lambda_{ij+1}$。若满足，则输出所对应的特征值 λ_i，从而恢复主密钥 K，否则，不能恢复主密钥 K。

2) 黑盒子的原理

① 子密钥生成阶段是根据式(5)设计的，即

$$\boldsymbol{P}^{-1}\boldsymbol{\Lambda}\boldsymbol{P}=\boldsymbol{A}$$

其中，$\boldsymbol{\Lambda}$ 是根据密钥分发者 D 提供的随机数所生成的 $2n$ 阶对角矩阵，$\boldsymbol{P}$ 是黑盒子生成的 $2n$ 阶随机可逆矩阵，所分发的子密钥 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 是矩阵 $\boldsymbol{P}$ 的列向量，并且所有列向量 $\boldsymbol{p}_{ij}$ 均线性无关。

② 主密钥恢复阶段，是根据式(3)设计的，即

$$\boldsymbol{A}\boldsymbol{p}_{ij}=\lambda_i\boldsymbol{p}_{ij}$$

其中，矩阵 $\boldsymbol{A}$ 是子密钥生成阶段所生成的矩阵，存储在黑盒子中。当参与者输入正确的子密钥 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$，即满足① $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 线性无关；②$\lambda_i=\lambda_{ij}=\lambda_{ij+1}$，黑盒子则输出该子密钥所对应的特征值 λ_i，否则，无法恢复主密钥。

3) 算例

以下用一个小例子说明黑盒子在本文方案中的用法。

子密钥生成阶段，主要功能程序如下。

① 密钥分发者 D 输入共享主密钥 K、集合的总个数 t 和各集合的人数 n_i：

```
K=input('请输入要分发的秘密 K:');
t=input('请输入集合的个数 t:') ;
    for j=1:t
        n_i=input('所对应的集合的人数:') ;
    end for
```

② 生成 $2n$ 阶随机可逆矩阵为

```
a=rand(2n,2n);
```

③ 密钥分发者 D 随机选定 $t-1$ 个元素 $a_1, a_2,\cdots, a_{t-1}\in GF(p)$，得到 λ_i，从而得到 $2n$ 阶对角矩阵为

```
  for j=1:t
        x_i=x_ii(1,j)
        fprintf('%d',x_i)
        n_i=input('所对应的集合的人数:') ;
      for i=1:t−1
        f(x)=f(x)=+a(1,i)(x^(i));
        f(x_i)=f(x_i)+a(1,i)(x_i^(i));
      end for
      for k=1:n_i
          for k=1:2
            E_i=[E_i mod(f(x_i),p)];
          end for
      end for
  end for
```

密钥分发者选取的素数为 7，a_1=3，主密钥 K=3，得到多项式 $s(x)\equiv 3+3x \pmod 7$，$\lambda_1=s(x_1)=s(1)=6$，

所对应集合有一个人，$\lambda_2=s(x_2)=s(4)=1$，所对应集合有一个人，从而得到对角矩阵为

$$\boldsymbol{\Lambda}=\begin{pmatrix}6&0&0&0\\0&6&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

黑盒子生成的随机可逆矩阵为

$$\boldsymbol{P}=\begin{pmatrix}1&0&1&0\\1&1&1&1\\1&1&0&0\\1&0&0&0\end{pmatrix}$$

生成的矩阵为

$$\boldsymbol{A}=\begin{pmatrix}1&0&0&5\\0&1&5&0\\0&0&6&0\\0&0&0&6\end{pmatrix}$$

得到的子密钥为 $\boldsymbol{p}_{11}=(1\ \ 1\ \ 1\ \ 1)^{\mathrm{T}}$、$\boldsymbol{p}_{12}=(0\ \ 1\ \ 1\ \ 0)^{\mathrm{T}}$、$\boldsymbol{p}_{21}=(1\ \ 1\ \ 0\ \ 0)^{\mathrm{T}}$和 $\boldsymbol{p}_{22}=(0\ \ 1\ \ 0\ \ 0)^{\mathrm{T}}$。

主密钥恢复阶段，主要功能程序如下。

① 判断线性相关性

```
La=[ ] ;
Pi=[ ] ;
for r=1:2
pi=input('输入子秘钥:') ;
lai=pi'·A·pi
      Pi=[Pi pi]
      La=[La lai]
end for
     m=size(Pi);
     s=rank(Pi);
     if(m>s)
          fprintf('线性相关，停止恢复主密钥\n')
     else
          fprintf('线性无关，继续恢复主密钥\n')
     end if
```

② 判断 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 所对应的特征值是否相同。

```
  if(La(1,1)==La(1,2))
       fprintf('特征值相同，继续恢复主密钥\n')
  else
       fprintf('特征值不同，停止恢复主密钥\n')
```

当参与者输入正确的子密钥为

$\boldsymbol{p}_{11}=(1\ \ 1\ \ 1\ \ 1)^{\mathrm{T}}$ 和 $\boldsymbol{p}_{12}=(0\ \ 1\ \ 1\ \ 0)^{\mathrm{T}}$；

黑盒子输出：线性无关，继续恢复主密钥；

特征值相同，继续恢复主密钥；

$\lambda_i=6$；

当参与者输入伪造的子密钥为

$\boldsymbol{p}_{11}=(1\ \ 1\ \ 1\ \ 1)^{\mathrm{T}}$ 和 $\boldsymbol{p}_{12}=(0\ \ 1\ \ 1\ \ 3)^{\mathrm{T}}$；

黑盒子输出：线性无关，继续恢复主密钥；

特征值不同，停止恢复主密钥；

当参与者输入伪造的子密钥为

$\boldsymbol{p}_{11}=(1\ \ 1\ \ 1\ \ 1)^{\mathrm{T}}$ 和 $\boldsymbol{p}_{12}=(2\ \ 2\ \ 2\ \ 2)^{\mathrm{T}}$；

黑盒子输出：线性相关，停止恢复主密钥；

end if

4.2 方案设计

本节将给出具体方案，该方案可分为 4 个步骤：系统描述、参数选取、秘密分割以及秘密恢复。

4.2.1 系统描述

秘密共享系统包含一个密钥分发者 D 和 n 个秘密参与者。n 个秘密参与者构成集合 B，B 被划分为几个不相交的集合，$B=\bigcup_{i=1}^{t}B_i$，其中，$|B_i|=n_i(1\leqslant i\leqslant t, n_1+n_2+\cdots+n_t=n)$。

4.2.2 参数选取

系统参数的选取是为了给后续工作做准备。

设 $GF(p)$是有限域（p 为素数，且 $p>n$）。密钥分发者 D 独立随机地选择 $t-1$ 个元素 $a_1, a_2,\cdots, a_{t-1}\in GF(p)$，得到多项式 $s(x)\equiv K+a_1x+\cdots+a_{t-1}x^{t-1}(\mathrm{mod}\ p)$。其中，共享秘密主密钥是 K。

4.2.3 秘密分割

首先，密钥分发者选择 t 个非零的、互不相同的元素 $x_1, x_2,\cdots, x_t\in GF(p)$，分别计算 $\lambda_i\equiv s(x_i)\ (\mathrm{mod}\ p)\ (i=1,2,\cdots,t)$，得到 $2n$ 阶对角矩阵 $\boldsymbol{\Lambda}$ 为

$$\boldsymbol{\Lambda}=\begin{pmatrix}\lambda_1&&&&&&&&\\&\ddots&&&&&&&\\&&\lambda_1&&&&&&\\&&&\lambda_2&&&&&\\&&&&\ddots&&&&\\&&&&&\lambda_2&&&\\&&&&&&\ddots&&\\&&&&&&&\lambda_t&\\&&&&&&&&\ddots\\&&&&&&&&&\lambda_t\end{pmatrix}\begin{matrix}\}\lambda_1\\\\\}\lambda_2\\\vdots\\\}\lambda_t\end{matrix}$$

其中，$\lambda_1,\lambda_2,\cdots,\lambda_t$ 是特征方程 $(\boldsymbol{A}-\lambda\mathbf{E})x=0$ 对应的特征根，并且 λ_1 有 $2n_1$ 个，λ_2 有 $2n_2$ 个，…，λ_t 有 $2n_t$ 个。

其次，密钥分发者随机生成一个 $2n$ 阶可逆矩阵 $\boldsymbol{P}$，进而得到矩阵为

$$\boldsymbol{A}=\boldsymbol{P}^{-1}\boldsymbol{\Lambda}\boldsymbol{P}$$

由线性代数知识可知，矩阵 $\boldsymbol{\Lambda}$ 和矩阵 $\boldsymbol{A}$ 具有相同的特征值。又由推论 1 可知，每个特征根 $\lambda_i(i=1,2,\cdots,t)$ 都对应着 $2n_i$ 个线性无关的特征向量，则 λ_1 对应的特征向量为 $\boldsymbol{p}_{11},\boldsymbol{p}_{12},\cdots,\boldsymbol{p}_{1,2n_1}$，$\lambda_2$ 对应的特征向量为 $\boldsymbol{p}_{21},\boldsymbol{p}_{22},\cdots,\boldsymbol{p}_{2,2n_2}$，…，$\lambda_t$ 对应的特征向量为 $\boldsymbol{p}_{t1},\boldsymbol{p}_{t2},\cdots,\boldsymbol{p}_{t,2n_t}$。

再次，密钥分发者将子密钥 $(x_i,\ \boldsymbol{p}_{ij})$ 和 $(x_i,\ \boldsymbol{p}_{ij+1})$ $(1\leqslant i\leqslant t,1\leqslant j\leqslant 2n_i)$ 秘密分发给第 i 个集合的参与者 B_{ij}。其中，x_i 是公开的。

最后，秘密参与者 B_{ij} 在得到子密钥 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 后，必须先验证子密钥的真实性。将 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 输入到黑盒中，判断是否满足① $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 线性无关；②$\lambda_i=\lambda_{ij}=\lambda_{ij+1}$。如果满足这 2 个条件，说明参与者得到子密钥是正确的，否则，则要求密钥分发者 D 重新分发子密钥，直到满足条件为止。

4.2.4　秘密恢复

本文方案要求恢复秘密参与者的人数不少于门限值 t，即每个参与者集合必须至少出一个人。

首先，为了保证恢复秘密的所有参与者提供的子密钥的真实性，在恢复秘密之前，需要每个参与者将自己手中的密钥 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 都要在黑盒子中进行验证。

① $\lambda_i=\lambda_{ij}=\lambda_{ij+1}$。

② $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 线性无关。

只有同时满足上述 2 个条件才可以进行下一步操作，否则，停止密钥恢复工作。

其次，假设集合 B_1 中参与密钥恢复的参与者为 B_{11}，其提供的子密钥是 $(x_1,\boldsymbol{p}_{11})$ 和 $(x_1,\boldsymbol{p}_{12})$。集合 B_2 中参与密钥恢复的参与者为 B_{21}，其提供的子密钥是 $(x_2,\boldsymbol{p}_{21})$ 和 $(x_2,\boldsymbol{p}_{22})$，依次类推，集合 B_t 中参与密钥恢复的参与者为 B_{t1}，其提供的子密钥是 $(x_t,\boldsymbol{p}_{t1})$ 和 $(x_t,\boldsymbol{p}_{t2})$。他们在黑盒子中输入自己提供的子密钥，分别得到所对应的特征值 λ_i。

最后，将 $(x_1,\ \lambda_1),(x_2,\ \lambda_2),\cdots,(x_t,\ \lambda_t)$ 代入方程 $f(x)\equiv K+a_1x+\cdots+a_{t-1}x^{t-1}(\mathrm{mod}\ p)$，得到方程

$$\begin{cases} f(x_1)=K+a_1\cdot x_1+\cdots+a_{t-1}\cdot x_1^{t-1}=\lambda_1 \\ f(x_2)=K+a_1\cdot x_2+\cdots+a_{t-1}\cdot x_2^{t-1}=\lambda_2 \\ \vdots \\ f(x_t)=K+a_1\cdot x_t+\cdots+a_{t-1}\cdot x_t^{t-1}=\lambda_t \end{cases} \tag{6}$$

由于 $f(x)$ 是 t–1 次曲线，如果知道 t 个点 (x_i,λ_i) $(1\leqslant i\leqslant t)$，曲线就可以按式(2)表达出来，而共享密钥 $K\equiv f(0)\ (\mathrm{mod}\ p)$。

5　方案分析

从正确性、完善安全性和欺诈检测这 3 个方面来分析本文方案。

5.1　正确性证明

命题 1　在参与者诚实而正确地执行方案的前提下，任意合法的授权子集都可以恢复密钥 K。

证明　设 G 是一个最小授权子集，$G=\{\boldsymbol{p}_{11},\boldsymbol{p}_{12},\boldsymbol{p}_{21},\boldsymbol{p}_{22},\cdots,\boldsymbol{p}_{t1},\boldsymbol{p}_{t2}\}$。在黑盒子中输入子密钥 $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 后即可得到集合 $H=\{\lambda_1,\lambda_2,\cdots,\lambda_t\}$，从而得到式(6)，则系数矩阵为

$$\boldsymbol{M}=\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_t & \cdots & x_t^{t-1} \end{pmatrix}$$

$\boldsymbol{M}$ 可以看成一个 $t\times t$ 范德蒙矩阵，则它的行列式 $N=\prod_{t\geqslant m>n\geqslant 1}(x_m-x_n)$。因为 $x_1,x_2,\cdots,x_t$ 互不相等，所以 $N\neq 0$。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 $f(x)$。证毕。

实质上，本文方案的正确性是建立在 Shamir 门限方案正确性的基础上的。

5.2　完善安全性证明

命题 2　当 G 中参与者总数不够时，无法恢复密钥 K。

证明　假设参与者有 m 个 $(m<t)$。参与者必须通过 m 个方程求解 t 个未知数，由线性方程组解的基本知识可知，其中至少有 t–m 个自由变量，则能得到正确秘密的概率最大为 $\frac{1}{q^{t-m}}$，与穷举无异，所以无法恢复密钥 K。证毕。

5.3　欺诈检测

5.3.1　检验密钥分发者是否可靠

命题 3　各参与者在收到子秘密之后，可通过式(3)检验密钥分发者是否可靠。

证明 在密钥分发阶段，本文方案要求密钥分发完毕后，参与者首先将得到的 2 种子密钥在黑盒子中进行验证。如果满足① $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 线性无关；② $\lambda_i=\lambda_{ij}=\lambda_{ij+1}$，则说明密钥分发者是诚实的，否则，说明密钥分发者存在欺诈行为。证毕。

5.3.2 *检测参与者是否诚实*

命题 4 在秘密恢复阶段，也可通过式(3)检验参与者是否诚实。

证明 在密钥恢复阶段，本文方案要求恢复密钥的参与者首先提供 2 种子密钥，然后将子密钥输入黑盒子中，最后将结果反馈给所有参与秘密恢复的参与者。如果满足① $\boldsymbol{p}_{ij}$ 和 $\boldsymbol{p}_{ij+1}$ 线性无关；② $\lambda_i=\lambda_{ij}=\lambda_{ij+1}$，则说明该参与者是诚实的，反之，则说明该参与者存在欺诈行为，可以对其进行责任追究。证毕。

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

6 方案的具体应用

下面用一个例子说明本文方案的可行性。

例 设有 B_1、B_2 这 2 个集合，集合 B_1 中有一个参与者 B_{11}，集合 B_2 中有一个参与者 B_{21}。为这 2 个用户分配密钥，并分析重构密钥 K 的过程。

1) 参数选取

密钥分发者随机选取一个素数 p=13，主密钥 K=3，a_1=4，得到多项式 $s(x)\equiv 3+4x(\mathrm{mod}\ 13)$。

2) 秘密分割

密钥分发者取 $\lambda_1=s(x_1)=s(3)=2$，$\lambda_2=s(x_2)=s(6)=1$。

得到对角矩阵为

$$\boldsymbol{\Lambda}=\begin{pmatrix}2&0&0&0\\0&2&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

黑盒子生成的 4 阶随机可逆矩阵 $\boldsymbol{P}$ 为

$$\boldsymbol{P}=\begin{pmatrix}1&1&0&1\\1&0&1&0\\1&0&0&0\\0&1&0&0\end{pmatrix}$$

生成矩阵 $\boldsymbol{A}$ 为

$$\boldsymbol{A}=\begin{pmatrix}1&0&1&1\\0&1&1&0\\0&0&2&0\\0&0&0&2\end{pmatrix}$$

其中，λ_1 对应的特征向量为 $\boldsymbol{p}_{11}=(1\ \ 1\ \ 1\ \ 0)^{\mathrm{T}}$ 和 $\boldsymbol{p}_{12}=(1\ \ 0\ \ 0\ \ 1)^{\mathrm{T}}$，$\lambda_2$ 对应的特征向量为 $\boldsymbol{p}_{21}=(0\ \ 1\ \ 0\ \ 0)^{\mathrm{T}}$ 和 $\boldsymbol{p}_{22}=(1\ \ 0\ \ 0\ \ 0)^{\mathrm{T}}$。可得 2 个子密钥 $k_{11}=(3,\boldsymbol{p}_{11})\cup(3,\boldsymbol{p}_{12})$，$k_{21}=(2,\boldsymbol{p}_{21})\cup(2,\boldsymbol{p}_{22})$。分别将 k_{11}、k_{21} 分发给集合 B_1 中的参与者 B_{11} 和集合 B_2 中的参与者 B_{21}。

3) 秘密恢复

假设持有子密钥 k_{11}、k_{21} 的1+1个参与者参与主密钥恢复工作，他们首先将自己手中的 2 种子密钥输入黑盒子中，假设参与密钥恢复的秘密参与成员提供的子密钥是正确的，则有 $\lambda_1=\lambda_{11}=\lambda_{12}=2$，$\lambda_2=\lambda_{21}=\lambda_{22}=1$，满足密钥恢复的条件，可以重构 $f(x)$。式子的两项分别为

$$2\frac{(x-6)}{(3-6)}=11\frac{(x-6)}{(-3)}=2(x-6)\cdot((-3)^{-1}\ \mathrm{mod}13)$$
$$=2(x-6)\times 4=8(x-6)$$
$$1\frac{(x-3)}{(6-3)}=1\frac{(x-3)}{3}=(x-3)(3^{-1}\ \mathrm{mod}13)$$
$$=(x-3)9=9(x-3)$$

所以，有

$$f(x)\equiv[8(x-6)+9(x-3)]\ \mathrm{mod}13$$
$$=(17x-75)\ \mathrm{mod}13=3+4x$$

所以 K=3，从而获得共享密钥。

7 结束语

本文提出了一种基于特征值的可验证的特殊门限秘密共享方案。方案中的每个参与者需持有 2 种子密钥，其优点是可以有效地保证密钥分发者分发子密钥的真实性和参与者提供子密钥的真实性。同时，本文方案利用黑盒子的设计理念，使方案的密钥分发者和参与者可以进行互相认证，实现了防欺诈功能。本文方案的贡献还在于，从特征值的角度出发设计了一种可验证的秘密共享方案。

参考文献：

[1] SHAMIR A. How to share a secret[J]. Communication ACM, 1979, 22(11): 612-613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C]//IEEE Computer Society. 1979: 313.

[3] ASMUTH C, BLOOM J. A modular approach to key safeguarding[J]. IEEE Transactions on Information Theory, 1983, 29(2):208-210.

[4] KARNIN E D, GREENE J, HELLMAN M E. On secret sharing systems[J]. IEEE Transactions on Information Theory, 1983, 29(1):35-41.

[5] CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]// Symposium on Foundations of Computer Science.2008:383-395.

[6] LIU C J, LI Z H, BAI C M, et al. Quantum-secret-sharing scheme based on local distinguishability of orthogonal seven-qudit entangled states[J]. International Journal of Theoretical Physics, 2018, 57(3):1-15.

[7] XU T T, LI Z H, BAI C M, et al. A new improving quantum secret sharing scheme[J]. International Journal of Theoretical Physics, 2017, 56:1-10.

[8] SINGH N, TENTU A N, BASIT A, et al. Sequential secret sharing scheme based on Chinese remainder theorem[C]// IEEE International Conference on Computational Intelligence and Computing Research. 2017:1-6.

[9] SONG Y, LI Y, WANG W. 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.

[10] PILARAM H, EGHLIDOS T, PILARAM H, et al. A lattice-based changeable threshold multi-secret sharing scheme and its application to threshold cryptography[J]. Scientia Iranica, 2017, 24(3):1448-1457.

[11] 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. 2017:556-563.

[12] ZHANG T, KE X, LIU Y. (*t*, *n*) multi-secret sharing scheme extended from Harn-Hsu's scheme[J]. Eurasip Journal on Wireless Communications & Networking, 2018, 2018(1):71.

[13] YUAN D, HE M, ZENG S, 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. 2017:269-275.

[14] 李滨. 基于特殊访问权限的差分秘密共享方案[J]. 四川大学学报(自然科学版), 2006(1): 78-83.
LI B. Differential secret sharing scheme based on special access permissions[J]. Journal of Sichuan University (Natural Science Edition), 2006(1): 78-83.

[15] 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.
School of Mathematic Sciences, Tongji University . Engineering mathematics, linear algebra[M]. Beijing: Higher Education Press. 2014.

[16] 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 E Q, ZHANG Y, CAO Y ,et al. A technique of locking a disk and secreting a whole disk[J]. Journal of Changchun Post & Telecommunication Institute, 1991(3):11-14.

[作者简介]

张艳硕（1979−），男，陕西宝鸡人，博士，北京电子科技学院讲师，主要研究方向为密码理论及其应用。

李文敬（1992−），女，山东济宁人，北京电子科技学院硕士生，主要研究方向为信息安全。

陈雷（1992−），男，河北邯郸人，北京电子科技学院硕士生，主要研究方向为信息安全。

毕伟（1980−），男，黑龙江哈尔滨人，博士，中思博安科技（北京）有限公司研究员，主要研究方向为信息安全和区块链技术。

杨涛（1977−），男，安徽芜湖人，博士，公安部第三研究所副研究员，主要研究方向为信息安全。