Available online at www.ijournalse.org

Emerging Science Journal

Vol. 4, No. 4, August, 2020

A Study on Multisecret-Sharing Schemes Based on Linear Codes

Selda Çalkavur [a*]

[a] *Kocaeli University, Faculty of Science, Math Department, 41380, Kocaeli, Turkey*

Abstract

Secret sharing has been a subject of study since 1979. In the secret sharing schemes there are some participants and a dealer. The dealer chooses a secret. The main principle is to distribute a secret amongst a group of participants. Each of whom is called a share of the secret. The secret can be retrieved by participants. Clearly the participants combine their shares to reach the secret. One of the secret sharing schemes is $a(t,n)-$ threshold secret sharing scheme. A $a(t,n)-$ threshold secret sharing scheme is a method of distribution of information among n participants such that $t \geq 1$ can recover the secret but $(t-1)$ cannot. The coding theory has been an important role in the constructing of the secret sharing schemes. Since the code of a symmetric $(v,k,\lambda)-$ design is a linear code, this study is about the multisecret-sharing schemes based on the dual code $C^{\perp}$ of F_2- code C of a symmetric $(v,k,\lambda)-$ design. We construct a multisecret-sharing scheme Blakley's construction of secret sharing schemes using the binary codes of the symmetric design. Our scheme is a threshold secret sharing scheme. The access structure of the scheme has been described and shows its connection to the dual code. Furthermore, the number of minimal access elements has been formulated under certain conditions. We explain the security of this scheme.

Keywords:

Secret Sharing;
Multisecret-Sharing;
Linear Code;
Symmetric Design.

Article History:

Received:	12	May	2020
Accepted:	09	July	2020
Published:	01	August	2020

1- Introduction

A secret sharing scheme is a process of distributing a secret to a set of participants in such a way that only certain subsets of them can determine the secret. The set of all subsets which can determine the secret is called the access structureof the scheme. Secret sharing chemes were introduced in 1979 [1, 2] and then different schemes were constructed. It was given a general introduction to secret sharing schemes in Stinson (1992) study [3]. An important class of secret sharing schemes is those which are based on linear codes. The relation between secret sharing schemes and linear codes was first presented in McEliece and Sarwate (1981) research [4]. Massey (1993) [5] used to linear codes to construct the secret sharing schemes. The access structure of schemes based on self-dual codes was analyzed in Dougherty et al. (2008) research using some properties of the codes [6].

Multisecret-sharing scheme is the other family of secret sharing schemes. This scheme was proposed in Harn (1995), He and Dawson (1994) and Li et al. (2005) studies [7-9]. Moreover, some authors were worked on multisecret-sharing scheme in Pang and Wang (2005) and Bai (2006) studies [10, 11]. In the multisecret-sharing schemes [9-11] there is a set of secrets can be shared at once or all p secrets cannot reconstruct. To recover the secret the participants need to submit a $pseudo-share$ computed from their secret share instead of the secret share itself.

Secret sharing schemes have been working recently. Especially we constructed a multisecret-sharing scheme based on error correcting codes in Çalkavur and Solé (2015) research [12]. In Alahmadi et al. (2020) [13] we presented a new multisecret-sharing scheme based on LCD codes. We explained some multisecret-sharing schemes over finite fields in Çalkavur and Solé (2020) [14]. Secret sharing schemes based on extension fields were explored in Çalkavur (2018) study [15]. We developed in Molla and Çalkavur (2018) research [16] a new approach to construct secret sharing

* **CONTACT**: Selda.calkavur@kocaeli.edu.tr

DOI: http://dx.doi.org/10.28991/esj-2020-01229

schemes based on field extensions. However, we constructed an image secret sharing method based on Shamir secret sharing in Calkavur (2018) study [17].

There are several known constructions of linear codes as row spaces of incidence matrices of designs. This paper deals with constructions of multisecret-sharing schemes based on binary linear codes of symmetric designs.

In this work we consider a multisecret-sharing scheme of the construction Blakley's method. The next section gives the basic preliminaries used in the paper. The construction is presented in Section 3. In this section we explain the access structure and the number of minimal access elements of the scheme. Section 4 collects concluding remarks.

2- Background and Preliminaries

In this section we give the basic preliminaries and some necessary mathematical information used in this work.

2-1- Linear Codes

Let q be a prime power and denote the finite field of order q by F_q. An $[n,k]-$code C over F_q is a subspace in $(F_q)^n$, where n is length of the code C and k is dimension of C. The dual code of C is defined to be the set of those vectors $(F_q)^n$ which are orthogonal to every codeword of C. It is denoted by $C^{\perp}$. The code $C^{\perp}$ is a $[n, n-k]-$ code. A generator matrix G for a linear code C is a $k \times n$ matrix for which the rows are a basis of C.

Let C be an $[n,k]-$code over F_q with generator matrix G. C contains q^k codewords and can be used to communicate any one of q^k distinct messages. We encode the message vector $x = x_1, x_2, \dots, x_k$ as the codeword xG.

If G is a generator matrix for C, then $C = \{uG | u \in (F_q)^k\}$. $u \to uG$ maps the vector space q^k onto a $k-$ dimensional subspace of $(F_q)^n$.

2-2- Secret Sharing

Secret sharing refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use their own.

In one type of secret sharing scheme there is one dealer and players. The dealer gives a share of the secret to the players, but only when specific conditions are fulfilled will the players be able to reconstruct the secret from their shares. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than players can such a system is called a $(t,n)-$threshold scheme.

Shamir's secret sharing method is an old cryptography algorithm. This scheme is a $(t,n)-$threshold scheme. Shamir's scheme was based on polynomial interpolation. Blakley's scheme is also a $(t,n)-$threshold scheme. Blakley uses hyperplane geometry to solve the secret sharing problem.

2-3- Symmetric Designs

A symmetric $(v,k,\lambda)-$design consists of a set of P of v points and a set of v subsets of P called blocks such that

1. Each block contains exactly k points,
2. Each point lies in exactly k blocks,
3. Each pairs of points occurs together in exactly λ blocks,
4. Intersection of each pair of blocks contain exactly λ points.

In a symmetric $(v,k,\lambda)-$ design the value $(k-\lambda)$ is called n the order of a symmetric $(v,k,\lambda)-$ design, where $n = k-\lambda$. The incidence matrix $A = [a_{ij}]$ of a symmetric $(v,k,\lambda)-$design is the $v \times v$ matrix whose rows are indexed by blocks and whose columns are indexed by points. The entries of matrix are defined as follows.

- $a_{ij} = 1$, if j^{th} point is in i^{th} block
- $a_{ij} = 0$, otherwise

Proposition 1.

If A is the incidence matrix of a symmetric $(v,k,\lambda)-$ design, then $|\det A| = k(k-\lambda)^{\frac{v-1}{2}}$ [18].

The F_q- code of a symmetric $(v,k,\lambda)-$design is a subspace of $(F_q)^v$ generated by the incidence matrix A of the symmetric design. The extended F_q- code $C^{ext.}$ of a symmetric $(v,k,\lambda)-$design is a code generated by the rows of the extended matrix is:

$$B=\begin{pmatrix} & & \vdots & 1 \\ & & \vdots & \vdots \\ & A & \vdots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ \lambda & \cdots & \lambda & k \end{pmatrix}.$$

3- Multisecret-Sharing Schemes Based on the Dual Code of the Binary Code of a Symmetric $(v,k,\lambda)-$Design

3-1- Scheme Description

The code of a symmetric $(v,k,\lambda)-$design is also linear code. It is known that every linear code can be used to construct the secret sharing schemes. In this section we examine a multisecret-sharing scheme based on the dual code of the binary code of a symmetric $(v,k,\lambda)-$design. Let:

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1v} \\ a_{21} & a_{22} & \cdots & a_{2v} \\ \vdots & \vdots & \cdots & \vdots \\ a_{v1} & a_{v2} & \cdots & a_{vv} \end{pmatrix}$$

be a $v\times v$ incidence matrix of a symmetric $(v,k,\lambda)-$design. The F_2- code C of a symmetric $(v,k,\lambda)-$design is a subspace of $(F_2)^{\mathrm{v}}$ generated by the rows of the incidence matrix A of the symmetric design.

Let $G=(g_0,g_1,\dots,g_{v-1})$ be a generator matrix of C, where $g_0,g_1,\dots,g_{v-1}$ are column vectors of C. So:

$$G=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1v} \\ g_{21} & g_{22} & \cdots & g_{2v} \\ \vdots & \vdots & \cdots & \vdots \\ g_{r1} & g_{r2} & \cdots & g_{rv} \end{pmatrix}$$

is a $r\times v$ matrix. Now we construct a multisecret-sharing scheme based on $C^{\perp}$, where $C^{\perp}$ is the dual code of the binary code C of a symmetric $(v,k,\lambda)-$design.

Let $(F_2)^v$ be the secret space and a vector in subspace of $(F_2)^{\mathrm{v}}$ be the secret. Let C be a $[v,r]-$code over F_2 generated by a symmetric $(v,k,\lambda)-$design and $C^{\perp}$ be an $[v,v-r]-$code over F_2.

3-2- Proposed Method

Consider the matrix:

$$G^{\perp}=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1v} \\ g_{21} & g_{22} & \cdots & g_{2v} \\ \vdots & \vdots & \cdots & \vdots \\ g_{(v-r)1} & g_{(v-r)2} & \cdots & g_{(v-r)v} \end{pmatrix},$$

Where $G^{\perp}$is a generator matrix of $C^{\perp}$. Let any element of $C^{\perp}$ be the secret $=(s_1,s_2,\dots,s_v)$. All of rows of generator matrix $G^{\perp}$ are minimal access elements and all of codewords of $C^{\perp}$ are participants in this scheme. We consider the row vectors of $G^{\perp}$ to calculate the shares y_i, $i=1,2,\dots,v$.

$$Y^T=G.S^T$$

We write the following linear equation system for each participant.

$$\begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_{v-r} \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_v \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{v-r} \end{pmatrix}$$

It can reach by solving this equation system.

Theorem 1.

In this multisecret-sharing scheme we have the following.

1) The access structure consists of the $(v-r)$ elements.
2) No element of number less than $(v-r)$ can be used in recovering the secret.

Proof.

1) The secret is recovered thanks to the rows of $G^{\perp}$ and their number is $(v-r)$.
2) The number of rows of $G^{\perp}$cannot be less than $(v-r)$ by definition. Otherwise the secret cannot be reached. So only $(v-r)$ elements can be used to recover the secret but $(v-r-1)$ cannot.

Corollary 1.

The multisecret-sharing scheme satisfying the hypothesis of the above theorem is also a $(v-r,\ 2^{v-r})-$ threshold secret sharing scheme.

Proof.

It is clear that the participants are all of elements of $C^{\perp}$ and their number is 2^{v-r}. The $(v-r)$ out of 2^{v-r} participants can be reached the secret by combining their shares.

3-3- Statistics on Coalitions

Theorem 2.

Let C be an $[v,r]-$ code over F_2 generated by a symmetric $(v,k,\lambda)-$design, where v is the length of C and r is dimension of C. In a multisecret-sharing scheme based on $C^{\perp}$ the number of minimal coalitions is $\binom{2^{v-r}}{v-r}$, where $C^{\perp}$ is the dual code of C.

Proof.

Recall that our scheme is a $(v-r,\ 2^{v-r})-$threshold scheme. This means $(v-r)$ out of 2^{v-r} participants can recover the secret. These $(v-r)$ participants consist of minimal access sets. So the number of minimal coalitions is $\binom{2^{v-r}}{v-r}$.

Theorem 3.

Suppose that C is F_2- code of a symmetric $(v,k,\lambda)-$design D. If $2\,|\,(k-\lambda)$, then there are altogether m minimal access elements in the multisecret-sharing scheme based on $C^{\perp}$ of C and m satisfy the inequality $\frac{1}{2}(v-1) \le m \le (v-2)$.

Proof.

If C is the F_2- code of a symmetric $(v,k,\lambda)-$design D and $2|(k-\lambda)$, then:

$$2 \le \dim C \le \frac{1}{2}(v+1) \ [20] \tag{1}$$

First we have to give the proof of this statement. Suppose that $2|(k-\lambda)$. If $2|k$, then we find that $2|k$. So the scalar product of any two blocks is equal to zero since the F_2-code C of D is generated by the blocks of D and C is self-orthogonal $(C \subseteq C^{\perp})$ with respect to Euclidean scalar product [18]. Therefore we obtain $\dim C \le v - \dim C$, $\dim C \le \frac{v}{2}$.

If $2|(k-\lambda)$, but $2 \nmid k$. Then consider $x=(x_1x_2\cdots x_vx_{v+1})$ and $y=(y_1y_2...y_vy_{v+1})$ be any two rows vectors of *B*, where *B* is the extended incidence matrix of a symmetric $(v,k,\lambda)-$design.

$\psi(x,y)=x_1y_1+\cdots+x_vy_v-\lambda x_{v+1}y_{v+1}$ is a bilinear form [18].

There are four options for x and y:

1) $x=(x_1,x_2,\cdots,x_v,1)$ and $y=(y_1,y_2,\cdots,y_v,1)$;

2) $x=(x_1,x_2,\cdots,x_v,1)$ and $y=(\lambda,\lambda,\cdots,\lambda,k)$;

3) $x=(\lambda,\lambda,\cdots,\lambda,k)$ and $y=(y_1,y_2,\cdots,y_v,1)$;

4) $x=(\lambda,\lambda,\cdots,\lambda,k)$ and $y=(\lambda,\lambda,\cdots,\lambda,k)$.

For the case 1) $\psi(x,y)=\lambda-\lambda.1.1=0$.

For the case 2) $\psi(x,y)=\lambda.k-\lambda.k=0$.

For the case 3) $\psi(x,y)=\lambda.k-\lambda.k\equiv 0 \pmod 2$.

For the case 4) $\psi(x,y)=v.\lambda^2-\lambda.k^2=\lambda(\lambda-k)\equiv 0 \pmod 2$.

The scalar products of two blocks are equal to 0 (mod 2). Therefore $\dim C^{ext.}\le\frac{v+1}{2}$.
Now we have to prove that $\dim C=\dim C^{ext.}$.

If $2 \nmid k$ The sum of first *v* columns of *B* is equal to $[k,\cdots,k,v\lambda]^T$. It is obtained that:

$k^{-1}[k,\cdots,k,v\lambda]^T=[1,\cdots,1,v\lambda k^{-1}]^T \pmod 2$ from $v\lambda k^{-1}\equiv(k^2-k+\lambda)k^{-1} \pmod 2 \equiv k \pmod 2$.

The last column of *B* is equal to $-k$ times of the sum of first *v* columns of *B* with respect to modulo 2. On the other hand the sum of first v rows of *B* is equal to $[k,k,\cdots,k,v]$. So $\lambda k^{-1}[k,k,\cdots,k,\lambda]\equiv[\lambda,\lambda,\cdots,\lambda,k] \pmod 2$.

Hence the last row of *B* is equal to λk^{-1} times the sum of first v rows of *B*. Therefore we obtain the last row of *B* is a linear combination of first v rows of *B* and also the last column of *B* is the linear combination of first *v* columns of *B*. We conclude that $rankA=rankB$, so $\dim C=\dim C^{ext.}$; $\dim C\le\frac{v+1}{2}$.

It is also clear that $\dim C\ge 2$ [18].

By Theorem 1, there are altogether $(v-r)=\dim C^{\perp}$ minimal access elements in the multisecret-sharing scheme based on $C^{\perp}$.

Now we consider the inequality (1).

$$2\le\dim C\le\frac{1}{2}(v+1).$$

Since $\dim C=v-\dim C^{\perp}$,

$$2\le v-\dim C^{\perp}\le\frac{1}{2}(v+1) \tag{2}$$

$$(2-v)\le-\dim C^{\perp}\le\frac{1}{2}(1-v) \tag{3}$$

$$\frac{1}{2}(v-1)\le\dim C^{\perp}\le(v-2) \tag{4}$$

$$\frac{1}{2}(v-1)\le m\le(v-2) \tag{5}$$

Theorem 4.

Let *C* be F_2-code of a symmetric $(v,k,\lambda)-$design *D*. If $2 \nmid (k-\lambda)$ and $2|k$, then in the multisecret-sharing scheme based on $C^{\perp}$ of F_2-code *C* of *D* there are altogether 1 minimal access elements.

Proof.

If *C* is F_2-code of a symmetric $(v,k,\lambda)-$design *D* and $2 \nmid (k-\lambda)$ and $2|k$, then $\dim C=v-1$ [20]. First we will prove it.

Suppose that $2 \nmid (k-\lambda)$ and $2|k$. Every row of *A* is orthogonal to (1, 1,…, 1) with respect to the scalar product:

$(x_1, x_2, \cdots, x_v).(1,1,\cdots,1) = x_1 + x_2 + \cdots + x_v = k \equiv 0 \pmod 2$:

Thus $\dim C \le v-1$.

The sum all of rows containing 0 in the i^{th} column is the vector $(k-\lambda, \cdots, k-\lambda, 0, k-\lambda, \cdots, k-\lambda)$, where the 0 is in the i^{th} column. These vectors generate the $(v-1)-$dimensional subspace of $(F_2)^v$.

By Theorem 1, there are altogether $(v-r) = \dim C^{\perp}$ minimal access elements in the multisecret-sharing scheme based on $C^{\perp}$. If we combine these results, then we obtain there are altogether $\dim C^{\perp} = v - \dim C = v - (v-1) = 1$ minimal access elements.

Theorem 5.

Let C be F_2-code of a symmetric $(v, k, \lambda)-$design D. If $2 \nmid (k-\lambda)$ and $2 \nmid k$, then in the multisecret-sharing scheme based on $C^{\perp}$ of F_2-code C of D there is no minimal access element.

Proof.

This is similar to the proof of Theorem 4. If C is F_2-code of a symmetric $(v, k, \lambda)-$design D and $2 \nmid (k-\lambda)$ and $2 \nmid k$, then $\dim C = v$ [18]. Now we will prove it.

Suppose that $2 \nmid (k-\lambda)$ and $2 \nmid k$. By Proposition 1, $|\det A| = k(k-\lambda)^{\frac{v-1}{2}}$.

Thus the matrix A is invertible over F_2. Hence $\dim C = v$. We combine this result with Theorem 1. So we obtain:

$$\dim C^{\perp} = v - \dim C = v - v = 0$$

This means there is no minimal access element. In this case, the secret cannot be reached.

Example 1.

Consider the symmetric $(7, 3, 1)-$symmetric design, where $v = 7, k = 3, \lambda = 1$. The set of points is $P = \{0, 1, 2, 3, 4, 5, 6\}$ and the blocks are $B_1 = \{0, 1, 3\}$, $B_2 = \{1, 2, 4\}$, $B_3 = \{2, 3, 5\}$, $B_4 = \{3, 4, 6\}$, $B_5 = \{4, 5, 0\}$, $B_6 = \{5, 6, 1\}$, $B_7 = \{6, 0, 2\}$.

The incidence matrix of this design is:

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

The F_2-code C of the symmetric $(7, 3, 1)-$design is a subspace of $(F_2)^7$ generated by the rows of the incidence matrix A.

$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ is a generator matrix of C. The codewords of C are $\{1101000, 0110100, 0011010, 0001101, 1000110, 0100011, 1010001, 0101110, 0010111, 1001011, 1100101, 1110010, 0111001, 1011100, 0000000, 1111111\}$.

We examine a multisecret-sharing scheme based on the dual code of the binary code of the symmetric $(7, 3, 1)-$design. C is the binary $[7, 4]-$code. The dual code of $C^{\perp}$ of C is a linear $[7, 3]-$code. So $|C^{\perp}| = 2^3 = 8$.

$G^{\perp} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ is a generator matrix of $C^{\perp}$. The codewords of $C^{\perp}$ are $\{0101110, 0010111, 1001011, 1100101, 1110010, 0111001, 1011100, 0000000\}$.

Let the secret vector be $S = (1101000)$. We calculate the shares as follows.

$$y_1^T = g_1.S^T = (0101110).(1101000) = 0$$
$$y_2^T = g_2.S^T = (1100101).(1101000) = 0$$
$$y_3^T = g_3.S^T = (0010111).(1101000) = 0$$

The participants (the rows of $G^{\perp}$) can reach the secret by combining their shares as below:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}. \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

It is seen that the secret $S = (1101000)$ by solving the above linear system. This scheme is also a $(3, 8) -$ threshold secret sharing scheme.

3-4- Security Analysis

Our scheme has been constructed based on the dual code of $F_2 -$ code of a symmetric $(v, k, \lambda) -$design. We use Blakley's method. The secret can be reached by the rows of generator matrix of the dual code. It is needed the following linear equation system.

$$G^{\perp}.S^T = Y^T$$

This system has always a solution and it is not easy to find it. Also it has a unique solution since we work over F_2. So the multisecret-sharing scheme is attractive in against cheating. This scheme is more resilient to algebraic attacks due to the reconstruction algorithm.

Moreover, one of the basic parameters in secret sharing is information rate ρ of the scheme, which is defined to be the ratio between the length (in bits) of the secret and the maximum length of the shares given to the participants. That is $\rho = \frac{\log |K|}{\max \log |S_p|}$ [19].

A secret sharing scheme is said to be ideal if its information rate is equal to one, which is the maximum possible value.

$\rho = \frac{\log v}{\max \log(v - r)}$ for our scheme. If the shares are too large, the memory requirements for the participants will be too strong and the algorithms used to compute the shares will become inefficient. $\rho > 1$ since $v > v - r$. By the above information this scheme is too strong to the possible attacks.

3-5- Comparison with Other Schemes

In this section, we compare our scheme with other secret sharing scheme. We denote the number of participants, the size of a secret, the number of coalitions for arithmetic over F_q by M, R, T in the following table. We consider a $[n, k, d \geq 2t + 1] -$ code over F_q and an $[v, r] -$code over F_2 generated by a symmetric $(v, k, \lambda) -$design.

Massey (1993) [5] has a single secret sharing scheme and constructed it based on linear codes. Ding et al. (1997) [20] used to linear algebra. In Çalkavur et al. [12] scheme, it is used to decoding to explain the reconstruction

algorithm. We use Blakley's method to recover the secret in the new scheme. Since the system has a unique solution, it is very difficult to find the secret by attackers. So our new system is too safe.

Table 1. Comparison with other schemes.

System	Massey (1993) [5]	Ding et al. (1997) [20]	Çalkavur and Solé (2015) [12]	This paper
M	$n-1$	n	n	2^{v-r}
R	q	q^k	q^k	2^{v-r}
T	$\binom{n}{k}$	$\binom{n}{k}$	$\geq \binom{n}{d-t}$	$v-r$
ρ	1	$\frac{k}{k-1}$	1	>1

4- Conclusion

In the present article, we have introduced a new multisecret-sharing scheme based on the dual code of the binary code of a symmetric (v,k,λ) −design. The reconstruction algorithm is based on Blakley's method. We determine the access structure and calculate the information rate of this scheme. We give the number of minimal access elements under certain conditions. We compare our scheme with the other schemes in the literature. The new system stands well, in terms of security.

5- Acknowledgments

I would like to thank to Dr. Patrick Solé for his valuable ideas.

6- Conflict of Interest

The author declares that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Blakley, G. R. "Safeguarding Cryptographic Keys." 1979 International Workshop on Managing Requirements Knowledge (MARK) (June 1979). doi:10.1109/mark.1979.8817296.

[2] Shamir, Adi. "How to Share a Secret." Communications of the ACM 22, no. 11 (November 1, 1979): 612–613. doi:10.1145/359168.359176.

[3] Stinson, D. R. "An Explication of Secret Sharing Schemes." Designs, Codes and Cryptography 2, no. 4 (December 1992): 357–390. doi:10.1007/bf00125203.

[4] McEliece, R. J., and D. V. Sarwate. "On Sharing Secrets and Reed-Solomon Codes." Communications of the ACM 24, no. 9 (September 1, 1981): 583–584. doi:10.1145/358746.358762.

[5] Massey, James L. "Minimal codewords and secret sharing." In Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, (1993): 276-279.

[6] Dougherty, Steven T., Sihem Mesnager, and Patrick Sole. "Secret-Sharing Schemes Based on Self-Dual Codes." 2008 IEEE Information Theory Workshop (May 2008). doi:10.1109/itw.2008.4578681.

[7] Harn, L. "Comment on" Multistage secret sharing based on one-way function"." Electronics Letters 31, no. 4 (1995): 262. doi:10.1049/el:19950201.

[8] He, Jingmin, and Edward Dawson. "Multistage secret sharing based on one-way function." Electronics Letters 30, no. 19 (1994): 1591-1592. doi:10.1049/el:19941076.

[9] Li, HuiXian, ChunTian Cheng, and LiaoJun Pang. "A New (t, N)-Threshold Multi-Secret Sharing Scheme." Lecture Notes in Computer Science (2005): 421–426. doi:10.1007/11596981_61.

[10] Pang, Liao-Jun, and Yu-Min Wang. "A New (t,n) Multi-Secret Sharing Scheme Based on Shamir's Secret Sharing." Applied Mathematics and Computation 167, no. 2 (August 2005): 840–848. doi:10.1016/j.amc.2004.06.120.

[11] Bai, Li. "A Reliable (k, N) Image Secret Sharing Scheme." 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (2006). doi:10.1109/dasc.2006.11.

[12] Çalkavur, Selda, and Patrick Solé. "Multisecret-Sharing Schemes and Bounded Distance Decoding of Linear Codes." International Journal of Computer Mathematics 94, no. 1 (October 16, 2015): 107–114. doi:10.1080/00207160.2015.1091071.

[13] Alahmadi, Adel, Alaa Altassan, Ahmad AlKenani, Selda Çalkavur, Hatoon Shoaib, and Patrick Solé. “A Multisecret-Sharing Scheme Based on LCD Codes.” Mathematics 8, no. 2 (February 18, 2020): 272. doi:10.3390/math8020272.

[14] Çalkavur, Selda, and Patrick Solé. “Some Multisecret-Sharing Schemes over Finite Fields.” Mathematics 8, no. 5 (April 25, 2020): 654. doi:10.3390/math8050654.

[15] Çalkavur, Selda. “Secret Sharing Schemes Based on Extension Fields.” European Journal of Pure and Applied Mathematics 11, no. 2 (April 27, 2018): 410–416. doi:10.29020/nybg.ejpam.v11i2.3226.

[16] Molla, Fatih, and Selda Çalkavur. “A New Approach to Construct Secret Sharing Schemes Based on Field Extensions.” European Journal of Pure and Applied Mathematics 11, no. 2 (April 27, 2018): 468–475. doi:10.29020/nybg.ejpam.v11i2.3250.

[17] Calkavur, Selda. “An Image Secret Sharing Method Based on Shamir Secret Sharing.” Current Trends in Computer Sciences & Applications 1, no. 2 (November 20, 2018). doi:10.32474/ctcsa.2018.01.000106.

[18] Lander, E. S. “Symmetric Designs: an Algebraic Approach” Cambridge University (January 20, 1983): 1–41. doi:10.1017/cbo9780511662164.002.

[19] Padró, Carles. “Robust Vector Space Secret Sharing Schemes.” Information Processing Letters 68, no. 3 (November 1998): 107–111. doi:10.1016/s0020-0190(98)00149-5.

[20] Ding, Cunsheng, Tero Laihonen, and Ari Renvall. "Linear multisecret-sharing schemes and error-correcting codes." Journal of Universal Computer Science 3, no. 9 (1997): 1023-1036.