Malaysian Journal of Mathematical Sciences 9(S) June: 89-101 (2015)
Special Issue: The 4th International Cryptology and Information Security Conference 2014 (Cryptology 2014)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

A Construction of Secret Sharing Scheme

***Goh Y. L. and Denis C. K. Wong**

Department of Mathematical and Actuarial Sciences,
University of Tunku Abdul Rahman,
Jalan Sungai Long, Bandar Sungai Long,
Cheras, 43000 Kajang,Selangor, Malaysia

E-mail: gohyl@utar.edu.my

*Corresponding author

ABSTRACT

In this paper, binary linear codes are used to construct the access structures of a secret sharing scheme. The relationship between the minimal codewords of a linear code and the minimal access structure are shown. Furthermore, we generalize the construction of secret sharing scheme by using semisimple group algebra codes. Finally, we study the access structures of a secret sharing scheme based on group algebra code defined by cyclic group of odd prime order over binary field.

Keywords: Secret sharing scheme, linear codes, group algebra codes

1. INTRODUCTION

To keep a secret efficiently and safely, Shamir, 1979 developed the concept of secret sharing scheme which is a rapidly developed field in cryptography. One of the well-known secret sharing scheme is constructed by Shamir, the (n, k) −theshold secret sharing scheme over F_q, which is defined as follows: A secret $s \in F_q$ is split into n shares $s_i \in F_q$ for $i = 1,2, \cdots, n$ in such a way that any k shares uniquely determine the secret but any $k - 1$ or fewer shares provide no information about the secret. McEliece and Sarwate, 1981 improved the (n, k) −theshold secret sharing scheme by introducing the following secret sharing scheme based on linear code: First, choose a $[n, k, n - k + 1] -$ linear MDS code C over F_q. The secret is chosen as the first digit of a codeword $v \in C$. The next $k - 1$ digits are chosen uniformly at random over F_q and the codeword v then computed. The $n-1$ shares are all the digits in v after the first digit. The threshold is k because the digits in any k positions of a codeword in an MDS code uniquely determine the full codeword, that is, any k positions are an information set.

In a more general setting, a secret sharing scheme involved a dealer, denoted by D, who is responsible for selecting a secret k, and then computing the shares s_i from the secret using some systematical algorithm. Other participants form a set P, who will share the secret. Furthermore, let $\tau \subseteq P$ where τ can determine the secret. τ is called the access structure and any subset of τ are called access sets. Recently, many researchers have constructed secret sharing scheme by using linear codes as the theory of algebraic coding theory have been systematically developed (Ashikhmin and Barg, 1998; Ding, Kohel and Ling, 2000; Li, Xue and Lai, 2010; Massey, 1993; Yuan and Ding, 2006).

Algebraic coding theory is important in modern digital communication; however noises might occur during the transmission of digital data across a communication channel. This may cause the received data to differ from the transmitted data. Therefore, error correcting and detecting codes are used in modern digital communication system. The study of group codes as an ideal in a group algebra FG has been developed long time ago (Berman, 1967; Berman, 1989). In 1993, Massey has shown a nice relationship between the access structure and the minimal codewords of the dual code of the underlying code Massey, 1993.

In this paper, a method to construct secret sharing scheme is proposed by using group algebra codes defined over various groups. The paper is organized into four sections. Section 2 introduces the group algebra codes. In section 3, the implementation of secret sharing scheme via group algebra codes are discussed. Finally, some constructions and remarks are given in the last section.

2. SECRET SHARING SCHEME BASED ON LINEAR CODES

Before we start with the construction of secret sharing scheme, we first recall some well-known definitions from error correcting code. A q–ary$[n,k,d]$ –linear code C is a subspace of F_q^n and a generator matrix of C is a $k \times n$ matrix where all rows of G form a basis for C. Any element of C is called a codeword of C.

Furthermore, the $n \times (n-k)$ matrix where all columns of H form a basis for $C^{\perp}$ is called the parity check matrix of C. The support of $v \in F_q^n$ is defined by the set $\{0 \leq i \leq n-1, v_i \neq 0\}$, and say that $w_1 \in F_q^n$ cover $w_2 \in F_q^n$ provided $supp(w_2) \subseteq supp(w_1)$. An element $v \neq 0$ is minimal if it covers its scalar multiples. Furthermore, a codeword whose first component is 1 and only covers its scalar multiples is called a minimal codeword. Clearly, every minimal codeword is a minimal vector. In this section, we show a construction of secret sharing scheme by using the matrices *G* and *H*. Massey, 1993 points out a nice relationship between a minimal codeword and a minimum access structure of a secret sharing scheme. Next, we will illustrate this relationship which is proposed by Massey.

Construction 1: Secret sharing scheme based on a [7,4,3] – binary linear code.

Let C be a [7,4,3] – binary linear code with the following generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Note that *C* is equivalent to the well-known binary Hamming code of length 7. Any codeword *v* in C can be written uniquely in the form

$$v = (v_1, v_2, v_3, v_4, v_1 + v_3 + v_4, v_1 + v_2 + v_4, v_2 + v_3 + v_4),$$

where $(v_1, v_2, v_3, v_4) \in F_2^4$ is the corresponding message word. The parity check matrix of C is

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is well known that $v' \in C$ if and only if $v'H = (0,0,0) \in F_2^3$. Suppose we let $v' = (a, b, c, d, e, f, g)$. Then, the condition $v'H = (0,0,0)$ produces the following system of equations:

$$a + c + d + e = 0 \tag{1}$$
$$a + b + d + f = 0 \tag{2}$$
$$b + c + d + g = 0 \tag{3}$$

From equation (1), we have

$$a = c + d + e. \tag{4}$$

From equation (2), we have

$$a = b + d + f. \tag{5}$$

By adding equations (1) and (3), we obtain

$$a = b + e + g. \tag{6}$$

Finally, by adding equations (2) and (3), we obtain

$$a = c + f + g. \tag{7}$$

Next, we setup the correspondence between each digit in a codeword, and the secret with distributions to participants as shown in Table 1. From equations (4) to (7), we see that the access structure for the secret sharing scheme with the above correspondence based on C are $\{P_2, P_3, P_4\}$, $\{P_1, P_3, P_5\}$, $\{P_1, P_4, P_6\}$ and $\{P_2, P_5, P_6\}$. Now, we consider the [7, 3, 4] – binary dual code $C^\perp$ of C which has the following generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

All codewords of $C^\perp$ are listed in Table 2.

TABLE 1: Correspondence between digits in codeword, secret and participants

Digit in codeword	**Secret and participants**
v_1	Secret
v_2	P_1
v_3	P_2
v_4	P_3
v_5	P_4
v_6	P_5
v_7	P_6

TABLE 2: Codewords in the [7, 3, 4] – binary dual code

$\mathcal{F}_2^3$	$C^{\perp}$
000	0000000
100	1011100
010	1101010
001	0111001
110	0110110
101	1100101
011	1010011
111	0001111

By inspecting through each codeword in $C^{\perp}$ and compare the access structures obtained above, we see that all possible access structures are corresponding to the minimal codeword in $C^{\perp}$ with a “1” in the first position as shown in Table 3.

TABLE 3: Correspondence between minimal codewords and access structure

Minimal codewords in $C^{\perp}$	$\longrightarrow$	Access structure based on C
1011100		$\{P_2, P_3, P_4\}$
1101010		$\{P_1, P_3, P_5\}$
1100101		$\{P_1, P_4, P_6\}$
1010011		$\{P_2, P_5, P_6\}$

Construction 2: Secret sharing scheme based on a binary [9,5,3] – linear code.

Let consider the [9,5,3] – binary code C with the following generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

The corresponding parity check matrix for C is

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

All codewords in $C^{\perp}$ are listed in the Table 4. For all $v = (v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9) \in C$, if we setup the correspondence as shown in Table 5, it follows that the access structure of the secret sharing scheme based on C are $A_1 = \{P_1, P_4, P_5\}$, $A_2 = \{P_1, P_3, P_6\}$, $A_3 = \{P_2, P_3, P_7\}$, $A_4 = \{P_2, P_4, P_8\}$, $A_5 = \{P_2, P_4, P_{5,} P_6, P_7\}$, $A_6 = \{P_2, P_3, P_{5,} P_6, P_8\}$, $A_7 = \{P_1, P_3, P_{5,} P_7, P_8\}$, and $A_8 = \{P_1, P_4, P_{6,} P_7, P_8\}$. Therefore, the minimal access structures are A_1, A_2, A_3 and A_4.

TABLE 4: All codewords in [9, 4, 4] – binary dual code of C

F_2^4	$C^{\perp}$
0000	000000000
1000	110011000
0100	110100100
0010	101100010
0001	101010001
1100	000111100
1010	011111010
1001	011001001
0110	011010110
0101	011110101
0011	000110011
1110	101011110
1101	101101101
1011	110101011
0111	110010111
1111	000001111

TABLE 5: Correspondence between digits in codeword, secret and participants

Digit in codeword	Secret and participants
v_1	Secret
v_2	P_1
v_3	P_2
v_4	P_3
v_5	P_4
v_6	P_5
v_7	P_6
v_8	P_7
v_9	P_8

In general, let $A = \{P_{i_1}, P_{i_2}, \cdots, P_{i_m}\}$ be a minimal access set of the secret sharing scheme based on a [*n*,*k*,*d*] – linear code C. Suppose the columns $g_{i_1}, \cdots, g_{i_m}$ of the generator matrix *G* of C are linear dependent. Then, we have $\sum_{k=1}^{m} \lambda_k g_{i_k} = 0$, where not all λ_j are 0. Without loss of generality, we may assume $\lambda_1 \neq 0$. Thus, we have $g_{i_1} = \sum_{k=2}^{m} \frac{\lambda_k}{\lambda_1} g_{i_k}$. Therefore, the participants $\{P_{i_2}, \cdots, P_{i_m}\}$ can learn the share of P_{i_1} by combining their shares and hence they can recover the secret which is a contradiction. Hence, we known that the columns $g_{i_1}, \cdots, g_{i_m}$ of *G* are linear independent.

Then, there exist a codeword $a = (1,0, \cdots ,0, a_{i_1}, 0, \cdots ,0, a_{i_m}, 0, \cdots ,0)$ $\epsilon C^{\perp}$. This must be truth if not then will contradict the fact that the rows of the parity check matrix *H* of C are also linearly independent. If $a_{i_j} = 0$ for some $j \in \{1, \cdots, m\}$, it follows that $\{P_{i_1}, \cdots, P_{i_{j-1}}, P_{i_{j+1}}, \cdots, P_{i_m}\}$ can recover the secret which contradict the minimality of the access structure A.

Conversely, if $c = (1, \cdots ,0, c_{i_1}, 0, \cdots ,0, c_{i_m}, 0, \cdots ,0)$ is a minimal codeword, it follows that all rows $g_0, g_{i_1}, \cdots, g_{i_m}$ of *G* are linear dependent. Thus, the set of participants $\{P_{i_1}, \cdots, P_{i_m}\}$ can recover the secret. If any proper subset of this can recover the secret, then there exists a nonzero codeword which c properly covers. This contradicts the minimality of c. Therefore, $\{P_{i_1}, \cdots, P_{i_m}\}$ is a minimal acccess set. Thus, we have the following proposition.

Proposition 1. The minimal access structures of a secret sharing scheme based on a $[n, k, d]$ – linear code C is the set of all minimal codewords v of the dual code $C^{\perp}$ of C, where v has a "1" in the first coordinate.

3. SECRET SHARING SCHEME BASED ON GROUP ALGEBRA CODES

Motivated by the construction described in the previous section, we next proposed a secret sharing scheme based on group algebra code.

Let F_q denote a finite field with q elements such that q is a prime. Given a finite group G of order n, the group algebra F_qG is a vector space over F_q, with basis G and so, is isomorphic to F_q^n as a vector space. The group algebra F_qG of G with coefficients in F is the set of all formal sums $\sum_{g\in G} a_g g$, where $a_g \in F$. Addition and multiplication in F_qG are defined as $\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g$ and $\left(\sum_{g\in G} a_g g\right)(\sum_{h\in G} b_h h) = \sum_{h\in G}\sum_{g\in G}(a_g b_h)gh$, respectively. A group algebra code is defined as an ideal of the group algebra F_qG. In particular, if G is a cyclic group then the ideal in F_qG is a cyclic code, and if G is an abelian group then the ideal in F_qG is an abelian code.

It is well-known that if $q \nmid n$, it follows from Maschke's Theorem (Theorem 1.9 in Berman, 1967) that the group algebra F_qG is semisimple and hence F_qG is a direct sum of minimal ideals, $F_qG = I_1 \oplus I_2 \oplus \cdots \oplus I_s$, where $I_j = F_qGe_j$ is the principal ideal of F_qG generated by e_j where e_j is an idempotent in F_qG for $j = 1,2,\cdots,s$. Let $M = \{e_j\}_{j=1}^{s}$ be the set of all pairwise orthogonal idempotents. Every ideal I of F_qG is a direct sum $I = I_{i_1} \oplus I_{i_2} \oplus \cdots \oplus I_{i_t}$, where $t \le s$. Now, write $F_qG = I \oplus J$, where $J = I_{j_1} \oplus I_{j_2} \oplus \cdots \oplus I_{j_{s-t}}$ is the direct sum of minimal ideals such that $I_{i_l} \neq I_{j_m}$ for all $1 \le l \le t$ and $1 \le m \le s - t$. Using these observations, we see that

$$\begin{aligned} I &= I_{i_1} \oplus I_{i_2} \oplus \cdots \oplus I_{i_t} \\ &= \langle e_{i_k} | k = 1,2,\cdots,t \rangle \\ &= \{u \in F_qG | ue_{i_h} = 0, \text{for all } h = 1,2,\cdots,s-t\}. \end{aligned}$$

There are some nice properties for the idempotent e_{i_u} for $u = 1,2,\cdots,s$. In general, an element $e \in F_qG$ is an idempotent if $e^2 = e$.

Furthermore, two idempotents e_1 and e_2 are orthogonal provided $e_1 e_2 = e_2 e_1 = 0$. A direct computation can show that if e is an idempotent, it follows that $1 - e$ is an idempotent orthogonal to e. Furthermore, if e_1 and e_2 are orthogonal, it follows that $e_1 + e_2$ is an idempotent.

To construct a secret sharing scheme via group algebra codes, we proposed the following algorithms. First, to construct the secret k and the corresponding shares, we proceed as follows:

Algorithm 1:

Choose a finite group G and a finite field F_q satisfying the condition that $gcd(|G|, q) = 1$. Construct all idempotents of $F_q G$. Hence, choose a set of idempotents to construct the following group algebra code

$$I = \{u \in F_q[G] | ue_{i_h} = 0, \text{for all } h = 1,2,\cdots, s-t\}.$$

The dealer D chooses a codeword $u \in I$ and write u in terms of group algebra element $u = \sum_{g \in G} a_g g$. Take the secret k as $a = a_e$, where e is the identity element of G and the remaining $|G| - 1$ coefficients a_g, for all $g \neq e$, in $u = \sum_{g \in G} a_g g$ are uniformly distributed to the set of participants $P = \{p_1, p_2, \cdots, p_{|G|-1}\}$.

Next, to recover the secret from a subset of participants and hence obtain the access structure, we used the following algorithm.

Algorithm 2:

Let $\tau \subseteq P$ and $\tau = \{P_{i_1}, P_{i_2}, \cdots, P_{i_k}\}$ such that $1 \leq k \leq |G| - 1$. Form the group algebra element $w = \sum_{j=1}^{k} a_{g_{i_j}} g_{i_j}$. Next, $w \in I$ if and only if $we_{i_h} = 0$, for all $h = 1,2,\cdots, s-t$. Form a homogeneous system of $s-t$ equations with k unknowns in which the access structure can be determined from these equations. Upon solving, we can recover the coefficients $a_{g_{i_j}}$ for all $j = 1,2,\cdots, k$ and hence the secret a.

Example 1. To illustrate the above algorithms, we first choose a finite group said the dihedral group of order 6, $D_6 = \langle r, s \mid r^3 = s^2 = 1,\ rs = sr^2 \rangle$. To ensure the semisimplicity of $F[D_6]$, we choose $F = \mathbb{R}$. By constructing the character table of D_6, we can obtain all the three idempotents of $F[D_6]$ which are listed as follows:

$$e_1 = \frac{1}{6}(\langle r\rangle + \langle r\rangle s),$$
$$e_2 = \frac{1}{6}(\langle r\rangle - \langle r\rangle s),$$
$$e_3 = \frac{1}{3}(1 - \langle r\rangle).$$

Next, we construct the following group algebra code:

$$I = \{u \in \mathbb{R}[D_6] | ue_1 = ue_2 = 0\}.$$

Any $u \in I$ can be written in the form $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s$. Hence,

$$u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s \ \in I$$

if and only if

$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 = 0$$

and

$$\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 - \lambda_5 - \lambda_6 = 0.$$

The dealer D chooses $u = 2 - \frac{1}{3}r - \frac{5}{3}r^2 \in I$. Take the secret k = 2 and distribute $-\frac{1}{3}$ to P_1 (corresponds to the term r) and $-\frac{5}{3}$ to P_2 (corresponds to the term r^2). To recover the secret k, the participants P_1 and P_2 together will form the group algebra element $w = k - \frac{1}{3}r - \frac{5}{3}r^2$. Hence, $w \in I$ if and only if $k - \frac{1}{3} - \frac{5}{3} = 0$, that is, k = 2.

Next, we give a detail treatment on constructing secret sharing scheme based on group algebra codes defined by cyclic group of order p over binary field. Our intention is to obtain information regarding the access structure of the constructed secret sharing scheme. We follow the approach used by Ding and Ling, 2000, whereby the authors constructed secret sharing scheme based on BIBD (Balanced Incomplete Block Design). We start with the following simple results.

Lemma 1. Let $G = \langle g \mid g^p = 1\rangle$ be a cyclic group of order p, where p is an odd prime. Then, $1 + g + g^2 + \cdots + g^{p-1} = 0$ holds in $F_2[G]$.

Proof. The result is follows directly from the fact that $(g+1)\left(\sum_{i=0}^{p-1} g^i\right) = g^p - 1 = 0$ and $g + 1 \neq 0$.

Q.E.D.

Lemma 2. Let $I = \{0\} \cup \prod_{h=1}^{p} A_h$,

where $A_h = \left\{(g^i + g^j)\left(\sum_{t=1}^{h} g^{K_t}\right) \mid K_t \in \{0,1,2,\dots,p-1\}\right\}$.

Then,

(i) All elements in A_h are distinct for $h = 1,2,\dots,p$.
(ii) For all $1 \leq h < w \leq p$, $A_h \cap A_w = \{\,\}$.

Proof. For part (i), the proof is by using mathematical induction on the integer $h \geq 1$. We show the case for $h = 1$, for the inductive step the proof is follows exactly the same way. When $h = 1$, we have $A_1 = \left\{(g^i + g^j)g^{K_1} \mid K_1 \in \{0,1,2,\dots,p-1\}\right\}$. Assume $(g^i + g^j)g^{K_1} = (g^i + g^j)g^{K_2}$ for distinct integers K_1 and K_2. Thus, upon cancellation, we obtained $K_1 = K_2$ which is a contradiction. For part (ii), assume there exists an element $x \in A_h \cap A_w$. Hence, we have $\sum_{t=1}^{h} g^{K_t} = \sum_{t=1}^{w} g^{K_t}$ for $1 \leq h < w \leq p$. Upon cancellation, we obtain $\sum_{j=h+1}^{w} g^{K_j} = 0$, and so $g^{K_{h+1}}(1 + g + g^2 + \cdots + g^{K_w - K_h - 1}) = 0$ which contradicts Lemma 1. Therefore, the result follows directly. **Q.E.D.**

Theorem 1. Consider I in Lemma 2. Then,

(i) $I = \langle g^i + g^j \rangle$ for all $1 \leq i < j \leq p$.
(ii) $|I| = 2^{p-1}$.
(iii) For all $v \in I$, $wt(v)$ is even.
(iv) I is a $[p, p-1, 2] - MDS$ code.

Proof. Part (i) is directly follows from the definition of principal ideal generated by the group algebra element $g^i + g^j$. For part (ii), we note that $|A_h| = \binom{p}{h}$ for $h = 1,2,\dots,p$. Hence, $|I| = \frac{\sum_{h=0}^{p}\binom{p}{h}}{2} = 2^{p-1}$. For part (iii), we prove by contradiction by asumming that there exists an element in I with odd weight which is impossible. The linearity of I follows from the property of ideal. The parameters of the code I in part (iv) follows immediately from parts (i) to (iii). **Q.E.D.**

Remark. From Theorem 1, we deduce that the secret sharing scheme based on I is for sharing secrets among $p-1$ participants. There are p possible access structures. Each access structure consists of 2^i participants for $1 \leq i \leq p-1$ and each participants is a member of exactly 2 access structures.

Example 2. Let $p=5$.
Consider $I = \langle g^2+g^3 \rangle = \left\{ (g^2+g^3) \sum_{i=0}^{4} a_i g^i \mid a_i \in F_2 \right\} = \{(a_2+a_3)+(a_3+a_4)g+(a_0+a_4)g^2+(a_0+a_1)g^3+(a_1+a_2)g^4 \mid a_i \in F_2\}$.

Suppose the dealer chooses the codeword $u = 1+g^2+g^3+g^4$. So the secret is 1, and the dealer distribute 0 to P_1, 1 to P_2, 1 to P_3 and 1 to P_4. Assume that the participants P_1 and P_2 wanted to compute the secret. Then, both participants will form the equations $a_3+a_4=0$ and $a_0+a_4=1$. However, by solving these two equations, both participants cannot compute the secret a_2+a_3. Next, assume that the participants P_1, P_2 and P_4 wanted to compute the secret. Then, the equations $a_3+a_4=0$, $a_0+a_4=1$ and $a_1+a_2=0$ are formed, in which case this system of homogeneous equations is solvable but do not have unique solution. We conclude that the secret can be recovered; however, it may not be a valid secret.

4. CONCLUSION

The two algorithms proposed here are depended heavily on the group algebra codes, in which the idempotents used to generate the codes play an equally important role in determining the minimal access structure of a constructed secret sharing scheme. Our future investigation is to use the group algebra codes obtained in Denis. and Ang, 2013a; 2013b together with algorithms 1 and 2 proposed here to obtain a nice relationship between minimal codewords and minimal access structures.

REFERENCES

Ashikhmin, A. and Barg, A. (1998). Minimal vectors in linear codes. *IEEE T. Inform. Theory*. **44**(5): 2010-2017.

Berman, S. D. (1967). Semisimple cyclic and abelian codes, II. *Kibernetika*. **3**: 21-30.

Berman, S. D. (1989). Parameter of abelian codes in the group algebra KG of $G = < a > \times < b >, a^p = b^p = 1, p$ is prime, over a finite field K with a primitive p th root of unity and related MDS-Codes. *Contempary Math*. **93**: 77-83.

Denis C.K., Wong and Ang, M. H. (2013a). Group algebra codes defined over extra special *p*-group of order p^{2r+1}. *JP Journal of algebra, number theory and appl*. **30**(1): 47- 60.

Denis C.K., Wong and Ang, M. H. (2013b). Group codes define over dihedral groups of small orders. *Malaysian Journal of Math. Sci*. **7**(S): 101-116.

Ding, C., Kohel, D. and Ling, S. (2000). Secret sharing with a class of ternary codes. *Theor. Comput. Sci*. **246**: 285-298.

Li, Z. H., Xue, T. and Lai, H. (2010). Secret sharing schemes from binary linear codes. *Information sci*. **180**: 4412-4419.

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

McElliece, R. J. and Sarwate, D. V. (1981). On sharing secrets and Reed Solomon codes. *Communications of the ACM*. **24**: 583-584.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*. **22**(11): 612-613.

Yuan, J. and Ding, C. (2006). Secret sharing schemes from three classes of linear codes. *IEEE T. Inform. Theory*. **52**(1): 206-212.