21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

Secret sharing in compartmented groups using ideal codes

Juan A. Lopez-Ramos[1] and Justo Peralta[2]

***Abstract*— We propose a secret sharing scheme based on rings or modules that admit a decomposition given by orthogonal idempotents of the ring. The secret is decomposed into partial secrets that belong to the projections induced by every idempotent. These projections are indeed ideal codes and thus the subsecrets are distributed among a group of users using the generator matrix of these ideal codes.**

I. INTRODUCTION

A secret sharing scheme is a method of distributing a secret s among a finite set of participants, such that, only some specific subsets of participants, when pooling their partial information together, which are known as the shares, can reconstruct the secret s, whereas, any other subset not allowed to do that can determine nothing about the secret. A special participant holding no share, is called the dealer and takes the responsibility to distribute the shares to each participant and to recover the secret s. Since Blakley, [3], and Shamir, [15], gave the first constructions of secret-sharing schemes, many are the authors who are interested in these schemes. Some recent works on secret sharing schemes based on graph structures are [2], [6] or [17]. There also exist two kinds of approaches to the construction of secret sharing schemes based on linear codes. The first one uses the encoding and decoding algorithms to compute the shares and to recover the secret from them and it was introduced by McEliece and Sarwate in [13] generalizing Shamir's scheme on polynomial interpolation ([15]) in terms of Reed-Solomon codes. The second uses a generator matrix and the first column of this to compute an information vector which is then encoded. The first coordinate of the corresponding codeword is the secret. This was introduced by Karnin, Green and Hellman in [9] and later, Massey introduced in [11] and [12] the concept of minimal codewords in order to characterize the subsets of users able to recover the secret in terms of the minimal codewords of the dual code.

One of the designs proposed by Simmons in [16] is secret-sharing in compartmented groups. A compartmented t_i-out of l_i secret-sharing scheme is a design where the secret is partitioned in such a way that reconstruction of the secret requires a specified level of concurrence by the participants in some specified number, perhaps all, of the compartments. Here t_i denotes the required concurrence of the i-th group of l_i trustees. In [4, Theorem 3] the author proposes a secret-sharing scheme for compartmented groups based in vector spaces over a finite field $GF(q)$. In [8] the authors use Shamir's secret-sharing scheme over $GF(q)$, [15], to give another solution to the situation of compartmented groups, and extend it to a more general and non-considered compartmented access structure by Brickell in [4].

Our aim in this paper is to use idempotents that provide decompositions of a ring to decompose any secret into partial secrets in the induced ideal codes and then distribute them into several compartmented groups using a secret-sharing scheme based on a generator matrix similar to that in [9].We show the good properties of our protocol and give examples over classical and non-commutative situations that fit with our scheme.

II. A MOTIVATING EXAMPLE

Let us consider the ring $\mathbb{Z}_2$ and let $N = \mathbb{Z}_2[x]/(x^{15}-1)$ a quotient ring of polynomials. Then N is a finitely generated left $\mathbb{Z}_2$-module with $B = \{1, x, x^2, \ldots, x^{14}\}$ as generating set of N and

$$e_1 = x^{14} + x^{13} + +x^{11} + x^{10} + x^7 + x^5 + 1$$
$$e_2 = x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3$$
$$e_3 = x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^8+x^7+x^6+x^4+x^3+x^2+x$$
$$e_4 = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x$$

a set of orthogonal idempotents such that

$$e_1 + e_2 + e_3 + e_4 = 1$$

Now let $s = x^{10} + x^5 + x^3 + x + 1 \in N$ be a secret that we would like to distribute among a group of users. Then we project our secret on every of the ideals given by e_i, $i = 1, \ldots, 4$. Thus if we write $s_i = se_i$, $i = 1, \ldots, 4$ we get that

$$s_1 = x^{14} + x^9 + x^8 + x^7 + x^5 + x^4 + x$$
$$s_2 = x^{13} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + x$$
$$s_3 = x^{14} + x^{12} + x^9 + x^7 + x^4 + x^2$$
$$s_4 = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1$$

Let us focus, without loss of generality, in the ideal code N_2 induced by the idempotent e_2. Then $N_2 =< e_2 >=< g >$ where $g = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$ is the monic polynomial of minimal degree in N_2. Then the generating set for the cyclic code N_2 is given by $G = \{g_1, g_2, g_3, g_4\} = \{g, xg, x^2g, x^3g\}$ and thus, its generator matrix is $G_2 =$

*This work was supported by grant FQM 211 Junta de Andalucia

[1]Juan A. Lopez-Ramos is with the Department of Mathematics, University of Almeria, 04120 Almeria, Spain jlopez@ual.es

[2]Justo Peralta is with the Department of Mathematics, University of Almeria, 04120 Almeria, Spain jperalta@ual.es

ISBN: 978-90-367-6321-9

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

On the other hand, $s_2 = \sum_{i=0}^{14} s_{2j} x^j$ and each $g_i \in G$ is analogously expressed with respect to B as $g_i = \sum_{i=0}^{14} r_{ij} x^j$, $i = 1, \ldots, 4$ that correspond to every row of G_2. Now we consider the equations given by

$$\sum_{i=1}^{4} r_{i1} x_{ij} = s_{ij}$$

It is clear that since $r_{11} = 1$ and $r_{i1} = 0$ for $i = 2, 3, 4$, then we may choose as a solution (s_{ij}, a, b, c) where a, b, c are randomly selected in $\mathbb{Z}_2$. Then we denote by w_j^2, $j = 1, \ldots, 15$ the polynomials whose coefficients are $w_{0j}^2 = s_{2,0}$, $w_{1j}^2 = a$, $w_{2j}^2 = b$ and $w_{3j}^2 = c$ we can choose

$$w_1^2 = x^3 + x, w_2^2 = x^2 + x + 1, w_3^2 = x^3 + 1,$$
$$w_4^2 = x^3 + x, w_5^2 = x^2 + x + 1, w_6^2 = x,$$
$$w_7^2 = x^3 + x^2 + 1, w_8^2 = x^2 + 1, w_9^2 = x^2 + 1,$$
$$w_{10}^2 = x + 1, w_{11}^2 = x^2 + x, w_{12}^2 = x^2,$$
$$w_{13}^2 = x^3 + x^2 + x, w_{14}^2 = x^2 + 1, w_{15}^2 = x^2 + x$$

Then, multiplying the matrix whose rows are given by the coefficients of w_j^2, $j = 1, \ldots 15$ by G_2 we get the matrix $u^2 =$

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

Let $\overline{u}_j^2$ be the column vector of u^2 for $j = 1, \ldots, 15$. Then it can be observe that $\overline{u}_1^2$ is given by the coefficients of s_2. Thus this column is kept secret and we give the column $\overline{u}_j^2$ to the party j, $j = 2, \ldots, 15$ of the group number 2.

Now we observe that since $\overline{u}_1^2 = \overline{u}_2^2 + \overline{u}_5^2$, we can recover the partial secret s_2 from the shares held by the parties 2 and 5. We note that exists several ways to recover the partial secret, for example using the columns vectors $\overline{u}_2^2, \overline{u}_{12}^2$ and $\overline{u}_{14}^2$.

This may be applied to every partial secret s_1, s_2, s_3 and s_4, that will give four different groups of users holding different shares to recover the corresponding partial secrets. Once every partial secret is recovered, s will be given by

$$s_1 + s_2 + s_3 + s_4$$

III. A COMPARTMENTED SECRET SHARING SCHEME

Throughout this paper A will be a division ring and R will denote an associative A-algebra with unit 1.

Let R be a finitely generated A-algebra and N a finitely generated left R-module. Then N is also finitely generated as an A-module, so let $\{b_1, \cdots, b_n\}$ be a generating set for N as A-module. Let us also assume that N has a decomposition $N = N_1 \oplus \cdots \oplus N_l$. Then, there exists a complete set of orthogonal idempotents $\{e_1, \cdots, e_l\}$ in $End_R(N)$ given by the corresponding projections $e_i : N \to N_i$, $i = 1, \ldots, l$. These endomorphisms clearly satisfy that $e_i e_j = 0$ for $i \neq j$ and $I_N = e_1 + \cdots + e_l$ since $N_i = Ne_i$ for $i = 1, \cdots, l$ (cf. [1, Corollary 6.20]. Therefore $a = a_1 + \cdots + a_l$ with $a_i \in N_i$, $i = 1, \cdots, l$ for every $a \in N$. Since N is finitely generated as an A-module, then so are the N_i for $i = 1, \cdots, l$. So let $\{g_{i_1}, \cdots, g_{i_{k_i}}\}$ be a generating set for N_i, $i = 1, \cdots, l$.

Now let the set of participants $\mathcal{P}$ be partitioned into l disjoint sets $\mathcal{P}_1, \cdots, \mathcal{P}_l$.

Algorithm 1 - Sharing the secret among members of $\mathcal{P}_i$ $i = 1, \cdots, l$.

1) Given a secret $s \in N$ then is partitioned into $s = s_1 + \cdots + s_l$ with $s_i = se_i \in N_i$, $i = 1, \cdots, l$. s_i will be called the *partial secrets*.

2) For every $i = 1, \cdots, l$ let $\{g_{i_1}, \cdots, g_{i_{k_i}}\}$ be a generating set for N_i. Now, $g_{i_h} = \sum_{j=1}^{n} r_{h,j}^i b_j$, with $r_{h,j}^i \in A$, $h = 1, \cdots, k_i$. Then, $s_i = \sum_{j=1}^{n} s_{i,j} b_j$, $s_{i,j} \in A$ and let $w_{j,1}^i, \cdots, w_{j,k_i}^i$ be a solution of the equations $s_{i,j} = \sum_{h=1}^{k_i} x_h r_{h,1}^i$ for $j = 1, \cdots, n$. Then we get that

$$(w_{j,1}^i, \cdots, w_{j,k_i}^i) \begin{pmatrix} r_{1,1}^i & \cdots & r_{1,n}^i \\ \vdots & & \vdots \\ r_{k_i,1}^i & \cdots & r_{k_i,n}^i \end{pmatrix} =$$

$$= (s_{i,j}, *, \ldots, *)$$

3) For every $i = 1, \cdots, l$ and $j = 1, \cdots, n$ we get $u_{j,h}^i = \sum_{s=1}^{k_i} w_{j,s}^i r_{s,h}^i$ where $u_{j,1}^i = s_{i,j}$. Then give the column vector $\begin{pmatrix} u_{1,j}^i \\ \vdots \\ u_{n,j}^i \end{pmatrix}$ to party j, $j = 2, \cdots, n$ of group i, $i = 1, \cdots, l$, namely P_j^i.

If we denote by G_i the generator matrix of N_i, $\begin{pmatrix} r^i_{1,1} & \cdots & r^i_{1,n} \\ \vdots & & \vdots \\ r^i_{k_i,1} & \cdots & r^i_{k_i,n} \end{pmatrix}$ we get a matrix representation of the precedent as follows

$$\begin{pmatrix} w^i_{1,1} & \dots & w^i_{1,k_i} \\ w^i_{2,1} & \dots & w^i_{2,k_i} \\ \vdots & & \vdots \\ w^i_{n,1} & \dots & w^i_{n,k_i} \end{pmatrix} \quad G_i =$$

$$= \begin{pmatrix} s_{i,1} & u^i_{1,2} & \cdots & \boxed{u^i_{1,j}} & \cdots & u^i_{1,n} \\ s_{i,2} & u^i_{2,2} & \cdots & u^i_{2,j} & \cdots & u^i_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ s_{i,n} & u^i_{n,2} & \cdots & u^i_{n,j} & \cdots & u^i_{n,n} \end{pmatrix}$$

Then participant j of group i, P^i_j will receive the detached column of the above matrix.

Algorithm 2 - Recovering the secret from members of $\mathcal{P}_i$ $i = 1, \cdots, l$.

1) Let $\mathbf{r}^i_{h_j}$, $j = 1, \dots, t_i$ be columns of G_i such that $\mathbf{r}^i_1$ can be written as a linear combination of them, namely
$$\mathbf{r}^i_1 = \sum_{j=1}^{t_i} \mathbf{r}^i_{h_j} x^i_j$$
and let $P^i_{i_1}, \dots, P^i_{t_i}$ be the corresponding participants of the group $\mathcal{P}_i$.
2) The dealer computes x^i_j $j = 1, \cdots, t_i$ (or takes them from a file, in case G_i is deleted after giving the shares to the participants and thus in that case, these should be computed in Algorithm 1 and stored) and takes the corresponding shares u^i_j, $j = 1, \dots, t_i$.
3) The dealer computes $s_{ij} = \sum_{k=1}^{t_i} u^i_{j,k} x^i_k$, and computes $s_i = \sum_{j=1}^{n} s_{ij} b_j$ for every $i = 1, \dots, l$.
4) The dealer recover the secret as $s = s_1 + \ldots + s_l$.

Theorem 3.1: Let P^i_j $j = t_1, \dots, t_i$, $i = 1, \dots, l$ be shares. Then they can recover the secret s if and only if the columns $\mathbf{r}^i_{t_1}, \dots, \mathbf{r}^i_{t_i}$ generates the column $\mathbf{r}^i_1$ of the generator matrix G_i for every $i = 1, \dots, l$.

Proof: Firstly we note that since N_i is finitely generated as A-module then G_i has rank t_i for some t_i for every $i = 1, \dots, l$ and so $\mathbf{r}^i_1 = \sum_{j=1}^{t_i} \mathbf{r}^i_{h_j} x^i_j$ for some $x^i_j \in A$ $j = 1, \cdots, t_i$. Then $s_{i,j} = u^i_{j,1} = \sum_{s=1}^{k_i} w^i_{j,s} r^i_{s,1} = \sum_{s=1}^{k_i} w^i_{j,s} \sum_{k=1}^{t_i} r^i_{s,h_k} x^i_k = \sum_{k=1}^{t_i} (\sum_{s=1}^{k_i} w^i_{j,s} r^i_{s,h_k}) x^i_k = \sum_{k=1}^{t_i} u^i_{j,k} x^i_k$.

Thus the secret s is recovered as exposed in Algorithm 2.

Let us suppose now that the parties are such that their corresponding columns do not generate $\mathbf{r}^i_1$, i.e., the system of equations $x_1 \mathbf{r}^i_1 + \ldots + x_{t_i} \mathbf{r}^i_{t_i} = \mathbf{0}$ is indeterminate, and so there exist as many possible values for s_i as there is in N_i, which means that they do not get any information on the real value of s_i.

Then let us assume that s_i cannot be recovered for some fixed i and let $s' = \sum_{j=1, j\neq i}^{l} s_j$ then $s' = s \sum_{j=1, j\neq i}^{l} e_j$. But $\sum_{j=1, j\neq i}^{l} e_j$ is an idempotent and so it has not inverse, so the precedent equation cannot be solved. Then we can try to find an element $r \in N$ such that $re_j = s_j$, $j \neq i$ (we are assuming that all e_j, $j \neq i$ are known). But then, the sequence $a_0 = r$, $a_{n+1} = a_n + x(\sum_{j=1, j\neq i}^{l} e_j - I_N)$ for every $x \in N$ verifies that $a_{n+1} e_j = a_n e_j + x e_j - x e_j = s_j$ for $j \neq i$. Therefore, from an element $r \in N$ verifying that $re_j = s_j (j \neq i)$ we get as many elements as there are in N with the same property. Thus every s_j is needed to recover s. ■

Remark 1: In the case of a semisimple ring, every left R-module has a decomposition of the form

$$M \cong Re_1^{(I_1)} \oplus \ldots \oplus Re_l^{(I_l)}$$

where e_i $i = 1, \dots, l$ are pairwise orthogonal idempotents. An idempotent is called *primitive* in case it cannot be expressed as a sum of two other non-trivial idempotents and given e a primitive idempotent, Re is called a primitive module. In case R is semisimple, then primitive modules are just simple modules. A set of pairwise orthogonal idempotents is said to be basic if Re_i, $i = 1, \dots, l$ is a complete set (and irredundant) of representatives of the primitive modules.

Then we note that existence of a complete orthogonal set characterizes the so-called *semiperfect rings*, i.e., a ring R such that the quotient ring $R/J(R)$, where $J(R)$ the Jacobson radical of R, is semisimple and idempotents lift modulo $J(R)$, (cf [1, Proposition 27.10]).

Remark 2: Let us observe that accordingly to [16], we get that the precedent protocol provides the desirable capabilities for such a scheme.

Firstly, it is a compartmented k_l of l_i shared secret scheme, since the secret s is partitioned in such a way that recovering of s requires the concurrence by participants of all the compartments l and a concurrence of k_l parties in every compartment is also required. This k_l minimum number of parties is given by the minimum number parties that give the appropriate linear combination to recover each of the partial secrets s_l.

The scheme is extrinsic since the value of a private piece of information depends only on its functional relationship to other shares, they are a solution of an equation that provides $s_{i,j}$, $j = 1, \dots, n$ and these are the coefficients of a linear combination that give each of the partial secrets s_i, $i = 1, \dots, l$.

Remark 3: Some other interesting properties are obtained for our secret sharing protocol. Firstly we get that the secret

s is expressed as a linear combination of the elements of the generating set $\{b_1, \ldots, b_n\}$ and that every party in $\mathcal{P}_\rangle$, namely P_j^i, receives a share of the form $(u_{1,j}^i, \ldots, u_{n,j}^i)$, which is used to recover each of the coefficients $s_{i,j}$ of the linear combination $s_i = \sum_{j=1}^{n} s_{i,j} b_i$, and thus the shares never are longer than the secret s. This enhances previous existing compartmented schemes where shares hold by the parties are longer than the secret as it can be checked in [4] or [8].

Secondly, as a consequence of the reasoning given at the end of the proof of Theorem 3.1, in case the dealer keeps secret one of the partial secrets, then the scheme is prepositioned, i.e., the secret cannot be recovered while this is not available and the same collection of partial secrets (and shares) can be used to reveal different secrets, just by changing the partial secret held by the dealer.

And finally, our protocol also provides the possibility to verify if the recover secret is not the previously shared in some cases, more precisely, the partial secrets. Since $s_i = se_i$ for every $i = 1, \ldots, l$, we get that $s_i e_i = se_i e_i = s_i e_i = s_i$, for every $i = 1, \ldots, l$, i.e., if for some reason one of the shares, namely u_j^i, is not correct, due to errors or even cheating by party P_j^i, then it could be that the recover partial secret s_i' is not in Ne_i and thus, $s_i' e_i \neq s_i'$. Then the dealer would detect that there is an error while recovering s_i. In that case, depending on the errors in u_j^i, the dealer can detect that P_j^i is cheating. To do so we just have to observe that in step 3 of Algorithm 1 we get a matrix whose first column gives the partial secret s_i, but also, the rows of that matrix are codewords of the code Ne_i. Thus, depending on the capability of error detection of this code, we will be able to determine the columns where the error were produced in the following manner:

1) The dealer considers the vectors
$$(s_{i,j}, u_{j,2}^i, *, u_{j,4}^i, *, \ldots, u_{j,n-2}^i, *, u_{j,n}^i)$$
where $*$ denotes that this position is unknown since the corresponding party is not collaborating to recover the secret s_i.
2) If error detection capability of Ne_i and the number of parties collaborating are big enough, then the dealer can substitute $*$ by any random number.
3) The dealer uses error detection capability of Ne_i to detect which of the entries of the vector constitute errors.
4) In case there exists too many unknown values, then the dealer may search for a codeword of the form
$$(*, u_{j,2}^i, c_3, u_{j,4}^i, c_5, \ldots, u_{j,n-2}^i, c_{n-1}, u_{j,n}^i)$$
and then operate as in the previous step, determining which of the $u_{j,k}^i$ are errors, but this could take too much time or even be impossible for existing several codewords such that coincide in all these known positions.

Remark 4: A brute force attack would consist in finding all possible complete sets of orthogonal idempotents and then, known one or more partial secrets, namely s_i, the attacker could try to recover the original secret s. By Remark 1, in case R is a semiperfect ring, then we can lift the set $\{e_1 + J(R), \ldots, e_l + J(R)\}$ of idempotents that generate the simple blocks of the semisimple ring $R/J(R)$ to a basic set of primitive idempotents, $\{e_1, \ldots, e_l\}$. Thus, any considered complete set of pairwise orthogonal idempotents as in the scheme is generated from the previous basic one. Therefore an attacker will get all possible complete sets of orthogonal idempotents, one of them will be the considered one. However knowing any of the shares does not give any information on the original secret as it is shown in the proof of Theorem 3.1. Therefore, recovering the original secret s implies knowing a necessary number of shares to recover every partial secret, i.e., getting as much information as the dealer.

Examples: 1. For our motivating example we get that, in the case of s_2, if we search for all possibilities to recover this partial secret we get that

$$x_2 = 1 + a_1 + a_2 + a_4 + a_6 + a_7 + a_{10};$$

$$x_3 = a_2 + a_3 + a_4 + a_5 + a_7 + a_9 + a_{10};$$

$$x_4 = a_1 + a_2 + a_3 + a_4 + a_6 + a_8 + a_9;$$

$$x_5 = 1 + a_1 + a_2 + a_3 + a_5 + a_7 + a_8;$$

$$x_6 = a_{10}; x_7 = a_9; x_8 = a_8; x_9 = a_7; x_{10} = a_6;$$

$$x_{11} = a_5; x_{12} = a_4; x_{13} = a_3; x_{14} = a_2; x_{15} = a_1$$

with $a_i \in Z_2$, $i = 1, \ldots, 10$, which gives 1024 possibilities, although there exist cases where some of the shares do not really contribute significatively to the recovering. For instance, in the case $a_i = 0$ for every $i = 1, \ldots, n$ we get, as previously pointed out, that users 2 and 5 of group 2 will be able to recover s_2.

2. Let us consider now an example over a group ring with G non-abelian. Let $G =< x, y | x^3 = id, y^5 = id, yx = x^4 y >$ be the (3,5,4)-metacyclic group ([14]). G has order 15 and thus the group ring $\mathbb{Z}_2 G$, by Maschke's Theorem is semisimple. Using GAP [18] we are able to compute the set of primitive idempotents

$$e_1 = 1 + x^2 + y^3 + x + x^2y^3 + y + xy^3 + x^2y +$$
$$+ y^4 + xy + x^2y^4 + y^2 + xy^4 + x^2y^2 + xy^2$$
$$e_2 = x^2 + x + x^2y^3 + xy^3 + x^2y + xy + x^2y^4 + xy^4 + x^2y^2 + xy^2$$
$$e_3 = y^3 + x^2y^3 + y + xy^3 + x^2y + y^4 + xy + x^2y^4 +$$
$$+ y^2 + xy^4 + x^2y^2 + xy^2$$
$$e_4 = y^3 + x^2y^3 + y + y^4 + xy + y^2 + xy^4 + x^2y^2$$
$$e_5 = y^3 + y + xy^3 + x^2y + y^4 + x^2y^4 + y^2 + xy^2$$

Once the corresponding generator matrices of the ideal codes $\mathbb{Z}_2Ge_i$ $i = 1, \ldots, 5$ are studied we consider the following complete set of orthogonal idempotents

$$\{e = e_1 + e_2 + e_3, e_4, e_5\}$$

Next we show the ideal codes $\mathbb{Z}_2Ge, Z_2Ge_4$ and Z_2Ge_5 as ideal codes with their corresponding parameters and generator matrices G_e, G_{e_4} and G_{e_5}. The matrices G'_e, G'_{e_4} and G'_{e_5} are the generator matrices of these codes in their standard form.

$$e = e_1 + e_2 + e_3 = 1 + x^2y^3 + xy^3 + x^2y + xy + x^2y^4 + \\ + xy^4 + x^2y^2 + xy^2$$

$\mathbb{Z}_2Ge$ is a $[15, 7, 3]$ linear code and G_e and G'_e are respectively

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

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

$\mathbb{Z}_2Ge_4$ is a $[15, 4, 8]$ linear code and G_4 and G'_4 are respectively

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

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

$\mathbb{Z}_2Ge_4$ is a $[15, 4, 8]$ linear code and G_5 and G'_5 are respectively

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

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

As it can be observed, the first column of G_e and G'_e has the same form and thus, solving the equations of step 2 in Algorithm 1 are trivial and they could be done similarly as in Section 1 in order to build the shares corresponding to the partial secret se. However this is not the case of G_4 and G_5. If we use these two matrices to get the shares for the partial secrets se_4 and se_5 we cannot solve the corresponding equations given in Algorithm 1. In the case that we use G'_4 and G'_5, we have to take into account that these correspond in fact to equivalent codes and thus the subsets of users able to recover the partial secrets will be the same up to the corresponding permutations of columns.

3. Let $N = \mathbb{Z}_5S_3$ be the group ring over the symmetric group S_3. Then N is a finitely generated left $\mathbb{Z}_5$-module with the elements S_3 as a generating set. By means of the theory of Young diagrams (cf. [5, Ch. IV]) and using GAP we get a complete set of orthogonal idempotents elements of N given by

$$e_1 = () + (2,3) + (1,2) + (1,2,3) + (1,3,2) + (1,3)$$
$$e_2 = () + 4(2,3) + 4(1,2) + (1,2,3) + (1,3,2) + 4(1,3)$$
$$e_3 = 2() + 2(2,3) + 3(1,2) + 3(1,2,3)$$
$$e_4 = 2() + 3(2,3) + 2(1,2) + 3(1,3,2)$$

Firstly we choose as our set of orthogonal idempotents $\{e_1 + e_2, e_3, e_4\}$ which gives the generator matrices G_1, G_2 and G_3 respectively:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 4 & 4 & 0 & 0 \\ 0 & 1 & 0 & 4 & 1 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 4 & 1 & 4 & 0 & 0 \\ 0 & 0 & 1 & 1 & 4 & 4 \end{bmatrix}$$

As can be observed, G_1 is not adequate for a secret-sharing scheme, since the shares would either reveal the partial secret or cannot contribute to its recovering and, therefore, its corresponding partial secret should be kept secret by the dealer. Then, taking in count that we cannot give the third and the second columns of G_2 and G_3 respectively, the subsets of shares that can recover the subsecrets would be given by:

$$\Gamma_2 = \{(x_2, x_5), (x_2, x_6), (x_4, x_5), (x_4, x_6), (x_2, x_4, x_5), \\ (x_2, x_5, x_6), (x_2, x_4, x_6), (x_4, x_5, x_6), (x_2, x_4, x_5, x_6)\}$$
$$\Gamma_3 = \{(y_3, y_4), (y_3, y_5), (y_3, y_6), (y_4, y_5), (y_4, y_6), (y_3, y_4, y_5), \\ (y_3, y_4, y_6), (y_3, y_5, y_6), (y_4, y_5, y_6), (y_3, y_4, y_5, y_6)\}$$

Another option, in order to keep secret nothing by the dealer is to consider the complete orthogonal set of idempotents, $\{e_1 + e_3, e_2 + e_4\}$, which gives the generator matrices G_1 and G_2 given by

$$\begin{bmatrix} 1 & 1 & 3 & 3 & 2 & 2 \\ 0 & 1 & 1 & 0 & 4 & 2 \\ 0 & 0 & 1 & 1 & 3 & 3 \end{bmatrix} \begin{bmatrix} 1 & 4 & 2 & 2 & 3 & 3 \\ 0 & 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 & 4 \end{bmatrix}$$

In this case we cannot give the second column of G_2. Now the access structure is given by: Γ_1, which is formed

by any group with three or more shares and $\Gamma_2 = \{(y_3, y_5), (y_4, y_6), (y_3, y_4, y_5), (y_3, y_5, y_6), (y_3, y_4, y_6), (y_4, y_5, y_6), (y_3, y_4, y_5, y_6)\}$

In [7] the authors classify minimal convolutional codes in $\mathbb{Z}_5 S_3$ with respect to some kind of automorphisms using the decomposition given by its primitive idempotents, and this has been recently extended in [10] using a derivation.

REFERENCES

[1] F. Anderson and K. Fuller, Rings and Categories of Modules, Springer-Verlag, New York, 1974.
[2] A. Beimel, T. Tassa, and E. Weinreb, Characterizing ideal weighted threshold secret sharing, SIAM J. Discrete Math., vol. 22, pp. 360-397, 2008
[3] G.R. Blakley, Safeguarding cryptographic keys, Proc. Amer. Fed. Inform. Proc. Soc. 1979 NCC, vol. 48, pp. 313-317, June 1979.
[4] E. Brickell, Some Ideal Secret Sharing Schemes, in Advances in Cryptology-Proceedings of CRYPTO'89 (J.-J. Quisquater and J. Vandewalle, eds.), vol. 434 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 468-475.
[5] C.W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras. Wiley-Interscience, New York, 1962.
[6] G. Di Crescenzo, and C. Galdi, Hypergraph decomposition and secret sharing, Discrete Appl. Math., vol. 157, pp. 928-946, 2009.
[7] S. Estrada, J.R. García-Rozas, J. Peralta, E. Sánchez-García, Group convolutional codes, Adv. Math. Commun., vol. 2, no. 1, pp. 8394, 2008.
[8] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, Secret Sharing in Multilevel and Compartemented Groups, in ACISP'98 (C. Boyd and E. Dawson, eds.), vol. 1438 of Lecture Notes in Computer Science, Springer-Verlag 1998, pp. 367-378.
[9] E.D. Karnin, J.W. Greene, and M.E. Hellman, On Secret Sharing Systems, IEEE Trans. Inform. Theory, vol. 29, no. 1, pp. 644-654, 1983.
[10] S.R. López-Permouth and S. Szabo, Convolutional codes with additional algebraic structure, J. Pure Appl. Algebra, vol. 217, pp. 958-972, 2013.
[11] J.L. Massey, Minimal codewords and secret sharing, Proc. 6th Jooint Swedish-Russian Workshop on Inform. Theory. Mölle, Sweden. August 22-27, 1993, pp. 276-279.
[12] J.L. Massey, Soome applications of coding theory in cryptography, in "Codes and Cyphers: Cyrptography and Coding IV" (Ed. P.G. Farrell), Esses, England: Formara Ltd., 1995, pp. 33-47.
[13] R.J. McEliece and D.V. Sarwate, On Sharing Secrets and Ree-Solomon Codes, Comm. ACM, vol. 24, pp. 583-584, 1981.
[14] R.E. Sabin, Metacyclic Error-Correcting Codes, AAECC, vol. 6, pp. 191-210, 1995.
[15] A. Shamir, How to Share a Secret, Communications of the ACM, vol. 22, pp. 612-613, Nov. 1979.
[16] G. Simmons, How to (Really) Share a Secret, in Advances in Cryptology-Proceedings of CRYPTO'88 (S. Goldwasser, ed.), vol 403 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 390-448.
[17] H. Sun, Decomposition Construction for secret sharing schemes with graph access structures in polynomial time, SIAM J. Discrete Math., vol. 24, no. 2, pp. 617-638, 2010.
[18] The GAP Group, *GAP – Groups, Algorithms, and Programming,* (http://www.gap-system.org).