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

\[
\begin{align*}
    e_1 &= x^{14} + x^{13} + x^{11} + x^{10} + x^7 + x^5 + 1 \\
    e_2 &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3 \\
    e_3 &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x \\
    e_4 &= x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x
\end{align*}
\]

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 \(s_i = s e_i, i = 1, \ldots, 4\) we get that

\[
\begin{align*}
    s_1 &= x^{14} + x^9 + x^8 + x^7 + x^5 + x^4 + x \\
    s_2 &= x^{13} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + x \\
    s_3 &= x^{14} + x^{12} + x^9 + x^7 + x^6 + x^4 + x^2 \\
    s_4 &= x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1
\end{align*}
\]

Let us focus, without loss of generality, in the ideal code \(N_2\) induced by the idempotent \(e_2\). Then \(N_2 = \langle g \rangle\) 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 \(G = \{g, xg, x^2g, x^3g\}\) and thus, its generator matrix is \(G_2 = \)
Thus this column is kept secret and we give the column $2$ to the party $j$, $j=2,\ldots,15$ of the group number $2$. Now we observe that since $\pi_2^1 = \pi_2^2 + \pi_2^3$, we can recover the partial secret $s_2$ from the shares held by the parties 2 and 5. We note that there exists several ways to recover the partial secret, for example using the columns vectors $\pi_2^2, \pi_2^1$ and $\pi_2^4$.

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 $\{b_1,\ldots,b_n\}$ 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 $\{e_1,\ldots,e_l\}$ in $\text{End}_R(N)$ given by the corresponding projections $e_i : N \rightarrow N_i$, $i=1,\ldots,l$.

These endomorphisms clearly satisfy that $e_ie_j = 0$ for $i \neq j$ and $I_N = e_1 + \cdots + e_l$ since $N_i = Ne_i$ for $i=1,\ldots,l$ (cf. [1, Corollary 6.20]). Therefore $a = a_1 + \cdots + a_l$ with $a_i \in N_i$, $i=1,\ldots,l$ for every $a \in N$. Since $N$ is finitely generated as an $A$-module, then so are the $N_i$ for $i=1,\ldots,l$. So let $\{g_1,\ldots,g_{il}\}$ be a generating set for $N_i$, $i=1,\ldots,l$.

Now let the set of participants $P$ be partitioned into $l$ disjoint sets $P_1,\ldots,P_l$.

**Algorithm 1 - Sharing the secret among members of $P_i$, $i=1,\ldots,l$.

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

2) For every $i=1,\ldots,l$ let $\{g_1,\ldots,g_{il}\}$ be a generating set for $N_i$. Now, $g_{ih} = \sum_{j=1}^n r_{ih,j} b_j$, with $r_{ih,j} \in A$, $h=1,\ldots,k_i$. Then, $s_i = \sum_{j=1}^{k_i} g_{ih,j}$ and let $u_{j}^{i,1},\ldots,u_{j}^{i,k_i}$ be a solution of the equations $s_{ij} = \sum_{h=1}^{k_i} x_h r_{ih,j} r_{ih,j}$ for $j=1,\ldots,n$. Then we get that

$$\begin{pmatrix} u_{j}^{i,1} & \cdots & u_{j}^{i,k_i} \end{pmatrix} = \begin{pmatrix} r_{ih,1} & \cdots & r_{ih,n} \\ \vdots & \vdots & \vdots \end{pmatrix}$$

3) For every $i=1,\ldots,l$ and $j=1,\ldots,n$ we get $u_{j,h}^{i} = \sum_{s=1}^{k_i} w_{i,j,s}^{i} r_{ish}^{i}$, where $w_{i,j,s}^{i} = s_{i,j}$. Then give the column vector

$$\begin{pmatrix} u_{n,j}^{i} \end{pmatrix}$$

to party $j$, $j=2,\ldots,n$ of group $i$, $i=1,\ldots,l$, namely $P_j$.
If we denote by $G_i$ the generator matrix of $N_i$, 
\[
\begin{pmatrix}
  r_{1,1}^i & \cdots & r_{1,n}^i \\
  \vdots & & \vdots \\
  r_{k_i,1}^i & \cdots & r_{k_i,n}^i 
\end{pmatrix}
\]
we get a matrix representation of the precedent as follows:

\[
\begin{pmatrix}
  w_{1,1}^i & \cdots & w_{1,k_i}^i \\
  w_{2,1}^i & \cdots & w_{2,k_i}^i \\
  \vdots & & \vdots \\
  w_{n,1}^i & \cdots & w_{n,k_i}^i 
\end{pmatrix}
\]

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 $r_1^i$, i.e., the system of equations $x_1 r_1^i + \ldots + x_t r_t^i = 0$ 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 $s' = \sum_{j=1,j\neq i}^t s_j$ then $s' = s \sum_{j=1,j\neq i}^t e_j$. But $\sum_{j=1,j\neq i}^t e_j$ 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 $r e_j = s_j \neq i$ (we are assuming that all $e_j$, $j \neq i$ are known). But then, the sequence $a_0 = r$, $a_{n+1} = a_n + x(\sum_{j=1,j\neq i}^t e_j - I_N)$ 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 $r e_j = s_j (j \neq i)$ 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 
\[
M \cong Re_1^{(1)} \oplus \ldots \oplus Re_l^{(1)}
\]
where $e_i = i, \ldots, l$ 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 $Re_i$, $i = 1, \ldots, l$ 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 [16], we get that the precedent protocol provides the desirable capabilities for such a scheme.

Firstly, it is a compartmented $k_i$ 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 for every concurrence of $k_i$ parties in every compartment is also required. This $k_i$ minimum number of parties is given by the minimum number parties that give the appropriate linear combination to recover each of the partial secrets $s_i$.

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 $s_{i,j}$, $j = 1, \ldots, n$ and these are the coefficients of a linear combination that give each of the partial secrets $s_i$, $i = 1, \ldots, l$.

**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 $\mathcal{P}_i$, namely $P^i_j$, receives a share of the form $(u^i_{1,j}, \ldots, u^i_{n,j})$, which is used to recover each of the coefficients $s_{i,j}$ of the linear combination $s_i = \sum_{j=1}^{n} s_{i,j} b_j$, 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 changing the partial secret held by the dealer.

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.

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

\[
x_2 = 1 + a_1 + a_2 + a_4 + a_5 + a_7 + a_{10};
\]

\[
x_3 = a_2 + a_3 + a_4 + a_5 + a_7 + a_9 + a_{10};
\]

\[
x_4 = a_1 + a_2 + a_3 + a_4 + a_6 + a_8 + a_9;
\]

\[
x_5 = 1 + a_1 + a_2 + a_3 + a_5 + a_7 + a_8;
\]

\[
x_6 = a_{10}; x_7 = a_9; x_8 = a_8; x_9 = a_7; x_{10} = a_6;
\]

\[
x_{11} = a_5; x_{12} = a_4; x_{13} = a_3; x_{14} = a_2; x_{15} = a_1
\]

with $a_i \in \mathbb{Z}_2$, $i = 1, \ldots, 10$, 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 $G$ nonabelian. Let $G = \langle x, y | x^3 = id, y^2 = id, yx = x^{-1}y \rangle > (3,5,4)$-metacyclic group ([14]). $G$ has order 15 and thus the group ring $\mathbb{Z}_2\mathcal{G}$, by Maschke’s Theorem is semisimple. Using GAP [18] we are able to compute the set of primitive idempotents

\[
e_1 = 1 + x^2 + y^3 + x + x^2 y^3 + y + xy^3 + x^2 y + y^4 + xy + x^2 y^4 + y^2 + x^2 y^4 + xy^2
\]

\[
e_2 = x^2 + x + x^2 y^3 + x + x^2 y^3 + y + x y + y^4 + x + y^4 + x + x^2 y^4 + y^2 + x^2 y^4 + xy^2
\]

\[
e_3 = y^3 + x^2 y^3 + y + xy^3 + x^2 y + x y^3 + y^4 + xy + x + y^4 + y^2 + x + x^2 y^4 + y^2 + x^2 y^4 + xy^2
\]

\[
e_4 = y^3 + x^2 y^3 + y + y^4 + x y + y^2 + xy^4 + x^2 y^2
\]

\[
e_5 = y^3 + y + xy^3 + x^2 y + y^4 + x^2 y^4 + y^2 + xy^2
\]
Once the corresponding generator matrices of the ideal codes $Z_2Ge_i$ for $i = 1, \ldots, 5$ 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 $Z_2Ge$, $Z_2Ge_4$ 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.

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

$Z_2Ge$ is a $[15, 7, 3]$ linear code and $G_e$ and $G'_e$ are respectively

$$Z_2Ge_4$$

$$Z_2Ge_5$$

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.

Let $N = Z_5S_3$ be the group ring over the symmetric group $S_3$. Then $N$ is a finitely generated left $Z_5$-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

$$e_1 = () + (2, 3) + (1, 2) + (1, 2, 3) + (1, 3, 2) + (1, 3)$$

$$e_2 = () + 4(2, 3) + 4(1, 2) + (1, 2, 3) + (1, 3, 2) + 4(1, 3)$$

$$e_3 = 2(1) + 2(2, 3) + 3(1, 2) + 3(1, 2, 3)$$

$$e_4 = 2(1) + 3(2, 3) + 2(1, 2) + 3(1, 3, 2)$$

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:

$$Z_2Ge_4$$

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:

$$\Gamma_2 = \{ (x_2, x_5), (x_2, x_6), (x_4, x_5), (x_2, x_5, x_6) \}$$

$$\Gamma_3 = \{ (y_3, y_4), (y_5, y_6), (y_3, y_5), (y_4, y_5), (y_3, y_4, y_5) \}$$

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

$$Z_2Ge_5$$

$$G_1 \quad G_2$$

In this case we cannot give the second column of $G_2$.

Now the access structure is given by: $\Gamma_1$, which is formed
by any group with three or more shares and \( \Gamma_2 = \{(y_3, y_5), (y_4, y_6), (y_3, y_4, y_5), (y_3, y_5, y_6), (y_3, y_4, y_6), (y_4, y_5, y_6)\} \)

In [7] the authors classify minimal convolutional codes in \( \mathbb{Z}_5S_3 \) 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