Generalized Subspace Subcodes With Application in Cryptology

Thierry P. Berger, Cheikh Thiécoumba Gueye, and Jean Belo Klamti

***Abstract*— Most codes with an algebraic decoding algorithm are derived from Reed-Solomon codes. They are obtained by taking equivalent codes, for example, generalized Reed-Solomon codes, or by using the so-called subfield subcode method, which leads to alternant codes over the underlying prime field, or over some intermediate subfield. The main advantage of these constructions is to preserve both the minimum distance and the decoding algorithm of the underlying Reed-Solomon code. In this paper, we explore in detail the subspace subcodes construction. This kind of codes was already studied in the particular case of cyclic Reed-Solomon codes. We extend this approach to any linear code over the extension of a finite field. We are interested in additive codes who are deeply connected to subfield subcodes. We characterize the duals of subspace subcodes. We introduce the notion of generalized subspace subcodes. We apply our results to generalized Reed-Solomon codes which leads to codes with interesting parameters, especially over a large alphabet. To conclude this paper, we discuss the security of the use of generalized subspace subcodes of Reed-Solomon codes in a cryptographic context.**

***Index Terms*— Additive code, subfield subcode, subspace subcode, punctured code, shortened code, projected code.**

I. Introduction

THE notion of subspace subcodes of Reed-Solomon (SS-RS) codes was introduced in the mid-1990's by Hattori *et al.* [15]. However this previous work concerns only subspace subcodes of cyclic Reed-Solomon codes of length $q^m - 1$ over the finite field $\mathbb{F}_{q^m}$. The problem was to find an exact formula for the dimension of subspace subcodes depending on the roots of the generator polynomial of the cyclic code.

Our approach is more general since we look at properties of subspace subcodes of any $\mathbb{F}_{q^m}$-linear code. We generalize also our study to generalized subspace subcodes, for which the projection subspaces may vary from coordinate to coordinate.

This paper is organized as follows: in Section II we recall some definitions and results in coding theory. We look in particular at the notions of shortened and punctured codes, the notion of additive block codes over the alphabet $\mathbb{F}_q^m$ and their link with q-ary image of a code over $\mathbb{F}_{q^m}$. We also specify the different notions of equivalence in the context of m-block codes over $\mathbb{F}_q^m$.

Section III is devoted to the study of subspace subcodes and their duals, the projected codes. We specify these notions in the context of q-ary image and we explain why subfield subcodes and trace codes are particular cases of subspace subcodes and projected codes.

In Section IV we generalize the notions of subspace subcodes and projected codes by changing the projections on each block of an additive code over $\mathbb{F}_q^m$. In the particular case of subspaces of dimension 1 or $m-1$, we explicit the link between generalized subspace subcodes of a code $\mathcal{C}$ and subspace subcodes of $\mathbb{F}_{q^m}$-linearly equivalent codes of $\mathcal{C}$. We also give a characterization of projections which preserve some elements of the permutation group of the parent code.

In Section V we specify our results in the context of Reed-Solomon codes and Generalized Reed-Solomon codes and give some examples. We introduce also the notion of exceptional subspace subcode. When a subspace subcode is exceptional, we introduce an orthogonal construction of subspace subcodes and provide some interesting examples.

Finally in Section VI we present some results on the security of generalized subspace subcodes of Reed-Solomon for cryptographic applications. In particular, we extend the Sidel'nikov Shestakov attack to the codes that are $GL_q(m)$-multipliers equivalent to a q-ary image of a Generalized Reed-Solomon code. We introduce an efficient algorithm for an exhaustive search of projections for a subspace subcode of a q-ary image code. We conclude by showing that the folding attack presented in [12], [13] holds also for induced quasi-cyclic or quasi-dyadic generalized subspace subcodes of Reed-Solomon codes.

II. Preliminaries

A. Shortened Codes and Punctured Codes

Shortening and puncturing codewords are classical transformations on codes. The reader can refer for instance to [10], [17], [19] for more details. Let $\mathcal{C}$ be an $[n, k, d]$ linear code and I be a subset of $\{1, 2, \ldots, n\}$.

Definition 1: The punctured code of $\mathcal{C}$ on positions I is the code $\mathrm{Punct}_I(\mathcal{C})$ obtained from the codewords of $\mathcal{C}$ by deleting the coordinates indexed by I.

Manuscript received May 17, 2018; revised January 2, 2019; accepted March 21, 2019. Date of publication April 11, 2019; date of current version July 12, 2019. C. T. Gueye and J. B. Klamti were supported in part by CEA-MITIC for CBC Project and in part by the Government of Senegal's Ministry of Higher Education and Research for ISPQ Project.

T. P. Berger is with XLIM, UMR 7252, Université de Limoges, F-87000 Limoges, France (e-mail: thierry.berger@unilim.fr).

C. T. Gueye and J. B. Klamti are with the Faculté des Sciences et Techniques, DMI, LACGAA, Université Cheikh Anta Diop, Dakar 5005, Sénégal (e-mail: cheikht.gueye@ucad.edu.sn; jklamty@gmail.com).

Communicated by V. Sidorenko, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2019.2909872

We denote by $\tilde{\mathcal{C}}_I$ the subcode of $\mathcal{C}$ constituted of codewords $c = (c_1, \ldots, c_n) \in \mathcal{C}$ such that $c_i = 0$ for all $i \in I$, that means: $\tilde{\mathcal{C}}_I = \{c = (c_1, \ldots, c_n) \in \mathcal{C} \mid c_i = 0,\ \forall i \in I\}$.

Definition 2: The shortened code of $\mathcal{C}$ on positions I is the code $\mathrm{Short}_I(\mathcal{C})$ obtained by puncturing its subcode $\tilde{\mathcal{C}}_I$ on I: $\mathrm{Short}_I(\mathcal{C}) = \mathrm{Punct}_I(\tilde{\mathcal{C}}_I)$.

If $I = \{j\}$, we denote $\mathrm{Punct}_I(\mathcal{C})$ by $\mathrm{Punct}_j(\mathcal{C})$ and $\mathrm{Short}_I(\mathcal{C})$ by $\mathrm{Short}_j(\mathcal{C})$.

Let $\mathcal{C}$ be an $[n, k, d]$ linear code and i, $1 \leq i \leq n$, be an integer. If the parameters of $\mathrm{Punct}_i(\mathcal{C})$ and $\mathrm{Short}_i(\mathcal{C})$ are respectively $[n-1, k_p, d_p]$ and $[n-1, k_s, d_s]$, then $d_s \geq d$, $d_s \geq d_p \geq d-1$ and, if $\mathrm{Punct}_i(\mathcal{C}) \neq \mathrm{Short}_i(\mathcal{C})$ then $k_p = k$ and $k_s = k-1$.

More generally, if $|I| = r$, then we have $d_s \geq d$, $k_s \geq k-r$, $d_p \geq d-r$ and $k_p \geq k-r$.

The following proposition is a well-known result describing the link between the shortened codes and the punctured codes ([17], p. 91, Lemma 8.5.1):

Proposition 1: The dual of a shortened code is the punctured of the dual code on the same positions: $(\mathrm{Short}_I(\mathcal{C}))^\perp = \mathrm{Punct}_I(\mathcal{C}^\perp)$.

B. Block Codes Over $\mathbb{E} = \mathbb{F}_q^m$

In this section, we will define the notion of block codes for which the alphabet is not a single element of a finite field $\mathbb{F}_q$, but an m-tuple of elements of $\mathbb{F}_q$. As we will see in Section II-D, this notion arises naturally then we want to represent for instance an element of the extension field $\mathbb{F}_{2^8}$ as a byte, *i.e.* an element of $\mathbb{F}_2^8$. In that situation, the relevant metric is not necessary at bit level, but at m-block level. Therefore, we will introduce the notion of block codes, *i.e.* codes having for alphabet the set of m-tuples $\mathbb{E} = \mathbb{F}_q^m$. For more details on block codes, the reader can refer to [4].

Definition 3: Let $(A, +)$ be an additive group. An additive code of length n over A is an additive subgroup of $(A^n, +)$.

Definition 4: An m-block code of length n over $\mathbb{E} = \mathbb{F}_q^m$ is an additive code over the additive group $(\mathbb{E}^n, +)$ which is stable by scalar multiplication by any element λ of $\mathbb{F}_q$. The integer m is the size of the blocks.

Note that the condition on the scalar multiplication is not necessary if $q = p$ is a prime number. Since $\mathbb{E}^n$ is an $\mathbb{F}_q$-linear vector space of dimension nm isomorphic to $\mathbb{F}_q^{nm}$, a block code is also an $\mathbb{F}_q$-linear code of length nm. However, in this paper we are not interested in its properties as code of length nm, but in its block properties. In particular, we look at its block-weight w_m, which denotes the number of non-zero blocks.

Since a block code C is an $\mathbb{F}_q$-linear code, it is possible to define the notion of generator matrix, which is nothing else than the generator matrix of the corresponding linear code of length mn over $\mathbb{F}_q$. Even if it is possible to construct the $\mathbb{F}_q$-dual of the linear code of length nm, the notion of duality for block code is not completely obvious. More details on additive block codes, some generalizations of generator matrices and a notion of block-duality can be found in [4].

To allow the comparison of m-block codes with linear codes over $\mathbb{F}_{q^m}$, we use the following notation for parameters as a code C which is either an m-block code or an $\mathbb{F}_{q^m}$-linear code: $[n, k, d]_{q^m}$, where n is the block-length of the code, $k = \log_{q^m}(|C|)$ is the pseudo-dimension of C relative to the size of the alphabet q^m and d is its block-minimum distance. If a code is $\mathbb{F}_{q^m}$-linear, its pseudo-dimension is nothing else than its dimension. In addition, an m-block code is a linear code over $\mathbb{F}_q$, so its pseudo-dimension is not necessarily an integer, but it is always a rational number with a denominator dividing m.

In the sequel, we use the following notations for m-block codewords: If $x \in \mathbb{E}^n$, we set $x = (\overline{x}_1, \ldots, \overline{x}_n)$ and $\overline{x}_i = (x_{i,1}, \ldots, x_{i,m}) \in \mathbb{E}$.

C. Linear Isometries of m-Block Codes

It is well-known [16] that the linear isometries for the Hamming distance on $\mathbb{F}_{q^m}^n$ form a group generated by the permutations of the support and the scalar multiplications by invertible elements of $\mathbb{F}_{q^m}$ on each coordinate. From a matrix point of view, it is the monomial group $\mathrm{Mon}_n(\mathbb{F}_{q^m})$ of $n \times n$ matrices over $\mathbb{F}_{q^m}$ with one and only one non-zero element on each row and each column.

These results can be extended to block codes. Clearly, if we permute the coordinates (at $\mathbb{E}$-level) of an m-block code C of length n, we obtain another m-block code C' with same length, pseudo-dimension and m-block distance.

More in detail, if $\pi \in \mathrm{Sym}(n)$ is a permutation of the symmetric group acting on $\{1, \ldots, n\}$, then $\pi(x) = (\overline{x}_{\pi^{-1}(1)}, \ldots, \overline{x}_{\pi^{-1}(n)})$. A permutation can be represented by a right multiplication of codewords by its matrix representation. However, in the case of block codes, we must pay attention to the level at which we work, since it is possible to apply $n \times n$ matrices on $\mathbb{E}^n$ or $nm \times nm$ matrices on $\mathbb{F}_q^{nm}$.

For a given permutation $\pi \in \mathrm{Sym}_n$, we denote by $\overline{\Pi}$ the permutation matrix of size $n \times n$ and by $\Pi = \overline{\Pi} \otimes I_m$ the corresponding $nm \times nm$ matrix. For instance, if $n = 3$, $m = 2$ and π is the circular permutation on 3 elements, then

$$\overline{\Pi} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and } \Pi = \left(\begin{array}{cc|cc|cc} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right).$$

The operation corresponding to scalar multiplications consists in applying some linear automorphisms of $\mathbb{E}$ on each coordinate (as element of $\mathbb{E}$). Let $GL_q(m)$ denotes the group of invertible matrices of size m with entries in $\mathbb{F}_q$. If $\overline{x} \in \mathbb{E}$ and $M \in GL_q(m)$, then the map $\overline{x} \mapsto \overline{x}M$ is a linear automorphism of $\mathbb{E}$ and $GL_q(m)$ is isomorphic to the group of linear automorphisms of $\mathbb{E}$.

Let $L = (M_1, \ldots, M_n) \in GL_q(m)^n$ be an ordered set of elements of $GL_q(m)$. It is easy to verify that the map $x = (\overline{x}_1, \ldots, \overline{x}_n) \mapsto L(x) = (\overline{x}_1 M_1, \ldots, \overline{x}_n M_n)$ is a linear isometry for the m-block distance. From a matrix point of view, it consists in multiplying on the right the elements of $\mathbb{E}^n = \mathbb{F}_q^{nm}$ by the n-block diagonal matrix $\mathrm{Diag}(L) = \mathrm{Diag}(M_1, \ldots, M_n)$.

Such a set L is called a *multiplier*. The following theorem gives a full characterization of isometries for m-block distance.

Theorem 1: The $\mathbb{F}_q$-isometries of $\mathbb{E}^n$ (*i.e.* linear isomorphisms preserving the Hamming block-weight) is the group generated by the m-block permutations and the multipliers.

Proof: We have already seen that m-block permutations and multipliers are linear isometries.

Reciprocally, let g be an isometry of $\mathbb{E}^n$. We look at the images of elements of $\mathbb{E}^n$ of block weight 1 by g. For $1 \leq i \leq n$, let V_i be the subspace of $\mathbb{E}^n$ of elements with all block component equal to 0 except the i-th: if $x \in V_i$, then $x = (0, \ldots, 0, \overline{x_i}, 0, \ldots, 0)$, $\overline{x_i} \in \mathbb{E}$. Pick an element $x \in V_i$. Since g is a block isometry, $y = g(x) \in V_j$ for some j, $1 \leq j \leq n$. Suppose that there exists another element $x' \in V_i$ such that $g(x') \in V_{j'}$, with $j \neq j'$. Clearly $w_m(x + x') = 1$ and $w_m(g(x + x')) = 2$. This implies that $g(V_i) = V_j$. So, g acts as a permutation on the set of V_i, which defines the block-permutation part of our isometry. Applying the inverse of this permutation to g, we can now suppose that, for all i, $g(V_i) = V_i$. If g_i denotes the restriction of g to V_i, g_i must be $\mathbb{F}_q$-linear, moreover, since g_i preserves the block weight, $Ker(g_i) = \{0\}$, so g_i is an automorphism, and g is a multiplier. ∎

We are now able to define the notion of equivalence of block codes.

Definition 5: Let C and C' be two m-block codes of length n over $\mathbb{E}$. The codes C and C' are equivalent if there is an isometry $f = L \circ \pi$, (where L is a multiplier and π a permutation) such that $C' = f(C)$.

To simplify the presentation of our results, we introduce three more restrictive notions of equivalence of codes.

Definition 6: Let C and C' be two m-block codes of length n over $\mathbb{E}$.

- C and C' are equivalent by permutation if there exists a permutation $\pi \in \mathrm{Sym}(n)$ such that $C' = \pi(C)$.
- C and C' are equivalent by multiplier if there exists a multiplier $L \in GL_q(m)^n$ $C' = L(C)$.
- C and C' are scalar equivalent if there exists a matrix $M \in GL_q(m)$ such that $C' = L_M(C)$ where L_M is the "scalar" multiplier $(M, \ldots, M)$.

If $m = 1$, the multiplication by $M \in GL_q(m)$ corresponds to the multiplication by an element $\beta \in \mathbb{F}_q^*$. So, the notion of scalar equivalence is trivial, since it is just the multiplication of codewords by a scalar β. However, this notion of scalar equivalence makes sense for m-block codes with $m > 1$.

There is no natural notion of duality for the block structure of a F_q-linear code over $\mathbb{E}^n$. However, we can look at the dual of a block code C considered as a code of length nm over $\mathbb{F}_q$.

Proposition 2: Let C be an additive code of length n over $\mathbb{E}$, $L = (M_1, \ldots, M_n) \in GL_q(m)^n$ be a multiplier and $C' = L(C)$. Let $L^* = ((M_1^{-1})^T, \ldots, (M_n^{-1})^T) \in GL_q(m)^n$. The relationship between the dual of C and the dual of C' is then $C'^{\perp} = L^*(C^{\perp})$.

Proof: Let $< ., . >$ denotes the inner product on $\mathbb{F}_q^{nm}$. If $x = (\overline{x}_1, \ldots, \overline{x}_n) \in \mathbb{E}^n$ and $y = (\overline{y}_1, \ldots, \overline{y}_n) \in \mathbb{E}^n$, then we have $< x, y >= \sum_{i=1}^n \sum_{j=1}^m x_{i,j}\, y_{i,j} = \sum_{i=1}^n \overline{x}_i \overline{y}_i^T$. Applying this property to $L(x)$ and $L^*(y)$, we obtain $< L(x), L^*(y) >= \sum_{i=1}^n \overline{x}_i M_i (\overline{y}_i (M_i^{-1})^T)^T = \sum_{i=1}^n \overline{x}_i M_i M_i^{-1} \overline{y}_i^T =< x, y >$.

Consequently, we have $< x, y >= 0$ if and only if $< L(x), L^*(y) >= 0$, which completes the proof. ∎

In addition, it is easy to verify that the dual of a permuted block code is the permuted block code of its dual.

D. q-Ary Images of a Code of Length n Over $\mathbb{F}_{q^m}$

Most examples of m-block codes arise when you want to represent a code on an extension field $\mathbb{F}_{q^m}$ with the elements of a prime field, typically $\mathbb{F}_2$ for $q = 2$.

As usual in this situation, we fix a basis $\mathcal{B} = (b_1, \ldots, b_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We denote by $\phi_{\mathcal{B}}$ the corresponding $\mathbb{F}_q$-linear isomorphism $\mathbb{F}_{q^m} \mapsto \mathbb{F}_q^m$.

The mapping $\phi_{\mathcal{B}}$ can be extended to the whole space $\mathbb{F}_{q^m}^n$: if $c = (c_1, \ldots, c_n) \in \mathbb{F}_{q^m}^n$, then $\Phi_{\mathcal{B}}(c) = (\phi_{\mathcal{B}}(c_1), \ldots, \phi_{\mathcal{B}}(c_n))$.

Definition 7: The q-ary image of a code $\mathcal{C}$ relative to the basis $\mathcal{B}$ is the image $\mathrm{Im}_q(\mathcal{C}) = \Phi_{\mathcal{B}}(\mathcal{C})$ of $\mathcal{C}$ by $\Phi_{\mathcal{B}}$.

The code $\mathrm{Im}_q(\mathcal{C})$ is clearly an $\mathbb{F}_q$-linear code of length nm. It can also be considered as an m-block code of length n. Note that this code is dependent on the choice of the basis $\mathcal{B}$. The following proposition describes the effect of a projection basis change. Its proof is a straightforward verification.

Proposition 3: Let $\mathcal{B}$ and $\mathcal{B}'$ be two basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $M \in GL_q(m)$ denotes the basis change matrix from $\mathcal{B}$ to $\mathcal{B}'$, *i.e.* the matrix such that $\phi_{\mathcal{B}'}(c) = \phi_{\mathcal{B}}(c)M$ for all $c \in \mathbb{F}_q^m$. The q-ary image $\Phi_{\mathcal{B}'}(\mathcal{C})$ of a code $\mathcal{C}$ relative to the basis $\mathcal{B}'$ is scalar equivalent by the multiplier L_M to its q-ary image $\Phi_{\mathcal{B}}(\mathcal{C})$ by $\Phi_{\mathcal{B}}$.

If we want to construct a generator matrix G of $\mathrm{Im}_q(\mathcal{C})$ over $\mathbb{F}_q$ from those $\mathcal{G}$ of $\mathcal{C}$ over $\mathbb{F}_{q^m}$, since $\mathrm{Im}_q(\mathcal{C})$ is not $\mathbb{F}_{q^m}$-linear, we need to take the multiples of the rows of $\mathcal{G}$ by the elements of $\mathbb{F}_{q^m}$. In fact, it is sufficient to take m multiples $\mathbb{F}_q$-linearly independent.

For the purpose of this paper, we need to introduce a specific generator matrix of the q-ary image of a code $\mathcal{C}$. For any element $\beta \in \mathbb{F}_{q^m}$, the map ϕ_β: $x \mapsto \beta x$ is an $\mathbb{F}_q$-linear automorphism of F_{q^m}. Its image by $\phi_{\mathcal{B}}$ is an automorphism of $\mathbb{F}_q^m$. We denote by M_β the matrix of the corresponding automorphism: with obvious notations, if $\phi_{\mathcal{B}}(x) = (x_1, \ldots, x_m)$ then $\phi_{\mathcal{B}}(\beta x) = (x_1, \ldots, x_m)M_\beta$.

Proposition 4: If $\mathcal{G} = (\beta_{i,j})$ is a $k \times n$ generator matrix of $\mathcal{C}$, then the $km \times nm$ matrix G obtained by replacing each entry $\beta_{i,j}$ by the corresponding $m \times m$ matrix $M_{\beta_{i,j}}$ is an $\mathbb{F}_q$-generator matrix of $\mathrm{Im}_q(\mathcal{C})$. Moreover, the matrix G is of full rank km.

Proof: The fact that G generates the full code $Im_{\mathcal{B}}(\mathcal{C})$ comes directly from the fact that $\Phi_{\mathcal{B}}$ is an isomorphism. In addition the two codes have the same number of elements, which implies that G is of rank km. ∎

As a direct consequence, we obtain the following corollary:

Corollary 1: If $\mathcal{C}$ is an $[n, k, d]$ $\mathbb{F}_{q^m}$-linear code, then $\mathrm{Im}_q(\mathcal{C})$ is an $[nm, km, d_q \geq d]$ $\mathbb{F}_q$-linear code.

Note that if we look at $\mathrm{Im}_q(\mathcal{C})$ as an m-block codes, these m-block parameters are $[n, k, d]_{q^m}$.

The construction described in Proposition 4 is of great importance for reconstructing an $\mathbb{F}_{q^m}$-linear code from one of its q-ary image. That is why we introduce the following definition:

Definition 8: Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear code and C its q-ary image relative to $\mathcal{B}$. If $\mathcal{G}$ is a generator matrix of $\mathcal{C}$, the matrix G described in Proposition 4 is called the canonical q-ary image of $\mathcal{G}$ (relative to the basis $\mathcal{B}$).

The main property of a generator matrix which is a canonical q-ary image of a generator matrix over $\mathbb{F}_{q^m}$ is the fact that it is possible to extract the $m \times m$ q-ary matrices which correspond to a representation of the finite field $\mathbb{F}_{q^m}$. In particular these matrices are either 0 or lie in a same cyclic group of order q^m-1 which is stable by addition if we add the null matrix. So, from a canonical q-ary image, it is possible to reconstruct $\mathbb{F}_{q^m}$ and the code $\mathcal{C}$ (up to the identification of $\mathbb{F}_{q^m}$ with its matrix group representation).

In addition, note that, up to a permutation of the support, a code $\mathcal{C}$ always admits a systematic generator matrix. It is easy to see that the canonical q-ary image of a systematic generator matrix is itself the systematic generator matrix of the q-ary image $Im_q(\mathcal{C})$. So, if a given m-block code C is a q-ary image of another code $\mathcal{C}$ over the extension $\mathbb{F}_{q^m}$, it is always possible to recover the extension field construction.

If $\mathcal{B}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the dual basis $\mathcal{B}^*$ of $\mathcal{B}$ is the unique basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that, for any element $\beta \in \mathbb{F}_{q^m}$, if M_β is the matrix corresponding to the multiplication by β in the representation associated to $\mathcal{B}$, the matrix corresponding to the multiplication by β associated to $\mathcal{B}^*$ is its transpose M_β^T.

The following proposition describes the link between the duality over $\mathbb{F}_q$ and the duality over $\mathbb{F}_{q^m}$.

Proposition 5: Let $\mathcal{C}$ be a code over $\mathbb{F}_{q^m}$ and $\mathcal{C}^\perp$ be its $\mathbb{F}_{q^m}$-dual. The dual of the q-ary image of $\mathcal{C}$ relative to the basis $\mathcal{B}$ is the q-ary image of its dual $\mathcal{C}^\perp$ relative to the dual basis $\mathcal{B}^*$ of $\mathcal{B}$.

Proof: Let $\mathcal{G} = (\beta_{i,j})$ and $\mathcal{H} = (\gamma_{i,j})$ be respectively a generator matrix of $\mathcal{C}$ and of its dual $\mathcal{C}^\perp$. A generator matrix of the q-ary images of $\mathcal{C}$ relative to $\mathcal{B}$, resp. of $\mathcal{C}^\perp$ relative to $\mathcal{B}^*$ is $G = (M_{\beta_{i,j}})$, resp. $H = (M^T_{\gamma_{i,j}})$. By definition, we have $\mathcal{G} \times \mathcal{H}^T = 0$, which implies

$$G \times H^T = (M_{\beta_{i,j}}) \times (M^T_{\gamma_{i,j}})^T = 0.$$

■

Example 1: We choose $q = 2$ and $m = 3$. So $\mathbb{F}_{q^m} = \mathbb{F}_2(\alpha)$, where α is a root of $X^3 + X + 1$. The identification between $\mathbb{F}_8$ and $\mathbb{F}_2^3$ is done using the basis $\mathcal{B} = (1, \alpha, \alpha^2)$.

The following matrix is a generator matrix of a Reed-Solomon code of parameters $[7, 2, 5]_8$ over $\mathbb{F}_8$. Such a code will be defined in Section V-B. It is denoted RS_2 since its dimension is 2.

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & \alpha & \alpha^4 & \alpha^6 & \alpha^3 & \alpha^2 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & \alpha & \alpha^6 \end{pmatrix}.$$

The matrix representation of the multiplication by α in $\mathbb{F}_2^3$ is $M_\alpha = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

For $i \in [1, 7]$, $M_{\alpha^i} = M_\alpha^i$. So, we can construct the canonical generator matrix of its binary image C relative to $\mathcal{B}$:

$$G = \left(\begin{array}{c|c|c|c|c|c|c} 100 & 000 & 010 & 001 & 101 & 110 & 001 \\ 010 & 000 & 001 & 111 & 100 & 011 & 110 \\ 001 & 000 & 110 & 101 & 010 & 111 & 011 \\ \hline 000 & 100 & 110 & 111 & 001 & 010 & 101 \\ 000 & 010 & 011 & 101 & 110 & 001 & 100 \\ 000 & 001 & 111 & 100 & 011 & 110 & 010 \end{array}\right)$$

As a 3-block code, the parameters of C are $[7, 2, 5]_8$. As a binary code, its parameters are $[21, 6, 7]_2$ (its minimum distance d was computed using MAGMA [9]).

III. Subspace Subcodes

The notion of subspace subcode was introduced by Hattori *et al.* [15]. However, this previous work was essentially devoted to the cyclic properties of subspace subcodes of Reed-Solomon codes of length $2^m - 1$. In [14], the authors studied the subspace subcodes of Gabidulin codes in the context of rank metric. Our approach concerns any m-block code or code over an extension field without looking at cyclic properties.

In this section, we will first introduce the notion of subspace subcodes of m-block codes and an interpretation in term of shortened codes. We then introduce the dual notion of projected codes, which are related to punctured codes. Finally, we specify our results in the context of q-ary images of a linear code over the extension field $\mathbb{F}_{q^m}$. In particular, we examine the relationship between subspace subcodes (resp. projected codes) and subfield subcodes (resp. trace codes).

A. Subspace Subcodes of m-Block Codes

In this section, we present the notion of subspace subcodes of m-block codes. The specific notion of subspace subcodes of codes over an extension field will be developed in Section III-C.

Let C be an m-block code over $\mathbb{E}$ and V be a subspace of $\mathbb{E}$ of dimension $\mu \leq m$.

Definition 9: The subspace subcode of C is the subcode $C_{|V}$ of codewords in C with coordinates in V: $C_{|V} = C \cap V^n$.

Since a subspace V of dimension μ is isomorphic to $\mathbb{F}_q^\mu$, a subspace subcode can be identified to an μ-block code. This can be done by the choice of a basis of V. Following Section II-D, if $\mathcal{B}_V$ denotes a basis of V, $\psi_{\mathcal{B}_V}$ is the mapping which sends an element $v \in V$ on the μ-tuple of its coordinates and $\Psi_{\mathcal{B}_V}$ is the extension of $\psi_{\mathcal{B}_V}$ to codewords in V^n.

Definition 10: The μ-block representation of a subspace subcode of C over a subspace $V \subset \mathbb{E}$ relative to a basis $\mathcal{B}_V$ is $SS_V(C) = \Psi_{\mathcal{B}_V}(C_{|V}) \subseteq (\mathbb{F}_q^\mu)^n$.

As in the case of q-ary image, the μ-block representation of a subspace subcode is dependent on the choice of the basis $\mathcal{B}_V$. Changing the basis $\mathcal{B}_V$ leads to another μ-block code representation, however all these representations are scalar equivalent at μ-block level.

Proposition 6: Two representations C_1 and C_2 of a same subspace subcode $C_{|V}$ are scalar equivalent. Reciprocally, if a μ-block code C_2 is scalar equivalent to a representation C_1

of a subspace subcode $C_{|V}$, then there exists a basis $\mathcal{B}'_V$ such that C_2 is the μ-block representation of another representation of $C_{|V}$ relative to $\mathcal{B}'_V$.

Proof: A basis of V corresponds to a generator matrix of V viewed as a linear code of length m and dimension μ over $\mathbb{F}_q$. A change of basis for V corresponds to a left multiplication by a matrix in $GL_q(\mu)$. The proof of our proposition comes directly from this remark and Definition 6. ∎

We want to emphasize that there is a subtlety in our notations of subspace subcodes: the code $C_{|V} = C \cap V^n$ is an m-block code, since it has coordinates in $V \subset \mathbb{F}_q^m$, whereas the notation $SS_V(C)$ denotes its representation as an μ-block code with an explicit or implicit choice of basis $\mathcal{B}_V$ for V.

The μ-block representation of a subspace subcode can be interpreted in term of shortened code.

Let $\mathcal{B}_V$ be a basis of V. We complete this basis into a basis $\widetilde{\mathcal{B}_V}$ of $\mathbb{E}$ by adding $m-\mu$ linearly independent vectors. If G_V is the generator matrix of V derived from $\mathcal{B}_V$, we obtain a matrix $\widetilde{G_V} \in GL_q(m)$ by adding $m-\mu$ linearly independent rows to G_V.

If $\overline{x} \in \mathbb{E}$, then the m-tuple $\overline{x}\widetilde{G_V}^{-1}$ gives the coordinates of $\overline{x}$ on this new basis $\widetilde{\mathcal{B}_V}$. So, an element $\overline{x}$ is in V if and only if the $m-\mu$ last coordinates of $\overline{x}\widetilde{G_V}^{-1}$ are 0.

Proposition 7: Let $\mathcal{B}_V$ be a basis of V and $\widetilde{G_V}$ be a matrix constructed as described previously. The representation relative to the basis $\mathcal{B}_V$ of a subspace subcode $C_{|V}$ as an μ-block code is the code obtained by applying to C the scalar multiplier $L_{\widetilde{G_V}^{-1}}$ and then by shortening the $m-\mu$ last coordinates of each block of size m.

Proof: It is a direct consequence of the previous remarks on $\overline{x}' = \overline{x}\widetilde{G_V}^{-1}$: $\overline{x} \in \mathbb{E}$ is in V if the $m-\mu$ last coordinates of $\overline{x}'$ are 0, and, under this hypothesis, the μ first coordinates of $\overline{x}'$ are those of $\overline{x}$ on the basis $\mathcal{B}_V$. ∎

Corollary 2: Let C be an m-block code of parameters $[n,k,d]_{q^m}$ and $C' = \mathrm{SS}_V(C)$ a μ-block subspace subcode of C. If k' and d' are respectively the μ-block pseudo-dimension and the μ-block minimum distance of C', then we have the following inequalities: $k' \geq (km - n(m-\mu))/\mu$ and $d' \geq d$.

Proof: The bounds are those obtained by considering the $\mathrm{SS}_V(C)$ code as a shortened code (cf. Section II-A). ∎

B. Projected Codes

In this section, we will introduce the notion of projected codes and show that these projected codes are duals of subspace subcodes.

As previously, μ denotes an integer less than or equal to m which is not necessarily a divisor of m. Let ψ be an $\mathbb{F}_q$-linear map from $\mathbb{E}$ onto $\mathbb{F}_q^\mu$ of full rank μ. We denote by Ψ the action of ψ on each coordinate of a word in $\mathbb{E}^n$.

Definition 11: The (μ-)projected code relative to ψ of an m-block code C of length n is the μ-block code $\mathrm{P}_\psi(C) = \Psi(C)$ of same length n.

In practice a projection map ψ is represented by an $m \times \mu$ matrix P_ψ of rank μ: $\psi(\overline{x}) = \overline{x}P_\psi$. The whole projection matrix Ψ is then $P_\Psi = \mathrm{Diag}(P_\psi, \ldots, P_\psi)$.

A projected code $\Psi(C)$ can be interpreted in term of punctured code. As in the previous Section, the matrix P_ψ can be completed in an invertible matrix P of size m by adding $m-\mu$ well-chosen columns.

Proposition 8: Let P_ψ be the matrix of a projection ψ and P its completion as a matrix of $GL_q(m)$. The projection code $\psi(C)$ can be constructed by applying the scalar multiplier L_P, and then by puncturing $m-\mu$ last coordinates of each m-block in order to obtain a μ-block code.

Proof: Let $I_{m,\mu}$ be the $m \times \mu$ matrix constituted from the identity matrix I_μ to which we add $m-\mu$ zero rows. Clearly, we have the equality $P_\psi = PI_{m,\mu}$. On another side, applying $\mathrm{Diag}(I_{m,\mu}, \ldots, I_{m,\mu})$ to an m-block codeword x corresponds to puncturing the $m-\mu$ last coordinates of each m-block of x, which complete our proof. ∎

Since puncturing and shortening operation are dual, the same results hold for the subspace subcodes and projection codes operations.

Proposition 9: Let C be an m-block code, $\mathcal{B}_V$ a basis of a vector space V and G_V the corresponding generator matrix of V. The dual of the representation of the subspace subcode $SS_V(C)$ relative to B_V is the projected code with projection matrix G_V^T.

Proof: Let $\widetilde{G_V}$ be a matrix constructed as above from G_V. Let C' be the image of C by the scalar multiplier $L_{\widetilde{G_V}^{-1}}$. Since the dual of a shortened code is a punctured code (Proposition 1), from Propositions 11 and 8, we deduce that $C'^{\perp}$ is the image of $C^{\perp}$ by the scalar multiplier $L_{\widetilde{G_V}^T}$. The result is then a direct application of Proposition 2. ∎

C. Subspace Subcodes of Codes Over an Extension Field

In this section, we specify our previous results in the context of linear codes over $\mathbb{F}_{q^m}$ and their q-ary image. At $\mathbb{F}_{q^m}$ level, one can naturally define a subspace subcode as follows:

Definition 12: Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_{q^m}$. Let $V \subset \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension $\mu \leq m$. The subspace subcode $\mathcal{C}_{|V}$ is the restriction of $\mathcal{C}$ to V^n: $\mathcal{C}_{|V} = \mathcal{C} \cap V^n$.

The code $\mathcal{C}_{|V}$ is no more $\mathbb{F}_{q^m}$-linear, but it remains $\mathbb{F}_q$-linear. The most famous example of such subspace subcodes is those of subfield subcodes. In that situation, $\mu = 1$ and V is the subfield $\mathbb{F}_q$.

If we want to construct a μ-block representation of a subspace subcode of a code $\mathcal{C}$ over the extension field $\mathbb{F}_{q^m}$, we need two steps:

- The first one is the choice of a basis $\mathcal{B}$ required to identify $\mathbb{F}_{q^m}$, to $\mathbb{F}_q^m$ as $\mathbb{F}_q$-vector spaces.
- The second one consists in choosing a basis $\mathcal{B}_V$ of V given as a generator matrix relative to the canonical basis of $\mathbb{E}$.

So, starting from a code $\mathcal{C}$, we construct first its q-ary image relative to $\mathcal{B}$, and then its representative as μ-block code using $\mathcal{B}_V$. Such a representative is denoted $SS_V(\mathcal{C})$.

From a dual point of view, one can also define μ-block projected codes of an $\mathbb{F}_{q^m}$ linear code $\mathcal{C}$.

Definition 13: Let ψ be an $\mathbb{F}_q$-linear projection from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q^\mu$ of full rank μ. Let Ψ be the extension of ψ to $(\mathbb{F}_{q^m})^n$.

The μ-projected code of $\mathcal{C}$ relative to ψ is the μ-block code $\Psi(\mathcal{C})$.

If we choose for ψ the trace function $Tr_q(x) = \sum_{i=0}^{m-1} x^{q^i}$, then we obtain the classical trace code.

One of the main results about subfield subcode and trace code is the fact that they are dual operations ([19], Th.11, Ch. 7 §7). Our approach shows that this result is a simple particular case of the duality of shortening and puncturing operations.

To conclude this section we want to emphasize two technical difficulties then we start from a code at $\mathbb{F}_{q^m}$ level.

The first one is related to the choice of the basis $\mathcal{B}$: for a fixed basis of V, if we change the basis $\mathcal{B}$ into another basis $\mathcal{B}'$, in accordance with this new choice, we have to change the generator matrix of V by multiplying on the right G_V by the appropriate basis change matrix. However, these operations have no effect on the obtained μ-block code.

The second one is on the duality: at $\mathbb{F}_{q^m}$ level, the fact that the dual of a μ-block representative of a subspace subcode of $\mathcal{C}$ is a μ-projection of its dual. However, Proposition 5 shows that it is necessary to use the dual basis $\mathcal{B}^*$ in the construction of the correct projection.

IV. Generalized Subspace Subcodes

As mentioned in the conclusion of [15], a natural way to generalize subspace subcodes is to use different subspaces on each component. In this section, we study this generalization and present some results on this topic, particularly for $\mu = 1$ and $\mu = m - 1$.

A. Definitions

Let C be an m-block linear code of length n. Let μ be an integer less than m. Let $V_1, \ldots, V_n$ be a set of n subspaces of $\mathbb{E}$ of dimension μ. Set $\overline{V} = (V_1, \ldots, V_n)$, constituted of n-tuples with the i-th coordinate in V_i.

Definition 14: The generalized (μ-)subspace subcode of C relative to $\overline{V}$ is $C_{|\overline{V}} = \mathcal{C} \cap \overline{V}$.

Let $\psi_1, \ldots, \psi_n$ be a set of n $\mathbb{F}_q$- linear projections of full rank μ from $\mathbb{E}$ onto $\mathbb{F}_q^\mu$. We denote by $\overline{\Psi}$ the $\mathbb{F}_q$-linear projection from $\mathbb{E}^n$ to $(\mathbb{F}_q^\mu)^n$ obtained by applying ψ_i to the i-th component of m-block codewords.

Definition 15: The generalized (μ-)projected code of C relative to $\overline{\Psi}$ is $\overline{\Psi}(\mathcal{C})$.

As in Section III-A, if we want to construct a μ-block representative of $C_{|\overline{V}}$, we need to choose a basis, *i.e.* a generator matrix G_{V_i} for each subspace V_i. Such a representative is denoted $GSS_{\overline{V}}(C)$.

The following proposition describes the relationship between generalized notions of subspace subcodes or projected codes and the multiplier equivalence of m-block codes.

Proposition 10: A generalized subspace subcodes of an m-block code C is a subspace subcode of a code C' which is multiplier equivalent to C (Definition 5 at m-block level). A generalized projected code of an m-block code C is a projected code of a code C' which is multiplier equivalent to C.

Proof: Let C be an m-block linear code, $\overline{V}$ an n-tuple of vector spaces V_i of dimension μ and G_{V_i} a generator matrix of V_i for $i \in [1, n]$.

We set $V = V_1$ and $G_V = G_{V_1}$. Since all the V_i's have the same dimension μ, there exists $n-1$ matrices $M_i \in GL_q(m)$, $2 \leq i \leq n$ such that $G_{V_i} = G_V \times M_i$. In addition, we set $M_1 = I_m$, the identity matrix. Let H be a parity-check matrix of C and $P = \mathrm{Diag}(G_{V_1}^T, \ldots, G_{V_n}^T)$. Clearly, a parity-check matrix of $GSS_{\overline{V}}(C)$ is $H \times P$.

From our previous remark, the matrix P can be decomposed as follows: $P = \mathrm{Diag}(M_1^T, \ldots, M_n^T) \times \mathrm{Diag}(G_V^T, \ldots, G_V^T)$.

Set $H' = H \times \mathrm{Diag}(M_1^T, \ldots, M_n^T)$. From Proposition 5, this matrix H' is a parity-check matrix of the code C' obtained by applying the multiplier $(M_1^{-1}, \ldots, M_n^{-1})$, and $GSS_{\overline{V}}(C) = SS_V(C')$.

The result on generalized projected code comes from duality. ∎

A first consequence of this proposition is the fact that the bounds on the parameters of subspace subcodes given in Corollary 2 apply to generalized subspace subcode.

Following the proof of Proposition 10, we present an algorithm to compute efficiently a generator matrix of a generalized subspace subcode of a code.

Algorithm 1*:* Generator matrix of $\mathrm{GSS}_{\overline{V}}(C)$

Input: G: a generator matrix of an m-block code C. For each $i \in [1..n]$, G_{V_i}: an $\mu \times m$ generator matrix of the subspace V_i where $\overline{V} = (V_1, \ldots, V_n)$.
Output: $\mathcal{G}$ and $\mathcal{H}$: a generator matrix and a parity check matrix of $\mathrm{GSS}_{\overline{V}}(C)$.

- Compute a parity check matrix H of C.
- Set $\mathcal{H} := H \times \mathrm{Diag}(G_{V_1}^T, \ldots, G_{V_n}^T)$. $\mathcal{H}$ is a generator matrix of the dual of $\mathrm{GSS}_{\overline{V}}(C)$.
- From $\mathcal{H}$, compute a generator matrix $\mathcal{G}$ of $\mathrm{GSS}_{\overline{V}}(C)$.

In conclusion of this section, we give an example limited to the construction of the projected code.

Example 2: We set $q = 2$, $m = 3$ and $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ with $\alpha^3 = \alpha + 1$.

The following matrix is a parity-check matrix of a 3-block code of length $n = 5$.

$$H = \left(\begin{array}{c|c|c|c|c} 100 & 000 & 101 & 100 & 101 \\ 010 & 000 & 111 & 010 & 111 \\ 001 & 000 & 011 & 001 & 011 \\ 000 & 100 & 011 & 100 & 111 \\ 000 & 010 & 110 & 010 & 100 \\ 000 & 001 & 111 & 001 & 110 \end{array}\right)$$

We choose $\overline{V} = V_1 V_2 V_1 V_2 V_3$, where V_1 is generated by 1 and α, V_2 by 1 and α^2 and V_3 by α and $\alpha^2 + 1$. We choose for respective generator matrices

$G_{V_1} = \begin{pmatrix} 100 \\ 010 \end{pmatrix}$, $G_{V_2} = \begin{pmatrix} 100 \\ 001 \end{pmatrix}$ and $G_{V_3} = \begin{pmatrix} 101 \\ 010 \end{pmatrix}$.

The generalized subspace subcode $\mathcal{C} = \mathrm{GSS}_{\overline{V}}(C)$ has for parity check matrix

$$P_\Psi(H) = H \times \mathrm{Diag}(G_{V_1}^T, G_{V_2}^T, G_{V_1}^T, G_{V_2}^T, G_{V_3}^T).$$

$$\mathcal{H} = P_\Psi(H) = \left(\begin{array}{c|c|c|c|c} 10 & 00 & 10 & 10 & 00 \\ 01 & 00 & 11 & 00 & 01 \\ 00 & 00 & 01 & 01 & 11 \\ 00 & 10 & 01 & 10 & 01 \\ 00 & 00 & 11 & 00 & 10 \\ 00 & 01 & 11 & 01 & 11 \end{array}\right)$$

Note that, due to the particular form of matrix G_{V_1} (resp. G_{V_2}) a multiplication of a 3-block by G_{V_1} (resp. G_{V_2}) consists in puncturing the last column (resp. the second column) of the corresponding 3-blocks.

B. Generalized Subspace Subcodes of Codes Over the Extension Field

Following the approach of Section III-C, the definition of generalized subspace subcodes can be directly adapted in the context of codes over the extension field $\mathbb{F}_{q^m}$ and their q-ary images.

However, there is one point that deserves our attention. The multiplier equivalence can be applied at $\mathbb{F}_{q^m}$ level or at q-ary image (*i.e.* at m-block code level). For instance, if we look at a multiplier for an $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$ of length n, such a multiplier is of the form $\Lambda = (\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^m}^*)^n$.

If we look at its action on the q-ary image of $\mathcal{C}$, using the same notation than those of Section II-D, it corresponds to the multiplier $L = (M_{\lambda_1}, \ldots, M_{\lambda_1})$. To avoid confusions, the multipliers of the form Λ are called $\mathbb{F}_{q^m}$-multipliers and denoted with Greek letters.

This leads to a natural question: are there generalized subspace subcodes of $\mathcal{C}$ that are not subspace subcode of a code $\mathcal{C}$ equivalent to $\mathcal{C}$ by an $\mathbb{F}_{q^m}$-multiplier Λ?

We will prove in the sequel of this section that the answer is negative for $\mu = 1$ and $\mu = m - 1$ and positive for $1 < \mu < m - 1$.

Beforehand, it is necessary to make a remark on a particular class of generalized subspace subcodes.

Remark 1: In the definition of a representative for an m-block subspace subcode, the same basis $\mathcal{B}_V$ of the vector space V is required. The definition of generalized subspace subcode relaxes this constraint: it is possible to choose the same subspace V on each component, but to change of the basis $\mathcal{B}_{V_i}$'s for the representation of elements of V as μ-tuples.

It is easy to verify that the μ-block codes obtained by the second possibility are multiplier equivalent as μ-block code, *i.e.* the multiplier corresponding to the change of basis on V can be applied after the construction of a subspace subcode.

Proposition 11: For any subspace V of dimension $\mu = 1$ and any $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$, any representation of the 1-subspace subcode $\mathrm{SS}_V(\mathcal{C})$ is the subfield subcode $\mathcal{C} \cap \mathbb{F}_q^n$.

Proof: Remember that $\mathbb{F}_q$ is a subspace of $\mathbb{F}_{q^m}$ of dimension 1. The subfield subcode is the subspace subcode $\mathrm{SS}_{\mathbb{F}_q}(\mathcal{C})$. Let V be a subspace of $\mathbb{F}_{q^m}$ of dimension 1 and $\{\alpha\}$ be basis of V. We have $V = \alpha\mathbb{F}_q$. In particular, if a codeword $c \in \mathcal{C}$ is in $\mathrm{SS}_{\mathbb{F}_q}(\mathcal{C})$, αc is in $\mathrm{SS}_V(\mathcal{C})$ and its representation in the basis $\{\alpha\}$ is c itself. The converse is obvious. ∎

By duality, we obtain the following corollary:

Corollary 3: For any linear projection $\psi \in \mathcal{L}(\mathbb{F}_{q^m}, \mathbb{F}_q)$ and any $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$, any representation of the 1-projected code $\mathrm{P}_\psi(\mathcal{C})$ is the trace code $Tr_q(\mathcal{C})$.

To extend this result to generalized subspace subcodes with subspaces of dimension 1, we need to recall a classical result on the trace function.

Lemma 1: Let f be a linear endomorphism of $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$. There exists a single element $\beta \in \mathbb{F}_{q^m}$ such that $f(x) = Tr_q(\beta x)$ for all $x \in \mathbb{F}_{q^m}$.

Proof: Let $T_q : \mathbb{F}_{q^m}^2 \mapsto \mathbb{F}_q$ be the map defined by $T_q(x, y) = Tr_q(xy)$. T_q is a non-degenerated bilinear map. In consequence, if f_β is the linear endomorphism defined by $f_\beta(x) = Tr_q(\beta x)$, then the application $\beta \mapsto f_\beta$ is an isomorphism between $\mathbb{F}_{q^m}$ and the linear group $\mathcal{L}(\mathbb{F}_{q^m}, \mathbb{F}_q)$. ∎

Note that Proposition 11 does not imply directly the fact that generalized subspace subcodes of a given code $\mathcal{C}$ are subcodes of $\mathbb{F}_{q^m}$-multiplier equivalent codes of $\mathcal{C}$, since in Definition 14, the equivalence is done on q-ary images and it is the notion of m-block equivalence. However we will prove that this result is true.

Theorem 2: Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear code. The generalized 1-subspace subcodes of $\mathcal{C}$ are exactly the subfield subcodes of the codes $\mathcal{C}'$ that are $\mathbb{F}_{q^m}$-multiplier equivalent to $\mathcal{C}$.

Dually, the generalized 1-projected codes $\overline{\Psi}(\mathcal{C})$ are exactly the trace codes of the codes $\mathcal{C}'$ that are $\mathbb{F}_{q^m}$-multiplier equivalent to $\mathcal{C}$.

Proof: We will prove the dual part of this theorem. From Lemma 1, there exists an $\mathbb{F}_{q^m}$-multiplier $\Lambda = (\lambda_1, \ldots, \lambda_n)$ such that $\overline{\Psi}(x) = (Tr_q(\lambda_1\overline{x_1}), \ldots, Tr_q(\lambda_n\overline{x_n}))$. If $\mathcal{C}' = L(\mathcal{C})$, then $\overline{\Psi}(\mathcal{C}) = Tr_q(\mathcal{C}')$. ∎

Similar result holds for $\mu = m - 1$, but Remark 1 must be taken in account. We need the following Lemma:

Lemma 2: The multiplicative group $\mathbb{F}_{q^m}^*$ is transitive on the $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ of dimension $m-1$, *i.e.* for any subspaces V and V' of $\mathbb{F}_{q^m}$ of dimension $m-1$, there exists an element $\alpha \in \mathbb{F}_{q^m}^*$ such that $V' = \alpha V$.

Proof: The non-degenerated bilinear map T_q defined in the proof of Lemma 1 able to define the notion of trace orthogonality. If V is a subspace of $\mathbb{F}_{q^m}$ of dimension μ, then $V^{\perp_T} = \{x \in \mathbb{F}_{q^m} \mid \forall y \in V,\ T_q(x, y) = 0\}$ is a subspace of dimension $\nu = m - \mu$ of $\mathbb{F}_{q^m}$. This correspondence is an one to one correspondence between μ-dimension and ν-dimension subspaces of $\mathbb{F}_{q^m}$.

In addition, if α is an invertible element of $\mathbb{F}_{q^m}$, we have $T_q(\alpha x, \alpha^{-1} y) = T_q(x, y)$. In particular $(\alpha V)^{\perp_T} = \alpha^{-1} V^{\perp_T}$. Consequently, since the multiplicative group $\mathbb{F}_{q^m}^*$ is transitive on the subspaces of dimension 1, it is also transitive on the subspaces of dimension $m - 1$. ∎

We deduce the following proposition and theorem for $\mu = m - 1$.

Proposition 12: Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear code. For $\mu = m - 1$, *i.e.* V is a hyperplane, the μ-subspace subcode $SS_V(\mathcal{C})$ does not depend on the choice of V. All its representations are μ-scalar equivalent. The same results hold for μ-projected codes.

Proof: The proof is essentially the same as those of Proposition 11. The only difference comes from the fact that, for $\mu = 1$ a change of representative corresponds to a scalar multiplication of codewords of $\mathcal{C}$, and for $\mu = m-1$ we have to take into account a change of basis of the hyperplane V, which introduces the μ-scalar equivalence of representatives. The results on projected codes is obtained by duality. ∎

The same reasoning on generalized subspace subcodes leads to the following result.

Theorem 3: Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear code. For $\mu = m-1$, if $GSS_V(\mathcal{C})$ is a generalized μ-subspace subcode of $\mathcal{C}$, then there exists a code $\mathcal{C}'$ $\mathbb{F}_{q^m}$-multiplier equivalent to $\mathcal{C}$ such that $GSS_V(\mathcal{C})$ is μ-block multiplier equivalent to a subspace subcode of $\mathcal{C}'$.

Dually, if $\overline{\Psi}(\mathcal{C})$ is a generalized μ-projection of $\mathcal{C}$, then there exists a code $\mathcal{C}'$ $\mathbb{F}_{q^m}$-multiplier equivalent to $\mathcal{C}$ such that $\overline{\Psi}(\mathcal{C})$ is μ-block multiplier equivalent to a μ-projection $\Psi(\mathcal{C})$ of $\mathcal{C}'$.

These results do not extend to $1 < \mu < m-1$, since the multiplicative group $\mathbb{F}_{q^m}^*$ is transitive on the subspaces of dimension 1 or $m-1$, but is not transitive on the subspaces of other dimension.

For instance, we have the following result:

Proposition 13: Let $\mu \neq 1$ be a divisor of m. There exist μ-subspace subcodes of a $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$ that are not subfield subcodes over $\mathbb{F}_{q^\mu}$ of any $\mathbb{F}_{q^m}$-linear code $\mathcal{C}'$.

Proof: To prove this result, it is sufficient to construct a μ-subspace subcode with a μ-block pseudo dimension which is not an integer. So, it cannot be equivalent to a subfield subcode over $\mathbb{F}_{q^\mu}$. In [15], for $q = 2$, $m = 6$, $n = 63$ and $\mu = 2$, the authors construct a 2-subspace subcode of parameters $[63, 42.5, d \geq 11]_4$ (Example 4.12) which cannot be equivalent to any $\mathbb{F}_4$-linear code. ∎

C. Induced Permutation Groups of Generalized Subspace Subcodes

The purpose of this section is to determine what are the conditions on the construction of subspace subcodes that preserve a permutation of the initial code over the extension field. Our approach is similar to that used in [1]–[3].

As usual, if $\mathcal{C}$ is a linear code of length n over the field $\mathbb{F}_{q^m}$, its permutation group $Per(\mathcal{C})$ is the subset of the symmetric group $\mathrm{Sym}(n)$ which leaves the code $\mathcal{C}$ globally invariant. For an m-block (or μ-block) code, following Section II-C, the notation $Per(C)$ denotes the subgroup of $\mathrm{Sym}(n)$ which leaves C globally invariant under the permutation of blocks.

In this section, we do not need to use the matrix approach for permutations, but only the representation using the indexes: $\pi(x) = (\overline{x}_{\pi^{-1}(1)}, \ldots, \overline{x}_{\pi^{-1}(n)})$, $\overline{x}_i \in \mathbb{E}$ or $\mathbb{F}_q^\mu$.

Our problem is the following: given a linear code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ which is invariant under a permutation π, what are the conditions for V or $\overline{V}$ such that $\mathrm{SS}_V(\mathcal{C})$ or $\mathrm{GSS}_{\overline{V}}(\mathcal{C})$ is invariant under π?

It is easy to verify that, for all subspace V, $\mathrm{Per}(\mathcal{C}) \subseteq \mathrm{Per}(\mathrm{SS}_V(\mathcal{C}))$, and for all projected code $\Psi(\mathcal{C})$, $\mathrm{Per}(\mathcal{C}) \subseteq \mathrm{Per}(\Psi(\mathcal{C}))$.

For the generalized subspace subcode, the situation is a little more delicate. We will decompose the problem under the distinct orbits of a permutation. So, we will look at first to a cyclic code, for which there is a single orbit of maximum length.

For the presentation of cyclic codes, it is simpler to change the indexation of codewords: the coordinates are numbered from 0 to $n-1$ instead of 1 to n.

The following permutation $\sigma_1(i) = i + 1 \bmod n$ is called the cyclic shift, and its action on codeword is the right shift $\sigma_1(c) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$.

Definition 16: A linear code $\mathcal{C}$ (or an m-block code C) of length n is cyclic if it is globally invariant under the action of the cyclic shift: $\sigma_1(c) \in \mathcal{C}$ for all $c \in \mathcal{C}$, *i.e.* $\sigma_1(C) = C$.

The following lemma solves this problem in the particular case of $\mathbb{F}_{q^m}$-multiplier equivalent $\mathbb{F}_{q^m}$-linear codes.

Lemma 3: Let $\mathcal{C}$ be a linear cyclic code of length n over $\mathbb{F}_{q^m}$. Let $\beta \in \mathbb{F}_{q^m}^*$ be an element of order dividing n. We set $\Lambda_\beta = (1, \beta, \beta^2, \ldots, \beta^{n-1})$. The code $\mathcal{C}' = \Lambda_\beta(\mathcal{C})$ is a cyclic $\mathbb{F}_{q^m}$-linear code of same parameters than $\mathcal{C}$.

Proof: We know that applying a multipliers isometry on a code does not change its parameters. We have to verify that $\mathcal{C}'$ is cyclic. Let $c' = (c'_0, \ldots c'_{n-1}) = \Lambda_\beta(c) = (c_0, \beta c_1, \ldots, \beta^{n-1} c_{n-1})$ be an element of $\mathcal{C}'$. Applying the circular shift to c', we obtain

$$\sigma_1(c') = (\beta c_1, \ldots, \beta^{n-1} c_{n-1}, c_0) = \beta\left(\Lambda_\beta(\sigma_1(c))\right)$$

which is an element of $\mathcal{C}'$ since $\mathcal{C}$ is cyclic. ∎

A natural idea is to try to extend this result to a q-ary image of $\mathcal{C}$ by using a matrix $M \in GL_q(m)$ of order dividing n. Unfortunately, it does not work for the following reason.

Let $D = \mathrm{Diag}(I_n, M, M^2, \ldots M^{n-1})$ be the diagonal block matrix corresponding to the successive powers of M. Applying D to a codeword $c \in Im_q(\mathcal{C})$ consists in multiplying each m-block of c on the right by a power of M. However, in the proof of Lemma 3, we need to factorize M on the left.

Let $\mathcal{G} = (\beta_{i,j})$ be a generator matrix of $\mathcal{C}$ and $G = (M_{\beta_{i,j}})$ its canonical q-ary image (Definition 8). Since G can be interpreted as an $k \times n$ matrix with matrix coefficients, it is possible to perform a left-multiplication $\ltimes$ of G by D as follows:

$$G' = G \ltimes D := (M^j \times M_{\beta_{i,j}})_{i,j}$$

The matrix G' can be considered as a generator matrix of an m-block code C' which is cyclic by the same reasoning as the proof of Lemma 3. Unfortunately, it is not equivalent to $\mathcal{C}$ and there is no guaranties on its minimum distance.

The only exception is to use a matrix M which commutes with the matrices $M_{\beta_{i,j}}$. In general the commutator of the cyclic group of order $q^m - 1$ generated by the non-zero matrices $M_{\beta_{i,j}}$ is reduced to this cyclic group, that leads to a matrix M corresponding to a matrix of multiplication M_β *i.e.* the situation described in Lemma 3.

In conclusion, if we want to construct an induced-cyclic generalized subspace subcode of a cyclic code, *i.e.* the cyclicity is inherited from the parent code $\mathcal{C}$, we have to apply first an $\mathbb{F}_{q^m}$-multiplier Λ_β which preserves the permutation, and

then to apply the subspace subcode construction. This method is described in Algorithm **2**.

Algorithm 2*:* Induced-cyclic GSS-code

Input: $\mathcal{G}$: a generator matrix of a cyclic linear code $\mathcal{C}$ of length n over $\mathbb{F}_{q^m}$.
Output: a cyclic generalized subspace subcode of $\mathcal{C}$

- Choose an element $\beta \in F_{q^m}^*$ such that $\beta^n = 1$. Compute $D = \mathrm{Diag}(1, \beta, \ldots, \beta^{n-1})$
- Compute the image $\mathcal{C}'$ of $\mathcal{C}$ by the isometry D.
- Choose a subspace V of F_q^m and return $SS_V(\mathcal{C}')$.

This construction can be easily generalized to any permutation $\sigma \in \mathrm{Per}(\mathcal{C})$ by applying on each orbit of σ the previous algorithm. Note that we can choose one subspace V_i per orbit, but it must be constant on a given orbit. Algorithm **3** describes this construction in details. We suppose in this algorithm that the coordinates of codewords are indexed following the orbits of the induced permutation σ, *i.e.* if σ is constituted of s orbits of respective lengths $\ell_1, \ldots, \ell_s$, then its decomposition into orbits is $(0, \ldots, \ell_1 - 1)(\ell_1, \ldots, \ell_1 + \ell_2 - 1) \ldots (n - \ell_s, \ldots n - 1)$.

Algorithm 3*:* Generalized subspace subcode with an induced permutation

Input: $\mathcal{G}$: a generator matrix of a linear code $\mathcal{C}$ of length n over $\mathbb{F}_{q^m}$ and a permutation $\sigma \in \mathrm{Per}(\mathcal{C})$. The coordinates are ordered following the orbits of σ.
Output: a generalized subspace subcode $C = \mathrm{GSS}_{\overline{V}}(\mathcal{C})$ of $\mathcal{C}$ such that $\sigma \in \mathrm{Per}(C)$.

- For each orbit $i \in [1, s]$ choose $\beta_i \in F_{q^m}^*$ such that $\beta_i^{\ell_i} = 1$. Compute $D_i = \mathrm{Diag}(1, \beta_i, \ldots, \beta_i^{\ell_i - 1})$
- Compute $D = \mathrm{Diag}(D_1, \ldots, D_s)$ and the image $\mathcal{C}'$ of $\mathcal{C}$ by the isometry D.
- For each orbit $i \in [1, s]$ choose a subspace V_i of dimension μ. Set $\overline{V}_i = (V_i, \ldots, V_i)$ (the V_i's are repeated ℓ_i times).
- Set $\overline{V} = (\overline{V}_1, \ldots, \overline{V}_n)$. Return $GSS_{\overline{V}}(\mathcal{C}')$.

Proposition 14: Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear code and $\sigma \in \mathrm{Per}(C)$. If C is a generalized subspace subcode of $\mathcal{C}$ obtained from Algorithm **3**, then C is invariant under the action of σ, *i.e.* $\sigma \in \mathrm{Per}(C)$.

Proof: We use the same notations as in Algorithm **3**. A direct generalization of Lemma 3 shows that $\mathcal{C}'$ is invariant under σ. Since the projections on V_i are constant on each orbit, C is invariant under σ. ∎

In the sequel, following for instance [1], we refer to such construction as "generalized subspace subcodes (or generalized projected codes) with induced permutation".

V. Generalized Subspace Subcodes of Reed-Solomon Codes

In order to obtain practical applications, it is natural to apply our results to the family of Reed-Solomon codes. Indeed, it is an infinite family of Maximum Distance Separable (MDS) codes over $\mathbb{F}_{q^m}$ which has an efficient decoding algorithm. MDS codes are those that meet the Singleton bound, *i.e.* their parameters satisfy the relation $k + d = n + 1$.

A. Previous Results on Subspace Subcodes of Reed-Solomon Codes

There are previous works on subspace subcodes of Reed-Solomon codes. The most important paper on this topic is those of Hattori *et al.* [15]. It is devoted to the study of subspace subcodes of cyclic Reed-Solomon codes of length $2^m - 1$. Using some properties of the roots of the generator polynomial, they found a complicated dimension formula and a simple lower bound on dimension for these subspace subcodes. Note that, for $\mu = 1$ or $\mu = m - 1$, it is shown that this lower bound is the exact value.

Later in 2004 *Spence* proved an *Hattori*'s conjecture concerning how to identify subspaces that can be used to build subspace subcodes of Reed-Solomon codes whose dimension exceeds this lower bound [22].

In this paper, we are not only interested by subspace subcodes of Reed-Solomon codes of length $n = q^m - 1$, but by any Reed-Solomon code of length $n \leq q^m + 1$. So our subfield subcodes of Reed-Solomon codes are no more cyclic, even up to permutation equivalence. In addition, in the next section, we will look at generalized subspace subcodes of Reed-Solomon codes, which are not cyclic, even for $n = q^m - 1$.

We will notice that the lower bound on the dimension given in [15] does not compare easily to those of Theorem 2 (this fact is also noticed in [15]).

B. Codes Derived From Reed-Solomon Codes

In this section, we will recall the definitions of Reed-Solomon codes and classical families of codes derived from Reed-Solomon codes. The main interest of all codes presented here is the fact that they can be decoded with the algebraic decoding algorithm of Reed-Solomon codes up to the error-correction capability $t = \lfloor (d - 1)/2 \rfloor$ of the parent Reed-Solomon code. More details and proofs can be found for instance in [19].

Definition 17: Let $S = (\alpha_1, \ldots, \alpha_n)$ be an ordered set of distinct elements of $\mathbb{F}_{q^m}$. The Reed-Solomon code of support S, length $n \leq q^m$ and minimum distance $d \leq n$ is the $\mathbb{F}_{q^m}$-linear code $\mathrm{RS}_k(S)$ (or RS_k if the support S is implicit) with generator matrix

$$\mathcal{G}_{\mathrm{RS}_k} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \quad \text{with } k = n + 1 - d.$$

These codes are evaluation codes of polynomials in $\mathbb{F}_{q^m}[x]$ of degree less than k:

$$\mathrm{RS}_k = \{(P(\alpha_1), \ldots, P(\alpha_n)) \mid P(x) \in \mathbb{F}_{q^m}[x] \\ \deg(P(x)) < k = n + 1 - d \}$$

They are MDS and have an efficient decoding algorithm.

Definition 18: The Generalized Reed-Solomon codes (GRS codes) are the $\mathbb{F}_{q^m}$-linear codes that are $\mathbb{F}_{q^m}$-multiplier equivalent to Reed-Solomon codes.

This definition of GRS codes may seem more restrictive than the usual equivalence by automorphism [16] since we do not take in account a possible permutation of coordinates. However, such a permutation is implicit in the choice of an order for the support of Reed-Solomon codes.

So a GRS code is entirely defined by a support $S = (\alpha_1, \ldots, \alpha_n)$, the multipliers $\Lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_{q^m}^{*n}$ and its dimension k or its minimum distance $d = n + 1 - k$. It has for generator matrix $\mathcal{G}_{\mathrm{RS}_k} \times \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$ and is denoted $\mathrm{GRS}_k(S, \Lambda)$.

The following proposition gives the description of the dual of a GRS code.

Proposition 15 ([11] Th. 1): We set $\Lambda = (\lambda_1, \ldots, \lambda_n)$, $\Lambda' = (\lambda'_1, \ldots, \lambda'_n)$ and $\lambda'_i = \left(\lambda_i \prod_{j \neq i} (\alpha_j - \alpha_i)\right)^{-1}$.

The dual of the GRS code $\mathrm{GRS}_k(S, \Lambda)$ is the GRS code $\mathrm{GRS}_{n-k}(S, \Lambda')$.

More details on GRS codes with specific permutation groups such as quasi-cyclic or quasi-dyadic groups can be found in Appendix.

C. Generalized Subspace Subcodes of Reed-Solomon Codes

In this section we interpret the results of Sections III-A and IV in the context of Reed-Solomon codes. We denote the Reed-Solomon codes (resp. Generalized Reed-Solomon codes) by RS codes (resp. GRS codes). .

We use the following notations:

- SF_{q^u}-RS: $\mathbb{F}_{q^u}$-subfield subcodes of RS codes $(u|m)$.
- SF_{q^u}-GRS: $\mathbb{F}_{q^u}$-subfield subcodes of GRS codes

If $u = 1$, subfield subcodes are denoted SF-RS or SF-GRS.

- SS-RS or μ-SS-RS: subspace subcodes of RS codes over a vector space of dimension μ.
- SS-GRS or μ-SS-GRS: subspace subcodes of GRS codes.
- GSS-RS, GSS-GRS: generalized subspace subcodes of RS codes or GRS codes.

As noted in Section III-A, subfield subcodes are particular cases of subspace subcodes, so we have SF_{q^u}-RS $\subset u$-SS-RS and SF_{q^u}-GRS $\subset u$-SS-GRS for $u|m$.

In addition, since the action of a $\mathbb{F}_{q^m}$ multiplier on a code over $\mathbb{F}_{q^m}$ correspond to a particular case of m-block multiplier on the q-ary image, we have GSS-RS=GSS-GRS and SS-GRS $\subset$ GSS-RS.

If we interpret the results of Theorem 2 and Theorem 3 in the context of Reed-Solomon codes, we obtain the following Theorem:

Theorem 4: For $\mu = 1$, the generalized subspace subcodes of Reed-Solomon codes are exactly the Alternant codes, *i.e.* the subfield subcodes of Generalized Reed-Solomon codes: *1-GSS-RS = SF_q-GRS*.

For $\mu = m - 1$, the generalized subspace subcodes of Reed-Solomon codes are exactly the subspace subcodes of Generalized Reed-Solomon codes *(m-1)-GSS-RS = (m-1)-SS-GRS*.

Note that, since GSS-RS=GSS-GRS, this theorem implies in particular that GSS-GRS=SS-GRS for $\mu = 1$ or $m - 1$. Be careful that this equality is a family equality: for $\mu = m - 1$, if we construct a generalized subspace subcode of a Generalized Reed-Solomon code, we obtain a subspace subcode of another Generalized Reed-Solomon code.

In addition, we give the following Proposition:

Proposition 16: For $1 < \mu < m - 1$, there exist some generalized subspace subcodes of Reed-Solomon codes that are not subspace subcodes of Generalized Reed-Solomon codes:

$$SS - GRS \subsetneq GSS - RS = \text{GSS-GRS}.$$

Proof: We give the sketch of the proof without specifying details.

We start from a GSS-RS code $C = GSS_{\overline{V}}(\mathrm{RS}_k)$ such that, if $\overline{V} = (V_1, V_2, \ldots)$, then, for all $\alpha \in \mathbb{F}_{q^m}^*$, $\alpha V_1 \neq V_2$. If C is a SS-GRS code, we prove that there exists an α such that $\alpha V_1 = V_2$, which contradicts the previous hypothesis. ∎

D. Examples of Interesting SS-RS Codes for μ Close to m

Let recall the MDS conjecture: if there exists an $[n, k, d = n+1-k]_q$ MDS code, meaning an MDS code of length n and dimension k over $\mathbb{F}_q$ then $n \leq q + 1$, except for particular cases ($k \leq 3$ or $k \geq n - 2$) [19] Ch.7 §7. We assume in the sequel that the MDS conjecture is true.

So, for instance, from a Reed-Solomon code of length $n = 2^m$ over $\mathbb{F}_{2^m}$, it is possible to construct an $(m$-1)-block code of length 2^m with parameters close to MDS codes and having an efficient decoding algorithm. These kinds of parameters cannot be attempted by the subfield subcode method.

As an example, we choose $\mu = 8$, which corresponds to bytes as μ-block symbols. The maximum length for a Reed-Solomon code over $\mathbb{F}_{2^8}$ is $n = 2^8 = 256$.

- If we want a code of length $n = 512$, we choose $m = 9$. For $d = 256$, we obtain a SS-RS code of parameters $[512, 225, 256]_{2^8}$. The Gilbert-Varshamov lower bound on the dimension of a linear code of length 512 and minimum distance 256 over $\mathbb{F}_{2^8}$ is $GV = 194$.
- If we want a code of length $n = 1024$, we choose $m = 10$. For $d = 512$, we obtain a SS-RS code of parameters $[1024, 385, 512]_{2^8}$. The Gilbert-Varshamov lower bound is $GV = 387$.
- If we want a code of length $n = 2048$, we choose $m = 11$. For $d = 1024$, we obtain a SS-RS code of parameters $[2048, 641, 1024]_{2^8}$. The Gilbert-Varshamov lower bound is $GV = 771$.

One can notice that the Gilbert-Varshamov bound is a lower bound. It is expected that a random linear code is over this bound. However, a random code does not possess a decoding algorithm, while SS-RS codes can be decoded with a Reed-Solomon decoder.

E. Exceptional Generalized Subspace Subcodes

The bound on the pseudo-dimension of a subspace subcode given in Corollary 2 leads to codes that are not very performant, in particular for small μ. However, there exist codes for

which the true dimension is larger. We will see at the next section that it is the case for BCH or Goppa codes.

Following this remark, we introduce the notion of exceptional GSS code:

Definition 19: Let C be an m-block code of dimension k and length n and $C' = GSS_{\overline{V}}(C)$ be a μ-generalized subspace subcode of C. Let k' be the pseudo-dimension of C' and $k_b = (km - n(m-\mu))/\mu$ be the bound of Corollary 2. The generalized subspace subcode C' is ordinary if $k' = k_b$ and is exceptional if $k' > k_b$.

Remark 2: It is important to understand that the definition of exceptional GSS code is dependant on the original code C, not on the subspace subcode C' itself. This fact will be explained in detail in the next section. Its occurs typically when we have $C_1 \subsetneq C_2$ and $C' = GSS_{\overline{V}}(C_1) = GSS_{\overline{V}}(C_2)$. In that situation C' can be exceptional then it is considered as a subspace subcode of C_1 and ordinary as a subspace subcode of C_2.

We set $\nu = m - \mu$. There exists a kind of duality between the construction of some μ-subspace subcodes and ν-subspace subcodes. If V is a μ-subspace of $\mathbb{F}_q^m$, we choose a linear projection ψ from $\mathbb{F}_q^m$ onto $\mathbb{F}_q^\nu$ such that $\mathrm{Ker}(\psi) = V$. As previously Ψ refers to the extension of ψ to the n-tuple over $\mathbb{F}_{q^m}^n$. Clearly, $\mathrm{Ker}(\Psi) = V^n$.

From these definitions and Section III-B, we deduce the following Lemma.

Lemma 4: Let V be a μ-subspace and ψ defined as previously. If Ψ_C denotes the restriction of Ψ to C, then $\mathrm{SS}_V(C) = \mathrm{Ker}(\Psi_C)$ and $\Psi(C) = \mathrm{P}_\psi(C)$. In particular $\dim_q(C) = \dim_q(\mathrm{SS}_V(C)) + \dim_q(\mathrm{P}_\psi(C))$.

A μ-subspace V of $\mathbb{F}_q^n$ can be considered as an $\mathbb{F}_q$-linear code of length m and dimension μ. Let $V^\perp$ be its dual code in the meaning of Coding Theory. The projection ψ such that $\mathrm{Ker}(\psi) = V$ is not unique, however, if M_ψ is its $m \times \nu$ corresponding matrix, then the condition $\mathrm{Ker}(\psi) = V$ is equivalent to saying that M_ψ^T is a parity check matrix of V, or a generator matrix of $V^\perp$.

We can now define the notion of orthogonality for subspace subcodes.

Definition 20: Let $\mathrm{SS}_V(C)$ be an μ-subspace subcode. Its orthogonal subspace subcode relative to C and V is the ν-subspace subcode $\mathrm{SS}_V^\perp(C) = \mathrm{SS}_{V^\perp}(C^\perp)$.

Remark that this definition is independent on the choice of block-code representations of $\mathrm{SS}_V(C)$ and $\mathrm{SS}_{V^\perp}(C^\perp)$. However, we will notice that this notion of orthogonality is not relative to the μ-block code $\mathrm{SS}_V(C)$, but to the m-block-code C. (see Section V-F for examples).

The code $\mathrm{SS}_{V^\perp}(C^\perp)$ is in fact the dual of $\mathrm{P}_\psi(C)$. From Lemma 4, we deduce the following Corollary:

Corollary 4: If $\mathrm{SS}_V(C)$ and $\mathrm{SS}_{V^\perp}(C^\perp)$ are defined as previously, then

$$\dim_q(\mathrm{SS}_{V^\perp}(C^\perp)) = \dim_q(\mathrm{SS}_V(C)) + n\nu - \dim_q(C).$$

Proof: The code $\mathrm{SS}_{V^\perp}(C^\perp)$ is the dual of $\mathrm{P}_\psi(C)$ as $\mathbb{F}_q$-linear code of length $n\nu$. In particular $\dim_q(\mathrm{SS}_{V^\perp}(C^\perp) = n\nu - \dim_q(\mathrm{P}_\psi(C))$. From Lemma 4, we have $\dim_q(\mathrm{P}_\psi(C)) = \dim_q(C) - \dim_q(\mathrm{SS}_V(C))$, which gives $\dim_q(\mathrm{SS}_{V^\perp}(C^\perp)) = \dim_q(\mathrm{SS}_V(C)) + n\nu - \dim_q(C)$. ■

If k is the pseudo-dimension of C then $\dim_q(C) = km$. From Corollary 2, we have $\dim_q(\mathrm{SS}_V(C)) \geq (km - n(m-\mu)) = km - n\nu$. Following some similar notion introduced in [15], if $\dim_q(\mathrm{SS}_V(C)) = (km - n(m-\mu))$, we refer this subspace subcode to an ordinary subspace subcode, else we refer it to an exceptional subspace subcode. In addition $\{0\}$ and its dual are considered as ordinary.

We can deduce the following proposition.

Proposition 17: A subspace subcode is ordinary if and only if its orthogonal is the null code. A subspace subcode is exceptional if and only if its orthogonal subspace subcode is exceptional.

Proof: Suppose that $\mathrm{SS}_V(C)$ is ordinary, which means $\dim_q(\mathrm{SS}_V(C)) = km - n\nu$. From Corollary 2, we deduce $\dim_q(\mathrm{SS}_{V^\perp}(C^\perp)) = \dim_q(\mathrm{SS}_V(C)) + n\nu - \dim_q(C) = 0$. Moreover if $\dim_q(\mathrm{SS}_{V^\perp}(C^\perp)) = 0$ then $\dim_q(\mathrm{SS}_V(C)) = \dim_q(C) - n\nu$.

If $\mathrm{SS}_V(C)$ is exceptional, then $0 < \dim_q(\mathrm{SS}_{V^\perp}(C^\perp)) < \nu$ and the orthogonal code of $\mathrm{SS}_{V^\perp}(C^\perp)$ is $\mathrm{SS}_V(C)$ which is neither 0 nor the full space, so $\mathrm{SS}_{V^\perp}(C^\perp)$ is exceptional. ■

To conclude this section, we give an algorithm to construct the orthogonal of a subspace subcode.

Algorithm 4: Generator matrix of $\mathrm{SS}_V^\perp(C)$

Input: G: a generator matrix of an m-block code C. M_V: a generator matrix of the subspace V.
Output: G and H: a generator matrix and a parity check matrix of $\mathrm{SS}_V^\perp(C)$.

- From M_V, compute a parity check matrix H_V of V.
- Set $\mathsf{H} := G \times (I_n \otimes H_V^T)$. H is a generator matrix of the dual of $\mathrm{SS}_V^\perp(C)$.
- From H, compute a generator matrix G of $\mathrm{SS}_V^\perp(C)$.

The parity check matrix H_V is not unique, a change of matrix H_V in Algorithm **4** leads to a scalar equivalent ν-block code in the meaning of Definition 6.

F. Exceptional SS-RS *Codes*

An interesting property of Reed-Solomon codes (or GRS codes) is the fact that, for a given extension field and a given support S of size n, they constitute a strict inclusion chain:

$$\mathrm{RS}_1(S) \subsetneq \mathrm{RS}_2(S) \subsetneq \ldots \mathrm{RS}_k(S) \ldots \subsetneq \mathrm{RS}_{n-1}(S) \subsetneq \mathrm{RS}_n(S).$$

However, when we look at the subspace subcodes of this inclusion chain, it is possible to have an equality of the type

$$\mathrm{SS}_V(\mathrm{RS}_k(S)) = \mathrm{SS}_V(\mathrm{RS}_{k+1}(S)) = \ldots = \mathrm{SS}_V(\mathrm{RS}_{k+r}(S)).$$

This situation leads to exceptional subspace subcodes (in the meaning of Section V-E), since we obtain the bound on dimension from $\mathrm{SS}_V(\mathrm{RS}_{k+r}(S))$ and the bound on the minimum distance from $\mathrm{SS}_V(\mathrm{RS}_k(S))$.

1) Orthogonal Subspace Subcodes for $\mu = m - 1$: As a first example, we consider classical cyclic Reed-Solomon codes of length $n = 2^m - 1$ over $\mathbb{F}_{2^m}$. Binary BCH codes are subfield subcodes of cyclic Reed-Solomon codes. In the sequel, the support $S = S_\alpha$ is fixed by the choice of a primitive root α.

Following the usual notation for BCH codes, we denote by BCH_d the BCH of constructed distance d, *i.e.* $\mathrm{BCH}_d = \mathrm{SS}_{\mathbb{F}_2}((\mathrm{RS}_{n-d+1}(S))$ with $n = 2^m - 1$.

We set $q = 2$ and $m = 5$. We consider classical cyclic Reed-Solomon codes of length $n = 2^5 - 1 = 31$ and we look at the corresponding binary BCH codes, that are subfield subcodes of Reed-Solomon codes.

The parameters of the corresponding BCH codes are as follows:

- $\mathrm{BCH}_1 = \mathbb{F}_2^{31}$.
- $\mathrm{BCH}_2 = \mathrm{BCH}_3$, parameters: [31, 26, 3].
  If we look at $\mathrm{BCH}_3 = \mathrm{SS}_{\mathbb{F}_2}((\mathrm{RS}_{29}(S))$, the bound given in Corollary 2 is $k' \geq 21$. Since $k' = \dim(\mathrm{BCH}_3) = 26$, the subspace subcode $\mathrm{SS}_{\mathbb{F}_2}(\mathrm{RS}_{29}(S))$ is exceptional.
- $\mathrm{BCH}_4 = \mathrm{BCH}_5$, parameters: [31, 21, 5].
  In this case, both $\mathrm{SS}_{\mathbb{F}_2}(\mathrm{RS}_{28}(S))$ and $\mathrm{SS}_{\mathbb{F}_2}(\mathrm{RS}_{27}(S))$ are exceptional, since the bounds on dimension are respectively $k' \geq 11$ and $k' \geq 16$.
- $\mathrm{BCH}_6 = \mathrm{BCH}_7$, parameters: [31, 16, 7].
  $\mathrm{SS}_{\mathbb{F}_2}((\mathrm{RS}_{26}(S))$ and $\mathrm{SS}_{\mathbb{F}_2}(\mathrm{RS}_{25}(S))$ are exceptional.
- $\mathrm{BCH}_8 = \ldots = \mathrm{BCH}_{11}$, parameters: [31, 11, 11].
  For $8 \leq k \leq 11$, $\mathrm{SS}_{\mathbb{F}_2}((\mathrm{RS}_k(S))$ is exceptional.
- $\mathrm{BCH}_{12} = \ldots = \mathrm{BCH}_{15}$, parameters: [31, 6, 15].
  For $12 \leq k \leq 15$, $\mathrm{SS}_{\mathbb{F}_2}((\mathrm{RS}_k(S))$ is exceptional.
- $\mathrm{BCH}_{16} = \ldots = \mathrm{BCH}_{31} = 0$ is the null code.

Using for instance MAGMA [9], one can verify that all these BCH codes, except for $d = 6$ or 7, are optimal with the meaning of, for a given length and a given dimension, they have the best possible minimum distance.

So, we can apply the results of Section V-E and derive some exceptional subspace subcodes for $\mu = m - 1 = 4$.

In Table I, the first column is the dimension of the code $\mathrm{RS}_k(S)$. The second column gives the parameters of $\mathrm{SS}^{\perp}_{\mathbb{F}_2}(RS_k(S))$. The third column gives the lower bound on the dimension derived from Corollary 2. The last column gives the value $n_\mu - d$, which corresponds to Near-MDS codes. Under the MDS conjecture, this value is an upper bound for a linear code over $\mathbb{F}_{q^m}$ of length n greater than $q^m + 3$. A priori, this upper bound is not tight.

Sometimes, distinct values of k lead to the same code. In that situation, we give the two values for k and for k_b.

Most of these codes have very nice parameters. For instance, under the MDS conjecture, the dimension of an $\mathbb{F}_{q^m}$-linear code of such length cannot excess $n - d$.

In particular, the best possible dimension for an $\mathbb{F}_{16}$-linear codes of length 31 and respective minimum distance 3, 4 and 5 are 28, 27 and 26, so the codes with parameters [31, 28.75, 3]$_{16}$, [31, 27.5, 4]$_{16}$ and [31, 26.25, 5]$_{16}$ are better than any $\mathbb{F}_{16}$-linear code.

We do not know any data base on best known linear codes over $\mathbb{F}_{16}$ and it does not exist a tight upper bound on the size of a non-linear code of fixed length, minimum distance and size of alphabet. So, it is possible that some of our examples have optimal parameters.

TABLE I

PARAMETERS OF $\mathrm{SS}^{\perp}_{\mathbb{F}_2}(RS_k(S))$ FOR $k \in [2, 27]$

$\dim(\mathrm{RS}_k)$	$\mathrm{SS}^{\perp}_{\mathbb{F}_2}(RS_k(S))$	k_b	N-MDS
2	[31, 28.75, 3]$_{16}$	28.5	28
3	[31, 27.5, 4]$_{16}$	27.25	27
4	[31, 26.25, 5]$_{16}$	26	26
5	[31, 25, 6]$_{16}$	24.75	25
6	[31, 23.75, 7]$_{16}$	23.5	24
7	[31, 22.5, 8]$_{16}$	22.25	23
8	[31, 21.25, 9]$_{16}$	21	22
9	[31, 20, 10]]$_{16}$	19.75	21
10	[31, 18.75, 11]$_{16}$	18.5	20
11	[31, 17.5, 12]$_{16}$	17.25	19
12	[31, 16.25, 13]$_{16}$	16	18
13	[31, 15, 14]$_{16}$	14.75	17
14	[31, 11.25, 15]$_{16}$	13.5	16
15	[31, 12.5, 16]$_{16}$	12.25	15
16 – 17	[31, 11.25, 18]$_{16}$	11 – 9.75	13
18	[31, 10, 19]$_{16}$	8.5	12
19	[31, 8.75, 20]$_{16}$	7.25	11
20 – 21	31, 7.50, 22]$_{16}$	6 – 4.75	9
22	[31, 6.25, 23]$_{16}$	3.5	8
23	[31, 5, 24]$_{16}$	2.25	7
24 – 25	[31, 3.75, 26]$_{16}$	1 – 0	5
26 – 27	[31, 2.50, 28]$_{16}$	0	3

Clearly, for $\mu < m - 1$, subspace subcodes will not have such interesting parameters, however, they have a decoding algorithm up to the error correcting capability.

2) Examples for μ Equals 3: For $q = 2^2$ or 2^3, there exists some databases for best known (linear) and upper bounds on either the minimum distance for a fixed dimension or dimension for a fixed minimum distance.

For $\mu = 3$ we found some codes that reach or overpass best known or optimal linear codes over $\mathbb{F}_8$.

As previously, k denotes the dimension of the underlying Reed-Solomon code.

Results for $m = 4$, $n = 16$ and $\mu = 3$:

- For $k = 13$, we obtain a $[16, 12, 4]_8$, which corresponds to an optimal linear code.
  The optimality means that it does not exist an $\mathbb{F}_8$-linear code of parameters [16, 12, 5] or [16, 13, 4].
- For $k = 14$, we obtain a $[16, 13.\overline{33}, 3]_8$, which is better than any linear code in the meaning that it does not exist an $\mathbb{F}_8$-linear code of parameters [16, 13, 4] or [16, 14, 3].

Results for $m = 5$, $n = 32$ and $\mu = 3$:

- For $k = 26$, we obtain a $[32, 22, 7]_8$, which corresponds to the parameters of the best know linear code in the meaning that we do not known if there is an $\mathbb{F}_8$-linear code of parameters [32, 22, 8] or [32, 23, 7].

3) Tests on the Orthogonal Construction: Following the approach of Sections V-F, we tried to found some exceptional codes for $\mu = 1$ and to deduce exceptional codes for $\mu = m - 1$.

Binary Goppa codes is an interesting subclass of Alternant codes (cf. [19] Ch.12 &3). In particular, if the Goppa polynomial $g(z)$ used in this construction has no multiple zero, then $g(z)$ and $g(z)^2$ generate the same Goppa code. From

our point of view, it implies that, for $\mu = 1$ some subspace subcodes of GRS codes having a support and a multiplier associated to these Goppa polynomials are exceptional. For this kind of parameters, we get results close to those of Table I.

We tested also subspace subcodes of random GRS codes with parameters similar to those of Table I. We did not get exceptional subspace subcodes, except of small pseudo-dimension (typically less than or equal to 3).

VI. Analysis of GSS-RS Codes in a Cryptographic Purpose

In this section, we do not want to propose a cryptosystem based on GSS-RS codes, but to study their properties from a cryptographic point of view.

We will describe how to construct efficiently a random SS-GRS code. We show that it is possible to extend the Sidel'nikov and Shestakov algorithm which able us to recover an underlying GRS code from a code wich is m-block equivalent to one of its q-ary image. We present an improvement of the exhaustive search of the secret parameters of a GSS-RS code. Finally, we show that the folding cryptanalysis against quasi-cyclic or quasi-dyadic Alternant code can be generalized to the case of induced quasi-cyclic or quasi-dyadic GSS-RS codes.

A. An Efficient Way to Construct Random Binary μ-GSS-RS Codes

Probably the simplest method for constructing a random GSS-RS code is to use the dual construction of a random projected codes. The first choice is to fix the parameters of our Reed-Solomon code: m, $n \leq q^m - 1$ and d, and the value of $\mu \leq m$.

- Step 1: choice of the RS code. We have to choose n distinct elements of $\mathbb{F}_{q^m}$ for the support $S = (\alpha_1, \ldots \alpha_n)$. It should be noted that the order of the elements is a sensitive information that can be used to mask the choice of a random permutation.
  Let $\mathcal{G}_{\mathrm{RS}_k}$ be a generator matrix of $\mathrm{RS}_k = \mathrm{RS}_k(S)$ and G_{RS_k} its q-ary image relative to a basis $\mathcal{B}$. The basis $\mathcal{B}$ does not have to be secret, since it will be masked later with the choice of projections ψ_i. Compute a q-ary parity-check matrix H_{RS_k} of G_{RS_k}.
- Step 2: construction of a random projected GRS code. We choose randomly n matrices M_i of size $m \times \mu$ over $\mathbb{F}_q$ of full rank μ. Compute $D = \mathrm{Diag}(M_1, \ldots, M_n)$ and $H = H_{\mathrm{RS}_k} \times D$.
- Public key: a generator matrix G (under systematic form) of the code with parity-check matrix H and the value d of the minimum μ-block distance.
- Secret key: the support S of the Reed-Solomon codes and the matrices M_i^T which give the representation of the vector spaces V_i's in the GSS-RS construction. These secret values allow to set the decoding algorithm up to $t = \lfloor (d-1)/2 \rfloor$ errors.

B. Generalization of Sidel'nikov Shestakov Algorithm

In this section, we look at the particular case $\mu = m$, so all the V_i's in the definition of generalized subspace subcodes are all equal to the whole finite field $\mathbb{F}_{q^m}$. Moreover, in that case the notion of generalized projected code is the same as generalized subspace subcode. The only choices in the construction of a GSS-RS code are the support of the underlying Reed-Solomon code (in particular the order on this support) and the different choice of matrices M_i, $1 \leq i \leq n$ for the projection on each coordinate.

In an equivalent way, this problem can be reformulated as follows: the starting point is a q-ary image of a fixed but unknown Reed-Solomon code. We apply an $\mathbb{F}_q$-linear multipliers isometry to this q-ary image and obtain an equivalent m-block code C. The problem is then: *From a generator matrix of C, Is it possible to reconstruct a Reed-Solomon code and an isometry which leads to the code C?*

Note that, due to some equivalence between Reed-Solomon, there are more than one solution to this problem, however, as soon as we have a solution, we are able to decode C up to the error capacity derived from the Reed-Solomon code. One want to notice that the permutation part of isometry is implicitly integrated in the choice of the support of the Reed-Solomon code, it is why we limit ourself to multipliers isometries.

If we restrict ourself to $\mathbb{F}_{q^m}$-linear equivalence, the corresponding problem is that of reconstructing the parameters of a Generalized Reed-Solomon code from one of its generator matrices. This can be done using the Sidel'nikov Shestakov algorithm [21]. This algorithm uses the uniqueness of the systematic generator matrix of a code and the link between the supports and scalars used in its definition and the redundant part of this matrix.

We will show that it is possible to adapt this algorithm in our situation.

Let $\mathcal{G} = \left(\mathcal{I}_k \middle| \mathcal{B}\right)$, $\mathcal{B} = \left(\beta_{i,j}\right)_{1 \leq i \leq k, k+1 \leq j \leq n}$ be the systematic generator matrix of the secret Reed-Solomon code. Using a basis $\mathcal{B}$, we construct the corresponding systematic generator matrix of its q-ary image:

$$G = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 & M_{1,k+1} & \ldots & M_{1,n} \\ 0 & \ddots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & M_{k,k+1} & \ldots & M_{k,n} \end{pmatrix}$$

with $M_{i,j} = M_{\beta_{i,j}}$.

We apply then a multipliers isometry $\mathrm{Diag}(D_1, \ldots, D_n)$, $D_i \in GL_q(m)$ in order to obtain a m-block code C. The systematic generator matrix of C is then

$$G = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 & M'_{1,k+1} & \ldots & M'_{1,n} \\ 0 & \ddots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & M'_{k,k+1} & \ldots & M'_{k,n} \end{pmatrix}$$

where $M'_{i,u} = D_i^{-1} M_{i,u} D_u$ for $i \in [1..k]$ and $u \in [k+1..n]$.

The following lemma describes the systematic generator matrix of a Reed-Solomon code. It is essentially Theorem 1 of [8] and Theorem 2 of [11] without restrictions on the length of the Reed-Solomon code.

Lemma 5: Let $\mathcal{G} = \left(\mathcal{I}_k \middle| \mathcal{B}\right)$ be the systematic generator matrix of the Reed-Solomon code of support $(\alpha_1, \ldots, \alpha_n)$ and dimension k. The coefficients $\beta_{i,j}$, $1 \leq i \leq k$, $k+1 \leq j \leq n$ of $\mathcal{B}$ are equal to

$$\beta_{i,u} = \prod_{j \in [1,k],\ j \neq i} \frac{\alpha_u - \alpha_j}{\alpha_i - \alpha_j}.$$

Proof: The i-th row of the systematic generator matrix $\mathcal{G}$ corresponds to the evaluation of the polynomial $P_i(X)$ of degree less than k such that $P_i(\alpha_i) = 1$ and $P_i(\alpha_i) = 0$ for $j \in [1,k],\ j \neq i$.

Clearly, this polynomial is $P_i(X) = \prod_{j \in [1,k],\ j \neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j}$.

The result is obtained by the evaluation of $P_i(X)$ in α_u for all u in $[k+1, n]$. ∎

The following corollary is a straightforward application of this Lemma.

Corollary 5 (Corollary 1 of [8]): For all i, j, u and v such that $1 \leq i, j \leq k$ and $k+1 \leq u, v \leq n$, we have the relation

$$\frac{\beta_{i,u}\beta_{j,v}}{\beta_{j,u}\beta_{i,v}} = \frac{(\alpha_u - \alpha_j)(\alpha_v - \alpha_i)}{(\alpha_u - \alpha_i)(\alpha_v - \alpha_j)}.$$

Note that $\beta_{i,u,j,v} = (\alpha_u - \alpha_j)(\alpha_v - \alpha_i)(\alpha_u - \alpha_i)^{-1}(\alpha_v - \alpha_j)^{-1}$ is a non-zero element of $\mathbb{F}_{q^m}$.

Using the isomorphism of $\mathbb{F}_{q^m}$ and $\mathbb{F}_q^m$ induced by the basis $\mathcal{B}$ in the construction of the q-ary image, we denote by $M_{i,u,j,v}$ the matrix of the multiplication by $\beta_{i,u,j,v}$.

We are able to prove the following Lemma:

Lemma 6: For all i, j, u and v such that $1 \leq i, j \leq k$ and $k+1 \leq u, v \leq n$, we have

$$M'_{i,u} {M'_{j,u}}^{-1} M'_{j,v} {M'_{i,u}}^{-1} = D_i^{-1} M_{i,u,j,v} D_i.$$

Proof: From Corollary 5, we deduce

$$M_{i,u,j,v} = M_{i,u} M_{j,u}^{-1} M_{j,v} M_{i,u}^{-1}.$$

Computing $M'_{i,u} {M'_{j,u}}^{-1} M'_{j,v} {M'_{i,u}}^{-1}$ from the definition $M'_{i,u} = D_i^{-1} M_{i,u} D_u$, we obtain the required equality. ∎

Note that, for a fixed i and any u, v, $j \neq i$ the matrices $D_i^{-1} M_{i,u,j,v} D_i$ are all in the same cyclic group of order $q^m - 1$ which corresponds to the representation of the extended finite field $\mathbb{F}_{q^m}$ relative to the basis $\mathcal{B}'$ obtained from $\mathcal{B}$ by D_i considered as a matrix of change of basis of $\mathbb{F}_q^m$.

In [11], Arne Dür characterized the automorphism group and the permutation group of Reed-Solomon codes. In Appendix A, we recall some results on permutation group and automorphism group of GRS codes. In particular, the automorphism group of a doubly-extended Reed-Solomon code is triply transitive on the support. The main consequence is the well-known fact that, if we want to recover the support of a GRS codes, it is always possible to fix arbitrary 3 elements of this support.

We are now able to describe the reconstruction algorithm.

- Step 1: Identifying the matrices $D_1^{-1} M_{1,u,j,v} D_1$ to elements of $\mathbb{F}_{q^m}$.
  We set $M'_{u,j,v} = D_1^{-1} M_{1,u,j,v} D_1$. As noticed previously, the matrices $M'_{u,j,v}$ are all in a same cyclic group of order $q^m - 1$ which corresponds to a representation of the multiplicative group $\mathbb{F}^*_{q^m}$. Consequently, the sum of any element of this group are either the null matrix M_0 or an element of this group.
  Suppose that at most one of the $M'_{u,j,v}$'s have a minimal polynomial $p(x)$ of degree m. It implies that $\{\sum_{s=0}^{m-1} \lambda_s {M'_{u,j,v}}^s \mid \lambda_i \in \mathbb{F}_q\}$ is isomorphic to the finite field $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/p(x)$.
  If there is no such matrix $M'_{u,j,v}$, we try with another conjugacy group $D_i^{-1} M_{i,u,j,v} D_i$, $1 \leq i \leq n$. If this does not work, it implies that the targeted Reed-Solomon code is not defined over $\mathbb{F}_{q^m}$, but over a subfield $\mathbb{F}_{q^{m'}}$ for some divisor m' of m.
  In all cases, it is possible to recover a representation as elements of a finite field of the set of matrices $D_i^{-1} M_{i,u,j,v} D_i$. Without loss of generality, in the sequel we suppose that $i = 1$. In addition, we also set $D_1 = I_m$, since, as mentioned previously, it can be integrated in the choice of the projection basis $\mathcal{B}$ for computing the q-ary image of the Reed-Solomon codes.
- Step 2: Recovering the support $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of the Reed-Solomon code.
  The assumption $D_1 = I_m$ and the identification of matrices $M'_{u,j,v}$ to elements of $\mathbb{F}_{q^m}$ implies that $\beta_{1,u,j,v} = (\alpha_u - \alpha_j)(\alpha_v - \alpha_1)(\alpha_u - \alpha_1)^{-1}(\alpha_v - \alpha_j)^{-1}$ is known for $1 < j \leq k$ and $k < u, v \leq n$, $u \neq v$.
  Since it is possible to fix arbitrary 3 points of the support, we set $\alpha_1 = 0$, $\alpha_2 = 1$ and $\alpha_{k+1} = \alpha$ (where α is a fixed primitive root of $\mathbb{F}_{q^m}$).
  For $j \in [3, k]$, we deduce the α_j's from equations
  $$\beta_{1,k+1,j,k+2} = \frac{(\alpha - \alpha_j)\alpha_{k+1}}{\alpha(\alpha_{k+1} - \alpha_j)}.$$
  For $v \in [k+2, n]$, we deduce the α_v's from equations
  $$\beta_{1,k+1,2,v} = \frac{\alpha_v(\alpha - 1)}{\alpha(\alpha_v - 1)}.$$
- Step 3: Recovering $\mathrm{Diag}(D_1, \ldots, D_n)$.
  Since the α_i's are known, we are able to construct the matrix G, *i.e.* to recover the matrices $M_{i,u}$ for $1 \leq i \leq k$ and $k < u \leq n$. From the given matrix G', we also know the matrices $M'_{i,u} = D_i^{-1} M_{i,u} D_u$.
  For $i = 1$ and $D_1 = I_m$, we have $D_u = M_{1,u}^{-1} M'_{1,u}$ for all $u \in [k+1, n]$.
  For $u = k+1$, we have $D_i = M_{i,k+1} D_{k+1} {M'_{i,k+1}}^{-1}$ for all $i \in [2, k]$.

C. Recovering the GSS-RS Structure by Exhaustive Search

Following the approach developed in Section 4.3 of [7] and the fact that it is possible to recover the extension field structure of a q-ary image of a code, we propose an algorithm which able us to recover the structure of a GSS-RS code.

Let $\overline{V} = (V_1, \ldots, V_n)$ be the μ-subspaces used for the construction of our GSS-RS code. We fix arbitrary a basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For $i \in [1..n]$, let M_i be a $\mu \times m$ generator matrix of the subspace V_i relative to the basis $\mathcal{B}$.

If M_i is known, we can identify the i-th μ-block coordinate of a codeword of our GSS-RS code to an element $\beta \in V_i \subset \mathbb{F}_{q^m}$.

If, for all i, M_i is known, each codeword can be identified to a codeword in $\mathbb{F}_{q^m}^n$ which lies in the starting Reed-Solomon code.

Let k' be the $\mathbb{F}_q$-dimension of our GSS-RS code. Taking the preimage of its $\mathbb{F}_q$-generator matrix, we obtain an $k' \times n$ matrix over $\mathbb{F}_{q^m}$ which have an $\mathbb{F}_{q^m}$-rank upper-bounded by k. Remembering that $k' > km - n(m - \mu)$ which is greater than k in practical applications, it is possible to distinguish a correct set of n matrices M_i from a random one.

So the $\mathbb{F}_{q^m}$ structure can be recovered by an exhaustive search on the matrices M_i.

D. Cryptanalysis of Quasi-Cyclic and Quasi-Dyadic GSS-RS Codes

The main disadvantage in the public key cryptography is the size of the public key which is a generator matrix of a code which looks like a random one [7], [8], [18]. A way to decrease this size is to use codes with non-trivial permutation group, which are easier to describe. This was done for example in [5] and [20] which use some particular subfield subcodes of quasi-cyclic and quasi dyadic codes.

Unfortunately, there exists an attack against these specific examples [12], [13]. We will explain in this section how this attack works against induced quasi-cyclic or quasi-dyadic GSS-RS codes.

Following the results of Section IV-C and Appendix A, it is easy to construct quasi-cyclic or quasi-dyadic induced generalized subspace subcodes and generalized projected codes of Reed-Solomon codes. For instance, if we look at the construction of the projected codes, we first construct a quasi-cyclic or a quasi-dyadic GRS code, and then we use a generalized projection which is constant on each orbit.

Definition 21: An induced quasi-cyclic (resp. quasi-dyadic) generalized projected Reed-Solomon code is a generalized projected code of a quasi-cyclic (resp. quasi-dyadic) GRS code in the meaning of Appendix B (resp. Appendix C) for which the projections are constant on the orbits of the quasi-cyclic permutation (resp. the quasi-dyadic permutation group).

The induced quasi-cyclic (resp. quasi dyadic) generalized subspace subcodes of Reed-Solomon codes are the duals of induced quasi-cyclic (resp. quasi dyadic) generalized projected Reed-Solomon codes.

Now, we will present the operation of folding on a code [12]. Let $\mathcal{C}$ be a linear code with a non-trivial permutation group $\mathrm{Per}(\mathcal{C})$. Let g be a subgroup of $\mathrm{Per}(\mathcal{C})$ such that the orbits of the coordinates under its action are all of the same length ℓ. Set $s = n/\ell$ and let orb_1^{g}, ..., orb_s^{g} be the decomposition of the support between the s distinct orbits.

Definition 22: [12] The folded code of $\mathcal{C}$ with respect to g, is the code $\overline{\mathcal{C}^{\mathsf{g}}}$ of length s obtained by summing the coefficients on each orbit orb_i^{g}:

$$\overline{\mathcal{C}^{\mathsf{g}}} = \left\{ \overline{c^{\mathsf{g}}} = (\overline{c_1}, \ldots, \overline{c_s}) \;\middle|\; \overline{c_i} = \sum_{j \in orb_i^{\mathsf{g}}} c_j,\ 1 \le i \le s,\ \forall c = (c_1, \ldots, c_n) \in \mathcal{C} \right\}.$$

Note that in the case of quasi-cyclic permutation group, g is generated by a single element σ of order dividing the quasi-cyclicity order ℓ.

We are restating without the proof one of the essential results of [12]. We want to emphasize that quasi-cyclic or quasi-dyadic GRS codes are exactly those described in Appendix. This property is fundamental in the proof of this theorem.

Proposition 18: Let $\mathcal{C}$ be a quasi-cyclic or a quasi-dyadic GRS code. The folded code of $\mathcal{C}$ obtained by taking for g either an element of the quasi-cyclic permutation group or a subgroup of the quasi-dyadic permutation group is a GRS code.

An additional fact is that there exists an explicit link between the parameters (*i.e.* the support and the scalars) of the original GRS code and its folded code. This is the basis of the cryptanalyses presented in [12].

The main result of this section is the fact that this kind of cryptanalysis works also for induced quasi-cyclic or quasi-dyadic GSS-RS codes.

Suppose that C is an induced quasi-cyclic or quasi-dyadic generalized Projected GRS code of order ℓ and index s.

Let ψ_1, ..., ψ_s be the s projections applied on each orbit.

Let $\overline{\Psi}^{\mathsf{g}} = (\psi_1, \ldots, \psi_1, \psi_2, \ldots, \psi_2, \ldots, \ldots, \psi_s, \ldots, \psi_s)$ be the projection obtained by repeating the ψ_i's ℓ times. So $C = \overline{\Psi}^{\mathsf{g}}(\mathrm{GRS}_k)$ where GRS_k is a GRS code invariant under the action of g.

Proposition 19: With the previous notations, the folded code $\overline{C^{\mathsf{g}}}$ is the $\overline{\Psi}$-projected of the folded code $\overline{\mathrm{GRS}_k^{\mathsf{g}}}$.

Proof: The ψ_i are linear mapping, so summing on a given orbit and applying ψ_i on the result give the same result than applying ψ_i on each coefficient of the orbit and then summing the coefficients. ∎

Using Proposition 18 and Proposition 19 shows that from the dual of an induced quasi-cyclic or quasi-dyadic GSS-RS code, the folding operation applied to its dual leads to obtain a Projected GRS code of length s.

Following the algebraic attack developed in [12], [13], the resistance against this kind of structural attacks is those of a code of length s instead of $n = \ell s$ then an induced quasi-cyclic or quasi-dyadic GSS-RS code is used.

VII. Conclusion

In this paper we studied in detail the notion of subspace subcodes and generalized subspace subcodes. We applied our results to the family of Reed-Solomon codes and obtained some codes with interesting parameters. We looked at potential application in code-based cryptography.

Concerning future works on this topic, it will be interesting to better understand the notion of orthogonal construction and exceptional subspace subcodes, since these codes have better parameters than those who meet the lower bound of Corollary 2.

For cryptographic application, it will be necessary to design a protocol with practical parameters taking in account the folding attacks.

APPENDIX

A. Permutation Group of GRS Codes

To better understand some properties of Reed-Solomon codes, we need to recall some results on automorphism group of Reed-Solomon codes. More details on automorphism groups of Reed-Solomon codes can be found in [1]–[3], [6], [11], [16].

Let α be a primitive root of $\mathbb{F}_{q^m}^*$, and $n = q^m - 1$. We set $S_\alpha = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. It is well-known that the Reed-Solomon codes of support S_α are cyclic. The shift permutation of a cyclic Reed-Solomon code corresponds to the permutation $\sigma_\alpha : x \mapsto \alpha x$ of the support of the code.

A cyclic Reed-Solomon code can be extended by adding a parity check symbol. This extended cyclic code is the Reed-Solomon code with support $\overline{S_\alpha} = (0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. This code is affine-invariant [1], [6], which means that it is invariant under any permutation of the support corresponding to an affine mapping $\sigma_{a,b} : x \mapsto ax+b$, $a \in \mathbb{F}_{q^m}^*$ and $b \in \mathbb{F}_{q^m}$.

It is possible to extend a second times a cyclic Reed-Solomon code by adding the ∞ point in the support. It is a bit technical and is described in detail in [11]. The main result is the fact that this doubly extended Reed-Solomon code is invariant under some automorphisms for which the underlying permutation is an homography $x \mapsto \frac{ax+b}{cx+d}$, a, b, c and d in $\mathbb{F}_{q^m}$, $ac - bd \neq 0$ and $x \in \overline{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m} \cup \{\infty\}$.

In addition, one can notice that the permutation group generated by σ_α is transitive on $\mathbb{F}_{q^m}^*$, the affine group is doubly transitive on $\mathbb{F}_{q^m}$ and the homographies group is triply transitive on $\overline{\mathbb{F}_{q^m}}$.

Applying one of these mapping to the support S of a Reed-Solomon code does not change the code. In particular, all the Reed-Solomon codes $\mathrm{RS}_k(S)$ of length $n = q^m - 1$ are equivalent. The same property holds for Reed-Solomon codes of length q^m or $q^m + 1$ (with the ∞ point in the support).

For any length $n \leq q^m + 1$ and any dimension k, if there exists an homography which sends a support S on another support S' of size n, then there exists a multiplier Λ such that $\mathrm{RS}_k(S)$ and $\mathrm{GRS}_k(S', \Lambda)$ are equal.

So it is always possible to fix arbitrary three distinct points of the support S of a Reed-Solomon code. This fact is used in cryptanalysis of cryptosystems based on GRS, Alternant or Goppa codes [12], [13], [21] and in Section VI-B.

Using the construction presented in Section IV-C, we are able to construct some GRS codes with prescribed permutations groups.

B. Quasi-Cyclic GRS Codes

Quasi-cyclic GRS codes arise when looking at the permutations of the support of the form $\sigma_\beta(x) = \beta x$, $\beta \in \mathbb{F}_{q^m}^*$ of order $\ell | q^m - 1$.

It can be done in two steps.

The first one consists in the construction of a quasi-cyclic Reed-Solomon code:

- We choose $\beta \in \mathbb{F}_{q^m}^*$ of order $\ell | q^m - 1$ and an index $s \leq s_{max} = (q^m - 1)/\ell$. The length of the code is then $n = s\ell$.
- We fix s disjoint orbits under σ_β. Up to a cyclic shift, they are of the form $\alpha^i S_\beta = (\alpha^i, \alpha^i\beta, \alpha^i\beta^2, \ldots, \alpha^i\beta^{\ell-1}), \quad i \in [0, s_{max} - 1]$.
- The support S of a quasi-cyclic Reed-Solomon code of order ℓ and index s is then the union of these s orbits.

The second one consists to choose a multiplier which preserves the quasi-cyclic structure. Following Section IV-C, it can be done as follows:

- We choose an element β' of order dividing ℓ ($\beta' = \beta^u$ for some u) and construct the ℓ-tuple $S_{\beta'} = (1, \beta', \beta'^2, \ldots, \beta'^\ell)$.
- For each orbit choose a scalar $\lambda_i \in \mathbb{F}_{q^m}^*$, $i \in [1, s]$. The multiplier Λ is then the union of the s ℓ-tuple $\lambda_i S_{\beta'}$.

This algorithm is the one that is used in [5] to construct quasi-cyclic Alternant code in the context of the design of a public key cryptosystem.

C. Quasi-Dyadic GRS Codes

Our presentation of dyadic and quasi-dyadic codes is not those used in [13], [20], but leads to the same quasi-dyadic codes. In this section, we set $q = 2$. Our starting point is a subgroup of the translation group acting on $\mathbb{F}_{2^m}$: $\{\tau_\beta : x \mapsto x + \beta \mid \beta \in \mathbb{F}_{2^m}\}$.

Let r be an integer less or equal to m and $n = 2^r$. Let V be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension r. The dyadic permutation group is then the group of translations $\mathrm{Pdy}_V = \{\tau_\beta \mid \beta \in V\}$ acting on V or one of its translated $V + \gamma$.

The quasi-dyadic permutation group is the same translation group Pdy_V, but acting on an union of s translates of V.

To make the link with the usual presentation of dyadic matrices, it is necessary to order the support V as follows: if $\mathcal{B}_V = (b_0, \ldots, bv_{r-1})$ is a basis of V, we denote by $V_{\mathcal{B}_V}$ the support containing all the elements of V ordered by the lexicographic order induced by $\mathcal{B}_V$. For instance, if $\mathcal{B} = (b_0, b_1, b_2)$, then $V_{\mathcal{B}} = (0, b_0, b_1, b_0+b_1, b_2, b_0+b_2, b_1+b_2, b_0+b_1+b_2)$.

A dyadic Reed-Solomon code of order 2^r is then a Reed-Solomon code of support $V_{\mathcal{B}}$.

A quasi-dyadic Reed-Solomon code of order 2^r and index s is a Reed-Solomon code having for support s translates of $V_{\mathcal{B}}$.

A quasi-cyclic GRS code is a GRS code having the same support than a quasi-dyadic Reed-Solomon code, with multiplier that is constant on each translate $\tau_\gamma(V_{\mathcal{B}})$.

One can show that this construction is equivalent to those of quasi-dyadic Cauchy codes given in [20].

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees and Olivier Ruatta for their helpful comments, remarks, and suggestions.

REFERENCES

[1] T. P. Berger, "Cyclic alternant codes induced by an automorphism of a GRS code," in *Finite Fields: Theory, Applications, and Algorithms* (Contemporary Mathematics), vol. 225, R. Mullin and G. Mullen, Eds. Waterloo, ON, Canada: AMS, 1999, pp. 143–154.

[2] T. P. Berger, "On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes, and extended Goppa codes," *Finite Fields Appl.*, vol. 6, pp. 255–281, Jul. 2000.

[3] T. P. Berger, "Goppa and related codes invariant under a prescribed permutation," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2628–2633, Nov. 2000.

[4] T. P. Berger and N. E. Amrani, "Codes over $L(GF(2)^m, GF(2)^m)$, MDS diffusion matrices and cryptographic applications," in *Codes, Cryptology, and Information Security* (Lecture Notes in Computer Science), vol. 9084, S. E. Hajji, A. Nitaj, C. Carlet, and E. Souidi, Eds. Cham, Switzerland: Springer, 2015, pp. 197–214.

[5] T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani, "Reducing key length of the McEliece cryptosystem," in *Progress in Cryptology—AFRICACRYPT*, (Lecture Notes in Computer Science), vol. 5580, B. Preneel, Ed. Berlin, Germany: Springer, 2009, pp. 77–97.

[6] T. P. Berger and P. Charpin, "The automorphism groups of BCH codes and of some affine-invariant codes over extension fields," *Des., Codes Cryptogr.*, vol. 18, pp. 29–53, Dec. 1999.

[7] T. P. Berger, P. Gaborit, and O. Ruatta, "Gabidulin matrix codes and their application to small ciphertext size cryptosystems," in *Progress in Cryptology—INDOCRYPT* (Lecture Notes in Computer Science), vol. 10698, A. Patra and N. P. Smart, Eds. Cham, Switzerland: Springer, 2017, pp. 247–265.

[8] T. P. Berger and P. Loidreau, "How to mask the structure of codes for a cryptographic use," *Des., Codes Cryptograph.*, vol. 35, no. 1, pp. 63–79, 2005.

[9] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, 1997.

[10] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes* (North Holland Mathematical Library). Amsterdam, The Netherlands: Elsevier, 1997.

[11] A. Dür, "The automorphism groups of Reed-Solomon codes," *J. Combinat. Theory, A*, vol. 44, no. 1, pp. 69–82, 1987.

[12] J. Faugère, A. Otmani, L. Perret, F. de Portzamparc, and J.-P. Tillich, "Structural cryptanalysis of McEliece schemes with compact keys," *Des. Codes Cryptogr.*, vol. 79, no. 1, pp. 87–112, 2016.

[13] J. Faugère, A. Otmani, L. Perret, and J.-P. Tillich, "Algebraic cryptanalysis of McEliece variants with compact keys," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 6110, H. Gilbert, Ed. Berlin, Germany: Springer, 2010, pp. 279–298.

[14] E. M. Gabidulin and P. Loidreau, "Properties of subspace subcodes of Gabidulin codes," *Adv. Math. Commun.*, vol. 2, no. 2, pp. 147–157, 2008.

[15] M. Hattori, R. J. McEliece, and G. Solomon, "Subspace subcodes of Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1861–1880, Sep. 1998.

[16] W. C. Huffman, "Groups and codes," in *Handbook Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 17.

[17] J. Justesen and T. Høholdt, *A Course in Error-Correcting Codes* (Mathematical Society). Zurich, Switzerland: European Mathematical Society, 2004.

[18] R. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol., Pasadena, CA, USA, Tech. Rep. 44, Jan. 1978, pp. 114–116.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1986.

[20] R. Misoczki and P. S. L. M. Barreto, "Compact McEliece Keys from Goppa codes," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 5867. Berlin, Germany: Springer, 2009, pp. 376–392.

[21] V. M. Sidelnikov and S. O. Shestakov, "On insecurity of cryptosystems based on generalized Reed-Solomon codes," *Discrete Math. Appl.*, vol. 2, no. 4, pp. 439–444, 1992.

[22] S. A. Spence, "Identifying high-dimension subspace subcodes of Reed-Solomon Codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1280–1282, Jun. 2004.

[23] C. Wieschebrink, "Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 6061, N. Sendrier, Ed. Berlin, Germany: Springer, 2010, pp. 61–72.

Thierry P. Berger received the Ph.D. degree and the French Habilitation (Mathematics) from the University of Limoges, France. From 1998 to 2014, he was Professor in the Department of Mathematics and Computer and the scientific head of the Cryptology and Information Security group.

He is currently Professor Emeritus at the University of Limoges. His research interests include finite algebra, automorphism group of codes, links between coding and cryptography, stream cipher and pseudorandom generators and dedicated block ciphers.

Cheikh Thiécoumba Gueye was Assistant Professor from 1997 to 2008 and Associate Professor from 2008 to 2012 at Cheikh Anta Diop University of Dakar (UCAD), Senegal, in the Department of mathematics and Computer Science.

Since October 2012 he is Full Professor at Cheikh Anta Diop University of Dakar (UCAD) and currently the head of the Laboratory of Algebra, Cryptology, Algebraic Geometry and Applications (LACGAA) of UCAD

His interests research is Coding Theory, Post-quantum Cryptography and Communications Security and Reliability.

Jean Belo Klamti achieved his PhD degree on 29 January 2018 at Cheikh Anta Diop University of Dakar (UCAD). He is member of DAGS team which responsed to the NIST's call for standardization of Post-quantum.

His research interests are Computational Algebra, Coding Theory, Post-quantum cryptography, Pseudorandom Generators, Designing of Algorithms, Software and hardware Implementation.