HAL
open science

On the security of Some Compact Keys for McEliece Scheme

Elise Barelli

To cite this version:

Elise Barelli. On the security of Some Compact Keys for McEliece Scheme. WCC 2017 - The Tenth International Workshop on Coding and Cryptography, Sep 2017, St Petersbourg, Russia. pp.1-9. hal-01674546

HAL Id: hal-01674546

https://inria.hal.science/hal-01674546v1

Submitted on 3 Jan 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the security of Some Compact Keys for McEliece Scheme

Élise Barelli

INRIA Saclay and LIX, CNRS UMR 7161 École Polytechnique,
91120 Palaiseau Cedex
elise.barelli@inria.fr

Abstract. In this paper we study the security of the key of compact McEliece schemes based on alternant/Goppa codes with a non-trivial permutation group, in particular quasi-cyclic alternant codes. We show that it is possible to reduce the key-recovery problem on the original quasi-cyclic code to the same problem on a smaller code derived from the public key. This result is obtained thanks to the *invariant* operation which gives the subcode whose elements are invariant under a permutation $\sigma \in \mathrm{Perm}(\mathcal{C})$. The fundamental advantage of this invariant code is that it preserves the alternant structure, ie: the invariant subcode of an alternant code is an alternant code. This approach improves the technique of Faugère, Otmani, Tillich, Perret and Portzamparc which uses *folded* codes of alternant codes obtained by using supports globally stable by an affine map. We use a simpler approach with a unified view on quasi-cyclic alternant codes and we extend the key-recovery to the non-affine case, for all codes obtained by using supports globally stable by a homography.

1 Introduction

In 1978, McEliece [14] introduced a public key encryption scheme based on linear codes and suggested to use classical Goppa codes which belong to the family of alternant codes. This proposition still remains secure but leads to very large public keys compared to other public-key cryptosystems. That is why, in despite of its fast encryption and decryption, McEliece scheme is limited for practical applications. To overcome this limitation, lot of activity devote to decrease the key size by choosing codes which admit a very compact public matrix. For instance, quasi-cyclic (QC) codes enable to build public key encryption schemes with short keys [9,3]. These first papers were followed by proposals using alternant and Goppa codes with different automorphism groups like quasi-dyadic (QD) Goppa codes [15].

The hope that the additional structure does not deteriorate the security of the cryptographic scheme was first eroded by algebraic attacks against QC and QD alternant codes [7]. Such attacks use the specific structure of QC/QD codes in order to build an algebraic system with much fewer unknowns than the generic case. A new approach has been used in [6,5] to explain that the reduction of the number of unknowns in the algebraic system comes from a smaller code hidden behind the public generator matrix. This smaller code can be obtained by summing up the codewords which belong to the same orbit under the action of the permutation group and is referred to as the *folded* code. (We advertise the reader that the folded codes referenced in [11] are not the same codes as in this paper.) A relation between the support and multiplier defining the alternant code and those of the folded code exists and is sufficient to find the original alternant code. This relation comes from the structure of the folded code: [5] shows that the folding operation preserves the structure of the dual code. That is, the folding of the dual of an alternant code (resp. a Goppa code) is the dual of an alternant code (resp. a Goppa code).

The folding approach is not enough to attack any alternant or Goppa code with a non trivial automorphism group: it only applies to codes with an automorphism induced by an affine transformation acting on the support and the multiplier, we call them *affine induced* automorphims. Another kind of quasi-cyclic alternant codes can be built from the action of the projective linear group on the support and multiplier. We use in this paper a smaller alternant code built from the public generator matrix of a quasi-cyclic alternant code induced by a projective linear transformation, called the *invariant* code and introduced by Loidreau in [12]. This invariant code can be built easily from the public generator matrix of the alternant code $\mathcal{C}$ since it is the kernel of the linear

map: $c \in \mathcal{C} \mapsto c - \sigma(c)$, where σ is a permutation of $\mathcal{C}$. We remark also that the folded code used by [5] is included in the invariant code. This allows us to extend the attack of [6,5] to the case of codes obtained by using supports globally stable by a homography.

Our main contribution is to consider more general tools coming from algebraic geometry and use the invariant code instead of folded code. This approach has two advantages. First the geometric point of view simplifies the attack by giving a unified view of quasi-cyclic alternant codes. It also simplifies some proofs and enables to consider alternant codes as algebraic geometric codes on the projective line. This method allows us to treat the general case of projective linear transformations. The second advantage is that the invariant code acts directly on the alternant code and not on the dual code. More precisely, we show the following results.

Theorem 2. *Let* $\mathrm{GRS}_k(x,y) := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) \subset \mathbb{F}_{q^m}^n$ *be a* σ*-invariant AG code, with* $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ *of order* ℓ *and* $\mathcal{P}$ *and* G *defined as (2) and (3). Then the invariant code* $\mathrm{GRS}_k(x,y)^\sigma$ *is a GRS code of length* n/ℓ *and dimension* k/ℓ*.*

Corollary 1. *Let* $\mathcal{A}_r(x,y) := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) \cap \mathbb{F}_q^n$ *be a* σ*-invariant alternant AG code, with* $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ *of order* ℓ *and* $\mathcal{P}$ *and* G *defined as (2) and (3). Then the invariant code* $\mathcal{A}_r(x,y)^\sigma$ *is an alternant code of length* n/ℓ *and order* r/ℓ*.*

This means that the key security of compact McEliece scheme based on alternant codes with some induced permutation is reduced to the key security of the short code obtained from the invariant operation.

2 Quasi-cyclic Alternant Codes

In this section, we introduce some notation about alternant codes. We denote by $\mathbb{F}_q$ the finite field with q elements, where q is a power of a prime p.

Let $x = (x_1, \ldots, x_n)$ be a n-tuple of distinct elements of $\mathbb{F}_q$, and $y = (y_1, \ldots, y_n)$ be an n-tuple of nonzero elements of $\mathbb{F}_q$. The generalised Reed-Solomon code of dimension k, denoted $\mathrm{GRS}_k(x,y)$, consists of vectors $(y_1 f(x_1), \ldots, y_n f(x_n))$ where f ranges over all polynomials of degree $< k$, with coefficients in $\mathbb{F}_q$. The vector x is called the *support* and y a *multiplier* of the code $\mathrm{GRS}_k(x,y)$. In order to define alternant codes, we use the following property whose a proof can be found in [13, Chap. 12].

Proposition 1. *The dual of* $GRS_k(x,y)$ *is* $GRS_{n-k}(x,y^\perp)$ *for some* $y^\perp \in (\mathbb{F}_q \setminus \{0\})^n$*.*

Definition 1. *Let* m *be a positive integer,* x *be an* n*-tuple of distinct elements of* $\mathbb{F}_{q^m}$ *and* y *be an* n*-tuple of nonzero elements of* $\mathbb{F}_{q^m}$*. The alternant code* $\mathcal{A}_k(x,y)$ *over* $\mathbb{F}_q$ *is the subfield subcode of* $GRS_k(x,y)^\perp$*, ie:* $\mathcal{A}_k(x,y) := GRS_k(x,y)^\perp \cap \mathbb{F}_q^n$*.*

2.1 Representation of $\mathcal{A}_k(x,y)$ as a subfield subcode of an AG code

For the rest of our work, it is convenient to use a projective representation of alternant codes. This is possible thanks to algebraic geometric codes introduced by Goppa in [10]. To avoid the confusion with classical Goppa codes which are specific alternant codes, we referred to algebraic geometric codes as AG codes. Any AG code considered in the following is an AG code on $\mathbb{P}^1_{\mathbb{F}_{q^m}}$, the projective line over $\mathbb{F}_{q^m}$. Recall some definitions in this case (cf [8,17] for further details).

For brevity we denote by $\mathbb{P}^1$ the projective line over $\mathbb{F}_{q^m}$. We can consider $\mathbb{F}_{q^m}(\mathbb{P}^1)$, the function field over $\mathbb{F}_{q^m}$ associated to the curve $\mathbb{P}^1$. A divisor of $\mathbb{P}^1$ is a formal sum, with integers coefficients, of points of $\mathbb{P}^1$ and for $f \in \mathbb{F}_{q^m}(\mathbb{P}^1)$, the principal divisor of f, denoted by (f), is defined as the formal sum of zeros and poles of f, counted with multiplicity. For a divisor G, we denote by $\deg(G)$ the degree of G and by $\mathcal{L}(G) := \{f \in \mathbb{F}_{q^m}(\mathbb{P}^1) \mid (f) \geq -G\} \cup \{0\}$, the Riemann-Roch space associated to G. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n distinct points of $\mathbb{P}^1$ with coordinates in $\mathbb{F}_{q^m}$

and G be a divisor such that $\deg(G) < n$ and G does not contain any point of $\mathcal{P}$. We consider the following map:

$$\begin{array}{rcl} \mathrm{Ev}_{\mathcal{P}} : \mathbb{F}_{q^m}(\mathbb{P}^1) & \longrightarrow & \mathbb{F}_{q^m}^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

The AG code $C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ is defined by $C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) := \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}(G)\}$.

Let $x = (x_1, \ldots, x_n)$ be an n-tuple of distinct elements of $\mathbb{F}_{q^m}$, and $y = (y_1, \ldots, y_n)$ be an n-tuple of nonzero elements of $\mathbb{F}_{q^m}$. Then $\mathrm{GRS}_k(x, y)$ is the AG code $C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ where $\mathcal{P} := \{(x_i : 1) | \, i \in \{1, \ldots, n\}\}$ and $G := (k-1)P_\infty - (f)$, with $f \in \mathbb{F}_{q^m}(\mathbb{P}^1)$ a function with pole order $n-1$ at P_∞, which is the interpolation polynomial of degree $n-1$ of $y_1, \ldots, y_n$ through the points $x_1, \ldots, x_n$. With the same notation, we have $\mathcal{A}_k(x, y) := C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)^\perp \cap \mathbb{F}_q^n$.

2.2 Induced permutations of Alternant Codes

We explain how we can construct an alternant code invariant under a prescribed permutation of the support $\{1, \ldots, n\}$, with n the length of the code. In [4], Dür determines the automorphism group of GRS codes and in [1,2], Berger uses this to construct families of alternant codes invariant under a permutation. In particular, Berger deals with some alternant codes invariant under a permutation induced by the action of an element of the projective semi-linear group $\mathrm{P}\Gamma\mathrm{L}_2(\mathbb{F}_{q^m})$ on the support and the multiplier. Here we will only be interested in projective linear transformations. First of all, we recall the definition of the projective linear group $\mathrm{PGL}_2(\mathbb{F}_{q^m})$. It is the automorphism group of the projective line $\mathbb{P}^1$ defined by:

$$\mathrm{PGL}_2(\mathbb{F}_{q^m}) := \left\{ \begin{array}{rcl} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ (x : y) & \longmapsto & (ax + by : cx + dy) \end{array} \middle| \begin{cases} a, b, c, d \in \mathbb{F}_{q^m}, \\ ad - bc \neq 0 \end{cases} \right\}.$$

The permutations of $\mathrm{PGL}_2(\mathbb{F}_{q^m})$ have also a matrix representation, ie:

$$\forall \sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m}), \text{ we write } \sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ with } ad - bc \neq 0. \tag{1}$$

Where the elements a, b, c and d are defined up to a multiplication by a nonzero scalar. Now, we deal with permutations of an alternant code. We recall the following definition.

Definition 2. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_{q^m}$. Let $\sigma \in S_n$ be a permutation, acting on $\mathcal{C}$ via $\sigma(c_1, \ldots, c_n) = (c_{\sigma(1)}, \ldots, c_{\sigma(n)})$. Then the permutation group of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, is $Perm(\mathcal{C}) := \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\}$.*

In the case of GRS codes, for appropriate dimension, Dür [4] shows that the whole permutation group is induced by the action of the projective linear group on the support of the code. The same property has been shown by Stichtenoth [16], with the representation of GRS codes as AG rational codes. More precisely, for appropriate parameters, every permutation of $\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ is induced by a projective linear transformation. We give the main definitions and theorems of [16].

We keep the notation of the previous section. Let G and G' be divisors of $\mathbb{P}^1$, we note $G \approx_{\mathcal{P}} G'$ if there exists $f \in \mathbb{F}_{q^m}(\mathbb{P}^1)$, $f \neq 0$, such that $G - G' = (f)$ and $f(P) = 1$, for all $P \in \mathcal{P}$. With this definition we have the following lemma:

Lemma 1. [16] *If $G \approx_{\mathcal{P}} G'$ then $\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G')$.*

Before giving the theorem which allows us to construct any GRS code invariant under a permutation, we define:

Definition 3. $\mathrm{Aut}_{\mathcal{P},G}(\mathbb{P}^1) := \{\sigma \in \mathrm{Aut}(\mathbb{P}^1) \mid \sigma(\mathcal{P}) = \mathcal{P} \text{ and } \sigma(G) \approx_{\mathcal{P}} G\}$.

Theorem 1. [16] *Let $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ be an AG code with $1 \leq deg(G) \leq n-3$. Then* $\mathrm{Perm}(\mathcal{C}) = \mathrm{Aut}_{\mathcal{P},G}(\mathbb{P}^1)$.

Now we have all the properties required to construct some alternant codes invariant under a permutation. We recall that a closed point of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ is an orbit of a point, with coordinates in a finite extension of $\mathbb{F}_{q^m}$, under the Frobenius transformation: $(x : y) \mapsto (x^{q^m} : y^{q^m})$. We consider $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ and $\ell = ord(\sigma)$. We define the support:

$$\mathcal{P} := \coprod_{i=1}^{n/\ell} Orb_\sigma(Q_i), \tag{2}$$

where the points $Q_i \in \mathbb{P}^1_{\mathbb{F}_{q^m}}$ are pairwise distinct with trivial stabiliser subgroup and $Orb_\sigma(Q_i) := \{\sigma^j(Q_i) \mid j \in \{1..\ell\}\}$. We define the divisor:

$$G := \sum_{i=1}^{s} t_i \sum_{j=1}^{\ell} \sigma^j(Q_i), \tag{3}$$

with Q_i closed points of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$, $s \in \mathbb{N}$, $t_i \in \mathbb{Z}$ for $i \in \{1, \ldots, s\}$ and $\deg(G) = \sum_{i=1}^{s} t_i \ell$.

The automorphism σ of $\mathbb{P}^1$ induces a permutation $\tilde{\sigma}$ of $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ defined by:

$$\begin{array}{rccc} \tilde{\sigma}\colon & \mathcal{C} & \longrightarrow & \mathcal{C} \\ & (f(P_1), \ldots, f(P_n)) & \longmapsto & (f(\sigma(P_1)), \ldots, f(\sigma(P_n))). \end{array}$$

Then $\tilde{\sigma}$ is also a permutation of $\mathcal{A} := \mathcal{C}^\perp \cap \mathbb{F}_q^n$. For short, we denote by $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ both the homography and the induced permutation on the code $\mathcal{C}$.

3 Subcodes of Alternant Codes

We can construct subcodes of $\mathcal{A}_r(x, y)$ with smaller parameters, by simple operations, which can be used to recover the alternant code $\mathcal{A}_r(x, y)$. We describe in the next section two subcodes: the *folded* code and the *invariant* code. Their interactions are also discussed. In the papers [6,5], the folding operation was used to recover dual of the considered alternant code. Here we do not need to use the dual code since the invariant code which is directly an alternant code. More precisely, we show that for alternant codes invariant under an induced permutation, the invariant operation preserves the algebraic structure of the code.

3.1 Invariant and Folded Codes

This section deals with subcodes called the *invariant* code and the *folded* code whose definitions are the following.

Definition 4. *Let $\mathcal{C}$ be a linear code and $\sigma \in Perm(\mathcal{C})$ of order ℓ, we consider the following map:*

$$\begin{aligned} \varphi\colon \mathcal{C} &\to \mathcal{C} \\ c &\mapsto \sum_{i=0}^{\ell-1} \sigma^i(c). \end{aligned}$$

The folded code of $\mathcal{C}$ is defined by $\mathrm{Fold}_\sigma(\mathcal{C}) := \mathrm{Im}(\varphi)$ and the invariant code of $\mathcal{C}$ is defined by $\mathcal{C}^\sigma := \ker(\sigma - \mathrm{Id})$.

The folded code was used in [6,5], in order to construct a structured subcode invariant by a given permutation σ. Indeed, by the previous definition, we remark that $\mathrm{Fold}_\sigma(\mathcal{C})$ is σ-invariant.

Proposition 2. *The codes $\mathrm{Fold}_\sigma(\mathcal{C})$ and $\mathcal{C}^\sigma$ are subcodes of $\mathcal{C}$ and we have: $\mathrm{Fold}_\sigma(\mathcal{C}) \subseteq \mathcal{C}^\sigma$.*

These two codes are not equal in the general case but we have the following lemma. We recall that p is the characteristic of $\mathbb{F}_q$ and $\ell = ord(\sigma)$.

Lemma 2. *If $p \nmid \ell$ then* $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$.

Proof. Let φ be the map of Definition 4, by the previous proposition we know that:

$$\mathrm{Im}(\varphi) \subseteq \ker(\sigma - \mathrm{Id}).$$

Now, we will show that $\dim(\mathrm{Im}(\varphi)) = \dim(\ker(\sigma - \mathrm{Id}))$.
By the rank–nullity theorem we know that:

$$\dim(\mathrm{Im}(\varphi)) = \dim(\mathcal{C}) - \dim(\ker(\varphi)).$$

Otherwise, $\sigma^\ell - \mathrm{Id} = (\mathrm{Id} + \sigma + \cdots + \sigma^{\ell-1})(\sigma - \mathrm{Id})$, with $\gcd(\sum_{i=0}^{\ell-1} X^i, X-1) = 1$ since $p \nmid \ell$. Hence we have $\mathcal{C} = \ker(\varphi) \oplus \ker(\sigma - \mathrm{Id})$, hence

$$\dim(\ker(\sigma - \mathrm{Id})) = \dim(\mathcal{C}) - \dim(\ker(\varphi)).$$

Therefore $\ker(\sigma - \mathrm{Id}) = \mathrm{Im}(\varphi)$ and $Fold(\mathcal{C}) = \mathcal{C}^\sigma$.

Remark 1. In [5] an example of the folded and the invariant codes of a σ-invariant alternant code $\mathcal{A}$ is given. In this example, the authors wrote that $\mathrm{Fold}_\sigma(\mathcal{A}) \subsetneq \mathcal{A}^\sigma$ but in this case these two codes must be equal. Indeed, for this example, $p = 3 \nmid 2 = ord(\sigma)$ and by the previous lemma we have $\mathrm{Fold}_\sigma(\mathcal{A}) = \mathcal{A}^\sigma$.

Remark 2. If $c \in \mathrm{Fold}_\sigma(\mathcal{C})$ or $c \in \mathcal{C}^\sigma$, then c takes constant value on the orbits under the action of σ: $\{i, \sigma(i), \ldots, \sigma^{\ell-1}(i)\}$. In order to work with codes without repeated coordinates, we choose $I \subset \{1, \ldots, n\}$ a set of representatives of orbits $\{\sigma^j(i) | j \in \{0, \ldots, \ell-1\}\}$ and we consider the codes restricted on this set: $\mathrm{Fold}_\sigma(\mathcal{C})|_I$ and $\mathcal{C}^\sigma|_I$. For short, we keep the notations $\mathrm{Fold}_\sigma(\mathcal{C})$ and $\mathcal{C}^\sigma$, for the restricted codes.

Here the subcode that we analyse is $\mathcal{C}^\sigma$, but this lemma allows us to use the $\mathbb{F}_q$-linear property of the folded operation in the equality case. More precisely, to apply the folding operation on a linear code $\mathcal{C}$ it suffices to apply folding operation on a basis of $\mathcal{C}$. This property will be useful in §3.2.3.

3.2 The Invariant Code of $\mathcal{A}_r(x, y)$

In order to study the invariant code of $\mathcal{A}_r(x, y)$, we first notice that the invariant operation commutes with the subfield subcode operation. Indeed, if $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$, σ-invariant then:

$$(\mathcal{C} \cap \mathbb{F}_q^n)^\sigma = \{c \in \mathcal{C} \mid c \in \mathbb{F}_q^n \text{ and } \sigma(c) = c\} = \mathcal{C}^\sigma \cap \mathbb{F}_q^n.$$

In order to prove that the invariant code of $\mathcal{A}_r(x, y)$ is also an alternant code we have to prove that the invariant code of a GRS code is a GRS code. Later on, the GRS codes will be described by $\mathcal{C}_\mathcal{L}(\mathbb{P}^1, \mathcal{P}, G)$, as in Section 2.2. The two lemmata to follow describe the action of an element $\sigma \in \mathrm{PGL}_2$ on the codes $\mathcal{C}_\mathcal{L}(\mathbb{P}^1, \mathcal{P}, G)$ and provide a description of $\mathcal{C}_\mathcal{L}(\mathbb{P}^1, \mathcal{P}, G)^\sigma$.

Lemma 3. *Let $c = Ev_\mathcal{P}(f) \in \mathcal{C}_\mathcal{L}(\mathbb{P}^1, \mathcal{P}, G)^\sigma$ such that $\sigma(c) = c$, then f is σ-invariant, ie: $f \circ \sigma = f$.*

Proof. Let $c = (f(P_1), \ldots, f(P_n)) \in \mathcal{C}$ such as $\sigma(c) = c$, then:

$$\begin{aligned} \forall i \in \{1, \ldots, n\},\ f(P_{\sigma(i)}) = f(P_i) &\Leftrightarrow \forall i \in \{1, \ldots, n\},\ f \circ \sigma(P_i) = f(P_i) \\ &\Leftrightarrow \forall i \in \{1, \ldots, n\},\ (f \circ \sigma - f)(P_i) = 0. \end{aligned}$$

Since $\sigma(G) = G$, $f \circ \sigma \in \mathcal{L}(G)$, and then $(f \circ \sigma - f) \in \mathcal{L}(G)$. Hence if $(f \circ \sigma - f)$ was nonzero, it should have at most $d < n$ zeros on $\mathbb{P}^1$, which is a contradiction. Therefore $(f \circ \sigma - f) \equiv 0$ and f is σ-invariant.

Lemma 4. *Let $\mathcal{C} := \mathcal{C}_\mathcal{L}(\mathbb{P}^1, \mathcal{P}, G)$ be a σ-invariant AG code and $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$. Then $\sigma' := \rho \circ \sigma \circ \rho^{-1}$ induces the same permutation on $\mathcal{C}$ as σ.*

Proof. We first prove that:

$$\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \rho^{-1}(\mathcal{P}), \rho^{-1}(G)) = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G).$$

Let $c = (f(P_1), \ldots, f(P_n))$ be a codeword of $\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$. Then, we have $c = (f \circ \rho \circ \rho^{-1}(P_1), \ldots, f \circ \rho \circ \rho^{-1}(P_n))$. As $f \in \mathcal{L}(G)$, the function $h = f \circ \rho \in \mathcal{L}(\rho^{-1}(G))$. Hence, $c \in \{\mathrm{Ev}_{\rho^{-1}(\mathcal{P})}(h) \mid h \in \mathcal{L}(\rho^{-1}(G))\} = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \rho^{-1}(\mathcal{P}), \rho^{-1}(G))$.
Now, for all $c = (f(P_1), \ldots, f(P_n)) \in \mathcal{C}$, we have:

$$\begin{aligned}\sigma'(c) &= (f \circ \rho \circ \sigma \circ \rho^{-1}(P_1), \ldots, f \circ \rho \circ \sigma \circ \rho^{-1}(P_n)) \\ &= (h \circ \sigma(\rho^{-1}(P_1)), \ldots, h \circ \sigma(\rho^{-1}(P_n)))\end{aligned}$$

with $h = f \circ \rho \in \mathcal{L}(\rho^{-1}(G))$. Since $\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \rho^{-1}(\mathcal{P}), \rho^{-1}(G)) = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$, σ' induces the same permutation of the code $\mathcal{C}$ as σ.

Theorem 2. *Let* $\mathrm{GRS}(x, y) := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) \subseteq \mathbb{F}_{q^m}^n$ *be a* σ*-invariant AG code, with* $\sigma \in \mathrm{PGL}_2(\mathbb{P}^1_{\mathbb{F}_{q^m}})$ *of order* ℓ *and* $\mathcal{P}$ *and* G *defined as (2) and (3). Then the invariant code* $\mathrm{GRS}(x, y)^\sigma$ *is a GRS code of length* n/ℓ.

Corollary 1. *Let* $\mathcal{A}(x, y) := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) \cap \mathbb{F}_q^n$ *be a* σ*-invariant alternant AG code, with* $\sigma \in \mathrm{PGL}_2(\mathbb{P}^1_{\mathbb{F}_{q^m}})$ *of order* ℓ *and* $\mathcal{P}$ *and* G *defined as (2) and (3). Then the invariant code* $\mathcal{A}(x, y)^\sigma$ *is an alternant code of length* n/ℓ.

In order to prove Theorem 2, we consider $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ with $\ell = ord(\sigma)$ and we define the support $\mathcal{P}$ and the divisor G as (2) and (3). Later on, to simplify the demonstrations we assume that all the orbits have the same length, equals to ℓ, and G is constructed from one closed point Q. The result remains true for the general case but here, in the definition (3), we assume that $s = 1$ and we denote $t_1 = t$.
We denote $\sigma^j(P_i) := (\alpha_{i\ell+j} : \beta_{i\ell+j})$, for $i \in \{0, \ldots, \frac{n}{\ell} - 1\}, j \in \{0, \ldots, \ell - 1\}$ and $\sigma^j(Q) := (\gamma_j : \delta_j)$, for $j \in \{0, \ldots, \ell - 1\}$.

Lemma 5. *With the previous notation, any* $f \in \mathcal{L}(G)$ *can be written as:*

$$f(X, Y) = \frac{F(X, Y)}{\prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)^t},$$

with $F \in \mathbb{F}_{q^m}[X, Y]$ *a homogeneous polynomial of degree* $t\ell$.

To the automorphism $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$, we associate a matrix $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as in (1). Three cases are possibles, depending on the eigenvalues of the matrix M:

1. $M \sim \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, with $\lambda_1 \neq \lambda_2 \in \mathbb{F}_{q^m}$,
2. $M \sim \begin{pmatrix} \lambda_1 & \mu \\ 0 & \lambda_1 \end{pmatrix}$, with $\lambda_1, \mu \in \mathbb{F}_{q^m}$,
3. $M \sim \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, with $\lambda_1 \neq \lambda_2 \in \mathbb{F}_{q^{2m}}$.

In the following, we study these three cases.

3.2.1 Case σ diagonalizable over $\mathbb{F}_{q^m}$ We suppose $\sigma = \rho \circ \sigma_d \circ \rho^{-1}$ with σ_d diagonal and $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ an automorphism of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$. W.l.o.g and by Lemma 4, one can assume that:

$$\begin{array}{rccc} \sigma: & \mathbb{P}^1 & \to & \mathbb{P}^1 \\ & (x : y) & \mapsto & (ax : y), \end{array} \tag{4}$$

with $a \in \mathbb{F}_{q^m}^*$.

Proposition 3. *Let $\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ be a σ-invariant AG code as in Theorem 2, with σ defined in (4). Let $\tilde{P}_i = (\alpha_i^\ell : \beta_i^\ell)$ and $\tilde{G} = t\tilde{Q}$, with $\tilde{Q} = \big((-1)^{\ell-1} \prod_{j=0}^{\ell-1} \gamma_j : \prod_{j=0}^{\ell-1} \delta_j\big)$, then $\mathcal{C}^\sigma = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$, which is a GRS code.*

Proof. Let $c = (f(P_1), \ldots, f(P_n)) \in \mathcal{C}$ such as $\sigma(c) = c$, by Lemma 3 $f \in \mathcal{L}(G)$ is σ-invariant, so $f(aX, Y) = f(X, Y)$. By Lemma 5, we have:

$$\frac{F(aX, Y)}{\left(\prod_{j=0}^{\ell-1} (a\delta_j X - \gamma_j Y)\right)^t} = \frac{F(X, Y)}{\left(\prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)\right)^t} \tag{5}$$

with $F \in \mathbb{F}_{q^m}[X, Y]$ an homogeneous polynomial of degree $t\ell$. Moreover the support of G is σ-invariant, so:

$$\prod_{j=0}^{\ell-1} (a\delta_j X - \gamma_j Y) = \prod_{j=0}^{\ell-1} (a\delta_j X - a\gamma_j Y) = a^\ell \prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)\cdot$$

Hence, (5) becomes $F(aX, Y) = a^{t\ell} F(X, Y)$, ie: $F(aX, Y) = F(X, Y)$, because $\ell = \mathrm{ord}(a)$. To study this kind of invariant polynomial we need to use the following proposition.

Proposition 4. [5, Prop 4] *Let $F \in \mathbb{F}_q[X, Y]$ be a homogeneous polynomial of degree $t\ell$, and $a \in \mathbb{F}_{q^m}$ of order ℓ. If $F(aX, Y) = F(X, Y)$, then $F(X, Y) = R(X^\ell, Y^\ell)$, with $R \in \mathbb{F}_{q^m}[X, Y]$ an homogeneous polynomial of degree t.*

We present here a simpler proof of Proposition 4.

Proof. The homogeneous polynomial F can be written as:

$$F(X, Y) = \sum_{i+j=t\ell} f_{ij} X^i Y^j,$$

with $f_{ij} \in \mathbb{F}_{q^m}$. Since $F(aX, Y) = F(X, Y)$, we have:

$$\sum_{i+j=t\ell} f_{ij} X^i Y^j = \sum_{i+j=t\ell} f_{ij} a^i X^i Y^j.$$

Hence $f_{ij} = a^i f_{ij}, \forall i, j \in \mathbb{N}$ such as $i + j = t\ell$. As the order of a is ℓ, we have $a^i \neq 1, \forall i \in \mathbb{N}$ such as $\ell \nmid i$. Therefore $f_{ij} = 0, \forall i \in \mathbb{N}$ such as $\ell \nmid i$.We can write:

$$F(X, Y) = \sum_{\substack{i,j \\ il+j=t\ell}} f_{ij} X^{\ell i} Y^j.$$

So we have $\ell | j$ and:

$$F(X, Y) = \sum_{i+j=t} f_{ij} X^{\ell i} Y^{\ell j}.$$

Therefore $F(X, Y) = R(X^\ell, Y^\ell)$, with $R \in \mathbb{F}_{q^m}[X, Y]$ an homogeneous polynomial of degree t. □

The product $\prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)$ is also σ-invariant and, by the previous proposition, we have:

$$\prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y) = \big(\prod_{j=0}^{\ell-1} \delta_j\big) X^\ell + (-1)^\ell \big(\prod_{j=0}^{\ell-1} \gamma_j\big) Y^\ell.$$

Therefore:

$$f(X, Y) = \frac{R(X^\ell, Y^\ell)}{\Big(\big(\prod_{j=0}^{\ell-1} \delta_j\big) X^\ell - (-1)^{\ell-1} \big(\prod_{j=0}^{\ell-1} \gamma_j\big) Y^\ell\Big)^t}.$$

□

3.2.2 Case σ trigonalizable over $\mathbb{F}_{q^m}$ Here we consider the case where σ is trigonalizable in $\mathbb{F}_{q^m}$. As in the previous section we only have to treat the case where σ is upper triangular. So w.l.o.g one can assume that:

$$\begin{array}{rccc} \sigma: & \mathbb{P}^1 & \to & \mathbb{P}^1 \\ & (x:y) & \mapsto & (x+by:y) \end{array} \tag{6}$$

with $b \in \mathbb{F}_{q^m}^*$. In this case, we have $\ell = \mathrm{ord}(\sigma) = p$.

Proposition 5. *Let $\mathcal{C} := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ be a σ-invariant AG code as in theorem 2, with σ defined in (6). Let $\tilde{P}_i = (\alpha_i^p - b^{p-1}\alpha_i\beta_i^{p-1} : \beta_i^p)$ and $\tilde{G} = t(\tilde{Q})$, with $\tilde{Q} = \big(\prod_{j=0}^{p-1}\gamma_j : \prod_{j=0}^{p-1}\delta_j\big)$, then $\mathcal{C}^\sigma = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$, which is a GRS code.*

Proof. Let $c = (f(P_1), \ldots, f(P_n)) \in \mathcal{C}$ such that $\sigma(c) = c$. By Lemma 3, f is σ-invariant so: $f(X+bY, Y) = f(X, Y)$. By Lemma 5, we have:

$$\frac{F(X+bY,Y)}{\Big(\prod_{j=0}^{p-1}\big(\delta_j(X+bY)-\gamma_jY\big)\Big)^t} = \frac{F(X,Y)}{\Big(\prod_{j=0}^{p-1}\big(\delta_jX-\gamma_jY\big)\Big)^t}, \tag{7}$$

with $F \in \mathbb{F}_q[X,Y]$ an homogeneous polynomial of degree tp. Moreover the support of G is σ-invariant, so:

$$\prod_{j=0}^{p-1}(\delta_j(X+bY)-\gamma_jY) = \prod_{j=0}^{p-1}(\delta_jX-(\gamma_j-b\delta_j)Y) = \prod_{j=0}^{p-1}(\delta_jX-\gamma_jY).$$

Hence, (7) becomes $F(X+bY,Y)) = F(X,Y)$. If we write $z = \frac{X}{Y}$, then we have $F(z+b,1) = F(z,1)$.

Proposition 6. [5, Prop 4] *Let $F \in \mathbb{F}_q[z]$ be a polynomial of degree $deg(F) \leq tp$ and $b \in \mathbb{F}_q^*$. If $F(z+b) = F(z)$, then $F(z) = R(z^p - b^{p-1}z)$, with $R \in \mathbb{F}_q[z]$ a polynomial of degree $deg(R) \leq t$.*

The product $\prod_{j=0}^{p-1}(\delta_jz-\gamma_j)$ is also σ-invariant and, by previous proposition, we have:

$$\prod_{j=0}^{p-1}(\delta_jz-\gamma_j) = \big(\prod_{j=0}^{p-1}\delta_j\big)\big(z^p-b^{p-1}z\big) + (-1)^p\prod_{j=0}^{p-1}\gamma_j.$$

Hence:

$$f(X,Y) = \frac{R(X^p-b^{p-1}XY^{p-1},Y^p)}{\Big(\big(\prod_{j=0}^{p-1}\delta_j\big)\big(X^p-b^{p-1}XY^{p-1}\big)-\big((-1)^{p-1}\prod_{j=0}^{p-1}\gamma_j\big)Y^p\Big)^t}.$$

□

3.2.3 Case σ diagonalizable in $\mathbb{F}_{q^{2m}}\backslash\mathbb{F}_{q^m}$ We suppose that $\sigma = \rho\circ\sigma_d\circ\rho^{-1}$ with σ_d diagonal in $\mathrm{GL}_2(\mathbb{F}_q^{2m})$ and ρ is an automorphism of $\mathbb{P}^1_{\mathbb{F}_{q^{2m}}}$. We want to extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. So we consider the set $\mathrm{Span}_{\mathbb{F}_{q^{2m}}} < \mathcal{C} >$, ie: $\mathcal{C}\otimes\mathbb{F}_{q^{2m}}$.

$$\begin{tikzcd} \mathcal{C}\otimes\mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) | f \in \mathcal{L}_{\mathbb{F}_{q^{2m}}}(G)\} \arrow[r, "\mathrm{Inv}_{\tilde{\sigma}}"] & \mathrm{Inv}_{\tilde{\sigma}}(\mathcal{C}\otimes\mathbb{F}_{q^{2m}}) \\ \mathcal{C} = \{\mathrm{Ev}_{\mathcal{P}}(f) | f \in \mathcal{L}_{\mathbb{F}_{q^m}}(G)\} \arrow[u, hook, "\text{Subfield Subcode}"] \arrow[r, "\mathrm{Inv}_{\tilde{\sigma}}"] & \mathrm{Inv}_{\tilde{\sigma}_d}(\mathcal{C}) \arrow[u, hook, "\text{Subfield Subcode}"'] \end{tikzcd}$$

By the previous section, the code $\mathrm{Inv}_{\tilde{\sigma}}(\mathcal{C}\otimes\mathbb{F}_{q^{2m}})$ is a GRS code.

Moreover the order ℓ of $\sigma_d := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is the order of $a \in \mathbb{F}_{q^{2m}}$, so $\ell \mid (q^{2m}-1)$. Since $q := p^s$, where $s \in \mathbb{N}^*$, we have $\ell \mid (p^{s2m}-1)$ and so $p \nmid \ell$. By Lemma 2, we have $\mathrm{Fold}_{\tilde{\sigma}} = \mathrm{Inv}_{\tilde{\sigma}}$. Since the application Fold_σ is $\mathbb{F}_q$-linear and $\mathcal{C}\otimes\mathbb{F}_{q^{2m}}$ has, by definition, a basis in $\mathbb{F}_{q^m}^n$, the code $\mathrm{Inv}_{\tilde{\sigma}}(\mathcal{C}\otimes\mathbb{F}_{q^{2m}})$ also has a basis in $\mathbb{F}_{q^m}^n$. Therefore, the subcode on $\mathbb{F}_{q^m}$ of the GRS code $\mathrm{Inv}_{\tilde{\sigma}}(\mathcal{C}\otimes\mathbb{F}_{q^{2m}})$ is a GRS code.

4 Conclusion

To summarise we showed that the key security of compact McEliece scheme based on alternant codes with some induced permutation is not better than the key security of the short code obtained from the invariant operation. This result was showed for permutation induced by the affine group and we extend it to the projective linear group. Another kind of quasi-cyclic alternant codes could be obtained from the action of the semilinear projective group on the support. By semilinear projective group, we mean transformation of the form: $x \mapsto \frac{ax^{q^i}+b}{cx^{q^i}+d}$, with $a, b, c, d \in \mathbb{F}_{q^m}^n$. These transformations induce a permutation on the alternant code $\mathcal{C} \cap \mathbb{F}_q^n$ but not on the GRS code $\mathcal{C}$. So we cannot use the same property of the invariant of a GRS code to study this kind of quasi-cyclic alternant code.

Moreover, key-recovery is generally more expensive than message recovery. With a good choice of parameters it might be possible to construct quasi-cyclic codes with high complexity of key recovery attack on the invariant code.

Acknowledgements This work is partially supported by a DGA-MRIS scholarship, by French ANR-15-CE39-0013-01 "Manta" and by European grant CORDIS ICT-645622 "PQCrypto". We would like to thank J.P. Tillich and J. Lavauzelle for helpful discussions, and A. Couvreur for many valuable comments on the preliminary versions of this paper.

References

1. Thierry P. Berger, *Goppa and related codes invariant under a prescribed permutation*, IEEE Trans. Inform. Theory **46** (2000), no. 7, 2628–2633.
2. _____, *On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes and extended Goppa codes*, Finite Fields Appl. **6** (2000), no. 3, 255–281.
3. Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani, *Reducing key length of the McEliece cryptosystem*, International Conference on Cryptology in Africa, Springer, 2009, pp. 77–97.
4. Arne Dür, *The automorphism groups of Reed-Solomon codes*, J. Combin. Theory Ser. A **44** (1987), 69–82.
5. Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, Frédéric de Portzamparc, and Jean-Pierre Tillich, *Folding alternant and Goppa codes with non-trivial automorphism groups*, IEEE Trans. Inform. Theory **62** (2016), no. 1, 184–198.
6. _____, *Structural cryptanalysis of McEliece schemes with compact keys*, Des. Codes Cryptogr. **79** (2016), no. 1, 87–112.
7. Jean-Charles Faugere, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich, *Algebraic cryptanalysis of McEliece variants with compact keys*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2010, pp. 279–298.
8. William Fulton and Richard Weiss, *Algebraic curves: an introduction to algebraic geometry*, vol. 3, Addison-Wesley Redwood City California, 1989.
9. Philippe Gaborit, *Shorter keys for code based cryptography*, Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005), 2005, pp. 81–91.
10. V. D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290.
11. Venkatesan Guruswami, *Linear-algebraic list decoding of folded Reed-Solomon codes*, Computational Complexity (CCC), 2011 IEEE 26th Annual Conference on, IEEE, 2011, pp. 77–85.
12. Pierre Loidreau, *Codes derived from binary Goppa codes*, Probl. Inf. Transm. **37** (2001), no. 2, 91–99.
13. Florence J. MacWilliams and Neil J. A. Sloane, *The theory of error-correcting codes*, fifth ed., North–Holland, Amsterdam, 1986.
14. Robert J. McEliece, *A public-key system based on algebraic coding theory*, pp. 114–116, Jet Propulsion Lab, 1978, DSN Progress Report 44.
15. Rafael Misoczki and Paulo SLM Barreto, *Compact McEliece keys from Goppa codes*, International Workshop on Selected Areas in Cryptography, Springer, 2009, pp. 376–392.
16. Henning Stichtenoth, *On automorphisms of geometric Goppa codes*, Journal of Algebra **130** (1990), no. 1, 113–121.
17. _____, *Algebraic function fields and codes*, Universitext, Springer, 1993.