

Structural attack on quasi-cyclic SSAG-code-based McEliece cryptosystems

Mathieu Lhotel

Université de Bourgogne Franche-Comté

February 14, 2022

ABSTRACT. *In this paper, we present a structural attack on quasi-cyclic SSAG-code-based McEliece cryptosystems, by showing that the knowledge of the invariant code allow us to recover the secret data. In particular, this shows that the security of such systems must rely on the security of the invariant code. We then propose a scheme based on Hermitian codes, from witch we study the security by analysing a brute force attack on the invariant code.*

***** OLD ABSTRACT *****

way to recover the defining equation of an algebraic curve \mathcal{Y} defined over a finite field, by using a coding theoretic approach. In particular, from the knowledge of the invariant code of a structured algebraic geometry code defined on \mathcal{Y} , we manage to recover enough points to recover the equation of the curve. We also give the link with McEliece cryptosystem using algebraic-geometry codes, as we prove that the security level of those cryptosystems reduces to the security of the underlying invariant code, which is easier to brute force.

1 Introduction (À RÉÉCRIRE)

In the area of post-quantum cryptography, public key cryptosystem using linear codes looks promising. The first such system was introduced by McEliece in 1978 [McE78] using binary classical Goppa codes. The main problem if this scheme is that the size of the public key (that is generating matrices of codes) is too large for certain practical use cases. Many propositions were made in order to correct this, mostly by considering codes with additional structure, e.g. quasi-cyclic codes. Moreover, replacing classical Goppa codes (defined over the projective line) by their natural generalization, AG-codes on curves, can also help in providing more flexibility.

However, recent works from Couvreur, Marquez-Corbella and Pellikaan [CMCP14] broke McEliece cryptosystems based on raw AG-codes on arbitrary genus curves. So, in the same way that classical Goppa codes can be seen as subfield subcodes of GRS codes, this leads to more specifically consider subfield subcodes of AG-codes (SSAG in short), for which there are only few propositions to date.

The present work describes an structural attack on McEliece's like scheme based on structured SSAG-codes. In fact, we show that the security of those system can be reduced to the security of the so-called invariant code, which can be constructed from the public key. Depending on the assumption of the scheme, this subcode, which was first introduced by [Loi01], leaks too much informations about the public codes which can be recovered from it. As a consequence, the parameters of the underlying scheme must be chosen carefully in order to keep a good security level.

As a contremesure to this attack, we also propose a scheme based on SSAG-codes from the Hermitian curve, and provide a set of parameters to secure the corresponding invariant code.

In Section 2, we will give some classical notations and definitions that will be useful later on, both in algebraic and coding theory. Section 3 will be devoted to the invariant code. In section 4, we describe our attack. Section 5 gives some simple applications, such as Kummer or Artin-Schreier covering. Section 6 will discuss the generalisation of the method to any covering with solvable Galois groups. Finally, we will propose in section 7 a scheme using QC-SSAG codes on the Hermitian curve which resists our attack, and describes known attacks against the invariant code and counter-measures.

***** OLD INTRO

In the study of algebraic function fields over finite fields, we will mainly be interested in the problem :

Suppose that L/K is a finite, algebraic extension of function fields over the finite field \mathbb{F}_{q^m} , with $q = p^s$. What kind of informations do we need to recover the defining equation of L , that is the minimal polynomial of an element $y \in L$ such that $L = K(y)$?

As another formulation, in a cover of smooth projective curves $\mathcal{Y} \rightarrow \mathcal{X}$, one can wonder how to recover the defining equation of \mathcal{Y} . In order to study this problem, we will consider the so-called algebraic-geometry codes. In 1978, McEliece (see [McE78]) introduced a cryptosystem based on coding theory, that turns out to be a good candidate for post-quantum cryptography. It has been shown that the main issue of this cryptosystem is that it involves large key sizes, which is the reason why a lot of work has been made in order to reduce it, while keeping a good security level. A good idea to overpass this problem is to consider structured AG-codes, that is codes with non trivial permutation group (see for example the case of quasi-cyclic codes in [Bar18], Chapter 5).

In this paper, we will see how to recover the equation of a curve (or equivalently, the defining equation of an algebraic function field) by using codes defined on the curve. To keep it in an algebraic point of view, we will see that "structured codes on a curve" corresponds to "orbits of places of an algebraic function field under the action of an automorphism of the corresponding curve".

In Section 2, we will give some classical notations and definitions that will be useful later on. Section 3 will be devoted to the method itself. Section 4 gives some simple applications, such as Kummer or Artin-Schreier covering. Section 5 will discuss the generalisation of the method to any covering with solvable Galois groups. Finally, we will propose in section 6 using QC-SSAG code on the Hermitian curve which resists our attack.

2 Notations and properties

2.1 Algebraic function fields

Let \mathbb{F}_{q^m} be the finite field with q^m elements, where $q = p^s$ is a power of a prime p and $m \geq 1$. A function field of one variable over \mathbb{F}_{q^m} is a field K such that there exists an element $x \in K$ such that $K/\mathbb{F}_{q^m}(x)$ is an algebraic and separable extension.

In our context, an algebraic function field K over \mathbb{F}_{q^m} will always be the function field of an algebraic curve \mathcal{X} defined over \mathbb{F}_{q^m} , that is, with classical notations, $K = \mathbb{F}_{q^m}(\mathcal{X})$.

We will denote by \mathbb{P}_K the set of places of K , and any place $P \in \mathbb{P}_K$ comes with its valuation ring O_P and its discrete valuation $\nu_P : K \rightarrow \mathbb{Z}$. The degree of the place P , denoted $\deg(P)$ is defined as the finite integer $\deg(P) := [O_P/P : \mathbb{F}_q] < \infty$. The divisor group of K , denoted $Div(K)$, is the set of formal sums

$$A = \sum_{P \in \text{Supp}(A)} \nu_P(A) \cdot P,$$

where $\text{Supp}(A)$ is a finite subset of \mathbb{P}_K , called the support of A , made of places such that $\nu_P(A) \neq 0$.

A place $P \in \text{Supp}(A)$ is called a zero of A if $\nu_P(A) > 0$ (resp. a pole of A if $\nu_P(A) < 0$). For a function $z \in K$, we denote by $(z)^K$, $(z)_0^K$ and $(z)_\infty^K$ its principal divisor, divisor of zeroes and divisor of poles respectively, that is $(z)^K = (z)_0^K + (z)_\infty^K$, where

$$(z)_0^K = \sum_{\nu_P(A) > 0} \nu_P(A) \cdot P \quad \text{and} \quad (z)_\infty^K = \sum_{\nu_P(A) < 0} \nu_P(A) \cdot P.$$

The degree of a divisor is naturally defined by the formula

$$\deg(A) = \sum_{P \in \text{Supp}(A)} \nu_P(A) \cdot \deg(P).$$

We will denote $Princ(K)$ the subgroup of $Div(K)$ made of principal divisors and $Div^0(K)$ the subgroup of degree zero divisors. Then the divisor class group of K is defined by $Cl(K) := Div(K)/Princ(K)$ and the group of divisor classes of degree zero by $Cl^0(K) := Div^0(K)/Princ(K)$.

Proposition 1. (see [Sti09], Proposition 5.1.3). *Let $h(K) := \#Cl^0(K)$ and $r \geq 1$. The number of divisor classes in $Cl(K)$ of degree r do not depend on r , and is equal to $h(K)$, called the number of divisor classes in K .*

We also make use of the following result, that gives an estimation of the class number using the genus of the function field.

Theorem 1. (see [?], Proposition 3.1.23). *Let K be an algebraic function field over \mathbb{F}_{q^m} with genus $g(K)$. Then the number of divisor classes $h(K)$ satisfies*

$$(\sqrt{q^m} - 1)^{2g(K)} \leq h(K) \leq (\sqrt{q^m} + 1)^{2g(K)}.$$

Given a divisor $A \in Div(K)$, its Riemann-Roch space is defined as the \mathbb{F}_q -vector space

$$\mathcal{L}(A) = \{z \in K \mid (z)^L \geq -A\} \cup \{0\},$$

and $l(A) := \dim_{\mathbb{F}_q}(\mathcal{L}(A))$ as its dimension.

Given a tower $\mathbb{F}_{q^m}(x) \subseteq K \subseteq L$ of function fields over \mathbb{F}_{q^m} , let us consider a place $Q \in \mathbb{P}_K$ and one of its extensions $P \in \mathbb{P}_L$, denoted $P \mid Q$. The ramification index will as usual be denoted $e(P \mid Q)$.

If $L := \mathbb{F}_{q^m}(\mathcal{Y})$ and $K := \mathbb{F}_{q^m}(\mathcal{X})$ are the function fields of two curves and if $\pi : \mathcal{Y} \rightarrow \mathcal{X}$ is the corresponding separable morphism, we will consider the pullback of $Q \in \mathbb{P}_K$ as the divisor

$$\pi^*Q = \sum_{P \mid Q} e(P \mid Q) \cdot P \in Div(L).$$

We will make great use of the following lemma, which shows that pullbacks preserve the notion of principal divisors :

Lemma 1. *Let $z \in L$ be a function. Then*

$$(z)^L = \pi^*(z)^K, \quad (z)_0^L = \pi^*(z)_0^K \text{ and } (z)_\infty^L = \pi^*(z)_\infty^K.$$

Proof. see [Sti09], proposition 3.1.9. □

2.2 Coding theory

As explained in the introduction, we will be dealing with SSAG-code, that is our AG-codes are defined over an extension \mathbb{F}_{q^m} of \mathbb{F}_q .

As before, let \mathbb{F}_q be a finite field with $q = p^s$ elements, and let $m \geq 1$ be an integer. Let us recall the definition of an AG code.

Definition 1. *Let \mathcal{X} be a smooth projective curve over \mathbb{F}_{q^m} with function field $L = \mathbb{F}_{q^m}(\mathcal{X})$, $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of n distinct places of degree 1 in L and $G \in \text{Div}(L)$ be a divisor such that $\text{Supp}(G) \cap \mathcal{P} = \emptyset$. Let us also suppose that $\deg(G) < n$. Then we define the AG-code associated to the triple $(\mathcal{X}, \mathcal{P}, G)$ as the \mathbb{F}_{q^m} -vector space*

$$\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \mid f \in L(G)\} \subseteq \mathbb{F}_{q^m}^n.$$

Definition 2. *With notation as above, we define the subfield subcode of $C_L(\mathcal{X}, \mathcal{P}, G)$ over \mathbb{F}_q , denoted $SSAG_q(\mathcal{X}, \mathcal{P}, G)$, as follows*

$$SSAG_q(\mathcal{X}, \mathcal{P}, G) = C_L(\mathcal{X}, \mathcal{P}, G) \cap \mathbb{F}_q^n.$$

In particular, we will be interested in "structured" codes, that is codes with non trivial permutation group. To be concrete, consider an automorphism subgroup $\Sigma \subseteq \text{Aut}(L)$, and denote by $\text{Orb}_\Sigma(P)$ the orbit of a place $P \in L$ under the action of this subgroup. Then if $\Sigma(\mathcal{P}) = \mathcal{P}$ and $\Sigma(G) = G$, then Σ induces a permutation $\tilde{\Sigma}$ on the code $C_L(\mathcal{X}, \mathcal{P}, G)$. In order to do this, the support \mathcal{P} and the divisor G have to be chosen carefully, that is they are made of distinct unions of orbits under the action of Σ . With this satisfied, it is clear that \mathcal{P} and G are Σ -invariant since by definition, each orbit of places in L is invariant. As a subfield subcode, the permutation $\tilde{\Sigma}$ also acts on the code $SSAG_q(\mathcal{X}, \mathcal{P}, G)$ over \mathbb{F}_q .

Example 1. If $\Sigma = \langle \sigma \rangle$ is cyclic of order ℓ generated by $\sigma \in \text{Aut}(L)$ and if \mathcal{P} and G are σ -invariant, the code $C_L(\mathcal{X}, \mathcal{P}, G)$ is said to be ℓ -quasi-cyclic. Notice that in this case, the code $SSAG_q(\mathcal{X}, \mathcal{P}, G)$ is also ℓ -quasi-cyclic.

Let us also recall the definition of the dual of a linear code as well as an easy lemma :

Definition 3. *Let \mathcal{C} be a $[n, k]$ -linear code over a finite field \mathbb{F}_q . Its dual code is defined by*

$$\mathcal{C}^\perp := \{y \in \mathbb{F}_q^n \mid xy^T = 0, \forall x \in \mathcal{C}\}.$$

It is easy to see that any generator matrix of \mathcal{C}^\perp is a parity check matrix of \mathcal{C} . In particular, $\mathcal{C}^{\text{perp}}$ is a $[n, n - k]$ -code over \mathbb{F}_q .

Finally, we will also need a result using duality of AG-codes.

Proposition 2. *Let $C_L(\mathcal{X}, \mathcal{P}, G)$ be an AG-code defined on a curve \mathcal{X} . Then there exists a divisor $G' \in \text{Div}(\mathcal{X})$ such that*

$$C_L(\mathcal{X}, \mathcal{P}, G)^\perp = C_L(\mathcal{X}, \mathcal{P}, G').$$

Proof. See [Sti09], proposition 2.2.10 □

3 Invariant code

Definition 4. Given an AG-code $(C) = C_L(\mathcal{X}, \mathcal{P}, G)$ that is invariant under the action of an automorphism group $\Sigma \subseteq \text{Aut}(L)$, we define its invariant code as the subcode

$$\mathcal{C}^\Sigma := \{c \in \mathcal{C} \mid \tilde{\Sigma}(c) = c\},$$

where $\tilde{\Sigma}$ is the permutation induced by Σ on the code.

In what follow, we will study the structure of the invariant code, which will be our main tools in the next parts. In particular, we will show that this subcode is nothing but an AG-code itself, defined on the quotient curve \mathcal{X}/Σ . Notice that in our context, the function field of the quotient curve is precisely the fixed field L^Σ of L . Let us start with the following lemma.

Lemma 2. Let \mathcal{P} and G be as in definition 1, and suppose that they are invariant under an automorphism $\sigma \in \text{Aut}(L)$. If $c = \text{Ev}_{\mathcal{P}}(g) \in C_L(\mathcal{X}, \mathcal{P}, G)$ is such that $\sigma(c) = c$, then g is σ -invariant, ie. $g \circ \sigma = g$.

Proof. Let us write $\mathcal{P} = \{P_1, \dots, P_n\}$, and let $c = (g(P_1), \dots, g(P_n))$ be such that $\sigma(c) = c$. Then we have

$$\begin{aligned} \forall i \in \{1, \dots, n\}, \quad g(P_{\sigma(i)}) = g(P_i) &\iff \forall i \in \{1, \dots, n\}, \quad (g \circ \sigma)(P_i) = g(P_i) \\ &\iff \forall i \in \{1, \dots, n\}, \quad (g \circ \sigma - g)(P_i) = 0. \end{aligned}$$

Since G is σ invariant, we have $g \circ \sigma \in L(G)$, and thus $g \circ \sigma - g \in L(G)$. This implies that the function $(g \circ \sigma - g)$ has at most $\deg(G) < n$ zeroes in L . Since the last equivalence above gives n zeroes to the same function, one have $(g \circ \sigma - g) \equiv 0$. The result follows. \square

Proposition 3. Let $G \in \text{Div}(L)$ be a divisor of L invariant by an automorphism $\sigma \in \text{Aut}(F)$. Then $L(G)^\sigma = L(\tilde{G})$ with $\tilde{G} \in \text{Div}(F^\sigma)$.

Proof. As G is supposed to be σ invariant, there exist $s \in \mathbb{N}^*$ and places $Q_1, \dots, Q_s \in \mathbb{P}_L$ such that

$$\text{Supp}(G) = \bigsqcup_{i=1}^s \text{Orb}_\sigma(Q_i),$$

that is

$$G = \sum_{i=1}^s t_i \sum_{Q \in \text{Orb}_\sigma(Q_i)} R,$$

for some $t_i \in \mathbb{Z}$. Now let $g \in L(G) \in L$ be such that $g \circ \sigma = g$ (ie. $g \in L(G)^\sigma \subseteq L^\sigma$).

For each $i \in \{1, \dots, s\}$, consider a place $Q'_i \in \mathbb{P}_{F^\sigma}$ be such that $Q_i \mid Q'_i$. It is well known that for every $Q \in \text{Orb}_\sigma(Q_i)$, one also have $Q \mid Q'_i$ and $e(Q|Q'_i) = e(Q_i|Q'_i)$. Since $g \in L(G)$, we know that

$$(g)_L \geq - \sum_{i=1}^s t_i \sum_{Q \in \text{Orb}_\sigma(Q_i)} Q$$

Note that for every $i \in \{1, \dots, s\}$, we have $e(Q_i|Q'_i)\nu_{Q'_i}(g) = \nu_{Q_i}(g)$, so we have

$$(g)_{L^\sigma} \geq - \sum_{i=1}^s \frac{t_i}{e(Q_i|Q'_i)} Q'_i.$$

Let us define $\tilde{G} := \sum_{i=1}^s \left\lfloor \frac{t_i}{e(Q_i|Q'_i)} \right\rfloor Q'_i \in \text{Div}(L^\sigma)$. Then we have $g \in L(\tilde{G}) \subseteq L^\sigma$. Hence $L(G)^\sigma \subseteq L(\tilde{G})$.

Conversly, let $g \in L^\sigma$ such that $g \in L(\tilde{G})$, with \tilde{G} defined as above. Then we have

$$(g)_L \geq - \sum_{i=1}^s e(Q_i|Q'_i) \cdot \left\lfloor \frac{t_i}{e(Q_i|Q'_i)} \right\rfloor \sum_{Q \in \text{Orb}_\sigma(Q_i)} Q \geq -G,$$

that is $g \in L(G) \cap L^\sigma = L(G)^\sigma$. \square

Theorem 2 (Structure of the invariant code). *Let $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$ be an AG-code defined on a curve \mathcal{X} with function field L , invariant under the action of an automorphism group $\Sigma \subseteq \text{Aut}(\mathcal{X})$. Then its invariant code is also an AG-code, defined on the quotient curve \mathcal{X}/Σ . In particular, there exist a support $\tilde{\mathcal{P}}$ on the quotient curve, as well as a divisor \tilde{G} such that*

$$\mathcal{C}^\Sigma = C_L(\mathcal{X}/\Sigma, \tilde{\mathcal{P}}, \tilde{G}).$$

Proof. This is a straightforward consequence of lemma 2 and Proposition 3. □

Remark 1. The above theorem can be precised a bit, since we can explicit $\tilde{\mathcal{P}}$ and \tilde{G} . Indeed, the divisor \tilde{G} is nothing but the one introduced in Proposition 1, while $\tilde{\mathcal{P}} := \{P' \in \mathbb{P}_{L^\sigma} ; P \mid P'\}$. In particular, they can be described by using the ramification in the cover $\mathcal{X} \rightarrow \mathcal{X}/\Sigma$.

Remark 2. Let \mathcal{C} be an AG-code on \mathcal{X} stable under $\Sigma \subseteq \text{Aut}(\mathcal{X})$, then

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

that is invariant and subfield subcode operations commute.

Corollary 1. *With the notations of Theorem 1, let $\text{SSAG}_q(\mathcal{X}, \mathcal{P}, G)$ be a subfield subcode of an AG-code and Σ acting on it. Then*

$$\text{SSAG}_q(\mathcal{X}, \mathcal{P}, G)^\Sigma = \text{SSAG}_q(\mathcal{X}/\Sigma, \tilde{\mathcal{P}}, \tilde{G}),$$

where $\tilde{\mathcal{P}}$ and \tilde{G} are defined as in remark 1.

Proof. Immediate consequence of Theorem 2 and Remark 2. □

4 Recovering the equation of a covering

Throughout all this section, let $q = p^s$ be a power of a prime, $m \geq 1$, and \mathbb{F}_{q^m} be the finite field with q^m elements. Let us consider a separable morphism

$$\pi : \mathcal{Y} \rightarrow \mathcal{X}$$

between curves defined over \mathbb{F}_{q^m} . It corresponds to a tower of function fields $\mathbb{F}_{q^m}(x) \subseteq K \subseteq L$, where $K = \mathbb{F}_{q^m}(\mathcal{X})$ and $L = \mathbb{F}_{q^m}(\mathcal{Y}) = \mathbb{F}_{q^m}(x, y)$. Since L is a finite algebraic extension of K , there exists an element $y \in L$ such that

$$L = K(y), \text{ and } H(x, y) = 0, \text{ } H \in \mathbb{F}_{q^m}[X, Y] \text{ irreducible.}$$

The key part of our attack will be to recover a defining equation of the curve \mathcal{Y} , that is the minimal polynomial of y over K . To this end, let us introduce the following concept :

Definition 5. *For a divisor $G \in \text{Div}(L)$, let us denote by $\tilde{G} \in \text{Div}(K)$ the largest divisor (according to the degree) such that*

$$\pi^* \tilde{G} \leq G.$$

Note that \tilde{G} is unique and thus well-defined.

Remark 3. *If $A \in \text{Div}(K)$, we have*

$$\widetilde{\pi^* A} = A.$$

Now, let us introduce a few notations. Denote by $\ell = [L : K]$ the degree of the extension L/K . Suppose that we are given a set of r places of degree one in K , say $\tilde{\mathcal{P}} = \{Q_1, \dots, Q_r\}$, that totally split in L/K . For any $1 \leq i \leq r$, one then have

$$\pi^* Q_i = P_{i,1} + \dots + P_{i,\ell}, \quad P_{i,j} \in \mathbb{P}_L$$

Denote by $\mathcal{P} = \{P_{i,j} \mid 1 \leq i \leq r \text{ and } 1 \leq j \leq \ell\}$ the set of all extensions of the Q_i 's in L . Let $G \in \text{Div}(L)$ be a divisor of degree d smaller than $n = \ell r$ such that $\text{Supp}(G) \cap \mathcal{P} = \emptyset$. Also, we denote by $\tilde{G} \in \text{Div}(K)$ its related divisor according to definition 5. Note that this implies that $\text{Supp}(\tilde{G}) \cap \tilde{\mathcal{P}} = \emptyset$ as well.

Remark 4. The situation above can also be described in the following way : consider a curve \mathcal{Y} with function field L , together with a subgroup $\Sigma \subseteq \text{Aut}(\mathcal{Y})$. We then get a cover $\mathcal{Y} \rightarrow \mathcal{Y}/\Sigma$, that is the function field $K = \mathbb{F}_{q^m}(\mathcal{Y}/\Sigma) = L^\Sigma$. If G is made of orbits under the action of Σ , then \mathcal{P} and G gives rise to an AG-code $C_L(\mathcal{Y}, \mathcal{P}, G)$ that is invariant under the action of Σ , and thus its invariant code is given by $C_L(\mathcal{Y}/\Sigma, \tilde{\mathcal{P}}, \tilde{G})$. As explained in the introduction, we will later be dealing with the subfield subcode version of those codes.

Before describing the procedure to recover the equation of \mathcal{Y} , let us put together our assumptions :

1. We know a parity check matrix H of the SSAG-code

$$\mathcal{C} = \text{SSAG}_q(\mathcal{Y}, \mathcal{P}, G);$$

2. We know a plane model of the quotient curve \mathcal{X} (ie. the defining equation of the function field K), the set of places $\tilde{\mathcal{P}}$ and the divisor $\tilde{G} \in \text{Div}(K)$ (that is exactly the invariant code);
3. We know how the morphism $\pi : \mathcal{Y} \rightarrow \mathcal{X}$ acts on the set of places \mathcal{P} , that is for every $P \in \mathcal{P}$, we know the corresponding place $Q \in \tilde{\mathcal{P}}$ such that $P \mid Q$ (ie. $Q = \pi(P)$);
4. We have "enough informations" on the pole divisor of y in K , where $y \in L$ is such that $L = K(y)$. This assumption will be discussed later, since the key point of the attack will be to control the divisor

$$\widetilde{(y)_\infty^L} \in \text{Div}(K).$$

In fact, we will need to understand its support in K , and how he ramifies in L/K .

Let us now explain what we plan to do. The main idea is to recover first the support \mathcal{P} , that are points on the curve \mathcal{Y} , in order to be able to recover its defining equation using interpolation. Thanks to hypothesis 2., we know the coordinates of the rational points corresponding to Q_i 's in the plane model of the curve \mathcal{X} . In fact, let us denote by α a primitive element of K over $\mathbb{F}_{q^m}(x)$, that is $K = \mathbb{F}_{q^m}(x, \alpha)$ (possible since $K/\mathbb{F}_{q^m}(x)$ is separable and algebraic). Then one can denote by $(x(Q_i) : \alpha(Q_i) : 1)$ the coordinate of the rational point in $\mathcal{X}(\mathbb{F}_{q^m})$ corresponding to the place $Q_i \in \tilde{\mathcal{P}}$.

As the curve \mathcal{Y} covers the plane model of \mathcal{X} , it admits a model in $\mathbb{P}^3(\mathbb{F}_{q^m})$; that is any $P \in \mathcal{P}$ corresponds to a point with coordinates $(x(P) : \alpha(P) : y(P) : 1) \in \mathbb{P}^3(\mathbb{F}_{q^m})$. Since places in \mathcal{P} are extensions of places in $\tilde{\mathcal{P}}$, they corresponds to points that have the same x and α coordinates, and equals to those of their restrictions in K . In other words, for all $1 \leq i \leq r$ and $1 \leq j \leq \ell$, the place $P_{i,j} \in \mathcal{P}$ corresponds to the point

$$(x(Q_i) : \alpha(Q_i) : y(P_{i,j}) : 1) \in \mathcal{Y}(\mathbb{F}_{q^m}).$$

As a result, from hypothesis 2, one only need to recover the y -evaluation of points in \mathcal{P} in order to conclude. So the key part will be to recover the row vector

$$\mathbf{y} = (y_{i,j})_{i,j}. \tag{1}$$

where $y_{i,j} := y(P_{i,j})$, for every $1 \leq i \leq r$ and $1 \leq j \leq \ell$.

In order to recover the vector \mathbf{y} , we will construst a system of linear equations of which it is a solution. For that, recall that by definition, the parity check matrix of the code $\mathcal{C} = \text{SSAG}_q(\mathcal{Y}, \mathcal{P}, G)$ satisfies

$$c \in \mathcal{C} \iff H \cdot c^T = 0. \tag{2}$$

Moreover, we know that a codeword $c \in \mathcal{C}$ comes from evaluation at $P_{i,j} \in \mathcal{P}$ of functions in the Riemann-Roch space of G , that is.

$$c = (f(P_{i,j})) , f \in L(G).$$

Of course, $L(G)$ is unknown since the divisor G is as well. But we actually don't need the whole $L(G)$ to recover \mathbf{y} . In fact, we are searching for a subspace $\mathcal{L} \subseteq L(G)$, big enough (we will explain it later), and made of functions that specifically have the form $g \cdot y$, where $g \in K$ and y is such that $L = K(y)$. In fact, if we found such a space, one have

$$\{c = (g(P_{i,j}) \cdot y(P_{i,j})) , 1 \leq i \leq r , 1 \leq j \leq \ell \text{ and } f \cdot y \in \mathcal{L}\} \subseteq \mathcal{C}.$$

In particular, since $g \in K$, the $g(P_{i,j})$ are known (recall the discussion above), and thus the right-hand side of (2) will gives us a system where everything is known but the $y(P_{i,j})$, that is exactly what we want.

Let us now explain how to get a space of functions $\mathcal{L} \subseteq L(G)$ as above. In particular, since we know the quotient curve (that is we know its function field K) as well as the morphism of curve $\pi : \mathcal{Y} \rightarrow \mathcal{X}$, we will construct \mathcal{L} as a pull-back of function in K . To be concrete, we are searching for a space of functions $\mathcal{F} \subseteq K$, as big as possible, such that the following holds :

$$\pi^* \mathcal{F} \cdot y \in L(G). \quad (3)$$

The following lemma gives us a good choice for the space \mathcal{F} , that will actually turn out to be the best one.

Lemma 3. *The space of functions $\mathcal{F} \subseteq K$, given by*

$$\mathcal{F} := L\left(\tilde{G} - \widetilde{(y)_\infty^L}\right) \subseteq L(\tilde{G})$$

satisfies condition (3) above.

Proof. The inclusion $\mathcal{F} \subseteq L(\tilde{G})$ easy follows from the fact that $\widetilde{(y)_\infty^L}$ is a positive divisor, and thus $\tilde{G} - \widetilde{(y)_\infty^L} \leq \tilde{G}$. Let us show that (3) holds. Let $f \in \mathcal{F} = L\left(\tilde{G} - \widetilde{(y)_\infty^L}\right)$. By definition, one have

$$(f)^K \geq -\left(\tilde{G} - \widetilde{(y)_\infty^L}\right),$$

and then

$$(\pi^* f)^L \geq -\pi^* \left(\tilde{G} - \widetilde{(y)_\infty^L}\right) = (y)_\infty^L - G , \quad \text{using remark 3.}$$

Now, one gets

$$(\pi^* f \cdot y)^L = (\pi^* f)^L + (y)^L \geq ((y)_\infty^L - G) + (y)^L = (y)_0^L - G \geq -G,$$

since $(y)_0^L$ is an effective divisor. In particular, we just proved that $\pi^* f \cdot y \in L(G)$ for every $f \in \mathcal{F}$, that is (3) holds. \square

Remark 5. As we are searching for a space \mathcal{F} as big as possible, we can see in the above proof that we made the best choice possible. In fact, since we want functions with specific form $g \cdot y$ where g doesn't depend on the variable y , one need to compensate this fact by "deleting" the term $-(y)_\infty^L$, which is the smallest as possible, that is we loose the least information as possible in order to have our condition satisfied.

Note that the space \mathcal{F} in lemma 3 can be explicitly determined in our situation, since it is a subspace of K which is supposed to be known (see hypothesis 2. and 4. above). In particular, the divisor

$$D := \tilde{G} - \widetilde{(y)_\infty^L} \in \text{Div}(K) \quad (4)$$

is known from now on. In particular, one can find a basis of its Riemann-Roch space, that is there exists functions $f_1, \dots, f_s \in K$ (where $s = l(D)$) such that

$$\mathcal{F} := L(D) = \langle f_1, \dots, f_s \rangle_{\mathbb{F}_q^m}.$$

Now let us consider the row vectors, for every $1 \leq k \leq s$:

$$\mathbf{u}_k := (\pi^* f_k(P_{i,j}))_{i,j}, \text{ with } 1 \leq i \leq r, 1 \leq j \leq \ell.$$

At this point, we are able to compute the \mathbf{u}_k 's the following way :

1. We first compute the vectors $\mathbf{a}_k := (f_k(Q_i))_i$, $1 \leq i \leq r$. This is easily done since both the f_k 's and Q_i 's are known by this point;
2. Next we use hypothesis 3. to recover the \mathbf{u}_k 's : In fact, we know by construction that for any fixed $1 \leq i \leq r$, one have

$$f_k(Q_i) = \pi^* f_k(P_{i,j}), \quad 1 \leq j \leq \ell,$$

since the function $\pi^* f_k$ doesn't act on the y -coordinates, as they are pull-backs of function in K . Since we know the indices (in \mathcal{P}) corresponding to the extension in L of any $Q \in \tilde{\mathcal{P}}$, one can re-build the \mathbf{u}_k 's by duplicating the value of $f_k(Q_i)$ in the corresponding coordinates.

Now, using (2) and (3) above, one gets

$$\mathbf{u}_k \star \mathbf{y} \in \mathcal{C}, \text{ for every } 1 \leq k \leq s,$$

where \star is the componentwise product of row vectors and \mathbf{y} is the desired vector. If we denote by $\mathbf{D}_k = \text{Diag}(\mathbf{u}_k)$, equation (2) leads to the linear system

$$\begin{pmatrix} H \cdot \mathbf{D}_1 \\ \vdots \\ H \cdot \mathbf{D}_s \end{pmatrix} \cdot \mathbf{y}^T = 0, \quad (5)$$

from which \mathbf{y} is a particular solution. Then if we have enough equations, we can hope to recover \mathbf{y} by solving it. Let us now give some more informations about this system.

Let us denote by

$$A := \begin{pmatrix} H \cdot \mathbf{D}_1 \\ \vdots \\ H \cdot \mathbf{D}_s \end{pmatrix}$$

the above matrix. It is clear that the vector \mathbf{y} is in the kernel of A , but since it's the only solution we are searching for, it can be interesting to investigate other solutions. In order to have unicity of the solution, we would like to have as much equations as possible. Thus, let us study how the parameters impact the number of equations and thus the space of solutions.

If S denotes the number of equations in the linear system (5), one have

$$S = \#\text{Rows}(H) \times s,$$

where $s := \ell(D)$. By definition, the number of rows of H equals $n - \dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = \ell r - \dim_{\mathbb{F}_{q^m}}(\mathcal{C})$. Using the Riemann-Roch theorem twice gives

$$s = l(D) \leq \deg \left(\tilde{G} - (\tilde{\mathbf{y}}_\infty)^L \right) + 1 - g(K),$$

and

$$\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) \leq \deg(G) + 1 - g(L).$$

Since $\deg(\tilde{G}) = \lfloor \frac{\deg(G)}{\ell} \rfloor$, it is clear from the above estimation that the number S of equations depend on both genera of L and K , as well as the degree of the divisor G (if $n = \ell r$ is fixed). In particular, if $g(K)$ and $g(L)$ are too high, we will probably have less equations (keep in mind that $g(L) \geq g(K)$ and that $g(L)$ can be computed from $g(K)$ (see. Hurwitz' formula, [Sti09], theorem 3.4.13)).

Moreover, if the cover $\pi : \mathcal{Y} \rightarrow \mathcal{X}$ is fixed, as well as the cardinality of the set \mathcal{P} (that is n); there exist an integer d_{\max} such that the number of equations is maximal for $\deg(G) = d_{\max}$.

On the other side, in all our computing experiments, we noticed that theses parameters (ie. $\deg(G)$ and both genera in particular) doesn't impact the structure of the kernel of A . This is actually a good remark since those kinds of problems usually tend to be harder in big genera situations. It turns out that it was pretty much predictable since it is possible to describe all solutions of the system, as explained in the next proposition.

Proposition 4. *Let $h \in L$ be a function such that*

$$(h)_\infty^L \leq (y)_\infty^L$$

holds. Then the evaluation vector $\mathbf{h} := (h_{i,j})_{i,j}$, where $h_{i,j} := h(P_{i,j})$, for every $1 \leq i \leq r$ and $1 \leq j \leq \ell$ is also in the kernel of A .

Proof. Recall the notations of section 3.2, take $h \in L$ as above, and a function $g \in \mathcal{F}$. By definition of \mathcal{F} , one have

$$(\pi^*g)^L \geq -\pi^* \left(\tilde{G} - (\widetilde{y})_\infty^L \right) = (y)_\infty^L - G.$$

Thus we have

$$(\pi^*g \cdot h)^L = (\pi^*g)^L + (h)^L \geq ((y)_\infty^L - G) + (h)^L = (h)_0^L + \underbrace{((y)_\infty^L - (h)_\infty^L)}_{\geq 0} - G \geq -G,$$

that is $\pi^*\mathcal{F} \cdot h \in L(G)$. This complete the proof. □

The above proposition proves that the space of solutions doesn't depend on the number of equations. We will see in some examples later that we can explicitly decide whenever a function gives a solution or not, depending on the divisor $(y)_\infty^L$. This leads to a problem : how to choose the correct solution, that is the vector \mathbf{y} . We will see in the next section that depending on the cover, and especially on the action of the automorphism group Σ , we can had to the system (5) others equations, that are only satisfied by \mathbf{y} , allowing us to separate it from other solutions.

5 Applications

5.1 About the quotient curve

As we saw in section 4, our procedure allows us to recover the defining equation of a curve \mathcal{Y} , provided that we are given enough informations about one of its quotient curve \mathcal{X} . One can also see the situation as follow: Given a plane curve \mathcal{X} , can we recover the defining equation of one of its cover \mathcal{Y} ? The natural question is then which kind of curve \mathcal{X} can be taken as ?

The easiest case is then \mathcal{X} equals the projective line $\mathbb{P}^1(\mathbb{F}_{q^m})$. In fact, this curve has genus 0 and we know exactly its rational places. We will come back at it in section 5.2.

In what follows, we will see that we can take a general classe of curves as the quotient curve \mathcal{X} . In particular, from hypothesis 4. (see section 4) it is clear that we need to "control" the pole divisor of a prime element of L/K , that is we would like $(\widetilde{y})_\infty^L$ to be as simple as possible (in terms of the cardinality of its support). In order to satisfy this condition, the function field K of the curve \mathcal{X} has to be well-chosen. In fact, take an separating element $x \in K$, such that $K/\mathbb{F}_{q^m}(x)$ is separable and algebraic. Thus there exist $\alpha \in K$ such that $K = \mathbb{F}_{q^m}(x, \alpha)$. Let us define the classe of curve were \mathcal{X} will be taken :

Definition 6. *For a curve \mathcal{X} over \mathbb{F}_{q^m} , we say that it has separated variables if its function field $K = \mathbb{F}_{q^m}(x, \alpha)$ is given by*

$$F_1(\alpha) = F_2(x) \text{ , } F_1, F_2 \in \mathbb{F}_q[T].$$

In this case, one have $[K : \mathbb{F}_{q^m}(x)] = \deg(F_1)$.

The following lemma explain why these curves are interesting in our case :

Lemma 4. *Let \mathcal{X} be a curve with separated variables, with function field $K = \mathbb{F}_{q^m}(x, \alpha)$ given by the equation*

$$F_1(\alpha) = F_2(x),$$

where $F, G \in \mathbb{F}_{q^m}[T]$ are two univariate polynomials with co-prime degrees, and denote by $\pi : \mathcal{X} \rightarrow \mathbb{P}^1(\mathbb{F}_{q^m})$ the corresponding morphism of curves. Let us denote by R_∞ the pole of x in $\mathbb{F}_{q^m}(x)$. Then R_∞ is totally ramified in $K/\mathbb{F}_{q^m}(x)$, and its unique extension $Q_\infty \in K$ is the unique pôle of $\alpha \in K$. In particular, one have

$$(\alpha)_\infty^K = \deg(F_2) \cdot Q_\infty.$$

Proof. Let Q_∞ be an extension of R_∞ in K . One have obviously

$$e(Q_\infty | R_\infty) \leq \deg(F_1) = [K : \mathbb{F}_{q^m}(x)].$$

On the other side, from the defining equation of K ; one gets

$$F_1(\alpha) = F_2(x) \Rightarrow \deg(F_1) \cdot \nu_{Q_\infty}(\alpha) = e(Q_\infty | R_\infty) \cdot \deg(F_2) \cdot \underbrace{\nu_{R_\infty}(x)}_{=-1},$$

and since $(\deg(F_1), \deg(F_2)) = 1$, we get $\deg(F_1) \mid e(Q_\infty | R_\infty)$, that is R_∞ is fully ramified in $K/\mathbb{F}_{q^m}(x)$ and $e(Q_\infty | R_\infty) = \deg(F_1)$. Moreover, we have

$$\begin{aligned} \deg(F_1) \cdot (\alpha)_\infty^K &= \deg(F_2) \cdot \pi^*(x)_\infty^{\mathbb{F}_q(x)} \\ &= \deg(F_2) \cdot \pi^* R_\infty \\ &= \deg(F_2) \cdot e(Q_\infty | R_\infty) \cdot Q_\infty, \end{aligned}$$

which gives the result on the divisor of poles of α in K . \square

The main point in these kind of curves is that we keep track of the place at infinity in the corresponding extension of function field, that will later allows us to look at this point in the tower $\mathcal{Y} \rightarrow \mathcal{X} \rightarrow \mathbb{P}^1(\mathbb{F}_{q^m})$, giving us a good way to describe the divisor $\widetilde{(y)}_\infty^L \in \text{Div}(K)$.

5.2 Kummer covering

Let \mathcal{X} be a curve over \mathbb{F}_{q^m} with separated variables (see. definition 6), those function field is given by $K = \mathbb{F}_{q^m}(x, \alpha)$, with

$$F_1(\alpha) = F_2(x), \quad F_1, F_2 \in \mathbb{F}_{q^m}[T]$$

and $(\deg(F_1), \deg(F_2)) = 1$.

Our first example of cover is the so-called Kummer covering.

Let $\ell \mid q - 1$ be an integer (not necessarily a prime). Consider the extension $L = K(y)$, with

$$y^\ell = f, \quad f \in K$$

and denote by $m := \deg((f)_\infty^K)$ the degree of the pole divisor of the function f . Suppose also that $(m, \ell) = 1$. Then L/K is a Kummer extension, it is cyclic of order $\ell = [L : K]$ and

$$\text{Gal}(L/K) = \{\sigma : y \mapsto \xi \cdot y \mid \xi \in \mu_\ell^*(\mathbb{F}_q)\}.$$

Note that this kind of extension have been studied a lot, and that we know the ramification in such an extension (see for example [Sti09], proposition 3.7.3).

Let us explain the hypothesis before describing our attack in this context (this is a special case of those given in section 4.). Denote by $\mathcal{Y} \rightarrow \mathcal{X}$ the morphism of algebraic curves that corresponds to the extension of function fields L/K . We are given an *SSAG-code* \mathcal{C} on the curve \mathcal{Y} , that is stable under the action of the Galois group $\text{Gal}(L/K)$. In the Kummer case, this group is well-know : it is cyclic of order ℓ and the corresponding action is completely determined by the choice of an ℓ^{th} root of unity $\xi \in \mu_\ell^*(\mathbb{F}_{q^m})$. Our hypotheses are the following :

1. We know a parity check matrix H of the code $\mathcal{C} = SSAG_q(\mathcal{Y}, \mathcal{P}, G)$;
2. The quotient curve \mathcal{X} is known (that is polynomials F_1 and F_2), as well as the structure of the invariant code of \mathcal{C} , ie. $\tilde{\mathcal{P}}$ and \tilde{G} such that $\mathcal{C}^\sigma = SSAG_q(\mathcal{X}, \tilde{\mathcal{P}}, \tilde{G})$;
3. The automorphism $\sigma \in Gal(L/K)$ that acts on \mathcal{C} is unknown, that is we don't know the corresponding root of unity ξ .

According to section 3.2, we need to control the divisor $\widetilde{(y)_\infty^L}$. Let us start with the following lemma.

Lemma 5. *Keep notations as in lemma 3. Then in the above situation, the place Q_∞ (the unique pole of α) is fully ramified in L/K , and its unique extension $P_\infty \in L$ is the unique pole of y in L .*

Proof. Well-known from Kummer theory. □

Proposition 5. *We have*

$$(x)_\infty^L = \ell \cdot \deg(F_1) \cdot P_\infty,$$

$$(\alpha)_\infty^L = \ell \cdot \deg(F_2) \cdot P_\infty,$$

and

$$(y)_\infty^L = m \cdot P_\infty.$$

Proof. Let R_∞ be the simple pole of x in $\mathbb{F}_{q^m}(x)$. It is totally ramified in $K/\mathbb{F}_{q^m}(x)$ (see lemma 5), so $(x)^K = \deg(F_1) \cdot Q_\infty$. We also know the divisor of poles of α in K , so using lemma 1 yields

$$(x)_\infty^L = \pi^*(x)_\infty^K = \deg(F_1) \cdot \pi^* Q_\infty = \ell \cdot \deg(F_1) \cdot P_\infty,$$

and

$$(\alpha)_\infty^L = \deg(F_2) \cdot \pi^* Q_\infty = \ell \cdot \deg(F_2) \cdot P_\infty.$$

Next, by hypothesis one have $(f)_\infty^K = m \cdot Q_\infty$ (recall that Q_∞ is the unique pole of x and α and K), so the equation $y^n = f$ gives

$$\begin{aligned} \ell \cdot (y)_\infty^L &= \pi^*(f)_\infty^K \\ &= m \cdot e(P_\infty | Q_\infty) \cdot P_\infty, \end{aligned}$$

that is $(y)_\infty^L = m \cdot P_\infty$. □

Remark 6. Considering these extensions, the study of the divisor of pole we are interested in is particularly simple because it is only supported by one place, that correspond to the point at infinity in $\mathbb{P}^1(\mathbb{F}_{q^m})$, that is totally ramified in the tower $\mathbb{F}_{q^m}(x) \subseteq K \subseteq L$.

The proposition 5 above allows us to give the precise structure of the divisor D (recall its definition in (4), section 3.2) in our context.

Corollary 2. *One have*

$$D = \tilde{G} - \left\lceil \frac{m}{\ell} \right\rceil \cdot Q_\infty \in Div(K).$$

Proof. From the structure of $(y)_\infty^L$ given in proposition 2, it is clear that

$$\text{Supp} \left(\widetilde{(y)_\infty^L} \right) = \{Q_\infty\}.$$

It remains to show that if D is defined as above, then $D = \widetilde{G - (y)_\infty^L}$. In fact, we have

$$\begin{aligned} \pi^* D &= \pi^* \left(G - \widetilde{\left\lceil \frac{m}{\ell} \right\rceil} \cdot Q_\infty \right) \\ &= \pi^* \tilde{G} - \left\lceil \frac{m}{\ell} \right\rceil \cdot \pi^* \widetilde{Q_\infty} \\ &= G - n \cdot \left\lceil \frac{m}{\ell} \right\rceil \cdot P_\infty \quad (\text{using remark 3}) \\ &\leq G - m \cdot P_\infty \\ &= G - (y)_\infty^L, \end{aligned}$$

the last equality coming from proposition 5. Moreover, this choice of D is optimal (ie. the biggest, see. definition 5) since m/ℓ can not be an integer (recall that m and ℓ are coprime). \square

Note that the divisor D in the above corollary is know in our context from our hypothesis, and thus one can construct the corresponding linear system (see (5) in section 3.2).

As we already mentionned earlier, the linear system (5) doesn't only have the vector \mathbf{y} as solution, but also any evaluation vector that comes from a function $h \in L$ such that

$$(h)_\infty^L \leq (y)_\infty^L = m \cdot P_\infty.$$

In the context of a Kummer covering, one can easily find other solutions. In fact, let $h := x^i \alpha^j \in K$ be a function that only depend on variables x and α , and $\mathbf{h} = \mathbf{x}^i \boldsymbol{\alpha}^j$ its corresponding row vector, following usual notations. Using proposition 5, and in particular the description of the pole divisors of x and α , one easily see that

$$(h)_\infty^L = \ell \cdot (i \cdot \deg(F_1) + j \cdot \deg(F_2)) \cdot P_\infty.$$

As a result, \mathbf{h} is also a solution of the system (5), provided that

$$\ell \cdot (i \cdot \deg(F_1) + j \cdot \deg(F_2)) \leq m.$$

Since we have found other solutions, one now need to choose the vector \mathbf{y} among them. This can be done by adding other equations to the system, that are only satisfied by the vector \mathbf{y} . Indeed, since the action of the automorphism group $\Sigma = \langle \sigma \rangle$ that acts on the support \mathcal{P} of the code \mathcal{C} is given by

$$\sigma : y \longmapsto \xi \cdot y,$$

with $\xi \in \mu_\ell^*(\mathbb{F}_{q^m})$, the components of the vector \mathbf{y} satisfy a geometric progression by orbit (recall that \mathcal{P} is made of orbit under the above action of the automorphism σ). To simplify a bit the situation, recall that the set \mathcal{P} is made of r orbits of lenght ℓ , and suppose in what follow that its elements are ordered orbit by orbit, that is if $\tilde{\mathcal{P}} = \{Q_1, \dots, Q_r\} \in \mathbb{P}_K$, then elements of \mathcal{P} at indices $(i-1)\ell + 1, \dots, i\ell$ correspond to the ℓ extensions of Q_i in L (for every $1 \leq i \leq r$). Let us consider the following bloc matrices

$$A(\xi) := \begin{pmatrix} B(\xi) & 0 & \cdots & 0 \\ 0 & B(\xi) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & B(\xi) \end{pmatrix}, \text{ where } B(\xi) = \begin{pmatrix} \xi & -1 & 0 & \cdots & 0 \\ 0 & \xi & -1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & -1 \\ -1 & 0 & \cdots & \cdots & \xi \end{pmatrix}$$

and ξ is the root of unity that defines σ , and $A(\xi) \in M_n(\mathbb{F}_{q^m})$. Then we have

$$A(\xi) \cdot \mathbf{y}^T = 0.$$

In particular, one gets

$$\begin{pmatrix} A(\xi) \\ H \cdot \mathbf{D}_1 \\ \vdots \\ H \cdot \mathbf{D}_s \end{pmatrix} \cdot \mathbf{y}^T = 0. \quad (6)$$

The relation (6) is enough to recover \mathbf{y} since the other solutions of (5) doesn't satisfy this geometric progression structure, because it is clear by construction that the evaluation vectors \mathbf{x} and $\boldsymbol{\alpha}$ are equals on each orbit of length ℓ , since σ only acts on y -coordinate of points on the curve \mathcal{Y} .

Remark 7. Since, σ (and so ξ) is supposed to be unknown at the beginning of the attack, one may have to test all the possibilities for ξ in order to find the correct one. This leads to solve at most $\#\mu_\ell^*(\mathbb{F}_q) = \varphi(\ell)$ linear systems like (6), which remains reasonable since $\varphi(\ell)$ is rather small.

In all our computing experiences, system (6) allows us to recover the desired vector \mathbf{y} . To finish the attack, one only have to recover the polynomial f that defines the extension L/K by using a multivariate interpolation method. You can find in annex A a detailed algorithm, as well as a complexity analysis.

5.3 Artin-Schreier covering

As in section 5.2, the quotient curve \mathcal{X} is taken as a curve over \mathbb{F}_{q^m} with separated variables, those function field $K = \mathbb{F}_q(x, \alpha)$ is given by

$$F_1(\alpha) = F_2(x), \quad F_1, F_2 \in \mathbb{F}_{q^m}[T]$$

and $(\deg(F_1), \deg(F_2)) = 1$.

Here, we will consider an Artin-Schreier cover of the curve \mathcal{X} . Let $p := \text{char}(\mathbb{F}_{q^m})$ denote the characteristic of the base field \mathbb{F}_{q^m} . Consider the extension $L = K(y)$, with

$$y^p - y = f, \quad f \in K$$

ans denote by $m := \deg((f)_\infty^K)$ the degree of the pole divisor of f in K . Suppose that $(m, p) = 1$. Then the extension L/K is an Artin-Schreier extension, it is cyclic of order p and

$$\text{Gal}(L/K) = \{\sigma : y \mapsto y + \beta, \beta \in \{0, \dots, p-1\}\}.$$

In this case, the hypotheses of our procedure are the same as in section 5.2, knowing that this time the automorphism is completely determined by the choice of the element $\beta \in \mathbb{F}_p$. Here again, our goal will be to recover the minimal polynomial of y over K , that is the function $f \in K$. Using the defining equation of the function field L and the fact that m is prime to p , one can show that the place $Q_\infty \in \mathbb{P}_K$ (defined in lemma 3) is totally ramified in L/K . As usual, we denote by P_∞ its unique extension in L . With our choices of parameters and hypotheses, we can prove that

Proposition 6. *We have*

$$(x)_\infty^L = p \cdot \deg(F_1) \cdot P_\infty,$$

$$(\alpha)_\infty^L = p \cdot \deg(F_2) \cdot P_\infty,$$

and

$$(y)_\infty^L = m \cdot P_\infty.$$

Proof. Similar to the proof of proposition 5 above. □

Note that this is exactly the same result as in the Kummer case. In particular, the divisor of poles of y in L is only supported by the place P_∞ . As a result, the divisor in K that we will use to construct our linear system is here given by

$$D = \tilde{G} - \left\lceil \frac{m}{p} \right\rceil \cdot Q_\infty \in \text{Div}(K).$$

This allows us to construct the linear system (5), since the above divisor can be constructed from our hypothesis.

In the Artin-Schreier case, one can proceed the same way to find other solutions of (5). In particular, a monomial $x^i \alpha^j \in K$ gives a solution vector if and only if

$$p \cdot (i \cdot \deg(F_1) + j \cdot \deg(F_2)) \leq m.$$

Note that this is pretty much the same condition as in Kummer case. Thus, one need a way to select the correct solution. For that, we add again other equations that are only satisfied by the vector \mathbf{y} , recalling that here, the action of the automorphism group $\langle \sigma \rangle$ on the set \mathcal{P} is given by

$$\sigma : y \mapsto y + \beta,$$

where $\beta \in \mathbb{F}_p$. Thus the vector \mathbf{y} we are searching for satisfies an arithmetic progression by orbit. In order to see it fluently, let us assume again that the support \mathcal{P} is ordered by orbit. Then let us consider the following bloc matrices :

$$C := \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & B \end{pmatrix}, \text{ where } B = \begin{pmatrix} -1 & 1 & 0 & \cdots & 0 \\ 0 & -1 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & \cdots & -1 \end{pmatrix}.$$

Then we have

$$C \cdot \mathbf{y}^T = \begin{pmatrix} \beta \\ \vdots \\ \beta \end{pmatrix},$$

where β is the element in \mathbb{F}_p that defines the automorphism σ (note that β is supposed to be unknown here, but as in Kummer case, we can search for it in reasonable time) . Thus, if we add this to (5) we get

$$\begin{pmatrix} C \\ H \cdot \mathbf{D}_1 \\ \vdots \\ H \cdot \mathbf{D}_s \end{pmatrix} \cdot \mathbf{y}^T = \begin{pmatrix} \beta \\ \vdots \\ \beta \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (7)$$

The above relation (7) allows us to isolate \mathbf{y} , since the other solutions do not satisfies this arithmetic progression, for the same reason as in the Kummer case. Thus one can finish the attack by retrieving the function f using an interpolation method.

5.4 Generalisation to solvable Galois covering

Above, we showed that we could apply our method to any Kummer or Artin-Schreier covering of a separated variable curve. Here we will see why those two examples are interesting. In fact, they both correspond to cyclic cover, and their common point is that the automorphism group $Aut(L/K)$ is cyclic. More especially, all extensions in sections 5.2 and 5.3 are Galois, with cyclic Galois group. The idea of this section is to consider a Galois extension of function fields L/K such that $Gal(L/K)$ is a solvable group.

In order to fix the ideas, let $K = \mathbb{F}_{q^m}(x)$ be the rational functions function field, and $L = K(y)$ be a Galois extension, that correspond the a separable cover $\mathcal{Y} \rightarrow \mathbb{P}^1(\mathbb{F}_{q^m})$ (note that we could more generally take K as the field of rational functions of a separated variable curve \mathcal{X} over \mathbb{F}_{q^m} , as we did before). We then suppose that $Gal(L/K)$ is solvable, that is we have sequence of normal subgroups

$$\{Id\} := \mathcal{G}_0 \triangleright \mathcal{G}_1 \triangleright \cdots \triangleright \mathcal{G}_t := Gal(L/\mathbb{F}_q(x)). \quad (8)$$

such that any quotient in (8) is cyclic. The idea is then to use the Galois theory to make the correspondance between subfields M of L and normal subgroups of $Gal(M/\mathbb{F}_q(x))$. (see for example [Sti09], annex A.12 for

more informations). With notations as above, for every $0 \leq i \leq t$, let us denote by $L_i := L^{\mathcal{G}_i}$ the subfield of L fixed by \mathcal{G}_i , with $L_t = \mathbb{F}_{q^m}(x)$ and $L_0 = L$. Then extensions L/L_i are Galois, with \mathcal{G}_i as Galois group. In particular, in order to recover the equation of the curve \mathcal{Y} , we propose to apply the procedure described in section 3 recursively.

For example, let us consider the normal subgroup $\mathcal{G}_{t-1} \subseteq \mathcal{G}_t$. It is well-known from Galois theory that $L_{t-1}/\mathbb{F}_{q^m}(x)$ is Galois, with Galois group equals to the quotient $\mathcal{G}_t/\mathcal{G}_{t-1}$, that is supposed to be cyclic. Thus, there exist an integer ℓ_{t-1} such that

$$\mathcal{G}_t/\mathcal{G}_{t-1} \simeq \mathbb{Z}/\ell_{t-1}\mathbb{Z},$$

and the extension $L_{t-1}/\mathbb{F}_{q^m}(x)$ is cyclic of order ℓ_{t-1} .

Repeating this for every subgroup in the sequence (8), we get the existence (and uniqueness) of integers $\ell_0, \ell_1, \dots, \ell_{n-1}$, as well as a tower of function fields

$$\mathbb{F}_{q^m}(x) := L_t \subseteq L_{t-1} \subseteq \dots \subseteq L_0 := L \quad (9)$$

such that extensions L_i/L_{i+1} are cyclic of order ℓ_i , for every $0 \leq i \leq t-1$.

Let us now formulate the hypothesis before describing how to recover the equation of the curve \mathcal{Y} (that is the defining equation of the function field L). As before, we are given an SSAG-code on \mathcal{Y} that is stable under the action of $\text{Gal}(L/\mathbb{F}_{q^m}(x))$, and especially we know one of its parity check matrix. We also suppose that we know the structure of the its invariant code on the projective line. In particular, recall that the invariant support $\tilde{\mathcal{P}}$ is a set of rational places on the projective line, and that the support $\mathcal{P} \subseteq \mathbb{P}_L$ correspond to all their extensions. In particular, places in $\tilde{\mathcal{P}}$ are totally split in $L/\mathbb{F}_{q^m}(x)$, and thus also in any sub-extension of the tower (9).

From this point, the plan is to ride up the tower (9), and thus to recover step by step the curve that corresponds to the function field L_i , together with the extensions of the places in $\tilde{\mathcal{P}}$ in it (for any $0 \leq i \leq t-1$). The crucial point is that any sub-extension L_i/L_{i+1} is cyclic, meaning that we will be able to apply section 5.3 if $\ell_i = p$ and section 5.2 otherwise. (see [Sti09], annex A.13 for a characterisation of cyclic extensions of function field).

Remark 8. The hypothesis that we know the action of $\text{Gal}(L/\mathbb{F}_{q^m}(x))$ on the support \mathcal{P} is really important in this context. In fact if we focus on the first step, one need to know the location in \mathcal{P} of the ℓ_{n-1} extensions of each place of $\tilde{\mathcal{P}}$. This is mandatory because while constructing the system (5), we use a parity check matrix of a folded code of the big one (and not the code itself), and this require to know which columns one need to delete.

As a more detailed example, let ℓ_1, ℓ_2 be two primes, that are coprime with $p = \text{char}(\mathbb{F}_{q^m})$. Consider a curve \mathcal{Y} over \mathbb{F}_{q^m} , with function field $L = \mathbb{F}_{q^m}(x, y)$, such that

$$P(x, y) = 0, \quad P \in \mathbb{F}_{q^m}[X, Y] \text{ irreducible.}$$

Let us assume $L/\mathbb{F}_{q^m}(x)$ is Galois of order $\ell_1\ell_2$. In particular, its Galois group is solvable. Let us denote by $S \subseteq \text{Gal}(L/\mathbb{F}_{q^m}(x))$ its unique ℓ_2 -Sylow (that is of course normal), and set $K = L^S$. We have :

1. $\mathbb{F}_{q^m}(x) \subseteq K = L^S \subseteq L$;
2. L/K is cyclic of order ℓ_2 , and $\text{Gal}(L/K) = S \simeq \mathbb{Z}/\ell_2\mathbb{Z}$;
3. $K/\mathbb{F}_{q^m}(x)$ is also cyclic, of order ℓ_1 , and $\text{Gal}(K/\mathbb{F}_{q^m}(x)) \simeq \mathbb{Z}/\ell_1\mathbb{Z}$.

Now, suppose we are given a parity check matrix of a code $\mathcal{C} = \text{SSAG}_q(\mathcal{Y}, \mathcal{P}, G)$ that is stable under $\text{Gal}(L/\mathbb{F}_{q^m}(x))$, together with its invariant code $\text{SSAG}_q(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$. We also suppose that we now how $\text{Gal}(L/\mathbb{F}_{q^m}(x))$ acts on the support \mathcal{P} . We then proceed as follow.

1. By assumption, the extension $K/\mathbb{F}_{q^m}(x)$ is cyclic of order ℓ_1 , with $(\ell_1, p) = 1$. Thus, it is well-known that this is a Kummer extension. As a result, there exists a polynomial $b \in \mathbb{F}_{q^m}[x]$ such that $K = \mathbb{F}_{q^m}(x, \alpha)$, with

$$\alpha^k = b(x), \quad b \in \mathbb{F}_{q^m}[T].$$

Let us denote by $m_1 := \deg(b)$, and suppose again that m_1 is prime to k (as we did in the classical Kummer case, note that it allows the point at infinity in $\mathbb{F}_{q^m}(x)$ to be totally ramified in $K/\mathbb{F}_{q^m}(x)$). Then, we can consider the divisor

$$D_1 := \tilde{G} - \widetilde{(\alpha)_\infty^K} = \tilde{G} - \left\lfloor \frac{m_1}{\ell_1} \right\rfloor \cdot R_\infty \in \mathbb{P}_{\mathbb{F}_{q^m}(x)},$$

where R_∞ is the pole of x in $\mathbb{F}_{q^m}(x)$. It can be constructed from our hypothesis, and allows us to construct a linear system as (5) in order to recover the evaluation vector α . However, note that in this case, we can't use the parity check matrix of the code \mathcal{C} on \mathcal{Y} , since we are not reconstructing the curve \mathcal{Y} . In fact, this step allows us to recover the quotient curve $\mathcal{X} = \mathcal{Y}/S$ with function field K , and for this we need the parity check matrix of the subcode of \mathcal{C} that is invariant under the subgroup $S \subseteq \text{Gal}(L/\mathbb{F}_{q^m}(x))$ of order ℓ_2 (ie. its unique ℓ_2 -Sylow). This matrix can be constructed from the one of (TO DO : ref) At this point, assume that we recovered the vector α using section 5.2.

- Using step 1 above, one can recover extensions of places in \tilde{P} , as elements in K . By interpolation, this gives the polynomial b and thus the defining equation of the curve \mathcal{X} (see section 5.2). In particular, we know at this point a set \mathcal{P}' that corresponds to extensions of places in \tilde{P} in K , as well as the divisor $G' := \pi^* \tilde{G}$, where $\pi : \mathcal{X} \rightarrow \mathbb{P}^1(\mathbb{F}_{q^m})$. Moreover, the subcode of \mathcal{C} that is invariant under the ℓ_2 -Sylow S of $\text{Gal}(L/\mathbb{F}_{q^m}(x))$ is given by

$$C_L(\mathcal{X}, \mathcal{P}', G').$$

- The next step is to use that we know on the curve \mathcal{X} to recover \mathcal{Y} . This corresponds to recover the extension L using informations on its fixed field $K = L^S$. As L/K is cyclic of order ℓ_2 , one need to assume that $\ell_2 \mid q^m - 1$, in which case there exist a function $f \in K$, with $m_2 := \deg((f)_\infty^K)$, such that $L = K(y)$, with

$$y^\ell = f(x, \alpha).$$

If $(m_2, \ell_2) = 1$, the place R_∞ (ie. the pole of x in $\mathbb{F}_{q^m}(x)$) is totally ramified in $L/\mathbb{F}_{q^m}(x)$, and we can use the divisor

$$D_2 := G' - \widetilde{(y)_\infty^L} = G' - \left\lfloor \frac{m_2}{\ell_2} \right\rfloor \cdot Q_\infty \in \mathbb{P}_K,$$

where Q_∞ is the unique extension of R_∞ in K , to build a linear system and thus recover the evaluation vector \mathbf{y} , that gives the y -coordinates of the points in \mathcal{P} . As in section 5.2, it allows us to recover the defining equation of \mathcal{Y} , as a cover of \mathcal{X} .

- Using previous steps, one can recover the minimal polynomial of y over $\mathbb{F}_{q^m}(x)$ and thus conclude.

6 Perspectives

**** REVOIR CETTE SECTION, ET POTENTIELLEMENT LA DÉPLACER ****

Let us put together our conclusions.

- For solvable automorphism group, there are 2 cases for each divisor ℓ of $\# \text{Aut}(L/\mathbb{F}_{q^m}(x))$:
 - If ℓ is prime to $p = \text{char}(\mathbb{F}_{q^m})$, thus it corresponds to a Kummer sub-extension. In this case, we need to have $\ell \mid q^m - 1$ in order to have $\mu_\ell(\mathbb{F}_{q^m}) \neq \{1\}$. Moreover the equation of this Kummer sub-extension L/K looks like

$$z^\ell = f,$$

where $f \in K$, $d := \deg((f)_\infty^K)$ and $L = K(z)$. We imposed above that d should be prime to ℓ . It allows to have a simple ramification of the point at infiny in each extension, but this is not mandatory. If this point had more that one extension, we would need to know any of them in order to construct the corresponding divisor D (cf. (4)).

- If $\ell = p$, it corresponds to an Artin-Schreier sub-extension L/K , with

$$z^p - z = f,$$

where $f \in K$, $d := \deg((f)_\infty^K)$ and $L = K(z)$. Here again, we imposed for the same reasons $(p, d) = 1$, as it is more convenient.

2. In both Kummer and Artin-Schreier cases, that turns out to be the elementary parts of the field of application of our procedure, we supposed before the attack that we knew the root of unity ξ that defines σ (resp. $\beta \in \mathbb{F}_p$ in Artin-Schreier cases). Actually it is not mandatory because when adding geometric (resp. arithmetic) progression to the system (5) in order to recover the good evaluation vector, we can guess the good ξ (resp. β) by solving a system for each until we get unicity of the solution. This cost at most ℓ (resp. p) tries, which is not so much in practical applications.
3. At any step of the procedure (see 1. above), we asked to know the degree d of the divisor of poles of the function $f \in K$. Actually we can also work by guessing it, ie. since $(d, [L : K]) = 1$ by assumption, we only want information about $\frac{d}{[L:K]}$ in order to construct D . So we can try a few values of this quotient until we get unicity of the solution at the end. Note however that this could raise the complexity too much.

As a matter of perspective results, it could be interesting to focus on covers where the support of the divisor of poles of y is more complicated, that is made of more than one point. In fact, if those are known, we can show that our procedure still works. The fact is that we have no reasons to know it (it actually is the point of the attack !), so at the moment it seems hard to generalize more.

In a coding theoretic point of view, our procedure gives "negatives" results, in the sense that it shows that for this kind of covers, the security of the public code (constructed as a structured SSAG-code on \mathcal{Y}) is reduced to those of its invariant subcode, which is smaller and thus easier to brute force. It then shows that cryptosystems constructed from it should focus on hiding the structure of the invariant code, which can sometimes break completely the system.

7 A McEliece scheme using quasi-cyclic SSAG-codes over the Hermitian curve

7.1 The proposed scheme

Let q be the power of a prime p and $m \geq 1$ refers to the extension degree of a field \mathbb{F}_{q^m} . Since the Hermitian curve is defined over a field with square cardinality, let us also denote $q_0 := p^s$ such that $m = 2s$ and thus $q^m = q_0^2$. We consider the Hermitian function field $\mathcal{H} = \mathbb{F}_{q_0^2}(x, y)$ over $\mathbb{F}_{q_0^2} = \mathbb{F}_{q^m}$ defined by the equation

$$y^{q_0} + y = x^{q_0+1}.$$

The idea is to construct a McEliece scheme using SSAG-code on the Hermitian curve, stable under the action of an automorphism of \mathcal{H} . There are two motivations to use this curve : first, it is a maximal curve, that it has the maximal number of rational points (that is $N(\mathcal{H}) = q_0^3 + 1$). It allows us to consider long codes, and thus more flexibility. Moreover, the automorphism group of \mathcal{H} is very large and has been well-studied (see for example [Sti09] or [?]); which permits us to chose a good automorphism σ acting on our code (it will turns to be really important later on, see section 7.4.2).

We use the following notations :

- let $\sigma \in \mathcal{H}$ be an automorphism of order ℓ (we will describe later how to construct it);
- let $n_0 \in \mathbb{N}^*$ and $\mathcal{P} := \bigsqcup_{i=1}^{n_0} \text{Orb}_\sigma(P_i)$ be a support made of n_0 distincts orbites under the action of σ ;
- let $s \in \mathbb{N}^*$ and $G = \sum_{i=1}^s t_i \sum_{Q \in \text{Orb}_\sigma(Q_i)} Q$ be an invariant divisor, with $Q_i \in \mathbb{P}_{\mathcal{H}}$ and $t_i \in \mathbb{Z}$. We also suppose that $\text{supp}(G) \cap \mathcal{P} = \emptyset$.

We now can describe the scheme :

Key generation We consider the quasi-cyclic code

$$\mathcal{C}_{\text{pub}} := \text{SSAG}_q(\mathcal{H}, \mathcal{P}, G)$$

constructed on the Hermitian curve \mathcal{H} with length $n = n_0 \cdot \ell \leq N(\mathcal{H})$ and dimension k . Let t be the correction capability of the code and $G_{\text{pub}} = (I_k | M)$ be a systematic generator matrix of \mathcal{C}_{pub} , where M is an ℓ -blocks-circulant matrix (possible since the code is QC). Thus G_{pub} can entirely be described by the set of rows

$$\rho(G_{\text{pub}}) := \{M_i \mid i \in \{1, \ell + 1, 2\ell + 1, \dots, (n - k) - \ell + 1\}\},$$

M_i being the i -th row of M .

- **Public key** : the set of rows $\rho(G_{\text{pub}})$ and the integer t .
- **Secret key** : the support \mathcal{P} and the divisor G .

Encryption A plain text $\mathbf{m} \in \mathbb{F}_q^k$ is encrypted by

$$\mathbf{y} = \mathbf{m}G_{\text{pub}} + \mathbf{e},$$

where $\mathbf{e} \in \mathbb{F}_q^n$ is a vector error such that $\omega(e) \leq t$.

Decryption Using a general decoding algorithm for algebraic geometry codes (see for example [HP95]), we can find a codeword $\mathbf{c} = \mathbf{y} - \mathbf{e} \in \mathcal{C}_{\text{pub}}$. From \mathbf{c} and the knowledge of G_{pub} , we can recover the message \mathbf{m} .

Note that in this scheme, the automorphism itself and the curve \mathcal{H} is considered as secret data, and only the order ℓ of σ is known from the public key. In previous sections, we have shown that the knowledge of the full invariant code allows us to attack the system, recovering the secret elements. It means that in order to secure our scheme, we need to ensure that the invariant code can not be recovered easily.

In what follow, we will describe some known attacks against the invariant SSAG-code, and then we will propose a set of parameters to block those attacks.

7.2 Invariant code on the projective line

In the proposed scheme, the public code is a QC-SSAG-code constructed on the Hermitian curve, ie.

$$\mathcal{C}_{\text{pub}} = \text{SSAG}_q(\mathcal{H}, \mathcal{P}, G),$$

that is invariant under some order ℓ automorphism $\sigma \in \text{Aut}(\mathcal{H})$. As shown by corollary 1, the invariant subcode (say \mathcal{C}_{inv}) is an SSAG-code on the quotient curve. Moreover, this code can be constructed in polynomial time (TO DO : ref) from the generator matrix of \mathcal{C}_{pub} and the action of the induced permutation on it (that is the public key). This means that a generator matrix of \mathcal{C}_{inv} must also be considered as a public data. From now on, let us denote by \mathbf{G}_{inv} a generator matrix of \mathcal{C}_{inv} .

In the particular case where the quotient curve $\mathcal{H}/\langle\sigma\rangle$ is the projective line $\mathbb{P}^1(\mathbb{F}_{q^m})$, it is possible to construct an algebraic system to recover the secret elements of \mathcal{C}_{inv} . Using the attack of section 5., we can then recover the public code, breaking the system. The key ingredient that allows us to build such a system is the fact that $\mathbb{P}^1(\mathbb{F}_{q^m})$ has genus 0, and thus has a trivial divisor class group.

From corollary 1, we know that the invariant code is given by

$$\mathcal{C}_{\text{inv}} := \text{SSAG}_q\left(\mathbb{P}^1(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, \tilde{G}\right),$$

To construct an algebraic system, we start from the inclusion

$$C_L(\mathbb{P}(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, \tilde{G})^\perp \subseteq \text{SSAG}_q(\mathbb{P}(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, \tilde{G})^\perp \otimes \mathbb{F}_{q^m},$$

that is a direct consequences of definitions (in the right-hand side, we have extended the scalars to \mathbb{F}_{q^m} since its the field definition of the AG-code). This means that for every codeword $\mathbf{c} \in C_L(\mathbb{P}(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, \tilde{G})^\perp$, we have

$$\mathbf{c} \cdot \mathbf{G}_{\text{inv}}^T = 0, \quad (10)$$

where \mathbf{G}_{inv} is a generator matrix of the invariant code $\mathcal{C}_{\text{pub}}^\sigma$ (that can be computed in polynomial time from the public data). Moreover, we know from proposition 2 that there exist a divisor $G' \in \text{Div}(\mathbb{P}^1(\mathbb{F}_{q^m}))$ such that

$$C_L(\mathbb{P}(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, \tilde{G})^\perp = C_L(\mathbb{P}^1(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, G').$$

As a consequence, the knowledge of a basis of the Riemann-Roch space $L(G')$ allows us to write formally codewords in $C_L(\mathbb{P}^1(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, G')$, without knowing the set $\tilde{\mathcal{P}}$. The key part is that the projective line $\mathbb{P}^1(\mathbb{F}_{q^m})$ has a trivial divisor class group. In particular, there exist a function h in the rational function field $\mathbb{F}_{q^m}(x)$ such that

$$G' = (h)^{\mathbb{F}_{q^m}(x)} + \deg(G') \cdot P_\infty,$$

where P_∞ is the usual notation for the pôle of x in $\mathbb{F}_{q^m}(x)$. From the last equality, we get

$$L(G') = \langle h(x)x^i \mid 0 \leq i \leq \deg(G') - 1 \rangle_{\mathbb{F}_{q^m}},$$

which is a dimension $r = \deg(G') - 1$ vector space over \mathbb{F}_{q^m} .

Let us write the unknown support $\tilde{\mathcal{P}} = (\tilde{P}_i)_{i=1}^{n_0}$, with $\tilde{P}_i = (x_i : 1)$. The goal is to recover the x_i 's. For that, we denote by $\mathbf{X} = (X_1, \dots, X_{n_0})$ and $\mathbf{Z} = (Z_1, \dots, Z_{n_0})$ two sets of formal variables, respectively corresponding to x_i 's and $h(x_i)$'s. From equation (10) above, we have the following system

$$\begin{pmatrix} Z_1 & \cdots & Z_{n_0} \\ Z_1 X_1 & \cdots & Z_{n_0} X_{n_0} \\ \vdots & \ddots & \vdots \\ Z_1 X_1^r & \cdots & Z_{n_0} X_{n_0}^r \end{pmatrix} \cdot \mathbf{G}_{\text{inv}}^T = 0.$$

The first row provides $k = \dim(\mathcal{C}_{\text{inv}})$ linear equations in the variables \mathbf{Z} , and since $k < n_0$, one can eliminate some variables in the set \mathbf{Z} . On the other hand, the 2-transitivity of the affine group on \mathbb{F}_{q^m} allows us to fix arbitrarily the unknowns x_1 and x_2 . Therefore, the above system consist in kr equations in $n_0 - 2$ variables \mathbf{X} and $n_0 - k$ variables \mathbf{Z} .

If we are able to solve this system, we recover the function h (and thus \tilde{G}) as well as the support $\tilde{\mathcal{P}}$; that is we have reconstructed the invariant code \mathcal{C}_{inv} . Since the security of the whole system rely on it, we have broke the scheme.

Remark 9. *The cost of solving the above system is hard to produce. It is possible to have an upper bound of the complexity in the case where the system has a specific form; which can be useful to estimate the security of schemes using SSAG-codes over the line. Thoses results can be found in [FOP⁺16a], [FOP⁺16b] and [FOPT10].*

Actually, if the quotient curve is $\mathbb{P}^1(\mathbb{F}_{q^m})$, the security is the same as the scheme using quasi cyclic Goppa codes, and thus there no advantages to use it. In particular, this means that the automorphisms σ should be chosen such that \mathcal{H}^σ is not rational. In the latter case, the fixed field has a more complex divisor class group and the above attack doesn't work. In the following section, we will describe the cost of an exhaustive search on the invariant code, depending on different parameters of the fixed field.

7.3 Brute force on the invariant code

Let us recall that the security of the private key of the scheme proposed in section 7.1 rely on the security of the invariant code. Thus, this section will be dedicated to the cost of an exhaustive search on the quotient curve. This will allow us to understand how to choose the automorphism σ in order to maximize the complexity of the exhaustive search. Let us rewrite

$$C_{\text{inv}} := \text{SSAG}_q(\mathcal{H}/\langle\sigma\rangle, \tilde{\mathcal{P}}, \tilde{G})$$

the invariant code. A brute force attack on it will consists in the three following steps :

1. Enumerating all the possible divisor classes of a given degree on the quotient curve $\mathcal{H}/\langle\sigma\rangle$;
2. Guess the good divisor \tilde{G} in the class;
3. Then guess the support $\tilde{\mathcal{P}}$ of length $n_0 := n/\ell$.

Let us first discuss the third step, which is the easiest to formalize.

Recovering the invariant support.

Here we assume that the two first steps were done and that a divisor \tilde{G} was found. To recover the invariant support there are two ways to proceed :

The first consists in an exhaustive search on all subset $S \subseteq \mathcal{H}/\langle\sigma\rangle(\mathbb{F}_{q^m})$ of length $n_0 = n/\ell$, then we get the good permutation using the SSA algorithm (see [?] for more details).

The second way is to solve a linear system as in section 7.2. In order to build it, we start by recalling that there exists (from proposition 2) a divisor $G' \in \text{Div}(\mathcal{H}/\langle\sigma\rangle)$ such that

$$C_L(\mathbb{P}(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, \tilde{G})^\perp = C_L(\mathbb{P}^1(\mathbb{F}_{q^m}), \tilde{\mathcal{P}}, G').$$

Here we don't know the quotient curve from our hypothesis. Nevertheless, let us suppose that the attacker found a way to recover it. It then becomes possible to compute the Riemann-Roch space $L(G') \subseteq \mathbb{F}_{q^m}(\mathcal{H}/\langle\sigma\rangle)$; ie. we have $L(G') = \langle f_1, \dots, f_s \rangle_{\mathbb{F}_{q^m}}$. As in section 7.2, one gets

$$\forall 1 \leq i \leq s, (f_i(\tilde{P}_1), \dots, f_i(\tilde{P}_{n_0})) \cdot \mathbf{G}_{\text{inv}}^T = 0,$$

where $\tilde{\mathcal{P}} = \{\tilde{P}_1, \dots, \tilde{P}_{n_0}\}$. In particular, let us introduce $2n_0$ formal variables X_1, \dots, X_{n_0} and Y_1, \dots, Y_{n_0} corresponding to the evaluation in x and y on the places of $\tilde{\mathcal{P}}$. Here, we supposed that the quotient curve is seen in a plane model. Thus this leads to the following system

$$\begin{pmatrix} f_1(X_1, Y_1) & \cdots & f_1(X_{n_0}, Y_{n_0}) \\ f_2(X_1, Y_1) & \cdots & f_2(X_{n_0}, Y_{n_0}) \\ \vdots & \ddots & \vdots \\ f_s(X_1, Y_1) & \cdots & f_s(X_{n_0}, Y_{n_0}) \end{pmatrix} \cdot \mathbf{G}_{\text{inv}}^T = 0.$$

Note that this method is nothing but a generalization of the method describe in 7.2, but this system is actually harder to solve since we cannot estimate the form of rational functions f_i . On the other hand, even if the system is polynomial, the complexity of solving it using Gröbner bases depend on the form and degree of the polynomials and is thus difficult to forecast.

Enumeration of divisor classes.

Here, we will first explain why it is not necessary to enumerate all divisors in the quotient curve $\mathcal{H} \backslash \langle \sigma \rangle$ in order to find the correct one. In fact, if the support is fixed, two different divisors can produce the same code. This fact comes from the structure of SSAG-codes inherited from AG ones. In order to precise this, let us introduce the notion of diagonal equivalent codes.

Definition 7. Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_{q^m}^n$ be two linear codes. We say they are diagonal equivalent, denoted $\mathcal{C}_1 \sim_{\text{diag}} \mathcal{C}_2$, if there exist n non zero scalars in \mathbb{F}_{q^m} , say $\lambda_1, \dots, \lambda_n$, such that

$$\mathcal{C}_1 = (\lambda_1, \dots, \lambda_n) \star \mathcal{C}_2 := \{(\lambda_1 c_1, \dots, \lambda_n c_n) \mid (c_1, \dots, c_n) \in \mathcal{C}_2\}.$$

Note that the diagonal equivalence between two codes \mathcal{C}_1 and \mathcal{C}_2 can be check by solving yet another linear system. In fact, let $\mathbf{G}_{\mathcal{C}_1}$ and $\mathbf{H}_{\mathcal{C}_2}$ be respectively a generator matrix of \mathcal{C}_1 and a parity check matrix of \mathcal{C}_2 . Let also W_1, \dots, W_n be n formal variables, and consider the following system

$$\mathbf{G}_{\mathcal{C}_1} \cdot \begin{pmatrix} W_1 & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & W_n \end{pmatrix} \cdot \mathbf{H}_{\mathcal{C}_2}^T = 0. \quad (11)$$

By definition 7, this system has at least one solution if and only if $\mathcal{C}_1 \sim_{\text{diag}} \mathcal{C}_2$, that is we have an easy way to check if two codes are diagonal equivalent.

Let us now explain why this property leads to a smarter brute force search on the divisor in the case on SSAG-codes. First, we deal with AG-codes which are easier to treat. The following result shows that the equivalence class of AG-codes depends only on the equivalence class of its divisor.

Theorem 3. (see [?], Corollary 4.15). Let \mathcal{X} be an algebraic curve of genus g and \mathcal{P} be a set of $n > 2g - 2$ rational places on \mathcal{X} . If G and H are two divisors on \mathcal{X} of same degree r such that $2g - 1 < r < n - 1$, then we have

$$C_L(\mathcal{X}, \mathcal{P}, G) \sim_{\text{diag}} C_L(\mathcal{X}, \mathcal{P}, H) \iff G \sim H.$$

In what follow, we denote by $AG_r(\mathcal{X}, \mathcal{P})$ the set of AG-code on the curve \mathcal{X} over \mathbb{F}_{q^m} , defined by a fixed support \mathcal{P} and any divisor of degree r . Then we have

Corollary 3. Let $\mathcal{P} \subseteq \mathcal{X}(\mathbb{F}_{q^m})$ be a support of lenght $n > 2g + 2$, where g is the genus of \mathcal{X} . Let also $r \in \mathbb{N}$ be such that $2g - 1 < r < n - 1$. Then

$$\#(AG_r(\mathcal{X}, \mathcal{P}) / \sim_{\text{diag}}) = h(\mathcal{X}),$$

where $h(\mathcal{X})$ is the number of divisor classes.

Proof. Immediate consequence of Theorem 3 and Proposition 1. □

The above estimation is sufficient if we want to perform a brute force search on an AG-code defined over a curve \mathcal{X} . In fact, we could proceed as follows.

1. Perform a brute force search among divisor classes of degree r (corresponding to the public AG-code), that is choose a representative divisor G' in the class.
2. Guess the support \mathcal{P}' (see above) and attempt to solve the system (11) to check whether the code $C_L(\mathcal{X}, \mathcal{P}', G')$ is diagonal equivalent to the public code.
3. If (11) has a solution $(\lambda_1, \dots, \lambda_n) \in (\mathbb{F}_{q^m}^*)^n$, then we have recovered the public code $(\lambda_1, \dots, \lambda_n) \star C_L(\mathcal{X}, \mathcal{P}', G')$.

By Theorem 3 and Corollary 3 we could have an estimation of the cost of a brute force search among divisor classes. Unfortunately, both theses results cannot be applied on subfield subcodes directly.

In the case of SSAG-codes, the situation is more complicated, but one can use the following result to have a first estimation on the number of SSAG codes.

Proposition 7. (see [?], Corollary 7.4). With above notations, if $n > 2g + 2$ and $2g - 1 < r < n$, then

$$\#AG_r(\mathcal{X}, \mathcal{P}) = (q^m - 1)^{n-1} h(\mathcal{X}).$$

Now let us denote by $SSAG_{q,r}(\mathcal{X}, \mathcal{P})$ the set of subfield subcodes on \mathbb{F}_q of AG codes on the curve \mathcal{X} , defined by the support \mathcal{P} and a divisor of degree r . Since we are taking subcodes, it is clear from the previous proposition that

$$\#SSAG_{q,r}(\mathcal{X}, \mathcal{P}) \leq \#AG_r(\mathcal{X}, \mathcal{P}) = (q^m - 1)^{n-1} h(\mathcal{X}).$$

Actually, we can decrease a little the previous bound with the following remark.

Remark 10. Let $\mathcal{C}_1, \mathcal{C}_2$ be two linear codes of length n over \mathbb{F}_{q^m} , and suppose that there exist $\lambda_1, \dots, \lambda_n \in \mathbb{F}_q^*$ such that $\mathcal{C}_1 = (\lambda_1, \dots, \lambda_n) \star \mathcal{C}_2$. Then their subfield subcodes on \mathbb{F}_q are equal, ie.

$$\mathcal{C}_1 \cap \mathbb{F}_q^n = \mathcal{C}_2 \cap \mathbb{F}_q^n.$$

This leads to the final upper bound

$$\#SSAG_{q,r}(\mathcal{X}, \mathcal{P}) \leq \frac{(q^m - 1)^{n-1}}{(q - 1)^{n-1}} h(\mathcal{X}).$$

In annex B, we will formally describe a brute search algorithm on the invariant SSAG-code and study its complexity.

Note that from the above approximation, it is clear that the complexity of the exhaustive search lower bounded by the number of divisor classes on the quotient curve, that is $h(\mathcal{H}/\langle \sigma \rangle)$. In particular, this will lead to choose optimally the automorphism $\sigma \in \text{Aut}(\mathcal{H})$ in order this number to be high enough. In the next section, we will discuss the choice of parameters in our system.

7.4 Suggested parameters

7.4.1 Choice of the quasi-cyclicity order ℓ

The main interest in using quasi-cyclic codes is that it allows us to reduce public key sizes. In particular, the large ℓ is, the smaller the public key is. This choice also influence the security of the scheme, as the security reduces to the security of the invariant code. In particular, if ℓ is too large, the invariant code will be rather small and probably less secured. Recall that it is always possible to build the invariant code from a public generator matrix and the permutation σ . Here we would like to choose ℓ such that it is not possible to construct any other intermediary code. We have two ways to avoid this.

1. **ℓ should be prime.** If there exist a prime $s \mid \ell$, then the power permutation σ^s also act on the public code. In particular, \mathcal{C}_{pub} is also s -quasi cyclic, that is one can construct another invariant code, ie. $\mathcal{C}_{\text{pub}}^{\sigma^s}$. Since this is possible for every divisor of ℓ , using Corollary 1, we are able to construct several SSAG codes smaller than the public code. Actually, we don't know if it makes the attack easier, but it is clear that every intermediary code provides information about the public support and divisor. As we want to give the least information as possible, ℓ will be chosen as a prime.
2. **ℓ should be such that q is in $\mu_{\ell-1}^*(\mathbb{F}_{q^m})$.** If this is satisfied, the polynomial $1 + z + z^2 + \dots + z^{\ell-1} \in \mathbb{F}_q[z]$ is irreducible. In fact, there exist another intermediary code that can be constructed from the knowledge of a generator matrix and the automorphism σ , that is the *folded code* (see [FOP⁺16a]). This code is the image of the public code \mathcal{C}_{pub} by the map $\text{id} + \sigma + \dots + \sigma^{\ell-1}$. Now, if the polynomial $1 + z + z^2 + \dots + z^{\ell-1}$ is reducible over \mathbb{F}_q , then it is possible to construct another intermediary subcode of \mathcal{C}_{pub} by computing its image by the map $P(\sigma)$, where P is a divisor of $1 + z + z^2 + \dots + z^{\ell-1}$. As in 1., we get another subcode of the public one that has a special structure related to the secret support and divisor. Actually we don't know if the knowledge of several folded code (note that we can always construct the full one) simplify an attack, but it could anyway be helpful for an attacker.

Remark 11. From the definition, it is clear that the folded code in σ -invariant, that is it is a subcode of $\mathcal{C}_{\text{pub}}^\sigma$. Now let p be the characteristic of \mathbb{F}_{q^m} . If $p \nmid \ell$, then those two codes are equal (see [?] , Lemma 3.2). In what follow, we will always have $p \nmid \ell$. Hence, if ℓ satisfies 1? and 2. above, then the only subcode of \mathcal{C}_{pub} that an attacker can construct is the invariant code. In particular, we can focus on the security of \mathcal{C}^σ without having to worry about possible other subcodes.

7.4.2 Choice of the automorphism σ

The complexity of the brute force attack on \mathcal{C}_{inv} , described in 7.3, depends on the class number of the quotient curve $h(\mathcal{H}/\langle\sigma\rangle)$. In particular, from Theorem 1, this number can be estimated using the genus $g(\mathcal{H}/\langle\sigma\rangle)$ of the quotient curve. In this section, we details how to construct an automorphism $\sigma \in \text{Aut}(\mathcal{H})$ of order ℓ , with ℓ satisfying conditions 1. and 2. above. After, we will see the influence of this choice on the genus of the quotient curve. A complete study on the automorphism group of the Hermitian curve can be found in [?]. In particular, they compute the class number as well as the genus of several quotient curve of the Hermitian curve, which will help us in choosing a good automorphism.

Seeking for an order ℓ automorphism.

Let us denote by $\mathcal{A} := \text{Aut}(\mathcal{H})$ the automorphism group of the Hermitian function field. It is isomorphic to the projective unitary group $\text{PGU}_3(\mathbb{F}_{q^2})$, and has order (see for example [Sti09])

$$\text{ord}(\mathcal{A}) = q_0^3(q_0^2 - 1)(q_0^3 + 1).$$

As we aim to find an automorphism σ of order ℓ satysfying the conditions in 7.4.1, we introduce the subgroup

$$\mathcal{A}(P_\infty) := \{\sigma \in \mathcal{A} \mid \sigma(P_\infty) = P_\infty\} \subseteq \mathcal{A},$$

consisting in all automorphisms fixing the point at infinity P_∞ in $\mathcal{H}(\mathbb{F}_{q_0^2})$. Let $F = \mathbb{F}_{q_0^2}(x, y) = \mathbb{F}_{q_0^2}(\mathcal{H})$ be the function field of \mathcal{H} , it is proven in [?] that such an automorphism acts as follows :

$$\begin{cases} \sigma(x) = ax + b \\ \sigma(y) = a^{q_0+1}y + ab^{q_0}x + c, \end{cases} \quad (12)$$

with $a \in \mathbb{F}_{q_0^2}^*$, $b \in \mathbb{F}_{q_0^2}$ and $b^{q_0+1} = c^{q_0} + c$ (see (2.2) in [?]). We have

$$\text{ord}(\mathcal{A}(P_\infty)) = q^3(q^2 - 1).$$

From 12, any automorphism $\sigma \in \mathcal{A}(P_\infty)$ can be identified to a triple a, b, c , with $a \in \mathbb{F}_{q_0^2}^*$, $b \in \mathbb{F}_{q_0^2}$ and $b^{q_0+1} = c^{q_0} + c$. For convenience, this automorphism will be denoted $\sigma = [a, b, c]$. The order of such a σ depends only on the order of a and the choice of c .

Lemma 6. (see [?], Lemma 4.1). *Let $\sigma = [a, b, c] \in \mathcal{A}(P_\infty)$, with $a \neq 1$. Then we have*

(i) *If $\text{ord}(a) \nmid q_0 + 1$, then $\text{ord}(\sigma) = \text{ord}(a)$;*

(ii) *If $\text{ord}(a) \mid q_0 + 1$ then*

$$\text{ord}(\sigma) = \begin{cases} \text{ord}(a) , & \text{if } c = \frac{ab^{q_0+1}}{a-1} \\ p \cdot \text{ord}(a) , & \text{otherwise} \end{cases}$$

where $p = \text{char}(\mathbb{F}_{q_0^2})$.

Now, let ℓ be an integer satisfying conditions 1. and 2. in 7.4.1, which also devides $q_0^2 - 1$. We chose randomly an element $a \in \mathbb{F}_{q_0^2}^*$ of order ℓ and $b \in \mathbb{F}_{q_0^2}$. If $\ell \mid q_0 + 1$, we choose $c = \frac{ab^{q_0+1}}{a-1}$, else we chose any c among the roots of $X^{q_0} + X - b^{q_0+1}$. From Lemma 6, we then gets an automorphism $\sigma = [a, b, c]$ of order ℓ .

The genus of $\mathcal{H}/\langle\sigma\rangle$.

The authors in [?] provide a formula to compute the genus of the curve $\mathcal{H}/\langle\sigma\rangle$ in our context.

Proposition 8. *Let $\sigma = [a, b, c] \in \mathcal{A}(P_\infty)$ be an automorphism of prime order $\ell > 2$. Then*

- (i) *If $\ell \mid (q_0 - 1)$, then $g(\mathcal{H}/\langle \sigma \rangle) = \frac{(q_0 - 1)q_0}{2\ell}$.*
- (ii) *If $\ell \mid (q_0 + 1)$ and $c = \frac{ab^{q_0+1}}{a-1}$, then $g(\mathcal{H}/\langle \sigma \rangle) = \frac{(q_0 - 1)(q_0 - (\ell - 1))}{2\ell}$.*

Proof. It is a particular case of [?], Theorem 4.4 □

Notice that since we want the quotient curve to have positive genus, ℓ should be strictly less than $q_0 + 1$. Using this Proposition and Theorem 1, we can estimate the class number $h(\mathcal{H}/\langle \sigma \rangle)$.

Corollary 4. *Let $\sigma = [a, b, c] \in \mathcal{A}(P_\infty)$ be an automorphism of prime order $\ell > 2$. Then we have*

- (i) *If $\ell \mid (q_0 - 1)$, then $h(\mathcal{H}/\langle \sigma \rangle) = \mathcal{O}\left(q_0^{\frac{q_0^2}{\ell}}\right)$.*
- (ii) *If $\ell \mid (q_0 + 1)$ and $c = \frac{ab^{q_0+1}}{a-1}$, then $h(\mathcal{H}/\langle \sigma \rangle) = \mathcal{O}\left(q_0^{\frac{q_0(q_0-\ell)}{\ell}}\right)$.*

We will see in annex B that the divisor class $h(\mathcal{H}/\langle \sigma \rangle)$ is an upper bound for the cost of the brute force algorithm. In our suggested parameters for the scheme (see section 7.4.4), this number will be large enough to reach a complexity larger than 2^{128} operations in \mathbb{F}_q .

7.4.3 Choice of the base field

In order to provide SSAG-codes over \mathbb{F}_q , defined on the Hermitian function field, we have to choose and extension \mathbb{F}_q of \mathbb{F}_q such that q^m is a square. Let us discuss the choice of q and m , and the related q_0 such that $q^m = q_0^2$.

- m should not be too large since it has a negative influence on the dimension of the code. In fact, for a fixed length n and a fixed divisor G , the dimension of the SSAG-code is lower bounded by $n - m(n - \dim(G))$. As a result, if m is too big, the rate (k/n) of the SSAG might be too low.
- Actually, the same remark holds for the choice of q_0 . In fact, recall that the genus of the Hermitian function fields is $g = \frac{q_0(q_0-1)}{2}$. Then the same estimation on the dimension k of the SSAG code leads to

$$k \geq n - m(n - \dim(G)) = n - m(n - \deg(G) + g - 1),$$

that is q_0 should not be too large as well.

- On the other hand, the choice $q = q_0$ and $m = 2$, which could be a good choice about the two previous points, is not encouraged. The formal argument in this direction is that the smaller the degree extension m is, the closer the structure of the SSAG code is from the AG one. Since AG-codes have been broken in polynomial time (see [?]), it might be possible to adapt this attack to SSAG-codes if they are too close to AG ones. In section 7.4.4, we will still give some parameters with $m = 2$ because it provides the best key sizes. However, we warn the reader that it could be the weakest keys.

7.4.4 Parameters

A Retrieving the equation of a cover : complexity analysis

In this first Annex, we will present a formal algorithm that describes the attack proposed in Section 5.2 in the special case of a Kummer covering of \mathbb{P}^1 . Recall that in this special case, we are led to solve linear systems of the form :

$$\begin{pmatrix} A(\xi) \\ H \cdot \mathbf{D}_1 \\ \vdots \\ H \cdot \mathbf{D}_s \end{pmatrix} \cdot \mathbf{y}^T = 0, \quad (\Delta(\xi))$$

that is a system with $s(n - k) + n$ equations for n unknowns; where $s = \dim(D)$ (see (4)) and n, k are respectively the length and dimension of the public SSAG-code. Let us suppose that a plane model of the Kummer covering is given by

$$y^\ell = f(x), \quad f \in \mathbb{F}_{q^m}[T], \quad m = \deg(f).$$

The following proposition gives the complexity of Algorithm 1 below

Proposition 9. *Let n, k be the length and the dimension of the public SSAG code. Let $r := n/\ell$ be the number of orbits in \mathcal{P} . If $r \geq m + 1$, then Algorithm 1 find a equation of the cover, as well as the secret structure of the public SSAG-code in $\mathcal{O}(\varphi(\ell)(n^\omega + n^{\omega-1}s(n - k)))$ over \mathbb{F}_{q^m} .*

Proof. [ref calcul formel ?] [?]

Recall that the complexity of solving a linear system with k equations and n unknowns is in $\mathcal{O}(n^{\omega-1}k)$ operations over the base field, where ω is the exponent of linear algebra. As a result, the cost of line 9. is $\mathcal{O}(n^\omega + n^{\omega-1}s(n - k))$ operations over \mathbb{F}_{q^m} . Since we have to seek for the correct root of unity ξ , this step might be repeated at most $\varphi(\ell)$ -times, where φ is the Euler totient function. Next, one have to realise one Lagrange's interpolation at line 13., in order to recover a defining equation of the Kummer cover. In particlar, let m denote the degree of the polynomial f we have to build. At the step of the algorithm, we have recovered all the points in \mathcal{P} , and thus if the number r of orbits in \mathcal{P} is larger that $m + 1$, Lagrange's interpolation find a unique polynomial f of degree m such that a plane model of the cover is given by $y^\ell = f(x)$ in $\mathcal{O}(m^2)$ operations over \mathbb{F}_{q^m} . Note that this step is negligible compared to the cost of line 9. Finally, the last step we have to care about is the step 17. In fact, at this stage of the algorithm, the whole cover is known and it remains to compute the pullback of the invariant divisor. As for the support, we need to recover the y -coordinates of points in $\text{Supp}(G)$. This can be done by finding roots of several polynomials. Indeed, from Kummer's theorem (see [Sti09], Theore 3.3.7), if $x(Q)$ denotes the x -coordinate of a point $Q \in \text{Supp}(\tilde{G})$, then the y -coordinates of then extensions of Q in $\text{Supp}(G)$ are exactly the roots of the polynomial $P_Q(T) = T^\ell - f(x(Q)) \in \mathbb{F}_{q^m}[T]$. This step can be done by factorizing each polynomial P_Q using Berlekamp algorithm, whose cost is $\mathcal{O}(\ell^\omega + q^m \ell^2)$ operations over \mathbb{F}_{q^m} . In any practical cases, the Length of the public code is larger that the cardinality of the base field, that is $n > q^m$ and thus this step is also negligible. As a result, the total cost of algorithm 1 is in $\mathcal{O}(\varphi(\ell)(n^\omega + n^{\omega-1}s(n - k)))$ over \mathbb{F}_{q^m} . \square

Note that this algorithm can be used in the case of Artin-Schreier covers of the projective line, by only changing a few lines. In fact, in the Artin-Schreier setup, we have to solve at most $p = \#(\mathbb{F}_p)$ linear system of the form (7), whose total cost is in $\mathcal{O}(p(n^\omega + n^{\omega-1}s(n - k)))$ over \mathbb{F}_{q^m} . As in Algorithm 1, this is the total cost of the corresponding algorithm since others steps are exactly the same.

Remark 12. [si la courbe quotient n'est pas P^1]

Remark 13. [cas Galoisien]

Algorithm 1 : Security reduction in Kummer case**Inputs**

- A parity check matrix H_{pub} of the public code;
- The full invariant structure, that is $\tilde{P} = (P_1, \dots, P_r)$ and \tilde{G} ;
- The quasi-cyclicity order ℓ and the degree $m = \deg(f)$.

Outputs

- The polynomial f ;
 - The secret structure \mathcal{P} and G .
1. $x \leftarrow \underbrace{(x(P_1), \dots, x(P_1), \dots, x(Q_r), \dots, x(Q_r))}_{\ell \text{ fois}}$
 2. $D \leftarrow \tilde{G} - \lceil d/\ell \rceil \cdot P_\infty \in Div(\mathbb{P}^1)$
 3. $s \leftarrow \dim(D)$
 4. $M \leftarrow$ set of primitive ℓ -th roots of unity
 5. $\text{cpt} := 0$
 6. while $\text{cpt} := 0$ do
 7. $\xi \xleftarrow{\$} M$
 8. $\text{Exclude}(M, \xi)$
 9. $S \leftarrow \text{Solve}(\Delta(\xi))$
 10. if $\dim(S) = 1$ then
 11. $\text{cpt} := 1$
 12. $y^* \xleftarrow{\$} S \setminus \{0\}$
 13. $f \leftarrow \text{Interpolate}(x, y^*)$
 14. $\mathcal{P} \leftarrow \{P_{ij} = (x_{ij} : y_{ij} : 1)\}$
 15. end if
 16. end while
 17. $G \leftarrow \pi^*(\tilde{G})$
 18. return \mathcal{X}, \mathcal{P} and G

B Brute force Algorithm on the invariant code

References

- [Bar18] Elise Barelli. *On the security of short McEliece keys from algebraic and algebraic geometry codes with automorphisms*. PhD thesis, universite Paris-Saclay, 2018.
- [CMCP14] Alain Couvreur, Irene Marquez-Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry codes based public key cryptosystems. *Proc. IEEE Int. Symposium Inf. Theory- ISIT*, pages 1446–1450, 2014.
- [FOP⁺16a] Jean-Charles Faugere, Ayoub Otmani, Ludovic Perret, Frederic de Portzamparc, and Jean-Pierre Tillich. Folding alternant and goppa codes with non-trivial automorphism groups. *IEEE. Trans. Inform. Theory* **62**, pages 184–198, 2016.
- [FOP⁺16b] Jean-Charles Faugere, Ayoub Otmani, Ludovic Perret, Frederic de Portzamparc, and Jean-Pierre Tillich. Structural cryptanalysis of mceliece schemes with compact keys. *Des. Codes Cryptogr.* **79**, pages 87–112, 2016.
- [FOPT10] Jean-Charles Faugere, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of mceliece variants with compact keys. *Advances in Cryptology - EURO-CRYPT 2010, LNCS*, pages 279–298, 2010.
- [HP95] Tom Høholdt and Ruud Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory* **41**, pages 1589–1614, 1995.
- [Loi01] Pierre Loidreau. Codes derived from binary goppa codes. *Probl. Inf. Transm.* **37**, pages 91–99, 2001.
- [McE78] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report 44*, pages 114–116, 1978.
- [Sti09] Henning Stichtenoch. *Algebraic Function Fields and Codes*. Springer, 2nd edition edition, 2009.