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

Mathieu Lhotel
Université de Bourgogne Franche-Comté
January 18, 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 particulat, this shows that the security of such systems must rely on the security of the invariant code. We then propose a sheme 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 theoritic 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 to large for certain practical use cases. Many propositions were made in order to correct this, mostly bu considering codes with additional structure, e.g. quasy-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 ans 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 to 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 contremeasure to this atteck, 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 gives some classical notations and definitions what 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 knows 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 $\mathcal{Y} \to \mathcal{X}$, 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 vue, we will see that "structured codes on a curve" corresponds to "orbites of places of an algebraic function field under the action of an automorphism of the corresponding curve".

In Section 2, we will gives some classical notations and definitions what 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 elements, were $q = p^s$ 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.

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 $\nu_P : K \to \mathbb{Z}$, . The degree of the place P, denoted deg(P) is define as the finite integer $\deg(\mathrm{P}) := [\mathrm{O_P}/\mathrm{P} : \mathbb{F}_\mathrm{q}] < \infty$. The divisor group of K, denoted $Div(K)$, is the set of formal sums

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

where 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 $P \in \mathrm{Supp(A)}$ 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

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

The degree of a divisor is naturally defined by the formula

$$\deg(\mathrm{A}) = \sum_{\mathrm{P} \in \mathrm{Supp(A)}} \nu_\mathrm{P}(\mathrm{A}) \cdot \deg(\mathrm{P}).$$

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

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

and $l(A) := \dim_{\mathbb{F}_\mathrm{q}}(\mathcal{L}(\mathrm{A}))$ 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 extension $P \in \mathbb{P}_L$, denoted $P \mid Q$. The ramification index will as usual be denoted $e(P|Q)$.
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 $\pi : \mathcal{Y} \to \mathcal{X}$ is the corresponding separable morphism, we will consider the pullback of $Q \in \mathbb{P}_K$ as the divisor

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

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

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

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

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 $L = \mathbb{F}_{q^m}(\mathcal{X})$, $\mathcal{P} = \{P_1, ..., P_n\}$ be a set of n distincts places of degree 1 in L and $G \in Div(L)$ be a divisor sucht that* $\mathrm{Supp(G)} \cap \mathcal{P} = \emptyset$. *Let us also suppose that* $\deg(\mathrm{G}) < \mathrm{n}$. *Then we define the AG-code associated to the triple $(\mathcal{X}, \mathcal{P}, G)$ as the $\mathbb{F}_{q^m}$-vector space*

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

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 $\Sigma \subseteq Aut(L)$, and denote by $Orb_\Sigma(P)$ 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 choosen carefully, that is they are made of distincts 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 $\sigma \in Aut(L)$ 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.

3 Invariant code

Definition 3. *Given an AG-code $(C) = C_L(\mathcal{X}, \mathcal{P}, G)$ that is invariant under the action of an automorphism group $\Sigma \subseteq Aut(L)$, 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, wi 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 $\mathcal{X}/\Sigma$. Notice that in our context, the function field of the quotient curve is precisly 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 $\sigma \in Aut(L)$. If $c = Ev_\mathcal{P}(g) \in C_L(\mathcal{X}, \mathcal{P}, G)$ is such that $\sigma(c) = c$, then g is σ-invariant, ie. $g \circ \sigma = g$.*

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

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

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 $\deg(\mathrm{G}) < n$ 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. □

Proposition 1. *Let $G \in Div(L)$ be a divisor of L invariant by an automorphism $\sigma \in Aut(F)$. Then $L(G)^\sigma = L(\tilde{G})$ with $\tilde{G} \in Div(F^\sigma)$.*

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

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

that is

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

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 $i \in \{1, ..., s\}$, 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 $Q \in Orb_\sigma(Q_i)$, 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

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

Note that for every $i \in \{1, ..., s\}$, 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 $\tilde{G} := \sum_{i=1}^{s} \left\lfloor \frac{t_i}{e(Q_i|Q'_i)} \right\rfloor Q'_i \in Div(L^\sigma)$. 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

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

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

Theoreme 1 (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 $\Sigma \subseteq Aut(\mathcal{X})$. Then its invariant code is also an AG-code, defined on the quotient curve $\mathcal{X}/\Sigma$. 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 1. □

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 $\mathcal{X} \to \mathcal{X}/\Sigma$.

Remark 2. Let $\mathcal{C}$ be an AG-code on $\mathcal{X}$ stable under $\Sigma \subseteq Aut(\mathcal{X})$, 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 $SSAG_q(\mathcal{X}, \mathcal{P}, G)$ be a subfield subcode of an AG-code and Σ acting on it. Then*

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

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

Proof. Immediate consequence of Theorem 1 and Remark 2. □

4 Recovering the equation of a curve

Throught 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

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

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

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

The key part of our attack will be to recover the 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 4. *For a divisor $G \in Div(L)$, let us denote by $\tilde{G} \in Div(K)$ 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 $A \in Div(K)$, 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 $\tilde{\mathcal{P}} = \{Q_1, ..., Q_r\}$, that totally split in L/K. For any $1 \leq i \leq r$, one then have

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

Denote by $\mathcal{P} = \{P_{i,j} \mid 1 \leq i \leq r \ and \ 1 \leq j \leq \ell\}$ the set of all extensions of the Q_i's in L. Let $G \in Div(L)$ be a divisor of degree d smaller that $n = \ell r$ such that $\mathrm{Supp(G)} \cap \mathcal{P} = \emptyset$. Also, we denote by $\tilde{G} \in Div(K)$ its related divisor according to definition 1. Note that this implies that $\mathrm{Supp}(\tilde{\mathrm{G}}) \cap \tilde{\mathcal{P}} = \emptyset$ 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 $\Sigma \subseteq Aut(\mathcal{Y})$. We then gets a cover $\mathcal{Y} \to \mathcal{Y}/\Sigma$, 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
$$\mathcal{C} = SSAG_q(\mathcal{Y}, \mathcal{P}, G);$$
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 $\tilde{G} \in Div(K)$ (that is exactly the invariant code);
3. We know how the morphism $\pi : \mathcal{Y} \to \mathcal{X}$ 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
$$\widetilde{(y)_\infty^L} \in Div(K).$$
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 rationnal 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, forall $1 \leq i \leq r$ 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

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

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 $\mathcal{C} = SSAG_q(\mathcal{Y}, \mathcal{P}, G)$ satisfies

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

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 know 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 $\pi : \mathcal{Y} \to \mathcal{X}$, 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 :

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

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

$$(\pi^* f)^L \geq -\pi^* \left(\tilde{G} - \widetilde{(y)_\infty^L} \right) = (y)_\infty^L - G \ , \quad \textit{using remark 4.}$$

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. □

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 explicitely 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

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

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

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

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

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

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

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

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 (cf. theorem 1) twice gives

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

and

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

Since $\deg(\tilde{\mathrm{G}}) = \lfloor \frac{\deg(\mathrm{G})}{\ell} \rfloor$, 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 $\pi : \mathcal{Y} \to \mathcal{X}$ 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 $\deg(\mathrm{G}) = \mathrm{d_{max}}$.

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

$$(h)^L_\infty \leq (y)^L_\infty$$

holds. Then the evaluation vector $\boldsymbol{h} := (h_{i,j})_{i,j}$,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 in proposition 1, and a function $g \in \mathcal{F}$. By definition of $\mathcal{F}$, one have

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

Thus we have

$$(\pi^* g \cdot h)^L = (\pi^* g)^L + (h)^L \geq ((y)^L_\infty - G) + (h)^L = (h)^L_0 + \underbrace{((y)^L_\infty - (h)^L_\infty)}_{\geq 0} - G \geq -G,$$

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 explicitely decide whenever a function gives a solution or not, depending on the divisor $(y)^L_\infty$. 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 3, 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 rationals places. Note that this case has already been treated in [Bar18] (section 5), we will come back at it in section 4.2.

In what follows, we will see that we can take a general classes of curves as the quotient curve $\mathcal{X}$. In particular, from hypthesis 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 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 5. *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*

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

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

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

Lemma 4. *Let $\mathcal{X}$ be a curve with separated variables, with function field $K = \mathbb{F}_q(x, \alpha)$ 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 $\pi : \mathcal{X} \to \mathbb{P}^1(\mathbb{F}_{q^m})$. 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

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

and since $(\deg(F_1), \deg(\mathrm{F_2})) = 1$, 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. □

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 $\mathcal{Y} \to \mathcal{X} \to \mathbb{P}^1(\mathbb{F}_{q^m})$, giving us a good way to describe the divisor $\widetilde{(y)_\infty^L} \in Div(K)$.

5.2 Kummer covering

Let $\mathcal{X}$ be a curve over $\mathbb{F}_{q^m}$ with separated variables (see. definition 2), those function field is given by $K = \mathbb{F}_{q^m}(x, \alpha)$, with

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

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

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

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

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

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 $\mathcal{Y} \to \mathcal{X}$ 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 $Gal(L/K)$. 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 3. *We have*

$$(x)_\infty^L = \ell \cdot \deg(\mathrm{F}_1) \cdot \mathrm{P}_\infty,$$
$$(\alpha)_\infty^L = \ell \cdot \deg(\mathrm{F}_2) \cdot \mathrm{P}_\infty,$$

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 3), 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 2 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

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

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

$$\begin{aligned} \pi^* D &= \pi^* \left(G - \widetilde{\left\lceil \frac{m}{\ell} \right\rceil \cdot Q_\infty} \right) \\ &= \pi^* \tilde{G} - \left\lceil \frac{m}{\ell} \right\rceil \cdot \pi^* \widetilde{Q_\infty} \\ &= G - n \cdot \left\lceil \frac{m}{\ell} \right\rceil \cdot P_\infty \quad (\textit{using remark } 4) \\ &\leq G - m \cdot P_\infty \\ &= G - (y)_\infty^L, \end{aligned}$$

the last equality coming from proposition 2. Moreover, this choice of D is optimal (ie. the biggest, see. Definition 1) since m/ℓ can not be an integer (recall that m and ℓ are coprime). □

Note that the divisor D in the above corollary is know in our context from the hypothesis p.10, and thus one can consctruct 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 easyly 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 2, and in particular the description of the pole divisors of x and α, one easyly see that

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

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

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

holds.

Since we have found other solutions, one now need to choose the vector $\mathbf{y}$ amoung 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 $\tilde{\mathcal{P}} = \{Q_1, ..., Q_r\} \in \mathbb{P}_K$, then elements of $\mathcal{P}$ at indices $(i-1)\ell + 1, ..., i\ell$ correspond to the ℓ extensions of Q_i in L (for every $1 \leq i \leq r$). Let us consider the following bloc matrices

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

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, if we recall the equation (5) from section 3.2, we get that $\mathbf{y}$ satisfies

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

The relation (6) is enough to recover $\mathbf{y}$ since the other solutions of (5) (given above) doesn't have 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 n, 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 $\varphi(\ell)$ s 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.

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

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

and $(\deg(F_1), \deg(F_2)) = 1$.
Here, we will consider an Artin-Schreier cover of the curve $\mathcal{X}$. Let $p := char(\mathbb{F}_{q^m})$ denote the characteristic of the base field $\mathbb{F}_{q^m}$. Consider the extension $L = K(y)$, with

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

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

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

In this case, the hypotheses of our procedure are the same as in section 4.2, 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 proove that

Proposition 4. *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 2 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

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

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

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

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 :

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

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 recall the equation (5) from section 3.2, we get that the vector $\mathbf{y}$ we are looking for satisfies

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

The above relation (7) allows us to isolate $\mathbf{y}$, since the other solutions do not satifies 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.

Complexity

5.4 Generalisation to solvable Galois covering

Above, we showed that our procedure could apply 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 4.2 and 4.3 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 $\mathcal{Y} \to \mathbb{P}^1(\mathbb{F}_{q^m})$ (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

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

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_{n-1}.

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

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

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

Let us know 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 AG-code on $\mathcal{Y}$ that is stable under the action of $Gal(L/\mathbb{F}_{q^m}(x))$, 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 $\tilde{P}$ 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 4.3 if $\ell_i = p$ and section 4.2 otherwise. (see [Sti09], annex A.13 for a caracterisation of cyclic extensions of function field).

Remark 8. The hypothesis that we know the action of $Gal(L/\mathbb{F}_{q^m}(x))$ 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 detailled example, let ℓ_1, ℓ_2 be two primes, that are coprime with $p = char(\mathbb{F}_{q^m})$. Consider a curve $\mathcal{Y}$ over $\mathbb{F}_{q^m}$, with function field $L = \mathbb{F}_{q^m}(x, y)$, such that

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

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 $S \subseteq Gal(L/\mathbb{F}_{q^m}(x))$ its unique ℓ_2-Sylow (that is of course normal). Let $K = L^S$. Then we have :

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

Now, suppose we are given a parity check matrix of a code $C_L(\mathcal{Y}, \mathcal{P}, G)$ that is stable under $Gal(L/\mathbb{F}_{q^m}(x))$, together with its invariant code $C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$. We also suppose that we now how $Gal(L/\mathbb{F}_{q^m}(x))$ 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
$$\alpha^k = b(x) \ , \ b \in \mathbb{F}_{q^m}[T].$$
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
$$D_1 := \tilde{G} - \widetilde{(\alpha)_\infty^K} = \tilde{G} - \left\lceil \frac{m_1}{\ell_1} \right\rceil \cdot R_\infty \in \mathbb{P}_{\mathbb{F}_{q^m}(x)},$$
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 $\boldsymbol{\alpha}$. 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 $S \subseteq Gal(L/\mathbb{F}_{q^m}(x))$ of order ℓ_2 (ie. its unique ℓ_2-Sylow). This matrix can be constructed from one of $\mathcal{C}$, by deleting the good columns (ie. we keep only one column for each orbit under T, since they corresponds to redundant informations.
At this point, assume that we recovered the vector $\boldsymbol{\alpha}$ using section 4.2.

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 4.2). In particular, we know at this point a set $\mathcal{P}'$ that corresponds to extensions of places in $\tilde{\mathcal{P}}$ in K, as well as the divisor $G' := \pi^*\tilde{G}$, where $\pi : \mathcal{X} \to \mathbb{P}^1(\mathbb{F}_{q^m})$. Moreover, the subcode of $\mathcal{C}$ that is invariant under the ℓ_2-Sylow S of $Gal(L/\mathbb{F}_{q^m}(x))$ is given by
$$C_L(\mathcal{X}, \mathcal{P}', G').$$

3. 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
$$D_2 := G' - \widetilde{(y)_\infty^L} = G' - \left\lceil \frac{m_2}{\ell_2} \right\rceil \cdot Q_\infty \in \mathbb{P}_K,$$
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 4.2, it allows us to recover the defining equation of $\mathcal{Y}$, as a cover of $\mathcal{X}$.

4. 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.

1. For solvable automorphism group, there are 2 cases for each divisor ℓ of $\#Aut(L/\mathbb{F}_{q^m}(x))$:

   - If ℓ is prime to $p = char(\mathbb{F}_{q^m})$, 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 $l = p$, 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 conveniant.

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 works 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 intersting to focus on covers where the support of the divisor of poles of y is more complicated, that is made of more that 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 theoritic point of vue, our procedure gives "negatives" results, in the sense that is 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 hidding 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 rationnal points (that is $N(\mathcal{H}) = q_0^3 + 1$). It allows us to consider longs codes, and thus more flexibility. Moreover, the automorphism group of $\mathcal{H}$ is very large and has been well-studied (see for example [Sti09]); which permets us to chose a good automorphism σ acting on our code (it will turns to be really important later on).

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 $\mathcal{P} := \bigsqcup_{i=1}^{n_0} Orb_\sigma(P_i)$ be a support made of n_0 distincts orbites under the action of σ;
- let $s \in \mathbb{N}^*$ and $G = \sum_{i=1}^{s} t_i \sum_{Q \in Orb_\sigma(Q_i)} Q$ 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

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

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 $\mathrm{G_{pub}} = (\mathrm{I_k}|\mathrm{M})$ be a systematic generator matrix of $\mathcal{C}_{\text{pub}}$, where M is an ℓ-blocks-circulant matrix (possible since the code is QC). Thus $\mathrm{G_{pub}}$ can entirely be described by the set of rows

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

M_i being the i-th row of M.

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

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

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

where $\mathbf{e} \in \mathbb{F}_\mathrm{q}^\mathrm{n}$ 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 $\mathrm{G_{pub}}$, 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 easyly.

In what follow, we will describe somes 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.

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

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

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 C_{inv}. Using the attack of section 4., 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

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

To construct an algebric system, we use the fact that by duality of AG-codes, one gets

$$inserersuite$$

7.3 Brute force on the invariant code

7.4 Suggested parameters

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.

[HP95] Tom Høholft 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.