On the security of Some Compact Keys for McEliece Scheme

Élise Barelli

INRIA Saclay and LIX, CNRS UMR 7161 École Polytechnique,
91120 Palaiseau Cedex

June 16, 2017

McEliece scheme

It is the first public key cryptosystem based on error-correcting codes.

Advantages:

- Fast encryption and decryption.
- Candidate for post-quantum cryptography

Drawback:

- Large key size

McEliece scheme

It is the first public key cryptosystem based on error-correcting codes.

Advantages:

- Fast encryption and decryption.
- Candidate for post-quantum cryptography

Drawback:

- Large key size

Structural attacks

$\rightarrow$ Let $\mathcal{F}$ be any family of linear codes.

$\rightarrow$ Let G be a **random looking** generator matrix of a code $\mathcal{C} \in \mathcal{F}$.

From G, can we recover the structure of the code $\mathcal{C}$?

Some propositions

- Binary Goppa codes (McEliece, 1978)
  $\rightarrow$ No structural attack

Some propositions

- Binary Goppa codes (McEliece, 1978)
  $\rightarrow$ No structural attack
- Generalised Reed-Solomon (GRS) (Niederreiter, 1986)
  $\rightarrow$ [Sidelnikov, Shestakov,1992]

Some propositions

- Binary Goppa codes (McEliece, 1978)
  - $\rightarrow$ No structural attack
- Generalised Reed-Solomon (GRS) (Niederreiter, 1986)
  - $\rightarrow$ [Sidelnikov, Shestakov,1992]
- Algebraic-geometry (AG) codes (Janwa, Moreno, 1996)
  - $\rightarrow$ [Faure, Minder, 2009]
  - $\rightarrow$ [Couvreur, Márquez-Corbella, Pellikaan, 2014]

Some propositions

- Binary Goppa codes (McEliece, 1978)
  $\rightarrow$ No structural attack
- Generalised Reed-Solomon (GRS) (Niederreiter, 1986)
  $\rightarrow$ [Sidelnikov, Shestakov,1992]
- Algebraic-geometry (AG) codes (Janwa, Moreno, 1996)
  $\rightarrow$ [Faure, Minder, 2009]
  $\rightarrow$ [Couvreur, Márquez-Corbella, Pellikaan, 2014]
- Concatenation of AG codes (Janwa, Moreno, 1996)
  $\rightarrow$ [Sendrier,1998] (for all concatenated codes)

Some propositions

- Binary Goppa codes (McEliece, 1978)
  $\rightarrow$ No structural attack
- Generalised Reed-Solomon (GRS) (Niederreiter, 1986)
  $\rightarrow$ [Sidelnikov, Shestakov,1992]
- Algebraic-geometry (AG) codes (Janwa, Moreno, 1996)
  $\rightarrow$ [Faure, Minder, 2009]
  $\rightarrow$ [Couvreur, Márquez-Corbella, Pellikaan, 2014]
- Concatenation of AG codes (Janwa, Moreno, 1996)
  $\rightarrow$ [Sendrier,1998] (for all concatenated codes)
- Subfied subcodes of AG codes (Janwa, Moreno, 1996)
  $\rightarrow$ No structural attack

Some propositions with compact keys

- Quasi-cyclic alternant codes (Berger, Cayrel, Gaborit, Otmani, 2009)
- Quasi-dyadic alternant codes (Misoczki, Baretto, 2009)

Structural attacks:

→ [Faugère, Otmani, Perret, Tillich, 2010]

→ [Faugère, Otmani, Perret, Portzamparc, Tillich, 2015]

→ [B., 2017]

Functions on a curve $\mathcal{X}$

We consider an algebraic curve $\mathcal{X} \subset \mathbb{P}^2(\mathbb{F}_{q^m})$, with affine equation:

$$F(x, y) = 0.$$

The function field over $\mathbb{F}_{q^m}$ of $\mathcal{X}$, denoted by $\mathbb{F}_{q^m}(\mathcal{X})$ is the fraction field of $\mathbb{F}_{q^m}[x, y]/(F)$.

A divisor of $\mathcal{X}$ is a formal sum, with integer coefficients, of points of $\mathcal{X}$. For $g \in \mathbb{F}_{q^m}(\mathcal{X})$, the principal divisor of g, denoted by (g), is defined as the formal sum of zeros and poles of g, counted with multiplicity.

We denote by $L(G) := \{g \in \mathbb{F}_{q^m}(\mathcal{X}) \mid (g) \geq -G\} \cup \{0\}$, the Riemann-Roch space associated to a divisor G.

AG codes on $\mathcal{X}$

Definition

Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of n distinct rational points of $\mathcal{X}$ and G be a divisor, then the AG code $C_L(\mathcal{X}, \mathcal{P}, G)$ is defined by:

$$C_L(\mathcal{X}, \mathcal{P}, G) := \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in L(G)\}.$$

$$\begin{array}{lcc} \mathbb{F}_{q^m} & C_L(\mathcal{X}, \mathcal{P}, G) \xleftrightarrow{\text{Dual}} & C_L(\mathcal{X}, \mathcal{P}, G') \\ & & \Big| \text{Subfield Subcode} \\ \mathbb{F}_q & & C_L(\mathcal{X}, \mathcal{P}, G') \cap \mathbb{F}_q^n \end{array}$$

$\mathcal{A}_r(\mathcal{X}, \mathcal{P}, G) := C_L(\mathcal{X}, \mathcal{P}, G') \cap \mathbb{F}_q^n$, where $r = \dim(C_L(\mathcal{X}, \mathcal{P}, G))$.

AG codes on $\mathbb{P}^1$

Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of n distinct points of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ and G be a divisor, then the AG code $C_L(\mathbb{P}^1, \mathcal{P}, G)$ is defined by:

$$C_L(\mathbb{P}^1, \mathcal{P}, G) := \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in L(G)\}.$$

AG codes on $\mathbb{P}^1$

Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of n distinct points of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ and G be a divisor, then the AG code $C_L(\mathbb{P}^1, \mathcal{P}, G)$ is defined by:

$$C_L(\mathbb{P}^1, \mathcal{P}, G) := \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in L(G)\}.$$

Proposition

The AG code $C_L(\mathbb{P}^1, \mathcal{P}, G)$ is the GRS code :

$$\mathrm{GRS}_k(x, y) := \{(y_1 f(x_1), \dots, y_n f(x_n)) \mid f \in \mathbb{F}_{q^m}[X]_{<k}\}.$$

where:

- $\rightarrow$ $\mathcal{P} := \{(x_i : 1) | \ i \in \{1, \dots, n\}\}$,
- $\rightarrow$ $G := (k-1)P_\infty - (g)$,

with $g \in \mathbb{F}_{q^m}(\mathbb{P}^1)$ a function such that for all $i \in \{1, \dots, n\}$, $g(x_i) = y_i \neq 0$.

Automorphim group of $\mathbb{P}^1$

$\mathrm{PGL}_2(\mathbb{F}_{q^m})$ is the automorphism group of the projective line $\mathbb{P}^1$ defined by:

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

Automorphim group of $\mathbb{P}^1$

$\mathrm{PGL}_2(\mathbb{F}_{q^m})$ is the automorphism group of the projective line $\mathbb{P}^1$ defined by:

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

Remark

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

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

Where the elements a, b, c and d are defined up to a multiplication by a nonzero scalar.

Support and divisor σ-invariant

Let σ be an automorphism of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$.

For a point $Q \in \mathbb{P}^1$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

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

where the points $Q_i \in \mathbb{P}^1_{\mathbb{F}_{q^m}}$ are pairwise distinct with trivial stabilizer subgroup.

Support and divisor σ-invariant

Let σ be an automorphism of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$.

For a point $Q \in \mathbb{P}^1$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

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

where the points $Q_i \in \mathbb{P}^1_{\mathbb{F}_{q^m}}$ are pairwise distinct with trivial stabilizer subgroup.
We define the **divisor**:

$$G := t \sum_{j=1}^{\ell} \sigma^j(R), \tag{2}$$

with R a point of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$, $t \in \mathbb{Z}$ and $\deg(G) = \ell t$.

Permutations of $\mathcal{A}_r(\mathbb{P}^1, \mathcal{P}, G)$

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

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

Then $\tilde{\sigma}$ is also a permutation of $\mathcal{A} := \mathcal{C}^{\perp} \cap \mathbb{F}_q^n$.

Equivalence classes of $\mathrm{PGL}_2(\mathbb{F}_{q^m})$

Lemma

Let $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ be an automorphism on $\mathbb{P}^1$. Then $\sigma' := \rho \circ \sigma \circ \rho^{-1}$ induces the same permutation on $\mathcal{C}$ as σ.

Equivalence classes of $\mathrm{PGL}_2(\mathbb{F}_{q^m})$

Lemma

Let $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ be an automorphism on $\mathbb{P}^1$. Then $\sigma' := \rho \circ \sigma \circ \rho^{-1}$ induces the same permutation on $\mathcal{C}$ as σ.

Three cases are possible, depending on the eigenvalues of the matrix $M := Mat(\sigma)$:

1. $M \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, with $b \in \mathbb{F}_{q^m}$,
2. $M \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, with $a \in \mathbb{F}_{q^m}$ or $a \in \mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$.

Invariant and folded codes: definitions

Let $\mathcal{C}$ be a linear code and $\sigma \in Perm(\mathcal{C})$ of order ℓ. Consider:

$$\varphi\colon c \in \mathcal{C} \mapsto \sum_{i=0}^{\ell-1} \sigma^i(c).$$

The *folded* code of $\mathcal{C}$ is defined by

$$\mathrm{Fold}_\sigma(\mathcal{C}) := \mathrm{Im}(\varphi)$$

and the *invariant* code of $\mathcal{C}$ is defined by

$$\mathcal{C}^\sigma := \ker(\sigma - \mathrm{Id}).$$

Invariant and folded codes: definitions

Let $\mathcal{C}$ be a linear code and $\sigma \in Perm(\mathcal{C})$ of order ℓ. Consider:

$$\varphi\colon c \in \mathcal{C} \mapsto \sum_{i=0}^{\ell-1} \sigma^i(c).$$

The *folded* code of $\mathcal{C}$ is defined by

$$\mathrm{Fold}_\sigma(\mathcal{C}) := \mathrm{Im}(\varphi)$$

and the *invariant* code of $\mathcal{C}$ is defined by

$$\mathcal{C}^\sigma := \ker(\sigma - \mathrm{Id}).$$

Proposition

The codes $\mathrm{Fold}_\sigma(\mathcal{C})$ and $\mathcal{C}^\sigma$ are subcodes of $\mathcal{C}$ and:

$$\mathrm{Fold}_\sigma(\mathcal{C}) \subseteq \mathcal{C}^\sigma.$$

If Char $(\mathbb{F}_{q^m}) \nmid \ell$ then $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$.

Invariant code of $\mathcal{A}_r(\mathbb{P}^1, \mathcal{P}, G)$

If $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$, σ-invariant then:

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

Invariant code of $\mathcal{A}_r(\mathbb{P}^1, \mathcal{P}, G)$

If $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$, σ-invariant then:

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

Theorem

Let $C_L(\mathbb{P}^1, \mathcal{P}, G) \subseteq \mathbb{F}_{q^m}^n$ be a σ-invariant AG code, with $\sigma \in \mathrm{PGL}_2(\mathbb{P}^1_{\mathbb{F}_{q^m}})$ of order ℓ and $\mathcal{P}$ and G defined as (1) and (2). Then the invariant code $C_L(\mathbb{P}^1, \mathcal{P}, G)^\sigma$ is a GRS code of dimension k/ℓ and length n/ℓ.

Corollary

The invariant code $\mathcal{A}_r(\mathbb{P}^1, \mathcal{P}, G)^\sigma$ is an alternant code of order r/ℓ and length n/ℓ.

Lemma

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

Lemma

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

Let $G := t \sum_{j=1}^{\ell} \sigma^j(R)$, with R a rational point of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ and $t \in \mathbb{Z}$. We denote:

$$\sigma^j(R) := (\gamma_j : \delta_j), \text{ for } j \in \{0, \ldots, \ell - 1\}.$$

Lemma

With the previous notation, any $f \in L(G)$ *can be written as:*

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

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

Case σ trigonalizable over $\mathbb{F}_{q^m}$:

$$\begin{array}{cccc} \sigma: & \mathbb{P}^1_{\mathbb{F}_{q^m}} & \to & \mathbb{P}^1_{\mathbb{F}_{q^m}} \\ & (X:Y) & \mapsto & (X+bY:Y) \end{array}$$

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

Case σ diagonalizable over $\mathbb{F}_{q^m}$:

$$\begin{array}{cccc} \sigma: & \mathbb{P}^1_{\mathbb{F}_{q^m}} & \to & \mathbb{P}^1_{\mathbb{F}_{q^m}} \\ & (X:Y) & \mapsto & (aX:Y), \end{array}$$

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

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$:

$$\begin{array}{cccc} \sigma: & \mathbb{P}^1_{\mathbb{F}_{q^{2m}}} & \to & \mathbb{P}^1_{\mathbb{F}_{q^{2m}}} \\ & (X:Y) & \mapsto & (aX:Y), \end{array}$$

with $a \in \mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$.

Case σ trigonalizable over $\mathbb{F}_{q^m}$

Proposition

If $F(X + bY, Y) = F(X, Y)$*, then*

$$F(X, Y) = R(X^p - b^{p-1}XY^{p-1}, Y^p)$$

with $R \in \mathbb{F}_q[X, Y]$ *a homogeneous polynomial of degree* t*.*

Case σ trigonalizable over $\mathbb{F}_{q^m}$

Proposition

If $F(X + bY, Y) = F(X, Y)$, *then*

$$F(X, Y) = R(X^p - b^{p-1}XY^{p-1}, Y^p)$$

with $R \in \mathbb{F}_q[X, Y]$ *a homogeneous polynomial of degree* t.

We denote $\sigma^j(P_i) := (\alpha_{i\ell+j} : \beta_{i\ell+j})$, for $i \in \{0, \ldots, \frac{n}{\ell} - 1\}$, $j \in \{0, \ldots, \ell - 1\}$.

Proposition

The code $C_L(\mathbb{P}^1, \mathcal{P}, G)^\sigma$ *is the GRS code* $C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$, *with:*

- $\tilde{P}_i = (\alpha_i^p - b^{p-1}\alpha_i\beta_i^{p-1} : \beta_i^p)$,
- $\tilde{G} = t(\tilde{R})$, *where* $\tilde{R} = \left((-1)^{p-1}\prod_{j=0}^{p-1}\gamma_j : \prod_{j=0}^{p-1}\delta_j\right)$.

Case σ diagonalizable over $\mathbb{F}_{q^m}$

Proposition

If $F(aX, Y) = F(X, Y)$, then

$$F(X, Y) = R(X^\ell, Y^\ell)$$

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

Case σ diagonalizable over $\mathbb{F}_{q^m}$

Proposition

If $F(aX, Y) = F(X, Y)$, then

$$F(X, Y) = R(X^\ell, Y^\ell)$$

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

Proposition

The code $(C_L(\mathbb{P}^1, \mathcal{P}, G))^\sigma$ is the GRS code $C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$, with

- $\tilde{P}_i = (\alpha_i^\ell : \beta_i^\ell)$,
- $\tilde{G} = t\tilde{R}$, *where* $\tilde{R} = \left((-1)^{\ell-1} \prod_{j=0}^{\ell-1} \gamma_j : \prod_{j=0}^{\ell-1} \delta_j\right)$.

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Idea

We extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. We consider $\mathcal{C} \otimes \mathbb{F}_{q^{2m}} := \mathrm{Span}_{\mathbb{F}_{q^{2m}}}(\mathcal{C})$, we have:

$$\mathcal{C} \otimes \mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in L_{\mathbb{F}_{q^{2m}}}(G)\}.$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Idea

We extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. We consider $\mathcal{C} \otimes \mathbb{F}_{q^{2m}} := \mathrm{Span}_{\mathbb{F}_{q^{2m}}}(\mathcal{C})$, we have:

$$\mathcal{C} \otimes \mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in L_{\mathbb{F}_{q^{2m}}}(G)\}.$$

$$\begin{tikzcd} \mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} \arrow[r, "\mathrm{Inv}_\sigma"] & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma \\ \mathbb{F}_{q^m} & \mathcal{C} \arrow[u, hook, "\text{Sub. Sub.}"] \arrow[r, "\mathrm{Inv}_\sigma"] & \mathcal{C}^\sigma \arrow[u, hook] \end{tikzcd}$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Idea

We extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. We consider $\mathcal{C} \otimes \mathbb{F}_{q^{2m}} := \mathrm{Span}_{\mathbb{F}_{q^{2m}}}(\mathcal{C})$, we have:

$$\mathcal{C} \otimes \mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in L_{\mathbb{F}_{q^{2m}}}(G)\}.$$

$$\begin{tikzcd}
\mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} \arrow[r, "\mathrm{Inv}_\sigma"] & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})_{\mathbb{F}_{q^{2m}}} \\
\mathbb{F}_{q^m} & \mathcal{C} \arrow[u, hook, "\text{Sub. Sub.}"] \arrow[r, "\mathrm{Inv}_\sigma"] & \color{red}{\mathcal{C}^\sigma} \arrow[u, hook]
\end{tikzcd}$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

- $\rightarrow$ $\mathcal{C} \otimes \mathbb{F}_{q^{2m}}$ has a basis in $\mathbb{F}_{q^m}^n$.
- $\rightarrow$ Here $p \nmid \ell$ then $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$. So $(\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma$ has also a basis in $\mathbb{F}_{q^m}^n$.

$$\begin{tikzcd}
\mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} \arrow[r, "\mathrm{Inv}_\sigma"] & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})_{\mathbb{F}_{q^{2m}}} \\
\mathbb{F}_{q^m} & \mathcal{C} \arrow[u, hook, "\text{Sub. Sub.}"] \arrow[r, "\mathrm{Inv}_\sigma"] & \color{red}{\mathcal{C}^\sigma} \arrow[u, hook]
\end{tikzcd}$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

$\rightarrow$ $\mathcal{C} \otimes \mathbb{F}_{q^{2m}}$ has a basis in $\mathbb{F}_{q^m}^n$.

$\rightarrow$ Here $p \nmid \ell$ then $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$. So $(\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma$ has also a basis in $\mathbb{F}_{q^m}^n$.

$$
\begin{tikzcd}
\mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} \arrow[r, "\mathrm{Inv}_\sigma"] & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})_{\mathbb{F}_{q^{2m}}} \\
\mathbb{F}_{q^m} & \mathcal{C} \arrow[u, hook, "\text{Sub. Sub.}"] \arrow[r, "\mathrm{Inv}_\sigma"] & \mathcal{C}^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G}) \arrow[u, hook', "\text{Sub. Sub.}"']
\end{tikzcd}
$$

Cyclic cover of $\mathbb{P}^1$

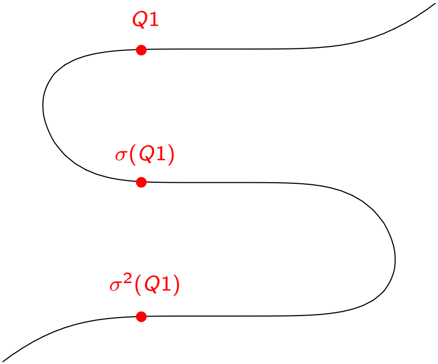
We consider the curve:

$$\mathcal{X} : y^\ell = f(x)$$

and the automorphism:

$$\sigma : \begin{array}{ccc} \mathcal{X} & \longrightarrow & \mathcal{X} \\ (x:y) & \longmapsto & (x:\xi y) \end{array}$$

where ξ is a ℓ-th root of unity.



Support and divisor σ-invariant

For a point $Q \in \mathcal{X}$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

$$\mathcal{P} := \coprod_{i=1}^{n/\ell} Orb_\sigma(Q_i), \tag{3}$$

where the points $Q_i \in \mathcal{X}$ are pairwise distinct with trivial stabilizer subgroup.

Support and divisor σ-invariant

For a point $Q \in \mathcal{X}$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

$$\mathcal{P} := \coprod_{i=1}^{n/\ell} Orb_\sigma(Q_i), \tag{3}$$

where the points $Q_i \in \mathcal{X}$ are pairwise distinct with trivial stabilizer subgroup.
We define the **divisor**:

$$G := s\ P_\infty, \tag{4}$$

with $s \in \mathbb{N}^*$, and P_∞ the point at infinity of the curve $\mathcal{X}$.

Support and divisor σ-invariant

For a point $Q \in \mathcal{X}$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

$$\mathcal{P} := \coprod_{i=1}^{n/\ell} Orb_\sigma(Q_i), \tag{3}$$

where the points $Q_i \in \mathcal{X}$ are pairwise distinct with trivial stabilizer subgroup.
We define the **divisor**:

$$G := s\ P_\infty, \tag{4}$$

with $s \in \mathbb{N}^*$, and P_∞ the point at infinity of the curve $\mathcal{X}$.

σ-invariant code

The automorphism σ induces a permutation on $\mathcal{C} = C_L(\mathcal{X}, \mathcal{P}, G)$.
The subfield subcode $\mathcal{A} := \mathcal{C} \cap \mathbb{F}_q^n$, is also σ-invariant.

Theorem

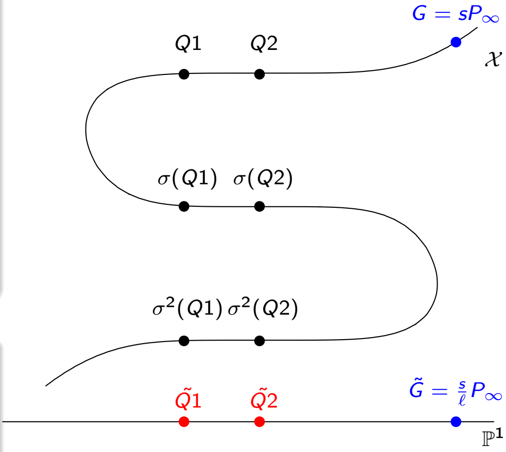
Let $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$ be an AG code, with $\mathcal{P}$ and G define as (3) and (4), and $\sigma \in \mathrm{Perm}(\mathcal{C})$ of order ℓ, then:

$$\mathrm{Inv}(\mathcal{C}) = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G}),$$

of length $\frac{n}{\ell}$ and dimension $\frac{s}{\ell}$.

Corollary

The invariant code $\mathrm{Inv}(\mathcal{A}_r(\mathcal{X}, \mathcal{P}, G))$ is an alternant code of order $\frac{r}{\ell}$ and length $\frac{n}{\ell}$.



Invariant code of σ-invariant AG codes

Lemma

Let $c := Ev_{\mathcal{P}}(f) \in C_L(\mathcal{X}, \mathcal{P}, G)$, with $\deg(G) < n$, such that $\sigma(c) = c$, then f is σ-invariant, ie: $f \circ \sigma = f$.

$$\begin{tikzcd} \mathcal{X} \arrow[loop above, "\sigma"] \arrow[d] \\ \mathcal{X}/\langle\sigma\rangle \end{tikzcd} \qquad \begin{tikzcd} \mathbb{F}_q(\mathcal{X}) \arrow[d, dash] \arrow[d, dash, bend right=60, "\ell"'] \\ \mathbb{F}_q(\mathcal{X})^{\sigma} \end{tikzcd}$$

$\sigma \in \mathrm{Aut}(\mathcal{X})$ of order ℓ.

Theorem

Let $\mathcal{P}$ be a σ-invariant set of rational points of $\mathcal{X}$ and G be a σ-invariant divisor of $\mathcal{X}$, then:

$$\mathrm{Inv}_{\sigma}(C_L(\mathcal{X}, \mathcal{P}, G)) = C_L(\mathcal{X}/\langle\sigma\rangle, \tilde{\mathcal{P}}, \tilde{G})$$

where $\tilde{\mathcal{P}}$ is a set of points of $\mathcal{X}/\langle\sigma\rangle$ and $\tilde{G}$ is a divisor of $\mathcal{X}/\langle\sigma\rangle$.

Quotient curves of $\mathcal{H}$

Let $\mathbb{F}_{q_0^2}$ be a finite field and consider the Hermitian curve, denoted by $\mathcal{H}$ of equation:

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

Quotient curves of $\mathcal{H}$

Let $\mathbb{F}_{q_0^2}$ be a finite field and consider the Hermitian curve, denoted by $\mathcal{H}$ of equation:

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

We denote $A(P_\infty) := \{\sigma \in \mathrm{Aut}(\mathcal{H}) \mid \sigma(P_\infty) = P_\infty\}$ then $\sigma \in A(P_\infty)$ is described by:

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

with $a \in \mathbb{F}_{q_0^2}^*$, $b \in \mathbb{F}_{q_0^2}$ and $b^{q_0+1} = c^{q_0} + c$.

Quotient curves of $\mathcal{H}$

Let $\mathbb{F}_{q_0^2}$ be a finite field and consider the Hermitian curve, denoted by $\mathcal{H}$ of equation:

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

We denote $A(P_\infty) := \{\sigma \in \mathrm{Aut}(\mathcal{H}) \mid \sigma(P_\infty) = P_\infty\}$ then $\sigma \in A(P_\infty)$ is described by:

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

with $a \in \mathbb{F}^*_{q_0^2}$, $b \in \mathbb{F}_{q_0^2}$ and $b^{q_0+1} = c^{q_0} + c$.

If we choose $a \neq 1$ such that $a^{q_0-1} = 1$, then $\mathrm{ord}(\sigma) = \mathrm{ord}(a)$ and the genus of the quotient curve is ([Bassa, Ma, Xing, Yeo, 2013]):

$$g(\mathcal{H}/\langle\sigma\rangle) = \frac{q_0 - 1}{2}.$$

Security of the invariant code

- The invariant code of an alternant AG code is an alternant AG code
- No specific attacks known for alternant AG codes

Security of the invariant code

- The invariant code of an alternant AG code is an alternant AG code
- No specific attacks known for alternant AG codes

Exhaustive search on the divisor:

We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are **diagonal-equivalent**, and we note $\mathcal{C}_1 \sim \mathcal{C}_2$, if there exist $\lambda_1, \ldots, \lambda_n$ nonzero elements such that:

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

Security of the invariant code

- The invariant code of an alternant AG code is an alternant AG code
- No specific attacks known for alternant AG codes

Exhaustive search on the divisor:

We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are **diagonal-equivalent**, and we note $\mathcal{C}_1 \sim \mathcal{C}_2$, if there exist $\lambda_1, \ldots, \lambda_n$ nonzero elements such that:

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

Theorem ([Munuera, Pellikaan, 1993])

If $\mathcal{P}$ is a set of $n > 2g - 2$ rational points of $\mathcal{X}$, where g is the genus of $\mathcal{X}$, and G and H are two divisors of the same degree $2g - 1 < t < n - 1$, then:

$$C_L(\mathcal{X}, \mathcal{P}, G) \sim C_L(\mathcal{X}, \mathcal{P}, H) \Leftrightarrow G \sim H.$$

Number of non equivalent AG codes

We denote $\mathrm{Div}^t(\mathcal{X})$ the group of divisors on $\mathcal{X}$ of degree t and $\mathrm{P}(\mathcal{X})$ the group of principal divisors on $\mathcal{X}$. Then we define the quotient group $\mathrm{Pic}^0(\mathcal{X}) := \mathrm{Div}^0(\mathcal{X})/\mathrm{P}(\mathcal{X})$.

For a fix dimension, the number of non equivalent AG codes on $\mathcal{X}$ with the support $\mathcal{P}$ is:

$$\#\mathrm{AGcode}(\mathcal{X}, \mathcal{P}) = \#\mathrm{Pic}^0(\mathcal{X}).$$

Number of non equivalent AG codes

We denote $\mathrm{Div}^t(\mathcal{X})$ the group of divisors on $\mathcal{X}$ of degree t and $\mathrm{P}(\mathcal{X})$ the group of principal divisors on $\mathcal{X}$. Then we define the quotient group $\mathrm{Pic}^0(\mathcal{X}) := \mathrm{Div}^0(\mathcal{X})/\mathrm{P}(\mathcal{X})$.

For a fix dimension, the number of non equivalent AG codes on $\mathcal{X}$ with the support $\mathcal{P}$ is:

$$\#\mathrm{AGcode}(\mathcal{X},\mathcal{P}) = \#\mathrm{Pic}^0(\mathcal{X}).$$

For the curve $\mathcal{H}/\langle\sigma\rangle$ on $\mathbb{F}_{q_0^2}$:

- $\#\mathrm{Pic}^0(\mathcal{H}/\langle\sigma\rangle) \approx {q_0}^{2g}$
- $g = \frac{q_0-1}{2}$
- $n \approx q_0^3$

$$\#\mathrm{AGcode}(\mathcal{H},\mathcal{P}) \approx (\sqrt[3]{n})^{\sqrt[3]{n}}$$

Number of non equivalent alternant AG codes

We look at non equivalent alternant of AG codes (on $\mathbb{F}_q$):

$$\#\mathcal{A}(\mathcal{X},\mathcal{P}) \leq (q^{m(n-1)} - q^{n-1})\#\mathrm{Pic}^0(\mathcal{X}).$$

Examples of parameters:

q_0	n	k	ISD	$\#Pic^0(\mathcal{H}/\sigma)$	$\#\mathcal{A}(\mathcal{H}/\sigma,\mathcal{P})$	Key size
11	1100	729	118	2^{34}	2^{7634}	163 Kbits
16	1950	1469	116	2^{60}	–	250 Kbits

Conclusion

Results:

1. Quasi-cyclic codes on $\mathbb{P}^1$
    - The invariant code of a quasi-cyclic GRS code is a GRS code.
    - The security of alternant codes with induced permutation from the projective linear group, is reduced to the security of the invariant code which is an alternant code.
2. Codes on cyclic cover of $\mathbb{P}^1$
    - We can recover the invariant code.
    - Thanks to the invariant code we can recover the support and the curve.

Conclusion

Results:

1. Quasi-cyclic codes on $\mathbb{P}^1$
   - The invariant code of a quasi-cyclic GRS code is a GRS code.
   - The security of alternant codes with induced permutation from the projective linear group, is reduced to the security of the invariant code which is an alternant code.
2. Codes on cyclic cover of $\mathbb{P}^1$
   - We can recover the invariant code.
   - Thanks to the invariant code we can recover the support and the curve.
3. Codes on Hermitian curve
   - Automorphism σ such that the quotient curve $\mathcal{H}/\langle\sigma\rangle$ is not $\mathbb{P}^1$
   - Maximal curve $\rightarrow$ good parameters for the code

Conclusion

Results:

1. Quasi-cyclic codes on $\mathbb{P}^1$
   - The invariant code of a quasi-cyclic GRS code is a GRS code.
   - The security of alternant codes with induced permutation from the projective linear group, is reduced to the security of the invariant code which is an alternant code.
2. Codes on cyclic cover of $\mathbb{P}^1$
   - We can recover the invariant code.
   - Thanks to the invariant code we can recover the support and the curve.
3. Codes on Hermitian curve
   - Automorphism σ such that the quotient curve $\mathcal{H}/\langle\sigma\rangle$ is not $\mathbb{P}^1$
   - Maximal curve $\rightarrow$ good parameters for the code

Perspectives:

1. Codes on cyclic cover of the Hermitian curve
2. Codes on cyclic cover of random plane curves

Thank you!