Short McEliece Key from Alternant Algebraic-geometry codes with automorphisms

Élise Barelli

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

AGCT 2017, Luminy

A code-based cryptosystem

Decoding problem

Let $\mathcal{C}$ be a random t-errors correcting code, and $y \in \mathbb{F}_{q^m}^n$.
Does there exist a vector $e \in \mathbb{F}_{q^m}^n$, of weight $w_H(e) \leq t$, such that $y - e \in \mathcal{C}$?

A code-based cryptosystem

Decoding problem

Let $\mathcal{C}$ be a random t-errors correcting code, and $y \in \mathbb{F}_{q^m}^n$.
Does there exist a vector $e \in \mathbb{F}_{q^m}^n$, of weight $w_H(e) \leq t$, such that $y - e \in \mathcal{C}$?

We consider a family $\mathcal{F}$ of linear codes with an efficient decoding algorithm.

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code of $\mathcal{F}$, we denote:

- M a generator matrix of $\mathcal{C}$
- $t \in \mathbb{N}^*$ the error-correcting capability
- $\mathcal{D}$ a t-errors correcting algorithm.

McEliece scheme

1. **Key generation:**
   Public key: (M, t)
   Private key: $\mathcal{D}$

McEliece scheme

1. **Key generation:**
   Public key: (M,t)
   Private key: $\mathcal{D}$
2. **Encryption:** A message $x \in \mathbb{F}_q^k$ is encrypted by:

$$y = c + e$$

where $c = xM$ is a codeword of $\mathcal{C}$ and $e \in \mathbb{F}_q^n$ is a random vector, of weight $w_H(e) \leq t$.

McEliece scheme

1. **Key generation:**
   Public key: (M,t)
   Private key: $\mathcal{D}$
2. **Encryption:** A message $x \in \mathbb{F}_q^k$ is encrypted by:
   $$y = c + e$$
   where $c = xM$ is a codeword of $\mathcal{C}$ and $e \in \mathbb{F}_q^n$ is a random vector, of weight $w_H(e) \leq t$.
3. **Decryption:** We use $\mathcal{D}$ to recover c, then we can recover x from c.

Properties

Advantages:

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

Drawback:

- Large key size

Properties

Advantages:

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

Drawback:

- Large key size

Structural attacks

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

-> Let M be a **random looking** generator matrix of a code $\mathcal{C} \in \mathcal{F}$.

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

Alternant AG codes

Definition

Let $\mathcal{X}$ be an algebraic curve, $\mathcal{P} = \{P_1, \ldots, P_n\}$ 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:

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

and

$$\mathcal{A}_r(\mathcal{X}, \mathcal{P}, G) := C_L(\mathcal{X}, \mathcal{P}, G)^{\perp} \cap \mathbb{F}_q^n,$$

where $r = \dim(C_L(\mathcal{X}, \mathcal{P}, G))$.

Some propositions

- Binary Goppa codes (codes over $\mathbb{P}^1$) (McEliece, 1978)
  $\rightarrow$ No structural attack

Some propositions

- Binary Goppa codes (codes over $\mathbb{P}^1$) (McEliece, 1978)
  $\rightarrow$ No structural attack
- Generalised Reed-Solomon (codes over $\mathbb{P}^1$) (Niederreiter, 1986)
  $\rightarrow$ [Sidelnikov, Shestakov,1992]

Some propositions

- Binary Goppa codes (codes over $\mathbb{P}^1$) (McEliece, 1978)
  - $\rightarrow$ No structural attack
- Generalised Reed-Solomon (codes over $\mathbb{P}^1$) (Niederreiter, 1986)
  - $\rightarrow$ [Sidelnikov, Shestakov,1992]
- Algebraic-geometry (AG) codes (on curve with genus > 0) (Janwa, Moreno, 1996)
  - $\rightarrow$ [Faure, Minder, 2009]
  - $\rightarrow$ [Couvreur, Márquez-Corbella, Pellikaan, 2014]

Some propositions

- Binary Goppa codes (codes over $\mathbb{P}^1$) (McEliece, 1978)
  $\rightarrow$ No structural attack
- Generalised Reed-Solomon (codes over $\mathbb{P}^1$) (Niederreiter, 1986)
  $\rightarrow$ [Sidelnikov, Shestakov,1992]
- Algebraic-geometry (AG) codes (on curve with genus > 0) (Janwa, Moreno, 1996)
  $\rightarrow$ [Faure, Minder, 2009]
  $\rightarrow$ [Couvreur, Márquez-Corbella, Pellikaan, 2014]
- Alternant 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:

$\rightarrow$ [Faugère, Otmani, Perret, Tillich, 2010]

$\rightarrow$ [Faugère, Otmani, Perret, Portzamparc, Tillich, 2015]

$\rightarrow$ [B., 2017]

Alternant codes on cyclic covers of $\mathbb{P}^1$

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

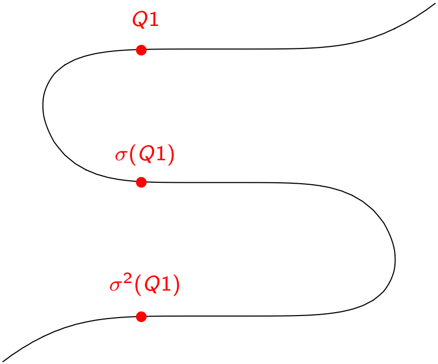
We consider the curve:

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

and the automorphism:

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

where ξ is a ℓ-th root of unity.



σ-invariant support and divisor

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

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

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

σ-invariant support and divisor

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

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

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

$$G := s\ P_\infty, \tag{2}$$

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

σ-invariant support and divisor

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

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

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

$$G := s\ P_\infty, \tag{2}$$

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 $\mathcal{A} := \mathcal{C}^\perp \cap \mathbb{F}_q^n$, is also σ-invariant.

Alternant codes on cyclic covers of $\mathbb{P}^1$

Security analysis

Invariant code

Definition

Let $\mathcal{C}$ be a linear code and $\sigma \in \mathrm{Perm}(\mathcal{C})$ then we define:

$$\mathcal{C}^\sigma := \{c \in \mathcal{C} \mid \sigma(c) = c\}.$$

If $\mathcal{C}$ is a σ-invariant linear code over $\mathbb{F}_{q^m}$ 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 of $\mathcal{A}_r(\mathcal{X}, \mathcal{P}, G)$

Theorem

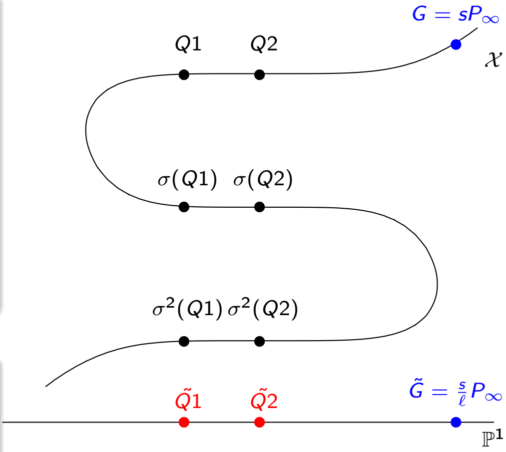
Let $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$ be an AG code, with $\mathcal{P}$ and G defined as (1) and (2), and $\sigma \in \mathrm{Perm}(\mathcal{C})$ of order ℓ, then:

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

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

Corollary

The invariant code $\mathcal{A}_r(\mathcal{X}, \mathcal{P}, G)^\sigma$ is $\mathcal{A}_{r/\ell}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$ of length $\frac{n}{\ell}$.



Recover $\mathcal{P}$ and $\mathcal{X}$

Let M be a generator matrix of $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$.
We assume that we know G and we want to recover $\mathcal{P}$ and $\mathcal{X}$ from M.

$$\mathcal{P} := \left\{ (x_i : \xi^j y_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\} \text{ and } j \in \{0, \ldots, \ell - 1\} \right\}.$$

Recover $\mathcal{P}$ and $\mathcal{X}$

Let M be a generator matrix of $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$.
We assume that we know G and we want to recover $\mathcal{P}$ and $\mathcal{X}$ from M.

$$\mathcal{P} := \left\{ (x_i : \xi^j y_i : 1) \mid i \in \{1, \dots, \frac{n}{\ell}\} \text{ and } j \in \{0, \dots, \ell - 1\} \right\}.$$

$\rightarrow$ Compute $\mathcal{C}^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$ from M

Recover $\mathcal{P}$ and $\mathcal{X}$

Let M be a generator matrix of $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$.
We assume that we know G and we want to recover $\mathcal{P}$ and $\mathcal{X}$ from M.

$$\mathcal{P} := \left\{ (x_i : \xi^j y_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\} \text{ and } j \in \{0, \ldots, \ell - 1\} \right\}.$$

→ Compute $\mathcal{C}^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$ from M

→ Recover $\tilde{\mathcal{P}} = \left\{ (x_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\} \right\}$

Recover $\mathcal{P}$ and $\mathcal{X}$

Let M be a generator matrix of $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$.
We assume that we know G and we want to recover $\mathcal{P}$ and $\mathcal{X}$ from M.

$$\mathcal{P} := \left\{ (x_i : \xi^j y_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\} \text{ and } j \in \{0, \ldots, \ell - 1\} \right\}.$$

- $\rightarrow$ Compute $\mathcal{C}^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$ from M
- $\rightarrow$ Recover $\tilde{\mathcal{P}} = \left\{ (x_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\} \right\}$
- $\rightarrow$ Recover y_i with a linear system which comes from:

$$L(sP_\infty) = \left\langle x^i y^j \mid i \geq 0,\ j \geq 0,\ \text{and } \ell i + (\ell - 1) j \leq s \right\rangle$$

Recover $\mathcal{P}$ and $\mathcal{X}$

Let M be a generator matrix of $\mathcal{C} := C_L(\mathcal{X}, \mathcal{P}, G)$.
We assume that we know G and we want to recover $\mathcal{P}$ and $\mathcal{X}$ from M.

$$\mathcal{P} := \left\{(x_i : \xi^j y_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\} \text{ and } j \in \{0, \ldots, \ell - 1\}\right\}.$$

- $\rightarrow$ Compute $\mathcal{C}^\sigma = C_L(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$ from M
- $\rightarrow$ Recover $\tilde{\mathcal{P}} = \left\{(x_i : 1) \mid i \in \{1, \ldots, \frac{n}{\ell}\}\right\}$
- $\rightarrow$ Recover y_i with a linear system which comes from:

$$L(sP_\infty) = \left\langle x^i y^j \mid i \geq 0,\ j \geq 0,\ \text{and } \ell i + (\ell - 1)j \leq s\right\rangle$$

- $\rightarrow$ Recover $\mathcal{X}$ from $\mathcal{P}$

Alternant codes on the Hermitian curve

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:

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

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 $b^{q_0+1} = c^{q_0} + c$.

For odd q_0, 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 denote $\mathcal{C}_1 \sim \mathcal{C}_2$, 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 denote $\mathcal{C}_1 \sim \mathcal{C}_2$, 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

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

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

Number of non equivalent AG codes

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

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

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

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

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

Number of non equivalent alternant AG codes

We look at non equivalent alternant of AG codes (over $\mathbb{F}_{q_0}$):

$$\#\mathcal{A}(\mathcal{X}, \mathcal{P}) \leq (q_0^{2(n-1)} - q_0^{n-1})\#\mathrm{Pic}^0(\mathcal{X}).$$

Example of parameters: $\mathcal{H}$ is defined on $\mathbb{F}_{11^2}$

n	k	Message security	$\#Pic^0(\mathcal{H}/\sigma)$	$\#\mathcal{A}(\mathcal{H}/\sigma, \mathcal{P})$	Key size
1100	729	2^{118}	2^{34}	2^{7634}	163 Kbits

Conclusion

Results:

1. 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. 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.
2. 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. 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.
2. 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