The Tangent Space Attack

Axel Lemoine[1,2]

October 3, 2025

1. Inria Paris, France
2. DGA, France

Plan

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Plan of this Section

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

Conclusion

The decoding problem

Definition 1 (Linear code)

An $[n, k]_q$-**linear code** $\mathscr{C}$ is a linear subspace of $\mathbb{F}_q^n$:

$$\mathscr{C} = \{\boldsymbol{m} \cdot \boldsymbol{G} \mid \boldsymbol{m} \in \mathbb{F}_q^k\} = \{\boldsymbol{x} \in \mathbb{F}_q^n \mid \boldsymbol{H} \cdot \boldsymbol{x}^\top = 0\}.$$

Problem (Decoding problem)

- ***Input:*** *$\mathscr{C}$ an $[n, k]_q$-code, $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ with $\boldsymbol{c} \in \mathscr{C}$ and $|\boldsymbol{e}| = t$;*
- ***Goal:*** *recover $\boldsymbol{c}$.*

The first code-based cryptosystem [McEliece, 1978]

Public key	gen. mat. $\boldsymbol{G}_{\text{pub}} \in \mathbb{F}_q^{k \times n}$ of an $[n, k]_q$-code $\mathscr{C}$
Private key	Efficient decoding algorithm derived from a structured gen. mat. $\boldsymbol{G}_{\text{priv}}$ of $\mathscr{C}$
Encryption	$\boldsymbol{m} \longmapsto \boldsymbol{m}\boldsymbol{G}_{\text{pub}} + \boldsymbol{e}$ where $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n, \ \lvert\boldsymbol{e}\rvert = t$
Decryption	Performed by a decoding algorithm using the **hidden** structure of $\boldsymbol{G}_{\text{priv}}$

Figure 1: Generic McEliece cryptosystem

Definition 2 (GRS codes)

$\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} \{(y_1 f(x_1), \ldots, y_n f(x_n)) \mid f \in \mathbb{F}_q[X]_{<r}\}$. A generator matrix is

$$\mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y}) = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1 x_1 & y_2 x_2 & \cdots & y_n x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & y_2 x_2^{r-1} & \cdots & y_n x_n^{r-1} \end{pmatrix}.$$

- **Private key:** $(\boldsymbol{x}, \boldsymbol{y}) \implies$ Welch-Berlekamp algorithm;
- **Public key:** $\boldsymbol{G} = \boldsymbol{P} \cdot \mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y})$ where $\boldsymbol{P} \stackrel{\$}{\leftarrow} \boldsymbol{GL}_r(\mathbb{F}_q)$.

[SS92]: *This turns out to be* ***insecure****...*

Subfield-subcodes of GRS codes.

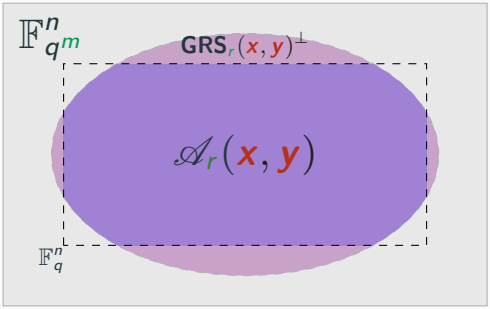


Figure 2: Alternant code

Definition 3 (Alternant codes)

$\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) \stackrel{\text{def}}{=} \mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y})^\perp \cap \mathbb{F}_q^n$.

- $\dim \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) \stackrel{\text{w.h.p}}{=} n - rm$;
- $(\boldsymbol{x},\boldsymbol{y}) \implies$ **Decoding algorithm**

Definition 4 (Goppa codes)

Let $\Gamma \in \mathbb{F}_{q^m}[X]$ such that $\deg \Gamma = r$ and $\Gamma(x_i) \neq 0,\ i = 1,\dots,n$.

$$\mathscr{G}(\boldsymbol{x},\Gamma) \stackrel{\text{def}}{=} \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}),\ \text{with } y_i = \Gamma(x_i)^{-1}.$$

Recovering the structure of an alternant code

Problem (Key recovery problem)

- ***Input:*** $\boldsymbol{H}_{\mathrm{pub}} \in \mathbb{F}_q^{rm \times n}$ *be a partity-check matrix of* $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$*;*
- ***Goal:*** *recover* $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r \times n}$ *a generator matrix of* $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$*.*

Plan of this Section

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Plan

McEliece cryptosystem

The notion of quadratic hull

- Unusual behavior of GRS codes
- From GRS codes to alternant codes

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Definition 5 (Componentwise product)

Given $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^n$, $\boldsymbol{a} \star \boldsymbol{b} \stackrel{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$.
If $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$ are two codes, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.
$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

[CCMZ15] $$\dim \mathscr{C}^{\star 2} = \begin{cases} \min\left\{\binom{\dim \mathscr{C}+1}{2}, n\right\} & \text{if } \mathscr{C} \text{ is random,} \\ \min\{2\dim \mathscr{C} - 1, n\} & \text{if } \mathscr{C} \text{ is a GRS code.} \end{cases}$$

Indeed: $(\boldsymbol{y}\boldsymbol{x}^i) \star (\boldsymbol{y}\boldsymbol{x}^j) - (\boldsymbol{y}\boldsymbol{x}^k) \star (\boldsymbol{y}\boldsymbol{x}^l) = 0$ whenever $i + j = k + l$.

Quadratic hull

Let $\boldsymbol{G} = (\boldsymbol{g}_1 | \ldots | \boldsymbol{g}_n) \in \mathbb{F}_q^{k \times n}$ a gen. mat of $\mathscr{C}$ and $\boldsymbol{S} = \mathbb{F}_q[x_1, \ldots, x_k] = \bigoplus_{d \geqslant 0} \boldsymbol{S}_d$.

Definition 6 (Quadratic hull [Ran20])

- **Algebraic view:** $I_2(\boldsymbol{G}) \stackrel{\text{def}}{=} \{f \in \boldsymbol{S}_2 \mid f(\boldsymbol{g}_1) = \ldots = f(\boldsymbol{g}_n) = 0\}$.
- **Geometric view:** $V_2(\boldsymbol{G}) \stackrel{\text{def}}{=} \{\boldsymbol{v} \in \mathbb{F}_q^k,\ \forall f \in I_2(\boldsymbol{G}),\ f(\boldsymbol{v}) = 0\}$.

Quadratic hull

Let $\boldsymbol{G} = (\boldsymbol{g}_1 | \ldots | \boldsymbol{g}_n) \in \mathbb{F}_q^{k \times n}$ a gen. mat of $\mathscr{C}$ and $\boldsymbol{S} = \mathbb{F}_q[x_1, \ldots, x_k] = \bigoplus_{d \geqslant 0} \boldsymbol{S}_d$.

Definition 6 (Quadratic hull [Ran20])

- **Algebraic view:** $I_2(\boldsymbol{G}) \stackrel{\text{def}}{=} \{f \in \boldsymbol{S}_2 \mid f(\boldsymbol{g}_1) = \ldots = f(\boldsymbol{g}_n) = 0\}$.
- **Geometric view:** $V_2(\boldsymbol{G}) \stackrel{\text{def}}{=} \{\boldsymbol{v} \in \mathbb{F}_q^k,\ \forall f \in I_2(\boldsymbol{G}),\ f(\boldsymbol{v}) = 0\}$.

Proposition 7

- $\dim I_2(\boldsymbol{G}) = \binom{k+1}{2} - \dim \mathscr{C}^{\star 2}$.

Quadratic hull

Let $\boldsymbol{G} = (\boldsymbol{g}_1 | \ldots | \boldsymbol{g}_n) \in \mathbb{F}_q^{k \times n}$ a gen. mat of $\mathscr{C}$ and $\boldsymbol{S} = \mathbb{F}_q[x_1, \ldots, x_k] = \bigoplus_{d \geqslant 0} \boldsymbol{S}_d$.

Definition 6 (Quadratic hull [Ran20])

- **Algebraic view:** $I_2(\boldsymbol{G}) \stackrel{\text{def}}{=} \{f \in \boldsymbol{S}_2 \mid f(\boldsymbol{g}_1) = \ldots = f(\boldsymbol{g}_n) = 0\}$.
- **Geometric view:** $V_2(\boldsymbol{G}) \stackrel{\text{def}}{=} \{\boldsymbol{v} \in \mathbb{F}_q^k,\ \forall f \in I_2(\boldsymbol{G}),\ f(\boldsymbol{v}) = 0\}$.

Proposition 7

- $\dim I_2(\boldsymbol{G}) = \binom{k+1}{2} - \dim \mathscr{C}^{\star 2}$.

*Let $\boldsymbol{G}' = \boldsymbol{P} \cdot \boldsymbol{G}$ be **another** generator matrix of $\mathscr{C}$.*

- ***Alg.*** $I_2(\boldsymbol{G}) = \{f^{\boldsymbol{P}} \mid f \in I_2(\boldsymbol{G}')\}$, *where* $f^{\boldsymbol{P}} \stackrel{\text{def}}{=} f((x_1, \ldots, x_k)\boldsymbol{P}^\top)$.
- ***Geom.*** $V_2(\boldsymbol{G}') = \{\boldsymbol{P} \cdot \boldsymbol{v}^\top \mid \boldsymbol{v} \in V_2(\boldsymbol{G})\}$.

Let $\mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) \subset \mathbb{F}_q^n$, and let $\boldsymbol{G} = \mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y})$.

Theorem 8

- $I_2(\boldsymbol{G})$ *is spanned by* $\{x_i x_j - x_k x_l \mid i + j = k + l\}$;
- $\dim I_2(\boldsymbol{G}) = \binom{r-1}{2}$;
- $V_2(\boldsymbol{G}) = \{(y, xy, x^2y, \ldots, x^{r-1}y) \mid (x, y) \in \mathbb{F}_q \times \mathbb{F}_q\}$.

The columns of $\boldsymbol{G}$ lie on the rational normal curve !

Plan

McEliece cryptosystem

The notion of quadratic hull

- Unusual behavior of GRS codes
- From GRS codes to alternant codes

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}$ (1)

Let $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. Since $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) = (\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}) \cap \mathbb{F}_q^n$,

$$\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) = \left\{ \boldsymbol{c} \in \mathbb{F}_q^n \mid \begin{pmatrix} y_1 & \cdots & y_n \\ \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & \cdots & y_n x_n^{r-1} \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0 \right\}.$$

Generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ (1)

Let $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. Since $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) = (\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp) \cap \mathbb{F}_q^n$,

$$\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) = \left\{ \boldsymbol{c} \in \mathbb{F}_q^n \mid \begin{pmatrix} y_1 & \dots & y_n \\ \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & \dots & y_n x_n^{r-1} \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0 \right\}.$$

Each row gives m equations. For example, replace

$$\begin{pmatrix} y_1 & y_2 & \dots & y_n \end{pmatrix} \longleftrightarrow \begin{pmatrix} y_{1,0} & y_{2,0} & \dots & y_{n,0} \\ y_{1,1} & y_{2,1} & \dots & y_{n,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,m-1} & y_{2,m-1} & \dots & y_{n,m-1} \end{pmatrix}$$

where $y_i = y_{i,0} + y_{i,1}\alpha + \ldots + y_{i,m-1}\alpha^{m-1}$.

Generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ (2)

Denote by

$$\Psi_\alpha : \begin{cases} \mathbb{F}_{q^m} & \xrightarrow{\simeq} \mathbb{F}_q^m \\ z = \sum_{j=0}^{m-1} z_j \alpha^j & \longmapsto (z_0, z_1, \ldots, z_{m-1}), \end{cases}$$

and naturally extend it to vectors : $\Psi_\alpha : \mathbb{F}_{q^m}^r \xrightarrow{\simeq} \mathbb{F}_q^{rm}$.

Generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ (2)

Denote by

$$\Psi_\alpha : \begin{cases} \mathbb{F}_{q^m} & \xrightarrow{\simeq} \mathbb{F}_q^m \\ z = \sum_{j=0}^{m-1} z_j \alpha^j & \longmapsto (z_0, z_1, \ldots, z_{m-1}), \end{cases}$$

and naturally extend it to vectors : $\Psi_\alpha : \mathbb{F}_{q^m}^r \xrightarrow{\simeq} \mathbb{F}_q^{rm}$.

Proposition 9

Let $\mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{g}_1 | \ldots | \boldsymbol{g}_n)$ *be a generator matrix of* $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$. *Then*

$$\Psi_\alpha(\mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y})) \stackrel{def}{=} (\Psi_\alpha(\boldsymbol{g}_1) | \ldots | \Psi_\alpha(\boldsymbol{g}_n))$$

is a generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$.

Generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ (2)

Denote by

$$\Psi_\alpha : \begin{cases} \mathbb{F}_{q^m} & \xrightarrow{\simeq} \mathbb{F}_q^m \\ z = \sum_{j=0}^{m-1} z_j \alpha^j & \longmapsto (z_0, z_1, \ldots, z_{m-1}), \end{cases}$$

and naturally extend it to vectors : $\Psi_\alpha : \mathbb{F}_{q^m}^r \xrightarrow{\simeq} \mathbb{F}_q^{rm}$.

Proposition 9

Let $\mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{g}_1 | \ldots | \boldsymbol{g}_n)$ *be a generator matrix of* $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$. *Then*

$$\Psi_\alpha(\mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y})) \stackrel{def}{=} (\Psi_\alpha(\boldsymbol{g}_1) | \ldots | \Psi_\alpha(\boldsymbol{g}_n))$$

is a generator matrix of $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$.

This will help

- Determine the quadratic hull of a dual alternant code;
- **mount a key recovery attack against alternant codes !**

Problem (Key recovery problem)

- ***Input:*** $\boldsymbol{H}_{\mathrm{pub}} \in \mathbb{F}_q^{rm \times n}$ *be a partity-check matrix of* $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$*;*
- ***Goal:*** *recover* $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r \times n}$ *a generator matrix of* $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$.

Key point: We do not have access to $\boldsymbol{H}_{\mathrm{sec}} = \Psi_\alpha(\boldsymbol{G})$.
Instead $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{P} \cdot \boldsymbol{H}_{\mathrm{sec}}$ with $\boldsymbol{P} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$.
Although $\boldsymbol{H}_{\mathrm{pub}} = \Psi_\alpha(\boldsymbol{G}')$, the matrix $\boldsymbol{G}'$ **is not** a generator matrix of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ in general.

In the following...

Let $\boldsymbol{G} = \mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_{q^m}^{r \times n}$ be a generator matrix of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$, $\boldsymbol{H}_{\mathrm{sec}} = \Psi_\alpha(\boldsymbol{G})$ and $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{P} \cdot \boldsymbol{H}_{\mathrm{sec}}$.

Goal

- *Establish a **fundamental** link between $I_2(\boldsymbol{G})$ and $I_2(\boldsymbol{H}_{\mathrm{sec}})$;*
- *Deduce interesting properties of $I_2(\boldsymbol{H}_{\mathrm{pub}})$.*

Sketch of answer: $V_2(\boldsymbol{H}_{\mathrm{sec}})$ seems to contain the points $\Psi_\alpha(\boldsymbol{v})$ for $\boldsymbol{v} \in V_2(\boldsymbol{G})$...

This leads to the concept of Weil restriction !

Plan of this Section

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Plan

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

- Definition and first properties
- Identifying Weil restrictions

A new attack against high-rate alternant codes

Conclusion

A first example

Consider the complex circle $\mathcal{X}$: $z_1^2 + z_2^2 - 1 = 0$.

A first example

Consider the complex circle $\mathcal{X}$: $z_1^2 + z_2^2 - 1 = 0$. Split each variable in real and imaginary parts: $z_1 = x_1 + iy_1,\ z_2 = x_2 + iy_2$.

A first example

Consider the complex circle $\mathcal{X}: \; z_1^2 + z_2^2 - 1 = 0$. Split each variable in real and imaginary parts: $z_1 = x_1 + iy_1, \; z_2 = x_2 + iy_2$.

Goal

Find algebraic conditions on (x_1, y_1, x_2, y_2) *expressing* $(x_1 + iy_1, x_2 + iy_2) \in \mathcal{X}$.

A first example

Consider the complex circle $\mathcal{X}: \; z_1^2 + z_2^2 - 1 = 0$. Split each variable in real and imaginary parts: $z_1 = x_1 + iy_1, \; z_2 = x_2 + iy_2$.

Goal

Find algebraic conditions on (x_1, y_1, x_2, y_2) *expressing* $(x_1 + iy_1, x_2 + iy_2) \in \mathcal{X}$.

Solution: substitute (z_1, z_2) in the defining equation of $\mathcal{X}$:

$$(x_1 + iy_1, x_2 + iy_2) \in \mathcal{X} \iff (x_1 + iy_1)^2 + (x_2 + iy_2)^2 - 1 = 0.$$

A first example

Consider the complex circle $\mathcal{X}: \ z_1^2 + z_2^2 - 1 = 0$. Split each variable in real and imaginary parts: $z_1 = x_1 + iy_1, \ z_2 = x_2 + iy_2$.

Goal

Find algebraic conditions on (x_1, y_1, x_2, y_2) expressing $(x_1 + iy_1, x_2 + iy_2) \in \mathcal{X}$.

Solution: substitute (z_1, z_2) in the defining equation of $\mathcal{X}$:

$$(x_1 + iy_1, x_2 + iy_2) \in \mathcal{X} \iff (x_1 + iy_1)^2 + (x_2 + iy_2)^2 - 1 = 0.$$

Now expand and gather the real and imaginary parts:

$$\begin{aligned}
(x_1 + iy_1, x_2 + iy_2) \in \mathcal{X} &\iff x_1^2 - y_1^2 + 2ix_1y_1 + x_2^2 - y_2^2 + 2ix_2y_2 - 1 = 0 \\
&\iff x_1^2 - y_1^2 + x_2^2 - y_2^2 - 1 + i(2x_1y_1 + 2x_2y_2) = 0. \\
&\iff \begin{cases} x_1^2 - y_1^2 + x_2^2 - y_2^2 - 1 = 0 \\ 2x_1y_1 + 2x_2y_2 = 0 \end{cases} \quad \hookrightarrow \mathcal{Y} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathcal{X}) \subset \mathbb{R}^4.
\end{aligned}$$

Formal definition

We work with $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. Define the two polynomial rings:

$$\boldsymbol{R} = \mathbb{F}_{q^m}[X_0, \ldots, X_{r-1}] \text{ and } \boldsymbol{S} = \mathbb{F}_q[x_{i,j} \mid 0 \leqslant i < r,\ j < m].$$

In order to split the variables with respect to α, we introduce

$$\Phi : \begin{cases} \boldsymbol{R} & \longrightarrow \boldsymbol{S} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} \\ X_i & \longmapsto \sum_{j<m} \alpha^j x_{i,j}. \end{cases}$$

For all $f \in \boldsymbol{R}$, write $\Phi(f) = \Phi_0(f) + \alpha\Phi_1(f) \ldots + \alpha^{m-1}\Phi_{m-1}(f)$ with $\Phi_j(f) \in \boldsymbol{S}$.

Definition 10

Let $I \subset \boldsymbol{R}$ be a prime ideal, and set $V = \mathbb{V}(I)$. We define

$$\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I) \stackrel{\text{def}}{=} \langle \Phi_j(f) \mid f \in I,\ 0 \leqslant j < m \rangle,$$

and we write $\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(V) \stackrel{\text{def}}{=} \mathbb{V}(\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I))$.

Proposition 11

Let $I \subset \boldsymbol{R}$ be a prime ideal and let $J = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I)$.

- $\dim J = m \times \dim I$.
- *The map*

$$\Psi_\alpha : \begin{cases} \mathbb{F}_{q^m}^r & \longrightarrow \mathbb{F}_q^{rm} \\ \boldsymbol{v} = (v_0, \ldots, v_{r-1}) & \longmapsto (v_{0,0}, \ldots, v_{0,m-1}, \ \ldots \ , v_{r-1,0}, \ldots, v_{r-1,m-1}) \end{cases}$$

induces a natural bijection between $\mathbb{V}_{\mathbb{F}_{q^m}}(I)$ and $\mathbb{V}_{\mathbb{F}_q}(J)$.

Let $\mathscr{C}$ be an $[n, k]_{q^m}$-code with generator matrix $\boldsymbol{G}$ and let $\boldsymbol{H}_{\mathrm{sec}} = \Psi_\alpha(\boldsymbol{G})$ be a parity-check matrix of $\mathscr{C}_{|\mathbb{F}_q}$. Let also $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{P} \cdot \boldsymbol{H}_{\mathrm{sec}}$.

Corollary 12

- $I_2(\boldsymbol{H}_{\mathrm{sec}}) \supset \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I_2(\boldsymbol{G}))$, *or equivalently* $V_2(\boldsymbol{H}_{\mathrm{sec}}) \subset \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I_2(\boldsymbol{G}))$;
- $I_2(\boldsymbol{H}_{\mathrm{pub}}) \supset \{f^{\boldsymbol{P}^{-1}} \mid f \in \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I_2(\boldsymbol{G}))\}$;
- $V_2(\boldsymbol{H}_{\mathrm{pub}}) \subset \boldsymbol{P} \cdot \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(V_2(\boldsymbol{G}))$.

Natural questions arise:

- When do we have $I_2(\boldsymbol{H}_{\mathrm{sec}}) = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I_2(\boldsymbol{G}))$?
- Can we use the Weil restriction to distinguish a (dual) subfield subcode from a random code ?
- Which varieties/subspaces are the Weil restriction of another variety/subspace ?

Weil-properness of alternant codes

We provide an answer to the first questions for alternant codes.
Define $\boldsymbol{G} = \mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y})$ and $\boldsymbol{H}_{\mathrm{sec}} = \Psi_\alpha(\boldsymbol{G})$.

Proposition 13

Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$. *If*

$$r \leqslant q \text{ and } \mathscr{C}^{\star 2} \neq \mathbb{F}_q^n,$$

then, by [FGOPT11], $I_2(\boldsymbol{H}_{\mathrm{sec}}) = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(I_2(\boldsymbol{G}))$.

Remark 14

When $r \leqslant q$, *and when*

$$n > \binom{rm+1}{2} - m\binom{r-1}{2},$$

heuristic of [FGOPT11] ensures $(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp)^{\star 2} \neq \mathbb{F}_q^n$.

We then talk about **Weil-proper** alternant codes.

Plan

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

- Definition and first properties
- Identifying Weil restrictions

A new attack against high-rate alternant codes

Conclusion

The simpler case of vector subspaces (1)

Take a complex line $L = \mathbb{C} \cdot \boldsymbol{u}$ where $\boldsymbol{u} = (z_1 \;\; z_2)^\top \in \mathbb{C}^2$. Observe that

$$\begin{aligned} L &= \left\{ (t_1 + it_2) \cdot \begin{pmatrix} x_1 + iy_1 \\ x_1 + iy_2 \end{pmatrix} \;\middle|\; (t_1, t_2) \in \mathbb{R}^2 \right\} \\ &= \left\{ \begin{pmatrix} t_1x_1 - t_2y_1 + i(t_1y_1 + t_2x_1) \\ t_1x_2 - t_2y_2 + i(t_1y_2 + t_2x_2) \end{pmatrix} \;\middle|\; (t_1, t_2) \in \mathbb{R}^2 \right\}. \end{aligned}$$

We see that if $\mathcal{P} = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(L)$, then

$$\mathcal{P} = \left\{ \begin{pmatrix} t_1 & -t_2 & 0 & 0 \\ t_2 & t_1 & 0 & 0 \\ 0 & 0 & t_1 & -t_2 \\ 0 & 0 & t_2 & t_1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{pmatrix} \;\middle|\; (t_1, t_2) \in \mathbb{R}^2 \right\}.$$

$$\mathcal{P} = \left\{ \begin{pmatrix} t_1 & -t_2 & 0 & 0 \\ t_2 & t_1 & 0 & 0 \\ 0 & 0 & t_1 & -t_2 \\ 0 & 0 & t_2 & t_1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{pmatrix} \mid (t_1, t_2) \in \mathbb{R}^2 \right\}.$$

We see that $\mathcal{P}$ is invariant under the action of $\boldsymbol{J}_2 = \mathrm{Diag}(\boldsymbol{J}, \boldsymbol{J})$ with $\boldsymbol{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Remark 15

$\boldsymbol{J}$ is the matrix of the $\mathbb{R}$-linear map $\mu_i : \begin{cases} \mathbb{C} & \longrightarrow \mathbb{C} \\ z & \longmapsto iz \end{cases}$ *with respect to the $\mathbb{R}$-basis $(1, i)$ of $\mathbb{C}$.*

$\boldsymbol{J}_2$-stability of $\mathcal{P}$ $\iff$ $\mathbb{C}$-linearity of L

Notation 16

Let $\boldsymbol{J}$ be the matrix of the $\mathbb{F}_q$-linear map

$$\mu_\alpha : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow \mathbb{F}_{q^m} \\ x & \longmapsto \alpha x \end{cases}$$

w.r.t. the $\mathbb{F}_q$-basis $(1, \alpha, \ldots, \alpha^{m-1})$ of $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. We also write $\boldsymbol{J}_r = Diag(\boldsymbol{J}, \ldots, \boldsymbol{J})$.

Theorem 17

A vector subspace $W \subset \mathbb{F}_q^{rm}$ is a Weil restriction $\iff$ it is $\boldsymbol{J}_r$-invariant.

$\boldsymbol{J}_r$-stability of W $\iff$ **$\mathbb{F}_{q^m}$-linearity of V**

Linear data associated to a variety: **tangent spaces !**

Definition 18 (Tangent space)

Let $I \subset \boldsymbol{R} = \mathbb{F}_{q^m}[X_0, \ldots, X_{r-1}]$ be a prime ideal and $V = \mathbb{V}(I)$. For any $\mathbb{F}_{q^m}$-rational point $P \in V(\mathbb{F}_{q^m})$, the **tangent space** of V at P is defined by

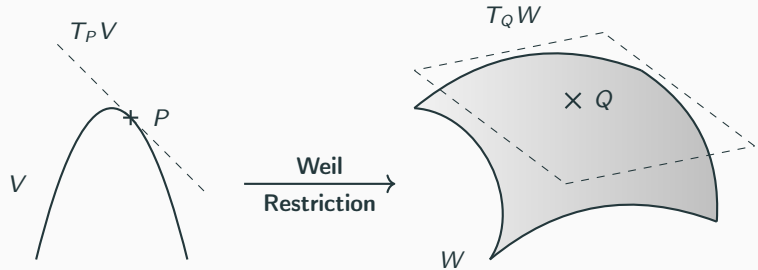
$$T_P V = \left\{ \boldsymbol{h} \in \mathbb{F}_{q^m}^r \mid \forall f \in I,\ \sum_{i<r} h_i \frac{\partial f}{\partial X_i}(P) = 0 \right\}.$$

In practice: $I = \langle f_1, \ldots, f_N \rangle \implies T_P V =$ **right-kernel** $\mathrm{Jac}(f_1, \ldots, f_N) = \left(\frac{\partial f_i}{\partial X_j} \right)_{i,j}$ at P.

Proposition 19

Let $W = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(V)$, $P \in V(\mathbb{F}_{q^m})$ *and* $Q = \Psi_\alpha(P) \in W(\mathbb{F}_q)$. *Then*

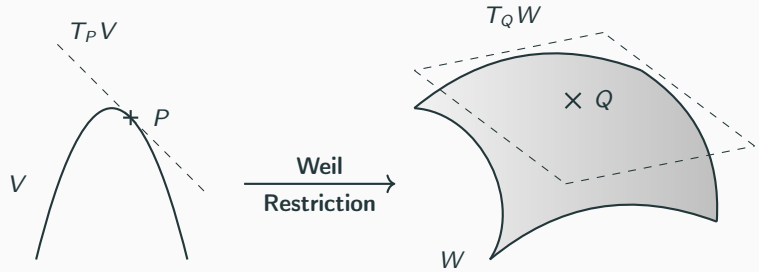
$$T_Q W = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(T_P V).$$



Proposition 19

Let $W = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(V)$, $P \in V(\mathbb{F}_{q^m})$ *and* $Q = \Psi_\alpha(P) \in W(\mathbb{F}_q)$. *Then*

$$T_Q W = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(T_P V).$$



$T_Q W$ is J_r-invariant !

Let $\boldsymbol{G} = \mathrm{Vand}_r(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_{q^m}^{r \times n}$ be a generator matrix of $\mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ with quadratic hull $\mathscr{X}$ (rational normal curve). If $\mathscr{C}$ is **Weil-proper** (high-rate regime + $r \leqslant q$). then

- All tangent spaces of $V_2(\boldsymbol{H}_{\mathrm{sec}})$ are $\boldsymbol{J}_r$-invariant;
- $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{P} \cdot \boldsymbol{H}_{\mathrm{sec}} \implies$ tangent spaces of $V_2(\boldsymbol{H}_{\mathrm{pub}})$ are **invariant** under the action of $\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}$.

This provides a distinguisher

Plan of this Section

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Plan

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

- Alternant case, with $r \leqslant q$
- Generalizations

Conclusion

The key-recovery problem

Problem

- ***Input:*** $\boldsymbol{H}_{\mathrm{pub}} \in \mathbb{F}_q^{rm \times n}$ *be a partity-check matrix of* $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$*;*
- ***Goal:*** *recover* $\boldsymbol{G} \in \mathbb{F}_{q^m}^{r \times n}$ *a generator matrix of* $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$.

Key points:

- We do not have access to $\boldsymbol{H}_{\mathrm{sec}} = \Psi_\alpha(\boldsymbol{G})$;
- $\boldsymbol{H}_{\mathrm{pub}} = \Psi_\alpha(\boldsymbol{G}')$ for some $\boldsymbol{G}'$, but this matrix **is not** a generator-matrix of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$...

Definition 20

For any vector-subspace $T \subset \mathbb{F}_q^{rm}$, we define the **stabilizer** of T to be

$$\mathrm{St}(T) = \{\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm} \mid \forall \boldsymbol{v} \in T,\ \boldsymbol{A}\boldsymbol{v}^\top \in T\}.$$

Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ be **Weil-proper** (high rate and $r \leqslant q$), and set $W = V_2(\boldsymbol{H}_{\mathrm{pub}})$. We have seen that

- For all point $Q \in W$, we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \mathrm{St}(T_Q W)$;

Definition 20

For any vector-subspace $T \subset \mathbb{F}_q^{rm}$, we define the **stabilizer** of T to be

$$\mathrm{St}(T) = \{\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm} \mid \forall \boldsymbol{v} \in T,\ \boldsymbol{A}\boldsymbol{v}^\top \in T\}.$$

Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ be **Weil-proper** (high rate and $r \leqslant q$), and set $W = V_2(\boldsymbol{H}_{\mathrm{pub}})$. We have seen that

- For all point $Q \in W$, we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \mathrm{St}(T_Q W)$;
- **Better:** we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \bigcap_{Q \in W} \mathrm{St}(T_Q W)$;

Definition 20

For any vector-subspace $T \subset \mathbb{F}_q^{rm}$, we define the **stabilizer** of T to be

$$\mathrm{St}(T) = \{\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm} \mid \forall \boldsymbol{v} \in T,\ \boldsymbol{A}\boldsymbol{v}^\top \in T\}.$$

Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ be **Weil-proper** (high rate and $r \leqslant q$), and set $W = V_2(\boldsymbol{H}_{\mathrm{pub}})$. We have seen that

- For all point $Q \in W$, we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \mathrm{St}(T_Q W)$;
- **Better:** we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \bigcap_{Q \in W} \mathrm{St}(T_Q W)$;
- **Betterer:** it seems like $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] = \bigcap_{Q \in W} \mathrm{St}(T_Q W)$!

Proposition 21

*By computing $\bigcap_i \mathrm{St}(T_{Q_i} W)$ for **sufficiently many** $Q_i \in W$, we **get access to** $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}]$.*

Definition 20

For any vector-subspace $T \subset \mathbb{F}_q^{rm}$, we define the **stabilizer** of T to be

$$\mathrm{St}(T) = \{\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm} \mid \forall \boldsymbol{v} \in T,\ \boldsymbol{A}\boldsymbol{v}^\top \in T\}.$$

Let $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ be **Weil-proper** (high rate and $r \leqslant q$), and set $W = V_2(\boldsymbol{H}_{\mathrm{pub}})$. We have seen that

- For all point $Q \in W$, we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \mathrm{St}(T_Q W)$;
- **Better:** we have $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] \subseteq \bigcap_{Q \in W} \mathrm{St}(T_Q W)$;
- **Betterer:** it seems like $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] = \bigcap_{Q \in W} \mathrm{St}(T_Q W)$!

Proposition 21

*By computing $\bigcap_i \mathrm{St}(T_{Q_i} W)$ for **sufficiently many** $Q_i \in W$, we **get access to** $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}]$.*

$$\boxed{\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}] = \boldsymbol{P} \cdot \mathbb{F}_q[\boldsymbol{J}_r] \cdot \boldsymbol{P}^{-1} \simeq \mathbb{F}_{q^m}}$$

Exploit the field structure

Once we have computed $\mathcal{A} \stackrel{\text{def}}{=} \boldsymbol{P} \cdot \mathbb{F}_q[\boldsymbol{J}_r] \cdot \boldsymbol{P}^{-1} \simeq \mathbb{F}_{q^m}$, we may compute some $\boldsymbol{A} \in \mathcal{A}$ whose minimal polynomial $\Pi_{\boldsymbol{A}}$ is that of $\boldsymbol{J}$, *i.e* that of α.

Proposition 22

- *There exists* $\boldsymbol{Q} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$ *such that* $\boldsymbol{J}_r = \boldsymbol{Q} \cdot \boldsymbol{A} \cdot \boldsymbol{Q}^{-1}$, *and* ***one may compute it****;*
- *There exists* $0 \leqslant j < m$ *such that* $\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1} = A^{q^j}$.

As a consequence, $(\boldsymbol{Q} \cdot \boldsymbol{P}) \cdot \boldsymbol{J}_r = \boldsymbol{J}_r^{q^j} \cdot (\boldsymbol{Q} \cdot \boldsymbol{P})$.

Exploit the field structure

Once we have computed $\mathcal{A} \stackrel{\text{def}}{=} \boldsymbol{P} \cdot \mathbb{F}_q[\boldsymbol{J}_r] \cdot \boldsymbol{P}^{-1} \simeq \mathbb{F}_{q^m}$, we may compute some $\boldsymbol{A} \in \mathcal{A}$ whose minimal polynomial $\Pi_{\boldsymbol{A}}$ is that of $\boldsymbol{J}$, *i.e* that of α.

Proposition 22

- *There exists* $\boldsymbol{Q} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$ *such that* $\boldsymbol{J}_r = \boldsymbol{Q} \cdot \boldsymbol{A} \cdot \boldsymbol{Q}^{-1}$, *and* ***one may compute it****;*
- *There exists* $0 \leqslant j < m$ *such that* $\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1} = A^{q^j}$.

As a consequence, $(\boldsymbol{Q} \cdot \boldsymbol{P}) \cdot \boldsymbol{J}_r = \boldsymbol{J}_r^{q^j} \cdot (\boldsymbol{Q} \cdot \boldsymbol{P})$.

Theorem 23

Let $\boldsymbol{S} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$. *If* $\boldsymbol{S} \cdot \boldsymbol{J}_r \cdot \boldsymbol{S}^{-1} = \boldsymbol{J}_r^{q^j}$ *for some* j, *then* ***S preserves Weil restrictions****.*

Exploit the field structure

Once we have computed $\mathcal{A} \stackrel{\text{def}}{=} \boldsymbol{P} \cdot \mathbb{F}_q[\boldsymbol{J}_r] \cdot \boldsymbol{P}^{-1} \simeq \mathbb{F}_{q^m}$, we may compute some $\boldsymbol{A} \in \mathcal{A}$ whose minimal polynomial $\Pi_{\boldsymbol{A}}$ is that of $\boldsymbol{J}$, *i.e* that of α.

Proposition 22

- *There exists* $\boldsymbol{Q} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$ *such that* $\boldsymbol{J}_r = \boldsymbol{Q} \cdot \boldsymbol{A} \cdot \boldsymbol{Q}^{-1}$, *and* ***one may compute it****;*
- *There exists* $0 \leqslant j < m$ *such that* $\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1} = A^{q^j}$.

As a consequence, $(\boldsymbol{Q} \cdot \boldsymbol{P}) \cdot \boldsymbol{J}_r = \boldsymbol{J}_r^{q^j} \cdot (\boldsymbol{Q} \cdot \boldsymbol{P})$.

Theorem 23

Let $\boldsymbol{S} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$. *If* $\boldsymbol{S} \cdot \boldsymbol{J}_r \cdot \boldsymbol{S}^{-1} = \boldsymbol{J}_r^{q^j}$ *for some* j, *then* ***S preserves Weil restrictions****.*

In short: $\boldsymbol{Q} \cdot \boldsymbol{H}_{\text{pub}} = (\boldsymbol{Q} \cdot \boldsymbol{P}) \cdot \Psi_\alpha(\boldsymbol{G}) = \Psi_\alpha(\boldsymbol{G}')$, and $\boldsymbol{G}'$ **is a generator matrix of** $\mathbf{GRS}_r(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$!

Algorithm 1 Recovering x' and y' from H_{pub} assuming Weil-properness

Input : H_{pub} a parity-check matrix of $\mathscr{A}_r(x, y)$.
Output : x' and y' such that $\mathscr{C} = \mathscr{A}_r(x', y')$.
Compute $I_2(H_{\mathrm{pub}})$, and define $W = V_2(H_{\mathrm{pub}})$
Compute $\mathcal{A} = P \cdot \mathbb{F}_q[J_r] \cdot P^{-1}$ by taking $\bigcap_i \mathrm{St}(T_{Q_i} W)$ for sufficiently many Q_i's
Compute $A \in \mathcal{A}$ such that $\Pi_A = \Pi_\alpha$
Compute $Q \in GL_{rm}(\mathbb{F}_q)$ satisfying $Q \cdot A \cdot Q^{-1} = J_r$
Compute $G' \in \mathbb{F}_{q^m}^{r \times n}$ such that $Q \cdot H_{\mathrm{pub}} = \Psi_\alpha(G')$
Recover (x', y') using either [SS92] or [GH78]
return (x', y').

Plan

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

- Alternant case, with $r \leqslant q$
- Generalizations

Conclusion

Alternant case, $r > q$

Surprisingly, the attack **still works** when $r > q$ (but we still need the **high-rate regime**)

Heuristic 24

Assume $r > q$ and take a point $P \in \mathcal{Y} = V_2(\boldsymbol{G})$. Let $Q = \Psi_\alpha(P)$ and $W = V_2(\Psi_\alpha(\boldsymbol{G}))$. Then

$$T_Q W = \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\mathbb{F}_{q^m} \cdot P).$$

Remark 25

Our attack handles the Goppa case where $r < q - 1$ in the high-rate regime, as they behave like generic alternant codes.

But unfortunately...

Heuristic 26

Assume $r \geqslant q - 1$ and take a point $P \in \mathcal{Y} = V_2(\boldsymbol{G})$ where $\boldsymbol{G}$ is a generator matrix of $\mathbf{GRS}_r(\boldsymbol{x}, \Gamma(x)^{-1})$. Let $Q = \Psi_\alpha(P)$ and $W = V_2(\Psi_\alpha(\boldsymbol{G}))$. Then

$$\dim T_Q W = 1.$$

[CFS01] Signature scheme remains **unbroken to this day**.

Plan of this Section

McEliece cryptosystem

The notion of quadratic hull

Weil restriction

A new attack against high-rate alternant codes

Conclusion

Conclusion and open problems

- Link **Duals of subfield-subcodes** $\longleftrightarrow$ **Weil restriction**;
- A new attack against high-rate:
  - Alternant codes;
  - Goppa codes, with $r < q - 1$;
  - SSAG codes whose degree is strictly inferior to q;
  - SSAG codes with 'generic' divisor.

Future work:

- Understands why the attack still works when $r > q$;
- Weil-restriction of **rational** varieties ?

Thank you for your attention.

Computing the stabilizers

Let $T \subset \mathbb{F}_q^{rm}$ be a $2m$-dimensional vector space and $\boldsymbol{A} \in \mathbb{F}_q^{rm \times rm}$. We may see T as a **linear code**: $T = \{\boldsymbol{m} \cdot \underbrace{\boldsymbol{G}}_{\in \mathbb{F}_q^{\mathbf{2}m \times rm}} \mid \boldsymbol{m} \in \mathbb{F}_q^{2m}\} = \{\boldsymbol{v} \in \mathbb{F}_q^{rm} \mid \underbrace{\boldsymbol{H}}_{\in \mathbb{F}_q^{(rm-\mathbf{2}m) \times rm}} \cdot \boldsymbol{v}^\top = 0\}$.

Now notice that: $\forall \boldsymbol{A} \in \mathbb{F}_q^{rm \times rm}$, $\boldsymbol{A} \in \mathrm{St}(T) \iff \boldsymbol{H} \cdot \boldsymbol{A} \cdot \boldsymbol{G}^\top = 0 \hookrightarrow 2m \times (rm - 2m)$ equations on the $A_{i,j}$'s.

Heuristic 27 (Maybe provable)

Experimental evidence show that as soon as we take at least N distinct points $Q_1, \ldots, Q_N \in W = V_2(\boldsymbol{H}_{\mathrm{pub}})$ where

$$N \stackrel{\text{def}}{=} \left\lceil \frac{(rm)^2}{2m(rm-2m)} \right\rceil = \left\lceil \frac{1}{\rho(1-\rho)} \right\rceil \text{ where } \rho = \frac{2}{r},$$

then $\bigcap_{i=1}^{N} \mathrm{St}(T_{Q_i} W) = \mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}]$. We may take the columns of $\boldsymbol{H}_{\mathrm{pub}}$ as the Q_i's.

We do have access to $\mathbb{F}_q[\boldsymbol{P} \cdot \boldsymbol{J}_r \cdot \boldsymbol{P}^{-1}]$!

On the structure of the stabilizers (1)

Proposition 28

- *For $x \in \mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$, write $x = x_0 + x_1\alpha + \ldots + x_{m-1}\alpha^{m-1}$. Define*

$$\mu_x : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow \mathbb{F}_{q^m} \\ y & \longmapsto xy. \end{cases}$$

  Then the matrix of μ_x in the basis $(1, \alpha, \ldots, \alpha^{m-1})$ is $x_0\boldsymbol{I} + x_1\boldsymbol{J} + \ldots + x_{m-1}\boldsymbol{J}^{m-1}$.

- *The map*

$$\mathrm{Mat}_\alpha : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow \mathbb{F}_q[\boldsymbol{J}] \\ x & \longmapsto x_0\boldsymbol{I} + x_1\boldsymbol{J} + \ldots + x_{m-1}\boldsymbol{J}^{m-1} \end{cases}$$

  is an isomorphism of $\mathbb{F}_q$-algebras.

In the same way, $\mathbb{F}_q[\boldsymbol{J}_r] \simeq \mathbb{F}_{q^m}$ for any integer r (recap: $\boldsymbol{J}_r = \mathrm{Diag}(\boldsymbol{J}, \ldots, \boldsymbol{J})$).

On the structure of the stabilizers (2)

Notation 29

For $\boldsymbol{P} \in \boldsymbol{GL}_{rm}(\mathbb{F}_q)$, we write

$$C_{\boldsymbol{P}} : \begin{cases} \mathbb{F}_q^{rm \times rm} & \longrightarrow \mathbb{F}_q^{rm \times rm} \\ \boldsymbol{M} & \longmapsto \boldsymbol{P} \cdot \boldsymbol{M} \cdot \boldsymbol{P}^{-1}. \end{cases}$$

*The map $C_{\boldsymbol{P}}$ is an **automorphism** of $\mathbb{F}_q^{rm \times rm}$.*

Corollary 30

Let $W = V_2(\boldsymbol{H}_{\mathrm{pub}})$. Then

$$\bigcap_{i=1}^{N} \mathrm{St}(T_{Q_i} W) = \boldsymbol{P} \cdot \mathbb{F}_q[\boldsymbol{J}_r] \cdot \boldsymbol{P}^{-1} \simeq \mathbb{F}_{q^m}.$$