The new distinguisher of alternant codes at degree 2

Axel Lemoine[1], Rocco Mora[2], Jean-Pierre Tillich[1]

Inria Paris, France

CISPA, Germany

June 19, 2024

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	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: Generic McEliece cryptosystem

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	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: Generic McEliece cryptosystem

- Recovering $\boldsymbol{G}_{\text{priv}}$ from $\boldsymbol{G}_{\text{pub}}$ must be **hard**;

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	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: Generic McEliece cryptosystem

- Recovering $\boldsymbol{G}_{\text{priv}}$ from $\boldsymbol{G}_{\text{pub}}$ must be **hard**;
- $\Longrightarrow$ Distinguishing $\boldsymbol{G}_{\text{pub}}$ from a random $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ must be **hard**.

Security of McEliece

Strongly relies on the hardness of the **distinguishing problem**.

Security of McEliece

Strongly relies on the hardness of the **distinguishing problem**.

Problem 1 (Distinguishing problem)

Data. $b \xleftarrow{\$} \{0,1\}$. *If* $b = 0$, $\boldsymbol{G} \leftarrow \mathbb{F}_q^{k \times n}$. *If* $b = 1$, $\boldsymbol{G} \leftarrow \boldsymbol{G}_{\mathbf{pub}}$.

Security of McEliece

Strongly relies on the hardness of the **distinguishing problem**.

Problem 1 (Distinguishing problem)

Data. $b \xleftarrow{\$} \{0,1\}$. *If* $b = 0$, $\boldsymbol{G} \leftarrow \mathbb{F}_q^{k \times n}$. *If* $b = 1$, $\boldsymbol{G} \leftarrow \boldsymbol{G}_{\mathbf{pub}}$.
Goal. *Given* $\boldsymbol{G}$, *find* b.

Security of McEliece

Strongly relies on the hardness of the **distinguishing problem**.

Problem 1 (Distinguishing problem)

Data. $b \xleftarrow{\$} \{0,1\}$. *If* $b = 0$, $\boldsymbol{G} \leftarrow \mathbb{F}_q^{k \times n}$. *If* $b = 1$, $\boldsymbol{G} \leftarrow \boldsymbol{G}_{\mathbf{pub}}$.
Goal. *Given* $\boldsymbol{G}$, *find* b.

In practise, $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ (degree r, extension degree m).

Security of McEliece

Strongly relies on the hardness of the **distinguishing problem**.

Problem 1 (Distinguishing problem)

Data. $b \xleftarrow{\$} \{0,1\}$. *If* $b = 0$, $\boldsymbol{G} \leftarrow \mathbb{F}_q^{k \times n}$. *If* $b = 1$, $\boldsymbol{G} \leftarrow \boldsymbol{G}_{\mathbf{pub}}$.
Goal. *Given* $\boldsymbol{G}$, *find* b.

In practise, $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ (degree r, extension degree m).

	FGOPT10	CMT23
Lowest dist. dim	$k_0 \sim \frac{r^2 m^2}{2}$	?

Figure: Existing distinguishers for alternant codes of degree r and extension degree m.

Security of McEliece

Strongly relies on the hardness of the **distinguishing problem**.

Problem 1 (Distinguishing problem)

Data. $b \xleftarrow{\$} \{0,1\}$. *If* $b = 0$, $\boldsymbol{G} \leftarrow \mathbb{F}_q^{k \times n}$. *If* $b = 1$, $\boldsymbol{G} \leftarrow \boldsymbol{G}_{\mathbf{pub}}$.
Goal. *Given* $\boldsymbol{G}$, *find* b.

In practise, $\mathscr{C} = \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ (degree r, extension degree m).

	FGOPT10	CMT23
Lowest dist. dim	$k_0 \sim \frac{r^2 m^2}{2}$	$k_0 \sim 0.21 r^2 m^2$ (This work !)

Figure: Existing distinguishers for alternant codes of degree r and extension degree m.

Plan

1. Distinguisher [FGOPT10]: nontrivial relations in a code
2. Distinguisher [CMT23]: **short** relations
3. Conclusion

Plan of this Section

1. Distinguisher [FGOPT10]: nontrivial relations in a code
2. Distinguisher [CMT23]: **short** relations
3. Conclusion

First example: GRS codes

Definition 2 (GRS codes)

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

First example: GRS codes

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 of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ is

$$\boldsymbol{G} = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1 x_1 & y_2 x_2 & \cdots & y_n x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & y_2 x_2^{r-1} & \cdots & y_n x_n^{r-1} \end{pmatrix}.$$

First example: GRS codes

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 of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ is

$$\boldsymbol{G} = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1 x_1 & y_2 x_2 & \cdots & y_n x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & y_2 x_2^{r-1} & \cdots & y_n x_n^{r-1} \end{pmatrix}.$$

- $\boldsymbol{G}_{\text{priv}} \leftarrow \boldsymbol{G}$;

First example: GRS codes

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 of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ is

$$\boldsymbol{G} = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1 x_1 & y_2 x_2 & \cdots & y_n x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & y_2 x_2^{r-1} & \cdots & y_n x_n^{r-1} \end{pmatrix}.$$

- $\boldsymbol{G}_{\text{priv}} \leftarrow \boldsymbol{G}$;
- $\boldsymbol{G}_{\text{pub}} \leftarrow \boldsymbol{P} \cdot \boldsymbol{G}$ for some $\boldsymbol{P} \stackrel{\$}{\leftarrow} \mathrm{GL}_r(\mathbb{F}_q)$.

First example: GRS codes

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 of $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})$ is

$$\boldsymbol{G} = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1 x_1 & y_2 x_2 & \cdots & y_n x_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1 x_1^{r-1} & y_2 x_2^{r-1} & \cdots & y_n x_n^{r-1} \end{pmatrix}.$$

- $\boldsymbol{G}_{\text{priv}} \leftarrow \boldsymbol{G}$;
- $\boldsymbol{G}_{\text{pub}} \leftarrow \boldsymbol{P} \cdot \boldsymbol{G}$ for some $\boldsymbol{P} \stackrel{\$}{\leftarrow} \mathrm{GL}_r(\mathbb{F}_q)$.

Does McEliece security hypothesis hold ?

(Square) distinguishability of GRS codes

Definition 3 (Schur's product)

Given $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^n$, $\boldsymbol{a} \star \boldsymbol{b} \stackrel{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$.

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

$$\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} = \begin{cases} \min\left\{n, \binom{r+1}{2}\right\} & \text{if } \mathscr{C} \text{ is a random } [n, r]_q\text{-code;} \\ \end{cases}$$

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

$$\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} = \begin{cases} \min\left\{n, \binom{r+1}{2}\right\} & \text{if } \mathscr{C} \text{ is a random } [n, r]_q\text{-code;} \\ \min\{n, 2r-1\} & \text{if } \mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}). \end{cases}$$

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

$$\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} = \begin{cases} \min\left\{n, \binom{r+1}{2}\right\} & \text{if } \mathscr{C} \text{ is a random } [n, r]_q\text{-code;} \\ \min\{n, 2r-1\} & \text{if } \mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}). \end{cases}$$

Indeed: $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2r-1}(\boldsymbol{x}, \boldsymbol{y}^{\star 2})$.

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

$$\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} = \begin{cases} \min\left\{n, \binom{r+1}{2}\right\} & \text{if } \mathscr{C} \text{ is a random } [n, r]_q\text{-code;} \\ \min\{n, 2r-1\} & \text{if } \mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}). \end{cases}$$

Indeed: $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2r-1}(\boldsymbol{x}, \boldsymbol{y}^{\star 2})$.

Explanation 4 (Nontrivial relations)

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

$$\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} = \begin{cases} \min\left\{n, \binom{r+1}{2}\right\} & \text{if } \mathscr{C} \text{ is a random } [n, r]_q\text{-code;} \\ \min\{n, 2r-1\} & \text{if } \mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}). \end{cases}$$

Indeed: $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2r-1}(\boldsymbol{x}, \boldsymbol{y}^{\star 2})$.

Explanation 4 (Nontrivial relations)

- $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ *basis of* ***random*** $\mathscr{C} \implies \{\boldsymbol{v}_i \star \boldsymbol{v}_j \mid i \leqslant j\}$ *basis of* $\mathscr{C}^{\star 2}$.

(Square) distinguishability of GRS codes

Definition 3 (Schur's 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, $\mathscr{C} \star \mathscr{D} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\{\boldsymbol{c} \star \boldsymbol{d} \mid (\boldsymbol{c}, \boldsymbol{d}) \in \mathscr{C} \times \mathscr{D}\}$.

$\mathscr{C}^{\star 2} \stackrel{\text{def}}{=} \mathscr{C} \star \mathscr{C}$.

$$\dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} = \begin{cases} \min\left\{n, \binom{r+1}{2}\right\} & \text{if } \mathscr{C} \text{ is a random } [n, r]_q\text{-code;} \\ \min\{n, 2r-1\} & \text{if } \mathscr{C} = \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}). \end{cases}$$

Indeed: $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2r-1}(\boldsymbol{x}, \boldsymbol{y}^{\star 2})$.

Explanation 4 (Nontrivial relations)

- $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ *basis of* ***random*** $\mathscr{C} \implies \{\boldsymbol{v}_i \star \boldsymbol{v}_j \mid i \leqslant j\}$ *basis of* $\mathscr{C}^{\star 2}$.
- $\mathcal{V} = \{\boldsymbol{y}, \boldsymbol{x} \star \boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1} \star \boldsymbol{y}\} \implies (\boldsymbol{x}^i \star \boldsymbol{y}) \star (\boldsymbol{x}^j \star \boldsymbol{y}) = (\boldsymbol{x}^k \star \boldsymbol{y}) \star (\boldsymbol{x}^l \star \boldsymbol{y})$ *each time* $i + j = k + l$.

Quadratic forms

Let $\mathscr{C}$ be an $[n,k]_q$-code of basis $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

Quadratic forms

Let $\mathscr{C}$ be an $[n,k]_q$-code of basis $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

$$P : \begin{cases} \mathbb{F}_q^{\binom{k+1}{2}} & \longrightarrow \mathscr{C}^{\star 2} \\ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} & \longmapsto \displaystyle\sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j. \end{cases}$$

Quadratic forms

Let $\mathscr{C}$ be an $[n,k]_q$-code of basis $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

$$P : \begin{cases} \mathbb{F}_q^{\binom{k+1}{2}} & \longrightarrow \mathscr{C}^{\star 2} \\ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} & \longmapsto \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j. \end{cases}$$

✓ $\mathscr{C}$ not random $\iff \dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} < \binom{k+1}{2}$

Quadratic forms

Let $\mathscr{C}$ be an $[n,k]_q$-code of basis $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

$$P : \begin{cases} \mathbb{F}_q^{\binom{k+1}{2}} & \longrightarrow \mathscr{C}^{\star 2} \\ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} & \longmapsto \displaystyle\sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j. \end{cases}$$

✓ $\mathscr{C}$ not random $\iff \dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} < \binom{k+1}{2} \iff \ker P \neq \{0\}$.

Quadratic forms

Let $\mathscr{C}$ be an $[n,k]_q$-code of basis $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

$$P : \begin{cases} \mathbb{F}_q^{\binom{k+1}{2}} & \longrightarrow \mathscr{C}^{\star 2} \\ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} & \longmapsto \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j. \end{cases}$$

✓ $\mathscr{C}$ not random $\iff \dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} < \binom{k+1}{2} \iff \ker P \neq \{0\}$.

Definition 5 (Code of relations)

$$\mathscr{C}_{\mathrm{rel}}(\mathcal{V}) \stackrel{\text{def}}{=} \ker P = \left\{ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} \in \mathbb{F}_q^{\binom{k+1}{2}},\ \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j = 0 \right\}.$$

Quadratic forms

Let $\mathscr{C}$ be an $[n,k]_q$-code of basis $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$.

$$P : \begin{cases} \mathbb{F}_q^{\binom{k+1}{2}} & \longrightarrow \mathscr{C}^{\star 2} \\ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} & \longmapsto \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j. \end{cases}$$

✓ $\mathscr{C}$ not random $\iff \dim_{\mathbb{F}_q} \mathscr{C}^{\star 2} < \binom{k+1}{2} \iff \ker P \neq \{0\}$.

Definition 5 (Code of relations)

$$\mathscr{C}_{\mathsf{rel}}(\mathcal{V}) \stackrel{\text{def}}{=} \ker P = \left\{ \boldsymbol{c} = (c_{i,j})_{i \leqslant j} \in \mathbb{F}_q^{\binom{k+1}{2}},\ \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j = 0 \right\}.$$

$$\dim_{\mathbb{F}_q} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \min \left\{ n, \binom{r+1}{2} - \underbrace{\frac{(r-1)(r-2)}{2}}_{\dim \mathscr{C}_{\mathsf{rel}}} = 2r - 1 \right\}$$

Real World McEliece: Alternant codes

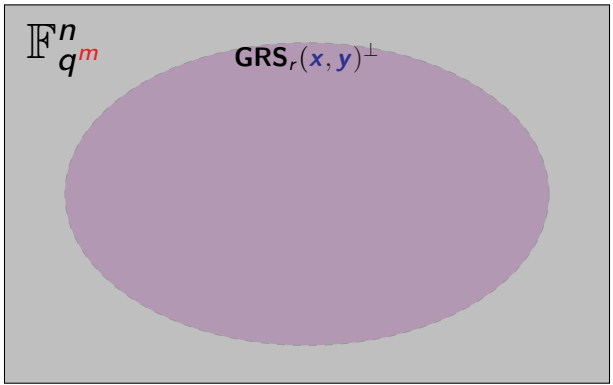
Subfield subcodes of GRS codes.

Real World McEliece: Alternant codes

Subfield subcodes of GRS codes.

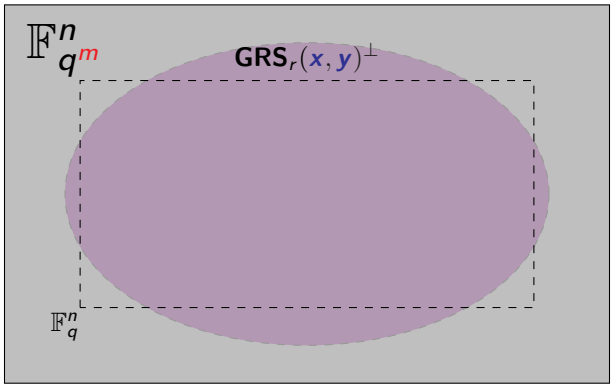
Real World McEliece: Alternant codes

Subfield subcodes of GRS codes.



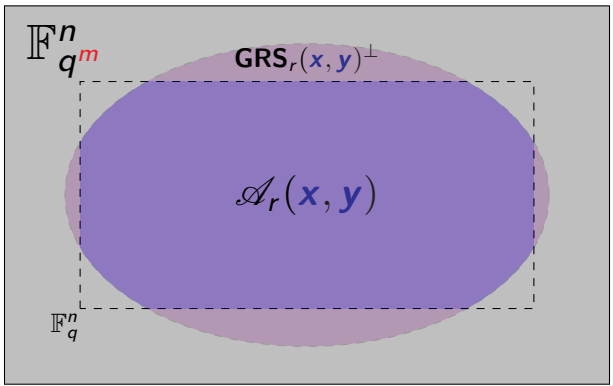
Real World McEliece: Alternant codes

Subfield subcodes of GRS codes.



Real World McEliece: Alternant codes

Subfield subcodes of GRS codes.



Properties of alternant codes

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

Properties of alternant codes

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

Dimension	$\geqslant n - rm$ ($= n - rm$ generically).
Minimum distance	$\geqslant r$
Efficient decoding algorithm	✓
Indistinguishability	?

Figure: Proporties of alternant codes

Properties of alternant codes

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

Dimension	$\geqslant n - rm$ ($= n - rm$ generically).
Minimum distance	$\geqslant r$
Efficient decoding algorithm	✓
Indistinguishability	?

Figure: Proporties of alternant codes

Proposition 6

Assume $r < q + 1$. Generically,

$$\dim_{\mathbb{F}_q} \left(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}\right)^{\star 2} = \min\left\{n, \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2)\right\}.$$

Plan of this Section

1. Distinguisher [FGOPT10]: nontrivial relations in a code
2. Distinguisher [CMT23]: **short** relations
3. Conclusion

Matrix code of relations

Definition 7

Matrix of a relation $\boldsymbol{c} = (c_{i,j})_{i \leqslant j} \in \mathscr{C}_{\mathsf{rel}}$:

$$M_{\boldsymbol{c}} = \begin{pmatrix} 2c_{1,1} & c_{1,2} & \dots & c_{1,k} \\ c_{1,2} & 2c_{2,2} & \dots & c_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1,k} & c_{2,k} & \dots & 2c_{k,k} \end{pmatrix}.$$

Matrix code of relations

Definition 7

Matrix of a relation $\boldsymbol{c} = (c_{i,j})_{i \leqslant j} \in \mathscr{C}_{\mathsf{rel}}$:

$$M_{\boldsymbol{c}} = \begin{pmatrix} 2c_{1,1} & c_{1,2} & \dots & c_{1,k} \\ c_{1,2} & 2c_{2,2} & \dots & c_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1,k} & c_{2,k} & \dots & 2c_{k,k} \end{pmatrix}.$$

Definition 8 (Matrix code of relations)

$\mathscr{C}_{\mathsf{mat}}(\mathcal{V}) = \{M_{\boldsymbol{c}},\ \boldsymbol{c} \in \mathscr{C}_{\mathsf{rel}}(\mathcal{V})\}$.

What does it mean to be short ?

Back to our GRS codes:

What does it mean to be short ?

Back to our GRS codes: if $\mathcal{V} = \{\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{r-1}\} = \{\boldsymbol{y}, \boldsymbol{x} \star \boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1} \star \boldsymbol{y}\}$, the relation

$$\boldsymbol{v}_0 \star \boldsymbol{v}_2 - \boldsymbol{v}_1^{\star 2} = 0$$

has matrix

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & \ldots \\ 0 & -2 & 0 & 0 & \ldots \\ 1 & 0 & 0 & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

which has rank 3 in characteristic $\neq 2$ and rank 2 in characteristic 2.

What does it mean to be short ?

Back to our GRS codes: if $\mathcal{V} = \{\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{r-1}\} = \{\boldsymbol{y}, \boldsymbol{x} \star \boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1} \star \boldsymbol{y}\}$, the relation

$$\boldsymbol{v}_0 \star \boldsymbol{v}_2 - \boldsymbol{v}_1^{\star 2} = 0$$

has matrix

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & \ldots \\ 0 & -2 & 0 & 0 & \ldots \\ 1 & 0 & 0 & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

which has rank 3 in characteristic $\neq 2$ and rank 2 in characteristic 2.
A relation $\boldsymbol{c} \in \mathscr{C}_{\mathsf{rel}}(\mathcal{V})$ is **short** if its matrix $M_{\boldsymbol{c}} \in \mathscr{C}_{\mathsf{mat}}(\mathcal{V})$ has a low rank.

What does it mean to be short ?

Back to our GRS codes: if $\mathcal{V} = \{\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{r-1}\} = \{\boldsymbol{y}, \boldsymbol{x} \star \boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1} \star \boldsymbol{y}\}$, the relation

$$\boldsymbol{v}_0 \star \boldsymbol{v}_2 - \boldsymbol{v}_1^{\star 2} = 0$$

has matrix

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & \ldots \\ 0 & -2 & 0 & 0 & \ldots \\ 1 & 0 & 0 & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

which has rank 3 in characteristic $\neq 2$ and rank 2 in characteristic 2.
A relation $\boldsymbol{c} \in \mathscr{C}_{\mathsf{rel}}(\mathcal{V})$ is **short** if its matrix $M_{\boldsymbol{c}} \in \mathscr{C}_{\mathsf{mat}}(\mathcal{V})$ has a low rank.

Consequence 9

Even if $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbb{F}_q^n$, ***short*** *relations might still be detectable...*

Finding short relations in characteristic 2

Let $\boldsymbol{M}$ be the generic skew-symmetric matrix of size r in characteristic 2, i.e

$$\boldsymbol{M} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & x_{1,2} & x_{1,3} & \cdots & x_{1,r-1} & x_{1,r} \\ x_{1,2} & 0 & x_{2,3} & \cdots & x_{2,r-1} & x_{2,r} \\ x_{1,3} & x_{2,3} & 0 & \cdots & x_{3,r-1} & x_{3,r} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{1,r-1} & x_{2,r-1} & x_{3,r-1} & \cdots & 0 & x_{r-1,r} \\ x_{1,r} & x_{2,r} & x_{3,r} & \cdots & x_{r-1,r} & 0 \end{pmatrix}$$

Finding short relations in characteristic 2

Let $\boldsymbol{M}$ be the generic skew-symmetric matrix of size r in characteristic 2, i.e

$$\boldsymbol{M} \stackrel{\text{def}}{=} \begin{pmatrix} 0 & x_{1,2} & x_{1,3} & \cdots & x_{1,r-1} & x_{1,r} \\ x_{1,2} & 0 & x_{2,3} & \cdots & x_{2,r-1} & x_{2,r} \\ x_{1,3} & x_{2,3} & 0 & \cdots & x_{3,r-1} & x_{3,r} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{1,r-1} & x_{2,r-1} & x_{3,r-1} & \cdots & 0 & x_{r-1,r} \\ x_{1,r} & x_{2,r} & x_{3,r} & \cdots & x_{r-1,r} & 0 \end{pmatrix}$$

Fact 10

$\boldsymbol{M}$ has rank $\leqslant 2$ if, and only if

$$\forall 1 \leqslant i < j < k < l \leqslant r,\ x_{i,j}x_{k,l} + x_{i,k}x_{j,l} + x_{i,l}x_{j,k} = 0.$$

Algebraic modeling

Modeling 11 ($\boldsymbol{M} \in \mathscr{C}_{\mathrm{mat}},\ \mathrm{rk}(\boldsymbol{M}) \leqslant 2$)

- $\mathrm{rk}(\boldsymbol{M}) \leqslant 2 \implies \forall 1 \leqslant i < j < k < l \leqslant r,\ x_{i,j}x_{k,l} + x_{i,k}x_{j,l} + x_{i,l}x_{j,k} = 0$;
- $\boldsymbol{M} \in \mathscr{C}_{mat} \implies L_1(\{x_{i,j}\}) = \ldots = L_t(\{x_{i,j}\}) = 0$ *where the* L_i*'s are* ***linear forms***.

Algebraic modeling

Modeling 11 ($\boldsymbol{M} \in \mathscr{C}_{\mathsf{mat}},\ \mathrm{rk}(\boldsymbol{M}) \leqslant 2$)

- $\mathrm{rk}(\boldsymbol{M}) \leqslant 2 \implies \forall 1 \leqslant i < j < k < l \leqslant r,\ x_{i,j}x_{k,l} + x_{i,k}x_{j,l} + x_{i,l}x_{j,k} = 0$;
- $\boldsymbol{M} \in \mathscr{C}_{mat} \implies L_1(\{x_{i,j}\}) = \ldots = L_t(\{x_{i,j}\}) = 0$ *where the* L_i*'s are* ***linear forms***.

These polynomials generate an **ideal** $\mathcal{I} \subseteq \mathbb{F}_q[\{x_{i,j}\}]$.

Algebraic modeling

Modeling 11 ($\boldsymbol{M} \in \mathscr{C}_{\mathsf{mat}},\ \mathrm{rk}(\boldsymbol{M}) \leqslant 2$)

- $\mathrm{rk}(\boldsymbol{M}) \leqslant 2 \implies \forall 1 \leqslant i < j < k < l \leqslant r,\ x_{i,j}x_{k,l} + x_{i,k}x_{j,l} + x_{i,l}x_{j,k} = 0$;
- $\boldsymbol{M} \in \mathscr{C}_{mat} \implies L_1(\{x_{i,j}\}) = \ldots = L_t(\{x_{i,j}\}) = 0$ *where the* L_i*'s are* ***linear forms***.

These polynomials generate an **ideal** $\mathcal{I} \subseteq \mathbb{F}_q[\{x_{i,j}\}]$.
Subspace $\mathcal{I}_2$: generated by the $\binom{r}{4}$ **quadratic equations** plus the equations of the form $x_{i,j}L_s$.

Algebraic modeling

Modeling 11 ($\boldsymbol{M} \in \mathscr{C}_{\mathsf{mat}},\ \mathrm{rk}(\boldsymbol{M}) \leqslant 2$)

- $\mathrm{rk}(\boldsymbol{M}) \leqslant 2 \implies \forall 1 \leqslant i < j < k < l \leqslant r,\ x_{i,j}x_{k,l} + x_{i,k}x_{j,l} + x_{i,l}x_{j,k} = 0$;
- $\boldsymbol{M} \in \mathscr{C}_{mat} \implies L_1(\{x_{i,j}\}) = \ldots = L_t(\{x_{i,j}\}) = 0$ *where the* L_i*'s are* ***linear forms***.

These polynomials generate an **ideal** $\mathcal{I} \subseteq \mathbb{F}_q[\{x_{i,j}\}]$.
Subspace $\mathcal{I}_2$: generated by the $\binom{r}{4}$ **quadratic equations** plus the equations of the form $x_{i,j}L_s$.
$\hookrightarrow$ **Hilbert function at degree 2:** $\mathrm{HF}(2) \stackrel{\text{def}}{=} \dim \mathbb{F}_q[\{x_{i,j}\}]/\mathcal{I}_2$.

The Hilbert function at degree 2 as a distinguisher

Goal. Distinguish $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}$ from a random $[n, rm]_q$-code

The Hilbert function at degree 2 as a distinguisher

Goal. Distinguish $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}$ from a random $[n, rm]_q$-code **assuming** $(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp})^{\star 2} = \mathbb{F}_q^n$.

The Hilbert function at degree 2 as a distinguisher

Goal. Distinguish $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ from a random $[n, rm]_q$-code **assuming** $(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp)^{\star 2} = \mathbb{F}_q^n$.

Proposition 12 (Random case)

*If $\mathscr{C}$ is a **non**-square-distinguishable random $[n, rm]_q$-code, then*

$$\mathrm{HF}_{\$}(2) = \frac{1}{rm+1}\binom{rm+1}{3}\binom{rm+1}{2} - \binom{rm}{2}(n-rm) + \binom{n-rm}{2}.$$

The Hilbert function at degree 2 as a distinguisher

Goal. Distinguish $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp$ from a random $[n, rm]_q$-code **assuming** $(\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^\perp)^{\star 2} = \mathbb{F}_q^n$.

Proposition 12 (Random case)

*If $\mathscr{C}$ is a **non**-square-distinguishable random $[n, rm]_q$-code, then*

$$\mathrm{HF}_{\$}(2) = \frac{1}{rm+1}\binom{rm+1}{3}\binom{rm+1}{2} - \binom{rm}{2}(n-rm) + \binom{n-rm}{2}.$$

What happens for generic alternant codes ?

First step: GRS codes

Lemma 13 (Bardet, Mora, Tillich)

It holds that

$$(\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^{\perp})_{\mathbb{F}_{q^m}} = \sum_{j=0}^{m-1} \mathbf{GRS}_r(\boldsymbol{x}^{q^j},\boldsymbol{y}^{q^j}).$$

With the usual assumption $\dim_{\mathbb{F}_q} \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) = n - rm$*, the sum becomes direct.*

First step: GRS codes

Lemma 13 (Bardet, Mora, Tillich)

It holds that

$$(\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^{\perp})_{\mathbb{F}_{q^m}} = \sum_{j=0}^{m-1} \mathbf{GRS}_r(\boldsymbol{x}^{q^j},\boldsymbol{y}^{q^j}).$$

With the usual assumption $\dim_{\mathbb{F}_q} \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y}) = n - rm$, *the sum becomes direct.*

Conjecture 14 (HF(2) for square-distinguishable Reed-Solomon codes)

If $2r-1 \leqslant n$, *then the Hilbert function at degree 2 associated with a* **GRS** *code of dimension* r *is given by*

$$\mathrm{HF}_{\boldsymbol{GRS}}(2) = \binom{\binom{r-1}{2}+1}{2} - \binom{r}{4} = \frac{1}{12}(r-1)(r-2)(r^2-3r+6).$$

From GRS codes to alternant codes

Theorem 15 (This work)

Assume Conjecture 14 holds. The Hilbert function at degree 2 of the algebraic modeling associated with a generic ***square-distinguishable*** *alternant code* $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ *is given by*

$$\mathrm{HF}_{\mathscr{A}}(2) = m\,\mathrm{HF}_{\boldsymbol{GRS}}(2) = \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

From GRS codes to alternant codes

Theorem 15 (This work)

Assume Conjecture 14 holds. The Hilbert function at degree 2 of the algebraic modeling associated with a generic ***square-distinguishable*** *alternant code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ is given by*

$$\mathrm{HF}_{\mathscr{A}}(2) = m\,\mathrm{HF}_{\boldsymbol{GRS}}(2) = \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

But what happens if $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ is not square-distinguishable ?

From GRS codes to alternant codes

Theorem 15 (This work)

Assume Conjecture 14 holds. The Hilbert function at degree 2 of the algebraic modeling associated with a generic ***square-distinguishable*** *alternant code* $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ *is given by*

$$\mathrm{HF}_{\mathscr{A}}(2) = m\,\mathrm{HF}_{\boldsymbol{GRS}}(2) = \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

But what happens if $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ is not square-distinguishable ?

Corollary 16

It holds that

$$\mathrm{HF}_{\mathscr{A}}(2) \geqslant \frac{m}{12}(r-1)(r-2)(r^2-3r+6).$$

A new regime for the distinguisher

Distinguishability condition: $\mathsf{HF}_{\$}(2) < \frac{m}{12}(r-1)(r-2)(r^2-3r+6)$.

A new regime for the distinguisher

Distinguishability condition: $\mathrm{HF}_{\$}(2) < \dfrac{m}{12}(r-1)(r-2)(r^2-3r+6)$.

Natural asymptotic regime: $r \longrightarrow +\infty$ and $m = \mathcal{O}(\log r)$.

A new regime for the distinguisher

Distinguishability condition: $\mathrm{HF}_{\$}(2) < \frac{m}{12}(r-1)(r-2)(r^2-3r+6)$.

Natural asymptotic regime: $r \longrightarrow +\infty$ and $m = \mathcal{O}(\log r)$.

Corollary 17

Assume $r < q+1$. The asymptotic lowest dimension k_0 for which alternant codes of degree r and extension degree m are 2-distinguishable satisfies

$$k_0 \sim \frac{1-\frac{1}{\sqrt{3}}}{2} r^2 m^2 \approx 0.21 r^2 m^2.$$

A new regime for the distinguisher

Distinguishability condition: $\mathrm{HF}_{\$}(2) < \frac{m}{12}(r-1)(r-2)(r^2-3r+6)$.

Natural asymptotic regime: $r \longrightarrow +\infty$ and $m = \mathcal{O}(\log r)$.

Corollary 17

Assume $r < q+1$. The asymptotic lowest dimension k_0 for which alternant codes of degree r and extension degree m are 2-distinguishable satisfies

$$k_0 \sim \frac{1-\frac{1}{\sqrt{3}}}{2} r^2 m^2 \approx 0.21 r^2 m^2.$$

Original square distinguisher from [FGOPT10] when $r < q+1$:

$$n > \binom{rm+1}{2} - m\frac{(r-1)(r-2)}{2} \quad \text{i.e} \quad k > k_0 = \binom{rm+1}{2} - rm - m\frac{(r-1)(r-2)}{2}$$

A new regime for the distinguisher

Distinguishability condition: $\mathrm{HF}_{\$}(2) < \frac{m}{12}(r-1)(r-2)(r^2-3r+6)$.

Natural asymptotic regime: $r \longrightarrow +\infty$ and $m = \mathcal{O}(\log r)$.

Corollary 17

Assume $r < q+1$. The asymptotic lowest dimension k_0 for which alternant codes of degree r and extension degree m are 2-distinguishable satisfies

$$k_0 \sim \frac{1-\frac{1}{\sqrt{3}}}{2} r^2 m^2 \approx 0.21 r^2 m^2.$$

Original square distinguisher from [FGOPT10] when $r < q+1$:

$$n > \binom{rm+1}{2} - m\frac{(r-1)(r-2)}{2} \quad \text{i.e} \quad k > k_0 = \binom{rm+1}{2} - rm - m\frac{(r-1)(r-2)}{2}$$

which leads to $k_0 \sim \frac{r^2 m^2}{2}$.

Plan of this Section

1. Distinguisher [FGOPT10]: nontrivial relations in a code
2. Distinguisher [CMT23]: **short** relations
3. Conclusion

Conclusion and future work

Conclusions.

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.
  $\Longrightarrow$ much wider regime than [FGOPT10] !

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.
  $\Longrightarrow$ much wider regime than [FGOPT10] !

Future work.

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.
  $\Longrightarrow$ much wider regime than [FGOPT10] !

Future work.

- Find a formula for $r \geqslant q + 1$;

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.
  $\Longrightarrow$ much wider regime than [FGOPT10] !

Future work.

- Find a formula for $r \geqslant q + 1$;
- Find another algebraic interpretation of the distinguisher;

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.
  $\Longrightarrow$ much wider regime than [FGOPT10] !

Future work.

- Find a formula for $r \geqslant q + 1$;
- Find another algebraic interpretation of the distinguisher;
- See if it can be turned into and attack.

Conclusion and future work

Conclusions.

- Understanding of the **new** distinguisher at degree 2 for large field size ($r < q + 1$).
- A proof for a regime of parameters which are 2-distinguishable **for sure**.
  $\Longrightarrow$ much wider regime than [FGOPT10] !

Future work.

- Find a formula for $r \geqslant q + 1$;
- Find another algebraic interpretation of the distinguisher;
- See if it can be turned into and attack.

Thank you for your attention.

Change of basis

What does *really* depend on the basis ?

Change of basis

What does *really* depend on the basis ?

Proposition 18

Let $\mathcal{A}, \mathcal{B}$ be two bases of the same code $\mathscr{C}$. There exists $\boldsymbol{P} \in \mathbf{GL}_k(\mathbb{F}_q)$ such that

$$\mathscr{C}_{mat}(\mathcal{A}) = \boldsymbol{P}^\top \mathscr{C}_{mat}(\mathcal{B}) \boldsymbol{P}.$$

Change of basis

What does *really* depend on the basis ?

Proposition 18

Let $\mathcal{A}, \mathcal{B}$ be two bases of the same code $\mathscr{C}$. There exists $\boldsymbol{P} \in \mathbf{GL}_k(\mathbb{F}_q)$ such that

$$\mathscr{C}_{mat}(\mathcal{A}) = \boldsymbol{P}^\top \mathscr{C}_{mat}(\mathcal{B}) \boldsymbol{P}.$$

$\Longrightarrow$ The number of rank r matrices does not depend on the basis !

Explicit algebraic modeling

Idea: compute a basis $(M_1, \ldots, M_N)$ of $\mathscr{C}_{\mathsf{mat}}$ and write

$$\boldsymbol{M} = \sum_{i=1}^{N} X_i M_i.$$

Explicit algebraic modeling

Idea: compute a basis $(M_1, \ldots, M_N)$ of $\mathscr{C}_{\mathsf{mat}}$ and write

$$\boldsymbol{M} = \sum_{i=1}^{N} X_i M_i.$$

$\hookrightarrow$ write quadratic equations ensuring that $\mathrm{rk}(\boldsymbol{M}) \leqslant 2$.

Explicit modeling for square-distinguishable Reed-Solomon codes

For $r = 5$, we have

$$\boldsymbol{M} = \begin{pmatrix} 0 & 0 & X_1 & X_2 & X_4 \\ 0 & 0 & X_2 & X_3 & X_5 \\ X_1 & X_2 & 0 & X_5 & X_6 \\ X_2 & X_3 & X_5 & 0 & 0 \\ X_4 & X_5 & X_6 & 0 & 0 \end{pmatrix}$$

Explicit modeling for square-distinguishable Reed-Solomon codes

For $r = 6$, we have

$$\boldsymbol{M} = \begin{pmatrix} 0 & 0 & X_1 & X_2 & X_4 & X_6 \\ 0 & 0 & X_2 & X_3 & X_5 & X_8 \\ X_1 & X_2 & 0 & X_5 + X_6 & X_7 & X_9 \\ X_2 & X_3 & X_5 + X_6 & 0 & X_9 & X_{10} \\ X_4 & X_5 & X_7 & X_9 & 0 & 0 \\ X_6 & X_8 & X_9 & X_{10} & 0 & 0 \end{pmatrix}$$

Explicit modeling for square-distinguishable Reed-Solomon codes

For $r = 8$, we have

$$\boldsymbol{M} = \begin{pmatrix} 0 & 0 & X_1 & X_2 & X_4 & X_6 & X_9 & X_{12} \\ 0 & 0 & X_2 & X_3 & X_5 & X_8 & X_{11} & X_{15} \\ X_1 & X_2 & 0 & X_5 + X_6 & X_7 & X_{10} & X_{14} & X_{17} \\ X_2 & X_3 & X_5 + X_6 & 0 & X_{10} + X_{11} + X_{12} & X_{13} & X_{16} & X_{19} \\ X_4 & X_5 & X_7 & X_{10} + X_{11} + X_{12} & 0 & X_{16} + X_{17} & X_{18} & X_{20} \\ X_6 & X_8 & X_{10} & X_{13} & X_{16} + X_{17} & 0 & X_{20} & X_{21} \\ X_9 & X_{11} & X_{14} & X_{16} & X_{18} & X_{20} & 0 & 0 \\ X_{12} & X_{15} & X_{17} & X_{19} & X_{20} & X_{21} & 0 & 0 \end{pmatrix}$$

And the equations

For $r = 6$, the Pfaffians of $\boldsymbol{M}$ of size 4 are

$$\begin{aligned}\mathrm{Pf}(\boldsymbol{M}, 2) = \{&X_2^2 + X_1X_3, X_2X_4 + X_1X_5, X_2X_6 + X_1X_8, X_3X_4 + X_2X_5,\\ &X_3X_6 + X_2X_8, X_5X_6 + X_4X_8, X_4X_5 + X_4X_6 + X_2X_7 + X_1X_9,\\ &X_5X_6 + X_6^2 + X_2X_9 + X_1X_{10}, X_6X_7 + X_4X_9, X_6X_9 + X_4X_{10},\\ &X_5^2 + X_5X_6 + X_3X_7 + X_2X_9, X_5X_8 + X_6X_8 + X_3X_9 + X_2X_{10},\\ &X_7X_8 + X_5X_9, X_8X_9 + X_5X_{10}, X_9^2 + X_7X_{10}\}.\end{aligned}$$

Actual McEliece specs

$G_{\mathrm{pub}} = S \cdot G_{\mathrm{priv}} \cdot P_\sigma$ where $S \in \mathrm{GL}_k(\mathbb{F}_q)$ and $P_\sigma \stackrel{\mathrm{def}}{=} (\delta_{i,\sigma(j)})_{i,j}$ for some $\sigma \in \mathfrak{S}_n$.

Actual McEliece specs

$G_{\text{pub}} = S \cdot G_{\text{priv}} \cdot P_\sigma$ where $S \in \mathrm{GL}_k(\mathbb{F}_q)$ and $P_\sigma \stackrel{\text{def}}{=} (\delta_{i,\sigma(j)})_{i,j}$ for some $\sigma \in \mathfrak{S}_n$.

Proposition 19

Let $\mathscr{C} \subset \mathbb{F}_q^n$ be a code. Then

$$(\mathscr{C} \cdot P_\sigma)^\perp = (\mathscr{C}^\perp) \cdot P_{\sigma^{-1}},$$

where $\mathscr{C} \cdot P_\sigma = \{w^\sigma \stackrel{\text{def}}{=} (w_{\sigma(1)}, \ldots, w_{\sigma(n)})\}$. If $\boldsymbol{G}$ is a generator matrix of $\mathscr{C}$, then $\boldsymbol{G}P$ is a generator matrix of $\mathscr{C} \cdot P$.

Actual McEliece specs

$G_{\text{pub}} = S \cdot G_{\text{priv}} \cdot P_\sigma$ where $S \in \mathrm{GL}_k(\mathbb{F}_q)$ and $P_\sigma \stackrel{\text{def}}{=} (\delta_{i,\sigma(j)})_{i,j}$ for some $\sigma \in \mathfrak{S}_n$.

Proposition 19

Let $\mathscr{C} \subset \mathbb{F}_q^n$ be a code. Then

$$(\mathscr{C} \cdot P_\sigma)^\perp = (\mathscr{C}^\perp) \cdot P_{\sigma^{-1}},$$

where $\mathscr{C} \cdot P_\sigma = \{w^\sigma \stackrel{\text{def}}{=} (w_{\sigma(1)}, \ldots, w_{\sigma(n)})\}$. If $\boldsymbol{G}$ is a generator matrix of $\mathscr{C}$, then $\boldsymbol{G}P$ is a generator matrix of $\mathscr{C} \cdot P$.

Corollary 20

$\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) \cdot P_\sigma = \mathscr{A}_r(\boldsymbol{x}^{\sigma^{-1}}, \boldsymbol{y}^{\sigma^{-1}})$.

Actual McEliece specs

By Proposition 19,

$$(\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})\cdot P_\sigma)^\perp = \mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^\perp \cdot P_{\sigma^{-1}}.$$

Delstarte's theorem: $\mathscr{A}_r(\boldsymbol{x},\boldsymbol{y})^\perp = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\mathbf{GRS}_r(\boldsymbol{x},\boldsymbol{y}))$ has generator matrix

$$\boldsymbol{G} \stackrel{\text{def}}{=} \begin{pmatrix} y_1^{(1)} & y_2^{(1)} & \cdots & y_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(m)} & y_2^{(m)} & \cdots & y_n^{(m)} \\ \vdots & \vdots & \ddots & \vdots \\ (y_1 x_1^{r-1})^{(1)} & (y_2 x_2^{r-1})^{(1)} & \cdots & (y_n x_n^{r-1})^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ (y_1 x_1^{r-1})^{(m)} & (y_2 x_2^{r-1})^{(m)} & \cdots & (y_n x_n^{r-1})^{(m)} \end{pmatrix}.$$

Therefore, $\boldsymbol{G}\cdot P_{\sigma^{-1}}$ is a generator matrix of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\mathbf{GRS}_r(\boldsymbol{x}^{\sigma^{-1}},\boldsymbol{y}^{\sigma^{-1}}))$.