Recent algebraic attacks on the McEliece cryptosystem

Jean-Pierre Tillich

Recent algebraic attacks on the McEliece cryptosystem

J.-P. Tillich (Inria de Paris)

June 21, 2023

Joint work

- "On the dimension and structure of the square of the dual of a Goppa code", R. Mora, J.-P. Tillich, Designs, Codes and Cryptography, 2022
- "Polynomial time key-recovery attack on high rate random alternant codes", M. Bardet, R. Mora, J.-P. Tillich, `https://arxiv.org/abs/2304.14757`
- "A new approach based on quadratic forms to attack the McEliece cryptosystem", A. Couvreur, R. Mora, J.-P. Tillich, `https://eprint.iacr.org/2023/950`

1. The McEliece cryptosystem

- 1978 McEliece cryptosystem based on Goppa codes.

- Secret Key : The algebraic structure of an $[n, k]_q$ Goppa code $\mathcal{C}$ which has an efficient decoding algorithm for decoding t errors

- Public Key : an arbitrary generator matrix $\boldsymbol{G}$ of $\mathcal{C}$.

- Encryption : $\boldsymbol{m} \in \mathbb{F}_q^k \longmapsto \boldsymbol{y} \stackrel{\text{def}}{=} \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| = t$.

- Decryption : $\boldsymbol{y} \longmapsto \boldsymbol{m} = \texttt{Decode}(\boldsymbol{y})$.

Advantages/drawbacks

Advantages

- Post Quantum, 4th-round finalist of the NIST competition;
- 55 years of research have not changed much the picture

> Compl. of key attacks $\gg$ Compl. of message attacks $\approx 2^{\alpha n}$ with $\alpha \approx$ Constant

- Efficient encryption and decryption

Drawbacks

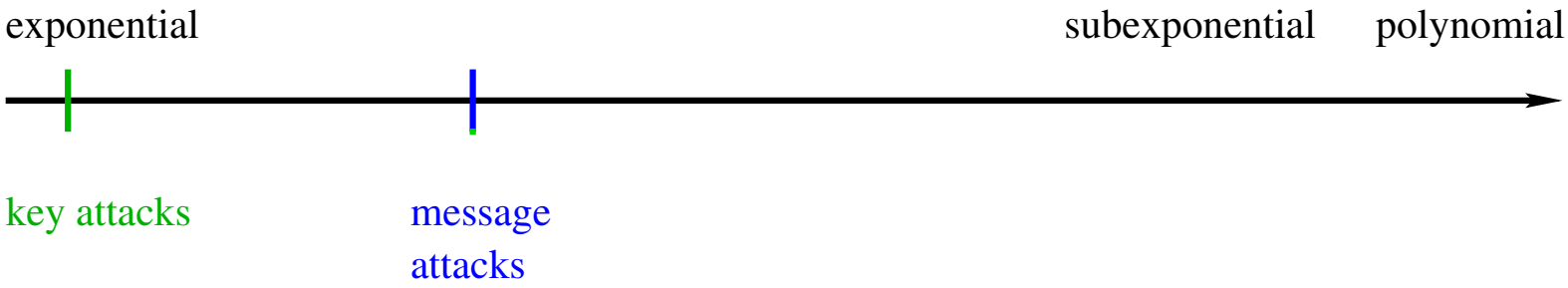
- Huge size of the keys, Classic McEliece $\approx$ 260 Kbytes.

Key Attacks/Message Attacks (pre 2011)

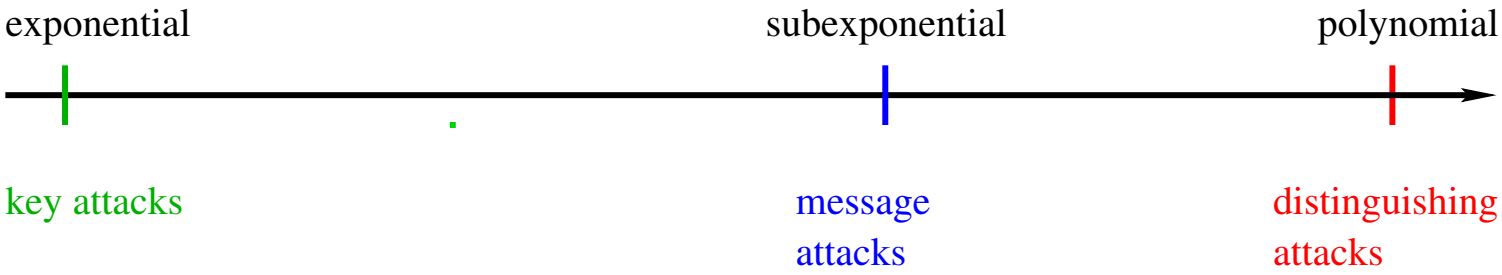
- Key attack:(pre 2011) Enumerating all Goppa polynomial + solving the code-equivalence problem
- Message attack: Decoding a generic linear code

Key Attacks/Message Attacks (2011)

- Distinguishing Attack [Faugère-Gauthier-Otmani-Perret-Tillich-2011]: distinguishing a Goppa/alternant code from a generic linear code
- $n - k = \Theta(n)$



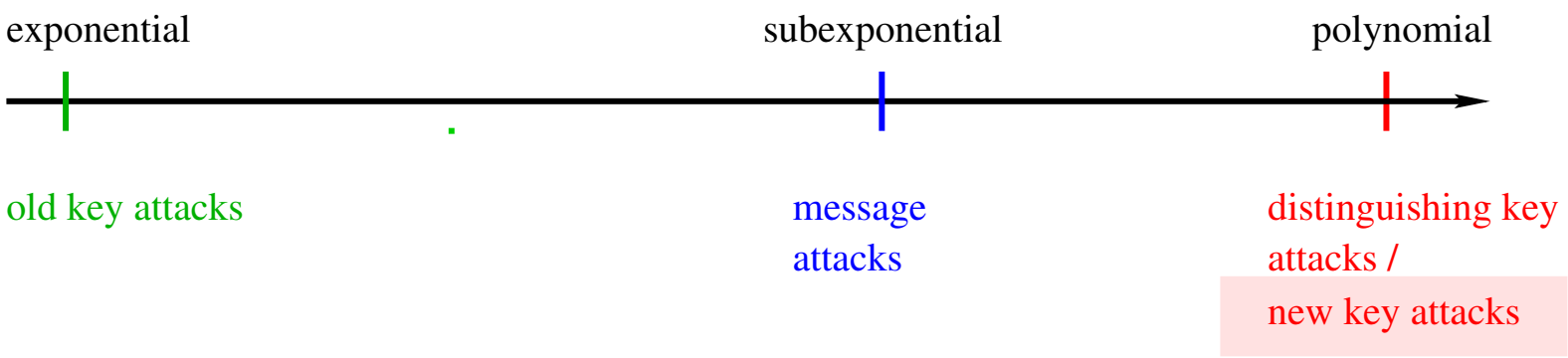
- $n - k = O\left(n^{\frac{1}{2}}\right)$



Key Attacks/Message Attacks [BMT23]

Assumptions:

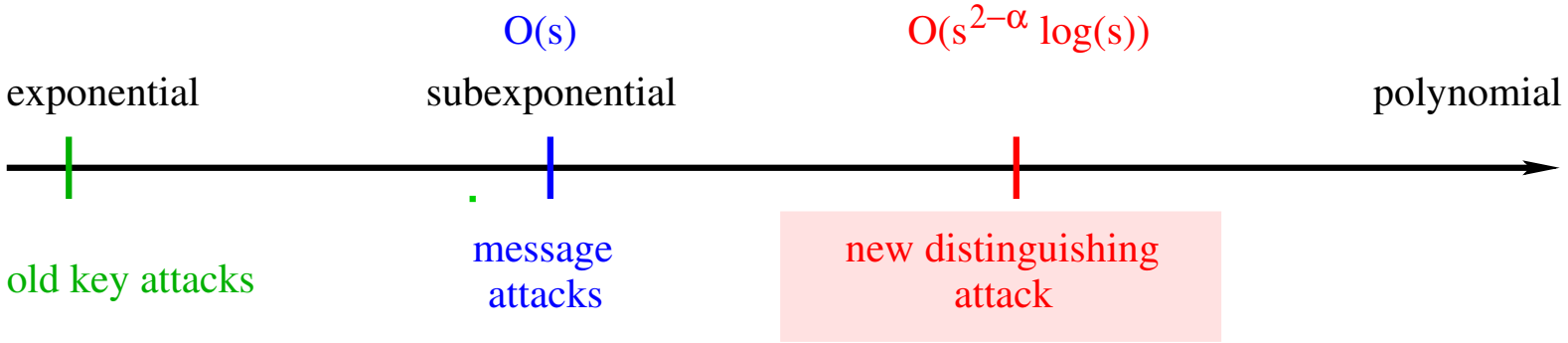
1. the code should be distinguishable ($\Rightarrow n - k = O\left(n^{\frac{1}{2}}\right)$) with the method of [FGOPT11]
2. should be a generic alternant code rather than a Goppa code
3. $q \in \{2, 3\}$



A new approach and a new distinguisher [CMT23]

- Associating a space of quadratic forms to an alternant/Goppa code and looking for low rank quadratic forms in it by Gröbner basis techniques
  $\Rightarrow$ a new distinguisher in characteristic 2

$$\begin{aligned} s &\stackrel{\text{def}}{=} n-k \\ n &= s^{\alpha} \\ \alpha &\in (1,2) \end{aligned}$$



A new approach and a new attack [CMT23]

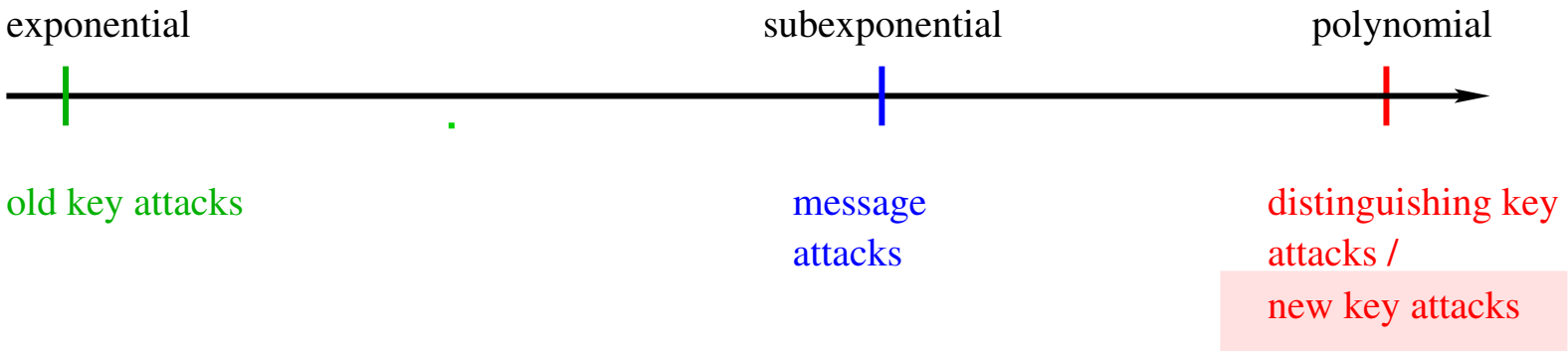
Assumption:

- Generic alternant and distinguishable [FGOPT11] codes

or

- distinguishable [FGOPT11] Goppa codes with

$$\deg(\text{Goppa polynomial}) < q - 1$$



2.Alternant and Goppa Codes

Generalized Reed-Solomon codes

Definition 1. [Generalized Reed-Solomon code] *k and n integers with $1 \leqslant k < n \leqslant q$ where q is a power of a prime number. The generalized Reed-Solomon code $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ of dimension k associated to a pair $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ where $\boldsymbol{x}$ is an n-tuple of distinct elements of $\mathbb{F}_q$ and the entries y_i are arbitrary nonzero elements in $\mathbb{F}_q$ is defined as:*

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} \Big\{ (y_1 p(x_1), \ldots, y_n p(x_n)) : p \in \mathbb{F}_q[X], \deg p < k \Big\}.$$

$\boldsymbol{x}$ is the support and $\boldsymbol{y}$ the multiplier.

[Sidelnikov-Shestakov1992]: recover from an arbitrary generator matrix of a GRS code $\mathcal{C}$, a tuple $(\boldsymbol{x}, \boldsymbol{y})$ such that $\mathcal{C} = \mathbf{GRS}(\boldsymbol{x}, \boldsymbol{y})$ (all what is needed to decode $\mathcal{C}$ efficiently).

Alternant codes

Definition 1. [alternant/Goppa code] *$\boldsymbol{x} \in \mathbb{F}_{q^m}^n, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ as in def. of GRS codes, $\Gamma \in \mathbb{F}_{q^m}[z]$, $\deg \Gamma = r$. The alternant code $\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y})$, resp. Goppa code $\mathbf{Gop}(\boldsymbol{x}, \Gamma)$ of support $\boldsymbol{x}$, degree r and extension degree m are defined by*

$$\begin{aligned}
\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y}) &\stackrel{def}{=} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp \cap \mathbb{F}_q^n \\
&= \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}^\perp) \cap \mathbb{F}_q^n \quad \textit{(subfield subcode of GRS)} \\
\mathbf{Gop}(\boldsymbol{x}, \Gamma) &= \mathbf{Alt}_r(\boldsymbol{x}, \frac{1}{\Gamma(\boldsymbol{x})})
\end{aligned}$$

$$\begin{aligned}
\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp &= \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}^\perp) \\
\boldsymbol{y}^\perp &\stackrel{\text{def}}{=} \left(\frac{1}{y_i \pi_x'(x_1)}, \cdots, \frac{1}{y_i \pi_x'(x_1)} \right) \\
\pi_x(x) &\stackrel{\text{def}}{=} (x - x_1) \cdots (x - x_n)
\end{aligned}$$

3. The square code

- Key ingredient for the [FGOPT11]/[MT22] distinguisher and the [BMT23] attack
- Introduced for cryptanalyzing the Berger-Loidreau scheme by Wieschebrink in 2010

The square code

Definition 2. [Componentwise product] *Given two vectors* $\boldsymbol{a} = (a_1, \ldots, a_n)$ *and* $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, *we denote by* $\boldsymbol{a} \star \boldsymbol{b}$ *the componentwise product*

$$\boldsymbol{a} \star \boldsymbol{b} \stackrel{def}{=} (a_1 b_1, \ldots, a_n b_n)$$

Definition 3. [Product of codes & square code] *The star product code denoted by* $\mathcal{A} \star \mathcal{B}$ *of* $\mathcal{A}$ *and* $\mathcal{B}$ *is the vector space spanned by all products* $\boldsymbol{a} \star \boldsymbol{b}$ *where* $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *range over* $\mathcal{A}$ *and* $\mathcal{B}$ *respectively. When* $\mathcal{B} = \mathcal{A}$, $\mathcal{A} \star \mathcal{A}$ *is called the square code of* $\mathcal{A}$ *and is rather denoted by* $\mathcal{A}^2$.

Dimension of the square code

$\mathcal{A}$ and $\mathcal{B}$ codes with respective bases $(\boldsymbol{a}_i)$ and $(\boldsymbol{b}_j)$.

1. $\dim(\mathcal{A} \star \mathcal{B}) \leqslant \dim(\mathcal{A}) \dim(\mathcal{B})$ (generated by the $\boldsymbol{a}_i \star \boldsymbol{b}_j$'s)
2. $\dim(\mathcal{A}^2) \leqslant \binom{\dim(\mathcal{A}) + 1}{2}$ (generated by the $\boldsymbol{a}_i \star \boldsymbol{a}_j$'s with $i \leqslant j$)

What is wrong with generalized Reed-Solomon codes ?

When $\mathcal{C}$ is a random code of length n, with high probability

$$\dim(\mathcal{C}^2) = \min\left\{\binom{\dim(\mathcal{C})+1}{2}, n\right\}$$

When $\mathcal{C}$ is a generalized Reed-Solomon code

$$\dim(\mathcal{C}^2) = \min\left\{2\dim(\mathcal{C}) - 1, n\right\}$$

The explanation

$\boldsymbol{c} = (y_1 p(x_1), \ldots, y_n p(x_n))$, $\boldsymbol{c}' = (y_1 q(x_1), \ldots, y_n q(x_n)) \in \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$

where p and q are two polynomials of degree at most $k-1$.

$$\boldsymbol{c} \star \boldsymbol{c}' = \left(y_1^2 p(x_1) q(x_2), \ldots, y_n^2 p(x_n) q(x_n)\right) = \left(y_1^2 r(x_1), \ldots, y_n^2 r(x_n)\right)$$

where r is a polynomial of degree $\leqslant 2k-2$.

$$\Longrightarrow \boldsymbol{c} \star \boldsymbol{c}' \in \mathbf{GRS}_{2k-1}(\boldsymbol{x}, \boldsymbol{y}^2)$$

What happens for alternant/Goppa codes [FGOPT11][MT22]?

Alternant/Goppa code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, degree r, ext. deg. m

$$\begin{aligned}
\dim \mathcal{C}^{\perp} &\overset{\text{typ.}}{=} rm \\
\dim\left(\left(\mathcal{C}_{\mathsf{Gop}}^{\perp}\right)^2\right) &\leqslant \dim\left(\left(\mathcal{C}_{\mathsf{alt}}^{\perp}\right)^2\right) \\
\dim\left(\left(\mathcal{C}^{\perp}\right)^2\right) &\leqslant \min\left(n, \underbrace{\binom{mr+1}{2}}_{\dim \mathcal{R}^2} - \Omega\left(mr^2 \log r\right)\right) \\
\mathcal{R} &\overset{\text{def}}{=} \text{random code of length } n, \text{ dim } rm
\end{aligned}$$

4. [BMT23] : filtration attack + Gröbner bases

- Transforming the distinguisher into an attack

A theorem

$\mathcal{C}$ a code of length n, $I, J \subset \{1, \cdots, n\}$

$$\begin{aligned} \boldsymbol{x}_J &= (x_j)_{j \in J} \\ \boldsymbol{x}_{\setminus I} &= (x_j)_{j \notin I} \\ \text{Shortened code } \mathbf{Sh}_I(\mathcal{C}) &= \{\boldsymbol{c}_{\setminus I} : \boldsymbol{c} \in c_i = 0, \forall i \in I\} \end{aligned}$$

Theorem 1. [BMT23] *Let* $\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y})$ *be an alternant code on* $\mathbb{F}_q$ *such that* $r \geqslant q+1$ *and let* $\mathcal{C} \stackrel{def}{=} \mathbf{Alt}_r(\boldsymbol{x}_{\setminus i}, \boldsymbol{y}_{\setminus i})^\perp$, $\mathcal{D} \stackrel{def}{=} \left(\mathbf{Sh}_i\left(\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y})^\perp\right)\right)^2$, *then*

$$\mathcal{C} \star \mathbf{Alt}_{r-1}(\boldsymbol{x}_{\setminus i}, \boldsymbol{y}_{\setminus i}(\boldsymbol{x}_{\setminus i} - x_i))^\perp \subseteq \mathcal{D}$$

Filtration

- For given subspaces $\mathcal{A}$ and $\mathcal{B}$, computing the largest subspace $\mathcal{X}$ such that

$$\mathcal{A} \star \mathcal{X} \subseteq \mathcal{B}$$

is just solving a linear system.

Conjecture 1. *For $r \geqslant q+1$ and if $\left(\mathbf{Sh}_i\left(\mathbf{Alt}_r(\boldsymbol{x},\boldsymbol{y})^\perp\right)\right)^2$ is not the full space. Let $\mathcal{X}$ be largest subspace such that $\mathcal{C} \star \mathcal{X} \subset \mathcal{D}$. Then for a generic alternant code*

$$\mathcal{X} = \mathbf{Alt}_{r-1}(\boldsymbol{x}_{\setminus i}, \boldsymbol{y}_{\setminus i}(\boldsymbol{x}_{\setminus i} - x_i))^\perp$$

For a Goppa code $\mathbf{Alt}_{r-1}(\boldsymbol{x}_{\setminus i}, \boldsymbol{y}_{\setminus i}(\boldsymbol{x}_{\setminus i} - x_i))^\perp \subset \mathcal{X}$

Filtration (ii)+attack

- $\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y}) \to \mathbf{Alt}_{r-1}(\boldsymbol{x}_{\setminus i}, \cdots)^{\perp} \to \cdots \to \mathbf{Alt}_q(\boldsymbol{x}_{\setminus I}, \cdots)^{\perp}$
- The support $\boldsymbol{x}$ and multiplier $\boldsymbol{y}$ of an alternant code $\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y})$ can be recovered efficiently by a suitable algebraic modeling + Gröbner bases techniques when $r = 3 \Rightarrow$

efficient attack when $q \in \{2, 3\}$

GRS codes

$$
\begin{aligned}
\mathcal{C} &\overset{\text{def}}{=} \mathbf{GRS}_k(\boldsymbol{x}_{\setminus i}, \boldsymbol{y}_{\setminus i}) \\
&= \{(y_j P(x_j))_{j\neq i} : \deg P \leqslant k-1\} \\
\mathcal{D} &\overset{\text{def}}{=} \left(\mathbf{Sh}_i\left(\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})\right)\right)^2 \\
&= \{(y_j (x_j - x_i)^2 P(x_j))_{j\neq i} : \deg P \leqslant 2k-4\} \text{ since} \\
\mathbf{Sh}_i\left(\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})\right) &= \{(y_j (x_j - x_i) P(x_j))_{j\neq i} : \deg P \leqslant k-2\} \\
\mathcal{X} &= \mathbf{GRS}_{k-2}(\boldsymbol{x}_{\setminus i}, \boldsymbol{y}_{\setminus i}(\boldsymbol{x}_{\setminus i} - x_i)^2) \\
&= \{(y_j (x_j - x_i)^2 P(x_j))_{j\neq i} : \deg P \leqslant k-3\}
\end{aligned}
$$

$$\boxed{\mathcal{C} \star \mathcal{X} = \mathcal{D}}$$

5. A new tool : quadratic forms

Going to the big field

$\mathcal{C} \subseteq (\mathbb{F}_q)^n$, $\mathcal{C}_{\mathbb{F}_{q^m}} \stackrel{\text{def}}{=}$ linear span of $\mathcal{C}$ over $\mathbb{F}_{q^m}$.

Proposition 1.

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

$$\boldsymbol{c}_a \stackrel{\text{def}}{=} \boldsymbol{y}\boldsymbol{x}^a \in \left(\mathbf{Alt}_r(\boldsymbol{x},\boldsymbol{y})^{\perp}\right)_{\mathbb{F}_{q^m}}$$

$$\boxed{\boldsymbol{c}_0 \star \boldsymbol{c}_2 = \boldsymbol{c}_1^2}$$

Quadratic relations between codewords

$\mathcal{C}$ an $[n,k]$-code over $\mathbb{F}$, $\mathcal{V} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ a basis of $\mathcal{C}$

$$\mathcal{C}_{\mathsf{rel}}(\mathcal{V}) \stackrel{\mathsf{def}}{=} \{\boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k} \mid \sum_{i \leqslant j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j = 0\} \subseteq \mathbb{F}^{\binom{k+1}{2}}$$

$$Q_{\boldsymbol{c}}(x_1, \cdots, x_k) = \sum_{i \leqslant j} c_{i,j} x_i x_j$$

$$\boldsymbol{x} \boldsymbol{M}_{\boldsymbol{c}} \boldsymbol{y}^{\mathsf{T}} = Q_{\boldsymbol{c}}(\boldsymbol{x} + \boldsymbol{y}) - Q_{\boldsymbol{c}}(\boldsymbol{x}) - Q_{\boldsymbol{c}}(\boldsymbol{y})$$

$$\mathcal{C}_{\mathsf{mat}}(\mathcal{V}) \stackrel{\mathsf{def}}{=} \{\boldsymbol{M}_{\boldsymbol{c}} = (m_{i,j})_{\substack{1 \leqslant i \leqslant k \\ 1 \leqslant j \leqslant k}} \mid \boldsymbol{c} = (c_{i,j})_{1 \leqslant i \leqslant j \leqslant k} \in \mathcal{C}_{\mathsf{rel}}(\mathcal{V})\}$$

$$\boldsymbol{M}_{\boldsymbol{c}} \stackrel{\mathsf{def}}{=} \begin{cases} m_{i,j} \stackrel{\mathsf{def}}{=} m_{j,i} \stackrel{\mathsf{def}}{=} c_{i,j}, & 1 \leqslant i < j \leqslant k, \\ m_{i,i} \stackrel{\mathsf{def}}{=} 2c_{i,i}, & 1 \leqslant i \leqslant k. \end{cases}$$

Low rank matrices

‘

$$\boldsymbol{c}_0 \star \boldsymbol{c}_2 = \boldsymbol{c}_1^2 \Rightarrow$$

$$\boldsymbol{M}_{\boldsymbol{c}} = \begin{array}{c} \text{odd characteristic} \\ \begin{pmatrix} 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & -2 & 0 & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \\ \text{rank } = 3 \end{array} \quad \begin{array}{c} \text{characteristic } 2 \\ \begin{pmatrix} 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \\ \text{rank } = 2 \end{array}$$

basis invariant, since $\exists$ an invertible matrix $\boldsymbol{P}$ such that

$$\mathcal{C}_{\mathsf{mat}}(\mathcal{A}) = \boldsymbol{P}\mathcal{C}_{\mathsf{mat}}(\mathcal{B})\boldsymbol{P}^{\mathsf{T}}$$

MinRank Problem

Problem 1. [odd characteristic] *Let* $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ *be* K *symmetric matrices in* $\mathbb{F}^{N\times N}$, *find an* $\boldsymbol{M} \in \langle \boldsymbol{M}_1, \cdots, \boldsymbol{M}_K \rangle_{\mathbb{F}}$ *of rank* 3.

Problem 2. [characteristic 2] *Let* $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K$ *be* K *skew-symmetric matrices in* $\mathbb{F}^{N\times N}$, *find an* $\boldsymbol{M} \in \langle \boldsymbol{M}_1, \cdots, \boldsymbol{M}_K \rangle_{\mathbb{F}}$ *of rank* 2.

- Geometric argument on matrix codes $\Rightarrow$ probability that there are rank 2 (char 2) or rank 3 matrix in a random matrix code of the same dimension(s) as $\mathcal{C}_{\mathsf{mat}}(\mathcal{V})$ when $\mathsf{rate}(\mathcal{C}) \leqslant 1/3$ is $o(1)$.

Algebraic modeling in characteristic 2

- $\mathcal{C}$ an $[n, k]$ code,
- $\mathcal{C}_{\mathsf{mat}}(\mathcal{V}) \in \mathbb{F}^{k\times k}$ the associated skew-symmetric matrix code $\dim \mathcal{C}_{\mathsf{mat}}(\mathcal{V}) = \binom{k}{2} - (n-k)$ when $\mathcal{C}$ is not [FGOPT11]-distinguishable.
- skew-symmetric $\boldsymbol{M} = (m_{ij})_{\substack{1\leqslant i\leqslant k\\ 1\leqslant j\leqslant k}} \in \mathbb{F}^{k\times k}$

$$\begin{aligned}
\operatorname{rank}(\boldsymbol{M}) \leqslant 2 &\Rightarrow \text{ all principal minors of } \boldsymbol{M} \text{ of size } 4 \text{ are } 0\\
&\Rightarrow m_{ab}m_{cd} + m_{ac}m_{bd} + m_{ad}m_{bc} = 0,\ \forall a, b, c, d\\
\boldsymbol{M} \in \mathcal{C}_{\mathsf{mat}}(\mathcal{V}) &\rightarrow n-k \text{ linear equations}
\end{aligned}$$

Hilbert Series

- Homogeneous ideal $\mathcal{I} \in \mathbb{K}[\boldsymbol{z}]$, $\boldsymbol{z} = (z_1, \ldots, z_n)$,
- Hilbert function of the ring $R = \mathbb{K}[\boldsymbol{z}]/\mathcal{I}$ defined as

$$\begin{aligned} \mathrm{HF}_R(d) &\stackrel{\text{def}}{=} \dim_{\mathbb{K}}(\mathbb{K}[\boldsymbol{z}]_d) - \dim_{\mathbb{K}}(\mathcal{I}_d) \\ \mathbb{K}[\boldsymbol{z}]_d &\stackrel{\text{def}}{=} \{f \in \mathbb{K}[\boldsymbol{z}] \mid \deg(f) = d\} \\ \mathcal{I}_d &\stackrel{\text{def}}{=} \mathcal{I} \cap \mathbb{K}[\boldsymbol{z}]_d \end{aligned}$$

Can be computed in time $\approx n^{\omega d}$

Generic linear code/Goppa or alternant code

- alternant/Goppa case: $\mathrm{HF}(d) > 0$ for all d.
- generic linear $[n, k]$-code:

$$\mathrm{HF}(d) = \max(0, \sum_{i=0}^{d} (-1)^i \binom{s}{i} \mathrm{HF}(d-i))$$

$$= \max(0, \sum_{i=0}^{d} (-1)^i \binom{s}{i} \left(\binom{k+d-i-2}{d-i}^2 - \binom{k+d-i-2}{d-i-1} \right.$$

where $s \stackrel{\text{def}}{=} n - k$.

$$d_0 \stackrel{\text{def}}{=} \min\{d : \mathrm{HF}(d) = 0\} \sim c\frac{k^2}{n-k}$$

Generalization of the distinguisher

- $\mathrm{HF}(1)$ = old distinguisher : $\boxed{\mathrm{HF}(1) = \binom{k+1}{2} - \dim \mathcal{C}^2}$

$\mathrm{HF}(2)$	$256 \geqslant n \geqslant 77$	$n = 76$	$n = 75$	$n = 74$	$n = 73$
Random code	0	10	71	133	196
Alternant code	**20**	**20**	71	133	196
Goppa code	**80**	**80**	**80**	133	196

Table 1: $HF(2)$ for random, alternant and Goppa codes with $q = 4, m = 4, r = 4$. In bold = distinguishable lengths.

6. New attack in the (old) distinguishable regime

Assumption 1. *The parameters are in the old distinguishable regime and* $r < q+1$ *(alternant) or* $r < q-1$ *(Goppa).*

- Recall that

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

  $\Rightarrow$ Basis $\mathcal{A}$ of $\left(\mathbf{Alt}_r(\boldsymbol{x},\boldsymbol{y})^{\perp}\right)_{\mathbb{F}_{q^m}}$ of the form

$$\mathcal{A} = (\boldsymbol{a}_0,\cdots,\boldsymbol{a}_{r-1},\boldsymbol{a}_0^q,\cdots,\boldsymbol{a}_{r-1}^q,\cdots,\boldsymbol{a}_0^{q^{m-1}},\cdots,\boldsymbol{a}_{r-1}^{q^{m-1}}),$$

$$\boldsymbol{a}_i \overset{\text{def}}{=} \boldsymbol{y}\boldsymbol{x}^i$$

- From [MT22] the quadratic relations are generated by

$$\boldsymbol{a}_a^{q^l} \star \boldsymbol{a}_b^{q^l} - \boldsymbol{a}_c^{q^l} \star \boldsymbol{a}_d^{q^l} \text{ for } a+b=c+d.$$

The Crucial Observation

The elements $\boldsymbol{A}$ of $\mathcal{C}_{\mathsf{mat}}(\mathcal{A})$ are of the form (blocks of size r)

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_0 & 0 & \cdots & 0 \\ 0 & \boldsymbol{A}_2 & & \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \boldsymbol{A}_{m-1} \end{bmatrix},$$

$$\text{If } \operatorname{rank}(\boldsymbol{A}) = rm - 1 \;\Rightarrow\; \exists j : \operatorname{rank}(\boldsymbol{A}_j) = r - 1,\ \operatorname{rank}(\boldsymbol{A}_i) = r,\ i \neq j$$

$$\text{if } \boldsymbol{v} \in \ker(\boldsymbol{A}) \;\Rightarrow\; \boldsymbol{v} = (\mathbf{0}_r, \ldots, \mathbf{0}_r, \boldsymbol{v}_j, \mathbf{0}_r, \ldots, \mathbf{0}_r)$$

$\Rightarrow$ identify the vectors generating a single GRS code $\mathbf{GRS}_r(\boldsymbol{x}^{q^j}, \boldsymbol{y}^{q^j})$

Conclusion/Open Problems

- Finding a distinguisher in odd characteristic
- Turning the distinguisher into an attack
- Attacking Goppa codes in the whole distinguishable regime
- A general methodology for studying the security of the McEliece cryptosystem