



**HAL**  
open science

# Recent algebraic attacks on the McEliece cryptosystem

Jean-Pierre Tillich

► **To cite this version:**

Jean-Pierre Tillich. Recent algebraic attacks on the McEliece cryptosystem. International Conference on Finite Fields and Their Applications 2023 (Fq15), Sihem Mesnager, Jun 2023, Aubervilliers (espace Condorcet), France. hal-04276638

**HAL Id: hal-04276638**

**<https://inria.hal.science/hal-04276638>**

Submitted on 9 Nov 2023

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# 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  $G$  of  $\mathcal{C}$ .
- Encryption :  $m \in \mathbb{F}_q^k \longmapsto y \stackrel{\text{def}}{=} mG + e$  with  $|e| = t$ .
- Decryption :  $y \longmapsto m = \text{Decode}(y)$ .

# Advantages/drawbacks

## Advantages

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

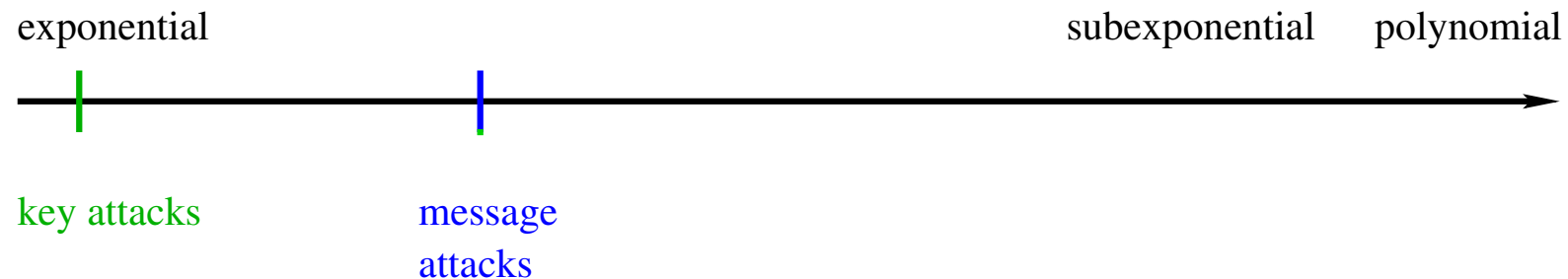
Compl. of key attacks  $\gg$  Compl. of message attacks  $\approx 2^{\alpha n}$   
with  $\alpha \approx \text{Constant}$

- Efficient encryption and decryption

## Drawbacks

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

# Key Attacks/Message Attacks (pre 2011)



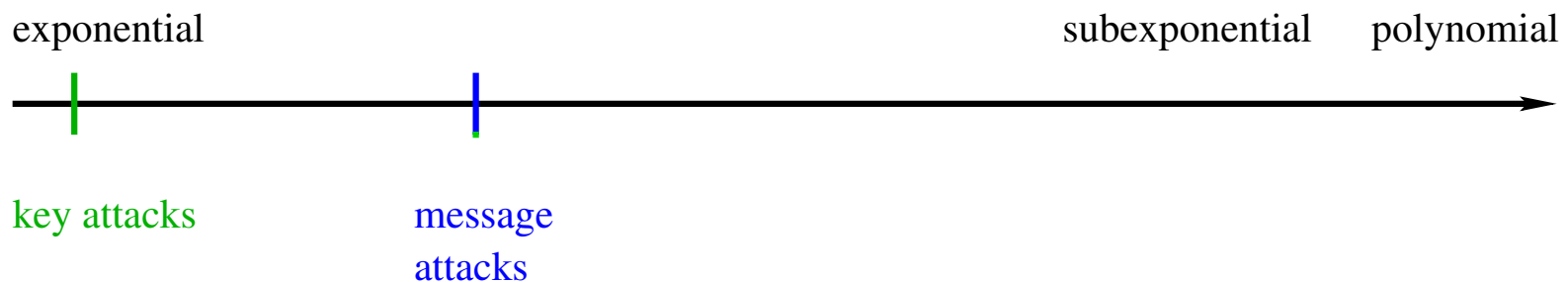
- ▶ **Key attack:** (pre 2011) Enumerating all Goppa polynomial + solving the code-equivalence problem
- ▶ **Message attack:** Decoding a generic linear code

# Key Attacks/Message Attacks (2011)

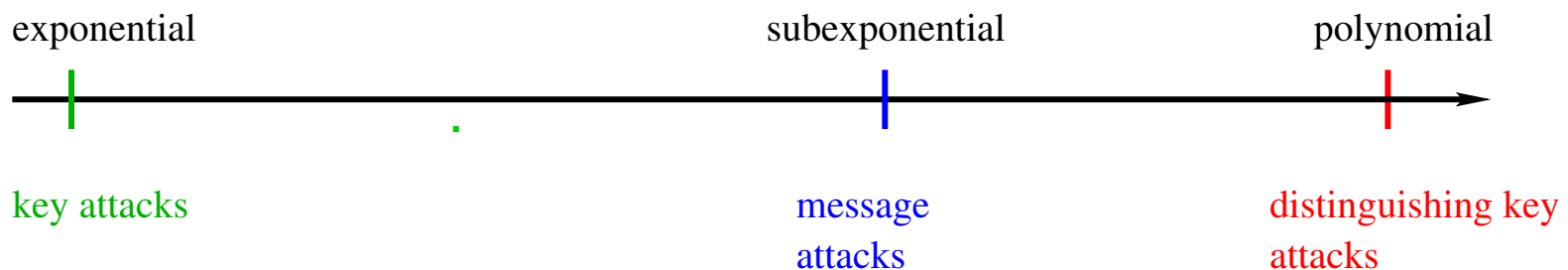
## ► Distinguishing Attack

[Faugère-Gauthier-Otmani-Perret-Tillich-2011]: distinguishing a Goppa/alternant code from a generic linear code

## ► $n - k = \Theta(n)$



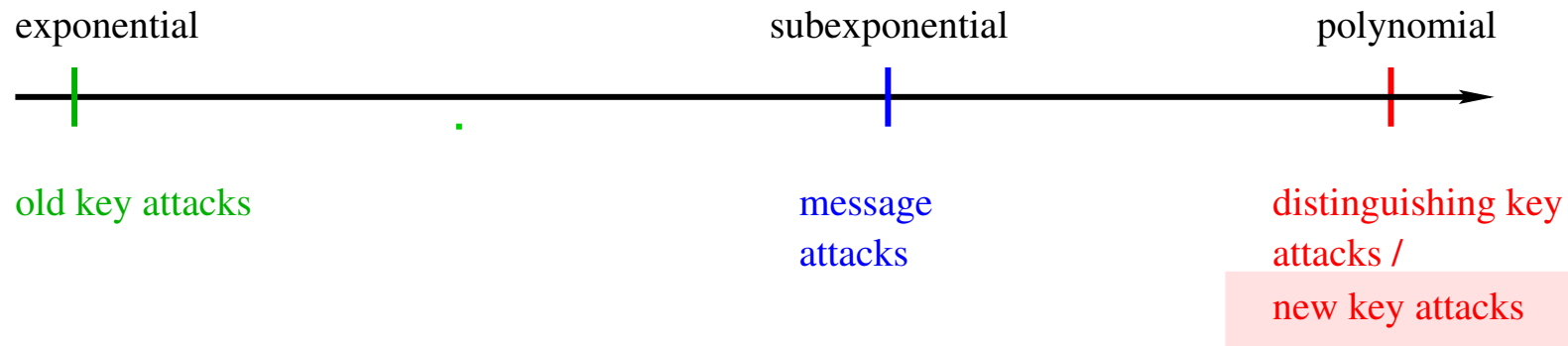
## ► $n - k = O(n^{\frac{1}{2}})$



# 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]

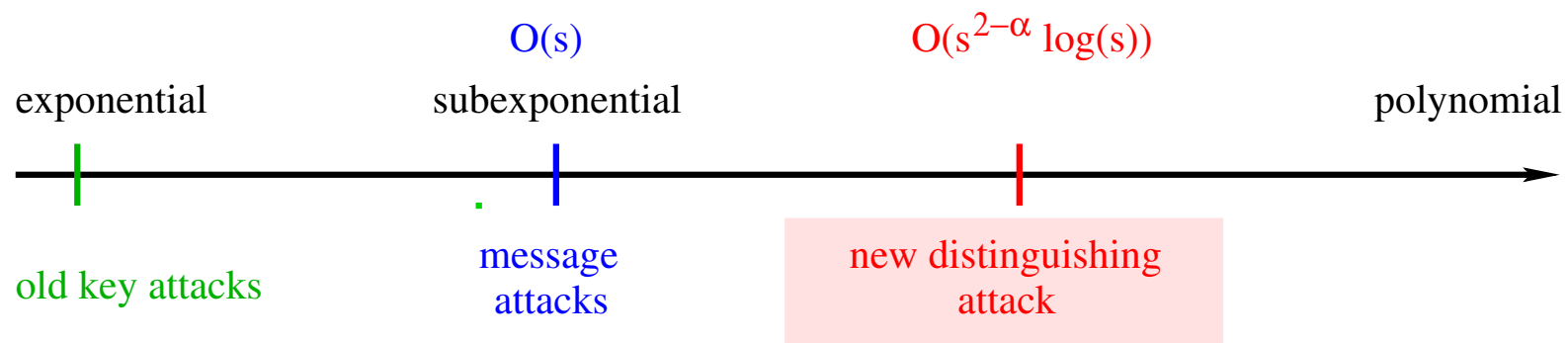
- ▶ Associating a space of quadratic forms to an alternant/Goppa code and looking for low rank quadratic forms in it by Gröbner basis techniques

⇒ a new distinguisher in characteristic 2

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

$$n = s^\alpha$$

$$\alpha \in (1, 2)$$



# A new approach and a new attack [CMT23]

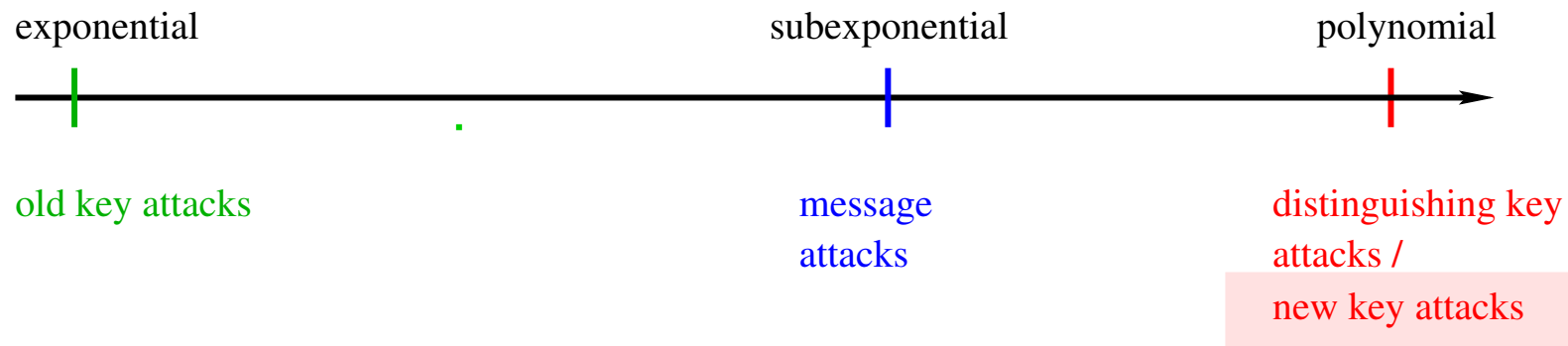
Assumption:

- 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  $1 \leq k < n \leq q$  where  $q$  is a power of a prime number. The generalized Reed-Solomon code  $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$  of dimension  $k$  associated to a pair  $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$  where  $\mathbf{x}$  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:

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

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

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

## Alternant codes

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

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

$$\mathbf{Gop}(\mathbf{x}, \Gamma) = \mathbf{Alt}_r\left(\mathbf{x}, \frac{1}{\Gamma(\mathbf{x})}\right)$$

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

## 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  $\mathbf{a} = (a_1, \dots, a_n)$  and  $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ , we denote by  $\mathbf{a} \star \mathbf{b}$  the componentwise product

$$\mathbf{a} \star \mathbf{b} \stackrel{\text{def}}{=} (a_1 b_1, \dots, a_n b_n)$$

**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*  $\mathbf{a} \star \mathbf{b}$  where  $\mathbf{a}$  and  $\mathbf{b}$  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  $(\mathbf{a}_i)$  and  $(\mathbf{b}_j)$ .

1.  $\dim(\mathcal{A} \star \mathcal{B}) \leq \dim(\mathcal{A}) \dim(\mathcal{B})$  (generated by the  $\mathbf{a}_i \star \mathbf{b}_j$ 's)

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



## 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

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

## The explanation

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

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

$$\mathbf{c} \star \mathbf{c}' = (y_1^2 p(x_1) q(x_1), \dots, y_n^2 p(x_n) q(x_n)) = (y_1^2 r(x_1), \dots, y_n^2 r(x_n))$$

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

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

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

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

$$\dim \mathcal{C}^\perp \stackrel{\text{typ.}}{=} rm$$

$$\dim \left( (\mathcal{C}_{\text{Gop}}^\perp)^2 \right) \leq \dim \left( (\mathcal{C}_{\text{alt}}^\perp)^2 \right)$$

$$\dim \left( (\mathcal{C}^\perp)^2 \right) \leq \min \left( n, \underbrace{\binom{mr+1}{2}}_{\dim \mathcal{R}^2} - \Omega(mr^2 \log r) \right)$$

$\mathcal{R} \stackrel{\text{def}}{=} \text{random code of length } n, \dim rm$

## 4. [BMT23] : filtration attack + Gröbner bases



- ▶ Transforming the distinguisher into an attack

## A theorem

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

$$\mathbf{x}_J = (x_j)_{j \in J}$$

$$\mathbf{x}_{\setminus I} = (x_j)_{j \notin I}$$

$$\text{Shortened code } \mathbf{Sh}_I(\mathcal{C}) = \{\mathbf{c}_{\setminus I} : \mathbf{c} \in \mathcal{C}, c_i = 0, \forall i \in I\}$$

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

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

## 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  $r \geq q + 1$  and if  $(\text{Sh}_i(\mathbf{Alt}_r(\mathbf{x}, \mathbf{y})^\perp))^2$  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

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

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

## Filtration (ii)+attack

- ▶  $\mathbf{Alt}_r(\mathbf{x}, \mathbf{y}) \rightarrow \mathbf{Alt}_{r-1}(\mathbf{x}_{\setminus i}, \dots)^\perp \rightarrow \dots \rightarrow \mathbf{Alt}_q(\mathbf{x}_{\setminus I}, \dots)^\perp$
- ▶ The support  $\mathbf{x}$  and multiplier  $\mathbf{y}$  of an alternant code  $\mathbf{Alt}_r(\mathbf{x}, \mathbf{y})$  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

$$\mathcal{C} \stackrel{\text{def}}{=} \mathbf{GRS}_k(\mathbf{x}_{\setminus i}, \mathbf{y}_{\setminus i})$$

$$= \{(y_j P(x_j))_{j \neq i} : \deg P \leq k - 1\}$$

$$\mathcal{D} \stackrel{\text{def}}{=} (\mathbf{Sh}_i(\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})))^2$$

$$= \{(y_j (x_j - x_i)^2 P(x_j))_{j \neq i} : \deg P \leq 2k - 4\} \text{ since}$$

$$\mathbf{Sh}_i(\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})) = \{(y_j (x_j - x_i) P(x_j))_{j \neq i} : \deg P \leq k - 2\}$$

$$\mathcal{X} = \mathbf{GRS}_{k-2}(\mathbf{x}_{\setminus i}, \mathbf{y}_{\setminus i}(\mathbf{x}_{\setminus i} - x_i)^2)$$

$$= \{(y_j (x_j - x_i)^2 P(x_j))_{j \neq i} : \deg P \leq k - 3\}$$

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



## 5. A new tool : quadratic forms

## Going to the big field

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

### Proposition 1.

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

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

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

# Quadratic relations between codewords

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

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

$$Q_{\mathbf{c}}(x_1, \dots, x_k) = \sum_{i \leq j} c_{i,j} x_i x_j$$

$$\mathbf{x} \mathbf{M}_{\mathbf{c}} \mathbf{y}^{\top} = Q_{\mathbf{c}}(\mathbf{x} + \mathbf{y}) - Q_{\mathbf{c}}(\mathbf{x}) - Q_{\mathbf{c}}(\mathbf{y})$$

$$\mathcal{C}_{\text{mat}}(\mathcal{V}) \stackrel{\text{def}}{=} \left\{ \mathbf{M}_{\mathbf{c}} = (m_{i,j})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq k}} \mid \mathbf{c} = (c_{i,j})_{1 \leq i \leq j \leq k} \in \mathcal{C}_{\text{rel}}(\mathcal{V}) \right\}$$

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

## Low rank matrices

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

odd characteristic

characteristic 2

$$M_{\mathbf{c}} = \begin{pmatrix} 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & -2 & 0 & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

rank = 3 rank = 2

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

$$\mathcal{C}_{\text{mat}}(\mathcal{A}) = \mathbf{P} \mathcal{C}_{\text{mat}}(\mathcal{B}) \mathbf{P}^{\top}$$

## MinRank Problem

**Problem 1. [odd characteristic]** Let  $M_1, \dots, M_K$  be  $K$  *symmetric* matrices in  $\mathbb{F}^{N \times N}$ , find an  $M \in \langle M_1, \dots, M_K \rangle_{\mathbb{F}}$  of rank 3.

**Problem 2. [characteristic 2]** Let  $M_1, \dots, M_K$  be  $K$  *skew-symmetric* matrices in  $\mathbb{F}^{N \times N}$ , find an  $M \in \langle M_1, \dots, M_K \rangle_{\mathbb{F}}$  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  $\mathcal{C}_{\text{mat}}(\mathcal{V})$  when  $\text{rate}(\mathcal{C}) \leq 1/3$  is  $o(1)$ .

## Algebraic modeling in characteristic 2

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

$\text{rank}(\mathbf{M}) \leq 2 \Rightarrow$  all principal minors of  $\mathbf{M}$  of size 4 are 0

$$\Rightarrow m_{ab}m_{cd} + m_{ac}m_{bd} + m_{ad}m_{bc} = 0, \forall a, b, c, d$$

$\mathbf{M} \in \mathcal{C}_{\text{mat}}(\mathcal{V}) \rightarrow n - k$  linear equations

# Hilbert Series

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

$$\text{HF}_R(d) \stackrel{\text{def}}{=} \dim_{\mathbb{K}}(\mathbb{K}[\mathbf{z}]_d) - \dim_{\mathbb{K}}(\mathcal{I}_d)$$

$$\mathbb{K}[\mathbf{z}]_d \stackrel{\text{def}}{=} \{f \in \mathbb{K}[\mathbf{z}] \mid \deg(f) = d\}$$

$$\mathcal{I}_d \stackrel{\text{def}}{=} \mathcal{I} \cap \mathbb{K}[\mathbf{z}]_d$$

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

# Generic linear code/Goppa or alternant code

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

$$\begin{aligned} \text{HF}(d) &= \max\left(0, \sum_{i=0}^d (-1)^i \binom{s}{i} \text{HF}(d-i)\right) \\ &= \max\left(0, \sum_{i=0}^d (-1)^i \binom{s}{i} \left( \binom{k+d-i-2}{d-i}^2 - \binom{k+d-i-2}{d-i-1} \right)\right) \end{aligned}$$

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

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



## Generalization of the distinguisher

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

$HF(2)$	$256 \geq n \geq 77$	$n = 76$	$n = 75$	$n = 74$	$n = 73$
Random code	0	10	71	133	196
Alternant code	<b>20</b>	<b>20</b>	71	133	196
Goppa code	<b>80</b>	<b>80</b>	<b>80</b>	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

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

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

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

$$\mathbf{a}_i \stackrel{\text{def}}{=} \mathbf{y}\mathbf{x}^i$$

► From [MT22] the quadratic relations are generated by

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

## The Crucial Observation

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

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

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

if  $\mathbf{v} \in \ker(\mathbf{A}) \Rightarrow \mathbf{v} = (\mathbf{0}_r, \dots, \mathbf{0}_r, \mathbf{v}_j, \mathbf{0}_r, \dots, \mathbf{0}_r)$

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

## 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