Algebraic attacks for the Rank Decoding Problem

Magali Bardet

magali.bardet@univ-rouen.fr

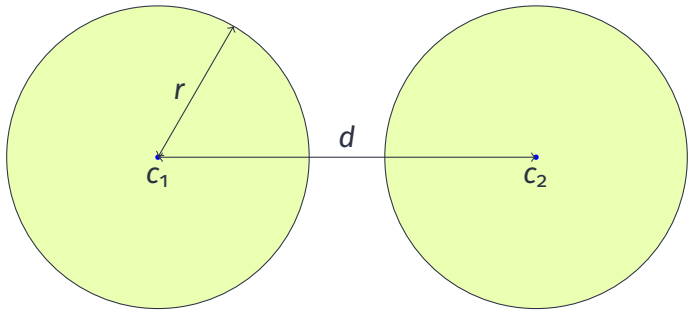
JNCF 2024,
March 4–8, 2024

Laboratoire d'Informatique,
du Traitement de
l'Information et des Systèmes

Coding Theory

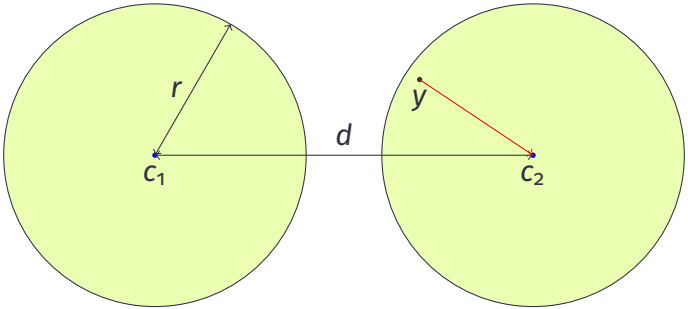
- A linear code = a linear subspace of $\mathbb{F}_q^N$, length N, dimension K.
- Generator matrix = $\boldsymbol{G} \in \mathbb{F}_q^{K \times N}$.
- Parity-check matrix = $\boldsymbol{H} \in \mathbb{F}_q^{(N-K) \times N}$ such that $\boldsymbol{G}\boldsymbol{H}^\top = 0$.
- $\mathbb{F}_q^N$ equipped with a distance.

Error correction



Minimal distance d, correction capacity $r \leq \frac{d-1}{2}$.
Nearest neighbor decoding.

Error correction



Minimal distance d, correction capacity $r \leq \frac{d-1}{2}$.
Nearest neighbor decoding.

Key generation

- Public key: a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ of a code $\mathscr{C} = \{\boldsymbol{x}\boldsymbol{G} : \boldsymbol{x} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$, r the correction capacity.

Key generation

- Public key: a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ of a code $\mathscr{C} = \{\boldsymbol{xG} : \boldsymbol{x} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$, r the correction capacity.
- Private key: an efficient decoding algorithm.

Key generation

- Public key: a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ of a code $\mathscr{C} = \{\boldsymbol{xG} : \boldsymbol{x} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$, r the correction capacity.
- Private key: an efficient decoding algorithm.
- Security: it is hard to decode efficiently from the public key.

Key generation

- Public key: a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ of a code $\mathscr{C} = \{\boldsymbol{xG} : \boldsymbol{x} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$, r the correction capacity.
- Private key: an efficient decoding algorithm.
- Security: it is hard to decode efficiently from the public key.

From codes to cryptography: McEliece cryptosystem

Key generation

- Public key: a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ of a code $\mathscr{C} = \{\boldsymbol{xG} : \boldsymbol{x} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$, r the correction capacity.
- Private key: an efficient decoding algorithm.
- Security: it is hard to decode efficiently from the public key.

Message encryption

- message $\boldsymbol{x} \in \mathbb{F}_q^K$, $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n$ of weight r.
- ciphertext $\boldsymbol{y} = \boldsymbol{xG} + \boldsymbol{e}$.

From codes to cryptography: McEliece cryptosystem

Key generation

- Public key: a generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ of a code $\mathscr{C} = \{\boldsymbol{xG} : \boldsymbol{x} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$, r the correction capacity.
- Private key: an efficient decoding algorithm.
- Security: it is hard to decode efficiently from the public key.

Message encryption

- message $\boldsymbol{x} \in \mathbb{F}_q^K$, $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n$ of weight r.
- ciphertext $\boldsymbol{y} = \boldsymbol{xG} + \boldsymbol{e}$.

Message decryption

- apply the decoding algorithm to decode $\boldsymbol{y}$ to $\hat{\boldsymbol{x}}\boldsymbol{G}$, output $\hat{\boldsymbol{x}}$.

Remarks

- given $\boldsymbol{y}$ it is easy to find $\boldsymbol{e}$ and $\boldsymbol{x}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$;

Remarks

- given $\boldsymbol{y}$ it is easy to find $\boldsymbol{e}$ and $\boldsymbol{x}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$;
- what is hard is to find such $\boldsymbol{e}$ with weight constraint: $w(\boldsymbol{e}) \leq r$.

Remarks

- given $\boldsymbol{y}$ it is easy to find $\boldsymbol{e}$ and $\boldsymbol{x}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$;
- what is hard is to find such $\boldsymbol{e}$ with weight constraint: $w(\boldsymbol{e}) \leq r$.
- equivalent formulation: given $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$ recover $\boldsymbol{e}$ such that $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{y}\boldsymbol{H}^\top$.
  $\rightarrow$ Niederreiter cryptosystem.

Remarks

- given $\boldsymbol{y}$ it is easy to find $\boldsymbol{e}$ and $\boldsymbol{x}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$;
- what is hard is to find such $\boldsymbol{e}$ with weight constraint: $w(\boldsymbol{e}) \leq r$.
- equivalent formulation: given $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$ recover $\boldsymbol{e}$ such that $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{y}\boldsymbol{H}^\top$.
  $\rightarrow$ Niederreiter cryptosystem.
- Decoding Problem or Syndrome Decoding Problem are equivalent.

Remarks

- given $\boldsymbol{y}$ it is easy to find $\boldsymbol{e}$ and $\boldsymbol{x}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$;
- what is hard is to find such $\boldsymbol{e}$ with weight constraint: $w(\boldsymbol{e}) \leq r$.
- equivalent formulation: given $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$ recover $\boldsymbol{e}$ such that $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{y}\boldsymbol{H}^\top$.
  $\rightarrow$ Niederreiter cryptosystem.
- Decoding Problem or Syndrome Decoding Problem are equivalent.
- usual distance = Hamming distance

$$d(\boldsymbol{c}, \boldsymbol{c}') = \#\{i : c_i \neq c'_i\}.$$

Code-based Signature scheme

- Private key = $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n$ of weight r;

Code-based Signature scheme

- Private key = $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n$ of weight r;
- Public key = $\boldsymbol{H} \xleftarrow{\$} \mathbb{F}_q^{(n-k)\times n}$ and $\boldsymbol{s}$ such that $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top$, $\mathscr{H}$ hash function.

Code-based Signature scheme

- Private key = $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n$ of weight r;
- Public key = $\boldsymbol{H} \xleftarrow{\$} \mathbb{F}_q^{(n-k)\times n}$ and $\boldsymbol{s}$ such that $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top$, $\mathscr{H}$ hash function.
- Interactive Zero-knowledge proof of knowledge that you know $\boldsymbol{e}$ without revealing any information on $\boldsymbol{e}$. Use of Random challenges.

Code-based Signature scheme

- Private key = $\boldsymbol{e} \xleftarrow{\$} \mathbb{F}_q^n$ of weight r;
- Public key = $\boldsymbol{H} \xleftarrow{\$} \mathbb{F}_q^{(n-k)\times n}$ and $\boldsymbol{s}$ such that $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top$, $\mathscr{H}$ hash function.
- Interactive Zero-knowledge proof of knowledge that you know $\boldsymbol{e}$ without revealing any information on $\boldsymbol{e}$. Use of Random challenges.
- Fiat-Shamir transform: non-interactive proof, challenges are computed from the message to be signed using a hash function.

Stern's Zero-knowledge protocol - Hamming metric

$$\begin{cases} w(\boldsymbol{e}) = r, \\ \boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}. \end{cases}$$

Stern's Zero-knowledge protocol - Hamming metric

$$\begin{cases} w(\boldsymbol{e}) = r, \\ \boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}. \end{cases} \iff \begin{cases} w(\pi(\boldsymbol{e})) = r, \\ (\boldsymbol{u}+\boldsymbol{e})\boldsymbol{H}^\top = \boldsymbol{s}', \end{cases} \quad \text{for } \pi \xleftarrow{\$} \mathfrak{S}_n, \boldsymbol{u} \xleftarrow{\$} \mathbb{F}_q^k.$$

Stern's Zero-knowledge protocol - Hamming metric

$$\begin{cases} w(\boldsymbol{e}) = r, \\ \boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}. \end{cases} \iff \begin{cases} w(\pi(\boldsymbol{e})) = r, \\ (\boldsymbol{u}+\boldsymbol{e})\boldsymbol{H}^\top = \boldsymbol{s}', \end{cases} \quad \text{for } \pi \xleftarrow{\$} \mathfrak{S}_n, \boldsymbol{u} \xleftarrow{\$} \mathbb{F}_q^k.$$

Prover	Verifier
$\pi \xleftarrow{\$} \mathfrak{S}_n, \boldsymbol{u} \xleftarrow{\$} \mathbb{F}_q^k$	
commit to $\begin{cases} c_1 = \mathscr{H}(\pi, \boldsymbol{u}\boldsymbol{H}^\top), \\ c_2 = \mathscr{H}(\pi(\boldsymbol{u})), \\ c_3 = \mathscr{H}(\pi(\boldsymbol{e}+\boldsymbol{u})) \end{cases}$	
	$i \xleftarrow{\$} \{1,2,3\}$
reveal $\begin{cases} i=1 & \boldsymbol{v} = \pi(\boldsymbol{e}), \boldsymbol{w} = \pi(\boldsymbol{u}) \\ i=2 & \pi, \boldsymbol{z} = \boldsymbol{e}+\boldsymbol{u} \\ i=3 & \pi, \boldsymbol{u} \end{cases}$	check $\begin{cases} i=1 & c_2, c_3, w(\boldsymbol{v}) = r \\ i=2 & c_3, c_1 \text{ with } \boldsymbol{z}\boldsymbol{H}^\top - \boldsymbol{s}. \\ i=3 & c_1, c_2. \end{cases}$

Rank metric Delsarte 1978

Codes over $\mathbb{F}_q^{mn}$ when $N = mn$

- A word $\boldsymbol{x} = (x_1, \ldots, x_{mn}) \in \mathbb{F}_q^{mn}$ is viewed as a (column) matrix

$$\boldsymbol{X} = \begin{pmatrix} x_1 & \ldots & x_{m(n-1)+1} \\ x_2 & \vdots & \vdots \\ x_m & \ldots & x_{mn} \end{pmatrix} \in \mathbb{F}_q^{m \times n}.$$

- The rank distance $d(\boldsymbol{X}, \boldsymbol{Y}) = \mathrm{Rank}(\boldsymbol{Y} - \boldsymbol{X})$.

Example 1

- $\boldsymbol{x} = (1,0,1,0,1,1,0,0,0,1,0,1,0,0,1,1,1,0,0,1) \in \mathbb{F}_2^{20}$.
- $\mathrm{Mat}(\boldsymbol{x}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 5}$
- The weight of $\boldsymbol{x}$ is 3.

Rank metric Gabidulin 1985

Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \ldots, \beta_m)$ as an $\mathbb{F}_q$-vector space.

Rank metric Gabidulin 1985

Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \ldots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
  - $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, basis $(1, \alpha, \alpha^2, \alpha^3)$.

Rank metric Gabidulin 1985

Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \ldots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
  - $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, basis $(1, \alpha, \alpha^2, \alpha^3)$.
- Correspondence $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) \in \mathbb{F}_q^{m \times n}$, $\boldsymbol{x} = \beta\, \mathrm{Mat}(\boldsymbol{x})$.

Rank metric Gabidulin 1985

Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \ldots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
  - $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, basis $(1, \alpha, \alpha^2, \alpha^3)$.
- Correspondence $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) \in \mathbb{F}_q^{m \times n}$, $\boldsymbol{x} = \beta\,\mathrm{Mat}(\boldsymbol{x})$.
  - $\boldsymbol{x} = (1+\alpha^2, 1+\alpha, \alpha+\alpha^3, \alpha^2+\alpha^3, 1+\alpha^3) \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 5}$

    and $(1, \alpha, \alpha^2, \alpha^3)\,\mathrm{Mat}(\boldsymbol{x}) = \boldsymbol{x}$.

Rank metric Gabidulin 1985

Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \ldots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
  - $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, basis $(1, \alpha, \alpha^2, \alpha^3)$.
- Correspondence $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) \in \mathbb{F}_q^{m \times n}$, $\boldsymbol{x} = \beta\,\mathrm{Mat}(\boldsymbol{x})$.
  - $\boldsymbol{x} = (1+\alpha^2, 1+\alpha, \alpha+\alpha^3, \alpha^2+\alpha^3, 1+\alpha^3) \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 5}$

    and $(1, \alpha, \alpha^2, \alpha^3)\,\mathrm{Mat}(\boldsymbol{x}) = \boldsymbol{x}$.
- Rank weight $|\boldsymbol{x}| = \mathrm{Rank}(\mathrm{Mat}(\boldsymbol{x})) = \dim(\langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q})$, support.

Rank metric Gabidulin 1985

Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \ldots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
  - $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, basis $(1, \alpha, \alpha^2, \alpha^3)$.
- Correspondence $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) \in \mathbb{F}_q^{m \times n}$, $\boldsymbol{x} = \beta\,\mathrm{Mat}(\boldsymbol{x})$.
  - $\boldsymbol{x} = (1+\alpha^2, 1+\alpha, \alpha+\alpha^3, \alpha^2+\alpha^3, 1+\alpha^3) \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 5}$

    and $(1, \alpha, \alpha^2, \alpha^3)\,\mathrm{Mat}(\boldsymbol{x}) = \boldsymbol{x}$.
- Rank weight $|\boldsymbol{x}| = \mathrm{Rank}(\mathrm{Mat}(\boldsymbol{x})) = \dim(\langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q})$, support.
  - $|\boldsymbol{x}| = 3$, the support of $\boldsymbol{x}$ is $\mathscr{V} = \langle 1+\alpha^2, 1+\alpha, \alpha+\alpha^3 \rangle_{\mathbb{F}_q}$.

General Matrix codes are $\mathbb{F}_q$-linear codes (Delsarte 1978)

They are $\mathbb{F}_q$-linear sub-spaces of $\mathbb{F}_{q^m}^n = \mathbb{F}_q^{mn} = \mathbb{F}_q^{m \times n}$, endowed with the rank metric.

Interesting Codes in Rank metric

General Matrix codes are $\mathbb{F}_q$-linear codes (Delsarte 1978)

They are $\mathbb{F}_q$-linear sub-spaces of $\mathbb{F}_{q^m}^n = \mathbb{F}_q^{mn} = \mathbb{F}_q^{m \times n}$, endowed with the rank metric.

Particular Matrix codes specified as $\mathbb{F}_{q^m}$-linear codes (Gabidulin 1985)

They are $\mathbb{F}_{q^m}$-linear sub-spaces of $\mathbb{F}_{q^m}^n$, endowed with the rank metric.

- $\mathbb{F}_{q^m}$-linear codes are particular matrix codes with a structure,
- Known families of $\mathbb{F}_{q^m}$-linear codes with decoding algorithms,
- $\mathbb{F}_{q^m}$-linear codes have a much shorter description (save a factor m)
  $\Rightarrow$ Shorter public keys in cryptography!

Specific family of codes

$\mathbb{F}_{q^m}$-linear codes in rank metric: $\mathscr{C} \subset \mathbb{F}_{q^m}^n$ has an additional structure

	$\mathbb{F}_{q^m}^n$-linear code	Matrix code in $\mathbb{F}_q^{nm}$
Field	$\mathbb{F}_{q^m}$	$\mathbb{F}_q$
Length	n	nm
Dimension	k	km
Codeword	$\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$	matrix $\boldsymbol{X} \in \mathbb{F}_q^{m \times n}$
Size of a basis	$knm \log(q)$	$kmnm \log(q)$

Rank Decoding Problem (RD)

- `Input`: an integer $r \in \mathbb{N}$, an $\mathbb{F}_{q^m}$-basis $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a subspace $\mathscr{C} \subset \mathbb{F}_{q^m}^n$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$.
- `Output`: $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that

$$\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e} \text{ and } \mathrm{Rank}(\boldsymbol{e}) \leq r.$$

Rank Decoding Problem (RD)

- `Input`: an integer $r \in \mathbb{N}$, an $\mathbb{F}_{q^m}$-basis $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a subspace $\mathscr{C} \subset \mathbb{F}_{q^m}^n$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$.
- `Output`: $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that

$$\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e} \text{ and } \mathrm{Rank}(\boldsymbol{e}) \leq r.$$

Syndrome formulation

$\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^\top$, $\boldsymbol{y}$ one solution of $\boldsymbol{y}\boldsymbol{H}^\top = \boldsymbol{s}$ without constraints on the weight of $\boldsymbol{y}$.
Given $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$, find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that

$$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top \text{ and } \mathrm{Rank}(\boldsymbol{e}) \leq r.$$

MinRank Problem = Matrix code Decoding Problem

Computational MinRank (affine)

- `Input`: integers $r, m, n \in \mathbb{N}$, and $K = k+1$ matrices $\boldsymbol{Y}, \boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_k) \in \mathbb{F}_q$, such that

$$\mathrm{Rank}\left(\boldsymbol{Y} + \sum_{i=1}^{k} x_i \boldsymbol{M}_i\right) \leq r.$$

Hardness of the decoding for $\mathbb{F}_q$-linear matrix codes

- MinRank is an NP-complete problem (Buss, Frandsen, and Shallit 1999),

Hardness of MinRank and RD

Hardness of the decoding for $\mathbb{F}_q$-linear matrix codes

- MinRank is an NP-complete problem (Buss, Frandsen, and Shallit 1999),

Hardness of the decoding for $\mathbb{F}_{q^m}$-linear codes

- RD is not "a priori" NP-hard.
- DP (Decoding problem, Hamming metric) $\leq_{\text{randomized}}$ RD ($m > n^2$) (Gaborit and Zémor 2016)
- RD $\leq$ MinRank. (J.-C. Faugère, Levy-dit-Vehel, and Perret 2008).

Signature schemes (authentication protocols) submitted to the NIST competition

- RYDE : RD.
- MIRA and MiRitH : MinRank.

Rank-metric Code-Based cryptography

Signature schemes (authentication protocols) submitted to the NIST competition

- RYDE : RD.
- MIRA and MiRitH : MinRank.

MinRank is also used to cryptanalyse multivariate (e.g. Rainbow, GeMSS, UOV) or code-based schemes (e.g. McEliece).

Hybrid approach Bardet, Briaud, Bros, et al. 2023

$$\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} = \boldsymbol{s}\boldsymbol{C}$$

Reduce to smaller problems

- if a positions of $\boldsymbol{e}$ are zero: a columns of $\boldsymbol{C}$ are zero, a linear equations in $\boldsymbol{x} \rightarrow$ reduce to a smaller instance with parameters $(m, n-a, k-a, r)$,

Hybrid approach Bardet, Briaud, Bros, et al. 2023

$$\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} = \boldsymbol{s}\boldsymbol{C}$$

Reduce to smaller problems

- if a positions of $\boldsymbol{e}$ are zero: a columns of $\boldsymbol{C}$ are zero, a linear equations in $\boldsymbol{x} \rightarrow$ reduce to a smaller instance with parameters $(m, n-a, k-a, r)$,
- if $a + r \leq k$: apply q^{ar} transforms to the system, $\boldsymbol{e}$ has the good shape for one of them;

$$\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} = \boldsymbol{s}\boldsymbol{C}$$

Reduce to smaller problems

- if a positions of $\boldsymbol{e}$ are zero: a columns of $\boldsymbol{C}$ are zero, a linear equations in $\boldsymbol{x}$ $\rightarrow$ reduce to a smaller instance with parameters $(m, n-a, k-a, r)$,
- if $a + r \leq k$: apply q^{ar} transforms to the system, $\boldsymbol{e}$ has the good shape for one of them;
- otherwise: apply a random transform, $\boldsymbol{e}$ has the good shape with probability $O(1/q^{ar})$.

$$\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} = \boldsymbol{s}\boldsymbol{C}$$

Reduce to smaller problems

- if a positions of $\boldsymbol{e}$ are zero: a columns of $\boldsymbol{C}$ are zero, a linear equations in $\boldsymbol{x}$ $\rightarrow$ reduce to a smaller instance with parameters $(m, n-a, k-a, r)$,
- if $a + r \leq k$: apply q^{ar} transforms to the system, $\boldsymbol{e}$ has the good shape for one of them;
- otherwise: apply a random transform, $\boldsymbol{e}$ has the good shape with probability $O(1/q^{ar})$.

$$\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} = \boldsymbol{s}\boldsymbol{C}$$

Reduce to smaller problems

- if a positions of $\boldsymbol{e}$ are zero: a columns of $\boldsymbol{C}$ are zero, a linear equations in $\boldsymbol{x} \rightarrow$ reduce to a smaller instance with parameters $(m, n-a, k-a, r)$,
- if $a + r \leq k$: apply q^{ar} transforms to the system, $\boldsymbol{e}$ has the good shape for one of them;
- otherwise: apply a random transform, $\boldsymbol{e}$ has the good shape with probability $O(1/q^{ar})$.

$$\text{Cost } q^{ar}\mathbb{C}_{RD}(m, n-a, k-a, r).$$

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$,
$\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n}, \boldsymbol{x} \in \mathbb{F}_{q^m}^{k}$ such that $\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y}$ and $\mathrm{Rank}(\boldsymbol{e}) \leq r$.

Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n, \boldsymbol{x} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y}$ and $\mathrm{Rank}(\boldsymbol{e}) \leq r$.
- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}\boldsymbol{H}_y{}^\top = \mathbf{o}$ and $\mathrm{Rank}(\boldsymbol{e}) \leq r$

Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$,
$\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n, \boldsymbol{x} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y}$ and $\mathrm{Rank}(\boldsymbol{e}) \leq r$.
- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}\boldsymbol{H}_y{}^\top = \mathbf{o}$ and $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^r$, $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{e} = (s_1, \ldots, s_r)\boldsymbol{C}$.

Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$,
$\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n, \boldsymbol{x} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y}$ and $\mathrm{Rank}(\boldsymbol{e}) \leq r$.
- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}\boldsymbol{H}_y{}^\top = \mathbf{0}$ and $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^r$, $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{e} = (s_1, \ldots, s_r)\boldsymbol{C}$.
- find $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^r$ and $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $(s_1, \ldots, s_r)\boldsymbol{C}\boldsymbol{H}_y{}^\top = 0$ (Ourivski and Johansson 2002).

Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$,
$\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n, \boldsymbol{x} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y}$ and $\mathrm{Rank}(\boldsymbol{e}) \leq r$.
- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}\boldsymbol{H}_y{}^\top = \mathbf{o}$ and $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^r$, $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{e} = (s_1, \ldots, s_r)\boldsymbol{C}$.
- find $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^r$ and $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $(s_1, \ldots, s_r)\boldsymbol{C}\boldsymbol{H}_y{}^\top = \mathrm{o}$ (Ourivski and Johansson 2002).
- find $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{C}\boldsymbol{H}_y{}^\top$ has a non-trivial left kernel. (Bardet, Bros, Cabarcas, et al. 2020).

Algebraic Modeling Bardet, Bros, Cabarcas, et al. 2020

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y{}^\top) = \left\{ P_J := \left| \boldsymbol{C}\boldsymbol{H}_y{}^\top \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- $\binom{n-k-1}{r}$ equations over $\mathbb{F}_{q^m}$ of degree r,
- rn variables $c_{i,j}$ over $\mathbb{F}_q$.
- a lot of solutions:
  - $\boldsymbol{A}\boldsymbol{C}$ is a solution for any $\boldsymbol{A} \in GL_r(\mathbb{F}_q)$.
  - any $\boldsymbol{C}$ of rank $< r$ is solution

  $\rightarrow$ look for $\boldsymbol{C} = (\boldsymbol{I}_r \ \boldsymbol{C}')$, $r(n-r)$ variables.

MaxMinors modeling

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y{}^\top) = \left\{ P_J := \left| \boldsymbol{C}\boldsymbol{H}_y{}^\top \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y{}^\top) = \left\{ P_J := \left| \boldsymbol{C}\boldsymbol{H}_y{}^\top \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- Cauchy-Binet formula: $\det(\boldsymbol{A}\boldsymbol{B}) = \sum_T \det(\boldsymbol{A}_{*,T}) \det(\boldsymbol{B}_{T,*})$.

$$P_J = \sum_{T \subset \{1..n\}, \#T = r} |\boldsymbol{C}|_{*,T} \left|\boldsymbol{H}_y\right|_{J,T}$$

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y{}^\top) = \left\{ P_J := \sum_{T\subset\{1..n\},\#T=r} |\boldsymbol{C}|_{*,T}\,|\boldsymbol{H}_y|_{J,T} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- Plücker coordinates ($N = \binom{n}{r} - 1$): injective map, easy to invert on its image.

$$p : \{\mathscr{W} \subset \mathbb{F}_q^n : \dim(\mathscr{W}) = r\} \to \mathbb{P}^N(\mathbb{F}_q)$$
$$\boldsymbol{C} \text{ generator matrix of } \mathscr{W} \mapsto (|\boldsymbol{C}|_{*,T})_{T\subset\{1..n\},\#T=r}$$

MaxMinors modeling

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y{}^\top) = \left\{ P_J := \sum_{T\subset\{1..n\},\#T=r} |\boldsymbol{C}|_{*,T} \left|\boldsymbol{H}_y\right|_{J,T} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- $\binom{n}{r}$ variables $c_T = |\boldsymbol{C}|_{*,T} \in \mathbb{F}_q$, $T \subset \{1..n\}$, $\#T = r$
- $\binom{n-k-1}{r}$ linear equations $P_J = 0$ with coefficients in $\mathbb{F}_{q^m}$,

MaxMinors modeling

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y{}^\top) = \left\{ P_J := \sum_{T\subset\{1..n\},\#T=r} |\boldsymbol{C}|_{*,T}\,|\boldsymbol{H}_y|_{J,T} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- $\binom{n}{r}$ variables $c_T = |\boldsymbol{C}|_{*,T} \in \mathbb{F}_q$, $T \subset \{1..n\}$, $\#T = r$
- $\binom{n-k-1}{r}$ linear equations $P_J = 0$ with coefficients in $\mathbb{F}_{q^m}$,
- spurious solutions: solutions over $\overline{\mathbb{F}_q}$ or outside the image of the Plücker map.

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y^\top) = \left\{ P_J := \sum_{T\subset\{1..n\},\#T=r} |\boldsymbol{C}|_{*,T} \left|\boldsymbol{H}_y\right|_{J,T} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- $\binom{n}{r}$ variables $c_T = |\boldsymbol{C}|_{*,T} \in \mathbb{F}_q$, $T \subset \{1..n\}$, $\#T = r$
- $\binom{n-k-1}{r}$ linear equations $P_J = 0$ with coefficients in $\mathbb{F}_{q^m}$,
- spurious solutions: solutions over $\overline{\mathbb{F}_q}$ or outside the image of the Plücker map.
- Unfolding = m times more equations over $\mathbb{F}_q$

$$\sum_{T\subset\{1..n\},\#T=r} |\boldsymbol{C}|_{*,T} \left|\boldsymbol{H}_y\right|_{J,T}^{q^\ell}, \quad \ell \in \{0..m-1\}.$$

(it uses the field equations $|\boldsymbol{C}|_{*,T}^q - |\boldsymbol{C}|_{*,T}$).

Solving in the Overdetermined case

$$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$$

If the equations over $\mathbb{F}_q$ are "as linearly independent as possible" $\rightarrow$ independence assumption.
No spurious solution outside the image of the Plücker map 😄.

Solving in the Overdetermined case

$$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$$

If the equations over $\mathbb{F}_q$ are "as linearly independent as possible" $\rightarrow$ independence assumption.
No spurious solution outside the image of the Plücker map 😄.

In the Underdetermined case

- Hybrid approach to reduce to the overdetermined case;

Solving in the Overdetermined case

$$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$$

If the equations over $\mathbb{F}_q$ are "as linearly independent as possible" $\rightarrow$ independence assumption.
No spurious solution outside the image of the Plücker map 😄.

In the Underdetermined case

- Hybrid approach to reduce to the overdetermined case;
- Use relations between the minors? 😢

Solving in the Overdetermined case

$$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$$

If the equations over $\mathbb{F}_q$ are "as linearly independent as possible" $\rightarrow$ independence assumption.
No spurious solution outside the image of the Plücker map 😄.

In the Underdetermined case

- Hybrid approach to reduce to the overdetermined case;
- Use relations between the minors? 😢
- Introduce another set of variables (e.g. ***x*** or ***s***).

Underdet. cases Bardet, Briaud, Bros, et al. 2023

$$\boldsymbol{xG} + \boldsymbol{y} = \boldsymbol{sC}, \quad \boldsymbol{x} \in \mathbb{F}_{q^m}^k, \boldsymbol{s} \in \mathbb{F}_{q^m}^r, \boldsymbol{C} \in \mathbb{F}_q^{r \times n}.$$

bilinear system with matrix form, degree drops at degree $r+2$. **?**

Underdet. cases Bardet, Briaud, Bros, et al. 2023

$$\boldsymbol{xG}+\boldsymbol{y}=\boldsymbol{sC},\quad \boldsymbol{x}\in\mathbb{F}_{q^m}^k,\boldsymbol{s}\in\mathbb{F}_{q^m}^r,\boldsymbol{C}\in\mathbb{F}_q^{r\times n}.$$

bilinear system with matrix form, degree drops at degree $r+2$. **?**

Support Minors modeling over $\mathbb{F}_{q^m}$

$$\left\{Q_I \stackrel{\text{def}}{=} \left|\begin{pmatrix}\boldsymbol{xG}+\boldsymbol{y}\\ \boldsymbol{C}\end{pmatrix}\right|_{*,I} : I\subset\{1..n\}, \#I=r+1\right\}$$

Underdet. cases Bardet, Briaud, Bros, et al. 2023

$$\boldsymbol{xG} + \boldsymbol{y} = \boldsymbol{sC}, \quad \boldsymbol{x} \in \mathbb{F}_{q^m}^k, \boldsymbol{s} \in \mathbb{F}_{q^m}^r, \boldsymbol{C} \in \mathbb{F}_q^{r \times n}.$$

bilinear system with matrix form, degree drops at degree $r+2$. **?**

Support Minors modeling over $\mathbb{F}_{q^m}$

$$\left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \boldsymbol{xG} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

- $\binom{n}{r}$ variables $c_T \in \mathbb{F}_q$, k variables $x_1, \ldots, x_k \in \mathbb{F}_{q^m}$,
- $\binom{n}{r+1}$ equations $Q_I = 0$ for $I \subset \{1..n\}$, $\#I = r+1$, viewed as affine bilinear equations over $\mathbb{F}_{q^m}$ in the x_i's and the c_T's.

Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \stackrel{\text{def}}{=} \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \stackrel{\text{def}}{=} \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\mathscr{Q}_s = \{Q_I : \#(I \cap \{1..k+1\}) = s\},$$
$$\mathscr{Q}_{\geq s} = \{Q_I : \#(I \cap \{1..k+1\}) \geq s\},$$

Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \stackrel{\text{def}}{=} \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\mathscr{Q}_s = \{Q_I : \#(I \cap \{1..k+1\}) = s\},$$
$$\mathscr{Q}_{\geq s} = \{Q_I : \#(I \cap \{1..k+1\}) \geq s\},$$

Proposition Bardet, Briaud, Bros, et al. 2023

$$\mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle_{\mathbb{F}_q}$$

Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \stackrel{\text{def}}{=} \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\mathscr{Q}_s = \{Q_I : \#(I \cap \{1..k+1\}) = s\},$$
$$\mathscr{Q}_{\geq s} = \{Q_I : \#(I \cap \{1..k+1\}) \geq s\},$$

Proposition Bardet, Briaud, Bros, et al. 2023

$$\mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle_{\mathbb{F}_q}$$
$$\langle \mathscr{P}, x_i \mathscr{P} : i \in \{1..k\}, \mathscr{Q}_{\geq 2} \rangle_{\mathbb{F}_q} = \langle \mathscr{Q}_1, \mathscr{Q}_{\geq 2} \rangle_{\mathbb{F}_q}$$

Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \stackrel{\text{def}}{=} \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\mathscr{Q}_s = \{Q_I : \#(I \cap \{1..k+1\}) = s\},$$
$$\mathscr{Q}_{\geq s} = \{Q_I : \#(I \cap \{1..k+1\}) \geq s\},$$

Proposition Bardet, Briaud, Bros, et al. 2023

$$\mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle_{\mathbb{F}_q}$$
$$\langle \mathscr{P}, x_i\mathscr{P} : i \in \{1..k\}, \mathscr{Q}_{\geq 2} \rangle_{\mathbb{F}_q} = \langle \mathscr{Q}_1, \mathscr{Q}_{\geq 2} \rangle_{\mathbb{F}_q}$$

$\mathscr{P}, x_i\mathscr{P} : i \in \{1..k\}, \mathscr{Q}_{\geq 2}$ are linearly independent over $\mathbb{F}_q$

Hints of Proof

- $\left| \begin{pmatrix} xG+y \\ C \end{pmatrix} H_y{}^\top \right|_{*,T} = 0$ + Cauchy-Binet formula + systematic form $\Rightarrow \mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle$.

Hints of Proof

- $\left|\begin{pmatrix} xG+y \\ C \end{pmatrix} H_y{}^{\top}\right|_{*,T} = 0$ + Cauchy-Binet formula + systematic form $\Rightarrow \mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle$.
- We introduce a monomial ordering and compare leading terms for $Q_I \in \mathscr{Q}_{\geq 2}$:

$$\begin{cases} \mathrm{LT}(Q_I) & = x_{i_1} c_{I \setminus \{i_1\}} \text{ for } i_1 = \min(I) \leq k, i_2 \leq k+1. \\ \mathrm{LT}(P_J) & = c_{J+k+1} \text{ for } J \subset \{1..n-k-1\}, \#J = r. \end{cases}$$

Hints of Proof

- $\left|\begin{pmatrix} xG+y \\ C \end{pmatrix} H_y{}^\top\right|_{*,T}$ = 0 + Cauchy-Binet formula + systematic form $\Rightarrow \mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle$.
- We introduce a monomial ordering and compare leading terms for $Q_I \in \mathscr{Q}_{\geq 2}$:

$$\begin{cases} \mathrm{LT}(Q_I) & = x_{i_1} c_{I \setminus \{i_1\}} \text{ for } i_1 = \min(I) \leq k, i_2 \leq k+1. \\ \mathrm{LT}(P_J) & = c_{J+k+1} \text{ for } J \subset \{1..n-k-1\}, \#J = r. \end{cases}$$

- $\left|\begin{pmatrix} xG+y \\ C \end{pmatrix} H^\top\right|_{*,J\cup\{n-k\}} = (-1)^r P_J$ + Cauchy-Binet formula + systematic form implies that $\mathscr{P} \subset \mathscr{Q}_1 + \langle \mathscr{Q}_{\geq 2} \rangle$.

Hints of Proof

- $\left|\begin{pmatrix} xG+y \\ C \end{pmatrix} H_y{}^\top\right|_{*,T}$ = 0 + Cauchy-Binet formula + systematic form $\Rightarrow \mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle$.
- We introduce a monomial ordering and compare leading terms for $Q_I \in \mathscr{Q}_{\geq 2}$:

$$\begin{cases} \mathrm{LT}(Q_I) & = x_{i_1} c_{I\setminus\{i_1\}} \text{ for } i_1 = \min(I) \leq k, i_2 \leq k+1. \\ \mathrm{LT}(P_J) & = c_{J+k+1} \text{ for } J \subset \{1..n-k-1\}, \#J = r. \end{cases}$$

- $\left|\begin{pmatrix} xG+y \\ C \end{pmatrix} H^\top\right|_{*,J\cup\{n-k\}} = (-1)^r P_J$ + Cauchy-Binet formula + systematic form implies that $\mathscr{P} \subset \mathscr{Q}_1 + \langle \mathscr{Q}_{\geq 2} \rangle$.
- same idea with another matrix for $x_i P_J$.

Solving SM over $\mathbb{F}_{q^m}$: too many solutions

With the equations $\mathscr{P}$ + $\mathscr{Q}_{\geq 2}$

- each linear equation P_J removes a variable c_{J+k+1} that does not appear in $\mathscr{Q}_{\geq 2}$,
- we can describe the vector spaces generated by $\mathscr{Q}_{\geq 2}$ for each bi-degree $(b, 1)$ in (x_i, c_T),
- the Macaulay matrices always have a rank = # rows (already Echelon Form!).

Solving SM over $\mathbb{F}_{q^m}$: too many solutions

With the equations $\mathscr{P}$ + $\mathscr{Q}_{\geq 2}$

- each linear equation P_J removes a variable c_{J+k+1} that does not appear in $\mathscr{Q}_{\geq 2}$,
- we can describe the vector spaces generated by $\mathscr{Q}_{\geq 2}$ for each bi-degree $(b, 1)$ in (x_i, c_T),
- the Macaulay matrices always have a rank = # rows (already Echelon Form!).

But...

- we can eliminate m times more variables c_J by unfolding the P_J's!
- that's SM-$\mathbb{F}_{q^m}^+$ = $\{Q_I : I\} + \{P_{i,J} : i, J\}$.
- we analyze the vector spaces generated by the equations in any bi-degree $(b, 1)$ in $\boldsymbol{x}_i, c_T \to$ syzygies $\to$ generic complexity.

- Macaulay matrix at bi-degree $(b, 1)$.
- The linear dependencies of the polynomials in $\mathscr{Q}_0$ come from $\left|\begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H_y}^\top\right|_{*,T} = 0 \mod \langle P_J \rangle$.
- With the unfolding, we also have $\left|\begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} (\boldsymbol{H_y}^{q^\ell})^\top\right|_{*,T_1} = 0 \mod \langle P_{i,J} \rangle$.
- At higher degree, $\left|\begin{pmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} (\boldsymbol{H_y}^{q^\ell})^\top\right|_{*,T_2} = 0 \quad (\#T_i = r+i)$.

Complexity of solving SM-$\mathbb{F}_{q^m}^+$

$$\mathscr{N}_b^{\mathbb{F}_q} = \mathscr{N}_b^{\mathbb{F}_{q^m}} - \mathscr{N}_{b,syz}^{\mathbb{F}_q},$$

$$\mathscr{N}_b^{\mathbb{F}_{q^m}} = \sum_{i=1}^{k} \binom{n-i}{r}\binom{k+b-1-i}{b-1} - \binom{n-k-1}{r}\binom{k+b-1}{b} \qquad (exact)$$

$$\mathscr{N}_{b,syz}^{\mathbb{F}_q} = (m-1)\sum_{i=1}^{b}(-1)^{i+1}\binom{k+b-i-1}{b-i}\binom{n-k-1}{r+i} \qquad (conjecture)$$

$$\mathscr{M}_b^{\mathbb{F}_q} = \binom{k+b-1}{b}\left(\binom{n}{r} - m\binom{n-k-1}{r}\right), \qquad (exact)$$

We can solve SM-$\mathbb{F}_{q^m}^+$ by linearization at bi-degree $(b,1)$ whenever $\mathscr{N}_b^{\mathbb{F}_q} \geq \mathscr{M}_b^{\mathbb{F}_q} - 1$ with a cost $\mathscr{O}\left(m^2 \mathscr{N}_b^{\mathbb{F}_q} {\mathscr{M}_b^{\mathbb{F}_q}}^{\omega-1}\right)$ operations in $\mathbb{F}_q$.

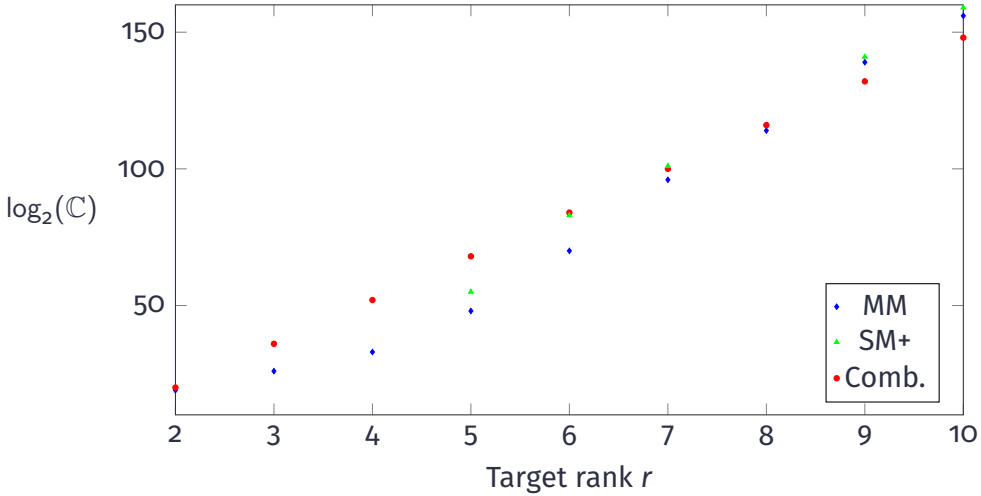


Figure: Theoretical complexities for MM-$\mathbb{F}_q$/SM-$\mathbb{F}_{q^m}^+$(hybrid) and for combinatorial attacks with fixed $(m, n, k) = (31, 33, 15)$ (RYDE-128). $d_{\text{RGV}}(m, n, k, q = 2) = 10$.

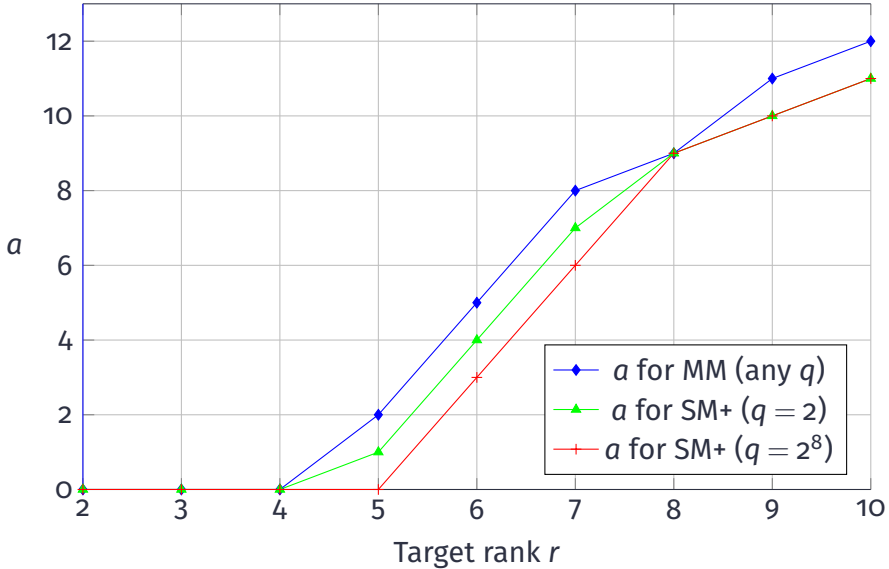


Figure: Optimal values of a with $(m, n, k) = (31, 33, 15)$, for MM-$\mathbb{F}_q$ and SM-$\mathbb{F}_{q^m}^+$.

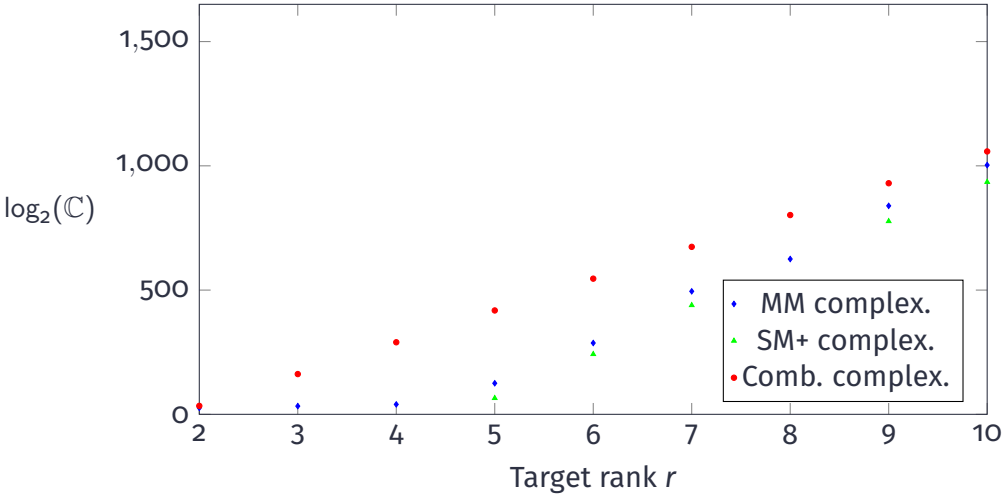


Figure: Same parameters as Fig. 1 but with $q = 2^8$.

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- $K < (m-r)(n-r)$: 0 or 1 solution *in the algebraic closure* of $\mathbb{F}_q$.

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- $K < (m-r)(n-r)$: 0 or 1 solution *in the algebraic closure* of $\mathbb{F}_q$.
- No need to add the field equations: already in the ideal!

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\text{Rank}\left(\sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- $K < (m-r)(n-r)$: 0 or 1 solution *in the algebraic closure* of $\mathbb{F}_q$.
- No need to add the field equations: already in the ideal!
- For very small q (e.g. $q = 2$): adding small degree equations can speed up the computation.

MinRank problem $\text{Rank}\left(\boldsymbol{M}_{\boldsymbol{x}} \overset{\text{DEF}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\boldsymbol{M}_{\boldsymbol{x}} \begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{C} \end{pmatrix} = \mathrm{O}_{m \times (n-r)}, \quad \boldsymbol{C} \in \mathbb{F}_q^{r \times (n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

MinRank problem $\text{Rank}\left(\boldsymbol{M_x} \stackrel{\text{DEF}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\boldsymbol{M_x}\begin{pmatrix}\boldsymbol{I}_{n-r}\\ -\boldsymbol{C}\end{pmatrix} = 0_{m\times(n-r)}, \quad \boldsymbol{C} \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

- Minors modeling (J. Faugère, Safey El Din, and Spaenlehauer 2010)

$$\text{Minors}_{r+1}(\boldsymbol{M_x}) = 0 \qquad \text{(Minors)}$$

MinRank problem $\text{Rank}\left(\boldsymbol{M_x} \stackrel{\text{DEF}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$\boldsymbol{M_x}\begin{pmatrix}\boldsymbol{I}_{n-r}\\ -\boldsymbol{C}\end{pmatrix} = \mathrm{O}_{m\times(n-r)}, \quad \boldsymbol{C} \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

$$\iff \boldsymbol{M_x} \text{ is orthogonal to the code } \begin{pmatrix}\boldsymbol{I}_{n-r} & -\boldsymbol{C}^\top\end{pmatrix}, \text{ dual } \begin{pmatrix}\boldsymbol{C} & \boldsymbol{I}_r\end{pmatrix}.$$

- Minors modeling (J. Faugère, Safey El Din, and Spaenlehauer 2010)

$$\text{Minors}_{r+1}(\boldsymbol{M_x}) = \mathrm{O} \qquad \text{(Minors)}$$

- Support Minors modeling, (Bardet, Bros, Cabarcas, et al. 2020)

$$\text{Minors}_{r+1}\begin{pmatrix}(\boldsymbol{M_x})_{j,*}\\ \boldsymbol{C} \quad \boldsymbol{I}_r\end{pmatrix} = \mathrm{O} \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

MinRank problem $\text{Rank}\left(M_x \overset{\text{DEF}}{=} \sum_{i=1}^{K} x_i M_i\right) \leq r$

- Kipnis-Shamir modeling (Kipnis and Shamir 1999)

$$M_x \begin{pmatrix} I_{n-r} \\ -C \end{pmatrix} = 0_{m\times(n-r)}, \quad C \in \mathbb{F}_q^{r\times(n-r)}, x_i \in \mathbb{F}_q \qquad \text{(KS)}$$

- Minors modeling (J. Faugère, Safey El Din, and Spaenlehauer 2010)

$$\text{Minors}_{r+1}(M_x) = 0 \qquad \text{(Minors)}$$

- Support Minors modeling, (Bardet, Bros, Cabarcas, et al. 2020)

$$\text{Minors}_{r+1}\begin{pmatrix} (M_x)_{j,*} \\ C \quad I_r \end{pmatrix} = 0 \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

- Same ideal ! $\langle Minors\rangle \subset \langle KS\rangle = \langle SM\rangle$ (Bardet and Bertin 2022; Guo and Ding 2022).

Conclusion

- Algebraic cryptanalysis is powerful ;
- importance of the algebraic modeling;
- design specific algorithms to be efficient;
- no general way, new analysis for each new class ;

- Aguilar Melchor, Carlos, Nicolas Aragon, Slim Bettaieb, et al. (Apr. 2019). *Rank Quasi Cyclic (RQC)*. Second round submission to the NIST post-quantum cryptography call.
- Baena, John, Pierre Briaud, Daniel Cabarcas, et al. (2022). “Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13509. LNCS. Springer, pp. 376–405.
- Bardet, Magali and Manon Bertin (Sept. 2022). “Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances”. In: *Post-Quantum Cryptography 2022*. Ed. by Jung Hee Cheon and Thomas Johansson. Vol. 13512. LNCS. Cham: Springer International Publishing, pp. 107–123.
- Bardet, Magali, Pierre Briaud, Maxime Bros, et al. (2023). “Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem”. In: *Designs, Codes and Cryptography* 91, pp. 3671–3707.

- Bardet, Magali, Maxime Bros, Daniel Cabarcas, et al. (2020). “Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems”. In: *Advances in Cryptology - ASIACRYPT 2020, International Conference on the Theory and Application of Cryptology and Information Security, 2020. Proceedings*. Vol. 12491. LNCS, pp. 507–536.
- Bayer, David and Michael Stillman (1988). “On the complexity of computing syzygies”. In: *Journal of Symbolic Computation* 6.2-3, pp. 135–147.
- Buss, Jonathan F., Gudmund S. Frandsen, and Jeffrey O. Shallit (June 1999). “The Computational Complexity of Some Problems of Linear Algebra”. In: *J. Comput. System Sci.* 58.3, pp. 572–596.
- Casanova, Antoine, Jean-Charles Faugère, Gilles Macario-Rat, et al. (Apr. 2019). *GeMSS: A Great Multivariate Short Signature*. Second round submission to the NIST post-quantum cryptography call.
- Delsarte, Philippe (1978). “Bilinear Forms over a Finite Field, with Applications to Coding Theory”. In: *J. Comb. Theory, Ser. A* 25.3, pp. 226–241.

- Faugère, Jean-Charles (2002). “A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)”. English. In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. Ed. by Teo Mora. New York: ACM Press, 75–83 (electronic).
- Faugère, Jean-Charles, Françoise Levy-dit-Vehel, and Ludovic Perret (2008). “Cryptanalysis of Minrank”. In: *Advances in Cryptology - CRYPTO 2008*. Ed. by David Wagner. Vol. 5157. LNCS, pp. 280–296.
- Faugère, Jean-Charles, Mohab Safey El Din, and Pierre-Jean Spaenlehauer (2010). “Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology”. In: *International Symposium on Symbolic and Algebraic Computation, ISSAC 2010, Munich, Germany, July 25-28, 2010*, pp. 257–264.
- Gabidulin, Ernst M. (1985). “Theory of codes with maximum rank distance”. In: *Problemy Peredachi Informatsii* 21.1, pp. 3–16.
- Gaborit, Philippe and Gilles Zémor (2016). “On the hardness of the decoding and the minimum distance problems for rank codes”. In: *IEEE Trans. Inform. Theory* 62(12), pp. 7245–7252.

- Giusti, M. (1984). “Some effectivity problems in polynomial ideal theory”. In: *Eurosam 84*. Ed. by John Fitch. Vol. 174. Lecture Notes in Computer Science. Cambridge, 1984. Berlin: Springer Berlin / Heidelberg, pp. 159–171.
- Guo, Hao and Jintai Ding (2022). “Algebraic Relation of Three MinRank Algebraic Modelings”. In: *Arithmetic of Finite Fields*. LNCS. Springer.
- Kipnis, Aviad and Adi Shamir (Aug. 1999). “Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization”. In: *Advances in Cryptology - CRYPTO’99*. Vol. 1666. LNCS. Santa Barbara, California, USA: Springer, pp. 19–30.
- Ourivski, Alexei V. and Thomas Johansson (2002). “New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications”. English. In: *Problems of Information Transmission* 38.3, pp. 237–246.
- Tao, Chengdong, Albrecht Petzoldt, and Jintai Ding (2021). “Efficient Key Recovery for All HFE Signature Variants”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*. Ed. by Tal Malkin and Chris Peikert. Vol. 12825. Lecture Notes in Computer Science. Springer, pp. 70–93.