A new approach based on quadratic forms to attack the McEliece cryptosystem

Alain Couvreur, **Rocco Mora** and Jean-Pierre Tillich

Asiacrypt 2023 - December 7th, 2023

The McEliece cryptosystem

- PKE with fast encryption and decryption but huge public key
- is 45 years old [McEliece 1978]
- Classic McEliece is a finalist at NIST PQ Standardization Process
- based on error correcting codes
- originally built upon Goppa codes
- broken several variants on other families:

- GRS codes
- Reed-Muller codes
- Algebraic Geometry codes
- etc...
- Quasi-cyclic Goppa codes
- Quasi-dyadic Goppa codes
- Wild Goppa codes
- etc...

The Goppa distinguishing problem

Goppa codes

- asymptotically meet Gilbert-Varshamov bound
- have the same weight distribution as random codes
- have trivial permutation group

Goppa distinguishing (GD) problem

Distinguish efficiently a generator matrix of a Goppa code from a randomly drawn one.

[Faugère, Gauthier-Umaña, Otmani, Perret, Tillich 2011]
The GD hardness assumption is false in the high-rate regime

- does not apply to Classic McEliece
- applies to CFS signature [Courtois, Finiasz, Sendrier 2001]

Overview of cryptanalysis on McEliece and our contributions

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

- $n = \Theta(s)$

  - $2^{\mathcal{O}(n)}$ — old key attack
  - $2^{\mathcal{O}(n)}$ — message attack

- $n = \Omega(s^2)$

  - $2^{\mathcal{O}(s)}$ — old key attack
  - $2^{\mathcal{O}(s)}$ — message attack
  - polynomial — new key attack $(q > r + 1)$
  - polynomial — distinguisher [FGOPT11]

- $n = \Theta(s^\alpha), \quad \alpha \in (1, 2)$

  - $2^{\mathcal{O}(s)}$ — old key attack
  - $2^{\mathcal{O}(s)}$ — message attack
  - $2^{\mathcal{O}(s^{2-\alpha} \log(s))}$ (subexponential) — new distinguisher

Alternant and Goppa codes: an alternative definition

- Goppa codes are subfield subcodes of GRS codes over a ground field $\mathbb{F}_q$
- In this talk: Extension of a code $\mathscr{C} \subseteq \mathbb{F}_q^n$ over a field extension $\mathbb{F}_{q^m}$

$$\mathscr{C}_{\mathbb{F}_{q^m}} = \langle \boldsymbol{c} \mid \boldsymbol{c} \in \mathscr{C} \rangle_{\mathbb{F}_{q^m}}.$$

Extension of the dual of an alternant code over a field extension

Define the *support* $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and the *multiplier* $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_{q^m}^n$, such that $x_i \neq x_j$ and $y_i \neq 0$. Then $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}_{\mathbb{F}_{q^m}}$ is spanned by the (secret) canonical basis

$$\mathcal{A} = (\underbrace{\boldsymbol{y}, \boldsymbol{x}\boldsymbol{y}, \ldots, \boldsymbol{x}^{r-1}\boldsymbol{y}}, \ldots, \underbrace{\boldsymbol{y}^{q^{m-1}}, (\boldsymbol{x}\boldsymbol{y})^{q^{m-1}}, \ldots, (\boldsymbol{x}^{r-1}\boldsymbol{y})^{q^{m-1}}})$$

Goppa code: $\mathscr{G}(\boldsymbol{x}, \Gamma) \stackrel{\text{def}}{=} \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ s.t.

$$y_i \stackrel{\text{def}}{=} \frac{1}{\Gamma(x_i)}, \quad \text{with } \Gamma \in \mathbb{F}_{q^m}[z],\ \deg(\Gamma) = r$$

Quadratic relationships

There exist quadratic relationships in $\mathcal{A}$

$$\mathcal{A} = (\boldsymbol{y}, \boldsymbol{xy}, \ldots, \boldsymbol{x}^{r-1}\boldsymbol{y}, \ldots, \boldsymbol{y}^{q^{m-1}}, (\boldsymbol{xy})^{q^{m-1}}, \ldots, (\boldsymbol{x}^{r-1}\boldsymbol{y})^{q^{m-1}})$$

Example

$$\boldsymbol{x}^2\boldsymbol{y} \star \boldsymbol{y} - (\boldsymbol{xy})^{\star 2} = 0$$

More in general, for a basis $\mathcal{V}$,

$$\sum_{i \leq j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j = 0$$

Quadratic forms and the matrix code of relationships

Any $\boldsymbol{c} = (c_{i,j})_{1 \le i \le j \le k}$, $\sum_{i \le j} c_{i,j} \boldsymbol{v}_i \star \boldsymbol{v}_j = 0$, defines a quadratic form:

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

The bilinear map given by the polar form of the quadratic form $Q_{\boldsymbol{c}}$ corresponds to a matrix $\boldsymbol{M_c} = (m_{i,j})$ such that, for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^k$,

$$\boldsymbol{x M_c y}^\intercal = Q_{\boldsymbol{c}}(\boldsymbol{x}+\boldsymbol{y}) - Q_{\boldsymbol{c}}(\boldsymbol{x}) - Q_{\boldsymbol{c}}(\boldsymbol{y}) \quad \to \quad \begin{cases} m_{i,j} \stackrel{\text{def}}{=} m_{j,i} \stackrel{\text{def}}{=} c_{i,j}, & 1 \le i < j \le k, \\ m_{i,i} \stackrel{\text{def}}{=} 2c_{i,i}, & 1 \le i \le k. \end{cases}$$

Matrix code of relationships

Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}$ and let $\mathcal{V} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ be a basis of $\mathscr{C}$,

$$\mathscr{C}_{\text{mat}}(\mathcal{V}) \stackrel{\text{def}}{=} \{\boldsymbol{M_c} = (m_{i,j})_{\substack{1 \le i \le k \\ 1 \le j \le k}} \mid \boldsymbol{c} = (c_{i,j})_{1 \le i \le j \le k} \in \mathscr{C}_{\text{rel}}(\mathcal{V})\} \subseteq \text{Sym}(k, \mathbb{F}).$$

$$\mathcal{A} = (\boldsymbol{y}, \boldsymbol{xy}, \ldots, \boldsymbol{x}^{r-1}\boldsymbol{y}, \ldots, \boldsymbol{y}^{q^{m-1}}, (\boldsymbol{xy})^{q^{m-1}}, \ldots, (\boldsymbol{x}^{r-1}\boldsymbol{y})^{q^{m-1}}).$$

Example: $\boldsymbol{x}^2\boldsymbol{y} \star \boldsymbol{y} - (\boldsymbol{xy})^{\star 2} = 0$, *i.e.* $\boldsymbol{a}_1 \star \boldsymbol{a}_3 - \boldsymbol{a}_2^{\star 2} = 0$

$$\boldsymbol{M_c} = \begin{array}{c} \\ \boldsymbol{y} \\ \boldsymbol{xy} \\ \boldsymbol{x}^2\boldsymbol{y} \\ \\ \vdots \\ \\ \end{array} \begin{array}{c} \begin{array}{cccc} \boldsymbol{y} & \boldsymbol{xy} & \boldsymbol{x}^2\boldsymbol{y} & \ldots \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & \\ 0 & -2 & 0 & 0 \\ 1 & 0 & 0 & \\ & & & \\ & 0 & & 0 \\ & & & \end{pmatrix} \end{array} \in \mathscr{C}_{\mathrm{mat}}(\mathcal{A}), \quad \mathrm{rank}(\boldsymbol{M_c}) = \begin{cases} 3, & \text{odd ch.} \\ 2, & \text{ch. } 2 \end{cases}$$

Low-rank matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{A})$

Isometry of matrix codes

But we have access to the public basis

$$\mathcal{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{rm}).$$

Proposition

Let $\mathcal{A}$ and $\mathcal{B}$ be two different bases of the same $[n, k]$ code $\mathscr{C} \subseteq \mathbb{F}^n$, with $\boldsymbol{P} \in \mathrm{GL}_k(\mathbb{F})$ transition matrix. Then

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

- The weight distribution is an invariant wrt rank-metric $d(\boldsymbol{X}, \boldsymbol{Y}) \stackrel{\mathrm{def}}{=} \mathrm{rank}(\boldsymbol{X} - \boldsymbol{Y})$.

  Low-rank matrices in $\mathscr{C}_{\mathrm{mat}}(\mathcal{B})$ too

- The dimension is an invariant

$$\dim_{\mathbb{F}} \mathscr{C}_{\mathrm{mat}}(\mathcal{V}) = \dim_{\mathbb{F}} \mathscr{C}_{\mathrm{rel}}(\mathcal{V}) = \binom{k+1}{2} - \dim_{\mathbb{F}} \mathscr{C}^{\star 2}$$

Random code

Let $\mathcal{V}$ be a basis of a random $[n, s]$ code. Does $\mathscr{C}_{\mathrm{mat}}(\mathcal{V})$ contain low-rank matrices?

Proposition

Let $\mathscr{R}$ be an $[n, k]$ random code over $\mathbb{F}_q$ and $\mathcal{V}$ a basis of $\mathscr{R}^{\perp}_{\mathbb{F}_{q^m}}$. If $\frac{k}{n} > \frac{2}{3}$, then $\mathscr{C}_{\mathrm{mat}}(\mathcal{V})$ contains rank 3 (rank 2 in ch. 2) matrices with negligible probability.

Classic McEliece	n	m	r	R
kem/mceliece348864	3488	12	64	0.77982
kem/mceliece460896	4608	13	96	0.72917
kem/mceliece6688128	6688	13	128	0.75120
kem/mceliece6960119	6960	13	119	0.77773
kem/mceliece8192128	8192	13	128	0.79688

Potential distinguisher for Classic McEliece rates

Symmetric MinRank problem for rank d

Let $\boldsymbol{M}_1, \cdots, \boldsymbol{M}_K \in \mathrm{Sym}(N, \mathbb{F})$. Find an $\boldsymbol{M} \in \langle \boldsymbol{M}_1, \cdots, \boldsymbol{M}_K \rangle_{\mathbb{F}}$ of rank $\leq d$.

$$\boxed{\mathrm{rank}(\boldsymbol{M}) \leq d \iff \mathrm{Minors}(\boldsymbol{M}, d+1) = \{0\}}$$

- In characteristic 2, $\mathscr{C}_{\mathrm{mat}}(\mathcal{B}) \subset \mathrm{Skew}(rm, \mathbb{F}_{q^m})$
- The determinant of a $2l \times 2l$ skew-symmetric matrix is the square of a polynomial in its entries, called Pfaffian:

$$\mathrm{Pf}(\boldsymbol{N})^2 = \det(\boldsymbol{N}), \quad \mathrm{Pf}\left(\begin{bmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{bmatrix}\right) = af - be + dc.$$

The Pfaffian ideal

Pfaffian ideal for rank 2

The Pfaffian ideal of rank 2 for $\boldsymbol{M}$ in characteristic 2 is

$$\mathcal{P}_2(\boldsymbol{M}) \stackrel{\text{def}}{=} \langle m_{i,j}m_{k,l} + m_{i,k}m_{j,l} + m_{i,l}m_{j,k} \mid 1 \leq i < j < k < l \leq rm \rangle.$$

$$\boxed{\boldsymbol{V}(\mathcal{P}_2(\boldsymbol{M})) = \boldsymbol{V}(\mathcal{I}(\text{Minors}(\boldsymbol{M}, 3)))}$$

Modeling: $\boldsymbol{M} \in \mathscr{C}_{\textbf{mat}}(\mathcal{B})$, rank$(\boldsymbol{M}) \leq 2$ (characteristic 2)

Variables: $m_{i,j}$, $1 \leq i < j \leq rm$, entries of $\boldsymbol{M}$ — $\binom{rm}{2}$ var.s

Equations:

- $m_{i,j}m_{k,l} + m_{i,k}m_{j,l} + m_{i,l}m_{j,k} = 0$ — $\binom{rm}{4}$ quadratic eq.s
- $L_1 = 0, \cdots, L_t = 0$ expressing that $\boldsymbol{M} \in \mathscr{C}_{\text{mat}}$ — $\binom{rm}{2} - \dim \mathscr{C}_{\text{mat}}$ linear eq.s

The complexity of solving the system through the Hilbert Series

$\mathcal{I} \subseteq \mathbb{K}[\boldsymbol{z}]$ homogeneous ideal

- $HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d) \overset{\text{def}}{=} \dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{z}]_d - \dim_{\mathbb{K}} \mathcal{I}_d,$
- $HS_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(z) \overset{\text{def}}{=} \sum_{d \geq 0} HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d) z^d$

$$\mathcal{P}_2^+(\boldsymbol{M}) \overset{\text{def}}{=} \underbrace{\mathcal{P}_2(\boldsymbol{M})}_{\text{quadratic}} + \underbrace{\langle L_1, \ldots, L_t \rangle}_{\text{linear}}$$

- Alternant/Goppa code:

$$\left.\begin{array}{lll} \text{quadratic equations} & \leftarrow & \text{non random} \\ \text{linear equations} & \leftarrow & \text{non random} \end{array}\right\} \text{complexity analysis is difficult}$$

Fact: alternant/Goppa case

Let $\mathcal{P}_2^+(\boldsymbol{M}) \overset{\text{def}}{=} \mathcal{P}(\boldsymbol{M}) + \langle L_1, \ldots, L_k \rangle$. Then

$$\forall d \in \mathbb{N}, \qquad HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) > 0.$$

- Random code:

$$\left.\begin{array}{ll} \text{quadratic equations} & \leftarrow \text{non random} \\ \text{linear equations} & \leftarrow \text{random} \end{array}\right\} \begin{array}{l}\text{easy to analyze knowing the} \\ \text{behavior of quadratic equations}\end{array}$$

Theorem [Ghorpade, Krattenthaler 2004]

Let $\boldsymbol{M} = (m_{i,j})_{i,j}$ be the generic $s \times s$ skew-symmetric matrix over $\mathbb{F}$. Then

$$HS_{\mathbb{F}_{q^m}[\boldsymbol{m}]/\mathcal{P}_2(\boldsymbol{M})}(z) = \frac{\sum_{d=0}^{s-3}\left(\binom{s-2}{d}^2 - \binom{s-3}{d-1}\binom{s-1}{d+1}\right)z^d}{(1-z)^{2s-3}}.$$

Heuristic: random case

Let $L_1, \ldots, L_k$ be the k linear relationships relative to the matrix code $\mathscr{C}_{\text{mat}}$ associated to a random $[n, s]$-code as above. Let $\mathcal{P}_2^+(\boldsymbol{M}) \stackrel{\text{def}}{=} \mathcal{P}(\boldsymbol{M}) + \langle L_1, \ldots, L_k \rangle$. Then

$$HS_{\mathbb{K}[\boldsymbol{z}]/\mathcal{P}_2^+(\boldsymbol{M})}(z) = \left[(1-z)^{k-2s+3}\sum_{d=0}^{s-3}\left(\binom{s-2}{d}^2 - \binom{s-3}{d-1}\binom{s-1}{d+1}\right)z^d\right]_+.$$

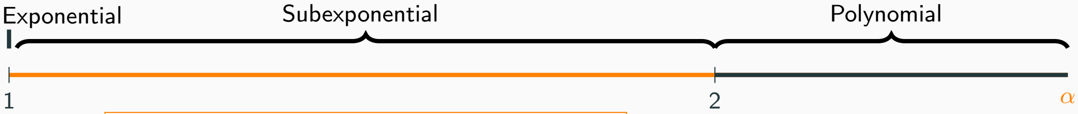
Asymptotics for the degree of regularity

Conjecture: asymptotics random case

Let $\mathcal{P}_2^+(\boldsymbol{M})$ be the Pfaffian ideal associated with a random $[n, k]$ code and $s = n - k$ with rate $> 2/3$. Let $d_0 = \min\{d : HF_{\mathbb{F}[\boldsymbol{m}]/\mathcal{P}_2^+(\boldsymbol{M})}(d) = 0\}$. Then

$$d_0 \sim c\frac{s^2}{k} \quad \text{with } c \approx \frac{1}{4}.$$

Since $HF_{\mathbb{K}[\boldsymbol{z}]/\mathcal{I}}(d)$ can be computed in time $\mathcal{O}\left(md\binom{n+d-1}{d}^{\omega}\right)$,



$$n \sim s^{\alpha} \quad \Rightarrow \quad \mathbb{C} = 2^{\mathcal{O}(s^{2-\alpha}\log(s))}$$

Conclusions...

- New approach based on quadratic forms and the rank invariant
- Modeling for characteristic 2 case in terms of a Pfaffian ideal
  - Upper bound of the complexity of the distinguisher from the Hilbert series
    $\rightarrow$ smoothly ranges between polynomial and exponential (subexponential)
- Efficient attack on some parameters distinguishable by [FGOPT11]:

code	technique/paper	$r(\geq 3)$	q
(generic) distinguishable alternant code	[this] + filtration from [Bardet, M., Tillich 23]	any	any
distinguishable Goppa codes	[this]	$< q-1$	any

...and open questions

- Deeper analysis of HF could lead to sharper complexity estimates
- Transform the new distinguisher into an attack for corresponding parameters

Thank you for the attention

for more details, `eprint.iacr.org/2023/950`