MinRank Gabidulin Encryption Scheme on Matrix Codes

Nicolas Aragon[1] Alain Couvreur[2,3,5] **Victor Dyseryn**[4,5] Philippe Gaborit[1]
Adrien Vinçotte[1]

[1]XLIM, Université de Limoges, France
[2]Inria
[3]LIX, École Polytechnique
[4]LTCI, Télécom Paris
[5]Institut Polytechnique de Paris, France

Bordeaux seminar - February 11, 2025

Families of post-quantum cryptography

- Euclidean lattices
- **Error-correcting codes**
  - Hamming metric
  - Rank metric
- Isogenies
- Quadratic Multivariate
- Hash-based

Families of code-based encryption

- Masking a code with deterministic decoding
  - Small ciphertext size
  - Large public key size
  - Examples: McEliece
- Masking a code with probabilistic decoding
  - Additional cyclic structure to reduce public key size
  - Larger parameters to avoid decryption failures
  - Examples: BIKE, ROLLO
- No masking
  - Fewer security assumptions
  - Larger ciphertext size, decryption failures
  - Examples: HQC, RQC

Comparison

Scheme	pk	ct
Our scheme, variant 1	98 kB	65 B
Classic McEliece	261 kB	96 B
Our scheme, variant 2	33 kB	207 B
ROLLO I	696 B	696 B
KYBER	800 B	768 B
BIKE	1540 B	1572 B
RQC	1834 B	3652 B
HQC	2249 B	4481 B

Figure: Comparison of different schemes for 128 bits of security

Outline

Error-correcting codes

Definition (Error-correcting code)

$$\mathcal{C} \underset{\mathbb{F}_q\text{-subspace}}{\subset} (\mathbb{F}_q)^n$$

- Length n,
- Dimension k,
- Minimal distance $d = \min_{\boldsymbol{x} \in \mathcal{C} \setminus \{\mathbf{0}\}} \{\|\boldsymbol{x}\|\}$.

Error-correcting codes

A code is given by either:

- a generating matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$

$$\mathcal{C} = \{\boldsymbol{x}\boldsymbol{G} | \boldsymbol{x} \in (\mathbb{F}_q)^k\}$$

- a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k) \times n}$

$$\mathcal{C} = \{\boldsymbol{y} \in (\mathbb{F}_q)^n | \boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{0}\}$$

Error-correcting codes

$$\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e} \underset{\text{decoding}}{\longrightarrow} \boldsymbol{e}$$

- For a random $\boldsymbol{G}$: exponential in $\|\boldsymbol{e}\| = w$
- For a "good" $\boldsymbol{G}$: polynomial when $\|\boldsymbol{e}\| \leq w_{max}$

Hamming and Rank metrics

Hamming metric

$$\mathcal{C} \subset (\mathbb{F}_q)^n$$

$$\|x\| = \#\{i \in [1, n] \mid x_i \neq 0\}$$

$$\mathcal{C}_{RS} = \{(P(g_1), \ldots, P(g_n))|\ \deg P < k\}$$

Rank metric

$$\mathcal{C} \subset (\mathbb{F}_{q^m})^n$$

$$\|x\| = \dim\langle x_1, ..., x_n\rangle_{\mathbb{F}_q}$$

$$\mathcal{C}_{Gab} = \left\{(P(g_1), \ldots, P(g_n))|\ \deg_q P < k\right\}$$

$$w_{max} = \frac{n-k}{2}$$

Advantage of rank metric

For a usual choice of $q = 2$, $m = n$, $k = n/2$, w equal to GV bound.

	Hamming metric	Rank metric
Cost of attack ($\log_q$ scale)	$\Theta(n)$	$\Theta(n^2)$
Size of public key	$\Theta(n^2)$	$\Theta(n^3)$

$\downarrow$

	Hamming metric	Rank metric
Size of public key	$\Theta(\lambda^2)$	$\Theta(\lambda^{1.5})$

McEliece encryption

Definition (Key generation)

$$\begin{cases} sk & = & \boldsymbol{g} \text{ (parameters of a code } \mathcal{C}) \\ pk & = & \boldsymbol{G} \text{ (random generating matrix of } \mathcal{C}) \end{cases}$$

Definition (Encrypt)

$\boldsymbol{x} \leftarrow \mathbb{F}_q^k$ (message)
$\boldsymbol{e} \leftarrow \mathcal{S}(\mathbb{F}_q^n, w)$
$\boldsymbol{c} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$.

Definition (Decaps)

From $\boldsymbol{c}$ use $\boldsymbol{g}$ and decoding algorithm of $\mathcal{C}$ to find $\boldsymbol{e}$ (and $\boldsymbol{x}$).

Outline

Problem

$$\boldsymbol{H} = \boldsymbol{S} \begin{pmatrix} 1 & 1 & \dots & 1 \\ \omega_1 & \omega_2 & \dots & \omega_n \\ \vdots & \vdots & & \vdots \\ \omega_1^{t-1} & \omega_2^{t-1} & \dots & \omega_n^{t-1} \end{pmatrix} \begin{pmatrix} \frac{1}{g(\omega_1)} & & & \\ & \frac{1}{g(\omega_2)} & & \\ & & \ddots & \\ & & & \frac{1}{g(\omega_n)} \end{pmatrix}$$

$\boldsymbol{G}$ generating matrix of a Goppa code, associated to $\boldsymbol{H}$, does not leak information

Problem

$$\boldsymbol{G} = \boldsymbol{S} \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & \vdots & & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}$$

$\boldsymbol{G}$ generating matrix of a Gabidulin code, leaks information

Reason for the problem

$$Fr : (\mathbb{F}_{q^m})^n \to (\mathbb{F}_{q^m})^n$$
$$(x_1, x_2, \ldots, x_n) \mapsto (x_1^q, x_2^q, \ldots, x_n^q)$$

$$\begin{pmatrix} \boldsymbol{G} \\ Fr(\boldsymbol{G}) \end{pmatrix} \text{ has rank } k+1 \text{ instead of } \min(2k, n).$$

- For a random $\mathcal{C}$: $Fr(\mathcal{C}) \cap \mathcal{C} = \{0\}$
- For a Gabidulin $\mathcal{C}$: $Fr(\mathcal{C}) \cap \mathcal{C} \neq \{0\}$

Reparation

$$\boldsymbol{G} = \boldsymbol{S}(\boldsymbol{G}_{\mathcal{G}}|\boldsymbol{X})\boldsymbol{P}$$

$\boldsymbol{G}$ still leaks information!

Outline

Our idea: turning vectors into matrices

$$(x_1, x_2, \ldots, x_n) \in (\mathbb{F}_{q^m})^n$$

$$\downarrow$$

$$\begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix} \in (\mathbb{F}_q)^{m \times n}$$

Our idea: turning vectors into matrices

Choose a basis $(\gamma_1, \ldots, \gamma_m)$ of $\mathbb{F}_{q^m}$.
For each i, $x_i = \sum_{j=1}^{m} x_{i,j}\gamma_j$.

$$\Psi_\gamma : (\mathbb{F}_{q^m})^n \to (\mathbb{F}_q)^{m \times n}$$

$$(x_1, x_2, \ldots, x_n) \mapsto \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Matrix error-correcting codes

Definition (Matrix error-correcting code)

$$\mathcal{C} \underset{\mathbb{F}_q\text{-subspace}}{\subset} (\mathbb{F}_q)^{m\times n}$$

- Size $m \times n$,
- Dimension K,
- Minimal distance $d = \min_{\boldsymbol{x}\in\mathcal{C}\setminus\{\boldsymbol{0}\}}\{\|\boldsymbol{x}\|\}$.

$$\begin{aligned}\Psi_\gamma : \mathbb{F}_{q^m}\text{-subspace } \mathcal{C}_{vec} &\mapsto \mathbb{F}_q\text{-subspace } \mathcal{C}_{mat}\\ (\dim)k &\mapsto K = mk\\ (\min \text{rank distance})d &\mapsto d\end{aligned}$$

Matrix error-correcting codes

A matrix code is given by either:

- A basis $(\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K) \in (\mathbb{F}_q^{m \times n})^K$

$$\mathcal{C} = \{\sum_i x_i \boldsymbol{M}_i | (x_1, \ldots, x_K) \in (\mathbb{F}_q)^K\}$$

- A parity-check basis $(\boldsymbol{N}_1, \ldots, \boldsymbol{N}_{mn-K}) \in (\mathbb{F}_q^{m \times n})^{mn-K}$

$$\mathcal{C} = \{\boldsymbol{M} \in (\mathbb{F}_q)^{m \times n} | \forall i, Tr(\boldsymbol{M}\boldsymbol{N}_i^t) = \boldsymbol{0}\}$$

Matrix McEliece encryption

Definition (Key generation)

$$\begin{cases} sk & = & \boldsymbol{g} \text{ (parameters of a code } \mathcal{C}_{vec}) + \text{basis } \gamma \\ pk & = & \mathcal{B} \text{ (random basis of } \Psi_\gamma(\mathcal{C}_{vec})) = (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K) \end{cases}$$

Definition (Encrypt)

$\boldsymbol{x} \leftarrow \mathbb{F}_q^K$ (message)
$\boldsymbol{E} \leftarrow \mathcal{S}(\mathbb{F}_q^{m \times n}, w)$
$\boldsymbol{C} = \sum_i x_i \boldsymbol{M}_i + \boldsymbol{E}$.

Definition (Decrypt)

From $\boldsymbol{C}$ use Ψ_γ^{-1} to transform into a vector $\boldsymbol{c}$, then use $\boldsymbol{g}$ and decoding algorithm of $\mathcal{C}_{vec}$ to find $\boldsymbol{E}$ (and $\boldsymbol{x}$).

Good masking?

$$(x_1, x_2, \ldots, x_n) \longrightarrow (x_1^q, x_2^q, \ldots, x_n^q)$$

$$\begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix} \longrightarrow \quad ?$$

Our hope

Given a vector code $\mathcal{C}_{vec} \subseteq \mathbb{F}_{q^m}^n$ and an $\mathbb{F}_q$–basis γ of $\mathbb{F}_{q^m}$. Then, the matrix code $\mathcal{C}_{mat} = \Psi_\gamma(\mathcal{C}_{vec})$ is indistinguishable from a random matrix code.

$$\left\{ \begin{array}{r} \mathcal{C}_{vec} \xleftarrow{\$} Gr(\mathbb{F}_{q^m}, k) \\ \gamma \xleftarrow{\$} GL(\mathbb{F}_{q^m}) \\ \mathcal{C}_{mat} = \Psi_\gamma(\mathcal{C}_{vec}) \end{array} \right\} \approx \{\mathcal{C} \xleftarrow{\$} Gr(\mathbb{F}_q^{m \times n}, km)\}$$

Detecting the linear structure

$$\mathrm{Stab}_L(\mathcal{C}_{mat}) = \left\{ \boldsymbol{P} \in \mathbb{F}_q^{m \times m} \mid \forall \boldsymbol{C} \in \mathcal{C}_{mat},\ \boldsymbol{PC} \in \mathcal{C}_{mat} \right\}.$$

- For a random $\mathcal{C}_{mat}$: $\dim(\mathrm{Stab}_L(\mathcal{C}_{mat})) \approx 1$
- For a code $\Psi_\gamma(\mathcal{C}_{vec})$: $\dim(\mathrm{Stab}_L(\mathcal{C}_{mat})) \geq m$

Outline

New Idea: Enhanced Matrix Codes Transformation

$$\mathcal{B} = (\boldsymbol{A}_1, \ldots, \boldsymbol{A}_K), \boldsymbol{A}_i \in \mathbb{F}_q^{m \times n}$$

$$\mathcal{RB} = \left(\boldsymbol{P} \begin{pmatrix} \boldsymbol{A}_1 & \boldsymbol{R}_1 \\ \boldsymbol{R}'_1 & \boldsymbol{R}''_1 \end{pmatrix} \boldsymbol{Q}, \ldots, \boldsymbol{P} \begin{pmatrix} \boldsymbol{A}_K & \boldsymbol{R}_K \\ \boldsymbol{R}'_K & \boldsymbol{R}''_K \end{pmatrix} \boldsymbol{Q} \right)$$

with

- $\boldsymbol{R}_i \in \mathbb{F}_q^{m \times \ell_2}, \boldsymbol{R}'_i \in \mathbb{F}_q^{\ell_1 \times m}, \boldsymbol{R}''_i \in \mathbb{F}_q^{\ell_1 \times \ell_2}$
- $\boldsymbol{P} \in \mathbf{GL}_{m+\ell_1}(\mathbb{F}_q)$
- $\boldsymbol{Q} \in \mathbf{GL}_{n+\ell_2}(\mathbb{F}_q)$

Our scheme

Definition (Key generation)

$$\begin{cases} sk & = & \boldsymbol{g}, \text{basis } \gamma, \boldsymbol{P}, \boldsymbol{Q} \\ pk & = & \mathcal{RB} \text{ (basis after transformation)} \end{cases}$$

Definition (Encryption)

$\boldsymbol{x} \leftarrow \mathbb{F}_q^K$ (message)
$\boldsymbol{E} \leftarrow \mathcal{S}(\mathbb{F}_q^{m \times n}, w)$
$\boldsymbol{C} = \sum_i x_i \boldsymbol{M}_i + \boldsymbol{E}$.

Definition (Decryption)

From $\boldsymbol{C}$ use $\boldsymbol{P}^{-1}$, $\boldsymbol{Q}^{-1}$, truncate and Ψ_γ^{-1} to transform into a vector $\boldsymbol{c}$, then use $\boldsymbol{g}$ and decoding algorithm of $\mathcal{C}_{vec}$ to find $\boldsymbol{E}$ (and $\boldsymbol{x}$).

Focus on decryption

$$\boldsymbol{C} = \sum_i x_i \boldsymbol{P} \begin{pmatrix} \boldsymbol{A}_i & \boldsymbol{R}_i \\ \boldsymbol{R}'_i & \boldsymbol{R}''_i \end{pmatrix} \boldsymbol{Q} + \boldsymbol{E}$$

Focus on decryption

$$\boldsymbol{P}^{-1}\boldsymbol{C}\boldsymbol{Q}^{-1} = \sum_i x_i \begin{pmatrix} \boldsymbol{A}_i & \boldsymbol{R}_i \\ \boldsymbol{R}'_i & \boldsymbol{R}''_i \end{pmatrix} + \boldsymbol{P}^{-1}\boldsymbol{E}\boldsymbol{Q}^{-1}$$

Focus on decryption

$$\boldsymbol{C}' = \sum_i x_i \boldsymbol{A}_i + \boldsymbol{E}'$$

$$\downarrow \Psi_\gamma^{-1}$$

$$\boldsymbol{c}' = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}'$$

$$\downarrow \text{Gabidulin decoding}$$

$$\boldsymbol{x}, \boldsymbol{e}'$$

Our combinatorial structural attack

Let $\boldsymbol{U} \in \mathbb{F}_q^{m\times(m+\ell_1)}$, $\boldsymbol{V} \in \mathbb{F}_q^{(n+\ell_2)\times n}$

$$\boldsymbol{U}\begin{pmatrix}\boldsymbol{A}_i & \boldsymbol{R}_i\\ \boldsymbol{R}_i' & \boldsymbol{R}_i''\end{pmatrix}\boldsymbol{V} = \boldsymbol{A}_i$$

if

- $\boldsymbol{U} = (\boldsymbol{U}_0 \mid \boldsymbol{0})$
- $\boldsymbol{V} = \begin{pmatrix}\boldsymbol{V}_0\\ \boldsymbol{0}\end{pmatrix}$

Our combinatorial structural attack

We only have access to

$$\boldsymbol{P}\begin{pmatrix}\boldsymbol{A}_i & \boldsymbol{R}_i\\ \boldsymbol{R}_i' & \boldsymbol{R}_i''\end{pmatrix}\boldsymbol{Q}$$

Our combinatorial structural attack

Sample $\boldsymbol{U} \in \mathbb{F}_q^{m\times(m+\ell_1)}$, $\boldsymbol{V} \in \mathbb{F}_q^{(n+\ell_2)\times n}$

$$\boldsymbol{UP}\begin{pmatrix}\boldsymbol{A}_i & \boldsymbol{R}_i\\ \boldsymbol{R}'_i & \boldsymbol{R}''_i\end{pmatrix}\boldsymbol{QV}$$

with the hope

- $\boldsymbol{UP} = (\boldsymbol{U}_0 \mid \boldsymbol{0})$
- $\boldsymbol{QV} = \begin{pmatrix}\boldsymbol{V}_0\\ \boldsymbol{0}\end{pmatrix}$

How to check: compute the left stabilizer algebra of $\boldsymbol{U}\mathcal{C}\boldsymbol{V}$ until you get a stabilizer of dimension $\geq m$.

Our combinatorial structural attack

The probability of finding a valid pair $\boldsymbol{U}, \boldsymbol{V}$ is

$$\mathbb{P} \approx \frac{q^{m^2+n(k+1)}}{q^{m(m+\ell_1)+(n+\ell_2)(k+1)}} = q^{-(m\ell_1+(k+1)\ell_2)}$$

which yields a complexity of

$$\widetilde{O}(q^{m\ell_1+(k+1)\ell_2})$$

Parameters

Sec.	q	k	m	ℓ_1	ℓ_2	r	pk	ct
128	2	17	37	3	3	10	76 kB	121 B
	2	25	37	3	3	6	78 kB	84 B
	2	35	43	2	2	4	98 kB	65 B
	2	47	53	2	2	3	166 kB	66 B
192	2	51	59	2	2	4	268 kB	89 B
256	2	23	47	3	3	12	191 kB	177 B
	2	37	53	3	2	8	274 kB	139 B
	2	71	79	2	2	4	667 kB	119 B

Figure: Reference parameters for our EGMC-Niederreiter encryption scheme

Parameters

Sec.	q	k	m	ℓ_1	ℓ_2	r	pk	ct
128	2	17	37	3	3	10	76 kB	121 B
	2	25	37	3	3	6	78 kB	84 B
	2	35	43	2	2	4	98 kB	65 B
	2	47	53	2	2	3	166 kB	66 B
192	2	51	59	2	2	4	268 kB	89 B
256	2	23	47	3	3	12	191 kB	177 B
	2	37	53	3	2	8	274 kB	139 B
	2	71	79	2	2	4	667 kB	119 B

Figure: Reference parameters for our EGMC-Niederreiter encryption scheme

Thank you for your attention!