Breaking ACDGV MinRank Gabidulin encryption schemes over matrix codes

Thai Hung Le[1,2]

[1] École normale supérieure, PSL University, CNRS, Inria, France
[2] LTCI, Telecom Paris, Institut Polytechnique de Paris, France
hung.le@ens.fr

Abstract. Enhanced Gabidulin Matrix Codes (EGMC), introduced by Aragon, Couvreur, Dyseryn, Gaborit, and Vinçotte at Asiacrypt 2024, were designed to hide the algebraic structure of Gabidulin matrix codes while enabling very compact McEliece- and Niederreiter-type encryption schemes, with ciphertexts as small as 65 bytes at the claimed 128-bit security level. Their security relies on the assumption that a masked EGMC code is hard to distinguish from a random matrix code. We show that this enhanced construction leaves enough structure for an equivalent code of the secret key to be recovered. Unlike previous cryptanalysis, our attack combines combinatorial and algebraic techniques to recover a Gabidulin-equivalent compressed code. This code can then be extended to a full-length equivalent secret key in polynomial time. As a result, the attack provides both a distinguisher and a key-recovery attack against the EGMC encryption schemes. The attack breaks all 16 proposed EGMC parameter sets by large margins. For example, for the claimed 128-bit parameter set $(2, 17, 37, 4, 0)$, it reduces the security level from 186 bits to 35 bits and in our implementation, the equivalent secret key of this parameter set is recovered in less than 10 minutes.

Keywords: Cryptanalysis · Gröbner basis · Gabidulin · Matrix codes.

1 Introduction

At Asiacrypt 2024, Aragon, Couvreur, Dyseryn, Gaborit, and Vinçotte introduced a new masking scheme for the Gabidulin matrix code enabling the application of the McEliece and Niederreiter framework to build encryption scheme [1]. The main idea is to start from an $\mathbb{F}_{q^m}$-linear Gabidulin code $\mathcal{C}_{\text{vec}}$, expand it to a matrix code $\mathcal{C}_{\text{mat}} = \Psi_\gamma(\mathcal{C}_{\text{vec}}) \subseteq \mathbb{F}_q^{m\times n}$ via an $\mathbb{F}_q$-basis γ of $\mathbb{F}_{q^m}$, then hide the inherited $\mathbb{F}_{q^m}$-structure by appending random extra columns/rows to the basis and scrambling it with invertible matrices P, Q, resulting in an Enhanced Gabidulin Matrix Code (EGMC). An adaptation of the McEliece and Niederreiter encryption framework to general matrix codes is introduced by hiding a basis of a secret matrix code, for which there exists an efficient decoding algorithm. The authors finally applied these two frameworks to EGMC and introduced two encryption schemes: EGMC-McEliece and EGMC-Niederreiter. By

analyzing possible attacks, the authors finally proposed two set of parameters for EGMC-Niederreiter encryption schemes that offer small ciphertext sizes. Later, at Eurocrypt 2026, Porwal, Wachter-Zeh, and Loidreau introduced an improved key-recovery attack on the schemes [12]. Their attack is based on the kernel attack against the underlying MinRank problem and breaks 5 of the 16 proposed parameter sets. Although the attack remains exponential, it reduces the claimed security of one parameter set targeting 192-bit security to about 161 bits, while that of a 256-bit parameter set is reduced to about 223 bits.

In this work, we introduce a new distinguisher and its extension into a key-recovery attack against the EGMC-McEliece and EGMC-Niederreiter encryption schemes. Unlike the combinatorial distinguisher from [1], which guesses both compression (or unscrambling) matrices U and V by brute force, our distinguisher guesses only one of the matrices and uses algebraic techniques to solve for the other one. We consider two variants of the attack: guess-V-solve-U, which guesses a column compression V and solves for the row compression U, and guess-U-solve-V, which guesses a row compression U and solves for the full dual space of the hidden compressed Gabidulin code.

Whenever the distinguisher succeeds, it reveals a punctured code of the secret $\mathbb{F}_{q^m}$-linear code. The second part of the attack extends the punctured code back to the original code in polynomial time by exploiting the structure of Gabidulin codes. Overall, the attack breaks all 16 parameter sets (see Table 1). For example, an implementation of the attack recovers the equivalent secret keys of the parameter set (2, 17, 37, 4, 0) targeting 128-bit security level within less than 10 minutes. Details of the implementation of the attack can be found at

`https://gitlab.di.ens.fr/hle/attack_egmc`.

Our attack is different from known attacks as the known distinguishers and key-recovery attacks against EGMC parameters are exponential due to the cost of either brute force or MinRank solver. In such a situation, one may hope to restore security by increasing the parameters. In contrast, our attack becomes polynomial-time whenever one of the two appending factors $\ell_1 = 0$ or $\ell_2 = 0$. For these parameter families, increasing parameters while keeping either $\ell_1 = 0$ or $\ell_2 = 0$ without changing the masking construction does not restore the post-quantum security because the algebraic solving step still reveals the remaining hidden compression matrix in polynomial time. A repair would have to keep both ℓ_1 and ℓ_2 nonzero and choose them large enough so that the minimum of the two directions of our attack exceeds the target security level. However, since increasing ℓ_1 and ℓ_2 directly increases the dimensions of the public matrix code, and hence the key and ciphertext sizes, whether such a repair remains competitive is still needed to be investigated. Table 1 summarizes the cost of our attack for both the reference parameters and the alternative parameters of the EGMC-Niederreiter encryption scheme and compares them with the best previous attack as in [1] and [12].

The rest of the paper is organized as follows. Section 2 recalls some preliminaries, the EGMC masking transformation, and the known attacks considered in the original article and in [12]. Section 3 introduces the hybrid distinguisher

Table 1: The cost of our attack versus the best previous attacks for the reference and alternate parameter sets. Complexities are given as $\log_2$ of the estimated gate count. The columns $V \to U$ and $U \to V$ give respectively the guess-V-solve-U and the guess-U-solve-V costs, with the better of the two shown in bold. The complexities of the best previous attacks are taken from [1,12].

Sec.	q	k	m	ℓ_1	ℓ_2	pk	ct	$V \to U$	$U \to V$	Previous best attack [1,12]
128	2	17	37	3	3	76 kB	121 B	**88**	164	165
	2	25	37	3	3	78 kB	84 B	**114**	164	150
	2	35	43	2	2	98 kB	65 B	**108**	135	145
	2	47	53	2	2	166 kB	66 B	**134**	155	147
	2	17	37	4	0	70 kB	111 B	**35**	186	112
	16	13	23	1	1	41 kB	138 B	**82**	130	148
	16	7	23	0	5	33 kB	207 B	183	**49**	160
192	2	51	59	2	2	268 kB	89 B	**142**	170	209
	2	23	43	5	0	133 kB	134 B	**38**	255	161
	2	33	47	5	0	173 kB	111 B	**41**	275	221
	2	41	53	4	0	230 kB	106 B	**41**	253	212
256	2	23	47	3	3	191 kB	177 B	**108**	198	240
	2	37	53	3	2	274 kB	139 B	**115**	214	262
	2	71	79	2	2	667 kB	119 B	**185**	213	289
	16	9	29	2	1	87 kB	334 B	**69**	272	223
	16	17	29	2	1	107 kB	218 B	**103**	273	304

in its two directions: guess-V-solve-U and guess-U-solve-V. Section 4 shows how to extend the recovered punctured code to an equivalent full secret Gabidulin code. Section 5 explains how this equivalent trapdoor decrypts both EGMC-McEliece and EGMC-Niederreiter ciphertexts. Section 6 shows the arguments for the rank-1 solving step, and Section 7 computes the cost for the concrete parameter sets.

2 Preliminaries

Notation

- We use ordinary letters for scalars, vectors, matrices, and calligraphic letters for vector spaces.
- For vectors x, y, $\langle x, y \rangle$ denotes their inner product $\sum_i x_i y_i$.
- For a vector v, $v[i]$ denotes its i-th coordinate. For a matrix M, $M[i, j]$ denotes its entry at i-th row and j-th column.
- Subscripts such as v_i and M_i denote a vector and a matrix in a families of vectors and matrices.
- For matrices A and B with the same number of rows, $[A \mid B]$ denotes their horizontal concatenation. The same convention is used for $[A_1 \mid \cdots \mid A_s]$.
- $M^\top$ denotes the transpose of a matrix M.
- $\mathbf{V}(I)$ denotes the variety of the ideal I.

– For any field $\mathbb{K}$, positive integers a, b, and $M = (M[i,j])$ we define the vectorization map that sends a matrix to a vector as

$$\begin{aligned} \mathrm{vec}_{a,b} : \mathbb{K}^{a\times b} &\longrightarrow \mathbb{K}^{ab} \\ M &\longmapsto (M[1,1], \ldots, M[1,b], M[2,1], \ldots, M[a,b]). \end{aligned}$$

The reshaping map is defined as the inverse of the vectorization map

$$\mathrm{mat}_{a,b} = \mathrm{vec}_{a,b}^{-1}.$$

– We define $\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ to be the Frobenius automorphism $\sigma(x) = x^q$.
– For a vector v, $v^{[q^i]}$ denotes the vector obtained by applying σ entrywise to v. For a matrix V, $V^{[q^i]}$ denotes the matrix obtained by applying σ entrywise to V.
– Two matrix codes $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^{a\times b}$ are called *equivalent* if there exist $L \in \mathrm{GL}_a(\mathbb{F}_q)$ and $R \in \mathrm{GL}_b(\mathbb{F}_q)$ such that $\mathcal{B} = L\mathcal{A}R$.
– For a positive integer n, we denote by $\mathrm{GL}_n(\mathbb{F}_q) = \{A \in \mathbb{F}_q^{n\times n} : \det(A) \neq 0\}$ the general linear group of invertible $n \times n$ matrices over $\mathbb{F}_q$. Its size is $|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$.
– For integers $0 \leq r \leq n$, we denote by $\mathrm{Gr}(r,n) = \{\mathcal{U} \subset \mathbb{F}_q^n : \dim_{\mathbb{F}_q}(\mathcal{U}) = r\}$ the Grassmannian of r-dimensional linear subspaces of $\mathbb{F}_q^n$. Its size is the Gaussian binomial coefficient $|\mathrm{Gr}(r,n)| = \binom{n}{r}_q = \prod_{i=0}^{r-1} \frac{q^n - q^i}{q^r - q^i}$.

2.1 Gabidulin Codes

Gabidulin codes [8,9] are a class of rank-metric codes that can be defined as an evaluation code on a class of q-polynomial of q-degree r in $\mathbb{F}_{q^m}[x]$ of the form

$$P(x) = a_0 x + a_1 x^q + a_2 x^{q^2} + \cdots + a_r x^{q^r}.$$

We denote by $\mathbb{F}_{q^m}[x]_{<k}$ the set of q-polynomials of q-degree strictly less than k. Let $k \leq n \leq m$ be integers, and let $g = \{g_1, \ldots, g_n\}$ be a set of n linearly independent elements of $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$, then the Gabidulin code of length n, dimension k, evaluation vector g, denoted $\mathcal{G}_g(n,k,m)$ is defined by:

$$\mathcal{G}_g(n,k,m) = \{(P(g_1), ..., P(g_n)) \mid P \in \mathbb{F}_{q^m}[x]_{<k}\}.$$

2.2 Gabidulin Matrix Codes

Let $\gamma = (\gamma_1, \ldots, \gamma_m)$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. The γ-expansion of an element in $\mathbb{F}_{q^m}$ to a vector in $\mathbb{F}_q^m$ is defined as the map:

$$\begin{aligned} \Psi_\gamma : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q^m \\ x = \sum_{i=1}^{m} x_i \gamma_i &\longmapsto (x_1, \ldots, x_m) \end{aligned}$$

We can extend Ψ_γ naturally coordinate-wise to a word $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ by reading the expanded coordinates as columns:

$$\Psi_\gamma(x) = \big[\Psi_\gamma(x_1) \mid \cdots \mid \Psi_\gamma(x_n)\big] \in \mathbb{F}_q^{m\times n}.$$

Its inverse therefore identifies a matrix in $\mathbb{F}_q^{m\times n}$ with the corresponding word in $\mathbb{F}_{q^m}^n$, column by column. When the basis γ is fixed, we simply write Ψ for Ψ_γ. Then a Gabidulin code can be turned into a Gabidulin matrix code of size $m\times n$ and dimension mk by applying the γ-extension. However, different γ-extensions of a Gabidulin code produce left-equivalent Gabidulin matrix codes (see [3]).

It is well-known that Gabidulin codes reach the Singleton bound, i.e. they have minimum rank distance $n-k+1$; and have efficient decoding algorithm up to the unique decoding radius $\frac{n-k}{2}$ [10]. However, Gabidulin codes can easily be distinguished from random $\mathbb{F}_{q^m}$-linear codes, and therefore cannot be directly used inside a McEliece-like cryptosystem [4,11].

Overbeck distinguisher for Gabidulin matrix codes The Gabidulin code, as a $\mathbb{F}_{q^m}$-linear code, can be distinguished from a $\mathbb{F}_q$-linear random code in polynomial time by computing the left stabilizer algebra [3]. In this section, we explain why a Gabidulin code can also be distinguished from a random $\mathbb{F}_{q^m}$-linear code in polynomial time using the Overbeck distinguisher [11].

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear $[n,k]$ code, we define the *Frobenius sum*

$$\Lambda_f(\mathcal{C}) \;=\; \mathcal{C} + \mathcal{C}^{[q^1]} + \cdots + \mathcal{C}^{[q^f]}.$$

Let G is a generator matrix of $\mathcal{C}$ then a generator matrix of $\Lambda_f(\mathcal{C})$ is obtained by stacking these Frobenius powers by rows:

$$G_{\Lambda,f} = \begin{bmatrix} G \\ G^{[q^1]} \\ \vdots \\ G^{[q^f]} \end{bmatrix}.$$

For a Gabidulin code $\mathcal{C}_{\mathrm{Gab}}$, one has $\dim_{\mathbb{F}_{q^m}} \Lambda_f(\mathcal{C}_{\mathrm{Gab}}) = \min\{n, k+f\}$, whereas for a random $[n,k]$ code one typically has $\dim_{\mathbb{F}_{q^m}} \Lambda_f(\mathcal{C}) = \min\{n, k(f+1)\}$, because the $f+1$ Frobenius shifts are generically $\mathbb{F}_{q^m}$-linearly independent. This gap yields a polynomial-time distinguisher and forms the basis of Overbeck's structural key-recovery: by choosing f appropriately, one reconstructs a larger Gabidulin code (with the same evaluation vector) from a suitable subcode and then recovers the evaluation vector g, obtaining an equivalent secret key. Computing $\dim \Lambda_f(\mathcal{C})$ amounts to Gaussian elimination on an $((f+1)k)\times n$ matrix over $\mathbb{F}_{q^m}$, with cost $\tilde{\mathcal{O}}\big(((f+1)k)^2\, n\big)$ operations in $\mathbb{F}_{q^m}$, and in the common regime $(f+1)k = \Theta(n)$ this is $\tilde{\mathcal{O}}(n^3)$. The subsequent recovery of the Gabidulin support/evaluation vector can be done in polynomial time, often stated as $\mathcal{O}(n^3)$ operations in $\mathbb{F}_{q^m}$.

2.3 Enhanced Gabidulin Matrix Codes (EGMC)

In [1], a new transformation, named "Random rows and columns matrix code transformation", was introduced to mask a secret Gabidulin matrix code. Its main goal is to prevent the Overbeck attack mentioned previously.

Definition 1 (Random Rows and Columns matrix code transformation [1]). *Let $m, n, K, \ell_1, \ell_2 \in \mathbb{N}$. Let $\mathcal{C}_{mat}$ be a matrix code of size $m \times n$ and dimension K over $\mathbb{F}_q$. Let $\mathcal{B} = (\mathbf{A}_1, \ldots, \mathbf{A}_K)$ be a basis of $\mathcal{C}_{mat}$. The Random Rows and Columns matrix code transformation consists in sampling uniformly at random the following matrices: $\mathbf{P} \xleftarrow{\$} \mathbf{GL}_{m+\ell_1}(\mathbb{F}_q)$, $\mathbf{Q} \xleftarrow{\$} \mathbf{GL}_{n+\ell_2}(\mathbb{F}_q)$ and $3K$ random matrices: $\mathbf{R}_i \xleftarrow{\$} \mathbb{F}_q^{m \times \ell_2}$, $\mathbf{R}'_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times n}$ and $\mathbf{R}''_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times \ell_2}$; and define the matrix code whose basis is:*

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

An Enhanced Gabidulin matrix code $\mathcal{EG}_{\boldsymbol{g}}(n, k, m, \ell_1, \ell_2)$ is the matrix code $\Psi_\gamma(\mathcal{G})$ on which we apply the Random Rows and Columns matrix code transformation above.

Definition 2 (EGMC$(k, m, n, \ell_1, \ell_2)$ distribution [1]). *Let $k, m, n, \ell_1, \ell_2 \in \mathbb{N}$ be such that $k \leq n \leq m$. The Enhanced Gabidulin Matrix Code distribution EGMC$(k, m, n, \ell_1, \ell_2)$ sample $\mathbf{g} = (g_1, \ldots, g_n)$ uniformly at random among all n-tuples of $\mathbb{F}_{q^m}$ that are $\mathbb{F}_q$-linearly independent, , a basis $\gamma \xleftarrow{\$} \mathcal{B}(\mathbb{F}_{q^m})$, $\mathbf{P} \xleftarrow{\$} \mathbf{GL}_{m+\ell_1}(\mathbb{F}_q)$, $\mathbf{Q} \xleftarrow{\$} \mathbf{GL}_{n+\ell_2}(\mathbb{F}_q)$ and $3km$ random matrices: $\mathbf{R}_i \xleftarrow{\$} \mathbb{F}_q^{m \times \ell_2}$, $\mathbf{R}'_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times n}$ and $\mathbf{R}''_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times \ell_2}$; computes $\mathcal{B} = (\mathbf{A}_1, \ldots, \mathbf{A}_{km})$ a basis of the matrix code $\Psi_\gamma(\mathcal{G})$, and outputs the matrix code with basis:*

$$\mathcal{RB} = \left(\mathbf{P} \begin{bmatrix} \mathbf{A}_1 & \mathbf{R}_1 \\ \mathbf{R}'_1 & \mathbf{R}''_1 \end{bmatrix} \mathbf{Q}, \ldots, \mathbf{P} \begin{bmatrix} \mathbf{A}_{km} & \mathbf{R}_{km} \\ \mathbf{R}'_{km} & \mathbf{R}''_{km} \end{bmatrix} \mathbf{Q} \right).$$

Definition 3 (EGMC-Indistinguishability problem [1]). *Given a matrix code $\mathcal{C}_{mat}$ of size $(m + \ell_1) \times (n + \ell_2)$ and dimension mk, the Decisional EGMC-Indistinguishability $(k, m, n, \ell_1, \ell_2)$ problem asks to decide with non-negligible advantage whether $\mathcal{C}_{mat}$ is sampled from the EGMC$(k, m, n, \ell_1, \ell_2)$ distribution or the uniform distribution over the set of $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^{(m+\ell_1)\times(n+\ell_2)}$ of dimension mk.*

Definition 4 (EGMC-Search problem [1]). *Let $k, m, n, \ell_1, \ell_2 \in \mathbb{N}$ be such that $k \leq n \leq m$, and $\mathcal{C}_{mat}$ sampled from the EGMC$(k, m, n, \ell_1, \ell_2)$ distribution. The EGMC-Search problem asks to retrieve the basis $\gamma \in \mathcal{B}(\mathbb{F}_{q^m})$ and the evaluation vector $\mathbf{g} \in \mathbb{F}_{q^m}^n$ used to construct $\mathcal{C}_{mat}$.*

It should be noted that the outputs of this search problem are not unique as changing γ corresponds to left multiplication by an invertible matrix over $\mathbb{F}_q$; changing the evaluation vector by an $\mathbb{F}_q$-linear transformation can produce

equivalent Gabidulin descriptions; and, the masking by (P, Q) further destroys uniqueness. We can say that what is normally and necessarily recoverable is an *equivalent trapdoor*, not the original $(\gamma, \mathbf{g})$.

2.4 EGMC-McEliece and EGMC-Niederreiter encryption schemes

In [1], the authors proposed two encryption schemes whose the public key is an Enhanced Gabidulin Matrix Code, and the secret key is the original Gabidulin matrix code and two scambling matrices (see Appendix C). The security of these encryption schemes is based on the conjectured difficulty of the EGMC-Indistinguishability problem.

2.5 Previous attacks on EGMC

This subsection recalls the attacks considered in the security analysis of EGMC [1] and in the cryptanalysis by Porwal, Wachter-Zeh, and Loidreau [12]. All of these attacks have exponential complexity.

The combinatorial distinguisher of EGMC In [1], the authors introduced a combinatorial distinguisher that solves the EGMC-Indistinguishability problem with the complexity of

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

The idea is to apply a projection map on both the row and column spaces of the public code $\mathcal{C}$ to get rid of the contributions of the matrices R_i, R_i' and R_i'' while not destroying the underlying $\mathbb{F}_{q^m}$-linear structure. Likewise, in the terminology used throughout the rest of the paper, these projection matrices are the row and column compression matrices: *the row compression is the matrix multiplying public codewords on the left, and the column compression is the matrix multiplying them on the right.* We guess two such compression matrices: a full-rank row compression $U = [\, U_0 \mid 0 \,] \in \mathbb{F}_q^{m\times(m+\ell_1)}$, where $U_0 \in \mathrm{GL}_m(\mathbb{F}_q)$; and for some integer n' such that $k < n' \leq n$, a full-rank column compression $V = \begin{bmatrix} V_0 \\ 0 \end{bmatrix} \in \mathbb{F}_q^{(n+\ell_2)\times n'}$ where $V_0 \in \mathbb{F}_q^{n\times n'}$.

The resulting compressed code is $U\mathcal{C}V = \{UMV : M \in \mathcal{C}\}$. Then we can distinguish any $\mathbb{F}_{q^m}$-linear code, and hence $\mathcal{C}$, from a random code by computing the dimension of the left stabilizer of $U\mathcal{C}V$. We need $n' > k$ because if $n' \leq k$, then any k-dimensional $\mathbb{F}_{q^m}$-linear code of length n' coincides with the whole ambient space $\mathbb{F}_{q^m}^{n'}$. Under matrix representation this is $\mathbb{F}_q^{m\times n'}$, whose left stabilizer algebra is the full matrix algebra $\mathcal{M}_m(\mathbb{F}_q)$. In that regime the method can not distinguish. Therefore the smallest informative choice is $n' = k + 1$.

Overbeck-like distinguishers of EGMC In EGMC-type constructions, the Frobenius map in the original Overbeck attack [11] is *not directly available* on the public matrix code, so an Overbeck attack cannot be applied directly. However,

an Overbeck-like distinguisher has been proposed in the security analysis of EGMC: One can use the fact that for a hidden Gabidulin matrix code there exist nontrivial multipliers D such that the span of $C + DC$ fails to fill the ambient space, while for a random code it typically does. This leads to a bilinear system in unknowns (D, M) with constraints of the form $\mathrm{Tr}(DCM^\top) = 0$ for all public basis matrices C; naive linearization yields too many variables (on the order of m^4) for only $\Theta(m^2)$ equations, suggesting infeasibility for the targeted parameters.

Key Recovery Attack based on the kernel attack of the Minrank problem [12] At Eurocrypt 2026, Porwal, Wachter-Zeh and Loidreau introduced a Minrank-based key-recovery attack against EGMC. The cost of the attack is still exponential but it breaks 5 over 16 parameter sets of EGMC. The attack exploits the fact that the hidden Gabidulin matrix code has a large left-stabilizer algebra, whereas a random public-looking matrix code has stabilizer dimension only 1. For public generators

$$B_i = P \begin{bmatrix} A_i & * \\ * & * \end{bmatrix} Q,$$

the attacker searches for a matrix F and public codewords $C_i \in \mathcal{C}_{\mathrm{pub}}$ such that

$$FB_i - C_i = P \begin{bmatrix} 0 & * \\ * & * \end{bmatrix} Q.$$

This is done by guessing left and right kernel vectors v, w and using the linear equations

$$v^\top \left(FB_i - \sum_j \mu_{i,j} B_j \right) w = 0$$

to solve for F and the coefficients $\mu_{i,j}$. Once such relations are found, they reveal enough information about the hidden row and column transformations P, Q to remove the appended random rows and columns, thereby recovering a code equivalent to $\mathcal{C}_{\mathrm{mat}}$.

Message attacks Two classes of attacks on the message are analyzed in the security analysis of EGMC in [1]: generic rank decoding attacks and MinRank attacks. These attacks do not exploit the hidden Gabidulin structure in the same way as the structural distinguishers above; they are recalled here to explain the baseline security model used for the proposed parameters.

Generic rank decoding. Given a ciphertext $y = xG_{\mathrm{pub}} + z$ with $\mathrm{Rank}(z) = r$, an attacker without the key faces the rank-metric decoding problem for a length-n code over $\mathbb{F}_{q^m}$. Generic rank decoding algorithms have exponential cost in the security parameters; historically, this was one motivation for rank-metric McEliece variants (before structural breaks).

Generic MinRank. For matrix-code McEliece/Niederreiter frames, decrypting without the secret key reduces to solving the following MinRank instance from public matrices M_i spanning the public code : $\mathrm{Rank}(Y - \sum_{i=1}^{K} x_i M_i) \leq r$. These attacks have exponential costs for proposed parameters of EGMC.

3 Hybrid Distinguisher for EGMC

This section introduces a new "hybrid" distinguisher for the EGMC Indistinguishability Problem. Let $k \leq n \leq m$ and $\mathcal{C} \subset \mathbb{F}_q^{(m+\ell_1)\times(n+\ell_2)}$ be the public $\mathbb{F}_q$-subspace of dimension mk, which is EGMC in our setting. Let $\mathcal{U}$ be the set of full-rank matrices $U \in \mathbb{F}_q^{m\times(m+\ell_1)}$, and let $\mathcal{V}$ be the set of full-rank matrices $V \in \mathbb{F}_q^{(n+\ell_2)\times(k+1)}$. For a chosen pair of matrices $(U, V) \in \mathcal{U} \times \mathcal{V}$, define

$$\begin{aligned} \delta_{U,V} : \mathbb{F}_q^{(m+\ell_1)\times(n+\ell_2)} &\longrightarrow \mathbb{F}_q^{m\times(k+1)} \\ X &\longmapsto UXV, \end{aligned}$$

and we set $\mathcal{S}_{U,V} = \delta_{U,V}(\mathcal{C}) \subseteq \mathbb{F}_q^{m\times(k+1)}$ the compressed code of $\mathcal{C}$ by U and V.

The hybrid distinguisher is based on the following main idea: *instead of guessing both a row compression and a column compression, one guesses one compression and solves algebraically for the other one.*

We present two directions. The first is the guess-V-solve-U direction, where one guesses a column compression $V \in \mathbb{F}_q^{(n+\ell_2)\times(k+1)}$ and solves for a row compression $U \in \mathbb{F}_q^{m\times(m+\ell_1)}$ such that the compressed code $\mathcal{S}_{U,V}$ is *equivalent* to a matrix representation of a $[k+1, k]$ Gabidulin code over $\mathbb{F}_{q^m}$. The second is the guess-U-solve-V direction, where one guesses U and solves for a full column compression V with a similar goal in mind.

Remark 1. To be more precise about the code equivalence property, from now on we work with an equivalence class of (U, V) where $(U', V') \sim (U, V)$ when there exist $G \in \mathrm{GL}_m(\mathbb{F}_q)$, $H \in \mathrm{GL}_{k+1}(\mathbb{F}_q)$ such that $(U', V') = (GU, VH)$. $\mathcal{S}_{U,V}$ is equivalent to a matrix representation of a $[k+1, k]$ Gabidulin code means that it is a $[k+1, k]$ Gabidulin code up to left and right multiplication by invertible matrices over $\mathbb{F}_q$. The specific subspace $\mathcal{S}_{U,V}$ depends on the choice of representative U, V, but this equivalence property depends only on the equivalence class of the pair.

3.1 Guess-V-solve-U direction

Phase 1: Guessing V. We treat V as the "guess" variable. We call V *valid* if there exists a matrix U such that the pair (U, V) compresses $\mathcal{C}$ into a subspace $\mathcal{S}_{U,V}$ such that $\mathcal{S}_{U,V}$ is equivalent to a $[k+1, k]$ Gabidulin code.

Due to the construction of the EGMC, we know that if $V = Q^{-1}V'$ and $V' = [(V'')^\top \mid 0]^\top$ where $V'' \in \mathbb{F}_q^{n\times(k+1)}$, $Q \in \mathrm{GL}_{n+\ell_2}(\mathbb{F}_q)$ (as in Definition 2), then there exists a pair (U, V) compressing $\mathcal{C}$ into the desired Gabidulin code.

Therefore, the probability of guessing a valid V among random full-rank matrices of size $(n+\ell_2)\times(k+1)$ is

$$\frac{|\mathrm{Gr}(k+1,n)|}{|\mathrm{Gr}(k+1,n+\ell_2)|} = \frac{\binom{n}{k+1}_q}{\binom{n+\ell_2}{k+1}_q} \approx q^{-(k+1)\ell_2}.$$

Phase 2: Algebraic Modeling. We first describe the overall idea before diving into details. For a valid guess V, the compressed code $\mathcal{S}_{U,V}$ should become, after the column-wise identification with $\mathbb{F}_{q^m}^{k+1}$, an $\mathbb{F}_{q^m}$-hyperplane. Thus it is annihilated by some nonzero vector $h \in \mathbb{F}_{q^m}^{k+1}$. We model this condition with the unknown row compression U and the unknown hyperplane vector h, obtaining a bilinear system in the entries of h and in the columns of U. We then linearize the system and compute its kernel. Since this linear system is underdetermined, its kernel contains many linearized solutions. Yet, the solutions coming from an actual pair (h,U) are precisely the kernel elements whose product matrix $W=(w_{j,s})$ has rank 1. We now explain the algebraic model in more details.

Using the coordinate-wise extension of $\Psi=\Psi_\gamma$, let $\mathrm{col}_{\mathbb{F}_{q^m}}$ denote the inverse word expansion on $k+1$ columns:

$$\begin{aligned}\mathrm{col}_{\mathbb{F}_{q^m}} = \left(\Psi^{-1}\right)^{\oplus k+1} : \mathbb{F}_q^{m\times(k+1)} &\longrightarrow \mathbb{F}_{q^m}^{k+1}\\ \left([x_1|\cdots|x_{k+1}]\right) &\longmapsto \left(\Psi^{-1}(x_1),\ldots,\Psi^{-1}(x_{k+1})\right).\end{aligned}$$

For a valid V, there exists U such that $\mathcal{S}_{U,V}$ has dimension mk since it is equivalent to a $[k+1,k]$ Gabidulin matrix code. Here, equivalence means there exists another basis γ' of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that $\mathcal{S}_{U,V}=\Psi_{\gamma'}(\mathcal{D})$ for an $\mathbb{F}_{q^m}$-linear code $\mathcal{D}\subseteq\mathbb{F}_{q^m}^{k+1}$ of dimension k. However, as the code is equivalence up to the left-multiplication by a matrix in $\mathrm{GL}_m(\mathbb{F}_q)$, we may assume $\gamma'=\gamma$. Therefore, we have the following proposition:

Proposition 1. *If $\mathcal{S}_{U,V}$ is equivalent to the matrix representation of a $[k+1,k]$ Gabidulin code over $\mathbb{F}_{q^m}$ then there exists a nonzero vector $h\in\mathbb{F}_{q^m}^{k+1}$, unique up to $\mathbb{F}_{q^m}^\times$-scaling, such that*

$$\mathrm{col}_{\mathbb{F}_{q^m}}(\mathcal{S}_{U,V}) = \{x\in\mathbb{F}_{q^m}^{k+1} : \langle h,x\rangle = 0\}.$$

Proof. We have $\mathcal{S}_{U,V}=\Psi_\gamma(\mathcal{D})$ for an $\mathbb{F}_{q^m}$-linear code $\mathcal{D}\subseteq\mathbb{F}_{q^m}^{k+1}$ of dimension k. That implies $\mathrm{col}_{\mathbb{F}_{q^m}}(\mathcal{S}_{U,V})=\mathcal{D}$. In other words, $\mathrm{col}_{\mathbb{F}_{q^m}}(\mathcal{S}_{U,V})$ is an $\mathbb{F}_{q^m}$-hyperplane in $\mathbb{F}_{q^m}^{k+1}$, so there exists a nonzero $h\in\mathbb{F}_{q^m}^{k+1}$, unique up to $\mathbb{F}_{q^m}^\times$-scaling, such that $\mathrm{col}_{\mathbb{F}_{q^m}}(\mathcal{S}_{U,V}) = \{x\in\mathbb{F}_{q^m}^{k+1} : \langle h,x\rangle=0\}$.

Using Proposition 1, the problem of finding U is equal to finding $h\in\mathbb{F}_{q^m}^{k+1}\setminus\{0\}$ such that

$$\left\langle h,\ \mathrm{col}_{\mathbb{F}_{q^m}}(\mathcal{S}_{U,V})\right\rangle = 0. \tag{1}$$

For a fixed basis $\{c_1, \ldots, c_{mk}\}$ of $\mathcal{C}$, Equation (1) has $(k+1)\times(m+\ell_1)$ bilinear variables over $\mathbb{F}_{q^m}$ and mk equations whose coefficients are over $\mathbb{F}_q$. Indeed, we set

$$\begin{aligned} s_i &= Uc_iV \in \mathcal{S}_{U,V} \quad \forall\, i = 1, \ldots, mk \\ D_i &= c_iV \in \mathbb{F}_q^{(m+\ell_1)\times(k+1)} \quad \forall\, i = 1, \ldots, mk. \end{aligned}$$

We write D_i as $[d_{i,1}|\cdots|d_{i,k+1}]$ with $d_{i,j} \in \mathbb{F}_q^{m+\ell_1}$ and $U \in \mathbb{F}_q^{m\times(m+\ell_1)}$ by columns $U = [u_1^{(\mathrm{vec})}|\cdots|u_{m+\ell_1}^{(\mathrm{vec})}]$ with $u_s^{(\mathrm{vec})} \in \mathbb{F}_q^m$. Then, we convert these columns $u^{(\mathrm{vec})}$ to a vector $u \in \mathbb{F}_{q^m}^{m+\ell_1}$ with the coordinates

$$u[s] = \Psi^{-1}\big(u_s^{(\mathrm{vec})}\big) \in \mathbb{F}_{q^m} \quad \forall\, s \in 1, \ldots, m+\ell_1.$$

Then for each (i,j) :

$$\begin{aligned} \Psi^{-1}(Ud_{i,j}) &= \Psi^{-1}\left(\sum_{s=1}^{m+\ell_1} d_{i,j}[s]u_s^{(\mathrm{vec})}\right) \\ &= \sum_{s=1}^{m+\ell_1} d_{i,j}[s]\Psi^{-1}\left(u_s^{(\mathrm{vec})}\right) \text{ because } d_{i,j}[s] \in \mathbb{F}_q \text{ and } \Psi \text{ is } \mathbb{F}_q\text{-linear} \\ &= \sum_{s=1}^{m+\ell_1} d_{i,j}[s]u[s] \ \in \ \mathbb{F}_{q^m}. \end{aligned}$$

Then we have

$$\begin{aligned} \textit{Equation (1)} &\iff \sum_{j=1}^{k+1} h[j]\cdot\Psi^{-1}(Ud_{i,j}) = 0 \\ &\iff \sum_{j=1}^{k+1}\sum_{s=1}^{m+\ell_1} d_{i,j}[s](h[j]u[s]) = 0. \end{aligned} \tag{2}$$

Now, we introduce the bilinear products

$$w[j,s] = h[j]u[s] \in \mathbb{F}_{q^m} \text{ where } \ 1 \le j \le k+1,\ 1 \le s \le m+\ell_1.$$

Then the constraints (2) become the linear system over $\mathbb{F}_{q^m}$:

$$\sum_{j=1}^{k+1}\sum_{s=1}^{m+\ell_1} d_{i,j}[s]w[j,s] = 0 \ \text{ for } i = 1, \ldots, mk, \tag{3}$$

where all coefficients $d_{i,j}[s]$ lie in the subfield $\mathbb{F}_q$. Let $N_w = (k+1)(m+\ell_1)$ and set

$$w = \big(w[j,s]\big)_{\substack{1\le j\le k+1\\ 1\le s\le m+\ell_1}} \in \mathbb{F}_{q^m}^{N_w}.$$

Then (3) is a homogeneous linear system of mk equations, with all coefficients in $\mathbb{F}_q$, while the N_w unknowns are in $\mathbb{F}_{q^m}$.

Let $A(V) \in \mathbb{F}_q^{mk \times N_w}$ be the coefficient matrix of (3) as these coefficents depend on the guess of V. In more details, its entries are the scalars $d_{i,j}[s] \in \mathbb{F}_q$ placed in the obvious way. Since all entries of $A(V)$ lie in $\mathbb{F}_q$, its right kernel over $\mathbb{F}_{q^m}$ is obtained from its right kernel over $\mathbb{F}_q$ by scalar extension $\ker_{\mathbb{F}_{q^m}} A(V) = \mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} \ker_{\mathbb{F}_q} A(V)$, identified with the $\mathbb{F}_{q^m}$-solution space by $\alpha \otimes x \mapsto \alpha x$, so the same $\mathbb{F}_q$-basis is also a basis of $\ker_{\mathbb{F}_{q^m}} A(V)$ after scalar extension. However, this does not mean that the kernel elements we seek have entries in $\mathbb{F}_q$ since the unknowns $w[j,s]$ are still $\mathbb{F}_{q^m}$-valued. It only means that, because the linear equations are defined over the subfield $\mathbb{F}_q$, the $\mathbb{F}_{q^m}$-solution space admits a basis with entries in $\mathbb{F}_q$.

In more details, if $A(V)$ has full row rank mk over $\mathbb{F}_q$ (equivalently over $\mathbb{F}_{q^m}$), then

$$\rho = \dim_{\mathbb{F}_{q^m}} \ker A(V) = N_w - mk = m + (k+1)\ell_1 \ .$$

For an $\mathbb{F}_q$-basis $b_1, \ldots, b_\rho \in \mathbb{F}_q^{N_w}$ of $\ker_{\mathbb{F}_q} A(V)$, we set

$$K_t = \mathrm{mat}_{k+1,m+\ell_1}(b_t) \in \mathbb{F}_q^{(k+1)\times(m+\ell_1)} \quad \text{for } t = 1, \ldots, \rho.$$

Because the variables originally come from the bilinear products $w[j,s] = h[j]u[s]$, any element of $\ker_{\mathbb{F}_{q^m}} A(V)$ can then be written uniquely with extension-field coefficients as

$$W(\alpha) = \sum_{t=1}^{\rho} \alpha[t] K_t \ \text{ where } \alpha = (\alpha[1], \ldots, \alpha[\rho]) \in \mathbb{F}_{q^m}^{\rho}.$$

Recovering a valid pair (h,u) therefore reduces to finding a nonzero kernel vector of $A(V)$ whose reshaped matrix (via the reshaping map) has rank 1. Thus, we seek a nonzero $W(\alpha)$ such that

$$\mathrm{Rank}_{\mathbb{F}_{q^m}}(W(\alpha)) = 1. \tag{4}$$

The rank-1 condition (4) is equivalent to the vanishing of all 2×2 minors of $W(\alpha)$. The quadratic system generated from these 2×2 minors has

$$N_{\mathrm{eq}} = \tbinom{k+1}{2} \tbinom{m+\ell_1}{2}$$

homogeneous quadratic equations in the ρ coordinates $\alpha[1], \ldots, \alpha[\rho]$ over $\mathbb{F}_{q^m}$.

Remark 2. Any rank-1 kernel vector $W = hu^\top$ produces a candidate pair (h,u), but not every such candidate corresponds to a valid U because the recovered U may be rank-deficient. The rank-1 extraction is just a necessary condition that we follow with the full-rank check in Phase 4 to filter out spurious candidates.

Algorithm 1: Phase 2: construct the linearized kernel

Input: $M = m + \ell_1$, $N = n + \ell_2$, $(C_i)_{i=1}^{mk} \subset \mathbb{F}_q^{M \times N}$ and $V \in \mathbb{F}_q^{N \times (k+1)}$.
Output: $A(V)$ and matrices $K_1, \ldots, K_\rho \in F^{(k+1) \times M}$ whose vectorizations form a basis of $\ker_{\mathbb{F}_q} A(V)$.

$\mathsf{Mat} \leftarrow 0_{mk \times (k+1)M}$
for $i = 1, \ldots, mk$ **do**
  $D_i \leftarrow C_i V \in \mathbb{F}_q^{M \times (k+1)}$
  Set $\mathsf{Mat}[i, (j-1)M + s] \leftarrow D_i[s, j]$ for $1 \leq j \leq k+1$, $1 \leq s \leq M$
$(b_1, \ldots, b_\rho) \leftarrow$ a basis of $\ker_{\mathbb{F}_q} \mathsf{Mat}$
$K_t \leftarrow \mathrm{mat}_{k+1,M}(b_t)$ for $t = 1, \ldots, \rho$
return $(\mathsf{Mat}, (K_t)_{t=1}^{\rho})$

Phase 3: Rank-1 solution extraction. A naive approach is to compute the Gröbner basis of the homogeneous quadratic system. However, the computation is often expensive because it tries to produce a complete symbolic elimination description of the ideal, and for quadratic determinantal systems the intermediate degree and number of S-polynomial reductions can grow quickly. As the system at the end of Phase 2 has symmetries, which will be explained shortly, we use the eigenvalue method for solving zero-dimensional polynomial systems (see [7], Chapter 2, Section 4) which significantly accelerates the solving process[3].

The first observation is that the quadratic system generated from 2×2 minors is projective because if α is a solution, so is $\lambda\alpha$ for every $\lambda \in \mathbb{F}_{q^m}^{\times}$. For an index t_0 such that $\alpha[t_0] \neq 0$, we set $\alpha[t_0] = 1$. After this, we get an affine system, with $\rho - 1$ unknowns.

Let $\mathcal{M}$ be the degree-2 Macaulay matrix obtained from linearization of the quadratic system. Experimentally, we observed that *at degree* 2 *the* $\mathcal{M}$ *nullity dimension is already* m *and remains* m *at higher degrees* (see Appendix A). Thus, we propose the following conjecture whose supporting arguments will be provided in Section 6.

Conjecture 1. Let $I \subseteq \mathbb{F}_q[\alpha[1], \ldots, \alpha[\rho - 1]]$ be the ideal generated by the 2×2 minors, and let $A = \mathbb{F}_q[\alpha[1], \ldots, \alpha[\rho - 1]]/I$ then

$$\dim_{\mathbb{F}_q} A = m.$$

The second observation is that, firstly, the 2×2 minors have coefficients in $\mathbb{F}_q$ because the kernel basis matrices K_t have entries in $\mathbb{F}_q$; and secondly we only need one rank-1 point whose coordinates lie in $\mathbb{F}_{q^m}$. Therefore it is more natural to keep the expensive quotient computation over $\mathbb{F}_q$ and let the less expensive extraction of the desired $\mathbb{F}_{q^m}$-solution for the final eigenvector evaluation step.

[3] This method is sometimes called Stickelberger-Eigenvalue method. An interesting history of the method can be found in the note of David A. Cox in [6].

The third observation is that as $A(V)$ has entries in $\mathbb{F}_q$, it commutes with σ. Denote $\sigma(W)$ as the entrywise application of σ to W, then we have

$$A(V)\sigma(W) = \sigma(A(V)W).$$

In consequence, $\ker_{\mathbb{F}_{q^m}}(A(V))$ is Frobenius-stable. In other words, if

$$P = (p_1, \ldots, p_{\rho-1}) \in \mathbf{V}_{\mathbb{F}_{q^m}}(I),$$

then, for $0 \leq i < m$,

$$P^{[q^i]} := (p_1^{q^i}, \ldots, p_{\rho-1}^{q^i}) \in \mathbf{V}_{\mathbb{F}_{q^m}}(I).$$

Thus $P, P^{[q]}, \ldots, P^{[q^{m-1}]}$ are Frobenius-conjugate zeros of I. Under Conjecture 1, the quotient has degree m, exactly the size of the orbit. This structure enables us to compute Macaulay row reductions over the small field $\mathbb{F}_q$ avoiding the cost of linear algebra over $\mathbb{F}_{q^m}$.

The eigenvalue method for zero-dimensional ideals. First, we recall a well known result in commutative algebra:

Theorem 1 (Finiteness Theorem).
Given a field F and polynomials $f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$, the system

$$f_1 = \ldots = f_s = 0 \tag{5}$$

has finitely many solutions over the algebraic closure $\overline{F}$ of F if and only if

$$A = F[x_1, \ldots, x_n]/\langle f_1, \ldots, f_s \rangle$$

has finite dimension over F.

The proof can be found in the proof of Theorem 6, Chapter 5, Section 3 of [5].

Theorem 2 (Eigenvalue Theorem). *Let $f \in F[x_1, \ldots, x_n]$ be a polynomial with a multiplication map $M_f : A \longrightarrow A$. When $\dim_F A < \infty$, the eigenvalues of M_f are the values of f at the finitely many solutions of Equation (5) over $\overline{F}$.*

The proof can be found in the proof of Theorem 4.5, Chapter 2, Section 4 of [7].

This finiteness is essential for the eigenvalue method. Theorem 2 applies to multiplication maps in the quotient algebra

$$A = \mathbb{F}_q[\alpha[1], \ldots, \alpha[\rho-1]]/I,$$

and a finite multiplication matrix M_f exists only when this quotient has a finite $\mathbb{F}_q$-basis. By the Finiteness Theorem, this is equivalent to the normalized ideal I being zero-dimensional, or equivalently to the affine rank-1 equations having only finitely many solutions over $\overline{\mathbb{F}}_q$. If I had a positive-dimensional component, then A would be infinite-dimensional. In our application, this finiteness hypothesis is supplied by Conjecture 1.

Next, we build the multiplication matrix of A with a separating coordinate (for exact definition and properties, refer to Proposition 4.1, Section 4, Chapter 2, in [7]), i.e., compute the linear map:

$$\begin{aligned} M_{\alpha[s]} : A &\longrightarrow A \\ f &\longmapsto \alpha[s] f. \end{aligned}$$

Let $\mathcal{B} = (b_1, \ldots, b_m)$ be a basis of A. For an eigenvalue $\lambda \in \mathbb{F}_{q^m}$, an eigenvector of $M_{\alpha[s]}^{\mathsf{T}}$, normalized so that its entry corresponding to 1 is 1, gives $(b_1(P), b_2(P), \ldots, b_m(P))$. After normalization, this reconstructs $\alpha(P)$, hence the rank-1 matrix $W(\alpha)$. The cost of this eigenvalue extraction is polynomial.

Algorithms 2 and 3 summarize the two stages of Phase 3. Except for Step 18 of Algorithm 3 being done over $\mathbb{F}_{q^m}$, all operations take place over $\mathbb{F}_q$. This explains the advantage of the eigenvalue method in comparison with a naive Gröbner-basis computation over $\mathbb{F}_{q^m}$. The total cost of Phase 3 is dominated by the cost of computing the basis of A over $\mathbb{F}_q$ and is estimated as

$$\mathcal{O}\Big(\tbinom{\rho+1}{2}^{\omega}\Big) = \mathcal{O}\Big(\tbinom{m+(k+1)\ell_1+1}{2}^{\omega}\Big) \tag{6}$$

where ω is the linear algebra exponent.

Remark 3. In Algorithm 2, we can reduce the number of variables from $\rho - 1$ to $m - 1$ before applying the eigenvalues extraction. Recall that the Gaussian elimination on the degree-2 Macaulay matrix $\mathcal{M}$ produces a linear system of rank $(\rho-1)-(m-1)$ on the degree-1 variables α. Under Conjecture 1 the kernel of $\mathcal{M}$ has dimension exactly m, so the linearized system has a $d = (m-1)$-dimensional affine solution family

$$\alpha \;=\; \tilde{\alpha}_0 \;+\; \sum_{i=1}^{d} c[i]\,\tilde{\alpha}_i \quad \text{for } c = (c[1], \ldots, c[d]) \in \mathbb{F}_{q^m}^d,$$

where the vectors $\tilde{\alpha}_i \in \mathbb{F}_q^{\rho-1}$ are obtained from the row-reduced echelon form of $\mathcal{M}$ and hence have entries in $\mathbb{F}_q$. The residual quadratic system

$$J \subset \mathbb{F}_q[c[1], \ldots, c[d]]$$

is generated by quadratic polynomials in $c[1], \ldots, c[d]$ whose coefficients lie in $\mathbb{F}_q$. For the correct V the zero-set $\mathbf{V}_{\mathbb{F}_q}(J')$ is finite of cardinality $\dim_{\mathbb{F}_q} A = m$, where $A = \mathbb{F}_q[c[1], \ldots, c[d]]/J'$ is the affine coordinate ring. This count matches the kernel nullity observed experimentally in Appendix A.

Algorithm 2: RankOne

Input: Kernel basis matrices $K_1, \ldots, K_\rho$.
Output: (α, W) with $W = \sum_t \alpha[t]K_t$, $\mathrm{Rank}_{\mathbb{F}_{q^m}} W = 1$, or $\perp$.

for $t_0 = 1, \ldots, \rho$ **do**
  // Normalize.
  $\alpha[t_0] \leftarrow 1$
  $\mathcal{M} \leftarrow \mathsf{Mac}_2(\sum_t \alpha[t]K_t)$// Build the degree-2 Macaulay matrix.
  $\mathcal{T} \leftarrow \mathsf{EigenvaluesSolve}(\mathcal{M})$
  // Verify and return an accepted candidate.
  foreach $x \in \mathcal{T}$ **do**
    Reconstruct α by inserting $\alpha[t_0] = 1$ into x
    if $\mathrm{Rank}_{\mathbb{F}_{q^m}} W = 1$ **then return** (α, W)
return $\perp$

Algorithm 3: EigenvaluesSolve

Input: A degree-2 Macaulay matrix $\mathcal{M}$.
Output: A list of vectors, or $\varnothing$.
// Compute the quotient basis.
Split $\mathcal{M} = [A \mid B]$, where columns of A correspond to the constant and degree-1 monomials, and columns of B correspond to the degree-2 monomials
Row-reduce B to get $\widetilde{B}$; applying the same row operations to A to get $\widetilde{A}$
$\mathcal{M} \leftarrow [\widetilde{A} \mid \widetilde{B}]$
Split $\widetilde{B}$ into $\widetilde{B}_0$, containing its zero rows, and $\widetilde{B}_1$, containing its nonzero rows
Let L_1, L_2 be the rows of $\widetilde{A}$ corresponding to $\widetilde{B}_0, \widetilde{B}_1$, respectively
$L_1 \leftarrow [c \mid D]$ where c is the first column of L_1, containing the constant terms; D its remaining $\rho - 1$ columns, containing the coefficients of $\alpha[t]_{t \neq t_0}$, in increasing index order
Compute x in $Dx = -c$
Compute y in $\widetilde{B}_1 y = -L_2 \begin{pmatrix} 1 \\ x \end{pmatrix}$
$\mathcal{B} \leftarrow \{1\}$
foreach *monomial* b *in* x *or* y **do**
  if b *is linearly independent of* $\mathcal{B}$ **then** append b to $\mathcal{B}$
$\delta \leftarrow |\mathcal{B}|$ // From Conjecture 1, we expect $\delta = m$.
if *no such basis is determined at degree* 2*, or* $\delta = 0$ **then return** $\varnothing$
// Compute the eigenvalues.
Write each entry of x as a linear combination of $\mathcal{B} = (1, b_2, \ldots, b_\delta)$, and store its coefficients in the corresponding row of C, so that $x = C(1, b_2, \ldots, b_\delta)^\mathsf{T}$
Choose an entry $x[s]$ of x
foreach *monomial* b_j *in* $\mathcal{B}$*, with* $b_1 = 1$ **do**
  Write $x[s]b_j$ as a linear combination of $\mathcal{B}$, and store its coefficients in column j of $T \in \mathbb{F}_q^{\delta \times \delta}$
Compute the eigenvalues $\lambda \in \mathbb{F}_{q^m}$ of T^T and corresponding eigenvectors v
// Recover coordinate vectors x.
$\mathcal{T} \leftarrow [\,]$
foreach *computed eigenvector* v *with* $v[1] \neq 0$ **do**
  $v \leftarrow v/v[1]$// Make the constant entry 1.
  $x^\star \leftarrow Cv$// Recover the original coordinates.
  Append $x^\star$ to $\mathcal{T}$
return $\mathcal{T}$

Phase 4: Factorization and reconstruction. Once a rank-1 matrix W is found, we resconstruct the row compression matrix U using Algorithm 4. The distinguisher succeeds if the algorithm recovers a *full-rank* matrix U.

Remark 4. Given a successful rank-1 extraction from Phase 3, the probability of U begin full-rank is overwhelmingly high (Step 5 in Algorithm 4). This probability is analyzed in Section 6.

Algorithm 4: Phase 4: reconstruct and verify U

Input: $(C_i)_{i=1}^{mk}$, V, a rank-1 matrix $W \in \mathbb{F}_{q^m}^{n' \times M}$, Ψ.
Output: U, or $\perp$.
1 Choose (j_0, s_0) with $W[j_0, s_0] \neq 0$
2 $u[s] \leftarrow W[j_0, s]$ for $s = 1, \ldots, M$
3 $h[j] \leftarrow W[j, s_0]/u[s_0]$ for $j = 1, \ldots, n'$ // $W = hu^{\mathsf{T}}$
4 $U \leftarrow [\Psi(u[1]) \mid \cdots \mid \Psi(u[M])] \in F^{m \times M}$
5 **if** $\mathrm{Rank}_F U < m$ **then return** $\perp$
6 **return** U

3.2 Guess-U-solve-V direction

The same idea can be run in the opposite direction. One may guess the row compression U and solve algebraically for a full column compression $V \in \mathbb{F}_q^{N \times m}$. For simplicity, and as in the concrete EGMC parameter sets considered below, we specialize this direction to $n = m$, so $N = m + \ell_2$.

Phase 1: Guessing U. Here, the probability of guessing the correct U is

$$\frac{|\mathrm{Gr}(m, m)|}{|\mathrm{Gr}(m, m + \ell_1)|} \approx q^{-m\ell_1}.$$

Phase 2: Algebraic modelling. Given a valid guess $U \in \mathbb{F}_q^{m \times (m+\ell_1)}$, let $C_1, \ldots, C_{mk}$ be an $\mathbb{F}_q$-basis of the public code $\mathcal{C}$. For each public basis matrix set $E_i = UC_i = (E_i[a, r]) \in \mathbb{F}_q^{m \times N}$. We want to find a full-rank column compression

$$V = \begin{bmatrix} v_1 \\ \vdots \\ v_N \end{bmatrix} \in \mathbb{F}_q^{N \times m} \text{ where } v_1, \ldots, v_N \in \mathbb{F}_q^m,$$

such that the compressed code UC_iV is annihilated by a full parity-check matrix of the hidden $[m, k]$ Gabidulin code. As in the previous direction, we write the unknown rows of V into extension field coordinates:

$$y[r] = \Psi^{-1}(v_r) \in \mathbb{F}_{q^m} \quad \forall r = 1, \ldots, N.$$

Fix a row-wise extension of Ψ, let $\mathrm{row}_{\mathbb{F}_{q^m}}$ denote the inverse row expansion on m rows:

$$\mathrm{row}_{\mathbb{F}_{q^m}} = (\Psi^{-1})^{\oplus m} : \mathbb{F}_q^{m\times m} \longrightarrow \mathbb{F}_{q^m}^m$$
$$\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} \longmapsto \big(\Psi^{-1}(x_1), \ldots, \Psi^{-1}(x_m)\big).$$

Since $E_i[a,r] \in \mathbb{F}_q$, we have

$$\big(\mathrm{row}_{\mathbb{F}_{q^m}}(E_i V)\big)_a = \sum_{r=1}^{N} E_i[a,r]\, y[r].$$

Let $s = m-k$, and let $H \in \mathbb{F}_{q^m}^{s\times m}$ be a parity-check matrix. Since left multiplication by any matrix in $\mathrm{GL}_s(\mathbb{F}_{q^m})$ gives the same parity-check space, we normalize $H = [I_s \mid B]$ where $B = (B[b,a]) \in \mathbb{F}_{q^m}^{s\times k}$. The parity-check condition is

$$\begin{aligned} & H\,\mathrm{row}_{\mathbb{F}_{q^m}}(E_i V)^{\mathsf{T}} = 0, \quad \forall i = 1,\ldots,mk \\ \Longrightarrow & \sum_{r=1}^{N} E_i[b,r]\, y[r] + \sum_{a=1}^{k}\sum_{r=1}^{N} E_i[s+a,r]\, B[b,a]\, y[r] = 0 \end{aligned} \tag{7}$$

for $1 \le i \le mk$ and $1 \le b \le s$. Let us denote $x[b,a,r] = B[b,a]\, y[r]$ for $1 \le b \le s, 1 \le a \le k, 1 \le r \le N$. Then (7) becomes the linear system

$$\sum_{r=1}^{N} E_i[b,r]\, y[r] + \sum_{a=1}^{k}\sum_{r=1}^{N} E_i[s+a,r]\, x[b,a,r] = 0 \quad \forall i = 1,\ldots,mk,\ b = 1,\ldots,s. \tag{8}$$

All coefficients lie in $\mathbb{F}_q$, so its solution space over $\mathbb{F}_{q^m}$ is the scalar extension of its kernel over $\mathbb{F}_q$. Hence, we are back to the problem of finding a rank-1 element in the kernel of dimension

$$\rho_H = m + \ell_2\big(1 + k(m-k)\big).$$

Phase 3: Rank-1 solution extraction. We therefore compute a basis $b_1, ..., b_{\rho_H}$ of the $\mathbb{F}_q$-kernel of (8), set $K_t = \mathrm{mat}_{1+sk,N}(b_t) \in \mathbb{F}_q^{(1+sk)\times N}$, and set to zero all the 2×2 minors of

$$Z(\alpha) = \sum_{t=1}^{\rho_H} \alpha[t] K_t.$$

After one projective normalization, the residual quotient is also conjectured to be zero-dimensional with supporting experimental evidence given in Appendix B, so the same eigenvalue method as in the guess-V-solve-U direction applies. The rank-1 extraction here uses a Macaulay matrix with $\binom{\rho_H+1}{2}$ columns after pro-

jective normalization, hence cost

$$\mathcal{O}\left(\binom{\rho_H+1}{2}^{\omega}\right)$$

over $\mathbb{F}_q$ where ω is the linear algebra exponent.

Phase 4: Factorization and reconstruction. Once a rank-1 point Z is found, the first row is $y = (y[1], \ldots, y[N])$. The candidate column compression is recovered by

$$V = \begin{bmatrix} \Psi(y[1])^{\mathsf{T}} \\ \vdots \\ \Psi(y[N])^{\mathsf{T}} \end{bmatrix} \in \mathbb{F}_q^{N\times m}.$$

If $y[r_0] \neq 0$, the entries of the normalized parity-check matrix are recovered from $B[b,a] = x[b,a,r_0]/y[r_0]$. The candidate is accepted only if V has rank m over $\mathbb{F}_q$.

4 Recovering the equivalent secret keys

When the distinguisher succeeds, we are given a matrix code $\mathcal{B}_0 = U_0\mathcal{C}V_0$ where $\mathcal{C}$ is the public EGMC code, $U_0 \in \mathbb{F}_q^{m\times(m+\ell_1)}$ and $V_0 \in \mathbb{F}_q^{(n+\ell_2)\times n'}$ are full-rank matrices. In the guess-U-solve-V direction, we have $n' = n = m$, thus $\mathcal{B}_0$ is equivalent to the matrix representation of an $[n,k]$ Gabidulin code over $\mathbb{F}_{q^m}$. Nevetheless, in the guess-V-solve-U direction, $n' = k+1 < n$, thus $\mathcal{B}_0$ is equivalent to the matrix representation of just a $[k+1,k]$ Gabidulin code over $\mathbb{F}_{q^m}$. This is a punctured code of the $[n,k]$ Gabidulin code over $\mathbb{F}_{q^m}$. Our goal now is to extend this short punctured Gabidulin code into a full equivalent $[n,k]$ Gabidulin description of the row-compressed public code. This section therefore applies to only the guess-V-solve-U direction.

It should be noted that a punctured generalized Reed-Solomons code can be extended by 1 digit while keeping the MDS property [13]. In an EGMC instance, the structure of the punctured Gabidulin code, together with the full row-compressed public code, instead lets us recover the hidden clean column space and thereby return to length n. Indeed, the punctured code reveals the hidden copy of $\mathbb{F}_{q^m}$ acting on the rows and hence the Frobenius map in the recovered coordinates. As a result, we can recover the equivalent secret keys after two steps. First, in Section 4.1, we reconstruct the punctured $[k+1,k]$ Gabidulin code in standard generator-matrix form. Finally, as the generator-matrix of Gabidulin codes is special, Section 4.2 shows an algorithm to extend the $[k+1,k]$ Gabidulin code back to the full $[n,k]$ Gabidulin code. The whole process is entirely polynomial-time linear algebra over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$.

4.1 Reconstruct the $[k+1, k]$ Gabidulin code over $\mathbb{F}_{q^m}$ in its standard form

Assume that we are given $\mathcal{B}_0 = U_0 \mathcal{C} V_0 \subseteq \mathcal{M}_{m\times(k+1)}(\mathbb{F}_q)$ of $\mathbb{F}_q$-dimension mk, and that $\mathcal{B}_0$ is equivalent to the matrix representation of a $[k+1, k]$ Gabidulin code over $\mathbb{F}_{q^m}$. Using the `BasisRecover` Algorithm from [12], we can find in polynomial time a basis γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and an evaluation vector $\mathbf{g}' = ({g'}_1, \ldots, {g'}_{k+1}) \in \mathbb{F}_{q^m}^{k+1}$ with $\mathbb{F}_q$-linearly independent coordinates such that $\mathcal{B}_0 = \Psi_\gamma\big(\mathcal{G}_k(\mathbf{g}')\big)$. We modified the `BasisRecover` algorithm so that it also returns the standard generator matrix in Moore form (see Definition 7, [2]) of the $[k+1, k]$ Gabidulin code, which will be used in the next step to extent the code to its full length.

$$M_{k+1,k}(\boldsymbol{g}') = \begin{bmatrix} {g'}_1 & {g'}_2 & \cdots & {g'}_{k+1} \\ {g'}_1^q & {g'}_2^q & \cdots & {g'}_{k+1}^q \\ \vdots & \vdots & \ddots & \vdots \\ {g'}_1^{q^{k-1}} & {g'}_2^{q^{k-1}} & \cdots & {g'}_{k+1}^{q^{k-1}} \end{bmatrix}.$$

Algorithm 5: `BasisRecover` [12]

Input: An $\mathbb{F}_q$-basis $B_1, \ldots, B_{mk}$ of $\mathcal{B}_0 \subseteq \mathbb{F}_q^{m\times(k+1)}$.
Output: γ, Φ_γ, $\mathbf{g}'$, and $M_k(\mathbf{g}')$, or $\perp$.

$\mathcal{L} \leftarrow \mathrm{Stab}(\mathcal{B}_0) = \{T \in \mathbb{F}_q^{m\times m} : T\mathcal{B}_0 \subseteq \mathcal{B}_0\}$
if $\dim_{\mathbb{F}_q} \mathcal{L} \neq m$ **then return** $\perp$
sample $T \in \mathcal{S}$ until its minimal polynomial $f_T(X) \in \mathbb{F}_q[X]$ has degree m, using at most $\left(1 - 2q^{\frac{-m}{2}} + 2q^{-m}\right)^{-1} \leq 2$ trials
if *no such T is found, or f_T is reducible* **then return** $\perp$
choose $0 \neq w \in \mathbb{F}_q^m$ and set $R_T \leftarrow [\, w \mid Tw \mid \cdots \mid T^{m-1}w \,] \in \mathrm{GL}_m(\mathbb{F}_q)$
find a root $\vartheta \in \mathbb{F}_{q^m}$ of f_T
$\gamma \leftarrow \left(1, \vartheta, \vartheta^2, \ldots, \vartheta^{m-1}\right) R_T^{-1} \in \mathbb{F}_{q^m}^m$
$\mathcal{C}_\gamma \leftarrow \Psi_\gamma^{-1}(\mathcal{B}_0) \subseteq \mathbb{F}_{q^m}^{k+1}$
apply the standard Overbeck algorithm to $\mathcal{C}_\gamma$ and obtain a vector $\mathbf{g}' \in \mathbb{F}_{q^m}^{k+1}$ with $\mathbb{F}_q$-linearly independent coordinates
$M_{k+1,k}(\mathbf{g}') \leftarrow [\, \mathbf{g}'; (\mathbf{g}')^{[q]}; \ldots; (\mathbf{g}')^{[q^{k-1}]} \,]$
return $(\gamma, \mathbf{g}', M_{k+1,k}(\mathbf{g}'))$

4.2 Extending the punctured code to a full length-n Gabidulin code

Let $\mathcal{D} = U_0 \mathcal{C} \subseteq \mathbb{F}_q^{m\times(n+\ell_2)}$ be the row-compressed public code. From previous step, we have:

$$\Psi_\gamma^{-1}(\mathcal{D}) V_0 = \mathcal{G}_k(\mathbf{g}') \subseteq \mathbb{F}_{q^m}^{k+1}.$$

Next, we define the puncture map

$$\pi : \Psi_\gamma^{-1}(\mathcal{D}) \longrightarrow \mathcal{G}_k(\mathbf{g}')$$

$$b \longmapsto bV_0 \ .$$

We have $\dim_{\mathbb{F}_q} \Psi_\gamma^{-1}(\mathcal{D})$ is at most mk over $\mathbb{F}_q$ because it is a linear image of the public code $\mathcal{C}$. The punctured Gabidulin code $\mathcal{G}_k(\mathbf{g}')$ also has dimension mk over $\mathbb{F}_q$. Since π is surjective, it is an $\mathbb{F}_q$-linear isomorphism. Thus, we can compute $b_0, ..., b_{k-1} \in \Psi_\gamma^{-1}(\mathcal{D}) \subset \mathbb{F}_{q^m}^{n+\ell_2}$ uniquely such that

$$b_i V_0 = (\mathbf{g}')^{[q^i]}, \tag{9}$$

then we seek a full-rank matrix $V \in \mathbb{F}_q^{(n+\ell_2)\times n}$ and a vector $\mathbf{g} \in \mathbb{F}_{q^m}^n$ of $\mathbb{F}_q$-rank n satisfying such that:

$$b_i V = (\mathbf{g})^{[q^i]}, \tag{10}$$

Recall that the construction of EGMC and the assumption that U_0 has been correctly guessed ensure the existence of a solution V having the form

$$V = Q^{-1} \begin{bmatrix} * \\ 0 \end{bmatrix} \text{ where } Q \in \mathrm{GL}_{n+\ell_2}(\mathbb{F}_q) \text{ and}$$

$$\begin{bmatrix} b_0 \\ \vdots \\ b_{k-1} \end{bmatrix} Q^{-1} = \left[M_{n,k}(\mathbf{g}) \mid \Delta \right] \text{ where } \Delta \text{ is a random matrix in } \mathbb{F}_{q^m}^{k\times \ell_2}.$$

Note that for any vectors $x \in \mathbb{F}_q^{n+\ell_2}$, we have

$$\langle b_0, x \rangle^{q^i} = \langle b_0^{[q^i]}, x \rangle.$$

Thus, for δ_i being rows of Δ, writing b_i in $\mathbb{F}_q$ basis via Ψ_γ gives us:

$$\begin{bmatrix} \Psi_\gamma(b_1 - b_0^{[q]}) \\ \vdots \\ \Psi_\gamma(b_{k-1} - b_0^{[q^{k-1}]}) \end{bmatrix} Q^{-1} = \left[\begin{array}{c|c} 0 & \begin{matrix} \Psi_\gamma(\delta_1 - \delta_0^{[q]}) \\ \vdots \\ \Psi_\gamma(\delta_{k-1} - \delta_0^{[q^{k-1}]}) \end{matrix} \end{array} \right] = \left[0 | \widetilde{\Delta} \right].$$

For $m(k-1) > \ell_2$, with high probablity, $\widetilde{\Delta}$ is full-rank ℓ_2 over $\mathbb{F}_q$, thus

$$\mathrm{Rank} \begin{bmatrix} \Psi_\gamma(b_1 - b_0^{[q]}) \\ \vdots \\ \Psi_\gamma(b_{k-1} - b_0^{[q^{k-1}]}) \end{bmatrix} = \ell_2.$$

Combining with Equation (10), the column space of V is

$$\mathcal{L} = \left\{ v \in \mathbb{F}_q^{n+\ell_2} : \langle b_i - b_0^{[q^i]}, v \rangle = 0 \text{ for } i = 1, \ldots, k-1 \right\},$$

and its dimension is n. Compute any $\mathbb{F}_q$-basis $v_1, \dots, v_n$ of $\mathcal{L}$, and setting

$$V = [\, v_1 \mid \cdots \mid v_n \,] \in \mathbb{F}_q^{N \times n}$$
$$\mathbf{g} = \big(\langle b_0, v_1 \rangle, \dots, \langle b_0, v_n \rangle\big) \in \mathbb{F}_{q^m}^n.$$

gives us the final solutions.

Algorithm 6 summarizes the extension procedure. The cost of the algorithm is polynomial-time linear algebra over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$.

Algorithm 6: `ExtendSupport`: extension to a full Gabidulin code

Input: A code $\mathcal{C} \subseteq \mathbb{F}_q^{(m+\ell_1)\times(n+\ell_2)}$; full-rank matrices $U_0 \in \mathbb{F}_q^{m\times(m+\ell_1)}$ and $V_0 \in \mathbb{F}_q^{(n+\ell_2)\times(k+1)}$; and $\gamma, \mathbf{g}'$ satisfying $U_0 \mathcal{C} V_0 = \Psi_\gamma(\mathcal{G}_k(\mathbf{g}'))$.

Output: A full-rank $V \in \mathbb{F}_q^{(n+\ell_2)\times n}$ and an evaluation vector $\mathbf{g} \in \mathbb{F}_{q^m}^n$ of $\mathbb{F}_q$-rank n, or $\perp$.

$N \leftarrow n + \ell_2$ and $d_s \leftarrow \Psi_\gamma^{-1}(U_0 C_s) \in \mathbb{F}_{q^m}^N$ for $1 \le s \le mk$
$\widetilde{\mathcal{D}} \leftarrow \mathrm{Span}_{\mathbb{F}_q}\{d_1, \dots, d_{mk}\}$
$\mathcal{A} \leftarrow \mathrm{Span}_{\mathbb{F}_q}\{d_1 V_0, \dots, d_{mk} V_0\}$
if $\dim_{\mathbb{F}_q} \mathcal{A} \neq mk$ **then return** $\perp$
for $i = 0, \dots, k-1$ **do**
  solve for $b_i \in \widetilde{\mathcal{D}} \subset \mathbb{F}_{q^m}^N$ the system $b_i V_0 = (\mathbf{g}')^{[q^i]}$;
$\mathcal{L} \leftarrow \ker_{\mathbb{F}_q}[\, \Psi_\gamma(b_1 - b_0^{[q]})^\mathsf{T} \mid \cdots \mid \Psi_\gamma(b_{k-1} - b_0^{[q^{k-1}]})^\mathsf{T} \,]^\mathsf{T}$
if $\dim_{\mathbb{F}_q} \mathcal{L} \neq n$ **then return** $\perp$
choose an $\mathbb{F}_q$-basis $v_1, \dots, v_n$ of $\mathcal{L}$ and set $V \leftarrow [\, v_1 \mid \cdots \mid v_n \,]$
for $j = 1, \dots, n$ **do**
  $g_j \leftarrow \langle b_0, v_j \rangle$
$\mathbf{g} \leftarrow (g_1, \dots, g_n)$
if $\mathrm{Rank}_{\mathbb{F}_q}(\mathbf{g}) \neq n$ **then return** $\perp$
if $\widetilde{\mathcal{D}} V \neq \mathcal{G}_k(\mathbf{g})$ *as $\mathbb{F}_q$-linear spaces* **then return** $\perp$
return $(V, \mathbf{g})$

5 Applications to EGMC-McElice and EGMC-Niederreiter

Here, using the recovered equivalent trapdoor, we explain polynomial-time decryption algorithms for the EGMC-McEliece/Niederreiter schemes.

5.1 Breaking the EGMC-McEliece scheme

Let $\mathrm{pk} = (M_1, \dots, M_{km})$ be a basis of the public matrix code $\mathcal{C}'_{\mathrm{mat}}$, and let a ciphertext be $Y = \sum_{i=1}^{km} \mu_i M_i + E$ where $\mathrm{Rank}(E) \le r$. Applying the recovered U, V yields

$$UYV = \sum_{i=1}^{km} \mu_i (U M_i V) + UEV.$$

Note that $\mathrm{Rank}(UEV) \le \mathrm{Rank}(E) \le r$ and since $M_i \in \mathcal{C}'_{\mathrm{mat}}$, each UM_iV belongs to $U\,\mathcal{C}'_{\mathrm{mat}}\,V = \Psi_\gamma\big(\mathcal{G}_k(\boldsymbol{g})\big)$, hence

$$UYV \in \Psi_\gamma\big(\mathcal{G}_k(\boldsymbol{g})\big) + \{Z : \mathrm{Rank}(Z) \le r\}.$$

Therefore, provided r is within the decoding radius of the recovered Gabidulin code, one can decode UYV and recover the unique codeword $C^\star = \sum_{i=1}^{km} \mu_i(UM_iV) \in \Psi_\gamma\big(\mathcal{G}_k(\boldsymbol{g})\big)$. It remains to recover the message μ. Since

$$C^\star = \sum_{i=1}^{km} \mu_i(UM_iV),$$

and the matrices UM_iV are known, μ is obtained by solving the linear system above over $\mathbb{F}_q$. The solution is unique because $\dim_{\mathbb{F}_q}\big(U\,\mathcal{C}'_{\mathrm{mat}}\,V\big) = mk$.

5.2 Breaking the EGMC-Niederreiter scheme

Let $\bar{H}$ be a parity-check matrix of the public matrix code $\mathcal{C}'_{\mathrm{mat}}$. In the Niederreiter variant, the ciphertext is a syndrome $c = \bar{H}\,\bar{e}^{\,t}$, where $\bar{e} = \mathrm{Unfold}(E)$ for some matrix $E \in \mathbb{F}_q^{(m+\ell_1)\times(n+\ell_2)}$ where $\mathrm{Rank}(E) \le r$. From the public syndrome c, first compute any vector $\bar{y} \in \mathbb{F}_q^{(m+\ell_1)(n+\ell_2)}$ such that $\bar{H}\,\bar{y}^{\top} = c$, and let $Y = \mathrm{Fold}(\bar{y})$. Then Y belongs to the affine space $Y \in E + \mathcal{C}'_{\mathrm{mat}}$, so there exists some $C \in \mathcal{C}'_{\mathrm{mat}}$ such that $Y = C + E$. Applying the recovered U, V yields

$$UYV = UCV + UEV,$$

where $UCV \in \Psi_\gamma(\mathcal{G}_k(\boldsymbol{g}))$ and $\mathrm{Rank}(UEV) \le r$. Therefore, Gabidulin decoding recovers the projected error $E^\star = UEV$.

To reconstruct the full error E, observe that E must satisfy both:

$$UEV = E^\star \quad \text{and} \quad \bar{H}\,\mathrm{Unfold}(E)^{\top} = c.$$

This is a linear system in the entries of E over $\mathbb{F}_q$. Solving it recovers E, and hence the plaintext $\mu = \mathrm{Unfold}(E)$.

6 Arguments for Conjecture 1

This section gives supporting arguments for Conjecture 1 in the guess-V-solve-U direction; the guess-U-solve-V direction can be argued analogously. First, in Proposition 2 we will prove that

$$\dim_{\mathbb{F}_q} A \ge m.$$

This also explains why the points in this hidden orbit pass the full-rank check in Phase 4. Second, in Proposition 3 we will prove that

$$\Pr[\dim_{\mathbb{F}_q} A > m] \le q^{(1-k)(m-1)+\ell_1}.$$

6.1 Full-rank preservation from Frobenius orbits

We recall necessary background to prove that

$$\dim_{\mathbb{F}_q} A \geq m.$$

Firstly, recall that $I \subseteq \mathbb{F}_q[\alpha[1], \ldots, \alpha[\rho-1]]$ is the ideal generated by the 2×2 minors of $W(\alpha) = \sum_t \alpha[t] K_t$. For $P = (p_1, \ldots, p_{\rho-1}) \in \mathbf{V}_{\mathbb{F}_{q^m}}(I)$, $W(P)$ is a rank-1 element of $A(V)$. We denote $[W(P)]$ as its class modulo multiplication by $\mathbb{F}_{q^m}^{\times}$. The projective rank-1 solution set is denoted as

$$\mathcal{S}(V) = \Big\{ [W(P)] : P \in \mathbf{V}_{\mathbb{F}_{q^m}}(I) \Big\}.$$

Recall that the whole $\ker_{\mathbb{F}_{q^m}}(A(V))$ is Frobenius-stable so does $\mathcal{S}(V)$. We therefore decompose it into disjoint Frobenius orbits:

$$\mathcal{S}(V) = \bigcup_{\nu \in T} \mathcal{O}_\nu, \tag{11}$$

where

$$\mathcal{O}_\nu = \{[W(P_\nu)], [W(P_\nu^{[q]})], \ldots, [W(P_\nu^{[q^{d_\nu - 1}]})]\}.$$

Here P_ν is a representative of the orbit and d_ν is the smallest positive integer such that $[W(P_\nu^{[q^{d_\nu}]})] = [W(P_\nu)]$. We introduce two following lemmas to explain how the orbit size controls the rank of the reconstructed matrix U.

Lemma 1. *Let $W = hu^{\mathsf{T}}$ be a rank-1 matrix over $\mathbb{F}_{q^m}$. Assume that $[\sigma^d(W)] = [W]$ for some $d > 0$ and $g = \gcd(d, m)$. If $u[s_0] \neq 0$, then, for every s,*

$$\frac{u[s]}{u[s_0]} \in \mathbb{F}_{q^g}.$$

In particular, if d is the Frobenius orbit size of $[W]$, then $d \mid m$.

Proof. The equality $[\sigma^d(W)] = [W]$ means that $\sigma^d(W) = \lambda W$ for some $\lambda \in \mathbb{F}_{q^m}^{\times}$. Since W has rank 1, its row space is the line generated by u^{T}; therefore $\sigma^d(u)$ is proportional to u. Hence, for every s,

$$\sigma^d\left(\frac{u[s]}{u[s_0]}\right) = \frac{u[s]}{u[s_0]}.$$

The fixed field of σ^d inside $\mathbb{F}_{q^m}$ is $\mathbb{F}_{q^g}$, with $g = \gcd(d, m)$, proving the first claim. Then because the Frobenius group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \sigma \rangle$ is cyclic of order m, we have $d \mid m$.

Lemma 2. *Let $u = (u[1], \ldots, u[b]) \in \mathbb{F}_{q^m}^b$ and $U(u)$ its matrix form over $\mathbb{F}_q$. If there exist $d \mid m$ such that $u[s] \in \mathbb{F}_{q^d}$ for every s, then $\mathrm{Rank}_{\mathbb{F}_q}(U(u)) \leq d$.*

Proof. The subfield $\mathbb{F}_{q^d}$ is a d-dimensional $\mathbb{F}_q$-vector space, hence every column of $U(u)$ lies in the d-dimensional subspace $\Psi(\mathbb{F}_{q^d}) \subseteq \mathbb{F}_q^m$. Therefore

$$\mathrm{Rank}_{\mathbb{F}_q}(U(u)) \leq d.$$

The next proposition shows that, for a valid guess of V, the set $\mathcal{S}(V)$ always contains the hidden Frobenius orbit and that this orbit has the expected size m.

Proposition 2. *For any valid guess of V,*

$$\dim_{\mathbb{F}_q} A \geq m.$$

Moreover, the rank-1 points in the hidden Frobenius orbit all reconstruct a full-rank row compression in Phase 4.

Proof. Let $W^* = h^*(u^*)^\mathsf{T}$ be the rank-1 kernel matrix obtained from the hidden row compression U^*. Since $\ker_{\mathbb{F}_{q^m}}(A(V))$ is Frobenius-stable, for every $i = 0, \ldots, m-1$,

$$[\sigma^i(W^*)] \in \mathcal{S}(V).$$

We first prove that these m projective points are distinct. Suppose, to the contrary, that $[\sigma^d(W^*)] = [W^*]$ for some $0 < d < m$. Choose s_0 with $u^*[s_0] \neq 0$, and set $g = \gcd(d, m)$. By Lemma 1, we have $u^* \in \mathbb{F}_{q^g}$. Since $g < m$, Lemma 2 gives $\mathrm{Rank}_{\mathbb{F}_q} U^* \leq g < m$. This contradicts the fact that

$$\mathrm{Rank}_{\mathbb{F}_q} U^* = \dim_{\mathbb{F}_q} \mathrm{Span}_{\mathbb{F}_q}\{u^*[1], \ldots, u^*[m + \ell_1]\} = m.$$

Therefore the hidden Frobenius orbit has size exactly m. After normalization, the same orbit gives m distinct zeros of the ideal I over $\mathbb{F}_{q^m}$ hence $\dim_{\mathbb{F}_q} A \geq m$. Finally, any point in this orbit has the form

$$\lambda\, \sigma^i(W^*) = (\lambda\, \sigma^i(h^*))\, \sigma^i(u^*)^\mathsf{T}$$

for some $\lambda \in \mathbb{F}_{q^m}^\times$. Frobenius and multiplication by a nonzero scalar are $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$, so they preserve the $\mathbb{F}_q$-span dimension of the entries of u^*. Thus every rank-1 point in the hidden orbit reconstructs a matrix $U(u)$ of rank m in Phase 4.

6.2 The probability of unwanted solutions

Here, we prove the following proposition:

Proposition 3. *Assume that m is prime, under the random-subspace model described below,*

$$\Pr\big[\dim_{\mathbb{F}_q} A > m\big] \;\leq\; q^{(1-k)(m-1)+\ell_1}.$$

For the concrete parameter sets the exponent is dominated by $-(k-1)(m-1)$, so this bound is negligible.

Proof. From Lemmas 1 and 2, any solution whose u-coordinates are projectively defined over a proper subfield can only give a rank-deficient compression. Thus a full-rank recovered $U(u)$ can only come from a solution whose coordinates generate the full $\mathbb{F}_q$-space $\mathbb{F}_{q^m}$. We consider two cases:

1. If we assume that m is prime, which is true for concrete parameters. Obviously, the only divisors of m are 1 and m. Therefore every orbit in Equation (11) has size either 1 or m. Furthermore, size-m orbits correspond to solutions not defined over any proper subfield ("generic"), while size-1 orbits correspond to solutions defined over $\mathbb{F}_q$ (projectively Frobenius-fixed). By Lemma 2, size-1 orbits satisfy $\mathrm{Rank}_{\mathbb{F}_q}(U(u)) \leq 1$, hence (except the trivial all-zero u which cannot happen for rank-1 W) typically $\mathrm{Rank}_{\mathbb{F}_q}(U(u)) = 1$. Thus, for prime m, orbit-size-1 solutions are the main systematic source of rank-deficient outputs; the hidden size-m orbit is full rank by Proposition 2.
2. If we assume that m is composite, although it is not the case with the concrete parameters. Then, orbit sizes can be any divisor $d \mid m$. In that case, orbit size d typically yields $\mathrm{Rank}_{\mathbb{F}_q}(U) \leq d$ by Lemma 2. In particular, size-1 orbits correspond to $\mathbb{F}_q$-defined solutions and often yield $\mathrm{Rank}_{\mathbb{F}_q}(U) = 1$, size-$d$ orbits (proper divisors $1 < d < m$) correspond to $\mathbb{F}_{q^d}$-defined solutions and often yield $\mathrm{Rank}_{\mathbb{F}_q}(U) = d$, and size-$m$ orbits correspond to "full field" solutions and allow $\mathrm{Rank}_{\mathbb{F}_q}(U) = m$.

Now we consider the following question: *For random EGMC public code, random V from Phase 1, if one selects a rank-1 solution* $[W]$ uniformly at random *from $\mathcal{S}(V)$, then what is the*

$$\Pr(\mathrm{Rank}_{\mathbb{F}_q}(U) < m \mid V) = \frac{\#\{[W] \in \mathcal{S}(V) : \mathrm{Rank}_{\mathbb{F}_q}(U(W)) < m\}}{\#\mathcal{S}(V)} \ ?$$

Firstly, from Equation (11) and the fact that m is prime for concrete parameters, the total number of projective rank-1 solutions admits the decomposition

$$\#\mathcal{S}(V) = m \cdot a_m(V) + a_1(V),$$

where $a_m(V)$ counts size-m orbits and $a_1(V)$ counts size-1 orbits. We denote $a = k + 1$ and $b = m + \ell_1$ and

$$L(V) = \{\, W \in \mathcal{M}_{a\times b}(\mathbb{F}_{q^m}) : \mathrm{vec}_{a,b}(W) \in \ker_{\mathbb{F}_{q^m}} A(V) \,\}.$$

The $\mathbb{F}_q$-rational part of the kernel is

$$L_0(V) = L(V) \cap \mathcal{M}_{a\times b}(\mathbb{F}_q).$$

Let $r_0 = \dim_{\mathbb{F}_q} L_0(V)$ and the projective rank-1 locus over $\mathbb{F}_q$ is

$$\Sigma_0 = \{[W] \in \mathbb{P}(\mathcal{M}_{a\times b}(\mathbb{F}_q)) : \ \mathrm{Rank}_{\mathbb{F}_q}(W) = 1\}.$$

Then, in the m prime case, size-1 Frobenius orbits correspond precisely to $\mathbb{F}_q$-rational rank-1 points:

$$a_1(V) = \#\big(\mathbb{P}(L_0(V)) \cap \Sigma_0\big).$$

Because every nonzero rank-1 matrix $W \in \mathcal{M}_{a\times b}(\mathbb{F}_q)$ can be written as $W = xy^\top$ for some nonzero column vector x and row vector $y^\top$ and such a factorization is unique up to multiplication by a scalar[4], the number of projective rank-1 matrices is

$$\#\Sigma_0 = \#\mathbb{P}^{a-1}(\mathbb{F}_q) \times \#\mathbb{P}^{b-1}(\mathbb{F}_q) = \left(\frac{q^a-1}{q-1}\right)\left(\frac{q^b-1}{q-1}\right)$$

while number of projective matrices of size $a\times b$ and projective (r_0-1)-subspaces are approximately

$$\begin{aligned}\#\mathbb{P}(\mathcal{M}_{a\times b}(\mathbb{F}_q)) &= \frac{q^{ab}-1}{q-1}\\ \#\mathbb{P}(L_0(V)) &= \frac{q^{r_0}-1}{q-1}.\end{aligned}$$

We model $\mathbb{P}(L_0(V))$ as a uniformly random projective (r_0-1)-subspace of $\mathbb{P}^{ab-1}(\mathbb{F}_q)$ independent of Σ_0. Under this model, the expected number of rank-1 $\mathbb{F}_q$-points is

$$\begin{aligned}\mathbb{E}[a_1(V)] &\approx \#\mathbb{P}(L_0(V)) \cdot \frac{\#\Sigma_0}{\#\mathbb{P}(\mathcal{M}_{a\times b}(\mathbb{F}_q))}\\ &= \frac{q^{r_0}-1}{q-1}\cdot\frac{(q^a-1)(q^b-1)}{(q-1)(q^{ab}-1)}\\ &\approx q^{\,r_0+a+b-ab-2}.\end{aligned} \tag{12}$$

Over $\mathbb{F}_{q^m}$, if $A(V)$ has full row rank mk (over $\mathbb{F}_{q^m}$, equivalently over $\mathbb{F}_q$), then

$$r = \dim_{\mathbb{F}_{q^m}} L(V) = ab - mk = (k+1)(m+\ell_1) - mk = m + (k+1)\ell_1.$$

Recall that in Phase 3 of the Hybrid Distinguisher, we have proven that the kernel over the extension field $\mathbb{F}_{q^m}$ is simply the scalar extension of the kernel over $\mathbb{F}_q$. Therefore

$$r_0 = \dim_{\mathbb{F}_q}(\ker_{\mathbb{F}_q} A) = \dim_{\mathbb{F}_{q^m}}(\ker_{\mathbb{F}_{q^m}} A) = r.$$

For $a = k+1$, $b = m+\ell_1$, $r_0 = m+(k+1)\ell_1$, Equation (12) gives the expectation:

$$\mathbb{E}[a_1(V)] \approx q^{(1-k)(m-1)+\ell_1}. \tag{13}$$

[4] This is known as the Segre embedding.

For $k \geq 2$, the exponent is dominated by $-(k-1)(m-1)$, predicting that $a_1(V)$ is very small. Therefore, Markov's inequality gives

$$\Pr\left(a_1(V) \geq 1\right) \;\leq\; \mathbb{E}[a_1(V)].$$

If $\mathbb{E}[a_1] \ll 1$, we can approximately assume $\Pr(a_1 \geq 1) \approx \mathbb{E}[a_1]$. Hence, under our random-subspace model and when (13) is $\ll 1$, the probability that we obtain base-field rank-1 solutions should be negligible. Empirically, we observe that, with overwhelming probability, $a_m(V) = 1$ for "valid" V, and the solution set size is $\#\mathcal{S}(V) = m$ (see Appendix A). Combined with the EGMC assumption $a_m(V) = 1$, this gives

$$\Pr\big[\#\mathcal{S}(V) > m\big] \;=\; \Pr\big[a_1(V) \geq 1\big] \;\leq\; q^{(1-k)(m-1)+\ell_1},$$

which gives

$$\Pr[\dim_{\mathbb{F}_q} A > m] \leq q^{(1-k)(m-1)+\ell_1}.$$

7 Complexity for concrete parameter sets

There are two directions of the distinguisher, thus the overall cost of the attack will be analyzed accordingly. In the guess-V-solve-U direction, the cost of the attack is

$$C_{V\to U} = \mathcal{O}\left(\underbrace{q^{(k+1)\ell_2}}_{V\text{-guess}}\underbrace{\binom{m+(k+1)\ell_1+1}{2}^{\omega}}_{\text{rank-1 extraction}}\right). \tag{14}$$

In the guess-U-solve-V direction, the cost of the attack is

$$C_{U\to V} = \mathcal{O}\left(\underbrace{q^{m\ell_1}}_{U\text{-guess}}\underbrace{\binom{m+\ell_2(1+k(m-k))+1}{2}^{\omega}}_{\text{rank-1 extraction}}\right). \tag{15}$$

In both directions, the $\omega = 2.8$ is the linear algebra constant. Our attack is especially strong when $\ell_1 = 0$ or $\ell_2 = 0$ because the exponential guessing factor disappears and the attack becomes polynomial-time. The final attack estimate is the better of the two directions:

$$\min\{\log_2 C_{V\to U}, \log_2 C_{U\to V}\}, \tag{16}$$

and the cost for concrete parameter sets are given in Table 1.

Acknowledgements The author would like to thank Brice Minaud for helpful discussions. This work was supported by the France 2030 ANR Project ANR-22-PECY-003 SecureCompute and the ANR grant PQMC (ANR-25-CE39-7662).

A Macaulay diagnostics for quadratic determinantal systems in guess-V-solve-U direction

Table 2: Small guess-V-solve-U quadratic determinantal systems: each degree entry gives the Macaulay rank/column count in corresponding degree D. The % column reports the percentage of full-rank U recoveries over 1000 trials per parameter set.

Parameters					Rank / columns			%
q	k	m	ℓ_1	ℓ_2	$D=2$	$D=3$	$D=4$	
2	2	4	1	0	24/28	80/84	206/210	66
2	2	4	1	1	24/28	80/84	206/210	99.5
2	3	4	1	0	32/36	116/120	326/330	94.6
2	3	4	1	1	32/36	116/120	326/330	100
2	3	6	1	0	49/55	214/220	709/715	99
2	3	6	1	1	49/55	214/220	709/715	100
2	6	7	1	0	98/105	553/560	2373/2380	100
2	6	7	1	1	98/105	553/560	2373/2380	100
2	5	7	1	0	84/91	448/455	1813/1820	100
2	5	7	1	1	84/91	448/455	1813/1820	100
2	4	7	1	0	71/78	357/364	1358/1365	100
2	4	7	1	1	71/78	357/364	1358/1365	100
2	4	7	2	0	146/153	962/969	4838/4845	100
2	4	7	2	2	146/153	962/969	4838/4845	100
2	4	5	1	0	50/55	215/220	710/715	100
2	4	5	1	1	50/55	215/220	710/715	100
2	3	5	1	0	40/45	160/165	490/495	100
2	3	5	1	1	40/45	160/165	490/495	100
2	3	5	1	2	40/45	160/165	490/495	100
2	3	5	1	3	40/45	160/165	490/495	100
2	2	5	1	0	31/36	115/120	325/330	100
2	2	5	1	1	31/36	115/120	325/330	100
2	4	5	2	0	115/120	675/680	3055/3060	100
2	4	5	2	2	115/120	675/680	3055/3060	100

B Macaulay diagnostics for quadratic determinantal systems in guess-U-solve-V direction

Table 3: Small guess-U-solve-V quadratic determinantal systems: each degree entry gives the Macaulay rank/column count in corresponding degree D. The % column reports the percentage of full-rank V recoveries over 1000 trials per parameter set.

Parameters				Rank / columns			%
q	k	m	ℓ_2	$D=2$	$D=3$	$D=4$	
2	2	4	1	41/45	161/165	491/495	81.0
2	3	4	1	32/36	116/120	326/330	94.0
2	3	4	2	74/78	360/364	1361/1365	80.0
2	3	6	1	130/136	810/816	3870/3876	100
2	6	7	1	98/105	553/560	2373/2380	100
2	4	5	1	50/55	215/220	710/715	100
2	3	5	1	73/78	359/364	1360/1365	100
2	2	5	1	73/78	359/364	1360/1365	100
2	4	5	2	115/120	675/680	3055/3060	100

C Encryption schemes based on EGMC

KeyGen (1^λ):

- Select a random $[m,k]_{q^m}$ Gabidulin code, with an efficient algorithm capable of decoding up to $\left\lfloor \frac{m-k}{2} \right\rfloor$ errors.
- Sample uniformly at random a basis $\gamma \xleftarrow{\$} \mathcal{B}(\mathbb{F}_{q^m})$.
- Compute a basis $(\boldsymbol{A}_1, \ldots, \boldsymbol{A}_{km})$ of the code $\Psi_\gamma(\mathcal{G})$.
- For i in range 1 to km, sample uniformly at random: $\boldsymbol{R}_i \xleftarrow{\$} \mathbb{F}_q^{m \times \ell_2}$, $\boldsymbol{R}'_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times m}$ and $\boldsymbol{R}''_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times \ell_2}$.
- Define the matrix code $\mathcal{C}_{mat}$ as explained in Definition 16.
- Sample uniformly at random matrices $\boldsymbol{P} \xleftarrow{\$} \mathbf{GL}_{m+\ell_1}(\mathbb{F}_q)$ and $\boldsymbol{Q} \xleftarrow{\$} \mathbf{GL}_{m+\ell_2}(\mathbb{F}_q)$.
- Define the code $\mathcal{C}'_{mat} = \boldsymbol{P}\mathcal{C}_{mat}\boldsymbol{Q}$.
- Let $\mathcal{B} = (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_{km})$ be a basis of $\mathcal{C}'_{mat}$.
- Return pk $= \mathcal{B}$ and sk $= (\mathcal{G}, \gamma, \boldsymbol{P}, \boldsymbol{Q})$.

Encrypt(pk, μ):

Input: pk $= (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_{km})$, $\mu \in \mathbb{F}_q^{km}$.

- Sample uniformly at random a matrix $\boldsymbol{E} \in \mathbb{F}_q^{(m+\ell_1)\times(m+\ell_2)}$ such that rank $\boldsymbol{E} \leq r$.
- Return $\boldsymbol{Y} = \sum_{i=1}^{km} \mu_i \boldsymbol{M}_i + \boldsymbol{E}$.

Decrypt(sk, $\boldsymbol{Y}$):

- Compute $\boldsymbol{P}^{-1}\boldsymbol{Y}\boldsymbol{Q}^{-1}$. Truncate the ℓ_1 last rows to obtain $\boldsymbol{M} \in \mathbb{F}_q^{m\times(m+\ell_2)}$.
- Compute $\Psi_\gamma^{-1}(\boldsymbol{M}) \in \mathbb{F}_{q^m}^{m+\ell_2}$. Let $\boldsymbol{y}$ be the first m entries.
- Apply the decoding algorithm of $\mathcal{G}$ on the word $\boldsymbol{y}$, it returns an error vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^m$.
- Compute $\boldsymbol{E}' = \Psi_\gamma(\boldsymbol{e})$.
- Solve the linear system:

$$\boldsymbol{Y} - (\boldsymbol{E}'|\boldsymbol{N})\boldsymbol{Q} = \sum_{i=1}^{km} \mu_i \boldsymbol{M}_i$$

whose $(k+\ell_2)m$ unknowns in $\mathbb{F}_q$ are the μ_i and the remaining part of the error $\boldsymbol{N}$ of size $m \times \ell_2$.

- Return $\hat{\mu}$ the solution of the above system.

Fig. 1: EGMC-McEliece encryption scheme

KeyGen (1^λ):

- Select a random $[m,k]_{q^m}$ Gabidulin code, with an efficient algorithm capable of decoding up to $\left\lfloor \frac{m-k}{2} \right\rfloor$ errors.
- Sample uniformly at random a basis $\gamma \xleftarrow{\$} \mathcal{B}(\mathbb{F}_{q^m})$.
- Compute a basis $(\boldsymbol{A}_1, \ldots, \boldsymbol{A}_{km})$ of the code $\Psi_\gamma(\mathcal{G})$.
- For i in range 1 to km, sample uniformly at random: $\boldsymbol{R}_i \xleftarrow{\$} \mathbb{F}_q^{m \times \ell_2}$, $\boldsymbol{R}'_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times m}$ and $\boldsymbol{R}''_i \xleftarrow{\$} \mathbb{F}_q^{\ell_1 \times \ell_2}$.
- Define the matrix code $\mathcal{C}_{mat}$ as explained above.
- Sample uniformly at random matrices $\boldsymbol{P} \xleftarrow{\$} \mathbf{GL}_{m+\ell_1}(\mathbb{F}_q)$ and $\boldsymbol{Q} \xleftarrow{\$} \mathbf{GL}_{m+\ell_2}(\mathbb{F}_q)$.
- Define the code $\mathcal{C}'_{mat} = \boldsymbol{P}\mathcal{C}_{mat}\boldsymbol{Q}$.
- Compute $\bar{\boldsymbol{H}} \in \mathbb{F}_q^{((m+\ell_1)(m+\ell_2)-mk)\times(m+\ell_1)(m+\ell_2)}$ a parity check matrix of $\mathcal{C}'_{mat}$.
- Return pk $= \bar{\boldsymbol{H}}$; sk $= (\gamma, \mathcal{G}, \boldsymbol{P}, \boldsymbol{Q})$

Encrypt(pk, μ):

Input: pk $= \bar{\boldsymbol{H}}$, a message $\mu \in \mathbb{F}_q^{(m+\ell_1)(m+\ell_2)}$ such that rank Fold$(\mu) \leq r$.

- For every integer i from 1 to $(m+\ell_1)(m+\ell_2)$, let $\boldsymbol{h}_i$ be the i-th column of $\bar{\boldsymbol{H}}$.
- Return $\boldsymbol{c} = \sum_{i=1}^{(m+\ell_1)(m+\ell_2)} \mu_i \boldsymbol{h}_i^\top$.

Decrypt(sk, $\boldsymbol{c}$):

Input: sk $= (\gamma, \mathcal{G}, \boldsymbol{P}, \boldsymbol{Q})$, $\boldsymbol{c} \in \mathbb{F}_q^{(m+\ell_1)(m+\ell_2)-mk}$.

- Find any $\bar{\boldsymbol{y}} \in \mathbb{F}_q^{(m+\ell_1)(m+\ell_2)}$ such that $\boldsymbol{c} = \sum_{i=1}^{(m+\ell_1)(m+\ell_2)} \bar{y}_i \boldsymbol{h}_i^\top$.
- Let $\boldsymbol{Y} =$ Fold$(\bar{\boldsymbol{y}})$. Compute $\boldsymbol{P}^{-1}\boldsymbol{Y}\boldsymbol{Q}^{-1}$. Truncate the ℓ_1 last rows to obtain $\boldsymbol{M} \in \mathcal{M}_{m\times(m+\ell)}(\mathbb{F}_q)$.
- Let $\boldsymbol{y}$ be the first m coordinates of $\Psi_\gamma^{-1}(\boldsymbol{M}) \in \mathbb{F}_{q^m}^{m+\ell_2}$.
- Let $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$, with rank$(\boldsymbol{e}) \leq r$. Apply the decoding algorithm of $\mathcal{G}$ on the word composed of the m first coordinates.
- Let $\boldsymbol{E} = \Psi_\gamma(\boldsymbol{e})$. Then $\boldsymbol{E} = (\boldsymbol{E}'|\boldsymbol{N}) \in \mathcal{M}_{m\times(m+\ell_2)}(\mathbb{F}_q)$ is a matrix whose the nm coefficients of $\boldsymbol{E}'$ are known, and $\boldsymbol{N}$ is the remaining part of the error.
- Solve the linear system $\boldsymbol{c} = \sum_{i=1}^{(m+\ell_1)(m+\ell_2)} \bar{e}_i \boldsymbol{h}_i^\top$ to find the ℓm values of $\boldsymbol{N}$, with $\bar{\boldsymbol{e}} =$ Unfold$(\boldsymbol{E})$ with unknown some coefficients.
- Return $\hat{\mu} =$ Unfold$(\boldsymbol{E})$.

Fig. 2: EGMC-Niederreiter encryption scheme

References

1. Aragon, N., Couvreur, A., Dyseryn, V., Gaborit, P., Vinçotte, A.: Minrank Gabidulin encryption scheme on matrix codes. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 68–100. Springer (2024)
2. Augot, D., Couvreur, A., Lavauzelle, J., Neri, A.: Rank-Metric Codes over arbitrary Galois extensions and rank analogues of Reed–Muller Codes. SIAM Journal on Applied Algebra and Geometry **5**(2), 165–199 (2021)
3. Couvreur, A., Debris-Alazard, T., Gaborit, P.: On the hardness of code equivalence problems in rank metric. arXiv preprint arXiv:2011.04611 (2020)
4. Couvreur, A., Zappatore, I.: An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes. In: International Conference on Post-Quantum Cryptography. pp. 3–37. Springer (2023)
5. Cox, D., Little, J., O'shea, D., Sweedler, M.: Ideals, varieties, and algorithms. Springer (1997)
6. Cox, D.A.: Stickelberger and the Eigenvalue Theorem. In: Commutative Algebra: Expository Papers Dedicated to David Eisenbud on the Occasion of his 75th Birthday, pp. 283–298. Springer (2021). https://doi.org/10.1007/978-3-030-89694-2_8
7. Cox, D.A., Little, J., O'Shea, D.: Using Algebraic Geometry, Graduate Texts in Mathematics, vol. 185. Springer, 2 edn. (2005)
8. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. Journal of combinatorial theory, Series A **25**(3), 226–241 (1978)
9. Gabidulin, E.: Combinatorial metrics in coding theory. In: 2nd International Symposium on Information Theory, 1973. Akademiai Kiado (1973)
10. Loidreau, P.: A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In: International Workshop on Coding and Cryptography. pp. 36–45. Springer (2005)
11. Overbeck, R.: Structural attacks for public key cryptosystems based on Gabidulin codes. Journal of cryptology **21**(2), 280–301 (2008)
12. Porwal, A., Wachter-Zeh, A., Loidreau, P.: Key Attack on the ACDGV Matrix Encryption Scheme. In: Advances in Cryptology - EUROCRYPT 2026 (2026), https://eprint.iacr.org/2025/1292, to appear
13. Seroussi, G., Roth, R.M.: On MDS extensions of generalized Reed-Solomon codes. IEEE Transactions on Information Theory **32**(3), 349–354 (2003)