A post-quantum encryption scheme based on linearized Reed-Solomon codes.

Kayodé Epiphane Nouetowa

Univ Rennes, CNRS, IRMAR - UMR 6625, Rennes Cedex, France*

Abstract

In this paper, we propose a new McEliece-type scheme in sum-rank metric based on linearized Reed-Solomon codes using, as a scrambling matrix, a homogeneous block-diagonal matrix whose entries in each block generate a small-dimensional vector space.

Key Words : Code based cryptography, sum-rank metric, post-quantum cryptography.

Acknowledgments.

This work was conducted within the France 2030 program, Centre Henri Lebesgue ANR-11-LABX-0020-01. It is also supported by the ANR-DFG project CROWD - ANR - CE 48 2022.

1 Introduction

Code-based cryptography has seen significant progress over the last two decades. It began in 1978 with the McEliece scheme proposed in [McE78] and based on Goppa codes in Hamming metric. The difficulty with this scheme is the large size of its keys. In 1991, the GPT cryptosystem [GPT91], another McEliece-type cryptosystem, was proposed in rank metric and based on Gabidulin codes [Gab85], which are rank metric equivalents of Reed-Solomon codes. However, the strong algebaic structure of those codes was successfully exploited for attacking the GPT cryptosystem in [Gib96], and its variants with the Overbeck attack [Ove05]. In [Loi17] Loidreau proposed a new scheme based on Gabidulin codes, using a matrix whose entries generate a small-dimensional vector space as a scrambler matrix to avoid Overbeck

*kayode-epiphane.nouetowa@univ-rennes.fr

attack's. But, Loidreau's scheme has been broken for certain parameters (see [Gha22, CC]). In order to avoid these attacks, a modification is proposed in [NL25]. In this article, drawing inspiration from Loidreau's scheme, we propose a new McEliece-type scheme based on the linearized Reed–Solomon codes introduced in [MP18]. These codes generalize the Gabidulin codes; to our knowledge, however, there is no polynomial-time Overbeck-type distinguisher for these codes. The structure of these codes makes efficient scrambling easier compared to Gabidulin codes. Our scheme achieves parameters with key sizes that are competitive with other well-known schemes.

The paper is structured as follows. Section 2 recalls essential background on linear codes, the sum-rank decoding problem, and known attacks addressing this problem. Section 3 recalls linearized Reed–Solomon codes and their duals, while Section 4 examines their distinguishability. In Section 5, we present a new encryption scheme in the sum-rank metric, we establish the conditions under which a structural attack may occur, and we propose concrete parameter sets for our construction.

2 Generalities

Let $\mathbb{F}_q$ denote the finite field with q elements where q is the power of a prime and let $\mathbb{F}_{q^m}$ denote the field with q^m elements i.e., the extension field of degree m of $\mathbb{F}_q$. $\mathbb{F}_{q^m}$ is also an $\mathbb{F}_q$-vector space of dimension m.

Definition 1. *An $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$ of length n and dimension k is a subspace of dimension k of $\mathbb{F}_{q^m}^n$.*

The notation $[n,k]_{q^m}$ is used to denote the parameters of a linear code. The code $\mathcal{C}$ can be represented as follows:

$$\mathcal{C} = \{\boldsymbol{x}\mathbf{G} \mid \boldsymbol{x} \in \mathbb{F}_{q^m}^k\} = \{\boldsymbol{c} \in \mathbb{F}_{q^m}^n \mid \mathbf{H}\boldsymbol{c}^t = 0\}$$

where $\mathbf{G} \in \mathbb{F}_{q^m}^{k\times n}$ and $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ are full-rank matrices called respectively a generator matrix and a parity check matrix of $\mathcal{C}$. The dual of $\mathcal{C}$ noted $\mathcal{C}^\perp$ is orthogonal to $\mathcal{C}$ with respect to the Euclidean scalar product. The code $\mathcal{C}^\perp$ is a $[n, n-k]_{q^m}$ code of generator matrix $\mathbf{H}$.
Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$. The **support** of $\mathbf{a}$, denoted by $\mathrm{supp}(\mathbf{a})$, is the $\mathbb{F}_q$-subspace generated by the coordinates of $\mathbf{a}$: $\mathrm{supp}(\mathbf{a}) \stackrel{def}{=} \langle a_1, \ldots, a_n\rangle_{\mathbf{F}_q}$. The **rank weight** of $\mathbf{a}$ over $\mathbb{F}_q$ is defined as the dimension of the support of $\mathbf{a}$ $w_R(\mathbf{a}) \stackrel{def}{=} \dim \mathrm{supp}(\mathbf{a})$. A rank code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ is a $[n,k]_{q^m}$ code endowed with the distance induced by the rank metric. The minimum rank distance of $\mathcal{C}$ is defined as $d_R(\mathcal{C}) \stackrel{def}{=} \min_{\mathbf{x}\in\mathcal{C}\setminus\{0\}} w_R(\mathbf{x})$.
Let $\boldsymbol{n} = (n_1, \ldots, n_\ell) \in (\mathbb{N}^*)^\ell$ and $n = n_1 + \cdots + n_\ell$. Suppose that $\mathbf{a} = (\mathbf{a}_1 \mid \ldots \mid \mathbf{a}_\ell)$ where $\mathbf{a}_i$ belongs to $\mathbb{F}_{q^m}^{n_i}$. The **sum-rank weight** of $\mathbf{a}$ over

$\mathbb{F}_q$ is $w_{\mathrm{SR}}(\mathbf{a}) \stackrel{def}{=} \sum_{i=1}^{\ell} w_R(\mathbf{a}_i)$. A sum-rank code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ is an $[n,k]_{q^m}$ code endowed with the distance induced by the sum-rank metric. The minimum sum-rank distance of $\mathcal{C}$ is defined as $d_{\mathrm{SR}}(\mathcal{C}) \stackrel{def}{=} \min_{\mathbf{x}\in\mathcal{C}\setminus\{0\}} w_{\mathrm{SR}}(\mathbf{x})$.

2.1 Sum-Rank decoding problem

The security of our scheme, presented later (see Section5), relies on the hardness of the sum-rank decoding (SRD) problem (see [PRR22]).

Definition 2 (SRD **problem**). *Let* $\boldsymbol{n} = (n_1, \ldots, n_\ell) \in (\mathbb{N}^*)^\ell$ *and* $\boldsymbol{r} = (r_1, \ldots, r_\ell) \in \mathbb{N}^\ell$ *vectors of integers,* $n = \sum_{i=1}^{\ell} n_i$ *and* $r = \sum_{i=1}^{\ell} r_i$. *Given* $(\mathbf{G}, \boldsymbol{y}, r) \in \mathbb{F}_{q^m}^{k\times n} \times \mathbb{F}_{q^m}^n \times \mathbb{N}^*$ *with* $\mathbf{G}$ *of full rank, the Sum-Rank Decoding problem SRD*$(\mathbf{n}, k, \mathbf{r}, m)$ *asks to compute* $\mathbf{e} = (\mathbf{e}_1 \mid \ldots \mid \mathbf{e}_\ell) \in \mathbb{F}_{q^m}^n$ *and* $\mathbf{x} \in \mathbb{F}_{q^m}^k$ *such that* $\boldsymbol{y} = \boldsymbol{x}\mathbf{G}+\mathbf{e}$, $\mathbf{e}_i \in \mathbb{F}_{q^m}^{n_i}$ *and* $w_R(\mathbf{e}_i) = r_i$ *for all* $i = 1, \ldots, \ell$.

If $\ell = 1$, the SRD$(\mathbf{n}, k, \mathbf{r}, m)$ problem is rank decoding problem and noted RD(n, k, r, m). When $\mathrm{supp}(\mathbf{e}_i) \cap \mathrm{supp}(\mathbf{e}_j) = \{0\}$ for all $i, j \in \{1, \ldots, \ell\}$ and $i \neq j$, $\mathbf{e}$ is referred to as an ℓ-error or blockwise error (see [ABD$^+$24, SZHW25] for more detail). In this case, $w_{\mathrm{SR}}(\mathbf{e}) = w_{\mathrm{R}}(\mathbf{e})$ and the SRD$(\mathbf{n}, k, \mathbf{r}, m)$ problem is called ℓ-RD$(\mathbf{n}, k, \mathbf{r}, m)$ problem in [ABD$^+$24, SZHW25].

2.1.1 Combinatorial attack

The combinatorial attack proposed in [AGHT18] for the RD(m, n, k, r) problem was adapted for the SRD$(\mathbf{n}, k, \mathbf{r}, m)$ problem in [PRR22] and then recently in [ABD$^+$24]. The global complexity of this attack in $\mathbb{F}_q$ operations is

$$\mathcal{O}((n-k)^\omega m^\omega q^{-m+\sum_{i=1}^{\ell} r_i(m-t_i)})$$

where ω is the linear algebra constant, $r_i \leq t_i \leq m$ and $\sum_{i=1}^{\ell} n_i t_i \leq m(n-k)$.

2.1.2 Algebraic attack

To solve problem SRD$(\mathbf{n}, k, \mathbf{r}, m)$, we can use the algebraic attack proposed in [SZHW25], which is an adaptation of the one proposed in [BBC$^+$20] for the ℓ-RD$(\mathbf{n}, k, \mathbf{r}, m)$ problem. The overall complexity of this attack in $\mathbb{F}_q$ operations is

$$\mathcal{O}(q^{\sum_{i=1}^{\ell} a_i r_i} m \binom{n-k-1}{r} (\prod_{i=1}^{\ell} \binom{n_i - a_i}{r_i})^{\omega-1})$$

where ω is the linear algebra constant and $(a_1, \ldots, a_\ell) \in \mathbb{N}^\ell$ such that $m\binom{n-k-1}{r} \geq \prod_{i=1}^{\ell} \binom{n_i - a_i}{r_i} - 1$.

3 Linearized Reed-Solomon codes

Consider the automorphism θ of $\mathbb{F}_{q^m}$ defined by: $a \mapsto a^q$. Gabidulin codes are the rank metric equivalent of Reed-Solomon codes. They are defined as follows.

Definition 3 (Gabidulin codes)**.** *Let $k, n \in \mathbb{N}$ such that $k < n \leq m$. Let $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ a vector of $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^m}$. The Gabidulin code $\mathcal{G}_k(\mathbf{g})$ with support vector $\mathbf{g}$ is the $[n,k]_{q^m}$ linear code of generator matrix*

$$G_k^\theta(\mathbf{g}) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ \theta(g_1) & \theta(g_2) & \cdots & \theta(g_n) \\ \vdots & \vdots & \vdots & \vdots \\ \theta^{k-1}(g_1) & \theta^{k-1}(g_2) & \cdots & \theta^{k-1}(g_n) \end{pmatrix}. \tag{1}$$

Such codes are known to have minimum distance $n-k+1$ for the rank metric and to benefit from a decoding algorithm correcting up to $\frac{n-k}{2}$.

Proposition 1. *[Gab85, Theorem 7] Let $\mathcal{G}_k(\mathbf{g}) \subset \mathbb{F}_{q^m}^n$, then there exists $\mathbf{h} \in \mathbb{F}_{q^m}^n$ of rank n such that $\mathcal{G}_{n-k}(\mathbf{h}) = \mathcal{G}_k(\mathbf{g})^\perp$ for the usual scalar product in $\mathbb{F}_{q^m}$.*

Let $a \in \mathbb{F}_{q^m}$, we define $N_0^\theta(a) = 1$ and $N_i^\theta(a) = \prod_{j=0}^{i-1} \theta^{i-1}(a)$ for all i in $\mathbb{N}^*$. For all $k \in \mathbb{N}^*$ we also define the diagonal matrix $D_k^\theta(a)$ as

$$D_k^\theta(a) = \text{diagonal}(N_0^\theta(a), \cdots, N_{k-1}^\theta(a)).$$

Definition 4 (Linearized Reed-Solomon codes [MP18])**.** *Let $\ell, n_1, \ldots, n_\ell \in \mathbb{N}^*$ such that $\ell \leq q-1$ and $n_i \leq m$. Let $\gamma \in \mathbb{F}_{q^m}^*$ be a primitive element and $i_1, \ldots, i_\ell \in \{0, \ldots, q-2\}$ pairwise distinct with $i_1 = 0$. Let $\mathbf{u_i} \in \mathbb{F}_{q^m}^{n_i}$ a vector of $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^m}$ for all $i \leq \ell$. Let $k \in \mathbb{N}^*$ and $n = n_1 + \cdots + n_\ell$ such that $k \leq n$. A **linearized Reed-Solomon code** is a $[n,k]_{q^m}$ linear code of generator matrix*

$$\mathbf{G} = (G_k^\theta(\mathbf{u}_1) | D_k^\theta(\gamma^{i_2}) G_k^\theta(\mathbf{u}_2) | \cdots | D_k^\theta(\gamma^{i_\ell}) G_k^\theta(\mathbf{u}_\ell)).$$

Such codes are known to have minimum distance $n-k+1$ in sum-rank metric and to benefit from a polynomial time decoding algorithm correcting up to $\frac{n-k}{2}$ (see [MPK19]).

Remark 1.

- *A Gabidulin code is a one block linearized Reed-Solomon code.*
- *The maximum number of blocks in a linearized Reed-Solomon code is $q-1$, and the length of each block is at most m (the order of θ). Therefore, we can construct the linearized Reed-Solomon codes of length up to $m(q-1)$ over $\mathbb{F}_{q^m}$ (see [Nou25, Chapter 6] for more details).*

Theorem 1. *[MPK19, Theorem 4] Consider a $[n,k]_{q^m}$ linearized Reed-Solomon code $\mathcal{C}$ with $\mathbf{G} = (G_k^\theta(\mathbf{u}_1)|D_k^\theta(\gamma^{i_2})G_k^\theta(\mathbf{u}_2)|\cdots|D_k^\theta(\gamma^{i_\ell})G_k^\theta(\mathbf{u}_\ell))$ a generator matrix as defined in Definition 4. The dual of $\mathcal{C}$ is a $[n,n-k]_{q^m}$ linearized Reed-Solomon code $\mathcal{C}^\perp$ of generator matrix*

$$\mathbf{H} = (G_{n-k}^{\theta^{-1}}(\mathbf{v}_1)|D_{n-k}^{\theta^{-1}}(\theta^{-1}(\gamma^{i_2}))G_{n-k}^{\theta^{-1}}(\mathbf{v}_2)|\cdots|D_{n-k}^{\theta^{-1}}(\theta^{-1}(\gamma^{i_\ell}))G_{n-k}^{\theta^{-1}}(\mathbf{v}_\ell))$$

where $\mathbf{v_i} \in \mathbb{F}_{q^m}^{n_i}$ is a vector of $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^m}$ for all $i = 1,\ldots,\ell$.

From now on, we will only consider linearized Reed-Solomon codes with blocks of the same length, i.e., $n_1 = \cdots = n_\ell = \eta$ and $n = \ell\eta$.

4 Linearized Reed-Solomon codes distinguishability

The main question here is how to distinguish linearized Reed-Solomon codes from a random code. In the specific case corresponding to Gabidulin codes, we have Overbeck's distinguisher, presented in [Ove05] and described as follows. Let $x = (x_1,\ldots,x_n) \in \mathbb{F}_{q^m}^n$. For any $i \in \mathbb{N}$, we define $\theta^i(x) = (\theta^i(x_1),\ldots,\theta^i(x_n))$. This definition naturally extends to matrix and codes. Let $\mathcal{C}$ a $[n,k]_{q^m}$ linear code. We define the τ-th θ-sum of $\mathcal{C}$ as:

$$\Gamma_\tau^\theta(\mathcal{C}) = \mathcal{C} + \theta(\mathcal{C}) + \ldots + \theta^\tau(\mathcal{C}).$$

- Let $\mathcal{C}$ be a $[n,k]_{q^m}$ random linear code, with a high probability we have $\dim \Gamma_\tau^\theta(\mathcal{C}) = min\{n, k(1+\tau)\}$.
- Let $\mathcal{G}$ be a $[n,k]_{q^m}$ Gabidulin code, we have $\dim \Gamma_\tau^\theta(\mathcal{G}) = min\{n, k+\tau\}$. When $\tau \in \{0,\ldots,n-k\}$, we get $\dim \Gamma_\tau^\theta(\mathcal{G}) = k+\tau$.

This difference in behavior between Gabidulin codes and random codes is called Overbeck's distinguisher. When the linearized Reed-Solomon code is different from a Gabidulin code, it behaves like a random code with respect to this distinguisher. In [HBH22] an Overbeck-like distinguisher is proposed, but this is an exponential time distinguisher.
The following method we propose gives us a polynomial-time distinguisher. Consider a $[n,k]_{q^m}$ linearized Reed-Solomon code $\mathcal{C}$ of generator matrix $\mathbf{G} = (G_k^\theta(\mathbf{u}_1)|D_k^\theta(\gamma^{i_2})G_k^\theta(\mathbf{u}_2)|\cdots|D_k^\theta(\gamma^{i_\ell})G_k^\theta(\mathbf{u}_\ell))$ as defined in Definition 4 such that $n_1 = \cdots = n_\ell = \eta$, $n = \ell\eta$ and $k \leq n$. If $k < \eta$, then each block of $\mathbf{G}$ generates a Gabidulin code for which we can apply the Overbeck distinguisher. Otherwise, if η doesn't divide k, we can do the following. Let $b = \lfloor \frac{k}{\eta} \rfloor + 1$ the smallest integer such that $k < b\eta$.

- Consider $\mathbf{G}_\mathrm{T}$ a submatrix of $\mathbf{G}$ consisting of b blocks of $\mathbf{G}$ and having the same number of rows as $\mathbf{G}$.

- Let $\mathbf{H}_{\mathrm{T}}$ be a parity check matrix of the $[b\eta, k]_{q^m}$ linearized Reed-Solomon code $\mathcal{C}_{\mathrm{T}}$ with generator matrix $\mathbf{G}_{\mathrm{T}}$.

The dual of $\mathcal{C}_{\mathrm{T}}$ is a $[b\eta, b\eta - k]_{q^m}$ linearized Reed-Solomon code. Since $b\eta - k < \eta$, using Overbeck distinguisher we can show that each block of $\mathbf{H}_{\mathrm{T}}$ generates a Gabidulin code. Therefore, $\mathcal{C}$ is different from a random code.

5 New encryption scheme

To design this new encryption scheme, we will draw inspiration from Loidreau's scheme [Loi17]. The main idea here is to choose several different subspaces of $\mathbb{F}_{q^m}$, of the same dimension and corresponding exactly to the number of blocks that make up the linearized Reed-Solomon code in question. Each of these subspaces will be used to scramble a single given block of the code.

Proposition 2. *Let $\lambda \geq 2$ an integer and $\mathcal{V}_i$ a λ-dimensional subspace of $\mathbb{F}_{q^m}$ for all $i = 1, \ldots, \ell$. Let $\mathbf{P}_i \in GL_\eta(\mathbb{F}_{q^m}) \cap \mathcal{M}_\eta(\mathcal{V}_i)$ and $\mathbf{P} = \mathrm{Diagonal}(\mathbf{P}_1, \ldots, \mathbf{P}_\ell)$ a block diagonal matrix. Let $\mathbf{e} = (\mathbf{e}_1 \mid \cdots \mid \mathbf{e}_\ell) \in \mathbb{F}_{q^m}^n$ with $\boldsymbol{e}_j \in \mathbb{F}_{q^m}^\eta$, such that $w_{\mathrm{SR}}(\boldsymbol{e}) \leq t$, we have $w_{\mathrm{SR}}(\mathbf{eP}) \leq \lambda t$.*

Proof. We have $w_{\mathrm{SR}}(\mathbf{eP}) = \sum_{j=1}^{\ell} w_R(\boldsymbol{e}_j \mathbf{P}_j)$. According to [Loi17, Proposition 1], $w_R(\boldsymbol{e}_j \mathbf{P}_j) \leq \lambda w_{\mathrm{R}}(\mathbf{e}_j)$. Therefore $w_{\mathrm{SR}}(\mathbf{eP}) \leq \lambda w_{\mathrm{SR}}(\mathbf{e})$. □

5.1 Description of the scheme

Let $n, k, \ell, \eta \in \mathbb{N}^*$ such that $\ell \leq q-1$, $\eta \leq m$, $n = \ell\eta$ and $k \leq n$. The three parts of the scheme can be described as follows:

◇ `Key generation`:

- Choose at random $\gamma \in \mathbb{F}_{q^m}$ a primitive element and $\{i_1, \ldots, i_\ell\} \in \{0, \ldots, q-2\}$ pairwise distinct.
- Choose at random $\mathbf{u}_1, \ldots, \mathbf{u}_\ell \in (\mathbb{F}_{q^m}^*)^\eta$ such that $w_R(\mathbf{u}_i) = \eta$.
- Compute $\mathbf{G} = (G_k^\theta(\mathbf{u}_1) | D_k^\theta(\gamma^{i_2}) G_k^\theta(\mathbf{u}_2) | \cdots | D_k^\theta(\gamma^{i_\ell}) G_k^\theta(\mathbf{u}_\ell))$.
- Choose at random $\mathcal{V}_1, \ldots, \mathcal{V}_\ell \subset \mathbb{F}_{q^m}$ λ-dimensional subspaces.
- Choose at random $\mathbf{P}_1, \ldots, \mathbf{P}_\ell$ such that $\mathbf{P}_i \in \mathrm{GL}_\eta(\mathbb{F}_{q^m}) \cap \mathcal{M}_\eta(\mathcal{V}_i)$.
- Compute $\mathbf{P} = \mathrm{Diagonal}(\mathbf{P}_1, \ldots, \mathbf{P}_\ell)$.
- Choose at random $\mathbf{S} \in \mathrm{GL}_k(\mathbb{F}_{q^m})$

  Return

  Public key: $\mathbf{G}_{pub} = \mathbf{SGP}^{-1}$

  Secret key: $(\mathbf{u}_1, \ldots, \mathbf{u}_\ell), \mathbf{P}$

◇ `Encryption` of $\mathbf{m} \in \mathbb{F}_{q^m}^k$:

– Choose at random $\mathbf{e}_1, \ldots, \mathbf{e}_\ell \in (\mathbb{F}_{q^m}^\eta)^*$, $\mathbf{e} = (\mathbf{e}_1 \mid \cdots \mid \mathbf{e}_\ell)$. such that $w_{\mathrm{SR}}(\mathbf{e}) \leq \lfloor \frac{n-k}{2\lambda} \rfloor$.
– Compute $\boldsymbol{y} = \mathbf{m}\mathbf{G}_{pub} + \mathbf{e}$.

◇ `Decryption` of $\boldsymbol{y}$:

– Compute $\boldsymbol{y}\mathbf{P} = \mathbf{m}\mathbf{S}\mathbf{G} + \mathbf{e}\mathbf{P}$.
– Since $w_{\mathrm{SR}}(\mathbf{e}) \leq \lfloor \frac{n-k}{2\lambda} \rfloor$ then $w_{\mathrm{SR}}(\mathbf{e}\mathbf{P}) \leq \lfloor \frac{n-k}{2} \rfloor$.
– Recover $\mathbf{m}\mathbf{S}$ by decoding $\boldsymbol{y}\mathbf{P}$ with the linearized Reed-Solomon code generated by $\mathbf{G}$ and multiply it by $\mathbf{S}^{-1}$ to recover $\mathbf{m}$.

Remark 2. *When $\ell = 1$, the secret code in our scheme of Section 5.1 is a Gabidulin code, and this scheme corresponds to Loidreau's scheme [Loi17].*

5.2 Public code distinguishability

The Loidreau encryption scheme, which is a special case of this new scheme, was attacked only for a few parameters by structural attacks based on the Coggia Couvreur distinguisher [CC]. Thus, we may ask under which conditions the public code in this new scheme is distinguishable from a random code.

We will first recall the Coggia and Couvreur distinguisher, which corresponds to the case $\ell = 1$. Consider $\mathbf{G}_{\mathrm{pub}} = \mathbf{S}G_k^\theta(\mathbf{u}_1)\mathbf{P}_1^{-1}$ a generator matrix of the public code, as defined in Loidreau's scheme. Let $\mathcal{C}_{\mathrm{pub}}$ the code generated by $\mathbf{G}_{\mathrm{pub}}$ and $\mathcal{C}_{\mathrm{pub}}^\perp$ its dual. We have $\dim \Gamma_\lambda^\theta(\mathcal{C}_{\mathrm{pub}}^\perp) \leq \lambda \dim \mathcal{C}_{\mathrm{pub}}^\perp + \lambda$. This implies that the public code $\mathcal{C}_{\mathrm{pub}}$ is different from a random one if $\lambda \dim \mathcal{C}_{\mathrm{pub}}^\perp + \lambda \leq \min\{n, (1+\lambda)\dim \mathcal{C}_{\mathrm{pub}}^\perp\}$.

Proposition 3. *Consider the $[\ell\eta, k]_{q^m}$ public code $\mathcal{C}_{\mathrm{pub}}$ generated by $\mathbf{G}_{\mathrm{pub}}$ defined in the new scheme. Assume that η doesn't divide k. Let $b = \lfloor \frac{k}{\eta} \rfloor + 1$. The code $\mathcal{C}_{\mathrm{pub}}$ is distinguished from a random code if*
$\lambda(b\eta - k) + \lambda < \min(\eta, (1+\lambda)(b\eta - k))$.

Proof. Recall that $\mathbf{G}_{\mathrm{pub}} = \mathbf{S}(G_k^\theta(\mathbf{u}_1)|D_k^\theta(\gamma^{i_2})G_k^\theta(\mathbf{u}_2)|\cdots|D_k^\theta(\gamma^{i_\ell})G_k^\theta(\mathbf{u}_\ell))\mathbf{P}^{-1}$. Let $b = \lfloor \frac{k}{\eta} \rfloor + 1$ and $\mathcal{C}_{\mathrm{T}}$ the truncated code from $\mathcal{C}_{\mathrm{pub}}$ with generator matrix $\mathbf{G}_{\mathrm{T}} = \mathbf{S}(G_k^\theta(\mathbf{u}_1)|D_k^\theta(\gamma^{i_2})G_k^\theta(\mathbf{u}_2)|\cdots|D_k^\theta(\gamma^{i_b})G_k^\theta(\mathbf{u}_b))\mathbf{P}_{\mathrm{T}}^{-1}$ where $\mathbf{P}_{\mathrm{T}} = \mathrm{Diagonal}(\mathbf{P}_1, \ldots, \mathbf{P}_b)$ is a block diagonal matrix. Since $\mathcal{C}_{\mathrm{T}}$ is a $[b\eta, k]_{q^m}$ code, its dual $\mathcal{C}_{\mathrm{T}}^\perp$ is a $[b\eta, b\eta - k]_{q^m}$ code. Considering Theorem 1, we can show that the generator matrix $\mathbf{H}_{\mathrm{T}}$ of $\mathcal{C}_{\mathrm{T}}^\perp$ is of the form

$$\mathbf{H}_{\mathrm{T}} = \mathbf{V}(G_{b\eta-k}^{\theta^{-1}}(\mathbf{v}_1)|D_{b\eta-k}^{\theta^{-1}}(\theta^{-1}(\gamma^{i_2}))G_{b\eta-k}^{\theta^{-1}}(\mathbf{v}_2)|\cdots|D_{b\eta-k}^{\theta^{-1}}(\theta^{-1}(\gamma^{i_b}))G_{b\eta-k}^{\theta^{-1}}(\mathbf{v}_b))\mathbf{P}_{\mathrm{T}}^t,$$

where $\mathbf{V} \in \mathrm{GL}_{b\eta-k}(\mathbb{F}_{q^m})$ and $\mathbf{v}_i \in (\mathbb{F}_{q^m}^*)^\eta$ such that $w_R(\mathbf{v}_i) = \eta$. Each block of $\mathbf{H}_{\mathrm{T}}$ is a generator matrix of a $[\eta, b\eta - k]_{q^m}$ code. Let $\mathcal{C}_{\mathrm{T}j}^\perp$ be the code generated by the j-th block of $\mathbf{H}_{\mathrm{T}}$ for all $j = 1, \ldots, b$. According

to Coggia-Couvreur distinguisher, we have $\dim \Gamma_\lambda^{\theta^{-1}}(\mathcal{C}_{\mathrm{T}j}^\perp) \leq \lambda \dim \mathcal{C}_{\mathrm{T}j}^\perp + \lambda$. Thus, $\mathcal{C}_{\mathrm{T}j}^\perp$ is distinguishable from a random code if $\lambda \dim \mathcal{C}_{\mathrm{T}j}^\perp + \lambda < \min\{\eta, (1+\lambda)\dim \mathcal{C}_{\mathrm{T}j}^\perp\}$, that is to say $\lambda(b\eta - k) + \lambda < \min(\eta, (1+\lambda)(b\eta - k))$. In this case, $\mathcal{C}_{\mathrm{T}j}^\perp$ and therefore $\mathcal{C}_{\mathrm{pub}}$ are distinguishable from a random code. □

5.3 Structural attacks

Recall that $\mathbf{y} = \mathbf{mG}_{pub} + \mathbf{e}$ where $\mathbf{e} = (\mathbf{e}_1 \mid \cdots \mid \mathbf{e}_\ell)$. If we write $\mathbf{y}$ like $\mathbf{y} = (\mathbf{y}_1 \mid \cdots \mid \mathbf{y}_\ell)$, then for all $j = 1, \ldots, \ell$ we get

$$\mathbf{y}_j = \mathbf{mS} D_k^\theta(\gamma^{i_j}) G_k^\theta(\mathbf{u}_j) \mathbf{P}_j^{-1} + \mathbf{e}_j.$$

If $k < \eta$, then $\mathbf{y}_j$ is the ciphertext in a Loidreau's scheme whose public code is generated by $\mathbf{S} D_k^\theta(\gamma^{i_j}) G_k^\theta(\mathbf{u}_j) \mathbf{P}_j^{-1}$. In this case, if the distinguisher (Proposition 3) is valid and the rank weight of $\mathbf{e}_j$ allows it, we can use the structural attacks proposed in [Gha22, CC], when $\lambda = 2$ or $\lambda = 3$.

5.4 Proposed parameters

The following table presents a set of parameters based on the complexity of the decoding attacks in sections 2.1.1 and 2.1.2, along with the public key and ciphertext sizes in the Niederreiter version.

m	n	k	η	t	λ	q	Sec. Target	pk-size	ct-size
25	75	27	25	12	2	4	136	7.91 kB	0.29 kB
32	90	30	30	15	2	4	200	14.06 kB	0.47 kB
36	108	36	36	18	2	4	310	24.04 kB	0.63 kB

5.4.1 Comparison with other schemes

Here, we compare the sum of the public key sizes and the ciphertext sizes of our scheme with those of other well-known schemes, including the NIST standard (see [MAB+18] for more details).

Scheme	128 bits	192 bits
New scheme	**8.2** kB	**14.53** kB
RQC	5.48 kB	8.54 kB
LowMS	5.76 kB	14.97 kB
HQC	6.73 kB	13.56 kB
Classic McEliece	261.2 kB	624.3 kB

6 Conclusion.

In this paper, we proposed a new encryption scheme based on linearized Reed-Solomon codes. Using these codes to design the scheme is advantageous in that their structure facilitates scrambling and we can construct very

long codes over a small field. We proposed parameters with competitive key sizes compared to other well-known schemes. As a future direction, we can try to construct an RQC-type scheme with this code family, the rank metric equivalent of the HQC scheme (the NIST standard [MAB+18]).

References

[ABD+24] Nicolas Aragon, Pierre Briaud, Victor Dyseryn, Philippe Gaborit, and Adrien Vinçotte. The blockwise rank syndrome learning problem and its applications to cryptography. In *International Conference on Post-Quantum Cryptography*, pages 75–106. Springer, 2024.

[AGHT18] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. A new algorithm for solving the rank syndrome decoding problem. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2421–2425. IEEE, 2018.

[BBC+20] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 507–536. Springer, 2020.

[CC] D Coggia and A Couvreur. On the security of a Loidreau rank metric code based encryption scheme. des. codes crypt. 88 (9), 1941–1957 (2020).

[Gab85] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy peredachi informatsii*, 21(1):3–16, 1985.

[Gha22] Anirban Ghatak. Extending coggia–couvreur attack on Loidreau's rank-metric cryptosystem. *Designs, Codes and Cryptography*, 90(1):215–238, 2022.

[Gib96] Keith Gibson. The security of the gabidulin public key cryptosystem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 212–223. Springer, 1996.

[GPT91] Ernst M Gabidulin, Aleksei Paramonov, and OV Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 482–489. Springer, 1991.

[HBH22] Felicitas Hörmann, Hannes Bartz, and Anna-Lena Horlemann. Distinguishing and recovering generalized linearized Reed–Solomon codes. In *Code-Based Cryptography Workshop*, pages 1–20. Springer, 2022.

[Loi17] Pierre Loidreau. A new rank metric codes based encryption scheme. In *International Workshop on Post-Quantum Cryptography*, pages 3–17. Springer, 2017.

[MAB+18] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loıc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and IC Bourges. Hamming quasi-cyclic (hqc). *NIST PQC Round*, 2(4):13, 2018.

[McE78] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244(1978):114–116, 1978.

[MP18] Umberto Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra*, 504:587–612, 2018.

[MPK19] Umberto Martínez-Peñas and Frank R Kschischang. Reliable and secure multishot network coding using linearized Reed-Solomon codes. *IEEE Transactions on Information Theory*, 65(8):4785–4803, 2019.

[NL25] Kayodé Epiphane Nouetowa and Pierre Loidreau. An analysis of a generalization of Loidreau's encryption scheme. In *2025 IEEE International Symposium on Information Theory (ISIT)*, pages 1–6. IEEE, 2025.

[Nou25] Kayodé Epiphane Nouetowa. *Codes tordus, dualité et décodage: application à la cryptographie*. PhD thesis, Université de Rennes, 2025.

[Ove05] Raphael Overbeck. A new structural attack for gpt and variants. In *International Conference on Cryptology in Malaysia*, pages 50–63. Springer, 2005.

[PRR22] Sven Puchinger, Julian Renner, and Johan Rosenkilde. Generic decoding in the sum-rank metric. *IEEE Transactions on Information Theory*, 68(8):5075–5097, 2022.

[SZHW25] Yongcheng Song, Jiang Zhang, Xinyi Huang, and Wei Wu. Blockwise rank decoding problem and lrpc codes: cryptosystems with smaller sizes. *IEEE Transactions on Information Theory*, 2025.