McEliece-type encryption based on Gabidulin codes with no hidden structure

Wenshuo Guo* and Fang-Wei Fu†

Abstract

This paper presents a new McEliece-type encryption scheme based on Gabidulin codes, which uses linearized transformations to disguise the private key. When endowing this scheme with the partial cyclic structure, we obtain a public key of the form GM^{-1}, where G is a partial circulant generator matrix of Gabidulin code and M as well as M^{-1} is a circulant matrix of large rank weight, even as large as the code length. Another difference from Loidreau's proposal at PQCrypto 2017 is that both G and M are publicly known. Recovering the private key can be reduced to deriving from M a linearized transformation and two circulant matrices of small rank weight. This new scheme is shown to resist all the known distinguisher-based attacks, such as the Overbeck attack and Coggia-Couvreur attack, and also has a very small public key size. For instance, 2592 bytes are enough for our proposal to achieve the security of 256 bits, which is 400 times smaller than Classic McEliece that has been selected into the fourth round of the NIST Post-Quantum Cryptography (PQC) standardization process.

Keywords Post-quantum cryptography · Code-based cryptography · Gabidulin codes · Partial cyclic codes · Linearized transformations

1 Introduction

Over the past decades, post-quantum cryptosystems (PQCs) have been drawing more and more attention from the cryptographic community. The most remarkable advantage of PQCs over classical cryptosystems is their potential resistance against attacks from quantum computers. In the area of PQC, cryptosystems based on coding theory are one of the most promising candidates. Apart from resisting quantum attacks, these cryptosystems also have faster encryption and decryption procedures. The first code-based cryptosystem was proposed by McEliece [37] in 1978. However, this scheme has never been used in practice due to the drawback of large key size. For instance, Classic McEliece [3] submitted to the NIST PQC project [39] requires 255 kilobytes of public key for the 128-bit security. To overcome this drawback, various improvements have been proposed one after another.

Gabidulin, Paramonov and Tretjakov (GPT) [19] proposed a rank-based encryption scheme by using Gabidulin codes in the McEliece setting. Research results show that the complexity of decoding general rank metric codes is much higher than that for Hamming metric codes. Rank-based cryptosystem, therefore, have a more compact representation of public keys. Unfortunately, the GPT cryptosystem was broken by Gibson [25, 26] and then by Overbeck [43].

*Wenshuo Guo is with the Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China. ws_guo@mail.nankai.edu.cn

†Fang-Wei Fu is with the Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China. fwfu@nankai.edu.cn

To resist these attacks, some reparations of GPT were proposed [17, 18, 20, 46]. However, because of Gabidulin codes being highly structured, all these variants are still vulnerable to structural attacks [28, 40, 44]. Specifically, Gabidulin codes contain a large subspace invariant under the Frobenius transformation, which makes Gabidulin codes distinguishable from general linear codes.

Faure and Loidreau [15] proposed a cryptosystem based on the p-polynomial reconstruction problem, which can be seen as a rank metric counterpart of the Augot-Finiasz cryptosystem [6]. The Faure-Loidreau cryptosystem is a scheme based on Gabidulin codes without hiding the algebraic structure, whose public key is a Gabidulin codeword corrupted by a word of rank weight beyond the error-correcting capability. This scheme remained secure until the work in [21], where the authors proposed a polynomial-time key recovery attack. Two reparations of this scheme designed to prevent this attack were proposed independently and differently in [31,47]. Bombar and Couvreur [12] investigated the supercode decoding of Gabidulin codes and deduced from this decoder a polynomial-time attack on these two reparations. Another Gabidulin code-based cryptosystem with no hidden structure is the one proposed in [2] and then submitted to the NIST standardization process [1], whose security relies on the difficulty of decoding rank quasi-cyclic (RQC) codes. What differs from McEliece-type schemes is that the ciphertext of RQC consists of two vectors. Apart from the algebraic attacks in [8,9], RQC has never been severely attacked.

Loidreau [34] proposed a McEliece-type cryptosystem using Gabidulin codes, whose public key is a matrix of the form GM^{-1}. The right scrambler matrix is chosen such that M has a small rank weight of λ. The public code then cannot be distinguished from random ones and therefore, Loidreau's proposal can prevent the Overbeck attack [44]. However, by operating the dual of the public code Coggia and Couvreur [14] presented an effective distinguisher and gave a practical key recovery attack for $\lambda = 2$. This attack was extended by Ghatak [24] to the case of $\lambda = 3$ and then by Pham and Loidreau [45]. Let H_{pub} be a parity-check matrix of the public code, then $H_{pub} = HM^T$ where H forms a parity-check matrix of Gabidulin code. Although Loidreau [36] claimed that one can publish G without losing security, one cannot derive H from H_{pub} because of M being kept secret. For this reason we still view this scheme as one with hidden structure.

Lau and Tan [29] (LT18) proposed a scheme based on Gabidulin codes with hidden structure. The public key consists of two matrices $G + UT$ and U, where G is a generator matrix of Gabidulin code and U is a partial circulant matrix, scrambled by a matrix T over the base field. Recently Guo and Fu [27] showed that one can recover T in polynomial time and completely break this scheme. By modifying the idea of LT18, Lau and Tan [30] (LT19) designed another scheme based on the so-called partial cyclic Gabidulin codes, also with hidden structure. The public key of LT19 consists of two vectors and therefore has a quite small size. This scheme can prevent the Guo-Fu attack and remains secure until now for properly chosen parameters.

Our contributions. Firstly, we introduce and investigate the properties of linearized transformations over linear codes. Secondly, we propose a McEliece-type encryption scheme, where linearized transformations are utilized to disguise the private key. The public matrix in our proposal appears quite random and consequently, all the known distinguisher-based attacks do not work any longer. Additionally, the use of the partial cyclic structure greatly reduces the public key size.

Recently NIST has completed the third round of the PQC standardization process. Three key-establishment mechanisms (KEMs) based on coding theory have been selected into the fourth round, these algorithms are Classic McEliece [3] based on Goppa codes and HQC [38]

as well as BIKE [4] based on quasi-cyclic moderate density parity check (QC-MDPC) codes. In contrast to these NIST PQC submissions and Loidreau's proposal, our scheme has the following innovations and advantages:

- The use of linearized transformations enhances the security against structural attacks. Before our work in the present paper, almost all the known approaches used to disguise the private information are based on linear transformations, which have been shown to fail in most cases.
- In the partial cyclic version, the algebraic structure of the underlying Gabidulin code can be published without losing security. This enables our proposal to be the first McEliece-type encryption scheme with no hidden structure.
- The use of the partial cyclic structure greatly shrinks the public key. However, one cannot use this technique in Loidreau's proposal, otherwise one can easily deduce an equivalent private key from the public information.
- The advantage over HQC and BIKE is that the decryption algorithm in our proposal is deterministic and therefore has no decryption failure that the former two ones confront.

The rest of this paper is arranged as follows. Section 2 introduces some notations and preliminaries used throughout this paper. Section 3 presents the RSD problem in coding theory and two types of generic attacks. In Section 4, we introduce the concept of linearized transformations and investigate their properties over linear codes. Section 5 describes our new proposal and gives some notes on the private key. Security analysis of the new proposal will be given in Section 6. In Section 7, we suggest some parameters for three security levels and compare the public key size with some other code-based cryptosystems. A few concluding remarks will be made in Section 8.

2 Preliminaries

We now present some notations used throughout this paper, as well as basic concepts of linear codes and rank metric codes. Then we introduce the so-called partial cyclic Gabidulin codes and some related results.

2.1 Notations and basic concepts

Let $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_{q^m}$ an extension of $\mathbb{F}_q$ of degree m. We call $\boldsymbol{a} \in \mathbb{F}_{q^m}^m$ a basis vector of $\mathbb{F}_{q^m}/\mathbb{F}_q$ if the components of $\boldsymbol{a}$ are linearly independent over $\mathbb{F}_q$. We call α a polynomial element if $(1, \alpha, \ldots, \alpha^{m-1})$ forms a basis vector of $\mathbb{F}_{q^m}/\mathbb{F}_q$, and α a normal element if $(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$ forms a basis vector respectively. Denote by $\mathcal{M}_{k,n}(\mathbb{F}_q)$ the space of $k \times n$ matrices over $\mathbb{F}_q$, and by $\mathrm{GL}_n(\mathbb{F}_q)$ the space of invertible matrices in $\mathcal{M}_{n,n}(\mathbb{F}_q)$. Let $\langle M \rangle_q$ be the vector space spanned by the rows of $M \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ over $\mathbb{F}_q$.

An $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is the orthogonal space of $\mathcal{C}$ under the Euclidean inner product over $\mathbb{F}_q^n$. A matrix $G \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ is called a generator matrix of $\mathcal{C}$ if its rows form a basis of $\mathcal{C}$. A generator matrix of $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$.

The rank support of $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ with respect to $\mathbb{F}_q$, denoted by $\mathrm{RS}_q(\boldsymbol{v})$, is the linear space spanned by the components of $\boldsymbol{v}$ over $\mathbb{F}_q$. The rank weight of $\boldsymbol{v}$, denoted by $\mathrm{rk}_q(\boldsymbol{v})$, is the dimension of $\mathrm{RS}_q(\boldsymbol{v})$ over $\mathbb{F}_q$. The rank support of $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, denoted by $\mathrm{RS}_q(M)$, is the

linear space spanned by the entries of M over $\mathbb{F}_q$. The rank weight of M, denoted by $\mathrm{rk}_q(M)$, is the dimension of $\mathrm{RS}_q(M)$ over $\mathbb{F}_q$. For $\boldsymbol{v} \in \mathbb{F}_{q^m}^u$, $M \in \mathcal{M}_{u,v}(\mathbb{F}_{q^m})$ and $N \in \mathcal{M}_{v,w}(\mathbb{F}_{q^m})$, it is easy to see that $\mathrm{rk}_q(\boldsymbol{v}M) \leqslant \mathrm{rk}_q(\boldsymbol{v}) \cdot \mathrm{rk}_q(M)$ and $\mathrm{rk}_q(MN) \leqslant \mathrm{rk}_q(M) \cdot \mathrm{rk}_q(N)$.

For $\alpha \in \mathbb{F}_{q^m}$ and a positive integer l, we define $\alpha^{[l]} = \alpha^{q^l}$ to be the l-th Frobenius power of α. For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$, let $\boldsymbol{v}^{[l]} = (v_1^{[l]}, \ldots, v_n^{[l]})$. For $M = (M_{ij}) \in \mathcal{M}_{u,v}(\mathbb{F}_{q^m})$, let $M^{[l]} = (M_{ij}^{[l]})$. For $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$, let $\mathcal{V}^{[i]} = \{\boldsymbol{v}^{[i]} : \boldsymbol{v} \in \mathcal{V}\}$. For $M \in \mathcal{M}_{u,v}(\mathbb{F}_{q^m}), N \in \mathcal{M}_{v,w}(\mathbb{F}_{q^m})$, it is clear that $(MN)^{[l]} = M^{[l]}N^{[l]}$. For $M \in \mathrm{GL}_n(\mathbb{F}_{q^m})$, clearly $(M^{[l]})^{-1} = (M^{-1})^{[l]}$.

2.2 Gabidulin code

Gabidulin codes are actually a rank metric counterpart of Reed-Solomon codes, which can be defined through the so-called Moore matrix as follows.

Definition 1 (Moore matrix). Let $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$, then the $k \times n$ Moore matrix generated by $\boldsymbol{g}$ is a matrix of the form

$$\mathrm{Mr}_k(\boldsymbol{g}) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}.$$

Definition 2 (Gabidulin code). For positive integers $k \leqslant n \leqslant m$ and $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(\boldsymbol{g}) = n$, the $[n, k]$ Gabidulin code $\mathrm{Gab}_k(\boldsymbol{g})$ generated by $\boldsymbol{g}$ is defined to be a linear code that has $\mathrm{Mr}_k(\boldsymbol{g})$ as a generator matrix.

Remark 1. An $[n, k]$ Gabidulin code $\mathrm{Gab}_k(\boldsymbol{g})$ has minimum rank weight $n - k + 1$ [19] and can therefore correct up to $\left\lfloor \frac{n-k}{2} \right\rfloor$ rank errors in theory. Several efficient decoding algorithms for Gabidulin code can be found in [16, 33, 48].

2.3 Partial cyclic code

Lau and Tan [30] used partial cyclic Gabidulin codes to reduce the public key size in rank-based cryptography. Now we introduce this family of codes and present some related results.

Definition 3 (Circulant matrix). For a vector $\boldsymbol{m} \in \mathbb{F}_q^n$, the circulant matrix generated by $\boldsymbol{m}$ is a matrix $M \in \mathcal{M}_{n,n}(\mathbb{F}_q)$ whose first row is $\boldsymbol{m}$ and i-th row is obtained by cyclically right shifting its $(i-1)$-th row for $2 \leqslant i \leqslant n$.

Definition 4 (Partial circulant matrix). For $k \leqslant n$ and $\boldsymbol{m} \in \mathbb{F}_q^n$, the $k \times n$ partial circulant matrix $\mathrm{PC}_k(\boldsymbol{m})$ generated by $\boldsymbol{m}$ is defined to be the first k rows of the circulant matrix generated by $\boldsymbol{m}$. Particularly, we denote by $\mathrm{PC}_n(\boldsymbol{m})$ the circulant matrix generated by $\boldsymbol{m}$.

Remark 2. Let $\mathrm{PC}_n(\mathbb{F}_q)$ be the space of $n \times n$ circulant matrices over $\mathbb{F}_q$. Chalkley [13] proved that $\mathrm{PC}_n(\mathbb{F}_q)$ forms a commutative ring under matrix addition and multiplication. It is easy to see that, for a partial circulant matrix $A \in \mathrm{PC}_k(\mathbb{F}_q)$ and a circulant matrix $B \in \mathrm{PC}_n(\mathbb{F}_q)$, AB forms a $k \times n$ partial circulant matrix.

Now we present a sufficient and necessary condition for a circulant matrix to be invertible, then make an accurate estimation of the number of invertible circulant matrices over $\mathbb{F}_q$.

Proposition 1. [41] *For* $\boldsymbol{m} = (m_0, \ldots, m_{n-1}) \in \mathbb{F}_q^n$, *let* $\boldsymbol{m}(x) = \sum_{i=0}^{n-1} m_i x^i \in \mathbb{F}_q[x]$. *A sufficient and necessary condition for* $\mathrm{PC}_n(\boldsymbol{m})$ *being invertible is* $\gcd(\boldsymbol{m}(x), x^n - 1) = 1$.

Proposition 2. [32] *For a monic $f(x) \in \mathbb{F}_q[x]$ of degree n, let $g_1(x), \ldots, g_r(x) \in \mathbb{F}_q[x]$ be r distinct monic irreducible factors of $f(x)$, i.e. $f(x) = \prod_{i=1}^{r} g_i(x)^{e_i}$ for some positive integers $e_1, \ldots, e_r$. Let $d_i = \deg(g_i)$ for $1 \leqslant i \leqslant r$, then*

$$\Phi_q(f) = q^n \prod_{i=1}^{r} (1 - \frac{1}{q^{d_i}}), \tag{1}$$

where $\Phi_q(f)$ denotes the number of monic polynomials coprime to $f(x)$ of degree less than n.

The following corollary is drawn directly from Propositions 1 and 2.

Corollary 1. *The number of invertible matrices in $\mathrm{PC}_n(\mathbb{F}_q)$ is $\Phi_q(x^n - 1)$.*

Now we introduce the concept of partial cyclic codes.

Definition 5 (Partial cyclic codes). For $k \leqslant n$ and $\boldsymbol{a} \in \mathbb{F}_q^n$, let $G = \mathrm{PC}_k(\boldsymbol{a})$ be a partial circulant matrix generated by $\boldsymbol{a}$, then $\mathcal{C} = \langle G \rangle_q$ is called an $[n, k]$ partial cyclic code.

Remark 3. Let $\boldsymbol{g} = (\alpha^{[n-1]}, \alpha^{[n-2]}, \ldots, \alpha)$ be a normal basis vector of $\mathbb{F}_{q^n}/\mathbb{F}_q$ and $G = \mathrm{Mr}_k(\boldsymbol{g})$, then G forms a $k \times n$ partial circulant matrix. We call $\mathcal{G} = \langle G \rangle_{q^n}$ an $[n, k]$ partial cyclic Gabidulin code generated by $\boldsymbol{g}$.

3 RSD problem and generic attacks

Now we introduce the well-known RSD problem in coding theory which lays the foundation of rank-based cryptography, as well as the best known generic attacks that will be useful to estimate the practical security of our proposal later in this paper.

Definition 6 (Rank Syndrome Decoding (RSD) Problem). Given positive integers m, n, k and t, let H be an $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ of full rank and $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$. The RSD problem with parameters (q, m, n, k, t) is to search for $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{s} = \boldsymbol{e}H^T$ and $\mathrm{rk}_q(\boldsymbol{e}) = t$.

The RSD problem has been used for designing cryptosystems since the proposal of the GPT cryptosystem in 1991. However, the hardness of this problem had never been proved until the work in [23], where the authors gave a randomized reduction of the RSD problem to an NP-complete decoding problem [10] in the Hamming metric.

Generic attacks on the RSD problem can be divided into two categories, namely the combinatorial attacks and algebraic attacks. The main idea of combinatorial attacks consists in solving a multivariate linear system obtained from the parity-check equation, whose variables are components of e_i under a basis of the rank support of $\boldsymbol{e}$ over $\mathbb{F}_q$. The complexity mainly lies in enumerating t-dimensional subspaces of $\mathbb{F}_{q^m}$. The best known combinatorial attacks up to now can be found in [5, 22, 42], as summarized in Table 1.

The main idea of algebraic attacks consists in converting an RSD instance into a multivariate quadratic system and then solving this system with algebraic approaches, such as the Gröbner basis techniques. Algebraic attacks are generally believed to be less efficient than combinatorial approaches until the work in [8, 9], whose complexity and applicable condition are summarized in Table 2, where $\omega = 2.81$ is the linear algebra constant.

4 Linearized transformations

Note that $\mathbb{F}_{q^m}$ can be viewed as an m-dimensional linear space over $\mathbb{F}_q$. Let $(\alpha_1, \ldots, \alpha_m)$ and $(\beta_1, \ldots, \beta_m)$ be two basis vectors of $\mathbb{F}_{q^m}/\mathbb{F}_q$. For any $\alpha = \sum_{i=1}^{m} \lambda_i \alpha_i \in \mathbb{F}_{q^m}$ with $\lambda_i \in \mathbb{F}_q$, we

Attack	Complexity
[42]	$\mathcal{O}\left(\min\left\{m^3t^3q^{(t-1)(k+1)}, (k+t)^3t^3q^{(t-1)(m-t)}\right\}\right)$
[22]	$\mathcal{O}\left((n-k)^3m^3q^{\min\left\{t\left\lceil\frac{mk}{n}\right\rceil,(t-1)\left\lceil\frac{m(k+1)}{n}\right\rceil\right\}}\right)$
[5]	$\mathcal{O}\left((n-k)^3m^3q^{t\left\lceil\frac{m(k+1)}{n}\right\rceil-m}\right)$

Table 1: Best known combinatorial attacks.

Attack	Condition	Complexity
[9]	$m\binom{n-k-1}{t} \geqslant \binom{n}{t} - 1$	$\mathcal{O}\left(m\binom{n-p-k-1}{t}\binom{n-p}{t}^{\omega-1}\right)$, where $p = \max\{1 \leqslant i \leqslant n : m\binom{n-i-k-1}{t} \geqslant \binom{n-i}{t} - 1\}$
[8]		$\mathcal{O}\left(\left(\frac{((m+n)t)^t}{t!}\right)^\omega\right)$
[9]	$m\binom{n-k-1}{t} < \binom{n}{t} - 1$	$\mathcal{O}\left(q^{at}m\binom{n-k-1}{t}\binom{n-a}{t}^{\omega-1}\right)$, where $a = \min\{1 \leqslant i \leqslant n : m\binom{n-k-1}{t} \geqslant \binom{n-i}{t} - 1\}$
		$\mathcal{O}\left(\frac{B_b\binom{k+t+1}{t}+C_b(mk+1)(t+1)}{B_b+C_b}A_b^2\right)$, where $A_b = \sum_{j=1}^{b}\binom{n}{t}\binom{mk+1}{j}$, $B_b = \sum_{j=1}^{b} m\binom{n-k-1}{t}\binom{mk+1}{j}$, $C_b = \sum_{j=1}^{b}\sum_{i=1}^{j}(-1)^{i+1}\binom{n}{t+i}\binom{m+i-1}{i}\binom{mk+1}{j-i}$, $b = \min\{0 < a < t+2 : A_a - 1 \leqslant B_a + C_a\}$
[8]		$\mathcal{O}\left(\left(\frac{((m+n)t)^{t+1}}{(t+1)!}\right)^\omega\right)$

Table 2: Best known algebraic attacks.

define a permutation of $\mathbb{F}_{q^m}$ as

$$\psi(\alpha) = \sum_{i=1}^{m} \lambda_i \psi(\alpha_i) = \sum_{i=1}^{m} \lambda_i \beta_i.$$

It is easy to see that ψ is $\mathbb{F}_q$-linearized, namely

$$\psi(\gamma_1\alpha + \gamma_2\beta) = \gamma_1\psi(\alpha) + \gamma_2\psi(\beta)$$

holds for any $\alpha, \beta \in \mathbb{F}_{q^m}$ and $\gamma_1, \gamma_2 \in \mathbb{F}_q$. By $\mathrm{LP}_m(\mathbb{F}_q)$ we denote the space of all $\mathbb{F}_q$-linearized permutations of $\mathbb{F}_{q^m}$.

In the sequel we will do further study on this family of permutations. Firstly, we present a basic fact about $\mathbb{F}_q$-linearized permutations of $\mathbb{F}_{q^m}$.

Proposition 3. *The total number of $\mathbb{F}_q$-linearized permutations of $\mathbb{F}_{q^m}$ is*

$$|\mathrm{LP}_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1}(q^m - q^i).$$

Let $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$ be an $\mathbb{F}_q$-linearized permutation of $\mathbb{F}_{q^m}$. For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$, let $\psi(\boldsymbol{v}) = (\psi(v_1), \ldots, \psi(v_n))$. For $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$, let $\psi(\mathcal{V}) = \{\psi(\boldsymbol{v}) : \boldsymbol{v} \in \mathcal{V}\}$. For $M = (M_{ij}) \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, let $\psi(M) = (\psi(M_{ij}))$. In these cases, we call ψ a linearized transformation over $\mathbb{F}_{q^m}/\mathbb{F}_q$.

For $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ and $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$, a natural question is how the rank weight of $\boldsymbol{v}$ varies under the action of ψ. For this reason, we introduce the following proposition.

Proposition 4. *A linearized transformation over $\mathbb{F}_{q^m}/\mathbb{F}_q$ is an isometry in the rank metric.*

Proof. For $n \leqslant m$, let $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(\boldsymbol{v}) = n$. If $\mathrm{rk}_q(\psi(\boldsymbol{v})) < n$, then there exists $\boldsymbol{b} \in \mathbb{F}_q^n \backslash \{\boldsymbol{0}\}$ such that $\psi(\boldsymbol{v})\boldsymbol{b}^T = \psi(\boldsymbol{v}\boldsymbol{b}^T) = 0$. This implies that $\boldsymbol{v}\boldsymbol{b}^T = 0$, which conflicts with $\mathrm{rk}_q(\boldsymbol{v}) = n$. More generally, suppose $\mathrm{rk}_q(\boldsymbol{v}) = r < n$, then there exist $Q \in \mathrm{GL}_n(\mathbb{F}_q)$ and $\boldsymbol{v}^* \in \mathbb{F}_{q^m}^r$ with $\mathrm{rk}_q(\boldsymbol{v}^*) = r$ such that $\boldsymbol{v} = (\boldsymbol{v}^* | \boldsymbol{0})Q$. It follows that $\psi(\boldsymbol{v}) = (\psi(\boldsymbol{v}^*)|\boldsymbol{0})Q$ and then $\mathrm{rk}_q(\psi(\boldsymbol{v})) = \mathrm{rk}_q(\psi(\boldsymbol{v}^*)) = \mathrm{rk}_q(\boldsymbol{v}^*) = \mathrm{rk}_q(\boldsymbol{v})$. □

Remark 4. Let $\mathbb{E}$ be an extension field of $\mathbb{F}_{q^m}$, then a linearized transformation over $\mathbb{E}/\mathbb{F}_{q^m}$ preserves the rank metric in $\mathbb{E}^n$ with respect to $\mathbb{F}_q$.

For $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$ and a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, it is clear that $\psi(\mathcal{C})$ is $\mathbb{F}_q$-linear, but generally no longer $\mathbb{F}_{q^m}$-linear. We call ψ fully linear if it preserves the $\mathbb{F}_{q^m}$-linearity of all linear codes over $\mathbb{F}_{q^m}$. The following theorem provides a sufficient and necessary condition for ψ being fully linear.

Theorem 7. *Let $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$ and $\boldsymbol{a} = (\alpha_1, \ldots, \alpha_m)$ be a basis vector of $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let $A = \psi(\boldsymbol{a}^T\boldsymbol{a})$, then a sufficient and necessary condition for ψ being fully linear is Rank$(A) = 1$.*

Proof. On the necessity aspect. Let $\mathcal{C} = \langle \boldsymbol{a} \rangle_{q^m}$ and $\boldsymbol{a}_i = \psi(\alpha_i \boldsymbol{a})$ be the i-th row of A. Note that ψ is fully linear, then $\psi(\mathcal{C})$ is $\mathbb{F}_{q^m}$-linear. Let $k = \dim_{q^m}(\psi(\mathcal{C}))$, then $(q^m)^k = |\psi(\mathcal{C})| = |\mathcal{C}| = q^m$ and hence $k = 1$. This implies that $\mathrm{Rank}(A) = 1$ because of $\boldsymbol{a}_i$ being contained in $\psi(\mathcal{C})$.

On the sufficiency aspect. Let $\mathcal{V} = \{\sum_{j=1}^m \lambda_j \boldsymbol{a}_j : \lambda_j \in \mathbb{F}_q\}$ and $\mathcal{V}_i = \{\mu \boldsymbol{a}_i : \mu \in \mathbb{F}_{q^m}\}$ for any $1 \leqslant i \leqslant m$. Note that A has rank 1 over $\mathbb{F}_{q^m}$, then there exists $\mu_{ij} \in \mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \backslash \{0\}$ such that $\boldsymbol{a}_j = \mu_{ij}\boldsymbol{a}_i$ for any $1 \leqslant i, j \leqslant m$. It follows that $\mathcal{V} = \{\sum_{j=1}^m \lambda_j \mu_{ij} \boldsymbol{a}_i : \lambda_j \in \mathbb{F}_q\}$ and furthermore $\mathcal{V} \subseteq \mathcal{V}_i$. Together with $|\mathcal{V}| = |\mathcal{V}_i| = q^m$, we have $\mathcal{V} = \mathcal{V}_i$. Hence for any $\mu \in \mathbb{F}_{q^m}$, there exist $\lambda_{i1}, \ldots, \lambda_{im} \in \mathbb{F}_q$ such that $\mu \boldsymbol{a}_i = \sum_{j=1}^m \lambda_{ij} \boldsymbol{a}_j$.

Let $\mathcal{C}$ be an arbitrary linear code over $\mathbb{F}_{q^m}$. For any $\boldsymbol{v} \in \psi(\mathcal{C})$, there exists $\boldsymbol{u} \in \mathcal{C}$ such that $\boldsymbol{v} = \psi(\boldsymbol{u})$. Meanwhile, there exists $M \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\boldsymbol{u} = \boldsymbol{a}M$. It follows that

$$\boldsymbol{a}_j M = \psi(\alpha_j \boldsymbol{a})M = \psi(\alpha_j \boldsymbol{a} M) = \psi(\alpha_j \boldsymbol{u}) \in \psi(\mathcal{C})$$

for any $1 \leqslant j \leqslant m$. Assume that $\sum_{i=1}^m a_i \alpha_i = 1$ for $a_i \in \mathbb{F}_q$, then $\boldsymbol{u} = \boldsymbol{a}M = \sum_{i=1}^m a_i \alpha_i \boldsymbol{a} M$. Hence

$$\mu \boldsymbol{v} = \mu \psi(\boldsymbol{u}) = \mu \psi(\sum_{i=1}^m a_i \alpha_i \boldsymbol{a} M) = \mu \sum_{i=1}^m a_i \psi(\alpha_i \boldsymbol{a}) M = \sum_{i=1}^m a_i \mu \boldsymbol{a}_i M.$$

Note that for any $\mu \in \mathbb{F}_{q^m}$ and $1 \leqslant i \leqslant m$, there exists $\lambda_{ij} \in \mathbb{F}_q$ such that $\mu \boldsymbol{a}_i = \sum_{j=1}^m \lambda_{ij} \boldsymbol{a}_j$. Hence

$$\mu \boldsymbol{v} = \sum_{i=1}^m a_i (\sum_{j=1}^m \lambda_{ij} \boldsymbol{a}_j) M = \sum_{i=1}^m \sum_{j=1}^m \lambda_{ij} a_i (\boldsymbol{a}_j M) \in \psi(\mathcal{C})$$

because of $\boldsymbol{a}_j M \in \psi(\mathcal{C})$ and $\psi(\mathcal{C})$ being $\mathbb{F}_q$-linear. Following this, we conclude that $\psi(\mathcal{C})$ is $\mathbb{F}_{q^m}$-linear and therefore ψ is fully linear over $\mathbb{F}_{q^m}$. □

Remark 5. Note that $\mathrm{Rank}(A)$ is independent of the basis vector. More generally, let $\boldsymbol{b}_1, \boldsymbol{b}_2$ be any two basis vectors of $\mathbb{F}_{q^m}/\mathbb{F}_q$, then there exist $Q_1, Q_2 \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $\boldsymbol{b}_1 = \boldsymbol{a}Q_1$ and $\boldsymbol{b}_2 = \boldsymbol{a}Q_2$. Let $A' = \psi(\boldsymbol{b}_1^T \boldsymbol{b}_2)$, then $A' = \psi((\boldsymbol{a}Q_1)^T \boldsymbol{a}Q_2) = \psi(Q_1^T \boldsymbol{a}^T \boldsymbol{a} Q_2) = Q_1^T A Q_2$, which implies that $\mathrm{Rank}(A') = \mathrm{Rank}(A)$.

Note that a fully linear transformation over $\mathbb{F}_{q^m}/\mathbb{F}_q$ always preserves the $\mathbb{F}_{q^m}$-linearity of a linear code over $\mathbb{F}_{q^m}$. However, for a specific linear code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, a linearized transformation that preserves the $\mathbb{F}_{q^m}$-linearity of $\mathcal{C}$ is not necessarily fully linear. Specifically, we introduce the following theorem.

Theorem 8. *For positive integers $k < n$, let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ be an $[n, k]$ linear code. Let $G = [I_k | A]$ be the systematic generator matrix of $\mathcal{C}$, where I_k is the $k \times k$ identity matrix and $A = (A_{ij}) \in \mathcal{M}_{k,n-k}(\mathbb{F}_{q^m})$. Let $\mathcal{A} = \{A_{ij}\}_{i,j=1}^{k,n-k}$, then we have the following statements.*

(1) *If $\mathcal{A} \subseteq \mathbb{F}_q$, then any $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$ is linear over $\mathcal{C}$. Furthermore, we have $\psi(\mathcal{C}) = \mathcal{C}$;*

(2) *If there exists $\alpha \in \mathcal{A}$ such that α is a polynomial element of $\mathbb{F}_{q^m}/\mathbb{F}_q$, then any $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$ linear over $\mathcal{C}$ must be fully linear.*

Proof. (1) Let $\boldsymbol{g}_i$ be the i-th row of G, then $\psi(\alpha \boldsymbol{g}_i) = \psi(\alpha)\boldsymbol{g}_i$ for any $\alpha \in \mathbb{F}_{q^m}$. For any $\boldsymbol{c} \in \mathcal{C}$, there exists $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{c} = \boldsymbol{\lambda} G$. Then we have

$$\psi(\boldsymbol{c}) = \psi(\boldsymbol{\lambda} G) = \psi(\sum_{i=1}^{k} \lambda_i \boldsymbol{g}_i) = \sum_{i=1}^{k} \psi(\lambda_i \boldsymbol{g}_i) = \sum_{i=1}^{k} \psi(\lambda_i)\boldsymbol{g}_i \in \mathcal{C},$$

which suggests that $\psi(\mathcal{C}) \subseteq \mathcal{C}$. Together with $|\psi(\mathcal{C})| = |\mathcal{C}|$, there will be $\psi(\mathcal{C}) = \mathcal{C}$.

(2) Without loss of generality, we consider the first row vector of G and assume that $\boldsymbol{g}_1 = (1, 0, \ldots, 0, \alpha, \star) \in \mathbb{F}_{q^m}^n$, where $\alpha \in \mathbb{F}_{q^m}$ is a polynomial element and "$\star$" represents some vector in $\mathbb{F}_{q^m}^{n-k-1}$. Note that ψ is linear over $\mathcal{C}$, or equivalently $\psi(\mathcal{C})$ is an $\mathbb{F}_{q^m}$-linear code. Apparently $\psi(\mathcal{C})$ has $\psi(G)$ as a generator matrix, which implies that there exists $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_{q^m}^k$ such that $\psi(\beta \boldsymbol{g}_1) = \boldsymbol{\lambda}\psi(G)$ for any $\beta \in \mathbb{F}_{q^m}$. It is clear that $\lambda_1 \in \mathbb{F}_{q^m}^*$ and $\lambda_i = 0$ for $2 \leqslant i \leqslant k$, which means $\psi(\beta \boldsymbol{g}_1)$ and $\psi(\boldsymbol{g}_1)$ are linearly dependent over $\mathbb{F}_{q^m}$. Then we can deduce that $(\psi(\beta), \psi(\alpha\beta)) = \lambda_1(\psi(1), \psi(\alpha))$ and furthermore $\psi(1)\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$. Let $\gamma = \frac{\psi(\alpha)}{\psi(1)}$, then

$$\psi(\alpha\beta) = \frac{\psi(\alpha)}{\psi(1)}\psi(\beta) = \gamma\psi(\beta).$$

Note that $\boldsymbol{a} = (1, \alpha, \ldots, \alpha^{m-1}) \in \mathbb{F}_{q^m}^m$ forms a basis vector of $\mathbb{F}_{q^m}/\mathbb{F}_q$, then we have

$$\psi(\alpha \boldsymbol{a}) = (\psi(\alpha), \ldots, \psi(\alpha^m)) = (\gamma\psi(1), \ldots, \gamma\psi(\alpha^{m-1})) = \gamma\psi(\boldsymbol{a}),$$

and furthermore $\psi(\alpha^i \boldsymbol{a}) = \gamma^i \psi(\boldsymbol{a})$ for $0 \leqslant i \leqslant m-1$. By Theorem 7, we have that ψ forms a fully linear transformation over $\mathbb{F}_{q^m}$.

□

The following corollary is derived immediately from Theorem 8.

Corollary 2. *Let m be a prime and $\mathcal{A}$ be defined as in Theorem 8. If there exists $\alpha \in \mathcal{A}$ such that $\alpha \notin \mathbb{F}_q$, then any $\mathbb{F}_q$-linear transformation ψ over $\mathbb{F}_{q^m}$ is fully linear as long as ψ is linear over $\mathcal{C}$.*

To describe exactly how much a linearized transformation disturbs the algebraic structure of linear codes, we introduce the concept of nonlinearity as follows.

Definition 9. Let $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$ and $A \in \mathcal{M}_{m,m}(\mathbb{F}_{q^m})$ be a matrix as defined in Theorem 7. The nonlinearity of ψ with extension degree m is defined as $\mathrm{NL}_m(\psi) = \frac{r}{m}$ where $r = \mathrm{Rank}(A)$.

A permutation of $\mathbb{F}_{q^m}$ leads to a polynomial of degree at most $q^m - 1$, which can be derived from the Lagrange Interpolation Formula [32]. An $\mathbb{F}_q$-linearized permutation ψ of $\mathbb{F}_{q^m}$ leads to a linearized polynomial $L_\psi(x)$ over $\mathbb{F}_{q^m}/\mathbb{F}_q$, which has the form of

$$\gamma_0 x + \gamma_1 x^{[1]} + \cdots + \gamma_{m-1} x^{[m-1]} \in \mathbb{F}_{q^m}[x].$$

Let $\boldsymbol{b}$ be a basis vector of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $B \in \mathcal{M}_{m,m}(\mathbb{F}_{q^m})$ a Moore matrix generated by $\boldsymbol{b}$. Note that $L_\psi(\boldsymbol{b}) = (\gamma_0, \ldots, \gamma_{m-1})B = \psi(\boldsymbol{b})$, then $(\gamma_0, \ldots, \gamma_{m-1}) = \psi(\boldsymbol{b})B^{-1}$.

The following proposition states a fact that one can figure out the nonlinearity of ψ directly from the coefficients of $L_\psi(x)$. Here by $\mathrm{wt}(\boldsymbol{v})$ we denote the Hamming weight of $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, namely the number of nonzero components of $\boldsymbol{v}$.

Proposition 5. *For any $\psi \in \mathrm{LP}_m(\mathbb{F}_q)$, let $L_\psi(x) = \sum_{i=0}^{m-1} \gamma_i x^{[i]}$ be the linearized permutation polynomial associated to ψ. Let $\boldsymbol{\gamma} = (\gamma_0, \ldots, \gamma_{m-1})$, then $\mathrm{NL}_m(\psi) = \frac{w}{m}$ where $w = \mathrm{wt}(\boldsymbol{\gamma})$.*

Proof. Let $w = \mathrm{wt}(\boldsymbol{\gamma})$, then there exist $0 \leqslant j_0 < \cdots < j_{w-1} \leqslant m-1$ such that $\gamma_{j_v} \neq 0$. Let $\boldsymbol{a} = (\alpha_0, \ldots, \alpha_{m-1})$ be a basis vector of $\mathbb{F}_{q^m}/\mathbb{F}_q$, and set

$$A = \begin{pmatrix} \alpha_0\alpha_0 & \alpha_0\alpha_1 & \cdots & \alpha_0\alpha_{m-1} \\ \alpha_1\alpha_0 & \alpha_1\alpha_1 & \cdots & \alpha_1\alpha_{m-1} \\ \vdots & \vdots & & \vdots \\ \alpha_{m-1}\alpha_0 & \alpha_{m-1}\alpha_1 & \cdots & \alpha_{m-1}\alpha_{m-1} \end{pmatrix} = \begin{pmatrix} \alpha_0\boldsymbol{a} \\ \alpha_1\boldsymbol{a} \\ \vdots \\ \alpha_{m-1}\boldsymbol{a} \end{pmatrix}.$$

Let $B = \psi(A)$, then

$$B = L_\psi(A) = \gamma_{j_0} A^{[j_0]} + \gamma_{j_1} A^{[j_1]} + \cdots + \gamma_{j_{w-1}} A^{[j_{w-1}]}.$$

It is easy to see that $\mathrm{Rank}(B) \leqslant w$ because of $\mathrm{Rank}(A^{[j_v]}) = 1$ for any $0 \leqslant v \leqslant w-1$. Let

$$\Lambda = \begin{pmatrix} \alpha_0^{[j_0]} & \alpha_0^{[j_1]} & \cdots & \alpha_0^{[j_{w-1}]} \\ \alpha_1^{[j_0]} & \alpha_1^{[j_1]} & \cdots & \alpha_1^{[j_{w-1}]} \\ \vdots & \vdots & & \vdots \\ \alpha_{m-1}^{[j_0]} & \alpha_{m-1}^{[j_1]} & \cdots & \alpha_{m-1}^{[j_{w-1}]} \end{pmatrix}.$$

It is clear that $\mathrm{Rank}(\Lambda) = w$, then there exist $1 \leqslant i_0 < \cdots < i_{w-1} \leqslant m$ such that the submatrix of Λ from the rows indexed by i_u is invertible. Let $I_u = \{i_0, \ldots, i_{w-1}\}$, then by Λ_{I_u} we denote the submatrix of Λ indexed by I_u, and B_{I_u} the submatrix of B respectively. Then

$$\Lambda_{I_u}^{-1} B_{I_u} = \gamma_{j_0} \Lambda_{I_u}^{-1} \begin{pmatrix} \alpha_{i_0}^{[j_0]} \boldsymbol{a}^{[j_0]} \\ \alpha_{i_1}^{[j_0]} \boldsymbol{a}^{[j_0]} \\ \vdots \\ \alpha_{i_{w-1}}^{[j_0]} \boldsymbol{a}^{[j_0]} \end{pmatrix} + \cdots + \gamma_{j_{w-1}} \Lambda_{I_u}^{-1} \begin{pmatrix} \alpha_{i_0}^{[j_{w-1}]} \boldsymbol{a}^{[j_{w-1}]} \\ \alpha_{i_1}^{[j_{w-1}]} \boldsymbol{a}^{[j_{w-1}]} \\ \vdots \\ \alpha_{i_{w-1}}^{[j_{w-1}]} \boldsymbol{a}^{[j_{w-1}]} \end{pmatrix} = \begin{pmatrix} \gamma_{j_0} \boldsymbol{a}^{[j_0]} \\ \gamma_{j_1} \boldsymbol{a}^{[j_1]} \\ \vdots \\ \gamma_{j_{w-1}} \boldsymbol{a}^{[j_{w-1}]} \end{pmatrix}.$$

It follows that $w = \mathrm{Rank}(\Lambda_{I_u}^{-1} B_{I_u}) \leqslant \mathrm{Rank}(B) \leqslant w$, which leads to the conclusion immediately. □

Remark 6. It is easy to see that ψ is fully linear if and only if the linearized permutation polynomial $L_\psi(x)$ induced by ψ has the form of $L_\psi(x) = \gamma x^{[i]}$ for some $\gamma \in \mathbb{F}_{q^m}^*$ and $0 \leqslant i \leqslant m-1$.

5 Our proposal

This section first presents a formal description of the new proposal, then gives some notes on the private key. It should be noted that the following description and notes are mainly aimed at the partial cyclic version.

5.1 Description of our proposal

For a desired security level, choose a field $\mathbb{F}_q$ and positive integers m, n, k, l, λ_1 and λ_2 such that $n = lm$. Let $\boldsymbol{g} = (\alpha^{[n-1]}, \alpha^{[n-2]}, \ldots, \alpha)$ be a normal basis vector of $\mathbb{F}_{q^n}/\mathbb{F}_q$ and $G = \mathrm{PC}_k(\boldsymbol{g}) \in \mathcal{M}_{k,n}(\mathbb{F}_{q^n})$. Let $\mathcal{G} = \langle G \rangle_{q^n}$ be an $[n, k]$ partial cyclic Gabidulin code. Our proposal consists of the following three procedures.

- Key generation

  For $i = 1, 2$, randomly choose an $\mathbb{F}_q$-linear space $\mathcal{V}_i \subseteq \mathbb{F}_{q^n}$ such that $\dim_q(\mathcal{V}_i) = \lambda_i$. Randomly choose $\boldsymbol{m}_i \in \mathcal{V}_i^n$ such that $\mathrm{rk}_q(\boldsymbol{m}_i) = \lambda_i$. Let $M_i = \mathrm{PC}_n(\boldsymbol{m}_i)$ and check whether M_i is invertible or not. If not, then rechoose $\boldsymbol{m}_i$. Randomly choose a linearized transformation ψ over $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ such that $\mathrm{NL}_l(\psi) \neq \frac{1}{l}$. Let $\boldsymbol{g}^* = \psi(\boldsymbol{g}M_1^{-1})M_2^{-1}$, then $\mathrm{PC}_k(\boldsymbol{g}^*) = \psi(GM_1^{-1})M_2^{-1}$. Let $t = \lfloor \frac{n-k}{2\lambda_1\lambda_2} \rfloor$, then the public key is published as $(\boldsymbol{g}^*, t)$, and the private key is $(\boldsymbol{m}_1, \boldsymbol{m}_2, \psi)$.

- Encryption

  For a plaintext $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$, randomly choose $\boldsymbol{e} \in \mathbb{F}_{q^n}^n$ with $\mathrm{rk}_q(\boldsymbol{e}) = t$. Then the ciphertext corresponding to $\boldsymbol{x}$ is computed as

  $$\boldsymbol{y} = \boldsymbol{x}\mathrm{PC}_k(\boldsymbol{g}^*) + \boldsymbol{e} = \boldsymbol{x}\psi(GM_1^{-1})M_2^{-1} + \boldsymbol{e}.$$

- Decryption

  For a ciphertext $\boldsymbol{y} \in \mathbb{F}_{q^n}^n$, compute

  $$\boldsymbol{y}M_2 = \boldsymbol{x}\psi(GM_1^{-1}) + \boldsymbol{e}M_2 = \psi(\boldsymbol{x}GM_1^{-1}) + \boldsymbol{e}M_2,$$

  and

  $$\boldsymbol{y}' = \psi^{-1}(\boldsymbol{y}M_2)M_1 = \boldsymbol{x}G + \boldsymbol{e}'$$

  where $\boldsymbol{e}' = \psi^{-1}(\boldsymbol{e}M_2)M_1$. Note that

  $$\mathrm{rk}_q(\boldsymbol{e}') \leqslant \mathrm{rk}_q(\psi^{-1}(\boldsymbol{e}M_2)) \cdot \lambda_1 = \mathrm{rk}_q(\boldsymbol{e}M_2) \cdot \lambda_1 \leqslant \mathrm{rk}_q(\boldsymbol{e}) \cdot \lambda_2 \cdot \lambda_1 \leqslant \lfloor \frac{n-k}{2} \rfloor.$$

  Applying the decoder of $\mathcal{G}$ to $\boldsymbol{y}'$ will lead to the plaintext $\boldsymbol{x}$.

Remark 7. For the case where no partial cyclic structure is used, the only difference is that it suffices to choose at random a generator matrix G of Gabidulin code and two matrices M_i with $\mathrm{rk}_q(M_i) = \lambda_i$. On the other hand, the design of the new proposal involves three finite fields, that is $\mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$. The reason why $\mathbb{F}_{q^m}$ is chosen to define ψ consists in two aspects. Specifically, if there is no such an intermediate field and ψ is defined over $\mathbb{F}_{q^n}/\mathbb{F}_q$, then the transformation will be $\mathbb{F}_q$-linearized and the plaintext has to be chosen from $\mathbb{F}_q^k$. Consequently, the practical security of this scheme will be bounded from above by $\mathcal{O}(q^k)$ and the transmission rate will be only $\frac{k}{n^2}$, which will greatly weaken the performance of the proposed scheme.

5.2 Why not hide Gabidulin code

Now we explain why Gabidulin code is not used as part of the private key. Firstly, we introduce the following proposition, which reveals the relationship between two normal basis vectors.

Proposition 6. *Let α be a normal element of $\mathbb{F}_{q^n}/\mathbb{F}_q$, then $\beta \in \mathbb{F}_{q^n}$ is normal if and only if there exists $Q \in \mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)$ such that*

$$(\beta^{[n-1]}, \beta^{[n-2]}, \ldots, \beta) = (\alpha^{[n-1]}, \alpha^{[n-2]}, \ldots, \alpha)Q.$$

Proof. The proof is trivial from a direct verification. □

Let $\boldsymbol{g}' \in \mathbb{F}_{q^n}^n$ be an arbitrary normal basis vector of $\mathbb{F}_{q^n}/\mathbb{F}_q$. By Proposition 6, there exists a matrix $Q \in \mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)$ such that $\boldsymbol{g}' = \boldsymbol{g}Q$. Let $G' = \mathrm{PC}_k(\boldsymbol{g}')$, then $G' = GQ$ and

$$\psi(GM_1^{-1})M_2^{-1} = \psi(G'Q^{-1}M_1^{-1})M_2^{-1} = \psi(G'M_1^{-1})Q^{-1}M_2^{-1} = \psi(G'M_1^{-1})M_2'^{-1},$$

where $M_2' = M_2Q \in \mathrm{PC}_n(\mathbb{F}_{q^n}) \cap \mathrm{GL}_n(\mathbb{F}_{q^n})$ satisfies $\mathrm{wt}_R(M_2') = \lambda_2$. Furthermore, it is clear that anyone possessing the knowledge of $\psi, \boldsymbol{g}', M_1$ and M_2' can decrypt any ciphertext in polynomial time. This implies that breaking this cryptosystem can be reduced to recovering ψ, M_1 and M_2'. Hence we conclude that it does not make a difference to keep the underlying Gabidulin code secret.

5.3 On the choice of ψ

We first explain why the secret transformation ψ cannot be fully linear over $\mathbb{F}_{q^n}$, then investigate the equivalence between different linearized transformations.

5.3.1 Why ψ cannot be fully linear

If ψ is fully linear over $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$, then by Remark 6 there exist $\gamma \in \mathbb{F}_{q^n}^*$ and $0 \leqslant j \leqslant l-1$ such that

$$\psi(GM_1^{-1}) = \gamma(GM_1^{-1})^{[mj]} = \gamma G^{[mj]}(M_1^{-1})^{[mj]} = \gamma G^{[mj]}(M_1^{[mj]})^{-1}.$$

It follows that

$$\psi(GM_1^{-1})M_2^{-1} = \gamma G^{[mj]}(M_1^{[mj]})^{-1}M_2^{-1} = G^{[mj]}(\gamma^{-1}M_2M_1^{[mj]})^{-1} = G'M'^{-1},$$

where $G' = G^{[mj]}$ and $M' = \gamma^{-1}M_2M_1^{[mj]}$. It is clear that $\mathrm{rk}_q(M') \leqslant \lambda_1\lambda_2$ and G' is a Moore matrix generated by $\boldsymbol{g}' = \boldsymbol{g}^{[mj]}$, a normal basis vector of $\mathbb{F}_{q^n}/\mathbb{F}_q$. This scheme then degenerates into an instance of Loidreau's proposal. In this situation, one can easily obtain $\boldsymbol{g}'$ by exhausting j because of l being quite small and $\boldsymbol{g}$ being publicly known, as explained in Section 5.2. By computing $\mathrm{PC}_n(\boldsymbol{g}^*)^{-1}\mathrm{PC}_n(\boldsymbol{g}')$ one can recover M' and therefore completely break this scheme.

5.3.2 Equivalence of ψ

For any $\beta \in \mathbb{F}_{q^n}^*$ and $\psi \in \mathrm{LP}_l(\mathbb{F}_{q^m})$, it is clear that $\beta\psi$ is also a linearized transformation, where $\beta\psi$ is defined by $\beta\psi(\alpha) = \beta \cdot \psi(\alpha)$ for any $\alpha \in \mathbb{F}_{q^n}$. Furthermore, let $\psi' = \beta\psi, M_2' = \beta M_2$, then $\mathrm{rk}_q(M_2') = \mathrm{rk}_q(M_2) = \lambda_2$ and

$$\psi(GM_1^{-1})M_2^{-1} = \beta^{-1}\psi'(GM_1^{-1})M_2^{-1} = \psi'(GM_1^{-1})(\beta M_2)^{-1} = \psi'(GM_1{}^{-1})M_2'^{-1}.$$

In terms of brute-force attack, ψ and ψ' are said to be equivalent. For any two transformations $\psi_1, \psi_2 \in \mathrm{LP}_l(\mathbb{F}_{q^m})$, we have either $\overline{\psi_1} = \overline{\psi_2}$ or $\overline{\psi_1} \cap \overline{\psi_2} = \varnothing$, where $\overline{\psi_i} = \{\beta\psi_i : \beta \in \mathbb{F}_{q^n}^*\}$.

Now we count the nonequivalent linearized transformations. By Proposition 3, the number of $\mathbb{F}_{q^m}$-linearized permutations of $\mathbb{F}_{q^n}$ is

$$|\mathrm{LP}_l(\mathbb{F}_{q^m})| = \prod_{i=0}^{l-1}(q^n - q^{mi}).$$

On the other hand, by Remark 6 the number of fully linear transformations over $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$ is $l(q^n - 1)$. Hence the number of nonequivalent linearized transformations is evaluated as

$$\mathcal{N}(\overline{\psi}) = \frac{|\mathrm{LP}_l(\mathbb{F}_{q^m})| - l(q^n - 1)}{q^n - 1} = \prod_{i=1}^{l-1}(q^n - q^{mi}) - l.$$

5.4 On the choice of $(\boldsymbol{m}_1, \boldsymbol{m}_2)$

In this section, we first investigate how to choose $(\boldsymbol{m}_1, \boldsymbol{m}_2)$ to avoid some structural weakness, then investigate the equivalence of $\boldsymbol{m}_1$.

5.4.1 How to choose $(\boldsymbol{m}_1, \boldsymbol{m}_2)$

Note that neither $\boldsymbol{m}_1$ nor $\boldsymbol{m}_2$ should be taken over $\mathbb{F}_{q^m}$, otherwise the proposed scheme will degenerate into a weak instance. This problem is investigated in the following two cases.

(1) If $\boldsymbol{m}_1 \in \mathbb{F}_{q^m}^n$, then $M_1, M_1^{-1} \in \mathrm{GL}_n(\mathbb{F}_{q^m})$. It follows that

$$\psi(GM_1^{-1})M_2^{-1} = \psi(G)M_1^{-1}M_2^{-1} = \psi(G)(M_1M_2)^{-1} = \psi(G)M^{-1},$$

where $M = M_1M_2$ satisfies $\mathrm{rk}_q(M) \leqslant \lambda_1\lambda_2$. A direct verification shows that, if one can recover ψ and M, then one can decrypt any ciphertext in polynomial time. Let $G'_{pub} = \mathrm{PC}_n(\boldsymbol{g}^*)$ and $G' = \mathrm{PC}_n(\boldsymbol{g})$, then it is clear that $G'_{pub} = \psi(G')M^{-1}$. If one can find ψ, then one can recover M by computing $G'_{pub}{}^{-1}\psi(G')$. This implies that breaking this cryptosystem can be reduced to finding the secret ψ.

(2) If $\boldsymbol{m}_2 \in \mathbb{F}_{q^m}^n$, then $M_2, M_2^{-1} \in \mathrm{GL}_n(\mathbb{F}_{q^m})$. It follows that

$$\psi(GM_1^{-1})M_2^{-1} = \psi(GM_1^{-1}M_2^{-1}) = \psi(GM^{-1}),$$

where $M = M_1M_2$ satisfies $\mathrm{rk}_q(M) \leqslant \lambda_1\lambda_2$. A direct verification shows that, one can decrypt any ciphertext with the knowledge of ψ, G and M. If one can find ψ, then one can recover GM^{-1} and hence M as explained above. This implies that breaking this cryptosystem can be reduced to finding the secret ψ.

5.4.2 Equivalence of $\boldsymbol{m}_1$

For $Q \in \mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)$, let $M_1' = M_1Q, M_2' = M_2Q$, then $\mathrm{rk}_q(M_1') = \mathrm{rk}_q(M_1), \mathrm{rk}_q(M_2') = \mathrm{rk}_q(M_2)$. It follows that

$$\psi(GM_1'^{-1})M_2^{-1} = \psi(GQ^{-1}M_1^{-1})M_2{}^{-1} = \psi(GM_1^{-1})Q^{-1}M_2^{-1} = \psi(GM_1{}^{-1})M_2'^{-1}.$$

In terms of brute-force attack on $\boldsymbol{m}_1$, it does not make a difference to multiply $\boldsymbol{m}_1$ with a matrix in $\mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)$. Let $\overline{\boldsymbol{m}}_1 = \{\boldsymbol{m}_1Q : Q \in \mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)\}$. In what follows, we count the number of nonequivalent $\overline{\boldsymbol{m}}_1$'s.

For a positive integer $\lambda < n$, let $\mathcal{V} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-space of dimension λ. For a matrix $M \in \mathrm{PC}_n(\mathcal{V}) \cap \mathrm{GL}_n(\mathcal{V})$ with $\mathrm{rk}_q(M) = \lambda$, assume that $M = \sum_{j=1}^{\lambda} \alpha_j A_j$, where α_j's form a basis of $\mathcal{V}$ over $\mathbb{F}_q$ and A_j's are nonzero matrices in $\mathrm{PC}_n(\mathbb{F}_q)$. Let $A \in \mathcal{M}_{\lambda,n}(\mathbb{F}_q)$ be a matrix whose j-th row is the first row of A_j, then A has full rank. Denote by $\mathcal{N}(A)$ the number of full-rank matrices in $\mathcal{M}_{\lambda,n}(\mathbb{F}_q)$, and by $\mathcal{N}(\mathcal{V})$ the number of λ-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. Then

$$\mathcal{N}(A) = \prod_{i=0}^{\lambda-1}(q^n - q^i) \text{ and } \mathcal{N}(\mathcal{V}) = \prod_{j=0}^{\lambda-1}\frac{q^n - q^j}{q^\lambda - q^j}.$$

The number of matrices $M \in \mathrm{PC}_n(\mathbb{F}_{q^n}) \cap \mathrm{GL}_n(\mathbb{F}_{q^n})$ with $\mathrm{rk}_q(M) = \lambda$ can be evaluated as

$$\mathcal{N}(M) = \mathcal{N}(\mathcal{V}) \cdot \mathcal{N}(A) \cdot \xi,$$

where

$$\xi = \frac{|\{M \in \mathrm{PC}_n(\mathcal{V}) \cap \mathrm{GL}_n(\mathcal{V}) : \mathrm{rk}_q(M) = \lambda\}|}{|\{M \in \mathrm{PC}_n(\mathcal{V}) : \mathrm{rk}_q(M) = \lambda\}|}.$$

As for ξ, we have the following proposition (see Appendix A for the proof).

Proposition 7. *If $q^\lambda - q^{\lambda-1} \geqslant 2n$, then $\xi \geqslant \frac{1}{2}$.*

Proposition 7 provides a sufficient condition for $\xi \geqslant \frac{1}{2}$. Actually, this inequality always holds according to our extensive experiments in MAGMA [11], even when the sufficient condition is not satisfied. Hence we suppose $\xi = \frac{1}{2}$ in practice. Finally, the number of nonequivalent $\overline{\boldsymbol{m}}_1$'s is evaluated as

$$\mathcal{N}(\overline{\boldsymbol{m}}_1) = \frac{\mathcal{N}(M_1)}{|\mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)|} \sim q^{(2\lambda_1-1)n}.$$

6 Security analysis

Attacks in code-based cryptography can be divided into two categories, namely the structural attacks and generic attacks. Structural attacks aim to recover the private key or an equivalent private key from the published information, with which one can decrypt any ciphertext in polynomial time. Generic attacks aim to recover the plaintext directly without knowing the private key. In what follows, we investigate the security of the new cryptosystem from these two aspects.

6.1 Structural attacks

This section mainly introduces some well-known structural attacks in rank-based cryptography and explains why our scheme can prevent these attacks.

6.1.1 Overbeck attack

The best known structural attacks on McEliece-type variants using Gabidulin codes are the Overbeck attack [44] and some of its derivations [28,40]. All these attacks are based on the fact that Gabidulin code contains a large subspace invariant under the Frobenius transformation. To prevent these attacks, Loidreau [34] proposed a cryptosystem that can be seen as a rank metric counterpart of the BBCRS cryptosystem [7] based on generalized Reed-Solomon (GRS) codes. In Loidreau's proposal, the secret code is disguised by right multiplying a matrix whose inverse has a small rank weight. This method of hiding information about the private key, as claimed by Loidreau, is able to resist the structural attacks mentioned above. A similar technique is applied in our proposal, which we believe can as well prevent these attacks.

6.1.2 Coggia-Couvreur attack

Coggia and Couvreur [14] presented an effective distinguisher for the Loidreau cryptosystem, and gave a practical key recovery attack for $\lambda = 2$ and the code rate being greater than $1/2$. Instead of operating the public code directly, the Coggia-Couvreur distinguisher considers the dual of the public code. Specifically, let $G_{pub} = GM^{-1}$ be the public matrix, where G is a generator matrix of an $[n, k]$ Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^N}$ and M is taken over a λ-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^N}$, where $N \geqslant n$. Let H be a parity-check matrix of $\mathcal{G}$, then $H_{pub} = HM^T$ forms a parity-check matrix of the public code $\mathcal{G}_{pub} = \langle G_{pub} \rangle_{q^N}$. As for $\mathcal{G}_{pub}^{\perp} = \langle H_{pub} \rangle_{q^N}$, the Coggia-Couvreur distinguisher states that the following equality holds with high probability

$$\dim_{q^N}(\mathcal{G}_{pub}^{\perp} + \mathcal{G}_{pub}^{\perp\,[1]} + \cdots + \mathcal{G}_{pub}^{\perp\,[\lambda]}) = \min\{n, \lambda(n-k) + \lambda\}.$$

However, for an $[n, k]$ random linear code $\mathcal{C}_{rand}$ over $\mathbb{F}_{q^N}$, the following equality holds with high probability

$$\dim_{q^N}(\mathcal{C}_{rand}^{\perp} + \mathcal{C}_{rand}^{\perp\,[1]} + \cdots + \mathcal{C}_{rand}^{\perp\,[\lambda]}) = \min\{n, (\lambda+1)(n-k)\}.$$

Now we explain why our scheme can prevent the Coggia-Couvreur attack. For simplicity, we consider the case of $l = 2$. Let $L(x) = \gamma_1 x + \gamma_2 x^{[m]} \in \mathbb{F}_{q^n}[x]$ be the linearized permutation polynomial associated to ψ, then

$$G_{pub} = \psi(GM_1^{-1})M_2^{-1} = (\gamma_1 GM_1^{-1} + \gamma_2 G^{[m]}(M_1^{-1})^{[m]})M_2^{-1}.$$

It is easy to see that there exists $Q \in \mathrm{PC}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)$ such that $G^{[m]} = GQ$, then

$$G_{pub} = G(\gamma_1 M_1^{-1} + \gamma_2 Q(M_1^{-1})^{[m]})M_2^{-1} = GM^{-1},$$

where $M = (\gamma_1 M_1^{-1} + \gamma_2 Q(M_1^{-1})^{[m]})^{-1} M_2$.

Although one can recover M directly by computing $\mathrm{PC}_n(\boldsymbol{g}^*)^{-1}\mathrm{PC}_n(\boldsymbol{g})$, it does not mean one can conduct decryption with the knowledge of G and M. This is because M appears quite random and $\mathrm{rk}_q(M)$ can be very large. For instance, we have run 1000 random tests for $q = 2, m = 50, n = 100$ and $\lambda_1 = \lambda_2 = 2$. It turned out that $\mathrm{rk}_q(M) \geqslant 86$ holds in all these tests. By the way, $\mathrm{rk}_q(M^{-1}) \geqslant 90$ holds in 1000 random tests. Consequently, $\mathrm{rk}_q(\boldsymbol{e}M)$ will be far beyond the error correcting capability of Gabidulin code and the dual of $\mathcal{G}_{pub} = \langle G_{pub} \rangle_{q^n}$ appears indistinguishable from random codes. Exactly, the following equality holds with high probability according to our experiments,

$$\dim_{q^n}(\mathcal{G}_{pub}^{\perp} + \mathcal{G}_{pub}^{\perp\,[1]} + \cdots + \mathcal{G}_{pub}^{\perp\,[\lambda]}) = \min\{n, (\lambda+1)(n-k)\}.$$

This convinces us that our proposal can prevent the Coggia-Couvreur attack. It is easy to see that the Coggia-Couvreur attack also does not work for the general case where no partial cyclic structure is used.

6.1.3 Loidreau attack

In a talk [35] at CBCrypto 2021, Loidreau proposed an attack to recover a decoder of the public code in the Loidreau cryptosystem with a complexity of $\mathcal{O}(((\lambda n+(n-k)^2)N)^\omega q^{(\lambda-1)N})$. With this decoder in hand, one can decrypt any ciphertext in polynomial time. Similar to the Coggia-Couvreur attack, this attack also operates the dual of the public code. However, an applicable condition for this attack is that the public matrix can be written as $G_{pub} = GM^{-1}$, where G is a generator matrix of Gabidulin code or its subcode and M has a small rank weight. Obviously the public matrix in our proposal does not satisfy this condition according to the analysis in Section 6.1.2, which implies that this attack does not work on our new cryptosystem.

6.1.4 A brute-force attack

Now we consider a potential brute-force attack against the duple $(\overline{\psi}, \overline{\boldsymbol{m}}_1)$. Notice that for any $\psi' \in \overline{\psi}, \boldsymbol{m}_1' \in \overline{\boldsymbol{m}}_1$, there exists $\boldsymbol{m}_2' \in \mathbb{F}_{q^n}^n$ with $\mathrm{rk}_q(\boldsymbol{m}_2') = \lambda_2$ such that $G_{pub} = \psi(G{M_1}^{-1})M_2^{-1} = \psi'(G{M_1'}^{-1})M_2'^{-1}$, where $M_1' = \mathrm{PC}_n(\boldsymbol{m}_1'), M_2' = \mathrm{PC}_n(\boldsymbol{m}_2')$. Let $G_{pub}' = \mathrm{PC}_n(\boldsymbol{g}^*), G' = \mathrm{PC}_n(\boldsymbol{g})$, then

$$G_{pub}' = \psi(G'M_1^{-1})M_2^{-1} = \psi'(G'M_1'^{-1})M_2'^{-1}.$$

This implies that one can compute $M_2' = {G_{pub}'}^{-1}\psi'(G'M_1'^{-1})$. Furthermore, a direct verification shows that one can decrypt any ciphertext with the knowledge of $\psi', \boldsymbol{m}_1', \boldsymbol{m}_2'$ and the public $\boldsymbol{g}$. Apparently the complexity of this brute-force attack by exhausting $(\overline{\psi}, \overline{\boldsymbol{m}}_1)$ is $\mathcal{O}(\mathcal{N}(\overline{\psi}) \cdot \mathcal{N}(\overline{\boldsymbol{m}}_1))$.

6.2 Generic attacks

A legitimate message receiver can always recover the plaintext in polynomial time, while an adversary without the private key has to deal with the underlying RSD problem presented in Section 3. Attacks that aim to recover the plaintext directly by solving the RSD problem are called generic attacks, the complexity of which only relates to the parameters of the cryptosystem. In what follows, we will show how to establish a connection between our proposal and the RSD problem.

Let $G_{pub} = \psi(GM_1^{-1})M_2^{-1} \in \mathcal{M}_{k,n}(\mathbb{F}_{q^n})$ be the public matrix, and $H_{pub} \in \mathcal{M}_{n-k,n}(\mathbb{F}_{q^n})$ a parity-check matrix of the public code $\mathcal{G}_{pub} = \langle G_{pub} \rangle_{q^n}$. Let $\boldsymbol{y} = \boldsymbol{x}G_{pub} + \boldsymbol{e}$ be the received ciphertext, then the syndrome of $\boldsymbol{y}$ with respect to H_{pub} can be computed as $\boldsymbol{s} = \boldsymbol{y}H_{pub}^T = \boldsymbol{e}H_{pub}^T$. By Definition 6, one obtains an RSD instance of parameters (q, n, n, k, t). Solving this RSD instance by the combinatorial attacks in Table 1 or the algebraic attacks in Table 2 will lead to the error vector $\boldsymbol{e}$, then one can recover the plaintext by solving the linear system $\boldsymbol{y} - \boldsymbol{e} = \boldsymbol{x}G_{pub}$.

7 Parameters and public key size

In this section, we consider the practical security of our proposal against the generic attacks presented in Section 3, as well as a brute-force attack against the duple $(\overline{\psi}, \overline{\boldsymbol{m}}_1)$ in Section 6.1.4, with a complexity of $\mathcal{O}(\mathcal{N}(\overline{\psi}) \cdot \mathcal{N}(\overline{\boldsymbol{m}}_1))$. The public key consists of a vector in $\mathbb{F}_{q^n}^n$, leading to a public key size of $n^2 \log_2(q)$ bits. In Table 3, we give some suggested parameters for the security of at least 128 bits, 192 bits, and 256 bits. After that, we compare the public key size with some other code-based cryptosystems in Table 5. It should be noted that, when considering the algebraic attacks in [8,9], the original parameters suggested in [30] should be updated. Specifically, the updated parameters and corresponding public key size are given in Table 4. It is clear that our proposal has an obvious advantage over other variants in public key representation.

Parameters							Public Key Size	Security
q	m	n	k	l	λ_1	λ_2		
2	55	110	54	2	2	2	1513	139
2	60	120	64	2	2	2	1800	198
2	72	144	72	2	2	2	2592	258

Table 3: Parameters and public key size (in bytes).

Parameters								Public Key Size	Security
q	m	n	k	λ_1	λ_2	r	t		
2	167	167	59	3	3	54	9	6973	129
2	194	194	86	3	3	54	9	9409	193
2	203	203	95	3	3	54	9	10303	265

Table 4: Updated parameters and public key size (in bytes) for LT19.

Security / Instance	128	192	256
Classic McEliece [3]	261120	524160	1044992
Loi17 [36]	34560		59136
LT19 [30]	6973	9409	10303
HQC [38]	2249	4522	7245
BIKE [4]	1541	3083	5122
RQC [1]	1834	2853	4090
Our proposal	1513	1800	2592

Table 5: Comparison on public key size (in bytes).

8 Conclusion

This paper has introduced the so-called linearized transformations over linear codes and presented a new McEliece-type public key encryption scheme based on Gabidulin codes. The innovation of this paper lies in using linearized transformations to hide the private key. Combining the technique of Loidreau's proposal, this new proposal can resist all the existing distinguisher-based attacks. When equipped with the partial cyclic structure, this scheme turns into one with no hidden structure and with a competitive public key size.

Acknowledgements This research is supported by the National Key Research and Development Program of China (Grant No. 2018YFA0704703), the National Natural Science Foundation of China (Grant No. 61971243), the Natural Science Foundation of Tianjin (20JCZDJC00610), and the Fundamental Research Funds for the Central Universities of China (Nankai University).

References

[1] Aguilar-Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bros, M., Couvreur, A., Deneuville, J.C., Gaborit, P., Zémor, G., Hauteville, A.: Rank quasi-cyclic (RQC). Second Round submission to NIST Post-Quantum Cryptography call (April 2020).

[2] Aguilar-Melchor, C., Blazy, O., Deneuville, J.-C., Gaborit, P., Zémor, G.: Efficient encryption from random quasi-cyclic codes. IEEE Trans. Inform. Theory 64(5), 3927–3943 (2018).

[3] Albrecht, M.R., Bernstein, D.J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C.J., Tomlinson, M., Wang, W.: Classic McEliece: conservative code-based cryptography. https://classic.mceliece.org/nist/mceliece-20201010.pdf. Accessed October 10, 2020.

[4] Aragon, N., Barreto, P.S., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T., Melchor, C.A., Misoczki, R., Persichetti, E., Sendrier, Tillich, J.-P., N., Vasseur, V., Zémor, G.: BIKE: bit flipping key encapsulation. https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf. Accessed October 10, 2020.

[5] Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.-P.: A new algorithm for solving the rank syndrome decoding problem. In: Proceedings of ISIT 2018, pp. 2421–2425. IEEE (2018).

[6] Augot, D., Finiasz, M.: A public key encryption scheme based on the polynomial reconstruction problem. In: Proceedings of EUROCRYPT 2003, LNCS vol. 2656, pp. 229–240. Springer (2003).

[7] Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani D.: Enhanced public key security for the McEliece cryptosystem. J. Cryptology 29(1), 1–27 (2016).

[8] Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.-P.: An algebraic attack on rank metric code-based cryptosystems. In: Proceedings of EUROCRYPT 2020, LNCS, vol. 12107, pp. 64–93. Springer (2020).

[9] Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.-P., Verbel, J.: Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In: Proceedings of ASIACRYPT 2020, LNCS, vol. 12491, pp. 507–536. Springer (2020).

[10] Berlekamp, E.R., McEliece, R.J., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory 24(3), 384–386 (1978).

[11] Bosma, W., Cannon, J., Playoust, C.: The MAGMA algebra system I: The user language. J. Symbolic Comput. 24 (3-4), 235–265 (1997).

[12] Bombar, M., Couvreur, A.: Decoding supercodes of Gabidulin codes and applications to cryptanalysis. In: Proceedings of PQCrypto 2021, LNCS, vol. 12841, pp. 3–22. Springer (2021).

[13] Chalkley, R.: Circulant matrices and algebraic equations. Math. Mag. 48(2), 73–80. Taylor & Francis (1975).

[14] Coggia, D., Couvreur, A.: On the security of a Loidreau rank metric code based encryption scheme. Des. Codes Cryptogr. 88(9), 1941–1957 (2020).

[15] Faure, C., Loidreau, P.: A new public-key cryptosystem based on the problem of reconstructing p-polynomials. In: Ytrehus, ∅. (Ed.): Proceedings of WCC 2005, LNCS, vol. 3969, pp. 30415. Springer (2006).

[16] Gabidulin, E.M.: Theory of codes with maximum rank distance. Prob. Peredachi Inf. 21(1), 3–16 (1985).

[17] Gabidulin, E.M.: Attacks and counter-attacks on the GPT public key cryptosystem. Des. Codes Cryptogr. 48(2), 171–177 (2008).

[18] Gabidulin, E.M., Ourivski, A.V., Honary, B., Ammar, B.: Reducible rank codes and their applications to cryptography. IEEE Trans. Inform. Theory 49(12), 3289–3293 (2003).

[19] Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their application in cryptology. In: Davies, D.W. (Ed.): Proceedings of EUROCRYPT 1991, LNCS, vol. 547, pp. 482–489. Springer (1991).

[20] Gabidulin, E.M., Rashwan, H., Honary, B.: On improving security of GPT cryptosystem. In: Proceedings of ISIT 2009, pp. 1110–1114. IEEE (2009)

[21] Gaborit, P., Otmani, A., Kalachi, H.T.: Polynomial-time key recovery attack on the Faure–Loidreau scheme based on Gabidulin codes. Des. Codes Cryptogr. 86(7),1391–1403 (2018).

[22] Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inf. Theory 62(2), 1006–1019 (2016).

[23] Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Inf. Theory 62(12), 7245–7252 (2016).

[24] Ghatak, A: Extending Coggia-Couvreur attack on Loidreau's rank-metric cryptosystem. Des. Codes Cryptogr. 90(1), 215–238 (2022).

[25] Gibson, K.: Severely denting the Gabidulin version of the McEliece public key cryptosystem. Des. Codes Cryptogr. 6(1), 37–45 (1995).

[26] Gibson, K.: The security of the Gabidulin public key cryptosystem. In: Proceedings of EUROCRYPT 1996, LNCS, vol. 1070, pp. 212–223. Springer (1996).

[27] Guo, W., Fu, F.-W.: Polynomial-time key recovery attack on the Lau-Tan cryptosystem based on Gabidulin codes. arXiv:2112.15466 [cs.IT] (2022).

[28] Horlemann-Trautmann, A.-L., Marshall, K., Rosenthal, J.: Extension of Overbeck's attack for Gabidulin-based cryptosystems. Des. Codes Cryptogr. 86(2), 319–340 (2018).

[29] Lau, T.S.C., Tan, C.H.: A new technique in rank metric code-based encryption. Cryptography 2(4), 32 (2018).

[30] Lau, T.S.C., Tan, C.H.: New rank codes based encryption scheme using partial circulant matrices. Des. Codes Cryptogr. 87(12), 2979–2999 (2019).

[31] Lavauzelle, J., Loidreau, P., Pham, B.-D.: RAMESSES, a rank metric encryption scheme with short keys. arXiv:1911.13119 [cs.CR] (2019).

[32] Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press (1997).

[33] Loidreau, P.: A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In: Ytrehus, ∅. (Ed.): Proceedings of WCC 2005, LNCS, vol. 3969, pp. 36–45. Springer (2005).

[34] Loidreau, P.: A new rank metric codes based encryption scheme. In: Lange, T., Takagi, T. (Eds.): Proceedings of PQCrypto 2017, LNCS, vol. 10346, pp. 3–17. Springer (2017).

[35] Loidreau, P.: Analysis of a rank metric codes based encryption scheme. https://drive.google.com/file/d/1FuMgqm0NfGMJOxaZyrIrI1OWn0UICwPo/view. Accessed July 1, 2021.

[36] Loidreau, P.: Analysis of a public-key encryption scheme based on distorted Gabidulin codes. https://www.wcc2022.uni-rostock.de/storages/uni-rostock/Tagungen/WCC2022/Papers/WCC_2022_paper_5.pdf Accessed July 1, 2022.

[37] McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Jet Propuls. Lab. DSN Progr. Rep. 42-44, 114–116 (1978).

[38] Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bos, J., Deneuville, J.-C., Dion, A., Gaborit, P., Lacan, J., Persichetti, E., Robert, J.-M., Véron, P., Zémor, G.: Hamming quasi-cyclic (HQC). http://pqc-hqc.org/doc/hqc-specification_2020-10-01.pdf. Accessed October 10, 2020.

[39] National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Post-quantum cryptography standardization (2017). https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization

[40] Otmani, A., Kalachi, H.T., Ndjeya, S.: Improved cryptanalysis of rank metric schemes based on Gabidulin codes. Des. Codes Cryptogr. 86(9), 1983–1996 (2018).

[41] Otmani, A., Tillich, J.-P., Dallot, L.: Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. Math. Comput. Sci. 3(2), 129–140 (2010).

[42] Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems Inform. Transm. 38(3), 237–246 (2002).

[43] Overbeck, R.: A new structural attack for GPT and variants. In: Proceedings of Mycrypt 2005, LNCS, vol. 3715, pp. 50–63. Springer (2005).

[44] Overbeck, R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptology 21(2), 280–301 (2008).

[45] Pham, B.-D., Loidreau, P.: An analysis of Coggia-Couvreur attack on Loidreau's rank-metric public-key encryption scheme in the general case. arXiv:2112.12445 [cs.CR] (2021).

[46] Rashwan H., Gabidulin, E.M., Honary, B.: Security of the GPT cryptosystem and its applications to cryptography. Secur. Commun. Netw. 4(8), 937–946 (2011).

[47] Renner, J., Puchinger, S., Wachter-Zeh, A.: LIGA: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. Des. Codes Cryptogr. 89(6), 1279–1319 (2021).

[48] Richter, G., Plass, S.: Error and erasure decoding of rank-codes with a modified Berlekamp-Massey algorithm. ITG FACHBERICHT, pp. 203–210 (2004).

A Proof of Proposition 7

Proof. For a λ-dimensional $\mathbb{F}_q$-linear space $\mathcal{V} \subseteq \mathbb{F}_{q^n}$, denote by $\mathcal{M}_\lambda(\mathcal{V})$ the set of all matrices with rank weight λ in $\mathrm{PC}_n(\mathcal{V})$. Let U be the set of all singular matrices in $\mathcal{M}_\lambda(\mathcal{V})$, and $V = \mathcal{M}_\lambda(\mathcal{V}) \cap \mathrm{GL}_n(\mathcal{V})$. In what follows, we will construct an injective mapping σ from U to V. First, we divide U into a certain number of subsets. For a matrix $M \in U$, let $\boldsymbol{m} = (m_0, m_1, \ldots, m_{n-1}) \in \mathcal{V}^n$ be the first row vector of M, namely $M = \mathrm{PC}_n(\boldsymbol{m})$. Let $\overline{M} = \{N \in U : M - N \text{ is a scalar matrix}\}$, a set of matrices in U whose first row resembles M at the last $n-1$ coordinates. Let $\boldsymbol{x} = (x, m_1, \ldots, m_{n-1})$, and $X = \mathrm{PC}_n(\boldsymbol{x})$. Denote by $f(x) \in \mathbb{F}_{q^n}[x]$ the determinant of X, then $f(x)$ is a polynomial of degree n. In the meanwhile, we have that $|\overline{M}|$ equals the number of roots of $f(x) = 0$ in $\mathcal{V}$, which indicates that $|\overline{M}| \leqslant n$. Let $\boldsymbol{m}^* = (m_1, \ldots, m_{n-1})$, then it is easy to see that $\mathrm{rk}_q(\boldsymbol{m}^*) \geqslant \lambda - 1$. Now we establish the mapping σ in the following two cases:

(1) $\mathrm{rk}_q(\boldsymbol{m}^*) = \lambda - 1$.

For a matrix $M_1 \in \overline{M}$, let $\boldsymbol{m}_1 = (\delta_1, \boldsymbol{m}^*)$ be the first row vector of M_1. Let $\mathcal{W} = \langle m_1, \ldots, m_{n-1} \rangle_q$, then $\dim_q(\mathcal{W}) = \lambda - 1$. Because of $q^\lambda - q^{\lambda-1} > n$, there exists $\delta_1' \in \mathcal{V} \backslash \mathcal{W}$ such that $f(\delta_1') \neq 0$, where $f(x)$ is defined as above. Let $\boldsymbol{m}_1' = (\delta_1', \boldsymbol{m}^*)$, then we have $M_1' = \mathrm{PC}_n(\boldsymbol{m}_1') \in \mathrm{GL}_n(\mathcal{V})$, and $\mathrm{rk}_q(\boldsymbol{m}_1') = \lambda$ in the meanwhile. We define $\sigma(M_1) = M_1'$.

For $2 \leqslant i \leqslant n$ and a matrix $M_i \in \overline{M} \backslash \{M_j\}_{j=1}^{i-1}$, if any, let $\boldsymbol{m}_i = (\delta_i, \boldsymbol{m}^*)$ be the first row vector of M_i. Because of $q^\lambda - q^{\lambda-1} - (i-1) > n$, there exists $\delta_i' \in \mathcal{V} \backslash (\mathcal{W} \cup \{\delta_j'\}_{j=1}^{i-1})$ such that $f(\delta_i') \neq 0$. Let $\boldsymbol{m}_i' = (\delta_i', \boldsymbol{m}^*)$, then we have $M_i' = \mathrm{PC}_n(\boldsymbol{m}_i') \in \mathrm{GL}_n(\mathcal{V})$, and $\mathrm{rk}_q(\boldsymbol{m}_i') = \lambda$ in the meanwhile. We define $\sigma(M_i) = M_i'$.

(2) $\mathrm{rk}_q(\boldsymbol{m}^*) = \lambda$.

For a matrix $M_1 \in \overline{M}$, let $\boldsymbol{m}_1 = (\delta_1, \boldsymbol{m}^*)$ be the first row vector of M_1. Because of $q^\lambda > n$, there exists $\delta_1' \in \mathcal{V}$ such that $f(\delta_1') \neq 0$, where $f(x)$ is defined as above. Let $\boldsymbol{m}_1' = (\delta_1', \boldsymbol{m}^*)$, then we have $M_1' = \mathrm{PC}_n(\boldsymbol{m}_1') \in \mathrm{GL}_n(\mathcal{V})$, and $\mathrm{rk}_q(\boldsymbol{m}_1') = \lambda$ in the meanwhile. We define $\sigma(M_1) = M_1'$.

For $2 \leqslant i \leqslant n$ and a matrix $M_i \in \overline{M} \backslash \{M_j\}_{j=1}^{i-1}$, if any, let $\boldsymbol{m}_i = (\delta_i, \boldsymbol{m}^*)$ be the first row vector of M_i. Because of $q^\lambda - (i-1) > n$, there exists $\delta_i' \in \mathcal{V} \backslash \{\delta_j'\}_{j=1}^{i-1}$ such that $f(\delta_i') \neq 0$. Let $\boldsymbol{m}_i' = (\delta_i', \boldsymbol{m}^*)$, then we have $M_i' = \mathrm{PC}_n(\boldsymbol{m}_i') \in \mathrm{GL}_n(\mathcal{V})$, and $\mathrm{rk}_q(\boldsymbol{m}_i') = \lambda$ in the meanwhile. We define $\sigma(M_i) = M_i'$.

It is easy to see that σ forms an injective mapping from U to V. Apparently $\sigma(U) = \{\sigma(M) : M \in U\} \subseteq V$, which implies that $|U| = |\sigma(U)| \leqslant |V|$. Together with $U \cap V = \varnothing$ and $\mathcal{M}_\lambda(\mathcal{V}) = U \cup V$, we have that

$$\xi = \sum_{\mathcal{V} \subseteq \mathbb{F}_{q^n}, \dim_q(\mathcal{V}) = \lambda} |V| \Big/ \sum_{\mathcal{V} \subseteq \mathbb{F}_{q^n}, \dim_q(\mathcal{V}) = \lambda} |\mathcal{M}_\lambda(\mathcal{V})| \geqslant \frac{1}{2}.$$

□