# Semilinear transformations in coding theory and their application to cryptography

Wenshuo Guo* and Fang-Wei Fu†

**Abstract**

This paper presents a brand-new idea of masking the algebraic structure of linear codes used in code-based cryptography. Specially, we introduce the so-called semilinear transformations in coding theory, make a thorough study on their algebraic properties and then creatively apply them to the construction of code-based cryptosystems. Note that $\mathbb{F}_{q^m}$ can be viewed as an $\mathbb{F}_q$-linear space of dimension $m$, a semilinear transformation $\varphi$ is therefore defined to be an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. After that, we impose this transformation to a linear code $\mathcal{C}$ over $\mathbb{F}_{q^m}$. Apparently $\varphi(\mathcal{C})$ forms an $\mathbb{F}_q$-linear space, but generally does not preserve the $\mathbb{F}_{q^m}$-linearity according to our analysis. Inspired by this observation, a new technique for masking the structure of linear codes is developed in this paper. Meanwhile, we endow the secret code with the so-called partial cyclic structure to make a reduction in public-key size. Compared to some other code-based cryptosystems, our proposal admits a much more compact representation of public keys. For instance, 1058 bytes are enough to reach the security of 256 bits, almost 1000 times smaller than that of the Classic McEliece entering the third round of the NIST PQC project.

## 1 Introduction

Over the past decades, post-quantum cryptography (PQC) have been drawing more and more attention from the cryptographic community. The most important advantage of PQC is their potential resistance against attacks from quantum computers. In post-quantum cryptography, cryptosystems based on coding theory are one of the most promising candidates. In addition to security in the future quantum era, these cryptosystems generally have fast encryption and decryption procedures. Code-based cryptography has quite a long history, nearly as old as RSA–one of the best known public-key cryptosystems. However, this family of cryptosystems have never been used in practical situations for the reason that they require large memory for public keys. For instance, the Classic McEliece [1] submitted to the NIST PQC project has a public-key size of 255 kilobytes for 128 bits security. To overcome this drawback, a variety of improvements for McEliece's original scheme [16] were proposed one after another. Generally these improvements can be divided into

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

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

two categories: one is to substitute Goppa codes used in the McEliece system with other families of codes endowed with special structures, the other is to use codes endowed with the rank metric. However, most of these invariants have been shown to be insecure against structural attacks.

The first cryptosystem based on rank metric codes, known as the GPT cryptosystem, was proposed by Gabidulin et al. in [2]. The main advantage of rank-based cryptosystems consists in their compact representation of public keys. For instance, 600 bytes are enough to reach the 100 bits security for the original GPT cryptosystem. After that, applying rank metric codes to the construction of cryptosystems became an important topic in code-based cryptography. Some of the representative variants based on Gabidulin codes can be found in [3–7]. Unfortunately, most of these invariants, including the original GPT cryptosystem, have been completely broken because of Gabidulin codes being highly structrued. Concretely, Gabidulin codes contain a large subspace invariant under the Frobenius transformation, which provids the feasibility for us to distinguish Gabidulin codes from general ones. Based on this observation, various structural attacks [24–28] on the GPT cryptosystem and some of their variants were designed. Apart from Gabidulin codes, another family of rank metric codes, known as the Low Rank Parity Check (LRPC) codes, and a probabilistic encryption scheme based on these codes were proposed in [8, 9]. Compared to Gabidulin codes, LRPC codes admit a weak algebraic structure. Encryption schemes based on these codes can therefore resist structural attacks designed for Gabidulin codes based cryptosystems. However, this type of cryptosystems generally have a decrypting failure rate, which can be used to devise a reaction attack [10] to recover the private key.

**Our contribution.** In the paper [11], Guo et al. claimed that $\varphi(\mathcal{C})$ does not preserve the $\mathbb{F}_{q^m}$-linearity with high probability according to their experiments on Magma, where $\varphi$ is an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$ and $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$. This inspires us to apply this kind of transformations to the construction of code-based cryptosystems. According to our analysis in the present paper, transformations that preserve the $\mathbb{F}_{q^m}$-linearity of all linear codes over $\mathbb{F}_{q^m}$ is indeed a composition of the Frobenius transformation and stretching transformation. An $\mathbb{F}_q$-linear transformation admitting this property is called a fully linear transformation over $\mathbb{F}_{q^m}$. Following this we give a sufficient and necessary condition for an $\mathbb{F}_q$-linear transformation being fully linear. Meanwhile we find that, in general cases, an $\mathbb{F}_q$-linear transformation preserving the $\mathbb{F}_{q^m}$-linearity is in fact fully linear. Note that the total number of $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$ is $\prod_{i=0}^{m-1}(q^m - q^i)$, while the total number of fully linear transformations is $m(q^m - 1)$ according to our analysis. This implies that a fully linear transformation occurs with extremely low probability when $q^m$ is large enough, which provides the feasibility for us to exploit this kind of transformations in code-based cryptography. To reduce the public-key size, we endow the underlying Gabidulin code with the partial cyclic structure.

The rest of this paper is organized as follows. Section 2 introduces some basic notations used throughout this paper, as well as definitions of Moore matrices and partial cyclic codes. Section 3 presents two hard problems in coding theory and some attacks on them that will be useful to estimate the security level of our proposal. In Section 4, we will introduce the concept of semilinear transformations, and investigate some of their algebraic properties. Section 5 is devoted to the description of our new proposal and some notes on the choice of secret keys, then we present the security analysis of our proposal in Section 6. After that, we give some suggested parameters for different security levels and make a comparison on public-key size with some other code-based cryptosystems in Section 7. And we will make a few concluding remarks in Section 8.

# 2 Preliminaries

In this section, we first introduce some notations used throughout this paper and recall some basic concepts in coding theory.

## 2.1 Notations and basic concepts

Let $\mathbb{F}_q$ a finite field of characteristic 2, and $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$ of degree $m$. A vector $\boldsymbol{a} \in \mathbb{F}_{q^m}^m$ is called a basis vector of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if components of $\boldsymbol{a}$ are linearly independent over $\mathbb{F}_q$. Particularly, we call $\alpha$ a polynomial element if $\boldsymbol{a} = (1, \alpha, \cdots, \alpha^{m-1})$ forms a basis vector of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and call $\alpha$ a normal element if $\boldsymbol{a} = (\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}})$ forms a basis vector of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For two positive integers $k$ and $n$, denote by $\mathcal{M}_{k,n}(\mathbb{F}_q)$ the space of all $k \times n$ matrices over $\mathbb{F}_q$, and by $GL_n(\mathbb{F}_q)$ the set of all invertible matrices in $\mathcal{M}_{n,n}(\mathbb{F}_q)$. For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_q)$, let $\langle M \rangle_q$ be the linear space spanned by rows of $M$ over $\mathbb{F}_q$.

A linear code $\mathcal{C}$ of length $n$ and dimension $k$ over $\mathbb{F}_{q^m}$ is a $k$-dimensional subspace of $\mathbb{F}_{q^m}^n$. The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is the orthogonal space of $\mathcal{C}$ under the usual inner product over $\mathbb{F}_{q^m}$. A matrix $G$ with full row rank is called a generator matrix of $\mathcal{C}$ if its row vectors form a basis of $\mathcal{C}$. A generator matrix $H$ of $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$. For a codeword $\boldsymbol{c} \in \mathcal{C}$, the Hamming support of $\boldsymbol{c}$, denoted by $\text{Supp}_H(\boldsymbol{c})$, is defined to be the set of coordinates of $\boldsymbol{c}$ at which the components are nonzero. The Hamming weight of $\boldsymbol{c}$, denoted by $\text{wt}_H(\boldsymbol{c})$, is the cardinality of $\text{Supp}_H(\boldsymbol{c})$. The minimum Hamming distance of $\mathcal{C}$ is defined as the minimum Hamming weight of nonzero codewords in $\mathcal{C}$. The rank support of $\boldsymbol{c}$, denoted by $\text{Supp}_R(\boldsymbol{c})$, is the linear space spanned by components of $\boldsymbol{c}$ over $\mathbb{F}_q$. The rank weight of $\boldsymbol{c}$, denoted by $\text{wt}_q(\boldsymbol{c})$, is the dimension of $\text{Supp}_R(\boldsymbol{c})$ over $\mathbb{F}_q$.

## 2.2 Gabidulin codes

Before presenting the definition of Gabidulin codes, we first introduce the concept of Moore matrices and some related results.

*Definition* 1 (Moore matrices). For a positive integer $i$, we introduce the notation $[i] = q^i$. With this notation, we define $\alpha^{[i]} = \alpha^{q^i}$ to be the $i$-th Frobenius power of $\alpha \in \mathbb{F}_{q^m}$. For a vector $\boldsymbol{g} = (g_1, \cdots, g_n) \in \mathbb{F}_{q^m}^n$, we define $\boldsymbol{g}^{[i]} = (g_1^{[i]}, \cdots, g_n^{[i]})$ to be the $i$-th Frobenius power of $\boldsymbol{g}$. A matrix $G \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ is called a Moore matrix generated by $\boldsymbol{g}$ if the $i$-th row vector of $G$ is exactly $\boldsymbol{g}^{[i-1]}$ for $1 \leqslant i \leqslant k$, namely we have

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}.$$

For an $[n, k]$ linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, the $i$-th Frobenius power of $\mathcal{C}$ is defined to be $\mathcal{C}^{[i]} = \{\boldsymbol{c}^{[i]} : \boldsymbol{c} \in \mathcal{C}\}$.

**Proposition 1.** *As for Moore matrices, we have the following statements.*

*(1) For two Moore matrices $A, B \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, apparently $A + B$ is also a Moore matrix.*

*(2) For a vector $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $\mathrm{wt}_q(\boldsymbol{a}) = s$, let $A \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ be a Moore matrix generated by $\boldsymbol{a}$. Then we have Rank$(A) = \min\{s, k\}$.*

*Definition* 2 (Gabidulin codes). For positive integers $k \leqslant n \leqslant m$, let $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{wt}_q(\boldsymbol{g}) = n$. Let $G \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ be the Moore matrix generated by $\boldsymbol{g}$, then an $[n, k]$ Gabidulin code $\mathcal{G}$ generated by $\boldsymbol{g}$ is defined to be the linear space $\langle G \rangle_{q^m}$.

Gabidulin codes can be seen as an analogue of GRS codes in the rank metric, both of which have pretty good algebraic structure. Similarly, Gabidulin codes are optimal in the rank metric, namely an $[n, k]$ Gabidulin code has minimum rank distance $d = n - k + 1$ [33] and can therefore correct up to $\lfloor \frac{n-k}{2} \rfloor$ rank errors.

## 2.3 Partial cyclic codes

In the paper [6], Lau et al. proposed the use of partial cyclic codes to shrink the public-key size in code-based cryptography. Now we formally introduce this family of codes and some related results.

*Definition* 3 (Partial circulant matrices). Let $\boldsymbol{m} = (m_0, \cdots, m_{n-1}) \in \mathbb{F}_q^n$. The circulant matrix $M \in \mathcal{M}_{n,n}(\mathbb{F}_q)$ generated by $\boldsymbol{m}$ is defined to be

$$M = \begin{pmatrix} m_0 & m_1 & \cdots & m_{n-1} \\ m_{n-1} & m_0 & \cdots & m_{n-2} \\ \vdots & \vdots & & \vdots \\ m_1 & m_2 & \cdots & m_0 \end{pmatrix}.$$

For a positive integer $k \leqslant n$, the $k \times n$ partial circulant matrix generated by $\boldsymbol{m}$ is defined to be the first $k$ rows of $M$. We denote by $\mathcal{P}_k(\boldsymbol{m})$ the partial circulant matrix with respect to $\boldsymbol{m}$, and by $\mathcal{P}_n(\boldsymbol{m})$ the circulant matrix particularly. Furthermore, we denote by $\mathcal{P}_n(\mathbb{F}_q)$ the set of all $n \times n$ circulant matrices over $\mathbb{F}_q$.

*Remark* 1. Chalkley in [23] proved that all circulant matrices over $\mathbb{F}_q$ form a commutative ring under matrix addition and multiplication. Following this, it is easy to see that for a $k \times n$ partial circulant matrix $A$ and a circulant matrix $B$ of order $n$, the product matrix $AB$ is also a $k \times n$ partial circulant matrix.

Since we will use an invertible circulant matrix as part of the secret key, it is necessary to make clear in what situation a circulant matrix is invertible and how many invertible circulant matrices of order $n \times n$ there will be over $\mathbb{F}_q$. The following two propositions first describe a necessary and sufficient condition for a circulant matrix being invertible, and then make an accurate estimation on the quantity of invertible circulant matrices over $\mathbb{F}_q$.

**Proposition 2.** *[21] For a vector $\boldsymbol{m} = (m_0, \cdots, m_{n-1}) \in \mathbb{F}_q^n$, we define $\boldsymbol{m}(x) = \sum_{i=0}^{n-1} m_i x^i \in \mathbb{F}_q[x]$. A sufficient and necessary condition for $\mathcal{P}_n(\boldsymbol{m})$ being invertible is $\gcd(\boldsymbol{m}(x), x^n - 1) = 1$.*

**Proposition 3.** *[22] For a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n$, let $g_1(x), \cdots, g_s(x) \in \mathbb{F}_q[x]$ be $s$ distinct irreducible factors of $f(x)$, namely we have $f(x) = \prod_{i=1}^{s} g_i(x)^{e_i}$ for some positive integers*

$e_1, \cdots, e_s$. *Let* $d_i = \deg(g_i(x))$ *for* $1 \leqslant i \leqslant s$*, the we have*

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

*where* $\Phi_q(f(x))$ *denotes the number of polynomials relatively prime to* $f(x)$ *of degree less than* $n$*.*

Now we introduce the concept of partial cyclic codes.

*Definition* 4 (Partial cyclic codes). For a vector $\boldsymbol{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$, let $G = \mathcal{P}_k(\boldsymbol{a})$ be the $k \times n$ partial circulant matrix generated by $\boldsymbol{a}$. An $[n, k]$ linear code $\mathcal{C}$ spanned by rows of $G$ over $\mathbb{F}_q$ is called a partial cyclic code.

*Remark* 2. For a basis vector $\boldsymbol{g} = (g^{[n-1]}, \cdots, g^{[1]}, g)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, let $G = \mathcal{P}_k(\boldsymbol{g})$ be the $k \times n$ partial matrix generated by $\boldsymbol{g}$. It is easy to verify that $G$ is a $k \times n$ Moore matrix. The linear code $\mathcal{G}$ generated by $G$ is called a partial cyclic Gabidulin code.

As for the total number of $[n, k]$ partial cyclic Gabidulin codes over $\mathbb{F}_{q^n}$, or equivalently the total number of normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we present the following proposition.

**Proposition 4.** *[22] Normal elements of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *are in one-to-one correspondence to circulant matrices in* $GL_n(\mathbb{F}_q)$*, which implies that the total number of normal elements of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *can be evaluated as* $\Phi_q(x^n - 1)$*.*

# 3 Hard problems in coding theory

*Definition* 5 (Syndrome Decoding (SD) Problem). Given positive integers $n, k$ and $t$, let $H$ be an $(n-k) \times n$ matrix over $\mathbb{F}_q$ and $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$. The SD problem with parameters $(q, n, k, t)$ is to find a vector $\boldsymbol{e} \in \mathbb{F}_q^n$ such that $\boldsymbol{s} = \boldsymbol{e}H^T$ and $\text{wt}_H(\boldsymbol{e}) = t$.

The SD problem, proved to be NP-complete by Berlekamp et al. in [15], plays a crucial role in both complexity theory and code-based cryptography. The NP-completeness implies that the best known algorithm of solving this problem requires exponential time. The first example of the SD problem being used in code-based cryptography is the McEliece cryptosystem [16] based on Goppa codes. A generalized version of this problem in the rank metric is the rank syndrome decoding problem defined as follows.

*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 $\mathbb{F}_{q^m}$ and $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$. The RSD problem with parameters $(q, m, n, k, t)$ is to find a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{s} = \boldsymbol{e}H^T$ and $\text{wt}_q(\boldsymbol{e}) = t$.

The RSD problem is an important issue in rank code-based cryptography, which has been used for designing cryptosystems since the proposal of the GPT cryptosystem [2] in 1991. However, the hardness of this problem had never been proved until the work in [14], where the authors gave a randomized reduction of the SD problem to the RSD problem.

Generally speaking, attacks on the RSD problem can be divided into two categories, namely the combinatorial attack and algebraic attack. The main idea of combinatorial attacks consists in solving a linear system obtained from the parity-check equation, whose unknowns are components of $e_i$ $(1 \leqslant i \leqslant n)$ with respect to a potential support of $\boldsymbol{e}$. Up to now, the best known combinatorial attacks can be found in [17, 19, 20], as summarized in Table 1.

| Attack | Complexity |
|---|---|
| [17] | $\mathcal{O}\left(\min\left\{m^3t^3q^{(t-1)(k+1)}, (k+t)^3t^3q^{(t-1)(m-t)}\right\}\right)$ |
| [19] | $\mathcal{O}\left((n-k)^3m^3q^{\min\left\{t\left\lceil\frac{mk}{n}\right\rceil,(t-1)\left\lceil\frac{m(k+1)}{n}\right\rceil\right\}}\right)$ |
| [20] | $\mathcal{O}\left((n-k)^3m^3q^{t\left\lceil\frac{m(k+1)}{n}\right\rceil-m}\right)$ |

Table 1: Best known combinatorial attacks on the RSD problem.

As for the algebraic attack, the main idea consists in converting an RSD instance into a quadratic system and then solving this system using algebraic approaches. Here in this paper, we mainly consider attacks proposed in [12,13,18,19], whose complexity and applicable condition are summarized in Table 2.

| Attack | Condition | Complexity |
|---|---|---|
| [19] | $\left\lceil\frac{(t+1)(k+1)-(n+1)}{t}\right\rceil \leqslant k$ | $\mathcal{O}\left(k^3t^3q^{t\left\lceil\frac{(t+1)(k+1)-(n+1)}{t}\right\rceil}\right)$ |
| [18] | | $\mathcal{O}\left(k^3m^3q^{t\left\lceil\frac{km}{n}\right\rceil}\right)$ |
| [12] | $m\binom{n-k-1}{t} \geqslant \binom{n}{t} - 1$ | $\mathcal{O}\left(m\binom{n-p-k-1}{t}\binom{n-p}{t}^{\omega-1}\right)$, where $\omega = 2.8$ and $p = \max\{p \in [n] : m\binom{n-i-k-1}{t} \geqslant \binom{n-i}{t} - 1\}$ |
| [13] | | $\mathcal{O}\left(\left(\frac{((m+n)t)^t}{t!}\right)^{\omega}\right)$ |
| [12] | $m\binom{n-k-1}{t} < \binom{n}{t} - 1$ | $\mathcal{O}\left(q^{at}m\binom{n-k-1}{t}\binom{n-a}{t}^{\omega-1}\right)$, where $a = \min\{a \in \mathbb{N} : m\binom{n-k-1}{t} \geqslant \binom{n-a}{t} - 1\}$ |
| [13] | | $\mathcal{O}\left(\left(\frac{((m+n)t)^{t+1}}{(t+1)!}\right)^{\omega}\right)$ |

Table 2: Best known algebraic attacks on the RSD problem.

# 4 Semilinear transformations

Note that $\mathbb{F}_{q^m}$ can be regarded as an $\mathbb{F}_q$-linear space of dimension $m$. Let $\boldsymbol{a} = (\alpha_1, \cdots, \alpha_m)$ and $\boldsymbol{b} = (\beta_1, \cdots, \beta_m)$ be two basis vectors of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We define an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$ as follows

$$\varphi(\alpha_1) = \beta_1, \cdots, \varphi(\alpha_m) = \beta_m.$$

This implies that for any $\alpha = \sum_{i=1}^m \lambda_i\alpha_i \in \mathbb{F}_{q^m}$ with $\lambda_i \in \mathbb{F}_q$, we have $\varphi(\alpha) = \sum_{i=1}^m \lambda_i\beta_i$. Furthermore, we introduce the following notations:

(1) For a vector $\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathbb{F}_{q^m}^n$, we define $\varphi(\boldsymbol{v}) = (\varphi(v_1), \cdots, \varphi(v_n))$;

(2) For a set $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$, we define $\varphi(\mathcal{V}) = \{\varphi(\boldsymbol{v}) : \boldsymbol{v} \in \mathcal{V}\}$;

(3) For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, we define $\varphi(M) = (\varphi(M_{ij}))$.

In the remaining part of this section, we will make a thorough study on this kind of transformations. Firstly, we introduce a basic fact about the $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$.

**Proposition 5.** *The total number of $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$ is*

$$\prod_{i=0}^{m-1}(q^m - q^i).$$

*Proof.* For a basis vector $\boldsymbol{a}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and an invertible matrix $A \in GL_m(\mathbb{F}_q)$, it is easy to see that $\boldsymbol{a}A$ is also a basis vector. On the contrary, let $\boldsymbol{b}$ be another basis vector, then there exists a unique $B \in GL_m(\mathbb{F}_q)$ such that $\boldsymbol{b} = \boldsymbol{a}B$. This enables us to conclude that, for a given basis vector $\boldsymbol{a}$, all the $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$ are in one-to-one correspondence to $GL_m(\mathbb{F}_q)$. By evaluating the cardinality of $GL_m(\mathbb{F}_q)$, we obtain the conclusion immediately. □

For a given vector $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$, a natural question is how the Hamming (rank) weight of $\boldsymbol{c}$ changes under the action of an $\mathbb{F}_q$-linear transformation $\varphi$. To answer this question, we introduce the following proposition.

**Proposition 6.** *An $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$ is an isometric transformation in both the Hamming metric and rank metric.*

*Proof.* Let $\alpha \in \mathbb{F}_{q^m}$ and $\varphi$ be an automorphism of $\mathbb{F}_{q^m}$, apparently we have $\varphi(\alpha) = 0$ if and only if $\alpha = 0$. Hence $\text{Supp}_H(\varphi(\boldsymbol{v})) = \text{Supp}_H(\boldsymbol{v})$ holds for any $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, which implies that $\text{wt}_H(\varphi(\boldsymbol{v})) = \text{wt}_H(\boldsymbol{v})$.

As for the rank metric, let $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ such that $\text{wt}_q(\boldsymbol{v}) = n$. If $\text{wt}_q(\varphi(\boldsymbol{v})) < n$, then there exists $\boldsymbol{b} \in \mathbb{F}_q^n \backslash \{\boldsymbol{o}\}$ such that $\varphi(\boldsymbol{v})\boldsymbol{b}^T = \varphi(\boldsymbol{v}\boldsymbol{b}^T) = 0$. Following this we have $\boldsymbol{v}\boldsymbol{b}^T = 0$, which conflicts with $\text{wt}_q(\boldsymbol{v}) = n$. More generally, let $\text{wt}_q(\boldsymbol{v}) = r < n$. Then there exist $\boldsymbol{v}^* \in \mathbb{F}_{q^m}^r$ with $\text{wt}_q(\boldsymbol{v}^*) = r$ and $Q \in GL_n(\mathbb{F}_q)$ such that $\boldsymbol{v} = (\boldsymbol{v}^* | \boldsymbol{o})Q$. Apparently we have $\varphi(\boldsymbol{v}) = (\varphi(\boldsymbol{v}^*)|\boldsymbol{o})Q$ and $\text{wt}_q(\varphi(\boldsymbol{v})) = \text{wt}_q(\varphi(\boldsymbol{v}^*)) = r$. □

For a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and an $\mathbb{F}_q$-linear automorphism $\varphi$ of $\mathbb{F}_{q^m}$, it is easy to see that $\varphi(\mathcal{C})$ is an $\mathbb{F}_q$-linear space, but generally no longer $\mathbb{F}_{q^m}$-linear. Formally, we classify the $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$ according to the following definition.

*Definition* 7. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $[n, k]$ linear code, and $\varphi$ be an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. If $\varphi(\mathcal{C})$ is also an $\mathbb{F}_{q^m}$-linear code, we say that $\varphi$ is linear on $\mathcal{C}$. Otherwise, we say that $\varphi$ is semilinear on $\mathcal{C}$. If $\varphi$ is linear on all linear codes over $\mathbb{F}_{q^m}$, we say that $\varphi$ is fully linear over $\mathbb{F}_{q^m}$. Otherwise, we say that $\varphi$ is semilinear over $\mathbb{F}_{q^m}$.

The following theorem provides a sufficient and necessary condition for $\varphi$ being fully linear over $\mathbb{F}_{q^m}$.

**Theorem 8.** *Let $\boldsymbol{a} = (\alpha_1, \cdots, \alpha_m)$ be a basis vector of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and $\varphi$ be an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. Let $A = [\varphi(\alpha_1\boldsymbol{a}), \cdots, \varphi(\alpha_m\boldsymbol{a})]^T$, then a sufficient and necessary condition for $\varphi$ being fully linear is that $A$ has rank* 1.

*Proof.* On the necessity aspect, assume that $\varphi$ is fully linear over $\mathbb{F}_{q^m}$. Let $\mathcal{C} = \langle \boldsymbol{a} \rangle_{q^m}$ be a linear code over $\mathbb{F}_{q^m}$, and $\boldsymbol{a}_i = \varphi(\alpha_i \boldsymbol{a})$ be the $i$-th row of $A$. Since $\varphi$ is linear on $\mathcal{C}$, there must be $\mu \boldsymbol{a}_i \in \varphi(\mathcal{C})$ for any $\mu \in \mathbb{F}_{q^m}$ and $1 \leqslant i \leqslant m$. This implies that there exists $\alpha \in \mathbb{F}_{q^m}$ such that $\mu \boldsymbol{a}_i = \varphi(\alpha \boldsymbol{a})$. Since components of $\boldsymbol{a}$ form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, there exists $\lambda_j \in \mathbb{F}_q$ $(1 \leqslant j \leqslant m)$ such that $\alpha = \sum_{j=1}^{m} \lambda_j \alpha_j$. Hence we have

$$\mu \boldsymbol{a}_i = \varphi(\alpha \boldsymbol{a}) = \varphi(\sum_{j=1}^{m} \lambda_j \alpha_j \boldsymbol{a}) = \sum_{j=1}^{m} \lambda_j \varphi(\alpha_j \boldsymbol{a}) = \sum_{j=1}^{m} \lambda_j \boldsymbol{a}_j.$$

Let $\mathcal{V}_i = \{\mu \boldsymbol{a}_i : \mu \in \mathbb{F}_{q^m}\}$ and $\mathcal{V} = \{\sum_{j=1}^{m} \lambda_j \boldsymbol{a}_j : \lambda_1, \cdots, \lambda_m \in \mathbb{F}_q\}$, apparently we have $\mathcal{V}_i \subseteq \mathcal{V}$. Note that $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ are linearly independent over $\mathbb{F}_q$, then we have $|\mathcal{V}_i| = |\mathcal{V}| = q^m$ and hence $\mathcal{V}_i = \mathcal{V}$. Particularly, we have $\boldsymbol{a}_j \in \mathcal{V}_i$ for any $1 \leqslant j \leqslant m$. This implies that $A$ has rank $1$ over $\mathbb{F}_{q^m}$.

On the sufficiency aspect, let $\mathcal{V}$ and $\mathcal{V}_i$ be defined as above. Note that $A$ has rank $1$ over $\mathbb{F}_{q^m}$, then for a fixed $\boldsymbol{a}_i$, there exists $\mu_j \in \mathbb{F}_{q^m}^*$ such that $\boldsymbol{a}_j = \mu_j \boldsymbol{a}_i$ for $1 \leqslant j \leqslant m$. This implies that $\mathcal{V} = \{\sum_{j=1}^{m} \lambda_j \mu_j \boldsymbol{a}_i : \lambda_j \in \mathbb{F}_q\}$. Apparently $\mathcal{V} \subseteq \mathcal{V}_i$, together with $|\mathcal{V}| = |\mathcal{V}_i|$ we have $\mathcal{V} = \mathcal{V}_i$. Hence for any $\mu \in \mathbb{F}_{q^m}$, there exist $\lambda_1, \cdots, \lambda_m \in \mathbb{F}_q$ such that $\mu \boldsymbol{a}_i = \sum_{j=1}^{m} \lambda_j \boldsymbol{a}_j$.

Let $\mathcal{C}$ be an arbitrary linear code over $\mathbb{F}_{q^m}^n$. For any $\boldsymbol{c} \in \varphi(\mathcal{C})$, there exists $\boldsymbol{u} \in \mathcal{C}$ such that $\boldsymbol{c} = \varphi(\boldsymbol{u})$. Furthermore, there exists $M \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\boldsymbol{u} = \boldsymbol{a}M$. Apparently we have

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

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

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

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 we have

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

because of $\boldsymbol{a}_j M \in \varphi(\mathcal{C})$ and $\varphi(\mathcal{C})$ being $\mathbb{F}_q$-linear. Furthermore, we have $\mu_1 \boldsymbol{c}_1 + \mu_2 \boldsymbol{c}_2 \in \varphi(\mathcal{C})$ for any $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \varphi(\mathcal{C})$ and $\mu_1, \mu_2 \in \mathbb{F}_{q^m}$. Following this we conclude that $\varphi(\mathcal{C})$ is $\mathbb{F}_{q^m}$-linear, and hence then $\varphi$ is fully linear over $\mathbb{F}_{q^m}$. □

The following theorem gives an accurate count of fully linear transformations over $\mathbb{F}_{q^m}$.

**Theorem 9.** *The total number of fully linear transformations over $\mathbb{F}_{q^m}$ is $m(q^m - 1)$.*

*Proof.* Let $\boldsymbol{a} = (1, \alpha, \cdots, \alpha^{m-1})$ be a basis vector of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and $\varphi$ be an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. By Theorem 8, a necessary condition for $\varphi$ being fully linear is that $\varphi(\alpha \boldsymbol{a}) = \gamma \varphi(\boldsymbol{a})$ or equivalently

$$(\varphi(\alpha), \varphi(\alpha^2), \cdots, \varphi(\alpha^m)) = \gamma(\varphi(1), \varphi(\alpha), \cdots, \varphi(\alpha^{m-1})) \tag{1}$$

holds for some $\gamma \in \mathbb{F}_{q^m}$. Assume that $\varphi(1) = \beta \in \mathbb{F}_{q^m}^*$, then we can deduce from (1) that

$$\varphi(\alpha^i) = \gamma \varphi(\alpha^{i-1}) = \gamma^i \beta \text{ for any } 1 \leqslant i \leqslant m.$$

Let $f(x) = x^m + \sum_{i=0}^{m-1} a_i x^i \in \mathbb{F}_q[x]$ be the minimal polynomial of $\alpha$, then we have

$$f(\alpha) = \alpha^m + \sum_{i=0}^{m-1} a_i \alpha^i = 0. \tag{2}$$

Because of $\varphi$ being $\mathbb{F}_q$-linear, applying $\varphi$ to both sides of (2) leads to the equation

$$\varphi(\alpha^m) + \sum_{i=0}^{m-1} a_i \varphi(\alpha^i) = \gamma^m \beta + \sum_{i=0}^{m-1} a_i \gamma^i \beta = 0.$$

This implies that $f(\gamma) = 0$, and there must be $\gamma = \alpha^{[i]}$ for some $0 \leqslant i \leqslant m-1$.

Moreover, it is easy to verify that $\varphi(\alpha^i \boldsymbol{a}) = \gamma^i \varphi(\boldsymbol{a})$ holds for any $1 \leqslant i \leqslant m-1$. By Theorem 8, with such a choice of $\gamma$ and $\beta$, $\varphi$ is fully linear over $\mathbb{F}_{q^m}$. Let $\Gamma = \{\alpha^{[i]} : 0 \leqslant i \leqslant m-1\}$, then all elements in $\Gamma \times \mathbb{F}_{q^m}^*$ are feasible for $\varphi$ being fully linear. Hence the total number of fully linear transformations over $\mathbb{F}_{q^m}$ is $m(q^m - 1)$. □

*Remark* 3. Let $\alpha$ be a polynomial element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and $\Gamma$ be the set of conjugates of $\alpha$. For any $\gamma \in \Gamma$ and $\beta \in \mathbb{F}_{q^m}^*$, the $\mathbb{F}_q$-linear transformation, determined by $\varphi(\alpha^i) = \beta\gamma^i$ for $0 \leqslant i \leqslant m-1$, forms a fully linear transformation over $\mathbb{F}_{q^m}$ according to Theorem 9. Note that $\gamma$ is a conjugate of $\alpha$, there exists $0 \leqslant j \leqslant m-1$ such that $\gamma = \alpha^{[j]}$. For any $\mu = \sum_{i=0}^{m-1} \lambda_i \alpha^i \in \mathbb{F}_{q^m}$ where $\lambda_i \in \mathbb{F}_q$, we have

$$\begin{aligned}\varphi(\mu) = \varphi(\sum_{i=0}^{m-1} \lambda_i \alpha^i) &= \sum_{i=0}^{m-1} \lambda_i \varphi(\alpha^i) = \sum_{i=0}^{m-1} \lambda_i \beta \gamma^i \\ &= \beta \sum_{i=0}^{m-1} \lambda_i (\alpha^{[j]})^i = \beta(\sum_{i=0}^{m-1} \lambda_i \alpha^i)^{[j]} = \beta \mu^{[j]}.\end{aligned}$$

This implies that a fully linear transformation over $\mathbb{F}_{q^m}$ can be seen as a composition of the Frobenius transformation and stretching transformation.

**Theorem 10.** *For two positive integers $k < n$, let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_{q^m}$. Let $G = [I_k | A]$ be a systematic generator matrix of $\mathcal{C}$, where $I_k$ is the $k \times k$ identity matrix and $A \in \mathcal{M}_{k,n-k}(\mathbb{F}_{q^m})$. Let $\mathcal{S} = \{A_{ij} : 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant n-k\}$, then we have the following statements.*

*(1) If $\mathcal{S} \subseteq \mathbb{F}_q$, then any $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$ is linear on $\mathcal{C}$. Furthermore, we have $\varphi(\mathcal{C}) = \mathcal{C}$;*

*(2) If there exists $\alpha \in \mathcal{S}$ such that $\alpha$ is a polynomial element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, then any $\mathbb{F}_q$-linear transformation $\varphi$ over $\mathbb{F}_{q^m}$ is fully linear if and only if $\varphi$ is linear on $\mathcal{C}$.*

*Proof.* (1) Let $\boldsymbol{g}_i$ be the $i$-th row of $G$, apparently we have $\varphi(\alpha \boldsymbol{g}_i) = \varphi(\alpha)\boldsymbol{g}_i$ for any $\alpha \in \mathbb{F}_{q^m}$. For any $\boldsymbol{c} \in \mathcal{C}$, there exists $\boldsymbol{x} = (x_1, \cdots, x_k) \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{c} = \boldsymbol{x}G$. Then we have

$$\varphi(\boldsymbol{c}) = \varphi(\boldsymbol{x}G) = \varphi(\sum_{i=1}^{k} x_i \boldsymbol{g}_i) = \sum_{i=1}^{k} \varphi(x_i \boldsymbol{g}_i) = \sum_{i=1}^{k} \varphi(x_i)\boldsymbol{g}_i \in \mathcal{C}.$$

By the definition of $\varphi(\mathcal{C})$, we have $\varphi(\mathcal{C}) \subseteq \mathcal{C}$. Together with $|\varphi(\mathcal{C})| = |\mathcal{C}|$, there will be $\varphi(\mathcal{C}) = \mathcal{C}$.

(2) The necessity is obvious, and it suffices to prove the sufficiency. Without loss of generality, we consider the first row of $G$ and assume that $\boldsymbol{g}_1 = (1, 0, \cdots, 0, \alpha, \star) \in \mathbb{F}_{q^m}^n$, 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 $\varphi$ is linear on $\mathcal{C}$, or equivalently $\varphi(\mathcal{C})$ is an $\mathbb{F}_{q^m}$-linear code that has $\varphi(G)$ as a generator matrix. For any $\beta \in \mathbb{F}_{q^m}$, it is easy to see that $\varphi(\boldsymbol{g}_1)$ and $\varphi(\beta\boldsymbol{g}_1)$ are linearly dependent over $\mathbb{F}_{q^m}$. Following this we have $\varphi(1)\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$, and then

$$\varphi(\alpha\beta) = \frac{\varphi(\alpha)}{\varphi(1)}\varphi(\beta) = \gamma\varphi(\beta),$$

where $\gamma = \frac{\varphi(\alpha)}{\varphi(1)}$. Because of $\alpha$ being a polynomial element, $\boldsymbol{a} = (1, \alpha, \cdots, \alpha^{m-1}) \in \mathbb{F}_{q^m}^m$ forms a basis vector of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Assume that $\varphi(\alpha^i) = \beta_i \in \mathbb{F}_{q^m}$ for $0 \leqslant i \leqslant m-1$, namely

$$\varphi(\boldsymbol{a}) = (\beta_0, \cdots, \beta_{m-1}).$$

Following this we have

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

and furthermore $\varphi(\alpha^i\boldsymbol{a}) = \gamma^i\varphi(\boldsymbol{a})$ for $0 \leqslant i \leqslant m-1$. By Theorem 8, we have that $\varphi$ forms a fully linear transformation over $\mathbb{F}_{q^m}$.

□

**Corollary 1.** *Let $m$ be a prime and $\mathbb{F}_{q^m}$ be the extension field of $\mathbb{F}_q$ of degree $m$, and $\mathcal{S}$ be defined as in Theorem 10. If there exists $\alpha \in \mathcal{S}$ such that $\alpha \notin \mathbb{F}_q$, then any $\mathbb{F}_q$-linear transformation $\varphi$ over $\mathbb{F}_{q^m}$ is fully linear as long as $\varphi$ is linear on $\mathcal{C}$.*

*Proof.* Note that $m$ is a prime, then any $\alpha \in \mathbb{F}_{q^m} \backslash \mathbb{F}_q$ is a polynomial element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Hence the conclusion is proved immediately from Theorem 10. □

# 5 Our proposal

## 5.1 Description of the cryptosystem

For a given security level, choose positive integers $m, n, k$ such that $n = 2m$ and $k = am + b$, where $1 < a < 2$ and $0 \leqslant b < (2-a)m$. Let $\boldsymbol{g} = (g^{[n-1]}, \cdots, g^{[1]}, g) \in \mathbb{F}_{q^n}^n$ be a basis vector of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $G = \mathcal{P}_k(\boldsymbol{g}) \in \mathcal{M}_{k,n}(\mathbb{F}_{q^n})$ be a partial circulant matrix. Let $\mathcal{G} = \langle G \rangle_{q^n}$ be the $[n, k]$ partial cyclic Gabidulin code over $\mathbb{F}_{q^n}$ generated by $\boldsymbol{g}$. Randomly choose an $\mathbb{F}_{q^m}$-linear transformation $\varphi$ over $\mathbb{F}_{q^n}$ such that $\varphi$ is not fully linear. Now we introduce the cryptosystem with the following three procedures.

- Key generation

  Randomly choose a vector $\boldsymbol{m} \in \mathbb{F}_{q^n}^n$ such that $\mathrm{wt}_{q^m}(\boldsymbol{m}) = 2$ and $\boldsymbol{m}(x)$ is coprime to $x^n - 1$. Let $M = \mathcal{P}_n(\boldsymbol{m}) \in GL_n(\mathbb{F}_{q^n})$ and compute $\varphi(GM)\varphi(M)^{-1} = \mathcal{P}_k(\boldsymbol{g}')$, where $\boldsymbol{g}' = \varphi(\boldsymbol{g}M)\varphi(M)^{-1}$. We publish $(\boldsymbol{g}', t)$ as the public key where $t = \lfloor \frac{n-k}{2} \rfloor$, and keep $(\boldsymbol{g}, \boldsymbol{m}, \varphi)$ as the secret key.

- Encryption

  For a plaintext $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$, randomly choose a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{wt}_q(\boldsymbol{e}) = t$. The ciphertext corresponding to $\boldsymbol{x}$ is computed as $\boldsymbol{y} = \boldsymbol{x}\mathcal{P}_k(\boldsymbol{g}') + \boldsymbol{e}$.

- Decryption

  With the knowledge of $\boldsymbol{g}$ and $\boldsymbol{m}$, we can recover $G$ and $M$. Let $\boldsymbol{y}$ be a valid ciphertext, then we compute
  $$\boldsymbol{y}\varphi(M) = \boldsymbol{x}\varphi(GM) + \boldsymbol{e}\varphi(M) = \varphi(\boldsymbol{x}GM + \boldsymbol{e}M),$$
  and
  $$\boldsymbol{y}' = \varphi^{-1}(\boldsymbol{y}\varphi(M))M^{-1} = \boldsymbol{x}G + \boldsymbol{e}.$$
  Since $\mathrm{wt}_q(\boldsymbol{e}) \leqslant t$, applying the fast decoder of $\mathcal{G}$ to $\boldsymbol{y}'$ reveals the error vector $\boldsymbol{e}$. Then we can recover $\boldsymbol{x}$ by solving the linear system $\boldsymbol{x}G = \boldsymbol{y}' - \boldsymbol{e}$ with $\mathcal{O}(n^3)$ operations in $\mathbb{F}_{q^n}$.

## 5.2 On the choice of $\varphi$

At first, we explain why the secret transformation $\varphi$ cannot be fully linear. Suppose $\varphi$ is fully linear over $\mathbb{F}_{q^n}$, then by Remark 3 there exist $\beta \in \mathbb{F}_{q^n}^*$ and $j \in \{0, 1\}$ such that

$$\varphi(GM) = \beta(GM)^{[j]} = \beta G^{[j]} M^{[j]}.$$

Following this we have

$$\varphi(GM)\varphi(M)^{-1} = \beta G^{[j]} M^{[j]} \cdot (\beta M^{[j]})^{-1} = G^{[j]}.$$

By Remark 2, $G^{[j]}$ generates an $[n, k]$ partial cyclic Gabidulin code. Apparently an adversary can decrypt any valid ciphertext with the knowledge of $G^{[j]}$, which means that the cryptosystem will be completely broken. Hence the cryptosystem is insecure in the case of $\varphi$ being fully linear over $\mathbb{F}_{q^n}$.

According to our experiments on Magma, the systematic form of $GM$ always has entries belonging to $\mathbb{F}_{q^n} \backslash \mathbb{F}_{q^m}$. Because of Corollary 1, an $\mathbb{F}_{q^m}$-linear transformation $\varphi$ linear on $\langle GM \rangle_{q^n}$ will be fully linear over $\mathbb{F}_{q^n}$ with extremely high probability. By Proposition 5, the total number of $\mathbb{F}_{q^m}$-linear transformations over $\mathbb{F}_{q^n}$ can be computed as $(q^n - 1)(q^n - q^m)$. By Theorem 9, the total number of fully linear transformations over $\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_{q^m}$ is $2(q^n - 1)$. Hence the total number of $\mathbb{F}_{q^m}$-linear transformations optional for our proposal is $(q^n - 1)(q^n - q^m) - 2(q^n - 1)$. The probability that a random choice of $\mathbb{F}_{q^m}$-linear automorphisms of $\mathbb{F}_{q^n}$ happens to be the secret transformation is evaluated as

$$\frac{1}{(q^n - 1)(q^n - q^m) - 2(q^n - 1)} \approx \frac{1}{q^{2n}}.$$

This implies that the complexity of recovering the secret transformation through the exhaustion method is $\mathcal{O}(q^{2n})$.

## 5.3 On the choice of $\boldsymbol{m}$

In this section, we first discuss how to choose the secret $\boldsymbol{m}$ to avoid some potential attack. For a random $\boldsymbol{m} \in \mathbb{F}_{q^n}^n$, let $\boldsymbol{m}' = \varphi(\boldsymbol{m})$ and $r = \mathrm{wt}_{q^m}(\boldsymbol{m}) = \mathrm{wt}_{q^m}(\boldsymbol{m}')$, then there must be $r = 1$ or $r = 2$. Now we divide this problem into the following two cases.

**Case 1:** $r = 1$. There exists $a \in \mathbb{F}_{q^n}$ and $\boldsymbol{m}_s \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{m} = a\boldsymbol{m}_s$. Let $M_s = \mathcal{P}_n(\boldsymbol{m}_s)$, then $M = \mathcal{P}_n(\boldsymbol{m}) = a\mathcal{P}_n(\boldsymbol{m}_s) = aM_s$. Suppose that $\alpha = \varphi(a)$ for some $\alpha \in \mathbb{F}_{q^n}$, then we have

$$\varphi(M) = \varphi(aM_s) = \varphi(a)M_s = \alpha M_s.$$

Following this we have $\varphi(GM) = \varphi(aGM_s) = \varphi(aG)M_s$, then the public matrix

$$\varphi(GM)\varphi(M)^{-1} = \varphi(aG)M_s \cdot (\alpha M_s)^{-1} = \alpha^{-1}\varphi(aG).$$

Apparently this yields a degenerated instance, which we think may cause some unknown structural vulnerability to the new proposal. For instance, suppose one has obtained the secret transformation $\varphi$ with some method, then one can recover $\alpha$ and $G$ by checking every possible $a \in \mathbb{F}_{q^n}^*$. After that, the adversary would be able to decrypt any ciphertext in polynomial time. The complexity of the brute-force attack is apparently bounded from above by $\mathcal{O}(q^n)$.

**Case 2:** $r = 2$. Let $\boldsymbol{a} = (a_1, a_2) \in \mathbb{F}_{q^n}^2$ be a basis vector of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^m}$, then there exists $M_s \in \mathcal{M}_{2,n}(\mathbb{F}_{q^m})$ such that $\boldsymbol{m} = \boldsymbol{a}M_s$. Let

$$D_{\boldsymbol{a}} = \big(a_1 I_n | a_2 I_n\big) \in \mathcal{M}_{n,2n}(\mathbb{F}_{q^n}) \text{ and } M_S = \begin{pmatrix} M_s^{(1)} \\ M_s^{(2)} \end{pmatrix} \in \mathcal{M}_{2n,n}(\mathbb{F}_{q^m}),$$

where $M_s^{(i)}$ is a circulant matrix generated by the $i$-th row vector of $M_s$. Then we have

$$M = \mathcal{P}_n(\boldsymbol{m}) = \mathcal{P}_n(\boldsymbol{a}M_s) = a_1 M_s^{(1)} + a_2 M_s^{(2)} = D_{\boldsymbol{a}} M_S,$$

and

$$\varphi(GM) = \varphi(GD_{\boldsymbol{a}}M_S) = \varphi(GD_{\boldsymbol{a}})M_S = \varphi\left(a_1 G | a_2 G\right) M_S.$$

Following this we have that the public matrix

$$\varphi(GM)\varphi(M)^{-1} = \varphi\left(a_1 G | a_2 G\right) M_S \varphi(M)^{-1}.$$

It is easy to see that $M_S\varphi(M)^{-1}$ consists of two circulant matrices joined vertically, and meanwhile we have $\big(\varphi(a_1)I_n | \varphi(a_2)I_n\big) M_S\varphi(M)^{-1} = I_n$. According to our experiments on Magma, different $\boldsymbol{m}$ always leads to different $M_S\varphi(M)^{-1}$. Hence it is reasonable to conclude that choosing $\boldsymbol{m}$ such that $\mathrm{wt}_{q^m}(\boldsymbol{m}) = 2$ is a better choice than $\mathrm{wt}_{q^m}(\boldsymbol{m}) = 1$.

**Further discussion on $\boldsymbol{m}$.** An observation on $\boldsymbol{m}$ is that for fixed $\boldsymbol{g}$ and $\varphi$, different choices of $\boldsymbol{m}$ may result in the same public key. For a secret $\boldsymbol{m} \in \mathbb{F}_{q^n}^n$ and an invertible $Q \in \mathcal{P}_n(\mathbb{F}_{q^m})$, there exists $\boldsymbol{m}_0 \in \mathbb{F}_{q^n}^n$ such that $\boldsymbol{m} = \boldsymbol{m}_0 Q$. Let $M = \mathcal{P}_n(\boldsymbol{m})$ and $M_0 = \mathcal{P}_n(\boldsymbol{m}_0)$, then we have $M = M_0 Q$ and

$$\varphi(GM)\varphi(M)^{-1} = \varphi(GM_0)Q \cdot (\varphi(M_0)Q)^{-1} = \varphi(GM_0)\varphi(M_0)^{-1}.$$

We say that $\boldsymbol{m}_0$ and $\boldsymbol{m}$ are equivalent if there exists $Q \in \mathcal{P}_n(\mathbb{F}_{q^m}) \cap GL_n(\mathbb{F}_{q^m})$ such that $\boldsymbol{m} = \boldsymbol{m}_0 Q$. Let $\overline{\boldsymbol{m}} = \{\boldsymbol{m}Q : Q \in \mathcal{P}_n(\mathbb{F}_{q^m}) \cap GL_n(\mathbb{F}_{q^m})\}$, called the equivalent class of $\boldsymbol{m}$. For any two vectors $\boldsymbol{m}_1, \boldsymbol{m}_2 \in \mathbb{F}_{q^n}^n$, apparently we have either $\overline{\boldsymbol{m}_1} = \overline{\boldsymbol{m}_2}$ or $\overline{\boldsymbol{m}_1} \cap \overline{\boldsymbol{m}_2} = \varnothing$. In practical situation, therefore, it is the quantity of nonequivalent $\boldsymbol{m}$ that really matters in terms of security. As for the quantity of nonequivalent $\boldsymbol{m}$, we have the following proposition.

**Proposition 7.** *Let*

$$\mathcal{N}(\overline{\boldsymbol{m}}) = |\{\overline{\boldsymbol{m}} : \boldsymbol{m} \in \mathbb{F}_{q^n}^n \text{ such that } \mathrm{wt}_{q^m}(\boldsymbol{m}) = 2 \text{ and } \mathcal{P}_n(\boldsymbol{m}) \in GL_n(\mathbb{F}_{q^n})\}|,$$

*then we have*

$$\mathcal{N}(\overline{\boldsymbol{m}}) = \frac{|S_1|}{|S_2|} - q^m - 1,$$

*where*

$$S_1 = \{\boldsymbol{m} \in \mathbb{F}_{q^n}^n : \mathcal{P}_n(\boldsymbol{m}) \in GL_n(\mathbb{F}_{q^n})\}$$

*and*

$$S_2 = \{\boldsymbol{m} \in \mathbb{F}_{q^m}^n : \mathcal{P}_n(\boldsymbol{m}) \in GL_n(\mathbb{F}_{q^m})\}.$$

*Proof.* Let $S_0 = \{\boldsymbol{m} \in \mathbb{F}_{q^n}^n : \mathrm{wt}_{q^m}(\boldsymbol{m}) = 1 \text{ and } \mathcal{P}_n(\boldsymbol{m}) \in GL_n(\mathbb{F}_{q^n})\}$, then we have $\mathcal{N}(\overline{\boldsymbol{m}}) = \frac{|S_1|-|S_0|}{|S_2|}$. It remains to estimate the value of $|S_0|$. It is easy to see that $\mathbb{F}_{q^m}^*$ forms a normal subgroup of $\mathbb{F}_{q^n}^*$. Denote by $\mathcal{R}$ the set of representatives of the quotient group $\mathbb{F}_{q^n}^* \backslash \mathbb{F}_{q^m}^*$, apparently $|\mathcal{R}| = \frac{q^n-1}{q^m-1} = q^m + 1$. For any $\boldsymbol{m} \in S_0$, there exist $\alpha \in \mathcal{R}$ and $\boldsymbol{m}_s \in S_2$ such that $\boldsymbol{m} = \alpha \boldsymbol{m}_s$. Furthermore, we have that there exists a one-to-one correspondence between $S_0$ and the Cartesian product $\mathcal{R} \times S_2$. Hence we have

$$|S_0| = |\mathcal{R}| \cdot |S_2| = (q^m + 1)|S_2|,$$

which yields the conclusion immediately. □

# 6 Security analysis

## 6.1 Existing structural attacks

Since Gabidulin et al. exploited Gabidulin codes in the design of cryptosystems, many variants based on these codes have been proposed one after another. Unfortunately, almost all of these cryptosystems were completely broken due to the inherent structural vulnerability of Gabidulin codes. The best known structural attacks are the one proposed by Overbeck in [24] and some of its derivations [25,26]. In this section, we will present the principle of this type of attacks and give an explanation of why our proposal can resist these attacks.

In Section 2, we have introduced the concept of Frobenius transformations. It is not difficult to see that Gabidulin codes keep a large subspace invariant under the Frobenius transformation. Formally, we introduce the following propositions without proving. These propositions provide us with a method of distinguishing Gabidulin codes from general ones.

**Proposition 8.** *Let $\mathcal{G} \subseteq \mathbb{F}_{q^n}^N$ be an $[N, K]$ Gabidulin code. In terms of the intersection of $\mathcal{G}$ and its Frobenius power $\mathcal{G}^{[1]}$, we have*

$$\dim(\mathcal{G} \cap \mathcal{G}^{[1]}) = K - 1.$$

**Proposition 9.** *Let $\mathcal{G} \subseteq \mathbb{F}_{q^n}^N$ be an $[N, K]$ Gabidulin code. For any positive integer $i$, the following equality holds*

$$\dim(\mathcal{G} + \mathcal{G}^{[1]} + \cdots + \mathcal{G}^{[i]}) = \min\{N, K + i\}.$$

**Proposition 10.** *[27] Let $\mathcal{C} \subseteq \mathbb{F}_{q^n}^N$ be an $[N, K]$ random linear code. For any positive integer $i$, the following equality holds with high probability*

$$\dim(\mathcal{C} + \mathcal{C}^{[1]} + \cdots + \mathcal{C}^{[i]}) = \min\{N, K(i + 1)\}.$$

In our proposal, we adopt two approaches to disguise the structure of Gabidulin codes. First we choose an invertible circulant matrix $M$ to perform a column-mixing transformation to columns of $G$. Note that entries of $M$ are taken from the extension field $\mathbb{F}_{q^n}$, the linear code $\langle GM \rangle_{q^n}$ is no longer a Gabidulin code in general. As a matter of fact,

$$\dim(\langle GM \rangle_{q^n} \cap \langle GM \rangle_{q^n}^{[1]}) = 2k - n \text{ and } \dim(\langle GM \rangle_{q^n} + \langle GM \rangle_{q^n}^{[1]}) = n$$

hold with extremely high probability according to our experiments on Magma. In other words, the linear code generated by $GM$ behaves more like a random code than a Gabidulin code. However, it is not enough to mask the secret Gabidulin code. This is because the total number of $[n, k]$ partial cyclic Gabidulin codes over $\mathbb{F}_{q^n}$ is bounded from above by $q^n$. It seems feasible to recover the generator vector $\boldsymbol{g}$ through the exhaustion method when $q^n$ is not large enough, and then one can recover $M$ by computing $\mathcal{P}_n(\boldsymbol{g})^{-1}\mathcal{P}_n(\boldsymbol{g}')$, where $\boldsymbol{g}'$ denotes the first row vector of $GM$. To avoid this potential weakness, we randomly choose an $\mathbb{F}_{q^m}$-linear transformation $\varphi$ to further distort the linear code $\langle GM \rangle_{q^n}$. According to our analysis, the transformed code is generally no longer $\mathbb{F}_{q^n}$-linear when $\varphi$ is not fully linear. General $\mathbb{F}_{q^n}$-linear operations on the matrix $\varphi(GM)$, including the Frobenius transformation designed for attacking classical Gabidulin codes based cryptosystems, will be extremely limited. This greatly increase the complexity of recovering the secret key with no doubt.

## 6.2 A potential plaintext recovery attack

Let $G_{pub} = \begin{pmatrix} \mathcal{P}_n(\boldsymbol{g}') \\ I_n \end{pmatrix}$ where $I_n$ is the identity matrix of order $n$, then the ciphertext can be expressed as

$$\boldsymbol{y} = \boldsymbol{x}\mathcal{P}_n(\boldsymbol{g}') + \boldsymbol{e} = (\boldsymbol{x}, \boldsymbol{e})G_{pub}.$$

Let $\boldsymbol{x}_1 \in \mathbb{F}_{q^m}^k$ and $\boldsymbol{x}_2 \in \mathbb{F}_{q^m}^n$ be two undetermined vectors, then we construct a linear system as

$$\boldsymbol{y} = (\boldsymbol{x}_1, \boldsymbol{x}_2)G_{pub}. \tag{3}$$

If the system (3) admits only a small number of solutions over $\mathbb{F}_{q^m}$, then one can recover the plaintext directly by solving this system in polynomial time. In particular, expanding this system over

$\mathbb{F}_{q^m}$ leads to another linear system with $2n$ equations and $k+n$ variables over $\mathbb{F}_{q^m}$, and solving this system requires $\mathcal{O}(8n^3)$ operations in $\mathbb{F}_{q^m}$. Our analysis shows that, however, this system admits quite a large number of solutions for a properly chosen $k$. In this situation, this kind of plaintext recovery attack will be infeasible. Before presenting our main result, we first introduce the following lemma.

**Lemma 11.** *Let $\boldsymbol{g} = (g^{[n-1]}, \cdots, g^{[1]}, g) \in \mathbb{F}_{q^n}^n$ be a basis vector of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then we have* $\mathrm{wt}_q(\boldsymbol{g} + \boldsymbol{g}^{[m]}) = m$.

*Proof.* It is easy to see that

$$\begin{aligned}\boldsymbol{g} + \boldsymbol{g}^{[m]} &= (g^{[n-1]} + g^{[m-1]}, \cdots, g^{[1]} + g^{[m+1]}, g + g^{[m]}) \\ &= (g^{[n-1]}, \cdots, g^{[1]}, g) \begin{pmatrix} I_m & I_m \\ I_m & I_m \end{pmatrix},\end{aligned}$$

where $I_m$ is the identity matrix of order $m$. Note that $\mathrm{wt}_q(\boldsymbol{g}) = n$, then we have

$$\mathrm{wt}_q(\boldsymbol{g} + \boldsymbol{g}^{[m]}) = \mathrm{Rank}(\begin{pmatrix} I_m & I_m \\ I_m & I_m \end{pmatrix}) = m.$$

□

**Theorem 12.** *The linear system $\boldsymbol{y} = (\boldsymbol{x}_1, \boldsymbol{x}_2)G_{pub}$ admits $q^{m(k-m)}$ solutions over $\mathbb{F}_{q^m}$.*

*Proof.* Note that a solution of a nonhomogeneous linear system can be expressed as a particular solution plus a generic solution of its homogeneous form. Hence the conclusion holds if and only if $(\boldsymbol{x}_1, \boldsymbol{x}_2)G_{pub} = \mathbf{0}$ has $q^{m(k-m)}$ solutions over $\mathbb{F}_{q^m}$. Note that

$$\begin{aligned}(\boldsymbol{x}_1, \boldsymbol{x}_2)G_{pub} &= \boldsymbol{x}_1\varphi(GM)\varphi(M)^{-1} + \boldsymbol{x}_2 \\ &= (\boldsymbol{x}_1\varphi(GM) + \boldsymbol{x}_2\varphi(M))\varphi(M)^{-1} \\ &= \varphi(\boldsymbol{x}_1GM + \boldsymbol{x}_2M)\varphi(M)^{-1},\end{aligned}$$

then we have

$$\begin{aligned}(\boldsymbol{x}_1, \boldsymbol{x}_2)G_{pub} = \mathbf{0} &\Leftrightarrow \varphi(\boldsymbol{x}_1GM + \boldsymbol{x}_2M) = \mathbf{0} \\ &\Leftrightarrow \boldsymbol{x}_1GM + \boldsymbol{x}_2M = \mathbf{0} \\ &\Leftrightarrow \boldsymbol{x}_1G + \boldsymbol{x}_2 = \mathbf{0}. \qquad (4)\end{aligned}$$

Let $(\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathbb{F}_{q^m}^{k+n}$ be a solution of the linear system (4), then $\boldsymbol{x}_1G = \boldsymbol{x}_2 \in \mathbb{F}_{q^m}^n$. This implies that $\boldsymbol{x}_1G = (\boldsymbol{x}_1G)^{[m]} = \boldsymbol{x}_1G^{[m]}$, resulting in a solution of the following linear system

$$\boldsymbol{x}_1(G + G^{[m]}) = \mathbf{0}. \qquad (5)$$

On the contrary. Let $\boldsymbol{x}_1 \in \mathbb{F}_{q^m}^k$ be an arbitrary solution of (5), and set $\boldsymbol{x}_2 = \boldsymbol{x}_1G$. Apparently $\boldsymbol{x}_2 \in \mathbb{F}_{q^m}^n$ and $(\boldsymbol{x}_1, \boldsymbol{x}_2)$ forms a solution of (4) over $\mathbb{F}_{q^m}$. This enables us to conclude that solutions of (4) over $\mathbb{F}_{q^m}$ are in one-to-one correspondence to that of (5).

In what follows, it sufficies to consider the solution space of (5). It is easy to see that $G+G^{[m]}$ is a Moore matrix of order $k\times n$ over $\mathbb{F}_{q^m}$ generated by $\boldsymbol{g}+\boldsymbol{g}^{[m]}$. By Lemma 11, we have $\mathrm{wt}_q(\boldsymbol{g}+\boldsymbol{g}^{[m]}) = m$. By Proposition 1, we have $\mathrm{Rank}(G + G^{[m]}) = m$ because of $k > m$. Hence the solution space of (5) is of dimension $k - m$ over $\mathbb{F}_{q^m}$. Eventually we have that the system (5), or equivalently the system (4), has $q^{m(k-m)}$ solutions over $\mathbb{F}_{q^m}$. This completes the proof. □

### 6.3 Conversion into an RSD instance

A legitimate message receiver can always recover the plaintext in polynomial time, while an adversary trying to obtain the plaintext has to deal with the so-called RSD problem introduced in Section 3. In what follows, we mainly talk about how to convert our proposal into an RSD instance.

Although theoretically we cannot ensure that $\varphi(GM)$ preserves the rank of $GM$, our experiments on Magma show that $\text{Rank}(\varphi(GM)) = \text{Rank}(GM)$ holds with extremely high probability. Let $G' = \varphi(GM)\varphi(M)^{-1}$, then it is reasonable to assume that $\text{Rank}(G') = \text{Rank}(GM) = k$. Let $H' \in \mathcal{M}_{n-k,n}(\mathbb{F}_{q^n})$ be a full rank matrix such that $G'H'^T = O$ and compute $\boldsymbol{s} = \boldsymbol{y}H'^T = \boldsymbol{e}H'^T$. Apparently we get an RSD instance of parameters $(q, n, n, k, t)$.

On the other hand. Since components of $\boldsymbol{e}$ are taken from $\mathbb{F}_{q^m}$, we can convert the problem of recovering $\boldsymbol{e}$ into solving an RSD instance over $\mathbb{F}_{q^m}$. Let $\boldsymbol{a}$ be a basis vector of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^m}$ and set

$$A = \begin{pmatrix} \boldsymbol{a} & & & \\ & \boldsymbol{a} & & \\ & & \ddots & \\ & & & \boldsymbol{a} \end{pmatrix} \in \mathcal{M}_{n-k,2(n-k)}(\mathbb{F}_{q^n}).$$

Apparently there exist $H_s \in \mathcal{M}_{2(n-k),n}(\mathbb{F}_{q^m})$ and $\boldsymbol{s}_s \in \mathbb{F}_{q^m}^{2(n-k)}$ such that $H' = AH_s$ and $\boldsymbol{s} = \boldsymbol{s}_s A^T$. Following this we have $\boldsymbol{s}_s A^T = \boldsymbol{e}H_s^T A^T$ and then $\boldsymbol{s}_s = \boldsymbol{e}H_s^T$. Finally we obtain an RSD instance of parameters $(q, m, n, 2k - n, t)$ over $\mathbb{F}_{q^m}$.

## 7 Parameters and public-key sizes

In this section, we evaluate the practical security of our proposal against general attacks presented in Section 3. The public key of our proposal is a vector in $\mathbb{F}_{q^n}^n$, leading to a public-key size of $n^2 \cdot \log_2(q)$ bits. In Table 3, we give some parameters for security of 128 bits, 192 bits and 256 bits. After that, we make a comparison on public-key size with some other code-based cryptosystems. It is easy to see that our proposal has large advantage over other variants in public-key representation.

| Parameters | | | | Public-key size | Security |
|---|---|---|---|---|---|
| $q$ | $m$ | $n$ | $k$ | | |
| 2 | 32 | 64 | 50 | 512 | 128 |
| 2 | 40 | 80 | 64 | 800 | 192 |
| 2 | 46 | 92 | 70 | 1058 | 256 |

Table 3: Parameters and public-key size (in bytes) for different security levels.

In addition to generic attacks described in Section 3, we should also consider the plaintext recovery attack discussed in Section 6.2, as well as a brute-force attack against the secret $\boldsymbol{g}, \boldsymbol{m}$ and $\varphi$. Denote by $\mathcal{N}(\boldsymbol{g})$ the quantity of all partial circulant Gabidulin codes of length $n$ and dimension $k$ over $\mathbb{F}_{q^n}$, by $\mathcal{N}(\overline{\boldsymbol{m}})$ the quantity of nonequivalent $\boldsymbol{m}$'s as described in Proposition 7, by $\mathcal{N}(\varphi)$ the quantity of all semilinear transformations over $\mathbb{F}_{q^n}$ and by $\mathcal{N}(\boldsymbol{x})$ the quantity of solutions of

| Security<br>Instance | 128 bits | 192 bits | 256 bits |
|---|---|---|---|
| Classic McEliece [1] | 261120 | 524160 | 1044992 |
| NTS-KEM [29] | 319488 | 929760 | 1419704 |
| KRW [30] | | | 578025 |
| HQC [31] | 2249 | 4522 | 7245 |
| BIKE [32] | 1540 | 3082 | 5121 |
| Lau-Tan [6] | 2421 | 3283 | 4409 |
| Our proposal | 512 | 800 | 1058 |

Table 4: Comparison on public-key size (in bytes) with other cryptosystems.

the linear system (3) over $\mathbb{F}_{q^m}$. For suggested parameters in Table 3, these values are presented in Table 5 using base-2 logarithmic representation. Apparently the complexity of recovering $\boldsymbol{g}$ or $\varphi$ is much lower than the corresponding security level. However, it remains unknown whether or not we can recover more information about the secret key with the knowledge of $\boldsymbol{g}$ or $\varphi$. Therefore, we still have confidence in security of our proposal up to now for parameters given in Table 5.

| $\mathcal{N}(\boldsymbol{g})$ | $\mathcal{N}(\overline{\boldsymbol{m}})$ | $\mathcal{N}(\varphi)$ | $\mathcal{N}(\boldsymbol{x})$ | Security |
|---|---|---|---|---|
| 63 | 2048 | 128 | 576 | 128 |
| 79 | 3200 | 160 | 960 | 192 |
| 91 | 4232 | 184 | 1104 | 256 |

Table 5

# 8 Conclusion

In this paper, a completely new technique is developed to distort the structure of linear codes used in code-based cryptography. Based on this masking technique, we exploit the so-called partial cyclic Gabidulin code to construct a code-based cryptosystem. According to our analysis, this cryptosystem can resist existing structural attacks, and admit quite a small public-key size compared to some other code-based cryptosystems. For instance, only 1058 bytes are enough to achieve the security of 256 bits, 987 times smaller than that of the Classic McEliece moving onto the third round of the NIST PQC standardization process.

# References

[1] Albrecht, M.R., Bernstein, D.J., et al.: Classic McEliece: conservative code-based cryptography. https://classic.mceliece.org/nist/mceliece-20201010.pdf. Accessed Octo-

ber 10, 2020.

[2] 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 Advances in Cryptology-EUROCRYPT'91, LNCS, vol. 547, pp. 482–489. Springer (1991).

[3] 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).

[4] 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).

[5] Faure, C., Loidreau, P.: A new public-key cryptosystem based on the problem of reconstructing $p$-polynomials. In: Ytrehus, $\varnothing$. (Ed.): Proceedings of WCC 2005, LNCS, vol. 3969, pp. 304–315. Springer (2005).

[6] 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).

[7] Berger, T., Loidreau, P.: Designing an efficient and secure public-key cryptosystem based on reducible rank codes. In: Proceedings of INDOCRYPT 2004, LNCS, vol. 3348, pp. 218–229. Springer (2004).

[8] Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography (WCC), vol. 2013, pp. 167–179. [Online]. Available: http://www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf

[9] Aragon, N., Gaborit, P., Hauteville, A., Ruatta, O., Zémor, G.: Low rank parity check codes: new decoding algorithms and applications to cryptography. IEEE Trans. Inform. Theory 65(12), 7697–7717 (2019).

[10] Samardjiska, S., Santini, P., Persichetti, E., Banegas, G.: A reaction attack against cryptosystems based on LRPC codes. In: Proceedings of LATINCRYPT 2019, LNCS, vol. 11774, pp. 197–216. Springer (2019).

[11] Guo, W., Fu, F.-W.: Expanded Gabidulin codes and their application to cryptography. arXiv:2107.01610 [cs.IT] (2021).

[12] Bardet, M., Bros, M., Cabarcas, D., et al.: 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).

[13] Bardet, M., Briaud, P., Bros, M., et al.: An algebraic attack on rank metric code-based cryptosystems. In: Proceedings of EUROCRYPT 2020, LNCS, vol. 12107, pp. 64–93. Springer (2020).

[14] 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).

[15] 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).

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

[17] 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).

[18] Goubin L., Courtois N.T.: Cryptanalysis of the TTM cryptosystem. In: Proceedings of Advances in Cryptology (ASIACRYPT 2000), LNCS, vol. 1976, pp. 44–57. Springer (2000).

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

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

[21] 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).

[22] Mullen, G.L., Panario, D.: Handbook of Finite Fields. CRC Press (2013).

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

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

[25] 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).

[26] 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).

[27] 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).

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

[29] Albrecht, M., Cid, C., Paterson, K.G., et al.: NTS-KEM. https://drive.google.com/file/d/1N3rv4HKCt9yU4xn6wuepsBUrfQW8cuFy/view. Accessed November 29, 2019.

[30] Khathuria, K., Rosenthal, J., Weger, V.: Encryption scheme based on expanded Reed-Solomon codes. Adv. Math. Commun. 15(2), 207–218 (2021).

[31] Melchor, C.A., Aragon, N., et al.: Hamming quasi-cyclic (HQC). http://pqc-hqc.org/doc/hqc-specification_2020-10-01.pdf. Accessed October 10, 2020.

[32] Aragon, N., Barreto, P.S., et al.: BIKE: bit flipping key encapsulation. https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf. Accessed October 10, 2020.

[33] Horlemann-Trautmann, A.-L., Marshall, K.: New criteria for MRD and Gabidulin codes and some rank-metric code constructions. arXiv:1507.08641 [cs.IT] (2015).