Semilinear Transformations in Coding Theory: A New Technique in Code-Based Cryptography

Wenshuo Guo* and Fang-Wei Fu†

Abstract

This paper presents a new technique for disturbing the algebraic structure of linear codes in code-based cryptography. Specifically, we introduce the so-called semilinear transformations in coding theory and then 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 φ is therefore defined as an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. Then we impose this transformation to a linear code $\mathcal{C}$ over $\mathbb{F}_{q^m}$. It is clear that $\varphi(\mathcal{C})$ forms an $\mathbb{F}_q$-linear space, but generally does not preserve the $\mathbb{F}_{q^m}$-linearity any longer. Inspired by this observation, a new technique for masking the structure of linear codes is developed in this paper. Meanwhile, we endow the underlying Gabidulin code with the so-called partial cyclic structure to reduce the public-key size. Compared to some other code-based cryptosystems, our proposal admits a much more compact representation of public keys. For instance, 2592 bytes are enough to achieve the security of 256 bits, almost 403 times smaller than that of Classic McEliece entering the third round of the NIST PQC project.

Keywords Post-quantum cryptography · Code-based cryptography · Rank metric codes · Gabidulin codes · Partial cyclic codes · Semilinear transformations

1 Introduction

Over the past decades, post-quantum cryptosystems (PQCs) have been drawing more and more attention from the cryptographic community. The most important advantage of PQCs 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 has never been used in practical situations for the reason that it requires large memory for public keys. For instance, Classic McEliece [1] submitted to the NIST PQC project has a public-key size of 255 kilobytes for the

*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

128-bit 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 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 variants 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-bit 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 variants, 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 provides the feasibility for us to distinguish Gabidulin codes from general ones. Based on this observation, various structural attacks [25–29] 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 has 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 and Fu mentioned a fact that $\varphi(\mathcal{C})$ generally does not preserve the $\mathbb{F}_{q^m}$-linearity according to their experiments on Magma, where $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$ and φ is an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. This inspires us to apply this family of transformations to construct code-based cryptosystems. According to our analysis in the present paper, a transformation that preserves 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 automorphism of $\mathbb{F}_{q^m}$ admitting this property is called a fully linear transformation over $\mathbb{F}_{q^m}$, otherwise we call it a semilinear transformation. Furthermore, we find that an $\mathbb{F}_q$-linear transformation preserving the $\mathbb{F}_{q^m}$-linearity of a linear code is fully linear in general cases. 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 $m(q^m - 1)$. This implies that a fully linear transformation occurs with an extremely low probability when q^m is large enough, which provides the feasibility for us to exploit this kind of transformation in code-based cryptography. As an application of semilinear transformations, we propose an encryption scheme based on the so-called partial cyclic Gabidulin codes.

The rest of this paper is organized as follows. Section 2 introduces some basic notations used throughout this paper, as well as the definitions of Moore matrices and partial cyclic codes. Section 3 presents two hard problems in coding theory and two types of 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 their algebraic properties when acting on linear codes. Section 5 is devoted to the description of our new proposal and some notes on the choice of the private 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. A few concluding remarks will be presented in Section 8.

2 Preliminaries

This section mainly presents some notation used throughout this paper, as well as basic concepts about Gabidulin codes and the so-called partial cyclic codes.

2.1 Notations and basic concepts

Let $\mathbb{F}_q$ be a finite field, 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 α 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 α a normal element if $\boldsymbol{a} = (\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}) \in \mathbb{F}_{q^m}^m$ forms a basis vector. 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 vector space spanned by the rows of M over $\mathbb{F}_q$.

An $[n, k]$ linear code $\mathcal{C}$ 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 $\mathbb{F}_{q^m}^n$. A $k \times n$ matrix G over $\mathbb{F}_{q^m}$ of 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 the components of $\boldsymbol{c}$ over $\mathbb{F}_q$. The rank weight of $\boldsymbol{c}$ with respect to $\mathbb{F}_q$, denoted by $\text{wt}_R(\boldsymbol{c})$, is defined to be the dimension of $\text{Supp}_R(\boldsymbol{c})$ over $\mathbb{F}_q$. For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, the rank support $\text{Supp}_R(M)$ of M is defined to be the linear space spanned by entries of M over $\mathbb{F}_q$. Similarly, the rank weight of M with respect to $\mathbb{F}_q$, denoted by $\text{wt}_R(M)$, is defined as the dimension of $\text{Supp}_R(M)$ over $\mathbb{F}_q$.

2.2 Gabidulin codes

Before introducing Gabidulin codes, we present the concept of Moore matrices and some related results.

Definition 1 (Moore matrices). For an integer i, we denote by $\alpha^{[i]} = \alpha^{q^i}$ the i-th Frobenius power of $\alpha \in \mathbb{F}_{q^m}$. By $\boldsymbol{g}^{[i]}$ we denote the component-wise i-th Frobenius power of $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$. 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 $1 \leqslant i \leqslant k$.

Remark 1. 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 $\mathcal{C}^{[i]} = \{\boldsymbol{c}^{[i]} : \boldsymbol{c} \in \mathcal{C}\}$. Furthermore, it is easy to verify that $\mathcal{C}^{[i]}$ is also an $[n, k]$ linear code over $\mathbb{F}_{q^m}$.

The following proposition describes simple algebraic properties of Moore matrices.

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

(2) *For a vector $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ and a matrix $Q \in \mathcal{M}_{n,l}(\mathbb{F}_q)$, let $A \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ be a Moore matrix generated by $\boldsymbol{a}$, then AQ is a $k \times l$ Moore matrix generated by $\boldsymbol{a}Q$.*

(3) *For positive integers* $k \leqslant n \leqslant m$ *and a vector* $\boldsymbol{a} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_{q^m}^n$ *with* $\mathrm{wt}_R(\boldsymbol{a}) = n$, *let* $A \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ *be a Moore matrix generated by* $\boldsymbol{a}$*. Then* A *has full row rank, that is Rank*$(A) = k$.

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

Now we introduce the definition of Gabidulin codes.

Definition 2 (Gabidulin codes). For positive integers $k \leqslant n \leqslant m$ and $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ with $\mathrm{wt}_R(\boldsymbol{g}) = n$. Let $G \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ be a Moore matrix generated by $\boldsymbol{g}$, then the $[n, k]$ Gabidulin code 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 generalized Reed-Solomon (GRS) codes in the rank metric, both of which have pretty good algebraic properties. An $[n, k]$ Gabidulin code has minimum rank distance $d = n - k + 1$ [38] and can correct up to $\lfloor \frac{n-k}{2} \rfloor$ rank errors in theory. Efficient decoding algorithms for Gabidulin codes can be found in [39–41].

2.3 Partial cyclic codes

Lau and Tan [6] proposed the use of partial cyclic codes to shrink public-key size in rank metric based cryptography. Now we formally introduce this family of codes and some related results.

Definition 3 (Partial circulant matrices). For a vector $\boldsymbol{m} \in \mathbb{F}_q^n$, the circulant matrix induced 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 $2 \leqslant i \leqslant n$. For a positive integer $k \leqslant n$, the $k \times n$ partial circulant matrix generated by $\boldsymbol{m}$, denoted by $PC_k(\boldsymbol{m})$, is defined to be the first k rows of M. Particularly, we denote by $PC_n(\boldsymbol{m})$ the circulant matrix generated by $\boldsymbol{m}$. Furthermore, we denote by $PC_n(\mathbb{F}_q)$ the set of all $n \times n$ circulant matrices over $\mathbb{F}_q$.

Remark 2. Chalkley [23] proved that $PC_n(\mathbb{F}_q)$ forms a commutative ring under usual matrix addition and multiplication. Let $\mathbf{1} = (1, 0, \cdots, 0) \in \mathbb{F}_q^n$, then $PC_k(\boldsymbol{m}) = PC_k(\mathbf{1}) \cdot PC_n(\boldsymbol{m})$ for any $\boldsymbol{m} \in \mathbb{F}_q^n$. It follows that for a $k \times n$ partial circulant matrix A over $\mathbb{F}_q$ and $B \in PC_n(\mathbb{F}_q)$, AB is also a $k \times n$ partial circulant matrix.

The following two propositions first describe a sufficient and necessary condition for a circulant matrix being invertible, and then make an accurate estimation on the number 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* $PC_n(\boldsymbol{m})$ *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* $g_1(x), \cdots, g_r(x) \in \mathbb{F}_q[x]$ *be* r *distinct irreducible factors of* $f(x)$*, i.e.* $f(x) = \prod_{i=1}^{r} g_i(x)^{e_i}$ *for some positive integers* $e_1, \cdots, e_r$*. Let* $d_i = \deg(g_i(x))$ *for* $1 \leqslant i \leqslant r$*, then*

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

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

Now we introduce the so-called partial cyclic codes.

Definition 4 (Partial cyclic codes). For a vector $\boldsymbol{a} \in \mathbb{F}_q^n$, let $G = PC_k(\boldsymbol{a})$ be a partial circulant matrix induced by $\boldsymbol{a}$. An $[n,k]$ linear code $\mathcal{C} = \langle G \rangle_q$ is called a partial cyclic code generated by $\boldsymbol{a}$.

Remark 3. For a normal element $g \in \mathbb{F}_{q^n}$ with respect to $\mathbb{F}_q$, let $\boldsymbol{g} = (g^{[n-1]}, g^{[n-2]}, \cdots, g)$ and $G = PC_k(\boldsymbol{g})$. Easily it can be verified that G is a $k \times n$ Moore matrix. An $[n,k]$ linear code $\mathcal{G} = \langle G \rangle_{q^n}$ is called a partial cyclic Gabidulin code generated by $\boldsymbol{g}$.

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

This section mainly discusses classical hard problems in coding theory on which the security of code-based cryptosystems relies, as well as some attacks on them that will be useful to estimate the security level of our proposal later in this paper.

Definition 5 (Syndrome Decoding (SD) Problem). Given positive integers n, k and t, let H be an $(n-k) \times n$ matrix over $\mathbb{F}_q$ of full rank and $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$. The SD problem with parameters (q, n, k, t) is to search for 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 first instance of the SD problem being used in code-based cryptography is the McEliece cryptosystem [16] based on Goppa codes. A rank metric counterpart of this problem is the rank syndrome decoding problem described 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 $\mathbb{F}_{q^m}$ 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 a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{s} = \boldsymbol{e}H^T$ and $\text{wt}_R(\boldsymbol{e}) = t$.

The RSD problem is an important issue in rank metric 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.

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 the attacks proposed in [12, 13, 18, 19], whose complexity and applicable condition are summarized in Table 2.

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

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

Attack	Condition	Complexity
[19]	$\left\lceil\frac{(t+1)(k+1)-(n+1)}{t}\right\rceil \leqslant k$	$\mathcal{O}\left(k^3t^3q^{t\lceil\frac{(t+1)(k+1)-(n+1)}{t}\rceil}\right)$
[18]		$\mathcal{O}\left(k^3m^3q^{t\lceil\frac{km}{n}\rceil}\right)$
[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 $\omega = 2.81$ and $p = \min\{1 \leqslant i \leqslant n : m\binom{n-i-k-1}{t} \geqslant \binom{n-i}{t}-1\}$
[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 $a = \min\{1 \leqslant i \leqslant n : m\binom{n-k-1}{t} \geqslant \binom{n-i}{t}-1\}$
[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 seen as an m-dimensional linear space over $\mathbb{F}_q$. 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 $\mathbb{F}_q$. For any $\alpha = \sum_{i=1}^{m} \lambda_i\alpha_i \in \mathbb{F}_{q^m}$ with $\lambda_i \in \mathbb{F}_q$, we define an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$ as

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

By $Aut_q(\mathbb{F}_{q^m})$ we denote the set of all $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$. Furthermore, we introduce the following notation:

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

In the remainder of this section, we will do further study on this type of transformations. Firstly, we present 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. It is easy to see that all the transformations in $Aut_q(\mathbb{F}_{q^m})$ 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 vector $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$, a natural question is how the Hamming (rank) weight of $\boldsymbol{c}$ varies under the action of a transformation $\varphi \in Aut_q(\mathbb{F}_{q^m})$. For this reason, we introduce the following proposition.

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

Proof. For any $\alpha \in \mathbb{F}_{q^m}$ and $\varphi \in Aut_q(\mathbb{F}_{q^m})$, obviously $\varphi(\alpha) = 0$ holds if and only if $\alpha = 0$. Hence we have $\text{Supp}_H(\varphi(\boldsymbol{v})) = \text{Supp}_H(\boldsymbol{v})$ 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 $\text{wt}_R(\boldsymbol{v}) = n$. If $\text{wt}_R(\varphi(\boldsymbol{v})) < n$, then there exists $\boldsymbol{b} \in \mathbb{F}_q^n \backslash \{\boldsymbol{0}\}$ such that $\varphi(\boldsymbol{v})\boldsymbol{b}^T = \varphi(\boldsymbol{v}\boldsymbol{b}^T) = 0$. This implies that $\boldsymbol{v}\boldsymbol{b}^T = 0$, which conflicts with $\text{wt}_R(\boldsymbol{v}) = n$. More generally, suppose that $\text{wt}_R(\boldsymbol{v}) = r < n$. Then there exist $\boldsymbol{v}^* \in \mathbb{F}_{q^m}^r$ with $\text{wt}_R(\boldsymbol{v}^*) = r$ and $Q \in GL_n(\mathbb{F}_q)$ such that $\boldsymbol{v} = (\boldsymbol{v}^*|\boldsymbol{0})Q$. It follows that $\varphi(\boldsymbol{v}) = (\varphi(\boldsymbol{v}^*)|\boldsymbol{0})Q$ and therefore $\text{wt}_R(\varphi(\boldsymbol{v})) = \text{wt}_R(\varphi(\boldsymbol{v}^*)) = r$. □

Remark 4. Let $\mathbb{K}$ be an extension field of $\mathbb{F}_{q^m}$. Similar to Proposition 6, we can deduce from a direct verification that an $\mathbb{F}_{q^m}$-linear automorphism of $\mathbb{K}$ preserves the rank weight of a vector in $\mathbb{K}^n$ with respect to $\mathbb{F}_q$.

For $\varphi \in Aut_q(\mathbb{F}_{q^m})$ and a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, it is clear that $\varphi(\mathcal{C})$ is an $\mathbb{F}_q$-linear space, but generally no longer $\mathbb{F}_{q^m}$-linear. Based on this observationm, we classify the $\mathbb{F}_q$-linear automorphisms of $\mathbb{F}_{q^m}$ as follows.

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

The following theorem provides a sufficient and necessary condition for $\varphi \in Aut_q(\mathbb{F}_{q^m})$ 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 $\varphi \in Aut_q(\mathbb{F}_{q^m})$. Let $A = \left[\varphi(\alpha_1\boldsymbol{a})^T, \cdots, \varphi(\alpha_m\boldsymbol{a})^T\right]^T$, then a sufficient and necessary condition for φ being fully linear is that A has rank 1.*

Proof. On the necessity aspect. Let $\mathcal{C} = \langle \boldsymbol{a} \rangle_{q^m}$ and $\boldsymbol{a}_i = \varphi(\alpha_i\boldsymbol{a})$ be the i-th row vector of A. Note that φ is fully linear over $\mathbb{F}_{q^m}$, then φ is linear on $\mathcal{C}$, or equivalently $\varphi(\mathcal{C})$ is $\mathbb{F}_{q^m}$-linear. Let $k = \dim_{q^m}(\varphi(\mathcal{C}))$, then $(q^m)^k = |\varphi(\mathcal{C})| = |\mathcal{C}| = q^m$ and therefore $k = 1$. The conclusion is proved immediately because of $\boldsymbol{a}_i$ $(1 \leqslant i \leqslant m)$ being contained in $\varphi(\mathcal{C})$.

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 $\lambda_{i1}, \cdots, \lambda_{im} \in \mathbb{F}_q$ 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 $\boldsymbol{c} \in \varphi(\mathcal{C})$, there exists $\boldsymbol{u} \in \mathcal{C}$ such that $\boldsymbol{c} = \varphi(\boldsymbol{u})$. Meanwhile, there exists $M \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\boldsymbol{u} = \boldsymbol{a}M$. It follows that

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

for any $1 \leqslant j \leqslant m$. Assume that $\sum_{i=1}^m a_i \alpha_i = 1$ 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

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

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

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

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

Remark 5. Note that the rank of A is independent of the basis vector. More generally, let $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ be another two basis vectors of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, then there exist $Q_1, Q_2 \in PC_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$ such that $\boldsymbol{a}_1 = \boldsymbol{a}Q_1$ and $\boldsymbol{a}_2 = \boldsymbol{a}Q_2$. Let $A' = \varphi(\boldsymbol{a}_1^T \boldsymbol{a}_2)$, then $A' = \varphi((\boldsymbol{a}Q_1)^T \boldsymbol{a}Q_2) = \varphi(Q_1^T \boldsymbol{a}^T \boldsymbol{a} Q_2) = Q_1^T A Q_2$, which leads to the conclusion that $\text{Rank}(A) = \text{Rank}(A')$.

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 $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is $m(q^m - 1)$.*

Proof. Let $\varphi \in Aut_q(\mathbb{F}_{q^m})$ and $\boldsymbol{a} = (1, \alpha, \cdots, \alpha^{m-1})$ where α is a polynomial element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. By Theorem 8, a necessary condition for φ being fully linear is that $\varphi(\alpha \boldsymbol{a}) = \gamma \varphi(\boldsymbol{a})$, or equivalently

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

holds for some $\gamma \in \mathbb{F}_{q^m}$. Assume that $\varphi(1) = \beta \in \mathbb{F}_{q^m}^*$, then we can deduce from (2) that

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

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

$$f(\alpha) = \alpha^m + \sum_{i=0}^{m-1} a_i \alpha^i = 0. \tag{3}$$

Because of φ being $\mathbb{F}_q$-linear, applying φ to both sides of (3) 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 $0\leqslant i\leqslant m-1$.

Conversely, let $\Gamma=\{\alpha^{[i]}:0\leqslant i\leqslant m-1\}$, then it is easy to verify that for any duple $(\gamma,\beta)\in\Gamma\times\mathbb{F}_{q^m}^*$, the $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$ determined by $\varphi(\alpha^i)=\beta\gamma^i\,(0\leqslant i\leqslant m-1)$ forms a fully linear transformation over $\mathbb{F}_{q^m}$. Hence all the fully linear transformations over $\mathbb{F}_{q^m}$ are in one-to-one correspondence to the Cartesian product $\Gamma\times\mathbb{F}_{q^m}^*$, which leads to the conclusion immediately. $\square$

Remark 6. For a polynomial element α of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, let $\Gamma=\{\alpha^{[i]}\}_{i=0}^{m-1}$ be the set of conjugates of α. 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 γ is a conjugate of α, then there exists $0\leqslant j\leqslant m-1$ such that $\gamma=\alpha^{[j]}$. For any $\mu=\sum_{i=0}^{m-1}\lambda_i\alpha^i\in\mathbb{F}_{q^m}$ with $\lambda_i\in\mathbb{F}_q$, we have

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

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 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 $\mathcal{S}=\{A_{ij}:1\leqslant i\leqslant k,1\leqslant j\leqslant n-k\}$, then we have the following statements.*

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

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

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

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

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

(2) With the necessity being obvious, it suffices to prove the sufficiency. Without loss of generality, we consider the first row vector 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 φ is linear on $\mathcal{C}$, or equivalently $\varphi(\mathcal{C})$ is an $\mathbb{F}_{q^m}$-linear code. Apparently $\varphi(\mathcal{C})$ has $\varphi(G)$ as a generator matrix, which implies that there exists $\boldsymbol{\lambda}=(\lambda_1,\cdots,\lambda_k)\in\mathbb{F}_{q^m}^k$ such that $\varphi(\beta\boldsymbol{g}_1)=\boldsymbol{\lambda}\varphi(G)$ 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 $\varphi(\beta\boldsymbol{g}_1)$ and $\varphi(\boldsymbol{g}_1)$ are linearly dependent over $\mathbb{F}_{q^m}$. Then we can deduce that $(\varphi(\beta),\varphi(\alpha\beta))=\lambda_1(\varphi(1),\varphi(\alpha))$ and furthermore $\varphi(1)\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)$. Let $\gamma=\frac{\varphi(\alpha)}{\varphi(1)}$, then

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

Because of α 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 $\mathbb{F}_q$. 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 φ forms a fully linear transformation over $\mathbb{F}_{q^m}$.

□

Corollary 1. *Let m be a prime and $\mathcal{S}$ be defined as above in Theorem 10. If there exists $\alpha \in \mathcal{S}$ such that $\alpha \notin \mathbb{F}_q$, then any $\mathbb{F}_q$-linear automorphism φ of $\mathbb{F}_{q^m}$ is fully linear if and only if φ 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

In this section, we will first give a formal description of our new proposal and then discuss how to choose the private key to avoid some potential structural weakness.

5.1 Description of our proposal

For a given security level, choose a finite field $\mathbb{F}_q$ and positive integers m, n, k, l, λ_1 and λ_2 such that $n = lm$. Let $\boldsymbol{g} = (g^{[n-1]}, g^{[n-2]}, \cdots, g) \in \mathbb{F}_{q^n}^n$ be a normal basis vector of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $G = PC_k(\boldsymbol{g}) \in \mathcal{M}_{k,n}(\mathbb{F}_{q^n})$ be a partial circulant matrix generated by $\boldsymbol{g}$. Denote by $\mathcal{G}$ the $[n, k]$ partial cyclic Gabidulin code over $\mathbb{F}_{q^n}$ that has G as a generator matrix. Now we introduce the cryptosystem with 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 $\mathrm{wt}_R(\boldsymbol{m}_i) = \lambda_i$. Let $M_i = PC_n(\boldsymbol{m}_i)$ and check whether or not M_i is invertible. If not, then rechoose $\boldsymbol{m}_i$ and repeat the process above. Randomly choose an $\mathbb{F}_{q^m}$-linear automorphism φ of $\mathbb{F}_{q^n}$ such that φ is not fully linear over $\mathbb{F}_{q^n}$. Compute $\varphi(GM_1^{-1})M_2^{-1} = PC_k(\boldsymbol{g}^*)$, where $\boldsymbol{g}^* = \varphi(\boldsymbol{g}M_1^{-1})M_2^{-1}$. We publish $(\boldsymbol{g}^*, t)$ as the public key where $t = \left\lfloor \frac{n-k}{2\lambda_1\lambda_2} \right\rfloor$, and keep $(\boldsymbol{m}_1, \boldsymbol{m}_2, \varphi)$ as the private key.

- Encryption

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

  $$\boldsymbol{y} = \boldsymbol{x}PC_k(\boldsymbol{g}^*) + \boldsymbol{e} = \boldsymbol{x}\varphi(GM_1^{-1})M_2^{-1} + \boldsymbol{e}.$$

- Decryption

For a ciphertext $\boldsymbol{y} \in \mathbb{F}_{q^n}^n$, we first recover $G = PC_k(\boldsymbol{g}), M_1 = PC_n(\boldsymbol{m}_1)$ and $M_2 = PC_n(\boldsymbol{m}_2)$. Then compute

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

and

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

Let $\boldsymbol{e}' = \varphi^{-1}(\boldsymbol{e}M_2)M_1$, then we have

$$\mathrm{wt}_R(\boldsymbol{e}') \leqslant \mathrm{wt}_R(\varphi^{-1}(\boldsymbol{e}M_2)) \cdot \lambda_1 = \mathrm{wt}_R(\boldsymbol{e}M_2) \cdot \lambda_1 \leqslant \mathrm{wt}_R(\boldsymbol{e}) \cdot \lambda_2 \cdot \lambda_1 \leqslant \left\lfloor \frac{n-k}{2} \right\rfloor.$$

Applying the fast decoder of $\mathcal{G}$ to $\boldsymbol{y}'$ will lead to 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 A note on the underlying Gabidulin code

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

Proposition 7. *Let α be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then $\beta \in \mathbb{F}_{q^n}$ is normal if and only if there exists $Q \in PC_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$ such that*

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

Proof. Trivial from a straightforward verification. □

Note that keeping the matrix $G = PC_k(\boldsymbol{g})$ secret cannot enhance the security of the cryptosystem. Let $\boldsymbol{g}' \in \mathbb{F}_{q^n}^n$ be another normal basis vector of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. By Proposition 7, there exists a matrix $Q \in PC_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$ such that $\boldsymbol{g} = \boldsymbol{g}'Q$. Let $G' = PC_k(\boldsymbol{g}')$, then $G = G'Q$ and

$$\varphi(GM_1^{-1})M_2^{-1} = \varphi(G'QM_1^{-1})M_2^{-1} = \varphi(G'M_1^{-1})QM_2^{-1} = \varphi(G'M_1^{-1})M_2'^{-1},$$

where $M_2' = M_2Q^{-1} \in PC_n(\mathbb{F}_{q^n}) \cap GL_n(\mathbb{F}_{q^n})$ satisfying $\mathrm{wt}_R(M_2') = \lambda_2$. Furthermore, it is easy to verify that anyone possessing the knowledge of $\varphi, \boldsymbol{g}', M_1$ and M_2' can decrypt any ciphertext in polynomial time. This implies that breaking this cryptosystem can be reduced to recovering φ, M_1 and M_2'. Hence we conclude that it does not make a difference to keep the underlying partial cyclic Gabidulin code secret.

5.3 On the choice of φ

First we explain why the secret transformation φ cannot be fully linear over $\mathbb{F}_{q^n}$. Assume that φ is fully linear over $\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_{q^m}$, then by Remark 6 there exist $\beta \in \mathbb{F}_{q^n}^*$ and $0 \leqslant j \leqslant l-1$ such that

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

It follows that

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

where $G' = G^{[mj]}$ and $M' = \beta^{-1}M_2M_1^{[mj]}$. On the one hand, $\langle G' \rangle_{q^n}$ forms an $[n, k]$ partial cyclic Gabidulin code according to $G' = PC_k(\boldsymbol{g}^{[mj]})$ and Remark 3. On the other hand, entries of M' are contained in an $\mathbb{F}_q$-linear space of dimension at most $\lambda_1\lambda_2$. Furthermore, a straightforward verification shows that one can decrypt any ciphertext in polynomial time with the knowledge of G' and M'. This suggests that the cryptosystem degenerates into a sub-instance of Loidreau's proposal [4], which has been completely broken in some cases [29–31]. Hence choosing φ to be fully linear over $\mathbb{F}_{q^n}$ may bring some security problems.

Furthermore, we choose the transformatin φ such that $\varphi(\langle GM_1^{-1} \rangle_{q^n})$ does not preserve the $\mathbb{F}_{q^n}$-linearity. According to our experimental results using Magma, the systematic form of GM_1^{-1} always has entries that serve as polynomial elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^m}$. To generate a transformation φ that is semilinear on $\langle GM_1^{-1} \rangle_{q^n}$, it suffices to choose a semilinear transformation over $\mathbb{F}_{q^n}$ because of Theorem 10.

In what follows, we will investigate the equivalence between different semilinear transformations. For any $\beta \in \mathbb{F}_{q^n}^*$ and a semilinear transformation φ over $\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_{q^m}$, it is easy to verify that $\beta\varphi$ is also a semilinear transformation, where $\beta\varphi$ is defined as $\beta\varphi(\alpha) = \beta \cdot \varphi(\alpha)$ for any $\alpha \in \mathbb{F}_{q^n}$. Furthermore, let $\varphi' = \beta\varphi$ and $M_2' = \beta M_2$, then we have $\text{wt}_R(M_2') = \text{wt}_R(M_2) = \lambda_2$ and

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

From the perspective of a brute-force attack, we say that φ and φ' are equivalent. We define $\overline{\varphi} = \{\beta\varphi : \beta \in \mathbb{F}_{q^n}^*\}$, called the equivalent class of φ. Apparently for any two transformations φ_1 and φ_2, we have either $\overline{\varphi_1} = \overline{\varphi_2}$ or $\overline{\varphi_1} \cap \overline{\varphi_2} = \varnothing$.

Now we make an estimation on the number of nonequivalent semilinear transformations. By Proposition 5, the number of $\mathbb{F}_{q^m}$-linear automorphisms of $\mathbb{F}_{q^n}$ can be computed as

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

By Theorem 9, the number of fully linear transformations over $\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_{q^m}$ is $l(q^n - 1)$. Denote by $\mathcal{N}(\overline{\varphi})$ the number of nonequivalent semilinear transformations, then

$$\mathcal{N}(\overline{\varphi}) = \frac{|Aut_{q^m}(\mathbb{F}_{q^n})| - l(q^n - 1)}{q^n - 1} \approx q^{(l-1)n}.$$

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

Firstly, we investigate how to choose $\boldsymbol{m}_1$ and $\boldsymbol{m}_2$ to evade some structural weakness. We point out that neither $\boldsymbol{m}_1$ or $\boldsymbol{m}_2$ should be taken over $\mathbb{F}_{q^m}$, otherwise this cryptosystem will be degenerated. Now we discuss this problem in the following two cases:

(1) If $\boldsymbol{m}_1 \in \mathbb{F}_{q^m}^n$, then there will be $M_1, M_1^{-1} \in GL_n(\mathbb{F}_{q^m})$. Following this, we have

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

where $M = M_1M_2$ satisfying $\mathrm{wt}_R(M) \leqslant \mathrm{wt}_R(M_1) \cdot \mathrm{wt}_R(M_2) = \lambda_1\lambda_2$. A straightforward verification shows that if one can recover φ and M, then one can decrypt any valid ciphertext in polynomial time. Let $G'_{pub} = PC_n(\boldsymbol{g}^*)$ and $G' = PC_n(\boldsymbol{g})$, then it can be verified that $G'_{pub} = \varphi(G')M^{-1}$. If one can manage to find φ, then one can recover M by computing ${G'_{pub}}^{-1}\varphi(G')$. This suggests that breaking this cryptosystem can be reduced to finding the secret φ.

(2) If $\boldsymbol{m}_2 \in \mathbb{F}_{q^m}^n$, then there will be $M_2, M_2^{-1} \in GL_n(\mathbb{F}_{q^m})$. Furthermore, we have

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

where $M = M_1M_2$ satisfying $\mathrm{wt}_R(M) \leqslant \mathrm{wt}_R(M_1) \cdot \mathrm{wt}_R(M_2) = \lambda_1\lambda_2$. Similarly, a straightforward verification shows that one can decrypt any valid ciphertext with the knowledge of φ, G and M. If one can manage to find φ, then one can recover GM^{-1} and then M using a similar method as above. This suggests that breaking this cryptosystem can be reduced to finding the secret φ.

Secondly, we discuss the equivalence of potential $\boldsymbol{m}_1$'s. For a matrix $Q \in PC_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$, let $M'_1 = M_1Q$ and $M'_2 = M_2Q$, then $\mathrm{wt}_R(M'_1) = \mathrm{wt}_R(M_1)$ and $\mathrm{wt}_R(M'_2) = \mathrm{wt}_R(M_2)$. Following this, we have

$$\varphi(G{M'_1}^{-1})M_2^{-1} = \varphi(GQ^{-1}M_1^{-1}){M'_2}^{-1} = \varphi(GM_1^{-1})Q^{-1}M_2^{-1} = \varphi(G{M_1}^{-1}){M'_2}^{-1}.$$

From the perspective of a brute-force attack against $\boldsymbol{m}_1$, it does not make a difference to multiply $\boldsymbol{m}_1$ by an invertible circulant matrix over $\mathbb{F}_q$. We define $\overline{\boldsymbol{m}}_1 = \{\boldsymbol{m}_1Q : Q \in PC_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)\}$, called the equivalent class of $\boldsymbol{m}_1$.

Now we make an estimation on the number of nonequivalent $\overline{\boldsymbol{m}}_1$'s. For a positive integer λ, let $\mathcal{V} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear space of dimension λ. For a matrix $M \in PC_n(\mathcal{V}) \cap GL_n(\mathcal{V})$ with $\mathrm{wt}_R(M) = \lambda$, there exists a decomposition $M = \sum_{j=1}^{\lambda} \alpha_j A_j$, where α_j's form a basis of $\mathcal{V}$ over $\mathbb{F}_q$ and A_j's are nonzero matrices in $PC_n(\mathbb{F}_q)$. Denote by $\mathcal{N}(A)$ the number of nonzero matrices in $PC_n(\mathbb{F}_q)$, and by $\mathcal{N}(\mathcal{V})$ the number of λ-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$, then

$$\mathcal{N}(A) = q^n - 1 \text{ and } \mathcal{N}(\mathcal{V}) = \prod_{j=0}^{\lambda-1} \frac{q^n - q^j}{q^\lambda - q^j} \approx q^{\lambda n - \lambda^2}.$$

The number of matrices $M \in PC_n(\mathbb{F}_{q^n}) \cap GL_n(\mathbb{F}_{q^n})$ with $\mathrm{wt}_R(M) = \lambda$ can be evaluated as

$$\mathcal{N}(M) = \mathcal{N}(\mathcal{V}) \cdot \mathcal{N}(A)^\lambda \cdot \xi \approx \xi q^{2\lambda n - \lambda^2},$$

where ξ denotes the probability of a random $M \in PC_n(\mathbb{F}_{q^n})$ with $\mathrm{wt}_R(M) = \lambda$ being invertible. As for the probability ξ, we have the following proposition.

Proposition 8. *If $q^\lambda - q^{\lambda-1} \geqslant 2n$, then $\xi \geqslant \frac{1}{2}$.*

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 $PC_n(\mathcal{V})$. Let U be the set of all singular matrices in $\mathcal{M}_\lambda(\mathcal{V})$, and $V = \mathcal{M}_\lambda(\mathcal{V}) \cap GL_n(\mathcal{V})$. 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 $\boldsymbol{m} = (m_0, m_1, \cdots, m_{n-1}) \in \mathcal{V}^n$ be the first row vector of M, namely $M = PC_n(\boldsymbol{m})$. Let $\overline{M} = \{N \in U : M - N \text{ is a scalar matrix}\}$, a set of matrices in U that resemble M at the last $n-1$ coordinates. Let $\boldsymbol{x} = (x, m_1, \cdots, m_{n-1})$, and $X = PC_n(\boldsymbol{x})$. 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 $\boldsymbol{m}^* = (m_1, \cdots, m_{n-1})$, then it is easy to see that $\mathrm{wt}_R(\boldsymbol{m}^*) \geqslant \lambda - 1$. Now we establish the mapping σ in the following two cases:

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

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 $\mathcal{W} = \langle m_1, \cdots, m_{n-1} \rangle_q$, 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 $M_1' = PC_n(\boldsymbol{m}_1') \in GL_n(\mathcal{V})$, and $\mathrm{wt}_R(\boldsymbol{m}_1') = \lambda$ 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 $M_i' = PC_n(\boldsymbol{m}_i') \in GL_n(\mathcal{V})$, and $\mathrm{wt}_R(\boldsymbol{m}_i') = \lambda$ in the meanwhile. We define $\sigma(M_i) = M_i'$.

(2) $\mathrm{wt}_R(\boldsymbol{m}^*) = \lambda$.

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 $M_1' = PC_n(\boldsymbol{m}_1') \in GL_n(\mathcal{V})$, and $\mathrm{wt}_R(\boldsymbol{m}_1') = \lambda$ 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 $M_i' = PC_n(\boldsymbol{m}_i') \in GL_n(\mathcal{V})$, and $\mathrm{wt}_R(\boldsymbol{m}_i') = \lambda$ 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

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

□

Remark 7. Proposition 8 provides a sufficient condition for $\xi \geqslant \frac{1}{2}$. Actually, this inequality always holds according to our extensive experiments on Magma, even when the sufficient condition is not satisfied. Hence we suppose that $\xi = \frac{1}{2}$ in practice. Finally, the number of nonequivalent $\overline{\boldsymbol{m}}_1$'s can be evaluated as

$$\mathcal{N}(\overline{\boldsymbol{m}}_1) = \frac{\mathcal{N}(M_1)}{|PC_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)|} \approx \frac{q^{2\lambda_1 n - \lambda_1^2}}{\Phi_q(x^n - 1)},$$

where $\Phi_q(x^n - 1)$ is defined as in (1).

In what follows, we will discuss how to generate in an efficient way the secret matrix $M_i \in PC_n(\mathbb{F}_{q^n}) \cap GL_n(\mathbb{F}_{q^n})$ such that $\text{wt}_R(M_i) = \lambda_i$. Let $M = \sum_{j=1}^{\lambda} \alpha_j A_j$ be defined as above. According to our experiments on Magma, if one of these A_j's is chosen to be invertible, then M is invertible with high probability. For example, let $M = \alpha_1 A_1 + \alpha_2 A_2$ be a circulant matrix of order 20 over $\mathbb{F}_{2^{20}}$. In the case of A_1 being randomly chosen from $PC_{20}(\mathbb{F}_2) \cap GL_{20}(\mathbb{F}_2)$ and A_2 being randomly chosen from $PC_{20}(\mathbb{F}_2)$, only 2 out of 1 million M's turn out to be singular. For the case of A_1 and A_2 being randomly chosen from $PC_{20}(\mathbb{F}_2)$, however, up to 252344 out of 1 million M's turn out to be singular. To efficiently generate the secret M_i, therefore, we adopt the following procedure:

1. Randomly choose $\alpha_1, \cdots, \alpha_{\lambda_i} \in \mathbb{F}_{q^n}$ that are linearly independent over $\mathbb{F}_q$;
2. Randomly choose nonzero matrices $A_1, \cdots, A_{\lambda_i} \in PC_n(\mathbb{F}_q)$ such that $A_1 \in GL_n(\mathbb{F}_q)$;
3. Compute $M_i = \sum_{j=1}^{\lambda_i} \alpha_j A_j$.
4. Check whether or not M_i is invertible. If not, go back to Step 2.

6 Security analysis

In code-based cryptography, there are mainly two types of attacks on a cryptosystem, namely the structural attack and generic attack. Structural attacks aim to recover the 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 the knowledge of the private key. In what follows, we will investigate the security of our new cryptosystem from these two perspectives.

6.1 Structural attacks

Ever since Gabidulin et al. applied Gabidulin codes to the construction of public-key cryptosystems [2], many variants based on this family of codes have been proposed. Unfortunately, most of these schemes were completely broken due to the inherent structural vulnerability of Gabidulin codes. The best known structural attacks are the one proposed by Overbeck in [25] and some of its derivations [26, 27].

To prevent these attacks, Loidreau [4] proposed a new Gabidulin codes based cryptosystem, which can be seen as a rank metric counterpart of the BBCRS cryptosystem [24] based on GRS codes. In Loidreau's proposal, the secret code is disguised by multiplying a matrix whose inverse is taken over an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. This method of hiding information about the private key, as claimed by Loidreau in the paper, was 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.

In [29], Coggia and Couvreur proposed an effective method to distinguish the public code of Loidreau's proposal from general ones, and gave a practical key-recovery attack in the case of $\lambda = 2$ and the code rate being greater than $1/2$. Instead of operating the public code directly, Coggia and Couvreur considered the dual of the public code. Specifically, let $G_{pub} = GM^{-1}$ be the public matrix of Loidreau's proposal, where G is a generator matrix of an $[n, k]$ Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^m}$ and entries of M are contained in a λ-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. Denote by H a parity-check matrix of $\mathcal{G}$, then $H_{pub} = HM^T$ forms a parity-check matrix of the public code $\mathcal{G}_{pub} = \langle G_{pub} \rangle_{q^m}$. As for the dual code $\mathcal{G}_{pub}^{\perp} = \langle H_{pub} \rangle_{q^m}$, the Coggia-Couvreur distinguisher states that the following equality holds with high probability

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

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

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

Not long after Coggia and Couvreur's work, this attack was generalized to the case of $\lambda = 3$ by Ghatak [30] and then by Duc and Loidreau [31].

In our proposal, the public matrix is $G_{pub} = PC_k(\boldsymbol{g}^*) = \varphi(GM_1^{-1})M_2^{-1}$. Let H_{pub} be a parity-check matrix of the public code $\mathcal{G}_{pub} = \langle G_{pub} \rangle_{q^n}$, then there will be $H_{pub} = HM_2^T$ where H is a parity-check matrix of the code $\mathcal{C} = \langle \varphi(GM_1^{-1}) \rangle_{q^n}$. Apparently one can distinguish $\langle GM_1^{-1} \rangle_{q^n}^{\perp}$ from general codes using the Coggia-Couvreur distinguisher, but it does not work on $\mathcal{C}^{\perp}$. For instance, the following equality holds with high probability according to our experiments on Magma for the case of $\lambda_1 = 2, 3$

$$\dim_{q^n}(\mathcal{C}^{\perp} + \mathcal{C}^{\perp [1]} + \cdots + \mathcal{C}^{\perp [\lambda_1]}) = \min\{n, (\lambda_1+1)(n-k)\}.$$

Therefore, we believe that our proposal can resist the Coggia-Couvreur attack.

In a talk [32] at CBCrypto 2021, Loidreau proposed an attack to recover a decoder of the public code with a complexity of $\mathcal{O}(((\lambda n + (n-k)^2)m)^{\omega} q^{(\lambda-1)m})$. With this decoder one can decrypt any ciphertext in polynomial time. Similar to the Coggia-Couvreur attack, this attack also considered the dual of the public code. However, an applicable condition for this attack is that the public matrix can be decomposed as $G_{pub} = GM^{-1}$, where G is a generator matrix of a Gabidulin code or one of its subcodes and entries of M are contained in an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. Obviously the public matrix in our proposal does not satisfy this condition, which implies that this attack does not work on our new cryptosystem.

At the end of this section, we consider a potential brute-force attack against the duple $(\overline{\varphi}, \overline{\boldsymbol{m}}_1)$. Note that for any $\varphi' \in \overline{\varphi}$ and $\boldsymbol{m}_1' \in \overline{\boldsymbol{m}}_1$, there exists $\boldsymbol{m}_2' \in \mathbb{F}_{q^n}^n$ with $\mathrm{wt}_R(\boldsymbol{m}_2') = \lambda_2$ such that $G_{pub} = \varphi(GM_1{}^{-1})M_2^{-1} = \varphi'(GM_1'^{-1})M_2'^{-1}$, where $M_1' = PC_n(\boldsymbol{m}_1')$ and $M_2' = PC_n(\boldsymbol{m}_2')$. Let $G_{pub}' = PC_n(\boldsymbol{g}^*)$ and $G' = PC_n(\boldsymbol{g})$, then $G_{pub}' = \varphi(G'M_1^{-1})M_2^{-1} = \varphi'(G'M_1'^{-1})M_2'^{-1}$. This implies that one can compute $M_2' = {G_{pub}'}^{-1}\varphi'(G'M_1'^{-1})$. Furthermore, a straightforward verification shows that one can decrypt any ciphertext with the knowledge of $\varphi', \boldsymbol{m}_1', \boldsymbol{m}_2'$ and the public $\boldsymbol{g}$. Apparently the complexity of this brute-force attack by exhausting $(\overline{\varphi}, \overline{\boldsymbol{m}}_1)$ is $\mathcal{O}(\mathcal{N}(\overline{\varphi}) \cdot \mathcal{N}(\overline{\boldsymbol{m}}_1))$.

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 $G_{pub} = \varphi(GM_1^{-1})M_2^{-1} \in \mathcal{M}_{k,n}(\mathbb{F}_{q^n})$ be the public matrix, and $H_{pub} \in \mathcal{M}_{n-k,n}(\mathbb{F}_{q^n})$ be 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, we obtain an RSD instance of parameters (q, n, n, k, t). Solving this RSD instance by the combinatorial attacks listed in Table 1 and algebraic attacks listed in Table 2 will lead to the error vector $\boldsymbol{e}$, then we can recover the plaintext by solving the liear system $\boldsymbol{y} - \boldsymbol{e} = \boldsymbol{x}G_{pub}$.

7 Parameters and public-key sizes

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 $(\overline{\varphi}, \overline{\boldsymbol{m}}_1)$ described in Section 6.1, with a complexity of $\mathcal{O}(\mathcal{N}(\overline{\varphi}) \cdot \mathcal{N}(\overline{\boldsymbol{m}}_1))$. The public key in 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 suggested parameters for the security level of 128 bits, 192 bits and 256 bits. After that, we make a comparison on public-key size with some other code-based cryptosystems in Table 4. It is easy to see 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	138
2	60	120	64	2	2	2	1800	197
2	72	144	72	2	2	2	2592	257

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

8 Conclusion

In this paper, we introduced a novel transformation in coding theory, which was defined as an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. According to their performance when acting on linear codes over $\mathbb{F}_{q^m}$, these transformations were divided into two categories, namely the fully linear transformation and semilinear transformation. As an application of semilinear transformations, a new technique was developed to conceal the secret information in code-based cryptosystems. To obtain a small public-key size, we exploited the so-called partial cyclic Gabidulin code to construct an encryption scheme, whose security does not rely on the confidentiality of the underlying Gabidulin code. According to our analysis, this cryptosystem can resist the existing structural attacks, and admits a much smaller public-key size compared to some other code-based cryptosystems. For instance, only 2592 bytes are enough for our proposal to achieve the security of 256 bits, 403 times smaller than that of Classic McEliece moving onto the third round of the NIST PQC standardization process.

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.

Security / Instance	128	192	256
Classic McEliece [1]	261120	524160	1044992
NTS-KEM [33]	319488	929760	1419704
KRW [34]			578025
Guo-Fu II [11]	79358	212768	393422
Guo-Fu I [11]	8021	20149	37005
LIGA [35]	5618	9565	13823
HQC [36]	2249	4522	7245
BIKE [37]	1540	3082	5121
Lau-Tan [6]	2421	3283	4409
Our proposal	1513	1800	2592

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

61971243), the Natural Science Foundation of Tianjin (20JCZDJC00610), and the Fundamental Research Funds for the Central Universities of China (Nankai University).

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 October 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, Ø. (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.: Two public-key cryptosystems based on expanded Gabidulin codes. arXiv: 2107. 01610v2 [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] 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).

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

[26] 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).

[27] 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).

[28] 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).

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

[30] Ghatak, A: Extending Coggia–Couvreur attack on Loidreau's rank-metric cryptosystem. Des. Codes Cryptogr. (2021). https://doi.org/10.1007/s10623-021-00972-7.

[31] Duc, P.B., Loidreau, P.: An analysis of Coggia-Couvreur Attack on Loidreau's Rank-metric public-key encryption scheme in the general case. https://drive.google.com/file/d/1Br7dqMUs2MZPvqVhzU4lf-Zi_iBIvn9y/view. Accessed July 1, 2021.

[32] Loidreau, P.: Analysing the key recovery complexity for a rank-metric code-based cryptosystem. https://drive.google.com/file/d/1FuMgqm0NfGMJOxaZyrIrI1OWn0UICwPo/view. Accessed July 1, 2021.

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

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

[35] 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).

[36] 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.

[37] 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.

[38] 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).

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

[40] 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).

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