Expanded Gabidulin Codes and Their Application to Cryptography

Wenshuo Guo[1] and Fang-Wei Fu[2]

Abstract

This paper presents a new family of linear codes, namely the expanded Gabidulin codes. Exploiting the existing fast decoder of Gabidulin codes, we propose an efficient algorithm to decode these new codes when the noise vector satisfies a certain condition. Further more, these new codes enjoy an excellent error-correcting capability because of the optimality of their parent Gabidulin codes. Based on different masking techniques, we give two encryption schemes by using expanded Gabidulin codes in the McEliece setting. According to our analysis, both of these two cryptosystems can resist the existing structural attacks. Compared to some other code-based cryptosystems, our proposals have obvious advantage in public-key representation without using the cyclic or quasi-cyclic structure.

1 Introduction

Over the past decades, cryptosystems based on coding theory have been drawing more and more attention due to the rapid development of quantum computers. The first code-based cryptosystem, known as the McEliece cryptosystem [1] based on Goppa codes, was proposed by McEliece in 1978. The principle for McEliece's proposal is to first encode the plaintext with a random generator matrix of the underlying Goppa code and then add some random errors. Since then various studies [2–6] have been made to investigate the security of the McEliece cryptosystem. Apart from some weak keys, the McEliece cryptosystem still remains secure in general cases.

In addition to potential resistance against quantum computer attacks, McEliece system has pretty fast encryption and decryption procedures. However, this system has never been used in practice due to its large public key size. To overcome this problem, some variants were proposed one after another. For instance, the authors in [7] proposed to use the automorphism groups of Goppa codes to build decodable error patterns of larger weight, which greatly enhances the system against decoding attacks. By doing this, smaller codes are allowed in the design of encryption schemes to reduce the public-key size. Unfortunately, this variant was shown to be vulnerable against the CPAs proposed in [8]. In [9], the authors proposed the family of quasi-dyadic Goppa codes, which admit a very compact representation of parity-check or generator matrix, for efficiently designing syndrome-based cryptosystems. However, the authors in [10] mounted an efficient key-recovery attack against this variant for almost all the proposed parameters.

[1]E-mail: ws_guo@mail.nankai.edu.cn
[2]E-mail: fwfu@nankai.edu.cn

Besides endowing Goppa codes with some special structures, replacing Goppa codes with other families of codes is another approach to shorten the public keys. For instance, Niederreiter [11] introduced a knapsack-type cryptosystem based on GRS codes. In Niederreiter's proposal, the message sender first converts the plaintext into a vector of fixed weight and then multiplys it with a parity-check matrix of the public code. The advantage of GRS codes lies in their optimal error-correcting capability, which enables us to reduce the public-key size by exploiting codes with smaller parameters. However, this variant was proved to be insecure by Sidelnikov and Shestakov in [12] for the reason that GRS codes are highly structured. But if we use Goppa codes in the Niederreiter setting, it was proved to be equivalent to the McEliece system in terms of security [13].

To strengthen resistance against structural attacks, the authors in [14] performed a column-mixing transformation instead of a simple permutation to the underlying GRS code. According to their analysis, this variant could prevent some well-known attacks, such as the Sidelnikov-Shestakov attack [12] and Wieschebrink's attack [15]. However, in [16] the authors presented a polynomial key-recovery attack in some cases. Although one can adjust the parameters to prevent such an attack, it would introduce some other problems such as the decryption complexity increasing dramatically and a higher request of error-correcting capability for the underlying code.

In [18] Gabiduin introduced a new family of rank metric codes, namely the Gabidulin codes, which can be seen as an analogue of GRS codes but endowed with the rank metric. The particular appeal of the rank metric is that the general decoding problem is much more difficult than that in the Hamming metric [19, 20]. This inspires us to obtain much smaller public-key sizes by building cryptosystems in the rank metric. In [21] the authors proposed the GPT cryptosystem by using Gabidulin codes in the McEliece setting, which requires only a few thousands bits for a security of 100 bits. Just like GRS codes based schemes, the GPT cryptosystem and some of its variants [22–25] have been subjected to many structural attacks [26–29] because of Gabidulin codes being highly structured. Faure and Loidreau proposed another rank metric code based cryptosystem [30] that is quite different from the GPT proposal. The security of this scheme can be reduced to the intractability of the problem of reconstructing linearized polynomials. Until the work in [31], the Faure-Loidreau scheme had never been severely attacked.

In [32] Loidreau designed a rank code based cryptosystem in the McEliece setting, in which the author imposed a column-mixing transformation to the secret code with the inverse of an invertible matrix whose entries are taken from an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension λ. Loidreau claimed that his proposal could prevent all the existing structural attacks. However, this claim was proved to be invalidated by the authors in [33] for the case of $\lambda = 2$ and the code rate being greater than $1/2$. Not long after this, the author in [34] generalized this attack to the case where $\lambda > 2$ and the code rate is greater than $1 - \frac{1}{\lambda}$.

In [17], the authors introduced the concept of expanded GRS codes and designed an encryption scheme by using these codes in the Niederreiter setting. Our work in the present paper is inspired by this variant but uses the so-called expanded Gabidulin codes as the underlying codes. Benefitting from the optimality of their parent Gabidulin codes, these new codes have excellent capability of correcting Hamming errors. This enables us to make a reduction in public-key sizes by exploiting smaller codes. Meanwhile, our proposals could resist the existing structural attacks such as Overbeck's attack, and some potential attack according to our analysis.

The remaining part of this paper is arranged as follows. In Section 2, notations and some basic concepts about rank metric codes will be given. In Section 3, we will introduce the so-called expanded Gabidulin codes, make a research on some of their algebraic properties, and propose an

efficient decoding algorithm for these new codes. Section 4 is devoted to the descripton of our two proposals. In Section 5 we present the security analysis of our proposals, including structural attacks and generic attacks. In Section 6, we give some suggested parameters for different security levels and make a comparison on public-key sizes with some other code-based cryptosystems. Following this, we will make a few concluding remarks in Section 7.

2 Preliminaries

2.1 Notations

Let q be a prime power. Denote by $\mathbb{F}_q$ a finite field with q elements, and by $\mathbb{F}_{q^m}$ an extension field of $\mathbb{F}_q$ of degree m. For two positive integers k and n, let $\mathcal{M}_{k,n}(\mathbb{F}_q)$ denote the space of all $k \times n$ matrices over $\mathbb{F}_q$, and $GL_n(\mathbb{F}_q)$ denote the general linear group formed by all invertible matrices in $\mathcal{M}_{n,n}(\mathbb{F}_q)$. For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, let $\langle M \rangle_{\mathbb{F}_{q^m}}$ be the vector space spanned by rows of M over $\mathbb{F}_{q^m}$.

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 full-rank matrix G is called a generator matrix of $\mathcal{C}$ if its row vectors form a basis of $\mathcal{C}$. A generator matrix H of the dual code $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$. For a codeword $\boldsymbol{c} \in \mathcal{C}$, the Hamming weight of $\boldsymbol{c}$, denoted by $w_H(\boldsymbol{c})$, is the number of nonzero coordinates of $\boldsymbol{c}$. The minimum Hamming distance of $\mathcal{C}$ is defined as the minimum Hamming weight of nonzero codewords in $\mathcal{C}$.

2.2 Rank metric codes

Now we recall some basic concepts about rank metric codes.

Definition 1. Let $\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_{q^m}^n$, the rank support of $\boldsymbol{x}$, denoted by $\mathrm{Supp}_R(\boldsymbol{x})$, is defined to be the linear space spanned by coordinates of $\boldsymbol{x}$ over $\mathbb{F}_q$. Formally we have

$$\mathrm{Supp}_R(\boldsymbol{x}) = \left\{ \sum_{i=1}^{n} \lambda_i x_i : \lambda_i \in \mathbb{F}_q, 1 \leqslant i \leqslant n \right\}.$$

Definition 2. For a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, the rank weight of $\boldsymbol{x}$, denoted by $w_R(\boldsymbol{x})$, is defined to be the dimension of $\mathrm{Supp}_R(\boldsymbol{x})$ over $\mathbb{F}_q$. Formally we have

$$w_R(\boldsymbol{x}) = \dim_q \big(\mathrm{Supp}_R(\boldsymbol{x})\big).$$

Definition 3. For two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$, the rank distance between $\boldsymbol{x}$ and $\boldsymbol{y}$, denoted by $d_R(\boldsymbol{x}, \boldsymbol{y})$, is defined to be the rank weight of $\boldsymbol{x} - \boldsymbol{y}$. Formally we have

$$d_R(\boldsymbol{x}, \boldsymbol{y}) = w_R(\boldsymbol{x} - \boldsymbol{y}).$$

Definition 4. For a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, the minimum rank distance of $\mathcal{C}$, denoted by $d(\mathcal{C})$, is defined to be the minimum rank weight of nonzero codewords in $\mathcal{C}$. Formally we have

$$d(\mathcal{C}) = \min\{w_R(\boldsymbol{c}) : \boldsymbol{c} \in \mathcal{C} \text{ and } \boldsymbol{c} \neq \boldsymbol{0}\}.$$

A linear code endowed with the rank metric is call a rank metric code. Similar to Hamming metric codes, the minimum rank distance of a rank metric code is bounded from above by the Singleton-type bound defined as follows.

Definition 5 (Singleton-type bound). For an $[n, k]$ rank metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, the minimum rank distance of $\mathcal{C}$ with respect to $\mathbb{F}_q$ satisfies the following inequality

$$d(\mathcal{C}) \leqslant n - k + 1.$$

Remark 1. A rank metric code attaining the Singleton-type bound is called a Maximum Rank Distance (MRD) code. Suppose $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is an $[n, k]$ MRD code, and let $\boldsymbol{c} \in \mathcal{C}$ be a codeword having the minimum Hamming weight. It is easy to see that $n - k + 1 \leqslant w_R(\boldsymbol{c}) \leqslant w_H(\boldsymbol{c}) \leqslant n - k + 1$. Hence we have $w_H(\boldsymbol{c}) = n - k + 1$, which enables us to conclude that an MRD code is MDS in the Hamming metric.

2.3 Gabidulin codes

Before giving the definition of Gabidulin codes, we shall introduce the concept of linearized polynomials. A linearized polynomial $f(x) \in \mathbb{F}_{q^m}[x]$ is a polynomial of the form

$$f(x) = \sum_{i=0}^{s} p_i x^{q^i}, \text{ where } p_i \in \mathbb{F}_{q^m}.$$

The q-degree of $f(x)$, denoted by $\deg_q(f)$, is the largest i such that $p_i \neq 0$.

Let $\mathcal{L}$ be the set of all linearized polynomials over $\mathbb{F}_{q^m}$. For a positive integer s, let $\mathcal{L}_{<s}$ be the set of linearized polynomials of q-degree less than s, namely we have

$$\mathcal{L}_{<s} = \{f(x) \in \mathcal{L} : \deg_q(f) < s\}.$$

Definition 6 (Gabidulin codes). For positive integers $k \leqslant n \leqslant m$ and a vector $\boldsymbol{g} = (g_1, \cdots, g_n) \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{g}) = n$, the Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{g})$ generated by $\boldsymbol{g}$ with length n and dimension k is defined to be

$$\mathrm{Gab}_{n,k}(\boldsymbol{g}) = \{(f(g_1), \cdots, f(g_n)) : f(x) \in \mathcal{L}_{<k}\}.$$

Equivalently, the Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{g})$ is defined to be a linear code having a generator matrix of the form

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

Similar to GRS codes in the Hamming metric, Gabidulin codes admit excellent error-correcting capability and simple algebraic structure. The following two theorems describe some properties of Gabidulin codes.

Theorem 7. *[35] A Gabidulin code is an MRD code. In other words, the minimum rank weight of* $\mathrm{Gab}_{n,k}(\boldsymbol{g})$ *attains the Singleton-type bound for rank metric codes.*

This implies that the Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{g})$ can correct up to $\lfloor \frac{n-k}{2} \rfloor$ rank errors, which is an important reason for Gabidulin codes being widely used in the design of cryptosystems.

Theorem 8. *[31] The dual of a Gabidulin code is also a Gabidulin code. Particularly, we have* $\mathrm{Gab}_{n,k}(\boldsymbol{g})^\perp = \mathrm{Gab}_{n,n-k}(\boldsymbol{h}^{q^{-(n-k-1)}})$ *for some* $\boldsymbol{h} \in \mathrm{Gab}_{n,n-1}(\boldsymbol{g})^\perp$ *with* $w_R(\boldsymbol{h}) = n$.

3 Expanded Gabidulin codes

3.1 Introducing expanded Gabidulin codes

Note that $\mathbb{F}_{q^m}$ can be regarded as an $\mathbb{F}_q$-linear space of dimension m. Suppose that $\mathcal{B} = \{\alpha_1, \alpha_2, \cdots, \alpha_m\} \subset \mathbb{F}_{q^m}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For any $\alpha \in \mathbb{F}_{q^m}$, there exists $(a_1, a_2, \cdots, a_m) \in \mathbb{F}_q^m$ such that $\alpha = \sum_{i=1}^m a_i\alpha_i$. Based on this observation, we define an $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$ with respect to $\mathcal{B}$ as follows

$$\begin{aligned} \phi_{\mathcal{B}} &: \mathbb{F}_{q^m} \mapsto \mathbb{F}_q^m, \\ \phi_{\mathcal{B}}(\alpha) &= (a_1, a_2, \cdots, a_m). \end{aligned}$$

As for a vector $\boldsymbol{v} = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_{q^m}^n$, we define $\phi_{\mathcal{B}}(\boldsymbol{v})$ to be the vector formed by performing the map $\phi_{\mathcal{B}}$ to each coordinate of $\boldsymbol{v}$, namely we have

$$\phi_{\mathcal{B}}(\boldsymbol{v}) = (\phi_{\mathcal{B}}(v_1), \phi_{\mathcal{B}}(v_2), \cdots, \phi_{\mathcal{B}}(v_n)) \in \mathbb{F}_q^{mn}.$$

Theoretically we can always compute $\phi_{\mathcal{B}}(\alpha)$ for any $\alpha \in \mathbb{F}_{q^m}$, but the authors in [17] did not specify how to do this in practice. Now we give an effective method of performing this operation, which is based on the following theorem.

Theorem 9. *Let $\mathcal{B} = \{\alpha_1, \cdots, \alpha_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, then there exists $\mathcal{B}^* = \{\alpha_1^*, \cdots, \alpha_m^*\} \subset \mathbb{F}_{q^m}$ such that for $1 \leqslant i, j \leqslant m$ we have*

$$\mathrm{Tr}(\alpha_i\alpha_j^*) = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j, \end{cases} \tag{1}$$

where $\mathrm{Tr}(\cdot)$ denotes the trace function $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$. Further more, the set $\mathcal{B}^*$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Proof. Assume that $\alpha_i^* = \sum_{j=1}^m a_{ij}\alpha_j$ where $a_{ij} \in \mathbb{F}_q$ for $1 \leqslant i \leqslant m$, then we have

$$\begin{cases} \mathrm{Tr}(\alpha_1\alpha_i^*) = \sum_{j=1}^m a_{ij}\mathrm{Tr}(\alpha_1\alpha_j) = 0, \\ \qquad\qquad \vdots \\ \mathrm{Tr}(\alpha_i\alpha_i^*) = \sum_{j=1}^m a_{ij}\mathrm{Tr}(\alpha_i\alpha_j) = 1, \\ \qquad\qquad \vdots \\ \mathrm{Tr}(\alpha_m\alpha_i^*) = \sum_{j=1}^m a_{ij}\mathrm{Tr}(\alpha_m\alpha_j) = 0. \end{cases} \tag{2}$$

Let Q be the coefficient matrix of (2), namely

$$Q = \begin{pmatrix} \mathrm{Tr}(\alpha_1\alpha_1) & \mathrm{Tr}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}(\alpha_1\alpha_m) \\ \mathrm{Tr}(\alpha_2\alpha_1) & \mathrm{Tr}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}(\alpha_m\alpha_1) & \mathrm{Tr}(\alpha_m\alpha_2) & \cdots & \mathrm{Tr}(\alpha_m\alpha_m) \end{pmatrix}.$$

It is easy to see that $Q \in \mathcal{M}_{n,n}(\mathbb{F}_q)$. Now we prove the invertibility of Q by contradiction. Assume that Q is singular, then there exists $\boldsymbol{\lambda} = (\lambda_1, \cdots, \lambda_m) \in \mathbb{F}_q^m \backslash \{\mathbf{0}\}$ such that $\boldsymbol{\lambda}Q = \mathbf{0}$. This

yields the following equations

$$\mathrm{Tr}(\alpha_1 \sum_{i=1}^{m} \lambda_i \alpha_i) = \cdots = \mathrm{Tr}(\alpha_m \sum_{i=1}^{m} \lambda_i \alpha_i) = 0.$$

Let $\beta_j = \alpha_j \sum_{i=1}^{m} \lambda_i \alpha_i \, (1 \leqslant j \leqslant m)$, then apparently $\beta_1, \cdots, \beta_m$ form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ because of $\sum_{i=1}^{m} \lambda_i \alpha_i \neq 0$. For any $\alpha \in \mathbb{F}_{q^m}$, there exist $a_1, \cdots, a_m \in \mathbb{F}_q$ such that $\alpha = \sum_{j=1}^{m} a_j \beta_j$. Further more, we have

$$\mathrm{Tr}(\alpha) = \sum_{j=1}^{m} a_j \mathrm{Tr}(\beta_j) = 0.$$

This enables us to obtain q^m roots of $\mathrm{Tr}(\cdot) = 0$, which contradicts the fact that $\mathrm{Tr}(\cdot)$ is a ploynomial of degree q^{m-1}. Hence the assumption does not hold and Q is invertible.

Let $\boldsymbol{a} = (\alpha_1, \cdots, \alpha_m)$ and Q_i be the i-th column of Q^{-1}, then we have $\alpha_i^* = \boldsymbol{a} Q_i \, (1 \leqslant i \leqslant m)$. Therefore we can obtain $\mathcal{B}^*$ by computing $\boldsymbol{a} Q^{-1}$, and apparently $\mathcal{B}^*$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. This concludes the proof. □

Remark 2. A set $\mathcal{B}^*$ that satisfies the condition (1) is called a dual basis of $\mathcal{B}$. Further more, it is easy to see that $\mathcal{B}^*$ is uniquely determined by $\mathcal{B}$. For any $\alpha \in \mathbb{F}_{q^m}$, assume that $a_1, \cdots, a_m \in \mathbb{F}_q$ satisfy $\alpha = \sum_{i=1}^{m} a_i \alpha_i$. Then we can obtain $a_j \, (1 \leqslant j \leqslant m)$ by computing $\mathrm{Tr}(\alpha \alpha_j^*)$ since

$$\begin{aligned} \mathrm{Tr}(\alpha \alpha_j^*) &= \mathrm{Tr}(\sum_{i=1}^{m} a_i \alpha_i \alpha_j^*) \\ &= \sum_{i=1}^{m} a_i \mathrm{Tr}(\alpha_i \alpha_j^*) \\ &= a_j. \end{aligned}$$

Finally we have $\phi_{\mathcal{B}}(\alpha) = (\mathrm{Tr}(\alpha \alpha_1^*), \cdots, \mathrm{Tr}(\alpha \alpha_m^*))$.

Now we formally introduce the concept of expanded Gabidulin codes.

Definition 10 (Expanded Gabidulin codes). Let $\mathcal{G}$ be an $[n, k]$ Gabidulin code over $\mathbb{F}_{q^m}$. For a basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, let $\phi_{\mathcal{B}}$ be the $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$ induced by $\mathcal{B}$. The expanded code of $\mathcal{G}$ with respect to $\phi_{\mathcal{B}}$ is defined as

$$\bar{\mathcal{G}} = \{\phi_{\mathcal{B}}(\boldsymbol{c}) : \boldsymbol{c} \in \mathcal{G}\}.$$

We call $\mathcal{G}$ the parent Gabidulin code of $\bar{\mathcal{G}}$.

The following theorem gives a method of constructing a generator (parity-check) matrix of an expanded Gabidulin code when we already know a generator (parity-check) matrix of its parent Gabidulin code.

Theorem 11. *Let $\mathcal{G} \subseteq \mathbb{F}_{q^m}^n$ be an $[n, k]$ Gabidulin code and $\mathcal{B} = \{\alpha_1, \cdots, \alpha_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The expanded code $\bar{\mathcal{G}}$ of $\mathcal{G}$ with respect to $\phi_{\mathcal{B}}$ is a linear code of length mn and dimension mk. Further more, we have the following two conclusions.*

(1) Suppose $G = \left[\boldsymbol{g}_1, \cdots, \boldsymbol{g}_k\right]^T$ *is a generator matrix of* $\mathcal{G}$*, then* $\bar{\mathcal{G}}$ *has an* $mk \times mn$ *generator matrix of the form*

$$\bar{G} = \left[\phi_{\mathcal{B}}(\alpha_1 \boldsymbol{g}_1), \cdots, \phi_{\mathcal{B}}(\alpha_m \boldsymbol{g}_1), \cdots, \phi_{\mathcal{B}}(\alpha_1 \boldsymbol{g}_k), \cdots, \phi_{\mathcal{B}}(\alpha_m \boldsymbol{g}_k)\right]^T.$$

(2) Let $H = \left[\boldsymbol{h}_1^T, \boldsymbol{h}_2^T, \cdots, \boldsymbol{h}_n^T\right]$ *be a parity-check matrix of* $\mathcal{G}$*, then*

$$\bar{H} = \left[\phi_{\mathcal{B}}(\alpha_1 \boldsymbol{h}_1)^T, \cdots, \phi_{\mathcal{B}}(\alpha_m \boldsymbol{h}_1)^T, \cdots, \phi_{\mathcal{B}}(\alpha_1 \boldsymbol{h}_n)^T, \cdots, \phi_{\mathcal{B}}(\alpha_m \boldsymbol{h}_n)^T\right] \tag{3}$$

forms a parity-check matrix of $\bar{\mathcal{G}}$*.*

Proof. (1) Firstly, it is easy to verify that $\bar{\mathcal{G}}$ forms a linear code over $\mathbb{F}_q$. Together with $|\bar{\mathcal{G}}| = |\mathcal{G}| = q^{mk}$, we have $\dim_q(\bar{\mathcal{G}}) = \log_q(|\bar{\mathcal{G}}|) = mk$. Apparently each row vector $\phi_{\mathcal{B}}(\alpha_i \boldsymbol{g}_j)$ of $\bar{G}$ $(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k)$ is contained in $\bar{\mathcal{G}}$. In the remaining part, it suffices to prove that $\bar{G}$ is of full rank.

Suppose that there exists a vector

$$\boldsymbol{x} = (x_{11}, \cdots, x_{m1}, \cdots, x_{1k}, \cdots, x_{mk}) \in \mathbb{F}_q^{mk}$$

such that $\boldsymbol{x}\bar{G} = \boldsymbol{0}$, then we have

$$\begin{aligned}
\boldsymbol{x}\bar{G} &= \sum_{j=1}^{k} \sum_{i=1}^{m} x_{ij} \phi_{\mathcal{B}}(\alpha_i \boldsymbol{g}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{k} \sum_{i=1}^{m} x_{ij} \alpha_i \boldsymbol{g}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{k} \beta_j \boldsymbol{g}_j) \\
&= \boldsymbol{0},
\end{aligned}$$

where $\beta_j = \sum_{i=1}^{m} x_{ij}\alpha_i$ $(1 \leqslant j \leqslant k)$.

By performing the inverse of $\phi_{\mathcal{B}}$ to both sides of the last equation, we can obtain $\sum_{j=1}^{k} \beta_j \boldsymbol{g}_j = (\beta_1, \cdots, \beta_k)G = \boldsymbol{0}$. This implies that $\beta_j = 0$ for $1 \leqslant j \leqslant k$. Further more, for $1 \leqslant j \leqslant k$ we have $x_{ij} = 0$ $(1 \leqslant i \leqslant m)$ because of $\alpha_1, \cdots, \alpha_m$ being a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Finally, we come to the conclusion that $\boldsymbol{x}\bar{G} = \boldsymbol{0}$ holds if and only if $\boldsymbol{x} = \boldsymbol{0}$, which means that $\bar{G}$ is of full rank.

(2) We first show that each row vector of $\bar{H}$ is contained in the dual code of $\bar{\mathcal{G}}$. For any $\bar{\boldsymbol{c}} = (c_{11}, \cdots, c_{m1}, \cdots, c_{1n}, \cdots, c_{mn}) \in \bar{\mathcal{G}}$, there exists $\boldsymbol{c} = (c_1, \cdots, c_n) \in \mathcal{G}$ such that $\bar{\boldsymbol{c}} = \phi_{\mathcal{B}}(\boldsymbol{c})$. By $\boldsymbol{c}H^T = \boldsymbol{0}$, we have

$$\begin{aligned}
\bar{\boldsymbol{c}}\bar{H}^T &= \sum_{j=1}^{n} \sum_{i=1}^{m} c_{ij} \phi_{\mathcal{B}}(\alpha_i \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{n} \sum_{i=1}^{m} c_{ij} \alpha_i \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{n} c_j \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\boldsymbol{c}H^T) \\
&= \boldsymbol{0}.
\end{aligned}$$

This implies that each row vector of $\bar{H}$ is contained in $\bar{\mathcal{G}}^{\perp}$.

It remains to prove that $\bar{H}$ is of full rank. To do this, it suffices to prove that there exist $m(n-k)$ columns of $\bar{H}$ linearly independent over $\mathbb{F}_q$. Without loss of generality, we consider the first $m(n-k)$ columns of $\bar{H}$ and let $\bar{H}_s$ be a submatrix of $\bar{H}$ formed by these columns. Suppose that

$$\boldsymbol{x} = (x_{11}, \cdots, x_{m1}, \cdots, x_{1r}, \cdots, x_{mr}) \in \mathbb{F}_q^{mr}$$

satisfies $\boldsymbol{x}\bar{H}_s^T = \mathbf{0}$ where $r = n - k$, then we have

$$\begin{aligned}
\boldsymbol{x}\bar{H}_s^T &= \sum_{j=1}^{r}\sum_{i=1}^{m} x_{ij}\phi_{\mathcal{B}}(\alpha_i \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{r}\sum_{i=1}^{m} x_{ij}\alpha_i \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{r} \beta_j \boldsymbol{h}_j) \\
&= \mathbf{0},
\end{aligned}$$

where $\beta_j = \sum_{i=1}^{m} x_{ij}\alpha_i \, (1 \leqslant j \leqslant r)$.

By performing the inverse of $\phi_{\mathcal{B}}$ to both sides of the last equation, we can obtain $\sum_{j=1}^{r} \beta_j \boldsymbol{h}_j = (\beta_1, \cdots, \beta_r)H_s^T = \mathbf{0}$, where H_s is the first r columns of H. Since Gabidulin codes are MDS in the Hamming metric, any r columns of H are linearly independent over $\mathbb{F}_{q^m}$. Hence $\beta_j = 0 \, (1 \leqslant j \leqslant r)$ and furthermore we have $\boldsymbol{x} = \mathbf{0}$ because of $\alpha_1, \cdots, \alpha_m$ being linearly independent over $\mathbb{F}_q$. This implies that $\bar{H}_s$ is of full rank and hence the conclusion is proved. □

We already know that Gabidulin codes are optimal in both Hamming metric and rank metric. However, expanded Gabidulin codes are far from optimal in the Hamming metric according to our analysis. Specially, we have the following theorem.

Theorem 12. *Let $\mathcal{G}$ be an $[n, k]$ Gabidulin code over $\mathbb{F}_{q^m}$. For a given basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, denote by $\bar{\mathcal{G}}$ the expanded code of $\mathcal{G}$ under the $\mathbb{F}_q$-linear isomorphism $\phi_{\mathcal{B}}$. Then the minimum Hamming distance of $\bar{\mathcal{G}}$ satisfies the following inequality*

$$n - k + 1 \leqslant d(\bar{\mathcal{G}}) \leqslant m(n-k) + 1.$$

In particular, with a proper choice of $\mathcal{B}$, the minimum Hamming distance of $\bar{\mathcal{G}}$ can reach to $n-k+1$.

Proof. For any $\bar{\boldsymbol{u}} \in \bar{\mathcal{G}}$, there exists $\boldsymbol{u} = (u_1, \cdots, u_n) \in \mathcal{G}$ such that $\bar{\boldsymbol{u}} = \phi_{\mathcal{B}}(\boldsymbol{u})$. Since $\mathcal{G}$ is MDS in the Hamming metric, there must be $w_H(\boldsymbol{u}) \geqslant n - k + 1$. Let $I = \{1 \leqslant i \leqslant n : u_i \neq 0\}$, then $|I| \geqslant n - k + 1$. Apparently $w_H(\bar{\boldsymbol{u}}) = \sum_{i \in I} w_H(\phi_{\mathcal{B}}(u_i)) \geqslant n - k + 1$ because of $w_H(\phi_{\mathcal{B}}(\alpha)) \geqslant 1$ for any $\alpha \in \mathbb{F}_{q^m}^*$. Hence we have $d(\bar{\mathcal{G}}) \geqslant n - k + 1$. On the other hand, by the Singleton bound for Hamming metric codes, it is easy to see that $d(\bar{\mathcal{G}}) \leqslant m(n-k) + 1$.

Let $\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathcal{G}$ with $w_H(\boldsymbol{v}) = n - k + 1$, and let $S = \{v_i \neq 0 : 1 \leqslant i \leqslant n\}$. If $S \subset \mathcal{B}$, then $w_H(\phi_{\mathcal{B}}(\boldsymbol{v})) = \sum_{i \in I} w_H(\phi_{\mathcal{B}}(v_i)) = n - k + 1$ because of $w_H(\phi_{\mathcal{B}}(\alpha)) = 1$ for any $\alpha \in \mathcal{B}$. This implies that $d(\bar{\mathcal{G}}) = n - k + 1$. □

3.2 Decoding expanded Gabidulin codes

As for Gabidulin codes, several efficient decoding algorithms already exist [18, 36, 37]. In this part, we mainly study the decoding problem of expanded Gabidulin codes. Our analysis shows that when the noise vector satisfies a certain condition, the original decoding problem can be reduced to decoding the parent Gabidulin codes.

Let $\mathcal{G} \subseteq \mathbb{F}_{q^m}^n$ be an $[n, k]$ Gabidulin code having H as a parity-check matrix. Denote by $\bar{\mathcal{G}}$ an expanded code of $\mathcal{G}$ induced by some $\mathbb{F}_q$-linear isomorphism $\phi_{\mathcal{B}}$. Suppose $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ is the received word, where $\boldsymbol{c} \in \bar{\mathcal{G}}$ and $\boldsymbol{e} = (\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n) \in \mathbb{F}_q^{mn}$ is the noise vector with $\boldsymbol{e}_j = (e_{1j}, \cdots, e_{mj}) \in \mathbb{F}_q^m \, (1 \leqslant j \leqslant n)$. Let E be an $n \times m$ matrix over $\mathbb{F}_q$, of which the j-th row vector is $\boldsymbol{e}_j$. If $\mathrm{Rank}(E) \leqslant \lfloor \frac{n-k}{2} \rfloor$, then we can design a fast decoder $\mathscr{D}_{\bar{\mathcal{G}}}$ for $\bar{\mathcal{G}}$ to decode $\boldsymbol{y}$ by exploiting the syndrome decoding procedure of $\mathcal{G}$.

Denote by $\bar{H}$ a parity-check matrix of $\bar{\mathcal{G}}$. It is easy to see that

$$\begin{aligned}
\boldsymbol{y}\bar{H}^T &= \boldsymbol{e}\bar{H}^T \\
&= \sum_{j=1}^{n}\sum_{i=1}^{m} e_{ij}\phi_{\mathcal{B}}(\alpha_i \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{n}\sum_{i=1}^{m} e_{ij}\alpha_i \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\sum_{j=1}^{n} e_j^* \boldsymbol{h}_j) \\
&= \phi_{\mathcal{B}}(\boldsymbol{e}^* H^T),
\end{aligned}$$

where $\boldsymbol{e}^* = (e_1^*, \cdots, e_n^*)$ with $e_j^* = \sum_{i=1}^{m} e_{ij}\alpha_i \, (1 \leqslant j \leqslant n)$. Since $w_R(\boldsymbol{e}^*) = \mathrm{Rank}(E) \leqslant \lfloor \frac{n-k}{2} \rfloor$, applying the decoding procedure of $\mathcal{G}$ to $\phi_{\mathcal{B}}^{-1}(\boldsymbol{y}\bar{H}^T) = \boldsymbol{e}^* H^T$ will lead to $\boldsymbol{e}^*$. Hence we can recover $\boldsymbol{e}$ by computing $\phi_{\mathcal{B}}(\boldsymbol{e}^*)$ and then the codeword $\boldsymbol{c}$ can be computed as $\boldsymbol{y} - \boldsymbol{e}$.

Apparently four steps are needed to decode expanded Gabidulin codes. Firstly, we shall compute the syndrome of the received word $\boldsymbol{y}$, which requires an operation of multiplying $\boldsymbol{y}$ and $\bar{H}^T$ together with a complexity of $\mathcal{O}(m^2 n(n-k))$ in $\mathbb{F}_q$. Secondly, we shall perform the inverse transformation of $\phi_{\mathcal{B}}$ to the syndrome obtained in the first step, requiring a complexity of $\mathcal{O}(mn)$ in $\mathbb{F}_{q^m}$. The third step shall call the fast decoder of the parent Gabidulin code to obtain an error vector $\boldsymbol{e}^*$ with $w_R(\boldsymbol{e}^*) \leqslant \lfloor \frac{n-k}{2} \rfloor$, which requires a complexity of $\mathcal{O}(\frac{5}{2}n^2 - \frac{3}{2}k^2)$ in $\mathbb{F}_{q^m}$ [36]. In the last step, we shall compute $\phi_{\mathcal{B}}(\boldsymbol{e}^*)$ through the method described in Remark 2 with a complexity of $\mathcal{O}(((m-1)(q-1)+1)mn)$ in $\mathbb{F}_{q^m}$. Finally the total complexity of decoding expanded Gabidulin codes is $\mathcal{O}(m^2 n(q-1) + mn(3-q) + \frac{5}{2}n^2 - \frac{3}{2}k^2)$ in $\mathbb{F}_{q^m}$ plus $\mathcal{O}(m^2 n(n-k))$ in $\mathbb{F}_q$.

4 Description of our proposals

4.1 Proposal I

Let $\mathcal{G} \subseteq \mathbb{F}_{q^m}^n$ be an $[n, k]$ Gabidulin code, correcting up to $t = \lfloor \frac{n-k}{2} \rfloor$ rank errors. Given a basis $\mathcal{B} = \{\alpha_1, \cdots, \alpha_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, let $\phi_{\mathcal{B}}$ be the $\mathbb{F}_q$-linear isomorphism induced by $\mathcal{B}$. Let $\bar{\mathcal{G}}$ be the expanded code of $\mathcal{G}$ with respect to $\phi_{\mathcal{B}}$. Denote by $\bar{H}$ a parity-check matrix of $\bar{\mathcal{G}}$ of the form (3).

For a positive integer $n-k<\lambda<m$, define $I_j=\{mj+1,\cdots,mj+\lambda\}$ for $0\leqslant j\leqslant n-1$. Let $S=\cup_{j=0}^{n-1}I_j$ and denote by $\bar{H}_S$ the submatrix of $\bar{H}$ being restricted to S. Let $\bar{\mathcal{G}}_S$ be the code that has $\bar{H}_S$ as a parity-check matrix and denote by $\bar{G}_S$ a generator matrix of $\bar{\mathcal{G}}_S$. It is easy to see that $\bar{\mathcal{G}}_S$ has length $N=\lambda n$ and dimension $K=\lambda n-m(n-k)$.

- Key generation
  Randomly choose a matrix $A\in GL_\lambda(\mathbb{F}_q)$. Denote by I_n the identity matrix of order n and set $T=I_n\otimes A$. Randomly choose a matrix $M\in GL_K(\mathbb{F}_q)$ such that $G_{pub}=M\bar{G}_ST^{-1}$ is of systematic form. We publish (G_{pub},t) as the public key, and keep $(\bar{H}_S,A,\mathscr{D}_{\bar{\mathcal{G}}})$ as the secret key.

- Encryption
  For a plaintext $\boldsymbol{x}\in\mathbb{F}_q^K$, randomly choose a matrix $E\in\mathcal{M}_{n,\lambda}(\mathbb{F}_q)$ with $\mathrm{Rank}(E)=t$. Let $\boldsymbol{e}=(\boldsymbol{e}_1,\cdots,\boldsymbol{e}_n)\in\mathbb{F}_q^N$, where $\boldsymbol{e}_i$ is the i-th row vector of E $(1\leqslant i\leqslant n)$. The ciphertext corresponding to $\boldsymbol{x}$ is computed as $\boldsymbol{y}=\boldsymbol{x}G_{pub}+\boldsymbol{e}$.

- Decryption
  For a ciphertext $\boldsymbol{y}\in\mathbb{F}_q^N$, let $\boldsymbol{e}'=\boldsymbol{e}T$ and compute

$$\boldsymbol{s}=\boldsymbol{y}T\bar{H}_S^T=\boldsymbol{x}M\bar{G}_ST^{-1}T\bar{H}_S^T+\boldsymbol{e}T\bar{H}_S^T=\boldsymbol{e}'\bar{H}_S^T.$$

  Applying the fast decoder $\mathscr{D}_{\bar{\mathcal{G}}}$ of $\bar{\mathcal{G}}$ to $\boldsymbol{s}$ will lead to a vector $\boldsymbol{e}''\in\mathbb{F}_q^{mn}$. The restriction of $\boldsymbol{e}''$ to S will be $\boldsymbol{e}'$, then we can recover $\boldsymbol{e}$ by computing $\boldsymbol{e}'T^{-1}$. The plaintext will be the restriction of $\boldsymbol{y}-\boldsymbol{e}$ to the first K coordinates.

Correctness of Decryption. Let $\boldsymbol{e}'=(\boldsymbol{e}'_1,\cdots,\boldsymbol{e}'_n)$, where $\boldsymbol{e}'_i=\boldsymbol{e}_iA$. Define $E'\in\mathcal{M}_{n,\lambda}(\mathbb{F}_q)$ to be the matrix whose i-th row vector is $\boldsymbol{e}'_i$. Let $\boldsymbol{e}''=(\boldsymbol{e}''_1,\cdots,\boldsymbol{e}''_n)$ where $\boldsymbol{e}''_i=(\boldsymbol{e}'_i,\boldsymbol{0})$ and $\boldsymbol{0}$ denotes the zero vector of length $m-\lambda$. Define $E''\in\mathcal{M}_{n,m}(\mathbb{F}_q)$ to be the matrix whose i-th row vector is $\boldsymbol{e}''_i$. It is easy to see that

$$E''=[E'|O]=[EA|O],$$

where O denotes the $n\times(m-\lambda)$ zero matrix. Apparently we have

$$\mathrm{Rank}(E'')=\mathrm{Rank}(E')=\mathrm{Rank}(E)=t,$$

which implies that $\boldsymbol{e}''$ satisfies the decodable condition given in Section 3.2. Then applying the fast decoder of $\bar{\mathcal{G}}$ to $\boldsymbol{s}=\boldsymbol{e}'\bar{H}_S^T=\boldsymbol{e}''\bar{H}^T$ will lead to $\boldsymbol{e}''$. The restriction of $\boldsymbol{e}''$ to S will be $\boldsymbol{e}'$.

4.2 Proposal II

Let $\mathcal{G}\subseteq\mathbb{F}_{q^m}^n$ be an $[n,k]$ Gabidulin code, correcting up to $\lfloor\frac{n-k}{2}\rfloor$ rank errors. For an $\mathbb{F}_q$-linear isomorphism $\phi_{\mathcal{B}}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$, let $\bar{\mathcal{G}}$ denote the expanded code of $\mathcal{G}$ induced by $\phi_{\mathcal{B}}$. According to Theorem 11, $\bar{\mathcal{G}}$ is a linear code of length $N=mn$ and dimension $K=mk$. Denote by $\bar{H}$ a parity-check matrix of $\bar{\mathcal{G}}$, and by $\bar{G}$ a generator matrix respectively. For a positive integer $\lambda\ll n$, let $u_f=\lfloor\frac{n}{\lambda}\rfloor$, $u_c=\lceil\frac{n}{\lambda}\rceil$ and $v=n-\lambda u_f$.

- Key generation
  Randomly choose an invertible matrix $A \in GL_{m\lambda}(\mathbb{F}_q)$ such that the $mv \times mv$ submatrix A_{sub} in the top left corner of A is also invertible. Set

$$T = \begin{pmatrix} A_{ten} & \\ & A_{sub} \end{pmatrix} \in GL_N(\mathbb{F}_q),$$

  where A_{ten} is the tensor product $I_{u_f} \otimes A$. Randomly choose an invertible matrix $M \in GL_K(\mathbb{F}_q)$ such that $G_{pub} = M\bar{G}T^{-1}$ is of systematic form. Then we publish (G_{pub}, t) as the public key where $t = \lfloor \frac{n-k}{2\lambda} \rfloor$, and keep $(\bar{H}, A, \mathscr{D}_{\bar{\mathcal{G}}})$ as the secret key.

- Encryption
  For a plaintext $\boldsymbol{x} \in \mathbb{F}_q^K$, randomly choose a matrix $E \in \mathcal{M}_{u_c,m\lambda}(\mathbb{F}_q)$ of the form

$$E = \begin{pmatrix} \boldsymbol{e}_1 & \cdots & \cdots & \boldsymbol{e}_{\lambda-1} & \boldsymbol{e}_\lambda \\ \boldsymbol{e}_{1+\lambda} & \cdots & \cdots & \boldsymbol{e}_{2\lambda-1} & \boldsymbol{e}_{2\lambda} \\ \vdots & & & \vdots & \vdots \\ \boldsymbol{e}_{1+(u_c-1)\lambda} & \cdots & \boldsymbol{e}_n & \cdots & \mathbf{0} \end{pmatrix} \tag{4}$$

  with $\mathrm{Rank}(E) = t$, where $\boldsymbol{e}_i \in \mathbb{F}_q^m \, (1 \leqslant i \leqslant n)$. Let $\boldsymbol{e} = (\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n) \in \mathbb{F}_q^N$, then the ciphertext corresponding to $\boldsymbol{x}$ is computed as $\boldsymbol{y} = \boldsymbol{x}G_{pub} + \boldsymbol{e}$.

- Decryption
  For a ciphertext $\boldsymbol{y} \in \mathbb{F}_q^N$, compute $\boldsymbol{s} = \boldsymbol{y}T\bar{H}^T = \boldsymbol{e}T\bar{H}^T$. Applying the syndrome decoding procedure $\mathscr{D}_{\bar{\mathcal{G}}}$ of $\bar{\mathcal{G}}$ to $\boldsymbol{s}$ will lead to $\boldsymbol{e}' = \boldsymbol{e}T$, then we can recover $\boldsymbol{e}$ by computing $\boldsymbol{e}'T^{-1}$. The restriction of $\boldsymbol{y} - \boldsymbol{e}$ to the first K coordinates will be the plaintext.

Correctness of Decryption. Before proving the correctness, we first introduce the following proposition.

Proposition 1. *Given λ matrices $M_1, M_2, \cdots, M_\lambda \in \mathcal{M}_{u,v}(\mathbb{F}_q)$, let*

$$M = [M_1, M_2, \cdots, M_\lambda] \text{ and } M' = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_\lambda \end{pmatrix}.$$

Suppose $\mathrm{Rank}(M) = t$, then there must be $\mathrm{Rank}(M') \leqslant \lambda t$.

Proof. Since $\mathrm{Rank}(M) = t$, there must be $\mathrm{Rank}(M_i) \leqslant t$ for $1 \leqslant i \leqslant \lambda$. Hence we have $\mathrm{Rank}(M') \leqslant \sum_{i=1}^{\lambda} \mathrm{Rank}(M_i) \leqslant \lambda t$. □

Now we return to the proof. From the decrypting process of Proposal II, we just need to prove that $\boldsymbol{e}'$ satisfy the decodable condition given in Section 3.2. Let $\boldsymbol{e}' = (\boldsymbol{e}'_1, \boldsymbol{e}'_2, \cdots, \boldsymbol{e}'_n)$ where $\boldsymbol{e}'_i \in \mathbb{F}_q^m \, (1 \leqslant i \leqslant n)$, then there exist $\boldsymbol{e}'_{n+1}, \cdots, \boldsymbol{e}'_{u_c\lambda} \in \mathbb{F}_q^m$ such that

$$E' = \begin{pmatrix} \boldsymbol{e}'_1 & \cdots & \cdots & \boldsymbol{e}'_{\lambda-1} & \boldsymbol{e}'_\lambda \\ \boldsymbol{e}'_{1+\lambda} & \cdots & \cdots & \boldsymbol{e}'_{2\lambda-1} & \boldsymbol{e}'_{2\lambda} \\ \vdots & & & \vdots & \vdots \\ \boldsymbol{e}'_{1+(u_c-1)\lambda} & \cdots & \boldsymbol{e}'_n & \cdots & \boldsymbol{e}'_{u_c\lambda} \end{pmatrix} = EA = [E'_1 \; E'_2 \; \cdots \; E'_\lambda],$$

where $E'_i \in \mathcal{M}_{u_c,m}(\mathbb{F}_q)$ $(1 \leqslant i \leqslant \lambda)$. Clearly we have $\text{Rank}(E') = \text{Rank}(E) = t$. Let

$$F = \begin{pmatrix} \boldsymbol{e}'_1 \\ \boldsymbol{e}'_2 \\ \vdots \\ \boldsymbol{e}'_n \end{pmatrix} \text{ and } F' = \begin{pmatrix} E'_1 \\ E'_2 \\ \vdots \\ E'_\lambda \end{pmatrix},$$

then $\text{Rank}(F) \leqslant \text{Rank}(F') \leqslant \lambda t \leqslant \lfloor \frac{n-k}{2} \rfloor$ because of Proposition 1.

Remark 3. The cryptosystem presented above aims at the general situation where λ does not divide n, or equivalently $u_f \neq u_c$. As for the case of $u_f = u_c$, just a few changes are needed in the key generation procedure. To generate the column scrambling matrix T^{-1}, any non-singular matrix $A \in GL_{m\lambda}(\mathbb{F}_q)$ is feasible for computing $T = I_{u_f} \otimes A$.

5 Security analysis

5.1 The distinguisher for Gabidulin codes

Before giving the analysis, we introduce the so-called Frobenius transformation and some algebraic properties of Gabidulin codes under this transformation that will be useful to explain why our proposals can prevent the related structural attacks.

For a non-negative integer i, denote by $[i]$ the i-th Frobenius power q^i, namely $[i] = q^i$. Under this notation, the quantity α^{q^i} can be simply written as $\alpha^{[i]}$ for any $\alpha \in \mathbb{F}_{q^m}$. Generalizing this transformation to a vector $\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathbb{F}_{q^m}^n$, there will be $\boldsymbol{v}^{[i]} = (v_1^{[i]}, \cdots, v_n^{[i]})$. As for a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, the i-th Frobenius power of $\mathcal{C}$ is defined as $\mathcal{C}^{[i]} = \{\boldsymbol{c}^{[i]} : \boldsymbol{c} \in \mathcal{C}\}$.

Now we introduce the following propositions without proving. These propositions provide us with a method of distinguishing Gabidulin codes from general ones.

Proposition 2. *Let $\mathcal{G} \subseteq \mathbb{F}_{q^m}^n$ 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 3. *Let $\mathcal{G} \subseteq \mathbb{F}_{q^m}^n$ 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 4. *[31] Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $[n,k]$ random linear code. For any positive integer i, the following equality holds with high probability*

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

5.2 Structural attacks

Existing attacks. Most cryptosystems based on Gabidulin codes have been proved to be insecure due to their vulnerability against structural attacks, such as Overbeck's attack [27], Coggia-Couvreu attack [33] and the attack proposed in [31]. Although these attacks were designed to cryptanalyze different variants, most of them rely on the fact that one can distinguish Gabidulin codes from general ones by observing how their dimensions behave under the Frobenius mapping according to Propositions 2, 3 and 4. However, this observation is no longer valid when considering our proposals. Since our proposals are built over the base field $\mathbb{F}_q$, apparently we have $\bar{\mathcal{G}}^{[i]} = \bar{\mathcal{G}}$ for any positive integer i. In this situation, Gabidulin codes will behave the same as general linear codes in terms of dimensions. Hence it is reasonable to conclude that all these attacks do not work on our proposals.

Potential attack. Let $\mathcal{B} = \{\alpha_1, \cdots, \alpha_m\} \subset \mathbb{F}_{q^m}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Denote by $\phi_{\mathcal{B}}$ the $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$ with respect to $\mathcal{B}$. For an $[n, k]$ Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^m}$, denote by $\bar{\mathcal{G}}$ the expanded code of $\mathcal{G}$ induced by $\phi_{\mathcal{B}}$.

Let $\mathcal{B}^* = \{\alpha_1^*, \cdots, \alpha_m^*\} \subset \mathbb{F}_{q^m}$ be another basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Define $\hat{\phi}_{\mathcal{B}^*}$ to be an $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_q^m$ to $\mathbb{F}_{q^m}$ such that for $\boldsymbol{a} = (a_1, \cdots, a_m) \in \mathbb{F}_q^m$,

$$\hat{\phi}_{\mathcal{B}^*}(\boldsymbol{a}) = \sum_{i=1}^{m} a_i \alpha_i^*.$$

For a vector $\boldsymbol{v} = (\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n) \in \mathbb{F}_q^{mn}$ where $\boldsymbol{a}_i \in \mathbb{F}_q^m$ $(1 \leqslant i \leqslant n)$, define $\hat{\phi}_{\mathcal{B}^*}(\boldsymbol{v}) = (\hat{\phi}_{\mathcal{B}^*}(\boldsymbol{a}_1), \cdots, \hat{\phi}_{\mathcal{B}^*}(\boldsymbol{a}_n))$. For the expanded Gabidulin code $\bar{\mathcal{G}}$, we define

$$\hat{\phi}_{\mathcal{B}^*}(\bar{\mathcal{G}}) = \{\hat{\phi}_{\mathcal{B}^*}(\boldsymbol{c}) : \boldsymbol{c} \in \bar{\mathcal{G}}\}.$$

It is easy to verify that $\hat{\phi}_{\mathcal{B}^*}(\bar{\mathcal{G}}) \subseteq \mathbb{F}_{q^m}^n$ forms an $\mathbb{F}_q$-linear space of dimension mk.

A potential adversary may randomly choose such a basis $\mathcal{B}^*$ and generate an $\mathbb{F}_q$-linear code by computing $\hat{\phi}_{\mathcal{B}^*}(\bar{\mathcal{G}})$. Theoretically $\hat{\phi}_{\mathcal{B}^*}(\bar{\mathcal{G}})$ could be the parent Gabidulin code of $\bar{\mathcal{G}}$ or some of its equivalent codes. If such an extreme case happens, then the encryption system will be completely broken. According to our analysis, however, this is merely a small probability event.

Let $\Phi = \hat{\phi}_{\mathcal{B}^*} \circ \phi_{\mathcal{B}}$ be a composite mapping. It is easy to verify that Φ forms an $\mathbb{F}_q$-linear automorphism over $\mathbb{F}_{q^m}$. If Φ is a stretching transformation, namely there exists $\gamma \in \mathbb{F}_{q^m}^*$ such that $\Phi(\alpha) = \gamma\alpha$ for any $\alpha \in \mathbb{F}_{q^m}$, then there must be $\Phi(\mathcal{G}) = \mathcal{G}$. For any $\gamma \in \mathbb{F}_{q^m}^*$, there exists a stretching transformation Φ induced by γ. Therefore, there are at least $q^m - 1$ $\mathbb{F}_q$-linear automorphisms Φ such that $\Phi(\mathcal{G})$ is also a Gabidulin code. In general case, however, $\Phi(\mathcal{G})$ is no longer a Gabidulin code, not even an $\mathbb{F}_{q^m}$-linear code. We will illustrate this point by Example 1.

On the other hand, the total number of $\mathbb{F}_q$-linear automorphisms over $\mathbb{F}_{q^m}$ can computed as $\prod_{i=0}^{m-1}(q^m - q^i)$. Among all these automorphisms, transformations that behave like a stretching transformation take a small proportion according to our experiments on Magma. For instance, we construct a $[15, 7]$ Gabidulin code over $\mathbb{F}_{3^{30}}$ and then perform one million random $\mathbb{F}_3$-linear automorphisms to this code, but none of these converted codes are $\mathbb{F}_{3^{30}}$-linear.

According to the analysis above, we believe that this potential attack against expanded Gabidulin codes is infeasible. Similar to the masking techniques exploited in [17], in Proposal I we first divide the underlying expanded Gabidulin code into n blocks, and then perform a mixcolumn transformation to each of these blocks by multiplying the punctured generator matrix with an invertible block

diagonal matrix. In Proposal II, we disguise the underlying code by mixing λ adjacent blocks instead of mixing columns inside each block. We believe that all these techniques further strengthen our two proposals against structural attacks.

Example 1. Let $f(x) = x^3+x+1$ be an irreducible polynomial over $\mathbb{F}_2$. Denote by $\mathbb{F}_8$ the extension field of $\mathbb{F}_2$ derived from $f(x)$. Let $\alpha \in \mathbb{F}_8^*$ such that $f(\alpha) = 0$, then $1, \alpha, \alpha^2$ form a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$. We define an $\mathbb{F}_2$-linear automorphism Φ over $\mathbb{F}_8$ as follows

$$\Phi(1) = \alpha^4, \Phi(\alpha) = \alpha^2, \Phi(\alpha^2) = \alpha^3.$$

Let $\boldsymbol{g} = (\alpha, \alpha^2, \alpha^3) \in \mathbb{F}_8^3$ and define a $[3, 2]$ Gabidulin code $\mathcal{G} \subseteq \mathbb{F}_8^3$ generated by $\boldsymbol{g}$. It is easy to verify that $\mathcal{G}$ has a generator matrix of the form

$$G = \begin{pmatrix} 1 & 0 & \alpha^3 \\ 0 & 1 & \alpha^4 \end{pmatrix}.$$

If there exists a word of $\langle \Phi(\boldsymbol{g}), \Phi(\boldsymbol{g}^2) \rangle_{\mathbb{F}_8}$ that is not contained in $\Phi(\mathcal{G})$, we conclude that $\Phi(\mathcal{G})$ is not $\mathbb{F}_8$-linear. Let $\boldsymbol{a} = \alpha\Phi(\boldsymbol{g})$, then $\boldsymbol{a} \notin \Phi(\mathcal{G})$ holds if and only if $\Phi^{-1}(\boldsymbol{a}) \notin \mathcal{G}$. Since $\Phi^{-1}(\boldsymbol{a}) = (\alpha^2, 1, \alpha)$, apparently we have $\Phi^{-1}(\boldsymbol{a}) \notin \mathcal{G}$. Hence the previous claim is true.

5.3 Generic attacks

Note that in Hamming metric code-based cryptography, the best known generic attack is the information set decoding (ISD) attack [38]. Since expanded Gabidulin codes are far from optimal according to Theorem 12, the Hamming weight of the intended error vector in the encryption procedure is much greater than the error-correcting capability of the public code with high probability. Hence the ISD attack is not applicable for our cases.

In what follows, we introduce two hard problems closely related to the security of our proposals, namely the rank syndrome decoding (RSD) problem and MinRank problem. Generally speaking, approaches to solve these two problems are mainly divided into two categories, namely the combinatorial approach and algebraic approach. In this paper, we consider the combinatorial attack on the RSD problem and the algebraic attack on the MinRank problem to evaluate the security level of our proposals.

5.3.1 Combinatorial attacks

Definition 13 (RSD problem). Let H be an $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ of full rank, $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and t be a positive integer. An RSD instance $\mathcal{R}(q, m, n, k, t)$ is to solve $\boldsymbol{s} = \boldsymbol{e}H^T$ for $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $w_R(\boldsymbol{e}) \leqslant t$.

The RSD problem plays a crucial role in rank-based cryptography. Although this problem is not known to be NP-complete, it is believed to be hard by the community. In the paper [39], the authors proved that if there were a probabilistic polynomial-time algorithm for solving the RSD problem, then a probabilistic polynomial-time algorithm can be obtained to solve the syndrome decoding problem in the Hamming metric, which has been proved to be NP-complete in [40]. Generally speaking, attacks on the RSD problem can be divided into two categories, namely the combinatorial attack and algebraic attack. Up to now, the best known combinatorial attacks can be found in [19, 41–43].

Now we recall the principle of the combinatorial attack proposed in [42]. Although there are some improvements [43] for this attack, they are not applicable for our cases. For an RSD instance $\mathcal{R}(q,m,n,k,t)$, we consider the following two cases to solve the problem.

Case 1: $n \geqslant m$. Let $\mathcal{V}$ be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension $t' \geqslant t$. If $\mathrm{Supp}_R(\boldsymbol{e}) \subseteq \mathcal{V}$, then each coordinate of $\boldsymbol{e}$ can be expressed as an $\mathbb{F}_q$-linear combination of a basis of $\mathcal{V}$. Computing $\boldsymbol{s} = \boldsymbol{e}H^T$ will result in a linear system of $n-k$ equations with nt' variables in $\mathbb{F}_q$. By expressing each monomial of these parity-check equations as a vector in $\mathbb{F}_q^m$ under a given basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we eventually obtain a system of $m(n-k)$ equations over $\mathbb{F}_q$ with nt' variables. Apparently this system has at least one solution when the condition $\mathrm{Supp}_R(\boldsymbol{e}) \subseteq \mathcal{V}$ is satisfied. To have only one solution with overwhelming probability, we should make sure that $m(n-k) \geqslant nt'$ and then $t' \leqslant m - \left\lceil \frac{km}{n} \right\rceil$. By solving this system, we can finally recover the error vector $\boldsymbol{e}$. The total complexity of this algorithm is $\mathcal{O}\left(m^3(n-k)^3/p\right)$, where $m^3(n-k)^3$ represents the average operations required for solving the linear system and p is the probability that a random $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension t' happens to contain $\mathrm{Supp}_R(\boldsymbol{e})$. By the Gaussian binomial coefficient, we have

$$p = \begin{bmatrix} m-t \\ t'-t \end{bmatrix}_q \Bigg/ \begin{bmatrix} m \\ t' \end{bmatrix}_q = \prod_{i=0}^{t'-t-1} \frac{q^{m-t}-q^i}{q^{t'-t}-q^i} \Bigg/ \prod_{i=0}^{t'-1} \frac{q^m-q^i}{q^{t'}-q^i} \approx \frac{1}{q^{t(m-t')}}.$$

By taking $t' = m - \left\lceil \frac{km}{n} \right\rceil$, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{t\left\lceil \frac{km}{n} \right\rceil}\right)$.

Case 2: $n < m$. For a given basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, elements of $\mathbb{F}_{q^m}$ are in a one-to-one correspondence to $\mathbb{F}_q^m$ under this basis. By replacing each coordinate of $\boldsymbol{e}$ with the corresponding column vector, we obtain an $m \times n$ matrix E over $\mathbb{F}_q$. Let $\mathcal{E}$ be the linear space spanned by rows of E over $\mathbb{F}_q$. If we can find a linear space $\mathcal{V} \subseteq \mathbb{F}_q^n$ of dimension t' such that $\mathcal{E} \subseteq \mathcal{V}$, then each row of E can be expressed as an $\mathbb{F}_q$-linear combination of a basis of $\mathcal{V}$. With a same analysis as Case 1, we eventually get a linear system of $m(n-k)$ equations over $\mathbb{F}_q$ with mt' variables. Let $mt' \leqslant m(n-k)$, then $t' \leqslant n-k$. On the other hand, the probability that a random subspace of $\mathbb{F}_q^n$ of dimension t' happens to contain $\mathcal{E}$ can be evaluated as

$$p = \begin{bmatrix} n-t \\ t'-t \end{bmatrix}_q \Bigg/ \begin{bmatrix} n \\ t' \end{bmatrix}_q = \prod_{i=0}^{t'-t-1} \frac{q^{n-t}-q^i}{q^{t'-t}-q^i} \Bigg/ \prod_{i=0}^{t'-1} \frac{q^n-q^i}{q^{t'}-q^i} \approx \frac{1}{q^{t(n-t')}}.$$

By taking $t' = n-k$, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{tk}\right)$.

Having introduced the general idea of the combinatorial attack on the RSD problem, we now apply it to the case of our two proposals.

Proposal I. In the case of $\lambda \geqslant n$, let $\mathcal{E}$ be the linear space spanned by columns of E of dimension t. Let $\mathcal{V}$ be a random subspace of $\mathbb{F}_q^n$ of dimension $t' \geqslant t$. If $\mathcal{E} \subseteq \mathcal{V}$, then each column of E can be expressed as a linear combination of a basis of $\mathcal{V}$ with t' undetermined coefficients in $\mathbb{F}_q$. With such a matrix E of this form, we can construct the error vector $\boldsymbol{e}$. Let H_{pub} be a parity-check matrix of the public code, and $\boldsymbol{y} = \boldsymbol{x}G_{pub} + \boldsymbol{e}$ be the received ciphertext. Then computing $\boldsymbol{y}H_{pub}^T = \boldsymbol{e}H_{pub}^T$ will result in a linear system of $m(n-k)$ equations with $\lambda t'$ variables in $\mathbb{F}_q$. To have only one solution, there should be $m(n-k) \geqslant \lambda t'$ and hence we have $t' \leqslant \left\lfloor \frac{m(n-k)}{\lambda} \right\rfloor$. With a same analysis as Case 2, the probability that a randomly chosen $\mathcal{V}$ happens to contain $\mathcal{E}$ can be evaluated as $p \approx q^{-t(n-t')}$. By taking $t' = \left\lfloor \frac{m(n-k)}{\lambda} \right\rfloor$, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{t\left(n-\left\lfloor \frac{m(n-k)}{\lambda} \right\rfloor\right)}\right)$.

In the case of $n > \lambda$, let $\mathcal{E}$ be the linear space spanned by rows of E of dimension t. Let $\mathcal{V}$ be a random subspace of $\mathbb{F}_q^\lambda$ of dimension $t' \geqslant t$ such that $\mathcal{E} \subseteq \mathcal{V}$. With a similar analysis as above, we can obtain a linear system of $m(n-k)$ equations with nt' variables in $\mathbb{F}_q$. Let $m(n-k) \geqslant nt'$, then $t' \leqslant m - \lceil \frac{km}{n} \rceil$. The probability that a randomly chosen $\mathcal{V}$ happens to contain $\mathcal{E}$ can be evaluated as $p \approx q^{-t(\lambda - t')}$. By taking $t' = m - \lceil \frac{km}{n} \rceil$, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{t\left(\lambda - m + \lceil \frac{km}{n} \rceil\right)}\right)$.

Proposal II. On the one hand. According to the description of Proposal II, the linear space $\mathcal{E} = \langle \boldsymbol{e}_1, \cdots, \boldsymbol{e}_n \rangle_{\mathbb{F}_q}$ has dimension at most λt. With a same analysis as Case 1, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{\lambda t \lceil \frac{km}{n} \rceil}\right)$ for $n \geqslant m$. With a same analysis as Case 2, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{\lambda t k}\right)$ for $n < m$.

On the other hand. These blocks $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ of $\boldsymbol{e}$ are obtained from a matrix $E \in \mathcal{M}_{u_c, m\lambda}(\mathbb{F}_q)$ with $\mathrm{Rank}(E) = t$. With a nontrivial $\lambda \geqslant 2$, apparently we have $u_c = \lceil \frac{n}{\lambda} \rceil < n < m\lambda$. Denote by $\mathcal{E}$ the linear space spanned by columns of E over $\mathbb{F}_q$. Let $\mathcal{V}$ be a random subspace of $\mathbb{F}_q^{u_c}$ of dimension $t' \geqslant t$. If $\mathcal{E} \subseteq \mathcal{V}$, then each column of E can be expressed as a linear combination of a basis of $\mathcal{V}$. With such a matrix E of this form, we can represent the error vector $\boldsymbol{e}$ with $m\lambda t'$ variables in $\mathbb{F}_q$. Let $m(n-k) \geqslant m\lambda t'$, then $t' \leqslant \lfloor \frac{n-k}{\lambda} \rfloor$. The probability that a random t'-dimensional subspace of $\mathbb{F}_q^{u_c}$ happens to contain $\mathcal{E}$ can be evaluated as

$$p = \begin{bmatrix} u_c - t \\ t' - t \end{bmatrix} \Big/ \begin{bmatrix} u_c \\ t' \end{bmatrix} \approx \frac{1}{q^{t(u_c - t')}}.$$

By taking $t' = \lfloor \frac{n-k}{\lambda} \rfloor$, we get a complexity of $\mathcal{O}\left(m^3(n-k)^3 q^{t(u_c - \lfloor \frac{n-k}{\lambda} \rfloor)}\right)$.

5.3.2 Algebraic attacks

Definition 14 (MinRank problem). For given positive integers n_1, n_2, m and t, let $M_1, M_2, \cdots, M_m \in \mathcal{M}_{n_1, n_2}(\mathbb{F}_q)$. A MinRank instance of parameter (q, n_1, n_2, m, t) is to search for m coefficients $x_1, x_2, \cdots, x_m \in \mathbb{F}_q$ such that $\mathrm{Rank}(\sum_{i=1}^m x_i M_i) \leqslant t$.

The MinRank problem was originally proposed by Buss et al. [44] as a natural question in linear algebra and proved to be NP-complete. This problem plays a central role in both multivariate cryptography [46] and rank-based cryptography [42]. The rank decoding (RD) problem, the dual of an RSD problem $\mathcal{R}(q, m, n, k, t)$, can be reduced to a structured MinRank instance of parameter $(q, m, n, mk+1, t)$ [47]. There are mainly three approaches to solve the MinRank problem, namely the Kipnis-Shamir (KS) modeling [48], minors modeling [49] and linear algebra search [50].

The authors in [49,51] investigated the "square" case of $n_1 = n_2 = n$, and gave an upper bound for the complexity of solving the MinRank problem in this situation. For a MinRank instance of parameter (q, n, n, m, t), the complexity is

$$\mathcal{O}\left(\binom{m + t(n-t) + \min\{m, t(n-t)\} + 1}{\min\{m, t(n-t)\} + 1}^\omega\right),$$

where $\omega = 2.8$ represents the linear algebra constant. In the paper [47], Faugère et al. managed to solve the MinRank instance of parameter (q, n, n, m, t) with a complexity of $\mathcal{O}\left(\log(q) n^{3(n-t)^2}\right)$ when the condition $m = (n-t)^2 + 1$ is satisfied.

For the "nonsquare" case, Bardet et al. [45] proposed to solve the MinRank instance of parameter (q, n_1, n_2, m, t) with a complexity of

$$\mathcal{O}\left(m(t+1)\binom{n_2}{t}^2\binom{m+b-1}{b}^2\right),$$

where b is the smallest positive integer such that $b < \min\{q, t+2\}$ satisfying the following condition

$$\binom{n_2}{t}\binom{m+b-1}{b} - 1 \leqslant \sum_{i=1}^{b}(-1)^{i+1}\binom{n_2}{t+i}\binom{n_1+i-1}{i}\binom{m+b-i-1}{b-i}.$$

In what follows, our analysis shows that decrypting any valid ciphertext in our proposals can be reduced to solving a MinRank instance. For the convenience of our statement, we first define an $\mathbb{F}_q$-linear isomorphism σ from $\mathbb{F}_q^{ns}$ to $\mathcal{M}_{n,s}(\mathbb{F}_q)$ for some positive integer s. For a vector $\boldsymbol{x} = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n) \in \mathbb{F}_q^{ns}$ with $\boldsymbol{x}_i \in \mathbb{F}_q^s\,(1 \leqslant i \leqslant n)$, we define $\sigma(\boldsymbol{x})$ as follows

$$\sigma(\boldsymbol{x}) = \left[\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\right]^T \in \mathcal{M}_{n,s}(\mathbb{F}_q).$$

Generalizing this definition to a set $\mathcal{X} \subseteq \mathbb{F}_q^{ns}$, we have $\sigma(\mathcal{X}) = \{\sigma(\boldsymbol{x}) : \boldsymbol{x} \in \mathcal{X}\}$. For any $\boldsymbol{x} \in \mathbb{F}_q^{ns}$, by $w_R(\boldsymbol{x})$ we mean the rank of $\sigma(\boldsymbol{x})$ hereafter when no ambiguity arises.

Proposal I. With the concept above, we now introduce the following proposition with respect to our first proposal.

Proposition 5. *Denote by $\boldsymbol{m}_i$ the i-th row vector of the public matrix $G_{pub}\,(1 \leqslant i \leqslant K)$, and $\mathcal{G}_{pub}$ the public code generated by G_{pub}. Let $\boldsymbol{y} = \boldsymbol{c}+\boldsymbol{e}$ be the received word, where $\boldsymbol{c} \in \mathcal{G}_{pub}$ and $\boldsymbol{e} \in \mathbb{F}_q^N$ with $w_R(\boldsymbol{e}) = t$. If there exist $a_0, a_1, \cdots, a_K \in \mathbb{F}_q$ such that $0 < w_R(a_0\boldsymbol{y} + \sum_{i=1}^K a_i\boldsymbol{m}_i) \leqslant t$, then there must be $a_0\boldsymbol{y} + \sum_{i=1}^K a_i\boldsymbol{m}_i = a_0\boldsymbol{e}$ and hence $\boldsymbol{e} = \frac{1}{a_0}(a_0\boldsymbol{y} + \sum_{i=1}^K a_i\boldsymbol{m}_i)$.*

Proof. It is easy to see that $\bar{\mathcal{G}}_S$ is obtained by shortening $\bar{\mathcal{G}}$ at S, then there must be

$$d(\bar{\mathcal{G}}_S) \geqslant d(\bar{\mathcal{G}}) \geqslant n - k + 1 \geqslant 2t + 1.$$

On the other hand, apparently we have $\mathcal{G}_{pub} = \langle \bar{G}_S T^{-1}\rangle_{\mathbb{F}_q} = \bar{\mathcal{G}}_S T^{-1}$. For any $\boldsymbol{u} \in \mathcal{G}_{pub}$, there exists $\boldsymbol{v} \in \bar{\mathcal{G}}_S$ such that $\boldsymbol{u} = \boldsymbol{v}T^{-1}$. Following this we have $\sigma(\boldsymbol{u}) = \sigma(\boldsymbol{v})A^{-1}$ and then

$$w_R(\boldsymbol{u}) = \text{Rank}(\sigma(\boldsymbol{u})) = \text{Rank}(\sigma(\boldsymbol{v})) = w_R(\boldsymbol{v}) \geqslant 2t + 1,$$

which implies that $d(\mathcal{G}_{pub}) \geqslant 2t + 1$. Hence if $a_0\boldsymbol{y} + \sum_{i=1}^K a_i\boldsymbol{m}_i = (a_0\boldsymbol{c} + \sum_{i=1}^K a_i\boldsymbol{m}_i) + a_0\boldsymbol{e}$ has rank weight of at most t, then there must be $a_0\boldsymbol{c} + \sum_{i=1}^K a_i\boldsymbol{m}_i = \boldsymbol{0}$ and $a_0 \neq 0$. Otherwise, there will be $w_R(a_0\boldsymbol{y} + \sum_{i=1}^K a_i\boldsymbol{m}_i) \geqslant t + 1$. This completes the proof. □

Based on the analysis above, decrypting a valid ciphertext in Proposal I can be reduced to solving a MinRank instance of parameter $(q, n, \lambda, K + 1, t)$. Formally, we introduce the following proposition without proving.

Proposition 6. *Suppose $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ is a valid ciphertext in Proposal I, where $\boldsymbol{c} \in \mathcal{G}_{pub}$ and $\boldsymbol{e} \in \mathbb{F}_q^N$ with $w_R(\boldsymbol{e}) = t$. Let $M_0 = \sigma(\boldsymbol{y})$ and $M_i = \sigma(\boldsymbol{m}_i)$ for $1 \leqslant i \leqslant K$. Then recovering $\boldsymbol{e}$ can be reduced to a MinRank instance of searching for $a_0, a_1, \cdots, a_K \in \mathbb{F}_q$ such that Rank$(\sum_{i=0}^K a_i M_i) \leqslant t$.*

Proposal II. Similar to Proposition 6, Proposal II can be reduced to a MinRank instance of parameter $(q, n, m, K+1, \lambda t)$. Formally, we introduce the following proposition without proving.

Proposition 7. *Suppose $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ is a valid ciphertext in Proposal II, where $\boldsymbol{c} \in \mathcal{G}_{pub}$ and $\boldsymbol{e} \in \mathbb{F}_q^N$ is the intended error vector. Let $M_0 = \sigma(\boldsymbol{y})$ and $M_i = \sigma(\boldsymbol{m}_i)$ for $1 \leqslant i \leqslant K$. Then recovering $\boldsymbol{e}$ can be reduced to a MinRank instance of searching for $a_0, a_1, \cdots, a_K \in \mathbb{F}_q$ such that Rank$(\sum_{i=0}^{K} a_i M_i) \leqslant \lambda t$.*

Apparently there exists at least one solution for this reduced MinRank instance. For a nontrivial $\lambda \geqslant 2$, the right column scrambler T^{-1} does not preserve the rank metric in general, thus we cannot decide as in Proposition 5 whether or not a solution reveals the intended error vector $\boldsymbol{e}$ or some of its multiples. But we can still give an answer to this question according to the following proposition.

Proposition 8. *Suppose $a_0, a_1, \cdots, a_K \in \mathbb{F}_q$ form a solution of the MinRank instance described in Proposition 7, then let $\boldsymbol{e}' = \sigma^{-1}(\sum_{i=0}^{K} a_i M_i) = (\boldsymbol{e}'_1, \cdots, \boldsymbol{e}'_n)$ with $\boldsymbol{e}'_i \in \mathbb{F}_q^m$ for $1 \leqslant i \leqslant n$. Define $E' \in \mathcal{M}_{u_c, m\lambda}(\mathbb{F}_q)$ to be the associated matrix of $\boldsymbol{e}'$ of the form (4). If Rank$(E') \leqslant t$, then there must be $\boldsymbol{e}' = a_0 \boldsymbol{e}$.*

Proof. Apparently $\boldsymbol{e}' = \sigma^{-1}(\sum_{i=0}^{K} a_i M_i) = a_0 \boldsymbol{y} + \sum_{i=1}^{K} a_i \boldsymbol{m}_i = a_0 \boldsymbol{e} + (a_0 \boldsymbol{c} + \sum_{i=1}^{K} a_i \boldsymbol{m}_i)$. On the one hand, $\boldsymbol{e}'$ can be viewed as a valid ciphertext obtained by encrypting $\boldsymbol{0} \in \mathbb{F}_q^K$ because of Rank$(E') \leqslant t$. Hence decrypting $\boldsymbol{e}'$ will lead to $\boldsymbol{e}'$ itself. On the other hand, $\boldsymbol{e}'$ can also be viewed as a valid ciphertext that has $a_0 \boldsymbol{e}$ as the intended error vector because of $a_0 \boldsymbol{c} + \sum_{i=1}^{K} a_i \boldsymbol{m}_i \in \mathcal{G}_{pub}$. Then decrypting $\boldsymbol{e}'$ will lead to $a_0 \boldsymbol{e}$. By the uniqueness of decryption, there must be $\boldsymbol{e}' = a_0 \boldsymbol{e}$. This completes the proof. □

6 Parameter choice and public-key size

In this section, we compute the public-key sizes and information rates of the proposed cryptosystems for security of 128 bits, 192 bits and 256 bits against the generic attacks described in Section 5.3. After that we will make a comparison with some other code-based cryptosystems on public-key sizes for different security levels.

In Proposal I, the public key is a systematic generator matrix of the public code with length $n\lambda$ and dimension $n\lambda - mr$ where $r = n - k$, resulting in a public-key size of $mr(n\lambda - mr) \cdot log_2(q)$ bits. In Proposal II, the public key is a systematic generator matrix of the public code with length mn and dimension mk, resulting in a public-key size of $rkm^2 \cdot log_2(q)$ bits. As for the information rates, this value is evaluated as $(n\lambda - mr)/n\lambda$ for Proposal I, and k/n for Proposal II respectively.

In Table 1 we consider the case of $q = 3$, in Table 2 we consider the case of $q = 7$, and in Table 3 we consider $q = 13$. By comparison of the calculation results in these three cases, it is easy to see that the greater the base field is, the smaller public-key sizes our two proposals will have.

For Proposal I, we suggest the parameter set $(q = 13, m = 17, n = 17, k = 11, \lambda = 16)$ for security of 128 bits, the parameter set $(q = 13, m = 22, n = 22, k = 16, \lambda = 21)$ for security of 192 bits, and the parameter set $(q = 13, m = 25, n = 25, k = 17, \lambda = 24)$ for security of 256 bits.

For Proposal II, we suggest the parameter set $(q = 13, m = 29, n = 29, k = 17, \lambda = 2)$ for security of 128 bits, the parameter set $(q = 13, m = 37, n = 37, k = 21, \lambda = 2)$ for security of 192 bits, and the parameter set $(q = 13, m = 43, n = 43, k = 23, \lambda = 2)$ for security of 256 bits.

Instance	Parameters	Key Size	Rate	Security
Proposal I	m=25, n=25, k=17, λ=24	15,850	0.67	128
	m=32, n=32, k=22, λ=31	42,604	0.68	192
	m=37, n=37, k=25, λ=36	78,114	0.67	256
Proposal II	m=43, n=43, k=19, λ=2	167,044	0.44	128
	m=57, n=57, k=33, λ=2	509,805	0.58	192
	m=67, n=67, k=39, λ=2	971,184	0.58	256

Table 1: Public-key sizes and information rates of the proposed cryptosystems in the case of $q = 3$ (in bytes).

Instance	Parameters	Key Size	Rate	Security
Proposal I	m=20, n=20, k=14, λ=19	10,949	0.68	128
	m=24, n=24, k=16, λ=23	24,256	0.65	192
	m=28, n=28, k=18, λ=27	46,771	0.63	256
Proposal II	m=35, n=35, k=23, λ=2	118,646	0.66	128
	m=45, n=45, k=29, λ=2	329,724	0.64	192
	m=51, n=51, k=31, λ=2	565,900	0.61	256

Table 2: Public-key sizes and information rates of the proposed cryptosystems in the case of $q = 7$ (in bytes).

Instance	Parameters	Key Size	Rate	Security
Proposal I	m=17, n=17, k=11, λ=16	8,021	0.63	128
	m=22, n=22, k=16, λ=21	20,149	0.71	192
	m=25, n=25, k=17, λ=24	37,005	0.67	256
Proposal II	m=29, n=29, k=17, λ=2	79,358	0.59	128
	m=37, n=37, k=21, λ=2	212,768	0.57	192
	m=43, n=43, k=23, λ=2	393,422	0.53	256

Table 3: Public-key sizes and information rates of the proposed cryptosystems in the case of $q = 13$ (in bytes).

Instance	128 bits	192 bits	256 bits
HQC	2,249	4,522	7,245
BIKE	1,540	3,082	5,121
Classic McEliece	261,120	524,160	1,044,992
NTS-KEM	319,488	929,760	1,419,704
KRW system			578,025
Proposal I	8,021	20,149	37,005
Proposal II	79,358	212,768	393,422

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

In Table 4, we make a comparison on public-key sizes with some other code-based cryptosystems. The first four instances, namely HQC [52], BIKE [53], NTS-KEM [54] and Classic McEliece [55], have been selected to move on to the third round of the NIST PQC Standardization Process. Note that the Classic McEliece published by the NIST PQC team is a merged version of NTS-KEM

and the original Classic McEliece for their specifications being very similar. The KRW system proposed in [17] is based on expanded GRS codes, which inspires us to exploit expanded Gabidulin codes in the design of encryption schemes. Compared to the KRW system, our proposals admit a more compact representation of public keys for the reason that the general decoding problem in the rank metric is much more difficult than that in the Hamming metric.

7 Conclusion

In this paper, we first introduce the concept of expanded Gabidulin codes and then build two cryptosystems by using these new codes in the McEliece setting. In our proposals the underlying code is divided into n blocks, with each block having size m. By the definition of expanded Gabidulin codes, each of these blocks corresponds to one coordinate of the parent Gabidulin code. To weaken this correspondence, in Proposal I we first shorten the expanded Gabidulin code and then perform a column-mixing transformation to each of these blocks. In Proposal II, we adopt a rather different column transformation to the expanded Gabidulin code by mixing λ neighbouring blocks. According to our analysis in Section 5.2, both of these two variants can resist the existing structural attacks. Compared to some other cryptosystems, our proposals have great advantage in public-key sizes without using the cyclic or quasi-cyclic structure. For instance, we have made a reduction in public-key sizes by 96% compared to Classic McEliece for the same security levels.

References

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

[2] Lee, P.J., Brickell, E.F.: An observation on the security of McEliece's public-key cryptosystem. In: Guenther, C.G. (Ed.): Proceedings of Advances in Cryptology-EUROCRYPT'88, LNCS, vol. 330, pp. 275–280. Springer (1988).

[3] Canteaut, A., Sendrier, N.: Cryptanalysis of the original McEliece cryptosystem. In: Ohta, K., Pei, D. (Eds.): Proceedings of ASIACRYPT'98, LNCS, vol. 1514, pp. 187–199. Springer (2000).

[4] Loidreau, P., Sendrier, N.: Weak keys in the McEliece public-key cryptosystem. IEEE Trans. Inf. Theory 47(3), 1207–1211 (2001).

[5] Faugère, J.-C., Gauthier-Umana, V., Otmani, A., Perret, L., Tillich, J.-P.: A distinguisher for high-rate McEliece cryptosystems. IEEE Trans. Inf. Theory 59(10), 6830–6844 (2013).

[6] Couvreur, A., Otmani, A., Tillich, J.-P.: Polynomial time attack on wild McEliece over quadratic extensions. IEEE Trans. Inf. Theory 63(1), 404–427 (2016).

[7] Loidreau, P.: Strengthening McEliece cryptosystem. In: Okamoto, T. (Ed.): Proceedings of ASIACRYPT 2000, LNCS, vol. 1976, pp. 585–598. Springer (2000).

[8] Kobara, K., Imai, H.: On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC. IEEE Trans. Inf. Theory 49(12), 3160–3168 (2003).

[9] Misoczki, R., Barreto, P.S.: Compact McEliece keys from Goppa codes. In: M.J. Jacobson Jr., Rijmen V., Safavi-Naini R. (Eds.): Proceedings of SAC 2009, LNCS, vol. 5867, pp. 376–392. Springer (2009).

[10] Faugère, J.-C., Otmani, A., Perret, L., Tillich J.-P.: Algebraic cryptanalysis of McEliece variants with compact keys. In: Gilbert, H. (Ed.): Proceedings of EUROCRYPT 2010, LNCS, vol. 6110, pp. 279–298. Springer (2010).

[11] Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Prob. Contr. Inform. Theory 15(2), 159–166 (1986).

[12] Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discret. Math. Appl. 2(4), 439–444 (1992).

[13] Li, Y.X., Deng, R.H., Wang, X.M.: On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Trans. Inf. Theory 40(1), 271–273 (1994).

[14] 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).

[15] Wieschebrink, C.: Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In: Sendrier, N. (Ed.): Proceedings of PQCrypto 2010, LNCS, vol. 6061, pp. 61–72. Springer (2010).

[16] Couvreur, A., Gaborit, P., Otmani, A., Tillich, J.-P.: Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Des. Codes Cryptogr. 73(2), 641–666 (2014).

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

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

[19] Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, pp. 368–381. Springer (1996).

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

[21] 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).

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

[23] Gabidulin, E.M., Rashwan, H., Honary, B.: On improving security of GPT cryptosystems. In: Proceedings of 2009 IEEE International Symposium on Information Theory, pp. 1110–1114. IEEE (2009).

[24] Loidreau, P.: Designing a rank metric based McEliece cryptosystem. In: Sendrier, N. (Ed.): Proceedings of PQCrypto 2010, LNCS, vol. 6061, pp. 142–152. Springer (2010).

[25] Rashwan, H., Gabidulin, E.M., Honary, B.: A smart approach for GPT cryptosystem based on rank codes. In: Proceedings of 2010 IEEE International Symposium on Information Theory, pp. 2463–2467. IEEE (2010).

[26] Gibson, K.: The security of the Gabidulin public key cryptosystem. In: Proceedings of Advances in Cryptology-EUROCRYPT'96, LNCS, vol. 1070, pp. 212–223. Springer (1996).

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

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

[29] 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).

[30] 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).

[31] 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).

[32] 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).

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

[34] Ghatak, A. Extending Coggia-Couvreur attack on Loidreau's rank-metric cryptosystem. arXiv:2007.07354 [cs.IT] (2020).

[35] 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).

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

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

[38] Peters, C.: Information-set decoding for linear codes over $\mathbb{F}_q$. In: Proceedings of PQCrypto 2010, LNCS, vol. 6061, pp. 81–94. Springer (2010).

[39] 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).

[40] 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).

[41] 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).

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

[43] 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).

[44] Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. J. Comput. Syst. Sci. 58(3), 572–596 (1999).

[45] 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. IACR (2020).

[46] Cabarcas, D., Smith-Tone, D., Verbel, J.A.: Key recovery attack for ZHFE. In: Proceedings of PQCrypto 2017, LNCS, vol. 10346, pp. 289–308. Springer (2017).

[47] Faugère, J.-C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Proceedings of Advances in Cryptology, LNCS, vol. 5157, pp. 280–296. Springer (2008).

[48] Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Proceedings of CRYPTO 1999, LNCS, vol. 1666, pp. 19–30. Springer (1999).

[49] Faugère, J.C., El Din, M.S., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptography. In: Proceedings of Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, pp. 257–264. ACM (2010).

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

[51] Faugère, J.-C., El Din, M.S., Spaenlehauer, P.-J.: Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree $(1, 1)$: algorithms and complexity. J. Symb. Comput. 46(4), 406–437 (2011).

[52] 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.

[53] 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.

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

[55] 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.