cryptography

MDPI

Article

A New Technique in Rank Metric Code-Based Encryption [†]

Terry Shue Chien Lau *,‡ and **Chik How Tan** ‡

Temasek Laboratories, National University of Singapore, T-Lab Building, 5A, Engineering Drive 1, #09-02, Singapore 117411, Singapore; tsltch@nus.edu.sg

* Correspondence: tsltlsc@nus.edu.sg; Tel.: +65-6516-1151

† This paper is an extended version of our paper published in 23rd Australasian Conference on Information Security and Privacy (ACISP 2018) .

‡ These authors contributed equally to this work.

Received: 29 August 2018; Accepted: 11 October 2018; Published: 15 October 2018

Abstract: We propose a rank metric codes based encryption based on the hard problem of rank syndrome decoding problem. We propose a new encryption with a public key matrix by considering the adding of a random distortion matrix over $\mathbb{F}_{q^m}$ of full column rank n. We show that `IND-CPA` security is achievable for our encryption under assumption of the Decisional Rank Syndrome Decoding problem. Furthermore, we also prove some bounds for the number of matrices of a fixed rank with entries over a finite field. Our proposal allows the choice of the error terms with rank up to $\frac{r}{2}$, where r is the error-correcting capability of a code. Our encryption based on Gabidulin codes has public key size of 13.68 KB, which is 82 times smaller than the public key size of McEliece Cryptosystem based on Goppa codes. For similar post-quantum security level of 2^{140} bits, our encryption scheme has a smaller public key size than the key size suggested by LOI17 Encryption.

Keywords: code-based cryptography; McEliece; public key encryption; provable security

1. Introduction

1.1. Background and Motivations

In 1978, McEliece [1] proposed a public-key cryptosystem based on Goppa codes in Hamming metric. A message $\boldsymbol{m}$ is encrypted with the public key $G_{pub} = SGP$, where G is a generator matrix of Goppa code, S is some random invertible matrix and P is a permutation matrix which S and P hide the structure of matrix G. The ciphertext $\boldsymbol{c}$ is computed by adding the codeword $\boldsymbol{m}G_{pub}$ with an error $\boldsymbol{e}$ of Hamming weight less than or equal to r, where r is the error correcting capability of Goppa code. By decoding $\boldsymbol{c}P^{-1}$ with respect to the Goppa code, $\boldsymbol{m}S$ can be obtained and thus retrieve $\boldsymbol{m} = \boldsymbol{m}SS^{-1}$. Although the original McEliece cryptosystem is still considered secured today, the large key size of Goppa codes (approximately 1 MB) is less practical in application. Many variants based on alternative families of codes were proposed to tackle this problem, yet many of them were proved to be insecure (for instance, [2,3]).

As an alternative for the Hamming metric, in 1985, Gabidulin introduced the rank metric and the Gabidulin codes [4] over a finite field with q^m elements, $\mathbb{F}_{q^m}$. Later, in 1991, Gabidulin et al. [5] proposed the first rank code based cryptosystem, namely the GPT cryptosystem that employs the similar idea as a McEliece cryptosystem to distort the public key matrix. They considered $G_{pub} = SG + X$, where S is a random invertible $k \times k$ matrix over $\mathbb{F}_{q^m}$, G is a generator matrix of Gabidulin codes, and X is a random matrix over $\mathbb{F}_{q^m}$ with column rank $t < n$. However, the GPT cryptosystem is shown to be insecure against Gibson's attack [6]. Since then, reparations on GPT were proposed (for instances, GPT [5], modified GPT [7,8], GGPT [9]); however, due to the weakness of Gabidulin codes containing huge vector space invariant under Frobenius automorphism, these cryptosystems were proved to be insecure by Overbeck's attack [10]. Then, proposals such as Gabidulin's General Reparation [11], Gabidulin, Rashwan and Honary [12], GPT with more general column scrambler [12], Loidreau's GGPT [13], and Smart Approach [14] that claimed to resist Overbeck's attack were proposed. The entries in P^{-1} need to be chosen over $\mathbb{F}_{q^m}$ and over $\mathbb{F}_q$ in a certain pattern so that the rank of $\boldsymbol{e}P^{-1}$ will be less than or equal to r. However, proposals with P of such pattern are proved to be insecure as they could be reduced into GGPT form by attacks proposed by [15,16]. In addition, some general rank syndrome decoding attacks on Gabidulin codes (for instances [17–19]) are able to attack the variants above with their suggested parameters in polynomial time.

In 2017, two new research papers about rank metric encryption scheme were presented. The first one is proposed by Gaborit et al. [20], namely RankPKE in their construction of a code-based identity-based encryption scheme. The second attempt is a McEliece type encryption proposed by Loidreau (LOI17) [21] that considers a scrambler matrix P with its inverse P^{-1} over V, a λ-dimensional subspace of $\mathbb{F}_{q^m}$. The term $\boldsymbol{c}P^{-1} = \boldsymbol{m}SG + \boldsymbol{e}P^{-1}$ has error $\boldsymbol{e}P^{-1}$ with $\boldsymbol{e}$ of rank t. In other words, the matrix P^{-1} amplifies the rank of $\boldsymbol{e}$, and this leads to larger public key size as t has to be λ times smaller than r.

1.2. Contributions

In this paper, we propose an encryption scheme based on the hard problem of rank syndrome decoding problem. Our construction hides the structure of the generator matrix of the code by adding a distortion matrix of column rank n, with an error of rank larger than r being added into the ciphertext. In particular, let $\boldsymbol{u} \in \mathbb{F}_{q^m}^n$ of rank n, a message $\boldsymbol{m} \in \mathbb{F}_{q^m}^{k'}$ is encrypted by

$$\boldsymbol{c}_2 = (\boldsymbol{m}\|\boldsymbol{m}_s)G_{pub} + \boldsymbol{e}_2 = (\boldsymbol{m}\|\boldsymbol{m}_s)(SG + \mathrm{Cir}_k(\boldsymbol{u})T) + \boldsymbol{e}_2,$$

where S is a random matrix in $GL_k(\mathbb{F}_{q^m})$, G is a generator matrix for a code $\mathcal{C}$ with error-correcting capability r, $\mathrm{Cir}_k(\boldsymbol{u})$ is a k-partial circulant matrix (refer to Definition 5 for formal definition), T is a random matrix in $\mathrm{GL}_n(\mathbb{F}_q)$, $\boldsymbol{m}_s$ is a random vector in $\mathbb{F}_{q^m}^{k-k'}$ and $\boldsymbol{e}_2$ is a random vector in $\mathbb{F}_{q^m}^n$ with rank $r_2 \leq \frac{r}{2}$. Note that the term $\boldsymbol{m}_s$ could be chosen such that the term $(\boldsymbol{m}\|\boldsymbol{m}_s)\mathrm{Cir}_k(\boldsymbol{u})T + \boldsymbol{e}_2$ in $\boldsymbol{c}_2$ has rank larger than $n - r_2$ (which is greater than r).

The term $\boldsymbol{c}_1 = (\boldsymbol{m}\|\boldsymbol{m}_s)\mathrm{Cir}_k(\boldsymbol{u}) + \boldsymbol{e}_1$ is included in the ciphertext, where $\boldsymbol{e}_1$ is a random vector in $\mathbb{F}_{q^m}^n$ with rank $r_1 \leq \frac{r}{2}$. Decryption could be performed by decoding $\boldsymbol{c}_2 - \boldsymbol{c}_1 T = (\boldsymbol{m}\|\boldsymbol{m}_s)SG + \boldsymbol{e}_2 - \boldsymbol{e}_1 T$ with respect to the code $\mathcal{C}$ whenever rank of $\boldsymbol{e}_2 - \boldsymbol{e}_1 T$ is less than or equal to r.

Advantages of Our Proposal. Our proposal has the following advantages:

i. The distortion matrix $\mathrm{Cir}_k(\boldsymbol{u})T$ is of column rank n, which hides the generator matrix G since T is random over $\mathbb{F}_q$.
ii. The error term $(\boldsymbol{m}\|\boldsymbol{m}_s)\mathrm{Cir}_k(\boldsymbol{u})T + \boldsymbol{e}_2$ has rank at least $n - r_2$. The adversary is not able to decode the ciphertext correctly since the generator matrix G is remained unknown and rank of $(\boldsymbol{m}\|\boldsymbol{m}_s)\mathrm{Cir}_k(\boldsymbol{u})T + \boldsymbol{e}_2$ is greater than r.
iii. For the case in LOI17 Encryption and other Gabidulin codes based cryptosystem, the multiplication of P^{-1} into $\boldsymbol{c}$ often amplifies the rank of the error term, resulting in a choice of error term with smaller rank in the ciphertext. Similarly, the rank of the error term in RankPKE has to be λ times smaller than r. On the contrary, in our proposal, we have freedom for the choice of $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ with rank $r_1 \leq \frac{r}{2}$ and $r_2 \leq \frac{r}{2}$, respectively.

We show that our encryption scheme has `IND-CPA` security under assumption of a Decisional Rank Syndrome Decoding problem. We propose Gabidulin codes as a choice of decodable code in our encryption. Furthermore, for similar post quantum security level of 2^{140} bits, our encryption scheme has smaller public key size as compared to key size suggested by LOI17 Encryption [21].

This paper is organized as follows: we review some preliminaries for rank metric and circulant matrix in Section 2. We also introduce the hard problems that our encryption is based on and name the known best attacks on the problem. In Section 3, we prove some bounds for the number of matrices of a fixed rank over a finite field and some related results. In Section 4, we describe our proposed cryptosystem and provide proofs for its advantages. In Section 5, we prove that our encryption scheme has `IND-CPA` security under assumption of Decisional Rank Syndrome Decoding problem. In Section 6, we propose the use of Gabidulin codes as a choice for the decodable code $\mathcal{C}$ in our encryption, and analyze its security. We also provide some parameters for the proposal based on the Gabidulin codes. Finally, we give our considerations of this paper in Section 7.

2. Preliminaries

In this section, we recall the definition of rank metric, which is the core of rank metric code based cryptosystems. We also introduce the Decisional Rank Syndrome Decoding problem, a hard problem in coding theory for our encryption scheme. We name the known best generic attacks on the Rank Syndrome Decoding problem.

2.1. Rank Metric

Let $\mathbb{F}_{q^m}$ be a finite field with q^m elements where q is a power of prime. In addition, let $\{\beta_1, \ldots, \beta_m\}$ be a basis of $\mathbb{F}_{q^m}$ over the base field $\mathbb{F}_q$.

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

Given a matrix M with coefficients in a field $\mathbb{F}$, the rank of M, $\text{rk}(M)$ is the dimension of the row span of M as a vector space over $\mathbb{F}$. We denote the row span of a matrix M over $\mathbb{F}$ by $\langle M \rangle_{\mathbb{F}}$, or $\langle M \rangle$ when the context is clear. We now define the rank metric of a vector on $\mathbb{F}_{q^m}^n$:

Definition 2. *Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. The rank of $\boldsymbol{x}$ in $\mathbb{F}_q$, denoted by $rk_q(\boldsymbol{x})$ is the rank of the matrix $X = (x_{ij}) \in \mathbb{F}_q^{m \times n}$, where $x_j = \sum_{i=1}^m x_{ij}\beta_i$.*

Equivalently, the rank of $\boldsymbol{x}$ is the dimension over $\mathbb{F}_q$ of the subspace of $\mathbb{F}_{q^m}$ which is spanned by the coordinates of $\boldsymbol{x}$. Note that the rank of a vector is a norm and is independent of the chosen basis. Similarly, we have the following definition of column rank for a matrix in $\mathbb{F}_{q^m}^{k \times n}$:

Definition 3. *Let $M \in \mathbb{F}_{q^m}^{k \times n}$. The column rank of M over $\mathbb{F}_q$, denoted by $colrk_q(M)$ is the maximum number of linearly independent columns over $\mathbb{F}_q$.*

We now state a few results related to the rank metric which are important prerequisites for results in later sections.

Lemma 1. *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $rk_q(\boldsymbol{x}) = r$, then there exists $\hat{\boldsymbol{x}} \in \mathbb{F}_{q^m}^r$ with $rk_q(\hat{\boldsymbol{x}}) = r$ and $U \in \mathbb{F}_q^{r \times n}$ with $rk_q(U) = r$ such that $\boldsymbol{x} = \hat{\boldsymbol{x}}U$. This decomposition is unique up to $GL_r(\mathbb{F}_q)$-operation between $\hat{\boldsymbol{x}}$ and U* [15].

Definition 4. *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ with $rk_q(\boldsymbol{x}) = r$ and decomposition $\boldsymbol{x} = \hat{\boldsymbol{x}}U$ as in Lemma 1. We call U a Grassman support matrix for $\boldsymbol{x}$ and $supp_{Gr}(\boldsymbol{x}) = \langle U \rangle_{\mathbb{F}_{q^m}}$ the Grassman support of $\boldsymbol{x}$.*

Lemma 2. *Let $M \in \mathbb{F}_{q^m}^{k \times n}$ and $colrk_q(M) = s < n$* [16] *. Then, there exists $M' \in \mathbb{F}_{q^m}^{k \times s}$ with $colrk_q(M') = s$ and K an invertible $n \times n$ matrix over $\mathbb{F}_q$ such that*

$$MK = \left(M' \mid \mathbf{0}_{k \times (n-s)} \right). \tag{1}$$

2.2. Circulant and Partial Circulant Matrix

As mentioned in Section 1, we use a k-partial circulant matrix as the distortion matrix for the code with an efficient decoding algorithm. Here, we give the definition of the circulant matrix and k-partial circulant matrix induced by a random vector, $\boldsymbol{x}$.

Definition 5. *Let $\boldsymbol{x} = (x_0, \dots, x_{n-1}) \in \mathbb{F}_{q^m}^n$. The circulant matrix induced by $\boldsymbol{x}$ is defined as*

$$Cir_n(\boldsymbol{x}) := \begin{pmatrix} x_0 & x_{n-1} & \dots & x_1 \\ x_1 & x_0 & \dots & x_2 \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & x_{n-2} & \dots & x_0 \end{pmatrix} \in \mathbb{F}_{q^m}^{n \times n}.$$

The k-partial circulant matrix, $Cir_k(\boldsymbol{x})$, induced by $\boldsymbol{x}$ is the first k rows of $Cir_n(\boldsymbol{x})$.

In fact, a k-partial circulant matrix induced by $\boldsymbol{x}$ has column rank depending on rank of $\boldsymbol{x}$. We have the following result, which helps us to ensure that the distortion matrix that we choose has column rank as desired:

Lemma 3. *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ with $rk_q(\boldsymbol{x}) = t$; then, $colrk_q(Cir_k(\boldsymbol{x})) \geq t$.*

Proof. Suppose to the contrary that $\mathrm{colrk}_q(\mathrm{Cir}_k(\boldsymbol{x})) < t$; then, there exists at most $t-1$ columns of $\mathrm{Cir}_k(\boldsymbol{u})$ that are linearly independent over $\mathbb{F}_q$. Consider the first row of $\mathrm{Cir}_k(\boldsymbol{x})$: $\{x_0, x_1, \dots, x_{n-1}\}$; then, at most $t-1$ elements in $\{x_0, x_1, \dots, x_{n-1}\}$ are linearly independent over $\mathbb{F}_q$. In other words, $\mathrm{rk}_q(\boldsymbol{x}) \leq t-1$, which is a contradiction to $\mathrm{rk}_q(\boldsymbol{x}) = t$. □

2.3. Hard Problems in Coding Theory

We describe the hard problems which our cryptosystem is based on.

Definition 6. ***Rank Syndrome Decoding Problem (RSD)**. Let H be a full rank $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$, $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and w an integer. The Rank Syndrome Decoding Problem RSD(q,m,n,k,w) needs to determine $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $rk_q(\boldsymbol{x}) = w$ and $H\boldsymbol{x}^T = \boldsymbol{s}^T$.*

The RSD problem is analogous to the classical syndrome decoding problem with Hamming metric. Recently, the RSD problem has been proven to be hard with probabilistic reduction to the Hamming setting [22].

Given $G \in \mathbb{F}_{q^m}^{k \times n}$, a full rank parity-check matrix of H in an RSD problem and $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$. Then, the dual version of $RSD(q,m,n,k,w)$ is to determine $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ and $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}_q(\boldsymbol{x}) = w$ and $\boldsymbol{y} = \boldsymbol{m}G + \boldsymbol{x}$.

Notation. If X is a finite set, we write $\boldsymbol{x} \overset{\$}{\leftarrow} X$ to denote assignment to $\boldsymbol{x}$ of an element randomly sampled from the distribution on X.

We now give the definition of Decisional version of RSD problem in its dual form:

Definition 7. ***Decisional RSD Problem (DRSD)**. Let G be a full rank $k \times n$ matrix over F_{q^m}, $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ and $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ of rank r. The Decisional RSD Problem $DRSD(q,m,n,k,w)$ needs to distinguish the pair $(\boldsymbol{m}G + \boldsymbol{x}, G)$ from $(\boldsymbol{y}, G)$ where $\boldsymbol{y} \overset{\$}{\leftarrow} \mathbb{F}_{q^m}^n$.*

It was proved that DRSD is hard in the worst case [20]. Therefore, DRSD is eligible to be a candidate of hard problems in coding theory. The hardness of our cryptosystem relies on the DRSD problem (refer to Section 5).

2.4. Generic Attacks on RSD

There are generally two types of generic attacks on the RSD problem, namely the combinatorial attack and algebraic attack.

Combinatorial Attack. The combinatorial approach depends on counting the number of possible supports of size r for a rank code of length n over $\mathbb{F}_{q^m}$, which corresponds to the number of subspaces of dimension r in $\mathbb{F}_{q^m}$. We summarize the best combinatorial attacks with their conditions and complexities in Table 1.

Table 1. Best combinatorial attacks on RSD with their conditions and complexities.

Conditions	Best Combinatorial Attacks
$m < n$, $m > k+1+r$	$O\left(\min\left\{(n-k)^3m^3q^{r\frac{(k+1)m}{n}-m}, r^3m^3q^{(r-1)(k+1)}\right\}\right)$ [19,23]
$m < n$, $m \leq k+1+r$	$O\left(\min\left\{(n-k)^3m^3q^{r\frac{(k+1)m}{n}-m}, (k+r)^3r^3q^{(m-r)(r-1)}\right\}\right)$ [19,23]
$m \geq n$, $\mathbf{s} \neq \mathbf{0}$	$O\left(\min\left\{(n-k)^3m^3q^{\min\left\{r\frac{(k+1)m}{n}-m, rk, (r-1)(k+1)\right\}}, r^3m^3q^{(r-1)(k+1)}\right\}\right)$ [17,19,23]
$m \geq n$, $\mathbf{s} = \mathbf{0}$	$O\left(\min\left\{(n-k)^3m^3q^{\min\left\{r\frac{(k+1)m}{n}-m, (r-1)k\right\}}, r^3m^3q^{(r-1)(k+1)}\right\}\right)$ [17,19,23]

Algebraic Attack. The nature of the rank metric favors algebraic attacks using Gröbner bases, as they are largely independent of the value q. These attacks became efficient when q increases. We summarize the complexity of algebraic attacks in Table 2.

Table 2. Best Algebraic Attacks on RSD with their conditions and complexities.

Attacks	**Conditions**	**Complexity**
CG-Kernel [24]		$O\left(k^3m^3q^{r\left\lceil\frac{km}{n}\right\rceil}\right)$
GRS-Basic Approach [17]	$n \geq (r+1)(k+1)-1$	$O\left(((r+1)(k+1)-1)^3\right)$
GRS-Hybrid Approach [17]	$\left\lceil\frac{(r+1)(k+1)-(n+1)}{r}\right\rceil \leq k$	$O\left(r^3k^3q^{r\left\lceil\frac{(r+1)(k+1)-(n+1)}{r}\right\rceil}\right)$

3. Rank of Matrix

The following are some results related to the rank of a matrix over a finite field, which is crucial for the construction of our encryption. We provide some bounds for the number of $m \times n$ matrices over $\mathbb{F}_q$ of rank $r < \min\{m, n\}$.

Proposition 1. *Denote $T_r^{(m\times n)}$ as the number of $m \times n$ matrices over $\mathbb{F}_q$ of rank r; then, $T_r^{(m\times n)} = \frac{Q_r(q^n)Q_r(q^m)}{Q_r(q^r)}$, where $Q_r(x) = \prod_{i=0}^{r-1}\left(x - q^i\right)$* [25,26].

We need the following lemma to give some bounds for $T_r^{(m\times n)}$.

Lemma 4. *For $0 \leq i \leq r-1$, if $m \geq n > r$, then*

$$q^{n-r} < \left(1 - \frac{q^i}{q^m}\right)\left(\frac{q^{n-i}-1}{q^{r-i}-1}\right) < q^{n-r}\left(\frac{q}{q-1}\right).$$

Proof. Expand $\left(1-\frac{q^i}{q^m}\right)\left(\frac{q^{n-i}-1}{q^{r-i}-1}\right) = \frac{q^{m+n-2i}+1-q^{n-i}-q^{m-i}}{q^{m-i}(q^{r-i}-1)}$; it suffices for us to show that $q^{n-r} < \frac{q^{m+n-2i}+1-q^{n-i}-q^{m-i}}{q^{m-i}(q^{r-i}-1)} < q^{n-r}\left(\frac{q}{q-1}\right)$. Since $m-r+1>0$, we have $q^{m-i}+q^{n-i} \leq q^{n+m-r-i}+1$, and thus

$$q^{m+n-2i}-q^{m+n-r-i} = q^{n+m-r-i}\left(q^{r-i}-1\right) < q^{m+n-2i}-q^{m-i}-q^{n-i}+1,$$

which implies that

$$q^{n-r} < \frac{q^{m+n-2i}+1-q^{n-i}-q^{m-i}}{q^{m-i}(q^{r-i}-1)}.$$

Since $1+i \leq r$, then $q^{m-i}+\left(q^{n-i}+q\right) < q^{m+1-i}+q^{n+1-i}$ and $q^{m+n+1-r-i} \leq q^{m+n-2i}$. Adding these inequalities gives us

$$q^{m+n+1-2i}+(q^{m-i}+q^{n-i}+q+q^{m+n+1-r-i}) < q^{m+n+1-2i}+1+(q^{m+1-i}+q^{n+1-i}+q^{m+n-2i}).$$

We have

$$\begin{aligned}
&(q^{m+n-2i}+1-q^{n-i}-q^{m-i})(q-1)\\
&= q^{m+n+1-2i}+q-q^{n+1-i}-q^{m+1-i}-q^{m+n-2i}-1+q^{m-i}+q^{n-i}\\
&< q^{m+n+1-2i}-q^{m+n+1-r-i}\\
&= q^{n-r+1}q^{m-i}\left(q^{r-i}-1\right),
\end{aligned}$$

which implies that

$$\frac{q^{m+n-2i}+1-q^{n-i}-q^{m-i}}{q^{m-i}\left(q^{r-i}-1\right)} < \frac{q^{n-r+1}}{q-1} = q^{n-r}\left(\frac{q}{q-1}\right).$$

This completes the proof for the inequalities. □

Now, we prove an upper bound and a lower bound for $T_r^{(m\times n)}$:

Proposition 2. *Let $r < min\{m,n\}$; then, the number of $m\times n$ matrices over $\mathbb{F}_q$ of rank r is bounded by*

$$q^{r(m+n-r)} < T_r^{(m\times n)} < \frac{q^{r(m+n+1-r)}}{(q-1)^r}.$$

Proof. Assuming that $m \geq n > r$, recall that $Q_r(x) = \prod_{i=0}^{r-1}(x-q^i)$, and we have

$$T_r^{(m\times n)} = \frac{Q_r(q^m)Q_r(q^n)}{Q_r(q^r)} = q^{mr}\prod_{i=0}^{r-1}\left(1-\frac{q^i}{q^m}\right)\left(\frac{q^{n-i}-1}{q^{r-i}-1}\right).$$

By Lemma 4,

$$\begin{aligned} q^{mr}\prod_{i=0}^{r-1}\left(q^{n-r}\right) &= q^{r(m+n-r)} \\ &< T_r^{(m\times n)} \\ &< q^{mr}\prod_{i=0}^{r-1}\left(q^{n-r}\left(\frac{q}{q-1}\right)\right) \\ &= \frac{q^{r(m+n+1-r)}}{(q-1)^r}. \end{aligned}$$

For $n \geq m > r$, the statement could be proved by switching the term m and n in the statement and in Lemma 4. □

Proposition 3. *Assuming that $m \geq n \geq 5$, then $T_{n-1}^{(m\times n)} = \frac{(q^n-1)}{(q-1)(q^m-q^{n-1})}T_n^{(m\times n)}$.*

Proof. Recalling Proposition 1,

$$\begin{aligned} T_{n-1}^{(m\times n)} &= \frac{Q_{n-1}(q^m)Q_{n-1}(q^n)}{Q_{n-1}(q^{n-1})} = \frac{\prod_{i=0}^{n-2}(q^n-q^i)\prod_{i=0}^{n-2}(q^m-q^i)}{\prod_{i=0}^{n-2}(q^{n-1}-q^i)} \\ &= \frac{(q^n-1)q^{n-2}\prod_{i=0}^{n-2}(q^{n-1}-q^i)\prod_{i=0}^{n-2}(q^m-q^i)}{(q^{n-1}-q^{n-2})\prod_{i=0}^{n-2}(q^{n-1}-q^i)} \\ &= \frac{(q^n-1)\prod_{i=0}^{n-2}(q^m-q^i)}{(q-1)} = \frac{(q^n-1)\prod_{i=0}^{n-1}(q^m-q^i)}{(q-1)(q^m-q^{n-1})} \\ &= \frac{(q^n-1)}{(q-1)(q^m-q^{n-1})}T_n^{(m\times n)}. \end{aligned}$$

This completes the statement. □

4. A New Encryption Scheme

In this section, we propose our new encryption scheme which consists of a public matrix distorted by a matrix of column rank n. We will discuss some strengths of this encryption after the description of the scheme.

Presentation of the Encryption Scheme, $\mathtt{PE} = (\mathcal{S}_{\text{PE}}, \mathcal{K}_{\text{PE}}, \mathcal{E}_{\text{PE}}, \mathcal{D}_{\text{PE}})$.

$\boxed{\textbf{Setup}, \mathcal{S}_{\text{PE}}}$ generates global parameters $m > n > k > k' \geq 1$, $k' = \left\lfloor \frac{k}{2} \right\rfloor$ and $r \leq \left\lfloor \frac{n-k}{2} \right\rfloor$. The plaintext space is $\mathbb{F}_{q^m}^{k'}$. Output parameters $= (m, n, k, k', r)$.

$\boxed{\textbf{Key Generation}, \mathcal{K}_{\text{PE}}}$ Generate invertible matrix $S \xleftarrow{\$} \mathbb{F}_{q^m}^{k\times k}$. Generate a generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ of a linear code $\mathcal{C}_G$ with an efficient decoding algorithm $\mathcal{C}_G.\mathfrak{Dec}(\cdot)$ able to correct error up to rank r. Generate vector $\boldsymbol{u} \xleftarrow{\$} \mathbb{F}_{q^m}^{n}$ such that $\text{rk}_q(\boldsymbol{u}) = n$. Generate invertible matrix $T \xleftarrow{\$} \mathbb{F}_q^{n\times n}$. Output public key $\kappa_{pub} = \left(G_{pub} = SG + \text{Cir}_k(\boldsymbol{u})T, \boldsymbol{u}\right)$ and private key $\kappa_{sec} = (S, G, T)$.

$\boxed{\textbf{Encryption}, \mathcal{E}_{\text{PE}}(\kappa_{pub}, \boldsymbol{m})}$ Let $\boldsymbol{m} \in \mathbb{F}_{q^m}^{k'}$ be the message to be encrypted. Generate random $\boldsymbol{m}_s \xleftarrow{\$} \mathbb{F}_{q^m}^{k-k'}$ satisfying $\text{rk}_q\left((\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u})\right) > \left\lceil \frac{3}{4}(n-k) \right\rceil$. Generate random $\boldsymbol{e}_1, \boldsymbol{e}_2 \xleftarrow{\$} \mathbb{F}_{q^m}^{n}$ such that $\text{rk}_q(\boldsymbol{e}_1) = r_1 \leq \frac{r}{2}$ and $\text{rk}_q(\boldsymbol{e}_2) = r_2 \leq \frac{r}{2}$. Compute $\boldsymbol{c}_1 = (\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u}) + \boldsymbol{e}_1$ and $\boldsymbol{c}_2 = (\boldsymbol{m}\|\boldsymbol{m}_s)G_{pub} + \boldsymbol{e}_2$. Output $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2)$ as the ciphertext.

$\boxed{\textbf{Decryption}, \mathcal{D}_{\text{PE}}(\kappa_{sec}, \boldsymbol{c})}$ Returns $(\boldsymbol{m} \| \boldsymbol{m}_s) = (\mathcal{C}_G.\mathfrak{Dec}(\boldsymbol{c}_2 - \boldsymbol{c}_1 T))\, S^{-1}$.

Remark 1. *By Proposition 2, the number of $\boldsymbol{e}_1$ that can be chosen is at least $T_{r_1}^{m \times n}$, which is at least $q^{r_1(m+n-r_1)}$. Similarly, the number of $\boldsymbol{e}_2$ that can be chosen is at least $T_{r_2}^{m \times n}$, which is at least $q^{r_2(m+n-r_2)}$*

Correctness. The correctness of our encryption scheme relies on the decoding capability of the code $\mathcal{C}$. Using the private keys, we have $\boldsymbol{c}_2 - \boldsymbol{c}_1 T = (\boldsymbol{m}\|\boldsymbol{m}_s)G_{pub} + \boldsymbol{e}_2 - ((\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u}) - \boldsymbol{e}_1)\, T = (\boldsymbol{m}\|\boldsymbol{m}_s)SG + \boldsymbol{e}_2 - \boldsymbol{e}_1 T$. Since $\text{rk}_q(\boldsymbol{e}_2 - \boldsymbol{e}_1 T) \leq \text{rk}_q(\boldsymbol{e}_2) + \text{rk}_q(\boldsymbol{e}_1 T) = \text{rk}_q(\boldsymbol{e}_2) + \text{rk}_q(\boldsymbol{e}_1) \leq r$, then the decoding algorithm can decode correctly and retrieve $(\boldsymbol{m}\|\boldsymbol{m}_s)S = \mathcal{C}_G.\mathfrak{Dec}(\boldsymbol{c}_2 - \boldsymbol{c}_1 T)$. Finally, compute $(\boldsymbol{m}, \boldsymbol{m}_s) = (\boldsymbol{m}\|\boldsymbol{m}_s)SS^{-1}$ to recover $(\boldsymbol{m}\|\boldsymbol{m}_s)$.

Strengths of the Proposed Encryption.

Recall from Section 1 that there are currently two approaches in constructing a rank metric code based encryption scheme. The idea of the first approach is to scramble the generator matrix G so that the matrix for encryption will appear to be random. As a result, the adversary is not able to decode it correctly. Therefore, the error chosen to encrypt the message in LOI17 Encryption must have rank λ times smaller than r. Nevertheless, in our construction, we can choose $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ with rank $r_1 \leq \frac{r}{2}$ and $r_2 \leq \frac{r}{2}$, respectively. Furthermore, the matrix G in our encryption is scrambled by adding a matrix X, i.e., $G_{pub} = SG + X$, where $X = \text{Cir}_k(\boldsymbol{u})T$ with column rank n as proved in the following:

Corollary 1. *Let $\boldsymbol{u} \in \mathbb{F}_{q^m}^n$ such that $rk_q(\boldsymbol{u}) = n$. Then, for any invertible $T \in \mathbb{F}_q^{n \times n}$, the column rank of $Cir_k(\boldsymbol{u})T$, $colrk_q(Cir_k(\boldsymbol{u})T) = n$.*

Proof. It suffices to show that $\text{colrk}_q(\text{Cir}_k(\boldsymbol{u})) = n$. Since $\text{colrk}_q(\text{Cir}_k(\boldsymbol{u})) \geq \text{rk}_q(\boldsymbol{u}) = n$ by Lemma 3, and $\text{colrk}_q(\text{Cir}_k(\boldsymbol{u})) \leq n$, then $\text{colrk}_q(\text{Cir}_k(\boldsymbol{u})) = n$. □

By Corollary 1, our $X = \text{Cir}_k(\boldsymbol{u})T$ chosen has column rank n instead of $t < n$. This will make the reduction of X into the form $XK = (X' \mid \boldsymbol{0})$ (as in Lemma 2) impossible, where K is an invertible $n \times n$ matrix over $\mathbb{F}_q$.

On the other hand, the second approach in constructing rank metric code based encryption is to make the generator matrix G publicly known, and introduces an error $\boldsymbol{e}$ with big rank (greater than r) into the ciphertext $\boldsymbol{c}$ to ensure the decoding for retrieval of plaintext $\hat{\boldsymbol{m}}$ is hard, i.e., $\boldsymbol{c} = \hat{\boldsymbol{m}}G + \boldsymbol{e}$ and $\text{rk}_q(\boldsymbol{e}) > r$.

In fact, in our encryption scheme, the error term $(\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u})T + \boldsymbol{e}_2$ in the ciphertext $\boldsymbol{c}_2$ has error larger than r, i.e., $\text{rk}_q((\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u})T + \boldsymbol{e}_2) > r$:

Proposition 4. *Let $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{F}_{q^m}^n$ such that $rk_q(\boldsymbol{u}) = n$. Given $\hat{\boldsymbol{m}} = (\boldsymbol{m}, \boldsymbol{m}_s) \in \mathbb{F}_{q^m}^k$ such that $rk_q((\boldsymbol{m}, \boldsymbol{m}_s)Cir_k(\boldsymbol{u})) > \lceil \frac{3}{4}(n-k) \rceil$. Then, for any $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^n$ such that $rk_q(\boldsymbol{e}_2) = r_2$, we have $rk_q((\boldsymbol{m}, \boldsymbol{m}_s)Cir_k(\boldsymbol{u})T + \boldsymbol{e}_2) > r$.*

Proof. Given $\hat{\boldsymbol{m}} = (\boldsymbol{m}\|\boldsymbol{m}_s) \in \mathbb{F}_{q^m}^k$ and $\text{rk}_q((\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u})) > \lceil \frac{3}{4}(n-k) \rceil$, then, for any $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^n$ such that $\text{rk}_q(\boldsymbol{e}_2) = r_2$,

$$\begin{aligned} \text{rk}_q((\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u})T + \boldsymbol{e}_2) &\geq \text{rk}_q((\boldsymbol{m}\|\boldsymbol{m}_s)\text{Cir}_k(\boldsymbol{u})T) - \text{rk}_q(\boldsymbol{e}_2) \\ &> \frac{3}{4}(n-k) - r_2 \geq \frac{3}{2}r - r_2 \\ &> \frac{3}{2}r - \frac{1}{2}r = r \end{aligned}$$

since $T \in \mathbb{F}_q^{n \times n}$ is invertible. □

By Proposition 4, we have $\text{rk}_q((\boldsymbol{m}\|\boldsymbol{m_s})\text{Cir}_k(\boldsymbol{u})T+\boldsymbol{e}_2)>r$. The adversary is not able to recover the plaintext $\boldsymbol{m}$ from $\boldsymbol{c}_2=(\boldsymbol{m}\|\boldsymbol{m_s})SG+((\boldsymbol{m}\|\boldsymbol{m_s})\text{Cir}_k(\boldsymbol{u})T+\boldsymbol{e}_2)$ even if he knows the structure of the generator matrix G. However, in practicality, G remains unknown to the adversary.

5. IND-CPA Secure Encryption

The desired security property of a public-key encryption scheme is indistinguishability under chosen plaintext attack (IND-CPA). This is normally defined by a security game that is interacting between a challenger and an adversary $\mathcal{A}$. The security game is described as follows:

Set up: Given a security parameter, the challenger first runs the key generation algorithm and send κ_{pub} to $\mathcal{A}$.

Challenge: $\mathcal{A}$ chooses two equal length plaintexts $\boldsymbol{m}_0$ and $\boldsymbol{m}_1$; and sends these to the challenger.

Encrypt challenge messages: The challenger chooses a random $b\in\{0,1\}$, computes a challenge ciphertext $\boldsymbol{c}=\mathcal{E}_{\mathtt{PE}}(\kappa_{pub},\boldsymbol{m}_b)$ and returns $\boldsymbol{c}$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ outputs a bit $b'\in\{0,1\}$. $\mathcal{A}$ wins if $b'=b$.

The advantage of an adversary $\mathcal{A}$ is defined as

$$\mathsf{Adv}^{\mathtt{IND-CPA}}_{\mathtt{PE},\mathcal{A}}(\lambda)=\left|\Pr[b'=b]-\frac{1}{2}\right|.$$

A secure public-key encryption scheme against chosen plaintext attack is formally defined as follows:

Definition 8. *A public-key encryption scheme* $\mathtt{PE}=(\mathcal{S}_{\mathtt{PE}},\mathcal{K}_{\mathtt{PE}},\mathcal{E}_{\mathtt{PE}},\mathcal{D}_{\mathtt{PE}})$ *is* (t,ϵ)*-*IND-CPA *secure if, for any probabilistic t-polynomial time, the adversary* $\mathcal{A}$ *has the advantage less than* ϵ*, that is,* $\mathsf{Adv}^{\mathtt{IND-CPA}}_{\mathtt{PE},\mathcal{A}}(\lambda)<\epsilon$.

Lemma 5. *Let* T_1, T_2 *and* F *be events. Suppose the event* $\mathsf{T}_2\wedge\neg\mathsf{F}$ *occurs if and only if* $\mathsf{T}_1\wedge\neg\mathsf{F}$ *occurs, then* $\left|\Pr[\mathsf{T}_2]-\Pr[\mathsf{T}_1]\right|\leq\Pr[\mathsf{F}]$(Difference Lemma [27]).

We have the following result which is important in our encryption.

Lemma 6. *Given* $m\geq n$, $k\geq 1$, $j\geq 2$ *and* $r<\frac{n}{2}$. *Let* $\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}^n_{q^m}$*, then there exists* $\boldsymbol{e}\in\mathbb{F}^n_{q^m}$ *with* $rk_q(\boldsymbol{e})=r'\leq\frac{r}{j}$ *such that* $rk_q(\boldsymbol{x}+\boldsymbol{e})\geq r'+1$ *and* $rk_q(\boldsymbol{y}+\boldsymbol{e})\geq r'+1$.

Proof. Let $\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}^n_{q^m}$ such that $\text{rk}_q(\boldsymbol{x})=a$ and $\text{rk}_q(\boldsymbol{y})=b$. We prove the statement by consider different cases for a and b.

Case 1 ($\frac{2}{j}r+1\leq a\leq n$ and $\frac{2}{j}r+1\leq b\leq n$): Let $\boldsymbol{e}$ be any element in $\mathbb{F}^n_{q^m}$ such that $\text{rk}_q(\boldsymbol{e})=r'\leq\frac{r}{j}$. Then $\text{rk}_q(\boldsymbol{x}+\boldsymbol{e})\geq\text{rk}_q(\boldsymbol{x})-\text{rk}_q(\boldsymbol{e})=a-\frac{r}{j}\geq\frac{2}{j}r+1-\frac{r}{j}=\frac{r}{j}+1\geq r'+1$. Similarly, $\text{rk}_q(\boldsymbol{y}+\boldsymbol{e})\geq\text{rk}_q(\boldsymbol{y})-\text{rk}_q(\boldsymbol{e})=b-\frac{r}{j}\geq\frac{2}{j}r+1-\frac{r}{j}=\frac{r}{j}+1\geq r'+1$.

Case 2 ($1\leq a\leq\frac{2}{j}r$ and $\frac{2}{j}r+1\leq b\leq n$): Since $\text{rk}_q(\boldsymbol{x})=a$, by Lemma 1, $\boldsymbol{x}=(x_1,\ldots,x_a)A$, where $x_1,\ldots,x_a$ are linearly independent and A is an $a\times n$ matrix over $\mathbb{F}_q$ of rank a. Let $\mathcal{X}=\{x_1,\ldots,x_a\}$, consider a basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ such that $\mathcal{X}\subset\mathcal{B}$ and let $\mathcal{B}_e=\mathcal{B}\setminus\mathcal{X}$. Note that $|\mathcal{B}_e|=m-a\geq n-a\geq n-\frac{2}{j}r>\frac{r}{j}\geq r'$. Then, we can form $\boldsymbol{e}$ of rank r' by choosing r' elements from $\mathcal{B}_e$, and we have $\text{rk}_q(\boldsymbol{x}+\boldsymbol{e})\geq r'+1$ since elements in $\boldsymbol{x}$ are linearly independent with elements in $\boldsymbol{e}$. With this $\boldsymbol{e}$, we have $\text{rk}_q(\boldsymbol{y}+\boldsymbol{e})\geq\text{rk}_q(\boldsymbol{y})-\text{rk}_q(\boldsymbol{e})=b-r'\geq\frac{2}{j}r+1-r'\geq r'+1$.

Case 3 ($\frac{2}{j}r+1\leq a\leq n$ and $1\leq b\leq\frac{2}{j}r$): This case follows the proof of Case 2 by interchanging the term a with b, and $\boldsymbol{x}$ with $\boldsymbol{y}$.

Case 4 ($1 \le a \le \frac{2}{j}r$ and $1 \le b \le \frac{2}{j}r$): Since $\mathrm{rk}_q(\boldsymbol{x}) = a$, by Lemma 1, $\boldsymbol{x} = (x_1, \dots, x_a)A$, where $x_1, \dots, x_a$ are linearly independent and A is an $a \times n$ matrix over $\mathbb{F}_q$ of rank a. Similarly, since $\mathrm{rk}_q(\boldsymbol{y}) = b$, by Lemma 1, $\boldsymbol{y} = (y_1, \dots, y_b)B$, where $y_1, \dots, y_b$ are linearly independent and B is an $b \times n$ matrix over $\mathbb{F}_q$ of rank b. Let $\mathcal{X} = \{x_1, \dots, x_a\}$ and $\mathcal{Y} = \{y_1, \dots, y_b\}$, consider a basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ such that $\mathcal{X} \cup \mathcal{Y} \subset \mathcal{B}$ and let $\mathcal{B}_e = \mathcal{B} \setminus (\mathcal{X} \cup \mathcal{Y})$.

If $j \ge 3$, since $|\mathcal{X} \cup \mathcal{Y}| \le \frac{4}{j}r$ and $jn \ge 3n \ge 6r$, then $|\mathcal{B}_e| \ge m - \frac{4}{j}r \ge n - \frac{4}{j}r \ge \frac{6}{j}r - \frac{4}{j}r > \frac{r}{j} > r'$. We can form $\boldsymbol{e}$ of rank r' by choosing $\frac{r}{j}$ elements from $\mathcal{B}_e$. Thus, we have $\mathrm{rk}_q(\boldsymbol{x} + \boldsymbol{e}) \ge r' + 1$ since elements in $\boldsymbol{x}$ are linearly independent with elements in $\boldsymbol{e}$, and $\mathrm{rk}_q(\boldsymbol{y} + \boldsymbol{e}) \ge r' + 1$ since elements in $\boldsymbol{y}$ are linearly independent with elements in $\boldsymbol{e}$.

If $j = 2$, then we further break this case into the following subcases:

$1 \le a \le \frac{r}{2}$ or $1 \le b \le \frac{r}{2}$: WLOG, assume that $1 \le a \le \frac{r}{2}$, then $|\mathcal{B}_e| = m - (a + b) \ge n - (a + b) \ge n - \left(\frac{r}{2} + r\right) > \frac{r}{2} \ge r'$. We can form $\boldsymbol{e}$ of rank r' by choosing r' elements from $\mathcal{B}_e$. Thus, we have $\mathrm{rk}_q(\boldsymbol{x} + \boldsymbol{e}) \ge r' + 1$ since elements in $\boldsymbol{x}$ are linearly independent with elements in $\boldsymbol{e}$, and $\mathrm{rk}_q(\boldsymbol{y} + \boldsymbol{e}) \ge r' + 1$ since elements in $\boldsymbol{y}$ are linearly independent with elements in $\boldsymbol{e}$.

$1 + \frac{r}{2} \le a \le r$ and $1 + \frac{r}{2} \le b \le r$: WLOG, assume that $a \ge b$. If $\mathcal{Y} \subseteq \mathcal{X}$, then $|\mathcal{B}_e| = m - a \ge n - a \ge n - r > \frac{r}{2} \ge r'$. We can form $\boldsymbol{e}$ of rank r' by choosing r' elements from $\mathcal{B}_e$. Thus, we have $\mathrm{rk}_q(\boldsymbol{x} + \boldsymbol{e}) \ge r' + 1$ since elements in $\boldsymbol{x}$ are linearly independent with elements in $\boldsymbol{e}$, and $\mathrm{rk}_q(\boldsymbol{y} + \boldsymbol{e}) \ge r' + 1$ since elements in $\boldsymbol{y}$ are linearly independent with elements in $\boldsymbol{e}$. If $\mathcal{Y} \not\subseteq \mathcal{X}$, let $\mathcal{Z} = \mathcal{X} \cap \mathcal{Y}$ and $t = |\mathcal{Z}|$. Let $a' = a - \frac{r}{2}$, $b' = b - \frac{r}{2}$, and $v = \frac{r}{2} - t$, pick v elements $x'_1, \dots, x'_v \in \mathcal{X} \setminus \mathcal{Z}$ and another v elements $y'_1, \dots, y'_v \in \mathcal{Y} \setminus \mathcal{Z}$. Then, considering $\mathcal{B}_{\mathcal{N}} = \mathcal{B} \setminus (\{x'_1, \dots, x'_v, y'_1, \dots, y'_v\} \cup \mathcal{Z})$, we have $|\mathcal{B}_{\mathcal{N}}| = m - (2v + t) \ge n - (2v + t) = n - (r - t) = n - r + t > n - r > \frac{r}{2} \ge r'$. We can form $\boldsymbol{e}$ of rank r' by choosing r' elements from $\mathcal{B}_{\mathcal{N}}$ (with at least one element from $\mathcal{B}_e$), and the elements picked will only decrease the rank of $\boldsymbol{x}$ and $\boldsymbol{y}$ at most by $a' - 1$ and $b' - 1$, respectively. Therefore, we have $\mathrm{rk}_q(\boldsymbol{x} + \boldsymbol{e}) \ge a - (a' - 1) \ge \frac{r}{2} + 1 \ge r' + 1$ and $\mathrm{rk}_q(\boldsymbol{y} + \boldsymbol{e}) \ge b - (b' - 1) \ge \frac{r}{2} + 1 \ge r' + 1$. □

Now, suppose the challenger adversary chooses two equal length plaintexts $\boldsymbol{m}_0, \boldsymbol{m}_1 \in \mathbb{F}_{q^m}^{k'}$ and sends these to the challenger. By the following lemma, the challenger is able to choose a random $\boldsymbol{m}_s \in \mathbb{F}_{q^m}^{k-k'}$, $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n}$ such that the conditions (2)–(7) are satisfied:

Lemma 7. *Given $\boldsymbol{m}_0, \boldsymbol{m}_1 \in \mathbb{F}_{q^m}^{k'}$ and $\boldsymbol{m}_s \in \mathbb{F}_{q^m}^{k-k'}$, there exists $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n}$ such that*

$$rk_q(\boldsymbol{e}_1) = r_1 \le r/2, \tag{2}$$

$$rk_q((\boldsymbol{0}_{k'} \| \boldsymbol{m}_s) Cir_k(\boldsymbol{u}) + \boldsymbol{e}_1) \ge r_1 + 1, \tag{3}$$

$$rk_q((\boldsymbol{m}_0 + \boldsymbol{m}_1 \| \boldsymbol{m}_s) Cir_k(\boldsymbol{u}) + \boldsymbol{e}_1) \ge r_1 + 1, \tag{4}$$

$$rk_q(\boldsymbol{e}_2) = r_2 \le r/2, \tag{5}$$

$$rk_q((\boldsymbol{0}_{k'} \| \boldsymbol{m}_s) G_{pub} + \boldsymbol{e}_2) \ge r_2 + 1, \tag{6}$$

$$rk_q((\boldsymbol{m}_0 + \boldsymbol{m}_1 \| \boldsymbol{m}_s) G_{pub} + \boldsymbol{e}_2) \ge r_2 + 1. \tag{7}$$

Proof. Let $\mathrm{rk}_q((\boldsymbol{0}_{k'} \| \boldsymbol{m}_s)\mathrm{Cir}_k(\boldsymbol{u})) = a_1$ and $\mathrm{rk}_q((\boldsymbol{m}_0 + \boldsymbol{m}_1 \| \boldsymbol{m}_s)\mathrm{Cir}_k(\boldsymbol{u}) = b_1$, $\mathrm{rk}_q((\boldsymbol{0}_{k'} \| \boldsymbol{m}_s)G_{pub}) = a_2$ and $\mathrm{rk}_q((\boldsymbol{m}_0 + \boldsymbol{m}_1 \| \boldsymbol{m}_s)G_{pub}) = b_2$. Then, apply Lemma 6 accordingly. □

Therefore, without knowing any information on $\boldsymbol{m}_s$, $\mathcal{A}$ is not able to distinguish between $\boldsymbol{c}_1 + (\boldsymbol{m}_0 \| \boldsymbol{0}_{k-k'})\mathrm{Cir}_k(\boldsymbol{u})$ and $\boldsymbol{c}_1 + (\boldsymbol{m}_1 \| \boldsymbol{0}_{k-k'})\mathrm{Cir}_k(\boldsymbol{u})$, between $\boldsymbol{c}_2 + (\boldsymbol{m}_0 \| \boldsymbol{0}_{k-k'})G_{pub}$ and $\boldsymbol{c}_2 + (\boldsymbol{m}_1 \| \boldsymbol{0}_{k-k'})G_{pub}$, as $\boldsymbol{e}_1$, $\boldsymbol{e}_2$ are chosen such that Labels (2)–(7) are satisfied. For convenience sake, we have the following notation:

Notation. Denote $E_{cir}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m}_s)$ as the set of all elements in $\mathbb{F}_{q^m}^{n}$ that satisfy (2)–(4); and $E_{G_{pub}}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m}_s)$ as the set of all elements in $\mathbb{F}_{q^m}^{n}$ that satisfy (5)–(7).

We now state the assumptions for which our encryption is based on:

The Decisional Rank Syndrome Decoding (DRSD) assumption. Let $\mathcal{D}$ be a distinguishing algorithm that takes as input a vector in $\mathbb{F}^n_{q^m}$ and a matrix $M \in \mathbb{F}^{k\times n}_{q^m}$, and outputs a bit. The DRSD advantage of $\mathcal{D}$ is defined as

$$\begin{aligned}\mathsf{Adv}^{\mathsf{DRSD}}_{M,n,k}(\mathcal{D}) = \Big|\Pr\Big[\boldsymbol{v} \xleftarrow{\$} \mathbb{F}^k_{q^m}, \boldsymbol{e} \xleftarrow{\$} \mathcal{E}_{n,w}, \boldsymbol{x} = \boldsymbol{v}M + \boldsymbol{e} : \mathcal{D}(M,\boldsymbol{x}) = 1\Big]& \\ - \Pr\Big[\boldsymbol{y} \xleftarrow{\$} \mathbb{F}^n_{q^m} : \mathcal{D}(M,\boldsymbol{y}) = 1\Big]\Big|&,\end{aligned}$$

where $\mathcal{E}_{n,w} := \{\boldsymbol{e} \in \mathbb{F}^n_{q^m} : \mathrm{rk}_q(\boldsymbol{e}) = w\}$. The DRSD_M assumption is the assumption that the advantage $\mathsf{Adv}^{\mathsf{DRSD}}_{M,n,k}(\mathcal{D})$ is negligible for any $\mathcal{D}$, i.e., $\mathsf{Adv}^{\mathsf{DRSD}}_{M,n,k}(\mathcal{D}) < \varepsilon_M$.

Now, we prove that our encryption is `IND-CPA` secure under $\mathrm{DRSD}_{\mathrm{Cir}_k(\boldsymbol{u})}$ and $\mathrm{DRSD}_{G_{pub}}$ assumptions.

Theorem 1. *Under the* $\mathrm{DRSD}_{\mathrm{Cir}_k(\boldsymbol{u})}$ *and* $\mathrm{DRSD}_{G_{pub}}$ *assumptions, the proposed public-key encryption scheme* `PE` *is* `IND-CPA` *secure.*

Proof. To prove the security of the scheme, we are using a sequence of games.

Game $\mathcal{G}_0$: This is the real `IND-CPA` attack game against an adversary $\mathcal{A}$ in the definition of semantic security. We run the following attack game algorithm:

```
$S \xleftarrow{\$} \mathbb{F}^{k\times k}_{q^m}, \boldsymbol{u} \xleftarrow{\$} \mathbb{F}^n_{q^m}, T \xleftarrow{\$} \mathbb{F}^{n\times n}_q, \kappa_{pub} \leftarrow (SG + \mathrm{Cir}_k(\boldsymbol{u})T, \boldsymbol{u}), \kappa_{sec} \leftarrow (S, G, T)$
$(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\kappa_{pub})$
$b \xleftarrow{\$} \{0,1\}, \boldsymbol{m_s} \xleftarrow{\$} \mathbb{F}^{k-k'}_{q^m}, \boldsymbol{e}_1 \xleftarrow{\$} E_{cir}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m_s}), \boldsymbol{e}_2 \xleftarrow{\$} E_{G_{pub}}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m_s}),$
$\boldsymbol{c}_1 \leftarrow (\boldsymbol{m}_b\|\boldsymbol{m_s})\mathrm{Cir}_k(\boldsymbol{u}) + \boldsymbol{e}_1, \boldsymbol{c}_2 \leftarrow (\boldsymbol{m}_b\|\boldsymbol{m_s})G_{pub} + \boldsymbol{e}_2$
$\hat{b} \leftarrow \mathcal{A}(\kappa_{pub}, \boldsymbol{c}_1, \boldsymbol{c}_2)$
if $\hat{b} = b$ then return 1 else return 0
```

Denote S_0 the event that $\mathcal{A}$ wins in Game $\mathcal{G}_0$. Then,

$$\mathsf{Adv}^{\mathtt{IND-CPA}}_{\mathtt{PE},\mathcal{A}}(\lambda) = \left|\Pr[S_0] - \frac{1}{2}\right|.$$

Game $\mathcal{G}_1$: We now make one small change to $\mathcal{G}_0$. In this game, we pick a random vector $\boldsymbol{y} \xleftarrow{\$} \mathbb{F}^n_{q^m}$ and replace $\boldsymbol{c}_1$ in $\mathcal{G}_0$ for $\mathcal{E}_{\mathtt{PE}}(\kappa_{pub}, (\boldsymbol{m}_b\|\boldsymbol{m_s}))$ by $\boldsymbol{c}_1 \leftarrow \boldsymbol{y}$:

```
$S \xleftarrow{\$} \mathbb{F}^{k\times k}_{q^m}, \boldsymbol{u} \xleftarrow{\$} \mathbb{F}^n_{q^m}, T \xleftarrow{\$} \mathbb{F}^{n\times n}_q, \kappa_{pub} \leftarrow (SG + \mathrm{Cir}_k(\boldsymbol{u})T, \boldsymbol{u}), \kappa_{sec} \leftarrow (S, G, T)$
$(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\kappa_{pub})$
$b \xleftarrow{\$} \{0,1\}, \boldsymbol{m_s} \xleftarrow{\$} \mathbb{F}^{k-k'}_{q^m}, \boldsymbol{e}_1 \xleftarrow{\$} E_{cir}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m_s}), \boldsymbol{e}_2 \xleftarrow{\$} E_{G_{pub}}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m_s}),$
$\boxed{\boldsymbol{y} \xleftarrow{\$} \mathbb{F}^n_{q^m}, \boldsymbol{c}_1 \leftarrow \boldsymbol{y},}$ $\boldsymbol{c}_2 \leftarrow (\boldsymbol{m}_b\|\boldsymbol{m_s})G_{pub} + \boldsymbol{e}_2$
$\hat{b} \leftarrow \mathcal{A}(\kappa_{pub}, \boldsymbol{c}_1, \boldsymbol{c}_2)$
if $\hat{b} = b$ then return 1 else return 0
```

We denote S_1 the event that $\mathcal{A}$ wins in Game $\mathcal{G}_1$. Under the $\mathrm{DRSD}_{\mathrm{Cir}_k(\boldsymbol{u})}$ assumption, the two games $\mathcal{G}_1$ and $\mathcal{G}_0$ are indistinguishable with $|\Pr[S_1] - \Pr[S_0]| \leq \varepsilon_{\mathrm{Cir}_k(\boldsymbol{u})}$.

Game $\mathcal{G}_2$: We now make one small change to $\mathcal{G}_1$. In this game, we pick a random vector $\boldsymbol{z} \xleftarrow{\$} \mathbb{F}^n_{q^m}$ and replace $\boldsymbol{c}_2$ in $\mathcal{G}_1$ for $\mathcal{E}_{\mathtt{PE}}(\kappa_{pub}, (\boldsymbol{m}_b\|\boldsymbol{m_s}))$ by $\boldsymbol{c}_2 \leftarrow \boldsymbol{z}$:

```
$S \xleftarrow{\$} \mathbb{F}_{q^m}^{k\times k}, \boldsymbol{u} \xleftarrow{\$} \mathbb{F}_{q^m}^{n}, T \xleftarrow{\$} \mathbb{F}_{q}^{n\times n}, \kappa_{pub} \leftarrow (SG + \mathrm{Cir}_k(\boldsymbol{u})T, \boldsymbol{u}), \kappa_{sec} \leftarrow (S, G, T)$
$(m_0, m_1) \xleftarrow{\$} \mathcal{A}(\kappa_{pub})$
$b \xleftarrow{\$} \{0,1\}, \boldsymbol{m_s} \xleftarrow{\$} \mathbb{F}_{q^m}^{k-k'}, \boldsymbol{e}_1 \xleftarrow{\$} E_{cir}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m_s}), \boldsymbol{e}_2 \xleftarrow{\$} E_{G_{pub}}(\boldsymbol{m}_0, \boldsymbol{m}_1, \boldsymbol{m_s}),$
$\boldsymbol{y} \xleftarrow{\$} \mathbb{F}_{q^m}^{n}, \boldsymbol{c}_1 \leftarrow \boldsymbol{y}, \boxed{\boldsymbol{z} \xleftarrow{\$} \mathbb{F}_{q^m}^{n}, \boldsymbol{c}_2 \leftarrow \boldsymbol{z},}$
$\hat{b} \leftarrow \mathcal{A}(\kappa_{pub}, \boldsymbol{c}_1, \boldsymbol{c}_2)$
if $\hat{b} = b$ then return 1 else return 0
```

We denote S_2 the event that $\mathcal{A}$ wins in Game $\mathcal{G}_2$. Under the $\mathrm{DRSD}_{G_{pub}}$ assumption, the two games $\mathcal{G}_2$ and $\mathcal{G}_1$ are indistinguishable with $|\Pr[S_2] - \Pr[S_1]| \leq \varepsilon_{G_{pub}}$.
As the ciphertext challenge $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2)$ is perfectly random, b is hidden to any adversary $\mathcal{A}$ without any advantage; therefore, $\Pr[S_2] = \frac{1}{2}$. We have

$$\begin{aligned}\mathsf{Adv}_{\mathtt{PE},\mathcal{A}}^{\mathtt{IND-CPA}}(\lambda) &= \left|\Pr[S_0] - \frac{1}{2}\right| = |\Pr[S_0] - \Pr[S_2]| \\ &\leq |\Pr[S_0] - \Pr[S_1]| + |\Pr[S_1] - \Pr[S_2]| \\ &\leq \varepsilon_{\mathrm{Cir}_k(\boldsymbol{u})} + \varepsilon_{G_{pub}}.\end{aligned}$$

Therefore, under the $\mathrm{DRSD}_{\mathrm{Cir}_k(\boldsymbol{u})}$ and $\mathrm{DRSD}_{G_{pub}}$ assumption, the proposed public-key encryption scheme `PE` is `IND-CPA` secure. □

6. Our Encryption Based on Gabidulin Codes

We propose Gabidulin code as the decodable code $\mathcal{C}$ in our encryption. We analyze the security of the scheme by considering possible structural attacks to cryptanalyze the system based on Gabidulin code. We also give some parameters for our proposal using Gabidulin codes.

6.1. Gabidulin Codes

First, we give the definition for Moore matrix and Gabidulin codes.

Definition 9. *A matrix $G = (G_{a,b}) \in \mathbb{F}_{q^m}^{k\times n}$ is called a* Moore matrix *induced by $\boldsymbol{g}$ if there exists a vector $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^{n}$ such that ith row of G is equal to $\boldsymbol{g}^{[i-1]}$ for $i = 1, \ldots, k$, i.e., G is in the form of*

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}, \tag{8}$$

where $[i] := q^i$ is the ith Frobenius power. Similarly, we define $G^{([i])} = \left(G_{a,b}^{[i]}\right)$. In addition, for any set $S \subset \mathbb{F}_{q^m}^{n}$, we denote $S^{(l)} = \{\boldsymbol{s}^{([l])} \mid \boldsymbol{s} \in S\}$.

Definition 10. *Let $\boldsymbol{g} \in \mathbb{F}_{q^m}^{n}$ with $rk_q(\boldsymbol{g}) = n$. The $[n,k]$-Gabidulin code $Gab_{n,k}(\boldsymbol{g})$ over $\mathbb{F}_{q^m}$ of dimension k and generator vector $\boldsymbol{g}$ is the code generated by a Moore matrix G induced by $\boldsymbol{g}$.*

The error-correcting capability of $\mathrm{Gab}_{n,k}(\boldsymbol{g})$ is $r = \lfloor \frac{n-k}{2} \rfloor$. There exist efficient decoding algorithms for Gabidulin codes up to the rank error correcting capability (for example, [4]).

6.2. Structural Attack on Gabidulin Code

We examine some common existing attacks against Gabidulin codes and argue that our proposal resists these attacks.

Frobenius Weak Attack. The principle of the Frobenius weak attack (for more details, please refer to [18]) is to form an extension code $\mathcal{C}_{ext}$ from the code $\mathcal{C}_{pub}$ generated by G_{pub} and the error term in the ciphertext. In particular,

$$\mathcal{C}_{ext} := \sum_{i=0}^{r-1} (\mathcal{C} + \langle \boldsymbol{e} \rangle)^{[t'i]},$$

where $\gcd(t', m) = 1$ and $\mathrm{rk}_q(\boldsymbol{e}) = r$. One of the necessary conditions for the complexity of solving the RSD for $\mathcal{C}$ to be polynomial time, via the proposed method is $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}_{ext}) \neq n$. Although in our system our error terms $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ both have ranks of $\frac{r}{2}$, due to the structure of G_{pub}, we have $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}_{ext}) = n$ when $\mathcal{C}$ is chosen to be generated by G_{pub}, which makes the system secure against this attack.

Key Recovery Attack. Consider the structure of G_{pub}:

$$\begin{aligned} G_{pub} &= SG + \mathrm{Cir}_k(\boldsymbol{u})T \\ &= \begin{pmatrix} s_{11} & \cdots & s_{1k} \\ \vdots & \ddots & \vdots \\ s_{k1} & \cdots & s_{kk} \end{pmatrix} \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix} \\ &\quad + \begin{pmatrix} u_0 & u_1 & \cdots & u_{n-1} \\ u_{n-1} & u_0 & \cdots & u_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-k+1} & u_{n-k+2} & \cdots & u_{n-k} \end{pmatrix} \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & \ddots & \vdots \\ t_{n1} & \cdots & t_{nn} \end{pmatrix}. \end{aligned}$$

Note that the above linear system has kn equations, with $k^2 + kn$ unknown variables over $\mathbb{F}_{q^m}$ and n^2 linear variables over $\mathbb{F}_q$. Now, consider $G_{pub}^{[i]}$:

$$\begin{aligned} G_{pub}^{[1]} &= S^{[1]}G^{[1]} + \mathrm{Cir}_k(\boldsymbol{u})^{[1]}T^{[1]} \\ &= \begin{pmatrix} s_{11}^{[1]} & \cdots & s_{1k}^{[1]} \\ \vdots & \ddots & \vdots \\ s_{k1}^{[1]} & \cdots & s_{kk}^{[1]} \end{pmatrix} \begin{pmatrix} g_1^{[1]} & \cdots & g_n^{[1]} \\ g_1^{[2]} & \cdots & g_n^{[2]} \\ \vdots & \ddots & \vdots \\ g_1^{[k]} & \cdots & g_n^{[k]} \end{pmatrix} + \begin{pmatrix} u_0^{[1]} & \cdots & u_{n-1}^{[1]} \\ u_{n-1}^{[1]} & \cdots & u_{n-2}^{[1]} \\ \vdots & \ddots & \vdots \\ u_{n-k+1}^{[1]} & \cdots & u_{n-k}^{[1]} \end{pmatrix} \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & \ddots & \vdots \\ t_{n1} & \cdots & t_{nn} \end{pmatrix}. \end{aligned}$$

This new linear system has kn equations, with $k^2 + n$ new unknown variables over $\mathbb{F}_{q^m}$. Then, the linear systems $G_{pub}, \ldots, G_{pub}^{[m-k]}$ have a total of $(m - k + 1)kn$ equations with a total of $(m - k + 1)k^2 + mn$ unknown variables over $\mathbb{F}_{q^m}$ and n^2 unknown variables over $\mathbb{F}_q$. However, note that solving the equations in $G_{pub}, \ldots, G_{pub}^{[m-k]}$ is equivalent to solving a multivariant quadratic problem.

Reduction Attack. Otmani, Kalachi, and Ndjeya [16] show that a matrix of the form $G_{pub} = SG + X$ where X is a random $k \times n$ matrix over $\mathbb{F}_{q^m}$ with column rank $t < r < n$ could be reduced into the form

$$G_{pub} = SG + X = S(G + S^{-1}X) = S(\bar{X} \mid \bar{G})Q, \tag{9}$$

where $\bar{X}$ is some random $k \times t$ matrix over $\mathbb{F}_{q^m}$, Q is an invertible $n \times n$ matrix over $\mathbb{F}_q$ and $\bar{G}$ is a generator matrix of a $[n - t, k]$-Gabidulin code generated by some $\boldsymbol{g}' \in \mathbb{F}_{q^m}^{n-t}$. By applying

Lemma 2, this reduction is possible due to the structure of X which can be written into the form of $XK = (X' \mid \mathbf{0}_{k\times(n-t)})$, where $\text{colrk}_q(X') = t$ and K is an invertible $n \times n$ matrix over $\mathbb{F}_q$. These $n-t$ columns of zeroes enable the adversary to decompose $G + S^{-1}X$ into random components, $\bar{X}$ and a Moore matrix component, $\bar{G}$. The adversary can then apply Overbeck's attack [10] and cryptanalyze the system.

However, in our encryption system, $G_{pub} = SG + \text{Cir}_k(\boldsymbol{u})T$. By Corollary 1, $\text{Cir}_k(\boldsymbol{u})T$ has column rank n, thus the adversary is not able to rewrite $\text{Cir}_k(\boldsymbol{u})T$ in the form of Label (1) which has columns of zero. Therefore, G_{pub} could not be reduced into components of random matrix and Moore matrix of the form (9). Overbeck's attack cannot be applied in our case.

Moore Decomposition Attack. The Moore Decomposition attack on GPT cryptosystem is the extension of the Overbeck attack [10]. Therefore, it suffices for us to show that a cryptosystem is resistant to the Moore Decomposition attack. We now briefly present the idea of Moore Decomposition attack in the following (for more details, please refer to Sections 3 and 4 [18]):

Consider $G_{pub} = SG + X = S(G + S^{-1}X)$, since $\text{colrk}_q(X) = t < r$, we have $\text{colrk}_q(S^{-1}X) = t$. Consider a minimal column rank Moore decomposition for $S^{-1}X = X_{\text{Moore}} + Z$, where X_{Moore} is a Moore matrix and Z is a non-Moore component which has the lowest possible column rank. Denote $s = \text{colrk}_q(Z)$. Since $d_R^{\min}(\text{Gab}_{n,k}(\boldsymbol{g})) = n - k + 1 \geq s + t + 2$, by Corollary 3.12 in [18], all the elements of rank one in $\sum_{i=0}^{s}\langle G + X\rangle^{([i])}$ belong to the Grassman support of X. The adversary is able to find a full rank matrix $U \in \mathbb{F}_q^{s'\times n}$ for $s \leq s' \leq t$ such that $\text{supp}_{\text{Gr}}(Z) \subseteq \langle U\rangle_{\mathbb{F}_{q^m}} \subseteq \text{supp}_{\text{Gr}}(X)$ and compute $H \in \mathbb{F}_q^{(n-s')\times n}$, a parity check matrix for $\langle U\rangle_{\mathbb{F}_{q^m}}$. By Theorem 4.1 in [18], the adversary can recover $\boldsymbol{m}$ in polynomial time.

In our encryption system, $\text{Cir}_k(u)T$ has column rank n by Corollary 1. Consider a minimal column rank Moore decomposition for $S^{-1}\text{Cir}_k(u)T = M_{\text{Moore}} + W$, where W is a non-Moore component which has the lowest possible column rank s. Note that, in our case, $t = n$, thus we have $d_R^{\min}(\text{Gab}_{n,k}(\boldsymbol{g})) = n - k + 1 < s + n + 2$. As it requires $d_R^{\min}(\text{Gab}_{n,k}(\boldsymbol{g})) > s + t + 2$ to apply Corollary 3.12 in [18], this condition is not satisfied in our case, thus Theorem 4.1 in [18] could not be used to recover the encrypted message.

6.3. Proposed Parameters

We propose some parameters for our encryption scheme. We consider $m > n$ and $r_1 = r_2 = \lfloor \frac{r}{2} \rfloor$. Denote the post-quantum complexity for combinatorial and algebraic attacks as "Comb" and "Alg", respectively. We use the complexities in Section 2.4 as the lower bound of the complexity by replacing $r = r_1 = r_2$ in the calculation. Following Loidreau's application [21] of Grover's algorithm, the exponential term in the decoding complexity should be square rooted [28]. The public key size is $\frac{knm+nm}{8}\log_2(q)$ bytes. Table 3 is the parameters for 2^{128} and 2^{256} bits post-quantum security.

Table 3. Parameters of our cryptosystem for 2^{128} and 2^{256} bits post-quantum security.

	q	m	n	k	r_1	r_2	r	**Public Key Size**	**Post-Quantum Security**
PC-I	2	71	67	22	11	11	22	13.68 KB	133
PC-II	2	85	83	16	16	16	33	14.99 KB	134
PC-III	2	103	101	29	18	18	36	39.01 KB	262
PC-IV	2	113	107	26	20	20	40	40.81 KB	268

Comparison with LOI17 Encryption for similar post-quantum decoding complexity (at 2^{140}) [21]. We include the formula $m^3 2^{\frac{1}{2}(r-1)\left\lfloor \frac{k\min\{m,n\}}{n} \right\rfloor}$ in the lower bounds as it was used in [21] to evaluate the complexities of the attack on RSD. Table 4 is the comparison for our encryption PCir and LOI17 encryption.

Table 4. Comparison of parameters between our cryptosystem and LOI17 Encryption.

Encryption	q	m	n	k	r_1	r_2	r	Public Key Size	Post-Quantum Security
PC-V	2	75	73	21	13	13	26	15.06KB	141
PC-VI	2	85	83	18	16	16	32	16.76KB	144
LOI17-I	2	128	90	24	-	-	11	21.50 KB	140
LOI17-II	2	128	120	80	-	-	4	51.00 KB	141

Our encryption has the following strengths:

i. Our encryption has larger rank of error r_1 and r_2.
ii. At similar security, our key size (15.06 KB) is smaller than the key size of LOI17 Encryption (21.50 KB). Our encryption scheme can provide better post quantum security with smaller key size.

7. Conclusions

This paper has proposed a new rank metric encryption based on the difficulty of the Rank Syndrome Decoding problem. We modify the original GPT cryptosystem with different considerations for the public matrix. The public matrix is distorted by adding $\text{Cir}_k(\boldsymbol{u})T$ of column rank n. Our encryption scheme has `IND-CPA` security under the $\text{DRSD}_{\text{Cir}_k(\boldsymbol{u})}$ and $\text{DRSD}_{G_{pub}}$ assumptions. Our proposal allows the choice for rank of errors to be $r_1 = r_2 = \lfloor \frac{r}{2} \rfloor$. Moreover, for similar post-quantum security level of 2^{140} bits, our encryption using Gabidulin codes has smaller public key size (15.1 KB) than the key size suggested by LOI17 Encryption (21.5 KB). Our encryption provides better security with smaller key size.

Author Contributions: Conceptualization, T.S.C.L. and C.H.T.; Formal Analysis, T.S.C.L. and C.H.T.; Writing—Original Draft Preparation, T.S.C.L.; Writing—Review and Editing, C.H.T.; Project Administration, C.H.T.; Funding Acquisition, C.H.T.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. McEliece, R.J. A public-key cryptosystem based on algebraic coding theory. *Coding Thv.* **1978**, *4244*, 114–116.
2. Sidelnikov, V.M.; Shestakov, S.O. On insecurity of cryptosystems based on generalied Reed-Solomon codes. *Discret. Math. Appl.* **1992**, *2*, 439–444. [CrossRef]
3. Baldi, M.; Chiaraluce, F. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In Proceedings of the IEEE International Symposium on Information Theory, Nice, France, 24–29 June 2007; pp. 2591–2595.
4. Gabidulin, E.M. Theory of codes with maximum rank distance. *Probl. Pereda. Inf.* **1985**, *21*, 3–16.
5. Gabidulin, E.M.; Paramonov, A.V.; Tretjakov, O.V. Ideals over a non-commutative ring and their application in cryptology. In Proceedings of the Worshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, 8–11 April 1991; pp. 482–489.
6. Gibson, J.K. Severely denting the Gabidulin version of the McEliece public-key cryptosystem. *Des. Codes Cryptogr.* **1995**, *6*, 37–45. [CrossRef]
7. Gabidulin, E.M.; Ourivski, A.V. Modified GPT PKC with right scrambler. *Electron. Notes Discret. Math.* **2001**, *6*, 168–177. [CrossRef]
8. Ourivski, A.V.; Gabidulin, E.M. Column Scrambler for the GPT cryptosystem. *Discret. Appl. Math.* **2003**, *128*, 207–221. [CrossRef]
9. Overbeck, R. Extending Gibson's attacks on the GPT cryptosystem. In Proceedings of the International Workshop on Coding and Cryptography, Bergen, Norway, 14–18 March 2005; pp. 178–188.
10. Overbeck, R. Structural attacks for public key cryptosystems based on Gabidulin codes. *J. Cryptol.* **2008**, *21*, 280–301. [CrossRef]
11. Gabidulin, E.M. Attacks and counter-attacks on the GPT public key cryptosystem. *Des. Codes Cryptogr.* **2008**, *48*, 171–177. [CrossRef]

12. Gabidulin, E.M.; Rashwan, H.; Honary, B. On improving security of GPT cryptosystems. In Proceedings of the IEEE International Symposium on Information Theory, Seoul, South Korea, 28 June–3 July 2009; pp. 1110–1114.
13. Loidreau, P. Designing a rank metric based McEliece cryptosystem. In Proceedings of the 3rd International Workshop on Post-Quantum Cryptography, Darmstadt, Germany, 25–28 May 2010; pp. 142–152.
14. Rashwan, H.; Gabidulin, E.M.; Honary, B. A smart approach for GPT cryptosystem based on rank codes. In Proceedings of the IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 2463–2467.
15. Horlemann-Trautmann, A.; Marshall, K.; Rosenthal, J. Extension of Overbeck's Attack for Gabidulin Based Cryptosystems. *Des. Codes Cryptogr.* **2018**, *86*, 319–340. [CrossRef]
16. Otmani, A.; Kalachi, H.T.; Ndjeya, S. Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes. *Des. Codes Cryptogr.* **2018**, *86*, 1983–1996. [CrossRef]
17. Gaborit, P.; Ruatta, O.; Schrek, J. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Inf. Theor.* **2016**, *62*, 1006–1019. [CrossRef]
18. Horlemann-Trautmann, A.; Marshall, K.; Rosenthal, J. Considerations for Rank-based Cryptosystems. In Proceedings of the IEEE International Symposium on Information Theory, Barcelona, Spain, 10–15 July 2016; pp. 2544–2548.
19. Ourivski, A.V.; Johansson, T. New technique for decoding codes in the rank metric and its cryptography applications. *Probl. Inf. Transm.* **2002**, *38*, 237–246. [CrossRef]
20. Gaborit, P.; Hauteville, A.; Phan, D.H.; Tillich, J.P. Identity-based Encryption from Codes with Rank Metric. In Proceedings of the 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; pp. 194–224.
21. Loidreau, P. A New Rank Metric Codes Based Encryption Scheme. In Proceedings of the 8th International Workshop on Post-Quantum Cryptography, Utrecht, The Netherlands, 26–28 June 2017; pp. 3–17.
22. Gaborit, P.; Zémor, G. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Trans. Inf. Theor.* 2016, *62*, 7245–7252. [CrossRef]
23. Aragon, A.; Gaborit, P.; Hauteville, A.; Tillich, J.P. A New Algorithm for Solving the Rank Syndrome Decoding Problem. In Proceedings of the 2018 IEEE International Symposium on Information Theory, Vail, CO, USA, 17–22 June 2018; pp. 2421–2425.
24. Goubin, L.; Courtois, N.T. Cryptanalysis of the TTM cryptosystem. In Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, 3–7 December 2000; pp. 44–57.
25. Landsberg, G. Über eine Azahibestimmung und eine damit zusammengängende Reihe. *J. Reine Angew. Math.* **1893**, *111*, 87–88.
26. Laksov, D.; Thorup, A. Counting Matrices with Coordinates in Finite Fields and of Fixed Rank. *Math. Scand.* **1994**, *74*, 19–33. [CrossRef]
27. Shoup, V. Sequences of Games: A Tool for Taming Complexity in Security Proofs. Available online: http://www.shoup.net/papers/games.pdf (accessed on 7 October 2018).
28. Bernstein, D.J. Grover vs. McEliece. In Proceedings of the 3rd International Workshop on Post-Quantum Cryptography, Darmstadt, Germany, 25–28 May 2010; pp. 73–80.