RAIRO-Theor. Inf. Appl. 55 (2021) 10
https://doi.org/10.1051/ita/2021010

RAIRO - Theoretical Informatics and Applications
www.rairo-ita.org

A NOVEL NIEDERREITER-LIKE CRYPTOSYSTEM BASED ON THE $(u|u+v)$-CONSTRUCTION CODES

Roumaissa Mahdjoubi[1], Pierre Louis Cayrel[2], Sedat Akleylek[3]
and Guenda Kenza[1,*]

Abstract. In this paper, we present a new variant of the Niederreiter Public Key Encryption (PKE) scheme which is resistant against recent attacks. The security is based on the hardness of the Rank Syndrome Decoding (RSD) problem and it presents a $(u|u+v)$-construction code using two different types of codes: Ideal Low Rank Parity Check (ILRPC) codes and λ-Gabidulin codes. The proposed encryption scheme benefits are a larger minimum distance, a new efficient decoding algorithm and a smaller ciphertext and public key size compared to the Loidreau's variants and to its IND-CCA secure version.

Mathematics Subject Classification. 11T71, 14G50.

Received December 21, 2020. Accepted July 29, 2021.

1. Introduction

In 1978, McEliece introduced the first public key encryption (PKE) scheme based on coding theory using as a private key a generator matrix of a binary Goppa code [26]. Later, Niederreiter proposed another PKE scheme using linear codes wherein the private key is the parity-check matrix of the code instead of its generator matrix [27]. Both of these schemes are based on equivalent $\mathcal{NP}$-complete problems [7] and they have an equivalent security levels for the same set of parameters.

The first PKE scheme based on rank metric codes was proposed in 1995 by Gabidulin, Paramonov and Tretjakov (GPT-PKE). Its security is based on the Rank Syndrome Decoding (RSD) problem which is proved to be NP-hard by a probabilistic reduction from the Syndrome Decoding problem [13].

In [14, 15, 30, 31], two structural attacks were given by Gibson and Overbeck on the GPT-PKE scheme. Further, Ayoub *et al.* [28] using these attacks have proven the vulnerability of any variant of the GPT-PKE scheme. Loidreau [23] proposed a set of parameters of reduced public key size with the aim to avoid those attacks. Gaborit *et al.* proposed in [9] a PKE scheme based on Low Rank Parity Check (LRPC) codes. They proved that their scheme is resistant to message attack and structural attacks on the key. It is worthy to note that the Niederreiter-PKE scheme based on reducible rank codes proposed by Khan *et al.* [19] can resist

Keywords and phrases: Niederreiter-PKE, ILRPC codes, λ-Gabidulin codes, rank-metric codes, IND-CCA security.

[1] Faculty of Mathematics, USTHB, Laboratory of Algebraand Number Theory, BP 32 El Alia, Bab Ezzouar, Algeria.
[2] Univ Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516, F-42023, Saint-Etienne, France.
[3] Department of Computer Engineering, Faculty of Engineering, Ondokuz Mayis University, Samsun, Turkey.

[*] Corresponding author: ken.guenda@gmail.com

to Overbeck's attack for chosen length $n \leq 30$. However, Horlemann-Trautmann *et al.* proposed in [18] an extension of Overbeck's attack which breaks most of the proposed variants. Recently, Bardet *et al.* [5] proposed an algebraic attack which breaks all LRPC approaches and eliminated NIST's candidates from its third round like ROLLO [3] and RQC [1].

One of the properties that are required for encryption schemes is the indistinguishability under (non-adaptive) chosen ciphertext attack (IND-CCA). It is more advantageous than the indistinguishability under chosen-plaintext attack (IND-CPA) which is equivalent to the property of semantic security. Al Shehhi *et al.* was proposed in [2] an IND-CCA secure version of Loidreau's PKE scheme with an overhead of 23% in the computational cost for encryption algorithm.

1.1. Motivation and contribution

In this paper, we propose a new variant of the Niederreiter-PKE scheme based on the RSD problem. We present a new family of $(u|u+v)$ codes constructed by two different types: ILRPC codes and λ-Gabidulin codes. We also provide its decoding algorithm. The proposed scheme is based on the same typical idea of Gabidulin *et al.* in [10] and we can express its benefits in:

- Reduced key sizes using properties of ILRPC codes compared to key sizes given in [22].
- Increasing the security to attacks by concatenating the generator matrix with a random chosen distortion matrix of full rank t_1 and using the shared decoding algorithm of both of ILRPC and λ-Gabidulin codes.
- Given larger minimum rank distance d expressed by d_1 and d_2 which are minimum rank distances of the ILRPC code and λ-Gabidulin code, respectively.

The proposed scheme is secure against the extended version of Overbeck's attack by using a scrambler matrix in the extension field, and against the recent attack [5] by choosing a proper set of parameters. We obtain a new decoding algorithm with complexity $\mathcal{O}(n^3)$. We also prove that the scheme is IND-CCA secure against any probabilistic polynomial time adversary. We then provide an optimal set of parameters for which we obtain smaller public key and ciphertext sizes when we compared it to Loidreau's variants.

1.2. Organization

This paper is organized as follows: In Section 2, we give preliminaries on the rank-metric codes, ILRPC codes, the λ-Gabidulin codes, the RSD problem and the Niederreiter-PKC. In Section 3, we define the new $(u|u+v)$ construction code in rank-metric and give its decoding algorithm, then we provide a cryptographic application of the codes in the Niederreiter-like PKE scheme based on the RSD problem. The security analysis is studied in Section 4 with some examples and comparison. Finally, we conclude the paper in Section 5.

2. Preliminaries

In this section, we provide some basic definitions in the rank metric.

2.1. Rank metric codes

Let $n, m \in \mathbb{N}$, $\mathbb{F}_q$ be a finite field of q elements and let $\mathbb{F}_{q^m}$ be an extension field of degree m. If $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $(a_1, \ldots, a_m)$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ then its associated $m \times n$ matrix is

$$X = \begin{bmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \ldots & x_{mn} \end{bmatrix},$$

where each column vector x_j of x can be represented as a sum $x_j = \sum_{i=1}^{m} x_{i,j}a_i$ for $j \in \{1,\dots,n\}$

The rank of the matrix X is the maximal number of vectors column x_j that are linearly independent over $\mathbb{F}_q$ and it defines the rank of x over $\mathbb{F}_q$. We denote it by $\texttt{rank}(x|\mathbb{F}_q) = \texttt{rank}(X|\mathbb{F}_q)$. The rank distance between two vectors x and y in $\mathbb{F}_{q^m}^n$ is defined by $\texttt{dist}(x,y) = \texttt{rank}(x-y|\mathbb{F}_q) = \texttt{rank}(X-Y|\mathbb{F}_q)$, where Y is the associated matrix of y.

For any code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_{q^m}$, the minimum rank distance is defined by

$$\begin{aligned} d &= \min\{\texttt{dist}(c_1,c_2)\ \forall\, c_1,c_2 \in \mathcal{C}, c_1 \neq c_2\} \\ &= \min\{\texttt{rank}(c|\mathbb{F}_q) \mid\ c \in \mathcal{C}, c \neq 0\}. \end{aligned}$$

This distance verifies the Singleton bound $d \leq n-k+1$ for $m \geq n$. When this inequality is achieved, the code will be a Maximal Rank Distance code (MRD). The rank error correcting capacity is then $t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{n-k}{2} \rfloor$.

A Gabidulin code $\mathcal{C}_{(g)}$ defines a class of MRD codes for $n \leq m$. Its $k \times n$ generator matrix G is defined for any set of elements $g_1,\dots,g_n$ from $\mathbb{F}_{q^m}$ those are linearly independent over $\mathbb{F}_q$ as follows:

$$G = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix}, \tag{2.1}$$

where $g^{[i]} = g^{q^i}$ means the i-th Frobenius power of g.

The $(n-k) \times n$ parity check matrix H of a Gabidulin code verifies $GH^\top = 0$ and it can be written as follows:

$$H = \begin{bmatrix} h_1 & h_2 & \dots & h_n \\ h_1^{[1]} & h_2^{[1]} & \dots & h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \dots & h_n^{[d-2]} \end{bmatrix}$$

where $h_i \in \mathbb{F}_{q^m}$ for $i = \{1,\dots,n\}$ are linearly independent over $\mathbb{F}_q$.

The main property on Gabidulin codes is the evaluation in a linearized polynomial $F(z) \in \mathbb{F}_q^m$ of degree lower than k on the generator vector g

$$\mathcal{C}_{(g)} = \{(F(g_1),\dots,F(g_n)), F(z) = \sum_{i=0}^{k-1} f_i z^{[i]}\}$$

where $f_i \in \mathbb{F}_{q^m}$ for $0 \leq i \leq k-1$ and $f_{k-1} \neq 0$.

We define the support of a vector in $\mathbb{F}_{q^m}^n$ as follows:

Definition 2.1. The **support** E of $g = (g_1,\dots,g_n) \in \mathbb{F}_{q^m}^n$ of dimension d is the $\mathbb{F}_q$ subvector space of $\mathbb{F}_{q^m}$ generated by the coordinates of g with $\texttt{rank}(g|\mathbb{F}_q) = d$ and $g_1,\dots,g_n$ are linearly independent.

Definition 2.2. (Gilbert-Varshamov Bound) Let $B^R = \left\{M \in \mathbb{F}_{q^m}^n / rank(M) \leq t\right\}$ be the ball of radius t centred around 0 for the rank metric. The Gilbert-Varshamov bound for rank metric codes is given by the smallest t for which $|B_t^R| \geq q^{m(n-k)}$. When $|B_t^R| \approx q^{m(n-k)}$ the Gilbert-Varshamov bound d_{GV} is given by

$$\begin{aligned} d_{GV} &= n(1-\sqrt{\tfrac{k}{n}}), && \text{if } m=n \\ &\approx \frac{1}{2}(m+n-\sqrt{(m+n)^2-4m(n-k)}), && \text{if else.} \end{aligned}$$

To ensure the uniqueness of the error decoding in rank metric codes, it is necessary that the minimum rank weight of the code d be smaller or equal to the Gilbert Varshamov bound. While for the error and erasure decoding algorithm, the case when d is beyond the Gilbert Varshamov bound can be considered.

2.2. Ideal low rank parity check codes

In this section, we recall the definition of the ideal LRPC (ILRPC) code [3].

Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$ linear rank metric code and given by the following definition.

Definition 2.3. Let F be a $\mathbb{F}_q$ subspace of dimension d of $\mathbb{F}_{q^m}$, (h_1, h_2) two vectors of $\mathbb{F}_{q^m}^n$ of support F and $P \in \mathbb{F}_q[X]$ a polynomial of degree n. Let H_1 and H_2 be two matrices given as follows:

$$H_1 = \begin{bmatrix} h_1 \\ Xh_1 \mod P \\ \dots \\ X^{n-1}h_1 \mod P \end{bmatrix}^\top \text{ and } H_2 = \begin{bmatrix} h_2 \\ Xh_2 \mod P \\ \dots \\ X^{n-1}h_2 \mod P \end{bmatrix}^\top.$$

The code C with parity check matrix $H = (H_1, H_2)$ is an ideal LRPC code of type $[2n, n]_{q^m}$.

This codes can counter the folding attack [16] for which we discuss more on it in Section 4. We recall its decoding algorithm in Algorithm 1 given in [11].

Algorithm 1 Rank Support Recover (RSR) algorithm [3]

```
Input : $F =< f_1, \dots, f_d >$, $s = (s_1, \dots, s_n)$ and $r$ (the dimension of $E$).
Output : A candidate for the vector space $E$.

Compute $S =< s_1, \dots, s_n >$
Precompute every $S_i$ for $i = 1$ to $d$
Precompute every $S_{i,i+1}$ for $i = 1$ to $d-1$
for $i$ from 1 to $d-2$ do
    $tmp \leftarrow S =< F \cdot (S_{i,i+1} + S_{i+1,i+2} + S_{i,i+2}) >$
    if $\dim(tmp) \leq rd$ then
        $S \leftarrow tmp$
    end if
end for
$E \leftarrow f_1^{-1} \cdot S \cap \dots \cap f_d^{-1} \cdot S$
return $E$.
```

2.3. λ-Gabidulin codes

The λ-Gabidulin is similar to the generalized Reed Solomon codes in Hamming metric [20]. It has similar construction of the generalized Reed Solomon codes in polynomial settings. We recall its definition as follows:

Definition 2.4. (λ-Gabidulin codes [20]) Let $g = (g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$ be linearly independent over $\mathbb{F}_q$ and $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_{q^m}^n$. The λ-Gabidulin code over $\mathbb{F}_{q^m}$ of dimension k associated with vector g and λ is the code generated by a matrix G_λ of the form

$$G_\lambda = \begin{bmatrix} \lambda_1 g_1 & \lambda_2 g_2 & \dots & \lambda_n g_n \\ \lambda_1 g_1^{[1]} & \lambda_2 g_2^{[1]} & \dots & \lambda_n g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 g_1^{[k-1]} & \lambda_2 g_2^{[k-1]} & \dots & \lambda_n g_n^{[k-1]} \end{bmatrix} \tag{2.2}$$

and its parity check matrix is given by

$$H_\lambda = \begin{bmatrix} \lambda_1^{-1} h_1 & \lambda_2^{-1} h_2 & \dots & \lambda_n^{-1} h_n \\ \lambda_1^{-1} h_1^{[1]} & \lambda_2^{-1} h_2^{[1]} & \dots & \lambda_n^{-1} h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{-1} h_1^{[n-k-1]} & \lambda_2^{-1} h_2^{[n-k-1]} & \dots & \lambda_n^{-1} h_n^{[n-k-1]} \end{bmatrix} \tag{2.3}$$

Any codeword c can be written as follows:

$$c = (f_0, \dots, f_{k-1}) G_\lambda = (\lambda_1 \sum_{i=0}^{k-1} f_i g_1^{[i]}, \dots, \lambda_n \sum_{i=0}^{k-1} f_i g_n^{[i]}) = (\lambda_1 F(g_1), \dots, \lambda_n F(g_n)).$$

Such codes have been selected for application in cryptography; the McEliece like cryptosystem and proved out that it can be resistant for the rank syndrome decoding problem (RSD) to known attacks for well chosen parameters.

These codes are not MRD and have minimum distance $d \leq n-k+1$. Further, they do not have weak structure as in the case of Gabidulin codes which have huge vector space invariant under the Frobenius automorphism. We recall its decoding algorithm in Algorithm 2.

Algorithm 2 Decoding algorithm for λ-Gabidulin code [20]

```
A received word $y = c + e$ with $c = fG_\lambda$ , $\mathtt{rank}(e) \leq \frac{r}{u}$ for $u = \mathtt{rank}(\lambda)$, $r = \lfloor \frac{n-k}{2} \rfloor$.
Recompute $y = fG_\lambda + e = (\lambda_1 F(g_1), \dots, \lambda_n F(g_n)) + (e_1, \dots, e_n)$
Multiplying $y$ by $\lambda_i^{-1}$ for $i = 0, \dots, n$ we get:
    $\hat{y} = (F(g_1), \dots, F(g_n)) + \hat{e}$
Apply the decoding algorithm for Gabidulin codes on $\hat{y}$ for $\mathtt{rank}(\hat{e}) \leq r$
Recover $c$
```

2.4. Rank-based cryptography

In this section, we recall the Rank Syndrome Decoding (RSD) problem.

Problem: *For a given $(n-k) \times n$ matrix H ($k \leq n$), a vector $s \in \mathbb{F}_{q^m}^{n-k}$ and an integer w. Find a codeword x which satisfies two conditions*

$$\begin{cases} \mathtt{rank}(x|\mathbb{F}_q) = w, \\ Hx^\top = s^\top. \end{cases}$$

Gaborit *et al.* [13] have provided a probabilistic reduction to the NP-complete Syndrome Decoding problem in the Hamming metric by proving Theorem 2.5.

Theorem 2.5 ([13])**.** *If the Rank Syndrome Decoding Problem is in ZPP, then we must have NP = ZPP.*

Key Generation(1^δ)	$(n,m,k,r) \leftarrow$ Select.Param(1^δ). $H \leftarrow$ Parity Check matrix of $[n,k]$RRCode $S \leftarrow \mathbb{F}_{q^m}^{(n-k)\times(n-k)}$ $P \leftarrow \mathbb{F}_{q^m}^{(n+t_1)\times(n+t_1)}$. $X \leftarrow \mathbb{F}_{q^m}^{k\times t_1}$ as given in equation (2.4) Set $H_X = [0 \mid H]$ orthogonal matrix of $G_X = [X \mid G]$ $D \leftarrow$ Decoding algorithm of Gabidulin codes [10]. *pk*: $H_{pub} = SH_XP \in \mathbb{F}_{q^m}^{(n-k)\times(n+t_1)}$. *sk*: (S,P,G,X) and D.
Encryption$(x$,$pk)$	$x \in \mathbb{F}_{q^m}^{n+t_1}$, $\mathtt{rank}(x) = t_2 = t - t_1$. $c = (c_1, c_2, \dots, c_{n-k}) = xH_{pub}^\top$
Decryption$(c$,$sk)$	Compute $c' = c(S^\top)^{-1}$ and $x_P = xP^\top$. $c' = x'(H_X^\top)$ $x' = (g_1, \dots, g_r) + x_P$, start with g_r using D to get the last information sub-block x_r. and g_{r-1} to get x_{r-1}, until g_1 and get x_1. Compute $x = x_P(P^\top)^{-1}$.

FIGURE 1. The Niederreiter PKE type of GPT-PKE scheme [19].

This problem can strengthen any scheme in the rank metric, that is because all the proposed algorithms to solve it are exponential.

2.5. Niederreiter PKE type of GPT-PKE

Niederreiter-PKE is the dual version of McEliece-PKE. They are based on equivalent problems for a given code in Hamming metric [6]. In the rank-metric, the Niederreiter-PKE type of GPT-PKE was proposed by Khan *et al.* [19] based on the RSD problem for rank reducible codes (RRC) defined by Gabidulin *et al.* in [10]. It used the parity check matrix of Gabidulin code and concealed its structure by the row/column scrambler and even distortion matrices; the distortion matrix will not appear after the decryption step. The fast decoding algorithm described in [32] is considered up to the rank error correcting capacity t. In Figure 1, we recall the description of Niederreiter-PKE type of GPT-PKE with a given (RRC) $[n = rN, k = rM]$ which is defined by r chosen $[N, N-d+1, d]$ -MRD codes of rank distance d for $M = N-d+1$. Its generator matrix G is a concatenation of the r canonical generator matrices. Also for the distortion matrix

$$X = \left[\begin{array}{cccc} X_1, & X_2, & \dots, & X_r \end{array}\right] = \begin{bmatrix} X_{11} & X_{12} & \dots & X_{1r} \\ 0 & X_{22} & \dots & X_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & X_{rr} \end{bmatrix}, \tag{2.4}$$

where $X_1, X_2, \dots, X_r$ are r distortion sub-matrices of column rank t_1 over $\mathbb{F}_q$ $(t_1 \leq t)$ which is the design parameter.

3. THE PROPOSED SCHEME

In this section, we define the new PKE scheme using $(u|u+v)$-construction code and we give its decoding algorithm.

3.1. The $(u|u+v)$-construction codes

In this section, we start by giving the general definition of the $(u|u+v)$-construction code in the rank metric.

Definition 3.1 (The $(u|u+v)$-construction)**.** Given two rank codes; an $[n_1, k_1, d_1]$ code $\mathcal{C}_1$, an $[n_2, k_2, d_2]$ code $\mathcal{C}_2$ with $n_1 = n_2 = \frac{n}{2}$ and a binary matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

We denote by $\mathcal{C}_3 = [\mathcal{C}_1|\mathcal{C}_2]\, A$ the rank code which consists of all vectors $(u|u+v)$, with $u \in \mathcal{C}_1$ and $v \in \mathcal{C}_2$.

The length of $\mathcal{C}_3$ is n, its dimension is $k = k_1 + k_2$ and its $n \times k$ generator matrix G over $\mathbb{F}_{q^m}$ is defined by

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}, \tag{3.1}$$

where G_1 and G_2 are generator matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

Therefore, the $(n-k) \times n$ parity check matrix of the code over $\mathbb{F}_{q^m}$ is defined by:

$$H = \begin{bmatrix} H_1 & 0 \\ -H_2 & H_2 \end{bmatrix}.$$

In Hamming metric the minimum distance of $(u|u+v)$-construction code is defined by $d = \min\{2d_1, d_2\}$, while it is not known in the rank-metric.

Proposition 3.2. *Let $\mathcal{C}_3$ be the $[n,k,d]$ code given in Definition 3.1. Let $\mathcal{C}_1$ be the ILRPC code and $\mathcal{C}_2$ be the λ-Gabidulin code. The minimum distance is upper bounded by*

$$d = d_1 + d_2 - \alpha,$$

where $\alpha = \dim(R_1 \cap R_2)$ for R_1 (resp. R_2) is the set of rows of any element c_1 in $\mathcal{C}_1$ (resp.c_2 in $\mathcal{C}_2$) which has the minimum rank distance d_1 (resp. d_2).

Proof. We start by the general definition of the code $\mathcal{C}_3$ given in Definition 3.1

$$C = \{xG \mid x \in \mathbb{F}_{q^m}^k\},$$

with G is the generator matrix of $\mathcal{C}_3$ of the form 3.1. Then, for any element c in $\mathcal{C}_3$, it can be written as follows

$$c = (x_1, x_2)G = \begin{bmatrix} x_1G_1 & x_1G_1 \\ 0 & x_2G_2 \end{bmatrix},$$

with $x_1 \in \mathbb{F}_{q^m}^{k_1}$ and $\mathbb{F}_{q^m}^{k_2}$. Similarly by the general definition of the code $\mathcal{C}_1$ (respectively $\mathcal{C}_2$) we denote by $c_1 = x_1G_1$ (respectively $c_1 = x_1G_2$). Hence, we can write the codeword c as follows

$$c = \begin{bmatrix} c_1 & c_1 \\ 0 & c_2 \end{bmatrix}.$$

Therefore, getting the minimum rank of $\mathcal{C}_3$ is related to get the minimum rank of every non nul $c \in \mathcal{C}_3$. *i.e.*

$$d = \min\{\mathtt{rank}(c|\mathbb{F}_q) \mid c \in \mathcal{C}_3, c \neq 0\}$$

We may simplify the rank weight of the expression of c and suppose $A = [c_1\ c_1]$ the matrix of size $k_1 \times n$ and $B = [0\ c_2]$ the matrix of size $k_2 \times n$. Without loss of generality, we assume $k^* = \max\{k_1, k_2\}$ and we propose that the matrix of the minimum dimension will be appended with rows of zeros until it achieves k^* rows in total. For that we get A and B of same size $k^* \times n$ and we can write the following property as well as given in [25]

$$\texttt{rank}\begin{pmatrix} A \\ B \end{pmatrix} = \texttt{rank}(A) + \texttt{rank}(B) - \dim(R_A \cap R_B),$$

where C_A and C_B are the row spaces of the matrices A and B respectively.
Clearly we have $\texttt{rank}(A) = \texttt{rank}(c_1)$ and $\texttt{rank}(B) = \texttt{rank}(c_2)$. Then we have

$$\begin{aligned}\texttt{rank}(c) = &\begin{pmatrix} A \\ B \end{pmatrix} \\ &= \texttt{rank}(c_1) + \texttt{rank}(c_2) - \dim(R_1 \cap R_2) \\ &= \texttt{rank}(c_1) + \texttt{rank}(c_2) - \alpha,\end{aligned}$$

with $\alpha = \dim(R_1 \cap R_2)$. Therefore, the minimum distance may be written as follows

$$\begin{aligned} d &= \min\{\texttt{rank}(c|\mathbb{F}_q) \mid c \in \mathcal{C}_3, c \neq 0\} \\ &= \min\{\texttt{rank}(c_1) + \texttt{rank}(c_2) - \alpha \mid c_i \in \mathcal{C}_i, c_i \neq 0, i \in \{1,2\}\} \\ &= d_1 + d_2 - \alpha. \end{aligned}$$

where $\alpha = \dim(R_1 \cap R_2)$ for R_1 (resp. R_2) is the set of rows of any element c_1 in $\mathcal{C}_1$ (resp.c_2 in $\mathcal{C}_2$) which has the minimum rank distance d_1 (resp. d_2). Hence, we conclude the result. □

3.2. Decoding algorithm

In this section, we propose to use the $(u|u+v)$- construction with codes in the rank-metric to reach the robustness of Niederreiter-PKE scheme against several attacks, the ILRPC and $\lambda-$Gabidulin codes. The advantage of this construction is to get an encryption scheme with shorter ciphertext size. Furthermore, it has a better error correcting capacity [24].

The two codes used in our scheme have decoding algorithms up to the error correcting capacity t of the code, which implies that the algorithm output is a list of one or two codewords containing the sent word [17].

We denote by D_1 a decoding Algorithm 1 for the LRPC code $\mathcal{C}_1$ which decodes up to $t^{(1)}$ errors and by D_2 the error-erasure decoding Algorithm 2 of λ-Gabidulin code $\mathcal{C}_2$ which decodes up to $t^{(2)}$ errors. Therefore, the error correcting capacity of $\mathcal{C}$ is: $t = \lfloor \frac{d-1}{2} \rfloor$

Let $y = xG + e$ be a received word, with :

- The word $x \in \mathcal{C}$ is equal to $(x_1, x_1 + x_2)$, with $x_1 \in \mathcal{C}_1$ and $x_2 \in \mathcal{C}_2$.
- The matrix G is the generator matrix of the form equation (3.1).
- The error vector $e = (e_1, e_2) \in \mathbb{F}_{q^m}^n$ verifies $\texttt{rank}(e|\mathbb{F}_q) \leq t$.

Namely, the received word y is:

$$y = xG + e = (y_1, y_2) = (x_1G_1 + e_1, x_1G_1 + x_2G_2 + e_2).$$

First, we can decode y_1 without loss of generality and recover x_1 since $\texttt{rank}(e_1|\mathbb{F}_q) \leq t^{(1)}$. Then, if we compute $y_2 - y_1 = x_2G_2 + (e_2 - e_1)$ then we may decode $y_2 - y_1$ using the decoding algorithm D_2 to obtain x_2, since $x_2 \in \mathcal{C}_2$ and we have to obtain the bound t_2 for the D_2 $\texttt{rank}(e_2 - e_1|\mathbb{F}_q) \leq t^{(2)}$. However, we will be able to detect it by checking that we corrected t errors in total. Hence, the algorithm outputs the whole codeword of the $(u|u+v)$-construction code.

Key Generation(1^δ)

$(n, m, k) \leftarrow$ Select.Param.(1^δ)
$H \leftarrow$ Parity check matrix of $(u|u+v)$ constructed code.
$S \xrightarrow{\$} \mathbb{F}_{q^m}^{(n-k)\times(n-k)}$
$P \xrightarrow{\$} \mathbb{F}_{q^m}^{(n+t_1)\times(n+t_1)}$
$X \xrightarrow{\$} \mathbb{F}_{q^m}^{k\times t_1}$ as in equation (3.2).
D is the given decoding Algorithm 3.
$H_X = [H|0]$ the dual code of $G_X = [G|X]$
pk: $H_{pub} = SH_XP \in \mathbb{F}_{q^m}^{(n-k)\times(n+t_1)}$.
sk: (S, G, P, X).

Encryption(x,pk)

$x \xrightarrow{\$} \mathbb{F}_{q^m}^{n}$ and $\gamma \xrightarrow{\$} \mathbb{F}_{q^m}^{t_1}$, with $\texttt{rank}(x) \leq t$
$c = (x, \gamma)H_{pub}^{\top}$

Decryption(c,sk)

Compute $c' = c(S^{\top})^{-1}$ and $x' = xP_1$ where $P^{\top} = [P_1 \ P_2]$.
Decode $c' = x'H^{\top}$ by D when $\texttt{rank}(x) \leq t$.
Compute $x = x'(P_1^{\top})^{-1}$.

FIGURE 2. Description of the Niederreiter-like encryption scheme.

Algorithm 3 Decoding algorithm for $(u|u+v)$- construction code.

- **Input**:
  - A received word $y = xG + e = (y_1, y_2)$ with $x = (x_1, x_1 + x_2) \in \mathcal{C}$ ($x_1 \in \mathcal{C}_1$ and $x_2 \in \mathcal{C}_2$) and $e = (e_1, e_2)$ of rank less than t ($\texttt{rank}(e_1|\mathbb{F}_q) \leq t^{(1)}$, $\texttt{rank}(e_2 - e_1|\mathbb{F}_q) \leq t^{(2)}$) and G the generator matrix of $\mathcal{C}$.
  - The decoding algorithm for LRPC codes D_1 by Algorithm 1 and for λ-Gabidulin codes D_2 by Algorithm 2.
- **Output** $x \in \mathbb{F}_{q^m}^n$ of rank weight $\texttt{rank}(x|\mathbb{F}_q) \leq t$.

```
Decode $y_1$ with $\texttt{rank}(e_1|\mathbb{F}_q) \leq t^{(1)}$ by $D_1$ and recover $x_1$.
Decode $y_2 - y_1$ by $D_2$ with $\texttt{rank}(e_2 - e_1|\mathbb{F}_q) \leq t^{(2)}$ and recover $x_2$.
Return $x = (x_1, x_2)$.
```

Remark 3.3. The PUM convolutional code [33] is not suitable for such a construction since it has semi infinite generator and parity check matrix which will not much well in the generator or the parity check matrix of the construction $(u|u+v)$.

3.3. Niederreiter-PKE based on $(u|u+v)$-construction codes

In this section, we provide a description for the proposed scheme and we present it in Figure 2. The scheme is a new variant of the Niederreiter-PKE scheme which we recall it in Section 2.5. We respect here the generator matrix of the $(u|u+v)-$construction code and we use the technique of adding random column scrambler in the parity check matrix of the code [21].

Key generation: For chosen security level (1^δ) we can fix n, k, m and the design parameter t_1. The public key is an $(n-k)\times(n+t_1)$ parity check matrix of the public code

$$H_{pub} = SH_XP,$$

where:

- $H_X = [H|0]$ is a concatenated matrix of H is a $(n-k) \times n$ parity check matrix code of a product-matrix proposed in Section 3.1, equation (3.1) and $(n-k) \times t_1$ zeros matrix. which is formulated as in Section 2.5. The matrix H_X is the dual of $G_X = [G|X]$, where G generates a $[n = n_1 + n_2, k = k_1 + k_2, d]$ $(u|u+v)$-constructed code from $[n_1, k_1]$ILRPC code and $[n_2, k_2]$ $\lambda-$Gabidulin code.
- The matrix S is a $(n-k) \times (n-k)$ non singular row scrambling matrix over $\mathbb{F}_{q^m}$.
- The matrix P is a $(n+t_1) \times (n+t_1)$ column scramble matrix over $\mathbb{F}_{q^m}$ as defined in [9].
- X is a $k \times t_1$ distortion matrix over $\mathbb{F}_{q^m}$ of full rank $t_1 \geq n-k$, of the form:

$$X = \begin{bmatrix} X_{11} & 0 \\ X_{21} & X_{22} \end{bmatrix}. \tag{3.2}$$

In other words, the dual matrix of H_X has the form $G_X = \left[\begin{array}{cc|cc} G_1 & G_1 & X_{11} & 0 \\ 0 & G_2 & X_{21} & X_{22} \end{array}\right]$.

The private key is the matrix (X, P, S, G) and the decoding algorithm suggested in Section 3.2.

Encryption: For sending a message $x = (x_1, x_2, \ldots, x_n)$ of rank w to the legitimate receiver, we randomly choose a vector $\gamma = (\gamma_1, \ldots, \gamma_{t1})$ and compute

$$c = (x_1, x_2, \ldots, x_n, \gamma_1, \ldots, \gamma_{t1}) H_{pub}^\top = y H_{pub}^\top$$

such that $x_i, \gamma_j \in \mathbb{F}_{q^m}$ for $i = 1, \ldots, n$, $j = 1, \ldots, t_1$ and $w \leq t$ with t_1 independent to t and w.

Decryption: To decrypt the message, we use the decoding algorithm proposed in Section (3.2), the legitimate receiver computes:

$$c(S^\top)^{-1} = yP^\top \begin{bmatrix} H^\top \\ 0 \end{bmatrix} .$$

We suppose that we have $P^\top = [P_1 \ P_2]$ where P_1 of size $(n+t_1) \times n$ and P_2 of size $(n+t_1) \times t_1$. We denote by $c' = c(S^\top)^{-1}$ and by $x' = x(P_1)$, such that
$c' = x'H^\top$.

Since the rank weight of x' is less than t, we apply the decoding algorithm presented in Section (3.2) on c' and we get x' then we multiply x' by $(P_1)^{-1}$.

Encryption correctness. This is related directly to the error correcting capacity t of the code C and the error should be less than or equal to t. In the decryption step, for $P^\top = [P_1 \ P_2]$, we compute

$$c' = xP^\top = [P_1 \ P_2] \begin{bmatrix} H^\top \\ 0 \end{bmatrix} = yP_1H^\top = x'H^\top,$$

where $c' = c(S^\top)^{-1}$ and $x' = xP_1$. If we have $\mathtt{rank}(x'|\mathbb{F}_q) \leq t$, then we can decode with Algorithm 3. Therefore, we can recover correctly $x(P_1)$ and extract $x = x(P_1)(P_1)^{-1}$. The information rate is equal to $\frac{k}{n}$, the decoding complexity is $\mathcal{O}(n^3)$ and the public key size is $(n-k)(n+t_1)mlog_2(q)$.

4. Security analysis

In this section, we show that our encryption scheme is secure against all known attacks which are classified into combinatorial and algebraic attacks. We also prove IND-CCA2 security which is the most considerable type among IND-CPA and IND-CCA, since the adversary can not submit the ciphertext to the challenger. The codes ILRPC and λ-Gabidulin are with large minimum distance to avoid attacks that try to recover the code structure by looking for low weight codewords either on the code or on its dual. Since we have a larger minimum distance d, such a property leads to avoid leakage information of the public key as it is shown in [24].

4.1. Combinatorial attacks

Usually, these attacks are the most efficient when q, n and k are small enough. The first such attack is given by Chabaud and Stern [8], their attack has a complexity $\mathcal{O}((nw+m)^3q^{(m-w)(w-1)})$. Then, Ourivski and Johanson [29] improved this attack to solve the problem of decoding an $[n,k]$ linear code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ with minimal rank distance d, it can be used after computing the generator matrix of the public key. The problem is formulated as follows:

Problem: *Given $G \in \mathcal{M}_{k\times n}(\mathbb{F}_{q^m})$ and $c \in \mathbb{F}_{q^m}^n$, find $u \in \mathbb{F}_{q^m}^k$ such that; $e = c - uG$ has the smallest rank $w = \mathtt{rank}(e|\mathbb{F}_q)$.*

The modeling of this problem leads the authors to solve a system of a set of quadratic equations by two strategies:

- Basis enumeration: this method requires $\mathcal{O}((k+w)^3q^{(w-1)(m-w)+2})$ binary operations.
- Coordinates enumeration: the complexity of this approach is $\mathcal{O}((k+w)^3w^3q^{(w-1)(k+1)})$ binary operations.

In [12], Gaborit *et al.* generalized the aforementioned attacks. Their idea is to use the notion of the support of a word in rank-metric in

$$\mathcal{O}(w^3k^3q^{(w-1)\lfloor\frac{(k+1)m}{n}\rfloor}).$$

Recently, it was improved in [4] the complexity of solving the RSD problem to

$$\mathcal{O}((n-k)^3m^3q^{w\lceil\frac{(k+1)m}{n}\rceil-m}). \tag{4.1}$$

In our case the error correcting capacity is better due to the large minimum rank distance, so this attack is not applicable.

– **Hauteville and Tillich's attack (2015) [16]**

Hauteville and Tillich introduced a key recovery attack on the LRPC-PKE encryption (in general, the quasi-cyclic codes). This attack is based on a folding and projecting technique. The point of this attack is to find a codeword of low weight d in a projected code over the ring $\mathbb{F}_q[X]/(X^n-1)$. It depends on the factorization of the polynomial (X^k-1) by steps described in [16]. In [3], they proposed the ILRPC code to withstand that attack when this codes are indistinguishable with random codes. We claim that the resulted code is also indistinguishable code.

Lemma 4.1. *The proposed $(u|u+v)$-construction code C_3 given in Definition 3.1 is indistinguishable from a random code.*

Proof. The property of indistiguishability is inherent from the problem of distinguishing an ILRPC code [3]. Hence, it is hard to distinguish for a given codeword if it is from a random code or from the $(u|u+v)$-construction code.

□

4.2. Algebraic attacks

Several algebraic attacks have been carried against the GPT-PKE scheme variants and can be considered against the Niederreiter-PKE scheme. Among these attacks we consider the following ones:

– **Gibson's attack (1995) [14]**

The purpose of Gibson's attack is to solve the next problem:

Problem: *Given* (G_{pub}, t_1) *the public key of the GPT-PKE scheme find a triple* $(\tilde{G}, \tilde{S}, \tilde{X})$ *such that* $G_{pub} = \tilde{S}\tilde{G} + \tilde{X}$.

We can give a solution of this problem in $\mathcal{O}((n-k)k^3 q^{mt_1})$ binary operation. The Gibson's attack can not be applied in our approach due to the existence of the full rank distortion matrix in the private key as it has been proven in [23].

– **Overbeck's attack (2008) [31]**

To realize Overbeck's attack, we construct a matrix $G^{'}$ defined as:

$$\tilde{G}^{'} = \begin{pmatrix} S & 0 & \dots & 0 \\ 0 & S^{[1]} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & S^{[n-k-1]} \end{pmatrix} \begin{pmatrix} X & G \\ X^{[1]} & G^{[1]} \\ \vdots & \vdots \\ X^{[n-k-1]} & G^{[n-k-1]} \end{pmatrix} P = S^{'}(X^{'}|G^{'})P,$$

where $S^{[i]}$ is the matrix obtained by applying the ith power of the Frobenius automorphism $\theta^i : x \to x^{q^i}$ to all coefficients of S.

In [23], Loidreau has shown that Overbeck's attack is not successful if $\texttt{rank}(X^{'}|G^{'}) = n + t_1 - 1$. In the proposed scheme we choose the rank $t_1 \geq n - k$ to avoid this attack. This property withstands also the recent extension of Overbeck's attack proposed in [18]. When the distortion matrix is not of full rank, it applies the extension of this matrix and searches elements of rank one to recover the encrypted message in polynomial time. Besides this, we choose the column scrambler P in the extension field to avoid the attack [19, 22], which means that the Frobenius automorphism of P will not be the same matrix P (*i.e.* $\theta(P) \neq P$).

$$\tilde{G}^{'} = \tilde{S}^{'} \begin{pmatrix} X & G \\ X^{[1]} & G^{[1]} \\ \vdots & \vdots \\ X^{[n-k-1]} & G^{[n-k-1]} \end{pmatrix} \begin{pmatrix} P \\ P^{[1]} \\ \vdots \\ P^{[n-k-1]} \end{pmatrix} .$$

– **Bardet *et al.*'s attack (2020) [5]**

The authors in [5] provided an improvement of algebraic attacks for solving MinRank and Rank Decoding problems without using Gröbner basis and breaks rank based parameters proposed to the NIST Standarization Process approaches like ROLLO and RQC [1, 3] .

Two modeling were proposed to solve these problems in two cases: "overdetermined case" when there are enough linear equations *i.e.*

$$m\binom{n-k-1}{w} \geq \binom{n}{w} - 1. \tag{4.2}$$

The complexity of the (m, n, k, w)-decoding algorithm in that case (Algorithm 1, [5]) is given as follows:

$$O\left(m\binom{n-k-1}{w}\binom{n}{w}^{\omega-1}\right), \tag{4.3}$$

operations over $\mathbb{F}_q$, with ω is the constant of linear algebra. The "underdetermined case" when (4.2) is not fulfilled. However, authors proposed to look for a reduction to the overdetermined case by:

- A hybrid attack and look for the smallest integer a such that $m\binom{n-k-1}{w} \geq \binom{n-a}{w} - 1$ holds and the complexity becomes $O\left(q^{a\cdot w} m\binom{n-k-1}{w}\binom{n-a}{w}^{\omega-1}\right)$ operations over $\mathbb{F}_q$.
- The super overdetermined case using the punctured code on the last p coordinates instead of the whole of the code. Taking the maximal number of p such that $m\binom{n-p-k-1}{w} \geq \binom{n-p}{w} - 1$ holds, will reduce the complexity into $O\left(m\binom{n-p-k-1}{w}\binom{n-p}{w}^{\omega-1}\right)$ operations over $\mathbb{F}_q$.

Otherwise, they solve the underdetermined case using direct linearization or by Support Minors Modeling in conjunction with the maximal minors of the code for which the best complexity will be set to Widemann's algorithm or Strassen's algorithm.

Some approaches could avoid it by changing their parameters to be larger but reasonable. Hence, we set similarly larger value for the set of parameters of the proposed scheme.

4.3. Indistinguishability security

In this section, we study the most required security proof, the indistinguishability under chosen ciphertext attack IND-CCA. Let $\mathbf{A}$ be a probabilistic polynomial time algorithm adversary on the proposed scheme proposed in this paper and let $\mathbf{C}$ be the challenger for which the game hopping is between $\mathbf{A}$ and $\mathbf{C}$. It generates the pair of keys (pk, sk) based on the secret parameter and he sends pk to $\mathbf{A}$ who will perform a number of operations of the encryption calls to send it to the decryption oracle $\mathbf{O}$ which outputs plaintexts. Then $\mathbf{A}$ chooses randomly two distinct plaintexts m_0 and m_1 in order to send them to $\mathbf{C}$. Then, $\mathbf{C}$ selects at random $b \in \{0,1\}$ and computes the ciphertext Encrypt(pk, m_b) in order to send it to $\mathbf{A}$.

```
$\mathbf{E} = Exp_{PKE,A}^{IND-CCA2,b}(\delta)$
$(pk, sk) \longleftarrow KeyGen(\delta)$
$(m_0, m_1) \longleftarrow \mathbf{A}(Find : pk)$
$y \longleftarrow \text{Encrypt}(pk, m_b)$
$b' \longleftarrow \mathbf{A}(Guess : y)$
Return $b'$.
```

Then, three types of indistinguishability appear

- IND-CPA : $\mathbf{A}$ guesses the value of b and performs a call to $\mathbf{O}$.
- IND-CCA : $\mathbf{A}$ may not make further calls to $\mathbf{O}$ before guessing the value of b.
- IND-CCA2 : $\mathbf{A}$ may make further calls to $\mathbf{O}$ but may not submit the challenge ciphertext c, and it should guess the value of b.

The proposed PKE scheme is indistinguishable when the adversary $\mathbf{A}$ could not guess b and has a negligible advantage, *i.e.* $Adv_{PKE,\mathbf{A}}^{IND}(\delta) \leq negl$ where δ is the chosen security level. We will give the proof of the last type of indistinguishability the (IND-CCA2) considering an experiment $\mathbf{E}$.

Theorem 4.2. *The Niederreiter-like PKE scheme based on the hardness the RSD is secure under IND-CCA2.*

Proof. To prove this theorem, we perform a sequence of games on the PKE scheme parameters on the experiment $\mathbf{E}$.

- G_0: We proceed the scheme naturally with its parameters, pk and the matrices S, P and the matrix X of full rank t_1. The adversary $\mathbf{A}$ has to recover the ciphertext for a given public key pk and a security parameter δ.
- G_1: We transform in the game G_0 its pk into a random one, in this time the probability that the adversary has to find the ciphertext using that public key is the same probability of solving an instance of the RSD problem. Hence, the advantage is given as follows:

$$Adv_{\mathbf{E},\mathbf{A}}^{G_1}(\delta) \leq Adv_{\mathbf{E},\mathbf{A}}^{RSD}(\delta)$$

TABLE 1. Different set of parameters for $(u|u+v)$ construction.

m	ILRPC $[n_1, k_1, w_1]$	λ-Gabidulin $[n_2, k_2, w_2]$	$(U\|U+V)$ $[n, k, w]$	$\|pk\|$ KB	$\|ct\|$ bits	a	Security level
47	(32,16,8)	(32,9,6)	(64,25,10)	5.7	1833	11	128
59	(42,21,9)	(42,12,8)	(84,33,14)	12.4	3009	22	192
67	(48,24,11)	(48,20,13)	(96,44,23)	19.1	3484	38	256

- G_2: We provide the same as in game G_1 and transform it for random value of y in $\mathbb{F}_{q^m}^n$. The adversary tries to guess b for that random y. He cannot distinguish the result of the encryption and the random value of y due to the indistinguishability of the $(u|u+v)$-construction code

$$Adv_{\mathbf{A},\mathbf{E}}^{G_2}(\delta) \leq Adv_{\mathbf{E},\mathbf{A}}^{G_1}(\delta) + Adv_{\mathbf{E},\mathbf{A}}^{(U|U+V)}(\delta)$$

Hence, we conclude that it is IND-CCA2 secure.

□

Beside to this, we claim that the randomness of the matrices S, P and X, chosen in the scheme, makes hard to find the exact matrices for each performance of such attacks.

4.4. Set of parameters

In this section, we give the set of parameters with its security levels, using the $(u|u+v)$-construction code with $[n_1 = 2k_1, k_1, d_1]$ ILRPC and $[n_2, k_2, d_2]$ λ-Gabidulin codes means that the degree of the extension field becomes lower than the length, with larger minimum distance d which is good to avoid leakage information of the public key.

For the parameters, we choose the matrix X of full rank t_1 to avoid Gibson's attack and this t_1 should be greater than $n-k$ to avoid Overbeck's attack. We also choose the matrix P with entries in $\mathbb{F}_{q^m}$ as proposed in [22]. Hence, we compute the sizes of the public key, secret key and ciphertext by using the following expressions:

- The public key size in systematic form: $k(n-k)m\log_2(q)$ bits.
- The ciphertext size: $(n-k)m\log_2$

For the secret key size one can recover the set of parameters with a random vector. This reduces the secret key size. We give in Table 1 some different set of parameters with sizes; public key $|pk|$ in KiloByte (KB) and the ciphertext $|ct|$ in bits with the best complexity of Bardet el al. [5].The column "a" indicates the smaller chosen integer for the hybrid attack since inequality (4.2) is not fulfilled with $\omega = 2.81$.

4.5. Comparison

In this section, we provide a comparison with the parameters given in [2, 22] with their security level upper than 128 for which they do not satisfy security level of the recent attack [5]. In the set of parameters of [22], σ design the dimension of the vector space over $\mathbb{F}_{q^m}$ which has entries of the matrix P. We benefit a reduction from the ciphertext and the public key sizes and we set security level used in the item of comparison (4.1).

In Table 2, we set the $[n_1 = 20, k_1 = 10, w_1 = 5]$ ILRPC code and for the λ-Gabidulin code we set $[n_2 = 20, k_2 = 6, w_2 = 4]$ with $m = 37$.

Hence, the error-correcting capacity is $t = \lfloor \frac{n-k}{2} \rfloor = 12$. We choose the design parameter t_1 such that $t_1 \geq n-k$ to withstand Overbeck's attack, in this example $t_1 = 25$. The rank weight of the ciphertext w should be less or equal to t. Therefore, the $(u|u+v)-$construction code in this case has the set of parameters $[40, 16, 10]$ and then we can obtain the public key size as 1.7 KB.

Table 2. Comparison of public key size and cipher text size between $(u|u+v)$-construction code, Al Shehhi *et al.* [2] and Loidreau [22] for different security levels.

PKC-(parameters)	Set of parameters	$\lvert pk\rvert$	$\lvert ct\rvert$	Security level
Loidreau [22] (n, m, k, σ, t)	$(90, 128, 24, 3, 11)$	21.5	1.44	≈ 140
Al Shehhi *et al.* [2] (m, n, k, σ, t)	$(64, 58, 28, 3, 5)$	6.56	0.46	128
$(u\lvert u+v)-$construction- (n, m, k_1, k_2, t_1, w)	$(40, 37, 10, 6, 25, 9)$	1.7	0.11	128

5. Conclusion

We present in this paper a variant of the Niederreiter cryptosystem based on the RSD problem using a simple type of codes. The $(u|u+v)$-construction code between the less structured ILRPC and λ-Gabidulin codes. We provide an efficient decoding algorithm due to the sharing properties of the two codes. This makes our PKE more secure against known attacks as we provide in its security analysis with combinatorial and algebraic attacks. Even with the recent attack [5], the scheme is secure for larger set of parameters and has a reasonable sizes of the public key and ciphertext. The constructed code is indistinguishable from random codes and has larger minimum distance d. Moreover, our PKE is secure under IND-CCA2 with much reduced public key size and ciphertext size for the adopted security level compared to Loidreau's [22] and to its IND-CCA secure version proposed by Al Shehhi *et al.* [2].

References

[1] C. Aguilar-Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.C. Deneuville, P. Gaborit and G. Zémor, Rank quasi-cyclic (rqc) (2017), https://pqc-rqc.org/doc/rqc-specification2017-11-30.pdf.

[2] H. Al Shehhi, E. Bellini, F. Borba, F. Caullery, M. Manzano and V. Mateu, An IND-CCA-secure code-based encryption scheme using rank metric. In: Buchmann J., Nitaj A., Rachidi T. (eds) Progress in Cryptology – AFRICACRYPT 2019. Vol. 11627 of *Lecture Notes in Computer Science*. Springer (2019).

[3] N. Aragon, O. Blazy, J.C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.P. Tillich, G. Zémor, C. Aguilar Melchor, S. Bettaieb, L. Bidoux, B. Magali and A. Otmani, ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER). Second round submission to the NIST post-quantum cryptography call (2019), https://pqc-rollo.org.

[4] N. Aragon, P. Gaborit, A. Hauteville and J-P. Tillich, Improvement of generic attacks on the rank syndrome decoding problem. *Des. Codes Cryptogr.* **35** (2005) 63–79.

[5] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich and J. Verbel, Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems. ASIACRYPT 2020, Vol. 12491 of *LNCS*. Springer (2020) 507–536.

[6] T.P. Berger and P. Loidreau, How to mask the structure of codes for a cryptographic use. *Designs Codes Cryptogr.* **35** (2005) 63–79.

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

[8] F. Chabaud and J. Stern, The cryptographic security of the syndrome decoding problem for rank distance codes. *ASIACRYPT* (1996) 368–381.

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

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

[11] P. Gaborit, G. Murat, O. Ruatta and G. Zémor, Low rank parity-check codes and their application to cryptography. In *The International Workshop on Coding and Cryptography (WCC 13)*, Bergen, Norway (2013) 13 p. hal-00913719.

[12] P. Gaborit, O. Ruatta and J. Schrek, On the complexity of the Rank Syndrome Decoding problem. *IEEE Trans. Inf. Theory* **62** (2016) 1006–1019.

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

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

[15] J.K. Gibson, The security of the Gabidulin public key cryptosystem. Vol. 1070 of *EUROCRYPT'96, LNCS* (1996) 212–223.

[16] A. Hauteville and J-P. Tillich, New algorithms for decoding in the rank-metric and an attack on the LRPC-PKC. *IEEE ISIT* (2015).

[17] F. Hernando and D. Ruano, Decoding of matrix-product codes. *J. Algebra Appl.* **12** (2013) 1250185.

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

[19] E. Kan, E. Gabidulin, B. Honary and H. Ahmed, Modified Niederreiter type of GPT-PKC based on reducible rank codes. *Des. Codes Cryptogr.* **70** (2014) 231–239.

[20] T.S.C. Lau and C.H Tan, A new Gabidulin-like code and its application in cryptography. In: Carlet C., Guilley S., Nitaj A., Souidi E. (eds) Codes, Cryptology and Information Security. C2SI 2019. Vol. 11445 of *Lecture Notes in Computer Science*. Springer, Cham. https://doi.org/10.1007/978-3-030-16458-4_16.

[21] J. Liu, Y. Wang, Z. Yi and Z. Lin, polarRLCE: a new code-based cryptosystem using polar codes. *Secur. Commun. Netw.* (2019) Article ID 3086975 https://doi.org/10.1155/2019/3086975.

[22] P. Loidreau, A new rank metric codes based encryption scheme. *PQCrypto*, Utrecht, Netherlands (2017) 3–17.

[23] P. Loidreau, *Métrique rang et cryptographie*. HDR thesis, France (2007).

[24] I. Marquez-Corbella and J-P Tillich, Using Reed-Solomon codes in the $(u|u+v)$ construction and an application to cryptography. *IEEE International Symposium on Information Theory (ISIT)* (2016).

[25] G. Marsaglia, Bounds for the rank of the sum of two matrices, No. D1-82-0343. In *Boeing Scientific Research Labs*, Seattle, WA (1964).

[26] R.J. McEliece, A public-key cryptosystem based on algebraic coding theory. *Des. Codes Cryptogr.* **8** (1978) 293–307.

[27] H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory* **15** (1986) 157–166.

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

[29] A.V. Ourivski and T. Johansson, New technique for decoding codes in the rank-metric and its cryptography applications. *Prob. Inf. Trans.* 38 (2002) 237–246.

[30] R. Overbeck, A new structural attack for GPT and variants. *Mycrypt* **3715** (2005) 50–63.

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

[32] D. Silva and F.R. Kschischang, Fast encoding and decoding of gabidulin codes. In *IEEE International Symposium on Information Theory* (2009) 2858–2862.

[33] A. Wachter-Zeh, Decoding of Block and Convolutional Codes in Rank Metric, Ph.D thesis, University of Rennes 1, France (2013).