An IND-CCA-Secure Code-Based Encryption Scheme Using Rank Metric

Hamad Al Shehhi[1], Emanuele Bellini[1], Filipe Borba[2], Florian Caullery[1], Marc Manzano[1], and Victor Mateu[1]

[1] Darkmatter LLC
{hamad.alshehhi,emanuele.bellini,florian.caullery,marcos.manzano,
victor.mateu}@darkmatter.ae
[2] Universidade Federal de Santa Catarina
filipeoborba@gmail.com

Abstract. The use of rank instead of Hamming metric has been proposed to address the main drawback of code-based cryptography: large key sizes. There exist several Key Encapsulation Mechanisms (KEM) and Public Key Encryption (PKE) schemes using rank metric including some submissions to the NIST call for standardization of Post-Quantum Cryptography. In this work, we present an IND-CCA PKE scheme based on the McEliece adaptation to rank metric proposed by Loidreau at PQC 2017. This IND-CCA PKE scheme based on rank metric does not use a hybrid construction KEM + symmetric encryption. Instead, we take advantage of the bigger message space obtained by the different parameters chosen in rank metric, being able to exchange multiple keys in one ciphertext. Our proposal is designed considering some specific properties of the random error generated during the encryption. We prove our proposal IND-CCA-secure in the QROM by using a security notion called disjoint simulatability introduced by Saito et al. in Eurocrypt 2018. Moreover, we provide security bounds by using the semi-oracles introduced by Ambainis et al.

Keywords: Post Quantum Cryptography · Code-based cryptography · Rank metric · IND-CCA · PKE · QROM.

1 Introduction

The use of standard public key cryptography algorithms such as RSA and ECDH has been a model to secure information in the last decades. However, in the past few years, the threat of a quantum computer breaking the security of all the standard public key cryptosystems in feasible time has forced the community to look for quantum resistant cryptographic schemes which can be implemented on traditional electronic computers. This field of research is called Post-Quantum Cryptography (PQC) [7]. The NIST call for proposals [24] has increased the motivation of the research community towards this topic. By the time of writing, some proposals were withdrawn from the competition as some major flaws were

discovered on their security. Some others had to modify their initial parameters to keep meeting the security requirements from NIST. This was caused by either a misconception on the security of some problems or by new attacks being presented. These challenges were expected given that the security assumptions on which these schemes rely are often not as well understood as the previous standard ones (e.g., discrete logarithm and integer factorization).

In 2017, a proposal from Loidreau [20] and its implementation [1], which is not part of the NIST competition, was presented. The scheme is a modification of the McEliece cryptosystem [21] using rank instead of Hamming metric. The advantage of which relies on the fact that the complexity of decoding with random codes in this metric is quadratic compared to the complexity of decoding in the Hamming metric. Therefore, code-based cryptosystems using rank metric require smaller key sizes. The first cryptosystem based on this metric was proposed by Gabidulin, Paramonov and Tretjakov (GPT) [14] and it used Gabidulin codes. It was broken by the Overbeck attack framework [26]. This attack on the GPT encryption scheme is able to, given a public key G, forge an alternative Gabidulin code able to decrypt the ciphertexts encrypted using G. To do this, it exploits the fact that the column scrambler matrix used to compute the public key in order to hide the structure of the private Gabidulin code is a matrix of elements over the base field $\mathbb{F}_q$. In Loidreau's scheme, this matrix is replaced by another one having coefficients in a random vectorial subset. That adaptation is enough to prevent Overbeck's attack framework.

Nowadays, many cryptographic protocols require to use a IND-CCA-secure cryptosystem in order to protect the privacy of the participants involved in it. Unfortunately, Loidreau's original proposal and its implementation [1] do not offer IND-CCA security, which implies no protection against malleability. Therefore, it cannot be used in many practical cases. The concept of ciphertext malleability was first introduced by Dolev et al. [11], and nowadays it is known that non-malleability against chosen ciphertext attacks is equivalent to IND-CCA-security. Furthermore, several techniques to turn a IND-CPA-secure cryptosystem into an IND-CCA-secure one have been presented. One of the most used solutions to turn an IND-CPA PKE scheme into a IND-CCA KEM is the Fujisaki-Okamoto transformation [12].

1.1 Our contribution

In this paper we propose an IND-CCA-secure variant of Loidreau's rank based PKE scheme. We present a construction inspired by ideas from recent transformation techniques [12, 18, 27] used to obtain IND-CCA KEM, or the hybrid PKE construction using symmetric key. However, in our case the target is a non-hybrid PKE scheme with a message space large enough to fit more than just one symmetric key. Our construction takes advantage of the bigger error space from rank metric and uses it as a random value required for the decryption validations. As a result, the proposed decryption algorithm does not require any encryption operation. We prove the IND-CCA security of our proposal in the QROM with a security proof based on previous works by Nojima et al, [25]

and Saito, Xagawa and Yamakawa [27] from which we borrow the central notion of *Disjoint Simulatability*.

Besides the theoretical description of the PKE scheme, we also prove our scheme suitable for real world scenarios by presenting new parameters and a performance comparison with the original implementation of Loidreau's scheme given in [1].

1.2 Structure

In the next section we recall some definitions needed to understand Loidreau's scheme and our modification such as *rank metric* and *Gabidulin codes* or the security requirements IND-CPA and IND-CCA. After that, we recall the original scheme in Section 3 and, in Section 4, we propose a new IND-CCA-secure PKE scheme and three parameter sets for different security levels. Section 5 is devoted to proving our proposal IND-CCA-secure in the QROM. Moreover, the performance of new algorithms and a comparison with the original ones and the resulting algorithms from applying SXY [27] transformation is provided in Section 5.2. Finally, Section 6 is devoted to the conclusions.

2 Preliminaries and notations

We denote by $\mathbb{F}_{q^m}$ the finite field of q^m elements and by $\mathbb{F}_{q^m}^n$ the vectorial space of dimension n over the field $\mathbb{F}_{q^m}$. We denote by $GL_n(\mathbb{F}_q)$ the set of all invertible square matrices of n rows and n columns with elements in $\mathbb{F}_q$. Besides that, in the algorithms we use $a \leftarrow\!\!\$\, B$ to note that a is a random element from B.

Let $e = (e_1, \ldots, e_n) \in \mathbb{F}_{q^m}^n$. The rank weight of a vector e is denoted as $\mathsf{rk}(e)$, and is defined as the rank of the matrix

$$E = \begin{pmatrix} e_{1,1} & \cdots & e_{n,1} \\ e_{1,2} & \cdots & e_{n,2} \\ \vdots & \ddots & \vdots \\ e_{1,m} & \cdots & e_{n,m} \end{pmatrix}$$

where $e_{i,j}$ is the j-th component of e_i seen as a vector over $\mathbb{F}_q$. The rank weight of a vector was introduced by Gabidulin in [13] to propose the error correcting codes defined below which can correct errors with repeating patterns, regardless of their Hamming weight.

Definition 1 (Gabidulin codes). *Let $k < n \leq m$ be non-negative integers and let $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. Let $[i] = q^i$ such that $x \to x^{[i]}$ is the i-th power of the Frobenius automorphism $x \to x^q$. Given the generator matrix*

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

a Gabidulin code is defined as

$$Gab_{k,n}(g) = \{xG \mid x \in \mathbb{F}_{q^m}^k\}.$$

Gabidulin Codes are the rank-metric equivalent of Reed Solomon Codes. These codes can correct errors of rank weight up to $\lfloor (n-k)/2 \rfloor$ in polynomial-time where k is the code dimension and n the code length [13].

2.1 Decisional Rank Syndrome Decoding (DRSD) Problem

Code-based cryptography using rank metric generally relies on the hardness of Rank Syndrome Decoding problem (RSD). In our security proof we use the decisional version of this problem to prove some properties of our proposal. Let us recall the definition.

Definition 2 (DRSD Problem). *Given G a full rank $k \times n$ matrix over $\mathbb{F}_{q^m}$, $x \in \mathbb{F}_{q^m}^k$, and $e \in \mathbb{F}_{q^m}^n$. Considering y a random value in $\mathbb{F}_{q^m}^n$, is it feasible to distinguish $(G, xG + e)$ from (G, y)?*

The hardness of the DRSD problem is proven in [15, Apendix B.2]

2.2 Hash functions

In our constructions, we use two different kinds of hash functions. One is the classical hash that we use for correctness, and the other is a hash function with a rather large output which will be obtained by using an eXtended Output Function (XOF). An XOF is a hash function whose output can be extended to an arbitrary desired length. A requirement for our XOF and hash function is to be secure against any quantum computer-aided attack. Fortunately, the SHA-3 and SHAKE as defined in [23] are proved to be secure in such attack scenarios [10].

2.3 Public-Key Encryption

A public-key encryption scheme PKE = $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ is defined by three algorithms. The key generation algorithm KGen receives as input a security parameter and outputs a keypair $(\mathsf{pk}, \mathsf{sk})$. The encryption algorithm Enc takes as input a public key pk and a message x from a finite message space M, and outputs a ciphertext $c \in \mathcal{C}$ where $\mathcal{C}$ is the ciphertext space and c is the encryption of the message m with the public key pk. The decryption algorithm Dec takes as input a secret key sk and a ciphertext $c \in \mathcal{C}$, and outputs a message $x \in M$ or a rejection symbol $\perp \notin M$.

Definition 3 (Perfect correctness). *A PKE scheme* PKE = $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *has perfect correctness if for any keypair* $(\mathsf{pk}, \mathsf{sk})$ *generated by* KGen *and for any message $x \in M$*

$$\Pr[\mathsf{Dec}_{\mathsf{sk}}(c) = x \mid c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(x)] = 1$$

2.4 IND-CPA and IND-CCA notions

We finally recall, following [6], the definitions of security notions for indistinguishability under chosen plaintext attack (IND-CPA) and indistinguishability under chosen ciphertext attack (IND-CCA) for PKE schemes.

Definition 4. *Let* $E = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an encryption scheme. Let* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *be an adversary, i.e. a pair of probabilistic polynomial time algorithms responsible, respectively, to generate a pair of messages given the public key and access to an oracle, and a guess on which of the two messages has been encrypted given access to the encryption of one of the two messages and to another oracle*[3]*. Let* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$ *and* $\lambda \in \mathbb{N}$*. For* $b \in \{0, 1\}$*, consider the* atk *indistinguishability experiment defined by the following steps:*

$\mathrm{Exp}_{E,\mathcal{A}}^{\mathrm{ind-atk}-b}(\lambda)$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(\lambda)$
2 : $(x_0, x_1, s) \leftarrow \mathcal{A}_1^{O_1(.)}(\mathsf{pk})$
3 : $y \leftarrow \mathsf{Enc}_{\mathsf{pk}}(x_b)$
4 : $b' \leftarrow \mathcal{A}_2^{O_2(.)}(x_0, x_1, s, y)$
5 : **return** b'

where, if $\mathrm{atk} = \mathrm{cpa}$*, the oracles functions* $O_1(.)$ *and* $O_2(.)$ *return the empty string, and if* $\mathrm{atk} = \mathrm{cca}$*, the oracles functions* $O_1(.) = O_2(.) = \mathsf{Dec}_{\mathsf{sk}}(.)$*. Then, the* $\mathrm{ind} - \mathrm{atk}$ *advantage of* $\mathcal{A}$ *over the encryption scheme is defined as*

$$\mathsf{Adv}_{E,\mathcal{A}}^{\mathrm{ind-atk}}(\lambda) = \Pr\left[\mathrm{Exp}_{E,\mathcal{A}}^{\mathrm{ind-atk}-1}(\lambda) = 1\right] - \Pr\left[\mathrm{Exp}_{E,\mathcal{A}}^{\mathrm{ind-atk}-0}(\lambda) = 1\right] .$$

A PKE scheme is secure against atk attack *if* $\mathsf{Adv}_{E,\mathcal{A}}^{\mathrm{ind-atk}}(\lambda)$ *is a negligible function of the security parameter* λ*.*

Informally, we consider a PKE scheme to be *secure against chosen-ciphertext attack* if a "reasonable" adversary cannot obtain "significant" advantage in distinguishing the cases $b = 0$ and $b = 1$ given access to the oracles, where reasonable reflects its resources usage. Still informally, the main difference between the two types of attacks consist in which oracle the adversary can access and when. In the IND-CPA game, the adversary has no access to the decryption oracle. However, in the IND-CCA game, the adversary has access to the decryption oracle. There exists two notions of IND-CCA security: IND-CCA1 security refers to the situation when the adversary can access the decryption oracle only before seeing the challenge ciphertext, while in the IND-CCA2 setting the adversary can access the decryption oracle even after seeing the challenge ciphertext, with the obvious constraint that he cannot ask the oracle to decrypt the challenge y. In this paper, when we refer to IND-CCA security, we mean IND-CCA2.

[3] The idea is that $\mathcal{A}_1$, once given the public key, is responsible to generate a test instance composed by two messages of its choice, while $\mathcal{A}_2$ receives a challenge ciphertext generated as a probabilistic function of the test instance, and must output a guess of which of the two messages has been encrypted.

2.5 Quantum Random Oracle Model (QROM)

It is common to provide security analysis in the Random Oracle Model (ROM). However, this model has been proven [8] not to be accurate when the attackers have access to a quantum computer. To deal with this case, a new model was defined. In this model, an adversary can quantumly query a random oracle. Therefore, some well-known techniques that were applied on the ROM, such as adaptive programmability or extractability, cannot be used in the QROM.

In the security proofs presented hereby we are going to use the notion of semi-classical oracles. This concept was recently introduced in [3] with the idea of allowing a quantum-accessible oracle to somehow measure the input and output. With this concept, the authors provided better bounds for some well-known problems resulting from the One-way to Hide (O2H) lemmas.

3 Loidreau's proposal

Loidreau's scheme chooses a randomly selected vector space of $\mathbb{F}_2^m$ of fixed dimension to scramble the codes. The idea can be interpreted as replacing the permutation matrix in a McEliece-like cryptosystem by a matrix multiplying the Hamming weight of the vectors.

Let us recall the original scheme $\mathrm{PKE}_{Lo} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ as defined in [20]:

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}_{pk}(x)$	$\mathsf{Dec}_{sk}(y)$
$k, n, m, \delta, t \leftarrow \mathrm{ParamSelect}(1^\lambda)$	$t \leftarrow \lfloor (n-k)/(2\delta) \rfloor$	$(x, e) \leftarrow \mathrm{decode}_{\mathsf{sk}}(yP)$
$G \leftarrow \mathrm{GenGabCode}(k, n, m)$	$e \leftarrow_{\$} \{z \in \mathbb{F}_{2^m}^n \mid \mathsf{rk}(z) = t\}$	**if** $(x, e) = \perp$
$S \leftarrow_{\$} GL_k(\mathbb{F}_{2^m})$	$y \leftarrow xG_{pub} + e$	**return** $\perp$
$V \leftarrow_{\$} \{\mathcal{V} \subset \mathbb{F}_{2^m} \mid \dim(\mathcal{V}) = \delta\}$	**return** y	**else**
$P \leftarrow_{\$} GL_n(V)$		**return** x
return $\mathsf{sk} = (G, S, P)$, $\mathsf{pk} = G_{pub} = SGP^{-1}$		

More precisely, in KGen algorithm, given a security parameter 1^λ the function $\mathrm{ParamSelect}(1^\lambda)$ provides appropriate values for k, n, m, δ, and t. After that, the function $\mathrm{GenGabCode}(k, n, m)$ randomly generates the generator matrix of a Gabidulin code as defined in Section 2. Then, S, V, and P are generated and the keypair is computed and returned.

In Dec algorithm, the function $\mathrm{decode}_{\mathsf{sk}}(yP)$ performs the decoding operation to recover xS and eP, from which it is easy to obtain (x, e) by using S^{-1} and P^{-1}. In the case of a decoding failure this function would return $\perp$.

It is worth noticing that matrix P is chosen so that it has all its entries in a vectorial subspace of dimension δ, then $\mathsf{rk}(eP) \leq \delta \mathsf{rk}(e) \leq \left\lfloor \frac{n-k}{2} \right\rfloor$ (see [20, Prop. 1]) which is decodable by the Gabidulin code.

The proof of correctness of the cryptosystem is based on the rank multiplication property, the same one used to show that the Low Rank Parity Check (LRPC) codes decoding procedure works.

4 Our proposal

Loidreau's scheme is One Way Encryption (OWE) as defined in [20]. It has the property that given a ciphertext it is hard to obtain the plaintext. However, it does not achieve IND-CPA security (and therefore not IND-CCA security either) which is a security notion often required on real-world scenarios and also the weakest security notion required in the NIST call for standardization of PQC [24].

In this section we propose a new scheme which we will prove IND-CCA-secure. The main idea is to use the randomly generated error from Loidreau's encryption scheme for multiple purposes:

1. As a source of randomness to generate a value to mask the codeword.
2. As the error used to hide the resulting codeword.
3. As a random parameter for a correctness validation during decryption.

Usually, in transformations such as Fujiaki-Okamoto, this validation is done in the decryption algorithm by re-computing the ciphertext given all the parameters obtained after decoding. Yet, in our proposal the correctness validation does not require the re-encryption using the public key.

Our PKE scheme $\text{PKE}_{new} = (\mathsf{KGen}, \mathsf{Enc}', \mathsf{Dec}')$ maintains the same key generation algorithm so it does not add any new parameter. For the remaining two algorithms we need two additional functions H and H'. The first one is an XOF function, and the other is hash function, as introduced in Section 2.2. The PKE_{new} algorithms are presented below:

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}'_{pk}(x)$	$\mathsf{Dec}'_{sk}(y)$
$k, n, m, \delta \leftarrow \text{ParamSelect}(1^\lambda)$	$t \leftarrow \lfloor (n-k)/(2\delta) \rfloor$	$(x', e') \leftarrow decode_{\mathsf{sk}}(yP)$
$G \leftarrow \text{GenGabCode}(k, n, m)$	$e \leftarrow_\$ \{z \in \mathbb{F}_{2^m}^n \mid \mathsf{rk}(z) = t\}$	**if** $(x', e') = \perp$
$S \leftarrow_\$ GL_k(\mathbb{F}_{2^m})$	$x^* \leftarrow x \| H'(e, x)$	**return** $\perp$
$V \leftarrow_\$ \{\mathcal{V} \subset \mathbb{F}_{2^m} \mid \dim(\mathcal{V}) = \delta\}$	$y \leftarrow (x^* + H(e))G_{pub} + e$	**else**
$P \leftarrow_\$ GL_n(V)$	**return** y	$x \| v = x' + H(e')$
return $\mathsf{sk} = (G, S, P)$,		**if** $H'(e', x) \neq v$ and
$\mathsf{pk} = G_{pub} = SGP^{-1}$		$\mathsf{rk}(e') \neq t$
		return $\perp$
		else
		return x

Notice that the confirmation hash (i.e. $H'(e, x)$) must be of a size that accommodates the desired security level. Otherwise, the security level of the scheme would be reduced to the security of finding a pre-image in H'. In practice, this causes a reduction in the message space because of the padding required. Fortunately, there exist sets of parameters that allow a bigger message space which can accommodate this restriction easily.

The security bounds of the scheme are different than the ones presented in the original proposal [20]. We consider newly proposed algorithms for solving the rank syndrome decoding problem from [16, 4, 5]. However, the complexity of finding a decoder given a public key remain the same as originally published.

- Decoding a ciphertext in the public code corresponds to the complexity of solving Bounded Distance binary Rank decoding (BDR) problem which is NP-hard. In this setting, formulas for the decoding complexity for a classical computer in terms of binary operations can be found in [16, 4, 5], where both combinatorial and algebraic attacks are described.
- The complexity of finding a proper decoder given a public key G_{pub} is $2^{(\delta-1)m-(\delta-1)^2}$ (see [20]).
- The complexity of distinguishing the public code from a random code is lower bounded by the complexity of recovering a proper decoder from a public key G_{pub}.

In [9], it is shown that a polynomial attack can be applied if $\delta = 2$ and $k \geq n/2$. The authors also claim that the attack can probably be applied more generally when $k/n \geq 1 - 1/\delta$.

Next, we propose a parameter set to provide three different security levels taking into consideration the message space and the known attacks to Loidreau's scheme [20], including [16], [4], [5], and [9]. In Table 1 the parameter set is presented as well as the resulting public key size (PK Size) in Kilo-bytes and message space in bytes. The table also includes the complexity of the best known attack to the cryptosystem for the chosen parameters. These attacks are decoding a ciphertext in the public code, noted as *Dec. Cplx.* for traditional electronic computers, or as *Quantum Dec. Cplx.* for quantum computers, and finding a proper decoder given a public key, noted as *PK Dec. Cplx.*

m	n	k	δ	t	PK size	Message Space	Dec. Cplx.	Quantum Dec. Cplx.	PK Dec. Cplx.
67	59	23	3	6	6.94 KB	193B	2^{130} [4, 16]	2^{82} [4]	2^{130}
89	96	32	4	8	22.78KB	356B	2^{193} [4, 5]	2^{115} [4]	2^{258}
89	159	49	5	11	59.96KB	546B	2^{259} [4]	2^{149} [4]	2^{340}

Table 1. Proposed parameters for our IND-CCA-secure scheme

5 Security

IND-CCA security is required for several applications in which the protocol security relies on this indistinguishability notion to protect the messages. Numerous works have proposed mechanisms to go from one construction with weaker security to another one meeting IND-CCA. In our security proof we take into consideration the concept of disjoint simulatability introduced in [27, Section 3] which helps on proving a Deterministic PKE (DPKE) to behave like a pseudorandom number generator. First, we recall the definition:

Definition 5 (Disjoint Simulatability). *Let $\mathcal{D}_M$ denote an efficiently sampleable distribution on a set M. A DPKE scheme* $\mathrm{DPKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$*, with plaintext and ciphertext spaces M and C is $\mathcal{D}_M$-disjoint simulatable if it provides the following two properties:*

- *Statistical Disjointness: there exists a Probabilistic Polynomial Time (PPT) algorithm S such that:*

$$Disj_{DPKE,S}(\lambda) := \max_{(\mathsf{sk},\mathsf{pk})\leftarrow\mathsf{KGen}(1^\lambda)} \Pr[c \in \mathsf{Enc}_{\mathsf{pk}}(M) | c \leftarrow S(\mathsf{pk})]$$

  is negligible.
- *Ciphertext Indistinguishability: for any PPT adversary A there exists a PPT algorithm S such that:*

$$Adv_{DPKE,\mathcal{D}_M,A,S} := \left| \begin{array}{l} \Pr\left[A(\mathsf{pk}, c^\star) \to 1 \middle| \begin{array}{c}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda), m^\star \leftarrow \mathcal{D}_M; \\ c^\star \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m^\star)\end{array}\right] \\ - \Pr\left[A(\mathsf{pk}, c^\star) \to 1 | (\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda), c^\star \leftarrow S(\mathsf{pk})\right] \end{array} \right|$$

  is negligible.

Our proposal as defined in Section 4 is not a DPKE. The first step required is to make it deterministic by simply adding the error e as an input to the encryption algorithm, precisely defining $\mathrm{DPKE}_{new} = (\mathsf{KGen}, \mathsf{Enc}'', \mathsf{Dec}'')$ as follows:

$\underline{\mathsf{KGen}(1^\lambda)}$

$k, n, m, \delta, t \leftarrow \mathrm{ParamSelect}(1^\lambda)$
$G \leftarrow \mathrm{GenGabCode}(k, n, m)$
$S \leftarrow_\$ GL_k(\mathbb{F}_{2^m})$
$V \leftarrow_\$ \{\mathcal{V} \subset \mathbb{F}_{2^m} | \dim(\mathcal{V}) = \delta\}$
$P \leftarrow_\$ GL_n(V)$
return $\mathsf{sk} = (G, S, P)$,
$\mathsf{pk} = G_{pub} = SGP^{-1}$

$\underline{\mathsf{Enc}''_{\mathsf{pk}}(x, e)}$

$x^* \leftarrow x || H'(e, x)$
$y \leftarrow (x^* + H(e))G_{pub} + e$
return y

$\underline{\mathsf{Dec}''_{\mathsf{sk}}(y)}$

$(x', e') \leftarrow decode_{\mathsf{sk}}(yP)$
if $(x', e') = \perp$
  return $\perp$
else
  $x||v = x' + H(e')$
  if $H'(e', x) \neq v$ and
    $\mathsf{rk}(e') \neq t$
    return $\perp$
  else
    return (x, e')

Now we assume the error received as input in the encryption function is of rank t, and the *ParamSelect* function chooses as defined before: $t = \lfloor (n-k)/(2\delta) \rfloor$.

Theorem 1. *The DPKE scheme* $\mathrm{DPKE}_{new} = (\mathsf{KGen}, \mathsf{Enc}'', \mathsf{Dec}'')$*, with message space* M *and ciphertext space* C*, is* $\mathcal{D}_M$*-disjoint simulatable.*

Proof (Theorem 1). From [27, Lemma 3.1], it is sufficient to prove sparseness and pseudorandomness. The first property is proved by showing the following value

$$\mathrm{Sparse}_{\mathrm{DPKE}} := \max_{(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KGen}()} \frac{|\mathsf{Enc}_{\mathsf{pk}}(M)|}{|C|} \tag{1}$$

to be negligible. In order to show that, lets denote by E the set of vectors of rank weight less than or equal to t in $\mathbb{F}_{2^m}^n$. Every component e_i of a vector $e \in E$ is a vector of a vectorial subspace of $V \subset \mathbb{F}_2^m$ of dimension t. The number of vectorial subspaces of $\mathbb{F}_2^m$ of dimension t is $\prod_{i=0}^{t-1}(2^m - 2^i)/(2^t - 2^i)$. We now have 2^t choices for each of the n components of e. Thus, we deduce that

$$|E| = 2^{tn} \prod_{i=0}^{t-1} \frac{2^m - 2^i}{2^t - 2^i}.$$

The code generated by G_{pub} possesses 2^{km} different codewords. Hence,

$$|\mathsf{Enc}_{\mathsf{pk}}(M)| = 2^{km+tn} \prod_{i=0}^{t-1} \frac{2^m - 2^i}{2^t - 2^i}.$$

Notice that encryptions with an error of rank less than t are included in this computation of $|\mathsf{Enc}_{\mathsf{pk}}(M)|$. These errors are not part of the encrypted ciphertext space, but it simplifies the computation and gives a sufficient upper bound. Finally, it is easy to see that $|C| = 2^{nm}$, therefore

$$\mathrm{Sparse}_{\mathrm{DPKE}} \leq 2^{n(t-m)+km} \prod_{i=0}^{t-1} \frac{2^m - 2^i}{2^t - 2^i}.$$

Considering the parameter sets provided in Table 1 we obtain the upper bound $\mathrm{Sparse}_{\mathrm{DPKE}} < 2^{-1390}$, which is negligible.

To prove the second part of the claim, pseudorandomness, we need to prove that we can see a ciphertext as a random value. First, let us exhibit a probability distribution from which an error $e \in \mathbb{F}_{2^m}^n$ of a given rank $t > 0$ can be sampled. One way to construct such an e is: sample t vectors $b_1, \ldots, b_t \in \mathbb{F}_2^m$ uniformly at random and draw n different sets of coefficients $\gamma_{1,i}, \ldots, \gamma_{t,i} \in \mathbb{F}_2, i \in \{1, \ldots, n\}$, all equally likely to be 0 or 1. Then we define e as

$$e = (\gamma_{1,1}b_1 + \ldots + \gamma_{t,1}b_t, \ldots, \gamma_{1,n}b_1 + \ldots + \gamma_{1,n}b_t).$$

Note that e is simply given by scalar multiplications and linear combinations of random variables following the uniform distribution over $\mathbb{F}_{2^m}^n$ (for the b_is) or

over $\{0,1\}$ (the $\gamma_{i,j}$). Hence, e can be efficiently sampled by a combination of those distributions which we will denote by $\mathcal{E}_t^n$.

From the discussion above, we can observe that, for $e \leftarrow \mathcal{E}_t^n$, $\mathsf{rk}(e) \leq t$. The case where $\mathsf{rk}(e) < t$ corresponds to the fact that $b_1, \ldots, b_t$ does not form a basis of the vector space of $\mathbb{F}_2^t$. That is, $b_{i+1} \in \text{span}(b_1, \ldots, b_i)$, for some $i < t$. Then, the probability of $\mathsf{rk}(e) < t$ is bounded above by $1/2^m + \ldots + 2^{t-1}/2^m = 2^{t-1}/2^m$. That probability is negligible given that $m \gg t$, which is the case for the set of parameters of our scheme (at maximum 2^{-63}).

Now, we can proceed with the following transformation:

- We can replace $c = xG_{pub} + e$ by $c = xG' + e$ where G' is a random $k \times n$ matrix over $\mathbb{F}_{2^m}$ because of the complexity of distinguishing the public code from a random code makes it unfeasible for a PPT adversary.
- We replace e with a random e' following the distribution described above.
- Now we can replace c by a random vector assuming the hardness of DRSD.

□

Lemma 1. *The public-key encryption scheme* $\text{DPKE}_{new} = (\mathsf{KGen}, \mathsf{Enc}'', \mathsf{Dec}'')$ *with message space* M *and ciphertext space* $\mathcal{C}$ *has perfect correctness.*

Proof. Let us assume

$$\exists c \in \mathcal{C} \mid c = \mathsf{Enc}''_{\mathsf{pk}}(x, e) \wedge c = \mathsf{Enc}''_{\mathsf{pk}}(x', e') \wedge (x \neq x' \vee e \neq e').$$

We can see $c = x_c G_{pub} + e$ where $x_c = \mathcal{F}(x, e) = (x || H'(e, x)) + H(e)$. Given that decoding is a deterministic function where $decode_{\mathsf{sk}}(c) = (x_c, e)$, then the values x_c and e are fixed for ciphertext c. Therefore, if such c exists, it means that $\exists x_c \in \mathbb{F}_{2^m}^k \mid x_c = \mathcal{F}(x, e) \wedge x_c = \mathcal{F}(x', e)$. Given that function $\mathcal{F}(x, e)$, as presented above, have, as leftmost bits, x XORed with $H(e)$, it is not possible for the output to be the same value when it receives the inputs (x, e) and (x', e) unless $x = x'$. Hence, the claim follows. □

As a last note, in the decryption algorithm we check that $\mathsf{rk}(e')$ equals t or not, in order to avoid possible decryption failures who might cause reaction attacks.

5.1 Security proof

In order to demonstrate our proposal to be IND-CCA-secure we use game-hopping proof technique. The first step for us is to define $\text{Game}_0^{\mathcal{A}}(1^\lambda)$ by copying the description of the experiment $\text{Exp}_{E,\mathcal{A}}^{\text{ind-atk}-b}(\lambda)$ where atk = cca. Apart from it, we add the encryption and decryption algorithms from PKE_{new}, defined in Section 4, which are used by the challenger to respond adversary queries $\mathcal{A}^{\mathsf{Enc}'_{\mathsf{pk}}(.)}(x_b)$, $\mathcal{A}_1^{\mathsf{Dec}'_{\mathsf{sk}}(.)}(\mathsf{pk})$, and $\mathcal{A}_2^{\mathsf{Dec}'_{\mathsf{sk}}(.)}(x_0, x_1, s, y)$.

$\text{Game}_0^{\mathcal{A}}(1^\lambda)$	$\mathsf{Enc}'_{\mathsf{pk}}(x)$	$\mathsf{Dec}'_{\mathsf{sk}}(y)$
$(\mathsf{pk},\mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$	$e \leftarrow\!\!\$\ \{z \in \mathbb{F}_{2^m}^n \mid \mathsf{rk}(z) = t\}$	$(x', e') \leftarrow decode_{\mathsf{sk}}(yP)$
$(x_0, x_1) \leftarrow \mathcal{A}_1^{\mathsf{Dec}'_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$	$x^* = x \mid\mid H'(e, x)$	**if** $(x', e') = \perp$
$y \leftarrow \mathcal{A}^{\mathsf{Enc}'_{\mathsf{pk}}(\cdot)}(x_b)$	$y \leftarrow (x^* + H(e))G_{pub} + e$	**return** $\perp$
$b' \leftarrow \mathcal{A}_2^{\mathsf{Dec}'_{\mathsf{sk}}(\cdot)}(x_0, x_1, y)$		**else**
return b'		$x \mid\mid v = x' + H(e')$
		if $H'(e', x) \neq v$ and $\mathsf{rk}(e') \neq t$
		return $\perp$
		else
		return x

The transition from $\text{Game}_0^{\mathcal{A}}$ to $\text{Game}_1^{\mathcal{A}}$ is basically a modification to show how Enc' and Dec' use Enc'' and Dec'' from the DPKE_{new}.

$\text{Game}_1^{\mathcal{A}}(1^\lambda)$	$\mathsf{Enc}'_{\mathsf{pk}}(x)$	$\mathsf{Dec}'_{\mathsf{sk}}(y)$
$(\mathsf{pk},\mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$	$e \leftarrow\!\!\$\ \{z \in \mathbb{F}_{2^m}^n \mid \mathsf{rk}(z) = t\}$	$(x', e') \leftarrow \mathsf{Dec}''_{\mathsf{sk}}(y)$
$(x_0, x_1) \leftarrow \mathcal{A}_1^{\mathsf{Dec}'_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$	$y \leftarrow \mathsf{Enc}''_{\mathsf{pk}}(x, e)$	**if** $(x', e') \neq \perp$
$y \leftarrow \mathcal{A}^{\mathsf{Enc}'_{\mathsf{pk}}(\cdot)}(x_b)$		**return** x'
$b' \leftarrow \mathcal{A}_2^{\mathsf{Dec}'_{\mathsf{sk}}(\cdot)}(x_0, x_1, y)$		**else**
return b'		**return** $\perp$

$\text{Game}_1^{\mathcal{A}}$ is the same as $\text{Game}_2^{\mathcal{A}}$ except that

$\text{Game}_2^{\mathcal{A}}(1^\lambda)$	$\mathsf{Enc}'_{\mathsf{pk}}(x)$	$\mathsf{Dec}'_{\mathsf{sk}}(y)$
$(\mathsf{pk},\mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$	$e \leftarrow\!\!\$\ \{z \in \mathbb{F}_{2^m}^n \mid \mathsf{rk}(z) = t\}$	$(x', e') \leftarrow \mathsf{Dec}''_{\mathsf{sk}}(y)$
$(x_0, x_1) \leftarrow \mathcal{A}_1^{\mathsf{Dec}'_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$	$y \leftarrow \mathsf{Enc}''_{\mathsf{pk}}(x, e)$	**if** $y = \mathsf{Enc}''_{\mathsf{pk}}(x', e')$
$y \leftarrow \mathcal{A}^{\mathsf{Enc}'_{\mathsf{pk}}(\cdot)}(x_b)$		**return** x'
$b' \leftarrow \mathcal{A}_2^{\mathsf{Dec}'_{\mathsf{sk}}(\cdot)}(x_0, x_1, y)$		**else**
return b'		**return** $\perp$

The transition from $\text{Game}_2^{\mathcal{A}}$ to $\text{Game}_3^{\mathcal{A}}$ consists on changing the interaction from the challenger $\mathcal{A}^{\mathsf{Enc}'_{\mathsf{pk}}(\cdot)}(x_b)$ for a random value in $\mathbb{F}_{2^m}^n$.

$\text{Game}_3^{\mathcal{A}}(1^\lambda)$	$\mathsf{Enc}_{\mathsf{pk}}(x)$	$\mathsf{Dec}_{\mathsf{sk}}(y)$
$(\mathsf{pk},\mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$	$e \leftarrow\!\!\$\ \{z \in \mathbb{F}_{2^m}^n \mid \mathsf{rk}(z) = t\}$	$(x', e') \leftarrow \mathsf{Dec}''_{\mathsf{sk}}(y)$
$(x_0, x_1, s) \leftarrow \mathcal{A}_1^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$	$y \leftarrow \mathsf{Enc}''_{\mathsf{pk}}(x, e)$	**if** $y = \mathsf{Enc}''_{\mathsf{pk}}(x', e')$
$y \leftarrow\!\!\$\ \mathbb{F}_{2^m}^n$		**return** x'
$b' \leftarrow \mathcal{A}_2^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(x_0, x_1, s, y)$		**else**
return b'		**return** $\perp$

Lemma 2. *The transition from $Game_0$ to $Game_1$ has*

$$\Pr[Game_0 = 1] = \Pr[Game_1 = 1]$$

Proof. The operations in Enc' algorithm are the same in both games. In the case of Dec', it uses the same operations but validates the information more times. Hence, the probability remains the same. □

Lemma 3. *The transition from $Game_1$ to $Game_2$ has*

$$\Pr[Game_1 = 1] = \Pr[Game_2 = 1]$$

Proof. Given that $\text{DPKE}_{new} = (\mathsf{KGen}, \mathsf{Enc}'', \mathsf{Dec}'')$ has perfect correctness, as proved in Lemma 1, checking if $(x', e') \neq \perp$ would have exactly the same result as checking if $y = \mathsf{Enc}''_{\mathsf{pk}}(x', e')$. Therefore, the probability remains the same. □

Lemma 4. *The adversary $\mathcal{A}$ would not be able to distinguish if she is playing in $Game_2$ or in $Game_3$ and*

$$\mathsf{Adv}^{\text{game}_3}_{PKE_{new},\mathcal{A}}(\lambda) = \mathsf{Adv}^{\text{game}_2}_{PKE_{new},\mathcal{A}}(\lambda) + Disj_{DPKE,S}(\lambda)$$

Proof. Given that $\text{DPKE}_{new} = (\mathsf{KGen}, \mathsf{Enc}'', \mathsf{Dec}'')$ with message space M is $\mathcal{D}_M$-disjoint simulatable as proved in Lemma 1, the encryption algorithm can be seen as a pseudorandom generator receiving as input $x \in M$ and $e \in E$. Given that $|M| \approx 2^{(k-2)m}$ and $|E| > 2^{486}$, the adversary $\mathcal{A}$ would not be able to distinguish if the oracle $\mathsf{Enc}'_{\mathsf{pk}}(.)$ retrieves $y = \mathsf{Enc}'_{\mathsf{pk}}(x_b)$ or $y \leftarrow_{\$} \mathcal{C}$. Therefore, the additional advantage from the previous game is based on the probability of distinguishing between a valid and an invalid ciphertext which is $\text{Disj}_{\text{DPKE},S}(\lambda)$. □

If an adversary is not able to distinguish between a random value and the result of the encryption algorithm, this basically means that regardless of the cleartext, the adversary does not learn anything from a ciphertext, not even if it is a proper encryption or not. However, there exist other attacks able to retrieve information from a code and, in these cases, adversary capabilities define the advantage to succeed in the IND-CCA experiment.

Theorem 2 (Security in the ROM). *Given the PKE scheme* DPKE_{new}*, for any* IND-CCA *adversary $\mathcal{A}$ without quantum capabilities*

$$\Pr\left[\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1\right] \approx \frac{1}{2},$$

where $\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1$ *is the event in which $b' = b$.*

Proof. As we have already seen, $\mathcal{A}$ could not distinguish between $\text{Exp}^{\text{IND-CCA}}_{E,\mathcal{A}}(\lambda)$ and Game_3. This means

$$\Pr\left[\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1\right] = \frac{1}{2} + \text{Adv}^{Game_3}_{PKE_{new},\mathcal{A}}(\lambda)$$

where

$$\mathsf{Adv}^{\text{game}_3}_{PKE_{new},\mathcal{A}}(\lambda) = \mathsf{Adv}^{\text{game}_2}_{PKE_{new},\mathcal{A}}(\lambda) + \text{Disj}_{\text{DPKE},S}(\lambda).$$

Given the security parameters defined in Section 4 we have that, for the lowest security parameters, the best algorithm to obtain the cleartext without knowledge of sk has complexity 2^{130}. Therefore

$$\mathsf{Adv}^{\text{game}_2}_{PKE_{new},\mathcal{A}}(\lambda) = 2^{-124}.$$

Hence,

$$\Pr\left[\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1\right] = \frac{1}{2} + 2^{-130} + 2^{-1390} \approx \frac{1}{2}$$

□

In order to provide proper bounds for a quantum adversary with access to semi-oracles as defined in [3], we need to recall the lemma for searching in an unstructured function [3, Lemma 2] based on the original O2H lemma [28] from Unruh.

Lemma 5 (Search in unstructured function). *Let H be a random function, drawn from a distribution such that $\Pr[H(x) = 1] \leq \lambda$ for all x. Let $\mathcal{B}$ be a q-query adversary with query depth d. Then*

$$\Pr\left[H(x) = 1 | b \leftarrow \mathcal{B}^{H()}\right] \leq 4(d+2)(q+1)\lambda.$$

The proof of this lemma is in [3, Section 4.1].

Theorem 3 (Security in the QROM). *Given the PKE scheme* DPKE_{new}*, for any* IND-CCA *q-query adversary $\mathcal{A}$ with query depth d and access to a quantum oracle*

$$\Pr\left[\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1\right] \approx \frac{1}{2},$$

where $\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1$ *is the event in which $b' = b$.*

Proof. As in the previous theorem, we first have that by indistinguishability from $\mathcal{A}$ perspective

$$\Pr\left[\text{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1\right] = \frac{1}{2} + \mathsf{Adv}^{\text{game}_3}_{PKE_{new},\mathcal{A}}(\lambda)$$

where

$$\text{Adv}^{Game_3}_{PKE_{new},\mathcal{A}}(\lambda) = \text{Adv}^{Game_2}_{PKE_{new},\mathcal{A}}(\lambda) + \text{Disj}_{\text{DPKE},S}(\lambda).$$

Given that $\mathcal{A}$ now have access to a quantum oracle, then her advantage is given by the hardness of solving the BDR problem. As stated in Section 4 the minimum security level would achieve 78bits of security. Moreover, from the previous Lemma 5 we can also bound the probability of finding x from $\mathsf{Enc}''_{\mathsf{pk}}(x, e)$ because the encryption function can be seen as a pseudorandom number generator. So, given that x_0 and x_1 are fixed, the adversary would have a bound defined by

$$\Pr\left[\mathsf{Enc}'_{\mathsf{pk}}(x_0, e) = y \mid y \leftarrow \mathcal{A}^{\mathsf{Enc}'()}\right] \leq 4(d+2)(q+1)2^{-486}.$$

Notice that, we consider only x_0 option and try to find a proper error. If it is not found, then the plaintext message would be x_1. Therefore, we have

$$\mathrm{Adv}^{Game_2}_{PKE_{new},\mathcal{A}}(\lambda) \leq 2^{-81} + 4(d+2)(q+1)2^{-553}.$$

Hence,

$$\Pr\left[\mathrm{Exp}^{\text{IND-CCA}}_{PKE_{new},\mathcal{A}}(\lambda) = 1\right] = \frac{1}{2} + 2^{-81} + 2^{-1390} + 4(d+2)(q+1)2^{-486} \approx \frac{1}{2}$$

□

5.2 Performance and comparison

We have implemented our IND-CCA-secure PKE scheme with the parameters of 128 bits of security. We use SHA-3-256 and SHAKE-128 implementations of the Open Quantum Safe project [22] for the functions H' and H respectively. All the tests have been run in a Macbook Pro with an Intel Core i7 processor at 2.9 Ghz. In Table 2[4], we compared the original implementation of [1] with both the original and the new parameters detailed in Section 4. This modification already provides a 50% increase on the amount of operations per second for encryption and a 100% for decryption. In the same table we also provide the performance information on our IND-CCA-secure version using our proposed parameters. We did not provide information about key generation as the algorithm has not been modified in our transformation.

	[1]	[1] New params	[2]
Encryption	21587 ops/s	30478 ops/s	23619 ops/s
Decryption	1127 ops/s	2207 ops/s	2108 ops/s

Table 2. Performance comparison for 128 bits security against quantum attackers between original implementation, original implementation with our new parameters, and our IND-CCA proposal.

Considering the same parameters for 128 bits of quantum security, the encryption operation is a bit slower than the non-IND-CCA-secure version. As a consequence, the number of encryptions per second are now reduced around 23%. This is because the encryption is a really fast operation, therefore, adding the computation of two hashes has a significant cost given that the rest of operations are a simple multiplication of two (small) matrices and several XOR operations. On the other hand, the decryption is only affected by a 5% because the cost of

[4] The parameters presented in this version of the paper slightly differ from the ones in [2], due to the fact that a new attack [5] has been published since AFRICACRYPT 2019. We plan to update Table 2 with the performance corresponding to the parameters presented in this paper.

the decryption operation is largely dominated by the decoding procedure so, the two hashes do not increase significantly the time taken by the operation.

Next, we would like to stress on the difference between our new scheme and the ones that could be obtained by using the generic transformation from OW-CPA to IND-CCA of [18] or from [27]. First, both transformations end up building an IND-CCA KEM instead of a PKE. These transformations require two extra hashes during the encapsulation and an additional re-encryption operation during the decapsulation. In the case of Loidreau's scheme, it would translate as a total of four extra hashes and a matrix multiplication for each encryption / decryption. Our scheme does not seem to need this additional matrix multiplication. Unfortunately, the available decoding algorithms for Gabidulin do not allow us to avoid this matrix multiplication. Indeed, the Welsh-Berlekamp [19] and Gao-like [29]) approaches directly output the message xS during the decryption procedure while the Berlekamp-Massey-like [17] algorithms outputs the error multiplied by the masking matrix eP. Hence, in both strategies, we have to compute a matrix multiplication to recover the original error which was added to the ciphertext during the encryption. Thus, the operations required for decryption in our scheme ended up having the same cost as in the generic transformations. However, this could change if a different decoding technique avoids these extra matrix multiplications.

Taking into consideration that our implementation is thread safe, and that we do not use the rest of the processors, these 23619 encryptions per second can easily be multiplied by 6. Therefore, the performance figures presented here make our scheme usable in practical applications. Moreover, our proposal can be used as a KEM like most of the proposals for NIST competition, but it can also be used for other purposes where the larger message space would allow to encrypt something bigger than just a key for each ciphertext. In fact, the message space is big enough to embed a few ciphertext from elliptic curve cryptography, and use our proposed scheme as a protection against quantum attacks. This way, many keys could be distributed using only one post quantum encryption.

6 Conclusions

We have presented an IND-CCA-secure version of Loidreau's public key encryption scheme. This proposal is usable for encrypting large messages as it can encrypt plaintexts of size 224, 384 or 448 bytes for a corresponding level of security of 128, 192 and 256 bits. Our proposal presents a overhead of 23% in the computational cost for encryption when compared to the original Loidreau's scheme. Thus, the new cryptosystem is still practical. Moreover, the transformation in the decryption has a similar cost as other transformations such as Hofheniz et al. [18] or Saito et al. [27]. Nevertheless, in our case, the cost of the decryption might be reduced by using an alternative decoding method able to retrieve both the codeword and error without requiring an additional matrix multiplication. As it is, the security proof relies on some properties which are specific for the Loidreau's scheme. Though, it is likely that our transformation might be adapted

or generalized to other post-quantum schemes, even in different settings, such as lattices. We leave this generalization as a future work.

References

1. Al Abdouli, A., Al Ali, M., Bellini, E., Caullery, F., Hasikos, A., Manzano, M., Mateu, V.: Drankula, a McEliece-like rank metric based cryptosystem implementation. In: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, ICETE 2018 - Volume 2: SECRYPT. pp. 230–241 (2018)
2. Al Shehhi, H., Bellini, E., Borba, F., Caullery, F., Manzano, M., Mateu, V.: An ind-cca-secure code-based encryption scheme using rank metric. In: International Conference on Cryptology in Africa. pp. 79–96. Springer (2019)
3. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. Cryptology ePrint Archive, Report 2018/904 (2018), https://eprint.iacr.org/2018/904
4. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.: A new algorithm for solving the rank syndrome decoding problem. In: IEEE International Symposium on Information Theory, ISIT. pp. 2421–2425 (2018)
5. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.P.: An algebraic attack on rank metric code-based cryptosystems. arXiv preprint arXiv:1910.00810 (2019)
6. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Advances in Cryptology - CRYPTO '98. LNCS, vol. 1462, pp. 26–45 (1998)
7. Bernstein, D.J., Buchmann, J., Dahmen, E.: Post Quantum Cryptography. Springer Publishing Company, Incorporated, 1st edn. (2008)
8. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 41–69. Springer (2011)
9. Coggia, D., Couvreur, A.: On the security of a Loidreau's rank metric code based encryption scheme. arXiv preprint arXiv:1903.02933 (2019)
10. Czajkowski, J., Bruinderink, L.G., Hülsing, A., Schaffner, C., Unruh, D.: Post-quantum security of the sponge construction. In: International Conference on Post-Quantum Cryptography. pp. 185–204. Springer (2018)
11. Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography (extended abstract). In: Proceedings of the 23rd Annual ACM Symposium on Theory of Computing. pp. 542–552 (1991)
12. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Annual International Cryptology Conference. pp. 537–554. Springer (1999)
13. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problems of Information Transmission (English translation of Problemy Peredachi Informatsii) **21**(1) (1985)
14. Gabidulin, E.M., Paramonov, A., Tretjakov, O.: Ideals over a non-commutative ring and their application in cryptology. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 482–489. Springer (1991)
15. Gaborit, P., Hauteville, A., Phan, D.H., Tillich, J.: Identity-based encryption from codes with rank metric. In: Advances in Cryptology – CRYPTO 2017. LNCS, vol. 10403, pp. 194–224 (2017)

16. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Transactions on Information Theory **62**(2), 1006–1019 (2016)
17. Gadouleau, M., Yan, Z.: Complexity of decoding Gabidulin codes. In: 42nd Annual Conference on Information Sciences and Systems, CISS 2008. pp. 1081–1085 (2008)
18. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. In: Theory of Cryptography Conference. pp. 341–371. Springer (2017)
19. Loidreau, P.: A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In: Coding and Cryptography. pp. 36–45 (2006)
20. Loidreau, P.: A new rank metric codes based encryption scheme. In: International Workshop on Post-Quantum Cryptography. pp. 3–17. Springer (2017)
21. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report pp. 114–116 (January and February 1978)
22. Mosca, M., Stebila, D., Contributors: Open quantum safe (2017), https://openquantumsafe.org/
23. NIST: Federal inf. process. stds. (nist fips) - 202 (2015), https://dx.doi.org/10.6028/NIST.FIPS.202
24. NIST: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (2016), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
25. Nojima, R., Imai, H., Kobara, K., Morozov, K.: Semantic security for the McEliece cryptosystem without random oracles. Des. Codes Cryptography **49**(1-3), 289–305 (2008)
26. Overbeck, R.: Structural attacks for public-key cryptosystems based on Gabidulin codes. Journal of Cryptology **21**(2), 280–301 (2008)
27. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 520–551. Springer (2018)
28. Unruh, D.: Revocable quantum timed-release encryption. J. ACM **62**(6), 49:1–49:76 (2015)
29. Wachter-Zeh, A.: Decoding of block and convolutional codes in rank metric. Ph.D. thesis, Université Rennes 1 (2013), https://tel.archives-ouvertes.fr/tel-0105674