REDOG and Its Performance Analysis*

Jon-Lark Kim[1], Jihoon Hong[2], Terry Shue Chien Lau[3], YounJae Lim[4], Chik How Tan[5], Theo Fanuela Prabowo[6], and Byung-Sun Won[7]

[1] Sogang University
jlkim@sogang.ac.kr
[2] Sogang University
rjekfl@sogang.ac.kr
[3] Multimedia University
terry.lau@mmu.edu.my
[4] DeepHelix Corp.
yjlim@deephelix.net
[5] National University of Singapore
tsltch@nus.edu.sg
[6] National University of Singapore
tsltfp@nus.edu.sg
[7] Sogang University
bswon@deephelix.net

Abstract. We propose a REinforced modified Dual-Ouroboros based on Gabidulin codes, shortly called REDOG. This is a code-based cryptosystem based on the well-known rank metric codes, Gabidulin codes. The public key sizes of REDOG are 14KB, 33KB, 63KB at the security levels of 128, 192, 256 bits respectively. There is no decoding failure in decryption. REDOG is IND-CPA. As a new result, we give the performance results of implementing REDOG including the time for Key generation, encryption, and decryption for each security level.

Keywords: Modified Dual-Ouroboros · Gabidulin code · λ-dimensional subspace.

1 Introduction

1.1 Design rationale

The original version of McNie series called McNie [13] had the features of both McEliece and Niederreiter cryptosystem and was designed to be secure against known structural attacks on code-based cryptosystems. Gaborit [14] suggested a message recovery attack which reduced the dimension of a random code in the public key. The security level of McNie decreased by almost a factor of 2, and the original parameters suggested for McNie suffer from relatively high

* This work is submitted to 'Korean Post-Quantum Cryptography Competition' (www.kpqc.or.kr). Jon-Lark Kim is a principal investigator.

decryption failure probability since LRPC (low rank parity check codes) decoding is a probabilistic decoding algorithm.

To overcome those disadvantages, Dual-Ouroboros which is a modification of McNie was proposed [7]. It was a non-cyclic dual version of Ouroboros-R [2], which also employed the LRPC codes. Kim et al. [8] suggested a modified Dual-Ouruboros(DO.Gab-PKE), which is a variant of Dual-Ouroboros obtained by replacing LRPC codes from Dual-Ouroboros by Gabidulin codes over $\mathbb{F}_{q^m}$. Gadibulin $[n, k]$ codes have advantage of the zero-decoding failure probability and have a fast decoding complexity of $O(n^2)$ operations over $\mathbb{F}_{q^m}$[11] and an improved decoding complexity of $O(nm^2 \log m)$ operations over the ground field $\mathbb{F}_q$ [17]. Moreover, the modified DO.Gab-PKE using Gabidulin codes provides a much stronger security against known plaintext-recovery attacks, including Overbeck's attack [15]. It was also shown in [8] that the DO.Gab-PKE achieves $\mathsf{IND-CPA}$ security, and the parameters achieve relatively lower key sizes compared to the other code-based PKE that has no decryption failure.

However, the modified DO.Gab-PKE did not specify the selection of secret key S to ensure the security of the modified DO.Gab-PKE. If the secret key S is invertible over $\mathbb{F}_{q^m}$ without any restriction, then the modified DO.Gab-PKE would be incorrect. If S is invertible over $\mathbb{F}_q$ without any restriction, the modified DO.Gab-PKE would be insecure. Therefore, we need to select S specifically so that the modified DO.Gab-PKE can be secure. This reinforced version was called the modified DO.Gab[Λ]-PKE in [10]. Therefore, in this proposal, we describe the modified DO.Gab[Λ]-PKE in [10], which is shortly called REDOG meaning a **RE**inforced modified **D**ual-**O**uroboros based on **G**abidulin codes.

1.2 Advantages and limitations

REDOG adopts the same scheme as the modified DO.Gab-PKE [8] and just clearly specifies how to select the secret key S in order to avoid the Frobenius weak attack [9]. By using the same encryption algorithm, the structural stability of the algorithm and the resistance to known attacks can be brought as it is. Moreover, by selecting the secret key S to be invertible matrix over a λ-dimensional subspace of $\mathbb{F}_{q^m}$, the public key matrix does not generate a r-Frobenius weak code [12]. Such an approach results in larger key size, for instance 14.25 KB of public key size required to achieve the 128-bit security level.

2 Preliminaries

In this section, we introduce necessary concepts and results on rank metric codes.

2.1 Rank metric codes

Let q be a prime power and $\mathbb{F}_{q^m}$ be the finite field with q^m elements. Consider a basis $\{\beta_1, ..., \beta_m\}$ of $\mathbb{F}_{q^m}$ over the base field $\mathbb{F}_q$.

Definition 1. An $[n, k]$ linear code of length n and dimension k is a linear subspace $\mathcal{C}$ of the vector space $\mathbb{F}_{q^m}^n$, i.e. $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Let $l \leqslant k$, then an $[n, l]$ linear subcode $\mathcal{C}'$ is an $[n, l]$ linear code such that $\mathcal{C}' \subseteq \mathcal{C}$.

Definition 2. Let $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{F}_{q^m}^n$. For each $1 \leqslant j \leqslant n$, $x_j = \sum_{i=1}^{m} c_{ij}\beta_i$ where $c_{ij} \in \mathbb{F}_q$. The rank of $\mathbf{x}$ in $\mathbb{F}_q$, denoted by $\mathrm{rk}(\mathbf{x})$ is defined as $\mathrm{rk}(\mathbf{x})$=$\mathrm{rk}(X)$ where $X = [c_{ij}] \in \mathbb{F}_q^{m\times n}$.

2.2 Gabidulin codes and partial cyclic codes

Definition 3. Let $\mathbf{x} = (x_0, ..., x_{n-1}) \in \mathbb{F}_{q^m}^n$. The circulant matrix $\mathrm{Cir}_n(\mathbf{x})$ induced by $\mathbf{x}$ is defined as

$$Cir_n(\mathbf{x}) = \left[x_{i-j \pmod n}\right]_{ij} = \begin{bmatrix} x_0 & x_{n-1} & \cdots & x_1 \\ x_1 & x_0 & \cdots & x_2 \\ \vdots & \vdots & \vdots & \vdots \\ x_{n-1} & x_{n-2} & \cdots & x_0 \end{bmatrix}$$

The $k \times n$-partial circulant matrix induced by $\mathbf{x}$, denoted by $\mathrm{Cir}_k(\mathbf{x})$ is defined as the first k rows of $\mathrm{Cir}_n(\mathbf{x})$.

Lau and Tan [9] defined the following code generated by $\mathrm{Cir}_k(\mathbf{x})$.

Definition 4. An $[n, k]$-partial cyclic code $\mathsf{PC}_{n,k}[\mathbf{x}]$ generated by $\mathbf{x} \in \mathbb{F}_{q^m}^n$ is a linear code with generator matrix $\mathrm{Cir}_k(\mathbf{x})$

These circulant matrices will be used as generator matrices of Gabidulin codes as in Section 3.3 in order to reduce the key sizes.

The following are the definitions for Moore matrix and Gabidulin codes.

Definition 5. Denote $[l] = q^l$ as the lth Frobenius power for an integer l. A matrix $G = [G_{ij}] \in \mathbb{F}_{q^m}^{k\times n}$ is called a *Moore matrix* induced by $\mathbf{g}$ if there exists a vector $\mathbf{g} = (g_1, ..., g_n) \in \mathbb{F}_{q^m}^n$ such that the ith row of G is equal to $\mathbf{g}^{[i-1]} = (g_1^{[i-1]}, ..., g_n^{[i-1]})$ for $1 \leqslant i \leqslant k$, i.e., G is of the form

$$G = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \vdots & \vdots \\ g_1^{[n-1]} & g_2^{[n-1]} & \cdots & g_n^{[n-1]} \end{bmatrix}. \tag{1}$$

Similarly, we define $G^{[l]} = \left[G_{ij}^{[l]}\right]$. For any set $S \subset \mathbb{F}_{q^m}^n$, we denote $S^{([l])} = \{\mathbf{s}^{[l]} | \mathbf{s} \in S\}$

Definition 6. *(Gabidulin code)* Let $\mathbf{g} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(\mathbf{g}) = n \leqslant m$. The $[n, k]$ Gabidulin code $\mathrm{Gab}_{n,k}(\mathbf{g})$ over $\mathbb{F}_{q^m}^n$ of dimension k with generator vector $\mathbf{g}$ is the code generated by a Moore matrix G induced by $\mathbf{g}$ in the form of Equation (1).

Theorem 1. There exists a Moore Matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ such that H is a parity-check matrix of a Gabidulin code. In other words, the dual of a Gabidulin code also a Gabidulin code.

The error-correcting capability of $\mathrm{Gab}_{n,k}(\mathbf{g})$ is $r = \left\lfloor \frac{n-k}{2} \right\rfloor$. There exist efficient decoding algorithms for Gabidulin codes which are able to correct error up to rank r (for instance [11] with decoding complexity $5/2\ n^2 - 3/2\ k^2$).

Definition 7. *(r-Frobenius weak)* Let C be an $[n,k]$-linear code. We say that C is r-Frobenius weak if for some s relatively prime to m and for a generic $\mathbf{e} \in \mathbb{F}_{q^m}^n$ of rank r, the space U spanned by the elements of rank one in $C_{\mathsf{ext}} = \sum_{i=0}^{r-1} \left(C + \langle \mathbf{e} \rangle_{\mathbb{F}_{q^m}}\right)^{[si]}$, fulfills $C \cap U = \{0\}$.

The algorithm of Frobenius weak attack [9] is as follows.

Algorithm : **FrobeniusWeakAttack**

Data : $\mathbf{y} = \mathbf{m}G_{\mathsf{pub}} + \mathbf{e}$ (a ciphertext where $\mathbf{m}$ is the plaintext), the public key $\mathsf{pk} = G_{\mathsf{pub}}$ with parameter $r = \mathrm{rk}(\mathbf{e})$

Result : The plaintext $\mathbf{m}$

1 Construct the matrix

$$G_{\mathsf{pub,ext}} = \begin{bmatrix} G_{\mathsf{pub}} \\ \mathbf{y} \\ \vdots \\ G_{\mathsf{pub}}^{[r-1]} \\ \mathbf{y}^{[r-1]} \end{bmatrix}.$$

2 Compute the space $\mathcal{U}$ generated by the elements of rank one in $\mathcal{C}_{\mathsf{ext}} = \langle G_{\mathsf{pub,ext}} \rangle_{\mathbb{F}_{q^m}}$.

3 Compute $u = \dim_{\mathbb{F}_{q^m}}(\mathcal{U})$.

4 **if** $u \leqslant n - k$ **then**

5 Compute a parity-check matrix $H_U \in \mathbb{F}_q^{(n-u)\times n}$ for $\mathcal{U}$.

6 Solve $\mathbf{y}(H_U)^T - \mathbf{m}[G_{\mathsf{pub}}(H_U)^T]$ for $\mathbf{m}$,

7 **return** $\mathbf{m}$.

8 **else**

9 **return** $\perp$

---

3 Specification

We describe key generation, encryption, and decryption of REDOG [10] as follows.

Setup: Generate global parameters with integers m, n, l, r, k such that $l < n$ and $\lambda t \leqslant r \leqslant \left\lfloor \frac{n-k}{2} \right\rfloor$. Output parameters $= (m, n, l, k, r, \lambda, t)$.

Key.Gen: Let $[H_1 H_2]$ be a parity check matrix for a $[2n-k, n]$ Gabidulin code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, where $H_2 \in \mathrm{GL}_{n-k}(\mathbb{F}_{q^m})$. Let Φ_H be an efficient decoding algorithm for $\mathcal{C}$ with error correcting capability of $r = \left\lfloor \frac{n-k}{2} \right\rfloor$. Let $\mathcal{H}$ be a hash function from $\mathbb{F}_{q^m}^{2n-k}$ to $\mathbb{F}_{q^m}^{l}$.
Generate a generator matrix G for a random $[n, l]$ code over $\mathbb{F}_{q^m}$. Generate a random $n \times n$ isometric matrix P.
Generate a random λ-dimensional subspace, $\Lambda \subset \mathbb{F}_{q^m}$ such that $1 \in \Lambda$.
Generate a random $(n-k) \times (n-k)$ invertible matrix $S^{-1} \in \mathrm{GL}_{n-k}(\Lambda)$.
Output public key and secret key pair
$\mathsf{pk} = (G, F = GP^{-1}H_1^T[H_2^T]^{-1}S), \mathsf{sk} = (P, H, S, \Phi_H)$.

Enc($\mathsf{pk}, \mathbf{m}$): Let $\mathbf{m} \in \mathbb{F}_{q^m}^{l}$ be the plaintext message to be encrypted. Generate randomly vector $\mathbf{e} = (e_1, e_2) \in \mathbb{F}_{q^m}^{2n-k}$ such that $\mathrm{rk}(\mathbf{e}){=}t$, $e_1 \in \mathbb{F}_{q^m}^{n}$ and $e_2 \in \mathbb{F}_{q^m}^{n-k}$. Let $\mathbf{m}' = \mathbf{m} + \mathcal{H}(\mathbf{e})$. Compute $c_1 = \mathbf{m}'G + e_1, c_2 = \mathbf{m}'F + e_2$.
Output ciphertext $\mathbf{c} = (c_1, c_2)$.

Dec(sk, c): Compute

$$\begin{aligned} & c_1 P^{-1} H_1^T - c_2 S^{-1} H_2^T \\ & \quad = \mathbf{m}' G P^{-1} H_1^T + e_1 P^{-1} H_1^T - \mathbf{m}' G P^{-1} H_1^T [H_2^T]^{-1} S S^{-1} H_2^T - e_2 S^{-1} H_2^T \\ & \quad = e_1 P^{-1} H_1^T - e_2 S^{-1} H_2^T \\ & \quad = (e_1 P^{-1}, -e_2 S^{-1}) \begin{bmatrix} H_1^T \\ H_2^T \end{bmatrix} \end{aligned}$$

Let $\mathbf{e}' = (e_1 P^{-1}, -e_2 S^{-1})$. Since $\mathrm{rk}(\mathbf{e}') \leqslant r$, apply Φ_H to obtain $\mathbf{e}'$.
Compute $e_1 = e_1 P^{-1} P$ and $e_2 = e_2 S^{-1} S$ to obtain $\mathbf{e} = (e_1, e_2)$.
Finally, solve the system $\mathbf{m}' G = c_1 - e_1$ to recover $\mathbf{m} = \mathbf{m}' - \mathcal{H}(e)$.

3.1 Notation

All the notations for specification are given above.

3.2 Specification of REDOG

REDOG is a reinforced version of the modified Dual-Ouruboros with Gabidulin (DO.Gab-PKE) [8]. We explain how to select the invertible matrix S.

For the secret key S,

1. If $S \in \mathrm{GL}_{n-k}(\mathbb{F}_{q^m})$ and F is in echelon form, then the decryption algorithm of the modified DO.Gab-PKE is incorrect.
2. If $S \in \mathrm{GL}_{n-k}(\mathbb{F}_q)$, then the decryption algorithm of the modified DO.Gab-PKE can be performed correctly.

We can recover the secret key of the modified DO.Gab-PKE with $S \in \mathrm{GL}_{n-k}(\mathbb{F}_q)$ in polynomial time which is the case 2. Thus the modified DO.Gab-PKE is insecure if $S \in \mathrm{GL}_{n-k}(\mathbb{F}_q)$.

To overcome this bad choice of S, we give an example to show that the modified DO.Gab-PKE can be both correct and secure if we impose some conditions on the secret key S. In particular, we employs Loidreau's approach [12] to consider matrix S^{-1} over some λ-dimensional subspace $\Lambda \subset \mathbb{F}_{q^m}$, which is a subspace of $\mathbb{F}_{q^m}$ and its $\mathbb{F}_q$-dimension is λ. Note that by the choice of Λ, $S = (S^{-1})^{-1}$ is not necessarily a matrix over Λ.

Take S^{-1} as an $(n-k) \times (n-k)$ invertible matrix over Λ, where Λ is a λ-dimensional subspace of $\mathbb{F}_{q^m}$ which contains the element 1, and take the error $\mathbf{e}$ as a random vector of rank $t \leqslant \left\lfloor \frac{r}{\lambda} \right\rfloor$.

From the decryption process, since $\mathrm{rk}(\mathbf{e}) = t$ and Λ is a λ-dimensional subspace of $\mathbb{F}_{q^m}$, we have $\mathrm{rk}(\mathbf{e}') = \lambda t \leqslant r$, and thus, the decoding algorithm Φ_H can recover $\mathbf{e}'$ correctly.

3.3 Parameter sets

We present our proposed parameters for REDOG in Table 1. We consider G to be an $(l \times n)$-partial circulant matrix, and S^{-1} to be an $(n-k) \times (n-k)$ circulant matrix. The public key size is $\mathsf{size}_{\mathsf{pk}} = m(n + l(n-k))/8$ bytes, the secret key size is $\mathsf{size}_{\mathsf{sk}} = (n^2 + (3n-2k)m)/8$ bytes, and the ciphertext size is $\mathsf{size}_{\mathsf{ct}} = (2n-k)m/8$ bytes.

Table 1. Proposed parameters for REDOG

Instance	$(n, k, l, q, m, r, \lambda, t)$	$\mathsf{size}_{\mathsf{pk}}$	$\mathsf{size}_{\mathsf{sk}}$	$\mathsf{size}_{\mathsf{ct}}$	Security level
REDOG-1	(44,8,37,2,83,18,3,6)	14.25KB	1.45KB	0.83KB	128
REDOG-2	(58,10,49,2,109,24,3,8)	32.84KB	2.52KB	1.44KB	192
REDOG-3	(72,12,61,2,135,30,3,10)	62.98KB	3.89KB	2.23KB	256

In order to compare REDOG with other code-based algorithms such as HQC, BIKE, and Classic McEliece, all of which are based on Hamming metric and advanced to the 4th round of the NIST PQC competition, we display their security level and the corresponding key sizes of these algorithms.

Note that HQC and BIKE algorithms have decryption failure which is a disadvantage although their key sizes are much smaller than REDOG. REDOG does not have a decryption failure. Classic McEliece has no decryption failure

but has large public key size of 1047KB at the 128 bits of security level while REDOG has a much smaller public key size of 14KB. Therefore, REDOG is a strong competitor for HQC, BIKE, and Classic McEliece.

Table 2. Security level and key sizes of HQC [1]

Instance	pk size	sk size	ct size
hqc-128	2,249bytes	40bytes	4,481bytes
hqc-192	4,522bytes	40bytes	9,026bytes
hqc-256	7,245bytes	40bytes	14,469bytes

Table 3. Security level and key sizes of BIKE [3]

Quantity	Size	AES-128	AES-192	AES-256
Private key	$w\lceil log_2(r) \rceil$	2,130bits	2,296bits	4,384bits
Public key	n	20,326bits	43,786bits	65,498bits
Ciphertext	n	20,326bits	43,786bits	65,498bits

Table 4. Parameters, security level and key sizes of Classic McEliece [16]

Variant	n	m	t	$k = n - mt$	pk size	sk size	Security level
mceliece6960119	6960	13	119	5413	1047KB	13.6KB	128
mceliece8192128	8192	13	128	6528	1358KB	13.75KB	256

4 Performance analysis

The public key size for REDOG is larger than the public key size for the modified DO.Gab-PKE because we have to choose S specifically so that REDOG can be secure. In what follows, we describe the relation between parameters. As the rank of the error is now t instead of r, the error correcting capability r has to increase, resulting in the increase for the value of $n-k$. Moreover, for H to be a parity-check matrix of a $[2n-k, n]$-Gabidulin code, it is required that $m \geqslant 2n-k$. Moreover, the paremeter l is always larger than or equal to $n-k$. As $n-k$ increases, the values for m and l increase. Therefore, the public key size is larger than the public key of the modified DO.Gab-PKE.

4.1 Description of platform

To implement our REDOG cryptosystem, we used the following software and hardware platforms:

- SageMATH 9.2 version
- Python 3.7.7 version
- Visual studio 2019
- 3.8GHz Intel(R) Core(TM) i7 processor with 32GB of memory

4.2 Performance of reference implementation

The performance results of implementing the REDOG cryptosystem using the platform described above are as follows.

Table 5. Performance of REDOG

Instance	$(n, k, l, q, m, r, \lambda, t)$	$\mathsf{KeyGen}_{\mathsf{time}}$	$\mathsf{Enc}_{\mathsf{time}}$	$\mathsf{Dec}_{\mathsf{time}}$	Security level
REDOG-1	(44,8,37,2,83,18,3,6)	2.5 sec	0.035 sec	1.434 sec	128
REDOG-2	(58,10,49,2,109,24,3,8)	4.7 sec	0.06 sec	3.254 sec	192
REDOG-3	(72,12,61,2,135,30,3,10)	10.0 sec	0.1 sec	6.366 sec	256

5 Security

5.1 Security definition

Problem 2 ([10]) (Rank syndrome decoding (RSD) Problem) Let H be a full rank $(n-k)\times n$ matrix over $\mathbb{F}_{q^m}$, $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$, and r an integer. The Rank Syndrome Decoding problem $\mathrm{RSD}_H(q,m,n,k,r)$ is to determine a vector $x \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}(\mathbf{x}) = r$ and $\mathbf{s} = \mathbf{x}H^T$.

The RSD problem is analogous to the classical syndrome decoding problem in Hamming metric, which was shown to be an NP-complete problem. Gaborit and Zémor (2014) showed that if there were efficient probabilistic algorithms for solving the RSD problem, then there would exist efficient probabilistic algorithm to solve the syndrome decoding problem in Hamming metric.

Problem 2 ([8],[10]) Given a full rank $\ell \times n$ matrix G' and a matrix $F = G'H_1^T[H_2^T]^{-1}S$ where $[H_1H_2]$ is a parity-check matrix for a Gabidulin code, and S is an invertible matrix. This problem is to distinguish F from R where R is a random $\ell \times (n-k)$ matrix over $\mathbb{F}_{q^m}$.

Problem 3 ([8],[10]) (Decisional rank syndrome decoding (DRSD) problem) Let H be a full rank $(n-k)\times n$ matrix over $\mathbb{F}_{q^m}$, $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ and r an integer. The Decisional Rank Syndrome Decoding problem $\mathrm{DRSD}_H(q,m,n,k,r)$ is to distinguish the distribution $(H,\mathbf{s})$ where $\mathbf{s} = \mathbf{x}H^T$ and $x \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}(\mathbf{x}) = r$, from the distribution $(H,\mathbf{y})$ where $\mathbf{y}$ is a random vector in $\mathbb{F}_{q^m}^{n-k}$.

Problem 2 is a form of matrix factorization problem. The random invertible matrix S prevents Overbeck's attack from being used to attack Problem 2. Problem 3 is the decisional version of the RSD problem. Therefore, these two problems were suitable to be the candidates for the hard problems which the modified DO.Gab-PKE is based on.

Theorem 2. *Theorem 2 ([8, Theorem 1]) The modified DO.Gab-PKE is IND-CPA secure under the assumptions of Problems 2 and 3.*

5.2 Security strength categories

The below information is on table 1.

To achieve 128 security in our cryptosystem, we need 14.25KB for $\mathsf{size_{pk}}$, 1.45KB for $\mathsf{size_{sk}}$, and 0.83KB for $\mathsf{size_{ct}}$.

To achieve 192 security in our cryptosystem, we need 32.84KB for $\mathsf{size_{pk}}$, 2.52KB for $\mathsf{size_{sk}}$, and 1.44KB for $\mathsf{size_{ct}}$.

To achieve 256 security in our cryptosystem, we need 62.98KB for $\mathsf{size_{pk}}$, 3.89KB for $\mathsf{size_{sk}}$, and 2.23KB for $\mathsf{size_{ct}}$.

5.3 Cost of known attacks

1. $\mathsf{IND}-\mathsf{CPA}$ security: REDOG achieves $\mathsf{IND}-\mathsf{CPA}$ security. Kim et al. [8] has shown that the modified Do.Gab-PKE achieves $\mathsf{IND}-\mathsf{CPA}$ security, so does REDOG. The only difference is the secret matrix S. In REDOG, $S^{-1} \in \mathrm{GL}_{n-k}(\Lambda)$, distinguishing F from a random R is no longer an easy instance of Problem 2, in Lau et al. [9]. Thus, by Theorem 2 in Lau et al. [9], REDOG achieves $\mathsf{IND}-\mathsf{CPA}$ security.
2. Key recovery attack : In the key equation $FS^{-1}H_2^T = GP^{-1}H_1^T$, there are $2(n-k)^2$ unknown variables of quadratic power and $n(n-k)$ unknown linear variables. Even if we rewrite the key equation over $\mathbb{F}_q$, there are a total of $(n-k)^2m + (n-k)m$ unknown variables of quadratic power and nm unknown linear variables. It is generally difficult to solve such equations, i.e., the complexity to solve for the solution is of high exponential power.
3. Our plaintext recovery attack : Rewrite the public key matrix

$$G_{\mathsf{pub}} = [G \mid GP^{-1}H_1^T[H_2^T]^{-1}S] = GP^{-1}[I_n \mid H_1^T[H_2^T]^{-1}] \begin{bmatrix} P & \mathbf{0} \\ \mathbf{0} & S \end{bmatrix}$$

   Although the matrix $[I_n \mid H_1^T[H_2^T]^{-1}]$ is a generator matrix for a Gabidulin code, the right scramble matrix $\begin{bmatrix} P & 0 \\ 0 & S \end{bmatrix}$ does not preserve the Frobenius invariant subspace. This implies that the extension matrix G_{ext} is of full rank, i.e. $\mathrm{rk}(G_{\mathsf{ext}}) = 2n-k$. Therefore, G_{pub} noes not generate an r-Frobenius weak code. Thus REDOG resists the Frobenius weak attack [4]. We perform simulations of the Frobenius weak attack on REDOG and the simulation result confirms that REDOG is secure against Frobenius weak attack.
4. Message recovery attacks.
   An adversary acn try to recover the message by directly attacking the ciphertext. This is now an instance of Rank Syndrome Decoding(RSD) problem, i.e., the problem of decoding a noisy codeword from a random code. The following are the best known attacks for solving the RSD problem with parameters (n, k, r).
   Description and cost of (Combinatorial attacks) These types of attacks consider the support of a codeword and apply an analogous ISD in rank metric sense. The best known strategy in Aragon et al. [5] has complexity $(n-k)^3m^3q^{r\frac{(k+1)m}{n}-m}$.
   Description and cost of (Algebraic attack) This attack is natural for rank metric case and is most useful when q^m increases. It uses several types of algebraic equations settings to try to solve a multivariate system with Gröbner basis. The best knwon attack in Gabidulin et al. [6] has complexity upper bounded by $r^3k^3q^{r\lceil\frac{(r+1)(k+1)-(n+1)}{r}\rceil}$

   Moreover, basis guessing attack to recover Λ : Since $1 \in \Lambda$, then the complexity of guessing basis $\{1, w_1, ..., w_{\lambda-1}\}$ is lower bounded by $q^{(\lambda-1)(m-(\lambda-1))}$.

6 Summary or Conclusion

We have proposed a code-based cryptosystem based on rank metric, called REDOG. In the 4th round of NIST PQC competition, only four algorithms such as BIKE, HQC, Classic McEliece, and SIKE were announced in July 2022. The first three algorithms are code-based cryptosystems based on Hamming metric. As an alternative to Hamming metric, it is highly desirable to consider code-based cryptosystems based on rank metric. The PI and some of the co-authors have worked on code-based cryptosystems based on rank metric and published them on journals/conferences. The parameters of REDOG are reasonably good when compared with the above three algorithms. Therefore, we believe that REDOG can be a strong candidate for the KPQC standardization.

References

1. C. Aguilar Melchor, et al. “Hamming quasi-cyclic (HQC)” NIST PQC Round 2.4 (2018): 13.
2. C. Aguilar-Melchor, A. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.C. Deneuville, P. Gaborit, A. Hauteville, G. Zémor, Ouroboros-R. http://pqc-ourob orosr .org (2017). Accessed 8 Dec 2019.
3. N. Aragon, et al. “BIKE: bit flipping key encapsulation.” (2017).
4. A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal. “Considerations for rank-based cryptosystems.” 2016 IEEE International Symposium on Information Theory (ISIT). Ieee, 2016.
5. N. Aragon, P. Gaborit, A. Hauteville, J.-P. Tillich, A new algorithm for solving the rank syndrome decoding problem. In: Proceedings of IEEE International Symposium on Information Theory (ISIT 2018), pp. 2421–2425 (2018).
6. E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Workshop on the Theory and Application of of Cryptographic Tech- niques, 482-489. Springer, 1991.
7. P. Gaborit, L. Galvez, A. Hauteville, J.-L. Kim, M.J. Kim, Y.-S. Kim, Dual-Ouroboros: an improvement of the McNie scheme. Adv. Math. Commun. (2019).
8. J.-L. Kim, Y.-S. Kim, L.E. Galvez, M.J. Kim, A modified Dual-Ouroboros public-key encryption using Gabidulin codes. Appl. Algebra Eng. Commun. Comput. 32, 147—156, (2021).
9. T.S.C. Lau, C.H. Tan, New rank codes based encryption scheme using partial circulant matrices. Des. Codes Cryptogr. 87(12), 2979—2999, (2019).
10. T. S. C. Lau, C. H. Tan, T. F. Prabowo, On the security of the modified Dual-ouroboros PKE using Gabidulin codes, Appl. Algebra Eng. Commun. Comput. 32, 681–699, (2021).
11. P. Loidreau, A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In: Proceedings of the International Workshop on Coding and Cryptography (WCC 2005), pp. 36–45, (2005).
12. P. Loidreau, A new rank metric codes based encryption scheme, 8th International Conference on Post-Quantum Cryptography, PQCrypto 2017, May 2017, Utrecht, France.
13. McNie and other cryptosystems, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization. Accessed 21 Nov 2019.
14. McNie comment from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1- Submissions, read official comments on McNie dated Dec 24, 2017 and (Dec. 26, 2017).
15. R. Overbeck, Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptol. 21(2), 280–301, (2008).
16. H. Singh, “Code based cryptography: Classic mceliece,” arXiv preprint arXiv:1907.12754 (2019).
17. A. Wachter-Zeh, V. Afanassiev, V. Sidorenko, Designs, Codes and Cryptography, 66, 57–73 (2013)