An analysis of a generalization of Loidreau's encryption scheme

Kayodé-Épiphane Nouetowa, Pierre Loidreau

An analysis of a generalization of Loidreau's encryption scheme

Kayodé-Épiphane Nouetowa†, Pierre Loidreau*
* DGA and Univ Rennes, CNRS, IRMAR - UMR 6625 F-35000 Rennes, France
Email: pierre.loidreau@univ-rennes.fr
† Univ Rennes, CNRS, IRMAR - UMR 6625 F-35000 Rennes, France
Email: kayode-epiphane.nouetowa@univ-rennes.fr

***Abstract*—We generalize the Gabidulin codes based encryption scheme presented by Loidreau in 2017, by combining the original idea with an idea proposed by Gabidulin, Rashwan and Honary in 2009. We then adapt the combinatorial attack proposed by Briaud and Loidreau in 2023 to evaluate the state of the art complexity of an algorithm recovering a decoder from the public-key. The enables to design, for a same security, schemes with smaller parameters than for the original scheme and to analyse the security of another modification of Loidreau's encryption scheme already published.**

ACKNOWLEDGMENTS.

The authors benefit from the support of the French Government Investissements d'Avenir program integrated to France 2030.

I. INTRODUCTION

Rank metric codes based encryption schemes can be seriously considered as interesting post-quantum resistent alternatives to classical encryptions schemes. The principle was introduced in 1991 to reduced the very large public-key size of MacEliece cryptosystem. The idea was to replace Goppa codes and Hamming metric by scrambled Gabidulin codes and rank metric. Since the origin many modifications were proposed almost all subject to the attacks presented in [1], [2], based on the fact that Gabidulin codes are strongly structured. Recently Loidreau proposed in [3] a novel way to hide the structure so that all the existing attacks are flawed. However, there are certain range of parameters were it is possible to distinguish the public-key from random in polynomial time, [4], [5]. Even worse it is possible to recover a decryption algorithm from this distinguisher. As this attack leads to a restriction on the choice of parameters in the Loidreau's scheme, Guo and Fu proposed in [6] two modifications of the Loidreau cryptosystem to avoid the Coggia-Couvreur attack. Furthermore, in [7], Briaud and Loidreau proposed a combinatorial attack. Thus the parameters proposed in the previous works need to be revised.

In this article our goal is to present a generalisation of the Loidreau's cryptosystem, which reduces the size of the secret key, and we analyse the impact of a combinatorial attack on this generalisation in the Coggia-Couvreur and Briaud-Loidreau framework. This leads to a cryptanalysis of the parameters presented in [6] as well as proposing new sets of parameters that are similar to the best proposed parameters in [8]. The rest of the paper is organised as follows: We begin by recalling some generalities about the rank metric and the Gabidulin code. Then we introduce some necessary background to understand the generalisation. Then we present our generalization and show how we can adapt Coggia-Couvreur distinguisher as well as Briaud-Loidreau attack. Finally we propose sets of parameters and compare our generalization to other existing encryption scheme, showing in particular that the parameters proposed in [6] do not satisfy the target security requirements.

II. GENERALITIES

Let q be a power of a prime and let $\mathbb{F}_q$ denote the finite field of order q. We consider the finite field extension of degree m: $\mathbb{F}_{q^m}/\mathbb{F}_q$. $\mathbb{F}_q$ is called the base field and $\mathbb{F}_{q^m}$ the extension field.

Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$. The rank weight of $\mathbf{a}$ is defined as the dimension of the $\mathbb{F}_q$-vector space generated by its components i.e.,

$$Rk(\mathbf{a}) := \dim \langle a_1, \ldots, a_n \rangle_{\mathbb{F}_q}$$

A rank code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ is a sub-vector space of $\mathbb{F}_{q^m}^n$ endowed to the distance induced by the rank metric. The minimum rank distance of $\mathcal{C}$ is defined as the smaller rank of the non zero code words

$$d_r(\mathcal{C}) \stackrel{def}{=} \min_{\mathbf{x} \in \mathcal{C} \setminus \{0\}} Rk(\mathbf{x})$$

Definition 1: Let integers $k \leq n \leq m$ and let $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ such that $Rk(\mathbf{g}) = n$. The k-dimensional Gabidulin code with support vector $\mathbf{g}$ denoted by $\mathcal{G}_k(\mathbf{g})$ is the linear code of generator matrix

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

where $[i] := q^i$.

A generator matrix of the form (1) is said to be in canonical form. The following proposition gives the dual of a Gabidulin code.

Proposition 1: [9] Let $\mathcal{G}_k(\mathbf{g}) \subset \mathbb{F}_{q^m}^n$, then there exists $\mathbf{h} \in \mathbb{F}_{q^m}^n$ of rank n such that $\mathcal{G}_{n-k}(\mathbf{h}) = \mathcal{G}_k(\mathbf{g})^{\perp}$ for the usual scalar product in $\mathbb{F}_{q^m}$.

Let $\mathbf{M} = (m_{i,j})$ be a matrix with entries in $\mathbb{F}_{q^m}$, $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$, and a positive integer μ. We define $\mathbf{x}^{[\mu]} := (x_1^{[\mu]}, \ldots, x_n^{[\mu]})$ and $\mathbf{M}^{[\mu]} := (m_{\mu,j}^{[\mu]})$. Given a code $\mathcal{C}$, the code $\mathcal{C}^{[\mu]}$ is defined by

$$\mathcal{C}^{[\mu]} := \{\mathbf{c}^{[\mu]} \mid \mathbf{c} \in \mathcal{C}\}.$$

The so-called GPT encryption scheme was first proposed by Gabidulin, Paramonov and Trejakov in 1991, [10]. It is an adaptation of McEliece's to rank metric. The family of Goppa code is replaced by the family of Gabidulin codes and in the original paper, the permutation by a rank 1-distortion matrix. The proposal was broken by Gibson in [11], [12]. Since then different variants have been proposed. In [2] the authors proove that the most general form of the public-key in these variants can be stated as follows:

$$\mathbf{G}_{pub} = \mathbf{S}\,(\mathbf{X} \mid \mathbf{G})\,\mathbf{P} \tag{2}$$

with $\mathbf{G}$ under the canonical form (1), $\mathbf{S}$ a full-rank matrix over $\mathbb{F}_{q^m}$, and $\mathbf{X}$ a matrix of small rank and $\mathbf{P}$ a full-rank matrix over the base field $\mathbb{F}_q$.

This general form was broken in [1]. The main reason is because $\mathbf{P}$ has entries in the base field $\mathbb{F}_q$ and is therefore invariant under the action of $x \mapsto x^\mu$.

III. Background

We present two specific variant of GPT encryption schemes. The first one was published in [13]. Though broken in [2] it is a starting point to the construction we will present later.

The second one published in [3]. It is the groundstone from which we will generalise by using ideas of the aforementioned variant.

The notation $\overset{\$}{\leftarrow}$ means that the term on the left is drawn from the set on the right according a specific probability distributions (not necesserally the same for the different variables). Although this distribution plays an important role in security reductions and has to be carefully chosen, for our purpose their expression is out of the context.

A. Gabidulin-Rashwan-Honary schem

Set γ be a positive integer such that $\gamma \leq \frac{n-k}{2}$.

- `KeyGen()`
  - $\mathbf{g} \overset{\$}{\leftarrow} \mathbb{F}_{q^m}^n$ of full rank n. Let $\mathbf{G}$ of the form (1)
  - $\mathbf{S} \overset{\$}{\leftarrow} \mathrm{GL}_k(\mathbb{F}_{q^m})$
  - $\mathbf{Q} = (\mathbf{Q}_1 \mid \mathbf{Q}_2) \overset{\$}{\leftarrow} \mathrm{GL}n(\mathbb{F}_{q^m})$ with $\mathbf{Q_1} \overset{\$}{\leftarrow} \mathcal{M}_{n,\gamma}(\mathbb{F}_{q^m})$ and $\mathbf{Q_2} \overset{\$}{\leftarrow} \mathcal{M}_{n,n-\gamma}(\mathbb{F}_q)$
  - **Return**

    Public key: $\mathbf{G}_{pub} = \mathbf{SGQ}^{-1}$

    Secret key: $\mathbf{G},\ \mathbf{S},\ \mathbf{Q}$)
- `Encrypt`$(\mathbf{m},\ \mathbf{G}_{pub})$
  - $\mathbf{e} \overset{\$}{\leftarrow} \mathbb{F}_{q^m}^n$ such that $Rk(\mathbf{e}) \leq \left\lfloor \frac{n-k}{2} \right\rfloor - \gamma$
  - **Return** $\mathbf{c} = \mathbf{mG}_{pub} + \mathbf{e}$
- `Decrypt`$(\mathbf{c}, \mathbf{G}, \mathbf{S}, \mathbf{Q})$
  - Compute $\mathbf{cQ} = \mathbf{mSG} + \mathbf{e}(\mathbf{Q_1} \mid \mathbf{Q_2})$
  - As

    $$Rk(\mathbf{e}(\mathbf{Q}_1 \mid \mathbf{Q}_2)) \leq \gamma + Rk(\mathbf{e}) \leq \left\lfloor \frac{n-k}{2} \right\rfloor$$

    we recover $\mathbf{mS}$ by decoding $\mathbf{cQ}$ in $\mathcal{G}_k(\mathbf{g})$. Finally, by multiplying with $\mathbf{S}^{-1}$ we recover $\mathbf{m}$.

B. Loidreau's encryption scheme

Proposed to avoid Overbeck's attack and its variants, Loidreau's encryption scheme is a McEliece-like Gabidulin codes based encryption scheme [3]. The novel idea behind the design of the scheme consists in scrambling the Gabidulin code with the help of a non-singular matrix whose inverse has entries in a $\mathbb{F}_q$-subspace $\mathcal{V}$ of $\mathbb{F}_{q^m}$ of small dimension $\lambda \geq 2$. The dimension has to be larger than 1, otherwise it is equivalent to using a raw Gabidulin code.

- `KeyGen()`
  - $\mathbf{g} \overset{\$}{\leftarrow} \mathbb{F}_{q^m}^n$ of full rank n. Let $\mathbf{G}$ of the form (1)
  - $\mathbf{S} \overset{\$}{\leftarrow} \mathrm{GL}_k(\mathbb{F}_{q^m})$
  - $\mathcal{V} \overset{\$}{\leftarrow}$ λ-dimensional subspace of $\mathbb{F}_q^m$
  - $\mathbf{P} \overset{\$}{\leftarrow} \mathrm{GL}_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_n(\mathcal{V})$
  - **Return**

    Public key: $\mathbf{G}_{pub} = \mathbf{SGP}^{-1}$

    Secret key: $\mathbf{G},\ \mathbf{S},\ \mathbf{P}$
- `Encrypt`$(\mathbf{m},\ \mathbf{G}_{pub})$
  - $\mathbf{e} \overset{\$}{\leftarrow} \mathbb{F}_{q^m}^n$ such that $Rk(\mathbf{e}) \leq \left\lfloor \frac{n-k}{2\lambda} \right\rfloor$
  - **Return** $\mathbf{c} = \mathbf{mG}_{pub} + \mathbf{e}$
- `Decrypt`$(\mathbf{c}, \mathbf{G}, \mathbf{S}, \mathbf{P})$
  - Compute $\mathbf{cP} = \mathbf{mSG} + \mathbf{eP}$
  - As

    $$Rk(\mathbf{eP}) \leq \lambda Rk(\mathbf{e}) \leq \left\lfloor \frac{n-k}{2} \right\rfloor$$

    we get $\mathbf{mS}$ by decoding of $\mathbf{cP}$ in $\mathcal{G}_k(\mathbf{g})$. Finally by multplying with $\mathbf{S}^{-1}$ we recover $\mathbf{m}$.

The following proposition shows that the only thing that needs to be secret in Loidreau's scheme is the scrambler matrix.

Proposition 2: Consider the generator matrix $\mathbf{G}_{pub} = \mathbf{SGP}^{-1}$ of the public code in Loidreau's encryption scheme and $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ a normal basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. $\mathbf{G}_{pub}$ can be write as

$$\mathbf{G}_{pub} = \mathbf{SG_{norm}P^{*-1}}$$

where $\mathbf{P^{*-1}}$ is the right inverse of $\mathbf{P}^* \in \mathcal{M}_{n,m}(\mathcal{V})$ and $\mathbf{G}_{norm}$ is the generator matrix of the Gabidulin code $\mathcal{G}_k(\alpha)$ of dimension k.

Proof. Given $\mathbf{g} \in \mathbb{F}_{q^m}^n$ with $rk(\mathbf{g}) = n$, there exist $\mathbf{M} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ of full rank n such that $\mathbf{g} = \alpha\mathbf{M}$. As $\mathbf{G}$ is the generator matrix of the Gabidulin code $\mathcal{G}_k(\mathbf{g})$ defined in canonical from, one has $\mathbf{G} = \mathbf{G}_{norm}\mathbf{M}$. Therefore $\mathbf{G}_{pub} = \mathbf{SG}_{norm}\mathbf{MP}^{-1}$. Since $\mathbf{M}$ is of full rank n, there exist $\mathbf{N} \in \mathcal{M}_{n,m}(\mathbb{F}_q)$ of full rank n such that $\mathbf{NM} = \mathbf{I}_n$.

Thus $\mathbf{PNMP}^{-1} = \mathbf{I}_n$, therefore $\mathbf{MP}^{-1}$ is the right inverse of $\mathbf{P}^* = \mathbf{PN}$ which has its entries in $\mathcal{V}$. ∎

Given a generator matrix $\mathbf{G}_{pub}$ of the public code $\mathcal{C}_{pub}$, one can compute a parity check matrix of $\mathcal{C}_{pub}$. Since $\mathbf{G}_{pub} = \mathbf{SGP}^{-1}$, we have

$$\mathbf{H}_{pub} = \mathbf{VHP}^T$$

where $\mathbf{V} \in \mathrm{GL}_{n-k}(\mathbb{F}_{q^m})$ and $\mathbf{H}$ is the parity check matrix of the Gabidulin code $\mathcal{G}_k(\mathbf{g})$. As the dual of a Gabidulin code is also a Gabidulin code, $\mathbf{H}_{pub}$ is a scrambled generators matrix of a Gabidulin code. Furthermore the scrambler matrix used for $\mathbf{H}_{pub}$ is $\mathbf{P}^T$ which has its entries in $\mathcal{V}$. So if $\mathcal{C}_{pub}^{\perp}$ is vulnerable, so is $\mathcal{C}_{pub}$. This leads to the dual attacks if the parameters are not chosen efficiently.

IV. A generalization of Loidreau's scheme

This section present the generalization of Loidreau's scheme. It can be seen as a combination of the original scheme with the idea introduced in Gabidulin-Rashwan-Honary's scheme. Then we study how Coggia-Couvreur distinguisher is impacted by this modification and finally we address the security of the scheme by adapting the idea in Briaud-Loidreau's paper. Finally we propose set of parameters. The generalization that we propose enable to choose $\lambda = 2$ for a security of 128 bits reducing thus significantly the public-key size and the ciphertext size compared to [3].

A. Description

Let λ and γ be two positive integers such that $\lambda, \gamma \leq \frac{n-k}{2}$.

- `KeyGen()`
  - $\mathbf{g} = (\mathbf{g}_1, \mathbf{g}_2) \xleftarrow{\$} \mathbb{F}_{q^m}^n$ with $Rk(\mathbf{g}) = n$ and $\mathbf{g}_2 \in \mathbb{F}_{q^m}^{n-\gamma}$ Let $\mathbf{G} = (\mathbf{G}_1 \mid \mathbf{G}_2)$ be the corresponding matrix in the canonical form (1).
  - $\mathbf{S} \xleftarrow{\$} \mathrm{GL}_k(\mathbb{F}_{q^m})$
  - $\mathbf{Q} = (\mathbf{Q}_1 \mid \mathbf{Q}_2) \xleftarrow{\$} \mathrm{GL}_n(\mathbb{F}_{q^m})$ with $\mathbf{Q_1} \xleftarrow{\$} \mathcal{M}_{n,\gamma}(\mathbb{F}_{q^m})$ and $\mathbf{Q_2} \xleftarrow{\$} \mathcal{M}_{n,n-\gamma}(\mathbb{F}_q)$
  - $\mathcal{V} \xleftarrow{\$} \lambda$-dimensional subspace of $\mathbb{F}_q^m$
  - $\mathbf{P} \xleftarrow{\$} \mathrm{GL}_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_n(\mathcal{V})$
  - **Return**

    Public key: $\mathbf{G}_{pub} = \mathbf{SGQ}^{-1}\mathbf{P}^{-1}$

    Secret key: $(\mathbf{G}_1 \mid \mathbf{G}_2),\ \mathbf{S},\ \mathbf{PQ_2}$
- `Encrypt`$(\mathbf{m},\ \mathbf{G}_{pub})$
  - $\mathbf{e} \xleftarrow{\$} \mathbb{F}_{q^m}^n$ such that $Rk(\mathbf{e}) \leq \left\lfloor \frac{n-k-\gamma}{2\lambda} \right\rfloor$
  - **Return** $\mathbf{c} = \mathbf{mG}_{pub} + \mathbf{e}$
- `Decrypt`$(\mathbf{c})$
  1) Compute $\mathbf{PQ}_2 = \mathbf{mSG}_2 + \mathbf{ePQ}_2$.
  2) As

$$Rk(\mathbf{ePQ_2}) = Rk(\mathbf{eP}) \leq \lambda Rk(\mathbf{e}) \leq \left\lfloor \frac{n-k-\gamma}{2} \right\rfloor$$

  we recover $\mathbf{mS}$ by decoding $\mathbf{PQ}_2$ in the Gabidulin code $\mathcal{G}_k(\mathbf{g}_2)$. Namely, its error-correction capability is $\left\lfloor \frac{n-k-\gamma}{2} \right\rfloor$. Finally by multiplying with $\mathbf{S}^{-1}$, we recover $\mathbf{m}$.

We analyse the security of the new proposed scheme in terms of distinguishability of the public-key to a randomly chosen matrix. The security concerning the rank decoding problems are already widely explored in the literature. We first show how to extend Coggia-Couvreur distinguisher and then Briaud-Loidreau combinatorial analysis.

B. Generalization of Coggia-Couvreur distinguisher

Our encryption scheme is clearly a generalization of Loidreau's. Namely, if $\mathbf{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$, then the matrix $\mathbf{PQ}$ has entries in $\mathcal{V}$.

The following lemma gives rewrites the public-key under a form which is more suitable to study the security.

Lemma 1: Let $\mathbf{G}_{pub}$ be the public-key of the encryption scheme. There exist $\mathbf{X} \in \mathcal{M}_{k,\gamma}(\mathbb{F}_{q^m})$, $\mathbf{P}^* \in \mathrm{GL}_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_n(\mathcal{V})$, and a matrix $\mathbf{G}^*$ generating of a k-dimensional Gabidulin code of lenth $n-\gamma$ under canonical form such that

$$\mathbf{G}_{pub} = \mathbf{S}(\mathbf{X} \mid \mathbf{G}^*)\mathbf{P}^{*-1}.$$

Proof. We have by construction $\mathbf{Q} = (\mathbf{Q}_1 \mid \mathbf{Q}_2)$ with $\mathbf{Q}_1 \in \mathcal{M}_{n,\gamma}(\mathbb{F}_{q^m})$ and $\mathbf{Q}_2 \in \mathcal{M}_{n,n-\gamma}(\mathbb{F}_q)$. According to Corollary 13 in [2], there exists $\mathbf{X} \in \mathcal{M}_{k,\gamma}(\mathbb{F}_{q^m})$, $\mathbf{T} \in \mathrm{GL}_n(\mathbb{F}_q)$, and a generator matrix $\mathbf{G}^*$ of a k-dimensional Gabidulin code of lenth $n-\gamma$ under canonical form such that $\mathbf{SGQ^{-1}} = \mathbf{S}(\mathbf{X} \mid \mathbf{G}^*)\mathbf{T}$. Therefore

$$\mathbf{G}_{pub} = \mathbf{S}(\mathbf{X} \mid \mathbf{G}^*)\mathbf{P}^{*-1}$$

where $\mathbf{P}^* = \mathbf{PT}^{-1} \in \mathrm{GL}_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_n(\mathcal{V})$. ∎

Now we consider the structure of a parity-check matrix of the code generated by the public-key.

Lemma 2: Any matrix of the form

$$\mathbf{H}_{pub} = \mathbf{V}^{-1} \begin{pmatrix} \mathbf{0} & \mathbf{H}^* \\ \mathbf{U} & \end{pmatrix} \mathbf{P}^{*T}$$

where $\mathbf{V} \in \mathrm{GL}_{n-k}(\mathbb{F}_{q^m})$, $\mathbf{U} \in \mathcal{M}_{\gamma,n}(\mathbb{F}_{q^m})$ of rank γ, $\mathbf{P}^* \in \mathrm{GL}_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_n(\mathcal{V})$ and $\mathbf{H}^*$ is a parity-check matrix of the Gabidulin code generated by $\mathbf{G}^*$ is a parity-check matrix of $\mathcal{C}_{pub}$.

Proof. According to Lemma 1 $\mathbf{G}_{pub} = \mathbf{S}(\mathbf{X} \mid \mathbf{G}^*)\mathbf{P}^{*-1}$ where $\mathbf{P}^* \in \mathrm{GL}_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_n(\mathcal{V})$. Let us denote by $\mathbf{H}^*$ a parity check matrix of the Gabidulin generated by $\mathbf{G}^*$. One has

$\begin{pmatrix} \mathbf{0} & \mathbf{H}^* \end{pmatrix} \mathbf{P}^{*T} \mathbf{G}_{pub}^T = 0$. Thus $\begin{pmatrix} \mathbf{0} & \mathbf{H}^* \end{pmatrix} \mathbf{P}^{*T}$ generates a subcode of $\mathcal{C}_{pub}^{\perp}$ of dimension $n-k-\gamma$. Since $\mathcal{C}_{pub}^{\perp}$ has dimension $n-k$, there exists $\mathbf{U} \in \mathcal{M}_{\gamma,n}(\mathbb{F}_{q^m})$ of rank γ such that $\mathbf{UP}^{*T}\mathbf{G}_{pub}^T = 0$ and $\begin{pmatrix} \mathbf{0} & \mathbf{H}^* \\ \mathbf{U} & \end{pmatrix} \mathbf{P}^{*T}$ is a matrix of rank $n-k$. ∎

From previous lemma we state the following proposition extending Coggia-Couvreur and Ghatak distinguisher, [4], [5].

Proposition 3: The public code $\mathcal{C}_{pub}$ satisfies the following inequality

$$\dim\left(\mathcal{C}_{pub}^{\perp} + \cdots + \mathcal{C}_{pub}^{\perp\,[\lambda]}\right) \leq \lambda \dim \mathcal{C}_{pub}^{\perp} + \lambda + \gamma.$$

Proof. According to Lemma 2, a parity check matrix of the public code $\mathcal{C}_{pub}$ is

$$\mathbf{V}\mathbf{H}_{pub} = \begin{pmatrix} \mathbf{0} & \mathbf{H}^* \\ \mathbf{U} & \end{pmatrix} \mathbf{P}^{*T}.$$

Let $\mathcal{C}_1$ be the code of length n and dimension $n-k-\gamma$ generated by $\begin{pmatrix} \mathbf{0} & \mathbf{H}^* \end{pmatrix} \mathbf{P}^{*T}$. Let $\mathcal{C}_2$ be the code of length n and dimension γ generated by $\mathbf{U}\mathbf{P}^{*T}$. Then $\mathcal{C}_{pub}^{\perp} \subset \mathcal{C}_1 + \mathcal{C}_2$. Thus

$$\begin{aligned} \dim\left(\mathcal{C}_{pub}^{\perp} + \cdots + \mathcal{C}_{pub}^{\perp\,[\lambda]}\right) &\leq \dim\left(\mathcal{C}_1 + \cdots + \mathcal{C}_1^{\,[\lambda]}\right) \\ &+ \dim\left(\mathcal{C}_2 + \cdots + \mathcal{C}_2^{\,[\lambda]}\right) \end{aligned}$$

Furthermore, since $\mathcal{C}_1$ is some kind of a Gabidulin code, we have $\dim\left(\mathcal{C}_1 + \cdots + \mathcal{C}_1^{\,[\lambda]}\right) \leq \lambda \dim \mathcal{C}_1 + \lambda$. Therefore

$$\dim\left(\mathcal{C}_{pub}^{\perp} + \cdots + \mathcal{C}_{pub}^{\perp\,[\lambda]}\right) \leq (\lambda \dim \mathcal{C}_1 + \lambda) + (\lambda+1)\gamma,$$

which is equal to $\lambda(n-k) + \lambda + \gamma$ ∎

To conclude, the public code $\mathcal{C}_{pub}$ of dimension k is distinguishable in polynomial time from a random code if

$$\lambda(n-k) + \lambda + \gamma < \min(n, (\lambda+1)(n-k)) \tag{3}$$

where the right term corresponds to the expected dimension of the sum of k-dimensional random codes elevated to successive powers $[i] = 0, \ldots, \lambda$.

C. Generalization of Briaud-Loidreau attack

In this section, we extend and adapt for our scheme the combinatorial attack presented in [7] for the original Loidreau encryption scheme. According to Lemma 2 a parity check matrix of the public code can be decomposed as

$$\mathbf{H}_{pub} = \mathbf{V}^{-1} \begin{pmatrix} \mathbf{0} & \mathbf{H}^* \\ \mathbf{U} & \end{pmatrix} \mathbf{P}^{*T}$$

Let $r = n-k-\gamma$ and $\alpha \in \mathbb{F}_{q^m}$ be a normal element. Consider $\mathbf{H}_{norm} = \left(\alpha^{[i+j-2]}\right)_{i=1,j=1}^{r,m}$. There exists $\mathbf{M} \in \mathcal{M}_{m,n-\gamma}(\mathbb{F}_q)$ of full rank $n-\gamma$ such that $\mathbf{H}^* = \mathbf{H}_{norm}\mathbf{M}$. Let us denote

$$\mathbf{P}^{*T} = \begin{pmatrix} \mathbf{P}_0 \\ \mathbf{P}_1 \end{pmatrix}$$

with $\mathbf{P}_0 \in \mathcal{M}_{\gamma,n}(\mathcal{V})$ and $\mathbf{P}_1 \in \mathcal{M}_{n-\gamma,n}(\mathcal{V})$. We get

$$\mathbf{V}\mathbf{H}_{pub} = \begin{pmatrix} \mathbf{H}_{norm}\mathbf{M}\mathbf{P}_1 \\ \mathbf{U}\mathbf{P}^{*T} \end{pmatrix} = \begin{pmatrix} \mathbf{H}_{norm}\mathbf{W} \\ \mathbf{R} \end{pmatrix} \tag{4}$$

where $\mathbf{W} = \mathbf{M}\mathbf{P}_1 \in \mathcal{M}_{m,n}(\mathcal{V})$ and $\mathbf{R} = \mathbf{U}\mathbf{P}^{*T} \in \mathcal{M}_{\gamma,n}(\mathbb{F}_{q^m})$. Let us denote by $\mathbf{y} = \mathbf{c} + \mathbf{e}$ the ciphertext. We split the study in two cases:

- Case $1 : \gamma = 0$
  If $\gamma = 0$ then we get

  $$\mathbf{V}\mathbf{H}_{pub} = \mathbf{H}_{norm}\mathbf{W} \tag{5}$$

  with $\mathbf{W}$ of full rank n. This case corresponds to the Loidreau's scheme. It is shown in [7] that the knowledge of a matrix $\mathbf{W}$ with coefficients in a λ-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ suffices to decrypt the ciphertext. Namely,

  $$\mathbf{V}\mathbf{H}_{pub}\mathbf{y}^T = \mathbf{V}\mathbf{H}_{pub}\mathbf{e}^T = \mathbf{H}_{norm}\mathbf{W}\mathbf{e}^T.$$

  Therefore $\mathbf{H}_{norm}\mathbf{W}\mathbf{c}^T = 0$ and $\mathbf{c}\mathbf{W}^T$ is a codeword of the Gabidulin code with parity check matrix $\mathbf{H}_{norm}$. Thus, if we know $\mathbf{W}$ one can use this Gabidulin code to decode $\mathbf{y}\mathbf{W}^T$ and use the fact that the map $\mathbf{c} \mapsto \mathbf{c}\mathbf{W}^T$ is one-to-one to recover $\mathbf{c}$. It is also proven in the same paper that the search of $\mathbf{W}$ can be done by solving the equation (5) with at least

  $$m^3(n-k)^5 q^{(\lambda-1)m - \lambda\lfloor n(1-R)R \rfloor}$$

  operations on $\mathbb{F}_q$, where $R = \frac{k}{n}$.
- Case $2 : \gamma \neq 0$ Consider $\mathbf{V}_1 \in \mathcal{M}_{n-k-\gamma,n-k}(\mathbb{F}_{q^m})$ and $\mathbf{V}_2 \in \mathcal{M}_{\gamma,n-k}(\mathbb{F}_{q^m})$ such that

  $$\mathbf{V} = \begin{pmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \end{pmatrix}.$$

  According to (4), one has

  $$\mathbf{V_1}\mathbf{H}_{pub} = \mathbf{H}_{norm}\mathbf{W}$$

  So one approach would be as for the previous case to complete the same procedure as is written in [7] by solving a similar system over $\mathbb{F}q$.
  Let $\mathcal{A} \in \mathbb{F}_{q^m}^{\lambda}$ be a basis of $\mathcal{V}$ over $\mathbb{F}_q$ and $\mathcal{B} \in \mathbb{F}_{q^m}^{m}$ a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$ obtained by extending $\mathcal{A}$. The number of unknowns and the number of equations over $\mathbb{F}_q$ in the basis $\mathcal{B}$ are respectively $m(n-k-\gamma)(n-k)+\lambda mn$ and $mn(n-k-\gamma)$. The search for $\mathbf{W}$ is therefore a two-stage process:
  - the search of a base $\mathcal{A}$ of $\mathcal{V}$;
  - Solving a system of linear equations over $\mathbb{F}_q$.

  A basis of $\mathcal{V}$ can be found with average $q^{\lambda m - \lambda^2}$ operations over $\mathbb{F}_q$. However the knowledge of any vector space $\mathcal{U}$ of dimension $\mu \geq \lambda$ satisfying $\beta\mathcal{V} \subset \mathcal{U}$ for some $\beta \in \mathbb{F}_{q^m}^*$ is sufficient to determine $\mathbf{W}$ as long as the system remains overdetermined. A basis of $\mathcal{U}$ can be found in $q^{(\lambda-1)m-\mu\lambda}$ operations on average over $\mathbb{F}_q$ [14]. The dimension of $\mathcal{U}$, μ can be chosen so that the number of equations is just under to the number of unknowns so that the system is slightly overdetermined. This gives an inequality $(n-k-\gamma)(n-k)+\mu n \leq n(n-k-\gamma)$ i.e. The integer $\mu \leq \lfloor nR(1-R) - \gamma R \rfloor$ where $R = \frac{k}{n}$ is the rate of the public code. The valued $\mu = \lfloor nR(1-R) - \gamma R \rfloor$ is the best choice in terms of complexity.
  Now to solve the system of the linear equation, we consider to use Wiedemann algorithm instead to Gauss elimination, because the matrix of the system is sparse. The cost of this solving can be estimated at

  $$P(m,n,k,\mu,\gamma) = m^3(n-k+\mu)[(n-k-\gamma)(n-k)+\mu n]^2$$

  operations over $\mathbb{F}_q$. In short, the lower bound of the overall complexity is given by

$(m, n, k, t, \lambda, \gamma)$	Sec. Target	pk-size	ct-size
$(98, 89, 10, 17, 2, 11)$	128	9.5 kO	0.94 kO
$(165, 122, 14, 23, 2, 14)$	192	26 kO	2 kO

TABLE I
PROPOSITION OF PARAMETERS

$$W_{Spec\_Inf} = P(m, n, k, \mu, \gamma) q^{(\lambda-1)m - \lambda\lfloor n(1-R)R - \gamma R \rfloor}.$$

A remark however is that contrarily to the previous case, finding $\mathbf{W}$ would not be sufficient to be able to decrypt the ciphertext at least in a straightforward approach. Namely we also have $\mathbf{V}_2\mathbf{H}_{pub} = \mathbf{R}$. Therefore, given $\mathbf{c} \in \mathcal{C}_{pub}$, $\mathbf{H}_{norm}\mathbf{W}\mathbf{c}^T = 0$ and $\mathbf{c}\mathbf{W}^T$ is a codeword of the Gabidulin code with parity check matrix $\mathbf{H}_{norm}$. Thus the knowledge of $\mathbf{W}$ allows to determine $\mathbf{c}\mathbf{W}^T$ by the decoding of $\mathbf{y}\mathbf{W}^T$. But we can no longer determine $\mathbf{c}$ uniquely knowing only $\mathbf{W}$ because the map $\mathbf{c} \mapsto \mathbf{c}\mathbf{W}$ is not one-to-one anymore since $\mathbf{W}$ has rank at most $n-\gamma$. Hence the attack we designed does not enable to recover the plaintext but suffices to distinguish the public-key from random.

D. Proposition of parameters

In table I we propose a set of parameters for $\lambda = 2$. For this set of parameters we give the minimum security achieved in bits by considering all the state of the art attacks including rank metric decoding based attacks and this precise work. We also provide the public-key and the ciphertext size that one can expect.

E. Comparisons with other unstructured rank metric based schemes

In [6] Guo and Fu presented two modification of Loidreau's scheme together with updated attractive parameters. We focus our attention to modification specifically on modification 2.

In this modification, a generator matrix of the public code is

$$\mathbf{G}_{pub} = \mathbf{S}(\mathbf{G} + \mathbf{M})\mathbf{P^{-1}}$$

where $\mathbf{M} \in \mathbb{F}_{q^m}^{k\times n}$ is such that the largest number of columns of $\mathbf{M}$ linearly independent over $\mathbb{F}_q$ is γ. By performing some elementary operations, we can write $\mathbf{M} = (\mathbf{X} \mid \mathbf{0})\mathbf{Q}$, where $\mathbf{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ and $\mathbf{X} \in \mathbb{F}_{q^m}^{k\times\gamma}$ is a random matrix of full rank γ. Thus

$$\mathbf{G}_{pub} = \mathbf{S}\left(\mathbf{X}^* \mid \mathbf{G}^*\right)\mathbf{P}^{*-1}$$

with $\mathbf{P}^{*-1} = \mathbf{Q}\mathbf{P}^{-1}$ and $[\mathbf{X}^* \mid \mathbf{G}^*] = (\mathbf{X} \mid \mathbf{0}) + \mathbf{G}\mathbf{Q}^{-1}$.

Therefore, we have rewritten the public-key of the modification under the same form that we had for Lemma 1. The difference we have with their proposal is that we can correct errors of larger rank, namely we correct errors up to rank $\lfloor (n-k-\gamma)/(2\lambda) \rfloor$, whereas they propose to correct errors of rank $\lfloor (n-k-2\gamma)/(2\lambda) \rfloor$.

Second, we can apply our security analysis to the parameters proposed for modification 2. They propose 3 sets of parameters with $q = 3$ and $\lambda = 2$.

1) $m = n = 44$, $k = 30$, $\gamma = 1$
2) $m = n = 51$, $k = 33$, $\gamma = 1$
3) $m = n = 57$, $k = 35$, $\gamma = 1$

All the proposed parameters are in the distinguishing range of our extension of Coggia-Couvreur distinguisher since they clearly satisfy (3). Moreover note that this modification is also vulnerable to the attack we presented in IV-C.

Recently the LowMS Key Encapsulation Mechanism (KEM) was published with very competitive parameters, [8]. This KEM is formed above Loidreau's encryption scheme, and we can use our adaptation on the public-key of LowMS. However we were not able to find better parameters than those that they propose in this submission concerning the public-key size. Namely they propose between 5 and 9 kBytes for a security of 128 bits and 15 and 17 kBytes for a security of 192 bits. Nevertheless our scheme has some advantages relatively to the LowMS scheme:

- There is no failure probability in the decryption procedure. This means that this has to be taken into account in security reductions, which complexifies the mode of operation and also that it has to be taken into account in implementations that should be resistant to side-channel attacks.
- It is based on the Rank Support Learning with errors problem which is an extenstion of the rank syndrome decoding problem and has been less investigated.

REFERENCES

[1] R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," *J. Cryptology*, vol. 21, no. 2, pp. 280–301, 2008.

[2] A. Otmani, H. Talé-Kalachi, and S. Ndjeya, "Improved cryptanalysis of rank metric schemes based on Gabidulin codes," *Des. Codes Cryptogr.*, vol. 86, no. 9, pp. 1983–1996, 2018.

[3] P. Loidreau, "A new rank metric codes based encryption scheme," in *PQCrypto 2017*, ser. LNCS, vol. 10346. Springer, 2017, pp. 3–17.

[4] D. Coggia and A. Couvreur, "On the security of a Loidreau rank metric code based encryption scheme," *Des. Codes Cryptogr.*, vol. 88, no. 9, pp. 1941–1957, 2020.

[5] A. Ghatak, "Extending Coggia-Couvreur attack on Loidreau's rank metric cryptosystem," *Des. Codes Cryptogr.*, vol. 90, pp. 215–238, 2022.

[6] W. Guo and F. Fu, "Two modifications for Loidreau's code-based cryptosystem," *Appl. Algebra Eng. Commun. Comput.*, vol. 35, no. 5, pp. 647–665, 2024.

[7] P. Briaud and P. Loidreau, "Cryptanalysis of Rank-Metric Schemes Based on Distorted Gabidulin Codes," in *14th International Workshop, PQCrypto 2023*, ser. LNCS, T. Johansson and D. Smith-Tone, Eds., vol. 14154, 2023, pp. 38–56.

[8] N. Aragon, V. Dyseryn, P. Gaborit, P. Loidreau, J. Renner, and A. Wachter-Zeh, "LowMS: a new rank metric code-based KEM without ideal structure," *Des. Codes Cryptogr.*, vol. 92, no. 4, pp. 1075–1093, 2024.

[9] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 3–16, 1985.

[10] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their applications to cryptography," in *Advances in Cryptology - EUROCRYPT'91*, ser. LNCS, no. 547, Brighton, Apr. 1991, pp. 482–489.

[11] K. Gibson, "Severely denting the Gabidulin version of the McEliece public key cryptosystem," *Des. Codes Cryptogr.*, vol. 6, no. 1, pp. 37–45, 1995.

[12] ——, "The security of the Gabidulin public key cryptosystem," in *Advances in Cryptology - EUROCRYPT '96*, ser. LNCS, U. Maurer, Ed., vol. 1070. Springer, 1996, pp. 212–223.

[13] E. M. Gabidulin, H. Rashwan, and B. Honary, "On improving security of GPT cryptosystems," in *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, 2009, pp. 1110–1114.
[14] N. Aragon, P. Gaborit, A. Hauteville, and J. Tillich, "A New Algorithm for Solving the Rank Syndrome Decoding Problem," in *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, Jun. 2018, pp. 2421–2425.