Applicable Algebra in Engineering, Communication and Computing (2024) 35:647–665
https://doi.org/10.1007/s00200-022-00577-0

ORIGINAL PAPER

Two modifications for Loidreau's code-based cryptosystem

Wenshuo Guo[1] · **Fang-Wei Fu**[1]

Received: 17 May 2022 / Revised: 28 July 2022 / Accepted: 4 August 2022 /
Published online: 16 August 2022

Abstract
This paper presents two modifications for Loidreau's cryptosystem, a rank metric-based cryptosystem constructed by using Gabidulin codes in the McEliece setting. Recently a polynomial-time key recovery attack was proposed to break this cryptosystem in some cases. To prevent this attack, we propose the use of subcodes to disguise the secret codes in Modification I. In Modification II, we choose a random matrix of low column rank to mix with the secret matrix. Our analysis shows that these two modifications can both resist the existing structural attacks. Furthermore, these modifications have a much more compact representation of public keys compared to Classic McEliece, which has been selected into the fourth round of the NIST-PQC project.

Keywords Code-based cryptography · Rank metric codes · Gabidulin codes · Loidreau's cryptosystem

1 Introduction

In 1978, McEliece [41] proposed the first code-based public-key cryptosystem, namely the McEliece cryptosystem based on Goppa codes. Since then cryptologists have made extensive study on its security [11, 16, 31, 33]. Apart from some weak keys [40], the McEliece cryptosystem remains secure up to now. The main drawback of this cryptosystem lies in its large public-key size, which makes it unpractical in many situations. To overcome this problem, many variants have been proposed. In 1986, Niederreiter [43] introduced a knapsack-type cryptosystem using GRS codes, which was shown to be insecure by Sidelnikov and Shestakov in [51]. But if we use Goppa codes in the Niederreiter setting, it was proved to be equivalent to the

✉ Wenshuo Guo
ws_guo@mail.nankai.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

[1] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China

McEliece cryptosystem in terms of security [34]. GRS codes allow us to reduce the public-key size due to their optimal error-correcting capability. Many variants based on GRS codes were proposed after Niederreiter's work. However, almost all of these variants were broken one after another because of GRS codes being highly structured. In the BBCRS cryptosystem [5], the authors proposed the use of a dense matrix rather than a permutation matrix to disguise the structure of the underlying GRS code. In this proposal, the column scrambler is a matrix of the form $(R+T)^{-1}$, where T is a sparse matrix and R is a dense matrix of low rank. With this approach, the public code seems quite different from GRS codes. This variant therefore can resist some known structural attacks, such as the Sidelnikov-Shestakov attack [51]. However, in [14, 15] the authors presented a polynomial-time key recovery attack against this variant in some cases. Although we can adjust the parameters to prevent such an attack, it would bring some other problems such as the decryption complexity increasing exponentially and a higher request of error-correcting capability for the underlying code.

In 1985 Gabiduin [18] introduced a new family of rank metric codes, known as the Gabidulin codes. Since the complexity of decoding general rank metric codes is much higher than that of decoding Hamming metric codes [12, 45], it is feasible to obtain much smaller public-key sizes by building cryptosystems in the rank metric. In [21] the authors proposed to use Gabidulin codes in the McEliece setting and introduced the GPT cryptosystem. Unfortunately, several structural attacks were put forward to completely break this system [27, 30, 46].To prevent these attacks, variants based on different masking skills for Gabidulin codes were proposed [19, 22, 37, 47, 48]. But in [44] the authors declared the failure of all the previous masking techniques for Gabidulin codes. In [17] Faure and Loidreau proposed a cryptosystem also relying on Gabidulin codes but not in the McEliece setting, which can be seen as a rank metric counterpart of Augot-Finiasz cryptosystem [4]. Until the work in [23], the Faure-Loidreau cryptosystem had never been severely attacked. Two reparations of this scheme aimed at resisting this attack were proposed independently and differently in [32, 49]. Bombar and Couvreur [9] investigated the supercode decoding of Gabidulin codes and induced from this decoder a polynomial-time attack on these two reparations. Loidreau [38] proposed a cryptosystem constructed by using Gabidulin codes in the McEliece setting. Different from the original GPT cryptosystem, the isometric matrix is replaced with a matrix whose inverse is taken over an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension λ. By doing this, the public code seems quite random. Loidreau claimed that his proposal could prevent the existing structural attacks. However, this claim was proved to be invalid by the authors in [13] when $\lambda = 2$ and the code rate is greater than 1/2. Soon after this, the author in [26] generalized this attack to the case of $\lambda > 2$ and the code rate being greater than $1 - \frac{1}{\lambda}$. However, it is feasible to prevent this attack even when the secret code rate is greater than $1 - \frac{1}{\lambda}$ according to our analysis in the present paper.

The rest of this paper is organised as follows. In Sect. 2 notations and some concepts about rank metric codes used throughout this paper are given. Section 3 is devoted to a simple description of Loidreau's cryptosystem. In Sect. 4 we shall introduce part of Coggia-Couvreur attack. Following this, our two modifications

for Loidreau's cryptosystem will be introduced in Sect. 5, then security analysis of our modifications will be given in Sect. 6. In Sect. 7, we will give some suggested parameters for different security levels and make a comparison on public-key size with some NIST-PQC submissions. Sect. 8 concludes this paper.

2 Preliminaries

2.1 Notations and basic concepts

Let q be a prime power. Denote by $\mathbb{F}_q$ the finite field with q elements, and by $\mathbb{F}_{q^m}$ an extension field of $\mathbb{F}_q$ of degree m. For positive integers k, n, denote by $\mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ the space of $k \times n$ matrices over $\mathbb{F}_{q^m}$, and by $GL_n(\mathbb{F}_{q^m})$ the space of invertible matrices in $\mathcal{M}_{n,n}(\mathbb{F}_{q^m})$. For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, the column rank of M with respect to $\mathbb{F}_q$, denoted by $\mathrm{Clr}_q(M)$, is the largest number of columns of M linearly independent over $\mathbb{F}_q$. Denote by $\langle M \rangle_{q^m}$ the vector space spanned by the rows of M over $\mathbb{F}_{q^m}$.

An $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ is a k-dimensional subspace of $\mathbb{F}_{q^m}^n$. The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is the orthogonal space of $\mathcal{C}$ under the usual Euclidean inner product over $\mathbb{F}_{q^m}^n$. A $k \times n$ full-rank matrix $G \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ is called a generator matrix of $\mathcal{C}$ if the vector space $\langle G \rangle_{q^m}$ is exactly the code $\mathcal{C}$. A generator matrix of $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$.

2.2 Rank metric codes

Now we recall some basic concepts about rank metric and rank metric codes.

Definition 1 For a vector $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{F}_{q^m}^n$, the rank support of $\boldsymbol{x}$ is defined to be $\mathrm{Supp}(\boldsymbol{x}) = \langle x_1, \cdots, x_n \rangle_q$.

Definition 2 For a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, the rank weight of $\boldsymbol{x}$ is defined as $w_R(\boldsymbol{x}) = \dim_q(\mathrm{Supp}(\boldsymbol{x}))$.

Remark 1 For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, the rank support of M is defined as $\mathrm{Supp}(M) = \sum_{i=1}^{k} \mathrm{Supp}(\boldsymbol{m}_i)$, where $\boldsymbol{m}_i$ denotes the i-th row of M. And the rank weight of M is defined as $w_R(M) = \dim_q(\mathrm{Supp}(M))$.

Definition 3 For two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$, the rank distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined as $d_R(\boldsymbol{x}, \boldsymbol{y}) = w_R(\boldsymbol{x} - \boldsymbol{y})$.

It is easy to verify that $d_R(\cdot, \cdot)$ defines a proper metric on $\mathbb{F}_{q^m}^n$. A linear code endowed with the rank metric is called a rank metric code.

Definition 4 For a rank metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, the minimum rank distance of $\mathcal{C}$ is defined to be $d(\mathcal{C}) = \min\{w_R(\boldsymbol{x}) : \boldsymbol{x} \in \mathcal{C} \backslash \{\boldsymbol{0}\}\}$.

Note that the minimum rank (Hamming) distance of a linear code equals its minimum rank (Hamming) weight. For Hamming metric codes, the minimum distance d of an $[n, k]$ linear code satisfies the Singleton bound $d \leqslant n - k + 1$ [35]. Similarly, the minimum rank distance of a rank metric code satisfies the following Singleton-style bound. And a rank metric code attaining the Singleton-style bound is called a Maximum Rank Distance (MRD) code.

Proposition 1 (Singleton-style bound) [20] *For positive integers $n \leqslant m$, let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $[n, k]$ rank metric code, then the minimum rank distance of $\mathcal{C}$ with respect to $\mathbb{F}_q$ satisfies the following inequality*

$$d(\mathcal{C}) \leqslant n - k + 1.$$

The following proposition states a fact that the maximum rank weight of a rank metric code is bounded from above by the column rank of its generator matrix.

Proposition 2 *For a matrix $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ with $\mathrm{Clr}_q(M) = r$, the maximum rank weight of the code $\langle M \rangle_{q^m}$ is bounded by r from above.*

Proof It suffices to prove that $w_R(\boldsymbol{v}) \leqslant r$ for any $\boldsymbol{v} \in \langle M \rangle_{q^m}$. Note that $\mathrm{Clr}_q(M) = r$, then there exists $Q \in GL_n(\mathbb{F}_q)$ such that $MQ = [M'|0]$, where $M' \in \mathcal{M}_{k,r}(\mathbb{F}_{q^m})$ with $\mathrm{Clr}_q(M') = r$. For any $\boldsymbol{v} \in \langle M \rangle_{q^m}$, there exists $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{v} = \boldsymbol{x}M$ and

$$\boldsymbol{v}Q = \boldsymbol{x}MQ = \boldsymbol{x}[M'|0] = (\boldsymbol{x}'||\boldsymbol{0}),$$

where $\boldsymbol{x}' \in \mathbb{F}_{q^m}^r$. Then $w_R(\boldsymbol{v}) = w_R(\boldsymbol{v}Q) \leqslant r$, which leads to the conclusion immediately.

2.3 Gabidulin codes

Gabidulin codes are actually an analogue of GRS codes in the rank metric, and these two types of codes resemble each other closely in the construction principle. GRS codes admit generator matrices with the Vandermonde structure, while Gabidulin codes can be described through Moore matrices defined as follows.

Definition 5 For $a \in \mathbb{F}_{q^m}$ and an integer s, we denote by $a^{[s]} = a^{q^s}$ the s-th Frobenius power of a. A matrix $G \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ is called a Moore matrix generated by $\boldsymbol{a} = (a_1, \cdots, a_n) \in \mathbb{F}_{q^m}^n$ if the s-th row of G equals the coordinate-wise Frobenius power $\boldsymbol{a}^{[s-1]} = (a_1^{[s-1]}, \cdots, a_n^{[s-1]})$ for $1 \leqslant s \leqslant k$, that is

$$G = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^{[1]} & a_2^{[1]} & \cdots & a_n^{[1]} \\ \vdots & \vdots & & \vdots \\ a_1^{[k-1]} & a_2^{[k-1]} & \cdots & a_n^{[k-1]} \end{pmatrix}. \tag{1}$$

For a matrix $G = (G_{ij}) \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, we define $G^{[s]} = (G_{ij}^{[s]})$. For a set $S \subseteq \mathbb{F}_{q^m}^n$, we define $S^{[s]} = \{\boldsymbol{x}^{[s]} : \boldsymbol{x} \in S\}$. For a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, it is easy to verify that $\mathcal{C}^{[s]}$ is also an $\mathbb{F}_{q^m}$-linear code.

Definition 6 (Gabidulin codes) For positive integers $k \leqslant n \leqslant m$, let $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{a}) = n$ and G be the $k \times n$ Moore matrix generated by $\boldsymbol{a}$. The $[n, k]$ Gabidulin code $\mathcal{G}_{n,k}(\boldsymbol{a})$ over $\mathbb{F}_{q^m}$ generated by $\boldsymbol{a}$ is defined to be the linear space $\langle G \rangle_{q^m}$.

A major reason for Gabidulin codes being widely used in the design of cryptosystems consists in their remarkable error-correcting capability and simple algebraic structure. Now we recall some properties of Gabidulin codes through the following two theorems.

Theorem 1 [28] *The Gabidulin code $\mathcal{G}_{n,k}(\boldsymbol{a})$ is an MRD code. In other words, $\mathcal{G}_{n,k}(\boldsymbol{a})$ attains the Singleton-style bound for rank metric codes.*

It is easy to see from Theorem 1 that $d(\mathcal{G}_{n,k}(\boldsymbol{a})) = n - k + 1$, which implies that any $\lfloor \frac{n-k}{2} \rfloor$ rank errors can be corrected in theory. Indeed, several efficient decoding algorithms for Gabidulin codes already exist [18, 36, 50].

Theorem 2 [23] *The dual code of $\mathcal{G}_{n,k}(\boldsymbol{a})$ is the Gabidulin code $\mathcal{G}_{n,n-k}(\boldsymbol{b}^{[-n+k+1)]})$ for some $\boldsymbol{b} \in \mathcal{G}_{n,n-1}(\boldsymbol{a})^{\perp}$ with $w_R(\boldsymbol{b}) = n$.*

3 Loidreau's cryptosystem

Now we give a simple description of Loidreau's cryptosystem proposed in [38]. For a desired security level, choose a finite field $\mathbb{F}_q$ and positive integers $\lambda \ll k < n \leqslant m$. Loidreau's cryptosystem consists of the following three algorithms.

- Key generation
  Randomly choose a vector $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{a}) = n$, let G be a generator matrix of $\mathcal{G}_{n,k}(\boldsymbol{a})$. Let $\mathcal{V} \subset \mathbb{F}_{q^m}$ be a randomly chosen $\mathbb{F}_q$-linear space of dimension λ. Randomly choose $P \in GL_n(\mathcal{V})$ such that $w_R(P) = \lambda$ and compute $G_{pub} = GP^{-1}$. We publish (G_{pub}, t) as the public key where $t = \lfloor \frac{n-k}{2\lambda} \rfloor$, and keep $(\boldsymbol{a}, P)$ as the private key.
- Encryption

For a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$, randomly choose a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{e}) = t$. The ciphertext corresponding to $\boldsymbol{m}$ is computed as $\boldsymbol{c} = \boldsymbol{m}G_{pub} + \boldsymbol{e}$.

– Decryption

For a ciphertext $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$, compute $\boldsymbol{c}' = \boldsymbol{c}P = \boldsymbol{m}G + \boldsymbol{e}P$. Because of $w_R(\boldsymbol{e}P) \leqslant w_R(\boldsymbol{e}) \cdot w_R(P) \leqslant \lfloor \frac{n-k}{2} \rfloor$, decoding $\boldsymbol{c}'$ will lead to $\boldsymbol{e}' = \boldsymbol{e}P$. Then one can recover $\boldsymbol{e}$ by computing $\boldsymbol{e}'P^{-1}$ and hence the plaintext $\boldsymbol{m}$ by solving the linear system $\boldsymbol{m}G_{pub} = \boldsymbol{c} - \boldsymbol{e}$.

4 Coggia–Couvreur attack

Before describing Coggia–Couvreur attack, we first introduce a distinguisher for Gabidulin codes, which provides an approach for us to distinguish Gabidulin codes from general ones.

4.1 A distinguisher for Gabidulin codes

Most cryptosystems based on Gabidulin codes have been proved to be insecure against structural attacks. Although these attacks were proposed to cryptanalyze different variants, the principle for them is based on the observation that one can distinguish Gabidulin codes from general ones by performing a simple operation on these codes.

Given a random linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension $k \leqslant n/2$, the expected dimension of the code $\mathcal{C} + \mathcal{C}^{[1]}$ equals $2k$, or equivalently $\mathcal{C} \cap \mathcal{C}^{[1]} = \{\boldsymbol{0}\}$ holds with high probability. But for a Gabidulin code $\mathcal{G}_{n,k}(\boldsymbol{a})$, we have $\mathcal{G}_{n,k}(\boldsymbol{a}) + \mathcal{G}_{n,k}(\boldsymbol{a})^{[1]} = \mathcal{G}_{n,k+1}(\boldsymbol{a})$, or equivalently $\dim_{q^m}(\mathcal{G}_{n,k}(\boldsymbol{a}) + \mathcal{G}_{n,k}(\boldsymbol{a})^{[1]}) = k + 1$. More generally, we have the following two propositions.

Proposition 3 [13] *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a random linear code of length n and dimension k. For a non-negative integer l and a positive integer $s < k$, we have*

$$\Pr\left(\dim_{q^m}(\mathcal{C} + \mathcal{C}^{[1]} + \cdots + \mathcal{C}^{[s]}) \leqslant \min\{n, (s+1)k\} - l\right) = \mathcal{O}(q^{-ml}).$$

Proposition 4 [13] *Let $k \leqslant n$ and s be a positive integer, then for any $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{a}) = n$, we have*

$$\mathcal{G}_{n,k}(\boldsymbol{a}) \cap \mathcal{G}_{n,k}(\boldsymbol{a})^{[1]} = \mathcal{G}_{n,k-1}(\boldsymbol{a}^{[1]});$$
$$\mathcal{G}_{n,k}(\boldsymbol{a}) + \cdots + \mathcal{G}_{n,k}(\boldsymbol{a})^{[s]} = \mathcal{G}_{n,k+s}(\boldsymbol{a}).$$

4.2 Description of Coggia–Couvreur attack

In this part we investigate the structural vulnerability of Loidreau's cryptosystem in the case of $\lambda = 2$ and the rate of the public code $\mathcal{C}_{pub} = \langle G_{pub} \rangle_{q^m}$ being greater than 1/2. The principle for Coggia-Couvreur attack lies in Propositions 3 and 4. Instead of operating the public code directly, Coggia and Couvreur considered the dual of the public code because of the following lemma.

Lemma 1 [13] *Any parity-check matrix H_{pub} of $\mathcal{C}_{pub}$ can be expressed as*

$$H_{pub} = H_{sec} P^T,$$

where H_{sec} is a parity-check matrix of the secret Gabidulin code $\mathcal{G}_{n,k}(\boldsymbol{a})$.

The authors considered the case of $\lambda = 2$, namely $\mathcal{V} \subseteq \mathbb{F}_{q^m}$ has dimension 2 over $\mathbb{F}_q$. Assume that $\mathcal{V} = \langle \alpha, \beta \rangle_{\mathbb{F}_q}$ for some $\alpha, \beta \in \mathbb{F}_{q^m}^*$. Let $H'_{sec} = \alpha H_{sec}$ and $P' = \alpha^{-1} P$, then $H_{pub} = H'_{sec} P'^T$. It is clear that H'_{sec} spans the same code as H_{sec} and entries of P' are contained in $\mathcal{V}' = \langle 1, \alpha^{-1}\beta \rangle_{\mathbb{F}_q}$. Hence it is reasonable to suppose $\mathcal{V} = \langle 1, \gamma \rangle_{\mathbb{F}_q}$ for some $\gamma \in \mathbb{F}_{q^m}^*$. In this situation, we express P^T in the form of

$$P^T = P_0 + \gamma P_1,$$

where $P_0, P_1 \in \mathcal{M}_{n,n}(\mathbb{F}_q)$.

According to Theorem 2, there exists $\boldsymbol{b} \in \mathcal{G}_{n,n-1}(\boldsymbol{a})^\perp$ with $w_R(\boldsymbol{b}) = n$ such that $\mathcal{G}_{n,k}(\boldsymbol{a})^\perp = \mathcal{G}_{n,n-k}(\boldsymbol{b})$. We define

$$\boldsymbol{g} = \boldsymbol{b} P_0, \boldsymbol{h} = \boldsymbol{b} P_1.$$

As for the triple $(\gamma, \boldsymbol{g}, \boldsymbol{h})$, the authors made the following two assumptions:

(1) $\mathcal{G}_{n,n-k+2}(\boldsymbol{g}) \cap \mathcal{G}_{n,n-k+2}(\boldsymbol{h}) = \{\boldsymbol{0}\}$ and $w_R(\boldsymbol{g}), w_R(\boldsymbol{h}) \geq n - k + 2$;
(2) $m > 2$ and γ is not contained in any proper subfield of $\mathbb{F}_{q^m}$.

The rationality for these two assumptions can be explained as follows. According to the authors' experiments in MAGMA [10], Assumption (1) holds with an extremely high probability. Apparently $m > 2$ is reasonable because of $m \geqslant n$. On the other hand, if γ is contained in some proper subfield of $\mathbb{F}_{q^m}$, then the adversary can find γ through the exhausting method for the reason that even the union of all proper subfields of $\mathbb{F}_{q^m}$ contains much less elements than $\mathbb{F}_{q^m}$. Hence γ cannot be contained in any proper subfield of $\mathbb{F}_{q^m}$.

The core of Coggia–Couvreur attack is to find the triple $(\gamma, \boldsymbol{g}, \boldsymbol{h})$ or its equivalent form (see [13] for more details). And with the knowledge of the triple $(\gamma, \boldsymbol{g}, \boldsymbol{h})$ or its equivalent form, one can decrypt any ciphertext in polynomial time and therefore completely break Loidreau's cryptosystem.

The following two lemmas are useful for analysing the security of our modifications.

Lemma 2 [13] *The code $\mathcal{C}_{pub}^{\perp}$ is spanned by*

$$\boldsymbol{g}+\gamma\boldsymbol{h}, \boldsymbol{g}^{[1]}+\gamma\boldsymbol{h}^{[1]}, \cdots, \boldsymbol{g}^{[n-k-1]}+\gamma\boldsymbol{h}^{[n-k-1]}. \tag{2}$$

Lemma 3 [13] *Under Assumption* (1), *we have that $\mathcal{C}_{pub}^{\perp}+\mathcal{C}_{pub}^{\perp\ [1]}$ is spanned by*

$$\boldsymbol{g}+\gamma\boldsymbol{h} \text{ and } \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]}, \cdots, \boldsymbol{g}^{[n-k-1]}, \boldsymbol{h}^{[n-k-1]} \text{ and } \boldsymbol{g}^{[n-k]}+\gamma^{[1]}\boldsymbol{h}^{[n-k]},$$

and

$$(\mathcal{C}_{pub}^{\perp}+\mathcal{C}_{pub}^{\perp\ [1]}) \cap (\mathcal{C}_{pub}^{\perp\ [1]}+\mathcal{C}_{pub}^{\perp\ [2]})$$

is spanned by

$$\boldsymbol{g}^{[1]}+\gamma^{[1]}\boldsymbol{h}^{[1]} \text{ and } \boldsymbol{g}^{[2]}, \boldsymbol{h}^{[2]}, \cdots, \boldsymbol{g}^{[n-k-1]}, \boldsymbol{h}^{[n-k-1]} \text{ and } \boldsymbol{g}^{[n-k]}+\gamma^{[1]}\boldsymbol{h}^{[n-k]}.$$

Remark 2 Similar to Lemma 3, it is easy to verify that

$$(\mathcal{C}_{pub}^{\perp}+\mathcal{C}_{pub}^{\perp\ [1]}) \cap (\mathcal{C}_{pub}^{\perp\ [1]}+\mathcal{C}_{pub}^{\perp\ [2]}) \cap \cdots \cap (\mathcal{C}_{pub}^{\perp\ [n-k-1]}+\mathcal{C}_{pub}^{\perp\ [n-k]}) \tag{3}$$

yields a code spanned by

$$\boldsymbol{g}^{[n-k-1]}+\gamma^{[n-k-1]}\boldsymbol{h}^{[n-k-1]} \text{ and } \boldsymbol{g}^{[n-k]}+\gamma^{[1]}\boldsymbol{h}^{[n-k]}. \tag{4}$$

The key point for Coggia–Couvreur attack is that one can obtain (4) by computing (3). But if $\mathcal{C}_{pub}^{\perp\ [i]}+\mathcal{C}_{pub}^{\perp\ [i+1]}(0 \leqslant i \leqslant n-k-1)$ happens to be the full space $\mathbb{F}_{q^m}^n$, computing (4) will lead to nothing but the full space itself, which means that Coggia-Couvreur attack will fail in this situation. Our first modification for Loidreau's cryptosystem is inspired by this observation. On the other hand, if $\mathcal{C}_{pub}^{\perp}$ does not contain the full code spanned by (2), then one cannot obtain (4) from (3) either even if $\mathcal{C}_{pub}^{\perp\ [i]}+\mathcal{C}_{pub}^{\perp\ [i+1]}(0 \leqslant i \leqslant n-k-1)$ is not the full space. Modification II is based on this observation and this is true according to our analysis in Sect. 6.

5 Our modifications

In code-based cryptography, randomness is widely used in both the key generation and encryption procedures. In terms of the intersection of a given linear code and a randomly chosen linear space, we have the following proposition.

Proposition 5 *Let n, k, l be positive integers with $k+l<n$. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be some fixed linear code of dimension k, and $\mathcal{V}$ be a randomly and uniformly chosen subspace of $\mathbb{F}_{q^m}^n$ of dimension l. Then with high probability, we have $\mathcal{C} \cap \mathcal{V} = \{\mathbf{0}\}$.*

Remark 3 Proposition 5 states a fact that for a linear code $\mathcal{C}$ and a randomly chosen linear space $\mathcal{V}$, we have that $\mathcal{C} \cap \mathcal{V} = \{\mathbf{0}\}$ with high probability. Meanwhile, it is reasonable to conclude that for a $k \times n$ full-rank matrix H and a randomly chosen $l \times n$

full-rank matrix A with $k+l<n$, the block matrix $\begin{pmatrix} A \\ H \end{pmatrix}$ has full rank with high probability.

5.1 Description of Modification I

For a desired security level, choose a finite field $\mathbb{F}_q$ and positive integers $\lambda \ll k < n \leqslant m$ and $l \geqslant k - \frac{n}{2}$. Our first modification consists of the following three procedures.

- Key generation
  Randomly choose $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{a}) = n$. Let $\mathcal{G} = \mathcal{G}_{n,k}(\boldsymbol{a})$ be an $[n, k]$ Gabidulin code with H as a parity-check matrix. Randomly choose $A \in \mathcal{M}_{l,n}(\mathbb{F}_{q^m})$ of full rank and set $H_{sub} = \begin{pmatrix} A \\ H \end{pmatrix}$. By Remark 3, H_{sub} has rank $n-k+l$ with high probability. Let G_{sub} be a generator matrix of $\langle H_{sub} \rangle_{q^m}^{\perp}$, which is actually a subcode of $\mathcal{G}$ of dimension $k' = k - l$. Randomly choose an $\mathbb{F}_q$-linear space $\mathcal{V} \subseteq \mathbb{F}_{q^m}$ with $\dim_q(\mathcal{V}) = \lambda$ and $P \in GL_n(\mathcal{V})$ with $w_R(P) = \lambda$. Without loss of generality, we assume that the submatrix of $G_{sub}P^{-1}$ from the first k' columns is invertible. Choose a matrix $S \in GL_{k'}(\mathbb{F}_{q^m})$ to change $G_{pub} = SG_{sub}P^{-1}$ into systematic form. We publish (G_{pub}, t) as the public key where $t = \lfloor \frac{n-k}{2\lambda} \rfloor$, and keep $(\boldsymbol{a}, P)$ as the private key.
- Encryption
  For a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^{k'}$, randomly choose $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{e}) = t$. Then the ciphertext corresponding to $\boldsymbol{m}$ is computed as $\boldsymbol{c} = \boldsymbol{m}G_{pub} + \boldsymbol{e}$.
- Decryption
- For a ciphertext $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$, compute $\boldsymbol{c}' = \boldsymbol{c}P = \boldsymbol{m}SG_{sub} + \boldsymbol{e}P$. Since $w_R(\boldsymbol{e}P) \leqslant w_R(\boldsymbol{e}) \cdot \lambda \leqslant \lfloor \frac{n-k}{2} \rfloor$. Applying the decoder of $\mathcal{G}$ to $\boldsymbol{c}'$ leads to $\boldsymbol{e}' = \boldsymbol{e}P$, then we compute $\boldsymbol{e} = \boldsymbol{e}'P^{-1}$. The restriction of $\boldsymbol{c} - \boldsymbol{e}$ to the first k' coordinates will be $\boldsymbol{m}$.

Remark 4 According to the analysis in Sect. 4.2, we can always suppose $1 \in \mathcal{V}$. If $\lambda = 1$, then $\mathcal{V} = \mathbb{F}_q$ and $P^{-1} \in GL_n(\mathbb{F}_q)$, which implies that G_{pub} spans a subcode of $\mathcal{G}$. Then one can exploit the r-Frobenius weak attack [29] to this modification. To prevent this attack, we should make sure that $\lambda \geqslant 2$ in Modification I.

5.2 Description of Modification II

For a desired security level, choose a finite field $\mathbb{F}_q$ and positive integers $\lambda \ll k < n \leqslant m$ and $l \ll \min\{k, n-k\}$. Our second modification consists of the following three procedures.

– Key generation

  Randomly choose $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{a}) = n$. Let $\mathcal{G} = \mathcal{G}_{n,k}(\boldsymbol{a})$ be an $[n, k]$ Gabidulin code with G as a generator matrix. Randomly choose $M \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ with $\mathrm{Clr}_q(M) = l$ and let $G_M = G + M$. It is easy to see that G_M is of full rank. Randomly choose an $\mathbb{F}_q$-linear space $\mathcal{V} \subseteq \mathbb{F}_{q^m}$ with $\dim_q(\mathcal{V}) = \lambda$ and $P \in GL_n(\mathcal{V})$ with $w_R(P) = \lambda$. Without loss of generality, we assume that the submatrix of $G_M P^{-1}$ from the first k columns is invertible. Choose a matrix $S \in GL_k(\mathbb{F}_{q^m})$ to change $G_{pub} = SG_M P^{-1}$ into systematic form. We publish (G_{pub}, t) as the public key where $t = \lfloor \frac{n-k-2l}{2\lambda} \rfloor$, and keep (S, G, P) as the private key.

– Encryption

  For a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$, randomly choose a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $w_R(\boldsymbol{e}) = t$. Then the ciphertext corresponding to $\boldsymbol{m}$ is computed as $\boldsymbol{c} = \boldsymbol{m}G_{pub} + \boldsymbol{e}$.

– Decryption

  For a ciphertext $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$, compute $\boldsymbol{c}' = \boldsymbol{c}P = \boldsymbol{m}SG + \boldsymbol{m}SM + \boldsymbol{e}P$. Because of

$$w_R(\boldsymbol{m}SM + \boldsymbol{e}P) \leqslant w_R(\boldsymbol{m}SM) + w_R(\boldsymbol{e}P) \leqslant l + \lambda t \leqslant \lfloor \frac{n-k}{2} \rfloor,$$

  applying the decoder of $\mathcal{G}$ to $\boldsymbol{c}'$ will lead to $\boldsymbol{m}SG$. Then the plaintext $\boldsymbol{m}$ can be recovered by solving the linear system $\boldsymbol{m}G_{pub} = \boldsymbol{c} - \boldsymbol{e}$ with a complexity of $\mathcal{O}(n^3)$.

Remark 5 With a similar analysis as in Remark 4, we should make sure that $\lambda \geqslant 2$ in this modification. Otherwise, Modification II can be reduced to the GPT cryptosystem that has been completely broken.

6 Security analysis

We now discuss the security of our two modifications in the following two cases, namely the structural attacks and the generic attacks.

6.1 Structural attacks

These attacks aim to recover the code structure or an equivalent private key from the public information. In [38], Loidreau's cryptosystem was shown to resist the invariant subspace attack, which is also known as Overbeck's attack. Note that our modifications exploit the same technique to disguise the structure of Gabidulin code, naturally we believe that our modifications can also prevent Overbeck's attack.

Loidreau [38] proposed an exponential attack to recover an efficient decoder of the public code for the case of $m = n$, which requires a complexity of $\mathcal{O}\big(((m-k)^2 m + \lambda m^2)^3 q^{(\lambda-1)m-(\lambda-1)^2}\big)$. In a talk [39] at CBCrypto 2021, Loidreau modified this attack to deal with the general case where $m = n$ is not a must, requiring a complexity of $\mathcal{O}\big(((n-k)^2 m + \lambda nm)^3 q^{(\lambda-1)m-(\lambda-1)^2}\big)$. When applying this modified attack to Modification I, we obtain a complexity of

$$\mathcal{O}\big(((n-k)(n-k+l)m+\lambda nm)^3 q^{(\lambda-1)m-(\lambda-1)^2}\big).$$

For Modification II, things are a little more complicated. Note that $\mathrm{Clr}_q(M)=l$, there exists $T\in GL_n(\mathbb{F}_q)$ such that $MT=[M^*|0]$ where $M^*\in\mathcal{M}_{k,l}(\mathbb{F}_{q^m})$ with $\mathrm{Clr}_q(M^*)=l$. Let $P'=PT$, then $G_{pub}=S[G_{lt}+M^*|G_{rt}]P'^{-1}$, where G_{lt} denotes the left most l columns of GT and G_{rt} the right most $n-l$ columns respectively. It is clear that G_{rt} generates an $[n-l,k]$ Gabidulin code, denoted by $\mathcal{G}_{rt}$. Let $H_{pub}\in\mathcal{M}_{n-k,n}(\mathbb{F}_{q^m})$ be a parity-check matrix of $\mathcal{C}_{pub}$, then H_{pub} can be expressed as

$$H_{pub}=\begin{pmatrix} A \\ 0|\,H_{rt}\end{pmatrix}P'^T, \tag{5}$$

where $A\in\mathcal{M}_{l,n}(\mathbb{F}_{q^m})$ and $H_{rt}\in\mathcal{M}_{n-k-l,n-l}(\mathbb{F}_{q^m})$ forms a parity-check matrix of $\mathcal{G}_{rt}$. Let $H_{mr}\in\mathcal{M}_{n-l-k,m}(\mathbb{F}_{q^m})$ be a Moore matrix generated by a vector whose components form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is easy to see that there exists $Q\in\mathcal{M}_{n,m}(\mathbb{F}_q)$ and $S'\in\mathcal{M}_{n-l-k,n-k}(\mathbb{F}_{q^m})$ such that

$$S'H_{pub}=H_{mr}Q^TP'^T=H_{mr}P''^T,$$

where $P''=P'Q$ and clearly $\mathrm{Supp}(P')=\mathrm{Supp}(P'')$. With a similar analysis to [39], one obtains a linear system of $(n-l-k)n$ equations and $(n-k)(n-k-l)m+\lambda mn$ variables by enumerating $\lambda-1$-dimensional supspaces of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The complexity of this attack is

$$\mathcal{O}\big(((n-k)(n-k-l)m+\lambda mn)^3 q^{(\lambda-1)m-(\lambda-1)^2}\big).$$

In the remaining part, we explain why our two modifications can prevent the Coggia-Couvreur attack. Firstly, we introduce a distinguisher for the public code of Loidreau's cryptosystem.

Proposition 6 [13] *For an instance of Loidreau's cryptosystem with parameters* (m,n,k,λ), *the dual of the public code satisfies*

$$\dim_{q^m}(\mathcal{C}_{pub}^{\perp}+\mathcal{C}_{pub}^{\perp\,[1]}+\cdots+\mathcal{C}_{pub}^{\perp\,[\lambda]})\leqslant\lambda\dim_{q^m}(\mathcal{C}_{pub}^{\perp})+\lambda.$$

However, for a random linear code we have the following proposition.

Proposition 7 [13] *For an* $[n,k]$ *random linear code* $\mathcal{C}_{rand}\subseteq\mathbb{F}_{q^m}^n$, *the following equality holds with high probability*

$$\dim_{q^m}(\mathcal{C}_{rand}^{\perp}+\mathcal{C}_{rand}^{\perp\,[1]}+\cdots+\mathcal{C}_{rand}^{\perp\,[\lambda]})=\min\{n,(\lambda+1)(n-k)\}.$$

6.1.1 Analysis of Modification I

Firstly, we shall introduce the following proposition.

Proposition 8 *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $[n, k]$ linear code that has G as a generator matrix. For any integer s, $\mathcal{C}^{[s]}$ is also an $[n, k]$ linear code over $\mathbb{F}_{q^m}$ and has $G^{[s]}$ as a generator matrix.*

Proof The proof is trivial and therefore omitted here. □

Let $\mathcal{C}_{pub} = \langle G_{pub} \rangle_{q^m}$ be the public code of Modification I. Now we show that $\mathcal{C}_{pub}^{\perp\ [i]} + \mathcal{C}_{pub}^{\perp\ [i+1]}$ $(0 \leqslant i \leqslant n-k-1)$ is exactly the full space $\mathbb{F}_{q^m}^n$, namely all these $n-k$ codes have dimension n. By Proposition 8, it suffices to compute the dimension of $\mathcal{C}_{pub}^{\perp} + \mathcal{C}_{pub}^{\perp\ [1]}$.

Let H_{pub} be a parity-check matrix of $\mathcal{C}_{pub}$, then $H_{pub} = H_{sub}P^T$ and

$$\mathcal{C}_{pub}^{\perp} = \langle H_{sub}P^T \rangle_{q^m} = \langle HP^T \rangle_{q^m} + \langle AP^T \rangle_{q^m}.$$

Hence

$$\mathcal{C}_{pub}^{\perp} + \mathcal{C}_{pub}^{\perp\ [1]} = \langle HP^T \rangle_{q^m} + \langle HP^T \rangle_{q^m}^{[1]} + \langle AP^T \rangle_{q^m} + \langle AP^T \rangle_{q^m}^{[1]}.$$

According to Lemma 3, $\langle HP^T \rangle_{q^m} + \langle HP^T \rangle_{q^m}^{[1]}$ is spanned by

$$\boldsymbol{g} + \gamma \boldsymbol{h} \text{ and } \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]}, \cdots, \boldsymbol{g}^{[n-k-1]}, \boldsymbol{h}^{[n-k-1]} \text{ and } \boldsymbol{g}^{[n-k]} + \gamma^{[1]}\boldsymbol{h}^{[n-k]}, \tag{6}$$

where $\gamma, \boldsymbol{g}$ and $\boldsymbol{h}$ are defined as in Sect. 4.

Note that these $2(n-k)$ vectors in (6) are linearly independent over $\mathbb{F}_{q^m}$. Indeed, if there exist $x_i, y_i \in \mathbb{F}_{q^m}$ $(0 \leqslant i \leqslant n-k-1)$ such that

$$x_0(\boldsymbol{g} + \gamma\boldsymbol{h}) + y_0(\boldsymbol{g}^{[n-k]} + \gamma^{[1]}\boldsymbol{h}^{[n-k]}) + \sum_{i=1}^{n-k-1} x_i\boldsymbol{g}^{[i]} + \sum_{i=1}^{n-k-1} y_i\boldsymbol{h}^{[i]} = \boldsymbol{0}.$$

Then we have

$$y_0\boldsymbol{g}^{[n-k]} + \sum_{i=0}^{n-k-1} x_i\boldsymbol{g}^{[i]} = -x_0\gamma\boldsymbol{h} - y_0\gamma^{[1]}\boldsymbol{h}^{[n-k]} - \sum_{i=1}^{n-k-1} y_i\boldsymbol{h}^{[i]}.$$

It is clear that $y_0\boldsymbol{g}^{[n-k]} + \sum_{i=0}^{n-k-1} x_i\boldsymbol{g}^{[i]} \in \mathcal{G}_{n,n-k+2}(\boldsymbol{g})$ and $-x_0\gamma\boldsymbol{h} - y_0\gamma^{[1]}\boldsymbol{h}^{[n-k]} - \sum_{i=1}^{n-k-1} y_i\boldsymbol{h}^{[i]} \in \mathcal{G}_{n,n-k+2}(\boldsymbol{h})$. Hence $x_i = y_i = 0\,(0 \leqslant i \leqslant n-k-1)$ because of Assumption (1).

By Proposition 3, we have that $\dim_{q^m}(\langle AP^T \rangle_{q^m} + \langle AP^T \rangle_{q^m}^{[1]}) = 2l$ holds with high probability. Together with $l \geqslant k - \frac{n}{2}$ and Proposition 5, we have that $\dim_{q^m}(\mathcal{C}_{pub}^{\perp} + \mathcal{C}_{pub}^{\perp\ [1]}) = n = \min\{2(n-k+l), n\}$. Furthermore, we have $\dim_{q^m}(\mathcal{C}_{pub}^{\perp\ [i-1]} + \mathcal{C}_{pub}^{\perp\ [i]}) = n$ because of Proposition 8, or equivalently $\mathcal{C}_{pub}^{\perp\ [i-1]} + \mathcal{C}_{pub}^{\perp\ [i]} = \mathbb{F}_{q^m}^n$ for $1 \leqslant i \leqslant n-k$, which means that by computing the intersection (3) the adversary can obtain nothing but the full space itself. Hence Coggia-Couvreur attack will fail in this situation.

6.1.2 Analysis of Modification II

Note that $\mathrm{Clr}_q(M) = l$, then $1 \leqslant \mathrm{Rank}(M) \leqslant l$. Assume that $\mathrm{Rank}(M) = l'$, then $\dim_{q^m}(\langle M\rangle_{q^m}) = l' \leqslant l$. By Proposition 2, we have $w_R(\boldsymbol{v}) \leqslant l$ for any $\boldsymbol{v} \in \langle M\rangle_{q^m}$. Together with $d(\mathcal{G}) = n-k+1 \gg l$, we have $\langle M\rangle_{q^m} \cap \mathcal{G} = \{\mathbf{0}\}$.

Let $\mathcal{C}_{pub} = \langle G_{pub}\rangle_{q^m} = \langle SG_M P^{-1}\rangle_{q^m}$, then a parity-check matrix for $\mathcal{C}_{pub}$ can be written as $H_{pub} = H_M P^T$, where H_M is an $(n-k)\times n$ full-rank matrix such that $SG_M H_M^T = 0$. It is easy to see that $\langle H_M\rangle_{q^m}$ contains a subcode of $\mathcal{G}^\perp$ of dimension $n-k-l'$. Hence $\mathcal{C}_{pub}^\perp$ contains a subcode of $\mathcal{C}_1$ of dimension $n-k-l'$, where $\mathcal{C}_1$ is spanned by

$$\boldsymbol{g}+\gamma\boldsymbol{h}, \boldsymbol{g}^{[1]}+\gamma\boldsymbol{h}^{[1]}, \cdots, \boldsymbol{g}^{[r]}+\gamma\boldsymbol{h}^{[r]}, \text{ where r=n-k-1.}$$

Similarly ${\mathcal{C}_{pub}^\perp}^{[1]}$ contains a subcode of $\mathcal{C}_2$ of dimension $n-k-l'$, where $\mathcal{C}_2$ is spanned by

$$\boldsymbol{g}^{[1]}+\gamma^{[1]}\boldsymbol{h}^{[1]}, \boldsymbol{g}^{[2]}+\gamma^{[1]}\boldsymbol{h}^{[2]}, \cdots, \boldsymbol{g}^{[r+1]}+\gamma^{[1]}\boldsymbol{h}^{[r+1]}.$$

Finally we have that $\mathcal{C}_{pub}^\perp + {\mathcal{C}_{pub}^\perp}^{[1]}$ contains a subcode of $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$ of dimension at most $2(n-k-l')$, where $\mathcal{C}$ is spanned by

$$\boldsymbol{g}+\gamma\boldsymbol{h} \text{ and } \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]}, \cdots, \boldsymbol{g}^{[r]}, \boldsymbol{h}^{[r]} \text{ and } \boldsymbol{g}^{[r+1]}+\gamma^{[1]}\boldsymbol{h}^{[r+1]}.$$

In Coggia–Couvreur attack, the adversary can obtain (4) by computing (3). Our analysis shows that the adversary cannot perform the same operation on Modification II to obtain (4). Here we demonstrate this point with the method of reduction to absurdity.

Assume that

$$\langle \boldsymbol{g}^{[r]}+\gamma^{[r]}\boldsymbol{h}^{[r]}, \boldsymbol{g}^{[r+1]}+\gamma^{[1]}\boldsymbol{h}^{[r+1]}\rangle_{q^m} \subseteq \bigcap_{i=0}^{r}(\mathcal{C}_{pub}^{\perp\,[i]} + \mathcal{C}_{pub}^{\perp\,[i+1]}). \tag{7}$$

Then for any $0 \leqslant i \leqslant r$, we have

$$\boldsymbol{g}^{[r]}+\gamma^{[r]}\boldsymbol{h}^{[r]}, \boldsymbol{g}^{[r+1]}+\gamma^{[1]}\boldsymbol{h}^{[r+1]} \in \mathcal{C}_{pub}^{\perp\,[i]} + \mathcal{C}_{pub}^{\perp\,[i+1]}. \tag{8}$$

Applying the inverse of the i-th Frobenius map to both sides of (8), there will be

$$\boldsymbol{g}^{[r-i]}+\gamma^{[r-i]}\boldsymbol{h}^{[r-i]}, \boldsymbol{g}^{[r-i+1]}+\gamma^{[1-i]}\boldsymbol{h}^{[r-i+1]} \in \mathcal{C}_{pub}^\perp + {\mathcal{C}_{pub}^\perp}^{[1]},$$

or equivalently

$$\boldsymbol{g}+\gamma\boldsymbol{h} \text{ and } \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]}, \cdots, \boldsymbol{g}^{[r]}, \boldsymbol{h}^{[r]} \text{ and } \boldsymbol{g}^{[r+1]}+\gamma^{[1]}\boldsymbol{h}^{[r+1]} \in \mathcal{C}_{pub}^\perp + {\mathcal{C}_{pub}^\perp}^{[1]}.$$

This implies that $\mathcal{C} \subseteq \mathcal{C}_{pub}^\perp + {\mathcal{C}_{pub}^\perp}^{[1]}$, which conflicts with the previous conclusion that $\mathcal{C}_{pub}^\perp + {\mathcal{C}_{pub}^\perp}^{[1]}$ contains a subcode of $\mathcal{C}$ of dimension at most $2(n-k-l')$. Hence

the Assumption (7) cannot be true and therefore the adversary cannot recover (4) from (3) as Coggia–Couvreur attack on Loidreau's cryptosystem. Therefore Coggia–Couvreur attack does not work on Modification II.

Furthermore, we show that the distinguisher based on Propositions 6 and 7 does not work on Modification II for properly chosen parameters. Here we follow the notation introduced in (5). Let $\mathcal{C}_0 = \langle AP'^T \rangle$ and $\mathcal{C}_1 = \langle [0|H_{rl}]P'^T \rangle$, then $\mathcal{C}_{pub}^{\perp} = \mathcal{C}_0 + \mathcal{C}_1$. It is easy to see that

$$\dim(\mathcal{C}_0 + \mathcal{C}_0^{[1]} + \cdots + \mathcal{C}_0^{[\lambda]}) = (\lambda+1)l \text{ and } \dim(\mathcal{C}_1 + \mathcal{C}_1^{[1]} + \cdots + \mathcal{C}_1^{[\lambda]}) = \lambda(n-k-l) + \lambda,$$

then with high probability

$$\dim(\mathcal{C}_{pub}^{\perp} + \mathcal{C}_{pub}^{\perp\,[1]} + \cdots + \mathcal{C}_{pub}^{\perp\,[\lambda]}) = (\lambda+1)l + \lambda(n-k-l) + \lambda = \lambda(n-k) + \lambda + l.$$

Together with Proposition 7, we conclude that if the parameters are chosen such that $n \leqslant \min\{\lambda(n-k) + \lambda + l, (\lambda+1)(n-k)\}$, then one cannot distinguish the public code $\mathcal{C}_{pub}$ from random ones.

6.2 Generic attacks

In the context of code-based cryptography, an adversary without the private key has to deal with the problem of decoding general linear codes or equivalently the syndrome decoding problem, which has been proved to be NP-complete by Berlekamp et al. in [8]. However, the general decoding problem in the rank metric, or equivalently the rank syndrome decoding (RSD) problem, is not known to be NP-complete. In the paper [25], the authors proved that a randomized reduction exists from the RSD problem to the general decoding problem in the Hamming metric.

In what follows, we will first introduce the RSD problem in coding theory, then present two types of attacks on this problem, namely the combinatorial attack and the algebraic attack. After that, we will establish a connection between our modifications and the RSD problem.

Definition 7 (Rank syndrome decoding (RSD) problem) For positive integers m, n, k and t, let $H \in \mathcal{M}_{n-k,n}(\mathbb{F}_{q^m})$ with full rank and $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$. The RSD problem $\mathcal{R}(q,m,n,k,t)$ is to search for $\boldsymbol{x} \in \mathbb{F}_{q^m}^{n}$ such that $\boldsymbol{s} = \boldsymbol{x}H^T$ and $w_R(\boldsymbol{x}) \leqslant t$.

Table 1 Best known combinatorial attacks on the RSD problem

Attack	Complexity
[45]	$\mathcal{O}\left(\min\left\{m^3t^3q^{(t-1)(k+1)}, (k+t)^3t^3q^{(t-1)(m-t)}\right\}\right)$
[24]	$\mathcal{O}\left((n-k)^3m^3q^{\min\left\{t\left\lceil\frac{mk}{n}\right\rceil,(t-1)\left\lceil\frac{m(k+1)}{n}\right\rceil\right\}}\right)$
[3]	$\mathcal{O}\left((n-k)^3m^3q^{t\left\lceil\frac{m(k+1)}{n}\right\rceil-m}\right)$

Table 2 Best known algebraic attacks on the RSD problem

Attack	Condition	Complexity
[24]	$\left\lceil \frac{(t+1)(k+1)-(n+1)}{t} \right\rceil \leqslant k$	$\mathcal{O}\left(k^3 t^3 q^{\left\lceil \frac{(t+1)(k+1)-(n+1)}{t} \right\rceil}\right)$
[7]	$m\binom{n-k-1}{t} \geqslant \binom{n}{t} - 1$	$\mathcal{O}\left(m\binom{n-p-k-1}{t}\binom{n-p}{t}^{\omega-1}\right)$, where $p = \max\{1 \leqslant i \leqslant n : m\binom{n-i-k-1}{t} \geqslant \binom{n-i}{t} - 1\}$
[6]		$\mathcal{O}\left(\left(\frac{((m+n)t)^t}{t!}\right)^{\omega}\right)$
[7]	$m\binom{n-k-1}{t} < \binom{n}{t} - 1$	$\mathcal{O}\left(q^{at} m\binom{n-k-1}{t}\binom{n-a}{t}^{\omega-1}\right)$, where $a = \min\{1 \leqslant i \leqslant n : m\binom{n-k-1}{t} \geqslant \binom{n-i}{t} - 1\}$
[6]		$\mathcal{O}\left(\left(\frac{((m+n)t)^{t+1}}{(t+1)!}\right)^{\omega}\right)$

The main idea of combinatorial attacks consists in solving a multivariate linear system obtained from the parity-check equation, whose variables are components of $e_i\,(1 \leqslant i \leqslant n)$ with respect to a potential support of $\boldsymbol{e}$. Up to now, the best known combinatorial attacks can be found in [3, 24, 45], as summarized in Table 1.

As for the algebraic attack, the main idea consists in converting an RSD instance into a quadratic system and then solving this system using algebraic approaches. Here in this paper, we mainly consider the attacks proposed in [6, 7, 24], whose complexity and applicable condition are summarized in Table 2, where $\omega = 2.81$ is the linear algebra constant.

Conversion into an RSD instance. For Modification I, let $H_{pub} \in \mathcal{M}_{n-k+l,n}$ be a parity-check matrix of the public code. Let $\boldsymbol{c} = \boldsymbol{m}G_{pub} + \boldsymbol{e}$ be a valid ciphertext, then compute $\boldsymbol{s} = \boldsymbol{c}H_{pub}^T = \boldsymbol{e}H_{pub}^T$. This implies that we obtain an RSD instance of parameters $(q, m, n, k-l, t)$. A similar analysis of Modification II leaves us an

Table 3 Parameters and public key size (in bytes)

Instance	Parameters					Key size	Security
	q	m	n	k	l		
Modification I	2	85	85	43	2	19168	136
	2	98	98	50	3	29364	203
	2	121	121	61	4	55176	276
Modification II	2	88	88	48	2	21120	132
	2	98	98	52	2	29302	192
	2	129	129	65	2	67080	279

Table 4 Comparison on public-key sizes (in bytes)

Security	128 bits	192 bits	256 bits
Instance			
HQC	2249	4522	7245
BIKE	1540	3082	5121
Classic McEliece	261120	524160	1044992
Modification I	19168	29364	55176
Modification II	21120	29302	67080

RSD instance of parameters (q, m, n, k, t). Apparently these two instances both have a unique solution because of the uniqueness of the decrypting process.

7 Parameters and public key sizes

Now we consider the practical security of our two modifications and give some suggested parameters. In Modification I, the public key is a systematic generator matrix of an $[n, k-l]$ rank metric code, resulting in a public-key size of $(k-l)(n-k+l)\cdot m\log_2(q)$ bits. In Modification II, the public key is a systematic generator matrix of an $[n, k]$ rank metric code, resulting in a public-key size of $k(n-k)\cdot m\log_2(q)$ bits.

In Table 3, we suggest some parameters for security of at least 128 bits, 192 bits, and 256 bits. When considering the practical security, we consider the complexity assessment of the structural attacks presented in Sect. 6.1, as well as the complexity of generic attacks described in Sect. 6.2. In Table 4, we make a comparison on public-key sizes with some other code-based cryptosystems that have been selected as the fourth round candidates of the NIST PQC Standardization Process. These candidates are HQC [42], BIKE [2], and Classic McEliece [1]. From Table 4 we can see that our modifications behave pretty well in public-key representation compared to Classic McEliece without using codes endowed with the cyclic or quasi-cyclic structure.

8 Conclusion

In this paper, we have presented two simple but effective approaches to repair Loidreau's cryptosystem. According to our analysis, both of these two modifications can resist the existing structural attacks designed for cryptosystems based on Gabidulin codes, including Overbeck's attack and Coggia–Couvreur attack. Additionally, our two modifications have an obvious advantage in public-key representation compared to some code-based cryptosystems that have been selected into the fourth round of the NIST PQC project.

Acknowledgements The authors are very grateful to Editor Prof. Teo Mora and the reviewers for their valuable comments and suggestions that greatly improved the presentation and quality of this paper. This research is supported by the National Key Research and Development Program of China (Grant No. 2018YFA0704703), the National Natural Science Foundation of China (Grant No. 61971243), the Natural Science Foundation of Tianjin (20JCZDJC00610), and the Fundamental Research Funds for the Central Universities of China (Nankai University).

References

1. Albrecht, M.R., Bernstein, D.J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C.J., Tomlinson, M., Wang, W.: Classic McEliece: conservative code-based cryptography. https://classic.mceliece.org/nist/mceliece-20201010.pdf. Accessed October 10 (2020)
2. Aragon, N., Barreto, P.S., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T., Melchor, C.A., Misoczki, R., Persichetti, E., Sendrier, Tillich, J.-P., N., Vasseur, V., Zémor, G.: BIKE: bit flipping key encapsulation. https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf. Accessed October 10 (2020)
3. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.-P.: A new algorithm for solving the rank syndrome decoding problem. In: Proceedings of ISIT 2018, pp. 2421–2425. IEEE (2018)
4. Augot, D., Finiasz, M.: A public key encryption scheme based on the polynomial reconstrution problem. In: Biham, E. (ed.): Proceedings of EUROCRYPT 2003, LNCS, vol. 2656, pp. 229–240. Springer (2003)
5. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D.: Enhanced public key security for the McEliece cryptosystem. J. Cryptol. **29**(1), 1–27 (2016)
6. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.-P.: An algebraic attack on rank metric code-based cryptosystems. In: Proceedings of EUROCRYPT 2020, LNCS, vol. 12107, pp. 64–93. Springer (2020)
7. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.-P., Verbel, J.: Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In: Proceedings of ASIACRYPT 2020, LNCS, vol. 12491, pp. 507–536. Springer (2020)
8. Berlekamp, E.R., McEliece, R.J., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory **24**(3), 384–386 (1978)
9. Bombar, M., Couvreur, A.: Decoding supercodes of Gabidulin codes and applications to cryptanalysis. In: Proceedings of PQCrypto 2021, LNCS, vol. 12841, pp. 3–22. Springer (2021)
10. Bosma, W., Cannon, J., Playoust, C.: The MAGMA algebra system I: The user language. J. Symbolic Comput. **24**(3–4), 235–265 (1997)
11. Canteaut, A., Sendrier, N.: Cryptanalysis of the original McEliece cryptosystem. In: Ohta, K., Pei, D. (eds.): Proceedings of ASIACRYPT 1998, LNCS, vol. 1514, pp. 187–199. Springer (2000)
12. Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Proceedings of ASIACRYPT 1996, pp. 368–381. Springer (1996)
13. Coggia, D., Couvreur, A.: On the security of a Loidreau rank metric code based encryption scheme. Des. Codes Cryptogr. **88**(9), 1941–1957 (2020)
14. Couvreur, A., Gaborit, P., Otmani, A., Tillich, J.-P.: Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. Des. Codes Cryptogr. **73**(2), 641–666 (2014)
15. Couvreur, A., Otmani, A., Tillich, J.-P., Gauthier-Umaña.: A polynomial-time attack on the BBCRS cryptosystem. In: Proceedings of PKC 2015, LNCS, vol. 9020, pp. 175–193. Springer (2015)
16. Faugère, J.-C., Otmani, A., Perret, L., de Portzamparc, F., Tillich, J.-P.: Structural cryptanalysis of McEliece schemes with compact keys. Des. Codes Cryptogr. **79**(1), 87–112 (2016)
17. Faure, C., Loidreau, P.: A new public-key cryptosystem based on the problem of reconstructing p -polynomials. In: Ytrehus, ∅. (ed.): Proceedings of WCC 2005, LNCS, vol. 3969, pp. 304–315. Springer (2005)
18. Gabidulin, E.M.: Theory of codes with maximum rank distance. Prob. Peredachi Inf. **21**(1), 3–16 (1985)
19. Gabidulin, E.M.: Attacks and counter-attacks on the GPT public key cryptosystem. Des. Codes Cryptogr. **48**(2), 171–177 (2008)

20. Gabidulin, E.M., Ourivski, A.V., Honary, B., Ammar, B.: Reducible rank codes and their applications to cryptography. IEEE Trans. Inf. Theory **49**(12), 3289–3293 (2003)
21. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their application in cryptology. In: Davies, D.W. (ed.): Proceedings of EUROCRYPT 1991, LNCS, vol. 547, pp. 482–489. Springer (1991)
22. Gabidulin, E.M., Rashwan, H., Honary, B.: On improving security of GPT cryptosystems. In: Proceedings of ISIT 2009, pp. 1110–1114. IEEE (2009)
23. Gaborit, P., Otmani, A., Kalachi, H.T.: Polynomial-time key recovery attack on the Faure–Loidreau scheme based on Gabidulin codes. Des. Codes Cryptogr. **86**(7), 1391–1403 (2018)
24. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inf. Theory **62**(2), 1006–1019 (2016)
25. Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Inf. Theory **62**(12), 7245–7252 (2016)
26. Ghatak, A.: Extending Coggia–Couvreur attack on Loidreau's rank-metric cryptosystem. Des. Codes Cryptogr. **90**(1), 215–238 (2022)
27. Gibson, K.: The security of the Gabidulin public key cryptosystem. In: Proceedings of EUROCRYPT 1996, LNCS, vol. 1070, pp. 212–223. Springer (1996)
28. Horlemann-Trautmann, A.-L., Marshall, K.: New criteria for MRD and Gabidulin codes and some rank-metric code constructions. Adv. Math. Commun. **11**(3), 533–548 (2017)
29. Horlemann-Trautmann, A.-L., Marshall, K., Rosenthal, J.: Considerations for rank-based cryptosystems. In: Proceedings of ISIT 2016, pp. 2544–2548. IEEE (2016)
30. Horlemann-Trautmann, A.-L., Marshall, K., Rosenthal, J.: Extension of Overbeck's attack for Gabidulin-based cryptosystems. Des. Codes Cryptogr. **86**(2), 319–340 (2018)
31. Kobara, K., Imai, H.: Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC. Kim, K. (ed.): Proceedings of PKC 2001, LNCS, vol. 1992, pp. 19–35. Springer (2001)
32. Lavauzelle, J., Loidreau, P., Pham, B.-D.: RAMESSES, a rank metric encryption scheme with short keys. arXiv:1911.13119 [cs.CR] (2019)
33. Lee, P.J., Brickell, E.F.: An observation on the security of McEliece's public-key cryptosystem. In: Guenther, C.G. (ed.): Proceedings of EUROCRYPT 1988, LNCS, vol. 330, pp. 275–280. Springer (1988)
34. Li, Y.X., Deng, R.H., Wang, X.M.: On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Trans. Inf. Theory **40**(1), 271–273 (1994)
35. Ling, S., Xing, C.: Coding Theory: A First Course. Cambridge University Press, Cambridge (2004)
36. Loidreau, P.: A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In: Ytrehus, ∅. (ed.): Proceedings of WCC 2005, LNCS, vol. 3969, pp. 36–45. Springer (2005)
37. Loidreau, P.: Designing a rank metric based McEliece cryptosystem. In: Sendrier, N. (ed.): Proceedings of PQCrypto 2010, LNCS, vol. 6061, pp. 142–152. Springer (2010)
38. Loidreau, P.: A new rank metric codes based encryption scheme. In: Lange, T., Takagi, T. (Eds.): Proceedings of PQCrypto 2017, LNCS, vol. 10346, pp. 3–17. Springer (2017)
39. Loidreau, P.: Analysing the key recovery complexity for a rank-metric code-based cryptosystem. https://drive.google.com/file/d/1FuMgqm0NfGMJOxaZyrIrI1OWn0UICwPo/view. Accessed July 1 (2021)
40. Loidreau, P., Sendrier, N.: Weak keys in the McEliece public-key cryptosystem. IEEE Trans. Inf. Theory **47**(3), 1207–1211 (2001)
41. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Jet Propuls. Lab. DSN Progr. Rep. **42–44**, 114–116 (1978)
42. Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bos, J., Deneuville, J.-C., Dion, A., Gaborit, P., Lacan, J., Persichetti, E., Robert, J.-M., Véron, P., Zémor, G.: Hamming quasi-cyclic (HQC). http://pqc-hqc.org/doc/hqc-specification_2020-10-01.pdf. Accessed October 10 (2020)
43. Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Prob. Control Inf. Theory **15**(2), 159–166 (1986)
44. Otmani, A., Kalachi, H.T., Ndjeya, S.: Improved cryptanalysis of rank metric schemes based on Gabidulin codes. Des. Codes Cryptogr. **86**(9), 1983–1996 (2018)
45. Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Probl. Inf. Transm. **38**(3), 237–246 (2002)
46. Overbeck, R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptol. **21**(2), 280–301 (2008)

47. Rashwan, H., Gabidulin, E.M., Honary, B.: A smart approach for GPT cryptosystem based on rank codes. In: Proceedings of ISIT 2010, pp. 2463–2467. IEEE (2010)
48. Rashwan, H., Gabidulin, E.M., Honary, B.: Security of the GPT cryptosystem and its applications to cryptography. Secur. Commun. Netw. **4**(8), 937–946 (2011)
49. Renner, J., Puchinger, S., Wachter-Zeh, A.: LIGA: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. Des. Codes Cryptogr. **89**(6), 1279–1319 (2021)
50. Richter, G., Plass, S.: Error and erasure decoding of rank-codes with a modified Berlekamp–Massey algorithm. ITG FACHBERICHT, pp. 203–210 (2004)
51. Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized Reed–Solomon codes. Discret. Math. Appl. **2**(4), 439–444 (1992)