Des. Codes Cryptogr.
DOI 10.1007/s10623-017-0434-5

Improved cryptanalysis of rank metric schemes based on Gabidulin codes

Ayoub Otmani[1] · **Hervé Talé Kalachi**[2,3] ·
Sélestin Ndjeya[3]

Received: 26 February 2016 / Revised: 19 September 2017 / Accepted: 23 October 2017

Abstract We prove that any variant of the GPT cryptosystem which uses a right column scrambler over the extension field as advocated by the works of Gabidulin et al. with the goal to resist to Overbeck's structural attack are actually still vulnerable to that attack. We show that by applying the Frobenius operator appropriately on the public key, it is possible to build a Gabidulin code having the same dimension as the original secret Gabidulin code but with a lower length. In particular, the code obtained by this way corrects less errors than the secret one but its error correction capabilities are beyond the number of errors added by a sender. Consequently, an attacker is able to decrypt any ciphertext with this degraded Gabidulin code. We also considered the case where an isometric transformation is applied in conjunction with a right column scrambler which has its entries in the extension field. We proved that this protection is useless both in terms of performance and security. Consequently, our results show that all the existing techniques aiming to hide the inherent algebraic structure of Gabidulin codes have failed.

Keywords Post-quantum cryptography · Gabidulin code · GPT encryption scheme · Overbeck's attack

Communicated by L. Storme.

✉ Ayoub Otmani
ayoub.otmani@univ-rouen.fr

Hervé Talé Kalachi
hervekalachi@gmail.com

Sélestin Ndjeya
ndjeyas@yahoo.fr

[1] LITIS (EA 4108), University of Rouen-Normandie, UFR des Sciences et des Techniques, BP 12 Avenue de l'Université, 76801 Saint-Etienne-du-Rouvray Cedex, France

[2] University of Rouen, UFR des Sciences et des Techniques, BP 12 Avenue de l'Université, 76801 Saint-Etienne-du-Rouvray Cedex, France

[3] Department of Mathematics, ERAL, University of Yaounde 1, Yaoundé, Cameroon

Published online: 02 November 2017

Mathematics Subject Classification 11T71 · 14G50

1 Introduction

The emergence of post-quantum cryptography was mainly enabled thanks to Shor [1,2] who proved that the discrete log problem and factorization can be solved in polynomial time with a hypothetical quantum computer. Recent progress in solving the discrete log problem, and the fact that important industrial investments are made to build a quantum computer have aroused concerns about the foundations of the real-world cryptography, prompting people to seek serious post-quantum alternatives.

Among all the existing solutions, McEliece scheme [3] is one of the oldest post-quantum public key encryption scheme. The innovative McEliece's approach rests on the use of the theory of error-correcting codes to design a one-way function of the form $\boldsymbol{m} \mapsto \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ where $\boldsymbol{G}$ generates a vector subspace of $\mathbb{F}_2^n$ and $\boldsymbol{e}$ being a random binary error vector of Hamming weight t_{pub}. McEliece used binary Goppa codes which are well-known for having a very fast decoding algorithm. Designed in 1978, it has withstood several attack attempts but, it suffers from an important drawback due to the enormous size of the public keys. In order to solve this problem, several modifications of the scheme have been proposed among which the use of rank metric codes instead of the Hamming metric. The first rank-metric scheme was proposed in [4] by Gabidulin, Paramonov and Tretjakov and now called the GPT cryptosystem. This scheme can be seen as an analogue of the McEliece cryptosystem based on the class of Gabidulin codes. An important operation in the key generation of the GPT cryptosystem is the "hiding" phase where the secret generator matrix $\boldsymbol{G}$ undergoes a transformation masking the inherent algebraic structure of the associated Gabidulin code. This transformation is a probabilistic algorithm that adds some randomness to its input. Originally, the authors in [4] proposed to use a *distortion* transformation that takes $\boldsymbol{G}$ and outputs the public matrix $\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}(\boldsymbol{G} + \boldsymbol{X})$ where $\boldsymbol{X}$ is a random matrix with a prescribed rank $t_{\boldsymbol{X}}$ and $\boldsymbol{S}$ is an invertible matrix. The presence of a distortion matrix has however an impact: the sender has to add an error vector whose rank weight is $t_{\text{pub}} = t - t_{\boldsymbol{X}}$ where t is the error correction capability of the secret underlying Gabidulin code. Hence, roughly speaking, the "hiding" phase publishes a degraded code in terms of error correction.

Gabidulin codes are often seen as the equivalent of Reed–Solomon codes in the Hamming metric and like them, they are highly structured. That is the reason why their use in the GPT cryptosystem has been the subject to several attacks. Gibson was the first to prove the weakness of the system through a series of successful attacks [5,6]. Following this failures, the first works which modified the GPT scheme to avoid Gibson's attack were published in [7,8]. The idea was to hide further the structure of Gabidulin code by considering isometries for the rank metric. Consequently, a *right column scrambler* $\boldsymbol{P}$ is introduced which is an invertible matrix with its entries in the base field $\mathbb{F}_q$ while the ambient space of the Gabidlun code is $\mathbb{F}_{q^m}^n$. But Overbeck designed in [9–11] a more general attack that dismantled all the existing modified GPT cryptosystems. His approach consists in applying an operator Λ_i which applies i times the Frobenius operation on the public generator matrix $\boldsymbol{G}_{\text{pub}}$. Overbeck observed that the dimension increases by 1 each time the Frobenius is applied. He then proved that by taking $i = n - k - 1$ the co-dimension becomes 1 if k is the rank of $\boldsymbol{G}_{\text{pub}}$ (which is also the dimension of the associated Gabidulin code). This phenomenon is a clearly distinguishing property of a Gabidulin code which cannot be encountered with a random linear code where the dimension would increase by k for each use of the Frobenius operator.

Overbeck's attack uses crucially two important facts, namely the column scrambler matrix $\boldsymbol{P}$ is defined on the based field $\mathbb{F}_q$ and the co-dimension of $\Lambda_{n-k-1}\left(\boldsymbol{G}_{\text{pub}}\right)$ is equal to 1. Several works then proposed to resist to this attack either by taking special distortion matrix so that the second property is not true as in [12,13], or by taking a column scrambler matrix defined over the extension field $\mathbb{F}_{q^m}$ as in [14–16].

In this paper, we study the security of the second approach. We show that, even if the column scrambler is defined on the extension field as it is done in [14–16], it is still possible to recover a secret Gabidulin code using precisely Overbeck's technique. Our analysis shows that by applying the operator Λ_i with $i < n-k-1$, we obtain a Gabidulin code whose error correction capability t^* is indeed strictly less than the error correction capability of the secret original Gabidulin code but, t^* is strictly greater than the number of added errors t_{pub}. In other words, an attacker is still able to decrypt any ciphertext and consequently, all the schemes presented in [14–16] are actually not resistant to Overbeck's attack unlike what was claimed by the authors. When the attack is implemented with the recommended parameters of [15,16], our experimental results show that the attack is extremely fast (less than one second). Moreover, our results outperform those given in [17,18] which were for a while the best attacks against the schemes of [14–16]. Note that the attacks of [17,18] are generic decoding algorithms whereas our approach is directed towards recovering the structure of a Gabidulin code.

2 Preliminary notions

The finite field with q elements is denoted by $\mathbb{F}_q$ where q is a power of a prime number. For any subfield $\mathbb{K} \subseteq \mathbb{F}$ of a field $\mathbb{F}$ and for any positive integers k and n such that $k \leqslant n$, the $\mathbb{K}$-vector space spanned by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ where each $\boldsymbol{b}_i \in \mathbb{F}^n$ is denoted by $\sum_{i=1}^{k} \mathbb{K}\, \boldsymbol{b}_i$. The set of matrices with m rows and n columns with entries in $\mathbb{F}$ is denoted by $\mathscr{M}_{m,n}(\mathbb{F})$. The group of invertible matrices of size n over $\mathbb{F}$ is denoted by $\mathsf{GL}_n(\mathbb{F})$.

Definition 1 (*Rank weight*) Let $\boldsymbol{A}$ be a matrix from $\mathscr{M}_{m,n}(\mathbb{F})$ where m and n are positive integers. The *rank weight* of $\boldsymbol{A}$ denoted by $|\boldsymbol{A}|$ is the rank of $\boldsymbol{A}$. The *rank distance* between two matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ from $\mathscr{M}_{m,n}(\mathbb{F})$ is defined as $|\boldsymbol{A} - \boldsymbol{B}|$.

It is a well-known fact that the rank distance on $\mathscr{M}_{m,n}(\mathbb{F})$ has the properties of a metric. But in the context of rank-metric cryptography, this rank distance is rather defined for vectors $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. The idea is to consider the field $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space and hence any vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ as a matrix from $\mathscr{M}_{m,n}\left(\mathbb{F}_q\right)$ by decomposing each entry $x_i \in \mathbb{F}_{q^m}$ into a m-tuple of $\mathbb{F}_q^m$ with respect to an arbitrary basis of $\mathbb{F}_{q^m}$. The rank weight of $\boldsymbol{x}$, also denoted by $|\boldsymbol{x}|$, is then its rank[1] viewed as a matrix of $\mathscr{M}_{m,n}\left(\mathbb{F}_q\right)$. Hence, it is possible to define a new metric on $\mathbb{F}_{q^m}^n$ that we recall explicitly in the following definition.

Definition 2 Let us consider the finite field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ of degree $m \geqslant 1$. The *rank weight* of a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ in $\mathbb{F}_{q^m}^n$ denoted by $|\boldsymbol{x}|$ is the dimension of the $\mathbb{F}_q$-vector space generated by $\{x_1, \ldots, x_n\}$

$$|\boldsymbol{x}| = \dim \sum_{i=1}^{n} \mathbb{F}_q x_i. \tag{1}$$

[1] This rank is of course independent of the choice of the basis of $\mathbb{F}_{q^m}$ since the rank of a matrix is invariant when multiplied by an invertible matrix.

Similarly, the column rank over $\mathbb{F}_q$ for any matrix $\boldsymbol{M}$ from $\mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ is also denoted by $|\boldsymbol{M}|$.

Remark 1 Take note of the fact that $|\boldsymbol{M}|$ represents $\dim \sum_i^n \mathbb{F}_q \boldsymbol{M}_i$ where $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_n$ are the columns of $\boldsymbol{M}$, that is to say the maximum number of columns that are linearly independent over $\mathbb{F}_q$.

Proposition 1 *Let $\boldsymbol{M}$ be a matrix from $\mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ and set $s = |\boldsymbol{M}|$ with $s < n$. There exist $\boldsymbol{M}^*$ in $\mathscr{M}_{k,s}\left(\mathbb{F}_{q^m}\right)$ with $\left|\boldsymbol{M}^*\right| = s$ and $\boldsymbol{T}$ in $\mathsf{GL}_n(\mathbb{F}_q)$ such that:*

$$\boldsymbol{M}\boldsymbol{T} = (\boldsymbol{M}^* \mid \boldsymbol{0}) \tag{2}$$

In particular for any $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{x}| = s$, there exists $\boldsymbol{T}$ in $\mathsf{GL}_n(\mathbb{F}_q)$ for which $\boldsymbol{x}\boldsymbol{T} = (\boldsymbol{x}^* \mid \boldsymbol{0})$ where $\boldsymbol{x}^* \in \mathbb{F}_{q^m}^s$ and $|\boldsymbol{x}^*| = s$.

This permits to state the following corollary.

Corollary 1 *For any $\boldsymbol{M} \in \mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ and for any $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$*

$$|\boldsymbol{m}\boldsymbol{M}| \leqslant |\boldsymbol{M}| \tag{3}$$

Definition 3 For any x in $\mathbb{F}_{q^m}$ and for any integer i, the quantity x^{q^i} is denoted by $x^{[i]}$. This notation is extended to vectors $\boldsymbol{x}^{[i]} = (x_1^{[i]}, \ldots, x_n^{[i]})$ and matrices $\boldsymbol{M}^{[i]} = \left(m_{ij}^{[i]}\right)$.

We also give the following lemmas, that will be useful in the sequel.

Lemma 1 *For any $\boldsymbol{A} \in \mathscr{M}_{\ell,s}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{B} \in \mathscr{M}_{s,n}\left(\mathbb{F}_{q^m}\right)$, and for any α and β in $\mathbb{F}_q$:*

$$(\alpha\boldsymbol{A} + \beta\boldsymbol{B})^{[i]} = \alpha\boldsymbol{A}^{[i]} + \beta\boldsymbol{B}^{[i]} \quad \textit{and} \quad (\boldsymbol{A}\boldsymbol{B})^{[i]} = \boldsymbol{A}^{[i]}\boldsymbol{B}^{[i]}.$$

In particular, if $\boldsymbol{S}$ is in $\mathsf{GL}_n(\mathbb{F}_{q^m})$ then $\boldsymbol{S}^{[i]}$ also belongs to $\mathsf{GL}_n(\mathbb{F}_{q^m})$.

Lemma 2 *Let $\boldsymbol{P} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix}$ where $\boldsymbol{A}$ and $\boldsymbol{D}$ are square matrices. $\boldsymbol{P}$ is non singular if and only if $\boldsymbol{A}$ and $\boldsymbol{D}$ are non singular. In that case, the inverse of $\boldsymbol{P}$ is:*

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{A}^{-1} & \boldsymbol{0} \\ -\boldsymbol{D}^{-1}\boldsymbol{C}\boldsymbol{A}^{-1} & \boldsymbol{D}^{-1} \end{pmatrix}$$

Let us recall that a (linear) code of length n over a finite field $\mathbb{F}$ is a linear subspace of $\mathbb{F}^n$. Elements of a code are called *codewords*. A matrix whose rows form a basis of a code is called a *generator matrix*. The dual of a code $\mathscr{C} \subset \mathbb{F}^n$ is the linear space denoted by $\mathscr{C}^\perp$ containing vectors $\boldsymbol{z} \in \mathbb{F}^n$ such that:

$$\forall \boldsymbol{c} \in \mathscr{C}, \quad \sum_{i=1}^n c_i z_i = 0.$$

An algorithm D is said to decode t errors in a code $\mathscr{C} \subset \mathbb{F}^n$ if for any $\boldsymbol{c} \in \mathscr{C}$ and for any $\boldsymbol{e} \in \mathbb{F}^n$ such that $|\boldsymbol{e}| \leqslant t$ we have $D(\boldsymbol{c} + \boldsymbol{e}) = \boldsymbol{c}$. Generally, we call such a vector $\boldsymbol{e}$ an *error* vector. We now introduce an important family of codes known for having an efficient decoding algorithm.

Definition 4 (*Gabidulin code*) Let $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{g}| = n$. The $(n, k)-$Gabidulin code denoted by $\mathscr{G}_k(\boldsymbol{g})$ is the code with a generator matrix $\boldsymbol{G}$ where:

$$\boldsymbol{G} = \begin{pmatrix} g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}. \tag{4}$$

Gabidulin codes are known to possess a fast decoding algorithm that can decode errors of weight t provided that $t \leqslant \lfloor \frac{1}{2}(n-k) \rfloor$. Furthermore, the dual of a Gabidulin code $\mathscr{G}_k(\boldsymbol{g})$ is also a Gabidulin code.

We end this section by an important well-known property about Gabidulin codes.

Proposition 2 *Let $\mathscr{G}_k(\boldsymbol{g})$ be a Gabidulin code of length n with generator matrix $\boldsymbol{G}$ and $\boldsymbol{T} \in \mathsf{GL}_n(\mathbb{F}_q)$. Then $\boldsymbol{GT}$ is a generator matrix of the Gabidulin code $\mathscr{G}_k(\boldsymbol{gT})$.*

Proof From Lemma 1, we have $(\boldsymbol{gT})^{[i]} = \boldsymbol{g}^{[i]}\boldsymbol{T}$. □

3 Rank metric encryption schemes

The concept of rank metric cryptography appeared in [4] where the authors propose a public key encryption scheme using codes in a rank metric framework. They adapted McEliece's general idea [3] developed for the Hamming metric to the rank metric context. The key tool in the design is to focus on linear codes having a fast rank-metric decoding algorithm like Gabidulin codes. In this section, we recall the general principle that underlies all the existing rank encryption metric schemes.

During the key generation phase, the integers k, ℓ, n and m are chosen such that $k < n \leqslant m$ and $0 \leqslant \ell \ll n$. This then randomly picks $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ with $|\boldsymbol{g}| = n$ and defines $\boldsymbol{G} \in \mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ as in (4), that is to say $\boldsymbol{G}$ is a generator matrix of the Gabidulin code $\mathscr{G}_k(\boldsymbol{g})$. The error-correction capability of $\mathscr{G}_k(\boldsymbol{g})$ is denoted by $t \overset{\text{def}}{=} \lfloor \frac{1}{2}(n-k) \rfloor$. An important step in the key generation is the "hiding" phase where $\boldsymbol{G}$ undergoes a transformation to mask the algebraic structure of Gabidulin codes. This transformation is actually a probabilistic algorithm that adds some randomness to its input. Originally, the authors in [4] proposed to use a *distortion* transformation $\mathscr{D} : \mathbb{F}_{q^m}^{k \times n} \longrightarrow \mathbb{F}_{q^m}^{k \times n}$ that sends any $\boldsymbol{G}$ to $\mathscr{D}(\boldsymbol{G}) = \boldsymbol{S}(\boldsymbol{G} + \boldsymbol{X})$ where $\boldsymbol{X}$ is a random matrix from $\mathbb{F}_{q^m}^{k \times n}$ with a prescribed rank $t_{\boldsymbol{X}}$ and $\boldsymbol{S}$ is an invertible matrix. The public key is then $\boldsymbol{G}_{\text{pub}} = \mathscr{D}(\boldsymbol{G})$ with the parameter $t_{\text{pub}} = t - t_{\boldsymbol{X}}$ while the private key is $(\boldsymbol{S}, \boldsymbol{G})$. The encryption algorithm takes as input a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ and generates a random $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{e}| \leqslant t_{\text{pub}}$ in order to compute the ciphertext $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{\text{pub}} + \boldsymbol{e}$. In the decryption step, the decoding algorithm of the Gabidulin code $\mathscr{G}_k(\boldsymbol{g})$ is applied to the ciphertext. This word can be decoded since the underlying codeword is corrupted by the error vector $\boldsymbol{mSX} + \boldsymbol{e}$ whose rank weight is $|\boldsymbol{mSX} + \boldsymbol{e}| \leqslant |\boldsymbol{mSX}| + |\boldsymbol{e}| \leqslant t$ since by Corollary 1 we have $|\boldsymbol{mSX}| \leqslant t_{\boldsymbol{X}}$.

However, Gibson proved [5,6] that the GPT encryption scheme [4] is vulnerable to a polynomial time key recovery attack. Consequently, Gabidulin and Ourivski proposed in [7] a reparation by considering a more general hiding transformation, combining a distortion matrix $\boldsymbol{X}$ and a right column scrambler $\boldsymbol{P}$. The hidden generator matrix is more precisely of the form:

$$\mathscr{D}(\boldsymbol{G}) = \boldsymbol{S}\left(\boldsymbol{X}_1 \mid \boldsymbol{G} + \boldsymbol{X}_2\right)\boldsymbol{P} \tag{5}$$

where $\boldsymbol{X}_1 \in \mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{X}_2 \in \mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ such that $|\boldsymbol{X}_2| < t$ and $\boldsymbol{P} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$. The public generator matrix is again $\boldsymbol{G}_{\text{pub}} \overset{\text{def}}{=} \mathscr{D}(\boldsymbol{G})$ which constitutes the public key with the public parameter $t_{\text{pub}} \overset{\text{def}}{=} t - t_2$, where $t_2 \overset{\text{def}}{=} |\boldsymbol{X}_2|$. The decryption computes $\boldsymbol{P}^{-1} = (\boldsymbol{Q}_1 \mid \boldsymbol{Q}_2)$, where $\boldsymbol{Q}_1 \in \mathscr{M}_{(n+\ell),\ell}\left(\mathbb{F}_q\right)$ and $\boldsymbol{Q}_2 \in \mathscr{M}_{(n+\ell),n}\left(\mathbb{F}_q\right)$. The last n components of $\boldsymbol{cP}^{-1}$ is the vector $\boldsymbol{mSG} + \boldsymbol{mSX}_2 + \boldsymbol{eQ}_2$ and since $\left|\boldsymbol{eQ}_2\right| \leqslant |\boldsymbol{e}|$ and $|\boldsymbol{mSX}_2| \leqslant |\boldsymbol{X}_2|$, it follows that $\left|\boldsymbol{mSX}_2 + \boldsymbol{eQ}_2\right| \leqslant t$. Applying a fast decoding algorithm to the last n components of $\boldsymbol{cP}^{-1}$ allows the legitimate user to get $\boldsymbol{mS}$ and easily $\boldsymbol{m}$.

We now state our first result about Gabidulin and Ouriviski reparation which proves that we can always consider $\boldsymbol{X}_2 = 0$.

Proposition 3 *Let $\boldsymbol{G}_{\text{pub}}$ be as in (5) and assume that $|\boldsymbol{X}_2| = t_2$. There exist $\boldsymbol{P}^* \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$, $\boldsymbol{X}^* \in \mathscr{M}_{k,(\ell+t_2)}\left(\mathbb{F}_{q^m}\right)$ and a matrix $\boldsymbol{G}^*$ that generates a $(n-t_2)-$Gabidulin code $\mathscr{G}_k\left(\boldsymbol{g}^*\right)$ such that*

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{X}^* \mid \boldsymbol{G}^*\right)\boldsymbol{P}^*. \tag{6}$$

Furthermore, the error correction capability t^* of $\mathscr{G}_k\left(\boldsymbol{g}^*\right)$ is equal to $t - \frac{1}{2}t_2$, and hence $t^* > t_{\text{pub}}$.

Proof Since $|\boldsymbol{X}_2| = t_2$ then by Proposition 1 there exist $\boldsymbol{T}_2$ in $\mathsf{GL}_n(\mathbb{F}_q)$ and $\boldsymbol{X}_2'$ in $\mathscr{M}_{k,t_2}\left(\mathbb{F}_{q^m}\right)$ such that $\boldsymbol{X}_2\boldsymbol{T}_2 = \left(\boldsymbol{X}_2' \mid \boldsymbol{0}\right)$. So by letting $\boldsymbol{T} = \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{T}_2 \end{pmatrix}$ we have:

$$\begin{aligned} \boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{X}_1 \mid \boldsymbol{G} + \boldsymbol{X}_2\right)\boldsymbol{P} &= \boldsymbol{S}\left(\boldsymbol{X}_1 \mid \boldsymbol{GT}_2 + \boldsymbol{X}_2\boldsymbol{T}_2\right)\boldsymbol{T}^{-1}\boldsymbol{P} \\ &= \boldsymbol{S}\left(\boldsymbol{X}_1 \mid \boldsymbol{G}' + \boldsymbol{X}_2\boldsymbol{T}_2\right)\boldsymbol{Q} \end{aligned}$$

where $\boldsymbol{G}' = \boldsymbol{GT}_2$ and $\boldsymbol{Q} = \boldsymbol{T}^{-1}\boldsymbol{P}$. Note that $\boldsymbol{G}'$ generates the $(n,k)-$Gabidulin code $\mathscr{G}_k\left(\boldsymbol{g}'\right)$ with $\boldsymbol{g}' = \boldsymbol{gT}_2 = (g_1', \ldots, g_n')$. Let us decompose $\boldsymbol{G}'$ as $(\boldsymbol{G}_1' \mid \boldsymbol{G}_2')$ where $\boldsymbol{G}_1' \in \mathscr{M}_{k,t_2}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{G}_2' \in \mathscr{M}_{k,(n-t_2)}\left(\mathbb{F}_{q^m}\right)$ we then have:

$$\boldsymbol{G}' + \boldsymbol{X}_2\boldsymbol{T}_2 = \left(\boldsymbol{G}_1' + \boldsymbol{X}_2' \mid \boldsymbol{G}_2'\right)$$

By setting $\boldsymbol{X} = \left(\boldsymbol{X}_1 \mid \boldsymbol{G}_1' + \boldsymbol{X}_2'\right)$ we get (6) and $\boldsymbol{G}_2'$ generates the $(n-t_2,k)-$Gabidulin $\mathscr{G}_k\left(\boldsymbol{g}_2'\right)$ where $\boldsymbol{g}_2' = (g_{t_2+1}', \ldots, g_n')$. The error-correction capability t^* of $\mathscr{G}_k\left(\boldsymbol{g}_2'\right)$ is given by $t^* = \frac{1}{2}(n - t_2 - k) = t - \frac{1}{2}t_2$ which implies $t^* > t - t_2$. □

The first important consequence of Proposition 3 is the possibility for a cryptanalyst, who is able to derive $(\boldsymbol{S}, \boldsymbol{G}^*, \boldsymbol{P}^*)$ from $\boldsymbol{G}_{\text{pub}}$ so that (6) is satisfied, to decipher any ciphertext $\boldsymbol{c} = \boldsymbol{mG}_{\text{pub}} + \boldsymbol{e}$ with $|\boldsymbol{e}| \leqslant t_{\text{pub}}$. Thus any successful structural attack on the description (6) leads to a successful attack on (5) and conversely since (6) corresponds to the special case where $\boldsymbol{X}_2 = \boldsymbol{0}$. Therefore the security of the scheme given [7] is equivalent to the one of a scheme where $\boldsymbol{X}_2 = \boldsymbol{0}$.

4 Distinguishing properties of gabidulin codes

We recall important algebraic properties about Gabidulin codes. It will explain why many attacks occur when the underlying code is a Gabidulin one. One key property is that Gabidulin codes can be easily distinguished from random linear codes. This singular behaviour has been precisely exploited by Overbeck [9–11] to mount attacks.

Definition 5 For any integer $i \geqslant 0$ let $\Lambda_i : \mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right) \longrightarrow \mathscr{M}_{ik,n}\left(\mathbb{F}_{q^m}\right)$ be the $\mathbb{F}_q$-linear operator that maps any $\boldsymbol{M}$ from $\mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ to $\Lambda_i(\boldsymbol{M})$ where by definition:

$$\Lambda_i(\boldsymbol{M}) \overset{\text{def}}{=} \begin{pmatrix} \boldsymbol{M}^{[0]} \\ \vdots \\ \boldsymbol{M}^{[i]} \end{pmatrix}. \tag{7}$$

For any code $\mathscr{G}$ generated by a matrix $\boldsymbol{G}$ we denote by $\Lambda_i(\mathscr{G})$ the code generated by $\Lambda_i(\boldsymbol{G})$.

Proposition 4 *Let $\boldsymbol{g}$ be in $\mathbb{F}_{q^m}^n$ with $|\boldsymbol{g}| = n$ and $n \leqslant m$. For any integers k and i such that $k \leqslant n$ and $i \leqslant n-k-1$ we have:*

$$\Lambda_i\left(\mathscr{G}_k(\boldsymbol{g})\right) = \mathscr{G}_{k+i}(\boldsymbol{g}). \tag{8}$$

The importance of Λ_i becomes clear when one compares the dimension of the code spanned by $\Lambda_i(\boldsymbol{G})$ for a randomly drawn matrix $\boldsymbol{G}$ and the dimension obtained when $\boldsymbol{G}$ generates a Gabidulin code.

Proposition 5 *If $\mathscr{A} \subset \mathbb{F}_{q^m}^n$ is a code generated by a random matrix from $\mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ then with a high probability:*

$$\dim \Lambda_i(\mathscr{A}) = \min\left\{n, (i+1)k\right\} \tag{9}$$

In the case of a Gabidulin code, we get a different situation as explained by Proposition 4. Thus there is a property that is computable in polynomial time distinguishes a Gabidulin code from a random one. This can be used in a cryptanalysis context. In fact, Overbeck [11] has proven that, for a public matrix $\boldsymbol{G}_p$ given by Eq. (5) with $\boldsymbol{X}_2 = \boldsymbol{0}$ (in particular all the entries of $\boldsymbol{P}$ belong to $\mathbb{F}_q$), it is possible (under certain conditions) to find in polynomial time an alternative decomposition of $\boldsymbol{G}_p$ of the from $\boldsymbol{S}^*\left(\boldsymbol{X}^* \mid \boldsymbol{G}^*\right)\boldsymbol{P}^*$ using the operator Λ_i. This decomposition allows to decrypt any ciphertext computed with $\boldsymbol{G}_p$. The reader can refer to Appendix A for details concerning the attack. The key reason explaining its success is given by the following proposition.

Proposition 6 *Let ℓ, k and n be positive integers with $\ell < n$ and $1 \leqslant k < n$. Let $\boldsymbol{G} \in \mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ being a generator matrix of a Gabidulin code, and $\boldsymbol{X}$ a randomly drawn matrix from $\mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$. Denote by $\mathscr{A}$ the code defined by the generator matrix $(\boldsymbol{X} \mid \boldsymbol{G})$. For any integer $i \geqslant 0$, we have*

$$k + i \;\leqslant\; \dim \Lambda_i(\mathscr{A}) \;\leqslant\; k + i + d \tag{10}$$

where $d = \min\left\{(i+1)k, \ell\right\}$.

Note that by construction $\ell \leqslant n$ and in Overbeck's attack, the integer i is equal to $n-k-1$ so that we have both $d = \ell$ and, with high probability, the upper bound in (10) is actually an equality, namely

$$\dim \Lambda_{n-k-1}(\mathscr{A}) = k + (n-k-1) + d = n + \ell - 1.$$

This implies that the dimension of $\Lambda_i(\mathscr{A})^{\perp}$ is equal to 1. This fact is then harnessed in [11] to recover an equivalent Gabidulin code which enables to decrypt any ciphertext.

Proposition 7 ([11]) *Assume that the public key is $\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G})\boldsymbol{P}$ with $\boldsymbol{X} \in \mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{P} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ and $\boldsymbol{G}$ generating a $(n,k)-$Gabdidulin code. We denote by $\mathscr{A}$ the code generated by $\boldsymbol{G}_{\text{pub}}$. If $\dim\left(\Lambda_{n-k-1}(\mathscr{A})^{\perp}\right)$ is equal to 1 then it is possible to* *recover, with $O\left((n+\ell)^3\right)$ field operations, alternative matrices $\boldsymbol{X}^* \in \mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{P}^* \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ and $\boldsymbol{G}^*$ generating a $(n,k)-$Gabdidulin code such that*

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{X}^* \mid \boldsymbol{G}^*\right)\boldsymbol{P}^*$$

Overbeck's attack uses crucially two important facts (see Appendix A for more details): the column scrambler matrix $\boldsymbol{P}$ is defined on the based field $\mathbb{F}_q$, and the co-dimension of $\Lambda_{n-k-1}(\mathscr{A})$ is 1. Several works propose to resist to Overbeck's attack either by taking special distortion matrix so that the second property is not true as in [12,13], or by taking a column scrambler matrix defined over the extension field $\mathbb{F}_{q^m}$ as in [14–16]. In this paper, we solely concentrate on the second approach. In [17,18] new generic decoding algorithms are presented whereas our approach is directed towards recovering the structure of a Gabidulin code. We will prove that all the existing schemes [14–16] can be broken simply with the techniques developed in [11].

5 Gabidulin's general reparation

In this section, we focus on the reparation given in [14]. This paper is the first to consider a column scrambler matrix defined over the extension field. We describe only the key generation and decryption steps of the scheme since the encryption operation is not modified. To the best of our knowledge, no structural attack has been mounted against this description. The author claimed that Overbeck's attack is not applicable but in Proposition 8, we prove that it is still possible to find an alternative private key using precisely Overbeck's technique.

Key generation

1. Pick at random $\boldsymbol{g}$ from $\mathbb{F}_{q^m}^n$ such that $|\boldsymbol{g}| = n$ and let $\boldsymbol{G}$ be a generator matrix of the Gabidulin code $\mathscr{G}_k(\boldsymbol{g})$.
2. Pick at random $\boldsymbol{X} \in \mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{S}$ in $\mathsf{GL}_k(\mathbb{F}_{q^m})$ and $\boldsymbol{P}$ in $\mathsf{GL}_{n+\ell}(\mathbb{F}_{q^m})$ such that there exist $\boldsymbol{Q}_{11}$ in $\mathscr{M}_{\ell,\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{Q}_{21}$ in $\mathscr{M}_{n,\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{Q}_{22}$ in $\mathscr{M}_{n,n}\left(\mathbb{F}_q\right)$ and $\boldsymbol{Q}_{12}$ in $\mathscr{M}_{\ell,n}\left(\mathbb{F}_{q^m}\right)$ with $\left|\boldsymbol{Q}_{12}\right| = s < t$ so that
$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix}. \tag{11}$$

The public key is $(\boldsymbol{G}_{\text{pub}}, t_{\text{pub}})$ with $t_{\text{pub}} = t - s$ and

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right)\boldsymbol{P}. \tag{12}$$

Decryption We have $\boldsymbol{c}\boldsymbol{P}^{-1} = \boldsymbol{m}\boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right) + \boldsymbol{e}\boldsymbol{P}^{-1}$. Suppose that $\boldsymbol{e} = (\boldsymbol{e}_1 \mid \boldsymbol{e}_2)$ where $\boldsymbol{e}_1 \in \mathbb{F}_{q^m}^{\ell}$ and $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n}$. We have:

$$\boldsymbol{e}\boldsymbol{P}^{-1} = \left(\boldsymbol{e}_1\boldsymbol{Q}_{11} + \boldsymbol{e}_2\boldsymbol{Q}_{21} \mid \boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}\right) \tag{13}$$

It is clear that $\left|\boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}\right| \leqslant \left|\boldsymbol{e}_1\boldsymbol{Q}_{12}\right| + \left|\boldsymbol{e}_2\boldsymbol{Q}_{22}\right| \leqslant s + t - s$. So the plaintext $\boldsymbol{m}$ is recovered by applying the decoding algorithm only to the last n components of $\boldsymbol{c}\boldsymbol{P}^{-1}$.

We state our main result proving that Overbeck's attack is still successful by considering this time the dual of the code generated by $\Lambda_i\left(\boldsymbol{G}_{\text{pub}}\right)$ with $i = n - s - k - 1$.

Proposition 8 *There exist $\boldsymbol{X}^* \in \mathscr{M}_{k,\ell+s}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{P}^* \in \mathsf{GL}_{n+\ell}\left(\mathbb{F}_q\right)$ and a generator matrix $\boldsymbol{G}^*$ that defines a $(n-s,k)-$Gabidulin code $\mathscr{G}_k(\boldsymbol{g}^*)$ such that*

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{X}^* \mid \boldsymbol{G}^*\right)\boldsymbol{P}^*. \tag{14}$$

Furthermore, the error correction capability t^* *of* $\mathscr{G}_k(\boldsymbol{g}^*)$ *is equal to* $t - \frac{1}{2}s$ *and hence* $t^* > t_{\text{pub}}$.

The proof of this proposition requires to prove the following lemma.

Lemma 3 *There exist* $\boldsymbol{P}_{11}$ *in* $\mathsf{GL}_{\ell+s}(\mathbb{F}_{q^m})$, $\boldsymbol{P}_{21}$ *in* $\mathscr{M}_{(n-s),(\ell+s)}(\mathbb{F}_{q^m})$ *and* $\boldsymbol{P}_{22}$ *in* $\mathsf{GL}_{n-s}(\mathbb{F}_q)$ *such that*

$$\boldsymbol{P} = \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{L} \end{pmatrix} \begin{pmatrix} \boldsymbol{P}_{11} & \boldsymbol{0} \\ \boldsymbol{P}_{21} & \boldsymbol{P}_{22} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{pmatrix} \tag{15}$$

with $\boldsymbol{L}$ *and* $\boldsymbol{R}$ *belonging to* $\mathsf{GL}_n(\mathbb{F}_q)$.

Proof By assumption, $|\boldsymbol{Q}_{12}| = s < t$. So there exist $\boldsymbol{R}$ in $\mathsf{GL}_n(\mathbb{F}_q)$ and $\boldsymbol{Q}'_{12}$ in $\mathscr{M}_{\ell,s}(\mathbb{F}_{q^m})$ such that $\boldsymbol{Q}_{12}\boldsymbol{R} = (\boldsymbol{Q}'_{12} \mid \boldsymbol{0})$. We set $\boldsymbol{Q}_{22}\boldsymbol{R} = (\boldsymbol{Q}'_{22} \mid \boldsymbol{Q}'_{23})$ where $\boldsymbol{Q}'_{22}$ belongs to $\mathscr{M}_{n,s}(\mathbb{F}_q)$ and $\boldsymbol{Q}'_{23}$ to $\mathscr{M}_{n,n-s}(\mathbb{F}_q)$. Note that we necessarily have $|\boldsymbol{Q}'_{23}| \leqslant n - s$ and therefore, there exists $\boldsymbol{L} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\boldsymbol{L}\boldsymbol{Q}'_{23} = \begin{pmatrix} \boldsymbol{0} \\ \boldsymbol{Q}''_{23} \end{pmatrix}$ with $\boldsymbol{Q}''_{23} \in \mathscr{M}_{n-s,n-s}(\mathbb{F}_q)$. Thus one can rewrite

$$\begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{L} \end{pmatrix} \boldsymbol{P}^{-1} \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{pmatrix} = \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{L} \end{pmatrix} \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{pmatrix} \tag{16}$$

$$= \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}'_{12} & \boldsymbol{0} \\ \boldsymbol{L}\boldsymbol{Q}_{21} & \boldsymbol{L}\boldsymbol{Q}'_{22} & \boldsymbol{L}\boldsymbol{Q}'_{23} \end{pmatrix} \tag{17}$$

Observe that there exist $\boldsymbol{Q}''_{11}$ in $\mathscr{M}_{\ell+s,\ell+s}(\mathbb{F}_{q^m})$ and $\boldsymbol{Q}''_{21}$ in $\mathscr{M}_{n-s,\ell+s}(\mathbb{F}_{q^m})$ so that we can write

$$\begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{L} \end{pmatrix} \boldsymbol{P}^{-1} \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{pmatrix} = \begin{pmatrix} \boldsymbol{Q}''_{11} & \boldsymbol{0} \\ \boldsymbol{Q}''_{21} & \boldsymbol{Q}''_{23} \end{pmatrix}.$$

Note that $\boldsymbol{Q}''_{23}$ and $\boldsymbol{Q}''_{11}$ are necessarily invertible and thanks to Lemma 2, the proof can be terminated. □

Remark 2 The proof of Lemma 3 is still true if it is assumed that $|\boldsymbol{Q}_{12}| < s$, and note that by construction s is necessarily less than or equal to ℓ.

We are now able to give a proof of Proposition 8.

Proof (*Proposition* 8) We keep the same notation as those of Lemma 3. Let us rewrite $\boldsymbol{G}\boldsymbol{L}$ as $(\boldsymbol{G}'_1 \mid \boldsymbol{G}'_2)$ where $\boldsymbol{G}'_1$ is in $\mathscr{M}_{k,s}(\mathbb{F}_{q^m})$ and $\boldsymbol{G}'_2$ in $\mathscr{M}_{k,n-s}(\mathbb{F}_{q^m})$, and set $\boldsymbol{Y} = (\boldsymbol{X} \mid \boldsymbol{G}'_1)$. Observe that $\boldsymbol{G}'_2$ generates a $(n-s,k)-$Gabidulin code. We then have

$$(\boldsymbol{X} \mid \boldsymbol{G}) \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{L} \end{pmatrix} \begin{pmatrix} \boldsymbol{P}_{11} & \boldsymbol{0} \\ \boldsymbol{P}_{21} & \boldsymbol{P}_{22} \end{pmatrix} = (\boldsymbol{Y} \mid \boldsymbol{G}'_2) \begin{pmatrix} \boldsymbol{P}_{11} & \boldsymbol{0} \\ \boldsymbol{P}_{21} & \boldsymbol{P}_{22} \end{pmatrix} = (\boldsymbol{X}^* \mid \boldsymbol{G}^*)$$

where $\boldsymbol{X}^* = \boldsymbol{Y}\boldsymbol{P}_{11} + \boldsymbol{G}'_2\boldsymbol{P}_{21}$ and $\boldsymbol{G}^* = \boldsymbol{G}'_2\boldsymbol{P}_{22}$ is a generator matrix of a $(n-s,k)-$Gabidulin code. Hence if we set $\boldsymbol{P}^* = \begin{pmatrix} \boldsymbol{I}_\ell & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{pmatrix}$, we have then rewritten $\boldsymbol{G}_{\text{pub}}$ as expected in (14). Lastly, remark that $t_{\text{pub}} = t - s$ and $t^* = \frac{1}{2}(n - s - k) = \frac{1}{2}(n-k) - \frac{1}{2}s > t - s$. □

6 Gabidulin, Rashwan and Honary variant

In [15,16], Gabidulin, Rashwan and Honary proposed an other variant where the column scrambler has its entries defined on the extension field. We will prove that their scheme is actually a special case of [14] and because of that, it suffers the same weakness. So, unlike what it is claimed by the authors, Overbeck's attack is still successful.

Key generation

1. Pick at random $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{g}| = n$ and let $\boldsymbol{G} \in \mathscr{M}_{k,n}\left(\mathbb{F}_{q^m}\right)$ be a generator matrix of the Gabidulin code $\mathscr{G}_k(\boldsymbol{g})$. Let t_{pub} be an integer $< t$ and set $a \overset{\text{def}}{=} t - t_{\text{pub}}$.
2. Pick at random $\boldsymbol{S}$ in $\mathsf{GL}_k(\mathbb{F}_{q^m})$ and $\boldsymbol{P} \in \mathsf{GL}_n(\mathbb{F}_{q^m})$ such that
$$\boldsymbol{P}^{-1} = \left(\boldsymbol{Q}_1 \mid \boldsymbol{Q}_2\right) \tag{18}$$
where $\boldsymbol{Q}_1 \in \mathscr{M}_{n,a}\left(\mathbb{F}_{q^m}\right)$ while $\boldsymbol{Q}_2 \in \mathscr{M}_{n,n-a}\left(\mathbb{F}_q\right)$ with $t = \frac{1}{2}(n-k)$ and $t_{\text{pub}} < t$. The public key is $(\boldsymbol{G}_{\text{pub}}, t_{\text{pub}})$ with
$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{SGP}. \tag{19}$$

Decryption We have $\boldsymbol{cP}^{-1} = \boldsymbol{mSG} + \boldsymbol{eP}^{-1}$ and $\boldsymbol{eP}^{-1} = \left(\boldsymbol{eQ}_1 \mid \boldsymbol{eQ}_2\right)$. Observe that $\left|\boldsymbol{eQ}_1\right| \leqslant a$ and $\left|\boldsymbol{eQ}_2\right| \leqslant |\boldsymbol{e}| \leqslant t_{\text{pub}}$. Moreover, since $a = t - t_{\text{pub}}$ we hence have

$$\left|\boldsymbol{eP}^{-1}\right| \leqslant \left|\boldsymbol{eQ}_1\right| + \left|\boldsymbol{eQ}_2\right| \leqslant t.$$

We now prove that Overbeck's attack is still successful by considering for this scheme the dual of $\Lambda_i\left(\boldsymbol{G}_{\text{pub}}\right)$ with $i = n - a - k - 1$. We first introduce the matrices $\boldsymbol{Q}_{11} \in \mathscr{M}_{a,a}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{Q}_{21} \in \mathscr{M}_{n-a,a}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{Q}_{12} \in \mathscr{M}_{a,n-a}\left(\mathbb{F}_q\right)$ and $\boldsymbol{Q}_{22} \in \mathscr{M}_{n-a,n-a}\left(\mathbb{F}_q\right)$ such that
$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix}. \tag{20}$$

Note that $\left|\boldsymbol{Q}_{12}\right| \leqslant a < t$. Furthermore, by looking at the proof of Lemma 3, we can see that this lemma and Proposition 8 are still true even if $\left|\boldsymbol{Q}_{12}\right| \leqslant s$. Hence, the scheme given in [15,16] is nothing else but a special case of [14] where $\boldsymbol{X} = \boldsymbol{0}$ and $\boldsymbol{Q}_{12}$ has all its entries in the base field $\mathbb{F}_q$. We have therefore the following corollary.

Corollary 2 *There exist $\boldsymbol{P}^* \in \mathsf{GL}_n(\mathbb{F}_q)$ and $\boldsymbol{X} \in \mathscr{M}_{k,a}\left(\mathbb{F}_{q^m}\right)$ such that*
$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G}^*)\boldsymbol{P}^* \tag{21}$$
where $\boldsymbol{G}^*$ is a generator matrix of a $(n-a,k)-$Gabidulin code whose error correction capability t^* is equal to $\lfloor\frac{1}{2}(t + t_{\text{pub}})\rfloor$, and hence $t^* > t_{\text{pub}}$.

Proof Apply Proposition 8 with $\ell = 0$ and $s = a$. Note that the error correction capability t^* of the code $\boldsymbol{G}^*$ is equal to $\frac{1}{2}(n-a-k)$ that is to say
$$t^* = t - \frac{1}{2}(t - t_{\text{pub}}) = \frac{1}{2}(t + t_{\text{pub}}) > t_{\text{pub}}.$$
□

We summarised in Table 1 our experimental results obtained with Magma V2.21-6. We give the time to find an alternative column scrambler matrix for each parameter proposed by the authors in [15] and [16].

Table 1 Parameters from [15,16] where $n = m$ and at least 80-bit security

m	k	t	t_{pub}	Time (s)
20	10	5	4	$\leqslant 1$
28	14	7	3	$\leqslant 1$
28	14	7	4	$\leqslant 1$
28	14	7	5	$\leqslant 1$
28	14	7	6	$\leqslant 1$
20	10	5	4	$\leqslant 1$

7 Discussion on a more general column scrambler

In [15] the authors proposed to reinforce the security by taking a more general column scrambler matrix of the form $\boldsymbol{T}\boldsymbol{P}$ where $\boldsymbol{T}$ is an invertible matrix with its entries in $\mathbb{F}_q$ and $\boldsymbol{P}$ defined over the extension field as it is done in [13–15]. We shall consider Gabidulin's general reparation [14] since [13,15] are particular cases. However, we emphasize that this new protection was only defined in [13,15]. Assuming that $\boldsymbol{P}$ is then as in (11), the public key is then of the form

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right)\boldsymbol{T}\boldsymbol{P}. \tag{22}$$

The decryption of a ciphertext $\boldsymbol{c}$ starts by calculating $\boldsymbol{c}\boldsymbol{P}^{-1}\boldsymbol{T}^{-1} = \boldsymbol{m}\boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right) + \boldsymbol{e}\boldsymbol{P}^{-1}\boldsymbol{T}^{-1}$ where $\boldsymbol{e}$ is of rank weight t_{pub} and $s = \left|\boldsymbol{Q}_{12}\right|$. Suppose that $\boldsymbol{e} = (\boldsymbol{e}_1 \mid \boldsymbol{e}_2)$ where $\boldsymbol{e}_1 \in \mathbb{F}_{q^m}^{\ell}$ and $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n}$, then we also have

$$\boldsymbol{e}\boldsymbol{P}^{-1}\boldsymbol{T}^{-1} = \left(\boldsymbol{e}_1\boldsymbol{Q}_{11} + \boldsymbol{e}_2\boldsymbol{Q}_{21} \mid \boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}\right)\boldsymbol{T}^{-1}. \tag{23}$$

It is clear that $\left|\boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}\right| \leqslant \left|\boldsymbol{e}_1\boldsymbol{Q}_{12}\right| + \left|\boldsymbol{e}_2\boldsymbol{Q}_{22}\right| \leqslant s + t_{\text{pub}}$ and hence

$$\left|\boldsymbol{e}\boldsymbol{P}^{-1}\boldsymbol{T}^{-1}\right| = \left|\boldsymbol{e}\boldsymbol{P}^{-1}\right| \leqslant \left|\boldsymbol{e}_1\boldsymbol{Q}_{11} + \boldsymbol{e}_2\boldsymbol{Q}_{21}\right| + \left|\boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}\right| \leqslant \ell + s + t_{\text{pub}}.$$

Therefore the plaintext $\boldsymbol{m}$ is recovered by applying the decoding algorithm only to the last n components of $\boldsymbol{c}\boldsymbol{P}^{-1}\boldsymbol{T}^{-1}$. But in this case, the rank weight of the last n components of $\boldsymbol{e}\boldsymbol{P}^{-1}\boldsymbol{T}^{-1}$ is not necessarily less than or equal to $t_{\text{pub}} + s$ but rather to $t_{\text{pub}} + s + \ell$. Consequently, the decryption will always succeed if it is assumed that $t_{\text{pub}} = t - s - \ell$ otherwise the decoding may fail. Hence, we see why this new reparation was just proposed for the case where $\ell = 0$ i.e. without any distortion matrix since otherwise its deteriorates the performances of the original scheme.

We now study more precisely the security this protection might bring in for the general scheme of [14]. First, rewrite $\boldsymbol{T}$ as

$$\boldsymbol{T} = \begin{pmatrix} \boldsymbol{T}_{11} & \boldsymbol{T}_{12} \\ \boldsymbol{T}_{21} & \boldsymbol{T}_{22} \end{pmatrix} \tag{24}$$

where $\boldsymbol{T}_{11} \in \mathscr{M}_{\ell,\ell}\left(\mathbb{F}_q\right), \boldsymbol{T}_{21} \in \mathscr{M}_{n,\ell}\left(\mathbb{F}_q\right), \boldsymbol{T}_{12} \in \mathscr{M}_{\ell,n}\left(\mathbb{F}_q\right)$ and $\boldsymbol{T}_{22} \in \mathscr{M}_{n,n}\left(\mathbb{F}_q\right)$. On the other hand, by Lemma 3 the matrix $\boldsymbol{P}$ can be expressed as (15). So we can find $\boldsymbol{X}_1$ in $\mathscr{M}_{k,(\ell+s)}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{X}_2$ in $\mathscr{M}_{k,(n-s)}\left(\mathbb{F}_{q^m}\right)$ such that

$$\left(\boldsymbol{X} \mid \boldsymbol{G}\right)\boldsymbol{T}\boldsymbol{P} = \left(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 + \boldsymbol{G}_1^*\right)$$

where $\boldsymbol{G}_1^*$ generates a $(n-s,k)-$Gabidulin code and $|\boldsymbol{X}_2| = |\boldsymbol{X}| \leqslant \ell$. From Proposition 3 and by taking $t_2 = \ell$, there exist $\boldsymbol{P}^* \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$, $\boldsymbol{X}^* \in \mathscr{M}_{k,(2\ell+s)}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{G}^*$ that generates a $(n-s-\ell)-$Gabidulin code such that

$$(\boldsymbol{X} \mid \boldsymbol{G})\, \boldsymbol{T}\boldsymbol{P} = \left(\boldsymbol{X}^{*} \mid \boldsymbol{G}^{*}\right) \boldsymbol{P}^{*}. \tag{25}$$

We have therefore proven the following proposition.

Proposition 9 *Assume that* $\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\,(\boldsymbol{X} \mid \boldsymbol{G})\, \boldsymbol{T}\boldsymbol{P}$ *where* $\boldsymbol{T} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ *and* $\boldsymbol{P}$ *has the form* (11)*. There exist* $\boldsymbol{P}^{*}$ *in* $\mathsf{GL}_{n+\ell}(\mathbb{F}_q)$*,* $\boldsymbol{X}^{*}$ *in* $\mathscr{M}_{k,(2\ell+s)}\left(\mathbb{F}_{q^m}\right)$ *and a matrix* $\boldsymbol{G}^{*}$ *that generates a* $(n-s-\ell, k)-$*Gabidulin code* $\mathscr{G}_k\,(\boldsymbol{g}^{*})$ *such that*

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}(\boldsymbol{X}^{*} \mid \boldsymbol{G}^{*})\boldsymbol{P}^{*}.$$

Furthermore, the correction capability t^{*} *of* $\mathscr{G}_k\,(\boldsymbol{g}^{*})$ *is greater than* $t - \frac{1}{2}(\ell + s)$*. In particular* $t^{*} > t_{\text{pub}}$.

This result shows that actually this new proposed protection does not improve the security even when applied with the scheme for which a distortion matrix $\boldsymbol{X}$ is used. An example where this protection was used and turns out to be useless is the scheme given in [13,15].

8 Conclusion

The apparition of Overbeck's attack prompted some authors to invent reparations to hide more the structure of the Gabidulin codes. One trend advocated the use of a right column scrambler with entries in the extension field as it is done in [14–16]. Our analysis shows that these reparations aiming at resisting Overbeck's structural attack fail precisely against it. By applying appropriately Overbeck's technique, we were able to construct a Gabidulin code that has the same dimension as the original one but with a lower length. Hence, we obtain a degraded Gabidulin code in terms of error correction capabilities but we prove that the degradation does not forbid the error correction of any ciphertext. We emphasize that our attack outperforms those given in [17,18] since these latest attacks are generic decoding algorithms whereas our approach is a key-recovery attack. Furthermore, the authors of [17,18] only focus themselves to the variant presented in [15,16] whereas our paper also shows the weakness of the more general variant presented in [14].

We also considered in Sect. 7 the case where an isometric transformation is applied in conjunction with a right column scrambler which has its entries in the extension field. We proved that this protection is useless both in terms of performance and security.

The other kind of reparation is followed by the series of works in [12,13] which propose to resist to Overbeck's attack by taking a distortion matrix $\boldsymbol{X}$ so that the co-dimension of $\Lambda_{n-k-1}\,(\mathscr{A})$ is equal to a where a is sufficiently large to prevent an exhaustive search. But these reparations were cryptanalyzed in [17,19].

Furthermore, since the attack in [19] only considers column scrambler matrices on the base field, one may try to avoid it by combining the reparations proposed in [12,13] with those of [14–16]. Nevertheless, our paper shows that the security of [14–16] can be reduced to the one with a column scrambler with entries in the base field. Consequently, using our results and then applying the general attack of [19] may break this "patched" scheme.

All these results show that almost all the variants of the GPT scheme based on Gabidulin codes are insecure.

Appendix A: Overbeck's attack

Let assume that $\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\,(\boldsymbol{X} \mid \boldsymbol{G})\, \boldsymbol{P}$ is the public generator matrix that generates $\mathscr{C}_{\text{pub}}$ with $\boldsymbol{P} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$, $\boldsymbol{X} \in \mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{G}$ generating a Gabidulin code $\mathscr{G}_k\,(\boldsymbol{g})$ where $|\boldsymbol{g}| = n$.

Observe that $\Lambda_i(\boldsymbol{G}_{\text{pub}})$ can be written as

$$\Lambda_i\left(\boldsymbol{G}_{\text{pub}}\right) = \boldsymbol{S}_{\text{ext}}\Big(\,\Lambda_i\left(\boldsymbol{X}\right) \mid \Lambda_i\left(\boldsymbol{G}\right)\Big)\boldsymbol{P} \quad \text{where} \quad \boldsymbol{S}_{\text{ext}} \overset{\text{def}}{=} \begin{pmatrix} \boldsymbol{S}^{[0]} & & \boldsymbol{0} \\ & \ddots & \\ \boldsymbol{0} & & \boldsymbol{S}^{[i]} \end{pmatrix}. \tag{26}$$

Since $\Lambda_i\left(\boldsymbol{G}\right)$ generates $\mathscr{G}_{k+i}\left(\boldsymbol{g}\right) = \mathscr{G}_{n-1}\left(\boldsymbol{g}\right)$, there exists $\boldsymbol{S}' \in \mathsf{GL}_{k(i+1)}(\mathbb{F}_{q^m})$ such that

$$\boldsymbol{S}'\Lambda_i\left(\boldsymbol{G}_{\text{pub}}\right) = \begin{pmatrix} \boldsymbol{X}^* & \boldsymbol{G}_{n-1} \\ \boldsymbol{X}^{**} & \boldsymbol{0} \end{pmatrix}\boldsymbol{P} \tag{27}$$

where $\boldsymbol{X}^* \in \mathscr{M}_{(n-1),\ell}\left(\mathbb{F}_{q^m}\right)$, $\boldsymbol{X}^{**} \in \mathscr{M}_{(k(i+1)-n+1),\ell}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{G}_{n-1} \in \mathscr{M}_{(n-1),n}\left(\mathbb{F}_{q^m}\right)$ generates $\mathscr{G}_{n-1}\left(\boldsymbol{g}\right)$. Using (27), one can deduce that by taking $i = n-k-1$

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{\text{pub}}) = n - 1 + \mathtt{rank}(\boldsymbol{X}^{**}).$$

In the particular case where $\mathtt{rank}(\boldsymbol{X}^{**}) = \ell$, $\dim \Lambda_i(\mathscr{C}_{\text{pub}}) = n + \ell - 1$ and thus $\dim \Lambda_i(\mathscr{C}_{\text{pub}})^{\perp} = 1$. Furthermore, if $\boldsymbol{h}$ is a non-zero vector from $\mathscr{G}_{n-1}\left(\boldsymbol{g}\right)^{\perp}$ and if we set $\boldsymbol{h}^* = (\boldsymbol{0} \mid \boldsymbol{h})\left(\boldsymbol{P}^{-1}\right)^T$ then under the assumption that $\mathtt{rank}(\boldsymbol{X}^{**}) = \ell$ we have

$$\Lambda_{n-k-1}(\mathscr{C}_{\text{pub}})^{\perp} = \mathbb{F}_{q^m}\boldsymbol{h}^*. \tag{28}$$

Proposition 10 *Let $\boldsymbol{v} \in \Lambda_{n-k-1}(\mathscr{C}_{\text{pub}})^{\perp}$ with $\boldsymbol{v} \neq \boldsymbol{0}$. Any matrix $\boldsymbol{T} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ that satisfies $\boldsymbol{vT} = \left(\boldsymbol{0} \mid \boldsymbol{h}'\right)$ with $\boldsymbol{h}' \in \mathbb{F}_{q^m}^n$ is an alternative column scrambler matrix, that is to say, there exist $\boldsymbol{Z}$ in $\mathscr{M}_{k,\ell}\left(\mathbb{F}_{q^m}\right)$ and $\boldsymbol{G}^*$ that generates a Gabidulin code $\mathscr{G}_k\left(\boldsymbol{g}^*\right)$ such that*

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\left(\boldsymbol{Z} \mid \boldsymbol{G}^*\right)\boldsymbol{T}.$$

Proof From (28) there exists $\alpha \in \mathbb{F}_{q^m}$ such that $\boldsymbol{v} = \alpha\boldsymbol{h}^* = (\boldsymbol{0} \mid \alpha\boldsymbol{h})\left(\boldsymbol{P}^{-1}\right)^T$ where $\boldsymbol{h}$ is a non zero vector of $\mathscr{G}_{n-1}\left(\boldsymbol{g}\right)^{\perp}$. Let $\boldsymbol{T} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ such that $\boldsymbol{vT}^T = (\boldsymbol{0} \mid \boldsymbol{h}')$ and consider the matrices $\boldsymbol{A} \in \mathscr{M}_{\ell,\ell}\left(\mathbb{F}_q\right)$ and $\boldsymbol{D} \in \mathscr{M}_{n,n}\left(\mathbb{F}_q\right)$ so that

$$\boldsymbol{TP}^{-1} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix}.$$

We have the following equalities

$$\tilde{\boldsymbol{h}}\boldsymbol{T}^T = (\boldsymbol{0} \mid \alpha\boldsymbol{h})\left(\boldsymbol{P}^{-1}\right)^T\boldsymbol{T}^T = (\boldsymbol{0} \mid \alpha\boldsymbol{h})\left(\boldsymbol{TP}^{-1}\right)^T = (\boldsymbol{0} \mid \boldsymbol{h}') \tag{29}$$

It comes out from (29) that $\boldsymbol{hB}^T = \boldsymbol{0}$ and hence $\boldsymbol{B} = \boldsymbol{0}$ since $|\boldsymbol{h}| = n$. So we can write $\boldsymbol{TP}^{-1} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix}$ and using Lemma 2, $\boldsymbol{PT}^{-1} = \begin{pmatrix} \boldsymbol{A}' & \boldsymbol{0} \\ \boldsymbol{C}' & \boldsymbol{D}' \end{pmatrix}$. Consequently,

$$\boldsymbol{G}_{pub}\boldsymbol{T}^{-1} = \boldsymbol{S}\left(\boldsymbol{X} \mid \boldsymbol{G}\right)\begin{pmatrix} \boldsymbol{A}' & \boldsymbol{0} \\ \boldsymbol{C}' & \boldsymbol{D}' \end{pmatrix} = \boldsymbol{S}\left(\boldsymbol{Z} \mid \boldsymbol{G}^*\right)$$

where $\boldsymbol{G}^* = \boldsymbol{GD}'$ is a generator matrix of a (n, k) −Gabidulin code. So $\boldsymbol{T}$ is an alternative column scrambler matrix for the system. □

References

1. Shor P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Goldwasser S. (ed.) FOCS, pp. 124–134 (1994).
2. Shor P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997).
3. McEliece R.J.: A public-key system based on algebraic coding theory, pp. 114–116. Jet Propulsion Lab (1978). DSN Progress Report 44.
4. Gabidulin E.M., Paramonov A.V., Tretjakov O.V.: Ideals over a non-commutative ring and their applications to cryptography. In: Advances in Cryptology—EUROCRYPT'91, Number 547 in Lecture Notes in Computer Science, pp. 482–489. Brighton (1991).
5. Gibson K.: Severely denting the Gabidulin version of the McEliece public key cryptosystem. Des. Codes Cryptogr. **6**(1), 37–45 (1995).
6. Gibson K.: The security of the Gabidulin public key cryptosystem. In: Ueli M. (ed.) Advances in Cryptology—EUROCRYPT '96. Lecture Notes in Computer Science, vol. 1070, pp. 212–223. Springer, New York (1996).
7. Gabidulin E.M., Ourivski A.V.: Modified GPT PKC with right scrambler. Electron. Notes Discret. Math. **6**, 168–177 (2001).
8. Gabidulin E.M., Ourivski A.V., Honary B., Ammar B.: Reducible rank codes and their applications to cryptography. IEEE Trans. Inform. Theory **49**(12), 3289–3293 (2003).
9. Overbeck R.: Extending Gibson's attacks on the GPT cryptosystem. In: Oyvind Y. (ed.) WCC 2005. Lecture Notes in Computer Science, vol. 3969, pp. 178–188. Springer, New York (2005).
10. Overbeck R.: A new structural attack for GPT and variants. In: Mycrypt. Lecture Notes in Computer Science, vol. 3715, pp. 50–63 (2005).
11. Overbeck R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptol. **21**(2), 280–301 (2008).
12. Loidreau P.: Designing a rank metric based McEliece cryptosystem. In: Nicolas S. (ed.) Post-Quantum Cryptography. Lecture Notes in Computer Science, vol. 6061, pp. 142–152. Springer, New York (2010).
13. Rashwann H., Gabidulin E., Honary B.: A smart approach for GPT cryptosystem based on rank codes. In: Proceedings IEEE International Symposium Information Theory—ISIT, pp. 2463–2467 (2010).
14. Gabidulin E.M.: Attacks and counter-attacks on the GPT public key cryptosystem. Des. Codes Cryptogr. **48**(2), 171–177 (2008).
15. Gabidulin E., Rashwan H., Honary B.: On improving security of GPT cryptosystems. In: Proceedings of IEEE International Symposium on Theory—ISIT, pp. 1110–1114 (2009).
16. Rashwan H., Gabidulin E., Honary B.: Security of the GPT cryptosystem and its applications to cryptography. Secur. Commun. Netw. **4**(8), 937–946 (2011).
17. Gaborit P., Ruatta O., Schrek J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inform. Theory **62**(2), 1006–1019 (2016).
18. Horlemann-Trautmann A-L, Marshall K, Rosenthal J: Considerations for rank-based cryptosystems. In: IEEE International Symposium on Information Theory (ISIT), pp. 2544–2548 (2016).
19. Horlemann-Trautmann A-L, Marshall K, Rosenthal J.: Extension of overbeck's attack for gabidulin based cryptosystems. Des. Codes Cryptogr. (2017).