Extension of Overbeck’s attack for Gabidulin-based cryptosystems

Anna-Lena Horlemann-Trautmann1 · Kyle Marshall2 · Joachim Rosenthal2

Received: 15 January 2016 / Revised: 22 December 2016 / Accepted: 11 February 2017 / Published online: 28 April 2017
© Springer Science+Business Media New York 2017

Abstract Cryptosystems based on codes in the rank metric were introduced in 1991 by Gabidulin, Paramanov, and Tretjakov (GPT) and have been studied as a promising alternative to cryptosystems based on codes in the Hamming metric. In particular, it was observed that the combinatorial solution for solving the rank analogy of the syndrome decoding problem appears significantly harder. Early proposals were often made with an underlying Gabidulin code structure. Gibson, in 1995, made a promising attack which was later extended by Overbeck in 2008 to cryptanalyze many of the systems in the literature. Improved systems were then designed to resist the attack of Overbeck and yet continue to use Gabidulin codes. In this paper, we generalize Overbeck’s attack to break the GPT cryptosystem for all possible parameter sets, and then extend the attack to cryptanalyze particular variants which explicitly resist the attack of Overbeck.

Keywords Cryptography · Public key cryptography · Rank metric · Gabidulin codes · Coding theory

Mathematics Subject Classification 94B05 · 11T71 · 14G50 · 81P94

This is one of several papers published in Designs, Codes and Cryptography comprising the Special Issue on Network Coding and Designs.
1 Introduction

Cryptosystems based on the hardness of the general decoding problem have received much attention because of their applications to post-quantum cryptography. The practical implementation of these systems, however, has suffered from the drawback of having a large key size relative to RSA or elliptic curve cryptography (ECC). Regardless, coding based cryptography remains one of the most feasible alternatives to traditional number theoretic cryptosystems for resisting quantum attacks such as Shor’s factoring algorithm. A large body of work has been produced in the study of cryptography based on codes in the Hamming metric, starting with McEliece [15]. It was observed that the cryptosystem he designed had efficient encryption and decryption procedures, however, the proposed public key sizes were significantly larger than keys for RSA or ECC, rendering the system infeasible in its original form.

The large size of the key in the McEliece cryptosystem is a consequence of the efficiency of combinatorial solutions to the general decoding problem for codes in the Hamming metric. The impetus for interest in codes in the rank metric were preliminary results concerning the rank syndrome decoding problem, in which the best algorithms were of significantly higher complexity [2,17]. This indicated that cryptosystems could be designed with far smaller parameters than those in the Hamming metric.

Cryptosystems based on codes in the rank metric were introduced earlier by Gabidulin, Paramonov, and Tretjakov (GPT) [5]. Since then, proposals for designs of cryptosystems have alternately been attacked and modified. The designs are often based on Gabidulin codes—the rank metric analogy of generalized Reed-Solomon codes—because of the scarcity of efficiently decodable codes in the rank metric. This has led to efficient structural attacks [9,18] and subsequently improvements in the designs of these codes and their parameters [4,13,14,19]. It should be noted that unlike the syndrome decoding problem in the Hamming metric, the rank syndrome decoding problem is not known to be NP-hard. Other related work has been done in improving algorithms for the rank syndrome decoding problem [8], and also designing rank-metric based cryptosystems which do not rely on Gabidulin codes [7].

The original GPT cryptosystem had its first significant attack by Gibson [9]. Overbeck then proposed an alternative attack that led to a successful polynomial time attack for many parameters of the GPT cryptosystem [18]. In the wake of these developments, two modifications, designed to use Gabidulin codes and yet resist the attack of Overbeck, stand out. They follow a similar idea—a more careful choice of distortion matrix—but have different approaches. The approach taken in [14] is based on enlarging the distortion matrix but restricting its rank, whereas the idea in [19] is based on careful design of the structure of the distortion matrix. While the ideas in these modifications are not necessarily mutually exclusive, an disadvantage of the former version is that it requires a large increase in the public key size in order to be secure against Overbeck’s attack. A disadvantage of the latter version is that the distortion matrices must necessarily be quite structured.

In this paper we present a new attack which can be seen as a generalization of Overbeck’s, and which allows us to cryptanalyze the systems presented in [14,19]. The paper is organized as follows: Sect. 2 provides some terminology as well as the necessary background regarding rank metric codes and the GPT cryptosystem and its variants. Section 3 provides some basic results that we will need to describe our attack. In particular, we need some basic results about Moore matrices as well as the behavior of matrices under the coordinate-wise Frobenius map. Section 4 outlines the attack on the GPT cryptosystem and Sect. 5 uses the method to cryptanalyze the aforementioned variants.
2 Background

Let \( \mathbb{F} \subset \mathbb{E} \) be two fields with \([\mathbb{E} : \mathbb{F}] = m\). We will refer to the rank in the following ways. Given a matrix \( M \) with coefficients in \( \mathbb{E} \), we mean by the rank of \( M \), the usual notion of the dimension of the row span of \( M \) as a vector space over \( \mathbb{E} \). We will denote the row span of a matrix \( M \) over \( \mathbb{E} \) by \( \langle M \rangle \). By column rank (over \( \mathbb{F} \)) of a matrix \( M \) with coefficients in \( \mathbb{E} \), we mean the rank of the column span of \( M \) as an \( \mathbb{E} \)-vector space and we will denote this by \( \text{colrk}(M) \). When we say the rank of a vector, \( x \in \mathbb{E}^n \), we mean the \( \mathbb{F} \)-rank of the matrix obtained by expanding \( x \) into an \( m \times n \) matrix according to some basis of \( \mathbb{E} \) over \( \mathbb{F} \). The rank defined in this way is invariant with respect to the choice of basis. An equivalent way to express the rank of a vector \( x \in \mathbb{E}^n \) is to take the dimension over \( \mathbb{F} \) of the subspace of \( \mathbb{E} \) which is spanned by the coordinates of \( x \).

If we are working over a base field \( \mathbb{F} = \mathbb{F}_q \) of cardinality \( q \), and an extension field \( \mathbb{E} = \mathbb{F}_{qm} \), then we denote by \([i]\) the \( i \)th Frobenius power, \( q^i \). The Frobenius map can be applied to a matrix or vector coordinate-wise. If \( M = (M_{a,b}) \) is any matrix (or vector) over \( \mathbb{F}_{qm} \), we define \( M^{(i)} = (M_{a,b}^{(i)}) \). It is easy to verify that \( \langle Mangle^{(i)} = \langle x^{(i)} \mid x \in \langle M \rangle \rangle = \langle M^{(i)} \rangle \).

**Definition 2.1** The *rank distance* between \( x, y \in \mathbb{F}_{qm}^n \) is defined to be

\[
d_R(x, y) = \text{rk}(x - y).
\]

This defines a metric on \( \mathbb{F}_{qm}^n \). If \( V \) is a subspace of \( \mathbb{F}_{qm}^n \), the *minimum rank distance* of \( V \) is given by

\[
d_R^{\text{min}}(V) = \min\{d_R(x, 0) \mid x \in V \setminus \{0\}\} = \min\{\text{rk}(x) \mid x \in V \setminus \{0\}\}.
\]

We will also use the term *weight* of \( x \), denoted by \( \text{wt}_R(x) \), to mean \( d_R(x, 0) \).

The Singleton bound for (linear) rank-metric codes is given by the inequality (see e.g. [3])

\[
d_R^{\text{min}}(V) \leq n - \dim(V) + 1.
\]

**Definition 2.2** A rank-metric code meeting the Singleton bound is called a *maximum rank-distance (MRD) code*.

The linear isometries of \( \mathbb{F}_{qm}^n \) with respect to the rank metric are given by \( (\mathbb{F}_{qm}^n) \times \text{GL}_n(\mathbb{F}_q) \) [1]. Throughout the paper we will make extensive use of the coordinate-wise Frobenius map. This map is a semi-linear isometry of the rank-metric with many useful properties. For more information on semi-linear rank isometries, see [16, 24].

**Definition 2.3** A matrix \( M \in \mathbb{F}_{qm}^{k \times n} \) is called a *Moore matrix* if there exists a \( \alpha \in \mathbb{F}_{qm}^n \) such that row \( i \) of \( M \) is equal to \( \alpha^{(i-1)} \) for \( i = 1, \ldots, k \). \( \alpha \) is called the generator of \( M \).

In the following lemma, we will summarize some of the important properties of Moore matrices. These results are known or are direct consequences of known results.

**Lemma 2.4** Fix \( k \leq N \), and let \( M \in \mathbb{F}_{qm}^{k \times N} \) be a Moore matrix with generator \( \alpha \), with \( \text{rk}(\alpha) = n \leq N \).

1. If \( k \leq n \), then \( \langle M \rangle \) has dimension \( k \), and minimum rank distance \( n - k + 1 \).
2. If \( k < n \), then \( \dim(\langle M \rangle \cap \langle M \rangle^{(1)}) = k - 1 \) and \( \dim(\langle M \rangle + \langle M \rangle^{(1)}) = k + 1 \).
3. If \( A \in \mathbb{F}_{qm}^{k \times N} \) is another Moore matrix then \( M + A \) is also a Moore matrix. Moreover, if the column rank of \( A \) is equal to \( r < n - k + 1 \), then the minimum rank distance of \( \langle M + A \rangle \) is at least \( n - k + 1 - r \).
4. If the minimum rank distance of \( \langle M \rangle \) is \( d > 1 \), then the minimum rank distance of \( \langle M \rangle + \langle M^{(1)} \rangle \) is equal to \( d - 1 \).

5. If the minimum rank distance of \( \langle M \rangle \) is \( d > 1 \), and \( E \in \mathbb{F}_q^{N \times (N-s)} \) is a full rank matrix, then \( ME \) is a Moore matrix and the minimum rank distance of \( \langle ME \rangle = \langle M \rangle E \) is at least \( d - s \).

**Proof** 1. The case \( n = N \) is given in [3, Theorems 6 and 7]. Thus we know that, if \( N > n \), we can puncture the vector space \( \langle M \rangle \) to get a space \( \langle M' \rangle \) of length \( n \), dimension \( k \) and minimum rank distance \( n - k + 1 \). Hence the minimum rank distance of \( \langle M \rangle \) is at least \( n - k + 1 \). That it cannot be greater follows from [11, Lemma 4.7].

2. The first statement follows easily from the Moore matrix structure. This implies that
\[
\dim(\langle M \rangle + \langle M^{(1)} \rangle) = \dim(\langle M \rangle) + \dim(\langle M^{(1)} \rangle) - \dim(\langle M \rangle \cap \langle M^{(1)} \rangle) = k + 1.
\]

3. The first statement follows from the fact that \( (x + y)^{[i]} = x^{[i]} + y^{[i]} \) for any \( x, y \in \mathbb{F}_q^m \). Therefore the Moore structure is preserved under addition of matrices. For the second part note that any element \( a \in \langle A \rangle \) has rank at most \( r \) and any non-zero element \( m \in \langle M \rangle \) has rank at least \( n - k + 1 \). Hence \( a \) can change the rank of \( m \pm a \) by at most \( r \), i.e. the rank of any non-zero element of \( \langle M + A \rangle \) has rank at least \( n - k + 1 - r \).

4. Since the minimum rank distance of \( \langle M \rangle \) is \( d > 1 \), it follows from 2. that \( \dim(\langle M \rangle + \langle M^{(1)} \rangle) = k + 1 \). Then part 1. implies that the minimum rank distance of \( \langle M + A \rangle \) is \( n - (k + 1) + 1 = d - 1 \).

5. Let \( E' \in \mathbb{F}_q^{N \times s} \) be such that \( [E \mid E'] \) has full rank. Then, \( [E \mid E'] \) is an isometry, and so \( \langle M[E \mid E'] \rangle \) has minimum rank distance \( d \). Removing the last \( s \) columns gives \( \langle ME \rangle \), which can only decrease the rank by at most \( s \).

A well-known class of codes in the rank metric are the Gabidulin codes [3]. Gabidulin codes are those whose generator matrix is a Moore matrix in which the generating vector has full rank:

**Definition 2.5** Fix \( k \leq n \leq m \), and let \( \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n \), \( \text{rk}(\alpha) = n \). The **Gabidulin code** of length \( n \) and dimension \( k \) over \( \mathbb{F}_q^m \), denoted by \( \text{Gab}_{n,k}(\alpha) \) is given by the row space of the matrix,

\[
G = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \ldots & \alpha_n^{[1]} \\ \vdots \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \ldots & \alpha_n^{[k-1]} \end{pmatrix}.
\]

From Lemma 2.4, we have that Gabidulin codes are MRD codes. Moreover, they have efficient decoding algorithms [3,21,22]. Gabidulin codes are also closed under the linear isometries of the rank-metric. Specifically, if \( \beta \in \mathbb{F}_q^* \) and \( \sigma \in \text{GL}_n(\mathbb{F}_q) \), then \( \beta \text{Gab}_{n,k}(\alpha) \sigma = \text{Gab}_{n,k}(\beta \alpha \sigma) \).

2.1 Decoding from an arbitrary generator matrix

McEliece cryptosystems based on Generalized Reed–Solomon (GRS) codes were effectively broken by Sidelnikov–Shestakov [20]. Their attack allows one to recover the generating vector of a GRS code, and therefore a decoding algorithm. Similarly, in the case of Gabidulin codes, a decoding algorithm can be found if one knows the canonical generator matrix of the code.
Using a simple method, we can also recover a decoding algorithm if the generator matrix is not in canonical form, as described in the following.

Consider the Gabidulin code $\text{Gab}_{n,k}(\alpha)$ with dimension $1 < k < n$ and generator matrix $SG$, where $S \in \text{GL}_k(\mathbb{F}_{q^m})$ and $G$ of the form (1). Then $\text{Gab}_{n,k}(\alpha) \cap \text{Gab}_{n,k}(\alpha)$ is the Gabidulin code $\text{Gab}_{n,k-1}(\alpha^{[k-1]})$ (see Lemma 2.4). Iterating with this new Gabidulin code, we can eventually obtain a code of dimension 1, which is generated by $\alpha^{[k-1]}$. If we take some non-zero element of this space, it has the form $\beta \alpha^{[k-1]}$, for some $\beta \in \mathbb{F}_{q^m}$. Applying the Frobenius map coordinate-wise $m - k + 1$ times, we obtain an element of the form $\beta^{[m-k+1]} \alpha$. Using this element, we can construct a generator matrix, $BG$, for $\text{Gab}_{n,k}(\alpha)$ which will have the form

$$BG = \begin{pmatrix} 
\beta^{[m-k+1]} \\
\vdots \\
\beta 
\end{pmatrix} \begin{pmatrix} 
\alpha_1 & \alpha_2 & \ldots & \alpha_n \\
\alpha_1^{[1]} & \alpha_2^{[1]} & \ldots & \alpha_n^{[1]} \\
\vdots & \vdots & \ldots & \vdots \\
\alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \ldots & \alpha_n^{[k-1]} 
\end{pmatrix}.$$ 

The change of basis from $SG$ to $BG$ is then given by $BS^{-1}$. For a message $m \in \mathbb{F}_{q^m}^k$, encoded as $mSG$, we can now decode with respect to $\text{Gab}_{n,k}(\beta^{[m-k+1]} \alpha)$ to obtain $mSB^{-1}$. Then, applying $BS^{-1}$, we can recover $m$.

2.2 GPT and GGPT cryptosystems

Let $S \in \text{GL}_k(\mathbb{F}_{q^m})$, $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a Gabidulin code, say $\text{Gab}_{n,k}(\alpha)$, capable of correcting $t'$ errors, and $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of column rank $t < t'$. We define

$$G_{\text{pub}} := SG + X.$$ 

We call a GPT cryptosystem one in which the public key is given by the pair

$$\kappa_{\text{pub}} = (G_{\text{pub}}, t' - t),$$

and the private key is given by

$$\kappa_{\text{pvt}} = (G, S).$$

An encryption of a message $m \in \mathbb{F}_{q^m}^k$ is given by

$$mG_{\text{pub}} + e = mSG + mX + e,$$

where $e \in \mathbb{F}_{q^m}^n$ is a randomly chosen vector of rank at most $t' - t$. The product $mS$ can be recovered from a decoding algorithm for $\text{Gab}_{n,k}(\alpha)$ because all elements of $\langle X \rangle$ have weight at most $t$. Specifically, if $\text{wt}_R(e) \leq t' - t$,

$$\text{wt}_R(mX + e) \leq \text{wt}_R(mX) + \text{wt}_R(e) \leq t'.$$

Inverting $S$, the message $m$ can then be recovered. We will call the elements of the form $mX$ the designed error associated with the encryption of $m$, and $X$ the designed error matrix.

In [14, 19] the authors consider an alternative version which we call the generalized GPT (GGPT) cryptosystem. This system uses a public matrix of the form

$$\hat{G}_{\text{pub}} := S[X \mid G]\sigma \in \mathbb{F}_{q^m}^{k \times (n + \hat{t})},$$

where $G$ is as before, $X \in \mathbb{F}_{q^m}^{k \times \hat{t}}$ is a matrix of column rank $\hat{t}$, $S \in \text{GL}_k(\mathbb{F}_{q^m})$, and $\sigma \in \text{GL}_{n+\hat{t}}(\mathbb{F}_{q})$. The public key is given by

$$\hat{G}_{\text{pub}} := S[X \mid G]\sigma \in \mathbb{F}_{q^m}^{k \times (n + \hat{t})},$$

where $G$ is as before, $X \in \mathbb{F}_{q^m}^{k \times \hat{t}}$ is a matrix of column rank $\hat{t}$, $S \in \text{GL}_k(\mathbb{F}_{q^m})$, and $\sigma \in \text{GL}_{n+\hat{t}}(\mathbb{F}_{q})$. The public key is given by
\[ \kappa_{\text{pub}} = (\hat{G}_{\text{pub}}, t'), \] (6)

and the private key is given by
\[ \kappa_{\text{pvt}} = (G, S, \sigma). \] (7)

In the GGPT cryptosystem, an encryption of \( m \in \mathbb{F}^k_{q^m} \) is given by
\[ m \hat{G}_{\text{pub}} + e, \]
with \( \text{rk}(e) \leq t' \). To recover \( m \), one first computes
\[ (m \hat{G}_{\text{pub}} + e)\sigma^{-1}, \]
and then ignores the first \( \hat{t} \) coordinates. Decoding the last \( n \) coordinates with respect to \( \text{Gab}_{n,k}(\alpha) \), one obtains \( mS \), and by applying \( S^{-1} \), the message \( m \) can be recovered.

### 2.3 Overbeck’s attack

We will describe Overbeck’s attack from [18] for the case of the GGPT cryptosystem; the attack for the GPT case is analogous. Let \( G \in \mathbb{F}^{k \times n}_{q^m} \) be a generator matrix for the Gabidulin code, \( \text{Gab}_{n,k}(\alpha) \). The first step in Overbeck’s attack is to consider the extended matrix (for some \( u \geq 1 \))
\[
G_{\text{ext}} := \begin{pmatrix} \sigma(S[X | G]) & \sigma(G^{(1)}) \\ \vdots & \vdots \\ \sigma(S[X | G]) & \sigma(G^{(u)}) \end{pmatrix} \sigma.
\]

Since the \( n \) right-most columns of \( G_{\text{ext}}\sigma^{-1} \) span the Gabidulin code \( \text{Gab}_{n,k+u}(\alpha) \), the matrix can be brought into the form of
\[ G'_{\text{ext}} = \hat{S}^t \begin{pmatrix} X^* & G^* \\ 0 & 0 \end{pmatrix} \sigma, \] (8)

by some suitable row transformation, where \( X^* \in \mathbb{F}^{(k+u) \times i}_{q^m} \), \( G^* \in \mathbb{F}^{(k+u) \times n}_{q^m} \) is a generator matrix of \( \text{Gab}_{n,k+u}(\alpha) \), and \( X^{**} \in \mathbb{F}^{(k-1)u \times i}_{q^m} \). If \( X^{**} \) has rank \( \hat{t} \), then any element of \( \langle G'_{\text{ext}} \rangle^\perp = (G_{\text{ext}})^\perp \) has the form \( \sigma^{-1}[0 \mid h] \), where \( h \in \text{Gab}_{n,k+u}(\alpha)^\perp \). With this information one can reconstruct the code \( \text{Gab}_{n,k}(\alpha) \) and recover the encrypted message.

In the case when \( X^{**} \) does not have full rank, Overbeck’s attack fails, since \( \text{Gab}_{n,k}(\alpha) \) cannot be reconstructed from the dual of \( (G_{\text{ext}})^\perp \). This is why, in [14], Loidreau suggests to use a randomly chosen \( X \) of low rank, \( a \), since then the rank of \( X^{**} \) can be bounded above. Specifically, to resist Overbeck’s attack, one should choose \( \hat{t} > (n - k)a \). However, this would drastically increase the key size of the cryptosystem. To avoid this problem of large key size, the Smart Approach considered in [19], is to design \( X \) in a structured way so that \( X^{**} \) is rank-deficient, without necessarily having to increase \( \hat{t} \). However the structure of \( X \) makes the Smart Approach more vulnerable to attacks. A more detailed description of these two systems is given in Sect. 5.
3 Preliminary results

In this section, we show that one can decompose a matrix (or vector) of low column rank into the product of two matrices, one of which has full column rank, and the other with elements restricted to $\mathbb{F}_q$. Moreover, we prove some results about the coordinate-wise Frobenius map, as well as the structure of the designed error matrix, which we will need later on in our attack.

We will denote by $M_{t\times n,r}(\mathbb{F}_q)$ the set of $t \times n$ matrices over $\mathbb{F}_q$ with rank $r$. The sphere around the origin of rank radius $t$ in $\mathbb{F}_q^{n \times m}$ will be denoted by

$$S_{n,t}^{\mathbb{F}_q^{m}} := \{ x \in \mathbb{F}_q^{m} \mid \text{rk}(x) = t \}.$$

Proposition 3.1

$$S_{n,t}^{\mathbb{F}_q^{m}} \cong S_{t,n}^{\mathbb{F}_q^{m}} \times M_{t\times n,t}(\mathbb{F}_q)/\text{GL}_t(\mathbb{F}_q),$$

where $M_{t\times n,t}(\mathbb{F}_q)/\text{GL}_t(\mathbb{F}_q)$ is the set of equivalence classes of $t \times n$ matrices over $\mathbb{F}_q$ of rank $t$, where two matrices are equivalent if they have the same row span.

Proof As representatives of the cosets in $M_{t\times n}(\mathbb{F}_q)/\text{GL}_t(\mathbb{F}_q)$ we consider the reduced row echelon form of the respective row span of the elements of the coset. Define the map

$$\varphi : S_{t,n}^{\mathbb{F}_q^{m}} \times M_{t\times n}(\mathbb{F}_q)/\text{GL}_t(\mathbb{F}_q) \rightarrow S_{n,t}^{\mathbb{F}_q^{m}},$$

$$(v, U) \mapsto vU.$$

We now show that $\varphi$ is bijective.

We first show that $\varphi$ is surjective. For this consider an arbitrary element in the image of $\varphi$, i.e. a vector $x \in \mathbb{F}_q^n$ of rank $t$, and let $x_{i_1}, \ldots, x_{i_t}$ be the first $t$ independent entries of $x$, in positions $i_1, \ldots, i_t$. Then, the remaining $n-t$ entries of $x$ can be expressed as an $\mathbb{F}_q$-linear combination of $x_{i_1}, \ldots, x_{i_t}$, thus we can write $x = (x_{i_1}, \ldots, x_{i_t})M$ for some matrix $M \in \mathbb{F}_q^{t \times n}$. Then there exists $S \in \text{GL}_t(\mathbb{F}_q)$ such that $U = SM$ is in reduced row echelon form. We get $(x_{i_1}, \ldots, x_{i_t})S \in S_{t,n}^{\mathbb{F}_q^{m}}$ and $x = \varphi((x_{i_1}, \ldots, x_{i_t})S, U)$, thus $\varphi$ is surjective.

To show injectivity, suppose that there are two preimages, i.e. $x = \varphi(v, U) = \varphi(v', U')$. Without loss of generality, we can assume that $U = [I_t \mid \ast]$. Denote by $U'_j$ the $j$th column of $U'$. Then we have

$$(x_1, \ldots, x_t) = v = (v'U'_1, \ldots, v'U'_t).$$

Since $v$ has rank $t$, $U'_1, \ldots, U'_t$ must be non-zero. Because $U'$ is in reduced row echelon form, we get $U' = [I_t \mid \ast]$ and hence

$$(x_1, \ldots, x_t) = v = v'.$$

We furthermore have $x_j = vU_j = v'U'_j$ for $j = t+1, \ldots, n$. Thus

$$vU_j = v'U'_j \iff vU_j = vU'_j \iff v(U_j - U'_j) = 0.$$  

Since $\text{rk}(v) = t$, we get $U_j - U'_j = 0$ for $j = t+1, \ldots, n$. Thus $U = U'$ and we have shown that $\varphi$ is injective. \hfill $\square$

One can think of the space $M_{t\times n,t}(\mathbb{F}_q)/\text{GL}_t(\mathbb{F}_q)$ as a set of matrices parameterizing the Grassmannian $\text{Gr}(t, \mathbb{F}_q^n)$, i.e. the space of $t$-dimensional subspaces of $\mathbb{F}_q^n$. According to the proof of Proposition 3.1, we can express a vector $x$ of rank $t$ as $x = \hat{x}U$ for any matrix representation $U$ of a certain element of the Grassmannian $\text{Gr}(t, \mathbb{F}_q^n)$.

We can easily extend the result of Proposition 3.1 from vectors of rank $t$ to matrices of column rank $t$. Then we get the following result.
Corollary 3.2 Let $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of rank $k$ and column rank $t$. Then there exist $V \in \mathbb{F}_{q^m}^{k \times n}$ with $\text{rk}(V) = k$ and $U \in \mathbb{F}_{q^m}^{t \times n}$ with $\text{rk}(U) = t$, such that $X = VU$.

Definition 3.3 Let $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of rank $k$ and column rank $t$ and $V \in \mathbb{F}_{q^m}^{k \times t}$, $U \in \mathbb{F}_{q^m}^{t \times n}$ such that $X = VU$. We call $\langle U \rangle$ the Grassmann support of $X$ which will be denoted by $\langle U \rangle = \text{supp}_{\text{Gr}}(X)$. By abuse of notation we will also call any matrix representation $U \in \mathbb{F}_{q^m}^{t \times n}$ of this space a Grassmann support of $X$.

Lemma 3.4 Let $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of rank $k$ and column rank $t \geq k$. Then $\langle X \rangle \subseteq \text{supp}_{\text{Gr}}(X)$ and the inclusion is strict if and only if $t > k$.

Proof Let $U \in \mathbb{F}_{q^m}^{t \times n}$ be the Grassmann support of $X$. By Corollary 3.2, we can write $X = VU$ for some $V \in \mathbb{F}_{q^m}^{k \times t}$. Thus every row of $X$ is a $\mathbb{F}_{q^m}$-linear combination of the rows of $U$, which implies that $\langle X \rangle \subseteq \langle U \rangle$. Since $\dim(\langle U \rangle) = t$ and $\dim(\langle X \rangle) = k$, we get equality if and only if $k = t$. \qed

The following two lemmas are needed to prove the main results of this section in Theorems 3.7 and 3.10.

Lemma 3.5 Let $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of column rank $t$ and $S \in \text{GL}_k(\mathbb{F}_{q^m})$. Then, $SX$ also has column rank $t$.

Proof Denote the $i$th column of $X$ by $X_i$. Assume that $SX$ has column rank less than $t$, i.e. for any $i_1 < \cdots < i_t \in \{1, \ldots, n\}$ there exist $a_1, \ldots, a_t \in \mathbb{F}_q$ such that

$$\sum_{\ell=1}^{t} a_{\ell} (SX)_{i_\ell} = 0 \iff \sum_{\ell=1}^{t} a_{\ell} X_{i_\ell} = 0 \iff \sum_{\ell=1}^{t} a_{\ell} X_{i_\ell} = 0.$$ 

This is a contradiction to the fact that the column rank of $X$ is $t$. \qed

The following properties of the coordinate-wise Frobenius map will be used throughout the paper. The first statement follows straightforwardly from the $\mathbb{F}_q$-linearity of the Frobenius map, the second and the third are known and can be found, for instance, in [10, 11].

Lemma 3.6 The following hold for any prime power $q$ and $0 < n \leq m$.

1. Let $x \in \mathbb{F}_q^n$ have rank $r$. Then, $x^{(1)}$ also has rank $r$.
2. Let $M \in \text{GL}_n(\mathbb{F}_q)$. Then, $(M^{-1})^{(1)} = (M^{(1)})^{-1}$.
3. Let $S \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q^n$-subspace. Then, $S^{(1)} = S$ if and only if $S$ has a basis contained in $\mathbb{F}_q^n$.

We saw in Lemma 3.4 that if a matrix $X$, with Grassmann support $U$, has column rank which is greater than its rank, then $\langle X \rangle \subsetneq \langle U \rangle$. The following theorem shows that we can use the Frobenius map to recover $\langle U \rangle$ from $X$.

Theorem 3.7 Let $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of column rank $t$. Then, for any $\ell \geq 0$,

$$\sum_{i=0}^{t-1} \langle X \rangle^{(i+1)} = \sum_{i=0}^{t} \langle X \rangle^{(i)} = \text{supp}_{\text{Gr}}(X).$$
In particular,

\[ \dim \left( \sum_{i=0}^{t-1} \langle X \rangle^{(i)} \right) = t. \]

**Proof** The chain of subspaces

\[ \langle X \rangle \subseteq \langle X \rangle + \langle X \rangle^{(1)} \subseteq \sum_{i=0}^{2} \langle X \rangle^{(i)} \subseteq \cdots \]

must eventually stabilize. Let \( \ell \) be such that,

\[ \sum_{i=0}^{\ell-1} \langle X \rangle^{(i)} = \sum_{i=0}^{\ell} \langle X \rangle^{(i)}. \]

Define \( s' := \dim \sum_{i=0}^{\ell-1} \langle X \rangle^{(i)} \). We have

\[ \left( \sum_{i=0}^{\ell-1} \langle X \rangle^{(i)} \right)^{(1)} \subseteq \sum_{i=1}^{\ell} \langle X \rangle^{(i)} \subseteq \sum_{i=0}^{\ell} \langle X \rangle^{(i)} = \sum_{i=0}^{\ell-1} \langle X \rangle^{(i)}. \]

Therefore we can use the third point of Lemma 3.6 and express the sum on the right as the row space of a matrix \( U' \in \mathbb{F}_{q}^{s' \times n} \) of (column) rank \( s' \). Thus there exists \( S \in \text{GL}_{k \ell} (\mathbb{F}_{q}^{m}) \) such that

\[ \begin{pmatrix} X^{(1)} \\ \vdots \\ X^{(\ell-1)} \end{pmatrix} = S \begin{pmatrix} U' \\ 0 \end{pmatrix}. \]

This implies that \( \langle X \rangle \subseteq \langle U' \rangle \). It follows from Proposition 3.1 that \( s' \geq t \). Moreover, by Lemma 3.5, the left side of (9) has column rank \( s' \). By the \( \mathbb{F}_{q} \)-linearity of the Frobenius map, the column rank of this matrix is equal to the column rank of \( X \), therefore we get \( t = s' \) and hence \( \text{supp}_{\text{Gr}}(X) = \langle U' \rangle \).

Note that a matrix \( X \in \mathbb{F}_{q}^{k \times n} \) can always be decomposed into a Moore matrix component \( X_{\text{Moore}} \) and a non-Moore matrix component \( Z \) as

\[ X = X_{\text{Moore}} + Z. \]

**Definition 3.8** We will call such a decomposition a **Moore decomposition**. There exists a Moore decomposition so that the non-Moore component has lowest possible column rank. In this case, we call the Moore decomposition a **minimum column rank Moore decomposition**.

Proposition 3.9 shows that, regardless of the choice of Moore decomposition, the Grassmann support of a non-Moore matrix component of a minimum column rank Moore decomposition is the same.

**Proposition 3.9** Suppose that \( X \in \mathbb{F}_{q}^{k \times n} \) is a matrix which has minimum column rank Moore decomposition \( X = A_{\text{Moore}} + A \), where \( A_{\text{Moore}} \) is a Moore matrix, and \( A \) has column rank \( s \). Then any other minimum column rank Moore decomposition \( X = B_{\text{Moore}} + B \) satisfies \( \text{supp}_{\text{Gr}}(A) = \text{supp}_{\text{Gr}}(B) \).
Proof Let $A$ have Grassmann support $U$, and $B$ have Grassmann support $V$. We can write $A = A'U$ and $B = B'V$ with $U, V \in \mathbb{F}_{q}^{r \times n}$ of full rank. Let $E \in \mathbb{F}_{q}^{s \times s}$ be a parity check matrix for $\langle V \rangle$. Then,

$$B_{\text{Moore}}E^T = XE^T - BE^T = XE^T = A_{\text{Moore}}E^T + AE^T,$$

which yields

$$(B_{\text{Moore}} - A_{\text{Moore}})E^T = AE^T.$$ 

Since $E$ is a matrix over $\mathbb{F}_q$, $(B_{\text{Moore}} - A_{\text{Moore}})E^T$ is a Moore matrix, therefore the matrix $AE^T$ must be a Moore matrix as well. This gives that $(AE^T)_i = (A_1E^T)(i-1) = A_1(i-1)E^T$ for $i = 1, \ldots, k$. Since $A$ itself is not necessarily a Moore matrix, row $i$ of $A$ must be of the form $A_i \in A_1(i-1) + \ker(E)$, for $i = 1, \ldots, k$. Then, we can write

$$A = \begin{pmatrix} A_{1(1)} & & & \\ \vdots & & & \\ A_{1(k-1)} & & & \\ \kappa_1 & & & \\ \kappa_2 & & & \\ \vdots & & & \\ \kappa_k & & & \\ \kappa' & & & \\ \tilde{A} & & & \\ \kappa'V & & & \end{pmatrix},$$

for $\kappa_1, \ldots, \kappa_k \in \ker(E) = \langle V \rangle$ and $\kappa' \in \mathbb{F}_q^{k \times s}$. If we let $F \in \mathbb{F}_q^{(n-s) \times n}$ be a parity check matrix for $\langle U \rangle$, then $AF^T = A'UF^T = 0$ and hence in particular $A_1F^T = 0$. Since $F$ is a matrix over $\mathbb{F}_q$, we also get $A_1(i)F^T = 0$ for $i = 1, \ldots, k - 1$. Hence,

$$0 = AF^T = \tilde{A}F^T + \kappa'VF^T = \kappa'VF^T.$$

Since $X = (A_{\text{Moore}} + \tilde{A}) + \kappa'V$ is also a Moore decomposition of $X$, then the column rank of $\kappa'V$ must be equal to $s$ and so $\langle V \rangle = \langle \kappa'V \rangle$. Thus,

$$\langle V \rangle F^T = 0,$$

and therefore, $\langle V \rangle = \langle U \rangle$, so the Grassmann supports of $A$ and $B$ are the same. \hfill \Box

Theorem 3.10 Let $M \in \mathbb{F}_{q}^{k \times n}$ be a Moore matrix and $X \in \mathbb{F}_{q}^{s \times n}$ be of column rank $s$, where $s$ is the rank of the non-Moore component in a minimum column rank Moore decomposition of $X$. Then, we have

$$\sum_{i=0}^{s} \langle M + X \rangle^{(i)} = \sum_{i=0}^{s} \langle M \rangle^{(i)} + \text{supp}_{Gr}(X).$$

Proof Let $U \in \mathbb{F}_q^{r \times n}$ be the Grassmann support of $X$. Moreover, let $X_i, M_i$ denote the $i$th row of $X$ and $M$ respectively, and let

$$X' = \begin{pmatrix} X_{1(1)} - X_2 \\ X_{2(1)} - X_3 \\ \vdots \\ X_{k-1(1)} - X_k \\ X_{k(1)} \end{pmatrix}, \quad M' = \begin{pmatrix} M_{1(1)} \\ \vdots \\ M_{k+s-1(1)} \end{pmatrix}, \quad X^* = \begin{pmatrix} X_{1} \\ X_{1(1)} \\ \vdots \\ X_{k(s-1)} \\ X_{1(s)} \\ \vdots \\ X_{k(s)} \end{pmatrix}. $$
Then the space \( \sum_{i=0}^{s} \langle M + X \rangle^{(l_i)} \) is generated by the row span of
\[
\begin{pmatrix}
M + X \\
(M + X)^{(l_1)} \\
\vdots \\
(M + X)^{(l_s)}
\end{pmatrix}
\]
for a suitable row transformation matrix \( \tilde{S} \).

Since \( U \in \mathbb{F}_q^{s \times n} \), we have \( U^{(l_i)} = U \) for \( i \geq 0 \). It follows that the rows of \( X' \) are elements of \( \langle U \rangle \), which implies that the Grassmann support \( \langle U' \rangle \) of \( X' \) is a subspace of \( \langle U \rangle \) and hence that \( X' \) has column rank \( s' \leq s \). By Theorem 3.7,
\[
\sum_{i=0}^{s'-1} \langle X' \rangle^{(l_i)} = \sum_{i=0}^{s-1} \langle X' \rangle^{(l_i)} = \langle U' \rangle \subseteq \langle U \rangle.
\]

We now want to show that \( \langle U' \rangle = \langle U \rangle \). Suppose for the sake of contradiction that the rank of \( U' \) is strictly smaller than \( s \). We write \( X \) as a Moore decomposition
\[
X = \begin{pmatrix}
X_1 \\
X_2 \\
\vdots \\
X_k
\end{pmatrix} = \begin{pmatrix}
X_1^{(l_1)} \\
X_2^{(l_1)} \\
\vdots \\
X_k^{(l_1)}
\end{pmatrix} + \begin{pmatrix}
0 \\
X_2 - X_1^{(l_1)} \\
\vdots \\
X_k - X_1^{(l_1)}
\end{pmatrix}.
\]
We note that \( X_{i+1} - X_i^{(l_1)} \in \langle U' \rangle \) for \( i = 1, \ldots, k - 1 \). Starting from the first non-zero row of \( X'' \), it follows that
\[
(X_2 - X_1^{(l_1)})^{(l_1)} = X_2^{(l_1)} - X_1^{(l_2)} \in \langle U' \rangle
\]
which implies
\[
X_2^{(l_1)} - X_1^{(l_2)} - (X_2^{(l_1)} - X_3) \in \langle U' \rangle \iff X_3 - X_1^{(l_2)} \in \langle U' \rangle.
\]
We recognize this as the second non-zero row of \( X'' \). Continuing in this fashion, we can obtain that every row of \( X'' \) must belong to \( U' \). Hence, \( X'' \) has column rank at most \( s' < s \). However, this contradicts the fact that the minimal column rank Moore decomposition has non-Moore part with column rank \( s \). Therefore, by Proposition 3.9, \( U' \) has rank \( s \) and we have \( \langle U' \rangle = \langle U \rangle \).

Hence, we have shown that the row space of the second matrix in (10) is equal to the row space of
\[
\begin{pmatrix}
M^* + X^* \\
U
\end{pmatrix}
\]
which is in turn equal to the row space of
\[
\begin{pmatrix}
M^* \\
U
\end{pmatrix}
\]
because we can cancel \( X^* \) by taking suitable elements of \( \langle U \rangle \), since \( \langle X^* \rangle \subseteq \langle U' \rangle = \langle U \rangle \).
This implies the statement. \( \square \)
Lemma 3.11 Let $X \in \mathbb{F}_{q^n}^{k \times n}$ have minimum column rank Moore decomposition, $X = X_{\text{Moore}} + Z$. Then,

$$\text{supp}_{\text{Gr}}(X_{\text{Moore}}) + \text{supp}_{\text{Gr}}(Z) = \text{supp}_{\text{Gr}}(X).$$

In particular, $\text{colrk}(X_{\text{Moore}}) \leq \text{colrk}(X)$.

Proof Define $\ell := \max\{\text{colrk}(X), \text{colrk}(X_{\text{Moore}}), \text{colrk}(Z)\}$. Using Theorems 3.7 and 3.10, we have

$$\text{supp}_{\text{Gr}}(X) = \sum_{i=0}^{\ell} \langle X \rangle^{(i)}$$

$$= \sum_{i=0}^{\ell} \langle X_{\text{Moore}} + Z \rangle^{(i)}$$

$$= \sum_{i=0}^{\ell} \langle X_{\text{Moore}} \rangle^{(i)} + \text{supp}_{\text{Gr}}(Z)$$

$$= \text{supp}_{\text{Gr}}(X_{\text{Moore}}) + \text{supp}_{\text{Gr}}(Z).$$

Corollary 3.12 Let $M \in \mathbb{F}_{q^n}^{k \times n}$ be a Moore matrix and $X$ be of column rank $t$ with minimum column rank Moore decomposition $X = X_{\text{Moore}} + Z$, where $\text{colrk}(Z) = s$. Suppose that $d_{\text{min}}^R((M)) \geq s + t + 2$. Then, all elements of rank one in

$$\sum_{i=0}^{s} \langle M + X \rangle^{(i)}$$

belong to $\text{supp}_{\text{Gr}}(X)$. Moreover, if $s = t$, the elements of rank one exactly span $\text{supp}_{\text{Gr}}(X) = \text{supp}_{\text{Gr}}(Z)$.

Proof Let $U$ be the subspace spanned by all elements of rank one in

$$\sum_{i=0}^{s} \langle M + X \rangle^{(i)}.$$

From Lemma 3.11, if $X = X_{\text{Moore}} + Z$, is a minimum column rank decomposition, then we know that $\text{supp}_{\text{Gr}}(Z) \subseteq \text{supp}_{\text{Gr}}(X)$. Let $H \in \mathbb{F}_{q}^{(n-t) \times n}$ be parity check matrix for $\text{supp}_{\text{Gr}}(X)$. From Lemma 2.4, we have

$$d_{\text{min}}^R\left(\sum_{i=0}^{s} \langle M + X \rangle^{(i)} H^T\right) = d_{\text{min}}^R\left(\sum_{i=0}^{s} \langle M \rangle^{(i)} H^T\right)$$

$$\geq (s + t + 2) - s - t$$

$$= 2.$$

Since $H$ is a matrix over $\mathbb{F}_q$, we get $\text{wt}_R(x) \leq \text{wt}_R(xH)$, and therefore we must have that $U \subseteq \text{supp}_{\text{Gr}}(X)$. By Theorem 3.10, $\text{supp}_{\text{Gr}}(Z) \subseteq U$ and if $s = t$ then $\text{supp}_{\text{Gr}}(Z) = \text{supp}_{\text{Gr}}(X)$. Therefore we have

$$\text{supp}_{\text{Gr}}(Z) = U = \text{supp}_{\text{Gr}}(X).$$

\qed
To set up our attack in Sect. 4, we must be able to find the elements of rank one in a linear rank metric code efficiently. To accomplish this, we only need to find the codewords that have all coordinates in $\mathbb{F}_q$ (all other rank one codewords are multiples of these). The following lemma shows how these codewords in $\mathbb{F}_q^n$ can be computed.

**Lemma 3.13** Let $G \in \mathbb{F}_{qm}^{k \times n}$ be in reduced row echelon form and denote by $G_i$ the $i$th row of $G$. Then the solutions to
\[
\sum_{i=1}^{k} a_i (G_i^{[1]} - G_i) = 0,
\]
for variables $a_i \in \mathbb{F}_q$, represent the codewords of $\langle G \rangle$ in $\mathbb{F}_q^n$.

**Proof** Any codeword can be written as an $\mathbb{F}_q$-linear combination of the rows of $G$. Since all rows of $G$ have their pivot equal to 1, a codeword with entries only in $\mathbb{F}_q$ needs to be an $\mathbb{F}_q$-linear combination of the rows. Thus, we get that any codeword in $\mathbb{F}_q^n$ can be written as $\sum_{i=1}^{k} a_i G_i$ for some $a_i \in \mathbb{F}_q$. Furthermore, we know that
\[
v \in \mathbb{F}_q^n \iff v^{[1]} - v = 0,
\]
hence
\[
\sum_{i=1}^{k} a_i G_i \in \mathbb{F}_q^n \iff \sum_{i=1}^{k} a_i (G_i^{[1]} - G_i) = 0.
\]

When expanded over $\mathbb{F}_q$, Eq. (11) gives rise to a linear system of equations with $k$ variables, which can efficiently be solved with standard methods.

### 4 Cryptanalysis of the GPT cryptosystem

In this section we explain our new attack to break the GPT cryptosystem, as defined in Sect. 2.2. Our attack extends Overbeck’s attack to cryptanalyze the system for all parameters. In Sect. 5, we show how this same idea can be used to cryptanalyze the GGPT variant.

Recall that the public key generator matrix is of the form
\[
G_{\text{pub}} := SG + X \in \mathbb{F}_{qm}^{k \times n},
\]
where $G$ is a generator matrix of a Gabidulin code $\text{Gab}_{n,k}(\alpha)$, $X \in \mathbb{F}_{qm}^{k \times n}$ is a matrix of column rank $t$, and $S \in \text{GL}_k(\mathbb{F}_q^m)$. Without loss of generality we assume that $G$ is in Moore matrix form.

Note that, as an attacker, we do not have a priori knowledge of the parameter $s$ (the column rank of the non-Moore part in the minimal column rank Moore decomposition of $X$). We can generally assume $s = t$, or else start with $s = 1$ and increase the value up to $t$ until the attack succeeds.

**Theorem 4.1** Consider a GPT cryptosystem as defined in Sect. 2.2, with public key generator matrix $G_{\text{pub}} = SG + X \in \mathbb{F}_{qm}^{k \times n}$. Let $S^{-1}X = X_{\text{Moore}} + Z$ be a minimal column rank Moore decomposition with $s = \text{colrk}(Z)$. Suppose an adversary can find a full rank matrix $U \in \mathbb{F}_q^{s' \times n}$ for $s \leq s' \leq t$ satisfying
\[
\text{supp}_{Gr}(Z) \subseteq \langle U \rangle \subseteq \text{supp}_{Gr}(X),
\]
where $\text{supp}_{Gr}(Z)$ denotes the support of $Z$ with respect to the generator of the code. Then the adversary can recover the private key matrix $S$.
then an encrypted message from a public key of the form (3) can be recovered in polynomial time.

**Proof** Let $H \in \mathbb{F}_q^{(n-s') \times n}$ be a parity check matrix for $\langle U \rangle$. Applying $H$ to the public key generator matrix yields

$$G_{\text{pub}}H^T = (SG + X)H^T = S(G + X_{\text{Moore}})H^T.$$  

From Lemma 3.11 we know that $\text{colrk}(X_{\text{Moore}}) \leq t$. Then, from Sect. 2.4, it follows that $\langle G + X_{\text{Moore}} \rangle$ has minimum rank distance at least $n - k + 1 - t$, and that $(G + X_{\text{Moore}})H^T$ has minimum rank distance at least $n - k + 1 - (t + s')$. Moreover, $GH^T + X_{\text{Moore}}H^T$ is a Moore matrix.

From the minimum distance we know that there are $n - (t + s')$ independent columns in this matrix, which generate a Gabidulin code of minimum distance $n - (t + s') - k + 1$, $\text{Gab}_{n-(t+s'),k}(\gamma)$, for some $\gamma \in \mathbb{F}_q^{n-(t+s')}$. From Sect. 2.1, we can recover a decoding algorithm for $\text{Gab}_{n-(t+s'),k}(\gamma)$ with respect to the submatrix formed by these $n - (t + s')$ columns. The error correction capability of $\text{Gab}_{n-(t+s'),k}(\gamma)$ is

$$\left\lfloor \frac{n - (t + s') - k}{2} \right\rfloor = \left\lfloor \frac{t' - t + s'}{2} \right\rfloor \geq t' - t \geq \text{rk}(e) \geq \text{rk}(eH^T),$$

where the last inequality follows from the fact that $H$ is a matrix over $\mathbb{F}_q$. For an encrypted message $m(SG + X) + e$, we have

$$(m(SG + X) + e)H^T = mS(GH^T + X_{\text{Moore}}H^T) + eH^T.$$  

When we restrict this to the above chosen independent columns, we can uniquely decode in the respective code $\text{Gab}_{n-(t+s'),k}(\gamma)$ and can therefore recover $m$.

We can now use the previous result to attack and break the GPT cryptosystem.

**Corollary 4.2** Consider a GPT cryptosystem as defined in Sect. 2.2 with public key generator matrix $G_{\text{pub}} = SG + X \in \mathbb{F}_q^{k \times n}$. For any such cryptosystem, an encrypted message can be recovered in polynomial time.\(^1\)

**Proof** As before, let $S^{-1}X = X_{\text{Moore}} + Z$ be a minimal column rank Moore decomposition. Denote by $s$ the column rank of $Z$. We first note that $d^R_{\text{min}}(|G|) \geq s + t + 2$, since

$$d^R_{\text{min}}(|G|) - 1 \geq \left\lfloor \frac{n - k}{2} \right\rfloor = t' \geq t \geq \frac{s + t}{2}.$$  

By Corollary 3.12, all the elements of rank one in $\sum_{i=0}^{s}(G + S^{-1}X)^{(i)}$ belong to $\text{supp}_{\text{Gr}}(S^{-1}X) = \text{supp}_{\text{Gr}}(X)$. With Lemma 3.13 we can find a basis matrix $U \in \mathbb{F}_q^{s \times n}$ for these elements of rank one in polynomial time. We have $\langle U \rangle \subseteq \text{supp}_{\text{Gr}}(X)$. On the other hand, by Theorem 3.10, $\text{supp}_{\text{Gr}}(Z) \subseteq \sum_{i=0}^{s}(G + S^{-1}X)^{(i)}$. Thus, we also have $\text{supp}_{\text{Gr}}(Z) \subseteq \langle U \rangle$. Therefore we can use Theorem 4.1 to recover the encrypted message. \(\square\)

\(^1\) The attack needs $O(k^2n^2(s^2 + k))$ operations over $\mathbb{F}_q$, plus the operations needed for the Gabidulin code decoding algorithm. E.g., the decoding algorithm of [23] needs $O(m^3 \log m)$ operations over $\mathbb{F}_q$.  

\(\copyright\) Springer
5 Cryptanalysis of GGPT variants

In this section we adapt our attack to break the GGPT cryptosystem, as defined in Sect. 2.2. To do so we will consider two variants of the GGPT separately. However, in both subsections we will consider a public key generator matrix of the form

\[ \hat{G}_{\text{pub}} := S[X \mid G] \sigma \in \mathbb{F}_{q^m}^{k \times (n+i)}, \]

where \( G \) is a generator matrix of some Gabidulin code \( \text{Gab}_{n,k}(\alpha) \), \( X \in \mathbb{F}_{q^m}^{k \times i} \) is a matrix of column rank \( i \), \( S \in \text{GL}_k(\mathbb{F}_{q^m}) \), and \( \sigma \in \text{GL}_{n+i}(\mathbb{F}_q) \). Without loss of generality we again assume that \( G \) is in Moore matrix form.

5.1 Smart approach variant

Recall from Sect. 2.3 that we can put the extended matrix into the form

\[ G_{\text{ext}} = \tilde{S} \begin{pmatrix} X^* & G^* \\ X^{**} & 0 \end{pmatrix} \sigma. \]

Rashwan et al. [19] proposed what they call the Smart Approach (SA). In this setting, they note that if \( X \in \mathbb{F}_{q^m}^{k \times i} \) is constructed from a Moore matrix of column rank \( a \) and a non-Moore component of column rank \( i - a \), then \( X^{**} \) will have rank \( i - a \). The paper gives no suggestions for design parameters of such a system. However, one implicit advantage of this construction is the ability to predict the rank of \( X^{**} \), and therefore to be able to reduce the public key by choosing a smaller designed error matrix.

In the SA variant we can write \( X = X_{\text{Moore}} + Z \) as a minimal column rank Moore decomposition, where \( X_{\text{Moore}} \) has column rank \( a \) and \( Z \) has column rank \( \hat{i} - a \). We can then rewrite

\[ \hat{G}_{\text{pub}} = S[X_{\text{Moore}} \mid G] \sigma + S[Z \mid 0] \sigma. \]

(12)

\( X' \) is a matrix of column rank \( \hat{i} - a \) and \( S^{-1} M \) is a Moore matrix generating a code with minimum rank distance at least \( n - k + 1 \).

**Theorem 5.1** Consider a GGPT cryptosystem as defined above. Suppose an adversary can find a matrix \( U' \in \mathbb{F}_q^{(i-a) \times (i+a)} \), such that \( \langle U' \rangle = \text{suppGr}(Z) = \text{suppGr}(X') \). Then an encrypted message from a public key of the form (5) can be recovered in polynomial time.

**Proof** We note that \( U' \) must be of the form \( U' = [U \mid 0] \sigma \), where \( U \in \mathbb{F}_q^{(i-a) \times i} \) is such that \( \text{suppGr}(Z) = \langle U \rangle \). Let \( H_U \in \mathbb{F}_q^{a \times i} \) be a parity check matrix for \( U \). A parity check matrix \( H_{U'} \in \mathbb{F}_q^{(a+a) \times (i+n)} \) for \( U' \) must be of the form

\[ (H_{U'})^T = \sigma^{-1} \begin{bmatrix} H^T_U \\ 0_{n \times a} \\ I_n \end{bmatrix} A, \]

for some \( A \in \text{GL}_{n+a}(\mathbb{F}_q) \).

We compute

\[ \hat{G}_{\text{pub}}(H_{U'})^T = S[X_{\text{Moore}} \mid G] \sigma (H_{U'})^T + S[Z \mid 0] \sigma (H_{U'})^T \]

\[ = S[X_{\text{Moore}} \mid G] \begin{bmatrix} H^T_U \\ 0_{n \times a} \\ I_n \end{bmatrix} A \]

\[ = S[X_{\text{Moore}} H^T_U \mid G] A. \]
\[ [X_{\text{Moore}} H_U^T | G] A \] is again a Moore matrix, generating a code of minimum distance at least \( n - k + 1 \). Hence, we can find \( n \) independent columns of \( \hat{G}_{\text{pub}}(H_U')^T \) which will form a Gabidulin code of minimum distance \( n - k + 1 \). Denote these columns by \( i = (i_1, \ldots, i_n) \) and the corresponding submatrix by \( G_i \). From Sect. 2.1, we can recover a decoding algorithm for \( \langle G_i \rangle \) with respect to \( G_i \).

We note that if \( e \) is an error of rank at most \( t' \), and we denote by \( e' \) the subvector of \( e(H_U')^T \) corresponding to columns \( i \), then

\[ \text{rk}(e') \leq \text{rk}(e(H_U')^T) \leq \text{rk}(e) \leq t'. \]

If we apply \( H_U' \) to an encrypted message of the form \( m \hat{G}_{\text{pub}} + e \), we obtain

\[ m \hat{G}_{\text{pub}}(H_U')^T + e(H_U')^T. \]

Restricting to the coordinates \( i \), we obtain

\[ m G_i + e', \]

which we can decode in the code \( \langle G_i \rangle \) to recover \( m \), since the error correction capability of \( \langle G_i \rangle \) is \( t' \geq \text{rk}(e') \).

**Corollary 5.2** Consider a GGPT cryptosystem as defined above. If

\[ \hat{t} - a < \frac{n - k - 1}{2} \]

we can recover an encrypted message in polynomial time.\(^2\)

**Proof** Recall that

\[ \hat{G}_{\text{pub}} = S[X_{\text{Moore}} | G] \sigma + S[Z | 0] \sigma \]

is a minimum column rank Moore decomposition. Then \( S^{-1} \hat{G}_{\text{pub}} = S^{-1} M + S^{-1} X' \) is also a minimal column rank Moore decomposition. \( S^{-1} M \) is a Moore matrix generating a code of minimum rank distance at least \( n - k + 1 \). Since, by the condition of this corollary,

\[ n - k + 1 \geq 2(\hat{t} - a) + 2, \]

it follows from Corollary 3.12 that all elements of rank one in

\[ \sum_{i=0}^{\hat{t}-a} (\hat{G}_{\text{pub}})^{(i)} = \sum_{i=0}^{\hat{t}-a} (S^{-1} \hat{G}_{\text{pub}})^{(i)} = \sum_{i=0}^{\hat{t}-a} (S^{-1} M + S^{-1} X')^{(i)} \]

span the space \( \text{supp}_{Gr}(X') = \text{supp}_{Gr}([Z | 0] \sigma) \). We can use Lemma 3.13 to find these elements of rank one, and obtain \( U' \in \mathbb{F}_q^{(\hat{t}-a) \times (\hat{t}+n)} \) such that \( \langle U' \rangle = \text{supp}_{Gr}(X') \). Then we can use Theorem 5.1 to recover the message. \(\)\(\)\(\)

The following example illustrates a case when Overbeck’s attack fails, but our attack recovers the encrypted message.

\(^2\) The attack needs \( O(k^2 n m^2 (t^2 + k)) \) operations over \( \mathbb{F}_q \), plus the operations needed for the Gabidulin code decoding algorithm.
Example 5.3 Let \( q = 2, n = 8, k = 3, \hat{i} = 3, a = 1 \) and \( g_1, \ldots, g_8 \in \mathbb{F}_{2^8} \) linearly independent over \( \mathbb{F}_2 \). Consider the generator matrix of a Gabidulin code

\[
G = \begin{pmatrix}
g_1 & g_2 & \cdots & g_8 \\
g_1^{(1)} & g_2^{(1)} & \cdots & g_8^{(1)} \\
g_1^{(2)} & g_2^{(2)} & \cdots & g_8^{(2)} \\
g_1^{(3)} & g_2^{(3)} & \cdots & g_8^{(3)}
\end{pmatrix},
\]

and, for some \( x \in \mathbb{F}_{2^8} \setminus \mathbb{F}_2 \), the matrices

\[
X_{\text{Moore}} = \begin{pmatrix}
x \\
x^{(1)} \\
x^{(2)} \\
x^{(3)}
\end{pmatrix}, \quad Z = \begin{pmatrix}
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0
\end{pmatrix}.
\]

Let

\[
X = X_{\text{Moore}} + Z
\]

and the public key generator matrix be

\[
\hat{G}_{\text{pub}} = [X \mid G] = \begin{pmatrix}
x & 1 & 1 & g_1 & g_2 & \cdots & g_8 \\
x^{(1)} & 1 & 0 & 1 & g_1^{(1)} & g_2^{(1)} & \cdots & g_8^{(1)} \\
x^{(2)} & 1 & 1 & 0 & g_1^{(2)} & g_2^{(2)} & \cdots & g_8^{(2)} \\
x^{(3)} & 1 & 0 & 1 & g_1^{(3)} & g_2^{(3)} & \cdots & g_8^{(3)}
\end{pmatrix}.
\]

For simplicity we let \( S = I_3 \) and \( \sigma = I_{11} \). We choose \( u = 1 \) and construct \( G_{\text{ext}} \), which can be put in the form

\[
G'_{\text{ext}} = \begin{pmatrix}
x & 0 & 0 & g_1 & g_2 & \cdots & g_8 \\
x^{(1)} & 0 & 0 & g_1^{(1)} & g_2^{(1)} & \cdots & g_8^{(1)} \\
x^{(2)} & 0 & 0 & g_1^{(2)} & g_2^{(2)} & \cdots & g_8^{(2)} \\
x^{(3)} & 0 & 0 & g_1^{(3)} & g_2^{(3)} & \cdots & g_8^{(3)}
\end{pmatrix} = \begin{pmatrix}
X^* \\
X^{**} \\
0
\end{pmatrix}
\]

by a suitable row transformation. Here Overbeck’s attack fails, because \( X^{**} \) does not have full rank. On the other hand, our attack succeeds, since we can directly recover the elements of rank one as \( \langle [X^{**} \mid 0] \rangle = \langle [Z \mid 0] \rangle \). Thus we can use Theorem 5.1 and recover any encrypted message.

5.2 Loidreau’s GGPT variant

As already mentioned in Sect. 2.3, in Loidreau’s GGPT variant [14] the designed error matrix, \( X \in \mathbb{F}_{q^m}^{\hat{i} \times n} \), is a randomly chosen matrix of rank \( a < \hat{i}/(n-k) \). We can assume that \( X \) has column rank \( \hat{i} \). In this case, to find the Grassmann support of \( X \) with the help of Theorem 3.7, we need to go up to the \( (\hat{i} - 1) \)-st Frobenius power. But, since

\[
\hat{i} - 1 > a(n-k) - 1 \geq n-k-1,
\]

we get that

\[
\sum_{i=0}^{i-1} G^{(i)} = \sum_{i=0}^{n-k-1} G^{(i)} = \mathbb{F}_q^m,
\]

hence the elements of rank one cannot help us reconstruct the Grassmann support of \( X \). Thus the attack of Sect. 5.1 would not succeed.
However, in this case, we can still use the idea of locating the elements of rank one; but now we want to recover the elements of the Gabidulin part of the code, instead of the Grassmann support of $X$. The strategy is effectively the same, although we must make some assumptions on the behavior of $X$ and random subcodes of Gabidulin codes.

First, we note that there is a suitable row transformation, $T$, so that

$$T\hat{G}_{\text{pub}} = \begin{pmatrix} X^* & G^* \\ 0 & G^{**} \end{pmatrix} \sigma, \quad (13)$$

where $X^* \in \mathbb{F}_q^{a \times i}$ is a matrix with the same row span as $X$, and $G^*$ and $G^{**}$ are matrices which span subcodes of $(G)$. One can easily see that $\langle [X^* \mid G^*] \sigma \rangle$ and $\langle [0 \mid G^{**}] \sigma \rangle$ intersect trivially. Our strategy will be to use the purely Gabidulin part $[0 \mid G^{**}]$ to generate a parity check matrix for $[X^* \mid 0]$.

We will now state the assumptions that we will use in our attack. The reason for making these assumptions is that we do not have good knowledge of the behavior of subcodes of Gabidulin codes. Nevertheless, in experiments, we found that our assumptions appear to be justified. All parameter sets tested have similar probabilities as the example parameters presented in Table 1.

**Assumption 1** Let $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix of a Gabidulin code, and $B \subset \langle G \rangle$ be a random subspace of $\langle G \rangle$ of codimension $a$. Set

$$\ell = \left\lceil \frac{n}{k-a} \right\rceil. \quad (14)$$

With high probability, we have

$$\sum_{i=0}^{\ell-1} B^{(i(k-a))} = \mathbb{F}_q^n. \quad (15)$$

The value of $\ell$ in (14) is the smallest possible value for which we can obtain equality in (15). One could choose $\ell$ larger than in (14), which we will remark on in the end of this section.

Since we can expect a random matrix whose rank is small relative to the dimension of the ambient space to not contain elements of rank one, we make the additional assumption:

**Assumption 2** Let $X \in \mathbb{F}_q^{k \times i}$ be a random matrix of rank $a$. For $\ell$ given in (14), if $\ell a \ll \hat{i}$, then with high probability,

$$\sum_{i=0}^{\ell-1} \langle X \rangle^{(i(k-a))}$$

contains no elements of rank one.

### Table 1

| $m$ | $n$ | $k$ | $a$ | $\hat{i}$ | Assumption 1 | Assumption 2 |
|-----|-----|-----|-----|---------|---------------|---------------|
| 24  | 24  | 12  | 3   | 40      | $\sim 1$     | $\sim 1$     |
| 24  | 24  | 12  | 4   | 52      | $\sim .998$  | $\sim 1$     |
Theorem 5.4 Let $S \in \text{GL}_k(\mathbb{F}_{qm})$, $\sigma \in \text{GL}_{t+n}(\mathbb{F}_q)$, $G \in \mathbb{F}_{qm}^{k \times n}$, and $X \in \mathbb{F}_{qm}^{k \times i}$ be of rank $a$, and consider Loidreau’s GGPT variant with public key

$$\hat{G}_{\text{pub}} = S[X \mid G] \sigma.$$ 

If Assumptions 1 and 2 are true, then we can break the Loidreau GGPT variant in polynomial time with high probability.

Proof Let $\ell$ be as in (14) and $T \hat{G}_{\text{pub}}$ as in (13). Consider the matrix

$$G''_{\text{ext}} := \left( \begin{array}{c} \hat{G}_{\text{pub}} \\ \hat{G}_{\text{pub}}^{((k-a)-1)} \\ \vdots \\ \hat{G}_{\text{pub}}^{((k-a)(\ell-1))} \end{array} \right) = \hat{S} \left( \begin{array}{c} (X^* \mid G^*) \\ (X^* \mid G^*)^{((k-a)-1)} \\ \vdots \\ (X^* \mid G^*)^{((k-a)(\ell-1))} \\ (0 \mid G^{**}) \\ (0 \mid G^{**})^{((k-a)-1)} \\ \vdots \\ (0 \mid G^{**})^{((k-a)(\ell-1))} \end{array} \right) \sigma.$$

Since $(G^{**})$ is a subcode of $(G)$ of codimension $a$, by Assumption 1, we have with high probability,

$$\sum_{i=0}^{\ell-1} \langle G^{**} \rangle^{((k-a)i)} = \mathbb{F}_{qm}^{n}.$$

Then, the bottom submatrix of $\tilde{G}$ has the same row span as $[0 \mid I_n]$, and hence, by using elementary operations, we can eliminate the second component of every row in the top submatrix of $\tilde{G}$. Then, the space generated by the rows of $G''_{\text{ext}}$ is the same as that generated by

$$G'''_{\text{ext}} = \left( \begin{array}{c} X^* \\ (X^*)^{((k-a)-1)} \\ \vdots \\ (X^*)^{((k-a)(\ell-1))} \\ 0 \end{array} \right) \sigma.$$

By Assumption 2, with high probability we have that

$$\sum_{i=0}^{\ell-1} \langle X^* \rangle^{((k-a)i)}$$

contains no elements of rank one, and therefore all elements of rank one in $\langle G''_{\text{ext}} \rangle = \langle G'''_{\text{ext}} \rangle$ must belong to $\langle [0 \mid I_n] \rangle \sigma$. With the help of Lemma 3.13 we can recover a matrix $U \in \mathbb{F}_q^{2 \times (t+n)}$ which is a basis for $\langle [0 \mid I_n] \rangle \sigma$. Then, any parity check matrix $H_U \in \mathbb{F}_q^{\hat{t} \times (\hat{t}+n)}$ for $\langle [0 \mid I_n] \rangle \sigma$ must have the form

$$H_U^T = \sigma^{-1} \begin{bmatrix} A \\ 0 \end{bmatrix} \in \mathbb{F}_q^{(\hat{t}+n) \times \hat{t}},$$
where $A \in \text{GL}_{\hat{t}}(\mathbb{F}_q)$. It follows that, if we compute

$$\hat{G}_{\text{pub}}H_U^T = S[X | G]\sigma H_U^T = SXA \in \mathbb{F}_{q^m}^{k \times \hat{t}},$$

then there exists a unique matrix $V = [A^{-1} | 0] \sigma \in \mathbb{F}_q^{\hat{t} \times (\hat{t} + n)}$ such that

$$\hat{G}_{\text{pub}}H_U^T V = SXAV = S[X | 0] \sigma.$$

We can find the matrix $V$ by observing that

$$(\hat{G}_{\text{pub}} - \hat{G}_{\text{pub}}H_U^TV)H_U^T = S[0 | G] \sigma H_U^T = 0. \quad (16)$$

This gives a linear system of equations with $\hat{t}(\hat{t} + n)$ variables and $k\hat{t}$ equations over $\mathbb{F}_q^m$. Since the variables can only take values in $\mathbb{F}_q$, we can expand each equation into $m$ equations over $\mathbb{F}_q$, obtaining a system of $km\hat{t}$ equations and $\hat{t}(\hat{t} + n)$ variables over $\mathbb{F}_q$. Hence, we can solve this system of equations if $km \geq \hat{t} + n$ (which is always satisfied).

Let $H_V \in \mathbb{F}_q^{n \times (\hat{t} + n)}$ be any dual matrix for $V$. Then, $H_V$ has the form

$$H_V^T = \sigma^{-1} \begin{bmatrix} 0 \\ B \end{bmatrix},$$

for some $B \in \text{GL}_n(\mathbb{F}_q)$. Therefore,

$$\hat{G}_{\text{pub}}H_V^T = S[X | G] \sigma H_V^T = SGB \in \mathbb{F}_q^{k \times n}$$

is a Gabidulin code of minimum distance $n - k + 1$, from which we can recover a decoding algorithm, as explained in Sect. 2.1. If we receive an encrypted message of the form $m\hat{G}_{\text{pub}} + e$, we can apply $H_V$, obtaining

$$mSGB + eH_V^T.$$ 

Since

$$\text{rk}(eH_V^T) \leq \text{wt}_{\text{R}}(e) \leq \ell',$$

we can recover the encrypted message, $m$, from the recovered decoding algorithm with respect to $SGB$. All the operations required for this attack can be performed in polynomial time.

We will conclude this section with an example where we analyze our attack against the parameters proposed by Loidreau [14] in order to resist Overbeck’s attack. It turns out that the proposed parameters are not secure against our attack.

**Example 5.5** Consider a Loidreau GGPT variant with $q = 2$, $m = n = 24$, $k = 12$, $a = 3$, and $\hat{t} = 40$, i.e. the first set of parameters from Table 1. Assume we, as an attacker, know the public generator matrix $\hat{G}_{\text{pub}} \in \mathbb{F}_{2^{24}}^{12 \times 64}$ and received an encrypted message $y$. We compute

$$(\hat{G}_{\text{pub}}(123)) = 3$$

and proceed as follows:

1. We compute $\hat{G}_{\text{pub}}(19), \hat{G}_{\text{pub}}(18)$ to obtain the extended matrix $G_{\text{ext}}^{\prime \prime} \in \mathbb{F}_{2^{24}}^{36 \times 64}$. This requires at most $1536 = 2 \cdot 12 \cdot 64$ Frobenius powers in $\mathbb{F}_{2^{24}}$. Using a normal basis to represent $\mathbb{F}_{2^{24}}$ over $\mathbb{F}_2$, this can be done very efficiently.
2. We find the elements of rank one in \( \langle G''_{\text{ext}} \rangle \), as described in Lemma 3.13. To do so we need to row reduce \( G''_{\text{ext}} \) and then solve a linear system over \( \mathbb{F}_2 \) with 36 unknowns and \( 24 \cdot 64 = 1536 \) equations. Then, if Assumptions 1 and 2 hold, we find some basis matrix \( U \in \mathbb{F}_2^{24 \times 64} \), such that \( \langle U \rangle \) contains all these elements of rank one.

3. We compute a parity check matrix \( H_U \) for \( U \).

4. We find a matrix \( V \in \mathbb{F}_2^{40 \times 64} \), solving Eq. (16).

5. We compute a parity check matrix \( H_V \in \mathbb{F}_2^{64 \times 24} \) for \( V \), and compute the product \( \hat{G}_{\text{pub}} H_T^T \).

6. We recover a decoding algorithm for the code \( \langle \hat{G}_{\text{pub}} H_T^T \rangle \), as described in Lemma 3.13, and decode \( y H_T^T \) with this algorithm.

We observe that Step 4 above is the most computationally intensive, and therefore we estimate the complexity of our attack based on this step. This is done by solving a \((40 \cdot 64) \times (24 \cdot 12 \cdot 40)\) system over \( \mathbb{F}_2 \) by Gaussian elimination on the resulting matrix. This requires on the order of \( 2^{39} \) operations over \( \mathbb{F}_2 \). Implementing the algorithm on a personal computer, we were able to break this system very efficiently.

For the parameters in the second row of the table, we can similarly break the system, albeit with slightly higher complexity due the larger parameters.

6 Conclusion

In this paper, we provide a new attack against cryptosystems based on Gabidulin codes, reconfirming that Gabidulin based cryptosystems are vulnerable from a structural perspective. Our attack generalizes Overbeck’s attack, focusing instead on recovering the elements of rank one, rather than the structure of the dual space. One principle advantage of our attack is that it can be extended to cryptanalyze certain variants of the generalized GPT system, which resist the original attacks of Gibson and Overbeck. In particular, we show that the Smart Approach and Loidreau’s GGPT variants are vulnerable to this attack.

To the best of the authors’ knowledge, attacking a cryptosystem by looking at the elements of rank one is a new approach which may need to be considered for the security of existing and future rank-metric based cryptosystems. As a next step the authors want to use this idea of finding elements of rank one to cryptanalyze the column scrambler variant of [6], which has so far resisted structural attacks. First results in this direction can be found in [12].

Acknowledgements This work was supported by SNF Grant No. 149716.

References

1. Berger T.P.: Isometries for rank distance and permutation group of Gabidulin codes. IEEE Trans. Inf. Theory 49(11), 3016–3019 (2003).
2. Chabaud F., Stern J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Advances in Cryptology—ASIACRYPT ’96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3–7, 1996, Proceedings, pp. 368–381 (1996).
3. Gabidulin E.M.: Theory of codes with maximum rank distance. Probl. Pereda. Inform. 21(1), 3–16 (1985).
4. Gabidulin E.M.: Attacks and counter-attacks on the GPT public key cryptosystem. Des. Codes Cryptogr. 48(2), 171–177 (2008).
5. Gabidulin E.M., Paramonov A.V., Tretjakov O.V.: Ideals over a non-commutative ring and their application in cryptography. In: Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT’91, pp. 482–489. Springer, Berlin (1991).
6. Gabidulin E.M., Rashwan H., Honary B.: On improving security of GPT cryptosystems. In: IEEE International Symposium on Information Theory, 2009 (ISIT 2009), pp. 1110–1114 (2009).
7. Gaborit P., Ruatta O., Schrek J., Zémor G.: New results for rank-based cryptography. In: Progress in Cryptology—AFRICACRYPT 2014—7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28–30, 2014, Proceedings, pp. 1–12 (2014).
8. Gaborit P., Ruatta O., Schrek J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inf. Theory 62(2), 1006–1019 (2016).
9. Gibson J.K.: Severely denting the Gabidulin version of the McEliece public key cryptosystem. Des. Codes Cryptogr. 6(1), 37–45 (1995).
10. Giorgetti M., Previtali A.: Galois invariance, trace codes and subfield subcodes. Finite Fields Their Appl. 16(2), 96–99 (2010).
11. Horlemann-Trautmann A.-L., Marshall K.: New criteria for MRD and Gabidulin codes and some rank-metric code constructions. arXiv:1507.08641 (2015).
12. Horlemann-Trautmann A.-L., Marshall K., Rosenthal J.: Considerations for rank-based cryptosystems. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT 2016), Barcelona, pp. 2544–2548 (2016).
13. Kshevetskiy A.: Security of GPT-like public-key cryptosystems based on linear rank codes. In: 3rd International Workshop on Signal Design and Its Applications in Communications, 2007 (IWSDA 2007), pp. 143–147 (2007).
14. Loidreau P.: Designing a rank metric based McEliece cryptosystem. In: Proceedings of the Third International Conference on Post-Quantum Cryptography (PQCrypto’10), pp. 142–152. Springer, Berlin (2010).
15. McEliece R.J.: A public-key cryptosystem based on algebraic coding theory. Deep Space Netw. Progr. Rep. 44, 114–116 (1978).
16. Morrison K.: Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. IEEE Trans. Inf. Theory 60(11), 1–12 (2014).
17. 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).
18. Overbeck R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptol. 21(2), 280–301 (2008).
19. Rashwan H., Gabidulin E.M., Honary B.: A smart approach for GPT cryptosystem based on rank codes. In: IEEE International Symposium on Information Theory, ISIT 2010, June 13–18, 2010, Austin, Texas, USA, Proceedings, pp. 2463–2467 (2010).
20. Sidelnikov V.M., Shestakov S.O.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl. 2, 439–444 (1992).
21. Silva D., Kschischang F.R.: Fast encoding and decoding of Gabidulin codes. In: IEEE International Symposium on Information Theory, 2009 (ISIT 2009), pp. 2858–2862 (2009).
22. Wachter-Zeh A.: Bounds on list decoding of rank-metric codes. IEEE Trans. Inf. Theory 59(11), 7268–7277 (2013).
23. Wachter-Zeh A., Afanassiev V., Sidorenko V.: Fast decoding of Gabidulin codes. Des. Codes Cryptogr. 66(1), 57–73 (2013).
24. Wan Z.-X.: Geometry of matrices. World Scientific, Singapore (1996). In memory of Professor L.K. Hua (1910–1985).