J. Cryptol. (2008) 21: 280–301
DOI: 10.1007/s00145-007-9003-9

Journal of
CRYPTOLOGY

Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes

R. Overbeck

Technishe Universität Darmstadt, Department of Computer Science, Cryptography and Computer Algebra Group, 64289 Darmstadt, Germany
overbeck@cdc.informatik.tu-darmstadt.de

Communicated by Lars R. Knudsen

Received 17 October 2005 and revised 9 February 2007
Online publication 5 September 2007

Abstract. In this paper we look at the Gabidulin version of the McEliece cryptosystem (GPT) and its variants. We give an overview over the existing structural attacks on the basic scheme, and show how to combine them to get an effective attack for every GPT variant. As a consequence, there are no secure parameter sets left for GPT variants, which one would like to use in practice.

Key words. Public key cryptography, Code based cryptography, Rank distance codes, Gabidulin codes

1. Introduction

The security of cryptosystems based on error correcting codes is connected to the hardness of the general decoding problem. The first cryptosystem, which is based on that technique is the one presented by McEliece in 1978 [14]. McEliece's cryptosystem is very fast in en- and decryption, has a reasonable information rate (1/2) and we can even build a signature scheme from it [3]. Furthermore, despite all efforts, for large public key sizes it remains secure—even against quantum computers.

To overcome the drawback of the public key size, several variants were proposed, but most of them showed to be insecure. This paper is a contribution to the cryptanalysis of such variants. We view the variants based on the 1991 proposal from Gabidulin, Paramonov and Tretjakov (GPT, [8]) to use *rank distance* codes instead of Hamming distance codes. The use of smaller public-key sizes seemed to be possible for these variants, as general decoding algorithms have higher complexity for the rank metric than for the Hamming-metric [12].

Gibson was the first to develop (exponential) structural attacks for the GPT variant of McEliece's cryptosystem, which worked well for the parameter sets originally proposed [10,11]. In order to avoid these attacks without enlarging the public key size, several modifications of the GPT scheme were proposed (see e.g. [15,18]).

Most of the GPT variants were shown to be strongly connected to the basic GPT scheme [18]. However, GPT and its variants remained secure until 2005, when a polynomial time attack on GPT was proposed [17]. It recovers a secret key for a given public key, and is claimed to be applicable to many parameter sets of all variants of GPT, too. We show, that the methods from [17] and [18] may be combined to attack the reducible rank codes variant of GPT, which was not cryptanalyzed in [17].

In the fist sections we give a short introduction of the concept of rank distance codes, basic notations and the proposed GPT variants. Then we give an overview of the existing attacks on GPT and variants. Finally, we extend the attack from [17] to a powerful attack on GPT with reducible rank codes and demonstrate, that it is not possible to avoid the attack by using subfield subcodes of Gabidulin codes.

2. Rank Distance Codes

Rank distance codes were presented by Gabidulin in 1985. They are linear codes over the finite field $\mathbb{F}_{q^m}$ for q (power of a) prime and $m \in \mathbb{N}$. As their name suggests they use a special concept of distance.

Definition 2.1. Let $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $b_1, \ldots, b_m$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We can write $x_i = \sum_{j=1}^m x_{ij} b_j$ for each $i = 1, \ldots, n$ with $x_{ij} \in \mathbb{F}_q$. The *rank norm* $\|\cdot\|_r$ is defined as follows:

$$\|x\|_r := \operatorname{rank}((x_{ij})_{1 \le i \le n, 1 \le j \le m}).$$

The rank norm of a vector $x \in \mathbb{F}_{q^m}^n$ is uniquely determined (independent of the choice of basis) and induces a metric, called *rank distance*. Further, if $T \in \mathbb{F}_q^{n \times n}$ is an invertible matrix, then $\|x \cdot T\|_r = \|x\|_r$.

Definition 2.2. We recall the basic notations of coding theory:

- An $[n, k]$-code $\mathcal{G}$ over a finite field $\mathbb{F}$ is a k-dimensional subvectorspace of the vector space $\mathbb{F}^n$.
- We call the code $\mathcal{G}$ an $[n, k, d]$ rank distance code if $d = \min_{x,y \in \mathcal{G}} \|x - y\|_r$.
- The matrix $G \in \mathbb{F}^{k \times n}$ is a generator matrix for the $[n, k]$ code $\mathcal{G}$ over $\mathbb{F}$, if the rows of G span $\mathcal{G}$ over $\mathbb{F}$.
- The matrix $H \in \mathbb{F}^{n \times (n-k)}$ is called check matrix for the code $\mathcal{G}$ if it is the right kernel of G.
- The code generated by $H^\top$ is called dual code of $\mathcal{G}$ and denoted by $\mathcal{G}^\perp$.

In [12] Ourivski and Johansson presented an algorithm which solves the general decoding problem in $\mathcal{O}((m\frac{d-1}{2})^3 q^{(d-3)(k+1)/2})$ operations over $\mathbb{F}_q$ for $[n, k, d]$ rank distance codes over $\mathbb{F}_{q^m}$. A special class of rank distance codes are the *Gabidulin codes* for which an efficient decoding algorithm exists [5]. We will define these codes by their generator matrix.

Definition 2.3. Let $g \in \mathbb{F}_{q^m}^n$ be a vector s.t. the components g_i, $i = 1, \ldots, n$ are linearly independent over $\mathbb{F}_q$. This implies that $n \leq m$. The $[n, k, d]$ Gabidulin code $\mathcal{G}$ is the rank distance code with generator matrix

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times n}. \tag{1}$$

An $[n, k]$ Gabidulin code $\mathcal{G}$ corrects errors up to rank $\lfloor \frac{n-k}{2} \rfloor$ and has minimum distance $d = n - k + 1$. The vector g is said to be a *generator vector* of the Gabidulin code $\mathcal{G}$ (It is not unique, as all vectors ag with $0 \neq a \in \mathbb{F}_{q^m}$ are generator vectors of $\mathcal{G}$). An error correction algorithm based on the "right Euclidian division algorithm" runs in $\mathcal{O}(d^3 + dn)$ operations over $\mathbb{F}_{q^m}$ for $[n, k, d]$ Gabidulin codes [5]. The dual code of an $[n, k]$ Gabidulin code is a $[n, n-k]$ Gabidulin code (see [5]). Further, if $T \in \mathbb{F}_q^{n \times n}$ is an invertible matrix, then $G \cdot T$ is the generator matrix of the Gabidulin code with generator vector gT.

For the further notation used throughout this paper see Appendix A. With these notations, let $h^{[q^{n-k-1}]}$ be the generator vector of this dual code, then we will call h the *check vector* of $\mathcal{G}$. Further, let J be a selection of $\bar{n} > k$ columns of the generator matrix G, then $G_{\cdot J}$ defines an $[\bar{n}, k]$ Gabidulin code.

3. The GPT Cryptosystem

The GPT cryptosystem was first presented in 1991 by Gabidulin, Paramonov and Tretjakov [8]. We present a more general version (GGPT, see [18]) first, which may be used to describe the original GPT cryptosystem as well as the variant with column scrambler (CS-GPT) from [7].

- *System Parameters*: $q, k < n \leq m, t < n - k - 1$ and $s \leq \min\{t, k\} \in \mathbb{N}$.
- *Key Generation*: First generate the following matrices:

$G \in \mathbb{F}_{q^m}^{k \times n}$	generator matrix of an $[n, k, d]$ Gabidulin code,
$X \in \mathbb{F}_{q^m}^{k \times t}$	random matrix of rank s over $\mathbb{F}_{q^m}$ and rank t over $\mathbb{F}_q$,
$S \in \mathbb{F}_{q^m}^{k \times k}$	random, non-singular matrix (the row scrambler) and
$T \in \mathbb{F}_q^{n \times n}$	random, non-singular matrix (the column scrambler).

Then compute the $k \times n$ matrix

$$G^{\text{pub}} = S([X|0] + G)T = S[G_{\cdot\{1,\ldots,t\}} + X|G_{\cdot\{t+1,\ldots,n\}}]T \in \mathbb{F}_{q^m}^{k \times n}, \tag{2}$$

where 0 denotes the $k \times (n - t)$ zero matrix. Choose $1 \leq r \leq \frac{n-k-t}{2}$. Further let $\mathcal{D}_{\mathcal{G}}$ be an efficient error correction algorithm for the Gabidulin code $\mathcal{G}$ generated by the matrix $G_{\cdot\{t+1,\ldots,n\}}$.

Table 1. Previously proposed parameters for GPT/GGPT.

Parameters				Size public key in bytes	WF general decoding
m	k	t	s		
48	10	16	3	2,880	2^{134}
48	16	18	4	1,608	2^{124}
48	24	8	2	6,912	2^{198}

- *Public Key*: (G^{pub}, r).
- *Private Key*: $(\mathcal{D}_{\mathcal{G}}, S, T)$ or (G, S, T) where G is of the form in (1).
- *Encryption*: To encode a plaintext $x \in \mathbb{F}_{q^m}^k$ choose a vector $z \in \mathbb{F}_{q^m}^n$ of rank norm r at random and compute the ciphertext c as follows:

$$y = xG^{\text{pub}} + z.$$

- *Decryption*: To decode a ciphertext y apply the decoding algorithm $\mathcal{D}_{\mathcal{G}}$ for $\mathcal{G}$ to $y' = (cT^{-1})_{\{t+1,\ldots,n\}}$. As T is an invertible matrix over $\mathbb{F}_q$, the rank norm of a vector does not change if it is multiplied with the isometry of the rank metric T^{-1}. Thus y' has at most rank distance $\frac{n-k-t}{2}$ to $\mathcal{G}$ and we obtain the codeword

$$xSG_{\{t+1,\ldots,n\}} = \mathcal{D}_{\mathcal{G}}(y').$$

  Now, we can compute the plaintext x.

The distortion matrix X is essential to mask the structure of G. We can recover the vector gT from SGT in $\mathcal{O}(k^3)$ operations over $\mathbb{F}_{q^m}$ by employing methods similar to the attack of Sidelnikov and Shestakov on the Niederreiter cryptosystem using GRS codes (see [5]). Some parameter sets may be found in Table 1, where $n = m$ and $q = 2$ (WF = operations over $\mathbb{F}_q$) .

3.1. *Simple Variants of GPT*

The original approach of the GPT cryptosystem, was to choose the parameters r and t such that $r = \frac{n-k}{2} - t$. If one does so, the legitimate user may recover $xSGT$ by applying the error correction algorithm for $\langle GT \rangle$ (which is a Gabidulin code, too) to the ciphertext y. An alternative description of the public generator matrix would be $G^{\text{pub}} = S(\bar{G} + \bar{X})$, where $\bar{G} = GT$ and $\bar{X} = [X|0]T$. However, this early version is broken, as we will show in the following.

Another variant is the CS-GPT: G and X are chosen s.t. all entries of S the public key are in a subfield $\mathbb{F}_{\text{SUB}}$ of $\mathbb{F}_{q^m}$. In this case, the plaintext and random errors z are chosen from $\mathbb{F}_{\text{SUB}}$ as well. This saves space when storing the public key. The most common instances of CS-GPT are the ones, where the public generator matrix may be written as

$$G^{\text{pub}} = \bar{S}[Y|\bar{G}] \cdot \bar{T} \in \mathbb{F}_{q^m}^{k \times n},$$

where $Y \in \mathbb{F}_{\text{SUB}}^{k \times t}$ is arbitrary, $\bar{G} \in \mathbb{F}_{\text{SUB}}^{k \times (n-t)}$ defines an $[n-t, k]$ Gabidulin code and $\bar{T} \in \mathbb{F}_q^{n \times n}$ as well as $\bar{S} \in \mathbb{F}_{\text{SUB}}^{k \times k}$ are invertible.

3.2. *The Niederreiter Variant of GPT*

We briefly introduce the Niederreiter variant of the GPT cryptosystem from [1]. On key generation we choose a $k-l$ dimensional subcode of an $[n,k]$ Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^m}$. Every check matrix of the subcode may be described as

$$(H^{\text{pub}}) = [H|A]S \in \mathbb{F}_{q^m}^{n\times(n-k+l)}, \tag{3}$$

where H is the $n\times(n-k)$ check matrix of $\mathcal{G}$, A is an $n\times l$ matrix of full rank and S is some invertible $(n-k+l)\times(n-k+l)$ matrix. The public key $(H^{\text{pub}}, r=(n-k)/2)$ is published, and the pair $(S,\mathcal{G})$ is taken to be the private key. To encode a plaintext $x\in\mathbb{F}_{q^m}^n$ of rank norm less then r, compute the ciphertext y as follows:

$$y = xH^{\text{pub}}.$$

In order to decode a ciphertext y apply the syndrome decoding algorithm $\mathcal{D}_{\mathcal{G}}$ for $\mathcal{G}$ to the syndrome build from the first $n-k$ columns of yS^{-1}.

3.3. *GPT with Reducible Rank Codes*

Most variants of the original GPT cryptosystem were proposed in order to avoid Gibson's attacks from [10,11]. In [9], the authors proposed to substitute the underlying code by a *reducible rank code*:

Definition 3.1. Let $\mathcal{G}_i = \langle G_i\rangle$, $i=1,\ldots,w$ be a family of $[n_i,k_i,d_i]$ codes over $\mathbb{F}_{q^m}$. Then the (linear) code $\mathcal{G}$ given by the generator matrix of the form

$$G = \begin{bmatrix} G_1 & 0 & \cdots & 0 \\ Y_{21} & G_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ Y_{w1} & Y_{w2} & \cdots & G_w \end{bmatrix} \in \mathbb{F}_{q^m}^{\sum k_i\times\sum n_i}$$

for some matrices $Y_{ij}\in\mathbb{F}_{q^m}^{k_i\times n_j}$ is called a reducible code. Further, $\mathcal{G}$ has length $n=\sum_{i=1}^w n_i$, dimension $k=\sum_{i=1}^w k_i$ and minimum distance $d=\min_{1\le i\le w}(d_i)$. Error correction may be done in sections, starting from the right. If all codes $\mathcal{G}_i$ are rank distance codes, we call $\mathcal{G}$ a reducible rank code.

Using reducible rank codes for the McEliece cryptosystem is quite a natural extension (RRC-GPT). In the examples from [9] the authors propose to take two Gabidulin codes G_1 and G_2 over $\mathbb{F}_{q^m}$ (with length n_i and dimension k_i, $i=1,2$) and a random matrix $Y=Y_{21}\in\mathbb{F}_{q^m}^{k_2\times n_1}$ to build a reducible rank code $\mathcal{G}$. As public generator matrix they choose

$$G^{\text{pub}} = S(G+[X_1\ X_2])T, \tag{4}$$

where $S\in\mathbb{F}_{q^m}^{k\times k}$ and $T\in\mathbb{F}_q^{n\times n}$ are non-singular and the rank of $X_i\in\mathbb{F}_{q^m}^{k\times n_i}$ over $\mathbb{F}_q$ is less than t_i for $i=1,2$. Using this construction, the authors of [9] propose that the

random errors added at encryption should have a rank less than $r = \min_{i=1,2}(\frac{n_i - k_i}{2} - t_i)$, where en- and decryption work as with GGPT. The authors of [9] considered every parameter set with $m_i \geq 24$ and $r \geq 4$ to provide sufficient security, even if X_1 and X_2 are zero matrices. Analogous to the construction above, one might choose to build the reducible rank code from $w > 2$ Gabidulin codes and an adapted distortion matrix.

Note, that because of the use of the column scrambler, we may choose X_i s.t. only the first t_i columns contain non-zero entries. All other choices correspond to an equivalent private key with X_i of the desired form and different T and G.

4. Exponential Attacks on GPT

Structural attacks (the ones, trying to recover a private key from the public one) had more impact on the cryptosystem than attacks employing general rank distance decoding algorithms. However, for carefully chosen parameter sets, many structural attacks have exponential running time.

Structural attacks take advantage of the main weakness of GPT in comparison with the McEliece PKC: Unlike Goppa codes, Gabidulin codes are highly structured. Some attacks are based on the following observation: If G is the generator matrix of a Gabidulin code, then G and $G^{[q]}$ look quite the same. (Both define Gabidulin codes with generator vectors g and $g^{[q]}$ respectively.) This property can be used, to distinguish a Gabidulin code from a random one.

4.1. *Gibson's Attacks*

Gibson presented two structural attacks on the GPT cryptosystem. They recover an alternative private-key from the GGPT public-key G^{pub}. On input of $G^{\text{pub}} = S([X|0] + G)T$, Gibson's attacks return $\widehat{G}$, $\widehat{X} \in \mathbb{F}_{q^m}^{k \times n}$ and $\widehat{S} \in \mathbb{F}_{q^m}^{k \times k}$, s.t.

(i) $\widehat{G}$ is a generator matrix of an $[n, k]$ Gabidulin code over $\mathbb{F}_{q^m}$,
(ii) $G^{\text{pub}} = \widehat{S}(\widehat{G} + \widehat{X})$ and
(iii) the rank of $\widehat{X}$ over $\mathbb{F}_q$ is not bigger than t.

Thus Gibson's attacks serve well for an attack on the GGPT cryptosystem, as an alternative column scrambler may be recovered from $\widehat{X}$. Gibson's first attack was developed for the case that the GGPT parameter s is very small. It is a variation of the approach for GPT without distortion matrix ($s = 0$), which recovers a generator vector of a Gabidulin code from its systematic generator matrix by solving some linear equations. If the parameter s is small enough, the attacker can guess some unknown values to eliminate the effect of the distortion matrix. This first attack takes

$$\mathcal{O}(m^3(n-k)^3 q^{ms}) \tag{5}$$

operations over $\mathbb{F}_{q^m}$. In [11] Gibson presented a different attack, which analyzes matrices of the form $G + G^{[q]}$. This attack is more efficient for larger values of s. It runs in

$$\mathcal{O}(k^3 + (k+t)f \cdot q^{f(k+2)} + (m-k)t \cdot q^f) \tag{6}$$

operations over $\mathbb{F}_{q^m}$, where $f \approx \max(0, t-2s, t+1-k)$. Note, that this attack runs in polynomial time if $f = 0$. The success of both attacks is based on some assumptions, which are claimed to be fulfilled with high probability for random instances of the GGPT cryptosystem. Nevertheless Gibson's attacks are not fast enough to attack the GGPT cryptosystem for all parameter sets of practical interest (compare Table 3).

4.2. *Ourivski's Attack on the Niederreiter Variant*

In 2003 A. Ourivski chose an approach similar to the one of the first attack from Gibson. He analyzed the public key and was able to recover the secret key by guessing some values and solving some linear equations afterwards. The number of elements an attacker has to guess using Ourivski's attack is expressed by the parameter f below.

Without loss of generality we may assume, that the matrix A in the public key of the Niederreiter GPT (see (3)) is of the following form:

$$A = \begin{bmatrix} 0 \\ \mathrm{Id}_l \\ \bar{A} \end{bmatrix} \in \mathbb{F}_{q^m}^{n \times l},$$

where $\bar{A} \in \mathbb{F}_{q^m}^{(k-l)\times l}$ and Id_k denotes the k-dimensional identity matrix. Let $v \leq l$ be the column-rank of $\bar{A}$ over $\mathbb{F}_q$ and $a \leq \min\{v, k-l\}$ be the rank of $\bar{A}$ over $\mathbb{F}_{q^m}$. Ourivski's attack takes

$$\mathcal{O}(3m^3 + nf \cdot q^{m(f-1)})$$

operations over $\mathbb{F}_q$, where $f \approx v + 1 - \min\{v, a(n-k)\}$ for most instances. Even if no proof is given, experiments corroborate Ourivski's estimation of f. Because $0 \leq v \leq l$, this attack runs in polynomial time, if $l \leq a(n-k)$. Ourivski states, that the parameter a should not be to small ($\geq$3), as otherwise a different attack approaches can be used to recover a private key. Thus, for the worst case with fixed a, the work factor for Ourivski's attack is

$$\mathcal{O}(3m^3 + nl \cdot q^{m(l-\mathcal{O}(1)(n-k))}).$$

5. Polynomial Time Attacks on GPT

The attack on the private key of GGPT presented in [17] runs in cubic time, but does not succeed for every parameter set. However, it succeeds for all parameter sets proposed previously and thus confirms that GGPT is inherently weak. To cryptanalyze GGPT, we take advantage of the behavior of the public generator matrix under the Frobenius automorphism:

Definition 5.1. Let M be an arbitrary $l \times n$ matrix over $\mathbb{F}_{q^m}$ and $f \in \mathbb{N}$. Then the operator λ_f is defined as

$$\lambda_f : \mathbb{F}_{q^m}^{l \times n} \longrightarrow \mathbb{F}_{q^m}^{(f+1)l \times n}$$
$$\Lambda_f(M) = \begin{bmatrix} M \\ (M)^{[q]} \\ \vdots \\ (M)^{[q^f]} \end{bmatrix}. \tag{7}$$

Depending on the connection between M and a Gabidulin code, the matrix $\Lambda_f(M)$ defines different subspaces of $\mathbb{F}_{q^m}^n$. The general idea is, to analyze $\Lambda_f(G^{\text{pub}})$. By this we can split the Gabidulin part from the random part of G^{pub}.

We first state some basic observations about the behavior of different matrices under the operator $\Lambda_f(M)$. The following lemma observes the behavior of generator matrices of Gabidulin codes:

Lemma 5.1. *If $M \in \mathbb{F}_{q^m}^{k \times n}$ defines an $[n, k]$ Gabidulin code with generator vector g and $f \leq n - k - 1$, then the subvectorspace spanned by the rows of $\Lambda_f(M)$ defines the $[n, k + f]$ Gabidulin code with generator vector g.*

Proof. Let G be a canonical generator matrix for $\mathcal{G}$, then there exists a matrix $S \in \mathbb{F}_{q^m}^{k \times k}$ such that $M = SG$. It follows, that $\langle \Lambda_f(M) \rangle = \langle \Lambda_f(G) \rangle$, and it is obvious, that the vectorspace spanned by the rows of $\Lambda_f(G)$ is an $[n, k + f]$ Gabidulin code. (Only the last row of $\Lambda_f(G)$ is not in $\langle \Lambda_{f-1}(G) \rangle$ and has the form $g^{[q^{k-1+f}]}$.) □

Note that identifying a Gabidulin code by an arbitrary generator matrix G may be done using this lemma: A check vector h of $\langle G \rangle$ is given by $\lambda_{n-k-2}(G)^{\perp}$. Unlike generator matrices of Gabidulin codes, random matrices tend to be mapped to matrices of high rank by λ_f, see [13]:

Lemma 5.2. *Let $M \in \mathbb{F}_{q^m}^{\ell \times n}$ be a random matrix of full column rank over $\mathbb{F}_q$. Then $\Lambda_f(M)$ has rank $\min(n, (f + 1) \cdot \ell)$ with probability $\geq (1 - 4q^{-m})$.*

Observe that if $\ell = 1$, then because of Lemma 5.1 the probability is 1. For the Niederreiter GPT, we can make the following assumption:

Assumption 5.1. Let $M \in \mathbb{F}_{q^m}^{\ell \times n}$ define a random $\ell > 1$ dimensional subcode of an $[n, k]$ Gabidulin code over $\mathbb{F}_{q^m}$ with generator vector g. Then with probability $\geq (1 - q^{-m})$, $\Lambda_f(M)$ defines a $\min\{k + f, (f + 1) \cdot \ell\}$ dimensional subcode of the $[n, k + f]$ Gabidulin code with generator vector g.

It is easy to see, that $\Lambda_f(M)$ defines a subcode of the $[n, k + f]$ Gabidulin code with generator vector g. The remaining part is to estimate the probability. However, it can

not be 1, as the rank of $\Lambda_1(M)$ is 3 for

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} G,$$

where G is the generator matrix of a $(3, n \geq 5)$ Gabidulin code over $\mathbb{F}_{2^n}$. Our estimation of the probability is based on experimental results. Unfortunately we are not able to give theoretical corroborated bounds.

5.1. *Attacking the Niederreiter Variant*

Even if Ourivski's attack on the Niederreiter GPT works well, it still has exponential work factor for special parameter sets. Nevertheless, it is not the only way to recover the secret key for the Niederreiter GPT. We present an attack, which recovers an alternative secret key in polynomial timefor many parameter sets by using Assumption 5.1

Theorem 5.1. *Let $\mathcal{G}_{\mathrm{SUB}}$ be a random $k-\ell$ dimensional subcode of an $[n,k]$ Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^m}$ defined by an instance of the Niederreiter GPT. Then we can recover the generator vector g of $\mathcal{G}$ from $\mathcal{G}_{\mathrm{SUB}}$ with probability $\geq (1-q^{-m})$ if $k-\ell > 1$ and $n-k-1 \geq \lceil \ell/(k-\ell-1) \rceil$. Further, this may be done in $\mathcal{O}(n^3)$ operations over $\mathbb{F}_{q^m}$.*

Proof. Let G_{SUB} be the generator matrix of $\mathcal{G}_{\mathrm{SUB}}$. To recover g from $\mathcal{G}_{\mathrm{SUB}}$ we choose $f \in \mathbb{N}$ such that $n-k-1 \geq f \geq \lceil \ell/(k-\ell-1) \rceil$. If Assumption 5.1 holds, $\lambda_f(G_{\mathrm{SUB}})$ has rank $k+f$ with probability $\geq (1-q^{-m})$ and defines a subcode of a $[n, k+f]$ Gabidulin code. Thus, in most cases, $\lambda_f(G_{\mathrm{SUB}})$ spans the $[n, k+f]$ Gabidulin code with generator vector g and we can recover g in $\mathcal{O}((k+f)^3)$ operations over $\mathbb{F}_{q^m}$ (see [5]). □

Note, that it is sufficient to know the generator vector g for the Gabidulin code $\mathcal{G}$ in the secret key of an Niederreiter GPT instance, to decrypt all ciphertexts.

For the parameter sets proposed e.g. in [2], the choice of $f = 1$ showed to be sufficient in all our experiments. I wish to thank P. Loidreau for pointing out, that the attack presented in this section may be combined with Ourivski's approach: The matrix $\Lambda_f(G^{\mathrm{pub}})$ will be the of higher rank as G^{pub} and is the public key of an instance of the Niederreiter GPT. Thus, one can try to employ Ourivski's approach to recover the secret key from it. Further, the upper bound of complexity of Ourivski's attack is lower for the Niederreiter GPT public key defined by $\Lambda_f(G^{\mathrm{pub}})$, than for the one defined by G^{pub}.

5.2. *Attacking GGPT*

As we have seen in the previous section, the structure of Gabidulin codes allows to recover the original code from a subcode. The same holds for many distorted Gabidulin codes like the public key of most GPT variants. In the following let (G^{pub}, r) be the public key of an instance of the GGPT cryptosystem with parameters q, m, n, k, t and s and (G, S, T) be a corresponding secret key as in Section 3. The attack strategy is almost always the same and can be summarized in the following way:

Table 2. Attacking GGPT.

(i) Determine the maximal f, such that $\Lambda_f(G^{\text{pub}})$ has not full rank.
(ii) If $\Lambda_f(G^{\text{pub}})^{\perp}$ has not full rank over $\mathbb{F}_q$, compute a column scrambler $\widehat{T}$, such that the first rows of $\Lambda_f(G^{\text{pub}})^{\perp}\widehat{T}^{\top}$ are zero. Otherwise the attack fails.
(iii) If the last columns of $G^{\text{pub}}\widehat{T}^{-1}$ generate a Gabidulin code, compute its generator vector $\widehat{g}$ and a row scrambler $\widehat{S}$ by one of the already known methods.
(iv) Verify that $\widehat{T}$ and $\widehat{S}$ are part of a valid secret key.

In the following we will analyze, in which case this strategy allows an attacker to build a valid secret key.

A crucial point for this type of attacks on the private key of GGPT is the analysis of the structure of the dual of $\Lambda_f(G^{\text{pub}})$. That structure depends mainly on f and the $k \times t$ distortion matrix X of rank s, which is used during the key generation phase of GGPT. We want to remind the reader that $n - t - k = 2r$.

Theorem 5.2. *For $0 \leq f \leq 2r-1$ there exists a dual matrix of $\Lambda_f(G^{\text{pub}})$ of the form*

$$\Lambda_f(G^{\text{pub}})^{\perp} = \begin{bmatrix} 0 & H_f^{\top} \\ B_1 & B_2 \end{bmatrix} \cdot (T^{-1})^{\top} \in \mathbb{F}_{q^m}^{(2r-f+\ell)\times n}, \tag{8}$$

where $H_f \in \mathbb{F}_{q^m}^{(n-t)\times(2r-f)}$ is the check matrix of a $k+f$ dimensional Gabidulin code $\mathcal{G}_f$ of length $n-t$, B_1 is some $\ell \times t$ matrix with $0 \leq \ell \leq t$ and B_2 is some $\ell \times (n-t)$ matrix.

Proof. First, we assume, that T and S are the identity matrix. The proof is analogous, if this is not the case. We may write

$$\Lambda_f(G^{\text{pub}}) = [\underbrace{\Lambda_f(G_{\cdot\{1,\ldots,t\}} + X)}_{t} \mid \underbrace{\Lambda_f(G_{\cdot\{t+1,\ldots,n\}})}_{n-t}] \in \mathbb{F}_{q^m}^{(k(f+1))\times n}.$$

By Lemma 5.1, the last $n-t$ columns of $\Lambda_f(G^{\text{pub}})$ define an $[n-t, k+f]$ Gabidulin code $\mathcal{G}_f$. Thus the subvectorspace spanned by the rows of

$$[0|H_f^{\top}] \in \mathbb{F}_{q^m}^{(2r-f)\times n},$$

where $H_f \in \mathbb{F}_{q^m}^{(n-t)\times(2r-f)}$ is the check matrix of $\mathcal{G}_f$, is in the dual space of $\Lambda_f(G^{\text{pub}})$. To get a matrix which defines the whole dual space of $\Lambda_f(G^{\text{pub}})$, we might have to add some more rows to $[0|H_f^{\top}]$. However, it is clear, that there will be at most t rows missing, as $\Lambda_f(G^{\text{pub}})$ has at least rank $k+f$. This proves the theorem. □

It can be shown, that the representation of $\Lambda_f(G^{\text{pub}})^{\perp}$ in (8) is normalized in a very strong way (see Lemma B.1 in Appendix B): Every H_i is uniquely determined by the secret key and $\langle H_{i+1}\rangle \subset \langle H_i\rangle$. This allows us to recover an alternative secret key if the

rank of $\Lambda_f(G^{\text{pub}})^\perp$ is at its lower bound $(2r-f)$ for some f. In that case, $\Lambda_f(G^{\text{pub}})^\perp$ is of the form

$$[0|H_f^\top]T \in \mathbb{F}_{q^m}^{(2r-f)\times n}, \tag{9}$$

and thus reveals information about T as it is not of full rank over $\mathbb{F}_q$. We are going to determine the rank of $\Lambda_f(G^{\text{pub}})^\perp$ in the following sections and show that every column scrambler deduced from (9) leads to a valid secret key.

Theorem 5.3. *If there exists an integer $f \le 2r-1$ s.t. the rank of $\Lambda_f(G^{\text{pub}})^\perp$ is $2r-f$, then the rank of $\Lambda_f(G^{\text{pub}})^\perp$ over $\mathbb{F}_q$ is exactly $n-t$. Further, every invertible matrix $\widehat{T} \in \mathbb{F}_q^{n\times n}$, which maps $\Lambda_f(G^{\text{pub}})^\perp$ to a matrix where the first t columns are zero is a column scrambler for a valid secret key. Thus, an attacker can recover a valid secret key in $\mathcal{O}(n^3)$ operations.*

Proof. With the conditions above, it follows from Theorem 5.2, that the matrix $\Lambda_f(G^{\text{pub}})^\perp$ is of the form of (8) with $l=0$ and thus of the form of (9). We can build $\Lambda_f(G^{\text{pub}})$ and $\Lambda_f(G^{\text{pub}})^\perp$ in $\mathcal{O}(n^3)$ operations over $\mathbb{F}_{q^m}$. Now we can choose a set N_1 of columns s.t. $\Lambda_f(G^{\text{pub}})^\perp_{\cdot N_1}$ is of column rank $n-t$ over $\mathbb{F}_q$. It follows, that $T_{N_1N_2}$ with $N_2 := \{t+1,\dots,n\}$ is invertible. We may assume without loss of generality that $N_1 = N_2$ and $H_f^\top = \Lambda_f(G^{\text{pub}})^\perp_{\cdot N_1}$. Let $\widetilde{T} \in \mathbb{F}_q^{t\times(n-t)}$ be the solution of the equation

$$\Lambda_f(G^{\text{pub}})^\perp_{\cdot\{1,\dots,t\}} = H_f^\top \cdot \widetilde{T}^\top$$

over $\mathbb{F}_q$. We define

$$\widehat{T}^{-1} := \begin{bmatrix} \mathrm{Id}_t & \widetilde{T} \\ 0 & \mathrm{Id}_{n-t} \end{bmatrix} \in \mathbb{F}_q^{n\times n}.$$

As H_0 and H_f are uniquely determined by G^{pub} and $\widehat{T}$, it follows, that $[0|H_0]$ is in the dual space of $G^{\text{pub}}\widehat{T}^{-1}$. Thus $\widehat{T}$ serves as an alternative column scrambler as the last $n-t$ columns of $G^{\text{pub}}\widehat{T}^{-1}$ define an $(n-t,k)$ Gabidulin code. Now, an row scrambler completing the equivalent secret key may be obtained from $(G^{\text{pub}} \cdot \widehat{T}^{-1})_{\cdot\{t+1,\dots,n\}}$ in $\mathcal{O}(k^3)$ operations [5]. □

5.3. *Insecure Parameter Sets for GGPT*

Given an f s.t. the conditions of Theorem 5.3 are fulfilled, for the GGPT public key, we can build an alternative private key in $\mathcal{O}(n^3)$ operations over $\mathbb{F}_{q^m}$. In this section we are going to determine for which parameter sets such a f exists. To do so, we will have to determine the rank of $\Lambda_f(G^{\text{pub}})^\perp$, as the attack works if the rank is small and is more likely to fail, if it is large. As we will see, the rank of $\Lambda_f(G^{\text{pub}})^\perp$ is strongly connected to the rank s of the distortion matrix $X \in \mathbb{F}_{q^m}^{k\times t}$.

Theorem 5.4. *Let $0 \le f \le 2r-1$, then the rank R of $\Lambda_f(G^{\text{pub}})^\perp$ is $\le n-k-f-\min\{t, fs, f(k-1)\}$ holds with probability $> (1-sq^{-m})(1-4q^{-m})$.*

Table 3. Attacking the GGPT cryptosystem.

Parameters				WF attack	WF best of
m	k	t	s	from [17]	Gibson's attacks
48	10	16	3	2^{28} (success probability 1)	2^{139}
48	16	18	4	2^{28} (success probability ≈ 1)	2^{200}
48	24	8	2	2^{28} (success probability 1)	2^{122}

We will assume that $s < k$ in the following, as all proofs and estimations are analogous otherwise, except, that you have to replace s with $k-1$. Before we prove the theorem we want to point out the consequences: All parameter sets, where

$$t \leq s \cdot (2r-1) \tag{10}$$

are insecure, as the conditions of Theorem 5.3 will be met for $f = 2r-1$. Furthermore, we may obtain an equivalent secret key with probability 1 for all parameter sets where

$$t \leq 2r-1 \quad \Longleftrightarrow \quad 1/2 \leq (n-k)/2 - t \tag{11}$$

for the same reasons. Equation (11) is true for all instances of the original GPT cryptosystem and most parameter sets for GGPT from Table 1. All in all, the attack presented above succeeds for all parameter sets proposed so far with high probability, and runs in polynomial time (see Table 3)

Proof of Theorem 5.4. Here we present a sketch of the proof, for a more detailed version see Appendix C. It can be shown, that $\Lambda_f(G^{\text{pub}})T^{-1}$ generates the same vector space as a Matrix of the form

$$\begin{bmatrix} Y & \lambda_{f+k-1}(G_{\{1\}\{t+1,\ldots,n\}}) \\ \lambda_{f-1}(\widetilde{X}) & 0 \end{bmatrix}, \quad \text{where } \widetilde{X} = X_{\{2,\ldots,k\}\cdot} + X^{[q]}_{\{1,\ldots,k-1\}\cdot}$$

and Y is some arbitrary matrix. As $\widetilde{X}_{\{1,\ldots,s\}\cdot}$ is a random matrix, it is of rank s with probability $\approx (1-sq^{-m})$. Lemma 5.2 yields that $\lambda_f(\widetilde{X})$ has rank $\min\{t, fs\}$ with probability $> (1-4q^{-m})$. However, $\widetilde{X}$ has rank at least 1, which proves the theorem. □

5.4. *Towards GGPT Instances Secure Against Structural Attacks*

We have seen, that instances of the GGPT cryptosystem and its variants, where (10) holds are insecure if Assumption 5.2 holds. However, we may choose parameter sets, s.t. this equation does not hold. Even though, we might be able recover an equivalent private key if there is a $f < 2r-1$, such that

$$\operatorname{rank}(\Lambda_f(G^{\text{pub}})^{\perp}) < n-t-1. \tag{12}$$

In that case, an attacker can proceed as follows:

Table 4. A modified attack on GGPT.

(i) Guess a set N_1 of $n-t$ positions such that $([0\|H_f^\top](T^{-1})^\top)_{\cdot N_1}$ has full column rank over $\mathbb{F}_q$.
(ii) Apply an attack on the Niederreiter GPT to the check matrix $(\Lambda_f(G^{\text{pub}})^\perp_{\cdot N_1})^\top$.
(iii) Recover the matrix $\Lambda_f(G^{\text{pub}})^\perp$ of the form in (8).
(iv) Build an alternative private key.

A set N_1 may be used by the attacker if $(T^{-1})_{N_1\{t+1,\ldots,n\}}$ is invertible. Guessing such a set can be done with sufficient probability if $T \in \mathbb{F}_q^{n\times n}$ was chosen at random:

Lemma 5.3. *The probability, that a random* $(n-t)\times(n-t)$ *matrix over* $\mathbb{F}_q$ *is invertible is larger than* 0.28.

Proof. The number of invertible $i \times i$ matrices over $\mathbb{F}_{q^m}$ is $\prod_{j=0}^{i-1}(q^{mi} - q^{mj})$ [19]. With the results from [4] we get the following bound:

$$\frac{1}{q^{(n-t)^2}} \cdot \prod_{j=0}^{n-t-1}(q^{(n-t)} - q^j) = \prod_{j=1}^{n-t}(1-q^{-j}) \geq 0.288788. \qquad \square$$

If the attacker has guessed a valid set N_1 he may assume without loss of generality that $(T^{-1})_{N_1N_2} = \mathrm{Id}_{n-t}$. If (12) holds, the check matrix $(\Lambda_f(G^{\text{pub}})^\perp_{\cdot N_1})^\top$ defines a subcode of an $[n-t, k+f]$ Gabidulin code of dimension at least 2. Therefore it corresponds to an instance of the Niederreiter GPT and the attacker can apply the attacks on the Niederreiter variant of GPT, to recover $[H_f|B_2^\top]$. If one of the attacks succeeds, an attacker can recover a dual matrix of $\Lambda_f(G^{\text{pub}})$ of the form given in (8) and from it an alternative column scrambler. Afterwards the attacker would be able to construct a valid alternative private key.

To get secure instances of GGPT, one could try to choose parameters in a way, such that there is no choice of f such that (12) holds. By Theorem 5.4 we know, that the latter is the case, e.g. if

$$s \leq \frac{2t-n}{2r}. \tag{13}$$

Such a parameter set could be $q = 2$, $m = n = 64$, $k = 8$, $t = 40$ and $s = 1$ with a binary work factor of 2^{87} for a general decoding attack and a public key size of 3584 bytes. However, these parameter sets are only secure against the presented structural attack, but not necessarily against attacks on the ciphertext [16].

Remark 5.1. Experiments showed, that Assumption 5.1 does not seem to hold for subcodes of Gabidulin codes defined by the check matrix $(\Lambda_f(G^{\text{pub}})^\perp_{\cdot N_1})^\top$. Thus, for these instances of the Niederreiter GPT, the success probability of the attack from Section 5.2 is very small. However, these subcodes are not truly random ones, but are generated in a very special way (They are more or less the intersection of several Gabidulin codes). Thus, this observation does not contradict Assumption 5.1. Further, Ourivski's attack may still be applied.

5.5. *A Simple Attack for "GPT with Reducible Rank Codes"*

In [18] the author presented a security reduction for GPT with reducible rank codes. The security reduction relies on the assumption, that all private keys of an instance of GGPT are strongly connected to each other. The main idea is, to view only parts of the public generator matrix, which define public generator matrices of the CS-GPT cryptosystem. We will limit ourselves to the case, where the secret RRC is build from two Gabidulin codes. Proofs are analogous for all other cases. To attack RRC-GPT we first rewrite the public generator matrix:

Lemma 5.4. *Let (G^{pub}, r) be the public key of an instance of the RRC-GPT cryptosystem as given in (4). Further, let (G, S, T) be the corresponding secret key. Then there exists an invertible matrix $\widehat{T} \in \mathbb{F}_q^{(n_1+n_2)\times(n_1+n_2)}$ such that*

$$G^{\text{pub}}\widehat{T}^{-1} = S\left[\begin{array}{c|c|c} Z_1 & G_1 & 0 \\ \hline Z_2 & Y & G_2 \end{array}\right], \tag{14}$$

where the matrices G_i are generator matrices of $[n_i - t_i, k_i]$ Gabidulin codes and $Z_i \in \mathbb{F}_{q^m}^{k_i\times(t_1+t_2)}$ as well as $Y \in \mathbb{F}_{q^m}^{k_2\times(n_1-t_1)}$ are arbitrary matrices.

Further, if the matrix S_{JK_2} is invertible for a subset $J \subseteq \{1, \ldots, k_1 + k_2\}$ and $K_2 := \{k_1 + 1, \ldots, k_1 + k_2\}$, then $G_{J.}^{\text{pub}}$ is an instance of the CS-GPT cryptosystem.

Proof. As the matrices X_1 and X_2 used on key generation are of column rank smaller than t_i over $\mathbb{F}_q$, we may assume without loss of generality, that only their first t_i columns contain non-zero entries. Thus, by exchanging the $(t_1 + i)$-th column of $G^{\text{pub}}T^{-1}$ with the $(n_1 + i)$-th column for $i = 1, \ldots, t_2$ and modifying T accordingly, we get a matrix $\widehat{T}$ with the desired properties. The fact that $G_{J.}^{\text{pub}}$ forms a instance of the CS-GPT follows from the observations above. □

The representation of the private key as in (14) suggests an iterative attack on RRC-GPT as summarized in Table 5. This attack strategy will only work, if for each CS-GPT instance defined by a submatrix of k rows of G^{pub} the same column scrambler may be used. Therefore, we make the following assumption:

Assumption 5.2. Let (G^{pub}, r) be the public key of a random instance of GGPT with parameters q, n, m, k, t and s. Further, let (G, S, T) and $(\widehat{G}, \widehat{S}, \widehat{T})$ be two valid secret

Table 5. Attacking RRC-GPT with an CS-GPT oracle.

(i) Guess a subset J of k rows, such that they form a instance of the CS-GPT.
(ii) Use an attack on CS-GPT to recover a partial column-scrambler $\widehat{T}$ from $G_{J.}^{\text{pub}}$.
(iii) Remove the influence of $\widehat{T}$ from G^{pub} and verify that the right part of the matrix defines a Gabidulin code.
(iv) If the latter is the case, recover a partial row scrambler, remove its influence from G^{pub} and eliminate the rows and columns belonging to the recovered Gabidulin code.
(v) Continue the procedure until you have recovered a valid secret key.

keys corresponding to (G^{pub}, r), then

$$(\widehat{T}T^{-1})_{N_1N_2} = 0,$$

where $N_1 := \{1, \ldots, t\}$ and $N_2 := \{t+1, \ldots, n\}$.

With other words, we assume, that for all instances of the GGPT we are going to view, all possible secret keys are closely related to each other:

$$\widehat{G}_{\cdot N_2}(\widehat{T}T^{-1})_{N_2N_2} = G_{\cdot N_2}.$$

We did not find any counterexamples in our experiments for random instances of GGPT and the assumption can be proven for many instances of GGPT (see Lemma B.2 in Appendix B). Therefore, we can reduce the problem of finding a alternative secret key for a given RRC-GPT public key to the problem to recover a secret key for CS-GPT instances.

Lemma 5.5. *With the notations from Lemma 5.4. Let $S_{K_2K_2}$ be invertible and $\widehat{T}$ be the column scrambler of a valid secret key for the CS-GPT public key defined by $G^{\text{pub}}_{K_2\cdot}$. Let $G^{\text{pub}}_{K_2\cdot}\widehat{T}^{-1} = \widehat{S}[A|B|\widehat{G}_2]$ where the matrices $A \in \mathbb{F}_{q^m}^{k_2\times(t_1+t_2)}$ and $B \in \mathbb{F}_{q^m}^{k_2\times(n_1-t_1)}$ are arbitrary. Further, assume, that Assumption 5.2 holds for all secret key pairs of $G^{\text{pub}}_{K_2\cdot}$ with column scramblers T and $\widehat{T}$. Then there exists a solution of*

$$G^{\text{pub}}\widehat{T}^{-1} = S_1 \cdot \left[\begin{array}{c|c|c} Z_1 & G_1 & 0 \\ \hline A & B & \widehat{G}_2 \end{array}\right] \cdot \left[\begin{array}{c|c} T_1 & \begin{array}{c} 0 \\ 0 \end{array} \\ \hline \begin{array}{cc} 0 & 0 \end{array} & \mathrm{Id}_{(n_2-t_2)} \end{array}\right], \tag{15}$$

for some invertible matrices $S_1 \in \mathbb{F}_{q^m}^{k\times k}$ and $T_1 \in \mathbb{F}_q^{(n_1+t_2)\times(n_1+t_2)}$.

Proof. Assumption 5.2 yields, that the last $n_2 - t_2$ columns of $[Z_1|G_1|0]T\widehat{T}^{-1}$ are zero. It follows, that the rank of matrix build from the last $n_2 - t_2$ columns of $G^{\text{pub}}\widehat{T}^{-1}$ has only rank k_2, which proves the lemma. □

We omit analyzing the impact of the proposed attack on RRC-GPT here, but leave it to the next section.

5.6. *A Modified Attack for "GPT with Reducible Rank Codes"*

Choosing a minor variation of the attack from Section 5.2, we get a even more powerful attack on RRC-GPT than in the section above. For most instances of RRC-GPT the following is true:

Assumption 5.3. For a RRC-GPT public key (G^{pub}, r), the matrix $G^{\text{pub}}T^{-1}$ is of the form in (14), with $\langle Y\rangle \not\subseteq \langle G_1\rangle$, a matrix Z_1 that has at least one row of full column rank over $\mathbb{F}_q$ and where $[Z_1|G_1]$ as well as $[Y|G_2]$ do not define a Gabidulin (sub-) codes.

This assumption is true with probability almost 1, if Z_1 and Y were chosen at random. In this case, an attacker may replace the first two steps of the attack described in Table 5 by the following: "Recover a partial column scrambler $\widehat{T}$ from the matrix $\Lambda_f(G^{\text{pub}})$, where $f = n_2 - k_2 - t_2 - 1$." This modified attack works for a variety of parameter sets as e.g. in the following case:

Theorem 5.5. *With Assumption 5.3: Let (G^{pub}, r) be a public key of an instance of RRC-GPT with parameters $q, m, n_1 = n_2, k_1 = k_2$ and $t_1 = t_2$. If $2t_1 + 1 \leq 2r$, then we can recover an alternative private key in $\mathcal{O}(m^3)$ operations over $\mathbb{F}_{q^m}$.*

Proof. Let $f = n_2 - k_2 - t_2 - 1 = 2r - 1$. Like in Theorem 5.4, by multiplying the matrix $\Lambda_f(G^{\text{pub}})$ with a non-singular matrix from the left, we can see that

$$\langle \Lambda_f(G^{\text{pub}}) \rangle = \left\langle \left[\begin{array}{c} \Lambda_f\left(\left[Z_1 | G_1 | 0 \right]\right) \\ \hline \Lambda_f\left(\left[Z_2 | Y | G_2 \right]\right) \end{array} \right] \right\rangle = \left\langle \left[\begin{array}{c|c|c} A_1 & 0 & 0 \\ A_2 & \widetilde{G}_1 & 0 \\ \hline A_3 & B_1 & 0 \\ A_4 & B_2 & \widetilde{G}_2 \end{array} \right] \right\rangle \in \mathbb{F}_{q^m}^{(f+1)k \times n},$$

where A_2 and A_4 are matrices with $n_2 - t_2 - 1$ rows, A_1 has the same number of rows as A_3, and the $\widetilde{G}_i$ define $[n_2 - t_2, n_2 - t_2 - 1]$ Gabidulin codes, with the same generator vector as G_i for $i = 1, 2$. Further, by the assumption made, $A_1 \in \mathbb{F}_{q^m}^{(k_2(f+1)-(f+k_2))\times 2t_2}$ has rank at least $\min\{2t_1, f\}$. The assumptions for Y imply that the matrix $[\widetilde{G}_1^{\perp}\ B_1^{\perp}] \in \mathbb{F}_{q^m}^{(n_2-t_2)\times k_2(f+1)}$ has rank $n_2 - t_2$. We conclude, that the rank of $\Lambda_{2r-1}(G^{\text{pub}})^{\perp}$ is one, and following the methods from Theorem 5.3, we can build a column scrambler $\widetilde{T}$ from it. This column scrambler is part of some secret key for the GGPT instance defined by $[Z_2\ Y\ G_2]T$. Note, that for the GGPT instance defined by $[Z_2\ Y\ G_2]T$, the matrices T and $\widetilde{T}$ are column scramblers for two secret keys, for which Assumption 5.2 is true. We may assume without loss of generality, that $S_{K_2K_2}$ is invertible, and may write $G^{\text{pub}}_{K_2} \widehat{T}^{-1} = \widehat{S}[A|B|\widehat{G}_2]$. It follows from Lemma 5.5, that the attacker may compute a matrix $\widetilde{S} \in \mathbb{F}_{q^m}^{2k_2 \times 2k_2}$ s.t.

$$\widetilde{S}^{-1} G^{\text{pub}} \widehat{T}^{-1} = \left[\begin{array}{c|c} S_1 & 0 \\ \hline 0 & \mathrm{Id}_{k_2} \end{array} \right] \cdot \left[\begin{array}{c|c|c} Z_1 & G_1 & 0 \\ \hline A & B & \widehat{G}_2 \end{array} \right] \cdot \left[\begin{array}{c|c} T_1 & \begin{array}{c} 0 \\ \hline 0 \end{array} \\ \hline \begin{array}{cc} 0 & 0 \end{array} & \mathrm{Id}_{(n_2-t_2)} \end{array} \right]$$

for some invertible matrices $S_1 \in \mathbb{F}_{q^m}^{k_1 \times k_1}$ and $T_1 \in \mathbb{F}_q^{(n_1+t_2)\times(n_1+t_2)}$. The first k_1 rows of the first $n_1 + 2t_2$ columns of $\widetilde{S}^{-1} G^{\text{pub}} \widehat{T}^{-1}$ define a GGPT instance, for which the attack from Section 5 succeeds with probability 1. Thus, we may recover alternative T_1 and S_1, which is sufficient to build an alternative private key for the RRC-GPT public key (G^{pub}, r). □

The attack described above succeeds for much more parameter sets, than named (even without the previous Assumption 5.3). Therefore we are not able to name practical parameter sets for RRC-GPT, which are secure. An (awkward) parameter set secure

against this type of attack would be $m = 152$, $n_1 = 152$, $n_2 = 24$, $k_1 = k_2 = 8$, $t_2 = 0$ and $t_1 = 128$, as we can determine from (13) by setting $s = 2k_2$.

6. Using Subfield Subcodes for GPT

We have seen, that the only way, to build a secure and efficient public key cryptosystem from Gabidulin codes would be by a redesign of the cryptosystem. However, one would have to be extremely careful, as we are going to show in this section.

One attempt to do such a redesign could be the use of subfield subcodes. This approach is quite tempting, as Goppa codes are subfield subcodes of GRS codes, and the McEliece scheme is secure if we use Goppa codes, but not in the case of GRS codes. As we will see, this proposal coincides with instances of RRC-GPT. However, in this situation Assumption 5.3 is not true and one could hope having found a secure variant of GPT.

6.1. *Subfield Subcodes of Gabidulin Codes*

Let $\mathcal{G}$ be an Gabidulin code over $\mathbb{F}_{q^N}$, $N = m\bar{m}$. We may consider $\mathbb{F}_{q^N}$ to be an extension field of degree $\bar{m}$ over $\mathcal{V}_m \simeq \mathbb{F}_{q^m}$. The $\mathcal{V}_m$-(subfield)-subcode of a $\mathcal{G}$ is the subcode consisting of the codewords of $\mathcal{G}$ which have only entries in $\mathcal{V}_m$. Such codes were first analyzed in [6] by E. Gabidulin and P. Loidreau.

For the analysis of the structure of subfield subcodes, we will need to define a mapping between $\mathbb{F}_{q^N}$ and $\mathcal{V}_m^{\bar{m}}$. We will write $\mathbb{F}_{q^m}$ instead of $\mathcal{V}_m$ in the following. Let $\alpha^{q^1}, \alpha^{q^2}, \ldots, \alpha^{q^{\bar{m}}}$ be a normal basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_{q^m}$. Then every element $x \in \mathbb{F}_{q^N}$ has a unique representation $x = \sum_{i=1}^{\bar{m}} x_i \alpha^{q^i}$ with $x_i \in \mathbb{F}_{q^N}$. We define φ to be the (bijective) mapping $\varphi : \mathbb{F}_{q^N} \to \mathbb{F}_{q^m}^{\bar{m}}; x \mapsto (x_1, \ldots, x_{\bar{m}})^\top$ such that $x = \sum_{i=1}^{\bar{m}} x_i \alpha^{q^i}$. For a matrix $M = (m_{ij})_{i=1,j=1}^{k,n}$ over $\mathbb{F}_{q^N}$ the matrix $\varphi(M)$ denotes the block matrix $(\varphi(m_{ij}))_{i=1,j=1}^{k,n}$. If $\bar{m} = 2$, then for two matrices $M = (m_{ij})_{i=1,j=1}^{k,n}$ and $\widetilde{M} = (\widetilde{m}_{ij})_{i=1,j=1}^{k,n}$ over $\mathbb{F}_{q^m}$, we will denote the matrix

$$\left(\varphi^{-1}\left(\begin{pmatrix} m_{ij} \\ \widetilde{m}_{ij} \end{pmatrix}\right)\right)_{i=1,j=1}^{k,n} \quad \text{with } \varphi^{-1}(M, \widetilde{M}).$$

The orbit of $\varphi(x)$ under the operation of the Frobenius field automorphism on x allows to determine the check matrix of the $\mathbb{F}_{q^m}$-subcode of a Gabidulin code over $\mathbb{F}_{q^N}$:

Lemma 6.1. *For all i, the space spanned by the rows of $\varphi(x^{q^i})$ is the row-space of $(\varphi(x)_1^{q^i}, \ldots, \varphi(x)_{\bar{m}}^{q^i})^\top$.*

Proof. Since $\alpha^{q^1}, \alpha^{q^2}, \ldots, \alpha^{q^{\bar{m}}}$ is a basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_{q^m}$, $\alpha^{q^{1+i}}, \alpha^{q^{2+i}}, \ldots, \alpha^{q^{\bar{m}+i}}$ is also a basis, which can be obtained from the above basis by multiplication by a non-singular matrix over $\mathbb{F}_{q^m}$, say Q, thus

$$\varphi(x^{q^i}) = (\varphi(x)_1^{q^i}, \varphi(x)_2^{q^i}, \ldots, \varphi(x)_{\bar{m}}^{q^i})^\top Q^\top. \qquad \square$$

Let $h = (h_1, h_2, \ldots, h_n)$ be a check vector of the $[n, k]$ Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^N}$. From Lemma 6.1 we know that both matrices

$$\varphi \begin{pmatrix} h \\ h^{[1/q]} \\ \vdots \\ h^{1/q^{n-k-1}} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} h_{11} & h_{21} & \cdots & h_{n1} \\ \vdots & \vdots & & \vdots \\ h_{11}^{1/q^{n-k-1}} & h_{21}^{1/q^{n-k-1}} & \cdots & h_{n1}^{1/q^{n-k-1}} \\ h_{12} & h_{22} & \cdots & h_{n2} \\ \vdots & \vdots & & \vdots \\ h_{12}^{q^{1/n-k-1}} & h_{22}^{1/q^{d-2}} & \cdots & h_{n2}^{1/q^{n-k-1}} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ h_{1\bar{m}} & h_{2\bar{m}} & \cdots & h_{n\bar{m}} \\ \vdots & \vdots & & \vdots \\ h_{1\bar{m}}^{1/q^{n-k-1}} & h_{2\bar{m}}^{1/q^{n-k-1}} & \cdots & h_{n\bar{m}}^{1/q^{n-k-1}} \end{pmatrix}^{\top} \tag{16}$$

are check matrices of the $\mathbb{F}_{q^m}$-subfield-subcode of $\mathcal{G}$. The lower bound of the dimension of the $\mathbb{F}_{q^m}$-subfield-subcode of $\mathcal{G}$ is $n - \bar{m}(n-k)$, thus only when $n > \bar{m}(n-k)$, it is guaranteed to be of higher dimension than zero. Analogous to the results from [6], for $\bar{m} = 2$ we get the following theorem, which is a direct consequence of the observation above:

Theorem 6.1. *Let $\mathcal{G}$ be an $[n, k]$ Gabidulin code over $\mathbb{F}_{q^{2m}}$ with, $k > m$. Then for the $\mathbb{F}_{q^m}$-subfield-subcode $\mathcal{G}_{\text{SUB}}$, there exists a non-singular matrix $T \in \mathbb{F}_2^{n \times n}$ such that $H \cdot T$ is the generator matrix of a reducible rank code build from two Gabidulin codes over $\mathbb{F}_{q^m}$ with dimension $n - k$. It follows, that $\mathcal{G}_{\text{SUB}}$ is a (scrambled) reducible rank code as well. and has minimum distance $d = n - k + 1$.*

6.2. *A Version of GPT Using Subfield Subcodes*

With Theorem 6.1, we can give a simple description of a variant of GPT using subfield subcodes. We will limit ourselves to the cases, where $\bar{m} = 2$, $n = N$ and $k > m$, which are the most interesting ones. The public generator matrix G^{pub} of an instance of such an GPT variant might be described as

$$G^{\text{pub}} = S \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} T \in \mathbb{F}_{q^m}^{2k \times n}, \tag{17}$$

where G_1 and G_2 are $[m, k]$ Gabidulin codes over $\mathbb{F}_{q^m}$ and $S \in \mathbb{F}_{q^m}^{2k \times 2k}$ and $T \in \mathbb{F}_q^{n \times n}$ are non-singular matrices. The secret key of such an GPT variant could be (G_1, G_2, S, T). Unfortunately, this design of a cryptosystem is insecure. The application of a distortion matrix won't change the situation too much, so we omit viewing that case.

Let h_i be the check vector of $\langle G_i \rangle$, $i = 1, 2$. With the results from above, the matrix $G^{\text{pub}} T^{-1}$ is the generator matrix of the $\mathbb{F}_{q^m}$-subcode of the $[2n, n+k]$ Gabidulin code over $\mathbb{F}_{q^{2m}}$ with check vector

$$h = (\varphi^{-1}(h_1, 0),\ \varphi^{-1}(0, h_2)).$$

Observe, that for any non-singular matrix $\gamma = (\gamma_{ij})_{i,j\in\{1,2\}} \in \mathbb{F}_{q^m}^{2\times 2}$ the $\mathbb{F}_{q^m}$-subcode of the $[2m, m+k]$ Gabidulin code over $\mathbb{F}_{q^{2m}}$ with check vector

$$h_\gamma = (\varphi^{-1}(\gamma_{11} \cdot h_1, \gamma_{12} \cdot h_1),\ \varphi^{-1}(\gamma_{21} \cdot h_2, \gamma_{22} \cdot h_2))$$

has generator matrix $G^{\text{pub}} T^{-1}$, too. Again we can apply λ_f as in Section 5.1. One can prove, that

$$(\Lambda_{n-k-1}(G^{\text{pub}}))^\perp = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix} \begin{bmatrix} h_1 & 0 \\ 0 & h_2 \end{bmatrix} (T^{-1})^\top$$

for some invertible matrix $(\gamma_{ij}) \in \mathbb{F}_{q^m}^{2\times 2}$. We know, that G^{pub} is the generator matrix of the $\mathbb{F}_{q^m}$-subcode of the $[2n, n+k]$ Gabidulin code with check vector $h(T^{-1})^\top$ and as well of the $[2n, n+k]$ Gabidulin code with check vector $h_\gamma (T^{-1})^\top$. As the latter one can correct errors of rank up to $\frac{n-k}{2}$, we can recover a valid alternative secret key by computing $(\Lambda_{n-k-1}(G^{\text{pub}}))^\perp$.

With other words, the application of the column scrambler T does not change the situation. Further, the method presented may be used to recover a generator vector of some Gabidulin code given the generator matrix of its subfield subcode in $\mathcal{O}(N^3)$ operations over $\mathbb{F}_{q^N}$. Even if we would use Gabidulin codes, which are not of full length ($n < N$), the methods presented in this paper allow to recover the generator vector from a description of the subfield subcode.

7. Conclusion

None of the existing GPT variants is secure for parameter sets of practical interest, as they may be attacked in polynomial time. Even if we would consider the remaining possible parameter sets to be secure, their long term security has to be doubted (compare [16]).

We have seen that neither the addition of random redundancy, distortion matrices or supplementary check vectors, nor the employment of reducible codes is sufficient to allow hide the structure of Gabidulin codes efficiently. Additionally, we have shown, that the use of subfield subcodes does not lead to a secure GPT variant, unlike in the case of the proposal from Niederreiter (Goppa codes are subfield subcodes of GRS codes). Because of their highly structured generator matrix, Gabidulin codes do not seem to be a good choice for cryptographic applications.

Appendix A. Notations

– We write $\mathcal{G} = \langle G \rangle$ if the linear $[n, k]$-code $\mathcal{G}$ over the field $\mathbb{F}$ is spanned by the rows of G.

- If the rows of an $(n-k)\times n$ matrix M span $\mathcal{G}^{\perp}$ we write $G^{\perp}=M$. With this notation $M^{\top}$ is a check matrix of $\mathcal{G}$.
- We will identify $x\in\mathbb{F}^n$ with $(x_1,\ldots,x_n), x_i\in\mathbb{F}$ for $i=1,\ldots,n$.
- For any (ordered) subset $\{j_1,\ldots,j_m\}=J\subseteq\{1,\ldots,n\}$ we denote the vector $(x_{j_1},\ldots,x_{j_m})\in\mathbb{F}^m$ with x_J. Similarly, we denote by $M_{.J}$ the submatrix of a $k\times n$ matrix M consisting of the columns corresponding to the indices of J and $M_{J'.}=((M^{\top})_{.J'})^{\top}$ for any (ordered) subset J' of $\{1,\ldots,k\}$.
- For a matrix $M=(m_{i,j})$ let $M^{[q]}$ denote the matrix $(m_{i,j}^{q})$.
- Block matrices will be given in brackets.

Appendix B. Lemmas

Lemma B.1. *With the notations from Theorem 5.2. The Gabidulin code $\mathcal{G}_f$ is uniquely defined by the secret key (G,S,T).*

Proof. Let $\widehat{H}_f$ be a check matrix of a second $[n-t,k+f]$ Gabidulin code $\widehat{\mathcal{G}}_f\neq\mathcal{G}_f$ s.t. the rows of $[0|\widehat{H}_f^{\top}]\cdot(T^{-1})^{\top}$ are in the dual space of $\Lambda_f(G^{\mathrm{pub}})$. Then we have

$$\Lambda_f(G^{\mathrm{pub}})\cdot T^{-1}\cdot\begin{bmatrix}0 & 0\\ H_f & \widehat{H}_f\end{bmatrix}=0,$$

and as $\widehat{\mathcal{G}}_f\neq\mathcal{G}_f$, the last $n-t$ columns of $\Lambda_f(G^{\mathrm{pub}})\cdot T^{-1}$ define a subcode of a Gabidulin code of dimension smaller than $k+f$. This is a contradiction to the fact, that (G,S,T) is a secret key for (G^{pub},r), as by Lemma 5.1 the matrix $(\Lambda_f(G^{\mathrm{pub}})\cdot T^{-1})_{\cdot\{t+1,\ldots,n\}}$ has rank $k+f$. □

Lemma B.2. *Let (G^{pub},r) be as in Lemma 5.2, where $\Lambda_{n-k-t-1}(G^{\mathrm{pub}})^{\perp}$ has rank 1. Then Assumption 5.2 holds for all pairs (G,S,T) and $(\widehat{G},\widehat{S},\widehat{T})$ of secret keys.*

Proof. Let $G^{\mathrm{pub}}=S([X|0]+G)T$. With the notation of Theorem 5.2: Let H_0 be a checkmatrix of the $[n-t,k]$ Gabidulin code $\mathcal{G}_0$ and let $\widehat{H}_0$ be a checkmatrix of the $[n-t,k]$ Gabidulin code $\widehat{\mathcal{G}}_0$, that is

$$G^{\mathrm{pub}}\widehat{T}^{-1}\begin{bmatrix}0\\ \widehat{H}_0\end{bmatrix}=0.$$

As the rank of $\Lambda_{n-k-t-1}(G^{\mathrm{pub}})^{\perp}$ is one, we can conclude that

$$T^{-1}\begin{bmatrix}0\\ H_{n-t-k-1}\end{bmatrix}=\widehat{T}^{-1}\begin{bmatrix}0\\ \widehat{H}_{n-t-k-1}\end{bmatrix}\quad\Longrightarrow\quad T^{-1}\begin{bmatrix}0\\ H_0\end{bmatrix}=\widehat{T}^{-1}\begin{bmatrix}0\\ \widehat{H}_0\end{bmatrix}.$$

For $1\leq i\leq n$ let $\boldsymbol{e}_i$ denote the n-vector over $\mathbb{F}_{q^m}$ with a 1 at the i-th position, and zeros at all other positions. With this notation,

$$\boldsymbol{e}_i\begin{bmatrix}0\\ \widehat{H}_0\end{bmatrix}=0\quad\Longrightarrow\quad\boldsymbol{e}_i\widehat{T}\cdot T^{-1}\begin{bmatrix}0\\ H_0\end{bmatrix}=0.$$

As the rank norm of $\boldsymbol{e}_i$ is one, the vector $(\boldsymbol{e}_i \widehat{T} \cdot T^{-1})_{\{t+1,\ldots,n\}}$ has rank norm at most one and can not be in the code $\langle G_2 \rangle$ if it is not zero. We conclude

$$\left\langle \left[\begin{array}{c|c} \mathrm{Id}_t & 0 \\ \hline 0 & 0 \end{array}\right] \widehat{T} \cdot T^{-1} \right\rangle = \left\langle \left[\begin{array}{c|c} \mathrm{Id}_t & 0 \\ \hline 0 & 0 \end{array}\right] \right\rangle. \qquad \square$$

Appendix C. Proof of Theorem 5.4

Proof. We have to estimate the rank of $\Lambda_f(G^{\mathrm{pub}})$ for given f and $G^{\mathrm{pub}} = S([X|0] + G)T$. As G is of the form in (1), the result of adding the $(j+1)$-th row of $G^{[q^i]}$ to the j-th row of $G^{[q^{i+1}]}$ is zero for $0 \le i \le f-1$ and $1 \le j \le k-1$. Remember that $G_{1\cdot} = g$. To further simplify notations, we define the following matrices:

$$M_k := \begin{bmatrix} 0 & \mathrm{Id}_{(k-1)} \\ 0 & 0 \end{bmatrix} \in \mathbb{F}_{q^m}^{k \times k} \quad \text{and} \quad \widetilde{X} := X_{\{2,\ldots,k\}\cdot} + (X^{[q]})_{\{1,\ldots,k-1\}\cdot} \in \mathbb{F}_{q^m}^{k-1 \times t}.$$

By removing the influence of S and adding the rows as mentioned above by using M_k, we get the following matrix of the same rank as $\Lambda_f(G^{\mathrm{pub}})$:

$$\begin{bmatrix} \mathrm{Id}_k & 0 & \cdots & 0 \\ M_k & \mathrm{Id}_k & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & M_k & \mathrm{Id}_k \end{bmatrix} \cdot \begin{bmatrix} S^{[q^0]} & 0 & \cdots & 0 \\ 0 & S^{[q^1]} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & S^{[q^f]} \end{bmatrix}^{-1} \cdot \lambda_f(S([X|0] + G)T)$$

$$= \left[\begin{array}{c|c} X + G_{\cdot\{1,\ldots,t\}} & G_{\cdot\{t+1,\ldots,n\}} \\ \hline \widetilde{X}^{[q^0]} & 0 \\ \hline X_{k\cdot}^{[q]} + g_{\{1,\ldots,t\}}^{[q^k]} & g_{\{t+1,\ldots,n\}}^{[q^k]} \\ \hline \vdots & \vdots \\ \hline \widetilde{X}^{[q^{f-1}]} & 0 \\ \hline X_{k\cdot}^{[q]} + g_{\{1,\ldots,t\}}^{[q^{k+f-1}]} & g_{\{t+1,\ldots,n\}}^{[q^{k+f-1}]} \end{array}\right] \cdot T \in \mathbb{F}_{q^m}^{((f+1)\cdot k) \times n}.$$

It remains to estimate the rank of $\lambda_{f-1}(\widetilde{X})$ as the right part of the matrix above has rank $k+f$ (it is generated by $\lambda_{k-1+f}(g_{\{t+1,\ldots,n\}})$). Fist observe, that the rank of $\widetilde{X}$ is larger than 1 or X has the form of a Gabidulin generator matrix, which is not the case. Furthermore, if $\widetilde{X}$ would be of column rank $< t$ over $\mathbb{F}_q$, then we can assume without loss of generality, that its last column is zero. It would follow, that $(G^{\mathrm{pub}} T^{-1})_{\cdot\{t,\ldots,n\}}$ defines a Gabidulin code or is of column rank $< n - t + 1$, but none of this cases is true. Thus, the rank of $\widetilde{X}$ over $\mathbb{F}_q$ is t. Second, any selection J of s columns of $\widetilde{X}$ forms a random matrix (as $X_{\cdot J}$ is random). In consequence, $\widetilde{X}$ has rank $\ge s$ with probability

larger than

$$\frac{1}{q^{ms^2}}\prod_{i=0}^{s-1}(q^{ms}-q^{mi}) \geq \prod_{i=0}^{s-1}(1-q^{m(i-s)}) \approx 1-\frac{s}{q^m}.$$

Observe further, that every matrix $\widetilde{X}_{\{1,\ldots,s\}\cdot}$ is generated by some matrix X of rank $\leq s$ (e.g. if $X_{(s+1)\cdot}=0$). We conclude, that the first s rows of $\widetilde{X}$ form a random matrix. which has column rank t over $\mathbb{F}_q$ with probability ≈ 1. Thus the Lemmas 5.1 and 5.2 yield the theorem. □

References

[1] T.P. Berger, P. Loidreau, Security of the Niederreiter form of the GPT public-key cryptosystem, in *IEEE International Symposium on Information Theory, Lausanne, Suisse* (IEEE Press, New York, 2002)

[2] T.P. Berger, P. Loidreau, How to mask the structure of codes for a cryptographic use, *Des. Codes Cryptogr.* **35**(1), 63–79 (2005)

[3] N. Courtois, M. Finiasz, N. Sendrier, How to achieve a McEliece-based digital signature scheme, in *Advances in Cryptology—ASIACRYPT 2001*, vol. 2248 (Springer, Berlin, 2001), pp. 157–174

[4] S.R. Finch, *Mathematical Constants*. Encyclopedia of Mathematics and Applications. Cambridge, 2003. See http://mathworld.wolfram.com/InfiniteProduct.html

[5] E.M. Gabidulin, On public-key cryptosystems based on linear codes, in *Proc. of 4th IMA Conference on Cryptography and Coding 1993*. Codes and Ciphers (IMA Press, Southend-on Sea, 1995)

[6] E.M. Gabidulin, P. Loidreau, Subfield subcodes of maximum-rank distance codes, in *Seventh International Workshop on Algebraic and Combinatorial Coding Theory*. ACCT, vol. 7, pp. 151–156 (2000)

[7] E.M. Gabidulin, A.V. Ourivski, Column scrambler for the GPT cryptosystem, *Discrete Appl. Math.* **128**(1), 207–221 (2003)

[8] E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, Ideals over a non-commutative ring and their applications to cryptography, in *Proc. Eurocrypt '91*. LNCS, vol. 547 (Springer, Berlin, 1991)

[9] E.M. Gabidulin, A.V. Ourivski, B. Honary, B. Ammar, Reducible rank codes and their applications to cryptography, *IEEE Trans. Inform. Theory* **49**(12), 3289–3293 (2003)

[10] J.K. Gibson, Severely denting the Gabidulin version of the McEliece public key cryptosystem, *Des. Codes Cryptogr.* **6**(1), 37–45 (1995)

[11] K. Gibson, The security of the Gabidulin public key cryptosystem, in *Proc. of Eurocrypt'96*. LNCS, vol. 1070 (Springer, Berlin, 1996), pp. 212–223

[12] T. Johansson, A.V. Ourivski, New technique for decoding codes in the rank metric and its cryptography applications, *Problems Inform. Transm.* **38**(3), 237–246 (2002)

[13] P. Loidreau, R. Overbeck, Decoding rank errors beyond the error-correction capability, in *Proc. of ACCT-10, Zvenigorod* (2006)

[14] R.J. McEliece, A public key cryptosystem based on algebraic coding theory, *DSN Prog. Rep.* **42–44**, 114–116 (1978)

[15] A.V. Ourivski, Recovering a parent code for subcodes of maximal rank distance codes, in *Proc. of WCC 03*, pp. 357–363 (2003)

[16] R. Overbeck, Decoding interleaved Gabidulin codes and ciphertext-security for GPT variants. Available at http://eprint.iacr.org/2006/222

[17] R. Overbeck, A new structural attack for GPT and variants, in *Proc. of Mycrypt 2005*. LNCS, vol. 3715 (Springer, Berlin, 2005), pp. 50–63

[18] R. Overbeck, Extending Gibson's attacks on the GPT cryptosystem, in *Proc. of WCC 2005*. LNCS, vol. 3969 (Springer, Berlin, 2006), pp. 178–188

[19] M. Ogle, T. Migler, K.E. Morrison, Weight and rank of matrices over finite fields, 2003. Available at http://www.calpoly.edu/~kmorriso/Research/research.html