A New Structural Attack for GPT and Variants

Raphael Overbeck

GK Electronic Commerce,
TU-Darmstadt,
Department of Computer Science,
Cryptography and Computer Algebra Group
overbeck@cdc.informatik.tu-darmstadt.de

Abstract. In this paper we look at the Gabidulin version of the McEliece cryptosystem (GPT) and its variants. We propose a new polynomial time attack, which recovers an alternative private key. Our attack is applicable to all variants proposed so far and breaks some of them completely.

Keywords: 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. In 1991 Gabidulin, Paramonov and Tretjakov proposed a variant of the McEliece scheme (GPT) [7] using *rank distance* codes instead of hamming distance codes. Smaller public-key sizes have been proposed for GPT than for the original McEliece cryptosystem, as general decoding algorithms are much slower for the rank metric than for the hamming-metric.

Gibson developed two structural attacks for the GPT cryptosystem (see e.g. [4] and [8]) and proved the parameter sets proposed in [7] and [4] to be insecure. A drawback of Gibson's attacks is, that they have exponential runtime if the secret key is carefully chosen. There were several attempts to modify the GPT cryptosystem, in order to avoid structural attacks, but most of these variants rely on security assumptions very similar to the ones for the original proposal (see [2] and [11]).

In this paper we build a new structural attack on the GPT cryptosystem. Unlike Gibson's attacks it has polynomial runtime, breaks the original GPT cryptosystem from [7] completely and is applicable to all GPT variants proposed so far.

The paper is structured as follows: First we give a short introduction to rank distance codes. Then we present the GPT cryptosystem and its Niederreiter variant. Finally we show how to attack the GPT cryptosystem.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 50–63, 2005.

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 (a power of a) prime and $m \in \mathbb{N}$. As their name says they use the concept of rank distance.

Definition 1. *Let $x = (x_1, \cdots, x_n) \in \mathbb{F}_{q^m}^n$ and $b_1, \cdots, b_m$ 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 $i = 1, \cdots, n$ with $x_{ij} \in \mathbb{F}_q$. The rank norm $\|x\|_r$ of x is defined as the rank of the matrix $(x_{ij}) \in \mathbb{F}_{q^m}^{n \times m}$.*

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.*

Definition 2. *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 [9] Ourivski and Johansson presented an algorithm which solves the general decoding problem in $\mathcal{O}\left((m\frac{d-1}{2})^3 q^{(d-3)(k+1)/2}\right)$ 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 [4]. We will define these codes by their generator matrix.

Definition 3. *Let $k \le n \le m \in \mathbb{N}$ and $g \in \mathbb{F}_{q^m}^n$ be a vector s.t. the components g_i, $i = 1, \cdots, n$ are linearly independent over $\mathbb{F}_q$. 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 $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors and has a minimum distance of $d = n - k + 1$. The dual code of an (n, k) Gabidulin code is an $(n, n - k)$ Gabidulin code (see [4]). The vector g is said to be a *generator vector* of the Gabidulin code $\mathcal{G}$ (it is not unique). Error correction based on the *right Euclidean division algorithm* takes $\mathcal{O}\left(d \log_2^2 d + dn\right)$ operations over $\mathbb{F}_{q^m}$ for (n, k, d) Gabidulin codes [4].

Throughout this paper we will use the following notation. We write $\mathcal{G} = \langle G \rangle$ if the (n, k)-code $\mathcal{G}$ over the field $\mathbb{F}$ has the generator matrix G. If the rows of a $(n - k) \times n$ matrix M span $\mathcal{G}^\perp$ we write $G^\perp = M$. We will identify $x \in \mathbb{F}^n$ with $(x_1, \cdots, x_n), x_i \in \mathbb{F}$ for $i = 1, \cdots, n$. For any (ordered) subset $\{j_1, \cdots j_m\} =: J \subseteq \{1, \cdots n\}$ we denote the vector $(x_{j_1}, \cdots, x_{j_m}) \in \mathbb{F}^m$ with x_J. Similarly, for a $k \times n$ matrix M we denote by $M_{\cdot J}$ the submatrix consisting of the columns corresponding to the indices of J and write $M_{J'\cdot} = \left(\left(M^\top\right)_{\cdot J'}\right)^\top$ for any (ordered) subset J' of $\{1, \cdots, k\}$. Block matrices will be given in brackets.

3 The GPT Cryptosystem

The GPT cryptosystem was first presented in 1991 by Gabidulin, Paramonov and Tretjakov [7]. Here we present a more generalized version (GGPT, see [11]), which may be used to describe the original GPT cryptosystem as well as the variant with column scrambler from [3].

- **System Parameters:** $q, k < n \leq m$, $s \leq t \in \mathbb{N}$, where $t < n - k - 1$.
- **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

  $$\begin{aligned} G' &= S\left(\left[X \middle| 0\right] + G\right)T \\ &= S\left[G_{\cdot\{1,\cdots,t\}} + X \middle| G_{\cdot\{t+1,\cdots,n\}}\right] T \in \mathbb{F}_{q^m}^{k \times n} \ , \end{aligned} \tag{2}$$

  where 0 denotes the $k \times (n-t)$ zero matrix. Choose $1 \leq e \leq \frac{n-k-t}{2}$. Further let $\mathcal{D}_\mathcal{G}$ be an efficient decoding algorithm for the Gabidulin code $\mathcal{G}$ generated by the matrix $G_{\cdot\{t+1,\cdots,n\}}$.
- **Public Key:** (G', e)
- **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 e at random and compute the ciphertext c as follows:

  $$c = xG' + z \ .$$

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

  $$xSG_{\{t+1,\cdots,n\}} = \mathcal{D}_\mathcal{G}\left(c'\right) \ .$$

  Now, we can compute the plaintext x.

In the original GPT cryptosystem, the parameterse e and t are chosen such that $e = \frac{n-k}{2} - t$. If we do 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 c.

The distortion matrix X is essential to mask the structure of G. We can recover the vector gT from SGT in $\mathcal{O}\left(k^3\right)$ 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 [4]). If the parameter s should be larger than $t/2$, as there exists a polynomial time attack on the private key [8]. In all examples we will choose $n = m$ and $q = 2$. Some parameter sets may be found in table 3 (All of these are secure against all previously published attacks).

3.1 The Niederreiter Variant of GPT

The security of the GGPT cryptosystem is strongly connected to the one of the Niederreiter variant, as we will see later on. We briefly introduce the Niederreiter variant of the GPT cryptosystem from [2]. 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

$$(H') = \left[H \middle| A\right] S \in \mathbb{F}_{q^m}^{n\times(n-k+l)},$$

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 $(H', e = (n-k)/2)$ 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 e, compute the ciphertext c as follows:

$$c = xH' \ .$$

In order to decode a ciphertext c apply the syndrome decoding algorithm $\mathcal{D}_\mathcal{G}$ for $\mathcal{G}$ to the syndrome build from the first $n-k$ columns of cS^{-1}. Table 1 shows public key sizes and approximate work factors (WF = operations over $\mathbb{F}_q$) for the fastest general decoding attack. Parameters were taken from [1].

Table 1. Parameter sets for the Niederreiter GPT

Parameters			Size Public	WF general
m	k	l	Key (Bytes)	decoding
25	15	5	469	2^{82}
32	24	4	960	2^{93}

4 Attacking the GPT Cryptosystem

Even though there were attempts to break the GPT cryptosystem by using general rank distance decoding algorithms, the structural attacks from Gibson (see e.g. [4], [8]) had more impact on the cryptosystem. However, for carefully chosen parameter sets, Gibson's attacks have exponential running time (see appendix). Several variants of GPT were proposed, but it was shown, that the security of the variants from [3] and [6] is connected to the security of GGPT (see [11]). The attempt to use Gibson's attack to cryptanalyze these variants failed for the variant from [6], but resulted in an attack for the variant from [3].

The main weakness of the GPT cryptosystem is, that it is difficult to hide the structure of the generator matrix of a Gabidulin code. As already noted by Gibson, the use of subfield subcodes (or group codes) seems much more promising for cryptographic applications. Here, we want to use some observations on Gabidulin codes: For a matrix M let $M^{[j]}$ denote the result of rising every element of M to the power of j. 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.) We are going to use this property to distinguish the Gabidulin part of the public code from the random one.

Let M be an arbitrary $l \times n$ matrix over $\mathbb{F}_{q^m}$ and $f \in \mathbb{N}$. While Gibson analyzed matrices of the form $M + M^{[q]}$ (compare [8]), we look at matrices of the form

$$\Lambda_f(M) := \begin{bmatrix} M \\ (M)^{[q]} \\ \vdots \\ (M)^{\left[q^f\right]} \end{bmatrix} \in \mathbb{F}_{q^m}^{((f+1)\cdot l)\times n}. \tag{3}$$

Lemma 1. *If $M \in \mathbb{F}_{q^m}^{l\times n}$ 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.*

Assumption 1. *Let $M \in \mathbb{F}_{q^m}^{l\times n}$ define a random $l > 1$ dimensional subcode of an (n,k) Gabidulin code over $\mathbb{F}_{q^m}$ with generator vector g. Then with probability $\mathcal{P}_1 \geq (1-q^{-m})$, $\Lambda_f(M)$ defines a* $\min\{k+f,(f+1)\cdot l\}$ *dimensional subcode of the $(n,k+f)$ Gabidulin code with generator vector g.*

Assumption 2. *Let $M \in \mathbb{F}_{q^m}^{l\times n}$ be a random matrix of full rank over $\mathbb{F}_{q^m}$ and of full column rank over $\mathbb{F}_q$. Then $\Lambda_f(M)$ has rank* $\min(n, f\cdot l)$ *with probability $\mathcal{P}_2 \geq (1-q^{-(m-1)})$.*

The proof for lemma 1 is obvious. For assumption 1, it is easy to see, that $\Lambda_f(M)$ defines a subcode of the $(n,k+f)$ Gabidulin code with generator vector g, so the remaining part is to estimate $\mathcal{P}_1$. Assumption 2 is based on empirical results as well as on observations from [5]. If $l = 1$, then because of theorem 1, the assumption is true, as $\mathcal{P}_2 = 1$. Experiments for parameters relevant for our attacks showed that $\mathcal{P}_1$ and $\mathcal{P}_2$ are almost 1 (see appendix). However, not the correctness, but only the success probability of the attacks proposed in the following sections depends on the assumptions above.

4.1 Attacking the Niederreiter Variant

The Niederreiter variant of the GPT cryptosystem was first attacked by A. Ourivski in [10]. Here we present a new attack, which recovers an alternative secret key in polynomial time by using assumption 1.

Theorem 1. *Let $\mathcal{G}_{\mathrm{SUB}}$ be a random $k-l$ dimensional subcode of an (n,k) Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^m}$ with generator vector g. Then we may recover g from $\mathcal{G}_{\mathrm{SUB}}$ with probability $\mathcal{P}_1$ if $k-l > 1$ and $n-k-1 \geq \lceil l/(k-l-1)\rceil$. Further, this may be done in $\mathcal{O}\left(n^3\right)$ operations over $\mathbb{F}_{q^m}$.*

Proof. Let G' 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 $n-k-1 \geq f \geq \lceil l/(k-l-1)\rceil$. If assumption 1 holds, $\Lambda_f(G')$ has rank $k+f$ with probability $\mathcal{P}_1$ and defines a subcode of a $(n,k+f)$ Gabidulin code. Thus, with probability $\mathcal{P}_1$, $\Lambda_f(G')$ spans the $(n,k+f)$ Gabidulin code with generator vector g and we can recover g in $\mathcal{O}\left((k+f)^3\right)$ operations over $\mathbb{F}_{q^m}$ (see [4]).

It follows, that if assumption 1 holds, we can recover the secret Gabidulin code $\mathcal{G}$ from the public key of an instance of the Niederreiter variant of GPT as long as $n-k-1 \geq \lceil l/(k-l-1) \rceil$. Let H be the check matrix of $\mathcal{G}$. To obtain an equivalent secret key, we can choose a set J of l columns of H', s.t. the matrix $\left[H \middle| H'_{\cdot J} \right]$ has full rank. Now we may solve the equation

$$H' = \left[H \middle| H'_{\cdot J} \right] \bar{S}$$

for $\bar{S}$ and obtain the alternative secret key $\left(\mathcal{G}, \bar{S}\right)$. Note, that employing this method, it only takes $\mathcal{O}\left((k+f)^3\right)$ operations over $\mathbb{F}_{q^m}$ to recover an alternative secret key.

For the parameter sets proposed e.g. in [1], the choice of $f = 1$ showed to be sufficient in all our experiments. Table 2 shows modified parameter sets for which the presented attack does not work. These parameters are not necessarily secure (see [10]).

Table 2. Modified parameter sets for the Niederreiter GPT

Parameters			Public Key	WF general
m	k	l	Size (Bytes)	decoding
32	24	20	448	2^{93}
64	52	47	2360	2^{288}

4.2 Attacking the GPT Cryptosystem

To recover an alternative secret key from the public key (G', e) of an instance of the GGPT cryptosystem, we want to use assumption 2. The general idea is, to observe the behavior of the matrix $\Lambda_f(G')$. We assume, that if the difference of the rank of $\Lambda_f(G')$ and $\Lambda_{f+1}(G')$ is only 1 for some f, then $\Lambda_f(G')$ will be strongly connected to a Gabidulin code. The following theorem describes the connection:

Theorem 2. *Let (G', e) be the public key of an instance of the GGPT cryptosystem with parameters q, m, n, k, t and s. Further, let (G, S, T) be the corresponding secret key. Then for $0 \leq f \leq n-t-k-1$, there exists a dual matrix of $\Lambda_f(G')$ of the form*

$$\Lambda_f(G')^{\perp} = \begin{bmatrix} 0 & H_f^{\top} \\ B_1 & B_2 \end{bmatrix} \cdot \left(T^{-1}\right)^{\top} \in \mathbb{F}_{q^m}^{(n-t-k-f+l)\times n}, \tag{4}$$

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

$$\Lambda_f\left(G'\right) = \left[\, \Lambda_f\left(G_{\cdot\{1,\cdots,t\}} + X\right) \middle| \Lambda_f\left(G_{\cdot\{t+1,\cdots,n\}}\right) \right] \in \mathbb{F}_{q^m}^{(kf)\times n}$$

By assumption 2, the last $n-t$ columns of $\Lambda_f\left(G'\right)$ define an $(n-t, k+f)$ Gabidulin code $\mathcal{G}_f$. Thus the subvectorspace spanned by the rows of

$$\left[\, 0 \middle| H_f^\top \right] \in \mathbb{F}_{q^m}^{(n-t-k-f)\times n},$$

where $H_f \in \mathbb{F}_{q^m}^{(n-t)\times(n-t-k-f)}$ is the check matrix of $\mathcal{G}_f$, is in the dual space of $\Lambda_f\left(G'\right)$. To get a matrix which defines the whole dual space of $\Lambda_f\left(G'\right)$, we might have to add some more rows to $\left[\, 0 \middle| H_f^\top \right]$. However, it is clear, that there will be at most t rows missing, as $\Lambda_f\left(G'\right)$ has at least rank $k+f$. This proves the theorem.

Observe, that $\mathcal{G}_f$ is uniquely defined by the secret key and f. Thus, knowing H_f for some f, we know all H_i for $0 \leq i \leq n-k-t-1$. We are going to determine the rank of $\Lambda_f\left(G'\right)^\perp$ in the following sections. For now, we assume, that it will be very near its lower bound $(n-t-k-f)$ and show, how to recover an alternative secret key in that case (compare example in the appendix).

Theorem 3. *Let (G', e) be as in theorem 2. Given an $f \leq n-t-k-1$ s.t. the rank of $\Lambda_f\left(G'\right)^\perp$ is $n-t-k-f$, then we may recover an alternative secret key, corresponding to G' in $\mathcal{O}\left(n^3\right)$ operations over $\mathbb{F}_{q^m}$.*

Proof. With the conditions above, it follows from theorem 2, that there is a matrix $\Lambda_f\left(G'\right)^\perp$ of the form

$$\left[\, 0 \middle| H_f^\top \right] \left(T^{-1}\right)^\top \in \mathbb{F}_{q^m}^{(n-t-k-f)\times n},$$

where H_f is as in theorem 2. We can recover such a matrix in $\mathcal{O}\left(n^3\right)$ operations over $\mathbb{F}_{q^m}$ [4]. Now we can choose a set N_1 of $n-t$ rows of G' s.t. $\Lambda_f\left(G'\right)^\perp_{\cdot N_1}$ is of column rank $n-t$ over $\mathbb{F}_q$. It follows, that $T_{N_1 N_2}$ with $N_2 = \{t+1, \cdots, n\}$ is invertible. We may assume without loss of generality that $N_1 = N_2$ and $H_f^\top = \Lambda_f\left(G'\right)^\perp_{\cdot N_1}$. Let $\tilde{T} \in \mathbb{F}_q^{t\times(n-t)}$ be the solution of the equation

$$\Lambda_f\left(G'\right)^\perp_{\cdot\{1,\cdots,t\}} = H_f^\top \cdot \tilde{T}^\top$$

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

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

where Id_k denotes the k-dimensional identity matrix. We may recover H_0 from H_f, as both are uniquely determined by G' and $\bar{T}$. It follows, that $\left[\, 0 \middle| H_0 \right]$ is in the dual space of $G'\bar{T}^{-1}$, and thus the last $n-t$ columns of $G'\bar{T}^{-1}$ define an $(n-t, k)$ Gabidulin code. Thus $\bar{T}$ serves as an alternative column scrambler. Now, we may obtain an equivalent secret key in $\mathcal{O}\left(k^3\right)$ operations by applying the methods from [4] to $\left(G' \cdot \bar{T}^{-1}\right)_{\cdot\{t+1,\cdots,n\}}$, which gives us an alternative row scrambler $\bar{S}$.

However, even if the rank of $\Lambda_f\left(G'\right)$ is larger than $n-t-k-f$, an attacker still may try to recover the secret key. He could guess a set N_1 of $n-t$ rowss.t. ($\left[\, 0 \middle| H_f \right] \left(T^{-1}\right)^\top$)$_{\cdot N_1}$ has full column rank over $\mathbb{F}_q$. Again we may assume w.l.o.g. that $N_1 = N_2$ and $\left(T^{-1}\right)_{N_1 N_2} = \mathrm{Id}_{n-t}$. Then, the matrix $\left(\Lambda_f\left(G'\right)^{\perp}_{\cdot N_1}\right)^{\top}$ corresponds to an instance of the Niederreiter version of GPT as long as $k + f - l > 1$. Thus, we might apply the attacks on the Niederreiter variant of GPT, to recover $\left[H_f \middle| B_2^{\top}\right]$. If one of the attacks succeeds, an attacker can recover a dual matrix of $\Lambda_f\left(G'\right)$ of the form given in equation (4) and from it an alternative column scrambler. Afterwards the attacker would be able to construct a valid alternative private key.

4.3 Strengths of the New Attack

Given an f s.t. the conditions of theorem 3 are fulfilled, for the GGPT public key, we can build an alternative private key in $\mathcal{O}\left(m^5\right)$ operations over $\mathbb{F}_q$. By now, we have no idea, for which parameter sets our attack might work. To estimate the success probability of our attack, we will have to determine the size of $\Lambda_f\left(G'\right)^{\perp}$. In the following we assume that $s < k$.

Theorem 4. *Let (G', e) be as in theorem 2. If assumption 2 holds for $s \times t$ matrices over $\mathbb{F}_{q^m}$, then the rank of the dual matrix of $\Lambda_f\left(G'\right)$ is at most $R = n - k - f - \min\{t, fs\}$ with probability $\mathcal{P}_2$.*

Proof. **(Theorem 4)** We have to estimate the rank of $\Lambda_f\left(G'\right)$ for given $G' = S\left(\left[X \middle| 0\right] + G\right)T$ and f (see equation 2). To simplify notations, we define the following matrices:

$$M_k := \begin{bmatrix} 0 & \mathrm{Id}_{(k-1)} \\ 0 & 0 \end{bmatrix} \in \mathbb{F}_{q^m}^{k \times k},\ \gamma_i := \left(\left[X \middle| 0\right] + G\right)_{k\cdot}^{[q^i]} \in \mathbb{F}_{q^m}^{1 \times n} \text{ and}$$

$$\tilde{X}_i := \left(X^{[q^{i-1}]}\right)_{\cdot\{2,\cdots,k\}} + \left(X^{[q^i]}\right)_{\cdot\{1,\cdots,k-1\}} \in \mathbb{F}_{q^m}^{k-1 \times t}.$$

To determine the rank of $\Lambda_f\left(G'\right)$ we use the property: If G is of the form in equation (1), then 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 $0 \leq i \leq f-1$ and $1 \leq j \leq k-1$. Thus, by removing the influence of S from $\Lambda_f\left(G'\right)$ and adding the rows as mentioned above by using M_k, we get the following matrix of the same rank as $\Lambda_f\left(G'\right)$:

$$\begin{bmatrix} \mathrm{Id}_k & 0 & \cdots & 0 \\ M_k & \mathrm{Id}_k & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & M_k & \mathrm{Id}_k \end{bmatrix} \cdot \begin{bmatrix} S^{[q^0]} & 0 & \cdots & 0 \\ 0 & S^{[q^1]} & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & S^{[q^f]} \end{bmatrix}^{-1} \cdot \Lambda_f\left(G'\right)$$

$$= \left[\begin{array}{cc} X + G_{\cdot\{1,\cdots,t\}} & G_{\cdot\{t+1,\cdots,n\}} \\ \hline \tilde{X}_1 & 0 \\ \hline \multicolumn{2}{c}{\gamma_1} \\ \hline \vdots & \vdots \\ \hline \tilde{X}_f & 0 \\ \hline \multicolumn{2}{c}{\gamma_f} \end{array}\right] \cdot T \in \mathbb{F}_{q^m}^{((f+1)\cdot k) \times n}.$$

With probability $\mathcal{P}_2$ the part of the matrix above build from the $[\tilde{X}_i\, 0]$ contains at least $\min\{t, fs\}$ linearly independent rows, as $(\tilde{X}_i)^{[q]} = \tilde{X}_{i+1}$ and $\operatorname{rank}(X_i) = s$. Therefore $\Lambda_f(G')$ has at least rank $k + f + \min\{t, fs\}$ with probability $\mathcal{P}_2$.

Note, that for $s = 1$ assumption 2 is correct, and the probability in the theorem above gets 1. Otherwise the conditions in theorem 3 are fulfilled with probability $\mathcal{P}_2$. We conclude, that all parameter sets, where there exists an $f \leq n - k - t - 1$, s.t. $t \leq fs$ are insecure. Furthermore, as $s \geq 1$, we may obtain a equivalent secret key from the public key with probability 1 for all parameter sets where

$$t \leq n - k - t - 1 \iff 1/2 \leq (n-k)/2 - t \ , \tag{5}$$

even if $s > 1$. This is true for all instances of the original GPT cryptosystem.

4.4 Experimental Results

Table 3 shows absolute run times the attack by methods from theorem 3 in comparison to the theoretical work factors (operations over $\mathbb{F}_q$) of the previous attacks. For all parameter sets we chose $f = n-t-k-1$. In our experiments our attack did not fail for any random instance of the original GPT cryptosystem. Operations were performed on a 500MHz Pentium III running Linux using an implementation in Java.

Table 3. Attacking the GPT cryptosystem

Parameters				average runtime	WF best of	WF general
m	k	t	s	of our attack	Gibson's attacks	decoding
48	10	16	3	51 min	2^{139}	2^{134}
48	16	18	4	58 min	2^{200}	2^{124}
48	24	8	2	102 min	2^{122}	2^{198}

In our experiments we chose X as the product of a random $k \times s$ matrix S_X of rank $s < k$ over $\mathbb{F}_{q^m}$ and a random $s \times t$ matrix $\bar{X}$ (of rank s over $\mathbb{F}_{q^m}$ and rank t over $\mathbb{F}_q$). For such choices of X the matrix $\Lambda_f(G')$ almost always had rank $(k + f + (s+1) \cdot \min(f, s) + s \cdot \max(0, f - s))$ or $k+f+t$. For special choices of S_X and random $\bar{X}$, we were able to create instances, where the rank of $\Lambda_f(G')$ reached the bound R. However, choosing S_X or $\bar{X}$ of a special form removes degrees of freedom in choosing the private key and thus does not seem to be a good choice.

4.5 On Secure Instances of GGPT

We have seen, that instances of the GPT cryptosystem and its variants, where

$$t \leq s \cdot (n - t - k - 1)$$

holds, are insecure if assumption 2 holds. For the GGPT variant 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 we can choose an f s.t. $k+f-t+fs > 1$, as described in section 4.2.

To get secure instances of the GGPT cryptosystem, one could try to choose parameters in a way, such that $t-fs > f+k$ for every possible choice of f. The latter is the case, e.g. if

$$s \leq \frac{2t-n}{n-t-k} \ .$$

A parameter set satisfying this condition would be $n = m = 64$, $k = 8$, $t = 40$ and $s = 1$ e.g. with a public key size of 3584 bytes. The attack in the given form is not applicable for such parameter sets. However, it seems very likely that the attack may be modified in such a way, that these parameter sets can be attacked, too.

5 Conclusion

We conclude that the original GPT cryptosystem from [7] is broken by our attack. Our attacks succeed with good probability for most parameter sets of GGPT and can even be extended to other variants of the GPT cryptosystem (compare [6], [11] and [3]). After several attacks on the GPT cryptosystem and its variants, it seems to be difficult to name secure parameter sets for GGPT, if there exist any. Even if we would consider the parameter set mentioned above to be secure, the GPT cryptosystem looses much of its advantages over the McEliece cryptosystem.

References

1. T.P. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. *Designs, Codes and Cryptography*, 35 (1), 2005.
2. T.P. Berger and P. Loidreau. Security of the Niederreiter form of the GPT public-key cryptosystem. In *IEEE International Symposium on Information Theory, Lausanne, Suisse*. IEEE, July 2002.
3. E. M. Gabidulin and A. V. Ourivski. Column scrambler for the GPT cryptosystem. *Discrete Applied Mathematics*, 128(1):207–221, 2003.
4. 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, 1995.
5. E.M. Gabidulin and P. Loidreau. Subfield subcodes of maximum-rank distance codes. In *Seventh International Workshop on Algebraic and Combinatorial Coding Theory*, volume 7 of *ACCT*, pages 151–156, 2000.
6. E.M. Gabidulin, A.V. Ourivski, B. Honary, and B. Ammar. Reducible rank codes and their applications to cryptography. *IEEE Transactions on Information Theory*, 49(12):3289–3293, 2003.
7. E.M. Gabidulin, A.V. Paramonov, and O.V. Tretjakov. Ideals over a non-commutative ring and their applications to cryptography. In *Proc. Eurocrypt '91*, volume 547 of *LNCS*. Springer Verlag, 1991.

8. K. Gibson. The security of the Gabidulin public key cryptosystem. In *Proc. of Eurocrypt'96*, volume 1070 of *LNCS*, pages 212–223. Springer Verlag, 1996.
9. T. Johansson and A.V. Ourivski. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38, No. 3:237–246, 2002.
10. A.V. Ourivski. Recovering a parent code for subcodes of maximal rank distance codes. In *Proc. of WCC 03*, pages 357–363, 2003.
11. R. Overbeck. Extending Gibson's attacks on the GPT cryptosystem. In *Proc. of WCC 2005*, pages 382–391, 2005.

A Appendix - Gibson's Attacks

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

(i) $\hat{G}$ is a generator matrix of an (n,k) Gabidulin code over $\mathbb{F}_{q^m}$,
(ii) $G' = \hat{S}\left(\hat{G} + \hat{X}\right)$ and
(iii) the rank of $\hat{X}$ 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 $\hat{X}$. Gibson's first attack was developed for the case that the GGPT parameter s is 1, but may be adapted to the case where $s \neq 1$ (see [4]). It takes

$$\mathcal{O}\left(m^3\,(n-k)^3\,q^{ms}\right) \tag{6}$$

operations over $\mathbb{F}_{q^m}$. In [8] Gibson presented a different attack, which is more efficient for larger values of s. It requires that $k+t+2 \leq n$ and runs in

$$\mathcal{O}\left(k^3 + (k+t)\,f \cdot q^{f(k+2)} + (m-k)\,t \cdot q^f\right) \tag{7}$$

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).

B Appendix - On Assumption 1

Besides our experimental results, we want to give some intuition, why assumption 1 seems to be reasonable. Let $G' = \bar{S}G$, where $\bar{S} \in \mathbb{F}_{q^m}^{(k-l)\times k}$ is of full rank and G is the generator matrix of the (n,k) Gabidulin code with generator vector g.

Now G' defines a subcode of the code generated by G. Let $\bar{G}$ be the generator matrix of the $(n, k+f)$ Gabidulin code with generator vector g. We may write

$$(G')^{[q^i]} = [\,\underbrace{\mathbf{0}|\cdots|\mathbf{0}}_{i \text{ times}}\,|\bar{S}^{[q^i]}|\,\underbrace{\mathbf{0}|\cdots|\mathbf{0}}_{f-i \text{ times}}\,]\,\bar{G} \in \mathbb{F}_{q^m}^{(k-l)\times n}\ ,$$

where $\mathbf{0}$ is the $k \times 1$ matrix with only zero entries. Then $\Lambda_f\,(G')$ may be written as

$$\Lambda_f\,(G') = \underbrace{\begin{bmatrix} \bar{S} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \bar{S}^{[q]} & & \vdots \\ \vdots & & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \bar{S}^{[q^f]} \end{bmatrix}}_{=:S} \bar{G} \in \mathbb{F}_{q^m}^{(f+1)(k-l)\times n}.$$

If $\bar{S}$ is a random matrix, then S seems to be of full rank, with high probability. In our experiments we did not find any counterexamples for randomly generated matrices $\bar{S}$, where we chose (n, k) Gabidulin codes with $n \geq 8$, $k \geq 4$ and the dimension of the subcode to be $l \geq 2$.

C Appendix - On Assumption 2

In order to estimate the probability $\mathcal{P}_2$ in assumption 2 we made several experiments for random matrices M. In all our experiments, we build $\Lambda_f\,(M)$ for all $1 \leq f \leq \lceil m/l \rceil$, where m is the extension degree of the field, and l is the rank of the matrix M. Table 4 shows the resulting probability estimates. We conclude, that it is reasonable to assume, that $1 - \mathcal{P}_2$ decreases exponentially fast with growing m.

Table 4. Experimental results for assumption 2

rows	columns	field	$\mathcal{P}_2$ estimate	# experiments
2	6	$\mathbb{F}_{q^6}$	$1 - 0.0289$	10000
2	6	$\mathbb{F}_{q^8}$	$1 - 0.0050$	10000
2	6	$\mathbb{F}_{q^{10}}$	$1 - 0.0010$	10000
2	8	$\mathbb{F}_{q^{10}}$	$1 - 0.0008$	10000
2	10	$\mathbb{F}_{q^{10}}$	$1 - 0.0018$	10000
3	10	$\mathbb{F}_{q^{10}}$	$1 - 0.0$	10000
4	10	$\mathbb{F}_{q^{10}}$	$1 - 0.0$	10000
5	10	$\mathbb{F}_{q^{10}}$	$1 - 0.0013$	10000
2	8	$\mathbb{F}_{q^{16}}$	$1 - 0.000033$	30000
2	10	$\mathbb{F}_{q^{16}}$	$1 - 0.0$	30000

D Appendix - A Small Example

For a better understanding of the attack on the GGPT cryptosystem presented in the previous sections, we provide an example with small parameters: $q = 2$, $m = n = 5$, $k = 2$, $t = s = 1$. As field we choose $\mathbb{F}_{q^5} = \mathbb{F}_2 / \left(X^5 + X^2 + 1\right)$. We write the elements of this field in their polynomial representation, thus $X^3 + 1 \hat{=} 01001$.

Assume, that we are given a public key (G', e) with $e = 1$ and

$$G' = \begin{pmatrix} 10101\ 10011\ 00111\ 01011\ 01111 \\ 00010\ 11001\ 10000\ 10011\ 00011 \end{pmatrix} .$$

The (unknown) secret key is (G, S, T) with

$$S = \begin{pmatrix} 10000\ 10100 \\ 01000\ 10000 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1\ 0\ 1\ 1\ 1 \\ 0\ 1\ 0\ 0\ 0 \\ 1\ 1\ 0\ 1\ 1 \\ 0\ 1\ 1\ 1\ 0 \\ 1\ 0\ 0\ 0\ 0 \end{pmatrix} .$$

To recover an alternative secret key, an attacker would choose the parameter $f = n - k - t - 1 = 1$ and build

$$\Lambda_f\left(G'\right) = \begin{pmatrix} 10101\ 10011\ 00111\ 01011\ 01111 \\ 00010\ 11001\ 10000\ 10011\ 00011 \\ 11100\ 01000\ 10101\ 01111\ 11111 \\ 00100\ 00110\ 01101\ 01000\ 00101 \end{pmatrix} .$$

The dual of $\langle \Lambda_f\left(G'\right) \rangle$ is defined by

$$\Lambda_f\left(G'\right)^{\perp} = \begin{pmatrix} 00100\ 01110\ 01100\ 01001\ 00001 \end{pmatrix} .$$

The attacker observes, that the last 4 columns of $\Lambda_f\left(G'\right)^{\perp}$ are linearly independent over $\mathbb{F}_2$, which is the rank of $\Lambda_f\left(G'\right)^{\perp}$ over $\mathbb{F}_2$. The legitimate user would be able to compute

$$\Lambda_f\left(G'\right)^{\perp} T^{\top} = \left[0 \middle| H_1\right] = \begin{pmatrix} 00000\ 01110\ 00010\ 01011\ 00100 \end{pmatrix} .$$

The attacker on the other hand can choose

$$\left(\ \Lambda_f\left(G'\right)^{\perp}\ \right)_{\{2,\cdots,5\}} = \begin{pmatrix} 01110\ 01100\ 01001\ 00001 \end{pmatrix}$$

to be his H_1. (He could choose any other submatrix of column rank 4 over $\mathbb{F}_2$, and each would lead to a different alternative secret key.) As a solution to the equation $(00100) = H_1 \tilde{T}^{\top}$ the attacker gets $\tilde{T} = \begin{pmatrix} 0\ 1\ 1\ 1 \end{pmatrix}$. Now,

$$G' \cdot \begin{bmatrix} 1 & \tilde{T} \\ 0 & \mathrm{Id}_4 \end{bmatrix}^{-1} = \begin{pmatrix} 10101\ 10011\ 10010\ 11110\ 11010 \\ 00010\ 11001\ 10010\ 10001\ 00001 \end{pmatrix} .$$

The last four columns of the matrix above define a Gabidulin code with generator vector $\begin{pmatrix} 01010\ 01001\ 00100\ 00001 \end{pmatrix}$. Thus, the attacker gets the row scrambler

$$\bar{S} = \begin{pmatrix} 11001\ 00011 \\ 11110\ 11111 \end{pmatrix}$$

and obtains a working alternative secret key.