Decoding Interleaved Gabidulin Codes and Ciphertext-Security for GPT variants
(preprint)

R. 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 view interleaved Gabidulin codes and describe how to correct errors up to a rank equal to the amount of redundancy of the code with high probability. We give a detailed proof for our estimation of the probability of correct decoding. In a second part, we view the application to variants of the GPT cryptosystem. For GGPT this leads to an efficient attack on the remaining secure instances, whereas it allows to derive at least partial information of the plaintext in the case of RRC-GPT.

Keywords: Interleaved codes, rank distance codes, code based cryptography, public key cryptography.

1 Introduction

Decoding beyond minimum distance is an important issue in coding theory. Recently it was shown, how to use interleaved codes to allow error correction beyond minimum distance in the case of GRS codes with high probability [1], [2]. This concept may be extended for interleaved Gabidulin codes [8], which are rank distance codes. In the first part of this paper, we present one of the possible decoding methods for (n, k) interleaved Gabidulin codes, which allows to correct errors of rank up to $\frac{r}{r+1}(n-k)$, where r is the *amount of interleaving*. Further, we give an upper bound for the probability of correct decoding ($1-4/q^m$, where $m \geq n$).

An application of this new decoding procedure is an attack on variants of the GPT cryptosystems, which we present in the second part of the paper. The GPT cryptosystem uses Gabidulin codes and is a variant of the cryptosystem based on error correcting codes presented 1978 by McEliece. While McEliece's cryptosystem remains unbroken for large public key sizes, the GPT cryptosystem was broken in 2005 [9]. Nevertheless, some variants of the GPT cryptosystem like GGPT and RRC-GPT resisted the attack, although parameters had to be modified. We show, that even for the modified parameter sets GGPT is insecure against our new attack. Further, this new attack allows to reveal at least partial information about the plaintext in the case of RRC-GPT.

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. In this section we recall the basic facts and give the notation used in the following sections.

Definition 2.1. *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 $\|\cdot\|_r$ is defined as follows:*

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

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

In [7] 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. For ease of notation we introduce the operator λ_f, which maps a matrix $M = (m_{ij})$ to a blockmatrix:

$$\begin{aligned} \lambda_f : \mathbb{F}_{q^m}^{m\times n} &\to \mathbb{F}_{q^m}^{mf\times n} \\ M &\mapsto \begin{bmatrix} M \\ M^{[q]} \\ \vdots \\ M^{[q^f]} \end{bmatrix}, \end{aligned}$$

where $M^{[x]} := (m_{ij}^x)$.

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

$$G = \lambda_{k-1}(g) . \tag{1}$$

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 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 $\mathcal{G}$). 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. A error correction algorithm based on the "right Euclidian division algorithm" runs in $\mathcal{O}\left(d\log_2^2 d + dn\right)$ operations over $\mathbb{F}_{q^m}$ for (n,k,d) Gabidulin codes [4]. Another nice property of Gabidulin codes is, that the dual code of an (n,k) Gabidulin code is a $(n,n-k)$ Gabidulin code:

Lemma 2.1. *Let $\mathcal{G}$ be an (n,k) Gabidulin code over $\mathbb{F}_{q^m}$ with generator vector g. Then $\mathcal{G}$ has a check matrix of the form*

$$H = \lambda_{n-k-1}\left(h_1^{1/q^{n-k-1}}\ h_2^{1/q^{n-k-1}}\ \cdots\ h_n^{1/q^{n-k-1}}\right)^\top \in \mathbb{F}_{q^m}^{n-k\times n}.$$

Further, the vector $h = \begin{pmatrix} h_1\ h_2\ \cdots\ h_n\end{pmatrix}$ is uniquely determined by g (independent from k) up to a scalar factor $\gamma \in \mathbb{F}_{q^m}\setminus\{0\}$. We will call h a check vector.

Proof. It is sufficient to prove, that if $\tilde{h}$ is in the dual space of the (n,k) Gabidulin code $\mathcal{G}_k$ with generator vector g, then $\tilde{h}^{[1/q]}$ is in the dual space of the $(n,k-1)$ Gabidulin code $\mathcal{G}_{k-1}$ with generator vector g:

$$\tilde{h} \in \mathcal{G}_k^\perp \Leftrightarrow \forall_{i\in\{0,\cdots,k-1\}} \sum_{j=1}^n \tilde{h}_j g_j^{q^i} = 0 \Rightarrow \forall_{i\in\{1,\cdots,k-1\}} \sum_{j=1}^n \tilde{h}_j^{1/q} g_j^{q^{i-1}} = 0.$$

If $h^{[q^{n-k-1}]}$ is the check vector of $\mathcal{G}$ and $\mathbb{F}$ is a subfield of $\mathbb{F}_{q^m}$, then the $\mathbb{F}$-subcode of $\mathcal{G}$ has check matrix $\lambda_{n-k-1}\left(\ h_{\mathbb{F}}\ \right)$, where the matrix $h_{\mathbb{F}}$ represents h over $\mathbb{F}$.

Throughout this paper we will use the following notation. We write $\mathcal{G} = \langle G\rangle$ if the linear (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 $G^\perp = M$. With this notation $M^\top$ is a check matrix of $\mathcal{G}$. 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, we denote by $M_{\cdot J}$ the submatrix of a $k\times n$ matrix M consisting of the columns corresponding to the indices of J and $M_{J'\cdot} = \left(\left(M^\top\right)_{\cdot J'}\right)^\top$ for any (ordered) subset J' of $\{1,\cdots,k\}$. Block matrices will be given in brackets.

Remark 2.1. Let J be a selection of $n' > k$ columns of the generator matrix G of an (n,k) Gabidulin code. Then $G_{\cdot J}$ defines an (n',k) Gabidulin code.

3 Interleaved Gabidulin Codes

In this section we introduce the general concept of interleaved codes. To do so, we define the mapping

$$\phi : \mathbb{F}_{q^{rm}} \rightarrow \mathbb{F}_{q^m}^r\ .$$

Starting from a (n,k,d) code $\mathcal{G}$ over $\mathbb{F}_{q^m}$ with generator matrix G, we build a (n,k) code $\mathcal{G}_{\mathrm{I}}$ over $\mathbb{F}_{q^{rm}}$ in the following way: The message $(x_1,\cdots,x_k) \in \mathbb{F}_{q^{rm}}^k$ will be converted into r codewords of $\mathcal{G}$:

$$y_i = (\phi(x_1)_i, \phi(x_2)_i, \cdots, \phi(x_k)_i)\, G \ , \ i = 1, \cdots, r$$

Then, these r codewords will be converted into a single one of length n over $\mathbb{F}_{q^{rm}}$, where at the j-th position we put the entry

$$z_j = \phi^{-1}\left((y_{1j}, y_{2j}, \cdots, y_{rj})\right) \ .$$

The interleaved code $\mathcal{G}_{\mathrm{I}}$ is the code consisting of all vectors $z \in \mathbb{F}_{q^{rm}}^n$, which can be generated in this way. Obviously, $\mathcal{G}_{\mathrm{I}}$ is an $\mathbb{F}_{q^m}$-linear (n,k,d) code over $\mathbb{F}_{q^{rm}}$. The parameter r is called the amount of interleaving.

3.1 Standard error correction

For a simple error correction we re-transform the received word $(\tilde{z}_1, \tilde{z}_2, \cdots, \tilde{z}_n)$ into r codewords of $\mathcal{G}$:

$$\tilde{y}_i = (\phi(\tilde{z}_1)_i, \phi(\tilde{z}_2)_i, \cdots, \phi(\tilde{z}_n)_i) \ , \ i = 1, \cdots, r$$

Now, one could use an error correction algorithm for $\mathcal{G}$ to correct the errors in all codewords, to recover the original y_i and obtain the partial messages $(\phi(x_1)_i, \phi(x_2)_i, \cdots, \phi(x_k)_i)$, which we re-transform into the original message x.

3.2 Correcting rank errors beyond minimum distance

In [8] the authors present two algorithms for correcting random rank errors beyond minimum distance in interleaved Gabidulin codes. Here, we present the probabilistic algorithm, the success probability of which depends on the input, only.

Let $\mathcal{G}_{\mathrm{I}}$ be the interleaved code over $\mathbb{F}_{q^{rm}}$ build from the (n,k,d) Gabidulin code $\mathcal{G}$ over $\mathbb{F}_{q^m}$ with generator vector g. Now, let $z' = z + e$, where $z \in \mathcal{G}_{\mathrm{I}}$ and e is of rank norm $t \leq n-k$. For error correction we view

$$\mathcal{H}_e := \left[\frac{\lambda_{n-t-2}(g)}{\lambda_{n-k-t-1}(\phi(z'))}\right]^{\perp} = \left[\frac{\lambda_{n-t-2}(g)}{\lambda_{n-k-t-1}(\phi(e))}\right]^{\perp} \in \mathbb{F}_{q^m}^{(n-t-1+(n-k-t)r)\times n} .$$

If the lower part $\lambda_{n-k-t-1}(\phi(e))$ has rank t, then $\mathcal{H}_e$ has dimension 1 as all the rows of $\lambda_{n-k-t-1}(\phi(e))$ are linearly independent of the rows of $\lambda_{n-t-2}(g)$. It is easy to see, that the vector h_e, which spans $\mathcal{H}_e$ has rank norm $n-t$ and reveals the error pattern of e. Thus, from h_e we can derive an invertible matrix $T \in \mathbb{F}_q^{n\times n}$, such that the $n-t$ leftmost columns of eT are zero, which is sufficient for error correction.

It remains to determine the rank of $\lambda_{n-k-t-1}(\phi(e))$. After [11] (compare lemma 3.3) the rank of $\phi(e)$ is r with probability

$$\prod_{i=0}^{r-1} \frac{\left(q^{mt} - q^{mi}\right)}{q^{mt}} \geq \left(\frac{q^{mt} - q^{mr}}{q^{mt}}\right)^r .$$

As we will see later (theorem 3.1) it follows, that with probability

$$\geq \left(1 - \frac{4}{q^m}\right)\left(\frac{q^{mt} - q^{mr}}{q^{mt}}\right)^r \tag{2}$$

the matrix $\lambda_{n-k-t-1}(\phi(e))$ has rank $\min\{(n-t-k)r, t\}$. We conclude that if $(n-t-k)r \geq t$, error correction is possible almost always. It follows, that we can correct errors of rank up to

$$t = \frac{r}{r+1}(n-k)$$

with overwhelming probability if $r \ll (n-k)$. The complexity of this way of error correction is $\mathcal{O}(n^3)$.

An example parameter set would be $q = 2$, $m = n = 24$, $k = 10$ and $r = 6$. In this setting, the correction of errors of rank 12 fails in less then one of 2^{22} cases.

3.3 The probability of correct decoding

To determine the probability of correct decoding we need to determine a lower bound for the probability, that the rank of $\lambda_{\left\lfloor \frac{t-1}{s} \right\rfloor}(M)$ is smaller than t if M is a random $s \times t$ matrix over $\mathbb{F}_{q^m}$ with full rank over $\mathbb{F}_q$.

For easier notation we write $\|M\|_q$ if we refer to the rank of M over $\mathbb{F}_q$, and analogous $\|M\|_{q^m}$ for the rank of M over $\mathbb{F}_{q^m}$. Our goal is to prove the following theorem:

Theorem 3.1. *Let M be a random $s \times t$ matrix over $\mathbb{F}_{q^m}$ with $s \leq t \leq m$. Then*

$$\mathcal{P}rob\left(\|\lambda_f(M)\|_{q^m} < t \;\middle|\; \|M\|_q = t \right) \leq \frac{4}{q^m},$$

where $f = \left\lfloor \frac{t-1}{s} \right\rfloor$.

As a direct consequence, we can bound the following probability, too:

Lemma 3.2. *Let M be a random $s \times t$ matrix over $\mathbb{F}_{q^m}$ with $s \leq t \leq m$. Then for all k*

$$\mathcal{P}rob\left(\|\lambda_k(M)\|_{q^m} < \min\{sk, t\} \;\middle|\; \|M\|_q = t \right) \leq \frac{4}{q^m}.$$

Before we are going to prove the theorem, we would like to recall some facts about the rank of random matrices (compare [11] and [3]):

Lemma 3.3. *, Considering all $m \times n$ matrices over $\mathbb{F}_q$, the fraction of the matrices of rank k is*

$$\frac{1}{q^{mn}} \prod_{i=0}^{k-1} \frac{\left(q^m - q^i\right)\left(q^n - q^i\right)}{\left(q^k - q^i\right)}.$$

The fraction of all $m \times n$ matrices over $\mathbb{F}_q$, which have full rank is larger than 0.288.

Unfortunately, we are not able to count the number of matrices M with $\|\lambda_f(M)\|_{q^m} < t$ directly. Thus, we have to rewrite the condition:

Lemma 3.4. *For any $s \times t$ matrix M over $\mathbb{F}_{q^m}$ with $s \leq t \leq m$ and $\|M\| = t$, the following two statements are equivalent:*

$$\|\lambda_f(M)\|_{q^m} < t \tag{3}$$

$$\Longleftrightarrow$$

$$\exists_{h \in \mathbb{F}_{q^m}^n, \|h\|_q > f+1} \forall_{\alpha \in \mathbb{F}_{q^m}^\times} \left(\lambda_f(\alpha h) \cdot M^\top = 0\right). \tag{4}$$

Proof. The proof for (4) $\Rightarrow$ (3) is quite simple and based on the following observation:

$$\left(hm^\top = 0 \wedge h^{[q]} m^\top = 0\right) \Rightarrow \left(h^{[q]} (m^{[q]})^\top = 0 \wedge h^{[q]} m^\top = 0\right).$$

From that, it follows immediately, that if a h exists, such that (4) is fulfilled, then $h^{[q^k]}$ is in the dual space of $\lambda_k(M)$ for all $0 \leq k \leq f$.
To proof (4) $\Leftarrow$ (3), we observe first, that it follows from (3), that there exists an $h \in \mathbb{F}_{q^m}^n$ in the dual space of $\lambda_f(M)$. Consequently all αh with $\alpha \in \mathbb{F}_{q^m}^\times$ are in that space, too. Using the fact, that

$$\left(mh^\top = 0 \wedge m^{[q]} h^\top = 0\right) \Rightarrow \left(mh^\top = 0 \wedge h^{[1/q]} m^\top = 0\right),$$

we conclude, that

$$(3) \;\Rightarrow \exists_{h \in \mathbb{F}_{q^m}} \forall_{\alpha \in \mathbb{F}_{q^m}^\times} \left(\lambda_f(\alpha h) \cdot M^\top = 0\right).$$

It remains to show, that such an h has norm $\|h\|_q > f+1$. If $\|h\|_q = r \leq f+1$, then there exists an invertible matrix $T \in \mathbb{F}_q^{t \times t}$, such that the matrix $\lambda_f(h)$ has non-zero entries in the r rightmost columns, only. Since the submatrix of $\lambda_f(h)$ consisting of the r rightmost columns has full rank, the r rightmost columns of $T^{-1} M^\top$ have only zero entries, which is a contradiction to the premise that $\|M\|_q = t$. We conclude, that h has rank norm $> f+1$, which proves the lemma.

With this modified statement, we are able to give an upper bound of the number of matrices M, where $\|\lambda_f(M)\|_{q^m} < t$. By this, we can finally prove the theorem above:

Proof. *(Theorem 3.1)* First, we determine the probability, that for a fixed $h \in \mathbb{F}_{q^m}^n$ with $\|h\|_q > f + 1$, we have

$$\left(\lambda_f(\alpha h) \cdot M^\top = 0\right).$$

for a random $s \times t$ matrix M with $\|M\|_q = t$. As the rank of $\lambda_f(h)$ over $\mathbb{F}_{q^m}$ is exact $f+1$, there exist at most $(q^m)^{s(t-f-1)}$ possibilities to choose M, such that the condition above is fulfilled. After lemma 3.3, there are more than $\frac{1}{4} \cdot (q^m)^{st}$ possibilities to choose a random $s \times t$ matrix M with $\|M\|_q = t$. Thus, for a fixed h, the probability, that the condition above is fulfilled for a random $s \times t$ matrix M of full rank over $\mathbb{F}_q$ is smaller than

$$4 \cdot (q^m)^{-s(f+1)}.$$

Now we determine the number of different vector spaces defined by $\lambda_f(h)$, where the norm of h is not to small. This number is smaller than

$$(q^{mt} - 1)/(q^m - 1) \approx q^{m(t-1)},$$

as $h \neq 0$ and all αh with $\alpha \in \mathbb{F}_{q^m}^\times$ define the same vector space. Thus, the probability, that the condition (4) is fulfilled for a random matrix M is smaller than the sum of the probabilities for the fixed h over the possible different vector spaces they define. As by lemma 3.4 we have (4) $\Leftrightarrow$ (3), we get the following bound:

$$\begin{aligned}\mathcal{P}rob\left(\|\lambda_f(M)\|_{q^m} < t \,\middle|\, \|M\|_q = t\right) &\leq q^{m(t-1)} \cdot 4 \cdot (q^m)^{-s(f+1)}. \\ &\leq 4 \cdot q^{-m},\end{aligned}$$

which proves the theorem.

Note, that theorem 3.1 gives an estimation of the number of subspace subcodes of (n, k) Gabidulin codes over $\mathbb{F}_{q^m}$, which do not have minimal dimension. For $n = m$ it was already proven in [5], that this number is 0.

Lemma 3.5. *Let $\mathcal{G}$ be an (n, k) Gabidulin code over $\mathbb{F}_{q^m}$, where $m = rs > n$. Then, the probability that the $\mathbb{F}_{q^s}$-subcode of $\mathcal{G}$ has dimension greater than* $\min\{0, n - r(n-k)\}$ *is smaller than* $4/q^m$.

Proof. The $\mathbb{F}_{q^s}$-subcode of $\mathcal{G}$ has a check matrix of the form $\lambda_{n-k-1}(M)$, where the i-th column of $M \in \mathbb{F}_{q^s}^{r \times n}$ represents the i-th entry of the generator vector of $\mathcal{G}$ over $\mathbb{F}_{q^s}$. Thus, the lemma follows directly from theorem 3.1.

4 Application to variants of the GPT cryptosystem

The GPT cryptosystem was first presented in 1991 by Gabidulin, Paramonov and Tretjakov. Here we present a more general version (GGPT, see [10]), which may be used to describe the original GPT cryptosystem as well as the variant with column scrambler (CS-GPT) from 2003 [10].

- **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

  $$\begin{aligned} G' &= S\left(\left[X \middle| 0\right] + G\right) T \\ &= S\left[G_{\cdot\{1,\cdots,t\}} + X \middle| G_{\cdot\{t+1,\cdots,n\}}\right] T \in \mathbb{F}_{q^m}^{k \times n} , \end{aligned} \tag{5}$$

  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.

The distortion matrix X is essential to mask the structure of G. If $t < (n-k-t-1)s$ there exist polynomial time attacks on the private key [9]. In all examples we will choose $n = m$ and $q = 2$. Some parameter sets may be found in table 4.1.

Parameters				size public key	WF best of	WF general
m	k	t	s	in bytes	Gibson's attacks	decoding
64	8	40	1	3,584	2^{111}	2^{87}
156	8	132	7 or 8	23,088	2^{1150}	2^{91}

Table 4.1. Previously proposed parameters for GGPT

4.1 Attacking ciphertexts of GGPT

In this section we describe, how to attack a received ciphertext $y = mG' + z$, where $z = \left[Z \middle| 0 \right] T_Z$ is of rank norm e with $Z \in \mathbb{F}_{q^m}^{k \times e}$ and $T_Z \in \mathbb{F}_q^{n \times n}$ invertible. The main idea is, to use the previously presented method for decoding interleaved codes beyond minimum distance. Here, of course, the interleaving degree is $r = 1$. In the decoding procedure we view the space

$$\mathcal{H}_z = \begin{bmatrix} \lambda_{n-k-t-e-1}(G') \\ \lambda_{n-k-t-e-1}(y) \end{bmatrix}^{\perp} = \begin{bmatrix} \lambda_{n-k-t-e-1}(G') \\ \lambda_{n-k-t-e-1}(z) \end{bmatrix}^{\perp}.$$

Obviously, $\lambda_{n-k-t-e-1}(z)$ has rank $e \leq n - t - k - e$, and thus for all vectors $h_z \in \mathcal{H}_z$:

$$\left(h_z T_Z^{\top} \right)_{\{1,\cdots,e\}} = 0.$$

Let H_z be the matrix generating $\mathcal{H}_z$, then by theorem 4.2 it has rank p over $\mathbb{F}_q$, where $n - e \geq p \geq k$. Let $\bar{T} \in \mathbb{F}_q^{n \times n}$ be a matrix such that only the p rightmost columns of $H_z \bar{T}^{\top}$ contain non-zero entries. Such a $\bar{T}$ is easy to recover from $\mathcal{H}_z$ (compare [9]). It follows that the p rightmost positions of $y\bar{T}^{-1}$ are error-free positions of $(y - z)\bar{T}^{-1}$ in the code $G'\bar{T}^{-1}$. This is sufficient for identifying z since the p rightmost positions of $G'\bar{T}^{-1}$ contain at least one information set (i.e. the rank of $(G'\bar{T}^{-1})_{\{n-p+1,\cdots,n\}}$ is k).

Theorem 4.2. *With the notations above: There exists at least one vector of rank norm $\geq k$ in $\mathcal{H}_z$.*

Proof. As the error vector

$$\left(zT^{-1} \right)_{\{t+1,\cdots,n\}}$$

which has to be corrected by the legitimate user is of rank norm $\leq e$, there exists an invertible matrix $\bar{T} \in \mathbb{F}_q^{n \times n}$, such that

$$\left[X \middle| 0 \right] T\bar{T}^{-1} = \left[X \middle| 0 \right] \text{ and } \left(z\bar{T}^{-1} \right)_J = 0,$$

where $J = \{t + e + 1, \cdots, n\}$. Let h_J be the check-vector of the $(n - t - e, k)$ Gabidulin code $\left(GT\bar{T}^{-1} \right)_{\cdot J}$, then $\left(0 \middle| h_J \right) (\bar{T}^{-1})^{\top}$ is in $\mathcal{H}_z$ and has rank norm $n - t - e = k + e \geq k$.

Note, that the attack runs in time $\mathcal{O}\left(n^3\right)$ and is applicable even in the case, where the column scrambler S is not of quadratic form like it was proposed for some variants (compare e.g. [9]).

4.2 Attacking ciphertexts of RRC-GPT

Most variants of the original GPT cryptosystem were proposed in order to avoid early exponential attacks on the private key. In [6], the authors proposed to substitute the underlying code by a *reducible rank code* build from several Gabidulin codes.

Definition 4.4. *Let $\mathcal{G}_i = \langle G_i \rangle$, $i = 1, \cdots, w$ be a family of linear error correcting codes over $\mathbb{F}_{q^m}$ where $\mathcal{G}_i$ is an (n_i, k_i, d_i) code. 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 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 $d = \min_{1 \leq i \leq w}(d_i)$. 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 [6] 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

$$G' = S \left[X \middle| G \right] T \in \mathbb{F}_{q^m}^{k \times n+t} , \tag{6}$$

where $S \in \mathbb{F}_{q^m}^{k \times k}$ and $T \in \mathbb{F}_q^{n+t \times n+t}$ are non-singular and the rank of $X \in \mathbb{F}_{q^m}^{k \times t}$ over $\mathbb{F}_q$ is t. The error correcting radius e of the code generated by G' is the one of $\mathcal{G}$.

Analogous to GGPT, a ciphertext has the form $y = mG + z$, where $z = \left[Z \middle| 0 \right] T_Z$ is of rank norm e with $Z \in \mathbb{F}_{q^m}^{k \times e}$ and $T_Z \in \mathbb{F}_q^{e \times (n+t)}$ invertible. To recover the message, an attacker can view the space

$$\mathcal{H}_z = \begin{bmatrix} \lambda_{n_2-k_2-e-1}(G') \\ \lambda_{n_2-k_2-e-1}(y) \end{bmatrix}^\perp = \begin{bmatrix} \lambda_{n_2-k_2-e-1}(G') \\ \lambda_{n_2-k_2-e-1}(z) \end{bmatrix}^\perp .$$

Again, for all vectors $h_z \in \mathcal{H}_z$:

$$(T_Z h_z)_{\{1,\cdots,e\}} = 0.$$

In the further analysis, we will concentrate on the case, where $t = 0$. In this case we are able to show, that the message m may be recovered from y in polynomial time:

Theorem 4.3. *With the notations above: Let $t = 0$, then one of the following statements holds:*

(i) $\forall_{h_z \in \mathcal{H}_z} \left(h_z (T^{-1})^\top \right)_{\{1,\cdots,n_1\}} = 0$ *or*
(ii) $\exists_{h_z \in \mathcal{H}_z} \left(h_z (T^{-1})^\top \right)_{\{1,\cdots,n_1\}} \neq 0.$

It follows, that we can recover m from $\mathcal{H}_z$.

Proof. Analogous to theorem 4.2, one can show, that there always exists a $h_z \in \mathcal{H}_z$ of rank norm $k_2 + e$, such that $\left(h_z(T^{-1})^\top\right)_{\{1,\cdots,n_1+t\}} = 0$ (even if $t \neq 0$). Thus, in the first case one can recover a matrix $\bar{T} \in \mathbb{F}_q^{(n+t)\times(n+t)}$, such that the last $k_2 + e$ columns from $G'\bar{T}^{-1}$ have no influence from the columns corresponding to G_1 and thus allow to recover S. Thus, it is easy to recover an alternative row and column scrambler in that case, which is sufficient to recover m.
In the second case, $\left(h_z(T^{-1})^\top\right)_{\{1,\cdots,n_1\}}$ is in the dual of $\lambda_{k_1+(n_2-k_2-e-1)}(g_1)$, where g_1 is the generator vector of G_1. Thus, h_z has rank norm $\geq k_1 + e$. Combining this with the previous observations we conclude that a matrix generating $\mathcal{H}_z$ has to have rank $\geq k_1 + k_2 + 2e$ over $\mathbb{F}_q$, which reveals m.

If $t \neq 0$, the security analysis is quite complicated and does not lead to simple criteria for secure parameter sets. However, even in the case where we can not recover m completely, $\mathcal{H}_z$ reveals lot of information about m and z. (The plaintext is then known to be in a subvectorspace $\mathcal{V} \subseteq \mathbb{F}_{q^m}^{k_1+k_2}$ of dimension at most $k_1 - e$.) This information obviously can be used in combination with the already existing attacks on RRC-GPT. Further, we would like to remark, that in the case where the reducible rank code is build from more than two Gabidulin codes, the same considerations hold.

5 Conclusion

We have shown how to correct rank errors beyond minimum distance for interleaved Gabidulin codes with high probability. Asymptotically we are able to correct errors of rank equal to the amount of the redundancy of the code in polynomial time with overwhelming probability.

The presented decoding method may be applied to attack all proposed variants of the GPT cryptosystem. An analysis of the resulting attack showed, that ciphertexts of GPT, CS-GPT and GGPT may be attacked in polynomial time. The same holds for certain parameter sets of the RRC-GPT, but not for all. However, we were not able to name a parameter set for RRC-GPT, which can be proven to resist the presented attack. However, even if a parameter set resists the attack, information about the plaintext is leaked. We conclude that RRC-GPT is a very weak cryptosystem, which should not be used for cryptographic applications.

References

1. D. Bleichenbacher, A. Kiayias, and M. Yung. Decoding of interleaved reed solomon codes over noisy data. In *Proc. of ICALP 2003*, volume 2719 of *LNCS*, pages 97–108, 2003.
2. A. Brown, L. Minder, and A. Shokrollahi. Probabilistic decoding of interleaved rs-codes on the q-ary symetric channel. In *Proc. of ISIT 2004*, pages 326–326, 2004.

3. S. R. Finch. *Mathematical Constants.* Encyclopedia of Mathematics and Applications. Cambridge, 2003. (see http://mathworld.wolfram.com/InfiniteProduct.html).
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. 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.
8. P. Loidreau and R.Overbeck. Decoding rank errors beyond the error-correction capability. In *Proc. of ACCT-10, Zvenigorod*, 2006. to appear.
9. R. Overbeck. A new structural attack for GPT and variants. In *Proc. of Mycrypt 2005*, volume 3715 of *LNCS*, pages 50–63. Springer Verlag, 2005.
10. R. Overbeck. Extending Gibson's attacks on the GPT cryptosystem. In *Proc. of WCC 2005*, volume 3969 of *LNCS*, pages 178–188. Springer Verlag, 2006.
11. 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.