On the Failure of the Smart Approach of the GPT Cryptosystem

Hervé Talé Kalachi

Abstract
This paper describes a new algorithm for breaking the smart approach of the GPT cryptosystem. We show that by puncturing the public code several times on specific positions, we get a public code on which applying the Frobenius operator appropriately allows to build an alternative secret key.

1 Introduction

Code-based cryptography first appeared in 1978, when McEliece proposed the first public key encryption scheme not based on number theory primitives. More precisely, he built a scheme (with Goppa codes) for which the security stands on two problems, namely the hardness of the Syndrome Decoding Problem in Hamming metric and the difficulty to distinguish a binary Goppa code from a random linear code. The public key is formed with a matrix which is a product of three matrices where is a generator matrix of the Goppa code, a permutation matrix and an invertible matrix. The scheme has various advantages such as:

- the encryption and decryption algorithms are very efficient compared to RSA.
- the syndrome decoding problem is known to be NP complete, and the best attacks for solving it are exponentials in the code length.
- the scheme is a potential candidate for post-quantum cryptography: classic McEliece scheme and some related schemes such as ROLLO and RQC are among the second Round Candidates of the NIST competition for post-quantum cryptography.

However McEliece scheme came with a big disadvantage: the size of the public keys is about five hundred thousands bits for a security level of only 80 bits. In order to solve this problem, several modifications of the scheme have been proposed among which the use of rank metric codes instead of the Hamming metric.

The first rank-metric scheme was proposed by and is now called the GPT cryptosystem. This scheme can be seen as an analog of the McEliece public key cryptosystem based on the class of Gabidulin codes, with the difference that the new public matrix if given
by $G_{\text{pub}} = S(G + X)$, where $X$ is a random matrix with a prescribed rank $t_X$ (the matrix $X$ is usually called the distortion matrix).

Gabidulin codes are often seen as “analogs” of Reed-Solomon codes (Niederreiter, 1986; Sidelnikov and Shestakov, 1992) in the Hamming metric and like them, they are highly structured. That is the reason why their use in the GPT cryptosystem has been the subject of several attacks. Gibson was the first to prove the weakness of the system through a series of successful attacks (Gibson, 1995, 1996). Following this failures, the first works which modified the GPT scheme to avoid Gibson’s attack were published by Gabidulin and Ourivski (2001) followed by Gabidulin et al. (2003). The idea is to hide further the structure of Gabidulin code by considering isometries for the rank metric. Consequently, a right column scrambler $P$ is introduced. This matrix $P$ is an invertible matrix with its entries in the base field $F_q$, while the ambient space of the Gabidulin code is $F_q^n$. But Overbeck (2005a,b, 2008) designed a more general attack that dismantled all the existing modified GPT cryptosystems. His approach consists in applying an operator $\Lambda_i$, which applies $i$ times the Frobenius operation on the public generator matrix $G_{\text{pub}}$. Overbeck observed that the dimension increases by 1 each time the Frobenius is applied. He then proved that by taking $i = n - k - 1$, the codimension becomes 1 if $k$ is the rank of $G_{\text{pub}}$ (which is also the dimension of the associated Gabidulin code). This phenomenon is a clearly distinguishing property of a Gabidulin code which cannot be encountered for instance with a random linear code where the dimension would increase by $k$ for each use of the Frobenius operator.

Overbeck’s attack uses crucially two important facts, namely the column scrambler matrix $P$ is defined on the based field $F_q$ and the codimension of $\Lambda_{n-k-1}(G_{\text{pub}})$ is equal to 1. Several works then proposed to resist to this attack either by taking special distortion matrix so that the second property is not true as proposed by Loidreau (2010) and Rashwann et al. (2010), or by taking a column scrambler matrix defined over the extension field $F_{q^m}$ as in Gabidulin (2008); Gabidulin et al. (2009); Rashwan et al. (2011); Gabidulin and Pilipchuk (2013, 2014). It was recently shown by Otmani et al. (2018) that the general construction from Gabidulin (2008) is vulnerable to a structural attack. This attack implies an attack on the variants from Gabidulin et al. (2009); Rashwan et al. (2011); Gabidulin and Pilipchuk (2014, 2013), since the construction of Gabidulin (2008) is a generalization of the constructions given by Gabidulin et al. (2009); Rashwan et al. (2011); Gabidulin and Pilipchuk (2014, 2013), Horlemann-Trautmann et al. (2017) also presented a cryptanalysis of the variant of Rashwan et al. (2010). This attack focus instead on recovering elements of rank one, rather than the dimension of the dual space. All the above attacks are structural attacks, which unlike generic attacks (or decoding attacks) exploit the structure of the public matrix. We refer the reader to the article from Bardet et al. (2020) for recent progress in term of generic attacks in rank metric.

In this paper, we present a new structural attack of the variant described by Rashwann et al. (2010). Contrary to the result of Horlemann-Trautmann et al. (2017), our attack exploits the structure of the dual space and is based on a new view of the “smart” approach (Rashwann et al., 2010). Concretely, we show that the reparation of Rashwann et al. (2010) is equivalent to insert some redundancies in the public code of a standard GPT cryptosystem. We then show how to remove the redundancies in order to be able to apply Overbeck’s attack on the public code obtained.
2 Preliminary Facts

The finite field with $q$ elements is denoted by $\mathbb{F}_q$ where $q$ is a power of a prime number. For any subfield $\mathbb{K} \subseteq \mathbb{F}$ of a field $\mathbb{F}$ and for any positive integers $k$ and $n$ such that $k \leq n$, the $\mathbb{K}$-vector space spanned by $b_1, \ldots, b_k$ where each $b_i \in \mathbb{F}^n$ is denoted by $\sum_{i=1}^k \mathbb{K} b_i$. The set of matrices with $m$ rows and $n$ columns and entries in $\mathbb{F}$ is denoted by $\mathcal{M}_{m,n}(\mathbb{F})$. The group of invertible matrices of size $n$ over $\mathbb{F}$ is denoted by $\text{GL}_n(\mathbb{F})$.

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

It is a well-known fact that the rank distance on $\mathcal{M}_{m,n}(\mathbb{F})$ has the properties of a metric. In the context of the rank-metric cryptography, this rank distance is rather defined for vectors $x \in \mathbb{F}_q^m$ (Gabidulin, 1985). The idea is to consider the field $\mathbb{F}_q^m$ as an $\mathbb{F}_q$-vector space and hence any vector $x \in \mathbb{F}_q^m$ as a matrix from $\mathcal{M}_{m,n}(\mathbb{F}_q)$ by decomposing each entry $x_i \in \mathbb{F}_q^m$ into an $m$-tuple of $\mathbb{F}_q^m$ with respect to an arbitrary basis of $\mathbb{F}_q^m$. The rank weight of $x$ also denoted by $|x|$ is then its rank viewed as a matrix of $\mathcal{M}_{m,n}(\mathbb{F}_q)$. Hence, it is possible to define a new metric on $\mathbb{F}_q^m$ that we recall explicitly in the following.

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

$$|x| = \dim \sum_{i=1}^n \mathbb{F}_q x_i. \quad (1)$$

Similarly, the column rank over $\mathbb{F}_q$ of a matrix $M$ from $\mathcal{M}_{k,n}(\mathbb{F}_q^m)$ is denoted by $|M|$, and is defined to be the dimension of $\sum_{i=1}^n \mathbb{F}_q M_i$ where $M_1, \ldots, M_n$ are the columns of $M$.

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

$$MT = (M^* \mid 0) \quad (2)$$

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

This permits to state the following corollary.

**Corollary 1**. For any $M \in \mathcal{M}_{k,n}(\mathbb{F}_q^m)$ and for any $m \in \mathbb{F}_q^k$

$$|mM| \leq |M| \quad (3)$$

**Proof**. Suppose that $|M| = s$ and let $T$ in $\text{GL}_n(\mathbb{F}_q)$ such that $MT = (M^* \mid 0)$ with $M^*$ in $\mathcal{M}_{k,s}(\mathbb{F}_q^m)$. We then have $|mM| = |mMT| = |m(M^* \mid 0)| \leq |M^*| \leq s$. $\square$

\footnote{This rank is of course independent of the choice of the basis of $\mathbb{F}_q^m$ since the rank of a matrix is invariant when multiplied by an invertible matrix.}
Notation 1. For any $x$ in $\mathbb{F}_{q^m}$ and for any integer $i$, the quantity $x^{q^i}$ is denoted by $x[i]$. This notation is extended to vectors $\mathbf{x}[i] = (x_1[i], \ldots, x_n[i])$ and matrices $M[i] = (m_{ij})$.

We also give a lemma that will be useful in the sequel.

Lemma 1. For any $A \in \mathcal{M}_{\ell,s}(\mathbb{F}_{q^m})$ and $B \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$, and for any $\alpha$ and $\beta$ in $\mathbb{F}_{q^m}$:

1. If $\ell = k$ and $s = n$ then
   $$(\alpha A + \beta B)[i] = \alpha A[i] + \beta B[i]$$

2. If $s = k$ then
   $$(AB)[i] = A[i]B[i].$$

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

$$(S[i])^{-1} = (S^{-1})[i]$$

Proof. The proof of the two points comes directly from the properties of the Frobenius operators (multiplicative and $\mathbb{F}_q$-linear). To finish, remark that for $S$ in $\text{GL}_n(\mathbb{F}_{q^m})$, since $SS^{-1} = I_n$ we also have $S[i](S^{-1})[i] = I_n$. This implies that $S[i]$ belongs to $\text{GL}_n(\mathbb{F}_{q^m})$ and $(S[i])^{-1} = (S^{-1})[i]$.

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

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

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

2.1 Gabidulin Codes

Definition 3. (Gabidulin, 1985) Let $g \in \mathbb{F}_{q^m}^n$ such that $|g| = n$. The $(n,k)$-Gabidulin code $G_k(g)$ is the code of length $n$ and dimension $k$ generated by the matrix

$$G = \begin{pmatrix} g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}. \quad (4)$$
Gabidulin codes are known to possess a fast decoding algorithm that can decode errors of weight $t$ provided that $t \leq \lfloor \frac{1}{2}(n-k) \rfloor$. Furthermore, the dual of a Gabidulin code $G_k(g)$ is also a Gabidulin code. We refer the reader to the papers from Gabidulin (1985); Loidreau (2007); Silva and Kschischang (2009); Wachter-Zeh (2013) for more details concerning Gabidulin codes and their decoding algorithms.

In the sequel, a matrix that has the structure of (4) will be called a $q-$Vandermonde matrix. The following proposition gives an important well-known property about Gabidulin codes.

Proposition 2. Let $G_k(g)$ be a Gabidulin code of length $n$ with generator matrix $G$ and $T \in \text{GL}_n(F_q)$. Then $GT$ is a generator matrix of the Gabidulin code $G_k(gT)$.

Proof. From Lemma 1 we have $(gT)^[i] = g^i T$ for any integer $i$. \hfill \square

In the following section, we briefly describe the general GPT cryptosystem (Gabidulin et al., 1991).

2.2 The general GPT cryptosystem

The key generation algorithm of the general GPT cryptosystem takes as input the integers $k, \ell, n$ and $m$ such that $k < n \leq m$ and $\ell \ll n$ and outputs the public key/private key pair $(pk, sk)$.

KeyGen($n, m, k, \ell, q$) = ($pk, sk$)

1. Let $G \in M_{k,n}(F_q[m])$ be a generator matrix of the Gabidulin code $G_k(g)$
2. Pick $S \in \text{GL}_k(F_q[m]), X \in M_{k,\ell}(F_q[m])$ and $P \in \text{GL}_{n+\ell}(F_q)$.
3. Compute $G_{\text{pub}} \overset{\text{def}}{=} S(\mid X \mid G)P$ and $t = \frac{n-k}{2}$
4. Return
   \[pk = (G_{\text{pub}}, t)\] and \[sk = (S, P).\]

To encrypt a message $m \in F_q^k$, apply the following function:

Encrypt($m, pk$) = $z$

1. Generate a random error-vector $e \in F_q^m$ with $|e|_q \leq t$
2. Return $z = mG_{\text{pub}} \oplus e$

The decryption function Decrypt() takes as input a ciphertext $z$ and the private key $sk$ and outputs the corresponding message $m$. 
Decrypt \((z, sk) = m'\)

1. First compute \(zP^{-1} = mS(X \mid G) + eP^{-1}\).
2. Extract the last \(n\) components \(z'\) of \(zP^{-1}\).
3. Apply a fast decoding algorithm of \(G_k(g)\) to \(z'\) to obtain \(m^*\).
4. Return \(m^*S^{-1}\)

Remark that \(z'\) will satisfy \(z' = mSG + e'\) where \(e'\) is a sub-vector of \(eP^{-1}\), hence \(|e'|_q \leq t\). The output \(m^*\) of the decoding algorithm for \(G_k(g)\) then satisfies \(m^* = mS\). So we have \(m' = m\). Overbeck (2008) proposed a very efficient attack on the general GPT cryptosystem. The attack exploits the distinguishing properties of Gabidulin codes.

### 2.3 Distinguishing Properties of Gabidulin Codes

We recall important algebraic properties about Gabidulin codes. One key property is that Gabidulin codes can be easily distinguished from random linear codes.

**Definition 4.** For any integer \(i \geq 0\) let \(\Lambda_i : \mathcal{M}_{k,n}(\mathbb{F}_{q^m}) \rightarrow \mathcal{M}_{(i+1)k,n}(\mathbb{F}_{q^m})\) be the \(\mathbb{F}_q\)-linear operator that maps any \(M\) from \(\mathcal{M}_{k,n}(\mathbb{F}_{q^m})\) to \(\Lambda_i(M)\) where by definition:

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

For any code \(G\) generated by a matrix \(G\) we denote by \(\Lambda_i(G)\) the code generated by \(\Lambda_i(G)\).

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

**Proposition 3.** (Overbeck, 2008) Let \(g\) be in \(\mathbb{F}_{q^m}^n\), with \(|g| = n\) with \(n \leq m\). For any integers \(k\) and \(i\) such that \(k \leq n\) and \(i \leq n - k - 1\) we have:

\[
\Lambda_i(G_k(g)) = G_{k+i}(g).
\]

**Proposition 4.** (Overbeck, 2008) If \(\mathcal{G} \subset \mathbb{F}_{q^m}^n\) is a code of dimension \(k\) generated by a random matrix from \(\mathcal{M}_{k,n}(\mathbb{F}_{q^m})\) then, with probability greater than \(1 - 4q^{-m}\) we have:

\[
\dim \Lambda_i(\mathcal{G}) = \min \{ n, (i+1)k \}
\]

In the case of a Gabidulin code, we get a different situation as explained by Proposition 3 namely \(\dim \Lambda_i(G_k(g)) = \min \{ n, k + i \}\). Therefore, we have a property that is verifiable in polynomial time, and allowing to distinguish a Gabidulin code from a random code. This can
be used in a cryptanalysis context. In fact, Overbeck (2008) has proven that, for a public matrix $G_{\text{pub}}$ given by $G_{\text{pub}} = S (X | G) P$ with $X \in \mathcal{M}_{k,\ell} (\mathbb{F}_{q^m})$, $P \in \text{GL}_{n+\ell}(\mathbb{F}_q)$ and $G$ generating a Gabidulin code $\mathcal{G}_k (g)$, (in particular all the entries of $P$ belong to $\mathbb{F}_q$), it is possible (under certain conditions) to find in polynomial time an alternative decomposition of $G_{\text{pub}}$ of the form $S^* (X^* | G^*) P^*$ using the operator $\Lambda_i$. This decomposition allows to decrypt any ciphertext computed with $G_{\text{pub}}$. The reader can refer to Overbeck (2008) for details concerning the attack.

The key reason explaining its success is given by the following proposition.

**Proposition 5.** Let us consider $\ell$, $k$ and $n$ be positive integers with $\ell < n$ and $1 \leq k < n$. Let $G$ be in $\mathcal{M}_{k,n} (\mathbb{F}_{q^m})$ as a generator matrix of a Gabidulin code, and $X$ be a randomly drawn matrix from $\mathcal{M}_{k,\ell} (\mathbb{F}_{q^m})$. Denote $\mathcal{A}$ as the code defined by the generator matrix $(X | G)$. Then for any integer $i \geq 0$

$$k + i \leq \dim \Lambda_i (\mathcal{A}) \leq k + i + d$$

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

Note that by construction $\ell \leq n$ and in Overbeck’s attack, the integer $i$ is equal to $n-k-1$ so that we have both $d = \ell$ and, with high probability, the upper bound in (8) is actually an equality, namely

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

This implies that the dimension of $\Lambda_i (\mathcal{A})^\perp$ is equal to 1. This fact is then harnessed by Overbeck (2008) to recover an equivalent Gabidulin code which enables to decrypt any ciphertext.

**Proposition 6.** (Overbeck, 2008) Assume that the public key is $G_{\text{pub}} = S (X | G) P$ with $X \in \mathcal{M}_{k,\ell} (\mathbb{F}_{q^m})$, $P \in \text{GL}_{n+\ell}(\mathbb{F}_q)$ and $G$ generates a Gabidulin code $\mathcal{G}_k (g)$. If the dimension of $\Lambda_{n-k-1} (\mathcal{A})^\perp$ is equal to 1, then it is possible to recover (with $O ((n + \ell)^3)$ field operations) alternative matrices $X^* \in \mathcal{M}_{k,\ell} (\mathbb{F}_{q^m})$, $P^* \in \text{GL}_{n+\ell}(\mathbb{F}_q)$ and $G^*$ that generates a $(n, k)$-Gabidulin code such that

$$G_{\text{pub}} = S (X^* | G^*) P^*$$

Overbeck’s attack uses crucially two important facts: the column scrambler matrix $P$ is defined on the based field $\mathbb{F}_q$, and the codimension of $\Lambda_{n-k-1} (\mathcal{A})^\perp$ is 1. Several works propose to resist to Overbeck’s attack by taking special distortion matrix so that the second property is not true as (Loidreau, 2010; Rashwann et al., 2010). In the sequel, we focus on the variant of Rashwann et al. (2010) which is usually called “the smart approach”. Horlemann-Trautmann et al. (2017) also proposed an attack of that variant, focusing instead on recovering elements of rank one rather than the dimension of the dual space. In the next section, we present a new attack that exploits the structure of the dual space and is based on a new view of the “smart” approach (Rashwann et al., 2010).
3 A New Attack on the Smart Approach of the GPT Cryptosystem

Here we describe the reparation given by Rashwann et al. (2010) and we give our new algorithm that recovers an alternative secret key in polynomial time.

3.1 Description

The only difference is in the key generation algorithm, specially in the choice of $X$. The authors proposed to take $X \in M_{k,\ell} (\mathbb{F}_q^n)$ that is a concatenation of a $q$–Vandermonde matrix $X_1 \in M_{k,a} (\mathbb{F}_q^n)$ and a random matrix $X_2 \in M_{k,\ell-a} (\mathbb{F}_q^n)$ with $0 < a < \ell$. That is to say $X = (X_1 \mid X_2)$.

With the above construction, it was shown by Rashwann et al. (2010) that the corresponding public code $C_{\text{pub}}$ satisfies $\dim \Lambda_{n-k-1} (C_{\text{pub}}) \neq 1$ and hence, Overbeck’s attack fails. In the following, we show that one can modify the public code $C_{\text{pub}}$ to make Overbeck’s attack succeed again.

3.2 Cryptanalysis

The attack we present here is inspired by the attack presented by Otmani and Kalachi (2015) in a hamming metric context. In the sequel, $G$ is a $q$–Vandermonde matrix from $M_{k,n} (\mathbb{F}_q^n)$ that generates a Gabidulin code $G_k (g)$, $g$ being the first row of $G$.

Let $S \in GL_k(\mathbb{F}_q^n)$, $X_2 \in M_{k,\ell-a} (\mathbb{F}_q^n)$, $b = (b_1, \cdots, b_a)$ and

$$X_1 = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} \\ \vdots & \ddots & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} \end{pmatrix}. \quad (9)$$

We have $G_{\text{pub}} = S (X_1 \mid X_2 \mid G) P$ with $P \in GL_{n+\ell}(\mathbb{F}_q)$. We start the cryptanalysis by the following lemma:

**Lemma 2.** There exists $P^* \in GL_{n+\ell}(\mathbb{F}_q)$ and $G^* \in M_{k,n+s} (\mathbb{F}_q^n)$ a generator matrix of a Gabidulin code such that $G_{\text{pub}} = S (0 \mid X_2 \mid G^*) P^*$

$s$ being an integer satisfying $0 \leq s \leq a$ and $n + s \leq m$.

**Proof.** Let $g' = (b \mid g) \in \mathbb{F}_q^{a+n}$. Since $|g'| > |g| = n$, let $s$ be an integer such that $|g'| = n + s$. Clearly, we have $s \leq a$ and $|(X_1 \mid G)| = |g'| = n + s$ from the definition of the column rank together with Lemma 1. From Proposition 1 there exists a matrix $Q \in GL_{n+a}(\mathbb{F}_q)$ such that $(X_1 \mid G) Q$ has $a-s$ many zero columns. More precisely, $(X_1 \mid G) Q = (0 \mid G^*)$ where $G^* \in M_{k,n+s} (\mathbb{F}_q^n)$ is a generator matrix of a Gabidulin code $G_k (g^*)$ with $g^* Q = (0 \mid g^*)$. This implies that there exists a matrix $R \in GL_{n+\ell}(\mathbb{F}_q)$ such that $(X_1 \mid X_2 \mid G) R = (0 \mid X_2 \mid G^*)$.

To finish the proof, take $P^* = R^{-1} P$. Since $g'$ belongs to $\mathbb{F}_q^{a+n}$, we have $|g'| = n + s \leq m$ by the definition of the rank weight. \qed
In the sequel, for any integer \( \ell \) and given two linear codes \( C \) and \( C' \), we will say that \( C \) is the code \( C' \) with \( \ell \) redundancies if a generator matrix of \( C \) is a generator matrix of \( C' \) with \( \ell \) additional columns. Let \( C_{\text{pub}} \) be the code generated by \( G_{\text{pub}} \). We then have the following proposition:

**Proposition 7.** The code \( C_{\text{pub}} \) is the public code of a general GPT cryptosystem with \( w = a - s \) redundancies.

**Proof.** We have \( G_{\text{pub}} = S (0 \mid X_2 \mid G^*) P^* \). Let us suppose that \( P^* = \begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} \) with \( Q_1 \in M_{w,n+\ell}(\mathbb{F}_q) \) and \( Q_2 \in M_{n+\ell - w,n+\ell}(\mathbb{F}_q) \). We have \( G_{\text{pub}} = S (X_2 \mid G^*) Q_2 \) and \( \text{rank}(Q_2) = n + \ell - w \). Let us suppose without loss of generality that the matrix \( Q_2^\ast \) of the first \( n + \ell - w \) columns of \( Q_2 \) is of full rank. Let \( G_{\text{pub}}^\ast = S (X_2 \mid G^*) Q_2^\ast \). Let \( X = S (X_2 \mid G^*) Q_2^\ast \) where \( Q_2^\ast \) is the last \( w \) columns of \( Q_2 \). Then \( G_{\text{pub}} = (G_{\text{pub}}^\ast \mid X) \). One can remark to finish that \( G_{\text{pub}}^\ast \) is a generator matrix of a general GPT cryptosystem.

From the above proposition, if \( w \) redundancies of \( C_{\text{pub}} \) are identified and removed, a cryptanalyst can use Overbeck’s attack to build an alternative secret key. One can remark that the notion of redundancies here is very related to the notion of “information set” [Prange, 1962] of the code \( C_{\text{pub}} \) generated by the matrix \( Q_2 \) in the proof of the previous proposition. In fact, we are looking for an information set of \( C_{\text{pub}} \), since the corresponding columns of such a set in \( G_{\text{pub}} \) will generate the public code of a general GPT cryptosystem. We will find such a set by eliminating progressively (one by one) \( w \) columns of \( G_{\text{pub}} \), corresponding to a “redundancy set” \( I = \{i_1,...,i_w\} \subset \{1,2,...,n+\ell\} \) of \( C_{\text{pub}} \), or redundancies of \( C_{\text{pub}} \). The reason we succeed by doing that is given by Proposition 8 By abuse of language, a set of \( w \) redundancies of \( C_{\text{pub}} \) will be also called a ”redundancy set” of \( C_{\text{pub}} \).

In the sequel, let \( f = n + s - k \) and \( \Lambda_f(C_{\text{pub}}) \) the code generated by \( \Lambda_f(G_{\text{pub}}) \). For any subset \( J \subset \{1,2,...,n+\ell\} \), we denote by \( C_{\text{pub}}^J \) the code obtained by puncturing \( C_{\text{pub}} \) at all the positions corresponding to the elements in \( J \). For a matrix \( M \) with \( n + \ell \) columns, \( M^J \) is the matrix obtained from \( M \) by removing all the columns with positions corresponding to the elements in \( J \). It is clear that \( J \) is a “redundancy set” of \( C_{\text{pub}} \) if and only if \( Q_2^J \) is non singular. We have the following proposition:

**Proposition 8.** A set \( I = \{i_1,...,i_w\} \subset \{1,2,...,n+\ell\} \) is a “redundancy set” of \( C_{\text{pub}} \) if and only if for any subset \( J \subset I \),

\[
\dim \Lambda_f(C_{\text{pub}}^J) = n + s + \ell - a
\]

**Proof.** We have:

\[
\dim \Lambda_f(C_{\text{pub}}^J) = \text{rank}(\Lambda_f(G_{\text{pub}}^J)) = \text{rank}(\Lambda_f(X_2 \mid G^*) Q_2^J)
\]

Since \( X_2 \) is a random matrix, with a high probability we have

\[
\dim \Lambda_f(C_{\text{pub}}^J) = \min\{\text{rank}(\Lambda_f(X_2 \mid G^*)), \text{rank}(Q_2^J)\} = \min\{n + s + \ell - a, \text{rank}(Q_2^J)\}
\]

\[\text{rank}(Q_2)\] is the rank over \( \mathbb{F}_{q^m} \) in contrast to \( |Q_2|_s \), which denotes the column rank over \( \mathbb{F}_q \).
If $I$ is a “redundancy set” of $C_{\text{pub}}$, we will always have $\text{rank}(Q_2^I) = \text{rank}(Q_2) = n+s+\ell-a$ and $\dim \Lambda_f(C_{\text{pub}}^J) = n+s+\ell-a$ for all $J \subset I$. Else, we will have $\text{rank}(Q_2^I) < n+s+\ell-a$ and $\dim \Lambda_f(C_{\text{pub}}^I) < n+s+\ell-a$.

It is easy for an adversary to use the previous proposition to identify a “redundancy set” $I$. To fully break the system, one can apply Overbeck’s attack with $f = n+s-k-1$, but the value of $s$ is not known. For the case $m = n$, it is easy to see thanks to Lemma 2 that $s$ is equal to 0 and in a general context ($n \leq m$), one can remark from the same lemma that the integer $s$ is the smallest one that satisfies

$$\text{rank}(\Lambda_{n+s-k}(G_{\text{pub}})) = \text{rank}(\Lambda_{n+s+1-k}(G_{\text{pub}}))$$

We summarise the attack in Algorithm 1.

**Algorithm 1** Key Recovery of The Smart Approach of the GPT Cryptosystem

| Input: $G_{\text{pub}}, t, a, k, n, \ell$ |
| Output: $s, J = \{i_1, ..., i_w\}, P^* \in \text{GL}_{n+\ell-a+s}({\mathbb F}_q) |

1: $s \leftarrow a$
2: **while** $\text{rank}(\Lambda_{n+s-k}(G_{\text{pub}})) = \text{rank}(\Lambda_{n+s+1-k}(G_{\text{pub}}))$ **do**
3: $s \leftarrow s - 1$
4: **end while**
5: $s \leftarrow s + 1$
6: $w \leftarrow a - s$
7: $y \leftarrow n + s + \ell - a$
8: $f \leftarrow n + s - k$
9: $Z \leftarrow \{1, ..., \text{Length}(C_{\text{pub}})\}$ and $J \leftarrow []$
10: $j \leftarrow \text{Random}(Z)$
11: **while** $\#J \neq w$ **do**
12: **if** $\dim(\Lambda_{n+s-k}(C_{\text{pub}}^j)) = y$ **then**
13: $J \leftarrow \text{HorizontalJoin}(J, [j])$
14: $C_{\text{pub}} \leftarrow C_{\text{pub}}^j$
15: $Z \leftarrow \{1, ..., \text{Length}(C_{\text{pub}})\}$
16: $j \leftarrow \text{Random}(Z)$
17: **else**
18: $Z \leftarrow Z \setminus \{j\}$
19: $j \leftarrow \text{Random}(Z)$
20: **end if**
21: **end while**
22: **return** $C_{\text{pub}}, J$
23: Define $G_{\text{pub}}$ as the generator matrix of $C_{\text{pub}}$
24: Apply Overbeck’s algorithm on $G_{\text{pub}}$ with $f = n + s - k - 1$
3.3 Complexity and Experimental Results

During the computation phase of $s$, the main computations are $\text{rank}(\Lambda_{n+s-k}(G_{\text{pub}}))$ and $\text{rank}(\Lambda_{n+s+1-k}(G_{\text{pub}}))$ which are computed with a complexity $O(k^3(n+a+1-k)^3)$. To identify a set of $w = a - s$ random redundancies, the main computation is $\dim(\Lambda_{n+s-k}(\mathcal{C}_{\text{pub}}))$ (for $j \in \{1, ..., n + \ell\}$) which can be done only once. So the complexity of this step is $O(k^3(n+s+1-k)^3)$. By considering the final step that consists to apply Overbeck’s attack, the overall complexity is $O(k^3(n+a+1-k)^3)$ operations on $\mathbb{F}_{q^m}$ since the complexity of this final step is $O((n+\ell)^3)$ operations on $\mathbb{F}_{q^m}$. We implemented the attack (for $m \leq 30$) and for several values of $a$ such that $am \geq 60$ as proposed by [Rashwann et al. (2010)] on Magma V2.21-6 and a secret key was always found in less than 5 seconds. This confirms the efficiency of the approach.

3.4 A Brief Comparison with the Attack from Horlemann-Trautmann et al. (2017)

Let $G_{\text{pub}}$ be a public generator matrix of the smart approach of the GPT cryptosystem. We recall that $G_{\text{pub}} = S(G \mid X_1 \mid X_2)P$ with $P \in \text{GL}_{n+\ell}(\mathbb{F}_q)$. Horlemann-Trautmann et al. (2017) decomposed $G_{\text{pub}}$ as follows:

$$G_{\text{pub}} = S(G \mid X_1 \mid 0)P + S(0 \mid 0 \mid X_2)P = S(G \mid X_1 \mid 0)P + SX_2P'$$

where $P' \in \mathcal{M}_{t-a,n+\ell}(\mathbb{F}_q)$ is a full rank matrix. They then consider the $\mathbb{F}_{q^m}$-linear code $\mathcal{C}'$ generated by $P'$ and show that the only elements of rank one in $\Lambda_{t-a}(\mathcal{C}_{\text{pub}})$ are those from $\mathcal{C}'$, after showing that $\mathcal{C}' \subset \Lambda_{t-a}(\mathcal{C}_{\text{pub}})$. This means that one can reconstruct the matrix $P'$ or an alternative $P^*$ by collecting elements of rank one in $\Lambda_{t-a}(\mathcal{C}_{\text{pub}})$ (these elements are found by solving a linear system parametrised by $\Lambda_{t-a}(G_{\text{pub}})$). They finish their attack by computing a parity check matrix $H_{P^*} \in \mathcal{M}_{n+\ell-t+a,n+\ell}(\mathbb{F}_q)$ of $\mathcal{C}'$ from $P^*$. Note that $H_{P^*}^T$ can be use in place of $P^{-1}$ during the decoding process, since $SX_2P'H_{P^*}^T = 0$ and $G_{\text{pub}}H_{P^*}^T = S(G \mid X_1 \mid 0)PH_{P^*}$ is a $q$-Vandermonde matrix. This attack have a complexity in $O(k^3nm^2(t^2 + k))$ operations in $\mathbb{F}_q$.

Our view of $G_{\text{pub}}$ is different. As explained in Proposition 7, $G_{\text{pub}}$ is a public matrix of a general GPT cryptosystem concatenated with some useless columns. We use the Frobenius operator to extract (from $G_{\text{pub}}$) a public matrix $G'_{\text{pub}}$ of the general GPT cryptosystem, and the last step is to apply Overbeck’s attack to $G'_{\text{pub}}$. We end-up with $O(k^3(n+a+1-k)^3)$ operations on $\mathbb{F}_{q^m}$.

One can remark that the cost of Horlemann-Trautmann et al. (2017) is better if we assume that $m$ and $n$ are equal or almost equal. But for very large $m$ compare to $n$, the cost of our attack is better.
4 Conclusion

In this paper, we have shown that the smart approach of the GPT cryptosystem proposed by Rashwann et al. (2010) to avoid Overbeck’s structural attack, is equivalent to insert some redundancies to the public code of a standard GPT cryptosystem. We show how to remove the redundancies in order to be able to apply Overbeck’s attack on the public code obtained. This allows a cryptanalyst to built an alternative secret key in polynomial time. Our attack is a new and simple way to show that the smart approach of the GPT cryptosystem is not secure.

5 Acknowledgement

The author would like to thank the anonymous reviewers for their valuable comments and suggestions which helped to improve the paper.

References

Bardet, M., M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J. Tillich, and J. A. Verbel (2020). Algebraic attacks for solving the rank decoding and minrank problems without gröbner basis. arXiv preprint arXiv:2002.08322.

Berlekamp, E., R. McEliece, and H. van Tilborg (1978, May). On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory 24(3), 384–386.

Bernstein, D. J., T. Lange, and C. Peters (2008). Attacking and defending the McEliece cryptosystem. In Post-Quantum Cryptography 2008, Volume 5299 of Lecture Notes in Comput. Sci., pp. 31–46.

Courtois, N., M. Finiasz, and N. Sendrier (2001). How to achieve a McEliece-based digital signature scheme. In Advances in Cryptology - ASIACRYPT 2001, Volume 2248 of Lecture Notes in Comput. Sci., Gold Coast, Australia, pp. 157–174. Springer.

Gabidulin, E. and N. Pilipchuk (2013). GPT cryptosystem for information network security. In International Conference on Information Society (i-Society 2013), Number 8, pp. 21–25.

Gabidulin, E. and N. Pilipchuk (2014). Modified GPT cryptosystem for information network security. International Journal for Information Security Research 4(8), 937–946.

Gabidulin, E., H. Rashwan, and B. Honary (2009). On improving security of GPT cryptosystems. In Proc. IEEE Int. Symposium Inf. Theory - ISIT, pp. 1110–1114. IEEE.

Gabidulin, È. M. (1985). Theory of codes with maximum rank distance. Problemy Peredachi Informatsii 21(1), 3–16.
Gabidulin, E. M. (2008). Attacks and counter-attacks on the GPT public key cryptosystem. *Des. Codes Cryptogr.* 48(2), 171–177.

Gabidulin, E. M. and A. V. Ourivski (2001). Modified GPT PKC with right scrambler. *Electron. Notes Discrete Math.* 6, 168–177.

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

Gabidulin, E. M., A. V. Paramonov, and O. V. Tretjakov (1991, April). Ideals over a non-commutative ring and their applications to cryptography. In *Advances in Cryptology - EUROCRYPT’91*, Number 547 in Lecture Notes in Comput. Sci., Brighton, pp. 482–489.

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

Gibson, K. (1996). The security of the Gabidulin public key cryptosystem. In U. Maurer (Ed.), *Advances in Cryptology - EUROCRYPT ’96*, Volume 1070 of *Lecture Notes in Comput. Sci.*, pp. 212–223. Springer.

Horlemann-Trautmann, A., K. Marshall, and J. Rosenthal (2017, Apr). Extension of overbeck’s attack for gabidulin based cryptosystems. *Designs, Codes and Cryptography*.

Loidreau, P. (2007, January). *Rank metric and cryptography*. Accreditation to supervise research, Université Pierre et Marie Curie - Paris VI.

Loidreau, P. (2010). Designing a rank metric based McEliece cryptosystem. In N. Sendrier (Ed.), *Post-Quantum Cryptography 2010*, Volume 6061 of *Lecture Notes in Comput. Sci.*, pp. 142–152. Springer.

McEliece, R. J. (1978). *A Public-Key System Based on Algebraic Coding Theory*, pp. 114–116. Jet Propulsion Lab. DSN Progress Report 44.

Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory* 15(2), 159–166.

Otmani, A. and H. T. Kalachi (2015). Square code attack on a modified sidelnikov cryptosystem. In *Codes, Cryptology, and Information Security - First International Conference, C2SI 2015, Rabat, Morocco, May 26-28, 2015, Proceedings - In Honor of Thierry Berger*, pp. 173–183.

Otmani, A., H. T. Kalachi, and S. Ndjeya (2018). Improved cryptanalysis of rank metric schemes based on gabidulin codes. *Des. Codes Cryptogr.* 86(9), 1983–1996.

Overbeck, R. (2005a). Extending Gibson’s attacks on the GPT cryptosystem. In O. Ytrehus (Ed.), *WCC 2005*, Volume 3969 of *Lecture Notes in Comput. Sci.*, pp. 178–188. Springer.

Overbeck, R. (2005b). A new structural attack for GPT and variants. In *Mycrypt*, Volume 3715 of *Lecture Notes in Comput. Sci.*, pp. 50–63.
Overbeck, R. (2008). Structural attacks for public key cryptosystems based on Gabidulin codes. *J. Cryptology* 21(2), 280–301.

Prange, E. (1962). The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory* 8(5), 5–9.

Rashwan, H., E. Gabidulin, and B. Honary (2011). Security of the GPT cryptosystem and its applications to cryptography. *Security and Communication Networks* 4(8), 937–946.

Rashwann, H., E. Gabidulin, and B. Honary (2010). A smart approach for GPT cryptosystem based on rank codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pp. 2463–2467. IEEE.

Sendrier, N. (2002). Cryptosystèmes à clé publique basés sur les codes correcteurs d’erreurs. In *Mémoire d’habilitation à diriger des recherches, Université Paris 6*.

Sidelnikov, V. M. and S. Shestakov (1992). On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. Appl.* 1(4), 439–444.

Silva, D. and F. R. Kschischang (2009). Fast encoding and decoding of gabidulin codes. In *IEEE International Symposium on Information Theory, ISIT 2009, June 28 - July 3, 2009, Seoul, Korea, Proceedings*, pp. 2858–2862. IEEE.

Wachtler-Zeh, A. (2013). Bounds on list decoding of rank-metric codes. *IEEE Trans. Inf. Theory* 59(11), 7268–7277.

**Hervé Talé Kalachi, Department of Computer Engineering, National Advanced School of Engineering of Yaounde, University of Yaounde 1, Po.Box: 8069 Yaounde-Cameroon**

*E-mail address*: herve.tale@univ-yaounde1.cm