ISSN 2277-3061

Enhancing the Security of the GPT Cryptosystem Against Attacks

Haitham Rashwan [1], Ernst M. Gabidulin [2], Bahram Honary [3], Haitham Cruickshank [1]

[1] Centre for Communication Systems Research (CCSR),
University of Surrey Guildford, GU2 7XH, UK
Email: h.rashwan@surrey.ac.uk

[2] Department of Radio Engineering,
Moscow Institute of Physics and Technology, Russia
Email:ernst.gabidulin@gmail.com

[3] School of Computing & Communication, InfoLab21, Lancaster University,
Email: b.honary@lancaster.ac.uk

Abstract:

The concept of Public key cryptosystems based on error correcting codes was invented by McEliece in 1978. In 1991 Gabidulin, Paramonov and Tretjakov proposed a new version of the McEliece cryptosystem (GPT) based on maximum rank distance codes instead of hamming distance codes. Respective structural attacks against different variants of the GPT cryptosystem were proposed by Gibson and lately by Overbeck. The Overbeck attack breaks all variants of the GPT cryptosystem and is turned out to be either polynomial or exponential depending on parameters of the cryptosystem. Furthermore, In 2013, Gaborit et al. have presented a decoding attack against the parameters of the simple variant of the GPT cryptosystem which were demonstrated to combat the GPT cryptosystem against Overbeck's attack.

In this paper, we introduce two new secure approaches against both the structural (Overbeck's attack) and decoding (brute force) attacks. The first one is called Distortion Matrix Approach (DMA), and the second is called Advanced Approach for Reducible Rank Codes (ARC). The DMA based on proper choice of a distortion matrix $\mathbf{X}$, while, the ARC based on a proper choice of a scramble matrix $\mathbf{P}$. Furthermore, we evaluate the simple variant of GPT cryptosystem against Gaborit et al. attack and demonstrate a new set of parameters which are secure against all known attacks. Our results show the proposed approaches combat the structural and decoding attacks with a large reduction in the key size in comparison to the original McEliece cryptosystem.

Keywords:

Public key cryptosystem; GPT cryptosystem; McEliece Cryptosytem; Algebraic Coded Cryptosystem; Rank codes; Goppa Codes; Error control coding.

1 Introduction

McEliece [1] introduced the first code-based public-key cryptosystem (PKC). The system is connected to the hardness of the general decoding problem. It is based on Goppa codes in the Hamming metric. It is a strong cryptosystem but the size of a public key is too large (500 000 bits) for practical implementations to be efficient. The choice of the code has a vital effect on the security of this type of cryptosystems. Some codes have a structure that can be recovered in polynomial time, hence breaking the cryptosystem completely. However, other codes still have protection against cryptanalysis. Niederreiter [2] introduced a new code based version of PKC based on check matrices of Generalized Reed-Solomon codes. It turned out that this cryptosystem is insecure [3]. Several modifications of this PKC [4, 5, 6], and [7] seem to be secure but no independent cryptanalysis was made on these cryptosystems.

Also, Gabidulin, Paramonov and Tretjakov proposed in [8] other version of McEliece's public key cryptosystem based on rank error correcting codes, which is now called the GPT cryptosystem. The GPT cryptosystem has two advantages over McEliece's Cryptosystem. Firstly, it is more robust against decoding attacks than McEliece's Cryptosystem [9]; secondly, the key size of the GPT is much smaller and more useful in terms of practical applications than McEliece's cryptosystem. There are two types to attack against the GPT cryptosystem and its variants: the first is structural attack, an attacker attempts to recover the private key (the hiding procedure) from the public key, based on the structural properties of the rank codes; the second attack is decoding attack, an attacker tries to correct rank errors by a general algorithm without any knowledge of the structure of a rank code. Decoding attack ia generic and depends only on the code parameters. In 1995, Gibson [10, 11] proposed the first structural attack which broke the GPT system for public keys of about 5 Kbits. The Gibson attack was efficient for practical values of parameters $n \leq 30$, where n is the length of rank code with the field F_{2^N} as an alphabet.

Several proposals of the GPT PKC were introduced to withstand Gibson's attack [12, 13]. One proposal was to use a rectangular row scramble matrix instead of a square matrix. The proposal allows working with subcodes of the rank codes which have much more complicated structure. Another proposal exploits a modification of Maximum Rank Distance (MRD) codes where the concept of a column scramble matrix was also introduced. Moreover, a new variant, which is called reducible rank codes, was also implemented to combat the GPT cryptosystem against structural attacks [14, 15]. All the above variants withstand Gibson attack. In 2005, R. Overbeck [16, 17], and [18] has proposed the second structural attack which is more effective than Gibson attack. His method is based on two factors: a) a column scrambler $\mathbf{P}$ that is defined over the base field, and b) the unsuitable choice of a distortion matrix $\mathbf{X}$. However, Overbeck managed to break completely all variants of the GPT cryptosystem based on the general and developed ideas of Gibson. In 2013, Gaborit et al. have presented two new generic approaches (decoding attacks) to attack Rank Syndrome Decoding (RSD) problem, both approaches have their own interest depending of the type of parameters considered [38]. Furthermore, they break the proposed parameters in [24], and [21] which were demonstrated to combat the GPT cryptosystem against Overbeck's attack.

In this paper, we introduce two new secure approaches against both the Overbeck and the decoding attacks. The first one is called Distortion Matrix Approach (DMA), and the second is called Advanced Approach for Reducible Rank Codes (ARC). The DMA based on proper choice of a distortion matrix $\mathbf{X}$, while, the ARC based on a proper choice of a scramble matrix $\mathbf{P}$. The DMA is proposed to improve the security of the smart approach [19] against little vulnerability which may affect its security, and as a consequence the system may be broken. Therefore, we address and show these vulnerabilities, and then we will describe a new construction of distortion matrix $\mathbf{X}$ which countermeasures the vulnerabilities of the smart approach. The ARC is designed to countermeasure Overbeck's attack against the reducible rank codes variant [14, 15]. Finally, we evaluate the simple variant of the GPT PKC which was proposed in [24] against Gaborit et al. attack and demonstrate a new set of parameters which are secure against all known attacks. Our results show the DMA is secure even the column scrambling matrix $\mathbf{P}$ is chosen over the base field, and the ARC is secure even the distortion matrix $\mathbf{X}$ does not exist. The proposed approaches combat the structural and decoding attacks with a large reduction in the key size in comparison to the original McEliece cryptosystem.

The rest of this paper is structured as follows. Section 2 introduces the related work. Section 3 describes the GPT cryptosystems. Section 4 discusses decoding and Overbeck's attacks against the GPT cryptosystem. The DMA will be presented in Section 5. Section 6 first takes a short introduction on reducible rank codes, and then the ARC will be described. Section 7 gives a short introduction on the simple variant, and afterward we demonstrate new parameters against attacks. Finally, Section 8 concludes the paper with some remarks.

2 Related Work

Overbeck's attack is a potential attack which breaks all variants of the GPT cryptosystem in a polynomial time. However, there are few methods were proposed to combat Overbeck's attack against the GPT cryptosystem. Kshevetskiy in [20] suggested a secure approach towards the choice of parameters for avoiding Overbeck's attack based on suitable choice of the distortion matrix $\mathbf{X}$. Independently, Loidreau proposed similar method in [21]. Although, they neither explained how the matrix $\mathbf{X}$ can be constructed in a secure manner nor explored the implications of that approach. Moreover, they recommended a set of parameters to be secure against Overbeck's attack. However, all parameters were proposed in [21] have been broken by Gaborit et al., and the second set of parameters which were supposed to be stronger than the first one are also attacked in a few seconds with hybrid Grobner bases attack as shown in [38]. In short, Both Kshevetskiy and Loidreau approaches are not considered to be secure against Gaborit et al. attack (decoding attack).

Gabidulin presented in [22] a secure approach for the standard variant of the GPT cryptosystem called an advanced approach which defines a particular column scrambler matrix $\mathbf{P}$ over the extension field without violating the standard mode of the GPT PKC. This approach is secure against all known attacks however it is not applicable for the reducible rank codes variant of the GPT PKC. Hence, the reducible rank codes have different constructions and principles than the standard rank codes [14]. In this paper, we will present the ARC approach as an appropriate secure approach for the reducible rank codes variant. We have applied the advanced approach for the simple variant of the GPT cryptosysrtem in [23], and reduced its public key size from 10 Kbits to 4 Kbits in [24]. Our method to reduce the public key size was based on choice of a set of parameters which were secure against all known attacks at that time. Recently, Gaborit et al. presented a decoding attack (new algorithm) which can break our proposed parameters in 5 days [38]. In this paper, we will evaluate the simple variant against Gaborit et al. attack and demonstrate secure parameters against all known attacks.

We have introduced a new approach called smart approach [19] which based on a proper choice of the distortion matrix $\mathbf{X}$. Recently, we have realized that the smart approach can be vulnerable to a new structural attack under certain conditions. Therefore, we will highlight the vulnerabilities of the smart approach, and then we will propose the DMA as an alternative approach for the Smart approach. In summary, the reducible rank codes variant is still vulnerable to Overbeck's attack, and the Smart approach requisites to be reconstructed in more powerful way in order to avoid any structural attacks in the future. In addition, both Kshevetskiy and Loidreau approaches are not considered to be secure against Gaborit et al. attack. Moreover, the simple variant GPT PKC is also vulnerable to Gaborit et al. attack using our proposed parameters in [24].

Our contributions are as follows:

1. We present the ARC approach to secure the reducible rank codes variant of GPT PKC.
2. We explore some vulnerabilities of the smart approach, and then, we will propose the DMA as an alternative approach for the Smart approach.
3. We evaluate the simple variant of GPT PKC against Gaborit et al. attack and demonstrate a new set of parameters which are secure against all known attacks.

3 The GPT Cryptosystem

We give a short introduction to rank codes in Section 3.1; and provide a description of the standard GPT cryptosystem in Section 3.2.

3.1 Rank Codes

Rank codes were introduced by Gabidulin in 1985 [34]. The rank codes are a linear codes generated by polynomial which can correct rank distance errors efficiently. The basic notions of rank codes are introduced as follows:

Let F_q be a finite field of q elements and let F_{q^N} be an extension field of degree N.

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a vector with coordinates in F_{q^N}.

The Rank norm of x is defined as the maximal number of x_i, which are linearly independent over the base field F_q and is denoted $\mathrm{Rk}(\mathbf{x} \mid \mathsf{F}_q)$.

Similarly, for a matrix $\mathbf{M}$ with entries in F_{q^N}, the column rank is defined as the maximal number of columns, which are linearly independent over the base field F_q, and is denoted $\mathrm{Rk}_{\mathrm{col}}(\mathbf{M} \mid \mathsf{F}_q)$.

We distinguish two ranks of the matrix:

1. The usual rank of matrix $\mathbf{M}$ over F_{q^N} – $\mathrm{Rk}(\mathbf{M} \mid \mathsf{F}_{q^N})$.
2. The column rank of a matrix $\mathbf{M}$ over the base field F_q – $\mathrm{Rk}_{\mathrm{col}}(\mathbf{M} \mid \mathsf{F}_q)$.

The column rank of the matrix M depends on the field. In particular, $\mathrm{Rk}_{\mathrm{col}}(\mathbf{M} \mid \mathsf{F}_q) \geq \mathrm{Rk}_{\mathrm{col}}(\mathbf{M} \mid \mathsf{F}_{q^N})$

The Rank distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as the rank norm of the difference $\mathbf{x}-\mathbf{y}$:

$$d(\mathbf{x},\mathbf{y}) = \mathrm{Rk}(\mathbf{x}-\mathbf{y} \,|\, \mathbb{F}_q)$$

Any linear (n,k,d) code $\mathrm{C} \subset \mathbb{F}_{q^N}^n$ fulfils the Singleton-style bound [34] for the rank distance:

$$Nk \le Nn - (d-1)\max\{N,n\} \tag{1}$$

A code C reaching that bound is called a Maximal Rank Distance (MRD) code.

The theory of optimal MRD (Maximal Rank Distance) codes is given in [34].

The notation $g^{[i]} := g^{q^{i \bmod N}}$ means the i-th Frobenius power of g. It allows to consider both positive and negative Frobenius powers i.

For $n \le N$, a generator matrix $\mathbf{G}_k$ of a (n,k,d) MRD code is defined by a matrix of the following form:

$$\mathbf{G}_k = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ g_1^{[2]} & g_2^{[2]} & \cdots & g_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix} \tag{2}$$

Where $g_1, g_2, \ldots, g_n$ are any set of elements of the extension field $\mathbb{F}_{q^N}$ which are linearly independent over the base field $\mathbb{F}_q$.

A code with the generator matrix (2) is referred to as (n,k,d) MRD code, where n is code length, k is the number of information symbols, d is code distance. For MRD codes, $d = n-k+1$. Let $\mathbf{m} = (m_1, m_2, \ldots, m_k)$ be an information vector of dimension k. The corresponding code vector is the n-vector

$$\mathbf{g}(\mathbf{m}) = \mathbf{m}\mathbf{G}_k$$

If $\mathbf{y} = \mathbf{g}(\mathbf{m}) + \mathbf{e}$ and $\mathrm{Rk}(\mathbf{e} \,|\, \mathbb{F}_q) = s \le t = \dfrac{d-1}{2}$, then the information vector $\mathbf{m}$ can be recovered uniquely from $\mathbf{y}$ by some decoding algorithm. There exist fast decoding algorithms for MRD codes [34], [35]. A decoding procedure requires elements of the $(n-k)\times n$ parity check matrix $\mathbf{H}$ such that $\mathbf{G}_k\mathbf{H}^T = \mathbf{0}$. For decoding, the matrix $\mathbf{H}$ should be of the form

$$\mathbf{H} = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ h_1^{[2]} & h_2^{[2]} & \cdots & h_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \cdots & h_n^{[d-2]} \end{bmatrix}, \tag{3}$$

where elements $h_1, h_2, \ldots, h_n$ are in the extension field $\mathbb{F}_{q^N}$ and are linearly independent over the base field $\mathbb{F}_q$.

3.2 Description of the GPT Cryptosystem

Overview of the GPT Cryptosystem.

The GPT cryptosystem is described as follows:

Plaintext: A Plaintext is any k-vector $\mathbf{m} = (m_1, m_2, \ldots, m_k)$, $m_s \in \mathbb{F}_{q^N}$, $s = 1,2,\ldots,k$.

Public key: In previous works, different representations of the public key are given. All of them can be reduced to the following form.

The Public key is a $k\times(n+t_1)$ generator matrix

$$\mathbf{G}_{pub}=\mathbf{S}\begin{bmatrix}\mathbf{X} & \mathbf{G}_k \\ & \end{bmatrix}\mathbf{P} \qquad (4)$$

Let us explain roles of the factors.

- The main matrix $\mathbf{G}_k$ is given by equation (2). It is used to correct rank errors. Errors of rank not greater than $t=\lfloor\frac{n-k}{2}\rfloor$ can be corrected.
- A matrix $\mathbf{S}$ is a row scrambler. This matrix is a non singular square matrix of order k over the extension field F_{q^N} .
- A matrix $\mathbf{X}$ is a distortion $(k\times t_1)$ matrix over F_{q^N} with full column rank $\mathrm{Rk}_{\mathrm{col}}(X\,|\,\mathrm{F}_q)=t_1$ and rank $\mathrm{Rk}(\mathbf{X}\,|\,\mathrm{F}_{q^N})=t_X\,,t_X\le t_1$. The matrix $[\mathbf{X} \quad \mathbf{G}_k]$ has full column rank $\mathrm{Rk}_{\mathrm{col}}(\begin{bmatrix}\mathbf{X} & \mathbf{G}_k \\ & \end{bmatrix}|\,\mathrm{F}_q)=n+t_1$.
- A nonsingular matrix $\mathbf{P}$ is a square column scramble matrix of order (t_1+n) over the base field F_q .
- t_1+n may be greater than N , but $n\le N$.

The Private keys are matrices $\mathbf{S},\mathbf{G}_k,\mathbf{X},\mathbf{P}$ separately and (explicitly) a fast decoding algorithm of an MRD code. Note also, that the matrix $\mathbf{X}$ is not used to decrypt a ciphertext and can be deleted after calculating the Public key.

Encryption: Let $\mathbf{m}=(m_1,m_2,\dots,m_k),m_j\in\mathrm{F}_{q^N}$, be a plaintext. The corresponding ciphertext is given by

$$\mathbf{c}=\mathbf{m}\mathbf{G}_{\mathrm{pub}}+\mathbf{e}=\mathbf{m}\mathbf{S}\,[\mathbf{X} \quad \mathbf{G}_k]\,\mathbf{P}+\mathbf{e}, \qquad (5)$$

where $\mathbf{e}$ is an artificial vector of errors of rank t_2 or less. It is assumed that $t_2\le t=\lfloor\frac{n-k}{2}\rfloor$

Decryption: The legitimate receiver upon receiving $\mathbf{c}$ calculates

$$\mathbf{c}^{'}=(c_1^{'},c_2^{'},\dots,c_{t_1+n}^{'})=$$

$$\mathbf{c}\mathbf{P}^{-1}=\mathbf{m}\mathbf{S}\begin{bmatrix}\mathbf{X} & \mathbf{G}_k \\ & \end{bmatrix}+\mathbf{e}\mathbf{P}^{-1}$$

Then from $\mathbf{c}^{'}$ the extracts the subvector

$$\mathbf{c}^{''}=(c_{t_1+1}^{'},c_{t_1+2}^{'},\dots,c_{t_1+n}^{'})=\mathbf{m}\mathbf{S}\mathbf{G}_k+\mathbf{e}^{''}, \qquad (6)$$

where $\mathbf{e}^{''}$ is the subvector of $\mathbf{e}\mathbf{P}^{-1}$. Then the legitimate receiver applies the fast decoding algorithm to correct the error $\mathbf{e}^{''}$, extracts $\mathbf{m}\mathbf{S}$ and recovers m as $\mathbf{m}=(\mathbf{m}\mathbf{S})\mathbf{S}^{-1}$.

In this system, the size of the public key is $V=k\times(t_1+n)\times N\times\log_2 q$ bits, and the information rate is $R=\frac{k}{t_1+n}$.

Figure 3.2 depicts how the GPT cryptosystem operates, and shows where the attacks can be made.

4 The security of the GPT PKC

There are two types of attacks against the GPT cryptosystem and its variants. The first one is the decoding attacks which are described in Section 4.1. The second is structural attacks, we focus on Overbeck's attack in this paper as one of the most powerful structural attack against GPT cryptosystem. Overbeck's attack is discussed in Section 4.2.

4.1 Decoding Attacks

An important part of a decryption procedure is correcting rank errors using a fast decoding algorithm known to the legitimate party. An unauthorized party may attempt to correct rank errors by a general algorithm without any knowledge of the structure of a rank code. We consider algorithms described in [36], [37] and [38].

Johansson and Ourivski proposed two algorithms for decoding an arbitrary (n,k) linear rank distance code over $\mathbf{F}_{q^N}$ [36]. These algorithms correct errors of rank $t = \left\lfloor \frac{n-k}{2} \right\rfloor$ in operations over F_q.

$$\min\{\mathrm{O}\left((Nt)^3 q^{(t-1)(k+1)}\right), \mathrm{O}\left((k+t)^3 t^3 q^{(t-1)(N+t_1-t)}\right)\} \tag{7}$$

Furthermore, Levy-dit-Vehel et al introduced an algorithm which was described in [37]. It requires

$$\mathrm{O}\left(\log(q)\cdot(N+t_1)^{3(N+t_1-t)}\right) \tag{8}$$

Operations over F_q which is more complex than the Johannson and Ourivski algorithms.

Recently, Gaborit et al. proposed two new algorithms in [38], the first algorithm is combinatorial and generalizes a particular Hamming distance attack based on the error support in a rank metric context; the second algorithm introduced a new algebraic setting for solving the Rank Syndrome Decoding (RSD) problem. These algorithms require

$$\min\left(\mathrm{O}(n-k)^3 N^3 q^{r\left\lfloor \frac{kN}{n} \right\rfloor}, \mathrm{O}(n-k)^3 N^3 q^{(r-1)\left\lfloor \frac{(k+1)N}{n} \right\rfloor}\right). \tag{9}$$

Operations in F_{q^N} .If there exists an integer $v \le k$ such that $n-v \ge (r+1)(k+1-v)-1$ then an algorithm exists with an average complexity bounded above by

$$O((nkv+t^3k^3)q^{tv}) \tag{10}$$

operations in F_{q^N} .Let us consider the following example as case study in order to evaluate the GPT cryptosystem against Decoding attacks. Complexities of the above attacks to correct $t=2$ rank errors are as follows:

$N = n = 12, t_1 = 4, k = 8, q = 2^8, d = 5, t = 2$.

1. Public key size $V = N \times k \times (t_1 + n) \times \log_2 q$ = $12 \times 8 \times 16 \times 8$ = 12288 bits.
2. Johannson and Ourivski algorithms Eq.(7) – 2^{85} operations in F_{256} .
3. Levy-dit-Vehel et al Eq. (8) – 2^{171} operations in F_{256} .
4. Gaborit et al. first algorithm Eq. (9) – 2^{88} operations in F_{256} .
5. Gaborit et al. second algorithm Eq. (10) – 2^{140} operations in F_{256} .

In brief, the Decoding attacks are infeasible for practical implementations against the GPT cryptosystem and its variants. Hence, the GPT cryptosystem is secure against the Decoding attacks.

4.2 Overbeck's Attack

Overbeck introduced a potential structural attack against the GPT cryptosystem and its variants [16, 17], and [18]. We summarize Overbeck's attack below. We outline the following notations to representing the fundamentals of Overbeck's attack. For $x \in \mathbb{F}_{q^N}$ let $\sigma(x) = x^q$ be the Frobenius automorphism.

For the matrix $\mathbf{T} = (t_{ij})$ over $\mathbb{F}_{q^N}$, let $\sigma(\mathbf{T}) = (\sigma(t_{ij})) = (t_{ij}^q)$.

For any integer s, let $\sigma^s(\mathbf{T}) = \sigma(\sigma^{s-1}(\mathbf{T}))$.

It is clear that $\sigma^N = \sigma$. Thus the inverse exists $\sigma^{-1} = \sigma^{N-1}$.

The following simple properties if σ are useful:

- $\sigma(a+b) = \sigma(a) + \sigma(b)$.
- $\sigma(ab) = \sigma(a)\sigma(b)$.
- In general, for matrices $\sigma(\mathbf{T}) \neq \mathbf{T}$.
- If $\mathbf{P}$ is a matrix over the base field $\mathbb{F}_q$, then $\sigma(\mathbf{P}) = \mathbf{P}$.

Description of Overbeck's attack: To break the GPT cryptosystem, a cryptanalyst constructs an integer u from the public key $\mathbf{G}_{\text{pub}} = \mathbf{S}[\mathbf{X} \quad \mathbf{G}_k]\mathbf{P}$, to provide its corresponding extended public key $\mathbf{G}_{\text{ext,pub}}$. Overbeck's attack is described as follows:

$$\mathbf{G}_{\text{ext,pub}} = \begin{Vmatrix} \mathbf{G}_{\text{pub}} \\ \sigma(\mathbf{G}_{\text{pub}}) \\ \sigma^2(\mathbf{G}_{\text{pub}}) \\ \cdots \\ \sigma^u(\mathbf{G}_{\text{pub}}) \end{Vmatrix} = \begin{Vmatrix} \mathbf{S} & [\mathbf{X} & \mathbf{G}_k] & \mathbf{P} \\ \sigma(\mathbf{S}) & [\sigma(\mathbf{X}) & \sigma(\mathbf{G}_k)] & \mathbf{P} \\ \sigma^2(\mathbf{S}) & [\sigma^2(\mathbf{X}) & \sigma^2(\mathbf{G}_k)] & \mathbf{P} \\ \cdots & \cdots\cdots\cdots & & \cdots \\ \sigma^u(\mathbf{S}) & [\sigma^u(\mathbf{X}) & \sigma^u(\mathbf{G}_k)] & \mathbf{P} \end{Vmatrix} \tag{11}$$

The property that $\sigma(\mathbf{P}) = \mathbf{P}$, if $\mathbf{P}$ is a matrix over the base field $\mathbb{F}_q$, as described in equation (11).

Rewrite this matrix as

$$\mathbf{G}_{\text{ext,pub}} = \mathbf{S}_{\text{ext}}[\mathbf{X}_{\text{ext}} \quad \mathbf{G}_{\text{ext}}]\mathbf{P}, \tag{12}$$

where

$$\mathbf{S}_{\text{ext}} = \text{Diag}(\mathbf{S} \quad \sigma(\mathbf{S}) \quad \dots \quad \sigma^u(\mathbf{S}))$$

$$\mathbf{X}_{\text{ext}} = \begin{bmatrix} \mathbf{X} \\ \sigma(\mathbf{X}) \\ \vdots \\ \sigma^u(\mathbf{X}) \end{bmatrix}, \quad \mathbf{G}_{\text{ext}} = \begin{bmatrix} \mathbf{G}_k \\ \sigma(\mathbf{G}_k) \\ \vdots \\ \sigma^u(\mathbf{G}_k) \end{bmatrix}$$

Choose

$$u = n - k - 1 \tag{13}$$

For a matrix

$$\mathbf{X} = \begin{bmatrix} X_{11} & X_{12} & \dots & X_{1,t_1} \\ X_{21} & X_{22} & \dots & X_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ X_{k-1,1} & X_{k-1,2} & \dots & X_{k-1,t_1} \\ X_{k,1} & X_{k,2} & \dots & X_{k,t_1} \end{bmatrix}, \tag{14}$$

let

$$\mathbf{X}_1 = \begin{bmatrix} X_{11} & X_{12} & \dots & X_{1,t_1} \\ X_{21} & X_{22} & \dots & X_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ X_{k-1,1} & X_{k-1,2} & \dots & X_{k-1,t_1} \end{bmatrix} \tag{15}$$

be the $(k-1)\times t_1$ matrix, obtained from $\mathbf{X}$ by deleting the last row. Let

$$\mathbf{X}_2 = \begin{bmatrix} X_{21} & X_{22} & \dots & X_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ X_{k-1,1} & X_{k-1,2} & \dots & X_{k-1,t_1} \\ X_{k,1} & X_{k,2} & \dots & X_{k,t_1} \end{bmatrix} \tag{16}$$

be the $(k-1)\times t_1$ matrix, obtained from $\mathbf{X}$ by deleting the first row.

Define a linear mapping $T : \mathrm{F}_{q^N}^{k\times t_1} \to \mathrm{F}_{q^N}^{(k-1)\times t_1}$ by the rule: if $\mathbf{X} \in \mathrm{F}_{q^N}^{k\times t_1}$, then

$$T(\mathbf{X}) = \mathbf{Y} = \sigma(\mathbf{X}_1) - \mathbf{X}_2$$

Let

$$\mathbf{Y}_{\text{ext}} = \begin{bmatrix} \mathbf{Y} \\ \sigma(\mathbf{Y}) \\ \sigma^2(\mathbf{Y}) \\ \dots \\ \sigma^{u-1}(\mathbf{Y}) \end{bmatrix} \tag{17}$$

Using suitable transformations of rows, therefore, equation (12) can be rewritten on the following form:

$$\tilde{\mathbf{G}}_{\text{pub,ext}} = \tilde{\mathbf{S}}_{\text{ext}} \begin{bmatrix} \mathbf{Z} & | & \mathbf{G}_{n-1} \\ \mathbf{Y}_{\text{ext}} & | & 0 \end{bmatrix} \mathbf{P} \tag{18}$$

where $\mathbf{G}_{n-1}$ is the generator matrix of the $(n, n-1, 2)$ MRD code.

Let us try to find a solution $\mathbf{u}$ of the system

$$\tilde{\mathbf{S}}_{\text{ext}} \begin{bmatrix} \mathbf{Z} & | & \mathbf{G}_{n-1} \\ \mathbf{Y}_{\text{ext}} & | & 0 \end{bmatrix} \mathbf{Pu}^T = \mathbf{0}, \tag{19}$$

where $\mathbf{u}$ is a vector-row over the extension field F_{q^N} of length $t_1 + n$. Represent the vector $\mathbf{Pu}^T$ as

$$\mathbf{Pu}^T = [\mathbf{y} \quad \mathbf{h}]^T,$$

Where the subvector $\mathbf{y}$ has length t_1 and $\mathbf{h}$ has length n. Hence, equation (19) is equivalent to the following equation:

$$\mathbf{Zy}^T + \mathbf{G}_{n-1}\mathbf{h}^T = \mathbf{0}, \tag{20}$$

$$\mathbf{Y}_{\text{ext}}\mathbf{y}^T = \mathbf{0} \tag{21}$$

Assume that the next condition is valid:

$$\mathrm{Rk}(\mathbf{Y}_{\text{ext}} \,|\, \mathrm{F}_{q^N}) = t_1 \tag{22}$$

Then the equation (21) has only the trivial solution $\mathbf{y}^T = \mathbf{0}$. Thus, the equation (20) becomes

$$\mathbf{G}_{n-1}\mathbf{h}^T = \mathbf{0} \tag{23}$$

It allows to find the first row of the parity check matrix for the code with the generator matrix equation (18) (see,[16, 17], and [18], for details). Hence this solution breaks a GPT cryptosystem and its variants in a polynomial time. The Overbeck attack requires $O((n+t_1)^3)$ operation over F_{q^N} in order to break the system.

The property that $\sigma(\mathbf{P}) = \mathbf{P}$ is valid if matrix $\mathbf{P}$ is over the base field F_q, as shown in equation (11). As a result of that, the first row of the parity check matrix $\mathbf{H}$ of the rank code can be obtained as described by Overbeck, and then the cryptosystem can be broken easily. However, if a matrix $\mathbf{P}$ is over the extension field F_{q^N}, then $\sigma(\mathbf{P}) \neq \mathbf{P}$. Consequently, the Overbeck's attack cannot be applied even the distortion matrix $\mathbf{X}$ does not exist. The distortion matrix $\mathbf{X}$ is an additional parameter to the GPT cryptosystem to increase its security. although, it is a fundamental parameter of the GPT cryptosystem.

5 Solution based on distortion matrix $\mathbf{X}$

In the following Sections: the Smart approach is described briefly in Subsection 5.1, and the Distortion matrix approach (DMA) is presented in Subsection 5.2.

5.1 Smart Approach

The smart approach was introduced in [19]. It is based on a particular choice of the distortion matrix $\mathbf{X}$. It allows for withstanding all known attacks even if the column scrambler matrix $\mathbf{P}$ over the base field F_q. In this Section, our intentions are to review and evaluate the overall security of the smart approach.

The cryptographer should choose the matrix $\mathbf{X}$ of the public key $\mathbf{G}_{\text{pub}} = \mathbf{S}\begin{bmatrix} \mathbf{X} & \mathbf{G}_k \end{bmatrix}\mathbf{P}$ in the following manner in order to countermeasure Overbeck's attack:

$$\begin{aligned}&\mathrm{Rk}_{\mathrm{col}}(\mathbf{X}\,|\,\mathsf{F}_q)=t_1,\\&\mathrm{Rk}_{col}(\mathbf{Y}\,|\,\mathsf{F}_q)=b,\\&\mathrm{Rk}(\mathbf{Y}_{\mathrm{ext}}\,|\,\mathsf{F}_{q^N})=t_1-a,\end{aligned} \qquad (24)$$

where $b \le t_1, a \ge 1$. In this case, equation (21) has q^{aN} solutions $\mathbf{y}^T$. Hence the exhaustive search over $\mathbf{y}^T$ is needed. The work function has order $O(q^{aN}(n+t_1)^3)$ and Overbeck's attack fails. However, it is not always the case therefore we consider two other cases to evaluate security of the Smart approach.

First case, consider that a matrix $\mathbf{X}$ is chosen in such a manner that the matrix $\mathbf{Y(X)}$ has all entries in the base field F_q, $b=t_1-a$, $a \ge 2$. It is possible to construct matrix $\mathbf{X}$ as described in equation (24), although the system will be vulnerable to an attack similar to Ovebeck's one. Thus the smart approach is vulnerable for $a \ge 2$.

The first open question: Is it possible to construct a matrix $\mathbf{X}$ to prevent the Overback attack for $a=1$?

Second case, allow matrix $\mathbf{Y}$ to be over the extension field F_{q^N}.

The second open question: Is it possible to construct the matrix $\mathbf{X}$ as in equation (24) in such way to prevent the Overback attack for $b = t_1,\ a \ge 1$?

We give answers for the first question in this Section, while answers of the second question will be in Section 5.2.

An overview of the Smart approach is demonstrated as follows:

The following result is evident. Let the column rank of $\mathbf{Y}$ be $\mathrm{Rk}_{\mathrm{col}}(\mathbf{Y}\,|\,\mathsf{F}_q)=s$. Then $\mathrm{Rk}_{\mathrm{col}}(\mathbf{Y}_{\mathrm{ext}}\,|\,\mathsf{F}_q)=s$. $\mathrm{Rk}(\mathbf{Y}_{\mathrm{ext}}\,|\,\mathsf{F}_{q^N}) \le \mathrm{Rk}(\mathbf{Y}_{\mathrm{ext}}\,|\,\mathsf{F}_q)=s=\mathrm{Rk}(\mathbf{Y}\,|\,\mathsf{F}_q)$.

Let $t_1 \le k$. Let $\mathbf{X}$ be a $k \times t_1$ matrix over the base field F_q:

$$\mathbf{X}=\begin{bmatrix}\mathbf{s_0}\\ \mathbf{s}_1\\ \vdots\\ \mathbf{s}_{k-1}\end{bmatrix}.$$

Here $\mathbf{s}_i, i=0,\ldots,k-1,$ are row vectors over F_q of dimension t_1. The corresponding $(k-1)\times t_1$ matrix $\mathbf{Y}=T(\mathbf{X})$ in this case is as follows:

$$\mathbf{Y}=T(\mathbf{X})=\begin{bmatrix}\mathbf{s}_0-\mathbf{s}_1\\ \mathbf{s}_1-\mathbf{s}_2\\ \vdots\\ \mathbf{s}_{k-2}-\mathbf{s}_{k-1}\end{bmatrix}. \qquad (25)$$

There exists a matrix $\mathbf{X}$ of full ordinary and column rank t_1 such that the matrix $\mathbf{Y}=T(\mathbf{X})$ has column rank t_1-1.

Proof. Choose a nonzero column vector $\mathbf{u}^{\mathrm{T}}=\begin{bmatrix}u_1 & u_2 & \ldots & u_{t_1}\end{bmatrix}^{\mathrm{T}}$ and a nonzero element $g \in \mathsf{F}_q$. Find all solutions $\mathsf{S}=\{\mathbf{s}\}$ of the equation

$$\mathbf{s}\mathbf{u}^{\mathrm{T}}=g. \qquad (26)$$

The set S contains exactly q^{t_1-1} different row vectors $\mathbf{s}$. Moreover, there exist among them subsets of t_1 vectors which are linearly independent over F_q. Use such a subset as rows of the matrix $\mathbf{X}$. Fill other rows by vectors from the set S. We have got the matrix $\mathbf{X}$ of full ordinary and column rank t_1. Note that

$$\mathbf{Yu}^{\mathrm{T}} = \begin{bmatrix} \mathbf{s}_0 - \mathbf{s}_1 \\ \mathbf{s}_1 - \mathbf{s}_2 \\ \vdots \\ \mathbf{s}_{k-2} - \mathbf{s}_{k-1} \end{bmatrix} \mathbf{u}^{\mathrm{T}} = 0, \qquad (27)$$

since the condition in equation (26) is valid. This means that columns of $\mathbf{Y}$ are linearly dependent over F_q. Hence $\mathrm{Rk}_{\mathrm{col}}(\mathbf{Y} \,|\, \mathsf{F}_q) = t_1 - 1$.

Let $N = n = 12, k = 8, d = 5, t = 2, t_1 = 4, q = 2^8, a = 1$

- Public key size $V = N \times k \times (t_1 + n) \times \log_2 q$ = $12 \times 8 \times 16 \times 8$ = 12288 bits.
- Information rate $R = \dfrac{k}{t_1 + n} = \dfrac{8}{16} = 0.5$.
- Minimum security – Overbeck's attack $q^{aN}(n + t_1)^3 = 2^{96} \cdot (14)^3 = 2^{108}$.
- Minimum security – Decoding attacks by Eq.'s (7)-(10) $\mathsf{O}\left((Nt)^3 q^{(t-1)(k+1)}\right) = 2^{85}$.

5.2 Distortion matrix approach (DMA)

We presented in the previous subsection the construction of the distortion matrix $\mathbf{X}$ over the base field F_q satisfying conditions in equation (24) for $b = t_1 - 1, a = 1$. The crucial point is the equality $\mathrm{Rk}_{col}(\mathbf{Y} \,|\, \mathbf{F}_q) = \mathrm{Rk}(\mathbf{Y}_{\mathrm{ext}} \,|\, \mathbf{F}_{q^N}) = t_1 - 1$. It seems that for $b < t_1, a \geq 2$ a distortion matrix $\mathbf{X}$ over the base field does not exist with property $\mathrm{Rk}_{col}(\mathbf{Y} \,|\, \mathbf{F}_q) = b$. Therefore we have to introduce a matrix $\mathbf{X}$ over the extension field F_{q^N} satisfying conditions in equation (24) for $b = t_1, a \geq 2$.

One method to provide the conditions (24) is proposed independently in [20] and [21]. They recommend to choose the matrix $\mathbf{X}$ over the extension field F_{q^N} in such a manner that the following conditions are satisfied:

$$\begin{array}{lclcl} t_1 & = & \mathrm{Rk}_{\mathrm{col}}(\mathbf{X} \,|\, \mathsf{F}_q) & > & n - k \\ r_X & = & \mathrm{Rk}(\mathbf{X} \,|\, \mathsf{F}_{q^N}) & = & \left\lfloor \dfrac{t_1 - a}{n - k} \right\rfloor \leq k \end{array} \qquad (28)$$

However, the column rank of matrix $\mathbf{Y}$ over the base field F_q has to be equal to t_1. They neither mentioned this fact nor proposed how the matrix $\mathbf{X}$ can be constructed. In addition, they recommended a set of parameters to be secure against Overbeck's attack. Although, all parameters sets proposed in [21] have been broken by Gaborit et al., the second set of parameters which were supposed to be stronger than the first one can in fact by attacked in a few seconds with hybrid Grbner bases attack as shown in [38].

The existing smart approach as described in the previous section has a column rank less than t_1 for the matrix $\mathbf{Y}$. Consequently, the main aim of this section is to show how the matrix $\mathbf{X}$ can be constructed to meet the conditions in equation (24) with $b = t_1$. The new construction of matrix $\mathbf{X}$ is described as follows:

Let $\mathbf{m}_0$ be a t_1 -vector of rank exactly t_1. Let $\mathbf{m}_1, \ldots, \mathbf{m}_{k-1}$ be t_1 -vectors and at least one of vectors has rank exactly t_1. Construct a matrix

$$\mathbf{X} = \begin{bmatrix} \mathbf{m}_0 \\ \mathbf{m}_0^{[1]} + \mathbf{m}_1 \\ \mathbf{m}_0^{[2]} + \mathbf{m}_1^{[1]} + \mathbf{m}_2 \\ \mathbf{m}_0^{[3]} + \mathbf{m}_1^{[2]} + \mathbf{m}_2^{[1]} + \mathbf{m}_3 \\ \vdots \\ \mathbf{m}_0^{[k-1]} + \mathbf{m}_1^{[k-2]} + \ldots + \mathbf{m}_{k-1} \\ \end{bmatrix} \tag{29}$$

This matrix has the column rank t_1 and the ordinary rank not greater than k.

Calculating the matrix $\mathbf{Y} = \sigma(\mathbf{X}_1) - \mathbf{X}_2$ gives

$$\mathbf{Y} = \sigma(\mathbf{X}_1) - \mathbf{X}_2 = -\begin{bmatrix} \mathbf{m}_1 \\ \mathbf{m}_2 \\ \mathbf{m}_3 \\ \vdots \\ \mathbf{m}_{k-1} \\ \end{bmatrix} \tag{30}$$

Let one of vectors, say, $\mathbf{m}_i$ be of rank t_1. Choose other vectors either as multiples of $\mathbf{m}_i$, or as the all zero vectors. Therefore

$$\begin{gathered} \mathrm{Rk}_{\mathrm{col}}(\mathbf{Y} \mid \mathsf{F}_q) = t_1, \mathrm{but} \\ \mathrm{Rk}(\mathbf{Y} \mid \mathsf{F}_{q^N}) = 1 \end{gathered} \tag{31}$$

It follows that

$$\begin{gathered} \mathrm{Rk}_{\mathrm{col}}(\mathbf{Y}_{\mathrm{ext}} \mid \mathsf{F}_q) = t_1, \mathrm{but} \\ \mathrm{Rk}(\mathbf{Y}_{\mathrm{ext}} \mid \mathsf{F}_{q^N}) = u = n - k - 1 \end{gathered} \tag{32}$$

Now choose $n - k - 1 = t_1 - a$, or $t_1 = n - k - 1 + a$. Then the equation (24) will be satisfied.

Let $N = n = 12, k = 8, d = 5, t = 2, q = 2^8, a = 2, t_1 = n - k - 1 + a = 5$.

- Public key size $V = N \times k \times (t_1 + n) \times \log_2 q$ = $12 \times 8 \times 17 \times 8$ = 13056 bits.
- Information rate $R = \dfrac{k}{t_1 + n} = \dfrac{8}{17} = 0.47$.
- Minimum security – Overbeck's attack $q^{aN}(n + t_1)^3$ = $2^{192}(17)^3$ = 2^{204}.
- Minimum security – Decoding attacks by Eq.'s (7)-(10) $O\left((Nt)^3 q^{(t-1)(k+1)}\right) = 2^{85}$.

As can be seen clearly from this Section that the DMA is secure against Overbeck's and decoding attacks.

6 Solution based on scramble matrix P

In the following Sections: firstly, we give a short introduction about reducible rank codes in Section 6.1; secondly, we review the GPT cryptosystem which based on reducible rank codes in Section 6.2; finally, we propose the Advanced approach for Reducible rank codes in Section 6.3.

6.1 Reducible rank codes

Let $\mathbf{G}^1, \mathbf{G}^2, \ldots, \mathbf{G}^r$ be generator matrices of linear (n_i, k_i) codes over the field F_{q^N}, $i = 1, \ldots, r$. We shall consider the case, when all $n_i = n$, $k_i = k$ and all $\mathbf{G}^i = \mathbf{G}_k$. The matrix $\mathbf{G}_k$ is the generator matrix of a MRD (n, k, d) code.

A code C is called reducible if its generator matrix $\mathbf{G}$ can be represented as

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_k & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{G}_{2,1} & \mathbf{G}_k & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{G}_{3,1} & \mathbf{G}_{3,2} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{G}_{r-1,1} & \mathbf{G}_{r-1,2} & \cdots & \mathbf{G}_k & \mathbf{0} \\ \mathbf{G}_{r,1} & \mathbf{G}_{r,2} & \cdots & \mathbf{G}_{r,r-1} & \mathbf{G}_k \end{bmatrix} \qquad (33)$$

Matrices $\mathbf{G}_{i,j}$ are random $k \times n$ matrices, $i = 2, \ldots, r$, $j = 1, \ldots, r-1$, over F_{q^N}. This matrix defines a MRD reducible rank code with parameters: length $n_{\text{total}} = nr$, dimension $k_{\text{total}} = kr$, rank code distance $d = n - k + 1$.

Let $\mathbf{m} = (\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_r)$ be an information sequence with entries in F_{q^N}. This sequence can be viewed as a concatenation of r subblocks of length k. Then the codeword is defined by

$$\mathbf{g} = \mathbf{mG} = (\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r),$$

where $\mathbf{g}_i$, $i = 1, 2, \ldots, r,$ is a subblock of length n:

$$\mathbf{g}_1 = \mathbf{m}_1\mathbf{G}_k + \mathbf{m}_2\mathbf{G}_{2,1} + \ldots + \mathbf{m}_r\mathbf{G}_{r,1},$$

$$\mathbf{g}_2 = \mathbf{m}_2\mathbf{G}_k + \mathbf{m}_3\mathbf{G}_{3,2} + \ldots + \mathbf{m}_r\mathbf{G}_{r,2},$$

$$\vdots$$

$$\mathbf{g}_{r-1} = \mathbf{m}_{r-1}\mathbf{G}_k + \mathbf{m}_r\mathbf{G}_{r,r-1},$$

$$\mathbf{g}_r = \mathbf{m}_r\mathbf{G}_k$$

To decode, begin with the last subblock $\mathbf{g}_r$ by applying to it a usual fast decoding algorithm for MRD codes, and obtain the last information subblock $\mathbf{m}_r$. Proceed further with $\mathbf{g}_{r-1} - \mathbf{m}_r\mathbf{G}_{r,r-1} = \mathbf{m}_{r-1}\mathbf{G}_k$ to obtain $\mathbf{m}_{r-1}$, and so on until $\mathbf{m}_1$.

6.2 The GPT PKC Based on Reducible Rank Codes

The GPT cryptosystem based on reducible rank codes is described as follows:

Plaintext: A Plaintext is any $k_{\text{total}} = kr$-vector $\mathbf{m} = (\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_r)$ consisting of r subblocks

$m_s \in \mathbb{F}_{q^N}^{k}$, $s = 1,2,\ldots,r$.

The Public key is the following generator matrix with size $k_{\text{total}} \times L$, where $L = n_{\text{total}} + t_1$:

$$\mathbf{G}_{\text{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{X} & \mathbf{G}\end{bmatrix}\mathbf{P} \qquad (34)$$

Let us explain roles of the factors.

The matrix $\mathbf{G}$ is a generator matrix (33).

The Private keys are matrices $\mathbf{S}, \mathbf{G}, \mathbf{X}, \mathbf{P}$ separately and (explicitly) a fast decoding algorithm of an MRD code.

Encryption: Let $\mathbf{m} = (\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_r)$ be a plaintext. Note that the product

$$\mathbf{mS}\begin{bmatrix}\mathbf{X} & \mathbf{G}\end{bmatrix}$$

can be represented as

$$[\mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r], \qquad (35)$$

where $\mathbf{g}_0$ is a distortion subblock of length t_1, while all the other subblocks of length n each form a code vector of reducible rank code. The corresponding ciphertext is calculated as

$$\mathbf{c} = \mathbf{mG}_{\text{pub}} + \mathbf{e} = \mathbf{mS}\begin{bmatrix}\mathbf{X} & \mathbf{G}\end{bmatrix}\mathbf{P} + \mathbf{e} = [\mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r]\mathbf{P} + \mathbf{e}, \qquad (36)$$

where $\mathbf{e}$ is an artificial vector of errors of rank t_2 or less. It is assumed that $t_1 + t_2 \le t = \lfloor \frac{n-k}{2} \rfloor$

Decryption: The legitimate receiver knows the matrix $\mathbf{P}$ and upon receiving $\mathbf{c}$ calculates

$$\begin{aligned}\mathbf{c}' &= \mathbf{cP}^{-1} = \mathbf{mS}\begin{bmatrix}\mathbf{X} & \mathbf{G}\end{bmatrix} + \mathbf{eP}^{-1} \\ &= [\mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r] + \mathbf{e}' \\ &= [\mathbf{g}_0 + \mathbf{e}_0', \mathbf{g}_1 + \mathbf{e}_1', \mathbf{g}_2 + \mathbf{e}_2', \ldots, \mathbf{g}_r + \mathbf{e}_r']\end{aligned} \qquad (37)$$

Assume that design parameters are chosen such that

$$\mathrm{Rk}(\mathbf{e}_i' \mid \mathbb{F}_q) \le t,\ i = 1,2,\ldots,r \qquad (38)$$

Then the legitimate user can recover the information sequence $\mathbf{m}$ starting with the last subblock and using known to him a fast decoding algorithm.

6.3 Advanced Approach for Reducible Rank Codes (ARC)

The legitimate user should choose its design parameters similar to equation (38). It was assumed in the previous works, that a column scrambler $\mathbf{P}$ is chosen over the base field $\mathbb{F}_q$. In this case, $\mathrm{Rk}(\mathbf{e} \mid \mathbb{F}_q) = \mathrm{Rk}(\mathbf{eP}^{-1} \mid \mathbb{F}_q)$. It is clear that always $\mathrm{Rk}(\mathbf{e}_i' \mid \mathbb{F}_q) \le \mathrm{Rk}(\mathbf{e}' \mid \mathbb{F}_q)$. Hence it was enough to choose artificial errors $\mathbf{e}$ with rank $\mathrm{Rk}(\mathbf{e} \mid \mathbb{F}_q) \le t$ to satisfy equation (38).

On the other hand, the crucial point of Overbeck's attacks is just the assumption that a column scrambler $\mathbf{P}$ is chosen over the base field $\mathbb{F}_q$. If it is not a case, then his attacks fail.

We establish conditions, when equation (38) is valid for a matrix $\mathbf{P}$ over the extension field $\mathbb{F}_{q^N}$.

Let $\mathbf{e}$ be a vector of length $n_{\text{total}} + t_1$ and let $\mathrm{Rk}(\mathbf{e} \mid \mathbb{F}_q) = t_2$. Let $\mathbf{L}$ be a $(n_{\text{total}} + t_1) \times n$ matrix of ordinary rank n

and consisting of ν columns having entries in F_q and $n-\nu$ columns having entries in F_{q^N} .

$$\mathrm{Rk}(\mathbf{eL}\,|\,\mathsf{F}_q) \le \min\{t_2,\nu\} + n - \nu \tag{39}$$

Proof. The column rank of the row vector $\mathbf{eL}$ is not greater than the sum of ranks of two subvectors. The first subvector originates from the product $\mathbf{e}$ and those columns of $\mathbf{L}$ which have entries in F_q. It is clear that the rank of this part equals $\min\{t_2,\nu\}$. The second part originates from the product $\mathbf{e}$ and those columns of $\mathbf{L}$ which have entries in F_{q^N}. Its rank is not greater than $n-\nu$. This concludes proof.

Choose $n-\nu \le t-t_2$. Then

$$\mathrm{Rk}(\mathbf{eL}\,|\,\mathsf{F}_q) \le t_2 + (t-t_2) = t \tag{40}$$

We will show now how the matrix $\mathbf{P}$ can be constructed. Therefore, its inverse matrix $\mathbf{P}^{-1}$ should be chosen and concatenated of submatrices as follows:

$$\mathbf{P}^{-1} = \begin{bmatrix} \mathbf{L}_0 & \mathbf{L}_1 & \mathbf{L}_2 & \dots & \mathbf{L}_r \end{bmatrix}$$

The submatrix $\mathbf{L}_0$ is a $(n_{\text{total}}+t_1)\times t_1$ matrix. Choose its entries in the extension field F_{q^N}.

Submatrices $\mathbf{L}_i, i=1,2,\dots,r,$ are $(n_{\text{total}}+t_1)\times n$ matrices. Choose in each matrix $\nu = n-t+t_2$ columns with entries in the base field F_q and $n-\nu = t-t_2$ columns with entries in the extension field F_{q^N}.

By definition that an artificial error $\mathbf{e}$ has rank t_2. Therefore we have for $i=1,2,\dots,r,$ that $\mathrm{Rk}(\mathbf{eL}\,|\,\mathsf{F}_q) \le t.$

We construct a proper column scrambler $\mathbf{P}$, which makes Overbeck's attacks invalid.

Let $N=n=15, k=7, d=9, t=4, t_1=2, t_2=2, q=2^8, r=2, n_{\text{total}}=30, k_{\text{total}}=14$. Let the extension field be $\mathsf{F}_{2^{15}}$.

- Public key size is a $k_{\text{total}}\times(n_{\text{total}}+t_1)\times N\times\log_2 q$ = $14\times32\times15\times8 = 53760$ bits
- Information rate $R = \dfrac{k_{\text{total}}}{(n_{\text{total}}+t_1)} = \dfrac{14}{32} = 0.44$
- Minimum security – Overbeck's attack $\mathsf{O}(q^{(t_2)N}(n_{\text{total}}+t_1)^3) = 2^{255}$.
- Minimum security – Decoding attacks by Eq.'s (7)-(10) $\mathsf{O}\left((Nt)^3 q^{(t-1)(k+1)}\right) = 2^{209}$.

According to this section Overbeck's attack based on reducible rank codes is ineffective.

7 Description of the Simple Variant of the GPT cryptosystem

The GPT cryptosystem is described as follows.

$$\mathbf{G}_{\text{pub}} = \mathbf{S}\mathbf{G}_k\mathbf{P}. \tag{41}$$

- The main matrix $\mathbf{G}_k$ is given by equation (2). It is used to correct rank errors. Errors of rank not greater than $t = \lfloor \dfrac{n-k}{2} \rfloor$ can be corrected.

- A matrix $\mathbf{S}$ is a row scrambler. This matrix is a non singular square matrix of order k over the extension field $\mathbb{F}_{q^N}$.
- A nonsingular matrix $\mathbf{P}$ is a square column scramble matrix of order n over the extension field $\mathbb{F}_{q^N}$.

Consider the public key of Eq. (41). No distortion matrix $\mathbf{X}$ is used. A ciphertext has the following form

$$\mathbf{c} = \mathbf{mSG}_k\mathbf{P} + \mathbf{e}, \tag{42}$$

where the rank $\mathrm{Rk}(\mathbf{e}\,|\,\mathbb{F}_q) = t_s$ of an artificial error $\mathbf{e}$ is less or equal to $t = \lfloor\frac{n-k}{2}\rfloor$.

Decoding attacks are based on the exhaustive search of possible artificial errors $\mathbf{e}$. It depends on the number of error vectors. If artificial errors are all possible n-vectors of rank t_s, then the complexity against Overbeck's attack is $O\left(q^{nt_s}\right)$. The Public key size is $V = N \times n \times k \times \log_2 q.$

Assume first that the column scrambler $\mathbf{P}$ is a matrix over the base field $\mathbb{F}_q$. The legitimate user knows the secret key $\mathbf{P}$ and $\mathbf{P}^{-1}$. The Decryption algorithm is as follows:

1. Get a ciphertext $\mathbf{c} = \mathbf{mSG}_k\mathbf{P} + \mathbf{e}$.
2. Multiply to the right by $\mathbf{P}^{-1}$. Get an intermediate ciphertext

$$\mathbf{c}' = \mathbf{cP}^{-1} = \mathbf{mSG}_k + \mathbf{eP}^{-1}. \tag{43}$$

Note that $\mathrm{Rk}(\mathbf{eP}^{-1}\,|\,\mathbb{F}_q) = \mathrm{Rk}(\mathbf{e}\,|\,\mathbb{F}_q) = t_s \le t = \lfloor\frac{n-k}{2}\rfloor$ since $\mathbf{P}^{-1}$ is over the base field $\mathbb{F}_q$.

3. Decode $\mathbf{c}'$ using a fast decoding algorithm and get $\mathbf{mS}$.
4. Get a plaintext $\mathbf{m}$ as $(\mathbf{mS})\mathbf{S}^{-1}$.

The situation is quite different if $\mathbf{P}$ is a matrix over the extension field $\mathbb{F}_{q^N}$.

We can assume from now on that Overbeck's attack cannot be implemented. But the cryptographer should select a secret column scrambler $\mathbf{P}$ over the extension field $\mathbb{F}_{q^N}$ and a public set E of artificial errors $\mathbf{e}$ such that

$$\mathrm{Rk}(\mathbf{eP}^{-1}\,|\,\mathbb{F}_q) \le t = \left\lfloor\frac{n-k}{2}\right\rfloor, \tag{44}$$

where $\mathbf{eP}^{-1}$ is an error in the intermediate ciphertext (43).

Choice of E

The public set of artificial errors is chosen as the set consisting of all n-vectors in $\mathbb{F}_{q^N}^n$ with rank $t_s < t$:

$$\mathsf{E} = \left\{\mathbf{e}\;\mathbf{e} \in \mathbb{F}_{q^N}^n,\ \mathrm{Rk}(\mathbf{e}\,|\,\mathbb{F}_q) = t_s\right\}.$$

Choice of $\mathbf{P}$

The cryptographer chooses an inverse matrix $\mathbf{P}^{-1}$ in the form $\mathbf{P}^{-1} = \left[\mathbf{Q}_1 \quad \mathbf{Q}_2\right]$, where $\mathbf{Q}_1$ is a submatrix of size $n \times (t - t_s)$ with entries in the extension field $\mathbb{F}_{q^N}$ while $\mathbf{Q}_2$ is a submatrix of size $n \times (n - t + t_s)$ with entries in the base field $\mathbb{F}_q$. Let $\mathbf{e}$ be any n-vector of rank t_s. Then the condition Eq. (44) is hold.

Proof. We have $\mathbf{e}\mathbf{P}^{-1} = \mathbf{e}\left[\mathbf{Q}_1 \quad \mathbf{Q}_2\right] = \left[\mathbf{e}\mathbf{Q}_1 \quad \mathbf{e}\mathbf{Q}_2\right]$. A vector $\mathbf{e}$ can be represented as $\mathbf{e} = \left[\mathbf{w}_1 \quad \mathbf{w}_2 \quad \dots \quad \mathbf{w}_{t_s}\right]\mathbf{A}$, where $\mathbf{w}_j$'s are linearly independent over $\mathbb{F}_q$ and $\mathbf{A}$ is the $t_s \times n$ matrix over $\mathbb{F}_q$ of rank t_s. Then $\mathbf{e}\mathbf{Q}_1 = \left[\mathbf{w}_1 \quad \mathbf{w}_2 \quad \dots \quad \mathbf{w}_{t_s}\right]\mathbf{B}_1$, where $\mathbf{B}_1 = \mathbf{A}\mathbf{Q}_1$ is the $t_s \times (t - t_s)$ matrix over the extension field $\mathbb{F}_{q^N}$. It is clear that $\mathrm{Rk}(\mathbf{e}\mathbf{Q}_1 \mid \mathbb{F}_q) \le t - t_s$. Similarly, $\mathbf{e}\mathbf{Q}_2 = \left[\mathbf{w}_1 \quad \mathbf{w}_2 \quad \dots \quad \mathbf{w}_{t_s}\right]\mathbf{B}_2$, where $\mathbf{B}_2 = \mathbf{A}\mathbf{Q}_2$ is the $t_s \times (n - t + t_s)$ matrix over the base field $\mathbb{F}_q$. It follows that $\mathrm{Rk}(\mathbf{e}\mathbf{Q}_2 \mid \mathbb{F}_q) = \min(t_s, n - t + t_s) \le t_s$. Hence

$$\mathrm{Rk}(\mathbf{e}\mathbf{P}^{-1} \mid \mathbb{F}_q) \le \mathrm{Rk}(\mathbf{e}\mathbf{Q}_1 \mid \mathbb{F}_q) + \mathrm{Rk}(\mathbf{e}\mathbf{Q}_2 \mid \mathbb{F}_q) \le (t - t_s) + t_s = t = \left\lfloor \frac{n-k}{2} \right\rfloor.$$

The matrix $\mathbf{P}^{-1}$ can be replaced by a matrix $\tilde{\mathbf{P}}^{-1} = \mathbf{P}^{-1}\mathbf{Q}$, where $\mathbf{Q}$ is any $n \times n$ non singular matrix over the base field $\mathbb{F}_q$.

Code parameters (n, N, k, t, t_s, q)	Over	OJ1	OJ2	MINI	HGb1	HGb2	Public Key	Security
$(20,20,10,5,4,2)$	2^{80}	2^{64}	2^{78}	2^{261}	2^{66}	2^{67}	4000	Insecure
$(20,20,10,5,4,2^2)$	2^{160}	2^{108}	2^{138}	2^{262}	2^{110}	2^{116}	8000	Secure
$(20,20,10,5,4,2^4)$	2^{320}	2^{196}	2^{258}	2^{263}	2^{198}	2^{216}	16000	Secure
$(20,20,10,5,4,2^8)$	2^{640}	2^{372}	2^{498}	2^{264}	2^{374}	2^{416}	32000	Secure

Table 1: Comparison between Decoding & Structural attacks of simple variants of the GPT PKC

In Table 1, we evaluate the security of the simple variant of the GPT PKC against both Overbeck and Decoding attacks using same parameters which were presenter by Gaborit et al. in [38] regarding the code is used. According to Table 1: â€™OJ1â€™ stands for the improved basis enumeration by Ouriski and Joahsson, â€™OJ2â€™ stands for coordinates enumeration as described in Eq.(7); â€™Overâ€™ stands for the complexity of the Overbeck attack, â€™MINIâ€™ stands for the complexity of the Levy-dit-Vehel et al algorithm Eq. (8), â€™HGb1â€™ stands for the complexity of Gaborit et al. first algorithm Eq. (9), and â€™HGb2â€™ stands for the complexity of Gaborit et al. second algorithm Eq. (10).

Our Results show that all known (decoding & structural) attacks are infeasible with $q = 2^2$ and above.\

8 Conclusion

We have presented two approaches as techniques of withstanding Overbeck's attack against the GPT cryptosystem and its variants. 1. Distortion Matrix Approach. It is shown that proper choice of the distortion matrix $\mathbf{X}$ over the extension field $\mathbb{F}_{q^N}$ allows the decryption by the authorized party and prevents the unauthorized party from breaking the system by means of any known attacks. This approach is more powerful against Overbeck's attack than the Smart approach.

2. Advanced Approach for Reducible Rank Codes. It is shown that a proper choice of the column scramble matrix $\mathbf{P}$ over the extension field $\mathbb{F}_{q^N}$ makes all new attacks ineffective. This approach is designed to secure the GPT cryptosystem based on reducible rank codes.

The two approaches are proposed to countermeasure the attack of the GPT public key cryptosystem based on rank codes. They provide better security comparing with other GPT cryptosystem approaches. Furthermore, We have evaluated the simple variant of GPT PKC against all known attacks including Gaborit et al. attack and demonstrated a new set of parameters which were secure against all known attacks. It has been demonstrated that the decoding attacks are infeasible for practical implementations with $q = 2^2$ and above. With all these merits, The GPT cryptosystem can be effectively used in many practical applications such as mobile applications.

References

[1] R.J. McEliece, "A Public Key Cryptosystem Based on Algebraic Coding Theory", JPL DSN Progress Report 42–44, Pasadena, CA, pp. 114–116, 1978.

[2] H. Niederreiter, (1986), "Knapsack-Type Cryptosystem and Algebraic Coding Theory", Probl. Control and Inform. Theory, vol. 15, pp. 19-34,1986.

[3] V.M.Sidelnikov, S.O.Shestakov, "On the Cryptosystem Based on Generalized Reed-Solomon Codes", Discrete Math., vol. 3, no.3, 1992 (in Russian.)

[4] E.M. Gabidulin, "Public-Key Cryptosystems Based on Linear Codes over Large Alphabets: Efficiency and Weakness", in: Codes and Ciphers, Editor: P.G. Farrell, pp. 17–32, Essex: Formara Limited, 1995.

[5] E. Gabidulin, O. Kjelsen, "How to Avoid the Sidel'nikov - Shestakov Attack", A. Chmora, S.B. Wicker (Ed's.), Error Control, Cryptology, and Speech Compression, pp. 33-40, Lecture Notes in Computer Science, No. 829, Springer-Verlag, 1994.

[6] E. Gabidulin, A. Ourivski, V. Pavloushkov, "On the modified Niederreiter cryptosystem", Proceedings of the information Theory and Networking Workshop, p. 50-53, 1999. - Metsovo, Greece, June - July 1999.

[7] M. Churusova, E. Gabidulin, "The modified Niederreiter cryptosystem based on new metric," Proc. 8th International Symposium on Communication Theory and Applications, July 17 – 22, 2005, Ambleside, UK, p. 66-70.

[8] E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, "Ideals over a Non-commutative Ring and Their Application in Cryptology", in: Advances in Cryptology — Eurocrypt '91, Editor: D.W. Davies, Lecture Notes in Computer Science, No. 547, pp. 482–489, Berlin and Heidelberg: Springer-Verlag, 1991.

[9] M. Gadouleau, Yan. Zhiyuan, "Security of the GPT-Type Cryptosystems," Information Theory, 2006 IEEE International Symposium on , vol., no., pp.724-728, 9-14 July 2006, doi: 10.1109/ISIT.2006.261627.

[10] J. K. Gibson, "Severely denting the Gabidulin version of the McEliece public key cryptosystem", Designs, Codes and Cryptography, 6(1), 1995, pp. 37–45.

[11] J. K. Gibson, "The security of the Gabidulin public-key cryptosystem", in: U. M. Maurer, ed. Advances in Cryptology – EUROCRYPT'96, LNCS 1070, 1996, pp. 212–223.

[12] E.M. Gabidulin, A.V. Ourivski, "Improved GPT Public Key Cryptosystems", In: P. Farrell, M. Darnell, B. Honary (Ed's), "Coding, Communications, and Broadcasting", Research Studies Press, 2000, pp. 73-102.

[13] A. V. Ourivski, E. M. Gabidulin, "Column Scrambler for the GPT Cryptosystem", Discrete Applied Mathematics. 128(1): 207-221 (2003).

[14] E. M. Gabidulin, A. V. Ourivski, B. Honary, B. Ammar, "Reducible Rank Codes and Their Applications to Cryptography". IEEE Transactions on Information Theory. 49(12): 3289-3293 (2003).

[15] A. S. Kshevetskiy, E. M. Gabidulin, "High-weight errors in public-key cryptosystems based on reducible rank codes". In: Proc. of ISCTA, 2005.

[16] R.Overbeck,: "A new structural attack for GPT and variants", In: Proc. of Mycryptâ€™2005, vol. 3517 of LNCS, pp. 5â€"63. Springer-Verlag (2005).

[17] R.Overbeck.: "Extending Gibson's attacks on the GPT cryptosystem", In Proc. of WCC 2005, volume 3969 of LNCS, pp. 178-188, Springer Verlag,2006.

[18] R.Overbeck : "Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes", Journal of Cryptology, volume 21, number 2, April 2008.

[19] H. Rashwan, E. M. Gabidulin, B. Honary, "A Smart approach for GPT cryptosystem based on rank codes", Proc. of 2010 IEEE International Symposium on Information Theory, ISIT'10, 2010.

[20] A.S.Kshevetskiy: "Security of GPT-like cryptosystems based on linear rank codes", Signal Design and Its Applications in Communications, 2007. IWSDA 2007. On page(s): 143-147.

[21] P. Loidreau, "Designing a rank metric based McEliece cryptosystem", PQCrypto 2010. The Third International Workshop on Post-Quantum Cryptography. Darmstadt, Germany, May 25-28, 2010.

[22] E. M. Gabidulin, "Attacks and counter-attacks on the GPT public key cryptosystem", Designs, Codes and

Cryptography. V. 48, No. 2/ August 2008. Pp. 171-177, Springer Netherlands, DOI 10.1007/s10623-007-9160-8.

[23] E. M. Gabidulin, H.Rashwan and B. Honary,, "On improving security of GPT cryptosystems", Proc. IEEE International Symposium on Information Theory , June 2009.

[24] H. Rashwan, E. Gabidulin, and B. Honary, "Security of the GPT cryptosystem and its applications to cryptography". Security and Communication Networks, 4(8):937â€“946, 2011a. ISSN 1939-0122. doi: 10.1002/sec.228. URL http://dx.doi.org/10.1002/ sec.228.

[25] L.A. Ray, R.N. Ellson, "Method and Apparatus for Credit Card Verification", U.S. Patent 5,321,751, June 1994.

[26] A. Juels, M. Wattenberg, "A Fuzzy Commitment Scheme", In G. Tsudik, ed., Sixth ACM Conference on Computer and Communications Security, pp 28-36, ACM Press. 1999.

[27] G. Di Crescenzo, R. Graveman, R. Ge, G. Arce, "Approximate Message Authentication and Biometric Entity Authentication", Proc. 9th Int. Conf. Financial Cryptography and Data Security, FC2005, LNCS 3570.

[28] E.C. Chang, Q. Li, "Small Secure Sketch for Point-Set Difference", Cryptology ePrint Archive, Report 2005/145, 2005, http://eprint.iacr.org/.

[29] L. O'Gorman, I. Rabinovich, "Photo-image authentication by pattern recognition and cryptography", Int. Conf.Pattern Recognition (ICPR '96), Vienna, Aug. 1996, pp. 949-953.

[30] L. O'Gorman, I. Rabinovich, "Secure Identification Documents Via Pattern Recognition and Public-Key Cryptography", IEEE Trans. Pattern Anal. Mach. Intell. 20(10): 1097-1102 (1998)

[31] M. Ruhl, M. Bern, D. Goldberg, "Secure notarization of paper text documents", Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms (Washington, D.C., United States, January, 2001).

[32] C. J. Kuo , C. S. Huang, "A Novel Image Coding Technique for Noisy Communications", Communications, Computers and Signal Processing, 1993., IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, vol. 1, 1993, pp. 260-263.

[33] J. Seberry and J. Pieprzyk, Cryptography: "An Introduction to Computer Security", ISBN 0-13-194986-1, Prentice Hall, 1989.

[34] E.M. Gabidulin, "Theory of Codes with Maximum Rank Distance", Probl. Inform. Transm., vol. 21, No. 1, pp. 1–12, July, 1985.

[35] E. M. Gabidulin, "A Fast Matrix Decoding Algorithm For Rank-Error-Correcting Codes", In: (Eds G. Cohen, S. Litsyn, A. Lobstein, G. Zemor), Algebraic coding , pp. 126-132, Lecture Notes in Computer Science No. 573, Springer-Verlag, Berlin, 1992.

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

[37] F. Levy-dit-Vehel, J.-Ch. Jean-Charles Faug'ere, and L. Perret,"Cryptanalysis of MinRank", Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008, Proceedings. Series: Lecture Notes in Computer Science. Subseries: Security and Cryptology , Vol. 5157. Wagner, David (Ed.). 2008. Pp. 280-296.

[38] P. Gaborit, O. Ruatta, and J. Schrek, "On the complexity of the Rank Syndrome Decoding problem", http:// arXiv:1301.1026v1 [cs.CR] 6 Jan 2013.

[39] D. J. Bernstein, T. Lange, C. Peters, Attacking and defending the McEliece cryptosystem, in PQCrypto 2008 [9] (2008), 31-46. URL: http://eprint.iacr.org/2008/318.