Algebraic attacks for solving the Rank Decoding and MinRank problems without Gröbner basis

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, Javier Verbel

Algebraic attacks for solving the Rank Decoding and MinRank problems without Gröbner basis

Magali Bardet[4,5], Maxime Bros[1], Daniel Cabarcas[6], Philippe Gaborit[1], Ray Perlner[2], Daniel Smith-Tone[2,3], Jean-Pierre Tillich[4], and Javier Verbel[6]

[1] Univ. Limoges, CNRS, XLIM, UMR 7252, F-87000 Limoges, France
maxime.bros@unilim.fr
[2] National Institute of Standards and Technology, USA
[3] University of Louisville
[4] Inria, 2 rue Simone Iff, 75012 Paris, France
[5] LITIS, University of Rouen Normandie, France
[6] Universidad Nacional de Colombia Sede Medellín, Medellín, Colombia

Abstract. Rank Decoding is the main underlying problem in rank-based cryptography. Based on this problem and quasi-cyclic versions of it, very efficient schemes have been proposed recently, such as those in the ROLLO and RQC submissions, which have reached the second round of the NIST Post-Quantum Cryptography Standardization Process. Two main approaches have been studied to solve the Rank Decoding problem: combinatorial ones and algebraic ones. While the former has been studied extensively in [23] and [10], a better understanding of the latter was recently obtained with [11] where it appeared that algebraic attacks can often be more efficient than combinatorial ones for cryptographic parameters. In particular, the results of [11] were based on Gröbner basis computations which led to complexity bounds slightly smaller than the claimed security of ROLLO and RQC cryptosystems. This paper gives substantial improvements upon this attack in terms both of complexity and of the assumptions required by the cryptanalysis. We present attacks for ROLLO-I-128, ROLLO-I-192, and ROLLO-I-256 with bit complexity respectively in 70, 86, and 158, to be compared to 117, 144, and 197 for the attack in [11]. Moreover, unlike that previous attack, the new one does not rely on Gröbner basis computations and thus does not require any assumption concerning the behavior of the so-called solving degree. This improvement relies upon a modeling slightly different from the one in [11]. For a case called "overdetermined", this modeling allows us to avoid Gröbner basis computations by going directly to solving a linear system. For the other case, called "underdetermined", we also improve the results in [11] by combining the Ourivski-Johansson modeling together with a new modeling for a generic MinRank instance; the latter modeling allows us to refine the analysis of MinRank's complexity given in [35]. MinRank is a problem of great interest for all multivariate-based cryptosystems, including GeMSS and Rainbow, which are at the second round of the aforementionned NIST competition, our new approach supersedes previous attacks for the MinRank problem. Finally, since the proposed parameters of ROLLO and RQC are completely broken by our new attack, we give examples of new parameters for ROLLO and RQC

that make them resistant to our attacks. These new parameters show that these systems remain attractive, with a loss of only about 50% in terms of key size for ROLLO-I.

Keywords: Post-quantum cryptography · NIST-PQC candidates · rank metric code-based cryptography · algebraic attack.

1 Introduction

Rank metric code-based cryptography. In the last decade, rank metric code-based cryptography has proved to be a powerful alternative to more traditional code-based cryptography based on the Hamming metric. This thread of research started with the GPT cryptosystem [21] based on Gabidulin codes [20], which are rank metric analogues of Reed-Solomon codes. However, the strong algebraic structure of those codes was successfully exploited for attacking the original GPT cryptosystem and its variants with the Overbeck attack [34] (see for example [32] for one of the latest related developments). This has to be traced back to the algebraic structure of Gabidulin codes that makes masking extremely difficult; one can draw a parallel with the situation in the Hamming metric where essentially all McEliece cryptosystems based on Reed-Solomon codes or variants of them have been broken. However, recently a rank metric analogue of the NTRU cryptosystem from [28] has been designed and studied, starting with the pioneering paper [22]. Roughly speaking, the NTRU cryptosystem relies on a lattice that has vectors of rather small Euclidean norm. It is precisely those vectors that allow an efficient decoding/deciphering process. The decryption of the cryptosystem proposed in [22] relies on LRPC codes that have rather short vectors in the dual code, but this time for the rank metric. These vectors are used for decoding in the rank metric. This cryptosystem can also be viewed as the rank metric analogue of the MDPC cryptosystem [31] that relies on short vectors in the dual code for the Hamming metric.

This new way of building rank metric code-based cryptosystems has led to a sequence of proposals [22,24,5,6], culminating in submissions to the NIST post-quantum competition [1,2], whose security relies solely on the decoding problem in rank metric codes with a ring structure similar to the ones encountered right now in lattice-based cryptography. Interestingly enough, one can also build signature schemes using the rank metric; even though early attempts which relied on masking the structure of a code [25,9] have been broken [15], a promising recent approach [8] only considers random matrices without structural masking.

Decoding $\mathbb{F}_{q^m}$-linear codes in Rank metric. In other words, in rank metric code-based cryptography we are now only left with assessing the difficulty of the decoding problem for the rank metric. The trend in rank metric code-based cryptography has been to consider a particular form of codes that are linear codes of length n over an extension $\mathbb{F}_{q^m}$ of degree m of $\mathbb{F}_q$, that is, $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$. Let $(\beta_1, \ldots, \beta_m)$ be any basis of $\mathbb{F}_{q^m}$ as a $\mathbb{F}_q$-vector space. Then words

of those codes can be interpreted as matrices with entries in the ground field $\mathbb{F}_q$ by viewing a vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ as a matrix $\mathrm{Mat}(\boldsymbol{x}) = (X_{ij})_{i,j}$ in $\mathbb{F}_q^{m \times n}$, where $(X_{ij})_{1 \leq i \leq m}$ is the column vector formed by the coordinates of x_j in the basis $(\beta_1, \ldots, \beta_m)$, that is, $x_j = \beta_1 X_{1j} + \cdots + \beta_m X_{mj}$.

Then the "rank" metric d on $\mathbb{F}_{q^m}^n$ is the rank metric on the associated matrix space, namely

$$d(\boldsymbol{x}, \boldsymbol{y}) := |\boldsymbol{y} - \boldsymbol{x}|, \quad \text{where we define } |\boldsymbol{x}| := \mathrm{Rank}\left(\mathrm{Mat}(\boldsymbol{x})\right).$$

Hereafter, we will use the following terminology.

Problem 1 ((m, n, k, r)-decoding problem).

Input: an $\mathbb{F}_{q^m}$-basis $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k)$ of a subspace $\mathcal{C}$ of $\mathbb{F}_{q^m}^n$, an integer $r \in \mathbb{N}$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ at distance at most r of $\mathcal{C}$ (i.e. $|\boldsymbol{y} - \boldsymbol{c}| \leq r$ for some $\boldsymbol{c} \in \mathcal{C}$).

Output: $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ and $|\boldsymbol{e}| \leq r$.

This problem is known as the Rank Decoding problem, written RD. It is equivalent to the Rank Syndrome Decoding problem, written RSD, for which one uses the parity check matrix of the code instead of the generator matrix. There are two approaches to solve RD instances: the combinatorial ones such as those in [23] and [10] and the algebraic ones, such as in [11]; the latter are one of the purposes of this article.

Even if the decoding problem is not known to be NP-complete for these $\mathbb{F}_{q^m}$-linear codes, there is a randomised reduction to an NP-complete problem [26] (namely to decoding in the Hamming metric). The region of parameters which is of interest for the NIST submissions corresponds to $m = \Theta(n)$, $k = \Theta(n)$ and $r = \Theta(\sqrt{n})$.

The MinRank problem. The MinRank problem was first mentioned in [13] where its NP-completeness was also proven. MinRank plays a role in multivariate-based cryptography which is similar to the one of Rank Decoding for rank metric code-based cryptography. Moreover, the Rank Decoding problem reduces to MinRank as explained in [18].

Problem 2 (MinRank problem).

Input: an integer $r \in \mathbb{N}$ and $K + 1$ matrices $\boldsymbol{Y}, \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$.

Output: field elements $x_1, x_2, \ldots, x_K \in \mathbb{F}_q$ such that

$$\mathrm{Rank}\left(\boldsymbol{Y} - \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

The current best known algorithms for solving the MinRank problem have exponential complexity bounds.

Algebraic attacks. This family of attacks consists in modeling the decoding problem into a system of multivariate polynomial equations and then solve this

system. In [11], the constructed system was solved by using Gröbner basis techniques. Similar approaches exist for solving the MinRank problem, such as the Kipnis-Shamir modeling [29] and the minors modeling (described for example in [19]); the complexity of solving MinRank using these modelings has been investigated in [18,19].

Our contribution. In this paper, we follow on from the approach in [11] and propose a slightly different modeling to solve the RD problem. This system can be solved "directly" by linearization, avoiding the use of Gröbner basis algorithms such as Faugère's F4 algorithm, see [17]. This new modeling brings on a substantial speed-up in the computations for solving the system. It results in the best practical efficiency and complexity bounds that are currently known for the decoding problem; in particular, it significantly improves upon the aforementionned similar approach in [11]. We provide dedicated algorithms for solving the systems, with less computations than a generic Gröbner basis algorithm, hence resulting in a better complexity. We present attacks for ROLLO-I-128, ROLLO-I-192, and ROLLO-I-256 with bit complexity respectively in 70, 86, and 158, to be compared to 117, 144, and 197 for the attack in [11]. The difference with [11] is significant since as there is no real quantum speed-up for solving linear systems, the best quantum attacks for ROLLO-I-192 remained the quantum attack based on combinatorial attacks, when our new attacks show that ROLLO parameters are broken and need to be changed.

Our analysis is divided into two categories: the "overdetermined" and the "underdetermined" case. An (m, n, k, r)-decoding instance is overdetermined if the condition

$$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1 \tag{1}$$

is fulfilled. In that case we obtain a complexity in

$$\mathcal{O}\left(m\binom{n-p-k-1}{r}\binom{n-p}{r}^{\omega-1}\right) \tag{2}$$

operations in the field $\mathbb{F}_q$, where ω is the constant of linear algebra and $p = \max\{i : i \in \{1..n\}, m\binom{n-i-k-1}{r} \geq \binom{n-i}{r} - 1\}$ represents, in case the overdetermined condition (1) is comfortably fulfilled, the use of punctured codes. This complexity clearly supersedes the previous results of [11] in terms of complexity and also by the fact that it does not rely on Gröbner Basis computations and hypothesis on the solving degree of the system. In a rough way for $r = \mathcal{O}(\sqrt{n})$ (the type of parameters used for ROLLO and RQC), the recent improvements on algebraic attacks can be seen as this: before [11] the complexity for solving RD involved a term in $O(n^2)$ in the upper part of a binomial coefficient, the modeling in [11] replaced it by a term in $\mathcal{O}\left(n^{\frac{3}{2}}\right)$ whereas our new modeling involves a term in $\mathcal{O}(n)$ at a similar position. This leads to a gain in the exponential coefficient of order 30% compared to [11] and of order 50% compared to approaches before [11]. Notice that for ROLLO and RQC only parameters

with announced complexities 128 and 192 bits satisfied condition (1) but not parameters with announced complexities 256 bits.

When condition (1) is not fulfilled, the instance can either be underdetermined or be brought back to the overdetermined area by an hybrid approach using exhaustive search with exponential complexity to guess few variables in the system. In the underdetermined case, our approach is different from [11]. Here we propose an approach using reduction to the MinRank problem. This leads to a new modeling to solve generic MinRank instances, also avoiding Gröbner basis computation and thus giving a more precise analysis of the MinRank problem than in [35]. In particular our new approach gives a better complexity for solving the MinRank problem with algebraic attacks.

Note that for some parameters proposed in [7,3], the condition (1) holds. Taking for ω the smallest value currently achievable in practice, which is $\omega \approx 2.8$ via Strassen's algorithm, this leads to an attack on the schemes proposed in these NIST submissions which is in all cases below the claimed classical security level and sometimes way below the previous attack in [11].

At last we also propose new parameters for ROLLO-I and RQC to be resistent to our new attacks. For ROLLO-I these new parameters remain attractive and require the use of a basic decoding rather than the decoding algorithm used in the NIST submission. For RQC it requires to slightly modify the support of the error, for which we propose an adaptation of our attack.

2 Notation

In the whole paper, we will focus on the case which is relevant for cryptographic applications, namely when the base field $\mathbb{F}_q$ has characteristic 2. Analogous results can be obtained for other field characteristics but involve putting the relevant signs wherever this is needed. We also use the following notation and definitions:

- Matrices and vectors are written in boldface font $\boldsymbol{M}$.
- The entry in row i and column j of a matrix $\boldsymbol{M}$ is denoted by $\boldsymbol{M}[i,j]$.
- The transpose of a matrix $\boldsymbol{M}$ is denoted by $\boldsymbol{M}^\mathsf{T}$.
- For a given ring $\mathcal{R}$, the set of matrices with n rows, m columns and coefficients in $\mathcal{R}$ is denoted by $\mathcal{R}^{n\times m}$.
- $\{1..n\}$ stands for the set of integers from 1 to n.
- For two subsets $I \subset \{1..n\}$ and $J \subset \{1..m\}$, we write $\boldsymbol{M}_{I,J}$ for the submatrix of $\boldsymbol{M}$ formed by its rows (resp. columns) with index in I (resp. J).
- We use the shorthand notation $\boldsymbol{M}_{*,J} = \boldsymbol{M}_{\{1..m\},J}$ and $\boldsymbol{M}_{I,*} = \boldsymbol{M}_{I,\{1..n\}}$, where $\boldsymbol{M}$ has m rows and n columns.
- $\alpha \in \mathbb{F}_{q^m}$ is a primitive element, so that $(1, \alpha, \ldots, \alpha^{m-1})$ is a basis of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space.
- For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$. The *support* of v is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ spanned by the vectors $v_1, \ldots, v_n$. Thus this support is the column space of the matrix $\mathrm{Mat}(\boldsymbol{v})$ associated to $\boldsymbol{v}$ (for any choice of basis), and its dimension is precisely $\mathrm{Rank}(\mathrm{Mat}(\boldsymbol{v}))$.

– An $[n,k]$ $\mathbb{F}_{q^m}$-linear code is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ of dimension k endowed with the rank metric.

3 Algebraic modeling of the decoding problem

In what follows, we consider the (m,n,k,r)-decoding problem for the code $\mathcal{C}$ and assume we have received $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ at distance r from $\mathcal{C}$ and look for the unique vectors $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{e}$ such that $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ and $|\boldsymbol{e}| = r$. The reasons why we consider that there is one single solution $\boldsymbol{e}$ of rank exactly r are the same as described in [11].

3.1 Ourivksi-Johansson modeling

We start from the Ourivski-Johansson's system ([33]), where

$$\boldsymbol{H}_y = \begin{pmatrix} -\boldsymbol{R}^\mathsf{T} & \boldsymbol{I}_{n-k-1} \end{pmatrix}$$

is a parity-check matrix of the code $\widetilde{\mathcal{C}} = \mathcal{C} + \langle \boldsymbol{y} \rangle$, $\begin{pmatrix} 1 & \alpha & \dots & \alpha^{m-1} \end{pmatrix}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and the error $\boldsymbol{e}$ is written $\boldsymbol{e} = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{m-1} \end{pmatrix} \boldsymbol{SC}$ where $\boldsymbol{S}$ represents a basis of the support of $\boldsymbol{e}$ in $\left(\mathbb{F}_q^m\right)^r$ and $\boldsymbol{C}$ the coordinates of $\boldsymbol{e}$ in this basis. We call the entries of $\boldsymbol{S}$ the *support variables* whereas the entries of $\boldsymbol{C}$ are called the *coefficient variables*.

Then $\boldsymbol{e}$ is a solution of the system

$$\begin{pmatrix} 1 & \alpha & \dots & \alpha^{m-1} \end{pmatrix} \boldsymbol{SCH}_y^\mathsf{T} = \boldsymbol{0}_{n-k-1}. \tag{3}$$

This system has a large number of solutions, that corresponds to the $\lambda\boldsymbol{e}$, with any non-zero $\lambda \in \mathbb{F}_{q^m}$ and to different bases of the support of $\boldsymbol{e}$. If we specialize one support and one λ, the system has exactly one solution in $\mathbb{F}_q$, provided that the error can be uniquely decoded and has weight exactly r.

It is shown in [11] that, when $\boldsymbol{S}$ is specialized with its first column to 1 and $\boldsymbol{S}_{\{1..r\},*} = \boldsymbol{I}_r$ and $\boldsymbol{C}$ has its first column equal to 1, then the solution of the system is also a solution of the system

$$\text{MaxMinors}(\boldsymbol{CH}_y^\mathsf{T}) = \boldsymbol{0}_{r \times (n-k-1)}$$

that consists in all maximal minors of degree r of the matrix $\boldsymbol{CH}_y^\mathsf{T}$, that is $\binom{n-k-1}{r}$ polynomials that can be expressed linearly in terms of $c_T = \det(\boldsymbol{C}_{*,T})$ where $T \subset \{1..n\}$ is a subset of size r. In the over-determined case, that is if $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$, then the system can be linearized and the values of all c_T recovered.

In the next section, we show that with a slightly different specialization, in the over-determined case, we can recover directly the values of all the variables in $\boldsymbol{C}$ only with linear algebra.

3.2 The system MaxMinors with the identity specialized in C

For the sake of presentation, we assume here that the first r coordinates of $\boldsymbol{e}$ are independent over $\mathbb{F}_q$. In [11] there is an algorithm to handle the general case by making several attempts, it can easily be adapted to find r components of $\boldsymbol{e}$ of rank r.

Under this assumption, we can specialize System (3) with the identity in the first columns of $\boldsymbol{C}$, and the value $\mathbf{1}^\mathsf{T} = \begin{pmatrix}1\ 0 \dots 0\end{pmatrix}^\mathsf{T}$ in the first column of $\boldsymbol{S}$. Precisely, we define

$$\mathcal{F}_C = \left\{ \begin{pmatrix}1\ \alpha \cdots \alpha^{m-1}\end{pmatrix} \begin{pmatrix}\mathbf{1}^\mathsf{T}\ \boldsymbol{S}'\end{pmatrix} \begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}'\end{pmatrix} \boldsymbol{H}_y^\mathsf{T} \right\}, \tag{4}$$

where $\mathbf{1}^\mathsf{T} \in \mathbb{F}_q^m$ is a column vector, $\boldsymbol{S} = \begin{pmatrix}\mathbf{1}^\mathsf{T}\ \boldsymbol{S}'\end{pmatrix}$ and $\boldsymbol{C} = \begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}'\end{pmatrix}$.

We will now show that the new system

$$\mathcal{F}_M = \text{MaxMinors}\left(\begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}'\end{pmatrix} \boldsymbol{H}_y^\mathsf{T} \right), \tag{5}$$

which is the set of all minors of size r of the matrix $\begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}'\end{pmatrix} \boldsymbol{H}_y^\mathsf{T}$, can be used to recover the values of the variables in $\boldsymbol{C}$.

Let $V_{\mathbb{F}_q}(\mathcal{F}_C)$ be the set of solutions of (4) with all variables in $\mathbb{F}_q$, that is

$$V_{\mathbb{F}_q}(\mathcal{F}_C) = \\ \left\{ (\boldsymbol{S}^*, \boldsymbol{C}^*) \in {\mathbb{F}_q}^{m(r-1)+r(n-r)} : \begin{pmatrix}1\ \alpha \cdots \alpha^{m-1}\end{pmatrix} \begin{pmatrix}\mathbf{1}^\mathsf{T}\ \boldsymbol{S}^*\end{pmatrix} \begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}^*\end{pmatrix} \boldsymbol{H}_y^\mathsf{T} = \mathbf{0} \right\}. \tag{6}$$

Let $V_{\mathbb{F}_q}(\mathcal{F}_M)$ be the set of solutions of (5) with all variables in $\mathbb{F}_q$, i.e.

$$V_{\mathbb{F}_q}(\mathcal{F}_M) = \left\{ \boldsymbol{C}^* \in {\mathbb{F}_q}^{r(n-r)} : \mathtt{Rank}_{\mathbb{F}_{q^m}} \left(\begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}^*\end{pmatrix} \boldsymbol{H}_y^\mathsf{T} \right) < r \right\}.$$

Proposition 1. *If $\boldsymbol{e}$ can be uniquely decoded and has rank r, then*

$$V_{\mathbb{F}_q}(\mathcal{F}_M) = \left\{ \boldsymbol{C}^* \in \mathbb{F}_q^{r(n-r)} : \exists \boldsymbol{S}^* \in \mathbb{F}_q^{m(r-1)} \text{ s.t. } (\boldsymbol{S}^*, \boldsymbol{C}^*) \in V_{\mathbb{F}_q}(\mathcal{F}_C) \right\}. \tag{7}$$

This means that the set $V_{\mathbb{F}_q}(\mathcal{F}_M)$ is the projection of the set $V_{\mathbb{F}_q}(\mathcal{F}_C)$ on the last $r(n-r)$ coordinates.

Proof. Let $(\boldsymbol{S}^*, \boldsymbol{C}^*) \in V_{\mathbb{F}_q}(\mathcal{F}_C)$, then the non-zero vector

$$\begin{pmatrix}1\ S_2^* \dots S_r^*\end{pmatrix} = \begin{pmatrix}1\ \alpha \cdots \alpha^{m-1}\end{pmatrix} \begin{pmatrix}\mathbf{1}^\mathsf{T}\ \boldsymbol{S}^*\end{pmatrix}$$

belongs to the left kernel of the matrix $\begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}^*\end{pmatrix} \boldsymbol{H}_y^\mathsf{T}$. Hence this matrix has rank less than r, and $\boldsymbol{C}^* \in V_{\mathbb{F}_q}(\mathcal{F}_M)$. Reciprocally, if $\boldsymbol{C}^* \in V_{\mathbb{F}_q}(\mathcal{F}_M)$, then the matrix $\begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}^*\end{pmatrix} \boldsymbol{H}_y^\mathsf{T}$ has rank less than r, hence its left kernel over $\mathbb{F}_{q^m}$ contains a non zero element $(S_1^*, \dots, S_r^*) = (1, \alpha, \dots, \alpha^{m-1})\boldsymbol{S}^*$ with the coefficients of $\boldsymbol{S}^*$ in $\mathbb{F}_q$. But S_1^* cannot be zero, as it would mean that $(0, S_2^*, \dots, S_r^*) \begin{pmatrix}\boldsymbol{I}_r\ \boldsymbol{C}^*\end{pmatrix}$ is an error of weight less than r solution of the decoding problem, and we assumed there are only one error of weight exactly r solution of the decoding problem. Then, $({S_1^*}^{-1}(S_2^*, \dots, S_r^*), \boldsymbol{C}^*) \in V_{\mathbb{F}_q}(\mathcal{F}_C)$. □

This means that solving the decoding problem is left to solve the MaxMinors system, that depends only on the $\boldsymbol{C}$ variables.

Proposition 2. *The system* MaxMinors$(\boldsymbol{C}\boldsymbol{H}_y^\mathsf{T})$ *contains* $\binom{n-k-1}{r}$ *polynomials of degree* r *over* $\mathbb{F}_{q^m}$*, indexed by the subsets* $J \subset \{1..n-k-1\}$ *of size* r*, that are the*

$$P_J = \sum_{\substack{\boldsymbol{T_1}\subset\{1..k+1\},\boldsymbol{T_2}\subset J,\\ \#\boldsymbol{T_1}+\#\boldsymbol{T_2}=r\\ \boldsymbol{T}=\boldsymbol{T_1}\cup(\boldsymbol{T_2}+k+1)}} (-1)^{\sigma_J(T_2)} \det(\boldsymbol{R}_{\boldsymbol{T_1},J\setminus\boldsymbol{T_2}}) \det(\boldsymbol{C}_{*,\boldsymbol{T}}), \tag{8}$$

where the sum is over all subsets $\boldsymbol{T}_1 \subset \{1..k+1\}$ *and* $\boldsymbol{T}_2$ *subset of* J*, with* $\#\boldsymbol{T}_1 + \#\boldsymbol{T}_2 = r$*, and* $\sigma_J(T_2)$ *is an integer depending on* T_2 *and* J*. We denote by* $\boldsymbol{T_2} + k + 1$ *the set* $\{i + k + 1 : i \in \boldsymbol{T_2}\}$*.*

Remark 1. There are $\binom{n}{r}$ different polynomials $\det(\boldsymbol{C}_{*,\boldsymbol{T}})$ involved in the $\binom{n-k-1}{r}$ equations, and each equation P_J contains $\binom{k+r+1}{r}$ such polynomials.

We have $c_{i,j} = \det(\boldsymbol{C}_{*,\{1..r\}\setminus\{i\}\cup\{j\}})$ for any $i \in \{1..r\}$ and $j \in \{r+1..n\}$, and $1 = \det(\boldsymbol{C}_{*,\{1..r\}})$.

For the proof, reader may refer to [11].

4 Solving Rank Decoding problem: overdetermined case

In this section, we show that, when the number of equations is sufficiently large, we can solve the system MaxMinors with only linear algebra computations, by linearisation on the polynomials $\det(\boldsymbol{C}_{*,\boldsymbol{T}})$.

4.1 The overdetermined case

The system MaxMinors can be viewed as a linear system with $m\binom{n-k-1}{r}$ linear equations over $\mathbb{F}_q$, in the $\binom{n}{r} - 1$ variables $c_{\boldsymbol{T}}$ representing the non constant polynomials $\det(\boldsymbol{C}_{*,\boldsymbol{T}})$, for all $\boldsymbol{T} \subset \{1..n\}$, $\#\boldsymbol{T} = r$, $\boldsymbol{T} \neq \{1..r\}$. According to Remark 1, if we are able to linearise this sytem with respect to the variables $c_{\boldsymbol{T}}$, then in particular we get the values of all the entries $c_{i,j}$ of the matrix $\boldsymbol{C}$.

In order to linearise this system, we can expand each equation over $\mathbb{F}_{q^m}$ as m equations over $\mathbb{F}_q$, and construct a matrix **MaxMin** with rows indexed by $(J,i) : J \subset \{1..n-k-1\}, \#J = r, 0 \leq i \leq m-1$ and columns indexed by $\boldsymbol{T} \subset \{1..n\}$ of size r, with the entry in row (J,i) and column $\boldsymbol{T}$ being the coefficient in α^i of the element $\pm\det(\boldsymbol{R}_{\boldsymbol{T_1},J\setminus\boldsymbol{T_2}}) \in \mathbb{F}_{q^m}$. More precisely, we have

$$\mathbf{MaxMin}[(J,i),\boldsymbol{T}] = \begin{cases} 0 & \text{if } \boldsymbol{T_2} \not\subset J \\ [\alpha^i](-1)^{\sigma_J(T_2)}(\det(\boldsymbol{R}_{\boldsymbol{T_1},J\setminus\boldsymbol{T_2}})) & \text{if } \boldsymbol{T_2} \subset J, \end{cases} \tag{9}$$
$$\text{with} \quad \boldsymbol{T_1} = \boldsymbol{T} \cap \{1..k+1\},$$
$$\text{and} \quad \boldsymbol{T_2} = (\boldsymbol{T} \cap \{k+2..n\}) - (k+1).$$

The matrix **MaxMin** can at most have rank $\binom{n}{r} - 1$, as a maximal rank of $\binom{n}{r}$ would imply that $\langle \text{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_y^\mathsf{T})\rangle = \langle 1\rangle$.

Proposition 3. *If* **MaxMin** *has rank* $\binom{n}{r}-1$ *(which implies that* $m\binom{n-k-1}{r} \geq \binom{n}{r}-1$*), then the right kernel of* **MaxMin** *contains only one element* $\begin{pmatrix}\boldsymbol{c} & 1\end{pmatrix} \in \mathbb{F}_q^{\binom{n}{r}}$ *with value 1 on its component corresponding to* $\det(\boldsymbol{C}_{\{1..r\}})$*. The components* $\boldsymbol{c}$ *of this vector contain the values of the* $\det(\boldsymbol{C}_{*,\boldsymbol{T}})$*,* $\boldsymbol{T} \neq \{1..r\}$*. This gives in particular the values of all the variables* $c_{i,j} = \det(\boldsymbol{C}_{*,\{1..r\}\setminus\{i\}\cup\{j\}})$*.*

Proof. If **MaxMin** has rank $\binom{n}{r}-1$, then as there is a solution to the system, a row echelon form of the matrix has the shape

$$\begin{pmatrix} \boldsymbol{I}_{\binom{n}{r}-1} & \boldsymbol{c}^{\mathsf{T}} \\ \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}$$

with $\boldsymbol{c}$ a vector in $\mathbb{F}_q$ of size $\binom{n}{r}-1$: we cannot get a jump in the stair of the echelon form as it would imply that Eq. (5) has no solution. Then $\begin{pmatrix}-\boldsymbol{c} & 1\end{pmatrix}$ is in the right kernel of **MaxMin**. □

It is then easy to recover the variables $\boldsymbol{S}$ from (4) by linear algebra. The following algorithm recovers the error if there is one solution to the system (4). It is shown in [11] how to deal with the other cases.

Input: Code $\mathcal{C}$, vector $\boldsymbol{y}$ at distance r from $\mathcal{C}$, such that $m\binom{n-k-1}{r} \geq \binom{n}{r}-1$ and **MaxMin** has maximal rank
Output: The error $\boldsymbol{e}$ of weight r such that $\boldsymbol{y}-\boldsymbol{e} \in \mathcal{C}$
Construct **MaxMin**, the $m\binom{n-k-1}{r} \times \binom{n}{r}$ matrix over $\mathbb{F}_q$ associated to the system MaxMinors Eq. (5) ;
Let $\begin{pmatrix}\boldsymbol{c} & 1\end{pmatrix}$ be the only such vector in the right kernel of MaxMinors ;
Compute the values $\boldsymbol{C}^* = (c^*_{i,j})_{i,j}$ from $\boldsymbol{c}$;
Compute the values $(S_1^*, \ldots, S_r^*) \in \mathbb{F}_{q^m}^r$ by solving the linear system

$$(S_1, \ldots, S_r)\boldsymbol{C}^*\boldsymbol{H}_y^{\mathsf{T}} = 0$$

and taking the unique value with $S_1^* = 1$;
return $(1, S_2^*, \ldots, S_r^*)\boldsymbol{C}^*$;

Algorithm 1: (m, n, k, r)-Decoding in the overdetermined case.

Proposition 4. *When* $m\binom{n-k-1}{r} \geq \binom{n}{r}-1$ *and* **MaxMin** *has maximal rank* $\binom{n}{r}-1$*, then Algorithm 1 recovers the error in complexity*

$$\mathcal{O}\left(m\binom{n-k-1}{r}\binom{n}{r}^{\omega-1}\right) \tag{10}$$

operations in the field $\mathbb{F}_q$*, where* ω *is the constant of linear algebra.*

Proof. To recover the error, the most consuming part is the computation of the left kernel of the matrix **MaxMin** in $\mathbb{F}_q^{m\binom{n-k-1}{r}\times\binom{n}{r}}$, in the case where

$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$. This can be done by computing an echelon form of **MaxMin**, in this case the complexity is bounded by Eq. (10). □

We ran a lot of experiments, with the code $\mathcal{C}$ a random code, and $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$, and we always got a matrix **MaxMin** with maximal rank. That is why we propose the following heuristic about the rank of **MaxMin**.

Heuristic 1 (Overdetermined case) *When* $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$*, with overwhelming probability, the rank of the matrix* **MaxMin** *is* $\binom{n}{r} - 1$.

Figure 1 gives the experimental results we obtained for $q = 2$, $r = 3, 4, 5$ and different values of n. We choose to keep m prime and close to $n/1.18$ to have a data set containing the parameters of the ROLLO-I cryptosystem. We choose for k the minimum between $\frac{n}{2}$ and the largest value leading to an overdetermined case. We have $k = \frac{n}{2}$ as soon as $n \geq 22$ for $r = 3$, $n \geq 36$ for $r = 4$, $n \geq 58$ for $r = 5$. Experimentally, it does not seem to influence the complexity. The figure shows that the estimated complexity is a good upper bound for the computation's complexity. It also shows that this upper bound is not tight.

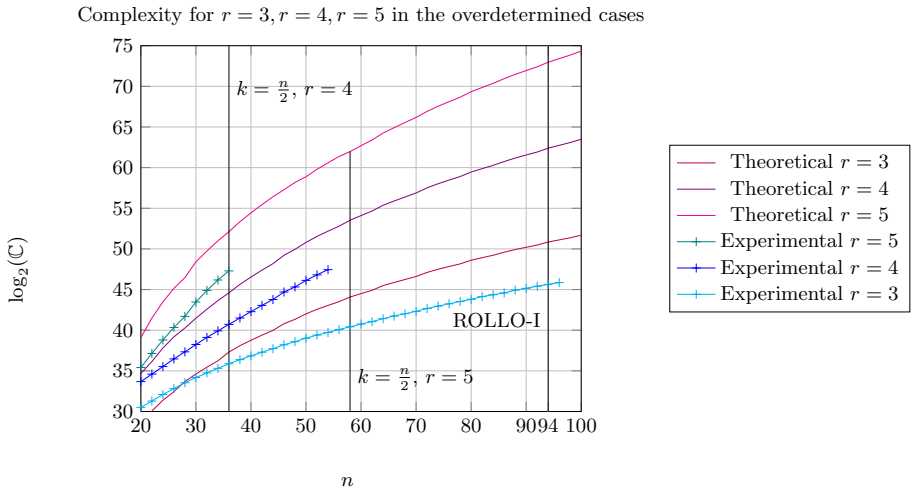

Fig. 1. Theoretical vs Experimental value of the complexity of the computation. The computations are done using `magma v2.22-2` on a machine with a Intel® Xeon® 2.00GHz processor. We measure the complexity in terms of clock cycles of the CPU, given by the `magma` function `ClockCycles()`. The theoretical value is the binary logarithm of $m\binom{n-k-1}{r}\binom{n}{r}^{2.81-1}$. m is the largest prime less than $n/1.18$, and k the minimum of $n/2$ (right part of the graph) and the largest value for which the system is overdetermined (left part).

Figure 2 shows the theoretical complexity, in the case where $n = 2k$ and m is prime and close to $n/1.18$. We take those parameters because they fit with the

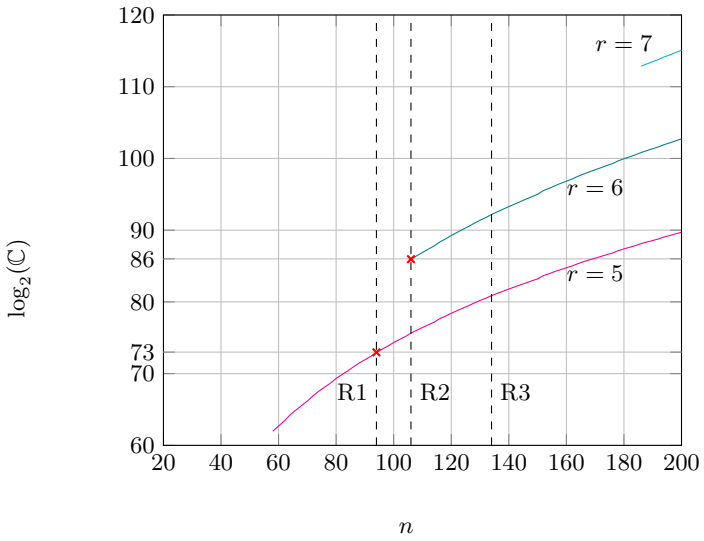

Fig. 2. Theoretical value of the complexity of the computation in the overdetermined cases, which is the binary logarithm of $m\binom{n-k-1}{r}\binom{n}{r}^{2.81-1}$. m is the largest prime less than $n/1.18$, $n = 2k$. The axis "R1, R2, R3" correspond to the values of n for the cryptosystems ROLLO-I-128; ROLLO-I-192 and ROLLO-I-256.

parameters in the cryptosystem ROLLO-I. When the parameters (m, n, k, r) do not satisfy the overdeterminess condition $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$, we do not put the complexity. The graph starts from the first value of n where $(n/1.18, n, 2k, r)$ is in the overdetermined case. We can see that theoretically, the cryptosystem ROLLO-I-128 with parameters $(79, 94, 47, 5)$ needs 2^{73} bit operations to decode an error, instead of the announced 2^{128} bits of security. In the same way, ROLLO-I-192 with parameters $(89, 106, 53, 6)$ would have 86 bits of security instead of 192. The parameters $(113, 134, 67, 7)$ for ROLLO-I-256 are not in the overdetermined case.

4.2 Improvements in the overdetermined case

There are two classical improvements that can be used in the overdetermined case. The first one is when the system is "super"-overdetermined, i.e. when the number of rows in **MaxMin** is really larger than the number of columns. In that case, it is not necessary to consider all equations, we just need the minimum number of them to be able to find the solution.

To select the good equations, we can take the system MaxMinors obtained by considering code $\mathcal{C}_y$ punctured on the p last coordinates, instead of the entire code. Puncturing code $\mathcal{C}_y$ is equivalent to shortening the dual code, i.e. consid-

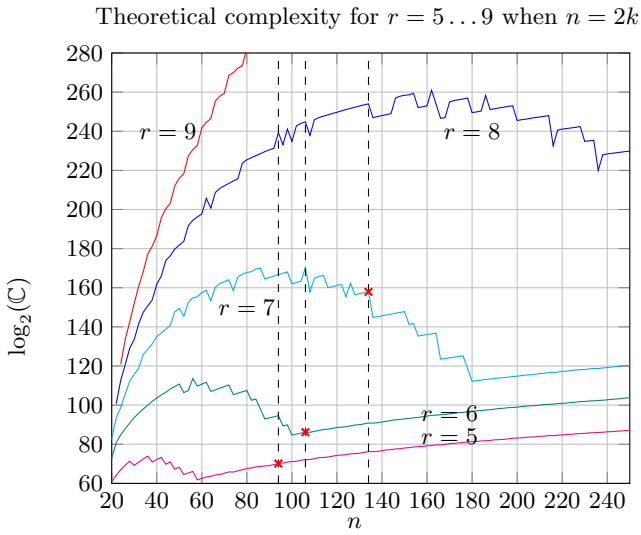

Fig. 3. Theoretical value of the complexity of RD in the overdetermined case (using punctured codes or specialisation). $\mathbb{C}$ is the smallest value between (13) and (12). m is the largest prime less than $n/1.18$, $n = 2k$. The dashed axes correspond to the values of n for the cryptosystems ROLLO-I-128; ROLLO-I-192 and ROLLO-I-256.

ering the system

$$\text{MaxMinors}\left(\boldsymbol{C}_{*,\{1..n-p\}}(\boldsymbol{H}_y^{\mathsf{T}})_{\{1..n-p\},\{1..n-k-1-p\}}\right). \tag{11}$$

as we take $\boldsymbol{H}_y$ is systematic form on the last coordinates. This system is formed by a sub-sequence of polynomials in MaxMinors that do not contains the variables $c_{i,j}$ with $n-p+1 \leq j \leq n$. This system contains $m\binom{n-p-k-1}{r}$ equations in $\binom{n-p}{r}$ variables $\boldsymbol{C}_{*,\boldsymbol{T}}$ with $\boldsymbol{T} \subset \{1..n-p-k-1\}$. If we take the maximal value of p such that $m\binom{n-p-k-1}{r} \geq \binom{n-p}{r} - 1$, we can still apply Algorithm 1 but the complexity is reduced for instance to

$$\mathcal{O}\left(m\binom{n-p-k-1}{r}\binom{n-p}{r}^{\omega-1}\right) \tag{12}$$

operations in the field $\mathbb{F}_q$ if we use Gaussian elimination.

4.3 Reducing to the overdetermined case: hybrid attack

Another classical improvement consists in using an hybrid approach mixing exhaustive search and linear resolution, like in [12]. This consists in specialising some variables of the system to reduce to the overdetermined case.

For instance, if we specialise a columns of the matrix $\boldsymbol{C}$, we are left with solving q^{ar} linear systems **MaxMin** of size $m\binom{n-k-1}{r} \times \binom{n-a}{r}$, and the global cost is

$$\mathcal{O}\left(q^{ar} m \binom{n-k-1}{r} \binom{n-a}{r}^{\omega-1}\right) \tag{13}$$

operations in the field $\mathbb{F}_q$ if we use Gaussian elimination. Figure 3 page 12 gives the best theoretical complexities obtained for $r = 5 \dots 9$ with the best values of a and p, for $n = 2k$. Table 1 page 20 gives the complexities of our attack (column "This paper") for all the parameters in the ROLLO and RQC submissions to the NIST competition; for the sake of clarity, we give the previous complexity from [11].

5 Solving Rank Decoding and MinRank problems: underdetermined case

This section generalizes the method of solving RD in the overdetermined case with just linear algebra to the underdetermined case and generic MinRank. This analysis may be applied to explain the behavior of Gröbner basis algorithms for solving these problems, and to provide an algorithm with a better complexity than Gröbner basis algorithms for these problems.

5.1 Rank Decomposition Modeling

In this section we describe a modeling of the MinRank problem which is especially illustrative of the connections between RD and more generic instances of MinRank. We will not use this modeling directly but will use it to establish the variables and terminology for a more advanced form of modeling in subsequent sections. This more advanced modeling which we call "Support Minors modeling" provides an improvement over previously known algebraic approach to solving generic MinRank problems and can be conveniently combined with the system MaxMinors to produce an improvement over previously known techniques for solving RD in the underdetermined case.

Recall that rank decoding problem may be treated as a special case of the MinRank Problem. We can reinterpret the RD problem as finding a non-trivial low-rank linear combination over $\mathbb{F}_q$ of $\widetilde{K} = m(k+1)$ matrices in $\mathbb{F}_q^{m \times n}$, given by

$$\left(M_1 \dots M_{\widetilde{K}}\right) = \left(1 \; \alpha \dots \alpha^{m-1}\right) \otimes \left(\widetilde{\mathcal{G}}_1 \dots \widetilde{\mathcal{G}}_{k+1}\right),$$

where $\widetilde{\mathcal{G}}_1, \dots, \widetilde{\mathcal{G}}_{k+1}$ are the rows of a generator matrix for $\widetilde{\mathcal{C}}$, and elements of $\mathbb{F}_{q^m}^n$ are represented as matrices over $\mathbb{F}_q^{m \times n}$. The possible linear combinations can be written as $\sum_{i=1}^{\widetilde{K}} x_i M_i$ in terms of variables x_i over $\mathbb{F}_q$. As with Ourivski and Johansson modeling (3), any low rank matrix $M = \sum_{i=1}^{\widetilde{K}} x_i M_i$ can be factored

into $m \times r$ and $r \times n$ matrices $\boldsymbol{S}$ and $\boldsymbol{C}$. This results in a modeling of the underlying MinRank problem we will dub Rank Decomposition modeling:

$$\boldsymbol{SC} = \sum_{i=1}^{\widetilde{K}} x_i M_i.$$

Note that in the above equation, the variables x_i only occur linearly. As such, we will dub them the "linear variables". Provided that $\widetilde{K} \leq mn$, we may eliminate these linear variables from $mn - \widetilde{K}$ of the above equations. The reader may verify that the resulting system is equivalent to the Ourivski and Johansson modeling (3) equations. However, in subsequent sections we will retain the linear variables, as their use will be required to set up a better method of modeling for both generic MinRank and the underdetermined case of RD.

We will however eliminate enough of the linear variables to get a 1-dimensional solution space for RD. Recall that the specialization used for $\boldsymbol{S}$ and $\boldsymbol{C}$ in the Ourivski and Johansson modeling (3) case set $m-1$ entries in the first column of $\boldsymbol{SC}$ to 0. Plugging this specialization into the Decomposition Modeling equation we find that this has the effect of producing $m-1$ linear equations involving only the x_i's. In subsequent analysis, we will therefore eliminate these $m-1$ linear variables, resulting in a Decomposition Modeling system with a 1-dimensional solution space involving only $K = mk + 1$ linear variables.

5.2 Support Minors Modeling for Generic MinRank

Consider a generic MinRank problem involving K matrices of dimension $m \times n$ with a target rank of r, where the Rank Decomposition Modeling equations are given by:

$$\boldsymbol{SC} = \sum_{i=1}^{K} x_i M_i.$$

Consider the m matrices of dimension $(r+1) \times n$ given by $\boldsymbol{C}$ stacked with a row, $\boldsymbol{r_j} = \boldsymbol{\pi_j} \sum_{i=1}^{K} x_i M_i$, of $\sum_{i=1}^{K} x_i M_i$, where $\boldsymbol{\pi_j}$ is the row vector with only one 1 on the jst column :

$$\boldsymbol{C}'_j = \begin{pmatrix} \boldsymbol{r_j} \\ \boldsymbol{C} \end{pmatrix}.$$

For any $\boldsymbol{S}, \boldsymbol{C}, x_i$ solving the Rank Decomposition Modeling form of the MinRank problem, we have that $\boldsymbol{r_j}$ is in the span of the rows of $\boldsymbol{C}$ and therefore each matrix $\boldsymbol{C}'_j$ has rank at most r. This allows us to set up a new modeling for the MinRank problem by setting the $(r+1) \times (r+1)$ minors of the matrices $\boldsymbol{C}'_j$ equal to zero. The resulting equations, of which there are $m\binom{n}{r+1}$ can be expressed via Cofactor expansion with respect to their first row. In this way they can be seen to be expressible as bilinear forms in the variables x_i and the $r \times r$ minors of $\boldsymbol{C}$, i.e. the variables $c_{\boldsymbol{T}}$. As there are $K\binom{n}{r}$ monomials that are bilinear in the variables x_i and the variables $c_{\boldsymbol{T}}$, and the solution space has dimension 1, we expect to

be able to solve the Support Minors Modeling system by direct linearization whenever:

$$m\binom{n}{r+1} \geq K\binom{n}{r} - 1. \tag{14}$$

We did a lot of experiments as explained in Section 5.5, and they suggest that it is the case.

Remark 2. Note that, in what follows, the Eq. (14) will sometimes be refered as the "$b = 1$ case".

5.3 Solving Support Minors Modeling at a higher degree

In the case where Eq. (14) does not hold we may produce a generalized version of Support Minors Modeling, multiplying the Support Minors Modeling equations by homogeneous degree $b-1$ monomials in the linear variables, resulting in a system of equations that are homogeneous degree 1 in the variables $c_{\boldsymbol{T}}$ and homogeneous degree b in the variables x_i. The strategy will again be to linearize over monomials. The most common cases are $q = 2$ and $q > b$. In the former case there are $\sum_{i=1}^{b}\binom{n}{r}\binom{K}{i}$ monomials, and in the latter case there are $\binom{n}{r}\binom{K+b-1}{b}$. For the time being, we will focus on the simpler $q > b$ case. There is however an unavoidable complication which occurs whenever we consider $b \geq q$. Unlike in the simpler $b = 1$ case, for $b \geq 2$ we cannot assume that all $m\binom{n}{r+1}\binom{K+b-2}{b-1}$ equations we produce in this way are linearly independent up to the point where we can solve the system by linearization. In fact, we can construct explicit linear relations between the equations starting at $b = 2$.

To construct a nontrivial linear relation at $b = 2$, let T_{jk} be the coefficients of a symmetric 2-tensor of dimension m. It then follows that the $(r+2)\times(r+2)$ minors of the following matrix expression are equal to zero:

$$\sum_{j=1}^{m}\sum_{k=1}^{m} T_{jk}\begin{pmatrix}\boldsymbol{r_j}\\ \boldsymbol{r_k}\\ \boldsymbol{C}\end{pmatrix}$$

To see this, note that the minors of the matrix $\begin{pmatrix}\boldsymbol{r_j}\\ \boldsymbol{r_k}\\ \boldsymbol{C}\end{pmatrix}$ are antisymmetric with respect to j and k, while the tensor T_{jk} used to contract the j and k indices is symmetric. The minors correspond to linear relations among the $b = 2$ equations, since they can be expanded via cofactor expansion as a sum of terms that are products of a linear polynomial in the x_i variables and a $b = 1$ equation corresponding to a minor of $\boldsymbol{C}'_k = \begin{pmatrix}\boldsymbol{r_k}\\ \boldsymbol{C}\end{pmatrix}$, and are therefore in the span of the $b = 2$ equations.

These linear relations may be mapped into relations among the $b = 3$ equations by multiplying each $b = 2$ equation in the cofactor expansion of the $b = 2$ linear relation by the same linear monomial in the x_i variables. However, the

resulting linear relations, are not themselves linearly independent, due to the fact that for any 3-tensor with coefficients T_{jkl}, the $r+3$ by $r+3$ minors of

$$\sum_{j=1}^{m}\sum_{k=1}^{m}\sum_{l=1}^{m} T_{jkl} \begin{pmatrix} \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{r_l} \\ \boldsymbol{C} \end{pmatrix}$$

are equal to zero and are in the span of the $b = 3$ linear relations derived from the $b = 2$ linear relations. This argument extends also to higher values of b, so that, if linear relations of the form considered above are the only relevant linear relations, then the number of linearly independent equations available for linearization at a given value of b is:

$$\text{Exp} = \sum_{i=1}^{b} (-1)^{i+1} \binom{n}{r+i} \binom{m+i-1}{i} \binom{K+b-i-1}{b-i}. \tag{15}$$

Experimentally, we found this to be the case with the only exceptions being:

1. When Exp exceeds the number of monomials for a smaller value of b, typically 1, the number of equations is observed to be equal to the number of monomials for all higher values of b as well, even if Exp does not exceed the total number of monomials at these higher values of b.
2. When the underlying MinRank Problem has a nontrivial solution and cannot be solved a $b = 1$, we find the maximum number of linearly independent equations is not the total number of monomials but is less by 1. This is expected, since when the underlying MinRank problem has a nontrivial solution, then the Support Minors Modeling equations have a 1 dimensional solution space.

We can also construct additional nontrivial linear relations starting at $b = r + 2$. The simplest example of this sort of linear relation occurs when $m > r + 1$. Note that each of the Support Minors modeling equations at $b = 1$ is bilinear in the x_i variables and a subset consisting of $r + 1$ of the variables $c_{\boldsymbol{T}}$. Note also, that there are a total of m equations derived from the same subset (One for each row of $\sum_{i=0}^{K} x_i M_i$.) Therefore, if we consider the Jacobian of the $b = 1$ equations with respect to the variables $c_{\boldsymbol{T}}$, the m equations involving only $r + 1$ of the variables $c_{\boldsymbol{T}}$ will form a submatrix with m rows and only $r + 1$ nonzero columns. We can therefore construct a left kernel vector for these equations whose coefficients are degree $r + 1$ polynomials in the x_i variables. Multiplying the equations by this kernel vector will produce zero, because the $b = 1$ equations are homogeneous, and multiplying equations from a bilinear system by a kernel vector of the Jacobian of that system cancels all the highest degree terms. This suggests that Eq. (15) needs to be modified when we consider values of b that are $r + 2$ or greater. These additional linear relations do not appear to be relevant in the most interesting range of b for attacks on any of the cryptosystems considered, however.

In summary, in the general case, we expect to be able to linearize at degree b whenever $b < r + 2$ and

$$\binom{n}{r}\binom{K+b-1}{b}-1 \leq \sum_{i=1}^{b}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K+b-i-1}{b-i} \quad (16)$$

Note that, for $b = 1$, we recovert the result (14).

5.4 The $q = 2$ case

The same considerations apply in the $q = 2$ case, but due to the field equations, $x_i^2 = x_i$, for systems with $b \geq 2$, a number of monomials will collapse to a lower degree. This results in a system which is no longer homogeneous. Thus, in this case it is most profitable to combine the equations obtained at a given value of b with those produced using all smaller values of b. Similar considerations to the general case imply that as long as $b < r + 2$ we will have

$$\text{Exp} = \sum_{j=1}^{b}\sum_{i=1}^{j}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}. \quad (17)$$

equations with which to linearize the

$$\sum_{j=1}^{b}\binom{n}{r}\binom{K}{j}$$

monomials that occur at a given value of b. We therefore expect to be able to solve by linearization when $b < r + 2$ and b is large enough that

$$\sum_{j=1}^{b}\binom{n}{r}\binom{K}{j} - 1 \leq \sum_{j=1}^{b}\sum_{i=1}^{j}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}. \quad (18)$$

5.5 Improvements for Generic Minrank

We can consider applying the Support Minors Modeling techniques to submatrices $\sum_{i=1}^{K} M_i' x_i$ of $\sum_{i=1}^{K} M_i x_i$. We generally find that the most beneficial settings use matrices with all m rows, but only $n' \leq n$ of the columns. Note that if $\sum_{i=1}^{K} M_i x_i$ has rank less than or equal to r, so does $\sum_{i=1}^{K} M_i' x_i$, so assuming we have a unique solution x_i to both systems of equations, it will be the same. It is always beneficial for the attacker to reduce n' to the minimum value allowing linearization at a given degree b, however, it can sometimes lead to an even lower complexity to reduce n' further and solve at a higher degree b.

We verified experimentally that the value of Exp correctly predicts the number of linearly independent polynomials. We constructed random systems (with and without a solution) for $q = 2, 13$, with $m = 7, 8$, $r = 2, 3$, $n = r+3, r+4, r+5$, $K = 3, \ldots, 20$. In all the cases, the number of linearly independent polynomials was as expected.

5.6 Using Support Minors Modeling in conjunction with MaxMin for RD

Recall that from MaxMin, we obtain $m\binom{n-k-1}{r}$ homogeneous linear equations in the variables $c_{\boldsymbol{T}}$. These can be used to produce equations over the same monomials as used for Support Minors Modeling with $K = mk + 1$. In the $q > b$ case, this can be done by multiplying the equations from MaxMin by homogeneous degree b monomials in the variables x_i. In the $q = 2$ case this can be done by multiplying the MaxMin equations by monomials of degree b or less. With all the arguments mentionned above and the experiments mentionned in Section 5.5, we can make a similar heuristic as Heuristic 1, this suggests that linearization is possible for $q > b$, $0 < b < r + 2$ whenever:

$$\begin{aligned}&\binom{n}{r}\binom{mk+b}{b} - 1 \leq \\ &m\binom{n-k-1}{r}\binom{mk+b}{b} + \sum_{i=1}^{b}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{mk+b-i}{b-i},\end{aligned} \tag{19}$$

and for $q = 2$, $0 < b < r + 2$ whenever:

$$A_b - 1 \leq B_c + C_b \tag{20}$$

where

$$\begin{aligned}A_b &:= \sum_{j=1}^{b}\binom{n}{r}\binom{mk+1}{j} \\ B_b &:= \sum_{j=1}^{b}\left(m\binom{n-k-1}{r}\binom{mk+1}{j}\right) \\ C_b &:= \sum_{j=1}^{b}\sum_{i=1}^{j}\left((-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{mk+1}{j-i}\right).\end{aligned}$$

For the latter, it leads to a complexity of

$$\mathcal{O}\left((B_b + C_b)A_b^{\omega-1}\right) \tag{21}$$

where b is the smallest positive integer so that the condition (20) is fulfilled. This complexity formula correspond to solving a linear system with A_b unknowns and $B_b + C_b$ equations, recall that ω is the constant of linear algebra.

One notices that for a large range of parameters, this system is particularly sparse, so one could take advantage of that to use Wiedemann algorithm [36]. More precisely, for values of m, n, r and k satisfying the conditions of ROLLO or RQC parameters (see Sections 7.1 and 7.2) and the condition (20), we typically find that $b \approx r$.

In this case, B_b equations consist of $\binom{k+r+1}{r}$ monomials, C_b equations consist of $(mk+1)(r+1)$ monomials, and the total space of monomials is of size A_b. The Wiedemann's algorithm complexity can be written in term of the average number of monomials per equation, in our case it is

$$\frac{B_b\binom{k+r+1}{r} + C_b(mk+1)(r+1)}{B_b + C_b}.$$

Thus the linearized system at degree b is sufficiently sparse that Wiedemann outperforms Strassen for $b \geq 2$. Therefore the complexity of support minors modeling bootstrapping MaxMin for RD is

$$\mathcal{O}\left(\frac{B_b\binom{k+r+1}{r} + C_b(mk+1)(r+1)}{B_b + C_b}\left(\sum_{j=1}^{b}\binom{n}{r}\binom{mk+1}{j}\right)^2\right) \tag{22}$$

where b is still the smallest positive integer so that the condition (20) is fulfilled.

A similar formula applies for the case $q > b$ and for parameters of other cryptosystems such as Rainbow and GeMMS.

6 Complexity of the attacks for different cryptosystems

6.1 Attacks against the Rank Decoding problem

Table 1 presents the complexity of our attack (see sections 4 and 5) against RD and gives the complexities (column "This paper") for all the parameters in the ROLLO and RQC submissions to the NIST competition and Loidreau cryptosystem [30]; for the sake of clarity, we give the previous best known complexity from [11] (last column).

Recall that when $a = 0$ it corresponds to the *overdetermined case*, when $p \neq 0$ it corresponds to the "super"-*overdetermined case*, see Section 4.2, when $a \neq 0$ it corresponds to the hybrid case, see Section 4.3. The third column gives the orignal rate of "overdeterminess" and the fifth column gives the final rate after modification.

6.2 Attacks against the MinRank problem

Tables 2 and 3 show the complexity of our attack against generic MinRank problem for GeMSS and Rainbow, two cryptosystems at the second round of the aforementioned NIST competition. The two tables also compare this new attack to the previous MinRank attacks, which use minors modeling in the case of GeMSS [14] and a linear algebra search [16] in the case of Rainbow. In table 3, the column "Best/Type" shows the complexity of the current best attack against Rainbow, which is not a MinRank attack.

Table 1. Complexity of the attack against Rank Decoding for different systems.

Cryptosystem	**Parameters** (m,n,k,r)	$\frac{m\binom{n-k-1}{r}}{\binom{n}{r}-1}$	a	p	$\frac{m\binom{n-k-p-1}{r}}{\binom{n-p-a}{r}-1}$	**This paper**	[11]
Loidreau ([30])	$(128,120,80,4)$	1.28	0	3	1.02	**64.2**	98
ROLLO-I-128	$(79,94,47,5)$	1.97	0	9	1.05	**70.2**	117
ROLLO-I-192	$(89,106,53,6)$	1.06	0	0	1.06	**86.2**	144
ROLLO-I-256	$(113,134,67,7)$	0.67	8	0	1.04	**158.1**	197
ROLLO-II-128	$(83,298,149,5)$	2.42	0	40	1.01	**93.0**	134
ROLLO-II-192	$(107,302,151,6)$	1.53	0	18	1.01	**110.5**	164
ROLLO-II-256	$(127,314,157,7)$	0.89	6	0	1.01	**169.8**	217
ROLLO-III-128	$(101,94,47,5)$	2.52	0	12	1.03	**69.5**	119
ROLLO-III-192	$(107,118,59,6)$	1.31	0	4	1.04	**88.0**	148
ROLLO-III-256	$(131,134,67,7)$	0.78	5	0	1.02	**137.7**	200
RQC-I	$(97,134,67,5)$	2.60	0	18	1.04	**76.6**	123
RQC-II	$(107,202,101,6)$	1.46	0	10	1.04	**100.9**	156
RQC-III	$(137,262,131,7)$	0.93	3	0	1.01	**143.8**	214

7 Examples of new parameters for ROLLO-I and RQC

In light of the attacks presented in this article, it is possible to give a few examples of new parameters for the rank-based cryptosystems, submitted to the NIST competition, ROLLO and RQC. Moreover, this section also contains an adaptation of the attacks to a newer version of RQC, using what we call *non-homogeneous error*.

For cryptographic purpose, parameters have to belong to an area which does not correspond to the overdetermined case and such that the hybrid approach would make the attack worse than in the underdetermined case.

Remark 3. In what follows, the complexity in the *underdetermined case* correspond to the complexity of our attack given by (22) or (21) if $b \leq 1$. Despite the fact that it is sometimes greater than the complexity for the *underdetermined case* described in [11], our attack has the advantage that it does not require a strong assumption on the *solving degree*. In fact, the latter could sometimes lead to complexities greater than expected if it was not bounded from above by $r+1$, even if so far experiments seem to confirm it is the case.

Alongside the algebraic attacks in this paper, the best combinatorial attack against RSD is in [4]; as a reminder, for attacking a $[n,k]$ code over $\mathbb{F}_{q^m}$ with target rank r, its complexity is

$$\mathcal{O}\left((nm)^2 q^{r\left\lceil \frac{m(k+1)}{n} \right\rceil - m}\right)$$

In what follows, one notices that the complexities of our attack against current parameters of ROLLO-I and RQC are given, even if they were already presented in Table 1; this is for the sake of clarity, so that the reader can compare them more easily with the new ones.

Table 2. Complexity comparison between the new and the previous MinRank attacks against GeMSS parameters. Recall that the previous attack used minors (see [14]). The new complexity is computed by finding the number of columns n' and the degree b that minimizes the complexity, as described in Section 5.

						Complexity	
(D, n, Δ, v)	n/m	K	r	n'	b	New	Previous
GeMSS128$(513, 174, 12, 12)$	174	162	34	61	2	158	522
GeMSS192$(513, 256, 22, 20)$	265	243	52	94	2	224	537
GeMSS256$(513, 354, 30, 33)$	354	324	73	126	3	304	1254
RedGeMSS128$(17, 177, 15, 15)$	177	162	35	62	2	160	538
RedGeMSS192$(17, 266, 23, 25)$	266	243	53	90	3	227	870
RedGeMSS256$(17, 358, 34, 35)$	358	324	74	120	3	305	1273
BlueGeMSS128$(129, 175, 13, 14)$	175	162	35	63	2	162	537
BlueGeMSS192$(129, 265, 22, 23)$	265	243	53	90	3	229	870
BlueGeMSS256$(129, 358, 34, 32)$	358	324	74	111	3	305	1273

Table 3. Comparison between the new MinRank attack, the previous best MinRank attack using linear algebra search, and the best known attack for Rainbow. Here the acronyms RBS and DA stand from Rainbow Band Separation and Direct Algebraic, respectively [16]. The new complexity is computed by finding the number of columns n' and the degree b that minimizes the complexity, as described in Section 5.

						Complexity		
Rainbow$(GF(q), v_1, o_1, o_2)$	n	K	r	n'	b	New	Previous	Best / Type
Ia$(GF(16), 32, 32, 32)$	96	33	64	84	2	162	161	145/RBS
IIIc$(GF(256), 68, 36, 36)$	140	37	104	132	1	217	585	215/DA
Vc$(GF(256), 92, 48, 48)$	188	49	140	176	2	281	778	275/DA

Remark 4. In this section, the notation is chosen to match the one in ROLLO and RQC submissions' specifications ([7] and [3]). One should be careful that here, n is the block-length and not the length of the code which can be either $2n$ or $3n$.

7.1 New parameters for ROLLO-I

For ROLLO-I one considers a $[2n, n]$-code over $\mathbb{F}_{q^m}$, there are two type of practical attacks:

- **message attack**: it corresponds to an attack on the RSD problem with target rank r on the $[2n, n]$ code.
- **key attack**: in this case, one attacks the secret key which generates the $[2n, n]$-code. It was proven in [24] that the structure of the code can be used so that the attacker is reduce to attacking a $\left[2n - \lfloor \frac{n}{d} \rfloor, n - \lfloor \frac{n}{d} \rfloor\right]$-code with the same target rank d (the rank of the small weight codeword used to generate the $[2n, n]$-code).

Remark 5. For ROLLO-I parameters, because of the previous attack ([11]), we used to consider $d = r + 1$, with the new parameters proposed here, it will not be necessary anymore.

Besides security constraints, the main constraints come from decoding; in order to be able to use the optimized algorithm for LRPC which has a Decoding Failure Rate (DFR) in $(n - 2(d + r) + 5)$, it is necessary that

- $m > 2rd - r$ ([27]).
- $(n - rd) > 7$ in order not to create parasite terms of order 2 in the DFR with the improved algorithm (with DFR of $2^{-3(n-rd+3)}$).

These constraints are the constraints which have been considered for the current parameters of ROLLO-I, but if one does not use the improved decoding algorithm for LRPC, it is also possible to consider the basic decoding algorithm. In that case, the DFR drops down to $(n - rd + 1)$, but it permits to get lower conditions on m, which is very important for algebraic attacks, i.e. the lower m, the higher complexity for the algebraic attacks. In that case it is sufficient to consider $m > \frac{5rd}{4}$ and still have $n - rd > 5$.

In all following tables, one considers $\omega = 2.81$ and uses the notation:

- **over/hybrid** is the cost of the hybrid attack; the value of a is the smallest to reach the overdetermined case, $a = 0$ means that parameters are already in the overdetermined case.
- **under** is the case of underdetermined attack.
- **comb** is the the cost of the best combinatorial attack mentionned above.
- **DFR** is the binary logarithm of the DFR.

Table 4 gives the complexity of current attacks on ROLLO-I, Table 5 gives examples of new parameters for ROLLO-I with the improved decoding algorithm, together with attacks complexities. At last, Table 6 gives examples of new parameters for ROLLO-I with the basic decoding algorithm (not currently used for NIST standardization). The "*"-symbol means that the best attacks are obtained on the derived code from key attack in the case $r = d$.

Instance	q	n	m	r	d	pk size (B)	over/hybrid	a	p	under	b	comb
ROLLO-I-128	2	47	79	5	6	465	70	0	9	107	1	129
ROLLO-I-192	2	53	89	6	7	590	86	0	0	121	1	192
ROLLO-I-256	2	67	113	7	8	947	158	8	0	154	2	294

Table 4. Current attacks on ROLLO-I

Instance	q	n	m	r	d	pk size (B)	DFR	over/hybrid	a	p	under	b	comb
newROLLO-I-128	2	67	113	7	8	947	-42	158	8	0	154	2	294
newROLLO-I-192	2	79	151	8	9	1491	-50	245	16	0	220	4	465
newROLLO-I-256	2	89	163	9	9	1813	-33	292*	18	0	256*	5	583

Table 5. New proposed parameters and attacks for improved decoding algorithm

Instance	q	n	m	r	d	pk size (B)	DFR	over/hybrid	a	p	under	b	comb
new2ROLLO-I-128	2	83	73	7	8	757	-27	233	18	0	180	3	195
new2ROLLO-I-192	2	97	89	8	8	1057	-33	258*	17	0	197*	3	256*
new2ROLLO-I-256	2	113	103	9	9	1454	-33	408*	30	0	283*	6	348*

Table 6. New proposed parameters and attacks for basic decoding algorithm

7.2 New parameters for RQC

There are two type of attacks for RQC, using the same notation that for the RQC submission:

- **key attack**: it is exactly the same attack as for ROLLO-I, one searches to attack a $[2n, n]$-code over $\mathbb{F}_{q^m}$ for an error of weight w.
- **message attack**: in that case there are two problems to consider: a genuine IRSD problem for a $[2n, n]$-code with secret a small word (r_1, r_2) of rank w_r and a security reduction of the ind-CPA property to decoding a $[3n, n]$-code still for the same weight w_r as for the secret key.

The latter differs from ROLLO-I for which a code of length $3n$ is never considered. Considering such a code makes life simpler for the attacker since in that case condition (1) is easier to fullfill.

A small modification of the error vector and implications. As a reminder, the reduction for RQC is done to solving a problem of the form:

$$\begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{rot}(\mathbf{h}) \\ \mathbf{0} & \mathbf{I}_n & \mathbf{rot}(\mathbf{s}) \end{pmatrix} .(r_1, e, r_2)^T = (s_1, s_2)^T$$

where everything is known to the attacker except the error vector (r_1, e, r_2). The vectors r_1 and r_2 have the same support E of dimension r and in practice e is also chosen in the support E. The main reason for this is the fact that in term of reduction, if e has not the same support than r_1 and r_2, the reduction is not done to a genuine RSD problem. To sum up, considering the support of e as the one of r_1 and r_2 permits to have a reduction to a clearly identified problem, at the cost of a loss of complexity to the advantage of the attacker.

Let us consider the impact on e on the decoding: for RQC the error to decode is $xr_1 + yr_2 + e$ (where 1 belongs to the support of (x, y)), this means that increasing the weight of r_1 or r_2 has a strong impact on the total weight because of the multiplication by x and y, increasing only independantly the weight of e has only a minor impact on the total weight to decode.

This remarks leads to considering a slight modification of the RQC algorithm, namely *the non-homogeneous error.*

We now consider that the support E' of e has dimension $w_{r'} = w_r + \delta$ and contains the support E of r_1 and r_2 of dimension w_r. Typically we choose $\delta \approx w_r$. The impacts are the following:

- it increases by δ the weight to search on a part of the error vector, intuitively we see that when δ increases, it makes the work of the attacker more complex. The idea is that the increase of delta will make the $[3n, n]$-advantage impractical.
- it increases by δ the weight to decode, but this can easily be handled by increasing slightly the parameters.

With this new version, the reductions have to change. The new problem with non-homogeneous error (r_1, e, r_2) reduces to attacking a support of weight simply w_r (and not $w_r+\delta$). This reduction makes sense for combinatorial attacks for which a reduction to only a weight w_r is enough because of the increase of parameters. For algebraic attacks it is not sufficient, but clearly the introduction of δ makes the situation more complex.

Adaptation of the hybrid attack in the case of non-homogeneous support. As a reminder, one writes the error as a product

$$(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})\boldsymbol{SC}$$

where $\boldsymbol{S}$ is a $m \times r$ matrix with entries in $\mathbb{F}_q$ consisting in a basis of the support of the error and $\boldsymbol{C}$ is a $r \times n$ matrix with entries in $\mathbb{F}_2$ consisting in the coordinates of each component of the error in this basis. Writting the new error in a similar way but with block matrices enables us to explicit its particular structure. Thus, the error vector (r_1, e, r_2) is written as a product of

$$(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})$$

with the two following matrices

$$\widetilde{\boldsymbol{S}} \;=\; \left[\begin{array}{c|c} \boldsymbol{S}_1 & \boldsymbol{S}_2 \end{array}\right] \;\in\; \mathbb{F}_q^{m \times (w_r + \delta)} \quad \text{and} \quad \widetilde{\boldsymbol{C}} \;=\; \left[\begin{array}{c|c|c} \boldsymbol{C}_1 & \boldsymbol{C}_2 & \boldsymbol{C}_3 \\ \hline 0 & \boldsymbol{C}_2' & 0 \end{array}\right] \;\in\; \mathbb{F}_q^{(w_r+\delta) \times n}.$$

The matrix $\boldsymbol{S}_1$ is a basis of E and $\widetilde{\boldsymbol{S}}$ is a basis of E' ($E \subset E'$).

Recall that for this special case we use the following notation: $3n$ is the length of the code and n is its dimension. As mentionned in Section 3.2, we have to specialize the first column of $\boldsymbol{S}$ (resp. $\widetilde{\boldsymbol{S}}$) to $(1, 0, \ldots, 0)^T$ and to put $\boldsymbol{C}$ (resp. $\widetilde{\boldsymbol{C}}$) in systematic form so that the attack works. Clearly, one tries to put the identity block in $\widetilde{\boldsymbol{C}}$ between its $n+1$-th and $2n$-th column.

The aforementionned attack relied on the condition (1) in which the right part of the inequality counts the number of distinct maximal minors in $\widetilde{\boldsymbol{C}}$. With this approach, the condition does not take advantage of the structure of $\widetilde{\boldsymbol{C}}$. In fact, as it contains two zero blocks, its number of maximal minors equal to zero is

$$M \;:=\; \sum_{i=0}^{\delta-1} \binom{2n}{w_r + \delta - i} \binom{n}{i}$$

So one gets a new condition:

$$m \binom{2n-1}{w_r + \delta} \;\geq\; \binom{3n}{w_r + \delta} - M - 1. \tag{23}$$

This new condition yields to a new complexity in the case where it is fulfilled and to a new hybrid approach if it is not. When the condition (23) it is fulfilled, the new complexity is

$$\mathcal{O}\left(m \binom{2n-1}{w_r + \delta} \left(\binom{3n}{w_r + \delta} - M \right)^{\omega - 1} \right).$$

If it is not, one wants to guess a columns of $\widetilde{\boldsymbol{C}}$ to perform an hybrid approach as mentionned above. One notices that once again the structure of $\widetilde{\boldsymbol{C}}$ can be used by the attacker, in fact the cost of the exponential part of the hybrid attack is reduced if one guesses columns for which the lower block is a zero block. Doing so, the exponentional term will drop from $q^{a(w_r+\delta)}$ down to q^{aw_r}. To sum

everything up, the cost of the new attack (both in the overdetermined case, i.e. when $a = 0$, and the hybrid case) is

$$\mathcal{O}\left(q^{aw_r} m\binom{2n-1}{w_r+\delta}\left(\binom{3n-a}{w_r+\delta} - \underbrace{\sum_{i=0}^{\delta-1}\binom{2n-a}{w_r+\delta-i}\binom{n}{i}}_{:=\ M_a}\right)^{\omega-1}\right)$$

where a is the smallest integer such that the following condition is fulfilled

$$m\binom{2n-1}{w_r+\delta} \ \geq \ \binom{3n-a}{w_r+\delta} - M_a - 1. \tag{24}$$

As for ROLLO, there are decoding constraints for RQC:

- one wants to decode the error $xr_1 + yr_2 + e$ of weight $w.w_r + \delta$, hence if the decoding code is a Gabidulin $[n, k]$-code, it means

$$w.w_r + \delta \leq \frac{n-k}{2}.$$

- one also needs $m \geq n$ for the Gabidulin code.

Table 7 gives the complexity of attacks on current RQC parameters, Table 8 gives examples of new parameters for RQC with the non-homogeneous error, together with attacks complexities. Those tables use the following notation :

- **hyb2n(a)**: hybrid attack for length $2n$ (n block size), a concerns the hybrid attack.
- **hyb3n(a)**: non-homogeneous hybrid attack for length $3n$ (n block size), a concerns the hybrid attack.
- **und2n**: underminated attack for length $2n$.
- **comb3n**: combinatorial attack for length $3n$.

Instance	q	n	m	k	w	w_r	pk size (B)	over/hybrid	a	p	under	b	comb
RQC-I	2	67	97	4	5	6	853	77	0	18	117	1	128
RQC-II	2	101	107	3	6	8	1391	101	0	10	141	1	192
RQC-III	2	131	137	3	7	9	2284	144	3	0	163	1	256

Table 7. Current attacks on RQC

One notices that all algebraic attacks are more efficient on the $[2n, n]$-code with w rather than on the $[3n, n]$-code with w_r. One also notices that for hyb2n(a), clearly the complexity lies between the usual hybrid attack for weight w_r and classical attack for weight $w_r + \delta$. Concerning the three types of parameters these complexities are respectively 133/420 ($a = 0/16$), 157/965 ($a = 0/44$) and 179/1012 ($a = 0/46$), the actual given complexity from non-homogeneous hybrid attacks lies in between.

Instance	q	n	m	k	w	w_r	δ	pk (B)	hyb2n(a)	hyb3n(a)	und2n	b	comb3n
newRQC-I	2	113	127	3	7	7	6	1793	160(6)	211(0)	158	1	184
newRQC-II	2	149	151	5	8	8	8	2812	331(24)	262(0)	224	3	268
newRQC-III	2	179	181	3	9	9	7	4049	553(44)	321(5)	324	6	378

Table 8. New parameters for RQC

8 Conclusion

In this paper we improve on the results by [11] on the Rank Decoding problem by providing a better analysis which permits to avoid the use of Gröbner basis and permits to completely break rank-based cryptosystems parameters proposed to the NIST Standardization Process, when analysis in [11] only attacked slightly these parameters (mostly corresponding to the overdeterminated case defined in [11]). A very important feature of our attack is that we can give its complexity without requiring any strong assumption on the so-called solving degree.

We generalize this approach to the case of the MinRank problem for which we obtain the best known complexity with algebraic attacks, again without relying on assumptions on the solving degree. We also proposed a new approach for the underdeterminated case as described in [11], for some parameters this attack supersedes the results of [11], in particular for attacking ROLLO-I-256 parameters, anew this new attack does not rely on assumption on the solving degree. At last we give examples of parameters for ROLLO-I and RQC resistant to our new attacks.

Overall the results proposed in this paper give a new and deeper understanding of the complexity of difficult problems based on the rank metric. These problems have a strong interest since many systems still in the second round of the NIST standardization process, like ROLLO, RQC, GeMSS or Rainbow can be attacked through these problems.

Acknowledgements

This work has been supported by the French ANR projects CBCRYPT (ANR-17-CE39-0007) and the MOUSTIC project with the support from the European Regional Development Fund (ERDF) and the Regional Council of Normandie.

Javier Verbel was supported for this work by Colciencias scholarship 757 for PhD studies and the University of Louisville facilities.

We would like to thank John B Baena, and Karan Khathuria for useful discussions. We thank the Facultad de Ciencias of the Universidad Nacional de Colombia sede Medellín for granting us access to the Enlace server, where we ran some of the experiments.

References

1. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Zémor, G.: Ouroboros-R. First round submission

to the NIST post-quantum cryptography call (Nov 2017), https://pqc-ouroborosr.org
2. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G.: Rank quasi cyclic (RQC). First round submission to the NIST post-quantum cryptography call (Nov 2017), https://pqc-rqc.org
3. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G., Couvreur, A., Hauteville, A.: Rank quasi cyclic (RQC). Second round submission to the NIST post-quantum cryptography call (Apr 2019), https://pqc-rqc.org
4. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.P.: A new algorithm for solving the rank syndrome decoding problem. In: Proc. IEEE ISIT (2018)
5. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.P., Zémor, G.: LAKE – Low rAnk parity check codes Key Exchange. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/LAKE.zip
6. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.P., Zémor, G.: LOCKER – LOw rank parity ChecK codes EncRyption. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/LOCKER.zip
7. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.P., Zémor, G., Aguilar Melchor, C., Bettaieb, S., Bidoux, L., Magali, B., Otmani, A.: ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER). Second round submission to the NIST post-quantum cryptography call (Mar 2019), https://pqc-rollo.org
8. Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: a rank metric based signature scheme. In: Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III. LNCS, vol. 11478, pp. 728–758. Springer (2019). https://doi.org/10.1007/978-3-030-17659-4_25, https://doi.org/10.1007/978-3-030-17659-4_25
9. Aragon, N., Gaborit, P., Hauteville, A., Ruatta, O., Zémor, G.: Ranksign – a signature proposal for the NIST's call. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/RankSign.zip
10. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.P.: A new algorithm for solving the rank syndrome decoding problem. In: 2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018. pp. 2421–2425. IEEE (2018). https://doi.org/10.1109/ISIT.2018.8437464
11. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.P.: An Algebraic Attack on Rank Metric Code-Based Cryptosystems. Advances in Cryptology - EUROCRYPT 2020 (May 2020), https://arxiv.org/abs/1910.00810
12. Bettale, L., Faugere, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology **3**(3), 177–197 (2009)
13. Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. J. Comput. System Sci. **58**(3), 572–596 (Jun 1999)
14. "Casanova, A., "Faugère, J., "Marario, G., "Patarin, J., "Perret, L., "Ryckeghem, J.: (gemss) a great multivariate short signature. Second round submission to the

NIST post-quantum cryptography call (Apr 2019), https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions/GeMSS-Round2.zip
15. Debris-Alazard, T., Tillich, J.P.: Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme. In: Advances in Cryptology - ASIACRYPT 2018. pp. 62–92. LNCS, Springer, Brisbane, Australia (Dec 2018)
16. Ding, J.: Rainbow. Second round submission to the NIST post-quantum cryptography call (Apr 2019), https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions/Rainbow-Round2.zip
17. Faugère, J.C.: A new efficient algorithm for computing gröbner bases (F4). J. Pure Appl. Algebra **139**(1-3), 61–88 (1999)
18. Faugère, J.C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of Minrank. In: Wagner, D. (ed.) Advances in Cryptology - CRYPTO 2008. LNCS, vol. 5157, pp. 280–296 (2008)
19. Faugère, J., Safey El Din, M., Spaenlehauer, P.: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: International Symposium on Symbolic and Algebraic Computation, ISSAC 2010, Munich, Germany, July 25-28, 2010. pp. 257–264 (2010). https://doi.org/10.1145/1837934.1837984
20. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)
21. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their applications to cryptography. In: Advances in Cryptology - EUROCRYPT'91. pp. 482–489. No. 547 in LNCS, Brighton (Apr 1991)
22. Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography WCC'2013. Bergen, Norway (2013), www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf
23. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Information Theory **62**(2), 1006–1019 (2016)
24. Gaborit, P., Ruatta, O., Schrek, J., Zémor, G.: New results for rank-based cryptography. In: Progress in Cryptology - AFRICACRYPT 2014. LNCS, vol. 8469, pp. 1–12 (2014)
25. Gaborit, P., Ruatta, O., Schrek, J., Zémor, G.: Ranksign: An efficient signature algorithm based on the rank metric (extended version on arxiv). In: Post-Quantum Cryptography 2014. LNCS, vol. 8772, pp. 88–107. Springer (2014), https://arxiv.org/pdf/1606.00629.pdf
26. Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Information Theory **62(12)**, 7245–7252 (2016)
27. Hauteville, A., Tillich, J.P.: New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem. In: Proc. IEEE ISIT (2015), http://dx.doi.org/10.1109/ISIT.2015.7282956
28. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Buhler, J. (ed.) Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings. LNCS, vol. 1423, pp. 267–288. Springer (1998)
29. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Advances in Cryptology - CRYPTO'99. LNCS, vol. 1666, pp. 19–30. Springer, Santa Barbara, California, USA (Aug 1999). https://doi.org/10.1007/3-540-48405-1

30. Loidreau, P.: A new rank metric codes based encryption scheme. In: Post-Quantum Cryptography 2017. LNCS, vol. 10346, pp. 3–17. Springer (2017)
31. Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.L.M.: MDPC-McEliece: New McEliece variants from moderate density parity-check codes (2012), http://eprint.iacr.org/2012/409
32. Otmani, A., Talé-Kalachi, H., Ndjeya, S.: Improved cryptanalysis of rank metric schemes based on Gabidulin codes. Des. Codes Cryptogr. **86**(9), 1983–1996 (2018). https://doi.org/10.1007/s10623-017-0434-5, https://doi.org/10.1007/s10623-017-0434-5
33. Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission **38**(3), 237–246 (2002). https://doi.org/10.1023/A:1020369320078
34. Overbeck, R.: A new structural attack for GPT and variants. In: Mycrypt. LNCS, vol. 3715, pp. 50–63 (2005)
35. Verbel, J., Baena, J., Cabarcas, D., Perlner, R., Smith-Tone, D.: On the complexity of "superdetermined" Minrank instances. In: Post-Quantum Cryptography 2019. LNCS, vol. 11505, pp. 167–186. Springer, Chongqing, China (May 2019). https://doi.org/10.1007/978-3-030-25510-7_10, https://doi.org/10.1007/978-3-030-25510-7_10
36. Wiedemann, D.: Solving sparse linear equations over finite fields. IEEE transactions on information theory **32**(1), 54–62 (1986)