Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems

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, USA
[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 [24] 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 together with a much more precise analysis of its complexity compared to the one in [11]. Against ROLLO-I-128, ROLLO-I-192, and ROLLO-I-256, our attack has bit complexity respectively in 71, 87, and 151, to be compared to 117, 144, and 197 for the attack in [11]. Moreover, unlike this previous attack, ours does not need generic Gröbner basis algorithms since it only requires to solve a linear system. This improvement relies upon a modeling slightly different from the one in [11] combined with a new modeling for a generic MinRank instance. The latter modeling allows us to solve the MinRank problem using only linear algebra as well and no longer generic Gröbner basis algorithms, in addition to this, this new algorithm enables us to refine the analysis of MinRank's complexity given in [38]. MinRank is a problem of great interest for all multivariate-based cryptosystems, including GeMSS and Rainbow, which are at the second round of the aforementioned NIST competition; our new approach supersedes previous attacks for the MinRank problem.

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 [22] based on Gabidulin codes [21], 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 [23]. 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 [23] 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 [23,25,5,6], culminating in submissions to the National Institute of Standards and Technology (NIST) post-quantum competition [2,3], 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 [26,9] have been broken [16], 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 $(\beta_1, \dots, \beta_m)$ 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 $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$ as a matrix $\mathrm{Mat}(\boldsymbol{x}) = (X_{ij})_{i,j}$ in $\mathbb{F}_q^{m \times n}$, where $(X_{ij})_{1 \le i \le m}$ is the column vector formed by the coordinates of x_j in the basis $(\beta_1, \dots, \beta_m)$, that is, $x_j = \beta_1 X_{1j} + \dots + \beta_m X_{mj}$.

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

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

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. There are two approaches to solve RD instances: the combinatorial ones such as those in [24] and [10] and the algebraic ones, such as in [11]. For some time it was thought that the combinatorial approach was the most threatening attack on such schemes especially when q is small and all the parameters rank-metric submissions, until it became apparent in [11] that even for $q = 2$ the algebraic attacks outperform the combinatorial ones. Roughly speaking, if the conjecture made in [11] holds, the complexity of solving by algebraic attacks the decoding problem is of order $2^{O(r \log n)}$ with a constant depending on the rate $R = k/n$ of the code.

Even if the decoding problem is not known to be NP-complete for these $\mathbb{F}_{q^m}$-linear codes, there is a randomized reduction to an NP-complete problem [27] (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. We will consider here the homogeneous version of this problem which corresponds to

Problem 2 (MinRank problem).

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

Output: field elements $x_1, x_2, \ldots, x_K \in \mathbb{F}_q$ that are not all zero such that

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

It plays a central role in public key cryptography. Many multivariate schemes are either directly based on the hardness of this problem [15] or strongly related to it as in [35,37,36] or as in the NIST post-quantum competition candidates Gui [17], GeMSS [14] or Rainbow [18]. It first appeared in this context as part of an attack against the HFE cryptosystem [35] by Kipnis and Shamir[29]. It is also central in rank metric code-based cryptography, because the RD problem reduces to MinRank as explained in [19] and actually the best algorithms for solving this problem are really MinRank solvers taking advantage of the $\mathbb{F}_{q^m}$ underlying structure as in [11]. However the parameter region generally differs. When the RD problem arising from rank metric schemes is treated as a MinRank problem we generally have $K = \theta(n^2)$ and r is rather small (often $r = \theta(\sqrt{n})$) whereas for the multivariate cryptosystems $K = \theta(n)$ but r is much bigger.

The current best known algorithms for solving the MinRank problem have exponential complexity. Many of them are obtained by an algebraic approach too consisting in modeling the MinRank problem by a system of multivariate polynomial equations and then solve it with Gröbner basis techniques. The main modelings are the Kipnis-Shamir modeling [29] and the minors modeling [20]. The complexity of solving MinRank using these modelings has been investigated in [19,20,38]. In particular [38] shows that the bilinear system that arises from the Kipnis-Shamir modeling behaves much better than generic bilinear systems with respect to Gröbner basis techniques.

Our contribution. In this paper, we follow on from the approach in [11] and propose a slightly different modeling to solve the RD problem. Roughly speaking the algebraic approach followed by [11] is to set up a bilinear system which is satisfied by the error we are looking for. This system is formed by two kinds of variables, the "coefficient" variables and the "support" variables which is implicitly the modeling considered in [33]. The breakthrough obtained in [11] was to realize that

- the coefficient variables have to satisfy "maximal minor" equations: the maximal minors of a certain $r \times (n-k-1)$ matrix (i.e. the $r \times r$ minors) with entries being linear forms in the coefficient variables have to be equal to 0.
- these maximal minors are themselves linear combinations of maximal minors c_T of an $r \times n$ matrix $\boldsymbol{C}$ whose entries are the coefficient variables.

This gives a linear system involving the c_T's and allows to find the c_T's provided that there are enough linear equations. Moreover the original bilinear system has many solutions and there is some freedom of choosing the coefficient variables and the support variables. With the choice made in [11] the information we obtain in this way about the minors of $\boldsymbol{C}$ is not enough to be able to recover the coefficient variables directly (i.e. the entries of $\boldsymbol{C}$). In this case the last step of the algebraic attack still has to compute a Gröbner basis for the algebraic system consisting of the original system plus the knowledge on the c_T's obtained from the linear system.

The new approach followed in this paper uses the fact that there is a better way to use the freedom on the coefficient variables and the support variables: we can actually specify so many coefficient variables that all the remaining entries that we do not know are essentially equal to some maximal minor c_T of $\boldsymbol{C}$. This approach allows to avoid completely the computation of the Gröbner basis: we obtain from the knowledge of the c_T's obtained from the aforementioned linear system the coefficient variables and plugging in theses values in the original bilinear system it just remains to solve a linear system involving the support variables. This new approach 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 aforementioned similar approach in [11]. 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. This really corresponds to the case where we have enough linear equations by our approach to find all the c_T's (and hence all the coefficient variables). 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 require generic Gröbner Basis algorithms. In a rough way for $r = \mathcal{O}\left(\sqrt{n}\right)$ (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 and a new way to solve it. Roughly speaking we start with a quadratic modeling of MinRank that we call "support minors modeling" which is bilinear in the aforementioned coefficient and support variables and linear in the so called "linear variables". The last ones are precisely the x_i's that appear in the MinRank problem. Recall that the coefficient variables are the entries of a $r \times n$ matrix $\boldsymbol{C}$. The crucial observation is now that for all positive integer b all maximal minors of any $(r+b) \times n$ matrix obtained by adding to $\boldsymbol{C}$ any b rows of $\sum_i x_i \boldsymbol{M}_i$ are equal to 0. These minors are themselves linear combinations of terms of the form mc_T where c_T is a maximal minor of $\boldsymbol{C}$ and m a monomial of degree b in the x_i's. We can predict the number of independent linear equations in the mc_T's we obtain this way and when the number of such equations is bigger than the number of mc_T's we can recover their values and solve the MinRank problem without computing Gröbner bases. This new approach is not only effective in the underdetermined case of the RD problem it can also be quite effective for some multivariate proposals made to the NIST competition. In the case of the RD problem, it improves the attacks on [7] made in [11] for the parameter sets with the largest values of r (corresponding to parameters claiming 256 bits of security). The multivariate schemes that are affected by this new attack are for instance GeMSS and Rainbow. On GeMSS it shows MinRank attacks together with this new way of solving MinRank come close to the best known attacks against this scheme. On Rainbow it outperforms slightly the best known attacks for certain high security parameter sets.

At last, not only do these two new ways of solving algebraically the RD or MinRank problem outperform previous algebraic approaches in certain parameter regimes, they are also much better understood: we do not rely on heuristics based on the the first degree fall as in [38,11] to analyze its complexity, but it really amounts to solve a linear system and understand the number of independent linear equations that we obtain which is something for which we have been able to give accurate formulas predicting the behavior we obtain experimentally.

2 Notation

In what follows, we use the following notation and definitions:

- Matrices and vectors are written in boldface font $\boldsymbol{M}$.
- The transpose of a matrix $\boldsymbol{M}$ is denoted by $\boldsymbol{M}^\intercal$.
- 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 a subset $I \subset \{1..n\}$, $\#I$ stands for the number of elements in I.
- 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 notations $\boldsymbol{M}_{*,J} = \boldsymbol{M}_{\{1..m\},J}$ and $\boldsymbol{M}_{I,*} = \boldsymbol{M}_{I,\{1..n\}}$, where $\boldsymbol{M}$ has m rows and n columns, and $\boldsymbol{M}_{i,j}$ for the entry in row i and column j.
- We denote the determinant of a matrix $\boldsymbol{M}$ by $|\boldsymbol{M}|$. We also use a notation inspired by the previous one for denoting the determinant of a submatrix, $|\boldsymbol{M}|_{I,J}$ denotes the determinant of the submatrix $\boldsymbol{M}_{I,J}$ and $|\boldsymbol{M}|_{*,J}$ denotes the principal minor of $\boldsymbol{M}$ obtained by taking the determinant of $\boldsymbol{M}_{*,J}$.

- $\alpha \in \mathbb{F}_{q^m}$ is a primitive element, that is to say that $(1, \alpha, \dots, \alpha^{m-1})$ is a basis of $\mathbb{F}_{q^m}$ seen as an $\mathbb{F}_q$-vector space.
- For $\boldsymbol{v} = (v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$, the *support* of $\boldsymbol{v}$ is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ spanned by the vectors $v_1, \dots, v_n$. 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.
- Unless otherwise specified, the *decoding problem* always refers to the Rank Decoding problem.

3 Algebraic modeling of the MinRank and the decoding problem

3.1 Modeling of MinRank

Here is the modeling for the MinRank problem that we consider, it is related to the modeling used for decoding in the rank metric in [11]. The starting point is that, in order to solve the equation in *Problem* 2, we look for a nonzero solution $(\boldsymbol{S}, \boldsymbol{C}, \boldsymbol{x}) \in \mathbb{F}_q^{m \times r} \times \mathbb{F}_q^{r \times n} \times \mathbb{F}_q^K$ of

$$\boldsymbol{S}\boldsymbol{C} = \sum_{i=1}^{K} x_i \boldsymbol{M}_i. \tag{3}$$

$\boldsymbol{S}$ is an unknown matrix whose columns give a basis for the column space of a matrix of rank $\leq r$ we are looking for (i.e. $\sum_{i=1}^{K} x_i \boldsymbol{M}_i$). The i-th column of $\boldsymbol{C}$ represents the coordinates of the i-th column of the aforementioned matrix in this basis. We call the entries of $\boldsymbol{S}$ the *support variables*, and the entries of $\boldsymbol{C}$ the *coefficient variables*. Note that in the above equation, the variables x_i only occur linearly. As such, we will dub them the *linear variables*.

Let $\boldsymbol{r}_j$ be the j-th row of the matrix $\sum_{i=1}^{K} x_i \boldsymbol{M}_i$. Equation (3) implies that each row $\boldsymbol{r}_j$ is in the rowspace of $\boldsymbol{C}$ (or in coding theoretic terms $\boldsymbol{r}_j$ should belong to the code $\mathcal{C}$ generated by $\boldsymbol{C}$, that is $\mathcal{C} := \{\boldsymbol{u}\boldsymbol{C}, \boldsymbol{u} \in \mathbb{F}_q^r\}$). This implies that the following $(r+1) \times n$ matrix $\boldsymbol{C}'_j$ is of rank $\leq r$:

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

Therefore, all the maximal minors of this matrix should be equal to 0. Notice that these maximal minors can be expressed via cofactor expansion with respect to their first row. In this way, they can be seen as bilinear forms in the variables x_i and the $r \times r$ minors of $\boldsymbol{C}$. These minors will play a fundamental role in the whole paper and we will use the following notation for them.

Notation 1 *Let $T \subset \{1..n\}$ with $\#T = r$. We let*

$$c_T := |\boldsymbol{C}|_{*,T}$$

be the maximal minor of $\boldsymbol{C}$ corresponding to the columns of $\boldsymbol{C}$ that belong to T.

These considerations lead to the following algebraic modeling.

Modeling 1 (Support Minors modeling) *We consider the system of bilinear equations, given by canceling the maximal minors of the m matrices $\boldsymbol{C}'_j$:*

$$\left\{ f = 0 \middle| f \in \mathbf{MaxMinors} \begin{pmatrix} \boldsymbol{r_j} \\ \boldsymbol{C} \end{pmatrix},\ j \in \{1..m\} \right\}. \tag{4}$$

This system contains:

- $m\binom{n}{r+1}$ *bilinear equations with coefficients in* $\mathbb{F}_q$,
- $K + \binom{n}{r}$ *unknowns:* $\boldsymbol{x} = (x_1, \cdots, x_K)$ *and the* c_T*'s,* $T \subset \{1..n\}$ *with* $\#T = r$.

We search for the solutions x_i, c_T*'s in* $\mathbb{F}_q$.

Remark 1.

1. One of the point of having the c_T as unknowns instead of the coefficients C_{ij} of $\boldsymbol{C}$ is that, if we solve (4) directly in the x_i and the C_{ij} variables, then there are actually plenty of solutions to (4) since when $(\boldsymbol{x}, \boldsymbol{C})$ is a solution for it, then $(\boldsymbol{x}, \boldsymbol{AC})$ is also a solution for any invertible matrix $\boldsymbol{A}$ in $\mathbb{F}_q^{r\times r}$. With the c_T variables we only expect a space of dimension 1 for the c_T corresponding to the transformation $c_T \mapsto |\boldsymbol{A}|\, c_T$ that maps a given solution of (4) to a new one.
2. Another benefit brought by replacing the C_{ij} variables by the c_T's is of course that it brings a big saving in the number of possible monomials for writing the algebraic system (4) (about $r!$ times less). This allows for instance for solving this system by direct linearization when the number of equations of the previous modeling is larger than or equal to the number of different $x_i c_T$ monomials minus 1, namely when

$$m\binom{n}{r+1} \geq K\binom{n}{r} - 1. \tag{5}$$

   This turns out to be "almost" the case for several multivariate cryptosystem proposals based on the MinRank problem where K is generally of the same order as m and n.

3.2 The approach followed in [11] to solve the decoding problem

In what follows, we consider the (m, n, k, r)-decoding problem for a code $\mathcal{C}$ of length n, dimension k over $\mathbb{F}_{q^m}$ and assume we have received $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ at distance r from $\mathcal{C}$ and look for $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{e}$ such that $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ and $|\boldsymbol{e}| = r$. We will assume in what follows that there is a unique solution to this problem (which is relevant for our cryptographic schemes). The starting point is the Ourivksi-Johansson approach, consisting in considering the linear code $\widetilde{\mathcal{C}} = \mathcal{C} + \langle \boldsymbol{y} \rangle$. By construction, $\boldsymbol{e}$ belongs to $\widetilde{\mathcal{C}}$ as well as all its multiples $\lambda\boldsymbol{e}$, $\lambda \in \mathbb{F}_{q^m}$. Looking for non-zero codewords in $\widetilde{\mathcal{C}}$ of rank weight r has at least $q^m - 1$ different solutions, namely all the $\lambda\boldsymbol{e}$ for $\lambda \in \mathbb{F}_{q^m}^{\times}$.

It is readily seen that finding such codewords can be done by solving the (homogeneous) MinRank problem with $\boldsymbol{M}_{ij} := \mathrm{Mat}(\alpha^{i-1}\boldsymbol{c}_j)$ (we adopt a bivariate indexing of the $\boldsymbol{M}_i$'s which is more convenient here), for $(ij) \in \{1..m\}\times\{1..k+1\}$ and where $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_{k+1}$ is an $\mathbb{F}_{q^m}$-basis of $\widetilde{C}$. This is a consequence of the fact that the $\alpha^{i-1}\boldsymbol{c}_j$'s form an $\mathbb{F}_q$-basis of $\widetilde{C}$. However, the problem with this approach is that $K = (k+1)m$ which is of order $\Omega(n^2)$ for the parameters relevant to cryptography. This is much more than for the multivariate cryptosystems based on MinRank and (5) is far from being satisfied here. However, as observed in [11], it turns out in this particular case, it is possible because of the $\mathbb{F}_{q^m}$ linear structure of the code, to give an algebraic modeling that only involves the coefficients variables, that is the entries of $\boldsymbol{C}$. It is obtained by introducing a parity-check matrix for $\widetilde{C}$, that is a matrix $\boldsymbol{H}$ whose kernel is $\widetilde{C}$:

$$\widetilde{C} = \{\boldsymbol{c} \in \mathbb{F}_{q^m}^n : \boldsymbol{c}\boldsymbol{H}^\intercal = 0\}.$$

In our $\mathbb{F}_{q^m}$ linear setting the solution $\boldsymbol{e}$ we are looking for can be written as

$$\boldsymbol{e} = \begin{pmatrix}1 \; \alpha \; \dots \; \alpha^{m-1}\end{pmatrix} \boldsymbol{S}\boldsymbol{C}, \tag{6}$$

where $\boldsymbol{S} \in \mathbb{F}_q^{m\times r}$ and $\boldsymbol{C} \in \mathbb{F}_q^{r\times n}$ play the same role as in the previous subsection: $\boldsymbol{S}$ 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. By writing that $\boldsymbol{e}$ should belong to $\widetilde{C}$ we obtain that

$$\begin{pmatrix}1 \; \alpha \; \dots \; \alpha^{m-1}\end{pmatrix} \boldsymbol{S}\boldsymbol{C}\boldsymbol{H}^\intercal = \boldsymbol{0}_{n-k-1}. \tag{7}$$

The algebraic system involving only the coefficient variables follows immediately from this.

Proposition 1 ([11], Theorem 2). *The maximal minors of the $r \times (n-k-1)$ matrix $\boldsymbol{C}\boldsymbol{H}^\intercal$ are all equal to 0.*

Proof. Consider the following vector in $\mathbb{F}_q^r$: $\boldsymbol{e}' := \begin{pmatrix}1 \; \alpha \; \dots \; \alpha^{m-1}\end{pmatrix} \boldsymbol{S}$ whose entries generate (over $\mathbb{F}_q$) the subspace generated by the entries of $\boldsymbol{e}$ (i.e. its support). Substituting $\begin{pmatrix}1 \; \alpha \; \dots \; \alpha^{m-1}\end{pmatrix} \boldsymbol{S}$ for $\boldsymbol{e}'$ in (7) yields

$$\boldsymbol{e}'\boldsymbol{C}\boldsymbol{H}^\intercal = \boldsymbol{0}_{n-k-1}.$$

This shows that the r rows of $\boldsymbol{C}\boldsymbol{H}^\intercal$ are not independent and that the $r \times n$ matrix $\boldsymbol{C}\boldsymbol{H}^\intercal$ is of rank $\leq r-1$. □

These minors $\boldsymbol{C}\boldsymbol{H}^\intercal$ are polynomials in the entries of $\boldsymbol{C}$ with coefficients in $\mathbb{F}_{q^m}$. Since these entries belong to $\mathbb{F}_q$, the nullity of each minor gives m algebraic equations corresponding to polynomials with coefficients in $\mathbb{F}_q$. This involves the following operation

Notation 2 *Let $\mathcal{S} := \{\sum_j a_{ij} m_{ij} = 0, 1 \leq i \leq N\}$ be a set of polynomial equations where the m_{ij}'s are the monomials in the unknowns that are assumed to belong to $\mathbb{F}_q$, whereas the a_{ij}'s are known coefficients that belong to $\mathbb{F}_{q^m}$. We* *define the a_{ijk}'s as $a_{ij} = \sum_{k=0}^{m-1} a_{ijk}\alpha^k$, where the a_{ijk}'s belong to $\mathbb{F}_q$. From this we can define the system "unfolding" over $\mathbb{F}_q$ as*

$$\textbf{UnFold}\left(\mathcal{S}\right) := \left\{ \sum_j a_{ijk} m_{ij} = 0, 1 \le i \le N, 0 \le k \le m-1 \right\}.$$

The important point is that the solutions of $\mathcal{S}$ over $\mathbb{F}_q$ are exactly the solutions of $\textbf{UnFold}\left(\mathcal{S}\right)$ over $\mathbb{F}_q$, so that in that sense the two systems are equivalent.

By using the Cauchy-Binet formula, it is proved [11, Prop. 1] that the maximal minors of $\boldsymbol{C}\boldsymbol{H}^{\intercal}$, which are polynomials of degree $\le r$ in the coefficient variables C_{ij}, can actually be expressed as *linear* combinations of the c_T's. In other words we obtain $m\binom{n-k-1}{r}$ linear equations over $\mathbb{F}_q$ by "unfolding" the $\binom{n-k-1}{r}$ maximal minors of $\boldsymbol{C}\boldsymbol{H}^{\intercal}$. We denote such a system by

$$\textbf{UnFold}\left(\textbf{MaxMinors}(\boldsymbol{C}\boldsymbol{H}^{\intercal})\right). \tag{8}$$

It is straightforward to check that some variables in $\boldsymbol{C}$ and $\boldsymbol{S}$ can be specialized. The choice which is made in [11] is to specialize $\boldsymbol{S}$ with its r first rows equal to the identity ($\boldsymbol{S}_{\{1..r\},*} = \boldsymbol{I}_r$), its first column to $\mathbf{1}^{\intercal} = (1, 0, \ldots, 0)^{\intercal}$ and $\boldsymbol{C}$ has its first column equal to $\mathbf{1}^{\intercal}$. It is proved in [11, Section 3.3] that if the first coordinate of $\boldsymbol{e}$ is nonzero and the top $r \times r$ block of $\boldsymbol{S}$ is invertible, then the solution of the previous specialized system is also a solution of the system without specialization. Moreover, this will always be the case up to a permutation of the coordinates of the codewords or a change of $\mathbb{F}_{q^m}$-basis.

It is proved in [11, Prop. 2] that a degree-r Gröbner basis of the unfolded polynomials **MaxMinors** can be obtained by solving the corresponding linear system in the c_T's.

However, this strategy of specialization does not reveal directly the entries of $\boldsymbol{C}$ (it only reveals the values of the c_T's). To finish the calculation it still remains to compute a Gröbner basis of the whole algebraic system as explained in [11, Step 5, §6.1]). There is a simple way to avoid this computation by specializing the variables of $\boldsymbol{C}$ in a different way. This is the new approach we will explain now.

3.3 The new approach to solve the decoding problem : specializing the identity in $\boldsymbol{C}$

As for the previous approach, we notice that if $(\boldsymbol{S}, \boldsymbol{C})$ is a solution of (7) then $(\boldsymbol{S}\boldsymbol{A}^{-1}, \boldsymbol{A}\boldsymbol{C})$ is also a solution of the same system for any invertible matrix $\boldsymbol{A}$ in $\mathbb{F}_q^{r \times r}$. Now, in the case where the first r columns of a solution $\boldsymbol{C}$ form a invertible matrix, we will still have a solution with the specialization

$$\boldsymbol{C} = \begin{pmatrix} \boldsymbol{I}_r & \boldsymbol{C}' \end{pmatrix}.$$

We can also specialize the first column of $\boldsymbol{S}$ to $\mathbf{1}^{\intercal} = \begin{pmatrix} 1 & 0 & \ldots & 0 \end{pmatrix}^{\intercal}$. If the first r columns of $\boldsymbol{C}$ are not independent, it suffices as in [11, Algorithm 1] to make several different attempts of choosing r columns. The point of this specialization is that

- the corresponding c_T's are equal to the entries C_{ij} of $\boldsymbol{C}$ up to an unessential factor $(-1)^{r+i}$ whenever $T = \{1..r\}\backslash\{i\} \cup \{j\}$ for any $i \in \{1..r\}$ and $j \in \{r+1..n\}$. This follows on the spot by writing the cofactor expansion of the minor $c_T = |\boldsymbol{C}|_{*,\{1..r\}\backslash\{i\}\cup\{j\}}$. Solving the linear system in the c_T's corresponding to (8) yields now directly the coefficient variables C_{ij}. This avoids the subsequent Gröbner basis computation, since once we have $\boldsymbol{C}$ we obtain $\boldsymbol{S}$ directly by solving (7) which has become a linear system.
- it is readily shown that any solution of (8) is actually a projection on the C_{ij} variables of a solution $(\boldsymbol{S}, \boldsymbol{C})$ of the whole system (see Proposition 3). This justifies the whole approach.

In other words we are interested here in the following modeling

Modeling 2 *We consider the system of linear equations, given by unfolding all maximal minors of* $\left(\boldsymbol{I}_r \; \boldsymbol{C}'\right) \boldsymbol{H}^\intercal$*:*

$$\left\{f = 0 \middle| f \in \mathbf{UnFold}\left(\mathbf{MaxMinors}\left(\left(\boldsymbol{I}_r \; \boldsymbol{C}'\right) \boldsymbol{H}^\intercal\right)\right)\right\}. \tag{9}$$

This system contains:

- $m\binom{n-k-1}{r}$ *linear equations with coefficients in* $\mathbb{F}_q$,
- $\binom{n}{r} - 1$ *unknowns: the* c_T*'s,* $T \subset \{1..n\}$ *with* $\#T = r$, $T \neq \{1..r\}$.

We search for the solutions c_T*'s in* $\mathbb{F}_q$.

Note that from the specialization, $c_{\{1..r\}} = 1$ is not an unknown.

For the reader's convenience, let us recall the specific form of these equations which is obtained by unfolding the following polynomials (see [11, Prop. 2] and its proof).

Proposition 2. *The system* $\mathbf{MaxMinors}(\boldsymbol{C}\boldsymbol{H}^\intercal)$ *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*

$$P_J = \sum_{\substack{T_1 \subset \{1..k+1\}, T_2 \subset J, \\ \#T_1 + \#T_2 = r \\ T = T_1 \cup (T_2 + k + 1)}} (-1)^{\sigma_J(T_2)} \left|\boldsymbol{R}\right|_{T_1, J\backslash T_2} c_T, \tag{10}$$

where the sum is over all subsets $T_1 \subset \{1..k+1\}$ *and* T_2 *subset of* J*, with* $\#T_1 + \#T_2 = r$*, and* $\sigma_J(T_2)$ *is an integer depending on* T_2 *and* J*. We denote by* $T_2 + k + 1$ *the set* $\{i + k + 1 : i \in T_2\}$.

Let us show now that the solutions of the linear system obtained this way are projections of the solutions of the original system. For this purpose, let us bring in

– The original system (7) over $\mathbb{F}_{q^m}$ obtained with the aforementioned specialization

$$\mathcal{F}_C = \left\{ \left(1\ \alpha \cdots \alpha^{m-1}\right) \left(\mathbf{1}^\intercal\ \boldsymbol{S}'\right) \left(\boldsymbol{I}_r\ \boldsymbol{C}'\right) \boldsymbol{H}^\intercal = \mathbf{0}_{n-k-1} \right\}, \tag{11}$$

where $\mathbf{1}^\intercal = \left(1\ 0 \dots 0\right)^\intercal$, $\boldsymbol{S} = \left(\mathbf{1}^\intercal\ \boldsymbol{S}'\right)$ and $\boldsymbol{C} = \left(\boldsymbol{I}_r\ \boldsymbol{C}'\right)$.

– The system in the coefficient variables we are interested in

$$\mathcal{F}_M = \left\{ f = 0 \middle| f \in \mathbf{MaxMinors}\left(\left(\boldsymbol{I}_r\ \boldsymbol{C}'\right) \boldsymbol{H}^\intercal\right) \right\}, \tag{12}$$

– Let $V_{\mathbb{F}_q}(\mathcal{F}_C)$ be the set of solutions of (11) with all variables in $\mathbb{F}_q$, that is

$$V_{\mathbb{F}_q}(\mathcal{F}_C) = \left\{ (\boldsymbol{S}^*, \boldsymbol{C}^*) \in {\mathbb{F}_q}^{m(r-1)+r(n-r)} : \left(1\ \alpha \cdots \alpha^{m-1}\right) \left(\mathbf{1}^\intercal\ \boldsymbol{S}^*\right) \left(\boldsymbol{I}_r\ \boldsymbol{C}^*\right) \boldsymbol{H}^\intercal = \mathbf{0} \right\}. \tag{13}$$

– Let $V_{\mathbb{F}_q}(\mathcal{F}_M)$ be the set of solutions of (12) with all variables in $\mathbb{F}_q$, i.e.

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

With these notations at hand, we will now show that solving the decoding problem is left to solve the **MaxMinors** system, that depends only on the $\boldsymbol{C}$ variables.

Proposition 3. *If* $\boldsymbol{e}$ *can be uniquely decoded and has rank* r*, then*

$$V_{\mathbb{F}_q}(\mathcal{F}_M) = \left\{ \boldsymbol{C}^* \in \mathbb{F}_q^{r(n-r)} : \exists \boldsymbol{S}^* \in \mathbb{F}_q^{m(r-1)} \text{ s.t. } (\boldsymbol{S}^*, \boldsymbol{C}^*) \in V_{\mathbb{F}_q}(\mathcal{F}_C) \right\}. \tag{14}$$

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

$$\left(1\ S_2^* \dots S_r^*\right) = \left(1\ \alpha \cdots \alpha^{m-1}\right) \left(\mathbf{1}^\intercal\ \boldsymbol{S}^*\right)$$

belongs to the left kernel of the matrix $\left(\boldsymbol{I}_r\ \boldsymbol{C}^*\right) \boldsymbol{H}^\intercal$. 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 $\left(\boldsymbol{I}_r\ \boldsymbol{C}^*\right) \boldsymbol{H}^\intercal$ 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 $(0, S_2^*, \dots, S_r^*) \left(\boldsymbol{I}_r\ \boldsymbol{C}^*\right)$ is an error of weight less than r solution of the decoding problem, and we assumed there is only one error of weight exactly r solution of the decoding problem. Then, $(S_1^{*-1}(S_2^*, \dots, S_r^*), \boldsymbol{C}^*) \in V_{\mathbb{F}_q}(\mathcal{F}_C)$. □

4 Solving the rank decoding problem: overdetermined case

In this section, we show that, when the number of equations is sufficiently large, we can solve the system given in modeling 2 with only linear algebra computations, by linearization on the c_T's.

4.1 The overdetermined case

The linear system given in Modeling 2 is described by the following matrix **MaxMin** with rows indexed by $(J, i) : J \subset \{1..n-k-1\}, \#J = r, 0 \le i \le m-1$ and columns indexed by $T \subset \{1..n\}$ of size r, with the entry in row (J, i) and column T being the coefficient in α^i of the element $\pm |\boldsymbol{R}|_{T_1, J \setminus T_2} \in \mathbb{F}_{q^m}$. More precisely, we have

$$\mathbf{MaxMin}[(J,i),T] = \begin{cases} 0 & \text{if } T_2 \not\subset J \\ [\alpha^i](-1)^{\sigma_J(T_2)}(|\boldsymbol{R}|_{T_1,J\setminus T_2}) & \text{if } T_2 \subset J, \end{cases} \tag{15}$$
$$\text{with} \quad T_1 = T \cap \{1..k+1\},$$
$$\text{and} \quad T_2 = (T \cap \{k+2..n\}) - (k+1).$$

The matrix **MaxMin** can have rank $\binom{n}{r} - 1$ at most; indeed if it had a maximal rank of $\binom{n}{r}$, this would imply that all c_T's are equal to 0, which is in contradiction with the assumption $c_{\{1..r\}} = 1$.

Proposition 4. *If* **MaxMin** *has rank* $\binom{n}{r} - 1$ *(which implies that* $m\binom{n-k-1}{r} \ge \binom{n}{r} - 1$*), 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* $c_{\{1..r\}}$. *The components* $\boldsymbol{c}$ *of this vector contain the values of the* c_T*'s,* $T \neq \{1..r\}$. *This gives in particular the values of all the variables* $C_{i,j} = (-1)^{r+i} c_{\{1..r\}\setminus\{i\}\cup\{j\}}$.

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

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

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. (12) has no solution. Then $\begin{pmatrix}\boldsymbol{c} & 1\end{pmatrix}$ is in the right kernel of **MaxMin**. $\square$

It is then easy to recover the variables $\boldsymbol{S}$ from (11) by linear algebra. The following algorithm recovers the error if there is one solution to the system (11). It is shown in [11, Algorithm 1] how to deal with the other cases, and this can be easily adapted to the specialization considered in this paper.

Proposition 5. *When* $m\binom{n-k-1}{r} \ge \binom{n}{r} - 1$ *and* **MaxMin** *has rank* $\binom{n}{r} - 1$, *then Algorithm 1 recovers the error in complexity*

$$\mathcal{O}\left(m\binom{n-k-1}{r}\binom{n}{r}^{\omega-1}\right) \tag{16}$$

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

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 rank $\binom{n}{r} - 1$
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. (12) ;
Let $\begin{pmatrix}\boldsymbol{c} & 1\end{pmatrix}$ be the only such vector in the right kernel of **MaxMin** ;
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

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

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.

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. (16). $\square$

We ran a lot of experiments with random codes $\mathcal{C}$ such that $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$, and the matrix **MaxMin** was always of rank $\binom{n}{r} - 1$. 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 $r = 5$. 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. Note that the experimental values are the complexity of the whole attack, including the build of the the matrix that require to compute the minors of $\boldsymbol{R}$. Hence for small values of n, it may happen that this part of the attack takes more time than the solving of the linear system. This explains why, for $r = 3$ and $n < 28$, the experimental curve is above the theoretical one.

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 parameters in the cryptosystem ROLLO-I. When the parameters (m, n, k, r) do not satisfy the condition $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$, we do not give 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

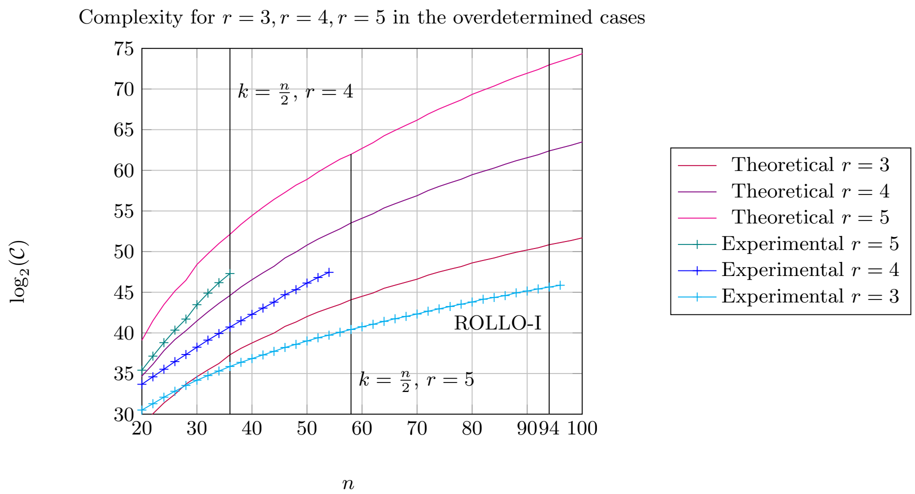

Fig. 1. Theoretical vs Experimental value of the complexity of the computation. The computations are done using `magma v2.22-2` on a machine with a Intel® Xeon® 2.00GHz processor (*Any mention of commercial products is for information only and does not imply endorsement by NIST*). We measure the experimental complexity in terms of clock cycles of the CPU, given by the `magma` function `ClockCycles()`. The theoretical value is the binary logarithm of $m\binom{n-k-1}{r}\binom{n}{r}^{2.81-1}$. The experimental values are the binary logaithms of the aforementionned experimental complexity 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).

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.

There are two classical improvements that can be used to lower the complexity of solving an algebraic system. The first one consists in selecting a subset of all equations, when some of them are redundant, see Section 4.2. The second one is the hybrid attack that will be explained in Section 4.3.

4.2 Improvement in the "super"-overdetermined case by puncturing

We consider the case 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 (i.e. the ones that are likely to be linearly independent), we can take the system **MaxMinors** obtained by considering code $\widetilde{C}$ punctured on the p last coordinates, instead of the entire code. Puncturing code $\widetilde{C}$ is equivalent to shortening the dual code, i.e. considering the system

$$\mathbf{MaxMinors}\left(\boldsymbol{C}_{*,\{1..n-p\}}(\boldsymbol{H}^\intercal)_{\{1..n-p\},\{1..n-k-1-p\}}\right). \tag{17}$$

Theoretical complexity for $r = 5, 6, 7$ in the *overdetermined* cases when $n = 2k$.

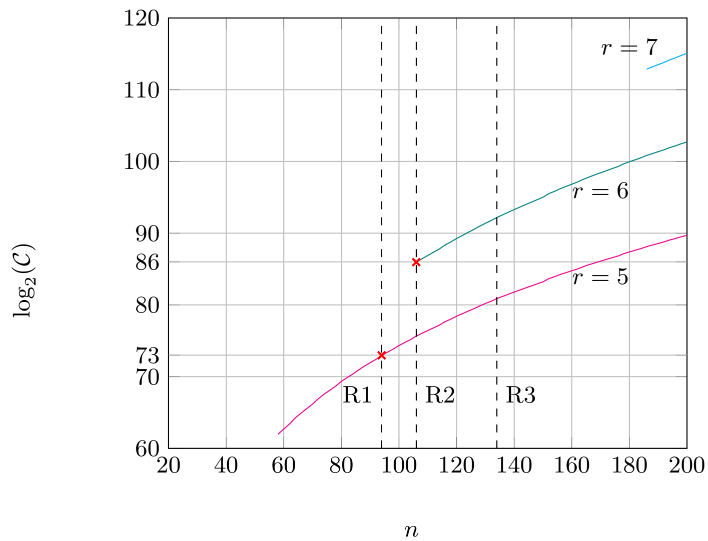

Fig. 2. Theoretical value of the complexity of the computation in the overdetermined cases, which is the binary logarithm of $m\binom{n-k-1}{r}\binom{n}{r}^{2.81-1}$. m is the largest prime less than $n/1.18$, $n = 2k$. The axis "R1, R2, R3" correspond to the values of n for the cryptosystems ROLLO-I-128;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

as we take $\boldsymbol{H}$ 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 $\boldsymbol{C}_{*,T}$ with $T \subset \{1..n-p-k-1\}$. 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

$$\mathcal{O}\left(m\binom{n-p-k-1}{r}\binom{n-p}{r}^{\omega-1}\right) \tag{18}$$

operations in the field $\mathbb{F}_q$.

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 specializing some variables of the system to reduce an underdetermined case to an overdetermined one.

For instance, if we specialize 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

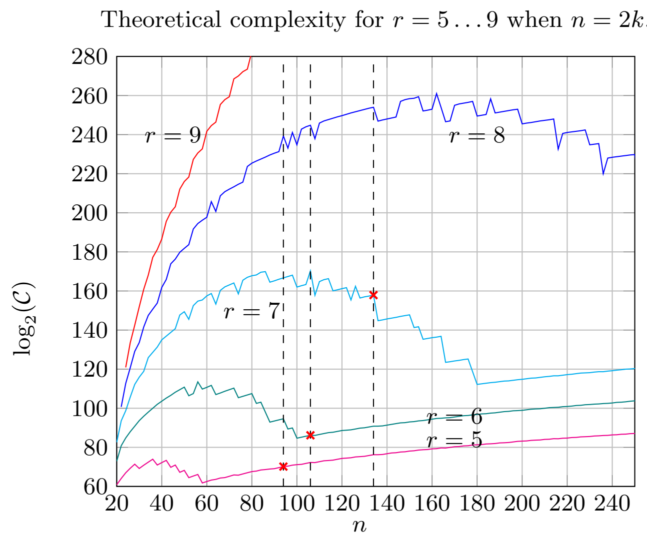

Fig. 3. Theoretical value of the complexity of RD in the overdetermined case (using punctured codes or specialization). $\mathcal{C}$ is the smallest value between (19) and (18). m is the largest prime less than $n/1.18$, $n = 2k$. The dashed axes correspond to the values of n for the cryptosystems ROLLO-I-128; ROLLO-I-192 and ROLLO-I-256.

cost is

$$\mathcal{O}\left(q^{ar} m \binom{n-k-1}{r} \binom{n-a}{r}^{\omega-1}\right) \tag{19}$$

operations in the field $\mathbb{F}_q$. In order to minimize the previous complexity (19), one chooses a to be the smallest integer such that the condition $m\binom{n-k-1}{r} \geq \binom{n-a}{r} - 1$ is fulfilled. Figure 3 page 17 gives the best theoretical complexities obtained for $r = 5 \ldots 9$ with the best values of a and p, for $n = 2k$. Table 1 page 26 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 analyzes the support minors modeling approach (Modeling 1).

5.1 Solving (3) by direct linearization

The number of monomials that can appear in Modeling 1 is $K\binom{n}{r}$ whereas the number of equations is $m\binom{n}{r+1}$. When the solution space of (3) is of dimension

1, we expect to solve it by direct linearization whenever:

$$m\binom{n}{r+1} \geq K\binom{n}{r} - 1. \tag{20}$$

We did a lot of experiments as explained in Section 5.6, and they suggest that it is the case.

Remark 2. Note that, in what follows, the Eq. (20) will sometimes be referred as the "$b = 1$ case".

5.2 Solving Support Minors Modeling at a higher degree

In the case where Eq. (20) 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_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 $b = 2$.

This comes from determinantal identities involving maximal minors of matrices whose first rows are some of the $\boldsymbol{r_j}$'s concatenated with $\boldsymbol{C}$. For instance we may write the trivial identity for any subset J of columns of size $r+2$:

$$\begin{vmatrix} \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{C} \end{vmatrix}_{*,J} + \begin{vmatrix} \boldsymbol{r_k} \\ \boldsymbol{r_j} \\ \boldsymbol{C} \end{vmatrix}_{*,J} = 0.$$

Notice that this gives trivially a relation between certain equations corresponding to $b = 2$ since a cofactor expansion along the first row of $\begin{vmatrix} \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{C} \end{vmatrix}_{*,J}$ shows that this maximal minor is indeed a linear combination of terms which is the multiplication of a linear variable x_i with a maximal minor of the matrix $\begin{pmatrix} \boldsymbol{r_k} \\ \boldsymbol{C} \end{pmatrix}$ (in other words an equation corresponding to $b = 2$). A similar result holds for $\begin{vmatrix} \boldsymbol{r_k} \\ \boldsymbol{r_j} \\ \boldsymbol{C} \end{vmatrix}_{*,J}$ where a cofactor expansion along the first row yields terms formed by a linear variable x_i multiplied by a maximal minor of the matrix $\begin{pmatrix} \boldsymbol{r_j} \\ \boldsymbol{C} \end{pmatrix}$. This result can be generalized by considering symmetric tensors $(S_{j_1,\cdots,j_r})_{\substack{1\leq j_1\leq m \\ \cdots \\ 1\leq j_r\leq m}}$ of dimension m of rank $b \geq 2$ over $\mathbb{F}_q$. Recall that these are tensors that satisfy

$$S_{j_1,\cdots,j_b} = S_{j_{\sigma(1)},\cdots,j_{\sigma(b)}}$$

for any permutation σ acting on $\{1..b\}$. This is a vector space that is clearly isomorphic to the space of homogeneous polynomials of degree b in $y_1, \cdots, y_m$ over $\mathbb{F}_q$. The dimension of this space is therefore $\binom{m+b-1}{b}$. We namely have

Proposition 6. *For any symmetric tensor* $(S_{j_1,\cdots,j_b})_{\substack{1\leq j_1\leq m\\ \cdots \\ 1\leq j_b\leq m}}$ *of dimension* m *of rank* $b \geq 2$ *over* $\mathbb{F}_q$ *we have*

$$\sum_{j_1=1}^{m}\cdots\sum_{j_b=1}^{m} S_{j_1,\cdots,j_b} \left| \begin{matrix} \boldsymbol{r_{j_1}} \\ \cdots \\ \boldsymbol{r_{j_b}} \\ \boldsymbol{C} \end{matrix} \right|_{*,J} = 0$$

where J *is any subset of* $\{1..n\}$ *of size* $r+b$.

Proof. Notice first that the maximal minor $\left| \begin{smallmatrix} \boldsymbol{r_{j_1}} \\ \cdots \\ \boldsymbol{r_{j_b}} \\ \boldsymbol{C} \end{smallmatrix} \right|_{*,J}$ is equal to 0 whenever at least two of the j_i's are equal. The left-hand sum reduces therefore to a sum of terms of the form $\sum_{\sigma\in S_b} S_{\sigma(j_1),\cdots,\sigma(j_b)} \left| \begin{smallmatrix} \boldsymbol{r_{\sigma(j_1)}} \\ \cdots \\ \boldsymbol{r_{\sigma(j_b)}} \\ \boldsymbol{C} \end{smallmatrix} \right|_{*,J}$ where all the j_i's are different. Notice now that from the fact that S is a symmetric tensor we have

$$\begin{aligned}\sum_{\sigma\in S_b} S_{\sigma(j_1),\cdots,\sigma(j_b)} \left| \begin{matrix} \boldsymbol{r_{\sigma(j_1)}} \\ \cdots \\ \boldsymbol{r_{\sigma(j_b)}} \\ \boldsymbol{C} \end{matrix} \right|_{*,J} &= S_{j_1,\cdots,j_b} \sum_{\sigma\in S_b} \left| \begin{matrix} \boldsymbol{r_{\sigma(j_1)}} \\ \cdots \\ \boldsymbol{r_{\sigma(j_b)}} \\ \boldsymbol{C} \end{matrix} \right|_{*,J} \\ &= 0\end{aligned}$$

because the determinant is an alternating form and there as many odd and even permutations in the symmetric group of order b when $b \geq 2$. $\square$

This proposition can be used to understand the dimension D of the space of linear equations we obtain after linearizing the equations we obtain for a certain b. For instance for $b = 2$ we obtain $m\binom{n}{r+1}K$ linear equations (they are obtained by linearizing the equations resulting from multiplying all the equations of the support minors modeling by one of the K linear variables). However as shown by Proposition 6 all of these equations are not independent and we have $\binom{n}{r+2}\binom{m+1}{2}$ linear relations coming from all relations of the kind

$$\sum_{j=1}^{m}\sum_{k=1}^{m} S_{j,k} \left| \begin{matrix} \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{C} \end{matrix} \right|_{*,J} = 0. \tag{21}$$

In our experiments, these relations turnt out to be independent yielding that the dimension D of this space should not be greater than $m\binom{n}{r+1}K - \binom{n}{r+2}\binom{m+1}{2}$. Experimentally, we observed that we indeed had

$$\mathrm{D}_{\mathrm{exp}} = m\binom{n}{r+1}K - \binom{n}{r+2}\binom{m+1}{2}.$$

For larger values of b things get more complicated but again Proposition 6 plays a key role here. Consider for example the case $b = 3$. We have in this case

$m\binom{n}{r+1}\binom{K+1}{2}$ equations obtained by multiplying all the equations of the support minors modeling by monomials of degree 2 in the linear variables. Again these equations are not all independent, there are $\binom{m+1}{2}\binom{n}{r+2}K$ equations obtained by mutiplying all the linear relations between the $b = 2$ equations derived from (21) by a linear variable, they are of the form

$$x_i \sum_{j=1}^{m}\sum_{k=1}^{m} S_{j,k} \left| \begin{smallmatrix} \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{C} \end{smallmatrix} \right|_{*,J} = 0. \tag{22}$$

But all these linear relations are themselves not independent as can be checked by using Proposition 6 with $b = 3$, we namely have for any symmetric tensor S_{jkl} of rank 3:

$$\sum_{j=1}^{m}\sum_{k=1}^{m} S_{i,j,k} \left| \begin{smallmatrix} \boldsymbol{r_i} \\ \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{C} \end{smallmatrix} \right|_{*,J} = 0. \tag{23}$$

This induces linear relations among the equations (22), as can be verified by a cofactor expansion along the first row of the left-hand term of (23) which yields an equation of the form

$$\sum_{i=1}^{m} x_i \sum_{j=1}^{m}\sum_{k=1}^{m} S^i_{j,k} \left| \begin{smallmatrix} \boldsymbol{r_j} \\ \boldsymbol{r_k} \\ \boldsymbol{C} \end{smallmatrix} \right|_{*,J} = 0$$

where the $\boldsymbol{S}^i = (S^i_{j,k})_{\substack{1\le j\le m \\ 1\le k\le m}}$ are symmetric tensors of order 2. We would then expect that the dimension of the set of linear equations obtained from (22) is only $\binom{m+1}{2}\binom{n}{r+2}K - \binom{n}{r+3}\binom{m+2}{3}$ yielding an overall dimension D of the linearized system of order

$$\mathrm{D} = m\binom{n}{r+1}\binom{K+1}{2} - \binom{m+1}{2}\binom{n}{r+2}K + \binom{n}{r+3}\binom{m+2}{3},$$

which is precisely what we observe experimentally. 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:

Heuristic 2

$$\mathrm{D}_{\mathrm{exp}} = \sum_{i=1}^{b} (-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K+b-i-1}{b-i}. \tag{24}$$

Experimentally, we found this to be the case with overwhelming probability (see Section 5.6) with the only general exceptions being:

1. When $\mathrm{D}_{\mathrm{exp}}$ 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 $\mathrm{D}_{\mathrm{exp}}$ 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.
3. When $b \geq r + 2$, the equations are not any more linearly independent, and we give an explanation in Section 5.4.

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

$$\binom{n}{r}\binom{K+b-1}{b} - 1 \leq \sum_{i=1}^{b}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K+b-i-1}{b-i} \quad (25)$$

Note that, for $b = 1$, we recover the result (20). As this system is very sparse, with $K(r+1)$ monomials per equation, one can solve it using Wiedemann algorithm [39]; thus the complexity to solve MinRank problem is

$$\mathcal{O}\left(K(r+1)\left(\binom{n}{r}\binom{K+b-1}{b}\right)^2\right) \quad (26)$$

where b is the smallest positive integer so that the condition (25) is fulfilled.

5.3 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

$$\mathrm{D}_{\mathrm{exp}} = \sum_{j=1}^{b}\sum_{i=1}^{j}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}. \quad (27)$$

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

$$\sum_{j=1}^{b}\binom{n}{r}\binom{K}{j} - 1 \leq \sum_{j=1}^{b}\sum_{i=1}^{j}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}. \quad (28)$$

Similarly to the general case for any q described in the previous section, the complexity to solve MinRank problem when $q = 2$ is

$$\mathcal{O}\left(K(r+1)\left(\sum_{j=1}^{b}\binom{n}{r}\binom{K}{j}\right)^{2}\right) \tag{29}$$

where b is the smallest positive integer so that the condition (28) is fulfilled.

5.4 Toward the $b \geq r+2$ case

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_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_T, the m equations involving only $r+1$ of the variables c_T will form a submatrix with m rows and only $r+1$ nonzero columns. Using a Cramer-like formula, we can therefore construct left kernel vectors for these equations; its coefficients would be 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. (24) 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.

5.5 Improvements for Generic Minrank

The two classical improvements Section 4.2 in the "super"-overdetermined cases the hybrid attack and Section 4.3 can also apply for Generic Minrank.

We can consider applying the Support Minors Modeling techniques to submatrices $\sum_{i=1}^{K} \boldsymbol{M}'_i x_i$ of $\sum_{i=1}^{K} \boldsymbol{M}_i x_i$. Note that if $\sum_{i=1}^{K} \boldsymbol{M}_i x_i$ has rank less than or equal to r, so does $\sum_{i=1}^{K} \boldsymbol{M}'_i x_i$, so assuming we have a unique solution x_i to both systems of equations, it will be the same. Generically, we will keep a unique solution in the smaller system as long as the decoding problem has a unique solution, i.e. as long as the Johnson bound $K \leq (m-r)(n-r)$ is satisfied.

We generally find that the most beneficial settings use matrices with all m rows, but only $n' \leq n$ of the columns. This corresponds to a puncturing of the corresponding $\mathbb{F}_q$ matrix code. 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.

On the other side, we can run exhaustive search on a variables x_i in $\mathbb{F}_q$ and solve q^a systems with a smaller value of b, so that the resulting complexity is smaller than solving directly the system with a higher value of b. This optimization is considered in the attack against ROLLO-I-256 (see Table 1); more detail about this example are given in Section 6.1.

5.6 Experimental results for Generic Minrank

We verified experimentally that the value of $\mathrm{D}_{\mathrm{exp}}$ 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 most of the cases, the number of linearly independent polynomials was as expected. For $q = 13$, we had a few number of non-generic systems (usually less than 1% over 1000 random sampling), and only in square cases where the matrices have a predicted rank equal to the number of columns. For $q = 2$ we had a higher probability of linear dependences, due to the fact that over a such small field, random matrices have a non-trivial probability to be non invertible. Anyway, as soon as the field is big enough or the number $\mathrm{D}_{\mathrm{exp}}$ is large compared to the number of columns, 100% of our experiments succeeded over 1000 samples.

5.7 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_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 mentioned above and the experiments mentioned in Section 5.6, we can make a similar heuristic as Heuristic 1, this suggests that linearization is possible for $q > b$, $0 < b < r + 2$ whenever:

$$\binom{n}{r}\binom{mk+b}{b} - 1 \leq \\ m\binom{n-k-1}{r}\binom{mk+b}{b} + \sum_{i=1}^{b}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{mk+b-i}{b-i}, \tag{30}$$

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

$$A_b - 1 \leq B_c + C_b \tag{31}$$

where

$$A_b := \sum_{j=1}^{b} \binom{n}{r}\binom{mk+1}{j}$$

$$B_b := \sum_{j=1}^{b} \left(m\binom{n-k-1}{r}\binom{mk+1}{j} \right)$$

$$C_b := \sum_{j=1}^{b}\sum_{i=1}^{j} \left((-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{mk+1}{j-i} \right).$$

For the latter, it leads to a complexity of

$$\mathcal{O}\left((B_b + C_b)A_b^{\omega-1}\right) \tag{32}$$

where b is the smallest positive integer so that the condition (31) 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 [39]. More precisely, for values of m, n, r and k of ROLLO or RQC parameters (see Table 4 and Table 5) for which the condition (31) is fulfilled, 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

$$\mathcal{O}\left(\frac{B_b\binom{k+r+1}{r} + C_b(mk+1)(r+1)}{B_b + C_b} A_b^2\right) \tag{33}$$

where b is still the smallest positive integer so that the condition (31) is fulfilled. A similar formula applies for the case $q > b$.

5.8 Last step of the attack

To end the attack on MinRank using Support Minors modeling or the attack on Rank Decoding using MaxMinors modeling in conjunction with Support Minors modeling, one needs to find the affectations for each unknowns. Indeed, unlike the case where one uses only MaxMinors modeling with the specialization in $\boldsymbol{C}$ (see Section 4), the direct linearization does not lead to affectations of the form $c_{i,j} = \mu_{i,j}$ where $\mu_{i,j}$ are elements in $\mathbb{F}_q$. In fact, with the Support Minors modeling one gets affectations of the form

$$x^\alpha c_{i,j} = \mu \in \mathbb{F}_q$$

where the x^α's are monomials of degree $b-1$ in the x_i's variables.

In order to extract the values of all the x_i's and thus finish the attack, one needs to specialize $x_1 = 1$, this is possible as long as $x_1 \neq 0$ since the solution space has dimension 1; if this specialization does not lead to a unique solution, one tries with x_2 and so on. Then, one computes quotients of the form

$$\frac{x_1}{x_l} = \frac{x_1 x^\alpha c_{i_0,j_0}}{x_l x^\alpha c_{i_0,j_0}}, \quad \deg(x^\alpha) = b-2 \tag{34}$$

for all the values of l in $\{2..K\}$ with a fixed minor c_{i_0,j_0}. Doing so, one gets the values of all the x_i's and thus finish the attack. This works as long as the minor c_{i_0,j_0} of $\boldsymbol{C}$ chosen is non-zero, if it is, one uses another one, and so on; our experiments always worked with one or two minors.

6 Complexity of the attacks for different cryptosystems and comparison with generic Gröbner basis approaches

6.1 Attacks against the Rank Decoding problem

Table 1 presents the best complexity of our attacks (see sections 4 and 5) against RD and gives the binary logarithm of 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). The third column gives the original rate for being overdeterminate. The column ‘a’ indicates the number of specialized columns in the hybrid approach (Section 4.3), when the system is not overdetermined. Column ‘p’ indicates the number of punctured columns in the “super”-overdetermined cases (Section 4.2). Column ‘b’ indicates that we use Support Minors Modeling in conjunction with MaxMin (Section 5.7).

Let us give more detail on the way to compute the best complexity for ROLLO-I-256 in Table 1. Recall that its parameters are $(m, n, k, r) = (113, 134, 67, 7)$. The attack from Section 4 only works with the hybrid approach, thus requiring $a = 8$ and resulting in a complexity of 158 bits (using (19) and $\omega = 2.81$). On the other hand, the attack from Section 5.7 needs $b = 2$ which results in a complexity of 154 (this time using Wiedemann's algorithm). However, if we specialize $a = 3$ columns in $\boldsymbol{C}$, we get $b = 1$ and the resulting complexity using Wiedemann's algorithm is 151.

Table 1. Complexity of the attack against Rank Decoding for different cryptosystems. The values in the column **This paper** are the smallest ones between Strassen's and Wiedemann's algorithm, the "*" indicates that it is Wiedemann.

	(m, n, k, r)	$\frac{m\binom{n-k-1}{r}}{\binom{n}{r}-1}$	a	p	b	**This paper**	[11]
Loidreau ([30])	$(128, 120, 80, 4)$	1.28	0	43	0	**65**	98
ROLLO-I-128	$(79, 94, 47, 5)$	1.97	0	9	0	**71**	117
ROLLO-I-192	$(89, 106, 53, 6)$	1.06	0	0	0	**87**	144
ROLLO-I-256	$(113, 134, 67, 7)$	0.67	3	0	1	**151***	197
ROLLO-II-128	$(83, 298, 149, 5)$	2.42	0	40	0	**93**	134
ROLLO-II-192	$(107, 302, 151, 6)$	1.53	0	18	0	**111**	164
ROLLO-II-256	$(127, 314, 157, 7)$	0.89	0	6	1	**159***	217
ROLLO-III-128	$(101, 94, 47, 5)$	2.52	0	12	0	**70**	119
ROLLO-III-192	$(107, 118, 59, 6)$	1.31	0	4	0	**88**	148
ROLLO-III-256	$(131, 134, 67, 7)$	0.78	0	0	1	**131***	200
RQC-I	$(97, 134, 67, 5)$	2.60	0	18	0	**77**	123
RQC-II	$(107, 202, 101, 6)$	1.46	0	10	0	**101**	156
RQC-III	$(137, 262, 131, 7)$	0.93	3	0	0	**144**	214

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 [18] 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.

6.3 Comparison between our approach and the use of generic Gröbner basis algorithms

Since our approach is an algebraic attack, it relies on solving a polynomial system, thus it does look like a Gröbner basis computation. In fact, we do compute a Gröbner basis of the system, as we compute the unique solution of the system, which represents its Gröbner basis.

Nevertheless, our algorithm is not a generic Gröbner basis algorithm as it only works for the special type of system studied in this paper: the RD and MinRank systems. As it is specifically designed for this purpose and for the reasons detailed below, it is more efficient than a generic algorithm.

There are three main reasons why our approach is more efficient than a generic Gröbner basis algorithm:

- We compute formally (that is to say at no extra cost except the size of the equations) new equations of degree r (the **MaxMinors** ones) that are

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	**154**	522
GeMSS192$(513, 256, 22, 20)$	265	243	52	94	2	**223**	537
GeMSS256$(513, 354, 30, 33)$	354	324	73	126	3	**299**	1254
RedGeMSS128$(17, 177, 15, 15)$	177	162	35	62	2	**156**	538
RedGeMSS192$(17, 266, 23, 25)$	266	243	53	95	2	**224**	870
RedGeMSS256$(17, 358, 34, 35)$	358	324	74	127	3	**301**	1273
BlueGeMSS128$(129, 175, 13, 14)$	175	162	35	63	2	**158**	537
BlueGeMSS192$(129, 265, 22, 23)$	265	243	53	95	2	**224**	870
BlueGeMSS256$(129, 358, 34, 32)$	358	324	74	127	3	**301**	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 [18]. 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	82	3	155	161	145/RBS
IIIc$(GF(256), 68, 36, 36)$	140	37	104	125	5	**208**	585	215/DA
Vc$(GF(256), 92, 48, 48)$	188	49	140	169	5	**272**	778	275/DA

already in the ideal, but not in the vector space

$\mathcal{F}_r := \langle uf : u$ monomial of degree $r-2$, f in the set of initial polynomials$\rangle$.

In fact, a careful analysis of a Gröbner basis computation with a normal strategy shows that those equations are in $\mathcal{F}_{r+1}$, and that the first degree fall for those systems is $r+1$. Here, we apply linear algebra directly on a small number of polynomials of degree r (see the two following items for more details), whereas a generic Gröbner basis algorithm would compute a lot of polynomials of degree $r+1$ and then reduce them in order to get those polynomials of degree r.

- A classical Gröbner basis algorithm using linear algebra and a normal strategy will construct matrices like the Macaulay ones, where the rows correspond to polynomials in the ideal and the columns to monomials of a certain degree. Here, we introduce variables c_T that represent maximal minors of $\boldsymbol{C}$, and thus represent not one monomial of degree r, but $r!$ monomials of degree r. As we compute the Gröbner basis by using only polynomials that can be expressed in terms of those variables (see the last item below), this reduces the number of columns of our matrices by a factor around $r!$ compared to generic Macaulay-like matrices.
- The solution can be found by applying linear algebra only to some specific equations, namely the MaxMinors ones in the overdetermined case, and in the underdetermined case, equations that have degree 1 in the c_T variables, and degree $b-1$ in the x_i variables (see Section 5.2). This enables us to deal with polynomials involving only the c_T variables and the x_i variables, whereas a generic Gröbner basis algorithm would consider all monomials up to degree $r+b$ in the x_l and the $c_{i,j}$ variables. This drastically reduces the number of rows and columns in our matrices.

For all of those reasons, in the overdetermined case, only an elimination on our selected MaxMinors equations (with a "compacted" matrix with respect to the columns) is sufficient to get the solution; so we essentially avoid going up to the degree $r+1$ to produce those equations, we select a small number of rows, and gain a factor $r!$ on the number of columns.

In the underdetermined case, we find linear equations by linearization on some well-chosen subspaces of the vector space $\mathcal{F}_{r+b}$. We have theoretical reasons to believe that our choice of subspace should lead to the computation of the solution (as usual, this is a "genericity" hypothesis), and it is confirmed by all our experiments.

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. With these new parameters, ROLLO and RQC would be resistant to our attacks, while still remaining attractive, for example with a loss of only about 50 % in terms of key size for ROLLO-I.

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.

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

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

Remark 3. In this section, the notation is chosen to match the one in ROLLO and RQC submissions' specifications ([7] and [1]). One should be careful that here, n is the block-length and not the length of the code which can be either $2n$ or $3n$.

In what follows, we consider $\omega = 2.81$ and we use the following notation, for ROLLO (Table 4):

- **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 mentioned above,
- **DFR** is the binary logarithm of the Decoding Failure Rate,

and for RQC (Table 5):

- **hyb2n(a)**: hybrid attack for length $2n$, the value of a is the smallest to reach the overdetermined case, $a = 0$ means that parameters are already in the overdetermined case,
- **hyb3n(a)**: non-homogeneous hybrid attack for length $3n$, a is the same as above. This attack corresponds to an adaptation of our attack to a non-homogeneous error of the RQC scheme, more details are given in [1],
- **und2n**: underdetermined attack for length $2n$,
- **comb3n**: combinatorial attack for length $3n$.

For more details about those parameters and the aforementioned attacks, reader may refer to the submissions specifications of ROLLO (see [7]) and RQC (see [1]).

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	213
new2ROLLO-I-192	2	97	89	8	8	1057	-33	258*	17	0	197*	3	283*
new2ROLLO-I-256	2	113	103	9	9	1454	-33	408*	30	0	283*	6	376*

Table 4. New parameters and attacks complexities for ROLLO-I.

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	205
newRQC-II	2	149	151	5	8	8	8	2812	331(24)	262(0)	224	3	289
newRQC-III	2	179	181	3	9	9	7	4049	553(44)	321(5)	324	6	401

Table 5. New parameters and attacks complexities 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 generic Gröbner basis algorithms 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 overdeterminate case defined in [11]).

We generalize this approach to the case of the MinRank problem for which we obtain the best known complexity with algebraic attacks. We also proposed a new approach for the underdeterminate case as described in [11], for some parameters this attack supersedes the results of [11], in particular for attacking ROLLO-I-256 parameters.

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., Bros, M., Couvreur, A., Deneuville, J.C., Gaborit, P., Hauteville, A., Zémor, G.: Rank quasi cyclic (RQC). Second round submission to the NIST post-quantum cryptography call (Apr 2020), https://pqc-rqc.org

2. 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
3. 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
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., Bardet, M., Otmani, A.: ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER). Second round submission to the NIST post-quantum cryptography call (Apr 2020), 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., Macario-Rat, 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. Courtois, N.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology - ASIACRYPT 2001. LNCS, vol. 2248, pp. 402–421. Springer, Gold Coast, Australia (2001)
16. 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)
17. Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D., Yang, B.Y.: Gui. First round submission to the NIST post-quantum cryptography call (Nov 2017), https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions/Rainbow-Round2.zip
18. Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D., Yang, B.Y.: 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
19. 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)
20. 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
21. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)
22. 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)
23. 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
24. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Information Theory **62**(2), 1006–1019 (2016)
25. 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)
26. 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
27. 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)
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. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding. LNCS, vol. 1070, pp. 33–48. Springer (1996). https://doi.org/10.1007/3-540-68339-9_4, https://doi.org/10.1007/3-540-68339-9_4
36. Petzoldt, A., Chen, M., Yang, B., Tao, C., Ding, J.: Design principles for HFEv-based multivariate signature schemes. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I. LNCS, vol. 9452, pp. 311–334. Springer (2015). https://doi.org/10.1007/978-3-662-48797-6_14, https://doi.org/10.1007/978-3-662-48797-6_14
37. Porras, J., Baena, J., Ding, J.: ZHFE, a new multivariate public key encryption scheme. In: Mosca, M. (ed.) Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings. LNCS, vol. 8772, pp. 229–245. Springer (2014). https://doi.org/10.1007/978-3-319-11659-4_14, https://doi.org/10.1007/978-3-319-11659-4_14
38. 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
39. Wiedemann, D.: Solving sparse linear equations over finite fields. IEEE transactions on information theory **32**(1), 54–62 (1986)