Bumpy RYDE: A New Hybrid Technique for Generic Rank-Metric Decoders

Hugo Beeloo-Sauerbier Couvée[1], Antonia Wachter-Zeh[1], Violetta Weger[2]

[1] Department of Electrical and Computer Engineering, Technical University of Munich, Germany.
{hugo.sauerbier-couvee, antonia.wachter-zeh}@tum.de *
[2] Department of Mathematics, Technical University of Munich, Germany. violetta.weger@tum.de **

Keywords: Rank-metric Codes, Generic Decoding, Signature Schemes, Algebraic Decoders

Abstract. The seminal work of [Bardet et al., 2020] has shown the potential of algebraic modelings to solve the Rank Syndrome Decoding Problem (R-SDP). For most parameter ranges, their algorithm first needs to perform a guessing step, making it a hybrid approach between combinatorial and algebraic solvers. In this paper, we present a novel guessing technique, which, when applied to [Bardet et al., 2020], is able to attack the proposed parameters of RYDE, a second-round candidate for the additional NIST standardization process. In particular, we show that all of the proposed RYDE parameters have to be updated: We can reduce the security of RYDE-1 to 104 bits, RYDE-3 to 153 bits, and RYDE-5 to 210 bits.

1 Introduction

Rank-metric codes are rapidly gaining attention lately due to being used in post-quantum-secure digital signature schemes and Key Encapsulation Mechanisms (KEMs). Since the launch of NIST's post-quantum cryptography standardization process in 2016, the field has evolved significantly. The first call ended with the selection of two KEMs and three signature schemes for standardization. However, development is far from finished; NIST opened an additional call for digital signatures in 2023, emphasizing the importance of novel schemes.

One leading approach in post-quantum cryptography uses hard problems from algebraic coding theory. Originating with McEliece's seminal work [23], code-based cryptography has grown into a major area of research. In particular, rank-metric-based cryptosystems have drawn interest for their compact key and ciphertext sizes. The rank-metric-based encryption schemes ROLLO [2] and RQC [3] were submitted to the first NIST call, and the digital signature schemes RYDE [5,4] and Mirath (merger of MIRA [6] and MiRitH [1]) have recently advanced to the second round of the additional NIST call. These proposals, and other schemes like Durandal [7] and LowMS [8], rely on the hardness of solving (variants of) the *Rank Syndrome Decoding Problem* (R-SDP) or the related *MinRank* problem.

* HBSC's and AWZ's work has been supported by the German Research Council (DFG) as an ANR-DFG project under Grant no. WA 3907/9-1.
** With the support of the Technical University of Munich – Institute for Advanced Study, funded by the German Excellence Initiative.

This paper deals with reducing the cost of solving the R-SDP: given a random parity-check matrix $\boldsymbol{H}$ of a code over a finite field $\mathbb{F}_{q^m}$ of dimension k and length n, a syndrome vector $\boldsymbol{s}$ and a rank weight t, find an error vector $\boldsymbol{e}$ with rank weight (at most) t, which satisfies the syndrome equations $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$.

Several generic decoding algorithms for the rank metric have been proposed, either of combinatorial or algebraic nature. On the one hand, the combinatorial attacks proposed in [9,16,19,24] employ the enumeration of certain subspaces, bases, or matrices combined with solving systems of linear equations. On the other hand, recent algebraic attacks on R-SDP and MinRank proposed in [10,13,14] exploit different algebraic modelings of the R-SDP as a system of polynomial equations that can be solved with computer algebra methods. These attacks have been celebrated as new benchmarks with lower costs in certain parameter regimes compared to the mentioned combinatorial attacks.

The algebraic modelings from [10,13,14] require that the system of equations is overdetermined. For most parameter ranges, this is not satisfied, and thus the authors suggest a hybrid approach, where they first guess certain entries of the error vector. This guessing step leads to a novel instance with reduced parameters, where the overdetermined condition is now satisfied. More in detail, given the parameters q, m, n, k, r, the overdetermined condition is given by

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

If this condition is not met, the authors propose guessing that a entries of $\boldsymbol{e}$ are zero. This requires q^{ar} trials on average but reduces the parameters to $q, m, n-a, k-a, r$.

In this paper, we advance their idea by proposing a different guessing step that results in a (surprisingly) significantly lower complexity. Instead of guessing a zero positions of $\boldsymbol{e}$, we choose a random a'-dimensional subspace $\mathcal{R}$ and append its basis vectors as rows to the parity-check matrix $\boldsymbol{H}$ and also append a' many zeros to the syndrome $\boldsymbol{s}$. This leads to a novel R-SDP instance with parameters $q, m, n, k-a', r$. In contrast to [10,13,14], we therefore also reduce the dimension k, but do *not* reduce the length n.

Our novel technique comes with a similar success probability but requires much fewer guesses to reach the overdetermined condition. This lower number of required guesses results in a remarkably smaller complexity of the decoder.

Using this novel guessing step in the algebraic modeling, we present an attack on *all* the parameters proposed in the second round submission of RYDE [4] and LowMS [8]. This brings all the proposed RYDE parameters below the claimed security level; see Table 1.

Instance	Security level	q	m	n	k	r	AGHT	a	Hybrid MM-$\mathbb{F}_q$	a'	NEW hybrid MM-$\mathbb{F}_q$
RYDE-1	128	2	53	53	45	4	149	37	170	14	**104**
RYDE-3	192	2	61	61	51	5	218	44	246	19	**153**
RYDE-5	256	2	67	67	55	6	289	48	318	24	**210**

Table 1. Comparison of the average time complexities of AGHT [9], hybrid MM-$\mathbb{F}_q$ [14], and our novel approach for RYDE parameters, where we take $\omega = 2$.

This paper is structured as follows. In Section 2, we provide all the necessary notation and definitions for the remainder of the paper. We also give a quick overview of the known

generic decoders in the rank metric in Section 3. In Section 4 we present the novel guessing step and apply it to the RYDE signature scheme, showing the significant reduction of the security level.

2 Preliminaries

Let q be a prime power and m be a positive integer. We denote by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_{q^m}$ its extension field of extension degree m.

For positive integers k, n we denote by $\mathbb{F}_q^{k\times n}$ the $k \times n$ matrices over $\mathbb{F}_q$. For $\boldsymbol{A} \in \mathbb{F}_q^{k\times n}$ we denote by $\boldsymbol{A}^\top$ its transpose matrix and by $\mathrm{rk}(\boldsymbol{A})$ its rank. For a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, we denote by $\langle x_1, \ldots, x_n\rangle_{\mathbb{F}_q}$ the $\mathbb{F}_q$-linear subspace spanned by the entries of $\boldsymbol{x}$.

Finally, the q-binomial coefficient is defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} = \frac{\prod_{i=1}^{n}(1-q^i)}{\prod_{i=1}^{k}(1-q^i)\prod_{i=1}^{n-k}(1-q^i)}.$$

There are two types of rank-metric codes; the first one considers linear subspaces in $\mathbb{F}_q^{m\times n}$, thus codewords are $m \times n$ matrices, and the code is $\mathbb{F}_q$-linear. Such codes are referred to as $\mathbb{F}_q$-*linear codes*; note that in this case, the decoding problem coincides with the MinRank problem [15].

We are more interested in the second case, that is, in $\mathbb{F}_{q^m}$-*linear codes*, which were used in the cryptosystems ROLLO [2], RQC [3], RYDE [5,4] and LowMS [8]. An $[n, k]$ linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, for integers $k \leq n$, is a k-dimensional linear subspace of $\mathbb{F}_{q^m}^n$. The elements of a code are called *codewords* and n is called the *length* of the code.

We call $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ a *generator matrix* of an $[n, k]$ linear code $\mathcal{C}$, if it has $\mathcal{C}$ as image, that is its rows span the subspace $\mathcal{C}$. Moreover, we call $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ a *parity-check matrix* of $\mathcal{C}$, if it has $\mathcal{C}$ as kernel:

$$\mathcal{C} = \{\boldsymbol{x}\boldsymbol{G} \mid \boldsymbol{x} \in \mathbb{F}_{q^m}^k\} = \{\boldsymbol{c} \in \mathbb{F}_{q^m}^n \mid \boldsymbol{c}\boldsymbol{H}^\top = 0\}.$$

The *rate* of an $[n, k]$ linear code is given by $R = \frac{k}{n}$. For $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ and a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ we call $\boldsymbol{s} = \boldsymbol{x}\boldsymbol{H}^\top \in \mathbb{F}_{q^m}^{n-k}$ a *syndrome.*

Definition 1. *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. The rank weight of $\boldsymbol{x}$ is given by the $\mathbb{F}_q$-dimension of the $\mathbb{F}_q$-vector space spanned by its entries, i.e.,*

$$\mathrm{wt_R}(\boldsymbol{x}) = \dim_{\mathbb{F}_q}(\langle x_1, \ldots, x_n\rangle_{\mathbb{F}_q}).$$

Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We define the *associated matrix* of $\boldsymbol{x}$ to be $\Gamma(\boldsymbol{x}) \in \mathbb{F}_q^{m\times n}$ with entries $\Gamma_{ij}(\boldsymbol{x})$, where

$$x_j = \sum_{i=1}^{m} \gamma_i \Gamma_{ij}(\boldsymbol{x}),$$

for all $j \in \{1, \dots, n\}$. Note that, if we consider the vector $\gamma = (\gamma_1, \dots, \gamma_m) \in \mathbb{F}_{q^m}^m$, we get $\boldsymbol{x} = \gamma\Gamma(\boldsymbol{x})$. Likewise, we define the *expansion* of an element $x \in \mathbb{F}_{q^m}$ to be the column vector $\Gamma(x) = (\Gamma_1(x), \dots, \Gamma_m(x))^\top \in \mathbb{F}_q^m$, where

$$x = \sum_{i=1}^{m} \gamma_i \, \Gamma_i(x) = \gamma\Gamma(x).$$

The rank weight of $\boldsymbol{x}$ is the same as the rank of the associated matrix of $\boldsymbol{x}$, i.e.,

$$\mathrm{wt_R}(\boldsymbol{x}) = \mathrm{rk}(\Gamma(\boldsymbol{x})),$$

for any basis Γ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. This is perfectly suitable, whenever $n \geq m$. We may refine the definition of the *rank support* to the two cases $n > m$ and $n \leq m$.

Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. The *rank support* of $\boldsymbol{x}$ is defined as

$$\mathrm{supp_R}(\boldsymbol{x}) = \begin{cases} \mathrm{colsp}(\Gamma(\boldsymbol{x})) \subseteq \mathbb{F}_q^m & \text{if } n \geq m, \\ \mathrm{rowsp}(\Gamma(\boldsymbol{x})) \subseteq \mathbb{F}_q^n & \text{if } n < m. \end{cases}$$

We alternatively refer to $\mathrm{colsp}(\Gamma(\boldsymbol{x}))$ as the *column support* of $\boldsymbol{x}$ and denote it as $\mathrm{supp_{col}}(\boldsymbol{x})$; likewise to $\mathrm{rowsp}(\Gamma(\boldsymbol{x}))$ as the *row support* of $\boldsymbol{x}$ and denote it as $\mathrm{supp_{row}}(\boldsymbol{x})$. The rank weight of $\boldsymbol{x}$ is also the $\mathbb{F}_q$-dimension of the rank support, i.e.,

$$\mathrm{wt_R}(\boldsymbol{x}) = \dim_{\mathbb{F}_q}(\mathrm{supp_R}(\boldsymbol{x})).$$

The rank weight induces a distance: the rank distance between $\boldsymbol{x}$ and $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ is given by

$$d_\mathrm{R}(\boldsymbol{x}, \boldsymbol{y}) \coloneqq \mathrm{wt_R}(\boldsymbol{x} - \boldsymbol{y}).$$

For a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ of rank weight t, we can uniquely (up to a change of basis) decompose $\boldsymbol{e}$ into

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{A} = (\alpha_1, \dots, \alpha_t) \begin{pmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_t \end{pmatrix},$$

where $\alpha_i \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$-linearly independent and $\boldsymbol{r}_i \in \mathbb{F}_q^n$ are also $\mathbb{F}_q$-linearly independent. The $\mathbb{F}_q$-span of the rows $\boldsymbol{r}_i$ coincides with the definition of support for $n < m$, that is

$$\mathrm{supp_R}(\boldsymbol{e}) = \mathrm{rowsp}(\boldsymbol{A}) = \langle \boldsymbol{r}_1, \dots, \boldsymbol{r}_t \rangle_{\mathbb{F}_q},$$

while the column span of $\Gamma(\boldsymbol{\alpha})$ coincides with the definition of support for $n \geq m$, i.e.,

$$\mathrm{supp_R}(\boldsymbol{e}) = \mathrm{colsp}(\Gamma(\boldsymbol{\alpha})).$$

Finally, we can define the minimum rank distance of a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, as

$$d_\mathrm{R}(\mathcal{C}) \coloneqq \min\{d_\mathrm{R}(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}\}.$$

In the rank-metric setting we have an analogous bound to the Gilbert-Varshamov bound, which we call the rank-metric Gilbert-Varshamov bound. For this, we define the *relative minimum rank distance* to be $\delta = d_\mathrm{R}(\mathcal{C})/n$ and when considering the extension degree m as function in n, we can define $M = \lim_{n\to\infty} m(n)/n$.

Proposition 1 ([22]). *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a random linear code of dimension $k = Rn$. For n large enough, we have that $\mathcal{C}$ has the relative minimum distance*

$$\delta = d_{\mathrm{R}}/n = M/2 + 1/2 - \sqrt{RM + (M-1)^2/4}$$

with high probability.

Interestingly, this bound does not depend on the field size q, which is in contrast to its Hamming-metric counterpart. In particular, if $M = 1$, which will often be the case for applications, we get $\delta = 1 - \sqrt{R}$. Let us denote the minimum distance on the Gilbert-Varshamov bound by d_{GV}^{R}, that is

$$d_{GV}^{\mathrm{R}} = n(M/2 + 1/2 - \sqrt{RM + (M-1)^2/4}).$$

Coding theory has found a crucial application in cryptography, by using the hardness of decoding a random linear code in the Hamming metric. One can formulate the same problem for rank-metric codes.

Problem 1 (Rank Syndrome Decoding Problem (R-SDP)). Given a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, a syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and $r \in \mathbb{N}$, find a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ of rank weight r, such that $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$.

For the R-SDP it is not known whether the problem is NP-hard. However, in [20], the authors give a randomized reduction from the SDP to the R-SDP, which hints at the hardness of this problem. The R-SDP is also strongly related to the MinRank problem, which has been shown to be NP-complete in [15].

Problem 2 (MinRank Problem). Let $\boldsymbol{G}_1, \ldots, \boldsymbol{G}_K \in \mathbb{F}_q^{m\times n}$ and $r \leq \min\{m, n\}$ be a positive integer. Find $(x_1, \ldots, x_K) \in \mathbb{F}_q^K$ such that

$$\mathrm{rk}(x_1\boldsymbol{G}_1 + \cdots + x_K\boldsymbol{G}_K) = r.$$

The MinRank problem coincides with the decoding problem for $\mathbb{F}_q$-linear codes and is thus equivalent to the respective syndrome decoding problem. While any $\mathbb{F}_{q^m}$-linear code can be regarded as an $\mathbb{F}_q$-linear code, the opposite is not true. Hence, the R-SDP is polynomial-time reducible to the MinRank problem; whether the other direction also holds true is still unknown.

3 Attacks on the R-SDP

Recall Problem 1, i.e., given a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, a syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and a positive integer, called the *target weight* $r \leq \min\{n, m\}$, find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{e}) = r$ such that $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$, which we call the *syndrome equations* or the *parity-check equations*.

Since we are interested in cryptographic applications, we will, unless stated otherwise, only consider R-SDP instances with *exactly one* solution, i.e., there exists a *unique* error $\boldsymbol{e}$ that satisfies the above conditions (when $\boldsymbol{s} = 0$ we assume unique *up to a scalar multiple*). Uniqueness always holds if $r \leq \lfloor \frac{d^{\mathrm{R}}-1}{2} \rfloor$ with d^{R} the minimum rank distance of the code corresponding to $\boldsymbol{H}$. For r attaining the rank-metric Gilbert-Varshamov bound,

i.e., $r = d_{GV}^{\mathrm{R}}$, uniqueness also holds with high probability. For this unique $\boldsymbol{e}$, denote its support by $E = \mathrm{supp}_{\mathrm{R}}(\boldsymbol{e})$.

Attacks on the R-SDP historically split into two categories; first, *combinatorial attacks* [9,16,19,24] with the strategy of guessing enough information about $\boldsymbol{e}$ so that the syndrome equations of the R-SDP instance can be reduced to an easily solvable full-rank system of linear equations over $\mathbb{F}_q$. For an efficient decoder, these guesses should be well-adapted to error vectors of rank weight r, i.e., the more rank-weight-r vectors satisfy these guesses, the fewer guesses we need to make, and the more efficient our algorithm. Researching what types of information require relatively few guesses to make and then iterating over these guesses is where combinatorics comes into play. Of course, these guesses should contain enough information to be usable to transform the syndrome equations into an easily solvable system. Existing combinatorial decoders involve guessing values of $\boldsymbol{e}$ or E [16,24] or guessing a *super-support* [9,19], i.e., a larger space containing E.

The second kind of attacks on the R-SDP are *algebraic attacks* [18,21], wherein one tries to model the equality $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{e}) = r$ or $\dim(E) = r$ algebraically as a system of (polynomial) equations on $\boldsymbol{e}$ in combination with the syndrome equations. Existing algebraic decoders use linearized polynomials [19], or determinants of certain submatrices called minors [14,13,10]. If the parameters of the R-SDP instance are such that the newly obtained system has sufficiently many equations to solve for all unknowns, the system is generally much faster solved than with purely combinatorial attacks. However, for many parameters, this is not the case, and we have to resort to *hybrid attacks*. In such an attack, we first, like in combinatorial attacks, guess partial information about $\boldsymbol{e}$ such that, when we follow up with algebraic modeling, we *do* get sufficiently many equations to solve for the unknowns.

3.1 Combinatorial decoders

We now give a brief overview of the best-known combinatorial decoders solving the R-SDP. The main idea of the most recent combinatorial decoders in [9,19] (denoted by GRS1, GRS2, GRS3, AGHT in Table 2) is to search for a space called a *super-support* S of suitable dimension containing the error support E. For a chosen super-support S, we use its basis over $\mathbb{F}_q$ to write $\boldsymbol{e}$ over $\mathbb{F}_q$ and then try to solve the resulting syndrome equations over $\mathbb{F}_q$. If the found solution does not have the correct rank weight, the super-support S is discarded and the process is repeated for a different super-support chosen at random. The cost of these algorithms is mainly given by the number of iterations required to find a super-support S with $E \subseteq S$.

The time complexity formulas in Table 2 provide an easy way of comparing the various algorithms. We note that AGHT always outperforms GRS2 and GRS3, so we only need to consider the decoders CS/OJ1, OJ2, GRS1, GRS4 and AGHT.

For a rough comparison, we omit the polynomial factors and define

$$M \coloneqq \frac{m}{n} \in \mathbb{R}_{>0}, \quad R \coloneqq \frac{k}{n} \in (0,1).$$

For $r \leq n - k + 1$, and in particular if r is on or close to the rank-metric GV-bound

$$\frac{r}{n} \approx \frac{M+1}{2} - \sqrt{RM + \frac{(M-1)^2}{4}} \leq 1 - R$$

Authors	Algorithm abbreviation	Main idea	Average time complexity in $\mathbb{F}_q$ operations
Chabaud-Stern (1996) [16]	CS	Basis enumeration	$\mathcal{O}\left((nr+m)^\omega q^{(r-1)(m-r)}\right)$
Ourivski-Johansson (2002) [24]	OJ1*	Basis enumeration	$\mathcal{O}\left((k+r)^\omega r^\omega q^{(r-1)(m-r)}\right)$
	OJ2*	Error enumeration	$\mathcal{O}\left((mr)^\omega q^{(r-1)(k+1)}\right)$
Gaborit-Ruatta-Schrek (2016) [19]	GRS1	Super(row)support	$\mathcal{O}\left((n-k)^\omega m^\omega q^{rk}\right)$
	GRS2	Super(column)support	$\mathcal{O}\left((n-k)^\omega m^\omega q^{r\left\lceil \frac{km}{n} \right\rceil}\right)$
	GRS3	Super(column)support	$\mathcal{O}\left((n-k)^\omega m^\omega q^{(r-1)\left\lceil \frac{(k+1)m}{n} \right\rceil}\right)$
	GRS4*	Annulator polynomial	$\mathcal{O}\left((mrk)^\omega q^{r\left\lceil \frac{(r+1)(k+1)-(n+1)}{r} \right\rceil}\right)$
Aragon-Gaborit-Hauteville-Tillich (2018) [9]	AGHT	Super(column)support	$\mathcal{O}\left((n-k)^\omega m^\omega q^{r\left\lceil \frac{(k+1)m}{n} \right\rceil - m}\right)$

Table 2. Overview of combinatorial generic rank-metric decoders with main idea behind the algorithm and time complexity. The number $2 \leq \omega \leq 3$ is the *matrix multiplication exponent*, also called *linear algebra constant*. For cryptographic analysis it is common to underestimate the time complexities by assuming $\omega = 2$. The algorithms marked with * make partial use of modeling the R-SDP as systems of polynomial equations, so are also considered *algebraic* to some extend.

(as commonly chosen in many cryptographic schemes, e.g. in RYDE [5,4]), we find that the following combinatorial decoders are generally the fastest in the given parameter regimes:

- AGHT for $M \leq 1$ and all R;
- OJ2 for $M > 1$ and $R \geq \frac{1}{2}$;
- GRS4 for $M > 1$ and $R < \frac{1}{2}$;
- GRS1 for $M \gg 1$, $R < \frac{1}{2}$ and $r = n - k + 1 \approx (1 - R)n$.

For completeness, we also note that AGHT and GRS4 could be slightly improved with *guessing-enhancement* [17]. When applied to AGHT, the resulting decoder is a combination of an exhaustive search of t values in $\mathbb{F}_q$ (with success probability q^{-t} for each guess) and AGHT as subroutine. As t values are guessed, an internal parameter concerning the super-support can be adjusted slightly within the AGHT algorithm, resulting in a reduced complexity $\mathcal{O}\left(q^{r\left\lceil \frac{(k+1)m-t}{n} \right\rceil - m}\right)$ (up to polynomial factors). When optimized for the guessing parameter t, the guessing-enhanced AGHT decoder has average time complexity

$$\mathcal{O}\left(\min_{0 \leq t \leq mn} ((n-k)m+t)^\omega q^{t+r\left\lceil \frac{(k+1)m-t}{n} \right\rceil - m}\right),$$

with $t = 0$ resulting in plain AGHT. Note that a larger $t > 0$ only gives an improvement if the remainder $(k+1)m \pmod n$ is between 1 and $r - 1$.

3.2 Algebraic attacks

The most recent algebraic attacks were developed in [11,14,10,13] and are celebrated as new benchmark in the cost of solving the R-SDP and MinRank problem. For this paper, two of these algorithms are of main importance and are considered the fastest decoders for most parameters: the MaxMinors (MM-$\mathbb{F}_q$) modeling decoder [14] and the SupportMinors (SM-$\mathbb{F}_{q^m}^+$) modeling decoder [13].

MaxMinors modeling decoder The MM-$\mathbb{F}_q$ decoder in [14] uses the modeling idea of [11], where the authors reformulate the R-SDP problem as a bilinear system of equations with coefficient variables and support variables. They observe that due to $\mathrm{wt_R}(\boldsymbol{e}) = r$, an $r \times (n-k-1)$ matrix in the modeling consisting of coefficient variables is rank-deficient, and hence its maximal minors are all zero, leading to a new system of polynomial equations. With the help of the Cauchy-Binet formula and by setting certain maximal minors as new variables, this system is then transformed into a system of $m\binom{n-k-1}{r}$ linear equations in $\binom{n}{r}$ variables over $\mathbb{F}_q$. Inherent to solving this system is the requirement

$$m\binom{n-k-1}{r} \geq \binom{n}{r} - 1 \tag{3.1}$$

which we call the *overdetermined case*. Further, this system needs to be of near full rank, which was found to hold true with high probability after running many experiments [14,13].

Heuristic 1 *The system of $m\binom{n-k-1}{r}$ linear equations in the MaxMinors modeling of a random R-SDP instance is with high probability of rank* $\min\{m\binom{n-k-1}{r}, \binom{n}{r} - 1\}$.

Assuming this heuristic, the MaxMinors modeling suffices to find a one-dimensional space of solutions in the new variables, from which the sought-after error $\boldsymbol{e}$ is easily obtained. The final cost of this MM-$\mathbb{F}_q$ decoder is mainly given by the cost of solving the associated system of linear equations, i.e.,

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

where again it is common to assume $\omega = 2$, taking into account that any structure of the linear system could be exploited.

In case the number of equations is much larger than the number of variables, called the *superdetermined case*, a puncturing argument can additionally be applied to reduce the parameters of the system, specifically replacing the length n by $n-p$. Using this technique, the new cost is then given by

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

where

$$p := \max\left\{i \in \{0, ..., n-k-1-r\} \mid m\binom{n-i-k-1}{r} \geq \binom{n-i}{r} - 1\right\}. \tag{3.2}$$

Hybrid technique In [14] and further explained in [13], the authors propose a workaround when the overdetermined condition is not satisfied, that is, we are in the so-called *underdetermined case* $m\binom{n-k-1}{r} < \binom{n}{r} - 1$. Their solution lies in guessing a entries of $\boldsymbol{e}$ to be zero for some $a \geq 1$ (within the modeling, this comes down to guessing ar many $\mathbb{F}_q$-variables to be zero, with success probability q^{-ar}), combined with a rerandomization method. This hybrid technique generalizes to reducing the R-SDP with instance parameters (q, m, n, k, r) to instance parameters $(q, m, n-a, k-a, r)$, with success probability q^{-ar}. We call this the *zero-reduction with parameter* a, denoted $\mathrm{Red}_{\mathrm{zero},\,a}$. Applied to a generic rank-metric decoder $\mathcal{A}$ gives the algorithm $\mathrm{Red}_{\mathrm{zero},\,a}(\mathcal{A})$ with description:

1. Set ar many $\mathbb{F}_q$-variables to zero, obtain reduced instance;
2. Try solving the reduced instance with decoder $\mathcal{A}$, obtain candidate solution $\hat{\boldsymbol{e}}$;
3. If no solution or if $\mathrm{wt}_{\mathrm{R}}(\hat{\boldsymbol{e}}) \neq r$, rerandomize and go back to 1. Else, if $\mathrm{wt}_{\mathrm{R}}(\hat{\boldsymbol{e}}) = r$, then $\boldsymbol{e} = \hat{\boldsymbol{e}}$ and we are done.

Proposition 2. *[14,13] Given a random R-SDP instance with unique solution and parameters (q, m, n, k, r), the average time complexity of a generic rank-metric decoder $\mathcal{A}$ with zero-reduction with parameter $a \geq 0$ solving the instance is given by*

$$TC_{\mathrm{Red}_{\mathrm{zero},\,a}(\mathcal{A})}(q, m, n, k, r) \;=\; q^{ar} \cdot TC_{\mathcal{A}}(q, m, n-a, k-a, r).$$

Here $TC_{\mathcal{A}}(q, m, n, k, r)$ denotes the average time complexity in $\mathbb{F}_q$ operations of a generic decoder $\mathcal{A}$ solving an R-SDP instance with parameters (q, m, n, k, r) with *unique* solution. Naturally we can set $a \geq 0$ to minimize $TC_{\mathrm{Red}_{\mathrm{zero},\,a}(\mathcal{A})}(q, m, n, k, r)$.

Specifically when applied to the MM-$\mathbb{F}_q$ decoder, the zero-reduction can reduce an *underdetermined instance* to an *overdetermined instance*, which can then be solved with the plain MM-$\mathbb{F}_q$ decoder. The average time complexity is then usually minimized for a around

$$a_{min} := \min\left\{ i \geq 0 \;\middle|\; m\binom{n-k-1}{r} \geq \binom{n-i}{r} - 1 \right\}. \tag{3.3}$$

$$\begin{aligned}
TC_{\text{Hybrid MM-}\mathbb{F}_q}(q, m, n, k, r) \;&=\; \min_{a \geq a_{min}} \; TC_{\mathrm{Red}_{\mathrm{zero},\,a}(\text{MM-}\mathbb{F}_q)}(q, m, n, k, r) \\
&=\; \min_{a \geq a_{min}} \; q^{ar} \cdot TC_{\text{MM-}\mathbb{F}_q}(q, m, n-a, k-a, r) \\
&= \mathcal{O}\left(\min_{a \geq a_{min}} \; m\, q^{ar} \binom{n-k-1}{r} \binom{n-a}{r}^{\omega-1} \right) \qquad (3.4) \\
&\approx \mathcal{O}\left(m\, q^{a_{min} r} \binom{n-k-1}{r} \binom{n-a_{min}}{r}^{\omega-1} \right). \qquad (3.5)
\end{aligned}$$

SupportMinors modeling decoder In [13], a similar approach to the MaxMinors decoder is taken but applied to a different matrix in the modeling of the R-SDP. The resulting SupportMinors modeling decoder SM-$\mathbb{F}_{q^m}^{+}$ then solves, for a parameter $b \geq 1$, a system over $\mathbb{F}_q$ of $\mathcal{N}_b(m, n, k, r)$ linear independent equations in $\mathcal{M}_b(m, n, k, r)$ variables, with

$$\begin{aligned}
\mathcal{N}_b(m, n, k, r) \;:=\; &\sum_{i=1}^{k} \binom{n-i}{r}\binom{k+b-1-i}{b-1} - \binom{n-k-1}{r}\binom{k+b-1}{b} \\
&- (m-1)\sum_{i=1}^{b} (-1)^{i+1} \binom{k+b-i-1}{b-i}\binom{n-k-1}{r+i}
\end{aligned}$$

and

$$\mathcal{M}_b(m,n,k,r) := \binom{k+b-1}{b}\left(\binom{n}{r} - m\binom{n-k-1}{r}\right).$$

Like for MM-$\mathbb{F}_q$, we again require the overdetermined condition

$$\mathcal{N}_b(m,n,k,r) \geq \mathcal{M}_b(m,n,k,r) - 1$$

to solve the system. If this is not satisfied we apply zero-reduction with parameter $a \geq a_{min}(b) := \min\{i \geq 0 \mid \mathcal{N}_b(m,n-i,k-i,r) \geq \mathcal{M}_b(m,n-i,k-i,r)-1\}$ and optimize for a and b. This gives us the final cost $TC_{\text{Hybrid SM-}\mathbb{F}^+_{q^m}}(q,m,n,k,r)$ of the hybrid SM-$\mathbb{F}^+_{q^m}$ decoder:

$$\mathcal{O}\left(\min_{b\geq 1}\min_{a\geq a_{min}(b)} m^2\,\mathcal{N}_b(m,n-a,k-a,r)\,\mathcal{M}_b(m,n-a,k-a,r)^{\omega-1}\right) \tag{3.6}$$

where we can optimistically set $\omega = 2$.

4 Novel Hybrid Attack Technique on R-SDP

Recall that for an R-SDP instance $(\boldsymbol{H},\boldsymbol{s},r)$ with parameters (q,m,n,k,r) we are given a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, a syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and a target rank weight r. For $\boldsymbol{s} \neq 0$ we assume that there exists a unique solution $\boldsymbol{e}$ satisfying both $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{e}) = r$ and $\boldsymbol{H}\boldsymbol{e}^\top = \boldsymbol{s}^\top$; for $\boldsymbol{s} = 0$ we assume a 1-dimensional space of solutions.

4.1 Row-support reduction

Consider a random a'-dimensional space $\mathcal{R} \subseteq \mathbb{F}_q^n$ for some parameter $0 \leq a' \leq k$, and let $\{\boldsymbol{r}_1,\ldots,\boldsymbol{r}_{a'}\}$ be any basis of $\mathcal{R}$. Recall that $\boldsymbol{e} = \boldsymbol{\alpha}A$ for some unknown $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^r$ of rank weight r and $A \in \mathbb{F}_q^{r\times n}$ of rank r. When we append the basis vectors $\boldsymbol{r}_i$ as rows below $\boldsymbol{H}$, and a' zeros below $\boldsymbol{s}^\top$, the equation

$$\begin{pmatrix} \boldsymbol{H} \\ -\boldsymbol{r}_1- \\ \vdots \\ -\boldsymbol{r}_{a'}- \end{pmatrix}\boldsymbol{e}^\top = \begin{pmatrix} \boldsymbol{H} \\ -\boldsymbol{r}_1- \\ \vdots \\ -\boldsymbol{r}_{a'}- \end{pmatrix}\boldsymbol{A}^\top\boldsymbol{\alpha}^\top = \begin{pmatrix} \boldsymbol{s}^\top \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{4.1}$$

is satisfied if and only if $\mathrm{supp}_{\mathrm{row}}(\boldsymbol{e}) = \mathrm{rowsp}(\boldsymbol{A}) = \mathrm{colsp}(\boldsymbol{A}^\top) \subseteq \mathcal{R}^\perp$. As $\mathrm{rowsp}(\boldsymbol{A})$ is an r-dimensional subspace and $\mathcal{R}^\perp$ a random $(n-a')$-dimensional subspace in $\mathbb{F}_q^n$, this happens with probability

$$\frac{\begin{bmatrix} n-a' \\ r \end{bmatrix}_q}{\begin{bmatrix} n \\ r \end{bmatrix}_q} = \prod_{i=0}^{r-1}\frac{q^{n-a'}-q^i}{q^n-q^i} \geq q^{-a'r}\prod_{i=1}^{\infty}(1-q^{-i}) \geq \frac{1}{4}\,q^{-a'r} \geq q^{-a'r-2}$$

for $q \geq 2$. This means that, if (4.1) is satisfied, we obtain $\boldsymbol{e}$ by solving the R-SDP instance $(\boldsymbol{H}',\boldsymbol{s}',r)$ given by

$$\boldsymbol{H}' := \begin{pmatrix} \boldsymbol{H} \\ -\boldsymbol{r}_1- \\ \vdots \\ -\boldsymbol{r}_{a'}- \end{pmatrix}, \qquad \boldsymbol{s}' := \begin{pmatrix} \boldsymbol{s} & 0 & \cdots & 0 \end{pmatrix}.$$

Since $\mathcal{R}$ is random, $\boldsymbol{H}'$ has with high probability full $\mathbb{F}_{q^m}$-rank, i.e., $(n-k+a')$. Hence we reduced solving an R-SDP instance with parameters (q,m,n,k,r) to solving an instance with parameters $(q,m,n,k-a',r)$, with success probability $\geq q^{-a'r-2}$. We call this reduction the *row-support reduction with parameter* a' denoted by $\mathrm{Red}_{\mathrm{supp}_r,a'}$. Note that since we are essentially guessing a' linear $\mathbb{F}_q$-equations that $\boldsymbol{e}$ satisfies, in addition to the syndrome equations $\boldsymbol{H}\boldsymbol{e}^\top = \boldsymbol{s}^\top$, the reduced instance cannot have more solutions than the original instance.

Clearly, we have to again assume that the new linear system has full rank.

Heuristic 2 *The system of* $m\binom{n-k+a'-1}{r}$ *linear equations in the MaxMinors modeling of a random R-SDP instance after the novel row-support heuristic is with high probability of rank* $\min\{m\binom{n-k+a'-1}{r}, \binom{n}{r}-1\}$.

We validated this heuristic by performing similar experiments as [14,13]. We adapted the code from https://github.com/mbardet/Rank-Decoding-tools that check Heuristic 1 to include tests on Heuristic 2 for the row-support reduced instances. The code can be found here: https://github.com/HBeelooSauerbierCouvee/generic-rank-decoding

Applied to a generic rank-metric decoder $\mathcal{A}$ gives the algorithm $\mathrm{Red}_{\mathrm{supp}_r,a'}(\mathcal{A})$ with description:

1. Choose a random a'-dimensional subspace of $\mathbb{F}_q^n$. Append its basis vectors below $\boldsymbol{H}$ to get $\boldsymbol{H}'$. Append a' zeros to $\boldsymbol{s}$ to get $\boldsymbol{s}'$;
2. Try solving the reduced instance $(\boldsymbol{H}', \boldsymbol{s}', r)$ with decoder $\mathcal{A}$, obtain candidate solution $\hat{\boldsymbol{e}}$;
3. If no solution or if $\mathrm{wt_R}(\hat{\boldsymbol{e}}) \neq r$, go back to 1. Else, if $\mathrm{wt_R}(\hat{\boldsymbol{e}}) = r$, then $\boldsymbol{e} = \hat{\boldsymbol{e}}$ and we are done.

Algorithm 1 Hybrid decoder with row-support reduction $\mathrm{Red}_{\mathrm{supp}_r,a'}$ with $0 \leq a' \leq k$

Input: Generic decoder $\mathcal{A}$, R-SDP instance $(\boldsymbol{H}, \boldsymbol{s}, r)$.
Output: $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $\boldsymbol{H}\boldsymbol{e}^\top = \boldsymbol{s}^\top$ and $\mathrm{wt_R}(\boldsymbol{e}) = r$.

1: $\boldsymbol{R} \xleftarrow{\$} \mathbb{F}_q^{a' \times n}$ until $\mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{R}) = a'$ (happens w.h.p.) // sample random full rank $(a' \times n)$-matrix /$\mathbb{F}_q$ (basis vectors of random a'-dim subspace $\mathcal{R} \subset \mathbb{F}_q^n$)

2: $\boldsymbol{H}' \leftarrow \begin{pmatrix} \boldsymbol{H} \\ \boldsymbol{R} \end{pmatrix}$ //append $\boldsymbol{R}$ below $\boldsymbol{H}$

3: $\boldsymbol{s}' \leftarrow \begin{pmatrix} \boldsymbol{s} & 0 & \cdots & 0 \end{pmatrix}$ // append a' zeros after $\boldsymbol{s}$

4: $\hat{\boldsymbol{e}} \leftarrow \mathcal{A}(\boldsymbol{H}', \boldsymbol{s}', r)$ // solve new reduced R-SDP instance with $\mathcal{A}$

5: If no $\hat{\boldsymbol{e}}$ or if $\mathrm{wt_R}(\hat{\boldsymbol{e}}) \neq r$, go back to 1.

6: Else, return $\boldsymbol{e} = \hat{\boldsymbol{e}}$. // solution $\hat{\boldsymbol{e}}$ is found and satisfies $\mathrm{wt_R}(\hat{\boldsymbol{e}}) = r$

We note that setting $a' = k$ and choosing $\mathcal{A}$ to be a standard $\mathcal{O}(n^\omega)$ solver of a full-rank system of n linear equations, we essentially get back the GRS1 decoder. This new hybrid reduction can therefore be seen as a parameterized middle ground between GRS1 (or AGHT for $n = m$) and any chosen decoder $\mathcal{A}$.

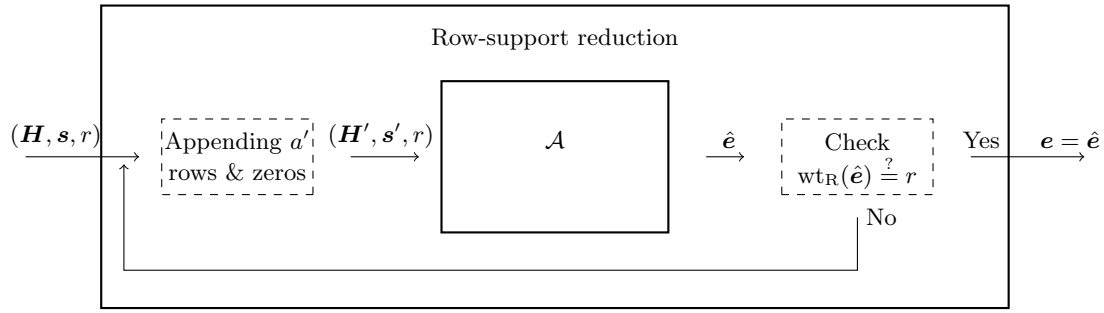


Fig. 1. Diagrammatic representation of hybrid decoder with row-support reduction

4.2 Time complexity and comparison

Recall that $TC_{\mathcal{A}}(q, m, n, k, r)$ denotes the average time complexity in $\mathbb{F}_q$ operations of a generic decoder $\mathcal{A}$ solving an R-SDP instance with parameters (q, m, n, k, r) with *unique* solution.

Proposition 3. *Given a random R-SDP instance with unique solution and parameters (q, m, n, k, r), the average time complexity of a generic rank-metric decoder $\mathcal{A}$ with row-support reduction with parameter $a' \geq 0$ solving the instance is given by*

$$TC_{\mathrm{Red}_{\mathrm{supp}_r,\, a'}(\mathcal{A})}(q, m, n, k, r) \;= \mathcal{O}\left(a'n\; q^{a'r+2} \cdot TC_{\mathcal{A}}(q, m, n, k - a', r)\right).$$

Proof. As (4.1) is satisfied with probability $\geq q^{-a'r-2}$, we need to loop back from Step 5 to Step 1 on average $q^{a'r+2}$ times. For each of these iterations, we need to sample $\mathcal{R}$ in Step 1 ($a'n$ operations) and decode with $\mathcal{A}$ in Step 4 (average time complexity $TC_{\mathcal{A}}(q, m, n, k - a', r)$). For every iteration $\boldsymbol{H}'$ has with high probability full $\mathbb{F}_{q^m}$-rank $(n - k + a')$, so this does not meaningfully affect the overall complexity. □

Naturally we can set $a' \geq 0$ to minimize $TC_{\mathrm{Red}_{\mathrm{supp}_r,\, a'}(\mathcal{A})}(q, m, n, k, r)$.

Specifically when we apply this in the MM-$\mathbb{F}_q$ decoder, the row-support reduction can reduce an *underdetermined instance* to an *overdetermined instance*, which can then be solved with the plain MM-$\mathbb{F}_q$ decoder. The average time complexity is then usually minimized for a' around

$$a'_{min} := \min\left\{i \geq 0 \mid m\binom{n-k-1+i}{r} \geq \binom{n}{r} - 1\right\}. \tag{4.2}$$

$$
\begin{aligned}
TC_{\text{New hybrid MM-}\mathbb{F}_q}(q,m,n,k,r) &= \min_{a' \geq a'_{min}} TC_{\text{Red}_{\text{supp}_r,\, a'}(\text{MM-}\mathbb{F}_q)}(q,m,n,k,r) \\
&= \min_{a' \geq a'_{min}} a'n\; q^{a'r+2} \cdot TC_{\text{MM-}\mathbb{F}_q}(q,m,n,k-a',r) \\
&= \mathcal{O}\left(\min_{a' \geq a'_{min}} ma'n\; q^{a'r+2} \binom{n-k-1+a'}{r} \binom{n}{r}^{\omega-1} \right) \qquad (4.3) \\
&\approx \mathcal{O}\left(ma'n\; q^{a'_{min}r+2} \binom{n-k-1+a'_{min}}{r} \binom{n}{r}^{\omega-1} \right). \qquad (4.4)
\end{aligned}
$$

Comparing to the hybrid MM-$\mathbb{F}_q$ with zero-reduction with parameter $a \geq a_{min}$ (equation (3.3)), we note that we often get $a'_{min} \ll a_{\min}$. So even though the plain MM-$\mathbb{F}_q$ in our new hybrid method deals with a larger parameter instance $(q, m, n, k-a', r)$ compared to $(q, m, n-a, k-a, r)$, this increase in complexity is often outweighed by the decrease of the exponential factor q^{ar} to $q^{a'r+2}$, as $a' \ll a$.

Let us now have a look at the impact of the new decoder for some proposed systems. We start with the RYDE signature scheme [4], which is a second round candidate in the additional NIST standardization process. For their second round submission, we can see in Table 3, that the number of guesses $a'_{min} \ll a_{min}$.

q	m	n	k	r	a_{min}	a'_{min}
2	53	53	45	4	37	**14**
2	61	61	51	5	44	**19**
2	67	67	55	6	48	**24**

Table 3. Comparison of $a_{\min}$ (Eq. (3.3)) and $a'_{\min}$ (Eq. (4.2)) for RYDE Round 2 parameters

In Table 4, we show the security reductions for *all* of the proposed RYDE parameters in the second round submission [4]. Here we compare the new technique, denoted by "MM-$\mathbb{F}_q$ row-supp red", to the AGHT [9] and the hybrid MM-$\mathbb{F}_q$ decoder from [12] with zero-reduction, denoted "MM-$\mathbb{F}_q$ zero-red". In Table 5 we further compare our new technique applied to the SupportMinor modeling, denoted by SM-$\mathbb{F}_{q^m}^+$ [13]. Also for this modeling technique, we can see that the new guessing step "row-supp red" leads to significant improvements.

Interestingly, the RYDE parameters proposed in the first round [5] are less susceptible to the new technique, as we can observe in Table 6.

Finally, we also apply the new algorithm to LowMS [8], where we again see a large security reduction.

We used Sage to compute the costs of the decoders in the tables below. The code is available here https://github.com/HBeelooSauerbierCouvee/generic-rank-decoding

Instance	Security level	q	m	n	k	r	AGHT	a	p	MM-$\mathbb{F}_q$ zero-red	a'	p	MM-$\mathbb{F}_q$ row-supp red
RYDE-1	128	2	53	53	45	4	149	37	0	170	14	0	**104**
RYDE-3	192	2	61	61	51	5	218	44	0	246	19	0	**153**
RYDE-5	256	2	67	67	55	6	289	48	0	318	24	0	**210**

Table 4. RYDE Round 2 parameters (field size q, extension degree m, code length n, code dimension k, rank weight r) with comparison of the average time complexities of AGHT, hybrid MM-$\mathbb{F}_q$ with zero-reduction (parameter a, Eq. (3.4)) and hybrid MM-$\mathbb{F}_q$ with row-support reduction (parameter a', Eq. (4.3)), where we take $\omega = 2$. Note that since $m = n$, we get no improvement from adding guessing enhancement to AGHT. Combining zero- or row-support reduction with puncturing with parameter p (Eq.(3.2)) does not yield an improvement for RYDE parameters.

Instance	Security level	q	m	n	k	r	a	b	SM-$\mathbb{F}_{q^m}^+$ zero-red	a'	b	SM-$\mathbb{F}_{q^m}^+$ row-supp red
RYDE-1	128	2	53	53	45	4	36	1	180	13	1	**114**
RYDE-3	192	2	61	61	51	5	43	1	254	18	1	**163**
RYDE-5	256	2	67	67	55	6	47	2	331	23	1	**218**

Table 5. RYDE Round 2 parameters (q, m, n, k, r) with comparison of the average time complexities of hybrid SM-$\mathbb{F}_{q^m}^+$ with zero-reduction (Eq. (3.6)) and hybrid SM-$\mathbb{F}_{q^m}^+$ with row-support reduction (Eq. (3.6) and Proposition 3), where we take $\omega = 2$.

Instance	Security level	q	m	n	k	r	AGHT	a	p	MM-$\mathbb{F}_q$ zero-red	a'	p	MM-$\mathbb{F}_q$ row-supp red
RYDE-1	128	2	31	33	15	10	148	12	2	153	8	0	**144**
RYDE-3	192	2	37	41	18	13	217	15	2	238	11	1	221
RYDE-5	256	2	43	47	18	17	284	15	2	309	12	2	296

Table 6. RYDE Round 1 parameters with comparison of the average time complexities of AGHT, hybrid MM-$\mathbb{F}_q$ with zero-reduction (Eq. (3.4)) and hybrid MM-$\mathbb{F}_q$ with row-support reduction (Eq. (4.3)), where we take $\omega = 2$.

Instance	Security level	q	m	n	k	r	a	b	SM-$\mathbb{F}_{q^m}^+$ zero-red	a	a'	b	SM-$\mathbb{F}_{q^m}^+$ row-supp red
RYDE-1	128	2	31	33	15	10	11	1	156	1	7	1	148
RYDE-3	192	2	37	41	18	13	14	2	241	2	9	1	226
RYDE-5	256	2	43	47	18	17	-	-	-	3	9	1	295

Table 7. RYDE Round 1 parameters with comparison of the average time complexities of hybrid SM-$\mathbb{F}_{q^m}^+$ with zero-reduction (Eq. (3.6)) and hybrid SM-$\mathbb{F}_{q^m}^+$ with row-support reduction (Eq. (3.6) and Proposition 3) combined with zero-reduction for parameter a, where we take $\omega = 2$.

Security level	q	m	n	k	r	AGHT	OJ2	a	p	MM-$\mathbb{F}_q$ zero-red	a'	p	MM-$\mathbb{F}_q$ row-supp red
128	2	61	50	25	7	185	176	10	0	119	6	1	**105**
128	2	67	66	33	7	201	224	10	0	126	6	0	**112**
192	2	101	74	37	8	339	287	13	0	167	8	1	**143**
192	2	79	78	39	8	273	301	16	1	191	9	0	**153**
256	2	101	88	44	9	385	382	19	0	243	12	1	**198**
256	2	107	106	53	9	413	454	22	0	275	13	0	**213**

Table 8. LowMS parameters with comparison of the average time complexities of AGHT, OJ2, hybrid MM-$\mathbb{F}_q$ with zero-reduction (Eq. (3.4)) and hybrid MM-$\mathbb{F}_q$ with row-support reduction (Eq. (4.3)), where we take $\omega = 2$. The previously computed values in [8] use $\omega = 2.8$ and $\omega = 3$.

References

1. Gora Adj, Luis Rivera-Zamarripa, Javier Verbel, Emanuele Bellini, Stefano Barbero, Andre Esser, Carlo Sanna, and Floyd Zweydinger. MiRitH. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
2. Carlos Aguilar Melchor, Nicolas Aragon, Magali Bardet, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Ayoub Otmani, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. ROLLO- Rank-Ouroboros, LAKE & LOCKER. *NIST PQC Call for Proposals*, 2020. Round 2 Submission.
3. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Maxime Bros, Alain Couvreur, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Rank Quasi-Cyclic (RQC). *NIST PQC Call for Proposals*, 2020. Round 2 Submission.
4. Nicolas Aragon, Magali Bardet, Loıc Bidoux, Jesús-Javier Chi-Domınguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Romaric Neveu, Matthieu Rivain, Jean-Pierre Tillich, and Adrien Vin***c***cotte. RYDE Signature Scheme. In *Second Round Submission to the additional NIST Postquantum Cryptography Call*, 2025.
5. Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, Jean-Pierre Tillich, and Adrien Vin***c***cotte. RYDE. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
6. Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu, Matthieu Rivain, and Jean-Pierre Tillich. MIRA. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
7. Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. 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 38*, pages 728–758. Springer, 2019.
8. Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, Pierre Loidreau, Julian Renner, and Antonia Wachter-Zeh. LowMS: a new rank metric code-based kem without ideal structure. *Designs, Codes and Cryptography*, 92(4):1075–1093, 2024.
9. Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. A new algorithm for solving the rank syndrome decoding problem. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2421–2425, 2018.
10. Magali Bardet and Manon Bertin. Improvement of algebraic attacks for solving superdetermined minrank instances. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography*, pages 107–123, Cham, 2022. Springer International Publishing.
11. Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich. An algebraic attack on rank metric code-based cryptosystems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 64–93. Springer, 2020.
12. Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. Revisiting algebraic attacks on MinRank and on the rank decoding problem. *arXiv preprint arXiv:2208.05471*, 2022.

13. Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. Revisiting algebraic attacks on MinRank and on the rank decoding problem. *Designs, Codes and Cryptography*, 91(11):3671–3707, Nov 2023.
14. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 507–536, Cham, 2020. Springer International Publishing.
15. Jonathan F Buss, Gudmund S Frandsen, and Jeffrey O Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572–596, 1999.
16. Florent Chabaud and Jacques Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 368–381. Springer, 1996.
17. Giuseppe D'Alconzo, Andre Esser, Andrea Gangemi, and Carlo Sanna. Sneaking up the ranks: Partial key exposure attacks on rank-based schemes. *Cryptology ePrint Archive*, 2024.
18. Jean-Charles Faugere, Fran**c**coise Levy-dit Vehel, and Ludovic Perret. Cryptanalysis of MinRank. In *Annual International Cryptology Conference*, pages 280–296. Springer, 2008.
19. Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Transactions on Information Theory*, 62(2):1006–1019, 2015.
20. Philippe Gaborit and Gilles Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Transactions on Information Theory*, 62(12):7245–7252, 2016.
21. Fran**c**coise Levy-dit Vehel and L Perret. Algebraic decoding of rank metric codes. *Proceedings of YACC*, pages 142–152, 2006.
22. Pierre Loidreau. Properties of codes in rank metric. *arXiv preprint cs/0610057*, 2006.
23. Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, DSN Progress report, Jet Propulsion Laboratory, Pasadena, 1978.
24. Alexei V Ourivski and Thomas Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38:237–246, 2002.