RAMESSES, a Rank Metric Encryption Scheme with Short Keys

Julien Lavauzelle, Pierre Loidreau, Ba-Duc Pham

RAMESSES, a Rank Metric Encryption Scheme with Short Keys

Julien Lavauzelle[1], Pierre Loidreau[2], and Ba-Duc Pham[1]

[1] Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
{julien.lavauzelle, ba-duc.pham}@univ-rennes1.fr
[2] Univ Rennes, DGA MI, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
pierre.loidreau@univ-rennes1.fr

Abstract. We present a rank metric code-based encryption scheme with key and ciphertext sizes comparable to that of isogeny-based cryptography for an equivalent security level. The system also benefits from efficient encryption and decryption algorithms, which rely on linear algebra operations over finite fields of moderate sizes. The security only relies on rank metric decoding problems, and does not require to hide the structure of a code. Based on the current knowledge, those problems cannot be efficiently solved by a quantum computer. Finally, the proposed scheme admits a failure probability that can be precisely controlled and made as low as possible.

Keywords: Post-quantum cryptography, encryption scheme, Gabidulin codes, rank-metric decoding problems

1 Introduction

With the growing probability of the existence of a near-future quantum computer, it has become important to propose alternatives to existing public-key encryption schemes and key exchange protocols based on number theory. The recent NIST Post-Quantum Cryptography Standardization process motivates proposals in this sense. Along with lattice-based cryptography, code-based cryptography is the most represented among proposals for encryption schemes or key-encapsulation mechanisms (KEMs). Code-based submissions generically rely on the hardness of decoding problems, either in the Hamming metric or in the rank metric. Hamming metric decoding problems enjoy a long-standing study and few practical improvements for more than fifty years, which ascertain their security. On the opposite, rank metric decoding problems have been studied for less than twenty years [8], and their solving complexity is not yet fully stabilized (see the recent results of [6]). Nevertheless, they benefit from much shorter keys and seem very attractive for practical implementation, culminating in submissions for the NIST standardization process [1, 2]. So as to further reduce the key sizes, designers often use specific structures as quasi-cyclicity (equivalent of Module-LWE for lattices) which could be suspected to introduce additional weaknesses [20].

In this paper we aim at designing a new one-way encryption scheme featuring very compact keys, based on rank metric decoding problems. The long-standing idea finds origins in [12] which was an extended idea of a proposal in Hamming metric [4]. The original rank metric encryption scheme was broken in [15], and a recent repair was proposed in [30]. However it implies to choose a specific code and a syndrome coming from a structured vector of moderate rank, which we want to avoid here.

Inspired from [12], we design a simple one-way encryption scheme with the following strengths.

- The security of the scheme only relies on decoding problems in rank metric (such as MinRank and Gab-SD) and does not require to hide the structure of a code. These decoding problems have been — and are still being — scrutinized in active research fields.
- Especially as a KEM, our proposal enables very small parameters for a given security target. Key sizes are competitive with isogeny-based proposals such as SIKE [5].
- Even if the decryption algorithm is probabilistic, it is easy to control the failure probability and to make it as small as possible without increasing to much the parameters.

A remaining weakness would be that underlying problems have been less investigated than others. However, our goal here is also to emulate research in this field to be able to ascertain the security of the scheme.

In a first section we introduce necessary notation and definitions. Then we describe the encryption scheme and we propose sets of parameters for security levels 1, 3, 5 of the NIST competition. Keys and ciphertext sizes are not larger than few hundreds of bytes. In the next section, we prove the consistency of the encryption scheme and we analyze its security by showing to which problems the security can be reduced, and by giving the complexity of algorithms solving these problems.

2 Preliminaries

2.1 Notation and definitions

Throughout the paper, we set $q = 2^n$ for some integer $n \geq 1$, and we let $\mathbb{F}_q$ denote the finite field with q elements. The field $\mathbb{F}_q$ can also be viewed as a vector space of dimension n over $\mathbb{F}_2$. The map $\theta : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^2$, is $\mathbb{F}_2$-linear and is called the Frobenius automorphism. Its inverse is the $(n-1)$-fold composition $\theta^{n-1} = \theta \circ \cdots \circ \theta$. For convenience, we sometimes write $x^{[i]} \coloneqq \theta^i(x)$, for $i \in [0, n-1] \coloneqq \{0, \ldots, n-1\}$.

Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_q^n$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. We define the extension map

$$\begin{aligned} \mathrm{Ext}_{\boldsymbol{\beta}} : \quad \mathbb{F}_q^n \quad &\to \quad \mathbb{F}_2^{n \times n} \\ \boldsymbol{a} = (a_1, \ldots, a_n) &\mapsto \boldsymbol{A} = (\boldsymbol{\alpha}_1^\top, \ldots, \boldsymbol{\alpha}_n^\top) \end{aligned}$$

where, for all $1 \leq j \leq n$, the vector $\boldsymbol{\alpha}_j \in \mathbb{F}_2^n$ consists of coordinates of $a_j \in \mathbb{F}_q$ in the basis $\boldsymbol{\beta}$, *i.e.* $a_j = \sum_{i=1}^{n} \beta_i A_{i,j}$. In particular, for every $\boldsymbol{A} \in \mathbb{F}_2^{n\times n}$, we have $\mathrm{Ext}_{\boldsymbol{\beta}}(\boldsymbol{\beta}\boldsymbol{A}) = \boldsymbol{A}$.

The *rank* of $\boldsymbol{a} \in \mathbb{F}_q^n$, denoted $\mathrm{rk}(\boldsymbol{a})$, is defined as the rank over $\mathbb{F}_2$ of its extension matrix $\boldsymbol{A} = \mathrm{Ext}_{\boldsymbol{\beta}}(\boldsymbol{a})$. Notice that $\mathrm{rk}(\boldsymbol{a})$ does not depend on the choice of the basis $\boldsymbol{\beta}$. We also define the row space of $\boldsymbol{a} \in \mathbb{F}_q^n$ with respect to $\boldsymbol{\beta}$ as

$$\mathrm{RowSp}_{\boldsymbol{\beta}}(\boldsymbol{a}) \coloneqq \{\boldsymbol{x}\,\mathrm{Ext}_{\boldsymbol{\beta}}(\boldsymbol{a}), \boldsymbol{x} \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^n\,.$$

Similarly, the column space of $\boldsymbol{a} \in \mathbb{F}_q^n$ is $\mathrm{ColSp}_{\boldsymbol{\beta}}(\boldsymbol{a}) \coloneqq \{sum_{i=1}^{n} x_i a_i \mid \boldsymbol{x} \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_q$.

We let $\mathrm{Gr}(t, \mathbb{F}_2^n)$ denote the set of subspaces of $\mathbb{F}_2^n$ of dimension t, which contains $\begin{bmatrix} n \\ t \end{bmatrix}_2 \coloneqq \frac{(2^n-1)(2^{n-1}-1)\cdots(2^{n-t+1}-1)}{(2^t-1)(2^{t-1}-1)\cdots(2^1-1)}$ elements. Each subspace $\mathcal{V} \in \mathrm{Gr}(t, \mathbb{F}_2^n)$ can be represented by the unique reduced row echelon form (RREF) of any matrix $\boldsymbol{V} \in \mathbb{F}_2^{n\times n}$ whose row space generates $\mathcal{V}$. We know from [21, 27] that this representation can be computed efficiently (in time $\tilde{O}(nt(n-t))$). Recall that a matrix is in reduced row echelon form if the following holds:

- the index of the pivot (*i.e.* the first non-zero coefficient) of row i is strictly larger than the index of the pivot of row $i-1$;
- all pivots are ones;
- each pivot is the only non-zero entry in its column.

We finally define $\mathcal{P}_{t,n} \coloneqq \{\boldsymbol{P} \in \mathbb{F}_2^{n\times n} \mid \mathrm{rk}(\boldsymbol{P}) = t, \boldsymbol{P} \text{ is in RREF}\}$.

2.2 Rank metric codes

In this paper, we embed $\mathbb{F}_q^n$ with the *rank metric*: for $\boldsymbol{a} \in \mathbb{F}_q^n$, the weight of $\boldsymbol{a}$ is defined as $\|\boldsymbol{a}\| \coloneqq \mathrm{rk}(\boldsymbol{a})$. We consider $\mathbb{F}_q$-linear codes, *i.e.* $\mathbb{F}_q$-linear subspaces $\mathcal{C} \subseteq \mathbb{F}_q^n$. Notice that the field extension degree n is also the length of the code $\mathcal{C}$. The dimension of a code $\mathcal{C}$ is $k = \dim_{\mathbb{F}_q}(\mathcal{C})$, and its minimum (rank) distance is $d = \min_{\boldsymbol{c}\in\mathcal{C}\setminus\{\boldsymbol{0}\}} \|\boldsymbol{c}\|$. A generator matrix (resp. a parity-check matrix) for $\mathcal{C}$ is a matrix $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$ (resp. $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$) such that $\mathcal{C} = \{\boldsymbol{a}\boldsymbol{G}, \boldsymbol{a} \in \mathbb{F}_q^k\}$ (resp. $\boldsymbol{H}\boldsymbol{c}^\top = \boldsymbol{0}$ for every $\boldsymbol{c} \in \mathcal{C}$).

Let us define $\boldsymbol{\beta}^{[i]} \coloneqq (\beta_1^{[i]}, \ldots, \beta_n^{[i]}) \in \mathbb{F}_q^n$. Its Moore matrix is defined as

$$\mathrm{Moore}_n(\boldsymbol{\beta}) \coloneqq \begin{pmatrix} \boldsymbol{\beta}^{[0]} \\ \vdots \\ \boldsymbol{\beta}^{[n-1]} \end{pmatrix} \in \mathbb{F}_q^{n\times n}$$

and it is invertible over $\mathbb{F}_q$. Hence $(\boldsymbol{\beta}^{[0]}, \ldots, \boldsymbol{\beta}^{[n-1]})$ is a basis of $\mathbb{F}_q^n$.

Definition 1 (Gabidulin code [10, 13]). *Let $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ be an ordered basis of $\mathbb{F}_q/\mathbb{F}_2$. The* Gabidulin code *of dimension k with evaluation vector $\boldsymbol{g}$ is the subspace $\mathrm{Gab}_k(\boldsymbol{g}) \subseteq \mathbb{F}_q^n$ generated by the k first rows of $\mathrm{Moore}_n(\boldsymbol{g})$.*

Algorithm 1: $\mathsf{KeyGen}(1^\lambda)$

Input:
Output: a pair of public/private keys $(\boldsymbol{k}_{\text{pub}}, \boldsymbol{k}_{\text{priv}})$
1 Pick $\boldsymbol{k}_{\text{priv}} \leftarrow_{\$} \{\boldsymbol{x} \in \mathbb{F}_q^n, \|\boldsymbol{x}\| = w\}$
2 Compute $\boldsymbol{k}_{\text{pub}} \in \mathbb{F}_q^{n-k}$ such that ${\boldsymbol{k}_{\text{pub}}}^\top = \boldsymbol{H}{\boldsymbol{k}_{\text{priv}}}^\top$
3 Output $(\boldsymbol{k}_{\text{pub}}, \boldsymbol{k}_{\text{priv}}) \in \mathbb{F}_q^{n-k} \times \mathbb{F}_q^n$

Gabidulin codes are optimal codes with respect to the rank metric [10] and they can be efficiently decoded [13] up to $\lfloor \frac{n-k}{2} \rfloor$ errors. By definition, the submatrix consisting in the k first rows of $\text{Moore}_n(\boldsymbol{g})$ is a generator matrix for $\text{Gab}_k(\boldsymbol{g})$. It is also clear that $\text{Gab}_k(\boldsymbol{g}) \subseteq \text{Gab}_{k+1}(\boldsymbol{g})$ for every $1 \leq k \leq n$, and we have $\text{Gab}_n(\boldsymbol{g}) = \mathbb{F}_q^n$. Hence, one can propose the following definition.

Definition 2 ($\boldsymbol{g}$-degree). *Let $\boldsymbol{x} \in \mathbb{F}_q^n$ and $\boldsymbol{X} = \text{Ext}_{\boldsymbol{g}}(\boldsymbol{x})$. The* $\boldsymbol{g}$-degree of $\boldsymbol{x}$, *denoted* $\deg_{\boldsymbol{g}}(\boldsymbol{x})$, *is the unique integer $\ell \in [0, n-1]$ such that $\boldsymbol{x} \in \text{Gab}_{\ell+1}(\boldsymbol{g}) \setminus \text{Gab}_\ell(\boldsymbol{g})$. Similarly, one defines the $\boldsymbol{g}$-degree of $\boldsymbol{X}$ as $\deg_{\boldsymbol{g}}(\boldsymbol{X}) = \deg_{\boldsymbol{g}}(\boldsymbol{x})$.*

In other words, a vector $\boldsymbol{x} \in \mathbb{F}_q^n$ of $\boldsymbol{g}$-degree ℓ can be written

$$\boldsymbol{x} = \lambda_\ell \boldsymbol{g}^{[\ell]} + \sum_{j=0}^{\ell-1} \lambda_j \boldsymbol{g}^{[j]}$$

for some non-zero $\lambda_\ell \in \mathbb{F}_q \setminus \{0\}$ and some ℓ-tuple $(\lambda_{\ell-1}, \ldots, \lambda_0) \in \mathbb{F}_q^\ell$.

Finally, the dual code $\text{Gab}_k(\boldsymbol{g})^\perp = \{\boldsymbol{a} \in \mathbb{F}_q^n \mid \forall \boldsymbol{c} \in \text{Gab}_k(\boldsymbol{g}), \sum_{i=1}^n a_i c_i = 0\}$ is also a Gabidulin code $\text{Gab}_{n-k}(\boldsymbol{h})$ for some basis $\boldsymbol{h} \in \mathbb{F}_q^n$ that can be efficiently computed from $\boldsymbol{g}$. In other words, there exists a parity-check matrix for $\text{Gab}_k(\boldsymbol{g})$ consisting in the $(n-k)$ first rows of a Moore matrix associated to some $\boldsymbol{h} \in \mathbb{F}_q^n$, see *e.g.* [13].

3 The encryption scheme

System parameters. Integers $1 \leq w, k, \ell, t \leq n$ are public parameters and specified according to the desired security level (see Section 4). We set $q = 2^n$, and we also make public a basis $\boldsymbol{g}$ of $\mathbb{F}_q/\mathbb{F}_2$. We let $\boldsymbol{H}$ denote a *fixed* parity-check matrix of $\text{Gab}_k(\boldsymbol{g})$.

Key generation. Alice picks uniformly at random a vector $\boldsymbol{k}_{\text{priv}} \in \mathbb{F}_q^n$ of rank w. As explained in Algorithm 1, the public key is the syndrome of $\boldsymbol{k}_{\text{priv}}$ with respect to the parity-check matrix $\boldsymbol{H}$ of $\text{Gab}_k(\boldsymbol{g})$, and the private key is $\boldsymbol{k}_{\text{priv}}$.

Encryption. The set of plaintexts is $\mathcal{P}_{t,n}$, as defined in Section 2.1. Encryption is presented in Algorithm 2. Notice that in steps 3-4, the computation of $\boldsymbol{p}'$ should be understood as a the generation of a uniform random vector such that $\text{RowSp}_{\boldsymbol{g}}(\boldsymbol{p}')$ is the rowspan of $\boldsymbol{P}$.

Algorithm 2: $\mathsf{Encrypt}(\boldsymbol{k}_{\mathrm{pub}}, \boldsymbol{P})$

Input: public key $\boldsymbol{k}_{\mathrm{pub}} \in \mathbb{F}_q^{n-k}$, plaintext $\boldsymbol{P} \in \mathcal{P}_{t,n}$
Output: ciphertext $\boldsymbol{u} \in \mathbb{F}_q^{n-k}$

Compute any $\boldsymbol{y} \in \mathbb{F}_q^n$ such that $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$
Pick $\boldsymbol{T} \leftarrow_{\$} \{\boldsymbol{M} \in \mathbb{F}_2^{n\times n}, \deg_{\boldsymbol{g}}(\boldsymbol{M}) = \ell\}$
Pick $\boldsymbol{S} \leftarrow_{\$} \{\boldsymbol{M} \in \mathbb{F}_2^{n\times n}, \mathrm{rk}(\boldsymbol{M}) = n\}$
Compute $\boldsymbol{p}' = \boldsymbol{g}\boldsymbol{S}\boldsymbol{P} \in \mathbb{F}_q^n$
Output $\boldsymbol{u} \in \mathbb{F}_q^{n-k}$ such that $\boldsymbol{u}^\top = \boldsymbol{H}(\boldsymbol{y}\boldsymbol{T} + \boldsymbol{p}')^\top$

Algorithm 3: $\mathsf{Decrypt}(\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{u})$

Input: private key $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$, ciphertext $\boldsymbol{u} \in \mathbb{F}_q^{n-k}$
Output: plaintext $\hat{\boldsymbol{P}} \in \mathcal{P}_{t,n}$, or failure

Compute a solution $\boldsymbol{x} \in \mathbb{F}_q^n$ to the linear system $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{u}^\top$.
Compute $\boldsymbol{z} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) \in \mathbb{F}_q^n$.
Decode $\boldsymbol{z}$ as a corrupted $\mathrm{Gab}_{k+\ell+w}(\boldsymbol{g})$-codeword. If success, one gets an error vector $\boldsymbol{a} \in \mathbb{F}_q^n$ of rank $\leq t$.
If $\mathrm{rk}(\boldsymbol{a}) < t$, output failure.
Otherwise, output $\hat{\boldsymbol{P}} = \mathtt{RREF}(\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{a}))$.

Decryption. We present in Algorithm 3 a decryption algorithm which may fail with negligible probability. The failure rate is devoted to be cryptographically small, and is bounded in Section 5.2. We also make use of an $\mathbb{F}_2$-linear map $V_{\boldsymbol{k}_{\mathrm{priv}}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{k}_{\mathrm{priv}}) = \boldsymbol{0}$. This map can be efficiently computed from the knowledge of the private key $\boldsymbol{k}_{\mathrm{priv}}$. Mathematical properties of this map are given in Section 5.1

In Algorithm 3, one needs to decode Gabidulin codes up to half their minimum distance, *i.e.* to decode errors of rank less than $\lfloor \frac{n-\dim \mathrm{Gab}}{2} \rfloor$. Many such algorithms can be found in the literature since the seminal work of Gabidulin [13]. Some of them are based on solving a so-called *key equation*, such as [14,24–26,29] and others use interpolation, for instance [19]. Fastest ones run in $\mathcal{O}(n^2)$ operations over $\mathbb{F}_q$.

4 Parameters

In Table 1, we propose three sets of parameters for RAMESSES as a KEM, according to the desired level of security. Table 2 proposes a set of parameters for RAMESSES as a PKE. There are generic transformations from PKEs to KEMs, widely used in the NIST competition. Note that the decryption failure can be finely tuned as is explained in Section 5.2. One can notice that the post-quantum security is much larger than half the classical one, which is unusual in code-based systems. Indeed the best current attacks against RAMESSES do not use enumeration techniques, which would benefit from the use of Grover

n	k	w	ℓ	t	classical security (bits)	post-quantum security (bits)	public key/ciphertext size (bytes)	private key size (bytes)
64	32	19	3	5	141 (≥ 128)	126	256	152
80	40	23	3	7	202 (≥ 192)	158	400	230
96	48	27	3	9	265 (≥ 256)	190	576	324

Table 1. Sets of parameters for RAMESSES as a KEM, with different levels of security. The security is estimated according to the current state of the art of algebraic attacks; the linear algebra constant is set to $\omega = \log_2(7) \simeq 2.807$. Decryption failure rates are respectively bounded by 2^{-40}, 2^{-50} and 2^{-60}.

n	k	w	ℓ	t	classical security (bits)	post-quantum security (bits)	public key/ciphertext size (bytes)	private key size (bytes)
164	116	27	3	9	≥ 256	≥ 256	984	554

Table 2. A set of parameters for RAMESSES as a PKE, with decryption failure rate $\leq 2^{-128}$. The security is estimated according to the current state of the art of algebraic attacks; the linear algebra constant is set to $\omega = \log_2(7) \simeq 2.807$.

algorithm, but Groebner bases algebraic techniques for which there is no known efficient quantum algorithmic speedup, as explained in Section 5.4.

Claimed security. The claimed security is computed according to known attacks reported in Section 5.4.

Public key size. The public key consists in a vector $\boldsymbol{k}_{\text{pub}} \in \mathbb{F}_q^{n-k}$. Thus, its size is $(n-k)n$ bits, or $\frac{(n-k)n}{8}$ bytes.

Private key size. For the private key $\boldsymbol{k}_{\text{priv}} \in \mathbb{F}_q^n$, Alice actually needs to store only the map $V_{\boldsymbol{k}_{\text{priv}}}$. From Section 5.1, this map is a monic polynomial over $\mathbb{F}_q$ of degree w. Hence only w coefficients over $\mathbb{F}_q$ actually need to be stored, the size of the private key is thus wn bits, or $\frac{wn}{8}$ bytes.

Ciphertext size. The ciphertext is a vector $\boldsymbol{u} \in \mathbb{F}_q^{n-k}$, hence its size is $(n-k)n$ bits, *i.e.* $\frac{(n-k)n}{8}$ bytes.

5 Analysis

5.1 Mathematical background

Gabidulin codes can be interpreted in the context of skew polynomial rings. Recall that θ represents the Frobenius automorphism $x \mapsto x^2$. The *skew polynomial ring* $\mathbb{F}_q[X;\theta]$, originally studied by Øre [22, 23], is the ring of univariate

polynomials defined by the non-commutative multiplicative rule

$$X \cdot a = \theta(a) \cdot X, \qquad a \in \mathbb{F}_q \,.$$

In our context, skew polynomials are also called linearized polynomials. One can define the evaluation of a skew polynomial $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}_q[X;\theta]$ at $x \in \mathbb{F}_q$ as follows:

$$P(x) \coloneqq \sum_{i=0}^{d} a_i \theta^i(x) = \sum_{i=0}^{d} a_i x^{2^i} \,.$$

The evaluation vector of P at $\boldsymbol{x} \in \mathbb{F}_q^n$ is defined as

$$P(\boldsymbol{x}) \coloneqq (P(x_1), \ldots, P(x_n)) \in \mathbb{F}_q^n \,.$$

Thus, the rows of $\mathrm{Moore}_n(\boldsymbol{g})$ can be seen as the evaluation vectors over $\boldsymbol{g}$, of the sequence of degree-ordered skew monomials $1, X, \ldots, X^{n-1}$. As a consequence, one can view Gabidulin codes as analogues of Reed-Solomon codes for skew polynomial rings:

$$\mathrm{Gab}_k(\boldsymbol{g}) = \{P(\boldsymbol{g}) \mid P \in \mathbb{F}_q[X;\theta], \deg P < k\} \,.$$

For $\boldsymbol{x} \in \mathbb{F}_q^n$, the polynomial $P(X) \in \mathbb{F}_q[X;\theta]$ of minimum degree such that $P(\boldsymbol{g}) = \boldsymbol{x}$ is the *$\boldsymbol{g}$-interpolating polynomial of $\boldsymbol{x}$* and is denoted $L_{\boldsymbol{x}}(X)$. By definition $\deg(L_{\boldsymbol{x}}) = \deg_{\boldsymbol{g}}(\boldsymbol{x})$.

Finally, given $\boldsymbol{e} \in \mathbb{F}_q^n$, the set of polynomials $P \in \mathbb{F}_q[X;\theta]$ satisfying $P(\boldsymbol{e}) = \boldsymbol{0}$ is a left-ideal $I_{\boldsymbol{e}}$ of $\mathbb{F}_q[X;\theta]$. Since skew polynomial rings are principal ideal domains, we can define the *minimum vanishing polynomial* $V_{\boldsymbol{e}}(X) \in \mathbb{F}_q[X;\theta]$ of $\boldsymbol{e}$ as the unique monic skew polynomial which generates $I_{\boldsymbol{e}}$. Notice that $\deg(V_{\boldsymbol{e}}) = \mathrm{rk}(\boldsymbol{e}) \geq n - \deg_{\boldsymbol{g}}(\boldsymbol{e})$.

The following lemma will be helpful for the analysis of the scheme consistency.

Lemma 1. *Let $P(X) \in \mathbb{F}_q[X;\theta]$ and $\boldsymbol{a} \in \mathbb{F}_q^n$. Then we have $\mathrm{RowSp}_{\boldsymbol{g}}(P(\boldsymbol{a})) \subseteq \mathrm{RowSp}_{\boldsymbol{g}}(\boldsymbol{a})$. Moreover, if $\mathrm{RowSp}_{\boldsymbol{g}}(P(\boldsymbol{a})) \neq \mathrm{RowSp}_{\boldsymbol{g}}(\boldsymbol{a})$, then there exists a non-zero $x = \sum_{i=1}^{n} \lambda_i a_i \in \mathrm{ColSp}(\boldsymbol{a})$ such that $P(x) = 0$.*

Proof. Let $\boldsymbol{B} \in \mathbb{F}_2^{n \times n}$ satisfy $\mathrm{RowSp}_{\boldsymbol{g}}(\boldsymbol{a}) = \{\boldsymbol{x} \in \mathbb{F}_2^n, \boldsymbol{x}\boldsymbol{B} = \boldsymbol{0}\}$. In particular, one can see that $\boldsymbol{a}\boldsymbol{B} = \boldsymbol{0}$. Hence, by $\mathbb{F}_2$-linearity $P(\boldsymbol{a})\boldsymbol{B} = P(\boldsymbol{a}\boldsymbol{B}) = \boldsymbol{0}$. Thus, every $\boldsymbol{y} \in \mathrm{RowSp}_{\boldsymbol{g}}(P(\boldsymbol{a}))$ satisfies $\boldsymbol{y}\boldsymbol{B} = \boldsymbol{0}$, leading to $\mathrm{RowSp}_{\boldsymbol{g}}(P(\boldsymbol{a})) \subseteq \mathrm{RowSp}_{\boldsymbol{g}}(\boldsymbol{a})$.

Assume now that $\mathrm{RowSp}_{\boldsymbol{g}}(P(\boldsymbol{a})) \neq \mathrm{RowSp}_{\boldsymbol{g}}(\boldsymbol{a})$. It implies that $\dim \mathrm{ColSp}(P(\boldsymbol{a})) < \dim \mathrm{ColSp}(\boldsymbol{a})$. Let $(a_{i_j})_{1 \leq j \leq k} \subset \mathbb{F}_q$ be an ordered basis of $\mathrm{ColSp}(\boldsymbol{a}) \subseteq \mathbb{F}_q$ over $\mathbb{F}_2$. Then there must exists a non-zero $(\lambda_j) \in \mathbb{F}_2^k$ such that $\sum_{j=1}^{k} \lambda_j P(a_{i_j}) = 0$, otherwise we would have $\dim \mathrm{ColSp}(P(\boldsymbol{a})) = k$. If we set $x = \sum_j \lambda_j a_{i_j} \in \mathbb{F}_q \setminus \{0\}$, then we get $P(x) = 0$ by $\mathbb{F}_2$-linearity. □

5.2 Consistency

In this section we characterize the output of algorithm Decrypt described in Section 3. As input, Decrypt receives a vector $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$ of rank w and a vector $\boldsymbol{u} \in \mathbb{F}_q^{n-k}$ such that $\boldsymbol{u} = \boldsymbol{H}(\boldsymbol{y}\boldsymbol{T} + \boldsymbol{p}')^\top$, where

– vector $\boldsymbol{y} \in \mathbb{F}_q^n$ satisfies $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{H}\boldsymbol{k}_{\text{priv}}{}^\top$,
– matrix $\boldsymbol{T} \in \mathbb{F}_2^{n\times n}$ has $\boldsymbol{g}$-degree ℓ,
– vector $\boldsymbol{p}' = \boldsymbol{g}\boldsymbol{S}\boldsymbol{P} \in \mathbb{F}_q^n$ has rank $t \coloneqq \lfloor \frac{n-k-\ell-w}{2} \rfloor$.

First, notice that $\boldsymbol{y} = \boldsymbol{k}_{\text{priv}} + \boldsymbol{c}$ for some $\boldsymbol{c} \in \text{Gab}_k(\boldsymbol{g})$. In the first step of Algorithm 3, a vector $\boldsymbol{x} \in \mathbb{F}_q^n$ solution to $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{u}^\top$ is computed. One can see that the set S of such solutions is

$$S = \{\boldsymbol{y}\boldsymbol{T} + \boldsymbol{p}' + \boldsymbol{c}' \mid \boldsymbol{c}' \in \text{Gab}_k(\boldsymbol{g})\} \subseteq \mathbb{F}_q^n \,.$$

Therefore, in step 2 of Algorithm 3, we have

$$\begin{aligned} \boldsymbol{z} = V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{x}) &= V_{\boldsymbol{k}_{\text{priv}}}((\boldsymbol{c}+\boldsymbol{k}_{\text{priv}})\boldsymbol{T} + \boldsymbol{p}' + \boldsymbol{c}') \\ &= V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{c}' + \boldsymbol{c}\boldsymbol{T}) + \underbrace{V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{k}_{\text{priv}})}_{\boldsymbol{0}}\boldsymbol{T} + V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{p}') \,. \end{aligned}$$

We notably used the $\mathbb{F}_2$-linearity of $V_{\boldsymbol{k}_{\text{priv}}}$. Also recall that, for any $\boldsymbol{a} \in \mathbb{F}_q^n$, $L_{\boldsymbol{a}}(X)$ denotes the $\boldsymbol{g}$-interpolating polynomial of $\boldsymbol{a}$. Then we get:

$$\boldsymbol{z} = (V_{\boldsymbol{k}_{\text{priv}}} \cdot (L_{\boldsymbol{c}'} + L_{\boldsymbol{c}\boldsymbol{T}}))(\boldsymbol{g}) + V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{p}') \,.$$

Moreover, $L_{\boldsymbol{c}\boldsymbol{T}} = L_{\boldsymbol{c}} \cdot L_{\boldsymbol{g}\boldsymbol{T}}$ yields $\deg(L_{\boldsymbol{c}\boldsymbol{T}}) \leq k - 1 + \ell$ since $\deg_{\boldsymbol{g}}(\boldsymbol{T}) = \ell$. Therefore, the polynomial $V_{\boldsymbol{k}_{\text{priv}}} \cdot (L_{\boldsymbol{c}'} + L_{\boldsymbol{c}\boldsymbol{T}})$ has degree at most $\deg(V_{\boldsymbol{k}_{\text{priv}}}) + \max\{\deg(L_{\boldsymbol{c}'}), \deg(L_{\boldsymbol{c}\boldsymbol{T}})\} \leq w + k - 1 + \ell$.

We also know that $\text{rk}(V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{p}')) \leq \text{rk}(\boldsymbol{p}') = \text{rk}(\boldsymbol{P}) = t = \lfloor \frac{n-k-\ell-w}{2} \rfloor$. Hence, in third step of Algorithm 3, any decoding algorithm for $\text{Gab}_{k+w+\ell}(\boldsymbol{g})$ that decodes errors of rank at most t will retrieve $V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{p}')$ from $\boldsymbol{z}$. Finally, Algorithm 3 outputs a matrix $\hat{\boldsymbol{P}} \in \mathcal{P}_{t,n}$ such that $\text{RowSp}(\hat{\boldsymbol{P}}) = \text{RowSp}_{\boldsymbol{g}}(V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{p}'))$.

As a consequence, decryption fails whenever $\text{RowSp}_{\boldsymbol{g}}(V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{p}')) \neq \text{RowSp}(\boldsymbol{P})$, where $\boldsymbol{P}$ is the original plaintext. First notice that $\text{RowSp}(\boldsymbol{P}) = \text{RowSp}_{\boldsymbol{g}}(\boldsymbol{p}')$. Then, Lemma 1 shows that if decryption fails, then there exists a non-zero $x \in \text{ColSp}(\boldsymbol{p}')$ such that $V_{\boldsymbol{k}_{\text{priv}}}(x) = 0$. Let us now recall that the set of zeroes of $V_{\boldsymbol{k}_{\text{priv}}}$ is exactly $\text{ColSp}(\boldsymbol{k}_{\text{priv}})$. Hence we get the following result.

Lemma 2. *Let $\boldsymbol{P} \in \mathcal{P}_{t,n}$. If, on input $(\boldsymbol{k}_{\text{priv}}, \mathsf{Encrypt}(\boldsymbol{k}_{\text{pub}}, \boldsymbol{P}))$ where $(\boldsymbol{k}_{\text{pub}}, \boldsymbol{k}_{\text{priv}}) \leftarrow \mathsf{KeyGen}$, algorithm $\mathsf{Decrypt}$ does not output $\boldsymbol{P}$, then matrix $\boldsymbol{S}$ has been chosen at step 4, such that $\text{ColSp}(\boldsymbol{k}_{\text{priv}}) \cap \text{ColSp}(\boldsymbol{S}\boldsymbol{P})) \neq \{0\}$.*

One can now estimate the probability of failure of $\mathsf{Decrypt}$.

Lemma 3. *Let $(\boldsymbol{k}_{\text{pub}}, \boldsymbol{k}_{\text{priv}}) \leftarrow \mathsf{KeyGen}$ be any pair of keys generated by KeyGen, on public parameters n, w, t. Then, for every $\boldsymbol{P} \in \mathcal{P}_{t,n}$,*

$$\mathbb{P}_{\boldsymbol{S},\boldsymbol{T},\boldsymbol{y}}\left(\hat{\boldsymbol{P}} \neq \boldsymbol{P} \;\middle|\; \begin{array}{l} \boldsymbol{u} \leftarrow \mathsf{Encrypt}(\boldsymbol{k}_{\text{pub}}, \boldsymbol{P}) \\ \hat{\boldsymbol{P}} \leftarrow \mathsf{Decrypt}(\boldsymbol{k}_{\text{priv}}, \boldsymbol{u}) \end{array}\right) \leq 2^{-(n-t-w)} \,.$$

Proof. Using Lemma 2, we have

$$\mathbb{P}_{\boldsymbol{S},\boldsymbol{T},\boldsymbol{y}}\left(\hat{\boldsymbol{P}} \neq \boldsymbol{P} \;\middle|\; \begin{array}{l} \boldsymbol{u} \leftarrow \mathsf{Encrypt}(\boldsymbol{k}_{\mathrm{pub}}, \boldsymbol{P}) \\ \hat{\boldsymbol{P}} \leftarrow \mathsf{Decrypt}(\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{u}) \end{array}\right) = \mathbb{P}_{\boldsymbol{S}}\big(\operatorname{ColSp}(\boldsymbol{k}_{\mathrm{priv}}) \cap \operatorname{ColSp}(\boldsymbol{SP}) \neq \{0\}\big).$$

It is easy to check that the probability that a t-dimensional random subspace of $\mathbb{F}_2^n$ intersects non-trivially a fixed subspace of dimension w is bounded by $\frac{(2^t-1)(2^w-1)}{2^n-1} \leq 2^{t+w-n}$. This concludes the proof. □

5.3 Security proof

Let us first introduce two problems to which the security of RAMESSES can be reduced. Problem 1 is an ad hoc problem. The search version of Problem 2 corresponds to decoding errors of rank w in a Gabidulin code; this problem is believed hard for w between $\frac{n-k}{2}$ and $n-k$, and a improvement in solving this problem would be significant in coding theory.

*Problem 1 (Syndrome correlation for Gabidulin codes (*CorGab*)).*
Let $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ be a fixed parity-check matrix of $\mathrm{Gab}_k(\boldsymbol{g})$, and $1 \leq \ell \leq n-1$.

- **Input:** access to distributions
  1. $\mathcal{D}_1$: $(\boldsymbol{H}\boldsymbol{x}^\top, \boldsymbol{H}\boldsymbol{T}^\top\boldsymbol{x}^\top)$, where $\boldsymbol{x} \leftarrow_{\$} \mathbb{F}_q^n$ and $\boldsymbol{T} \leftarrow_{\$} \mathcal{M}_\ell$,
  2. $\mathcal{D}_2$: $(\boldsymbol{H}\boldsymbol{x}^\top, \boldsymbol{r}^\top)$, where $\boldsymbol{x} \leftarrow_{\$} \mathbb{F}_q^n$ and $\boldsymbol{r} \leftarrow_{\$} \mathbb{F}_q^{n-k}$.
- **Goal:** distinguish between $\mathcal{D}_1$ and $\mathcal{D}_2$.

Problem 2 (Syndrome decoding for Gabidulin codes, Gab-SD*).*
Let $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ be a fixed parity-check matrix of $\mathrm{Gab}_k(\boldsymbol{g})$, and $\frac{n-k}{2} < w < n-k$.

- **Input:** access to distributions
  1. $\mathcal{D}_1$: $\boldsymbol{H}\boldsymbol{x}^\top$, where $\boldsymbol{x} \leftarrow_{\$} S_w$,
  2. $\mathcal{D}_2$: $\boldsymbol{r}^\top$, where $\boldsymbol{r} \leftarrow_{\$} \mathbb{F}_q^{n-k}$.
- **Goal:** distinguish between $\mathcal{D}_1$ and $\mathcal{D}_2$.

We now shortly show the indistinguishability under chosen plaintext attacks (IND-CPA) of RAMESSES with the following sequence of games.

Game 0. The real scheme with plaintext $\boldsymbol{P}$.

Game 1. We modify **Game 0** as follows. In the key generation, the vector $\boldsymbol{k}_{\mathrm{priv}}$ is now picked uniformly at random in $\mathbb{F}_q^n$, without any rank constraint.

Game 2. We modify **Game 1** as follows. In the encryption algorithm, $\boldsymbol{H}(\boldsymbol{y}\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}_{(1)})^\top$ is replaced by $\boldsymbol{r} + \boldsymbol{H}(\boldsymbol{g}\boldsymbol{S}\boldsymbol{P}_{(1)})^\top$, where $\boldsymbol{r}$ is generated uniformly at random in $\mathbb{F}_q^{n-k}$.

Game 3. We modify **Game 2** as follows. The plaintext $\boldsymbol{P}_{(1)}$ is replaced by the plaintext $\boldsymbol{P}_{(2)}$.

Game 4. This game is identical to **Game 1**, except that the plaintext is $\boldsymbol{P}_{(1)}$ is replaced by the plaintext $\boldsymbol{P}_{(2)}$.

Game 5. The real scheme with plaintext $\boldsymbol{P}_{(2)}$.

One can then prove that the advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathbf{Dist}}$ for an adversary $\mathcal{A}$ to distinguishing the encryption of $\boldsymbol{P}_{(1)}$ and $\boldsymbol{P}_{(2)}$ satisfies:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathbf{Dist}} \leq 2(\mathrm{Adv}_{\mathcal{A}}^{\textsc{Gab-sd}} + \mathrm{Adv}_{\mathcal{A}}^{\textsc{CorGab}}) .$$

Roughly speaking, one actually mimics the security proof given in [3]. The $2\mathrm{Adv}_{\mathcal{A}}^{\textsc{Gab-sd}}$ term comes from transitions between games 0 and 1, and games 4 and 5, whereas transitions between games 1 and 2, and games 3 and 4 yield the $2\mathrm{Adv}_{\mathcal{A}}^{\textsc{CorGab}}$ term. Games 2 and 3 are information-theoretically indistinguishable since $\boldsymbol{r}$ is random.

5.4 Existing attacks

In the following, we denote by λ the desired security parameter, *i.e.*, any attack against the cryptosystem must cost at least 2^λ operations over $\mathbb{F}_2$.

Exhaustive search attacks. In order to avoid attacks by exhaustive search, one has the following constraints on the parameters.

1. $|\mathcal{P}_{t,n}| = \begin{bmatrix} n \\ t \end{bmatrix}_2 \geq 2^\lambda$, satisfied when $t(n-t) \geq \lambda$.
2. $|\{\boldsymbol{k}_{\mathrm{priv}}\}| \geq \begin{bmatrix} n \\ w \end{bmatrix}_2 \geq 2^\lambda$, satisfied when $w(n-w) \geq \lambda$.
3. $|\mathcal{M}_\ell| \geq 2^\lambda$, satisfied when $(\ell+1)n \geq \lambda$.

Attack by decoding beyond the unique decoding radius of Gabidulin codes. Let $\boldsymbol{e}' \in \mathbb{F}_q^n$ be *any* solution of $\boldsymbol{H}\boldsymbol{e}'^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$ of rank $\leq w$. From the consistency analysis one can see that $\boldsymbol{e}'$ can be used as an alternate private key in the Decrypt algorithm. The computation of such a vector $\boldsymbol{e}'$ actually corresponds to the search version of Gab-SD problem.

This problem is easy for $w \leq \lfloor \frac{n-k}{2} \rfloor$ (it corresponds to half-minimum-distance decoding) and for $w \geq n-k$ (equivalent to interpolation for linearized polynomials). For our concern, we have $\lfloor \frac{n-k}{2} \rfloor < w < n-k$, and we believe that the search version of Gab-SD is hard in this range of parameters.

A solution consists in enumerating vector spaces of dimension slightly higher than w, checking whether they guessed correctly a large part of the solution space, and in such case, interpolating the solution. Roughly speaking, the number of valid choices for the subspace is large, but the complexity of finding one remains exponential in the code length. Precisely, in our settings ($m = n$, and $n-k$ even) the number of vector spaces to test before finding one solution is on average

$$\mathcal{N}_{Class-\textsc{Gab-sd}} \approx 0.3 \cdot 2^{\delta(n+k-2\delta)} ,$$

where $\delta \coloneqq w - \lfloor \frac{n-k}{2} \rfloor > 0$. This quantity is used as a bound for the complexity of solving Gab-SD. By using a straightforward Grover algorithm, we obtain that the number of iterations to be completed on a quantum computer is roughly

$$\mathcal{N}_{Quant-\textsc{Gab-sd}} \approx 0.55 \cdot 2^{\frac{\delta}{2}(n+k-2\delta)} .$$

Attack via *a reduction to a quadratic system over* $\mathbb{F}_2$. Given a vector $\boldsymbol{e} \in \mathbb{F}_q^n$ with $\mathrm{rk}(\boldsymbol{e}) = w$, any solution $\boldsymbol{y} \in \mathbb{F}_q^n$ to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{H}\boldsymbol{e}^\top$ can be written as $\boldsymbol{y} = \boldsymbol{c}+\boldsymbol{e}$ for some $\boldsymbol{c} \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$. Therefore, $\boldsymbol{y}$ satisfies

$$V_{\boldsymbol{e}}(\boldsymbol{y}) = (V_{\boldsymbol{e}} \cdot U)(\boldsymbol{g})\,, \tag{1}$$

where $U(X) = \sum_{i=0}^{k+\ell-1} u_i X^i \in \mathbb{F}_q[X, \theta]$. Hence, an attack would consist in searching for $V_{\boldsymbol{e}}$ and U in the previous equation, for some fixed $\boldsymbol{y}$ solution to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$.

Equation (1) can be turned into a quadratic system over $\mathbb{F}_2$ (see Appendix A for details). Using results of Bardet *et al.* [7], the solving complexity would be in $\mathcal{O}(2^{0.561\,n^2})$, which remains much larger than the complexity of the previous attack.[3]

Attack via *a reduction to a* MinRank *instance.* The recovery of a representative $\boldsymbol{p}' = \boldsymbol{g}\boldsymbol{S}\boldsymbol{P} \in \mathbb{F}_q^n$ of the plaintext $\boldsymbol{P}$, given only a ciphertext $\boldsymbol{u}$ and $\boldsymbol{k}_{\mathrm{priv}}$, can be modeled as follows. First, one computes (i) any solution $\boldsymbol{x} \in \mathbb{F}_q^n$ of $\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{u}^\top$, and (ii) any solution $\boldsymbol{y} \in \mathbb{F}_q^n$ to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$. Due to the form of the ciphertext, this leads us to

$$\boldsymbol{x} - \boldsymbol{y}\boldsymbol{T} - \boldsymbol{c} = \boldsymbol{p}'\,, \tag{2}$$

where $\boldsymbol{c} \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$ and $\boldsymbol{T} \in \mathbb{F}_2^{n\times n}$ are unknown to the attacker. Notice that $\boldsymbol{T}$ lies in a $\mathbb{F}_2$-vector space of dimension $(\ell+1)n$, since $\boldsymbol{g}\boldsymbol{T} \in \mathrm{Gab}_{\ell+1}(\boldsymbol{g})$. Two kinds of attacks can then be mounted to solve (2).

First, Equation (2) can be written $\boldsymbol{x} = (\boldsymbol{c} + \boldsymbol{y}\boldsymbol{T}) + \boldsymbol{p}'$, which means that the problem can be rephrased as decoding an error $\boldsymbol{p}'$ of rank t in the underlying code

$$\mathcal{D} \coloneqq \mathrm{Gab}_{k+\ell}(\boldsymbol{g}) + \mathrm{span}_{\mathbb{F}_2}\big(\{\boldsymbol{y}\boldsymbol{T} \mid \boldsymbol{T} \in \mathcal{M}_\ell\}\big)\,.$$

Notice that $\mathcal{D} \subseteq \mathbb{F}_q^n$ is an $\mathbb{F}_2$-linear code of $\mathbb{F}_2$-dimension at most $(k+2\ell+1)n$. One can then write $\boldsymbol{y}\boldsymbol{T} = L_{\boldsymbol{y}}(\boldsymbol{g}\boldsymbol{T})$, which yields $\mathcal{D} = \mathrm{Gab}_{k+\ell}(\boldsymbol{g}) + L_{\boldsymbol{y}}(\mathrm{Gab}_{\ell+1}(\boldsymbol{g}))$. A straightforward decoding approach would lead to an attack in time roughly 2^{kr}. One could also try to decode in the smallest $\mathbb{F}_q$-linear code containing $\mathcal{D}$, and use the additional structure provided by the $\mathbb{F}_q$-linearity. This structure has been widely employed in the recent improvements, see [6]. However, it is unlikely that the $\mathbb{F}_q$-dimension of $\mathrm{span}_{\mathbb{F}_q}(\mathcal{D}) = \mathrm{Gab}_{k+\ell}(\boldsymbol{g}) + \mathrm{span}_{\mathbb{F}_q}(L_{\boldsymbol{y}}(\mathrm{Gab}_{\ell+1}(\boldsymbol{g})))$ is small, since the $\mathbb{F}_2$-endomorphism of $\mathbb{F}_q[X, \theta]$ defined by $P \mapsto L_{\boldsymbol{y}}P$ is not $\mathbb{F}_q$-linear.

Second, one can see Equation (2) as an instance of MinRank, a problem formally introduced by Courtois in [9] after the cryptanalysis of HFE [17].

*Problem 3 (*MinRank *search problem).* Let $\mathbb{K}$ be a field.

– **Input:** $\boldsymbol{M}_0, \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{K}^{N\times n}$ and an integer t.

[3] However, notice that the system to be solved in [7] is assumed random, and such that no specialization of variables can be made. This is unlikely the case for our system, but it requires a finer analysis — which is not the scope of this paper — to understand whether improvements can be made in order to solve the system.

– **Goal:** Find $(x_1, \ldots, x_K) \in \mathbb{K}^K$ such that $\mathrm{rk}_{\mathbb{K}}(\boldsymbol{M}_0 - \sum_{i=1}^{K} x_i \boldsymbol{M}_i) \leq t$.

Let us denote by $\{\boldsymbol{T}_1, \ldots, \boldsymbol{T}_{n(\ell+1)}\} \subseteq \mathbb{F}_2^{n \times n}$ an $\mathbb{F}_2$-basis of $\mathrm{Gab}_{\ell+1}(\boldsymbol{g})$, the smallest vector space containing $\mathcal{M}_\ell$. Similarly, $\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{c})$ can be written in some basis $\{\boldsymbol{C}_1, \ldots, \boldsymbol{C}_{n(k+\ell)}\} \subseteq \mathbb{F}_2^{n \times n}$ of the $\mathbb{F}_2$-vector space of dimension $n(k+\ell)$ representing $\mathrm{Gab}_{k+\ell}(\boldsymbol{g})$. Applying $\mathrm{Ext}_{\boldsymbol{g}}$ to Equation (2), we get:

$$\boldsymbol{X} - \sum_{i=1}^{n(\ell+1)} t_i \boldsymbol{Y}\boldsymbol{T}_i - \sum_{i=1}^{n(k+\ell)} c_i \boldsymbol{C}_i = \boldsymbol{P}',$$

where $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{P}') = (\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{x}), \mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{y}), \mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{p}'))$. Since $\mathrm{rk}(\boldsymbol{P}') = t$, one gets an instance of the MinRank problem, with one "base matrix" $\boldsymbol{X} \in \mathbb{F}_2^{n \times n}$ and $K \coloneqq n(k+2\ell+1)$ "summand matrices" $\{\boldsymbol{Y}\boldsymbol{T}_1, \ldots, \boldsymbol{Y}\boldsymbol{T}_{n(\ell+1)}, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_{n(k+\ell)}\}$.

There exist several approaches to solve the MinRank problem. In [16], Goubin and Courtois gave an algorithm which finds a solution in expected time $\mathcal{O}(K^3 2^{t\lceil K/n \rceil})$. In 1999, Kipnis and Shamir [17] proposed a multivariate formulation of MinRank which can be solved by computing Groebner bases. Such computations can be run in time $\mathcal{O}(\binom{m+d-1}{d}^{\omega})$, where $2 \leq \omega < 3$ is the linear algebra constant, $m = t(n-t) + K$ and d is the *degree of regularity* of the system [18]. Faugère, Levy-dit-Vehel and Perret [11] proved that, in the Kapnis-Shamir formalism, any instance can be reduced to a simpler one if $\Delta \coloneqq K - (n-t)^2 > 0$. In our case, setting $w \geq \ell + 1$ ensures that $\Delta \leq 0$. Moreover, the authors proved that the degree of regularity is lower than what is expected for random systems, and it seems to be upper bounded by $t + 2$ heuristically. This heuristic was confirmed by Verbel *et al.* [28] for superdetermined instances, and by Bardet *et al.* [6] in the context of decoding low rank errors in random codes. Finally, the latter work also presents instances for which the solving degree decreases to $d = t$. We choose to consider this conservative setting; the running time for the computation of the associated Groebner basis is thus in

$$\mathcal{O}\left(\binom{t(n-t) + n(k+2\ell+1) + t - 1}{t}^{\omega} \right).$$

To sum up, the reduction to MinRank leads us to the following bounds on the parameters:

$$w \geq \ell + 1, \qquad \omega \cdot \log \tbinom{n(k+2\ell+t+1) - t^2 + t - 1}{t} \geq \lambda, \qquad t(k+2\ell+1) \geq \lambda\,.$$

6 Conclusion

The parameters we proposed for RAMESSES are deliberately aggressive so that to encourage research in studying the security of the encryption scheme. The simplicity and versatility of the scheme enables very efficient tuning for many sets of parameters, without making them grow prohibitively. Namely, the size of keys and ciphertexts grow linearly with the security parameter; this is usually not the case in other code-based encryption schemes where sizes (notably the public key size) grow quadratically with the security level, except for systems using structural tricks to reduce the key size.

References

1. C. Aguilar Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, A. Otmani, O. Ruatta, J.-P. Tillich, and G. Zémor. ROLLO: Rank-Ouroboros, LAKE and LOCKER. *Submission to the NIST Post-Quantum Standardization project*, 2017.
2. C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, A. Couvreur, J.-C. Deneuville, P. Gaborit, A. Hauteville, and G. Zémor. RQC: Rank Quasi-Cyclic. *Submission to the NIST Post-Quantum Standardization project*, 2017.
3. C. Aguilar Melchor, O. Blazy, J. Deneuville, P. Gaborit, and G. Zémor. Efficient encryption from random quasi-cyclic codes. *IEEE Trans. Information Theory*, 64(5):3927–3943, 2018.
4. D. Augot and M. Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. *Advanceds in Cryptology - EUROCRYPT 2003*, 2656:229–240, May 2003.
5. R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, D. Jao, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik. Supersingular Isogeny Key Encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2017.
6. M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J. Tillich. An Algebraic Attack on Rank Metric Code-Based Cryptosystems. *CoRR*, abs/1910.00810, 2019.
7. M. Bardet, J. Faugère, B. Salvy, and P. Spaenlehauer. On the complexity of solving quadratic Boolean systems. *J. Complexity*, 29(1):53–75, 2013.
8. F. Chabaud and J. Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology ASIACRYPT'96*, number 1163 in LNCS, pages 368–381, May 1996.
9. N. Courtois. Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 402–421. Springer, 2001.
10. P. Delsarte. Bilinear Forms over a Finite Field, with Applications to Coding Theory. *J. Comb. Theory, Ser. A*, 25(3):226–241, 1978.
11. J. Faugère, F. Levy-dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In D. A. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008.
12. C. Faure and P. Loidreau. A New Public-Key Cryptosystem Based on the Problem of Reconstructing p-Polynomials. In O. Ytrehus, editor, *Coding and Cryptography International Workshop*, pages 304–315. Springer, 2006.
13. E. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.
14. E. M. Gabidulin. A Fast Matrix Decoding Algorithm for Rank-Error-Correcting Codes. In G. D. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, editors, *Algebraic Coding, First French-Soviet Workshop, Paris, France, July 22-24, 1991, Proceedings*, volume 573 of *Lecture Notes in Computer Science*, pages 126–133. Springer, 1991.

15. P. Gaborit, A. Otmani, and H. Talé Kalachi. Polynomial-time key recovery attack on the Faure-Loidreau scheme based on Gabidulin codes. *Des. Codes Cryptogr.*, 86(7):1391–1403, 2018.
16. L. Goubin and N. Courtois. Cryptanalysis of the TTM Cryptosystem. In T. Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*, pages 44–57. Springer, 2000.
17. A. Kipnis and A. Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In M. J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.
18. D. Lazard. Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *Computer Algebra, EUROCAL '83, European Computer Algebra Conference, London, England, March 28-30, 1983, Proceedings*, volume 162 of *Lecture Notes in Computer Science*, pages 146–156. Springer, 1983.
19. P. Loidreau. A Welch-Berlekamp Like Algorithm for Decoding Gabidulin Codes. In Ø. Ytrehus, editor, *Coding and Cryptography, International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers*, volume 3969 of *Lecture Notes in Computer Science*, pages 36–45. Springer, 2005.
20. P. Loidreau. On cellular codes and their cryptographic applications. In *Proceedings of ACCT 2014, Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, 2014.*, 2014. https://perso.univ-rennes1.fr/pierre.loidreau/ACCT/QC_Crypto_ACCT14.pdf.
21. Y. Medvedeva. Fast enumeration for Grassmannian space. In *2012 XIII International Symposium on Problems of Redundancy in Information and Control Systems*, pages 48–52, 2012.
22. Ø. Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35(3):559–584, 1933.
23. Ø. Ore. Theory of non-commutative polynomials. *Annals of mathematics*, pages 480–508, 1933.
24. A. Paramonov and O. Tretjakov. An analogue of Berlekamp-Massey algorithm for decoding codes in rank metric. *Proceedings of Moscow Inst. Physics and Technology (MIPT)*, 1991.
25. G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *Proceedings of the 2004 IEEE International Symposium on Information Theory, ISIT 2004, Chicago Downtown Marriott, Chicago, Illinois, USA, June 27 - July 2, 2004*, page 398. IEEE, 2004.
26. R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. Information Theory*, 37(2):328–336, 1991.
27. N. Silberstein and T. Etzion. Enumerative Coding for Grassmannian Space. *IEEE Trans. Information Theory*, 57(1):365–374, 2011.
28. J. A. Verbel, J. Baena, D. Cabarcas, R. A. Perlner, and D. Smith-Tone. On the Complexity of "Superdetermined" Minrank Instances. In J. Ding and R. Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 167–186. Springer, 2019.
29. A. Wachter-Zeh, V. B. Afanassiev, and V. Sidorenko. Fast decoding of Gabidulin codes. *Des. Codes Cryptogr.*, 66(1-3):57–73, 2013.

30. A. Wachter-Zeh, S. Puchinger, and J. Renner. Repairing the Faure–Loidreau Public-Key Cryptosystem. In *IEEE Int. Symp. Inf. Theory (ISIT)*, 2018.

A A quadratic system model

Without loss of generality, we here assume that $\boldsymbol{g} = (g^{q^0}, g^{q^1}, \ldots, g^{q^{n-1}})$ is a normal basis of $\mathbb{F}_q/\mathbb{F}_2$. Recall that any solution $\boldsymbol{y} \in \mathbb{F}_q^n$ to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{H}\boldsymbol{e}^\top$ satisfies

$$V_{\boldsymbol{e}}(\boldsymbol{y}) = (V_{\boldsymbol{e}} \cdot U)(\boldsymbol{g}), \tag{3}$$

where $\mathrm{rk}(\boldsymbol{e}) = w$, and $U(X) = \sum_{i=0}^{k+\ell-1} u_i X^i \in \mathbb{F}_q[X, \theta]$. The attack would consist in searching for $V_{\boldsymbol{e}}$ and U in the previous equation, for some fixed $\boldsymbol{y}$ solution to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$.

Let us now write $V_{\boldsymbol{e}}(X) = \sum_{i=0}^{w} v_i X^i$, and denote by $(v_{r,i})_{1\le r\le n} \in \mathbb{F}_2^n$ (resp. $(u_{s,j})_{1\le s\le n}$) the decomposition of v_i (resp. u_j) in the basis $\boldsymbol{g}$. Then, Equation (3) rewrites

$$\Big(\sum_{i=0}^{w}\sum_{r=1}^{n} v_{r,i}\boldsymbol{B}^{q^r}\boldsymbol{C}^i\Big)\,\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{y}) = \sum_{i=0}^{w}\sum_{j=0}^{k+\ell-1}\sum_{r=1}^{n}\sum_{s=1}^{n} v_{r,i}u_{s,j}\;\boldsymbol{B}^{q^r+q^{s+i}}\boldsymbol{C}^{i+\ell}, \tag{4}$$

where $\boldsymbol{B} = \mathrm{Ext}_{\boldsymbol{g}}(g\cdot\boldsymbol{g}) \in \mathbb{F}_2^{n\times n}$ is the matrix of the multiplication by g in $\mathbb{F}_q$, and $\boldsymbol{C} \in \mathbb{F}_2^{n\times n}$ is the right-cyclic-shift matrix. Equation (4) thus defines a quadratic system over $\mathbb{F}_2$, with $n(w+k+\ell+1)$ unknowns coefficients $(v_{r,i})_{r,i}$ and $(u_{s,j})_{s,j}$, involved in n^2 equations (the coefficients of the matrices).

Though the above system is not random (random systems are believed to be the hardest), we report one result concerning the complexity of random Boolean quadratic systems. In [7], Bardet *et al.* gave an algorithm solving such a system. Without any specialization of variables, its running time is in $O(2^{2H(M(\alpha))N_{\mathrm{var}}})$, where N_{var} is the number of variables, $\alpha \coloneqq N_{\mathrm{eq}}/N_{\mathrm{var}}$ is the ratio between equations and variables,

$$H(t) \coloneqq -t\log_2(t) - (1-t)\log_2(1-t)$$

is the binary entropy function, and

$$M(x) \coloneqq -x + \frac{1}{2} + \frac{1}{2}\sqrt{2x^2 - 10x - 1 + 2(x+2)\sqrt{x(x+2)}}\,.$$

In our case, $N_{\mathrm{var}} = \frac{n^2}{\alpha}$ and the parameters have been chosen such that $\alpha = \frac{n}{k+w+\ell+1} \in (1.0, 1.33)$. It leads to $H(M(\alpha)) > 0.372$, hence $\frac{2H(M(\alpha))}{\alpha} > 0.561$. In other terms, this approach leads to:

$$0.561\, n^2 \ge \lambda$$

under the assumptions that the system *behaves like* a random system and we do not specialize variables.