Cryptanalyse Algébrique de Schémas Post-Quantiques et Hypothèses Associées

Pierre Briaud

THÈSE DE DOCTORAT DE SORBONNE UNIVERSITÉ

Spécialité

Informatique

École doctorale Informatique, Télécommunications et Électronique (Paris)

Présentée par

Pierre Briaud

Pour obtenir le grade de

DOCTEUR de SORBONNE UNIVERSITÉ

Algebraic Cryptanalysis of Post-Quantum Schemes and Related Assumptions

soutenue publiquement le 11 décembre 2023

devant le jury composé de :

Jean-Pierre Tillich	Inria	Directeur
Louis Goubin	Université de Versailles Saint-Quentin-en-Yvelines	Rapporteur
Antoine Joux	CISPA Helmholtz Center for Information Security	Rapporteur
Martin Albrecht	King's College London et SandboxAQ	Examinateur
Magali Bardet	Université de Rouen	Examinatrice
Pierre-Alain Fouque	Université de Rennes 1	Examinateur
Vincent Neiger	Sorbonne Université	Examinateur
Guénaël Renault	ANSSI	Examinateur

présidé par : Pierre-Alain Fouque

Contents

Introduction

The original purpose of cryptography was to guarantee the secrecy of messages by encrypting them before the transmission. Since then, the field had to go beyond this initial goal due to its large-scale use and the development of computers in the second part of the 20th century. At that time, a revolution was also the invention of public-key cryptography in 1976 [DH76]. It allowed parties to securely communicate without meeting to agree on a common secret. As such *asymmetric* algorithms typically rely on hardness assumptions about computational problems, this also strengthened the role of mathematics and theoretical computer science in the discipline.

The paradigm to argue security is that an attacker that breaks the scheme can be used as a subroutine to solve the intractable mathematical problem. It is thus important that there does not exist any efficient solver. Another constraint is that the assumption should contain enough expressivity for the intended application. This explains why arbitrary hard problems are in general not relevant. Hopefully, some coming from number theory were also shown to meet our second condition. The two most prominent ones are by far Integer Factorization and the Discrete Logarithm problem, for which all the best known algorithms are exponential or subexponential. A majority of public-key schemes are based upon these assumptions or closely related ones.

However, in 1994, Peter Shor introduced a polynomial time quantum algorithm [Sho94] for these problems. Assuming that it can be implemented, this implies that all current asymmetric mechanisms will be insecure in a model where the attacker has quantum capabilities. This lead to rethink cryptography with new alternative assumptions believed to resist quantum computers. To encourage efforts in that direction, the National Institute of Standards and Technology (NIST) initiated in 2017 a competition to select the most promising candidates. Clearly, a prerequisite for such proposals remains their resistance to *classical* algorithms. Our work will focus on this setting and we will not consider quantum adversaries.

Algebraic Cryptanalysis

The idea of recovering the cryptographic secret by solving a multivariate polynomial system over a finite field goes back way beyond the boom in post-quantum schemes. It was for example used in the analysis of symmetric ciphers [CP02; CM03] and also on the elliptic curve version of the Discrete Logarithm problem [Sem04]. It is however clear that the approach has taken new scope in this recent context. Indeed, it has been shown to affect code-based, lattice-based and multivariate proposals, which constitute

the majority of the NIST submissions.

This general method takes the name of *algebraic cryptanalysis*. It requires both a polynomial modeling of the cryptographic application and a study of solving algorithms applied to these equations. These techniques are traditionally analyzed thanks to the notions of *ideals* and *Gröbner bases*. A recurrent challenge is that generic bounds given by computer algebra do not take into account the specificities in the input system. They are due to algebraic properties of the scheme or of the hard problem under scrutiny but also more directly to the shape of the equations.

MinRank Problem

Most of our contributions concern the analysis of MinRank [BFS99] and related variants. This hardness assumption states that it is computationally difficult to find a non-zero low rank linear combination between (full-rank) public matrices.

It was brought in cryptography by [Cou01b] to design a zero-knowledge authentication protocol. At about the same time, one also noted its strong connection with the security of code-based schemes in the rank metric. More precisely, the generic decoding problem for this metric – the Rank Decoding (RD) problem – can be expressed as a MinRank instance with a structure coming from an extension field. On the contrary, in the area of multivariate cryptography where it is the most popular, MinRank is not part of the security reduction. There, it only serves as a cryptanalytic tool to retrieve the private key. For a given scheme, it is thus important to select the right instance or to find possibly easier ones. Addressing this second question was in particular the crux in the devastating attacks of [Beu21a; TPD21].

Given its recentness compared to code-based and lattice-based assumptions, the cryptanalysis of MinRank is not established yet. For example, we do not have a complete picture of hardness for random instances in function of the parameters. In fact, since MinRank appears almost exclusively in a structured form, it is not even clear that such a result would be of any help. What is certain is that the nature of the problem paves the way for both algebraic and combinatorial techniques, regardless of this structure.

Several polynomial modelings have already been proposed for MinRank. The analysis of the oldest ones has been shown to be nicely connected to the theory of determinantal ideals [FSS10]. This relation remains to be understood for more recent systems which lead to cryptanalysis breakthroughs, especially Support-Minors (SM) [Bar+20b]. Independently, the extra structure in variants calls for a new analysis of these generic modelings. It also leaves room for finding more relevant ones tailored to these versions.

Structured Systems

We also studied other systems that are no longer related to MinRank but which still admit particular features. In cryptography, the main solving technique boils down to

computing a Gröbner basis in some graded order using an F_4/F_5-type of algorithm [Fau99; Fau02], whose complexity is exponential in the maximal degree of a polynomial appearing in this calculation. The challenge for the cryptanalyst is then to derive a tight bound on this parameter based on the algebraic properties of the equations.

This has already been achieved in contexts where this structure is not apparent. For example, polynomial systems arising from the direct attack on (variants) of Hidden Field Equations (HFE) [Pat96] seem to have the same shape as random quadratic ones. However, it was quickly noticed that the degree reached by the solver on these equations is lower than the one on the latter [JF03]. It is now well-known that this parameter is controlled by the rank of the MinRank problem which underlies the scheme [DH11; DK12; DY13].

In the worst case scenario, such properties cannot be exploited or even uncovered. In this situation, cryptographers do not hesitate to base their analysis uniquely on experiments. Concretely, this means picking numerical parameter values and run the solver on the resulting small-scale systems to see a general trend. The other extreme would be to use the specific structure in order to speed-up the computation, for instance by tweaking the general-purpose Gröbner basis algorithm. This undoubtedly requires a much deeper understanding of the system.

Contributions

The content of this manuscript is dedicated to the cryptanalysis of several types of primitives and it falls almost exclusively within the scope of algebraic cryptanalysis. Some of our works encompass all the aspects of such an attack, from deriving the modeling to the cost estimate, while some others are restricted to the latter step. We have attempted to exploit potential features in the input equations as far as possible.

Analysis of existing systems. Even when we proposed a new polynomial modeling, this came from a study of the previous choices to understand why they were not necessarily the most suitable. Thus, we first describe our contributions regarding the analysis step.

- In [Bae+22], we demonstrated that the Support-Minors modeling could indeed be applied to the MinRank problem introduced by [TPD21]. Tao *et. al* were not able to estimate this solver due to the big-field structure. In addition and more generally, we addressed the question of memory complexity when using SM.

- The results in [Bar+23] on the RD problem were also obtained from a preliminary analysis of SM. In this structured context, our experiments showed that the modeling does not behave as suggested in [Bar+20b] due to some algebraic relations. We provided conjectures for the number of such cancellations and we managed to explain a good part of them. It turns out that we also recover the MaxMinors (MM) equations of [Bar+20a] when we run Gröbner bases on SM.

- In [BBBG23], we focused on the Non Homogenous Rank Decoding (NHRD) problem. This is a variant of RD where the error has a specific form. This shape was used in [Agu+20] to boost the original RD solver by setting unknowns to zero in both MM and SM. However, this method also causes a loss in the number of equations which was not considered in their estimates. We have tried to understand this drop in the case of MM to obtain a more accurate cost formula.

- The bilinear equations studied in [BL23] had been introduced by Loidreau at WCC 2022[1] but our work is the first attempt to analyze them. We showed that there exist degree fall polynomials coming from the kernel of structured Jacobians, which allowed to partially explain the early steps of the Gröbner algorithm. Even if this content does not lead to an attack, it should give a better grasp of the indistinguishability assumption which underlies Loidreau's cryptosystem.

- The systems encountered in [Bou+23] are standard in the context of algebraic cryptanalysis on arithmetization-oriented ciphers but they differ a great deal from our other applications. This type of attacks is also rather new and each symmetric design has its particularities. We managed to complement our experimental study with a partial interpretation of the observed behaviour.

Starting from a new modeling.

- The work of [BTV21] corresponds to a full algebraic attack on a new multivariate encryption scheme [RLT21]. The authors had already proposed an *ad hoc* MinRank instance relevant to key-recovery. Sadly, in contrast to rank attacks on HFE, the link between its solutions and the final (equivalent) key was unclear. Our first step was thus to identify solutions which are suitable for an attack. By exploiting their specific shape, we gave a polynomial strategy based on a dedicated modeling.

- The analysis in [Bar+23] also lead us to introduce another system for the RD problem. Our arguments suggest that it may lead to better complexities than the former SM method of [Bar+20b].

- The Rank Support Learning (RSL) problem is variant of RD with $N \geqslant 1$ decoding instances where the coordinates in all the errors belong to the same subspace of $\mathbb{F}_{q^m}$. In [BB21], we gave a new SM-type modeling tailored to RSL. Its analysis was in fact the starting point of [Bar+23] and the same proof techniques are used in both papers.

- Our cryptanalysis of the Regular Syndrome Decoding (RSD) problem [BØ23] can also be seen as building upon a new algebraic system since it is not explicitly mentioned in the literature. Our main contribution was to study its specific features. There, the structural part comes from quadratic polynomials which model the regular distribution. We have been able to fully understand these equations. This

[1] https://www.wcc2022.uni-rostock.de/home.

analysis already provides a rather precise picture of the full modeling because the rest of the polynomials are not structured and may be treated as random at least in a first stage.

Hybrid techniques. In some of our works [BB21; Bar+23; BØ23], we also proposed a hybrid approach by fixing unknowns in the initial system. The general goal is to obtain a better cost in parameter zones where the plain algebraic attack does not perform extremely well. Contrary to the folklore method where these variables are randomly selected, we took care to choose structured specializations for which the resulting system still keeps a similar shape. This is important because it may give better results while allowing us to rely on the initial analysis. This also places the approach as a natural interpolation between the original solver and combinatorial techniques which are often better understood. Finally, we contributed to improving these latter algorithms in the context of NHRD [BBBG23] and we have managed to apply them to the Loidreau scheme [BL23].

Impact for Cryptographic Proposals

Multivariate cryptography. By building upon the almost-break of [TPD21], we obtained the best known attack on variants of HFE. In particular, we managed to break the parameters of pHFEv- [ØSV21] which were resistant to [TPD21]. Concerning the Sidon cryptosystem, the scheme can in theory be repaired by picking another type of Sidon space. However, such a new construction has not been found so far.

Rank-based cryptography. Our work has contributed to strengthen the analysis of cryptosystems relying on the rank metric. This was especially needed in the context of the NIST call since algebraic methods had been much less studied than combinatorial techniques. In the case of RD, [Bar+23] now represents the state-of-the-art. To the best of our knowledge and even though it is not competitive when the number N of instances is rather small, our approach on RSL [BB21] is still the only attack of algebraic nature tailored to this problem.

Regular Syndrome Decoding. On some parameters used in pseudorandom correlation generators [BCGI18], our approach has been shown to outperform standard techniques such as ISDs and Statistical Decoding. This was especially true with the help of the hybrid component.

Selecting parameters. The analysis of [BBBG23] and [Bou+23] are part of design papers and they allowed to instantiate our proposals. As is often the case for this type of ciphers, algebraic attacks were the limiting ones for Anemoi.

Organisation du Manuscrit

Ce document est divisé en quatre grandes parties. La première contient des notions préliminaires tandis que les trois autres sont dédiées à nos contributions, classées de manière thématique. Au sein de chaque partie, nous avons tenté d'adopter un ordre logique entre les chapitres, sauf dans la Partie IV où cela nous a semblé difficile.

Partie I Elle se compose de trois chapitres.

- Dans le Chapitre 1, nous donnons des éléments de cryptographie asymétrique et de cryptanalyse. Nous formalisons aussi le cadre de la cryptanalyse algébrique dans lequel s'inscrivent la quasi-totalité de nos travaux.
- L'étude de complexité pour ce type d'attaques amène à analyser des algorithmes de résolution de systèmes d'équations multivariées sur un corps fini. Le Chapitre 2 introduit la théorie des idéaux polynomiaux et des bases de Gröbner qui sont sous-jacents à ces méthodes. Il donne aussi un aperçu des principales techniques utilisées en cryptanalyse algébrique.
- Le Chapitre 3 revient en détail sur les problèmes difficiles desquels sont issues les modélisations rencontrées dans cette thèse. Lorsque cela est pertinent, nous présentons aussi les constructions cryptographiques basées sur les hypothèses de sécurité associées.

Partie II Cette partie est consacrée à nos résultats de cryptanalyse sur des schémas multivariés qui font intervenir une extension de corps $\mathbb{F}_{q^n}$.

- Nous étudions la trappe *Hidden Field Equations* (HFE) et ses variantes dans le Chapitre 4. Nous améliorons une attaque récente basée sur une instance MinRank particulière en employant la modélisation Support-Minors, que nous arrivons à analyser dans ce contexte.
- Le Chapitre 5 donne une attaque polynomiale sur un nouveau mécanisme de chiffrement reposant sur des sous-espaces particuliers de $\mathbb{F}_{q^n}$ appelés espaces de Sidon. Là encore, nous considérons un problème MinRank spécifique. Nous proposons un système algébrique dédié pour le résoudre et nous montrons que cela permet de casser le schéma.

Partie III Elle contient nos attaques contre la plupart des hypothèses de difficulté considérées en cryptographie en métrique rang. C'est la plus fournie de ce manuscrit.

- Mon travail de thèse le plus ancien s'est intéressé au problème Rank Support Learning. Il est décrit dans le Chapitre 6. Nous y introduisons la première approche purement algébrique contre ce problème. Nous donnons aussi une méthode combinatoire issue d'un article ultérieur dont l'idée de départ est similaire.

- Le Chapitre 7 revient sur le problème plus fondamental du décodage générique. Nous utilisons les mêmes techniques de preuve que dans le chapitre précédent afin de corriger l'analyse de complexité des solveurs algébriques existants. Ces outils nous permettent aussi d'estimer le coût de résolution d'une nouvelle modélisation que nous proposons. Enfin, nous présentons une approche hybride structurée s'appliquant aux systèmes algébriques utilisés contre le problème de décodage. Elle a l'avantage de se généraliser à n'importe quelle attaque connue contre MinRank.

- Dans le Chapitre 8, nous nous focalisons sur une variante où le vecteur de bruit a une forme particulière. La difficulté de ce problème est utilisée dans RQC et dans une nouvelle amélioration de ce cryptosystème. En tenant compte de la structure de l'erreur, nous analysons la modélisation algébrique MaxMinors et nous adaptons l'approche combinatoire standard dans ce cadre précis.

- Le Chapitre 9 s'intéresse à un distingueur pour le schéma de Loidreau basé sur des équations bilinéaires. Nous proposons une meilleure technique de résolution s'inspirant des attaques combinatoires contre le décodage générique et nous mettons en évidence des chutes de degré dues à la structure qui apparaissent dans les premières étape de l'algorithme de base de Gröbner appliqué au système.

Partie IV Elle réunit nos deux travaux qui ne sont pas reliés au problème MinRank sous-jacent aux parties II et III.

- Le Chapitre 10 étudie une autre forme d'erreur spécifique dite *régulière* dans le cas du décodage en métrique de Hamming. Alors que le problème initial est plutôt sujet à des méthodes combinatoires, cette structure supplémentaire permet l'application de techniques algébriques. Notre approche se base sur un système relativement élémentaire pour lequel nous conjecturons une série de Hilbert et dans lequel nous proposons de fixer des variables en accord avec la structure. Nous montrons qu'elle peut être compétitive vis-à-vis des attaques connues dans des zones de paramètres utilisées par les générateurs de pseudo-aléa corrélé (PCG).

- Un nouveau type de cryptographie symétrique utilisé dans les preuves zero-knowledge s'avère vulnérable aux méthodes algébriques. La permutation Anemoi a été récemment proposée afin de gagner en efficacité dans plusieurs systèmes de preuve. Dans le Chapitre 11, nous étudions sa résistance contre deux modélisations afin de déterminer ses paramètres.

Publications

[Bae+22] John Baena, Pierre Briaud, Daniel Cabarcas, Ray A. Perlner, Daniel Smith-Tone, and Javier A. Verbel. "Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow". In: *CRYPTO 2022*. Vol. 13509. LNCS. Springer, 2022, pp. 376–405 (cit. on pp. xi, 59, 69).

[BB21] Magali Bardet and Pierre Briaud. "An Algebraic Approach to the Rank Support Learning Problem". In: *PQCrypto 2021*. Vol. 12841. LNCS. Springer, 2021, pp. 442–462 (cit. on pp. xii, xiii, 51, 91, 92, 95, 103).

[Bar+23] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. "Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem". In: *Designs, Codes and Cryptography* (2023) (cit. on pp. xi–xiii, 91, 107, 120).

[BBBG23] Loïc Bidoux, Pierre Briaud, Maxime Bros, and Philippe Gaborit. "RQC revisited and more cryptanalysis for Rank-based Cryptography". In: *IEEE Transactions on Information Theory* (2023) (cit. on pp. xii, xiii, 52, 91, 92, 104, 131, 133–135, 145).

[Bou+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. "New Design Techniques For Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations And Jive Compression Mode". In: *CRYPTO 2023*. Vol. 14085. LNCS. Springer, 2023, 507–539 (cit. on pp. xii, xiii, 187, 191, 196).

[BL23] Pierre Briaud and Pierre Loidreau. "Cryptanalysis of rank-metric schemes based on distorted Gabidulin codes". In: *PQCrypto 2023*. Vol. 14154. LNCS. Springer, 2023, pp. 38–56 (cit. on pp. xii, xiii, 149).

[BØ23] Pierre Briaud and Morten Øygarden. "A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions". In: *EUROCRYPT 2023*. Vol. 14008. LNCS. Springer, 2023, pp. 391–422 (cit. on pp. xii, xiii, 165, 177, 180, 181).

[BTV21] Pierre Briaud, Jean-Pierre Tillich, and Javier Verbel. "A Polynomial Time Key-Recovery Attack on the Sidon Cryptosystem". In: *SAC 2021*. Vol. 13203. LNCS. Springer, 2021, pp. 419–438 (cit. on pp. xii, 39, 75).

Notation

Generic Notation

Symbol	Meaning
	Integers
$\mathbb{N},\ \mathbb{Z},\ \mathbb{Z}_{>0}$	Natural numbers, integers, positive integers
$\{a..b\}$	The set of integers between a and b
$\#I$	The cardinality of a set I
$\binom{a}{b},\ \binom{a}{b}_q$	Binomial coefficient, Gaussian binomial coefficient
	Vectors
$\boldsymbol{v}$	Bold lowercase letters denote row vectors
$\boldsymbol{v}^\mathsf{T}$	Transpose of the vector $\boldsymbol{v}$
$v_i,\ \boldsymbol{v}_I$	The i-th component of $\boldsymbol{v}$ and the vector $(v_i)_{i\in I}$ for $I \subset \{1..\ell\}$
	Matrices
$\boldsymbol{M}$	Bold capital letters denote matrices
$\boldsymbol{M}^\mathsf{T}$	Transpose of the matrix $\boldsymbol{M}$
$\boldsymbol{M}_{i,j}$	The entry in row i and column j
$\boldsymbol{M}_{I,*}$	The submatrix obtained by considering row indexes in I
$\boldsymbol{M}_{*,J}$	The submatrix obtained by considering column indexes in J
$\boldsymbol{I}_n$	The identity matrix of size n
$\mathrm{rk}(\boldsymbol{M})$	The rank of the matrix $\boldsymbol{M}$
$\lvert\boldsymbol{M}\rvert,\ \lvert\boldsymbol{N}_{*,J}\rvert,\ \lvert\boldsymbol{P}_{I,*}\rvert$	Determinant of the square matrix $\boldsymbol{M}$ (or of square submatrices $\boldsymbol{N}_{*,J}$, $\boldsymbol{P}_{I,*}$)
$\boldsymbol{M} \otimes \boldsymbol{N}$	Kronecker product between two matrices $\boldsymbol{M}$ and $\boldsymbol{N}$
$\begin{bmatrix}\boldsymbol{M}\ \boldsymbol{N}\end{bmatrix},\ \begin{bmatrix}\boldsymbol{M}\\ \boldsymbol{N}\end{bmatrix}$	Concatenation between two matrices $\boldsymbol{M}$ and $\boldsymbol{N}$ (with appropriate sizes)
	Algebraic structures
$R,\ \mathcal{R}$	An arbitrary ring
$\mathbb{K},\ \overline{\mathbb{K}}$	A field and its algebraic closure
$\mathbb{F}_q$	For a prime power q, the field with q elements
$\mathbb{F}_{q^n}$	Degree n extension of $\mathbb{F}_q$
$x^{[\ell]}$	For $\ell \in \mathbb{N}$ and $x \in \mathbb{F}_{q^n}$, the image x^{q^ℓ} of x under the ℓ-th iterate of the Frobenius map

Polynomials and Ideals

The notation $\boldsymbol{x} = (x_1, \ldots, x_n)$ stands for a vector of variables and we let $\mathbb{K}[\boldsymbol{x}]$ denote the ring of multivariate polynomials in the variables $\boldsymbol{x}$ with coefficients in $\mathbb{K}$. The polynomial system (resp. sequence) containing the polynomials $f_i \in \mathbb{K}[\boldsymbol{x}]$ for $1 \leqslant i \leqslant m$ will be denoted by $\mathcal{F} \stackrel{def}{=} \{f_1, \ldots, f_m\}$ (resp. $(f_1, \ldots, f_m)$). The *ideal* generated by this system is defined by

$$\langle \mathcal{F} \rangle \stackrel{def}{=} \langle f_1, \ldots, f_m \rangle \stackrel{def}{=} \left\{ \sum_{i=1}^{m} g_i f_i : (g_1, \ldots, g_m) \in \mathbb{K}[\boldsymbol{x}]^m \right\}.$$

Finally, the letter I may denote an arbitrary polynomial ideal.

Linear Codes

A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of dimension k. We say that it has parameters $[n, k]_q$. A generator matrix for $\mathcal{C}$ is a full-rank matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ whose rowspace is equal to $\mathcal{C}$, *i.e.*, $\mathcal{C} = \left\{ \boldsymbol{m}\boldsymbol{G},\ \boldsymbol{m} \in \mathbb{F}_q^k \right\}$. The dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp \stackrel{def}{=} \left\{ \boldsymbol{h} \in \mathbb{F}_q^n : \forall \boldsymbol{c} \in \mathcal{C},\ \boldsymbol{c}\boldsymbol{h}^\mathsf{T} = 0 \right\}.$$

It is an $[n, n-k]_q$ linear code and we call parity-check matrix for $\mathcal{C}$ any full-rank generator matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k) \times n}$ of $\mathcal{C}^\perp$. Finally, the *puncturing* and *shortening* operations are classical ways to construct new linear codes from existing ones. For $I \subset \{1..n\}$, the puncturing $\mathcal{P}_I(\mathcal{C}) \subset \mathbb{F}_q^{n-\#I}$ of $\mathcal{C}$ at I is the $[n - \#I, k' \leqslant k]_q$-code defined by

$$\mathcal{P}_I(\mathcal{C}) \stackrel{def}{=} \left\{ \boldsymbol{c}_{\{1..n\} \setminus I} : \boldsymbol{c} \in \mathcal{C} \right\}. \tag{1}$$

Similarly, the shortening at the same positions is

$$\mathcal{S}_I(\mathcal{C}) \stackrel{def}{=} \left\{ \boldsymbol{c}_{\{1..n\} \setminus I} : \boldsymbol{c} \in \mathcal{C} \text{ and } \boldsymbol{c}_I = \boldsymbol{0}_I \right\}. \tag{2}$$

We have $\mathcal{S}_I(\mathcal{C}^\perp) = \mathcal{P}_I(\mathcal{C})^\perp$ and $\mathcal{S}_I(\mathcal{C})^\perp = \mathcal{P}_I(\mathcal{C}^\perp)$, so that this shortening operation is in some sense dual to puncturing.

Asymptotic Notation

We consider the standard Bachmann–Landau notation for two functions $f,\ g :\ \mathbb{N} \to \mathbb{R}$:

$$f(n) \stackrel{def}{=} \mathcal{O}\left(g(n)\right) \Leftrightarrow \exists M > 0,\ \forall n \in \mathbb{N},\ f(n) \leqslant M \left|g(n)\right|,$$

$$f(n) \stackrel{def}{=} \Omega\left(g(n)\right) \Leftrightarrow \exists m > 0,\ \forall n \in \mathbb{N},\ f(n) \geqslant m \left|g(n)\right|,$$

$$f(n) \stackrel{def}{=} o(g(n)) \Leftrightarrow \lim_{n \to +\infty} \frac{f(n)}{g(n)} = 0.$$

Also, we will write $f \sim_{n \to +\infty} g$ if $(f - g)(n) = o(g(n))$ and $f(n) = \widetilde{\mathcal{O}}\left(g(n)\right)$ if there exists some constant $c > 0$ such that $f(n) = \mathcal{O}\left(g(n) \left|\log g(n)\right|^c\right)$.

Part I
Preliminaries

Chapter 1
Relevant Concepts in Cryptology

This first preliminary chapter introduces some notions in cryptology in order to put our work into this broader domain.

Cryptology traditionally encompasses the areas of *cryptography* and *cryptanalysis*. Historically, the goal of cryptography was to devise mechanisms to guarantee the secrecy of communications. Due to emerging applications which do not require to transmit data, the motivation is now more general but a similar security concern remains. Cryptanalysis gathers all the methods which aim at discovering flaws in such cryptographic constructions.

Contents

1.1 Public-Key Cryptography

At the core of the development of cryptography is the initial belief that two people had to agree on a secret way of encrypting and decrypting messages in order to communicate. Nowadays, the field of *symmetric cryptography* is the closest one to this original idea since the parties need to share a common string, the *secret key*, in such mechanisms. The most iconic scheme of this type is undoubtedly the Advanced Encryption Standard or AES [DR02], which has been widely used since its standardization.

However, symmetric cryptography does not answer the question of distributing these secret keys. History as well as the growing number of interactions through insecure channels in everyday life applications have shown that this issue had to be addressed in a secure but also efficient way. Luckily, in 1976, at about the same time as the early stages of the Internet, the pioneering work of Diffie and Hellman [DH76] circumvented this problem by finding an alternative to the secret-key paradigm to build cryptography. Their new approach gave rise to what we call *public-key* or *asymmetric cryptography*. It relies on the existence of *trapdoor one-way functions*, *i.e.*, functions which are easy to evaluate but whose inversion is far more complicated without the knowledge of a secret

quantity, a *trapdoor*. Since they are a special case of general one-way functions, whose existence would imply $\mathsf{P} \neq \mathsf{NP}$, this abstract construction is related to one of the most famous open conjectures in theoretical computer science.

Diffie and Hellman have not been able to find a concrete example to approximate such ideal functions. Shortly after, in 1978, Rivest, Shamir and Adleman suggested to use the exponentiation modulo the product N of two large prime numbers p and q. It lead to the RSA cryptosystem [RSA78] which can be seen as the first realization of public-key cryptography. Several other candidate trapdoor functions have been proposed since then, still tied to problems mostly from number theory which are assumed to be intractable. This is not the first time that mathematics had come to the rescue of cryptology. The introduction of a mathematical formalism in this area since the 19th century actually explains why the field became a *science* well before the birth of asymmetric cryptography. Relying on algebraic structures not initially tailored to computer science is also a reason why public-key algorithms are computationally less efficient than secret-key solutions. This justifies the use of *hybrid encryption* to combine the advantages of both types of cryptography.

A common feature in asymmetric schemes is a **Keygen** algorithm to produce a pair of keys $(\mathsf{sk}, \mathsf{pk})$. The *secret key* sk is kept by only one party while the *public key* pk can be freely distributed. The way these keys are used depends on the intended application.

Encryption schemes. The most basic purpose of asymmetric cryptography is to ensure confidential communication. This can be achieved thanks to *public-key encryption* (PKE). Let us assume that Alice wants to securely transmit a message m to Bob. First, **Keygen** provides a private key sk to the latter as well as a public key pk which is known to any user. Alice can thus apply the encryption algorithm **Encrypt** with input pk to obtain the *ciphertext* $c = \mathbf{Enc}(\mathsf{pk}, m)$. Only the owner of the secret key sk, namely Bob, can finally **Decrypt** to recover $m = \mathbf{Dec}(\mathsf{sk}, c)$.

While this seems reasonably satisfactory, this solution does not guarantee that the message m was *really* sent by Alice. To ensure the *authenticity* of communication, one can use *digital signatures*.

Digital signatures. In addition to **Keygen**, a digital signature scheme consists of two algorithms $(\mathbf{Sign}, \mathbf{Verify})$. As in a PKE, the **Keygen** procedure generates a keypair $(\mathsf{sk}', \mathsf{pk}')$ but this time sk' is sent to Alice. To show that she is legitimate, Alice then builds a signature $\sigma = \mathbf{Sign}(\mathsf{sk}', m)$ that she typically appends to her message. An arbitrary signature $\widetilde{\sigma}$ is publicly verifiable using pk' by computing $\mathbf{Verify}(\mathsf{pk}', \widetilde{\sigma}, m)$. This boolean value indicates whether $\widetilde{\sigma}$ is a valid signature for m or not.

Since a signature is tied to a given plaintext, such a mechanism also ensures *integrity*. This means that the message cannot be corrupted during the communication.

Advanced functionalities. Due the development of technology and computer-based communication, cryptography needs to answer new challenges which arise from these

applications. Most of the time, they require cryptographic constructions with more advanced *functionalities*.

In this context, a PKE and or a digital signature can still serve as the fundation provided it has *specific* properties. The whole scheme is then obtained by adding external algorithms. Interestingly enough, number-theoretic assumptions have proven helpful to find such building blocks. For example, the RSA cryptosystem is multiplicatively homomorphic and the Paillier scheme [Pai99] enjoys a similar property but for addition. The latter is based on the Decisional Composite Residuosity Assumption (DCRA), which becomes easy if one knowns how to efficiently factor large numbers. In the same fashion, Identity-Based-Encryption (IBE) and group signatures are generalizations of PKE and digital signatures whose early constructions [BF01; BBS04] heavily rely on bilinear maps on appropriate groups.

However, some other applications have required brand new building blocks. For instance, secure two-party computation (2PC) was introduced along with the notion of garbled circuit [Yao86]. Since the goal is not restricted to secure communication anymore, it is quite understandable that PKE and signatures were no longer sufficient. Still, note that mathematics remain extremely present. Very often, they help to realize a partial step towards the final functionality. To continue the example above, garbled circuits rely on oblivious transfer (OT), whose initial construction [Rab05] is based on the RSA assumption.

1.2 Security and Cryptanalysis

Attempts to find weaknesses in cryptographic mechanisms are traditionally referred to as *attacks*. Due to Kerchkoffs's principle [Ker83], such techniques are able to exploit a public specification of the scheme. A consequence is that a cryptosystem which resists several years of analysis by the community may be more trusted than a proposal that no one has examined.

To study these attacks, modern cryptography has introduced a more precise framework which goes beyond the intuitive meaning of security. Roughly speaking, it consists in formalizing the capabilities of the adversary Eve (the *model*) and what we allow her to achieve (the *security notion*). A security notion aims at making more precise a security goal for a scheme in order to have a *proof* that this scheme indeed meets this requirement. By construction, the security of asymmetric primitives is related to mathematical problems which are believed to be difficult in the considered model of computation. In this context, a security proof (or *reduction*) strengthens this connection by showing that an adversary which can efficiently attack the targeted notion can be used to solve efficiently the associated problem.

In fact, hardness assumptions remain the focus of cryptanalysis even when such a reduction is missing. A *security level* which measures *concrete security* is often obtained from the computational cost of the best known attacks. Finally, a *break* traditionally refers to an attack whose complexity is below this security level.

1.3 Algebraic Cryptanalysis

Algebraic cryptanalysis can be defined as the very general family of attacks which are based on solving a system of multivariate equations. Even if it is difficult to give the precise date of the first algebraic attack, the broad idea can already be traced back to the work of Shannon [Sha49]. The general structure is in two steps:

1. **Modeling.** First, we set up a multivariate system which describes the scheme from the knowledge of its specification. The requirement is that solving this system should allow to recover the secret (message, private key, ...). The variables are the secret itself or they can be related to it in a less direct way. In this second case, additional steps might be needed to recover this secret.

2. **System solving.** As cryptosystems mainly operate on discrete data, there will be no ambiguity in the definition of "solving" in our context: the set of solutions is a finite list of vectors. Similarly to other types of cryptanalytic attacks, an algebraic attack is said to be practical if we can *efficiently* recover these solutions. However, to some extent, modern cryptography also considers non-practical ones[1]. In this situation, the work of the cryptanalyst is to estimate a theoretical cost.

Both steps are equally important but they also go hand in hand. The first step is the closest one to the initial cryptographic design and it sometimes calls for *creativity*. A presumably good modeling should contain as much information as possible about the scheme because this information may help for the solving process. Concretely, we would like to find "simple" equations or as many equations as possible. However, we cannot make a definitive statement on the quality of a modeling without studying efficient algorithms for solving it. In particular, *analyzing* them may be challenging. Very often, this is because we apply *generic* techniques to systems with *specific* features.

Regardless of its feasibility, the minimal condition to mount an algebraic attack is that the cryptographic algorithm can be expressed into a set of multivariate equations. For this reason, algebraic cryptanalysis is sufficiently general to be applied to both symmetric and asymmetric schemes.

1.4 Post-Quantum Cryptography

While a large part of cryptography, starting from most of the symmetric primitives, does not seem too strongly affected by the added capabilities of quantum computers, the same does not hold for public-key cryptosystems. There is nothing really wrong with the initial paradigm itself but sadly the essential building block which is used to instantiate it is now defective. Indeed, both the Discrete Logarithm problem and Integer Factorization are particular instances of the so-called Hidden Subgroup problem for finite abelian groups, which can be solved in polynomial time by Shor's algorithm [Sho94]. In response,

[1] For instance to derive security levels and parameters.

the keysize in current public-key mechanisms would have to be increased exponentially, leading to truly uncompetitive schemes. In contrast, it is generally acknowledged that doubling this keysize for most of the symmetric primitives should be sufficient to hedge against Grover's algorithm [Gro96].

Hopefully, this very fact also implies that building quantum-safe public-key cryptography should not be too hard, at least in theory. It is just a matter of replacing the flawed building block by a quantum-resistant one. In particular, the community has already started to consider new hardness assumptions for which quantum computers do not seem to help. Each of these difficult problems is associated to a branch of what we call *post-quantum cryptography*. Interestingly enough, research in some of these branches is prior to Shor's algorithm. The most important ones[2] are:

- **Code-based cryptography**, relying on the hardness of decoding random linear codes and other closely related assumptions,
- **Hash-based cryptography**, relying on the security of a given hash function,
- **Isogeny-based cryptography**, relying on difficult problems defined in terms of isogenies between elliptic curves,
- **Lattice-based cryptography**, relying on the hardness of finding short vectors in Euclidean lattices and other closely related assumptions,
- **Multivariate cryptography**, where most schemes are based on the difficulty of solving random multivariate quadratic systems.

Even though the underlying assumptions are believed to be quantumly intractable, they already provide extra material to *classical* cryptanalysts and in particular to algebraic cryptanalysts. Indeed, some of them still involve a sufficient amount of structure for such techniques to apply. This structure is often vital to build the cryptographic trapdoor. Sometimes, more artificially, it is also a way to enhance the efficiency of a given cryptographic construction. In Chapter 3, we will go back to some of these hard problems through the lens of algebraic cryptanalysis.

Post-quantum standardization effort. To fully migrate to post-quantum cryptography, we need to duplicate all the work performed for number-theoretic cryptography by building efficient schemes based on new assumptions and later combine them into procotols in order to reach more advanced functionalities. It turns out that these hard problems also allowed to solve new cryptographic challenges. The most obvious example so far is undoubtedly *Fully Homomorphic Encryption* (FHE) [Gen09], which has long been regarded as the holy grail of cryptography [Mic10]. Indeed, all FHE proposals or at least those used in commercial solutions are lattice-based.

The large-scale deployment of post-quantum cryptography also calls for standards. To this end, the American National Institute of Standards and Technology (NIST)

[2]Presented in alphabetical order to avoid any unnecessary debate.

launched in 2017 a process – often referred to as the NIST PQC competition (or project) – to standardize post-quantum PKE and digital signatures. The initial call for proposals gathered 82 submissions, most of them belonging to one of the abovementioned branches. They have been analyzed in-depth by the entire cryptographic community and the selection has been narrowed down through a series of 3 rounds. The outcome of the Third Round was announced in July 2022: four candidates have been selected for standardization and four additional algorithms have continued in a Fourth Round for further study [Ala+22]. Among them, it should be noted that SIKE [Jao+17] was subject to severe cryptanalysis since then [CD23; Mai+23; Rob23] and is now considered as broken.

Table 1.1: Third Round outcome: ready for standardization.

Public-Key Encryption/KEMs	**Digital Signatures**
CRYSTALS-Kyber	CRYSTALS-Dilithium
	Falcon
	SPHINCS$^+$

Table 1.2: Third Round outcome: Fourth Round candidates.

Public-Key Encryption/KEMs	**Digital Signatures**
BIKE	
Classic McEliece	
HQC	
SIKE (broken)	

Most of the content of this thesis is closely related to the NIST PQC project. First, the whole process has been a clear boost for the post-quantum branches which are arguably the most vulnerable to algebraic cryptanalysis, namely multivariate cryptography and code-based cryptography relying on the rank metric. More directly, a part of my PhD work applies to some of the NIST candidates, for instance the rank-based schemes ROLLO [Ara+19c] and RQC [Agu+20] and the multivariate-based GϵMSS [Cas+20] and Rainbow [Din+20].

This selection process should not be considered complete. At the end of the Third Round, NIST also asked for additional proposals for signature schemes. The main justification was a lack of diversity among the candidates retained after the Third Round. In particular, NIST was no longer interested in solutions based on structured lattices. Another motivation was to have schemes with short signatures and fast verification. These features are indispensable for some applications and they seemed to lack in the algorithms kept after the Third Round.

Chapter 2
Solving Polynomial Systems

The purpose of this chapter is to present the main notions relevant to the System Solving step of an algebraic attack, from the underlying theory to the description of the solving algorithms and their complexity analysis.

Contents

2.1 Ideals and Varieties

The first algebraic object which may come in mind to formalize system solving is the one of *algebraic variety*. The variety of a system $\mathcal{F} = \{f_1, \ldots, f_m\}$ in n variables over a field $\mathbb{K}$ can be defined as the subset of $\overline{\mathbb{K}}^n$ on which all the f_i's vanish simultaneously. This object is in fact associated to the *ideal* $I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[\boldsymbol{x}]$ since it does not depend on a generating set and we will denote it by $\mathcal{V}(I)$ or $\mathcal{V}(\langle \mathcal{F} \rangle)$. To restrict ourselves to solutions belonging to a subfield $\mathbb{L} \subset \overline{\mathbb{K}}$, another convenient definition is

$$\mathcal{V}_{\mathbb{L}}(I) \stackrel{def}{=} \{\boldsymbol{z} \in \mathbb{L}^n : f_i(\boldsymbol{z}) = 0 \text{ for all } 1 \leqslant i \leqslant m\} = \{\boldsymbol{z} \in \mathbb{L}^n : \forall f \in I,\ f(\boldsymbol{z}) = 0\}\,.$$

Note that we recover $\mathcal{V}(I) = \mathcal{V}_{\overline{\mathbb{K}}}(I)$. More specifically, we will be interested in $\mathcal{V}_{\mathbb{K}}(I)$ when $\mathbb{K}$ is the finite field $\mathbb{F}_q$. If $I_{\mathbb{F}_q}$ stands for the ideal generated by $\mathcal{F} \cup \{x_i^q - x_i : 1 \leqslant i \leqslant n\}$, we obtain $\mathcal{V}\left(I_{\mathbb{F}_q}\right) = \mathcal{V}_{\mathbb{F}_q}(I)$.

Coming back to the general case, one can go in the opposite direction from an arbitrary set a points $\mathcal{W} \subset \mathbb{K}^n$ by defining

$$I(\mathcal{W}) \stackrel{def}{=} \{f \in \mathbb{K}[\boldsymbol{x}] : \forall \boldsymbol{z} \in \mathcal{W},\ f(\boldsymbol{z}) = 0\}. \tag{2.1}$$

This choice of notation is hardly arbitrary since any such subset of $\mathbb{K}[\boldsymbol{x}]$ is trivially a polynomial ideal, that we call *the* ideal of $\mathcal{W}$.

Radical ideals. This subset is far from being the unique ideal whose elements vanish on $\mathcal{W}$. Informally, it can be seen as the biggest one of this kind: if for some $\ell \in \mathbb{Z}_{>0}$ the polynomial f^ℓ belongs to $I(\mathcal{W})$, it easily follows that $f \in I(\mathcal{W})$. This motivates the following definition.

Definition 2.1 (Radical ideal). An ideal $I \subset \mathbb{K}[\boldsymbol{x}]$ is said to be radical if for any $f \in \mathbb{K}[\boldsymbol{x}]$, the existence of $\ell \in \mathbb{Z}_{>0}$ such that $f^\ell \in I$ implies $f \in I$.

The ideal introduced in Equation (2.1) is indeed radical according to Definition 2.1. In the general case, the radical $\sqrt{I}$ corresponds to the smallest radical ideal containing I. More explicitly,

$$\sqrt{I} = \left\{f \in \mathbb{K}[\boldsymbol{x}] :\ \exists \ell \in \mathbb{Z}_{>0},\ f^\ell \in I\right\}.$$

The famous (strong) Nullstellensatz [CLO15, 4, §2, Theorem 6] states that if I is an ideal over an algebraically closed field $\mathbb{K}$, then $I(\mathcal{V}(I)) = \sqrt{I}$.

Zero-dimensional ideals. Another relevant notion for our applications is that of *zero-dimensional ideals*, *i.e.*, such that the associated variety is *finite*. Our interest in this definition is due to the fact that any ideal of the form $I_{\mathbb{F}_q}$ as we have just described is both radical and of dimension 0. For the sake of simplicity, we do not expand on the concept of Krull dimension and we only give the following property of 0-dimensional ideals.

Proposition 2.1 (Degree of a zero-dimensional ideal). *Let $I \subset \mathbb{K}[\boldsymbol{x}]$ be a* 0*-dimensional ideal,* i.e.*, such that $\#\mathcal{V}(I) < +\infty$. Then, the quotient $\mathbb{K}[\boldsymbol{x}]/I$ is a $\mathbb{K}$-vector space of finite dimension. This dimension is called the* degree *of I, denoted* $\deg(I)$.

Similarly to the degree of a polynomial in the univariate case, this notion is closely related to the number of solutions to an ideal. More precisely, it counts the number of solutions in $\overline{\mathbb{K}}$ with multiplicities, so that $\deg(I) \leqslant \#\mathcal{V}(I)$ and the equality holds when I is radical. We finish by giving a classical bound on the degree when the number of equations is the same as the number of variables.

Proposition 2.2 (Bézout bound). *Let $I = \langle f_1, \ldots, f_n \rangle \subset \mathbb{K}[\boldsymbol{x}]$ be a zero-dimensional ideal and let $d_1, \ldots, d_n$ be the degrees of $f_1, \ldots, f_n$ respectively. We have*

$$\deg(I) \leqslant \prod_{i=1}^{n} d_i.$$

In practice, an ideal I as in our theoretical exposition will be given by a fixed set of generators. However, as such, these polynomials might not really help to obtain the properties of I we want. In that respect, *Gröbner bases* that we now introduce turn out to be more useful.

2.2 Gröbner Bases

A first and rather standard way to present Gröbner bases is to view them as a generalization of the row echelon form for linear systems. In this section, we give their definition as well as some elementary facts. We also provide some background on homogeneous ideals.

2.2.1 Monomial Orderings

To carry on the analogy with linear systems, note that the row echelon form (even *reduced*) is not unique because there are several ways to associate a matrix to a given linear system in n variables. For instance, there are $n!$ different *orders* on the columns which correspond to $n!$ distinct orders on the unknowns. Similarly, a Gröbner basis will be defined at least implicitly with respect to a *monomial ordering*. A monomial in $\mathbb{K}[\boldsymbol{x}]$ refers to any product of the form $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, and the notion of monomial ordering has to go beyond simply ordering variables because we now deal with higher degree polynomials.

Definition 2.2 (Monomial ordering). A monomial ordering $\prec$ of $\mathbb{K}[\boldsymbol{x}]$ is a relation on the set $\mathcal{M}$ of monomials of $\mathbb{K}[\boldsymbol{x}]$ such that:

- the ordering $\prec$ is total on $\mathcal{M}$;
- if $\mu_1 \prec \mu_2$ and $\nu \in \mathcal{M}$, then $\mu_1 \nu \prec \mu_2 \nu$;
- $\prec$ is a well-ordering, *i.e.*, every nonempty subset of $\mathcal{M}$ has a smallest element under $\prec$.

In the following, we will mostly focus on the so-called Lexicographical (LEX) and Degree Reverse Lexicographical (DRL) orderings.

Definition 2.3 (Lexicographical ordering). Given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, we define:

- $x_1^{\alpha_1} \ldots x_n^{\alpha_n} \prec_{\text{lex}} x_1^{\beta_1} \ldots x_n^{\beta_n}$ if the leftmost non-zero entry $\boldsymbol{\alpha} - \boldsymbol{\beta}$ is negative.

On variables, we obtain $x_n \prec_{\text{lex}} \cdots \prec_{\text{lex}} x_1$. On higher degree monomials, LEX is still quite intuitive as it corresponds to the usual way of arranging words in alphabetical order. To compare two monomials, one has to look at the largest variables first and then keep in mind that a given variable dominates any monomial which involves smaller variables.

Example 2.1. In $\mathbb{K}[x_1, x_2, x_3]$ we have $x_1^2x_2^2x_3^{12} \prec_{\text{lex}} x_1^3x_2^2x_3$ because $(2, 2, 12) - (3, 2, 1) = (-1, 0, 11)$ and $x_3^7 \prec_{\text{lex}} x_2^5x_3$ because $(0, 0, 7) - (0, 5, 1) = (0, -5, 7)$.

As above, we can obtain $n!$ analogous orders by sorting the initial variables in a different way. Perhaps more crucially, the LEX order is an *elimination* ordering: if $\mathcal{G}$ is a LEX-Gröbner basis of $I \subset \mathbb{K}[\boldsymbol{x}]$, the set $\mathcal{G} \cap \mathbb{K}[x_{v+1}, \ldots, x_n]$ is a LEX-Gröbner basis of the ideal $I \cap \mathbb{K}[x_{v+1}, \ldots, x_n]$ for any $0 \leqslant v \leqslant n-1$. As we will see below, this feature makes it well-suited to solve polynomial systems.

Contrary to LEX, the Degree Reverse Lexicographical ordering is a *graded* ordering. This means that monomials are sorted by total degree first, the total degree of $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ being defined as

$$\deg(x_1^{\alpha_1} \ldots x_n^{\alpha_n}) \stackrel{def}{=} \textstyle\sum_{i=1}^{n} \alpha_i.$$

In case of a tie on this degree, variables involved come into play according to the following rule. We keep the same notation as in Definition 2.3.

Definition 2.4 (Degree Reverse Lexicographical ordering). If $\deg(x_1^{\alpha_1} \ldots x_n^{\alpha_n}) = \deg(x_1^{\beta_1} \ldots x_n^{\beta_n})$, $x_1^{\alpha_1} \ldots x_n^{\alpha_n} \prec_{\text{drl}} x_1^{\beta_1} \ldots x_n^{\beta_n}$ if and only if the rightmost non-zero entry in $\boldsymbol{\alpha} - \boldsymbol{\beta}$ is positive.

This second ordering is less intuitive. Among monomials of a given degree D, the largest monomial is x_1^D, then come those in x_1 and x_2 only, then involving x_1, x_2 and x_3, etc. Between two monomials in the same variables $x_1, \ldots, x_j$, the smallest one contains the largest power of x_j.

Example 2.2. In $\mathbb{K}[x_1, x_2, x_3]$ we have $x_1^3x_2^5x_3^2 \prec_{\text{drl}} x_1^2x_2^9x_3$ because $(3, 5, 2) - (2, 9, 1) = (1, -4, 1)$. The graded LEX ordering would sort these monomials in reverse order.

In practice, DRL is of interest because it seems to give faster computation time compared to other orders. However, we can always imagine the possibility of a more appropriate choice which benefits from the structure of the input system. The main issue is that it is unknown how to discover such an ordering in general.

2.2.2 Gröbner Bases: Definitions and Basic Properties

This section gives the definition of a Gröbner basis for an ideal I with respect to a monomial order $\prec$ as well as some elementary properties. Even if this notion does not depend the generating set, we will often talk about Gröbner bases of any polynomial system $\mathcal{F}$ which generates I.

For a polynomial $f = \sum_{\mu \in \mathcal{M}} a_\mu \mu \in \mathbb{K}[\boldsymbol{x}]$, we denote the leading monomial by $\mathrm{LM}_\prec(f)$, *i.e.*, $\max_\prec \{\mu \in \mathcal{M},\ a_\mu \neq 0\}$, the leading coefficient by $\mathrm{LC}_\prec(f) \stackrel{def}{=} a_{\mathrm{LM}_\prec(f)}$ and the leading term by $\mathrm{LT}_\prec(f) \stackrel{def}{=} \mathrm{LC}_\prec(f)\mathrm{LM}_\prec(f)$. For an ideal I or more generally for a set S, we define the *monomial ideal*

$$\mathrm{LM}_\prec(I) \stackrel{def}{=} \langle \{\mathrm{LM}_\prec(f),\ f \in I\} \rangle .$$

Dickson's lemma [CLO15, 2, §4, Theorem 5] states that such an ideal is finitely generated by *monomials*.

Definition 2.5 (Gröbner basis). Let $\prec$ be a monomial ordering and let $I \subset \mathbb{K}[\boldsymbol{x}]$ be an ideal. A Gröbner basis for I with respect to $\prec$ is any subset $\mathcal{G} = \{g_1, \ldots, g_k\} \subset I$ such that

$$\mathrm{LM}_\prec(I) = \langle \mathrm{LM}_\prec(g_1), \ldots, \mathrm{LM}_\prec(g_k) \rangle .$$

A first consequence of Definition 2.5 is that $\mathcal{G}$ is actually a generating set for I, hence the name *basis*. Furthermore, it is easy to see that such a Gröbner basis is not *unique*. Any set of polynomials obtained by adding other elements of I is a larger Gröbner basis and we can also disrupt the non-leading monomials of the polynomials in $\mathcal{G}$ to obtain another Gröbner basis $\mathcal{G}'$ such that $\#\mathcal{G}' = \#\mathcal{G}$. This apparent issue is solved by the following definition.

Definition 2.6 (Reduced Gröbner basis). A Gröbner basis $\mathcal{G}$ for an ideal I is said to be reduced if for every polynomial $g \in \mathcal{G}$ we have $\mathrm{LC}(g) = 1$ and $\mu \notin \mathrm{LM}(\mathcal{G} \backslash \{g\})$.

Indeed, for a given monomial ordering, any ideal has a unique reduced Gröbner basis.

Normal forms. The introduction of Gröbner bases by Buchberger [Buc65] was motivated by the study of the Ideal Membership problem. Given a set of polynomials $\{h_1, \ldots, h_m\}$ and $f \in \mathbb{K}[\boldsymbol{x}]$, the goal is to decide whether $f \in I = \langle h_1, \ldots, h_m \rangle$. In the univariate case $n = 1$, the ring $\mathbb{K}[\boldsymbol{x}]$ is principal so that any ideal I is generated by one element. To solve the problem, a convenient generator is the gcd g of all polynomials in I because we simply have to check whether f is divisible by g. This g is easily seen to be the only element in the reduced Gröbner basis of I. In the general case as well, Gröbner bases allow to solve the Ideal Membership problem by computing *normal forms*. The normal form of a polynomial f with respect to an ideal I extends the notion of *remainder* which makes sense when $n = 1$.

Proposition 2.3 (Normal form, Proposition 1 p. 83, [CLO15]). *Given an ideal $I \subset \mathbb{K}[\boldsymbol{x}]$, a polynomial $f \in \mathbb{K}[\boldsymbol{x}]$ and a monomial ordering $\prec$, there exists a unique decomposition $f = \rho + g$ such that $g \in I$ and such that no monomials present in ρ belong to the ideal $LM_\prec(I)$. The polynomial ρ is called the Normal Form of f with respect to I and denoted by $NF_{I,\prec}(f)$ or simply $f\ mod_\prec\ I$.*

Proof. To prove uniqueness, we consider two decompositions $f = \rho_1 + g_1$ and $f = \rho_2 + g_2$ such that $g_1 \neq g_2$ belong to I and such that $\rho_1 \neq \rho_2$ do not have any monomials in $\mathrm{LM}_\prec(I)$. An ideal being stable by addition, the polynomial $\rho_1 - \rho_2 = g_2 - g_1$ belongs to I and, a fortiori, $\mathrm{LM}_\prec(\rho_1 - \rho_2) \in \mathrm{LM}_\prec(I)$. By assumption on ρ_1 and ρ_2, this implies $\rho_1 - \rho_2 = 0$ and $g_1 = g_2$. To prove existence, we rely on the following Algorithm 1.

Algorithm 1: Normal form.

Input: A monomial ordering $\prec$, a Gröbner basis $\mathcal{G}$ for an ideal I with respect to $\prec$ and a polynomial $f \in \mathbb{K}[\boldsymbol{x}]$.
Output: A polynomial $\rho \in \mathbb{K}[\boldsymbol{x}]$ such that $f - \rho \in I$ and such that no monomials present in ρ belong to the ideal $\mathrm{LM}_\prec(I)$.

$\rho \leftarrow f$
while $\exists$ *monomial* t *in* ρ *and* $g \in \mathcal{G}$ *such that* $LM_\prec(g) \mid t$ **do**
  $\rho \leftarrow \rho - \frac{t}{\mathrm{LM}_\prec(g)} g$
end
return ρ

This algorithm terminates as there is no infinitely decreasing sequence of monomials with respect to $\prec$ (this is a consequence of Dickson's lemma). Its correctness is trivial in regard to the condition in the **while** loop. □

Due to its reduction step, Algorithm 1 can be viewed as a multivariate extension of the Euclidean division for univariate polynomials. Note also that it strongly relies on the knowledge of a Gröbner basis for I. This shows that Gröbner bases are a crucial tool for efficient computation in $\mathbb{K}[\boldsymbol{x}]/I$, which may have broader applications than testing Ideal Membership.

Algorithm 1 can be generalized. For that purpose, we need to order polynomials and thus consider polynomial sequences. For a sequence $\mathcal{S} = (s_1, \ldots, s_\ell)$ such that $\{s_1, \ldots, s_\ell\}$ is not necessarily a Gröbner basis, there still exists a *reduction algorithm*. Its output on a polynomial f is a polynomial usually called the reduction of f modulo $\mathcal{S}$, that we denote by $\rho \overset{def}{=} NF_{\mathcal{S},\prec}(f)$ or $\rho \overset{def}{=} f \bmod_\prec \mathcal{S}$. Even if we do not make this algorithm explicit, see [CLO15, Theorem 3 p. 64], two remarks are in order. The first one is that this ρ coincides with the result of Algorithm 1 when $\{s_1, \ldots, s_\ell\}$ is a Gröbner basis. If $\pi(\mathcal{S})$ stands for an arbitrary permutation of the input sequence, the second one is that $NF_{\mathcal{S},\prec}(f)$ and $NF_{\pi(\mathcal{S}),\prec}(f)$ are in general different.

Buchberger's algorithm [Buc76]. From now on, we fix an arbitrary order $\prec$ and our notations become implicit with respect to it. For such an ordering, the work of Buchberger already provides a Gröbner basis algorithm. It is based on the following definition, whose motivation is to generate new leading terms by cancellation.

Definition 2.7 (S-polynomial). Let f, g be nonzero polynomials in $\mathbb{K}[\boldsymbol{x}]$ and let $\mu = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$. The S-polynomial of the polynomial pair $\{f, g\}$ with respect to $\prec$ is defined as

$$S(f,g) \overset{def}{=} \frac{\mu}{\mathrm{LM}(f)} f - \frac{\mu}{\mathrm{LM}(g)} g.$$

By construction, the S-polynomial $S(f, g)$ is a polynomial combination between f and g. Given a Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_\ell\}$, this already explains that the result of Algorithm 1 on $S(g_i, g_j)$ for any $1 \leqslant i < j \leqslant \ell$ will be zero. For an arbitrary set of polynomials, the converse is also true.

Theorem 2.1 (Buchberger's first criterion, Theorem 6 p. 86, [CLO15]). *Let $I = \langle \mathcal{G} \rangle \subset \mathbb{K}[\boldsymbol{x}]$ be an ideal. The set $\mathcal{G} = \{g_1, \ldots, g_\ell\}$ is a Gröbner basis if and only if for all $1 \leqslant i < j \leqslant \ell$, the S-polynomial $S(g_i, g_j)$ reduces to 0 modulo $\mathcal{G}$.*

From there, Buchberger's algorithm proceeds incrementally starting from the set $\mathcal{G}$ given by the input polynomial sequence. It consists in (a) selecting one pair of elements in $\mathcal{G}$ and compute the S-polynomial (b) reducing it modulo the current basis (c) adding the remainder to $\mathcal{G}$ if it is not zero, and overall repeating steps (a)(b)(c) until the conclusion of Theorem 2.1 is satisfied. A full description can be found in [CLO15, Theorem 2 p. 91].

2.2.3 Solving with Gröbner Bases

Even though other types of algorithms also exist[1], we will be mostly interested in solving strategies based, at least implicitly, on computing Gröbner bases.

In this context, let us come back to the role played by the LEX ordering. From its elimination property given in Section 2.2.1, we can obtain the following result.

Proposition 2.4. *The LEX-Gröbner basis of a 0-dimensional ideal I is of the form $\mathcal{G}_{lex} = \cup_{j=1}^{n} \mathcal{G}_j$, where*

$$\mathcal{G}_j \overset{def}{=} \left\{ g_{j,1}(x_j, \ldots, x_n), \ldots, g_{j,s_j}(x_j, \ldots, x_n) \right\} \subset \mathbb{K}[x_j, \ldots, x_n],$$

such that $s_j \geqslant 1$ for $1 \leqslant j \leqslant n-1$ and $s_n = 1$. In particular, we have

$$\mathcal{G}_n = \{ g_{n,s_n}(x_n) \} \overset{def}{=} \{ g_n(x_n) \}.$$

The shape of the Gröbner basis in Proposition 2.4 is already enough for our purposes. Indeed, we can proceed by back substitution starting from a fixed root of $g_n(x_n)$ and then solving a sequence of univariate polynomials. Under certain assumptions, it is even enough to solve only one univariate equation.

Proposition 2.5 (Shape position, [GM87]). *A 0-dimensional ideal I is said to satisfy the Shape Lemma (or is in Shape position) if the LEX-Gröbner basis of I is of the form*

$$\{x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\},$$

where $\deg(g_n) = \deg(I)$ and $\deg(g_i) < \deg(I)$ for $1 \leqslant i \leqslant n-1$.

[1] For instance exhaustive search.

Even if we will not need such a result, this proposition turns out to be *generic* for radical ideals after a linear change of coordinates. More importantly for us, Proposition 2.4 and Proposition 2.5 show that solving the system is almost straightforward once the LEX-Gröbner basis $\mathcal{G}_{\text{lex}}$ is known.

Unfortunately, obtaining it directly is in general slower than with another monomial ordering. On the contrary, as already mentioned, computing DRL-Gröbner bases is faster from a practical perspective. This explains that the standard approach produces $\mathcal{G}_{\text{lex}}$ by means of another algorithm taking $\mathcal{G}_{\text{drl}}$ as input.

Change of ordering. To move between two Gröbner bases for 0-dimensional systems, one usually employs FGLM [FGLM93]. This procedure can be understood as a linear algebra algorithm in $\mathbb{K}[\boldsymbol{x}]/I$, where the knowledge of the first Gröbner basis allows for efficient computation. Its complexity will be estimated by

$$\mathcal{O}(n\deg(I)^{\omega}), \tag{2.2}$$

where n is the number of variables and where $2 \leqslant \omega \leqslant 3$ is a linear algebra exponent. As $\deg(I) \leqslant \#\mathcal{V}(I)$, this cost is polynomial in the number of solutions.

2.2.4 Homogeneous Ideals

Homogeneous polynomials correspond to polynomials whose all monomials have the same total degree. For $d \in \mathbb{N}$, let us denote by $R_d \overset{def}{=} \mathbb{K}[\boldsymbol{x}]_d$ the vector space of homogeneous polynomials of degree d in $R = \mathbb{K}[\boldsymbol{x}]$. Since a classical basis is the set of all degree d monomials, elementary combinatorics give $\dim_{\mathbb{K}}(R_d) = \binom{n+d-1}{d}$. A homogeneous ideal is generated by homogeneous polynomials. Such an ideal I can be expressed as the direct sum

$$I = \bigoplus_{d\in\mathbb{N}} I_d,$$

where $I_d \overset{def}{=} I \cap R_d$ is finite-dimensional. The quotient ring R/I can then be written as $R/I = \bigoplus_{d\in\mathbb{N}} R_d/I_d$.

To capture the combinatorial structure of such a quotient, we will adopt the following definitions.

Definition 2.8 (Hilbert function and Hilbert series). Let $I \subset R$ be a homogeneous ideal. The Hilbert function $\mathcal{HF}_{R/I}$ of the quotient ring R/I is defined by

$$\begin{aligned} \mathcal{HF}_{R/I} : \mathbb{N} &\longrightarrow \mathbb{N} \\ d &\longmapsto \dim_{\mathbb{K}}(R_d/I_d), \end{aligned}$$

and the Hilbert series $\mathcal{H}_{R/I}$ is the formal series defined by

$$\mathcal{H}_{R/I}(z) \overset{def}{=} \sum_{d=0}^{\infty} \mathcal{HF}_{R/I}(d) z^d.$$

The case of 0-dimensional ideals is of particular interest. For such ideals, the quotient R/I is a finite-dimensional vector space. Therefore, the Hilbert series is a polynomial whose evaluation at 1 gives

$$\mathcal{H}_{R/I}(1) = \sum_{d=0}^{\infty} \dim_{\mathbb{K}}(R_d/I_d) = \dim_{\mathbb{K}}(R/I) = \deg(I).$$

Finally, the degree of this polynomial is one less than the following integer which deserves definition.

Definition 2.9 (Degree of regularity). Let $I \subset R$ be a 0-dimensional homogeneous ideal. The degree of regularity of I, denoted $d_{\text{reg}}(I)$, is the smallest integer $d \in \mathbb{N}$ such that $I_d = R_d$.

2.3 Generic Sequences

This section introduces *regular* and *semi-regular* sequences. We believe that presenting these objects prior to describing solving algorithms may help the reader to better understand their complexity analysis. A first reason is that such systems do not have particular algebraic properties, which explains that their Hilbert series are known. Since regularity is a generic property for polynomial equations (see Theorem 2.3 below), another more pragmatic one is that we hope to encompass most practical applications.

Genericity. In algebraic geometry, a property is said to be *generic* in an irreducible algebraic variety X if it holds on a non-empty Zariski open subset of X. In our case, this variety is given by a family of polynomial sequences which is also a vector space of finite dimension. In the following, we consider the vector space $\mathcal{E}_{m,n,\boldsymbol{d}}$ of homogeneous sequences $(f_1, \ldots, f_m)$ in $\mathbb{K}[\boldsymbol{x}]$ such that $\deg(f_i) = d_i$ for $1 \leqslant i \leqslant m$.

2.3.1 Regular Sequences

The notion of regularity aims at describing the relationship between the dimension of an ideal and the number of its generators. We caution the reader that it should not be confused with the one of *degree of regularity* (Definition 2.9).

Definition 2.10 (Regular sequence). A homogeneous sequence $(f_1, \ldots, f_m)$ in R is regular if for all $1 \leqslant i \leqslant m$, the polynomial f_i does not divide 0 in the quotient ring $R/\langle f_1, \ldots, f_{i-1}\rangle$.

In other words, the sequence $(f_1, \ldots, f_m)$ is regular if and only if all algebraic relations between the f_i's are a consequence of those of the form $f_i f_j - f_j f_i = 0$. In the general case, such relations are called *syzygies* and these particular ones are referred to as *trivial*.

Definition 2.11 (Syzygy). Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a polynomial sequence in R (affine or homogeneous). A syzygy for $\mathcal{F}$ is a vector $(s_i)_{1 \leqslant i \leqslant m} \in R^m$ such that $\sum_{i=1}^{m} s_i f_i = 0$.

Its degree is defined as $\max_{1 \leqslant i \leqslant m} (\deg(f_i) + \deg(s_i))$. Finally, the set of all syzygies of $\mathcal{F}$ is an R-module denoted by $\mathrm{Syz}(\mathcal{F})$.

We will come back to this definition in more depth when discussing the complexity of computing Gröbner bases. Prior to that, we note that the very simple form of $\mathrm{Syz}(\mathcal{F})$ in the regular case allows to obtain an explicit formula for the Hilbert series as initially announced.

Theorem 2.2 (Exercise p. 137, [Frö98]). *Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a homogeneous regular sequence in $\mathcal{E}_{m,n,\boldsymbol{d}}$. We have*

$$\mathcal{H}_{R/\langle \mathcal{F} \rangle}(z) = \frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1-z)^n}. \tag{2.3}$$

Conversely, any sequence in $\mathcal{E}_{m,n,\boldsymbol{d}}$ whose Hilbert series is as in Equation (2.3) is regular.

In the particular case $m = n$, we obtain the polynomial

$$\mathcal{H}_{R/\langle \mathcal{F} \rangle}(z) = \prod_{i=1}^{n} \left(1 + \cdots + z^{d_i - 1}\right).$$

This implies that an ideal I generated by a regular sequence with as many equations as variables is zero-dimensional with degree of regularity

$$d_{\mathrm{reg}}(I) = \sum_{i=1}^{n} (d_i - 1) + 1. \tag{2.4}$$

This quantity is often referred to as the *Macaulay bound* [Laz83; Mac02]. Moreover, the degree of I is easily seen to be equal to $\deg(I) = \prod_{i=1}^{n} d_i$, which corresponds to the upper bound in Proposition 2.2.

Finally, as mentioned above, "almost all" sequences in $\mathcal{E}_{m,n,\boldsymbol{d}}$ are regular when $n \geqslant m$.

Theorem 2.3. *When $n \geqslant m$, the set of regular sequences is a non-empty Zariski open subset of $\mathcal{E}_{m,n,\boldsymbol{d}}$.*

Proof. See [Par10]. Note that the nonemptiness is trivial since the set of regular sequences in $\mathcal{E}_{m,n,\boldsymbol{d}}$ already contains $(x_1^{d_1}, \ldots, x_m^{d_m})$. □

2.3.2 Semi-Regular Sequences

Sadly, Definition 2.10 is not relevant for systems such that $m > n$ which abound in our applications. This is because the polynomial f_i will always be a zero divisor in $R/\langle f_1, \ldots, f_{i-1} \rangle$ for $n < i \leqslant m$. With this in mind, the notion of regularity has been extended to this *overdefined* case $m > n$ by Bardet in her thesis.

Definition 2.12 (Semi-regular sequence, [Bar04]). Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a homogeneous sequence such that the ideal $I = \langle \mathcal{F} \rangle$ is 0-dimensional with degree of regularity d_{reg}. It is said to be *semi-regular* if $I \neq R$ and if for any $1 \leqslant i \leqslant m$, the equality $g_i f_i = 0$ in $R/\langle f_1, \ldots, f_{i-1} \rangle$ with $\deg(g_i f_i) < d_{\text{reg}}$ implies $g_i = 0$ in $R/\langle f_1, \ldots, f_{i-1} \rangle$.

Over $\mathbb{F}_2$, the Frobenius map $x \mapsto x^2$ is the identity. This fact is taken into account in the following definition, for boolean systems.

Definition 2.13 (Semi-regular sequence over $\mathbb{F}_2$, [Bar04]). Let S denote the quotient ring $\mathbb{F}_2[\boldsymbol{x}]/\langle x_1^2, \ldots, x_n^2 \rangle$. A homogeneous sequence $\mathcal{F} = (f_1, \ldots, f_m)$ with degree of regularity d_{reg} is semi-regular over $\mathbb{F}_2$ if $I \neq S$ and if for $1 \leqslant i \leqslant m$, the equality $g_i f_i = 0$ in $S/\langle f_1, \ldots, f_{i-1} \rangle$ with $\deg(g_i f_i) < d_{\text{reg}}$ implies $g_i = 0$ in $S/\langle f_1, \ldots, f_i \rangle$.

It should not be so surprising that one knows the Hilbert series of a semi-regular sequence. First, this is a polynomial of degree at most d_{reg}. Moreover, the syzygies in degree $< d_{\text{reg}}$ which are captured by the definitions are of the same nature as for regular systems. In that respect, the proofs of Theorem 2.4 and Theorem 2.5 below are extremely similar to the one of Theorem 2.2.

Theorem 2.4 (Proposition 3.2.5 p. 58, [Bar04]). *Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a semi-regular sequence in $\mathcal{E}_{m,n,\boldsymbol{d}}$ and let $S_{m,n,\boldsymbol{d}}(z) \stackrel{def}{=} \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}$. We have*

$$\mathcal{H}_{R/\langle \mathcal{F} \rangle}(z) = \left[S_{m,n,\boldsymbol{d}}(z) \right]^+,$$

with $\left[\sum_{j \geqslant 0} a_j z^j \right]^+ \stackrel{def}{=} \sum_{j \geqslant 0} c_j z^j$, where $c_j = a_j$ if $a_i > 0$ for $0 \leqslant i \leqslant j$ and $c_j = 0$ otherwise (truncation after the first-non positive coefficient).

Theorem 2.5 (Corollary 3.3.8 p. 68, [Bar04]). *Let $\mathcal{F} = (f_1, \ldots, f_m)$ be a boolean semi-regular sequence in $\mathcal{E}_{m,n,\boldsymbol{d}}$ and let $T_{m,n,\boldsymbol{d}}(z) \stackrel{def}{=} \frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})}$. We have*

$$\mathcal{H}_{R/\langle \mathcal{F} \rangle}(z) = \left[T_{m,n,\boldsymbol{d}}(z) \right]^+.$$

In these theorems, we reserve the term "Hilbert series" for the polynomial $\mathcal{H}_{R/\langle \mathcal{F} \rangle}$ and we will refer to $S_{m,n,\boldsymbol{d}}$ (resp. $T_{m,n,\boldsymbol{d}}$) as the generating series of the ideal $\langle \mathcal{F} \rangle$. Finally, note that there is no analogue of Theorem 2.3 regarding the genericity of semi-regular sequences. Such a result relies on the famous Fröberg conjecture [Frö85], which has only been proven in some specific cases (see [Bar04, Theorem 1.6.4 p. 22]).

Over a finite field, the Zariski topology is discrete and the set of semi-regular sequences in $\mathcal{E}_{m,n,\boldsymbol{d}}$ is obviously finite. To obtain a rough estimate for the probability of being semi-regular, we can divide its cardinality by $\#\mathcal{E}_{m,n,\boldsymbol{d}}$ (keeping in mind that this number is possibly zero and for sure not computable in practice).

2.4 Solving Techniques

While Buchberger's method [Buc76] is already a Gröbner basis algorithm, it is difficult to analyze. This is due both to the dependency on the monomial order and the fact that polynomial pairs are chosen at random to compute S-polynomials. However, relying on a *graded ordering* seems to give a somewhat natural choice[2] by selecting pairs of smaller degree first. It also allows to continue the analogy with linear algebra.

2.4.1 Macaulay Matrix, Lazard's Theorem

This link will be more concrete thanks to the notion of *Macaulay matrix*, which can be understood as a direct generalization of the matrix of a linear system.

Definition 2.14 (Macaulay matrix, [Mac94]). The Macaulay matrix in degree d of a sequence $\mathcal{F} = (f_1, \dots, f_m)$ such that $\deg(f_i) = d_i$ with respect to a graded monomial order $\prec$, denoted[3] $\mathcal{M}\mathrm{ac}_{\leqslant d}(\mathcal{F})$, is the coefficient matrix of $(\mu_{i,j} f_j)_{i,\ 1 \leqslant j \leqslant m}$ where $\mu_{i,j}$ is any monomial of degree $\leqslant d - \deg(f_i)$ and whose columns are indexed by all monomials of degree $\leqslant d$ sorted in decreasing order with respect to $\prec$.

Since the order on the rows is less important, we will mostly talk about Macaulay matrices of systems rather than of sequences. A crucial remark is that row operations on $\mathcal{M}\mathrm{ac}_{\leqslant d}(\mathcal{F})$ readily correspond to polynomial combinations between the f_i's, hence operations in the ideal generated by $\mathcal{F}$. In particular, one can grasp polynomial reduction in terms of Gaussian elimination.

If $\mathcal{F}$ is homogeneous generating an ideal I, we may restrict ourselves to the submatrix of $\mathcal{M}\mathrm{ac}_{\leqslant d}(\mathcal{F})$ given by the rows corresponding to monomials $\mu_{i,j}$ of exact degree $d - \deg(f_i)$ and then remove the rightmost columns labelled by degree $< d$ monomials since they will be all-zero. Let us denote by $\mathcal{M}\mathrm{ac}_d(\mathcal{F})$ the final result. This time, performing Gaussian elimination yields a basis for I_d. Moreover, as we have considered columns in decreasing order, the associated leading terms give $\mathrm{LT}(I_d)$.

Theorem 2.6 (Lazard's theorem, [Laz83]). *Let $\mathcal{F} = (f_1, \dots, f_m)$ be a homogeneous sequence such that $\deg(f_i) = d_i$. There exists a degree D for which the polynomials corresponding to the rows in the row-echelon form of $\mathcal{M}ac_d(\mathcal{F})$ for $d = \min(d_i)_{i=1}^m$ to $d = D$ are a Gröbner basis, with respect to $\prec$, of the ideal generated by $\mathcal{F}$.*

Following [CG21, Definition 6], the *least possible* degree D in Theorem 2.6 will be referred to as the *solving degree* of $\mathcal{F}$. From our discussion, it is easy to see that it is an invariant of the ideal. Indeed, when the ideal is homogeneous, it coincides with the maximal degree of a polynomial in the reduced Gröbner basis (see for example [CG21, Remark 7]).

[2] Sometimes called *normal strategy*.

[3] The monomial ordering $\prec$ will be implicit in the notation.

The case of an affine system $\mathcal{F}$ can reduce to the homogeneous one. For instance, we may consider the homogenized system $\mathcal{F}^{(z)} = \{f_1^{(z)}, \ldots, f_m^{(z)}\}$ obtained by introducing an extra variable z and then applying the map

$$\begin{aligned} \mathbb{K}[\boldsymbol{x}] &\longrightarrow \mathbb{K}[\boldsymbol{x}, z] \\ f(x_1, \ldots, x_n) &\longmapsto f^{(z)}(x_1, \ldots, x_n, z) \stackrel{def}{=} \left(\frac{1}{z}\right)^{\deg(f)} f\left(\frac{x_1}{z}, \ldots, \frac{x_n}{z}\right). \end{aligned} \tag{2.5}$$

Theorem 2.6 states that Gaussian elimination on $\mathcal{M}\mathrm{ac}_d(\mathcal{F}^{(z)})$ up to the solving degree of $\mathcal{F}^{(z)}$ gives a Gröbner basis. To come back to the initial system, we may specialize the corresponding polynomials by

$$\begin{aligned} \mathbb{K}[\boldsymbol{x}, z] &\longrightarrow \mathbb{K}[\boldsymbol{x}] \\ f^{(z)}(x_1, \ldots, x_n, z) &\longmapsto f(x_1, \ldots, x_n) \stackrel{def}{=} f^{(z)}(x_1, \ldots, x_n, 1). \end{aligned}$$

General complexity bound. We can now deduce an upper bound on the cost of computing a Gröbner basis following Lazard's approach.

Proposition 2.6 (Proposition 1, [BFS15]). *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset \mathbb{K}[\boldsymbol{x}]$ be a homogeneous system in n variables with solving degree D. The number of $\mathbb{K}$-operations to compute a Gröbner basis for $\mathcal{F}$ is upper bounded by*

$$\mathcal{O}\left(mD\binom{n+D-1}{D}^{\omega}\right), \tag{2.6}$$

where $2 \leqslant \omega \leqslant 3$ is the linear algebra exponent.

Proof. The complexity is clearly dominated by that of Gaussian elimination on the Macaulay matrix $\mathcal{M}\mathrm{ac}_D(\mathcal{F})$, which has $\leqslant m\binom{n+D-1}{D}$ rows and $\binom{n+D-1}{D}$ columns. Note that Storjohann's algorithm [Sto00] allows to compute the row echelon form of an $M \times N$ matrix of rank r in $\mathcal{O}(MNr^{\omega-2})$ operations. The result follows since the rank of $\mathcal{M}\mathrm{ac}_D(\mathcal{F})$ is upper bounded by $\binom{n+D-1}{D}$. □

Corollary 2.1. *The number of $\mathbb{K}$-operations to compute a Gröbner basis for an affine system $\mathcal{F}$ containing m equations in n variables such that $\mathcal{F}^{(z)}$ has solving degree D_z can be upper bounded by*

$$\mathcal{O}\left(mD_z\binom{n+D_z}{D_z}^{\omega}\right), \tag{2.7}$$

where $2 \leqslant \omega \leqslant 3$ is the linear algebra exponent.

Obtaining the solving degree. In Lazard's approach, the operating degree D must be given as input to the algorithm. Another remark is that the costs in Equation (2.6) and Equation (2.7) are exponential in the solving degree. These two observations make it crucial to estimate this value in order to understand the complexity of computing a

Gröbner basis. For a homogeneous 0-dimensional ideal I, this reduces to studying the dimensions of the vector spaces I_d. In favorable cases, they can simply be read-off if we know the Hilbert series. More systematically, we may consider the associated Macaulay matrices. For an affine system $\mathcal{F}$, it is not even clear that the solving degree of $\mathcal{F}^{(z)}$ and the cost given in Corollary 2.1 will be a good approximation of the original Gröbner basis complexity.

2.4.2 Generic Algorithms

This subsection presents the main solving algorithms which are generally considered in algebraic cryptanalysis. At a very theoretical level, they can be obtained by combining ideas from Buchberger's and Lazard's methods. In particular, we may express all these techniques in terms of Macaulay matrices. Finally, we will refer to them as *generic* because they do not exploit particular features of the input system.

Faugère's algorithms. Faugère's F_4 [Fau99] and F_5 [Fau02] represent the state-of-the-art in terms of Gröbner basis computation. In fact, they are used in a much broader set of applications than the field of cryptology. Since describing these algorithms in depth is outside the scope of this exposition, we simply stress the most important ideas.

Instead of considering polynomial pairs one at a time as in Buchberger's original approach, the F_4 algorithm picks several pairs simultaneously. This is usually done according to the normal strategy, by selecting all pairs for which the degree of the S-polynomial is minimal. Once these *critical pairs* have been chosen, a pre-processing phase builds a matrix containing the reductions by the current basis. Then, one performs row-reduction as in Lazard's method. Even though they are in general as wide as in Lazard's, matrices in F_4 are usually much smaller regarding the number of rows. Another advantage is that the set of critical pairs can be updated using Buchberger's criterion (Theorem 2.1). This allows to avoid redundant computation and more importantly to ensure termination without requiring an input solving degree. From a cryptanalytic perspective, understanding how F_4 works is relevant since it is the default algorithm implemented in the Magma computer algebra system [BCP97]. This software has been adopted by a large part of the community and it is also the one used in most of our experiments.

The rationale of F_5 is to avoid *reductions to zero* in a much more systematic way than in F_4. They correspond to row operations on the Macaulay matrix yielding zero linear combinations. Coming back to the polynomial representation, these reductions are associated to algebraic relations in the original system. More precisely, the F_5 criterion predicts the ones which are triggered by trivial syzygies. In the (semi)-regular case, this means that all unnecessary computation can be avoided. To implement this criterion, F_5 introduced the notion of *signature*. This algorithm later gave rise to a wide class of Gröbner basis techniques relying on the same concept. We refer to [EF17] for a detailed outline of this research area.

XL family. The XL algorithm [CKPS00] was introduced for cryptanalytic purposes. Its popularity among cryptographers lies in its simplicitly. Indeed, it was originally described in terms of linearization even without mentioning Gröbner bases.

The idea is to use Gaussian elimination on a Macaulay matrix in order to generate a univariate equation. This formulation shows that an implicit LEX-like order has to be chosen and that the operations in XL are actually performed within Lazard's method. A comparison with F_5 was later made in [Ars+04], showing that XL offers no advantage. Indeed, the degree D_{XL} reached by the latter is never smaller than that of Gröbner basis algorithms and the XL matrices can be huge in comparison to F_5. This second point must not sound surprising as very little care is taken in removing reductions to zero.

In more recent papers, XL corresponds to a somewhat different algorithm. When the system has a unique solution, it stands for a solver based on computing vectors in the right kernel of a Macaulay matrix. If this matrix sparse enough, the hope is to benefit from the use of the Wiedemann algorithm [Wie86] or its further improvements [Cop94; Tho02]. Indeed, a row-echelon form is no longer required. In fact, the original paper by Courtois *et al.* does not even mention sparse linear algebra. We may often refer to this strategy as the "XL-Wiedemann approach". Note that it has been implemented and studied in [CCNY12]. In a very favorable setting where the degree is known, the complexity is a follows. This bound implicitly assumes that the matrix is close to being square of size the number of columns or that the cost of obtaining a full-rank square submatrix is negligible compared to the XL complexity.

Proposition 2.7. *Let D be such that the Macaulay matrix $\mathcal{M}ac_{\leqslant D}(\mathcal{F})$ has a non-trivial right kernel, let n_μ its row weight and let $M_{\leqslant D}$ the number of columns. The cost of the XL-Wiedemann approach by finding a solution to the linear system $\mathcal{M}ac_{\leqslant D}(\mathcal{F})\boldsymbol{v}^\mathsf{T} = 0$ is given by*

$$\mathcal{O}\left(n_\mu M_{\leqslant D}^2\right). \tag{2.8}$$

Remark 2.1. We will often choose a hidden constant equal to 3 for the Block-Wiedemann algorithm, see for example [BBD08, Proposition 3 p. 219].

2.4.3 Towards Specific Strategies

Particular properties of the input polynomials – among others, the presence of algebraic structure or symmetries – must be taken into account in the analysis of generic solvers. Indeed, they directly impact the ranks of the Macaulay matrices, the degree of regularity, and more generally the Hilbert series of the ideal. A partial knowledge of these objects is sometimes sufficient to derive a first cost estimate. In some cases, specific features can be further exploited to devise enhanced algorithms.

Removing reductions to zero. A more complete understanding of the syzygy module may help to avoid redundant computation by incorporating dedicated criteria in the Gröbner basis algorithm. Even though including them might be cumbersome and

even if the asymptotic complexity is not better, this represents a noticeable improvement in terms of running time and required memory in practice.

In this spirit, [FSS11] and [GNS23] proposed tweaked versions of F_5 tailored to bilinear and determinantal systems respectively. We will come back to bilinear sequences in Section 2.5.2. Prior to these works, note that the idea of discarding unnecessary reductions using extra knowledge on the system had already been suggested by Traverso [Tra96]. However, his algorithm requires a Hilbert series, which is rarely available.

Hybrid techniques. On a given polynomial system, hybrid methods usually consist in (a) choosing a subset of variables, (b) fixing them to some value, (c) solving the specialized equations with less unknowns, and overall repeating (a)(b)(c) for all specializations until a solution is found. These algorithms may be viewed as a way to benefit from a small field size or as an interpolation between exhaustive search and Gröbner basis solvers when the initial parameter range is not favorable.

The hybrid approach has been studied by [BFP10; BFP12] in the case of semi-regular sequences. Their analysis calls for an assumption on the semi-regularity of the systems obtained after specialization. In a structured context, the effect of fixing unknowns will actually depend on the way these variables are chosen. This type of situation will be recurrent in this thesis.

2.5 Systems in Applications

Systems encountered in the cryptographic context may exhibit some characteristics which are not the ones of generic sequences. As already mentioned, these particularities play an essential role in the study of solving algorithms and they can make it tricky. In fact, the absence of features is also difficult to quantify. For instance, Theorem 2.2 (resp. Theorem 2.4) shows that proving regularity (resp. semi-regularity) is as hard as obtaining the Hilbert series of the system.

We now briefly review two standard traits – affine polynomials in Section 2.5.1 and bilinear structure in Section 2.5.2 – which are often present in our applications. However, note that the considered modeling may have a much more specific shape.

2.5.1 Affine Polynomials

In Corollary 2.1, we obtained a first upper bound on the complexity of computing Gröbner bases for affine sequences. In fact, in this context, we can define a solving degree without relying on the homogenized system. In [DS13], this term is introduced vaguely as the highest degree of a polynomial involved in the solving algorithm.

Definition 2.15 (Solving degree, Definition 6, [CG21]). Let $\mathcal{F}$ be a polynomial system in $\mathbb{K}[\boldsymbol{x}]$. The solving degree of $\mathcal{F}$ with respect to a graded order $\prec$ is the least degree d such that the rowspace of $\mathcal{M}\mathrm{ac}_{\leqslant d}(\mathcal{F})$ contains a Gröbner basis of $\mathcal{F}$.

This notion is no longer an invariant of the ideal since it highly depends on a generating set. For instance, let us consider a radical ideal I whose variety contains a single element $(a_1, \ldots, a_n) \in \bar{\mathbb{K}}^n$. On the one hand, it is well-known that the set $\mathcal{G} = \{x_1 - a_1, \ldots, x_n - a_n\}$ is a reduced Gröbner basis of I for any term order. Its solving degree in the sense of Definition 2.15 is thus equal to 1 for any graded order. On the other hand, the solving degree of another set of generators can be much larger. This example thus shows that contrary to the homogeneous case, the highest degree of a polynomial in the reduced Gröbner basis can be *strictly less* than the solving degree.

2.5.1.1 First Fall Degree

A more fine-grained analysis of the solving degree calls for the notion of *degree fall*. For that purpose, we need to consider the homogeneous sequence $\mathcal{F}^{(h)} = (f_1^{(h)}, \ldots, f_m^{(h)})$ such that $f_i^{(h)}$ is the homogeneous part of highest degree in f_i. Let us assume that there exists a degree d syzygy $(t_i)_{1 \leqslant i \leqslant m}$ for $\mathcal{F}^{(h)}$ in the sense of Definition 2.11, where $(t_i)_{1 \leqslant i \leqslant m}$ is a vector of homogeneous polynomials. In the polynomial $p = \sum_{j=1}^{m} t_i f_i$, we notice that the homogeneous parts of degree d cancel out and thus $\deg(p) < d$. Moreover, if there does not exist any syzygy $(s_i)_{1 \leqslant i \leqslant m}$ for $\mathcal{F}$ such that $s_i^{(h)} = t_i$ for $1 \leqslant i \leqslant m$, this polynomial does not reduce to zero.

Definition 2.16 (Degree fall polynomial, first fall degree). Let $\mathcal{F}$ be an affine sequence. A *degree fall polynomial* for $\mathcal{F}$ corresponds to any polynomial p as described above. The *first fall degree*, denoted d_{ff}, is defined as the smallest integer d such that a syzygy in degree d for $\mathcal{F}^{(h)}$ yields a degree fall polynomial for $\mathcal{F}$.

Upper bounds on the first fall degree are much easier to obtain than on the solving degree since it suffices to find non-trivial syzygies for $\mathcal{F}^{(h)}$. However, the relationship between the two can be complex.

The situation is favorable when the sequence $\mathcal{F}^{(h)}$ is semi-regular. Indeed, the first degree fall polynomials occur at the degree of regularity and the rest of the computation deals with polynomials of smaller degree. The complexity of solving the homogeneous sequence is then used to estimate the overall cost.

Proposition 2.8 (Proposition 6, [BFSY05]). *Let $\mathcal{F}$ be an affine sequence such that $\mathcal{F}^{(h)}$ is semi-regular with degree of regularity d_{reg}. The number of operations in $\mathbb{K}$ to compute a Gröbner basis of $\mathcal{F}$ with respect to a graded ordering can be upper bounded by*

$$\mathcal{O}\left(md_{reg}\binom{n + d_{reg} - 1}{d_{reg}}^{\omega}\right), \tag{2.9}$$

where $2 \leqslant \omega \leqslant 3$ is the linear algebra exponent.

In the general case, the gap between first fall degree and solving degree might be large. For instance, [DS13] provides systems with a low d_{ff} but a high solving degree. Even if these examples may sound pathological, computer algebra [BMT21] and algebraic cryptanalysis offer many others where the two degrees do not coincide. Also, and perhaps

paradoxically, this first fall degree is often adopted by cryptanalysts as an approximation of the solving degree.

One has to be cautious in relying on such an assumption. On the one hand, an estimation only based on the first fall degree will clearly underestimate the real cost if d_{ff} turns out to be smaller than the solving degree. On the other hand, there is also a chance that the first fall polynomials leak some information related to the secret. In such a case, the first fall degree fall remains the key parameter in the attack complexity.

2.5.1.2 Exploiting Degree Falls

More broadly than the cryptographic setting, it is well-known that Gröbner basis techniques using the normal strategy can benefit from degree fall equations[4]. For instance, in the case of F_4, critical pairs constructed with these lower degree polynomials will be treated first. They may in turn yield new degree falls in the subsequent steps. This sort of domino effect often explains the early termination of the algorithm. In fact, this is also what motivates the above cryptanalytic assumption.

Another advantage comes from their definition. Indeed, degree falls for a sequence $\mathcal{F}$ can be pre-computed if syzygies of $\mathcal{F}^{(h)}$ are known. Adding these equations to the system before computing a Gröbner basis will actually help to side-step the early stages of the algorithm[5]. An alternative is to consider them as a new polynomial system especially when they have a specific shape. Of course, it is only relevant if this second system is easier to solve than the original one. This type of situation will arise several times in this manuscript.

2.5.2 Bilinear Equations

In virtue of their surprisingly high proportion in cryptographic applications, bilinear systems also deserve a dedicated section. A bilinear sequence in two blocks of variables $\boldsymbol{x} = (x_1, \ldots, x_{n_x})$ and $\boldsymbol{y} = (y_1, \ldots, y_{n_y})$ is a quadratic sequence such that the degree 2 part in each equation only contains monomials of the form $x_i y_j$. For the sake of simplicity, results in this section will be given for homogeneous bilinear polynomials. In the case of an affine bilinear system $\mathcal{F}$, we let the reader apply them to $\mathcal{F}^{(h)}$ and derive statements on the degree fall polynomials for $\mathcal{F}$ as explained above.

2.5.2.1 Jacobian Matrices and Syzygies

The study of Jacobian matrices is at the core of the analysis of bilinear sequences. In general, these matrices are defined for arbitrary vector-valued functions in several variables.

Definition 2.17 (Jacobian matrix with respect to $\boldsymbol{x}$). For a sequence $\mathcal{F} = (f_1, \ldots, f_m) \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]^m$, the Jacobian with respect to $\boldsymbol{x}$ is the $m \times n_x$ matrix denoted

[4] In the context of XL, these polynomials were referred to as *mutants*.

[5] We note that the definition of solving degree in [CG23] is based on Macaulay matrices with degree falls added (see the discussion before Definition 1.1 there).

by $\mathrm{Jac}_{\boldsymbol{x}}(\mathcal{F})$ whose entry in row i and column j is the partial derivative $\frac{\partial f_i}{\partial x_j}$. We define $\mathrm{Jac}_{\boldsymbol{y}}(\mathcal{F})$ analogously.

If $\mathcal{F}$ is homogenous bilinear, the matrix $\mathrm{Jac}_{\boldsymbol{x}}(\mathcal{F})$ (resp. $\mathrm{Jac}_{\boldsymbol{y}}(\mathcal{F})$) contains linear forms in the $\boldsymbol{y}$ variables (resp. $\boldsymbol{x}$ variables). Lemma 2.1 shows the crucial connection between the left kernel of this matrix and the syzygy module of $\mathcal{F}$.

Lemma 2.1 (Consequence of Equation (1), [FSS11]; Proposition 1, [Ver+19]). *Let $\mathcal{F} = (f_1, \ldots, f_m) \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$ be a homogeneous bilinear sequence and let $\mathcal{H} = (h_1, \ldots, h_m) \subset \mathbb{K}[\boldsymbol{y}]^m$ be a polynomial sequence. We have $\sum_{i=1}^m h_i f_i = 0$ if and only if $\mathcal{H}$ viewed as a vector belongs to the left kernel of $Jac_{\boldsymbol{x}}(\mathcal{F})$.*

To find kernel vectors, one usually employs the following result. Applied to Jacobian matrices, it yields generic syzygies for bilinear systems.

Lemma 2.2 (Lemma 3.1, [FSS11]). *Let $\boldsymbol{M} \in \mathbb{K}[\boldsymbol{y}]^{m \times t}$ be a matrix of linear forms such that $t < m$. For any subset $J = \{j_1 < j_2 < \cdots < j_{t+1}\} \subset \{1..m\}$ of size $t+1$, let us consider the row vector of maximal minors of $\boldsymbol{M}$ defined by*

$$\boldsymbol{v}_J \overset{def}{=} (\ldots, \underbrace{0}_{j \notin J}, \ldots, \underbrace{(-1)^{\ell+1} |\boldsymbol{M}|_{J \setminus j_\ell, *}}_{j = j_\ell}, \ldots).$$

Then, we have $\boldsymbol{v}_J \boldsymbol{M} = 0$.

Corollary 2.2. *Let $\mathcal{F} = (f_1, \ldots, f_m) \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$ be a homogeneous bilinear sequence such that $|\boldsymbol{x}| = n_x$ and $|\boldsymbol{y}| = n_y$. Let us assume that $n_x < m$. Then, there exist degree $n_x + 2$ syzygies from vectors in the left kernel of $\mathrm{Jac}_{\boldsymbol{x}}(\mathcal{F})$. A similar result can be obtained with the other Jacobian provided that $n_y < m$.*

Most of the time, see [FSS11, Conjecture 4.1], these vectors $\boldsymbol{v}_J$ generate the left kernel. Based on this observation, [FSS11] define the notion of bi-regular bilinear sequence. Roughly speaking, the syzygy module comes down to the relations given in Corollary 2.2. As already mentioned, the authors also devise a dedicated version of F_5 which removes all reductions to zero for such systems.

More generally, for an affine sequence of $n_x + n_y$ polynomials which is 0-dimensional, the authors show that the maximal degree D reached by the Gröbner basis for a graded order is upper bounded by

$$D \leqslant \min(n_x + 1, n_y + 1). \tag{2.10}$$

2.5.2.2 Bilinear Systems Obtained from Matrix Products

Even if they do not yield bi-regular sequences, a special type of systems relevant to our purposes will contain equations which are the coefficients in a matrix equality $\boldsymbol{A}\boldsymbol{X}\boldsymbol{Y} = \boldsymbol{0}_{p \times n}$, where $\boldsymbol{A} \in \mathbb{K}^{p \times m}$ is a matrix of scalars, where $\boldsymbol{X} \in \mathbb{K}[\boldsymbol{x}]^{m \times r}$ contains the variables of the block $\boldsymbol{x} = (x_{i,j})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant r}$ and where the entries of $\boldsymbol{Y} \in \mathbb{K}[\boldsymbol{y}]^{r \times n}$

are linear forms in the $\boldsymbol{y}$ variables. The following Lemma 2.3 gives the shape of the Jacobian with respect to $\boldsymbol{x}$ in this case. For an $m \times n$ matrix $\boldsymbol{M}$, we denote by $\mathrm{row}(\boldsymbol{M}) \stackrel{def}{=} \left(\boldsymbol{M}_{\{1\},*} \ \ldots \ \boldsymbol{M}_{\{m\},*}\right)$ the row vector formed by the concatenation of the rows of $\boldsymbol{M}$ and similarly $\mathrm{col}(\boldsymbol{M}) \stackrel{def}{=} \mathrm{row}(\boldsymbol{M}^{\mathsf{T}})$.

Lemma 2.3 (Lemma 1 in [Bar+20a]). *The Jacobian matrix of the system $\boldsymbol{AXY} = \boldsymbol{0}_{p\times n}$ with respect to the $\boldsymbol{x}$ variables is given by*

$$\mathrm{Jac}_{\mathrm{row}(\boldsymbol{X})}\left(\mathrm{row}(\boldsymbol{AXY})\right) = \boldsymbol{A} \otimes \boldsymbol{Y}^{\mathsf{T}} \in \mathbb{F}[\boldsymbol{y}]^{np\times mr}$$
$$\mathrm{Jac}_{\mathrm{col}(\boldsymbol{X})}\left(\mathrm{col}(\boldsymbol{AXY})\right) = \boldsymbol{Y}^{\mathsf{T}} \otimes \boldsymbol{A} \in \mathbb{F}[\boldsymbol{y}]^{np\times mr}.$$

2.5.2.3 Strategies in Practice

When the system is not generic, we cannot always exploit the expression of the Jacobians. A more systematic approach is to investigate specific Macaulay matrices adapted to the bilinear structure. Let us denote by $\mathbb{K}[\boldsymbol{x},\boldsymbol{y}]_{(A,B)} \stackrel{def}{=} \mathbb{K}[\boldsymbol{x}]_A \otimes \mathbb{F}[\boldsymbol{y}]_B$ the vector space of bi-homogeneous polynomials of bi-degree (A,B) in $\mathbb{K}[\boldsymbol{x},\boldsymbol{y}]$.

Definition 2.18 (Macaulay matrix indexed by bi-degree). Let $\mathcal{F} = (f_1,\ldots,f_m)$ be a homogeneous bilinear sequence. The Macaulay matrix in bi-degree (A,B) is the matrix $\mathcal{M}\mathrm{ac}_{(A,B)}(\mathcal{F})$ whose rows correspond to the polynomials μf_j for all monomials $\mu \in \mathbb{F}[\boldsymbol{x},\boldsymbol{y}]_{(A-1,B-1)}$ and $1 \leqslant j \leqslant m$ and whose columns correspond to all monomials in $\mathbb{F}[\boldsymbol{x},\boldsymbol{y}]_{(A,B)}$.

Remark 2.2. Definition 2.18 can be easily generalized to the bi-homogeneous setting.

Let I be the bi-homogeneous ideal generated by $\mathcal{F}$ and let $I_{(A,B)} \stackrel{def}{=} I \cap \mathbb{K}[\boldsymbol{x},\boldsymbol{y}]_{(A,B)}$. The dimension of this vector space is exactly the rank of $\mathcal{M}\mathrm{ac}_{(A,B)}(\mathcal{F})$. In the case when I is also 0-dimensional, let d be the smallest integer such that $I_{(A,B)} = \mathbb{K}[\boldsymbol{x},\boldsymbol{y}]_{(A,B)}$ for all pairs (A,B) with $A+B=d$. Note that we may also have $I_{(A',B')} = \mathbb{K}[\boldsymbol{x},\boldsymbol{y}]_{(A',B')}$ at some bi-degree (A',B') such that $A'+B' < d$. In particular, one can imagine XL strategies which target a particular matrix $\mathcal{M}\mathrm{ac}_{(A,B)}(\mathcal{F})$ instead of another $\mathcal{M}\mathrm{ac}_{(A',B')}(\mathcal{F})$ even when $A+B = A'+B'$. This type of method based on Definition 2.18 has already been adopted in [PS20; Beu21a].

Finally, let us come back to the hybrid approach. There, we might be tempted to specialize variables in only one of the blocks. Due to Equation (2.10), we should probably focus on the smallest one. In the extreme case when this set of unknowns is tiny, we can even consider to fix it completely and then simply solve linear equations.

Chapter 3
Post-Quantum Assumptions and Algebraic Cryptanalysis

This chapter gives an overview of the difficult mathematical problems that we will study in the second half of this thesis. In parallel, it describes some cryptosystems based on the associated hardness assumptions.

Contents

3.1 MinRank

Most of our contributions are closely or remotely related to the MinRank problem. Very often, we will encounter it in a structured setting. First, of course, we need to define the assumption in its most general form.

3.1.1 Formulation

The MinRank problem was introduced in [BFS99], where it is proven to be NP-complete. A bit later, Courtois suggested to use it in cryptography [Cou01b].

Problem 3.1 (MinRank problem). *Given an integer $d \in \mathbb{N}$, $K+1$ matrices $\boldsymbol{M}_0, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{n_r \times n_c}$ and $\mathbb{L}$ a finite extension of $\mathbb{F}_q$, find field elements $x_1 \ldots, x_K \in \mathbb{L}$ such that*

$$\mathrm{rk}\left(\boldsymbol{M}_0 + \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant d.$$

Remark 3.1. Problem 3.2 will be called *homogeneous* if $\boldsymbol{M}_0 = \boldsymbol{0}_{n_r \times n_c}$ and *affine* otherwise.

Note that we only provide the search version. In fact, most applications focus on instances with a solution. Finally, even though the standard statement is $\mathbb{L} = \mathbb{F}_q$, we need to adopt the more general one given in Problem 3.1. The reason will become apparent in the upcoming sections.

From the very start, in the restricted case $\mathbb{L} = \mathbb{F}_q$, Courtois noted the strong connection between MinRank and the following problem from coding theory.

Problem 3.2 (Decoding problem). *Given $\mathcal{C}$ an $\mathbb{F}_q$-linear code of dimension k and length n, a metric wt over $\mathbb{F}_q^n$, an integer $d \in \mathbb{N}$ and a vector $\boldsymbol{y} \in \mathbb{F}_q^n$, find a codeword $\boldsymbol{c} \in \mathcal{C}$ and a vector $\boldsymbol{e}$ such that $wt(\boldsymbol{e}) \leqslant d$ and $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$.*

In the setting when the matrices are square and diagonal, [Cou01a, §23.2.2] trivially shows that MinRank is equivalent to Problem 3.2 in the Hamming metric, denoted wt_H. Roughly speaking, the diagonals of the $\boldsymbol{M}_i$'s for $1 \leqslant i \leqslant K$ generate the linear code $\mathcal{C}$ and the diagonal of $\boldsymbol{M}_0$ corresponds to the vector $\boldsymbol{y}$.

A link with MinRank can still be drawn in general but one needs to change both the code and the metric. In this case, the code is obtained from all the entries of the $\boldsymbol{M}_i$'s.

Definition 3.1 (Matrix code). A matrix code is an $[n_r \cdot n_c, K]_q$-linear code whose codewords will be viewed as matrices of size $n_r \times n_c$ over $\mathbb{F}_q$.

The relevant distance more tailored to Problem 3.1 is called the *rank metric*. The rank weight of $\boldsymbol{M} \in \mathbb{F}_q^{n_r \times n_c}$ is defined as $wt(\boldsymbol{M}) \stackrel{def}{=} \mathrm{rk}\,(\boldsymbol{M})$ and the Decoding problem for a matrix code $\mathcal{C}_{\mathrm{mat}} \subset \mathbb{F}_q^{n_r \times n_c}$ with basis $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K$, target weight d and noisy codeword $\boldsymbol{Y}$ asks to find $(x_1, \ldots, x_K) \in \mathbb{F}_q^K$ such that

$$\mathrm{rk}\left(\boldsymbol{Y} - \textstyle\sum_{j=1}^{K} x_i \boldsymbol{M}_i\right) \leqslant d.$$

The key here is that $(\boldsymbol{M}_0 = -\boldsymbol{Y}; \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K)$ and $d \in \mathbb{N}$ is not anything more than an affine MinRank instance with $K+1$ matrices in $\mathbb{F}_q^{n_r \times n_c}$, rank d and whose solutions are searched in $\mathbb{F}_q$. Going in the reverse direction from an affine MinRank problem is analogous. Thus, MinRank and Problem 3.2 in the rank metric are equivalent.

The average number of solutions to a random instance of Problem 3.2 is usually measured in terms of the *Gilbert-Varshamow distance* $d_{GV,wt}(q,n,k)$. We will define it as a *uniqueness bound*. Roughly speaking, it is the largest integer d such that

$$\#\{\boldsymbol{x} \in \mathbb{F}_q^n : wt(\boldsymbol{x}) \leqslant d\} \leqslant q^{n-k}. \tag{3.1}$$

In this case of the Hamming metric, Equation (3.1) becomes

$$\sum_{j=0}^{d} \binom{n}{j} (q-1)^j \leqslant q^{n-k}. \tag{3.2}$$

3.1.2 Use in Cryptography

In addition to its NP-hardness, the exponential cost of solving algorithms [Cou01a, §24] was another motivation for introducing MinRank in the cryptographic context.

The first proposal is the Courtois' zero-knowledge authentication protocol [Cou01b], which can be turned into a signature scheme by using the Fiat-Shamir transform [FS87]. The drawback of this construction is that it is quite intricate and inefficient, mostly due its soundness error of $\frac{2}{3}$. This explains why MinRank-based cryptography had not really progressed in the next two decades. Hopefully, recent paradigms allowed to change this landscape. By reducing the soundness error, they helped to devise significantly more competitive schemes. For instance, MR-DSS [BESV22] is an evolution of Courtois' which combines the notion of *σ-protocol with helper* [Beu20] together with *cut-and-choose* techniques [KKW18]. Things are now moving very rapidly. Indeed, [BESV22] has already been superseded by other contestants [ARV23; Fen22] based on the *MPC-in-the-Head* approach [IKOS07]. All these constructions enjoy security reductions from the hardness of MinRank. This means that solving average instances of Problem 3.1 is the only way to attack them.

Cryptography relying on the random MinRank assumption already calls for characterizing *genericity*. On this aspect, we prefer to refer to [FSS10] for more formalism. For random instances, one may use the Gilbert-Varshamow distance to estimate the number of solutions over $\mathbb{F}_q$. From Equation (3.1) and the number of rank $\leqslant d$ matrices in $\mathbb{F}_q^{n_r \times n_c}$, this bound corresponds to the largest integer d such that

$$\sum_{j=0}^{d} \left(\prod_{i=0}^{j-1} (q^{n_c} - q^i) \right) \begin{bmatrix} n_r \\ j \end{bmatrix}_q \leqslant q^{n_r n_c - K}. \tag{3.3}$$

By approximating the left-hand side of Equation (3.3), one can recover the more standard condition

$$K \leqslant (n_r - d)(n_c - d). \tag{3.4}$$

On the one hand, when this inequality is strict, a generic affine MinRank problem will not have a solution (even in $\overline{\mathbb{F}_q}$). On the other hand, cryptographic instances always have one: in this regime, it is expected to be unique. Finally, intuition from coding theory suggests that MinRank should be the hardest when K is large. This may also

be seen, to some extent, on the attack costs given in Section 3.1.3. In fact, as long as $K < (n'_r - d)(n'_c - d)$ for $n'_r \leqslant n_r$ and $n'_c \leqslant n_c$, we can imagine to solve a MinRank instance with submatrices in $\mathbb{F}_q^{n'_r \times n'_c}$ and still obtain the solution we want. The result is that MR-DSS and [ARV23] chose parameters such that $K = (n_r - d)(n_c - d) - 2$.

3.1.3 Cryptanalysis

We now present the main solving strategies for the MinRank problem. Their cost will be given on an affine MinRank instance $\boldsymbol{M}_0, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{n_r \times n_c}$ without any specific features and with a unique solution $\boldsymbol{M} = \boldsymbol{M}_0 + \sum_{i=1}^{K} x_i \boldsymbol{M}_i$ of rank $\leqslant d$.

3.1.3.1 Kernel Search

A first approach, sometimes called *combinatorial*, only uses linear algebra techniques. An exhaustive list of attacks in this framework can be found in [Cou01a, §24]. We here focus on Goubin's kernel search (also called *kernel attack*) [GC00]. In fact, Courtois notes that it is more powerful than any other algorithm mentioned in [Cou01a, §24]. To describe it, let us assume without loss of generality that $n_r \geqslant n_c$. Let us also recall that the entries of $\boldsymbol{M}$ are linear in the unknowns x_i for $1 \leqslant i \leqslant K$.

The kernel attack repeatedly tests the consistency of linear systems in these x_i's until one of them has a solution. Each of these systems is obtained by performing a guess on a vector in the (right) kernel of $\boldsymbol{M}$. Since any vector $\boldsymbol{v}_j \in \mathbb{F}_q^{n_c}$ such that $\boldsymbol{M}\boldsymbol{v}_j^\intercal = \boldsymbol{0}_{n_r \times 1}$ yields n_r linear equations in the x_i's, we require at least $\lceil \frac{K}{n_r} \rceil$ linearly independent ones in order to test consistency. In fact, we even need K linearly independent equations among the $n_r \lceil \frac{K}{n_r} \rceil \geqslant K$ collected ones by picking this minimum number of vectors[1]. Since a random non-zero vector lies in $\ker(\boldsymbol{M})$ with probability q^{-d}, we expect to test about $q^{d\lceil \frac{K}{n_r} \rceil}$ linear systems before finding a consistent one. The attack complexity in $\mathbb{F}_q$ operations is thus given by

$$\mathcal{O}(q^{d\lceil \frac{K}{n_r} \rceil} K^\omega), \tag{3.5}$$

where $2 \leqslant \omega \leqslant 3$ is the linear algebra constant.

Echoing the above remark, note that this cost is an increasing function of K. More crucially, it highly depends on q. Aside from hybrid techniques, this value will have much less impact on algebraic attacks.

3.1.3.2 Early Algebraic Algorithms

Algebraic approaches mainly differ in the choice of the polynomial equations. The first two MinRank modelings were the so-called Kipnis-Shamir and Minors systems. In our exposition, we will assume that the $n_c - d$ leftmost columns of $\boldsymbol{M}$ are in the linear span of the rightmost d ones.

[1] Note that the latter issue as well as the linear independence of the $\boldsymbol{v}_j$'s when guessing these vectors is never formally discussed in [GC00; Cou01a]. Still, this should happen with at least constant probability so that their analysis is not really affected.

Kipnis-Shamir modeling. This method was proposed in [KS99]. It consists in introducing extra variables which correspond to a systematic basis of $\ker(\boldsymbol{M})$. Note that this vector space is of dimension at least $n_c - d$. From our assumption on $\boldsymbol{M}$, one is left with solving the following equations.

Modeling 1 (Kipnis-Shamir [KS99]). *The Kipnis-Shamir modeling is the affine bilinear system in the unknowns $x_i \in \mathbb{F}_q$ and $\boldsymbol{K} \in \mathbb{F}_q^{d\times(n_c-d)}$ whose polynomials are the entries of the matrix*

$$\left(\boldsymbol{M}_0 + \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \begin{bmatrix} \boldsymbol{I}_{n_c-d} \\ \boldsymbol{K} \end{bmatrix}.$$

Remark 3.2. We may refer to the x_i's as the *linear variables*. The coefficients of $\boldsymbol{K}$ will be called *kernel variables*.

The original approach on Modeling 1 was relinearization, see [KS99, §5.2]. As mentioned in the last sentence of Section 2.5.2.3, another one is to fix all the kernel variables to obtain a linear system. This actually gives the kernel attack.

Applying Gröbner bases was later suggested by [FLP08]. They observe that Kipnis-Shamir does not behave as a regular system regarding both the solving degree (conjectured to be $\approx d+2$) and the size of the variety. On the one hand, they manage to upper bound the number of solutions with a Bézout bound argument [FLP08, Theorem 2]. Their result directly exploits the multi-homogeneous structure. Indeed, each equation has the stronger property that it involves only one column in $\boldsymbol{K}$. On the other hand, this feature is not used to estimate the solving degree.

This issue was partially tackled in [FSS10]. The authors make the assumption that the system behaves as a bi-regular one. In turn, they obtain the desired upper bound from the analysis of generic bilinear sequences [FSS11]. Nonetheless, their estimate is not sharp: Kipnis-Shamir equations seem to be solved faster in practice than bi-regular ones[2]. Since the polynomials are multi-homogeneous in addition to being bilinear, this should not sound so surprising.

The latter property actually translates into a specific shape for the Jacobian matrices which is the one described in Section 2.5.2.2. Based on the work of [FSS11] that we recalled in Section 2.5.2.1, the authors of [Ver+19] exhibit generic degree falls from degree $d+2$ to $d+1$ for the Kipnis-Shamir system. This partly explains the behaviour conjectured in [FLP08].

Minors modeling. The Minors approach can be considered as folklore but it seems to appear later than Kipnis-Shamir in the literature. It is based on the fact that solving the problem is equivalent to solving the system of all $(d+1)\times(d+1)$ minors of $\boldsymbol{M}$.

Modeling 2 (Minors). *The Minors modeling on an affine MinRank instance $\boldsymbol{M}_0, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{n_r\times n_c}$ with target rank d is the system in the linear variables x_i whose equations are given by all $(d+1)\times(d+1)$ minors of $\boldsymbol{M}$,* i.e.*,*

$$\{|\boldsymbol{M}_{A,B}| : A \subset \{1..n_r\},\ \#A = d+1 \text{ and } B \subset \{1..n_c\},\ \#B = d+1\}.$$

[2] This observation is already made in the conclusion of [FSS11].

The first occurrence of this modeling is [Cou01c, §8], where it is used to solve the MinRank problem of [KS99]. Later, it is proven in [FLP08] that the Minors equations are included in the ideal generated by Kipnis-Shamir. As a consequence, [FLP08] did not study Modeling 2 on its own.

A more in-depth analysis based on the theory of determinantal ideals is performed in [FSS10; FSS13]. In the regime where $n_r = n_c = n$ and when there is equality in Equation (3.4), [FSS10] show that the Minors approach may outperform the Kipnis-Shamir one. In fact, the authors use it to break the parameter set C from Courtois' scheme [Cou01b] which seemed to resist the Kipnis-Shamir method. Since $K > (n-d)^2$ in this case, some linear variables are fixed before applying Modeling 2.

3.1.3.3 Support-Minors

The Support-Minors modeling was introduced in [Bar+20b]. We chose to separate it from the rest of the algebraic attacks due to its relevance in our contributions.

The starting point, quite reminiscent of Kipnis-Shamir, is to factor the secret rank d matrix as

$$\boldsymbol{M} = \boldsymbol{M}_0 + \sum_{i=1}^{K} x_i \boldsymbol{M}_i \stackrel{def}{=} \boldsymbol{D}\boldsymbol{C}, \tag{3.6}$$

where $\boldsymbol{D} \in \mathbb{L}^{n_r \times d}$ and $\boldsymbol{C} \in \mathbb{K}^{d \times n_c}$ are unknown. Then, for $1 \leqslant j \leqslant n_r$, let $\boldsymbol{r}_j \stackrel{def}{=} \boldsymbol{M}_{\{j\},*}$ be the j-th row of $\boldsymbol{M}$ and let

$$\boldsymbol{C}_j \stackrel{def}{=} \begin{bmatrix} \boldsymbol{r}_j \\ \boldsymbol{C} \end{bmatrix}. \tag{3.7}$$

Note that the rank of $\boldsymbol{C}_j$ is at most d. Thus, one can derive equations as in the Minors modeling. More precisely, by setting all the $(d+1) \times (d+1)$ minors of this matrix to zero and by repeating the process for $1 \leqslant j \leqslant n_r$, we obtain:

Modeling 3 (Naive Support-Minors). *The Naive Support-Minors modeling to solve an affine MinRank instance $\boldsymbol{M}_0, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{n_r \times n_c}$ with target rank d is the system in the linear variables x_i and in the entries of $\boldsymbol{C}$ with equations*

$$\{|(\boldsymbol{C}_j)_{*,J}| : 1 \leqslant j \leqslant n_r \text{ and } J \subset \{1..n_c\},\ \#J = d+1\},$$

where $\boldsymbol{C}_j$ is defined in Equation (3.7).

By construction, Modeling 3 has a lot in common with both Kipnis-Shamir and the Minors modeling. Actually, it has been shown in [BB22] that the Kipnis-Shamir equations are included in Modeling 3 and that the associated ideals are the same. This paper also grasps the degree falls of [Ver+19] in terms of the Support-Minors equations. At first sight, all these results seem to indicate that Modeling 3 is not really better than Kipnis-Shamir. In particular, they do not explain the evident success of this approach compared to previous works.

Minor variables. The main advantage of [Bar+20b] is on the practical side. In fact, the authors do not focus on plain Modeling 3. Instead, they consider a more compact system obtained from it by a change of variables.

Let $1 \leqslant j \leqslant n_r$ and let $J \subset \{1..n_c\}$ be a subset of $d+1$ columns in $\boldsymbol{C}_j$. By Laplace expansion along the first row, [Bar+20b] indeed note that the maximal minor $|(\boldsymbol{C}_j)_{*,J}|$ is bilinear in the coefficients of $(\boldsymbol{r}_j)_J$ and in a second block given by some maximal minors of $\boldsymbol{C}$. Recalling that the entries of $\boldsymbol{r}_j$ are linear in the x_i's, this gives a bilinear equation in x_i for $1 \leqslant i \leqslant K$ and $\left|\boldsymbol{C}_{*,J\setminus\{\ell\}}\right|$ for $\ell \in J$. In turn, setting $c_T = |\boldsymbol{C}_{*,T}|$ for any subset $T \subset \{1..n_c\}$ of size d as new unknowns in Modeling 3 in place of the coefficients of $\boldsymbol{C}$ yields the following Modeling 4. This set of equations is the genuine Support-Minors system.

Modeling 4 (Support-Minors (SM)). *The Support-Minors modeling to solve an affine MinRank instance $\boldsymbol{M}_0, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{n_r \times n_c}$ with target rank d is the Naive Support-Minors modeling 3 whose equations are viewed as bilinear in the linear variables x_i and in the so-called* minor *variables $c_T = |\boldsymbol{C}_{*,T}|$, where $T \subset \{1..n_c\}$, $\#T = d$. For $J \subset \{1..n_c\}$, $\#J = d+1$ and $1 \leqslant j \leqslant n_r$, we will denote by $Q_{j,J}$ the polynomial $|(\boldsymbol{C}_j)_{*,J}|$.*

Remark 3.3. The change of unknowns $c_T = |\boldsymbol{C}_{*,T}|$ can be understood in terms of Plücker coordinates, see [BV88, p.6].

We now describe the solving approach adopted in [Bar+20b]. Since the system is bilinear, they apply the specific type of XL technique sketched at the end of Section 2.5.2.3. Note that it will succeed as long as the initial MinRank problem has $\leqslant 1$ solution.

Multiplying by linear variables. The particularity of their algorithm is that it simply constructs Macaulay matrices of the form $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{Q})$ for $b \geqslant 1$, where $\mathcal{Q}$ stands for the SM polynomials. In other words, equations are only multiplied by the x_i's.

By an inclusion-exclusion argument, [Bar+20b] deduce the least degree b for which the linear system $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{Q})\boldsymbol{v}^\mathsf{T} = 0$ has a non-trivial solution. Note also that the row weight of the Macaulay matrix does not depend on b. This is because multiplying an equation by variables does not change the number of monomials. The base case $b = 1$ is tackled in Lemma 3.1.

Lemma 3.1. *Each SM polynomial contains at most $(K+1)(d+1)$ monomials. Moreover, for $J \subset \{1..n_c\}$, $\#J = d+1$ and $1 \leqslant j \leqslant n_r$, the ones present in $Q_{j,J} = |(\boldsymbol{C}_j)_{*,J}|$ only depend on J.*

Proof. Let $J = \{j_1 < \cdots < j_{d+1}\}$ and $1 \leqslant j \leqslant n_r$. By Laplace expansion along the first row of $(\boldsymbol{C}_j)_{*,J}$, the monomials in $Q_{j,J}$ belong to the set

$$\left\{x_i c_{J\setminus j_u} :\ 1 \leqslant u \leqslant d+1 \text{ and } 1 \leqslant i \leqslant K\right\} \cup \left\{c_{J\setminus j_u} :\ 1 \leqslant u \leqslant d+1\right\}.$$

The latter contains $(K+1)(d+1)$ elements which are independent from j. □

The increased sparsity of $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{Q})$ for large b justifies the use of the Wiedemann algorithm. The corresponding complexity can be obtained from Proposition 2.7.

The restriction to bi-degree $(b,1)$ matrices was initially motivated by the great imbalance between the two blocks of unknowns in practice. Indeed, we observe that $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{Q})$ is generally much smaller than any other $\mathcal{M}\mathrm{ac}_{(u,v)}(\mathcal{Q})$ such that $u+v = b+1$. The multiplication by c_T variables is also more complicated to analyze. In fact, it call for understanding the role of *Plücker relations* (see for example [Jac96, Equation (3.4.10) p. 110]). In our notation, for any subsets $J = \{j_1 < \cdots < j_{d+1}\} \subset \{1..n_c\},\ \#J = d+1$ and $U \subset \{1..n_c\},\ \#U = d-1$, they correspond to the degree 2 cancellations

$$\sum_{\ell=1}^{d+1} (-1)^\ell c_{U\cup\{j_\ell\}} c_{J\setminus\{j_\ell\}} = 0.$$

3.2 Multivariate Cryptography

In Part II, we will study specific MinRank instances arising from multivariate schemes. The first occurrence of Problem 3.1 in this field dates back to the historical attack on Hidden Field Equations (HFE) [KS99]. At about the same time as [Cou01b], Courtois noticed that it naturally appears in the analysis [Cou01c, §8].

3.2.1 Introduction

Even without mentioning MinRank, multivariate cryptography (MPKC) can already be seen as the post-quantum branch which is the most prone to algebraic cryptanalysis. Indeed, it is directly built upon the difficulty of solving random quadratic equations.

To formalize the corresponding hardness assumption, we adopt the following terminology. For a sequence $(p_1,\ldots,p_m) \subset \mathbb{F}_q[\boldsymbol{x}]$, we consider the *polynomial map*

$$\begin{aligned} \mathcal{P} : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^m \\ \boldsymbol{a} &\longmapsto (p_1(\boldsymbol{a}),\ldots,p_m(\boldsymbol{a}))\,. \end{aligned}$$

It is said to be *quadratic* if the input polynomials have total degree at most 2.

Problem 3.3 (MQ problem). *Given a quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and a target $\boldsymbol{t} \in \mathbb{F}_q^m$, find a preimage of $\boldsymbol{t}$,* i.e.*, a vector $\boldsymbol{s} \in \mathbb{F}_q^n$ such that $\mathcal{P}(\boldsymbol{s}) = \boldsymbol{t}$.*

Problem 3.3 is known to be NP-hard. On average, in practice, it is also believed to be exponentially hard as long as $m \sim n$. A consequence is that there already exist constructions whose security is only based on MQ [SSH11b; Che+18; Beu20].

However, the classical approach to MPKC requires another type of assumption. The idea is to use a quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with a special structure that makes it easily invertible. This map is called the *central map* and it plays the role of a trapdoor. The public key is then defined as the composition $\mathcal{P} \overset{def}{=} \mathcal{T}\circ\mathcal{F}\circ\mathcal{S}$, where $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ are randomly generated affine maps of maximal rank. To rely on MQ,

the crux is now that $\mathcal{P}$ should be indistinguishable from a random quadratic system. However, since the central map $\mathcal{F}$ is often *ad hoc*, very little attention has been given to formalize such an assumption and more generally to provable security for trapdoor-based MPKC [SSH11a].

This standard way of building multivariate cryptography is often referred to as the *butterfly construction*. It can be used in both encryption mechanisms and signature schemes.

Encryption. The ciphertext $\boldsymbol{c} \overset{def}{=} \mathcal{P}(\boldsymbol{m}) \in \mathbb{F}_q^m$ corresponds to the evaluation of the public key $\mathcal{P}$ at the message $\boldsymbol{m} \in \mathbb{F}_q^n$. Note that we must have $m \geqslant n$ for decryption to be injective. The decryption process consists in inverting each secret key component. In other words, we compute $\mathcal{S}^{-1}\left(\mathcal{F}^{-1}\left(\mathcal{T}^{-1}(\boldsymbol{c})\right)\right)$ to recover the plaintext.

Signature. We do no longer need $m \geqslant n$. In fact, the lack of this constraint may explain why the panorama is more promising for signature algorithms than it is for encryption schemes. To sign a message $\boldsymbol{m} \in \mathbb{F}_q^m$ when $m < n$, we apply the abovementioned decryption algorithm to a vector $(\boldsymbol{m}, \boldsymbol{r}) \in \mathbb{F}_q^n$, where $\boldsymbol{r} \in \mathbb{F}_q^{n-m}$ is randomly generated. If this vector does not have an inverse by $\mathcal{P}$, we sample another $\boldsymbol{r'} \in \mathbb{F}_q^{n-m}$ and we start again with $(\boldsymbol{m}, \boldsymbol{r'})$. Verifying a signature $\tilde{\boldsymbol{\sigma}}$ is straightforward. We simply compare the m leftmost components of $\mathcal{P}(\tilde{\boldsymbol{\sigma}})$ to the original message.

While the complexity of encryption (resp. verification) only depends on the degree of the public equations[3], the cost of decryption (resp. signing) is related to the structure of $\mathcal{F}$. This gives another constraint on the choice of this map in addition to the security requirement.

3.2.2 Big-Field Schemes

The historical method was to consider a trapdoor which admits a simple description over an extension field. The general structure is $\mathcal{F} \overset{def}{=} \phi \circ F \circ \phi^{-1}$, where $F \in \mathbb{F}_{q^n}[X]$ is of degree D and where $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear isomorphism. Since we want a quadratic system, the polynomial F only involves monomials of the form $X^{q^i+q^j}$ for $i,\ j \in \mathbb{N}$. The rationale is that inversion reduces to univariate solving.

This *big-field* approach was pioneered by Matsumoto and Imai with the C* cryptosystem [MI88]. The scheme was later broken by Patarin [Pat95], who proposed a generalization called Hidden Field Equations (HFE) [Pat96]. In fact, most of the recent constructions can be obtained from these two proposals by applying *modifiers*, such as [CS19; CYS15] from C* and [Pet+15; DCPS17; Cas+20] from HFE.

Finally, we want to mention the Sidon cryptosystem [RLT21] that we will study in Chapter 5. It cannot be viewed as a big-field scheme per se since it does not a have butterfly shape. Still, as we will see, it heavily relies on an extension field.

[3] This actually justifies the choice of quadratic polynomials.

3.2.2.1 Central Map and Cryptanalysis

The C* cryptosystem was defined with a polynomial $F(X) = X^{q^\alpha+1}$ for some integer $\alpha \in \mathbb{N}$ such that $\gcd(q^\alpha+1, q^n-1) = 1$. This is in fact a monomial which can be inverted via simple exponentiation. To avoid the attack of [Pat95], HFE considers a more general one of the form

Definition 3.2 (HFE polynomial).

$$F(X) = \sum_{\substack{i,j\in\mathbb{N} \\ q^i+q^j\leqslant D}} \alpha_{i,j} X^{q^i+q^j} + \sum_{\substack{k\in\mathbb{N} \\ q^k\leqslant D}} \beta_k X^{q^k} + \gamma, \tag{3.8}$$

where $\alpha_{i,j},\ \beta_k$ and γ are random elements in $\mathbb{F}_{q^n}$.

Inversion now requires to factor degree $\leqslant D$ polynomials over $\mathbb{F}_{q^n}$ using, for example, Berlekamp's algorithm [Ber70]. To speed-up this step, it thus seems legitimate to choose the value of D as small as possible. However, this would cause a serious problem for security. The key notion here is the *rank* of the central map, which corresponds to the rank of F when seen as a quadratic form in $(X^0, \dots, X^{q^{n-1}})$. This is because attack complexities increase with this value. Finally, note that it is bounded by $\log_q(D)$ in the case of HFE.

The *direct attack* is a message attack which applies to any MPKC. *Rank attacks* are more specific. While they are not limited to big-field schemes, we will only study them in that context.

Direct attack. This method consists in inverting the public system as if it was a random MQ instance. For that purpose, all known solving algorithms can be employed. In particular, using Gröbner bases lead to break the first HFE challenge of Patarin [JF03]. There, it was observed that the solving degree of $\mathcal{P}$ differs significantly from the one of a regular sequence. Note that this already contradicts our handwaving assumption on the security of $\mathcal{F}$. Perhaps surprisingly, this degree seems to depend on D but not on n. For some parameters, [JF03, §4, Table 2] even provides an upper bound. Their argument actually relies on the rank of the central map, even if implicitly.

Rank attacks. These are attacks on the secret key which more directly exploit the low rank of the central map. Indeed, they model key-recovery as an instance of Problem 3.1 whose rank is equal to the one of $\mathcal{F}$. The initial C* attack [Pat95] falls into this category. Since then, similar methods have been used on other schemes such as HFE [Pet+15; VS17] or PFLASH/EFLASH [CS17]. The cryptanalysis works of [DS05; Beu21a; Beu22] on Rainbow [Din+20] show that this approach is in fact not restricted to big-field constructions.

Beyond these two techniques, *differential attacks* can also affect MPKC. A good example of this is given by the cryptanalysis of SFLASH [DFS07; DFSS07]. However, we seem to have good confidence that HFE-based proposals resist this type of methods [Smi10].

Coming back to parameters, one thus wants a low degree D for efficiency but a bound $\log_q(D)$ which is not too small for security. This is a first reason why HFE instantiations stick to $q = 2$ in general. Concretely, Patarin's initial challenge achieving 80 bit security was $q = 2$, $m = n = 80$ and $D = 96$. This would yield a ciphertext or signature size of 80 bits.

3.2.2.2 Rank Attacks

In contrast to the schemes presented in Section 3.1, MinRank only appears in the cryptanalysis. Even though attacks relying on it may involve other steps, solving Problem 3.1 will often be the dominant cost. Finally, the underlying instance will be structured due to the use of an extension field.

Since rank attacks are a particular type of key-recovery attacks, let us start the following definition.

Definition 3.3 (Equivalent keys). For an asymmetric scheme, two secret keys sk_1 and sk_2 are equivalent if there is a public key pk such that $(\mathsf{sk}_1, \mathsf{pk})$ and $(\mathsf{sk}_2, \mathsf{pk})$ are two valid keypairs. For a butterfly MPKC, this corresponds to two tuples $(\mathcal{T}_1, \mathcal{F}_1, \mathcal{S}_1)$ and $(\mathcal{T}_2, \mathcal{F}_2, \mathcal{S}_2)$ such that $\mathcal{F}_1$ and $\mathcal{F}_2$ are valid central maps satisfying

$$\mathcal{T}_1 \circ \mathcal{F}_1 \circ \mathcal{S}_1 = \mathcal{T}_2 \circ \mathcal{F}_2 \circ \mathcal{S}_2.$$

In the case of HFE and its variants, the structure of such a set of keys is well-known [WP11, Theorem 4.13]. Concretely, in the attacks that we will describe, any non-zero solution to the MinRank problem will yield several equivalent keys. In the subsequent steps, the cardinality of this keyset will give degrees of freedom to the attacker for fixing variables. Due to construction, the Sidon cryptosystem is also affected by a rank attack. However, in this case, the relationship between the set of MinRank solutions and the set of equivalent keys was unknown. It will in fact be instrumental in our approach [BTV21].

The rest of this section presents the early rank attacks on HFE. We will only focus on the MinRank step.

Historical attack [KS99]. As already mentioned, the first attempt can be attributed to Kipnis and Shamir. Let us assume that q is odd and let $\boldsymbol{F} = [f_{i,j}]_{i,j=0}^{n-1} \in \mathbb{F}_{q^n}^{n\times n}$ be the matrix of the quadratic form in $\underline{X} = (X^0, \ldots, X^{q^{n-1}})$ associated to the HFE polynomial of Equation (3.2) by $F(X) \stackrel{def}{=} \underline{X}\boldsymbol{F}\underline{X}^\mathsf{T}$. Recall that this matrix has rank at most $d \stackrel{def}{=} \lceil \log_q(D) \rceil$. To put it very briefly, the attack of [KS99] targets a multiple of the form $\boldsymbol{W}\boldsymbol{F}\boldsymbol{W}^\mathsf{T}$, where $\boldsymbol{W} \in \mathbb{F}_{q^n}^{n\times n}$ is a secret invertible matrix, as a solution to a homogeneous MinRank instance with rank d, matrices in $\mathbb{F}_{q^n}^{n\times n}$ and scalars $x_i \in \mathbb{F}_{q^n}$.

Revisiting Kipnis-Shamir's approach [BFP13]. Instead of relying on univariate maps over the extension field as in the original paper, [BFP13] gives a new description

of the attack of [KS99] by using matrix-vector products. For our purposes, it will be more convenient to focus on this reinterpretation.

Let $\boldsymbol{\beta} \stackrel{def}{=} (\beta_1, \ldots, \beta_n)$ be a basis of $\mathbb{F}_{q^n}$ when viewed as an $\mathbb{F}_q$-vector space and let $\boldsymbol{M} \in \mathbb{F}_{q^n}^{n \times n}$ be the associated Moore matrix defined by $\boldsymbol{M} \stackrel{def}{=} [\beta_{i+1}^{q^j}]_{i,j=0}^{n-1}$. We consider the following $\mathbb{F}_q$-linear isomorphism ϕ between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$ attached to the basis $\boldsymbol{\beta}$:

$$\phi : x \mapsto (x, \ldots, x^{q^{n-1}})\boldsymbol{M}^{-1}.$$

Its inverse is $\phi^{-1} : \boldsymbol{v} \mapsto (\boldsymbol{v}\boldsymbol{M})_1$. Also, for $0 \leqslant k \leqslant n-1$, let $\boldsymbol{F}^{*k} \in \mathbb{F}_{q^n}^{n \times n}$ be the matrix representing the polynomial F^{q^k}. The coefficient in position (i, j) is equal to $f_{i-k,j-k}^{q^k}$, which means that this matrix can be obtained from $\boldsymbol{F}$ by shifting its entries k times to the northwest[4] and raising them to the power q^k. Finally, for $1 \leqslant i \leqslant n$, let $\boldsymbol{\Sigma}_i \in \mathbb{F}_q^{n \times n}$ denote the symmetric matrix representing the quadratic polynomial $f_i \in \mathcal{F}$, *i.e.*, $f_i(\boldsymbol{x}) \stackrel{def}{=} \boldsymbol{x}\boldsymbol{\Sigma}_i\boldsymbol{x}^\mathsf{T}$. Since $\mathcal{F} = \phi \circ F \circ \phi^{-1}$, we have for any vector $\boldsymbol{v} \in \mathbb{F}_q^n$

$$(\boldsymbol{v}\boldsymbol{\Sigma}_1\boldsymbol{v}^\mathsf{T}, \ldots, \boldsymbol{v}\boldsymbol{\Sigma}_n\boldsymbol{v}^\mathsf{T}) = (\boldsymbol{v}\boldsymbol{M}\boldsymbol{F}^{*0}\boldsymbol{M}^\mathsf{T}\boldsymbol{v}^\mathsf{T}, \ldots, \boldsymbol{v}\boldsymbol{M}\boldsymbol{F}^{*n-1}\boldsymbol{M}^\mathsf{T}\boldsymbol{v}^\mathsf{T}).$$

Let us come back to the public polynomials. In the same way as above, let $\boldsymbol{P}_i \in \mathbb{F}_q^{n \times n}$ represent p_i for $1 \leqslant i \leqslant n$. Let also $\boldsymbol{S} \in \mathbb{F}_q^{n \times n}$ and $\boldsymbol{T} \in \mathbb{F}_q^{n \times n}$ invertible matrices associated to the linear maps $\mathcal{S}$ and $\mathcal{T}$ respectively. It is shown in [BFP13] that

$$(\boldsymbol{P}_1, \ldots, \boldsymbol{P}_n)\boldsymbol{T}^{-1}\boldsymbol{M} = (\boldsymbol{S}\boldsymbol{M}\boldsymbol{F}^{*0}\boldsymbol{M}^\mathsf{T}\boldsymbol{S}^\mathsf{T}, \ldots, \boldsymbol{S}\boldsymbol{M}\boldsymbol{F}^{*n-1}\boldsymbol{M}^\mathsf{T}\boldsymbol{S}^\mathsf{T}). \tag{3.9}$$

From this equation, as both $\boldsymbol{M}$ and $\boldsymbol{S}$ are invertible, one eventually obtains a MinRank problem.

Problem 3.4 (Theorem 2, [BFP13]). *Recovering one column of $\boldsymbol{V} \stackrel{def}{=} \boldsymbol{T}^{-1}\boldsymbol{M} \in \mathbb{F}_{q^n}^{n \times n}$ amounts to solving the homogeneous instance of Problem 3.1 with target rank $d = \lceil \log_q(D) \rceil$, matrices $\boldsymbol{M}_i \stackrel{def}{=} \boldsymbol{P}_i \in \mathbb{F}_q^{n \times n}$ and unknowns $x_i \in \mathbb{F}_{q^n}$ for $1 \leqslant i \leqslant n$.*

3.2.2.3 Modifiers

Modifiers refer to generic techniques which aim at strengthening the security of a multivariate scheme by making both the direct attack and rank attacks less efficient. This section focuses on the minus and vinegar modifiers, which are the most relevant ones for HFE.

- **Minus.** Its consists in dropping $1 \leqslant a \leqslant n-1$ polynomials from the public key, for example $p_1, \ldots, p_a$. This amounts to considering $\mathcal{P}^- = \tau_a \circ \mathcal{P}$, where $\tau_a : \mathbb{F}_q^m \to \mathbb{F}_q^{m-a}$ is the projection on the last $n-a$ coordinates. Since the system now contains less equations than variables, this tweak can only yield signature schemes.

[4] Indexes $i-k$ and $j-k$ are taken modulo n.

- **Vinegar.** We introduce $v \geqslant 1$ extra unknowns $\boldsymbol{y_v} \stackrel{def}{=} (y_1, \ldots, y_v)$ and we consider the modified central polynomial

$$F(X, \boldsymbol{y}_v) = \sum_{\substack{i,j \in \mathbb{N} \\ q^i + q^j \leqslant D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{i \in \mathbb{N} \\ q^i \leqslant D}} \beta_i(\boldsymbol{y}_v) X^{q^i} + \gamma(\boldsymbol{y}_v), \tag{3.10}$$

  where this time $\alpha_{i,j} \in \mathbb{F}_{q^n}$, the β_i's are linear maps $\mathbb{F}_q^v \to \mathbb{F}_{q^n}$ and γ is a quadratic map $\mathbb{F}_q^v \to \mathbb{F}_{q^n}$. The new central map is $\mathcal{F} = \phi \circ F \circ \psi : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^n$, where

$$\begin{aligned} \psi : \mathbb{F}_q^n \times \mathbb{F}_q^v &\longrightarrow \mathbb{F}_{q^n} \times \mathbb{F}_q^v \\ (x, y) &\longmapsto (\phi^{-1}(x), y). \end{aligned}$$

  To sign a message $\boldsymbol{m} \in \mathbb{F}_{q^n}$, we compute the preimage $\overline{\boldsymbol{m}} = \mathcal{T}^{-1}(\boldsymbol{m})$ and we lift it to $\mathbb{F}_{q^n}$ by applying ϕ. Then, we pick random vinegar variables $\boldsymbol{y} \in \mathbb{F}_q^v$ to construct a genuine HFE polynomial $F_{\boldsymbol{y}}(X) \stackrel{def}{=} F(X, \boldsymbol{y})$. Finally, we proceed as in the standard scheme by inverting a univariate equation. If it does not have a solution, we select new vinegar values $\boldsymbol{y}'$ and we start again with the HFE polynomial $F_{\boldsymbol{y}'}$.

Using those two modifiers in combination gives the so-called HFEv- signature scheme. Its security with respect to the direct attack was analyzed in [DH11; DK12; DY13]. All these works aim at obtaining a tight upper bound on the solving degree of the public system. Similarly, HFEv- better resists rank attacks compared to the original construction:

- a HFE polynomial $F(X, \boldsymbol{y})$ with partial degree D in X and v vinegars corresponds to a rank $d + v$ matrix when viewed as a quadratic form in $(\underline{X}, \boldsymbol{y})$;
- with a minuses, an attacker can only consider linear combinations between $n - a$ fixed matrices in Problem 3.4, for example $\boldsymbol{P}_{a+1}, \ldots, \boldsymbol{P}_n$. The vector space generated by these elements will not necessarily contain rank d matrices anymore.

In short, relying on [KS99; BFP13], the natural MinRank problem to attack HFEv- with a minuses and v vinegars has target rank $d + a + v$ instead of d. With this in mind, the G*e*MSS proposal [Cas+20] which is based on this trapdoor had been submitted to NIST with good confidence in its security. Another similar construction was Gui [Pet+15] but it failed to reach the Second Round.

Rank attack on HFEv- by Tao *et al.* The confidence in HFE variants has been significantly affected by a recent attack [TPD21]. The breakthrough in this work was to consider another MinRank problem on HFEv- with rank simply equal to d. Since it is independent from the effect of the modifiers, solving this instance lead to a much smaller complexity compared to previous attacks based on Problem 3.4. Overall, [TPD21] strongly broke the G*e*MSS parameters and it contributed to the disqualification of the scheme after the Third Round.

In reaction to this attack, [ØSV21] proposed to apply another modifier called *Projection*. This tweak was originally introduced for another scheme [CYS15]. The point of this approach is that it is more efficient than increasing the degree D of the central polynomial to obtain the same security against [TPD21]. In turn, the authors provided parameters which are immune to this former attack.

For the sake of clarity, details on both the attack of [TPD21] and Projection are deferred to Chapter 4.

3.3 Rank-Based Cryptography

Code-based cryptography is undoubtedly the second area of post-quantum cryptography where algebraic cryptanalysis was shown to be very effective. It also yields structured MinRank versions, especially in the rank metric setting. This way of building cryptosystems started at about the same time as number-theoretic cryptography when McEliece proposed the first public-key encryption scheme based on error-correcting codes in 1978 [McE78].

3.3.1 Introduction

The Decoding problem is the main underlying assumption for code-based cryptography. Recalling the notation of Problem 3.2, we may often express it in terms of a full-rank generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$ for the linear code $\mathcal{C}$. This problem also has a dual version, where $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ corresponds to a parity-check matrix.

Problem 3.5 (Syndrome Decoding problem). *Given a full-rank matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$, a metric wt over $\mathbb{F}_q^n$, an integer $d \in \mathbb{N}$ and $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$, find a vector $\boldsymbol{e} \in \mathbb{F}_q^n$ such that $wt(\boldsymbol{e}) \leqslant d$ and $\boldsymbol{e}\boldsymbol{H}^\intercal = \boldsymbol{s}$.*

Regardless of the metric, Problem 3.2 and Problem 3.5 are equivalent. The *Generic* version of these assumptions corresponds to a code $\mathcal{C}$ which is random among all codes of parameters $[n, k]_q$. We will refer to it as DP when wt is the Hamming metric. There, too, it is known to be NP-hard [BMT78].

McEliece's scheme. As for the MQ problem, it is possible to devise cryptosystems which are only based on DP [Ale03]. However, the security of the iconic proposal [McE78] calls for another type of hard problem. This is because it is trapdoor-based, the trapdoor being given by a family of codes with an efficient decoding algorithm. To still rely on Generic DP, the crux is that codes in this family should admit generator matrices $\boldsymbol{G}$ which are *indistinguishable* from random matrices. At a very high level, this assumption can be compared to the one we described when defining butterfly MPKC. In code-based cryptography, the major difference is that it is *formalized*. As a result, the McEliece scheme has a security proof.

Its construction is as follows. Let F_{good} be a suitable family of codes as we discussed. For the code in this family with parity-check matrix $\boldsymbol{H}$, let $\mathcal{A}_{\text{decode},\boldsymbol{H}}$ denote an efficient decoding algorithm. Finally, let $d \in \mathbb{N}$ smaller than the error correction capacity.

McEliece's scheme (sketch).

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}(\mathsf{pk}, \boldsymbol{m})$	$\mathsf{Dec}(\mathsf{sk}, \boldsymbol{y})$
$\boldsymbol{H} \leftarrow\!\!\$\, F_{\text{good}}$	$\boldsymbol{e} \leftarrow\!\!\$\, \{\boldsymbol{x} \in \mathbb{F}_q^n,\ wt_H(\boldsymbol{x}) \leqslant d\}$	$\boldsymbol{e}' \leftarrow\!\!\$\, \mathcal{A}_{\text{decode},\boldsymbol{H}}(\boldsymbol{y}\boldsymbol{H}^\mathsf{T})$
$\mathsf{sk} \leftarrow \mathcal{A}_{\text{decode},\boldsymbol{H}}$	$\boldsymbol{y} \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$	$I, \boldsymbol{G}_{I,*} \in \mathrm{GL}_k(\mathbb{F}_q)$
$\mathsf{pk} \leftarrow \boldsymbol{G} \in \mathbb{F}_q^{k\times n},\ \boldsymbol{G}\boldsymbol{H}^\mathsf{T} = \boldsymbol{0}$	**return** $\boldsymbol{y}$	**return** $(\boldsymbol{y} - \boldsymbol{e}')_I \boldsymbol{G}_{I,*}^{-1}$
return $(\mathsf{sk}, \mathsf{pk})$		

McEliece's original proposal for F_{good} was the family of binary Goppa codes, which admit efficient decoding. Following his work, many attempts were made by simply substituting these codes with another family, for example Generalized Reed–Solomon (GRS) codes, Reed-Muller codes or Geometric codes (which can be seen as a higher genus version of GRS codes). However, a lot of them were shown to be insecure due to their too strong algebraic structure. So far, binary Goppa codes as well as MDPC codes [MTSB13] are the few remaining ones which have not been ruled out by cryptanalysis. In fact, the latter do not have any algebraic structure since they are a generalization of LDPC codes. LDPC codes are characterized by a sparse parity-check matrix with constant row weight. In MDPC, this weight is of the order of $\widetilde{\mathcal{O}}(\sqrt{n})$. This increase is crucial as it permits to avoid attacks based on finding low weight codewords in the dual while still allowing acceptable error correction performance. Quasi-cyclic MDPC codes are used in the BIKE NIST submission [Ara+17a].

Finally, it is quite natural to wonder if algebraic techniques can affect McEliece's instantiations relying on algebraic codes. This is indeed the case and until very recently, as shown by a series of works [FOPT10; Fau+11; BMT23; CMT23].

Using the rank metric. Even though we defined it in the context of MinRank, the rank metric was introduced much earlier. It dates back to the work of Gabidulin, who relied on it to build a McEliece-type PKE [GPT91]. Since then, this new approach to code-based cryptography has been shown to be extremely fruitful to design various types of primitives. Interestingly enough, the NIST PQC project has also provided new momentum. We usually refer to this area as *rank metric code-based cryptography* or *rank-based cryptography*.

3.3.2 Rank Decoding

However, the terminology hides a fundamental aspect regarding the hardness assumption. If this type of cryptography were relying on generic instances of Problem 3.2 in the rank metric, a better name would have been *MinRank-based cryptography*. In fact, rank-based

schemes do not use random matrix codes. They focus on standard linear codes but over an extension field $\mathbb{F}_{q^m}$[5].

To see why these codes give specific matrix codes, let us start with some notation. Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$ be a fixed basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}$ and let $(\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_m)$ be the canonical basis of $\mathbb{F}_q^m$. We now have an $\mathbb{F}_q$-linear isomorphism

$$\begin{aligned} \mathcal{L}_{\boldsymbol{\beta}} : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q^m \\ \beta_i &\longmapsto \boldsymbol{\varepsilon}_i. \end{aligned}$$

For a vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$, we consider[6] $\mathrm{Mat}(\boldsymbol{x}) = (X_{ij})_{i,j} \in \mathbb{F}_q^{m \times n}$ the matrix obtained by applying $\mathcal{L}_{\boldsymbol{\beta}}$ coordinatewise. Note the relation $\boldsymbol{x} = \boldsymbol{\beta}\,\mathrm{Mat}(\boldsymbol{x})$. The point now is that an $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$ of length n and dimension k is isomorphic to a matrix code of parameters $[m \cdot n, km]_q$. Indeed, if $(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k) \in (\mathbb{F}_{q^m}^n)^k$ is an $\mathbb{F}_{q^m}$-basis of $\mathcal{C}$, the set of matrices $\big(\mathrm{Mat}(\beta_i \boldsymbol{g}_j)\big)_{1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant k}$ generates a matrix code $\mathcal{C}_{\mathrm{mat}}$ over $\mathbb{F}_q$ of the desired parameters.

Similarly, we can define a notion of distance for vectors in $\mathbb{F}_{q^m}^n$ from the underlying rank metric on $\mathbb{F}_q^{m \times n}$ and the abovementioned isomorphism:

$$|\boldsymbol{x}| \stackrel{def}{=} wt(\mathrm{Mat}\,(\boldsymbol{x})) = \mathrm{rk}\,(\mathrm{Mat}\,(\boldsymbol{x})).$$

Remark 3.4. We often use the letter r instead of d for the weight in this context.

An important remark is that we can read it on the vectorial representation in $\mathbb{F}_{q^m}^n$ as the dimension of the following $\mathbb{F}_q$-vector space.

Definition 3.4 (Support of a word in $\mathbb{F}_{q^m}^n$). The *support* of a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ is the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ defined by $\mathrm{Supp}(\boldsymbol{x}) \stackrel{def}{=} \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$.

Lemma 3.2. *We have* $|\boldsymbol{x}| = \dim_{\mathbb{F}_q}(\mathrm{Supp}(\boldsymbol{x}))$.

We are now ready to state the relevant assumption for rank-based cryptography. It simply corresponds to Problem 3.2 in the rank metric restricted to matrix codes isomorphic to $\mathbb{F}_{q^m}$-linear codes. This problem can also be viewed as another structured version of MinRank.

Problem 3.6 (Rank Decoding (RD) problem). *Given a full-rank matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$, an integer $r \in \mathbb{N}$ and $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$, find a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{e}| \leqslant r$ and $\boldsymbol{y} - \boldsymbol{e} = \boldsymbol{m}\boldsymbol{G}$ for some $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$.*

Remark 3.5. We will sometimes call the triple $(\boldsymbol{y}, \mathcal{C}, r)$ a *problem instance*, where $\mathcal{C}$ is the $\mathbb{F}_{q^m}$-linear code generated by $\boldsymbol{G}$. More precisely, we may refer to it as an RD instance *of parameters* (m, n, k, r).

[5] We need to change the notation compared to Section 3.2.2 since the degree is not always correlated with the length n.

[6] This notation is implicit with respect to $\boldsymbol{\beta}$ as the discussion does not depend on the choice of basis.

Due to $\mathbb{F}_{q^m}$-linearity, Problem 3.6 is not a priori NP-hard contrary to both MinRank and Generic DP. Still, there exists a randomized reduction to the latter due to Gaborit and Zémor [GZ16]. Its interest remains theoretical since it holds for $m > n^2$ while the cryptographically relevant zone is m of the order of n. In particular, several years of cryptanalysis efforts may sound as a better security argument.

Finally, once again, we may derive a Gilbert-Varshamov distance $d_{GV,||}(q^m, n, k)$. It is no surprise that the condition is simply Equation (3.3) with $r = d,\ n_r = m,\ n_c = n$ and $K = km$:

$$\sum_{j=0}^{r} \left(\prod_{i=0}^{j-1} (q^n - q^i) \right) \binom{m}{j}_q \leqslant q^{m(n-k)}. \tag{3.11}$$

3.3.3 Pre-NIST Constructions

There are at least two reasons for using the Rank Decoding problem in place of MinRank to build a rank-based version of McEliece. The first one is that all known families of matrix codes with efficient decoding algorithm come from $\mathbb{F}_{q^m}$-linear codes. The second one is for efficiency. Indeed, the latter have a more compact description than random matrix codes. The systematic generator matrix of an $[n, k]_{q^m}$-code can be stored in memory by using $k(n-k)\log_2(q^m) = mk(n-k)\log_2(q)$ bits, which is m times less than the $mk(mn-km)\log_2(q) = m^2k(n-k)\log_2(q)$ ones needed to represent a generic matrix code of parameters $[m \cdot n, k \cdot m]_q$. This m factor explains why rank-based schemes can achieve smaller key sizes compared to their Hamming metric counterparts.

The GPT cryptosystem [GPT91] and early variants relied on Gabidulin codes [Gab85], which are the rank metric analogue of Reed-Solomon codes.

Definition 3.5 (Gabidulin code). Let $(k, n, m) \in \mathbb{N}^3$ such that $k \leqslant n \leqslant m$ and let $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ whose coordinates are linearly independent over $\mathbb{F}_q$. The *Gabidulin code* $\mathcal{G}_{\boldsymbol{g}}(n, k, m)$ is the code of parameters $[n, k]_{q^m}$ defined by

$$\mathcal{G}_{\boldsymbol{g}}(n, k, m) \stackrel{def}{=} \left\{ P(\boldsymbol{g}) : \deg_q(P) < k \right\},$$

where P ranges through the set of q-polynomials, $\deg_q(.)$ is the q-degree and $P(\boldsymbol{g}) \stackrel{def}{=} (P(g_1), \ldots, P(g_n))$.

A code as in Definition 3.5 is known to have minimum distance $n - k + 1$. Moreover, it benefits from an efficient decoder that can correct up to $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors.

Here as well, their strong algebraic structure lead to devastating attacks [Ove05]. Later, another breakthrough came from the introduction of LRPC codes [Ara+19a]. An LPRC code with row weight d can be defined from a parity-check matrix whose entries belong to a subspace of $\mathbb{F}_{q^m}$ of dimension d. Such a code admits an efficient decoding algorithm by exploiting codewords of low rank weight in the dual very much as MDPC decoding takes advantage of dual vectors of small Hamming weight. This structure allowed to devise rank-based analogues of the MDPC scheme [Ara+19a; Ara+17b;

Ara+17c] which further lead to the NIST candidate ROLLO [Ara+19c]. Another rank-metric contestant but with a radically different construction was RQC [Agu+20]. As its name suggests, it is the rank-metric equivalent of the HQC cryptosystem [Agu+21].

Ideal codes. To reduce the keysize even more, ROLLO and RQC actually consider $\mathbb{F}_{q^m}$-linear codes with larger automorphism groups.

Let $P \in \mathbb{F}_q[X]$ denote a polynomial of degree n. The linear map

$$\psi_P \ : \ \boldsymbol{u} = (u_0, \dots, u_{n-1}) \mapsto \boldsymbol{u}(X) = \textstyle\sum_{i=0}^{n-1} u_i X^i$$

is a vector space isomorphism between $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_{q^m}[X]/\langle P \rangle$. As the latter is also a ring, we define a product over $\mathbb{F}_{q^m}^n$ by transport of structure via $\boldsymbol{u} \cdot_P \boldsymbol{v} \stackrel{def}{=} \psi_P^{-1}\left(\boldsymbol{u}(X)\boldsymbol{v}(X) \bmod P\right)$. Since

$$\boldsymbol{u} \cdot_P \boldsymbol{v} = \psi_P^{-1}\left(\sum_{i=0}^{n-1} u_i X^i \times \boldsymbol{v}(X) \bmod P\right) = \sum_{i=0}^{n-1} u_i \psi_P^{-1}\left(X^i \boldsymbol{v}(X) \bmod P\right),$$

the multiplication by $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ corresponds the product on the right by

Definition 3.6 (Ideal matrix). Let $P \in \mathbb{F}_q[X]$ a polynomial of degree n and let $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$. The ideal matrix generated by $\boldsymbol{v}$ and P is

$$\mathcal{IM}_P(\boldsymbol{v}) \stackrel{def}{=} \begin{bmatrix} \boldsymbol{v} \\ \psi_P^{-1}\left(X\psi_P(\boldsymbol{v}) \bmod P\right) \\ \vdots \\ \psi_P^{-1}\left(X^{n-1}\psi_P(\boldsymbol{v}) \bmod P\right) \end{bmatrix} \in \mathbb{F}_{q^m}^{n \times n}.$$

In the following, the notation will be implicit with respect to P.

In short, we have $\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{u}\mathcal{IM}(\boldsymbol{v}) = \boldsymbol{v}\mathcal{IM}(\boldsymbol{u}) = \boldsymbol{v} \cdot \boldsymbol{u}$.

The codes used in these submissions are called *ideal codes*. Roughly speaking, their generator matrices are block matrices with blocks as in Definition (3.6). The motivation is exactly the same as relying on module lattices or quasi-cyclic codes since they have a more compact description.

Loidreau's scheme [Loi17]. At PQCrypto 2017, Loidreau proposed a new McEliece-type scheme relying on Gabidulin codes. It uses a different kind of masking compared to GPT and its descendants in order to counteract Overbeck's attack. The idea is to right multiply the generator matrix which reveals the structure by an invertible matrix whose entries lie in a small $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension λ.

Security. The security of all these primitives is based on the intractability of Problem 3.6. In fact, using an ideal structure requires a version where the code $\mathcal{C}$ is an ideal code. So far, there are no known attacks which exploit this extra feature.

As ROLLO is a McEliece-type scheme, its security is also related to distinguishing LRPC codes from random ones. In the ideal case, this problem was shown to be significantly easier when $P = X^n - 1$ since this polynomial can be factored over the small field $\mathbb{F}_q$ as $X^n - 1 = (X-1)\sum_{j=0}^{n-1} X^j$ [HT15]. However, when P is irreducible or when there is no such structure, it is believed to be difficult. Even though there is no reduction to Problem 3.6, all solving approaches boil down to using techniques from RD attacks. Similarly, Loidreau's cryptosystem is based on the difficulty of distinguishing the hidden Gabidulin code from a random one. The hardness of this problem highly depends on the value of λ. First, we recover the broken GPT proposal when $\lambda = 1$. When $\lambda = 2$ and when the code rate is greater than $1/2$, Coggia and Couvreur have proposed a distinguisher that can be turned into a polynomial-time attack [CC20]. However, in the general case, an higher value of λ seems to resist structural attacks. The intuition is that when this parameter grows, the problem becomes closer to the indistinguishability assumption for LRPC codes of the same weight (which is slightly better understood as we have just seen).

Finally, a nice aspect of RQC is that there is no structural masking. In other words, the Rank Decoding problem is the only hardness assumption.

3.3.4 Cryptanalysis

In this section, we outline the main techniques to solve Problem 3.6. In fact, all MinRank algorithms described in Section 3.1.3 can already be applied. However, as such, they do not exploit the $\mathbb{F}_{q^m}$-linear structure.

Section 3.3.4.1 presents *combinatorial attacks*, which can be seen as an RD version of Goubin's kernel search. In Section 3.3.4.2 and Section 3.3.4.3, we will describe algebraic modelings which are *tailored* to the Rank Decoding problem. In all cases, our exposition implicitly assumes that the input instance has a unique solution.

3.3.4.1 Combinatorial Methods

The core idea in combinatorial attacks is to perform a guess on a subspace $F \subset \mathbb{F}_{q^m}$ of dimension $w \geqslant r$ which contains the support of $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and then to use this information to solve a linear system derived from the parity-check equations. The main requirement is that the dimension of F cannot be too large compared to r for this system to be overdefined. In that respect, such techniques can also be grasped as a rank-based adaptation of Prange's algorithm [Pra62].

In these algorithms, the final complexity is dominated by the inverse of the probability of a correct guess. In the case of RD, the crux is that the probability can be greatly increased thanks to $\mathbb{F}_{q^m}$-linearity. This value has been improved in a series of papers [CS96; OJ02; GRS16; AGHT18].

The point of [AGHT18] is to relax the original condition $\mathrm{Supp}(\boldsymbol{e}) \subset F$. Instead, they guess a subspace F which contains an *arbitrary* multiple $\alpha\,\mathrm{Supp}(\boldsymbol{e})$, $\alpha \in \mathbb{F}_{q^m}^*$. The cost of their attack in $\mathbb{F}_q$-operations is

$$\mathcal{O}\left((n-k)^3 m^3 q^{r\lceil\frac{(k+1)m}{n}\rceil - m}\right). \tag{3.12}$$

3.3.4.2 Ourivski-Johanson Modeling

The seminal work of [OJ02] can be considered as the first algebraic attack on the Rank Decoding problem. However, at that time, the complexity derived from the initial anaysis did not seem to improve upon that of combinatorial techniques.

Statement of the modeling. The starting point is to reduce Problem 3.6 to the one of finding a weight r codeword in the code $\mathcal{C}_{\boldsymbol{y}} \stackrel{def}{=} \mathcal{C} \oplus \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$, where $\mathcal{C}$ is generated by the rows of $\boldsymbol{G}$. Indeed, as long as the RD instance has a unique solution, all these vectors are expected to be of the form $\lambda \boldsymbol{e}$, $\lambda \in \mathbb{F}_{q^m}^*$. For the purposes of notation, let us still denote by $\boldsymbol{e}$ any of these non-zero scalar multiples and let $\boldsymbol{H}_{\boldsymbol{y}} \in \mathbb{F}_{q^m}^{(n-k-1)\times n}$ be the systematic parity-check matrix for $\mathcal{C}_{\boldsymbol{y}}$. We thus obtain

$$\boldsymbol{e}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}} = \boldsymbol{0}. \tag{3.13}$$

Then, by using the weight constraint, [OJ02] rewrite Equation (3.13) as a bilinear system[7]. In fact, they do it in the same way as in the Support-Minors approach. Even though the latter applies to generic MinRank, it is worth mentioning now that it was initially motivated by applications to rank-based cryptography.

As in Equation (3.6), the low rank matrix representation $\mathrm{Mat}(\boldsymbol{e}) \in \mathbb{F}_q^{m\times n}$ is expressed as a product $\boldsymbol{S}\boldsymbol{C}$, where $\boldsymbol{S}$ and $\boldsymbol{C}$ are full-rank matrices of unknowns in $\mathbb{F}_q^{m\times r}$ and $\mathbb{F}_q^{r\times n}$ respectively. The columns of $\boldsymbol{S}$ are a basis of the space $\mathcal{L}_\beta(\mathrm{Supp}(\boldsymbol{e})) \subset \mathbb{F}_q^m$ while the i-th column of $\boldsymbol{C}$ contains the coordinates of e_i in this basis for $1 \leqslant i \leqslant n$.

Modeling 5 (Ourivski-Johansson ($\mathcal{OJ}$)). *Let $\mathcal{C}$ be the underlying $[n,k]_{q^m}$-code of an RD instance with target weight r and noisy codeword $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$. Let $\mathcal{C}_{\boldsymbol{y}} \stackrel{def}{=} \mathcal{C} \oplus \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$ and let $\boldsymbol{H}_{\boldsymbol{y}} \stackrel{def}{=} \left(-\boldsymbol{R}^{\mathsf{T}}\ \boldsymbol{I}_{n-k-1}\right)$ be a systematic parity-check matrix for this linear code. The Ourivski-Johansson modeling is the system in the unknowns $\boldsymbol{S} \in \mathbb{F}_q^{m\times r}$ and $\boldsymbol{C} \in \mathbb{F}_q^{r\times n}$ whose equations are the entries of the row vector*

$$(\beta_1, \ldots, \beta_m)\boldsymbol{S}\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}}.$$

The authors eventually fix $\boldsymbol{S}_{*,1} = \boldsymbol{\varepsilon}_1$ in Modeling 5 since the target is an arbitrary non-zero scalar multiple of the initial error. The resulting system contains $n-k-1$ affine bilinear equations over $\mathbb{F}_{q^m}$ in $(r-1)m + rn$ variables over $\mathbb{F}_q$.

[7] Simply presented as "quadratic" in [OJ02].

3.3.4.3 MaxMinors Modeling

Unfortunately, until very recently, there had been little progress in algebraic attacks since the work of [OJ02]. We can still mention the RD modeling of [GRS16] which exploits $\mathbb{F}_{q^m}$-linearity by using q-polynomials. This situation has just changed, mostly because rank-based NIST candidates required a more thorough study of algebraic techniques. For instance, new attacks [Bar+20a; Bar+20b] have shown that these methods could outperform combinatorial approaches in the parameter range which was critical for the submissions. This was in fact the main argument not to select these schemes to advance further on in the process.

A key ingredient of these recent works is the following Modeling 6. In [Bar+20a], its equations were initially found as degree fall polynomials for the Ourivski-Johansson system. The proof exploits the shape of Modeling 5 together with the content recalled in Sections 2.5.2.1 and 2.5.2.2. More simply, we can also check that these polynomials vanish on the RD solutions.

Modeling 6 (MaxMinors). *Keeping the notation of Modeling 5, the MaxMinors modeling is the system in the variables from $\boldsymbol{C}$, denoted $\mathcal{P}_{\mathbb{F}_{q^m}}$, defined by $\{P_J\}_{J\subset\{1..n-k-1\},\ \#J=r}$, where*

$$P_J \stackrel{def}{=} \left|\boldsymbol{C}(\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}})_{*,J}\right|. \tag{3.14}$$

Modeling 6 contains $\binom{n-k-1}{r}$ affine equations over $\mathbb{F}_{q^m}$. Since they are computed as $r \times r$ minors of a matrix whose coefficients are linear in the entries of $\boldsymbol{C}$, they have degree r in these unknowns.

Unfolding over $\mathbb{F}_q$. A recurring feature in Modelings 5 and 6 is that the coefficients of the polynomials belong to $\mathbb{F}_{q^m}$ while the variables are searched in $\mathbb{F}_q$. If I stands for the ideal generated by $\mathcal{P}_{\mathbb{F}_{q^m}}$, we are thus more interested by the ideal $I_{\mathbb{F}_q}$ with basis $\mathcal{P}_{\mathbb{F}_{q^m}} \cup \{\boldsymbol{C}_{i,j}^q - \boldsymbol{C}_{i,j}\}$ as defined in Section 2.1. This ideal being radical, it contains

$$\mathcal{P}_{\text{Frob}} \stackrel{def}{=} \{f^{q^\ell} \bmod \{\boldsymbol{C}_{i,j}^q - \boldsymbol{C}_{i,j}\} : f \in \mathcal{P}_{\mathbb{F}_{q^m}} \text{ and } 0 \leqslant \ell \leqslant m-1\} \subset \mathbb{F}_{q^m}[\boldsymbol{C}_{i,j}]. \tag{3.15}$$

Remark 3.6. The set of field equations is a Gröbner basis so we really compute normal forms here.

In practice, we may prefer to work with coefficients over $\mathbb{F}_q$. For that purpose, we generalize the usual trace operator of the extension field $\mathbb{F}_{q^m}$ to $f \in \mathbb{F}_{q^m}[\boldsymbol{C}_{i,j}]$ by

$$\text{Tr}(f) \stackrel{def}{=} f + f^q + \cdots + f^{q^{m-1}} = \sum_{\ell=0}^{m-1} f^{[\ell]}. \tag{3.16}$$

Let now $\boldsymbol{\beta}' = (\beta'_1, \ldots, \beta'_m)$ be an $\mathbb{F}_q$-basis of the extension field[8]. It is easy to see that the following system

$$\mathcal{P}_{\mathbb{F}_q} \stackrel{def}{=} \{\text{Tr}(\beta'_\ell f) \bmod \{\boldsymbol{C}_{i,j}^q - \boldsymbol{C}_{i,j}\} : f \in \mathcal{P}_{\mathbb{F}_{q^m}} \text{ and } 1 \leqslant \ell \leqslant m\} \tag{3.17}$$

[8] A convenient choice in the analysis will be the dual basis $\boldsymbol{\beta}^*$ of the basis $\boldsymbol{\beta}$ considered above.

can be obtained from $\mathbb{F}_{q^m}$-linear combinations between polynomials in $\mathcal{P}_{\text{Frob}}$. Finally, for any $\alpha \in \mathbb{F}_{q^m}$ and any monomial $\mu \in \mathbb{F}_{q^m}[\boldsymbol{C}_{i,j}]$, let us observe that

$$\text{Tr}(\alpha\mu) \bmod \{\boldsymbol{C}_{i,j}^q - \boldsymbol{C}_{i,j}\} = \text{Tr}(\alpha)\mu \bmod \{\boldsymbol{C}_{i,j}^q - \boldsymbol{C}_{i,j}\}.$$

This shows that $\mathcal{P}_{\mathbb{F}_q} \subset \mathbb{F}_q[\boldsymbol{C}_{i,j}]$ and that the monomial content is the same in both $\mathcal{P}_{\mathbb{F}_q}$ and $\mathcal{P}_{\mathbb{F}_{q^m}}$ (since $\mathcal{P}_{\mathbb{F}_{q^m}}$ only contains squarefree monomials). The crucial advantage of $\mathcal{P}_{\mathbb{F}_q}$ is that the solutions now boil down to the ones we want.

Modeling 7 (MaxMinors over $\mathbb{F}_q$ (MM-$\mathbb{F}_q$)). *Let $\boldsymbol{\beta}' = (\beta'_1, \ldots, \beta'_m)$ be an arbitrary $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. The MaxMinors modeling over $\mathbb{F}_q$ is the system given in Equation (3.17), where $\mathcal{P}_{\mathbb{F}_{q^m}}$ is Modeling 6. For $1 \leqslant \ell \leqslant m$ and $J \subset \{1..n-k-1\}$, $\#J = r$, we set*

$$P_{\ell,J} \overset{def}{=} Tr(\beta'_\ell P_J) \bmod \{\boldsymbol{C}_{i,j}^q - \boldsymbol{C}_{i,j}\}.$$

Using Modeling 7. As already mentioned, the MaxMinors modeling was instrumental in both [Bar+20a] and [Bar+20b]. The initial approach of [Bar+20a] was to combine it with the former bilinear Modeling 5 unfolded over $\mathbb{F}_q$. This can be understood as the generic way to take advantage of degree fall polynomials in a Gröbner basis algorithm. The subsequent paper [Bar+20b] makes a much better use of these equations. Some elements of their work have been presented when describing the Support-Minors modeling. For instance, it was noticed in [Bar+20a; Bar+20b] that the MaxMinors polynomials are *linear* in the minor variables $c_T = |\boldsymbol{C}|_{*,T}$ of $\boldsymbol{C}$. This is consequence of

Lemma 3.3 (Cauchy-Binet formula). *Let $\mathcal{R}$ denote an arbitrary ring, let $\boldsymbol{A} \in \mathcal{R}^{r\times n}$ and let $\boldsymbol{B} \in \mathcal{R}^{n\times r}$. We have*

$$|\boldsymbol{AB}| = \sum_{J\subset\{1..n\},\ \#J=r} |\boldsymbol{A}_{*,J}||\boldsymbol{B}_{J,*}|.$$

Another contribution of [Bar+20b] was to fix variables by considering an identity block $\boldsymbol{I}_r$ for the r leftmost columns of $\boldsymbol{C}$. First, the resulting system still has solutions with constant probability. Second, and more importantly, this new specialization offers a significant benefit: we can simply solve for the c_T's and then recover the individual entries of $\boldsymbol{C}$ from $c_{\{1..r\}\setminus\{i\}\cup\{j\}} = \boldsymbol{C}_{i,j}$.

In this way, solving RD was performed by inverting the linear system in the minor variables given by Modeling 7. In particular, if the weight r is below the Gilbert-Varshamov bound and if $m\binom{n-k-1}{r} \geqslant \binom{n}{r} - 1$ (*overdetermined case*), it was considered that this approach succeeds under a heuristic on the rank of the system.

Assumption 1 (Heuristic 1, [Bar+20b]). *When $m\binom{n-k-1}{r} \geqslant \binom{n}{r} - 1$, with very high probability, the rank of Modeling 7 is equal to $\binom{n}{r} - 1$.*

Otherwise, in the *underdetermined case*, [Bar+20b] propose two different strategies:

- The first one is a form of hybrid approach by adding random linear constraints on the c_T variables.

- The second one is to combine Modeling 7 with the Support-Minors modeling applied to the underlying MinRank instance.

These two approaches will be examined in much more detail in Chapter 7.

3.3.5 Modern Schemes and New Assumptions

In addition to the cryptosystems presented in Section 3.3.3, rank-based cryptography has been in the spotlight thanks to many other works. Moveover, among them, the IBE scheme of [GHPT17] and the Durandal signature scheme [Ara+19b] show that it should not be limited to PKEs and KEMs. They may even suggest that the rank metric is more suitable for some applications than the Hamming metric.

3.3.5.1 Rank Support Learning

Designing more versatile rank-based primitives has required the introduction of new assumptions. In particular, both [GHPT17] and [Ara+19b] rely on the so-called Rank Support Learning (RSL) problem.

Problem 3.7 (Rank Support Learning (RSL) problem). *Given a full-rank matrix* $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ *and a matrix* $\boldsymbol{E}\boldsymbol{H}^\intercal \in \mathbb{F}_{q^m}^{N\times(n-k)}$*, where the coefficients of* $\boldsymbol{E} \in \mathbb{F}_{q^m}^{N\times n}$ *lie in a subspace* $\mathcal{V} \subset \mathbb{F}_{q^m}$ *of dimension* r*, find* $\mathcal{V}$*.*

Remark 3.7. In other words, a problem instance corresponds to N instances of RD whose errors $(\boldsymbol{e}_i \overset{def}{=} \boldsymbol{E}_{i,*})_{1\leqslant i\leqslant N}$ have the same support $\mathcal{V} \subset \mathbb{F}_{q^m}$. Thus, RSL trivially reduces to RD.

Problem 3.7 was defined in [GHPT17] but its straightforward adaptation to the Hamming metric had already been used for cryptographic purposes [KKS97; KKS05]. This latter version can be solved in polynomial time when $N \geqslant r$ [GHPT17, §4.2]. On Rank Support Learning, a polynomial algorithm of the same nature only exists whenever $N \geqslant nr$ [GHPT17, §4.2]. A bit later, the IBE of [GHPT17] was broken with different techniques [DT18]. The authors proposed an algebraic attack on RSL which applies when $N > kr$. In this regime, the complexity was expected to be subexponential. In spite of this, we still have more flexibility in the number of errors than in the Hamming case.

Durandal signature scheme. More recently, the RSL problem was used to build a rank-metric signature scheme [Ara+19b]. Relying on this assumption allowed to adapt the Schnorr-Lyubashevsky framework [Sch91; Lyu09] to the code-based setting, which had not been possible so far in the Hamming metric. To avoid the attack of [DT18], the original parameters were chosen such that $N = k(r-2)$ or $N = k(r-1)$. In fact, at the time of [BB21], they were already obsolete due to [Bar+20a; Bar+20b].

3.3.5.2 Improving Existing Schemes

These recent attacks have for sure affected the confidence of the cryptographic community in the associated schemes, a fortiori those submitted to NIST. On the positive side, one can also view them as a way to better understand the complexity of solving RD. Besides, NIST kept encouraging further research on rank metric cryptography[9] [Moo+20].

Subsequent works aimed at mitigating the impact of such attacks in order to maintain attractive parameters for ROLLO and RQC.

In the initial ones, the weight of the error was of the order of $\mathcal{O}(\sqrt{n})$. This seemed to correspond to a vulnerable zone in regard to algebraic techniques. Thus, it was proposed in [Agu+22] to pick a larger weight. Concretely, they increase the weight of the error to decode from $r = \mathcal{O}(\sqrt{n})$ to a value closer to the Gilbert-Varshamov distance. At this point, from computation on concrete parameters, algebraic attacks were believed to be relatively less efficient than combinatorial techniques. However, so far, there is no theoretical result underlying such an assumption. The idea of [Agu+22] was also employed in [Ara+22]. In these works, note that the benefit of using it comes at the price of relying on RSL rather than on RD.

To limit the effect of cryptanalysis, the RQC submitters considered *non-homogeneous* errors [Agu+20]. Regarding security, this slight variation in the noise distribution lead them to formalize a structured version of RD called the Non-Homogeneous Rank Decoding (NHRD) problem.

Problem 3.8 (Non-Homogeneous Rank Decoding (NHRD) problem). *Given a full-rank matrix* $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n+n_1)\times(2n+n_1)}$*, integers* $(w_1, w_2) \in \mathbb{N}^2$ *and* $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n+n_1}$*, find a vector* $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3) \in \mathbb{F}_{q^m}^{2n+n_1}$*,* $\boldsymbol{e}_1 \in \mathbb{F}_{q^m}^{n}$*,* $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n_1}$*,* $\boldsymbol{e}_3 \in \mathbb{F}_{q^m}^{n}$*, such that* $\boldsymbol{e}\boldsymbol{H}^\intercal = \boldsymbol{s}$*,* $|(\boldsymbol{e}_1, \boldsymbol{e}_3)| \leqslant w_1$*,* $|\boldsymbol{e}_2| \leqslant w_1 + w_2$ *and* $\mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_3) \subset \mathrm{Supp}(\boldsymbol{e}_2)$*.*

Remark 3.8. We recover the Rank Decoding problem when $w_2 = 0$.

RQC is restricted to a setting where $n_1 = n$. In Chapter 8, we will motivate and study the general version due to a new proposal [BBBG23] which relies on it.

3.4 Regular Syndrome Decoding

In addition to MinRank and some variants, we studied a structured version of Problem 3.2 in the Hamming metric.

Problem 3.9 (Regular Syndrome Decoding (RSD) problem). *Let* $(t, k, N) \in \mathbb{N}^3$ *and* $n \stackrel{def}{=} tN$*. Given a full-rank matrix* $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ *and a vector* $\boldsymbol{s} \in \mathbb{F}_q^n$*, find a vector* $\boldsymbol{e} \stackrel{def}{=} (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_t)$ *which is the concatenation of* t *random blocks* $\boldsymbol{e}_i \in \mathbb{F}_q^N$ *with* $wt_H(\boldsymbol{e}_i) = 1$ *and such that* $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\intercal$*.*

[9] "Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth."

As we can see, its specificity lies in the error distribution. In the following, the corresponding vector $\boldsymbol{e}$ will be referred to as *regular*.

Problem 3.9 was proposed by Augot, Finiasz and Sendrier [AFS05] as the underlying assumption for the Fast Syndrome-Based hash function. It is also present in subsequent work [FGS07; BLPS11; MDCE11]. Much later, this problem was used in Fiat-Shamir code-based signatures relying on the MPC-in-the-Head paradigm [FJR22; CCJ23]. In [FJR22], the original zero-knowledge proof for Problem 3.2 is adapted to Problem 3.9 in order to reach better size-performance trade-offs[10]. In [CCJ23], the MPC protocol is radically different since it is tailored to the regular distribution. Last but not least, another field of application is in secure computation. The introduction of RSD in this context was pioneered by [HOSS18]. As of now, we especially encounter it in Pseudorandom Correlation Generators (PCGs) [BCGI18; Boy+19b; Boy+19a; Yan+20; WYKW21]. Since our work targets the parameter setting adopted by these primitives, we will spend a bit more time to describe them.

3.4.1 Pseudorandom Correlation Generators

Pseudorandom correlation generators refer to cryptographic constructions which allow parties to locally generate long sources of correlated randomness from the knowledge of short correlated seeds. As it is often straightforward to securely compute the desired functionality from such long vectors, obtaining them efficiently is the cornerstone. In PCGs, this efficiency lies in the short interactive phase which only serves as producing the seeds.

At the core of these schemes is a pseudorandom generator (PRG) based on the Decoding Problem[11]. The pseudorandomness of the ouput is ensured by the hardness assumption while its linear nature allows to preserve the target correlation. This PRG is either $(\boldsymbol{m}, \boldsymbol{e}) \mapsto \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ (Primal) or $\boldsymbol{e} \mapsto \boldsymbol{e}\boldsymbol{H}^\intercal$ (Dual), where the sparse vector $\boldsymbol{e}$ comes from a function secret sharing scheme [BGI15]. The point of using Problem 3.9 in place of Problem 3.2 is simply for better performance. Indeed, it is less costly to securely share a regular vector $\boldsymbol{e}$ than a random one of the same weight.

These primitives all adopt a very particular setting. First and foremost, the noise rate t/n is extremely low compared to the one usually considered in code-based cryptography. Second, the field size q can be large, typically $q \geqslant 256$. The rest of the parameters depends on the instantiation. In the Primal case, since the PRG input contains an arbitrary vector $\boldsymbol{m} \in \mathbb{F}_q^k$, one selects a very small code rate k/n to maximize the expansion factor. The Dual case $\boldsymbol{e} \mapsto \boldsymbol{e}\boldsymbol{H}^\intercal$ does not exhibit the same constraint since the seed is just the compact description of a sparse vector. By fixing the weight and increasing n, one can get an output size mostly independent of the seed size. In this situation, the code rate is constant.

[10] The scheme of [FJR22] considers a generalization where the error is made of $d \geqslant 1$ blocks with constant weight (RSD corresponds to $d = t$).

[11] PCG proposals often use the Learning Parity with Noise (LPN) terminology.

3.4.2 Previous Cryptanalysis

The work of Chapter 10 will focus on the specific parameter range that we have just described. In this case, the mapping $\boldsymbol{e} \mapsto \boldsymbol{e}\boldsymbol{H}^\intercal \in \mathbb{F}_q^{n-k}$ is expected to be injective regardless of the regular constraint[12]. This means that an algorithm to solve the Decoding problem will always output the regular solution when applied to Problem 3.9. Thus, in our regime, RSD should be easier than Problem 3.2.

We will now present the main attacks which are relevant to this setting. For a more detailed exposition, we refer to [HOSS18; CCJ23].

- Since we restrict ourselves to a highly injective map, we will not expand on neither Generalised Birthday Attacks [Wag02; CJ04; Kir11] nor Linearization Attacks [BM97; Saa07] which are mostly tailored to multiple solutions. Note however that these techniques can be enhanced using the regular distribution [CCJ23].

- The most important class of algorithms on the plain Decoding problem is arguably Information Set Decoding (ISD). This refers to a series of improvements [Ste89; FS09a; BLP11; MMT11; BJMM12; MO15] upon the work of Prange [Pra62] that we briefly mentioned in Section 3.3.4.1. The basic idea is to guess k error-free positions and then solve a linear system. In these improvements, one has to make a further assumption of the weight distribution of the error vector. Thus, taking advantage of the regular noise is not necessarily immediate.

- A last type of approach is Statistical Decoding [Jab01]. Recently, the 2.0 version of [CDMT22] showed that this technique can outperform ISDs in the standard code-based crypto setting when the code rate is sufficiently small.

In light of these attacks, Boyle *et al.* proposed parameters to instantiate Problem 3.2 in PCGs [BCGI18, §5.1]. Later constructions also use them in a black box manner [Yan+20; WYKW21]. What is important is that these parameters are kept the same for RSD while it is precisely the zone where we could expect better solving algorithms. On their values, the authors note that the limiting attack is either Prange, ISDs or Statistical Decoding. Another remark is that advanced ISDs do not perform extremely well due to the tiny noise regime [CS16].

More recently, [LWYY22] studied the same parameter range but in a slightly more general context (larger fields or integer rings, various noise distributions). There, the authors claim that the estimates of [BCGI18] are too conservative over large fields regarding the ISD cost. Roughly speaking, the advantage of ISDs compared to Prange quickly deteriorates when q increases [Can17]. In addition, they argue that the complexity of Statistical Decoding is much higher than presented in [BCGI18]. In particular, this is no longer the best attack even by taking into account the algorithm of [CDMT22]. As this improvement is still quite new, a further analysis in this specific regime and/or tailored to the regular shape remains to be made.

[12] In the binary case, this will happen as long as $2^k \geqslant \binom{n}{d}$.

3.5 ZK-Friendly Symmetric Primitives

We finally introduce a specific type of symmetric designs which are vulnerable to algebraic techniques. They belong to a larger branch of symmetric cryptography which is motivated by emerging applications in FHE, MPC and ZK proofs based on hash functions. In contrast to the traditional symmetric-key setting which operates over $\mathbb{F}_2$ and which turns out to be inefficient in this context, they work over a large finite field $\mathbb{F}_q$ (where q is a prime of cryptographic size or 2^e with $e \geqslant 64$).

3.5.1 General Approach

Hash functions used in ZK should be such that it is easy to prove the knowledge of a preimage. Note that the existence of several different proof systems may call for more particular requirements.

In symmetric cryptography, a standard technique to build a hash function is to start by constructing a *permutation*. The rough security goal is that it should behave as a randomly sampled one. As a first approximation, we may consider such a pseudorandom permutation P as being a keyless block cipher. Its general form is *iterative*, namely

$$P \stackrel{def}{=} R_{n_r} \circ R_{n_r-1} \circ \cdots \circ R_0,$$

where the R_i's correspond to cryptographically weak but simple transformations and where $n_r \in \mathbb{N}$ is the number of rounds. Security is guaranteed by a careful selection of these transformations (called *round functions*) and by a large enough value of n_r once this choice has been made. A very frequent construction is that of Substitution-Permutation Network (SPN) ciphers. There, the round function is the composition of a linear layer, an Sbox, and an addition of constants (possibly in a different order).

The reason why classical block ciphers are not suited in this *arithmetization-oriented* (AO) context is because the efficiency requirement is different. Indeed, we do not necessarily need a permutation P which is easy to compute and invert but simply a one with fast verification. More precisely, given a pair $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_q^m \times \mathbb{F}_q^m$, it should be efficient to *check that* $P(\boldsymbol{x}) = \boldsymbol{y}$. Another reason is due to the performance metric. This time, in contrast to binary instructions, the relevant operations are the addition and the multiplication over a large field. A first design concern was thus to minimize the amount of $\mathbb{F}_q$-products, which explains why the initial attempts relied on a round function $R : \mathbb{F}_q^m \to \mathbb{F}_q^m$ with a low degree model. More precisely, there should exist a polynomial map $\mathcal{P} : \mathbb{F}_q^{2m} \to \mathbb{F}_q^m$ *with low multiplicative complexity* such that $\boldsymbol{y} = R(\boldsymbol{x})$ if and only if $\mathcal{P}(\boldsymbol{x}, \boldsymbol{y}) = 0$. In particular, MiMC and its variants [Alb+16] as well as Poseidon [Gra+21; GKS23] have adopted the simplest Sbox $x \mapsto x^d$ where $d \in \mathbb{Z}_{>0}$ is the smallest degree for which this map is a permutation. A more subtle approach initiated by Jarvis [AD18] and employed later in the Rescue family [Aly+20; SAD20] was to consider a permutation whose *inverse* is of low degree.

3.5.2 Algebraic Techniques on Block Ciphers

The first application of algebraic cryptanalysis to symmetric schemes largely predates the advances in AO constructions. It dates back at least to [CP02] where it was used on the AES. Given a message/ciphertext pair, the authors model key-recovery as a quadratic system whose unknowns come from the key and from intermediate variables introduced at each round. Even though the original complexity claim was later shown to be incorrect [Ars+04; CL05], this attempt contributed to popularize algebraic methods in block cipher cryptanalysis.

Note that early works in that direction already contain findings which are worth mentioning before studying AO ciphers. The first one that highly differs from the public-key setting is that the cost of computing an arbitrary Gröbner basis should not be taken as an indicator of the overall complexity. For instance, [BPW06a] showed that the AES modeling proposed in [MR02] is a Gröbner basis for a "degree-then-LEX" order while the scheme still resists algebraic methods. The same proof technique was used in [BPW06b] to construct the block ciphers Flurry and Curry. The goal there was to give proposals immune to classical techniques (*e.g.*, linear and differential attacks) but for which the standard modeling by introducing intermediate state variables is already a Gröbner basis. These works rely on the following well-known result.

Proposition 3.1 (Buchberger's second criterion, Prop. 4 p. 106, [CLO15]). *Let $\mathcal{G} \subset \mathbb{K}[\boldsymbol{x}]$ be a finite set and let $f,\ g \in \mathcal{G}$ whose leading monomials are coprime. Then, the S-polynomial $S(f,g)$ reduces to 0 modulo $\mathcal{G}$.*

In the strategy described in Section 2.2.3, this means that the change-of-order step becomes the dominant part. Luckily for the AES, it appeared to be the bottleneck. Indeed, its cost in the case of [BPW06a] was argued to be higher than the one of exhaustive key search.

The crucial difference for AO primitives is that algebraic attacks typically become the limiting ones. In some cases, this is due to the low degree representation that we have just mentioned. A more likely and general reason is that classical techniques devised for the field $\mathbb{F}_2$ do not translate well to the large field setting (they are at least less well understood). Regarding the Gröbner basis step, it was proven that it can be neglected in MiMC [Alb+19] using the same argument as above. On an arbitrary cipher, its cost is often derived assuming (semi-)regularity or from an experimental bound on the solving degree. Here as well, the complexity of FGLM can be dominant and it boils down to estimating the degree of the ideal. In this context, some systems were observed to reach the Bézout bound (Proposition 2.2) but others also had less solutions. Such a particular behaviour in Jarvis was observed and analyzed by Faugère and Perret based on the underyling multi-homogeneous structure [BGL20, Appendix A].

Part II
Cryptanalysis of Multivariate Schemes

Chapter 4 Analyzing Support-Minors on HFE Variants

The content of this chapter is a joint work with John Baena, Daniel Cabarcas, Ray Perlner, Daniel Smith-Tone and Javier Verbel [Bae+22]. It has been published at CRYPTO 2022.

We give a rank attack on HFEv- which consists in solving the MinRank instance of Tao *et al.* by applying Support-Minors. As noted in [TPD21], the unmodified XL algorithm introduced by [Bar+20b] would fail in this context due to the big-field structure. Thus, we decided to adopt a more standard Gröbner basis approach that we managed to estimate precisely. This analysis was missing in [TPD21] and it even allowed us to improve upon their conjectures.

The second part of [Bae+22] is more general. We study the memory complexity of attacks based on the Support-Minors modeling. Our results apply in particular to the rectangular MinRank attack on Rainbow [Beu21a], where this issue had been a major point of discussion[1]. Even if I actively participated in the writing, most of the ideas were due to Ray Perlner and Daniel Smith-Tone. For this reason, the corresponding content does not appear in this manuscript. We refer to the eprint version [Bae+21].

Contents

[1] https://troll.iis.sinica.edu.tw/by-publ/recent/response-ward.pdf.

4.1 Preliminaries

We start by providing more specific background in order to better understand our contributions. Section 4.1.1 introduces the MinRank problem of [TPD21] which is the basis for our work. Section 4.1.2 presents the Projection modifier. HFEv- with Projection, pHFEv- for short, was proposed in [ØSV21] as being immune to [TPD21]. Its parameters are now obsolete due to our attack.

4.1.1 Considered MinRank Problem

As discussed at the end of Section 3.2.2.3, the main component of [TPD21] is a new MinRank instance to attack HFE variants. What was crucial at that time is that the rank $d = \left\lceil \log_q(D) \right\rceil$ does not depend on the modifiers.

To describe their approach, we assume that q is an odd prime power[2] and we keep the notation that we used for Problem 3.4. In particular, let $\boldsymbol{\beta} \stackrel{def}{=} (\beta_1, \ldots, \beta_n)$ be a basis of the vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $\boldsymbol{M} \stackrel{def}{=} [\beta_{i+1}^{q^j}]_{i,j=0}^{n-1}$. Since we deal with vinegar variables, we consider the augmented matrix

$$\widetilde{\boldsymbol{M}} \stackrel{def}{=} \begin{bmatrix} \boldsymbol{M} & 0 \\ 0 & \boldsymbol{I}_v \end{bmatrix} \in \mathbb{F}_{q^n}^{(n+v)\times(n+v)}. \tag{4.1}$$

Let us recall that the solutions to Problem 3.4 allowed to recover the coefficients of a matrix depending only on the outer map $\mathcal{T}$, namely $\boldsymbol{V} = \boldsymbol{T}^{-1}\boldsymbol{M}$ in Equation (3.9). In [TPD21], the rank d matrix is related to the inner map $\mathcal{S} : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$. More precisely, the authors aim at obtaining the matrix

$$\boldsymbol{U} \stackrel{def}{=} \widetilde{\boldsymbol{M}}^{-1}\boldsymbol{S}^{-1} \in \mathbb{F}_{q^n}^{(n+v)\times(n+v)}, \tag{4.2}$$

where $\boldsymbol{S} \in \mathbb{F}_q^{(n+v)\times(n+v)}$ is an invertible matrix representing $\mathcal{S}$. For that purpose, they solve the following MinRank instance.

Problem 4.1 (Theorem 2, [TPD21]). *Let $\boldsymbol{P}_1, \ldots, \boldsymbol{P}_{n-a} \in \mathbb{F}_q^{(n+v)\times(n+v)}$ denote the symmetric matrices associated to the HFEv- public polynomials and let $(\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_{n+v})$ be the canonical basis of $\mathbb{F}_q^{n+v}$. For $1 \leqslant i \leqslant n+v$, let*

$$\boldsymbol{M}_i \stackrel{def}{=} \boldsymbol{\varepsilon}_i\boldsymbol{P}_* \stackrel{def}{=} \begin{bmatrix} \boldsymbol{\varepsilon}_i\boldsymbol{P}_1 \\ \vdots \\ \boldsymbol{\varepsilon}_i\boldsymbol{P}_{n-a} \end{bmatrix} \in \mathbb{F}_q^{(n-a)\times(n+v)}. \tag{4.3}$$

Then, the first row $\boldsymbol{u} \stackrel{def}{=} (u_1, \ldots, u_{n+v})$ of the matrix $\boldsymbol{U}$ defined in Equation (4.2) is a non-zero solution to the homogeneous MinRank problem described by the $\boldsymbol{M}_i$'s with target rank $d = \left\lceil \log_q(D) \right\rceil$.

[2] The results can be extended to the even characteristic, see for instance [Bae+21, Appendix A].

As in the original MinRank problem proposed by Kipnis and Shamir [KS99], we are interested in solutions over $\mathbb{F}_{q^n}$ while the public matrices are over $\mathbb{F}_q$. In particular, the following observation of [TPD21] was already present in previous literature on big-field MPKC [KS99; JDH07; BFP13; VS17].

Fact 1. *Let $\boldsymbol{v} \in \mathbb{F}_{q^n}^{n+v}$ be a non-zero solution to Problem 4.1. Then, for any $\lambda \in \mathbb{F}_{q^n}^*$, the vector $\lambda\boldsymbol{v} = (\lambda v_1, \ldots, \lambda v_{n+v})$ is another non-zero solution. Moreover, for any $0 \leqslant j \leqslant n-1$, the same goes for the vector $\boldsymbol{v}^{[j]} \stackrel{def}{=} (v_1^{[j]}, \ldots, v_{n+v}^{[j]})$.*

This result should also be confronted with more rigorous ones on equivalent keys, e.g., [WP11]. First, we do not expect spurious solutions. Second, any non-zero solution $\boldsymbol{u}'$ as in Fact 1 is the first row of a matrix $\boldsymbol{U}'$ leading to an equivalent map $\mathcal{S}'$. For the rest of the key-recovery, we refer to [TPD21, Algorithm 1] and [TPD21, Algorithm 2].

Before we go on, we want to mention a similarity between [TPD21] and the rectangular MinRank attack on Rainbow [Beu21a]. Even if we did not describe the latter, one thing in common in these two works is that any matrix $\boldsymbol{M}_i$ from the MinRank instance contains data from *all* the public polynomials (see for instance Equation (4.3)). This is in contrast to earlier attacks where each matrix was associated to only one equation (*e.g.*, $\boldsymbol{M}_i = \boldsymbol{P}_i$ in Problem 3.4). Rectangular MinRank problems of the same type have also been considered in the cryptanalysis of UOV [Beu+23, §4.5] and variants of it [FI23].

4.1.2 Projection Modifier

The Projection modifier was introduced in order to repair the SFLASH signature scheme after the break of [DFSS07], which lead to the design of PFLASH [CYS15]. In reaction to [TPD21], the authors of [ØSV21] also applied this modifier to HFEv-. In this context, Projection consists in replacing the map $S : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$ by $S = \overline{L} \circ S' : \mathbb{F}_q^{n+v-p} \to \mathbb{F}_q^{n+v}$, where $S' : \mathbb{F}_q^{n+v-p} \to \mathbb{F}_q^{n+v-p}$ is invertible and $\overline{L} : \mathbb{F}_q^{n+v-p} \to \mathbb{F}_q^{n+v}$ is full-rank represented by a matrix

$$\begin{bmatrix} \boldsymbol{\Lambda} & 0 \\ 0 & \boldsymbol{I}_v \end{bmatrix} \in \mathbb{F}_q^{(n+v-p)\times(n+v)}.$$

The point now is that the rank of the matrix is bounded by $d + p$ instead of d (cf. [ØSV21, Proposition 2]) and this upper bound is believed to be tight ([ØSV21, Table 1]). In contrast to previous modifiers, this means that Problem 4.1 with Projection admits a higher target rank. This very fact allowed [ØSV21] to find secure parameters for their new pHFEv- scheme by starting from weak HFEv- parameters. Even though the complexity of inverting pHFEv- is q^p times more than the one of inverting HFEv- for the same degree D, it is also faster than solving a HFE polynomial of degree $q^p D$. Projection is thus interesting in that it is more efficient than simply increasing the degree of the central map to obtain the same security.

The current G*e*MSS parameters as well as those of pHFEv- are given in Table 4.1. In [ØSV21], a secure pHFEv- parameter set was constructed from a G*e*MSS one by choosing the least value of p such that the attack of [TPD21] is just above the security level.

Table 4.1: G*e*MSS and pHFEv- parameter sets.

Scheme	q	n	v	D	a	p from [ØSV21]
G*e*MSS128	2	174	12	513	12	0
BlueG*e*MSS128	2	175	14	129	13	1
RedG*e*MSS128	2	177	15	17	15	4
G*e*MSS192	2	265	20	513	22	5
BlueG*e*MSS192	2	265	23	129	22	7
RedG*e*MSS192	2	266	25	17	23	10
G*e*MSS256	2	354	33	513	30	10
BlueG*e*MSS256	2	358	32	129	34	11
RedG*e*MSS256	2	358	35	17	34	14

4.2 Applying Support-Minors

The first approach to solve Problem 4.1 retained in [TPD21] was to use the Minors modeling (Modeling 2). Even if Support-Minors (SM) was already known at that time, the authors considered that the large solution set from Fact 1 seemed to make the XL technique of [Bar+20b] based on multiplying by linear variables inapplicable. For this reason, they decided to run a standard Gröbner basis algorithm that also multiplies by minor variables. The complexity formula for this method [TPD21, p. 15] assumes that the solving degree of SM is equal to 3 and it only relies on experiments.

In our work, we proceed according to their second strategy. However, we manage to grasp the early steps of the Gröbner basis computation. Our analysis turns out to be sufficient – in the range of parameters of interest – to derive a less conjectural estimate.

- In Section 4.2.1, we consider a specialized SM system – Modeling 8 – by fixing two variables. This modeling still admits solutions due to the properties of Problem 4.1 and that of the SM polynomials.

- In Section 4.2.2, we show that both the specialization and an advantageous parameter range trigger degree 1 equations which are obtained as linear combinations between the initial affine bilinear polynomials.

- By substitution in Modeling 8, these degree 1 polynomials allow to derive a quadratic system – Modeling 9 – in only $n-1$ variables. In Section 4.2.3, we solve it using Gröbner bases.

4.2.1 Our Specialization

We set $\boldsymbol{Z} \stackrel{def}{=} \sum_{j=1}^{n+v} u_i \boldsymbol{M}_i$ for a candidate rank d matrix[3] and we consider its transpose $\boldsymbol{Z}^\mathsf{T}$. As in [Bar+20b; Beu21a; TPD21], we restrict ourselves to a subset of Support-Minors equations obtained from a submatrix in $\mathbb{F}_q[\boldsymbol{u}]^{(n+v)\times n'}$. Up to relabelling of the linear variables, we also fix $u_{n+v} = 1$. This specialization is exactly the same as in [BFP13, Theorem 7] and [TPD21], among many others. From Fact 1, we thus expect a variety of the form $\{\widetilde{\boldsymbol{u}}, \widetilde{\boldsymbol{u}}^{[1]}, \ldots, \widetilde{\boldsymbol{u}}^{[n-1]}\}$, where $(\widetilde{\boldsymbol{u}})_{n+v} = 1$. By [TPD21, Proposition 5 & Algorithm 1], recall that there exists an invertible matrix $\boldsymbol{U}' \in \mathbb{F}_{q^n}^{(n+v)\times(n+v)}$ representing an equivalent map such that

$$\boldsymbol{U}'_{\{1..n\},*} = \begin{bmatrix} \widetilde{\boldsymbol{u}} \\ \vdots \\ \widetilde{\boldsymbol{u}}^{[n-1]} \end{bmatrix} \in \mathbb{F}_{q^n}^{n\times(n+v)}. \tag{4.4}$$

Finally, since we can choose an arbitrary submatrix $\boldsymbol{Z}^\mathsf{T}_{*,J}$ of $\boldsymbol{Z}^\mathsf{T}$ with $\#J = n'$, we can make sure that this submatrix is full-rank on its first d columns. Therefore, we fix the minor variable $c_{\{1\ldots d\}}$ to 1.

Modeling 8. *Let $\boldsymbol{Z}$ be a target rank d matrix of the form $\boldsymbol{Z} \stackrel{def}{=} \sum_{j=1}^{n+v} u_i \boldsymbol{M}_i$. We consider the SM equations obtained from $n' \leqslant n - a$ columns in $\boldsymbol{Z}^\mathsf{T}$ with coefficients in $\mathbb{F}_q$ and solutions in $\mathbb{F}_{q^n}$, in which we fix $u_{n+v} = 1$ and $c_{\{1\ldots d\}} = 1$.*

This gives an affine bilinear system with $(n+v)\binom{n'}{d+1}$ equations. There are $(n+v)\binom{n'}{d}$ monomials and in particular $(n+v-1)(\binom{n'}{d}-1)$ quadratic ones of the form $u_i c_T$ for $1 \leqslant i < n+v$ and $T \neq \{1..d\}$.

We can clearly pick a number of columns $n' \leqslant n - a$ that yields a sub-system with more equations than monomials. This will be the case when $(n+v)\binom{n'}{d+1} \geqslant (n+v)\binom{n'}{d}$, *i.e.*, $n' \geqslant 2d+1$. This is indeed achievable on G*e*MSS because the value of $n-a$ is much higher than $2d+1$ in practice. Also, for these parameters, we do not go beyond the MinRank uniqueness bound given by Equation (3.4) page 31 even when $n' = 2d+1$.

4.2.2 Linear Degree Fall Polynomials

From now on we assume that the number of columns is $n' \geqslant 2d+1$. If the corresponding Modeling 8 were to have a unique solution, the XL approach of [Bar+20b] would succeed in degree $b = 1$. Here however, it is not clear how to apply this technique. Indeed, the linear system given by the Macaulay matrix has a large kernel. More precisely, since we expect Modeling 8 to have n solutions which correspond to n linearly independent vectors $\{\boldsymbol{v}, \boldsymbol{v}^{[1]}, \ldots, \boldsymbol{v}^{[n-1]}\}$ such that the first $n+v-1$ components of $\boldsymbol{v}$ are $(\widetilde{\boldsymbol{u}})_1, \ldots, (\widetilde{\boldsymbol{u}})_{n+v-1}$, this kernel should have dimension $\geqslant n$. Moreover, for large enough n, this bound was tight in our experiments. Thus, we adopt the following Assumption 2 in the rest of the analysis.

[3] This notation is the one of [TPD21, Theorem 2].

Assumption 2. *Let $n' \geqslant 2d+1$. We assume that the number of linearly independent equations in Modeling 8 is equal to*

$$\mathcal{N}_{\mathcal{Q}} \stackrel{def}{=} (n+v)\tbinom{n'}{d} - n.$$

Linear polynomials. Based on this assumption, we prove that there is a set $\mathcal{L}$ of degree 1 polynomials obtained from linear combinations between the initial equations. In other words, there are degree falls from degree 2 to degree 1 in the Support-Minors system $\mathcal{Q}$.

Lemma 4.1. *Under Assumption 2, one can generate $\mathcal{N}_{\mathcal{L}}$ such linearly independent polynomials, where*

$$\mathcal{N}_{\mathcal{L}} \geqslant \tbinom{n'}{d} + v - 1.$$

Proof. By Assumption 2, the system of Modeling 8 contains $\mathcal{N}_{\mathcal{Q}} = (n+v)\tbinom{n'}{d} - n$ linearly independent equations. Note that one has

$$\mathcal{N}_{\mathcal{Q}} \geqslant (n+v-1)\left(\tbinom{n'}{d} - 1\right).$$

This means that the number of linearly independent *affine bilinear* equations is greater than the number of *bilinear* monomials. In particular, there are non-trivial linear combinations between the bilinear parts of the equations that are zero. In turn, by performing linear algebra operations on Modeling 8, we obtain at least

$$\underbrace{\left((n+v)\tbinom{n'}{d} - n\right)}_{\mathcal{N}_{\mathcal{Q}}} - \underbrace{(n+v-1)\left(\tbinom{n'}{d} - 1\right)}_{\#\text{bilinear monomials}} = \tbinom{n'}{d} + v - 1$$

linearly independent affine degree 1 polynomials. □

Eliminating variables. We use the system $\mathcal{L}$ to simplify unknowns. For instance, we choose to eliminate first and foremost all the $n_{c_T} \stackrel{def}{=} \binom{n'}{d} - 1$ minor variables by considering an order such that $c_T > u_{n+v-1} > \cdots > u_1 > u_{n+v} = 1$. Let $\mathcal{M}\text{ac}_{\leqslant 1}(\mathcal{L})$ denote the Macaulay matrix whose columns are sorted accordingly. Lemma 4.2 shows that we have a good control on the shape of its row echelon form and that Lemma 4.1 is actually an equality.

Lemma 4.2. *Under Assumption 2, the reduced row echelon form of $\mathcal{M}ac_{\leqslant 1}(\mathcal{L})$ reads*

$$\boldsymbol{L} \stackrel{def}{=} \begin{bmatrix} \boldsymbol{I}_{n_{c_T}} & * \\ 0 & \boldsymbol{K} \end{bmatrix} \in \mathbb{F}_q^{\mathcal{N}_{\mathcal{L}} \times (n_{c_T}+n+v)}, \tag{4.5}$$

where $\boldsymbol{K} \in \mathbb{F}_q^{(\mathcal{N}_{\mathcal{L}} - n_{c_T}) \times (n+v)}$ is row reduced. Moreover, we have $\mathcal{N}_{\mathcal{L}} = n_{c_T} + v$.

Proof. We denote by $\boldsymbol{L}$ the echelon form of $\mathcal{M}\mathrm{ac}_{\leqslant 1}(\mathcal{L})$, namely

$$\boldsymbol{L} \stackrel{def}{=} \begin{bmatrix} \boldsymbol{N} & * \\ 0 & \boldsymbol{K} \end{bmatrix}, \text{where } \boldsymbol{N} \in \mathbb{F}_q^{n_{c_T} \times n_{c_T}} \text{ and } \boldsymbol{K} \in \mathbb{F}_q^{(\mathcal{N}_{\mathcal{L}} - n_{c_T}) \times (n+v)}.$$

Let us assume that this matrix is not systematic on its first n_{c_T} rows, *i.e.*, $\boldsymbol{N} \neq \boldsymbol{I}_{n_{c_T}}$. On that hypothesis, there is a set of $v_0 \geqslant \mathcal{N}_{\mathcal{L}} - n_{c_T} + 1 \geqslant v + 1$ linearly independent vectors in the row space of $\boldsymbol{L}$ which have zero in their leftmost n_{c_T} entries. This yields v_0 linearly independent vectors $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{v_0} \in \mathbb{F}_q^{n+v}$ orthogonal to $\widetilde{\boldsymbol{u}} \in \mathbb{F}_{q^n}^{n+v}$. In fact, since these vectors are over $\mathbb{F}_q$, they are orthogonal to $\widetilde{\boldsymbol{u}}^{[j]}$ for any $0 \leqslant j \leqslant n-1$. Thus, the matrix

$$\boldsymbol{U}'_{\{1..n\},*} = \begin{bmatrix} \widetilde{\boldsymbol{u}} \\ \vdots \\ \widetilde{\boldsymbol{u}}^{[n-1]} \end{bmatrix} \in \mathbb{F}_{q^n}^{n \times (n+v)}$$

is not full-rank. This is a contradiction since $\boldsymbol{U}'$ is invertible.

For the second part of the proof, the number of rows $\mathcal{N}_{\mathcal{L}} - n_{c_T}$ in $\boldsymbol{K}$ is at least v by Lemma 4.1. In addition, since the vector $\widetilde{\boldsymbol{u}}$ is a solution to the MinRank problem, there exists $\boldsymbol{w} \in \mathbb{F}_{q^n}^{n_{c_T}}$ corresponding to the minor variables such that

$$\mathcal{M}\mathrm{ac}_{\leqslant 1}(\mathcal{L})(\boldsymbol{w}, (\widetilde{\boldsymbol{u}})_{n+v-1}, \ldots, (\widetilde{\boldsymbol{u}})_1, 1)^{\mathsf{T}} = \boldsymbol{0}.$$

By the same argument, as the matrix $\mathcal{M}\mathrm{ac}_{\leqslant 1}(\mathcal{L})$ has its entries in $\mathbb{F}_q$, we obtain n vectors in the right kernel:

$$\forall 0 \leqslant j \leqslant n-1,\ \mathcal{M}\mathrm{ac}_{\leqslant 1}(\mathcal{L})(\boldsymbol{w}^{[j]}, (\widetilde{\boldsymbol{u}})_{n+v-1}^{[j]}, \ldots, (\widetilde{\boldsymbol{u}})_1^{[j]}, 1)^{\mathsf{T}} = \boldsymbol{0}.$$

As we recover $\boldsymbol{U}'_{\{1..n\},\{1..n+v-1\}}$, these vectors are linearly independent. This shows that the rank of $\boldsymbol{K}$ is at most $(n + v - n) = v$, hence $\mathcal{N}_{\mathcal{L}} - n_{c_T} = v$. □

From Lemma 4.2, it is then possible to express all the minor variables as well as v linear variables in terms of the remaining $n_u \stackrel{def}{=} n - 1$ linear variables. Moreover, by reordering the linear variables if necessary, we may further assume that the remaining ones are $u_1, \ldots, u_{n-1}$. In this case, the matrix corresponding to the homogeneous degree 1 parts (by dropping the last column of $\boldsymbol{L}$) is of the form

$$\boldsymbol{L}^{\text{left}} \stackrel{def}{=} \boldsymbol{L}_{*,\{1..n_{c_T}+v+n_u\}} = \begin{bmatrix} \boldsymbol{I}_{n_{c_T}} & 0 & \boldsymbol{Y} \\ 0 & \boldsymbol{I}_v & \boldsymbol{W} \end{bmatrix} \in \mathbb{F}_q^{\mathcal{N}_{\mathcal{L}} \times (n_{c_T}+v+n_u)}, \tag{4.6}$$

where $\boldsymbol{Y} \in \mathbb{F}_q^{n_{c_T} \times n_u}$ and $\boldsymbol{W} \in \mathbb{F}_q^{v \times n_u}$.

4.2.3 Solving a Quadratic System

The end of Section 4.2.2 shows that by substituting $\mathcal{L}$ in Modeling 8, the bilinear parts reduce to quadratic parts in only $n_u = n - 1$ linear variables.

Modeling 9 (Quadratic System). *We consider the affine quadratic system in $n_u = n - 1$ linear variables $u_1, \ldots, u_{n-1}$ obtained by plugging the linear polynomials of $\mathcal{L}$ into the equations from Modeling 8.*

The final stage of our approach is to solve Modeling 9 using Gröbner bases. Before starting, note that this system is extremely overdetermined since we have $\mathcal{N}_{\mathcal{Q}} - \mathcal{N}_{\mathcal{L}} = (n+v-1)\left(\binom{n'}{d} - 1\right) = (n_u + v)n_{c_T} \geqslant n_u n_{c_T}$ quadratic equations in n_u variables. In particular, this should already correspond to a weak zone for MQ when n_{c_T} is not too small. Our precise analysis actually considers two situations in line with this first observation.

Case $n_{c_T} \geqslant n_u$. Modeling 9 is even more overdetermined. In Proposition 4.1, we prove that the Gröbner basis computation actually terminates in degree 2. We rely on Assumption 2 and on the following Assumption 3 about the echelon form $\boldsymbol{L}^{\text{left}}$ from Equation (4.6).

Assumption 3. *The matrix $\boldsymbol{Y} \in \mathbb{F}_q^{n_{c_T} \times n_u}$ in Equation (4.6) is full rank.*

Note that this assumption should hold with high probability if $\boldsymbol{Y}$ behaves as a random matrix. However, since this matrix actually comes from the scheme, we have also performed simulations to verify Assumptions 2 and 3. According to the results we obtained for different sets of parameters (q, n, v, D, a), it seems that if n' is chosen such that $n' \geqslant 2d + 1$ and $n_{c_T} \geqslant n_u$, then these assumptions are satisfied almost 100% of the times. The reader might find helpful to experimentally explore these assumptions using the SageMath notebook [BV21].

Proposition 4.1. *Under Assumptions 2 and 3 and if $n_{c_T} \geqslant n_u$, a Gröbner basis for Modeling 9 can be obtained by Gaussian elimination on the initial equations.*

Proof. By Assumption 2 and the first part of Lemma 4.2, the number of affine quadratic equations which remain after the linear algebra step in Modeling 8 and that we can expect in Modeling 9 is equal to $\mathcal{N}_{\mathcal{Q}} - \mathcal{N}_{\mathcal{L}} = (n+v-1)\left(\binom{n'}{d} - 1\right) = (n_u + v)n_{c_T}$. As we cannot construct extra degree falls between them, this implies that the linear span of these equations contains an equation with leading monomial $u_i c_T$ for any T, $\#T = d$, $T \neq \{1..d\}$ and any $1 \leqslant i \leqslant n_u + v$. Recall from Equation (4.6) the matrix

$$\boldsymbol{L}^{\text{left}} = \begin{bmatrix} \boldsymbol{I}_{n_{c_T}} & 0 & \boldsymbol{Y} \\ 0 & \boldsymbol{I}_v & \boldsymbol{W} \end{bmatrix} \in \mathbb{F}_q^{\mathcal{N}_{\mathcal{L}} \times (n_{c_T} + v + n_u)},$$

where $n_u = n - 1$, $\boldsymbol{Y} \in \mathbb{F}_q^{n_{c_T} \times n_u}$ and $\boldsymbol{W} \in \mathbb{F}_q^{v \times n_u}$. We also denote by $\boldsymbol{c}$ the row vector of length n_{c_T} whose components are the minor variables and $(u_1, \ldots, u_{n+v-1}) \overset{def}{=} (\boldsymbol{u}_+, \boldsymbol{u}_-)$, where $\boldsymbol{u}_+$ is of length n_u (remaining linear variables) and $\boldsymbol{u}_-$ is of length v (removed linear variables). Then, there is a vector of constants $\alpha \in \mathbb{F}_q^{n_{c_T}}$ such that

$$\boldsymbol{c}^{\mathsf{T}} = -\boldsymbol{Y}\boldsymbol{u}_+^{\mathsf{T}} - \alpha^{\mathsf{T}}. \tag{4.7}$$

Since $\boldsymbol{Y}$ is full rank by Assumption 3, the linear system in the $\boldsymbol{u}_+$ variables given by Equation (4.7) can be inverted when $n_{c_T} \geqslant n_u$. Thus, all $\binom{n_u+1}{2}$ quadratic leading monomials will be found in the span of Modeling 9. □

Case $n_{c_T} < n_u$. In this situation, we do no longer control the value of the solving degree. Still, we can argue that it is quite low for a significant range of parameters due to the high number of equations. This discussion is essentially for the sake of completeness because we can ensure that $n_{c_T} \geqslant n_u$ with the parameters of G*e*MSS.

We keep the notation from the proof of Proposition 4.1. Recall that the linear system of Equation (4.7) expresses the c_T variables in terms of the remaining $n_u = n - 1$ linear variables $u_1, \ldots, u_{n-1}$ and that it is full rank by Assumption 3. When $n_{c_T} < n_u$, there exists a set $(\gamma_i)_{i=1}^{n_{c_T}}$ of linear variables which can be written in function of these minor variables. Let us denote the $n_u - n_{c_T}$ remaining ones by $(\delta_j)_j$, so that $\binom{n_u - n_{c_T}+1}{2}$ quadratic monomials $\delta_i\delta_j$ are missing in degree 2. Now, Modeling 9 initially contains $\geqslant n_u n_{c_T}$ equations, which is generally much more than

$$\binom{n_u+1}{2} - \binom{n_u-n_{c_T}+1}{2} = n_u n_{c_T} + \tfrac{1}{2}(n_u - n_{c_T}^2 - 1)$$

the possible number of leading monomials of the form $\gamma_i\gamma_j$ or $\gamma_i\delta_j$. In such a case, for each of these monomials μ, we hope to construct an equation $f_\mu = \mu + \ell_\mu$ such that $\deg(\ell_\mu) = 1$. Let us finally explain why the missing quadratic monomials $\delta_i\delta_j$ might be found in degree 3. For the sake of clarity, we do the reasoning for δ_1^2. For $1 \leqslant i \leqslant c_T$, let $\mu_{i,1} \stackrel{def}{=} \gamma_i\delta_1$ and let $\mu_{i,2} \stackrel{def}{=} \gamma_i\delta_2$. Then, the S-polynomial

$$S(f_{\mu_{i,1}}, f_{\mu_{i,2}}) = \delta_2\ell_{\mu_{i,1}} - \delta_1\ell_{\mu_{i,2}}$$

is a polynomial of degree 2 which is found in degree 3 during the Gröbner basis computation. Finally, we can expect it to contain δ_1^2 for at least one index $1 \leqslant i \leqslant c_T$ if we treat the ℓ_μ's as random linear forms.

4.3 Complexity of Solving MinRank

In this section, we estimate the running time of our attack on G*e*MSS. As we have just seen, the total cost comes down to two major steps, first generating Modeling 9 from Modeling 8 and then solving Modeling 9 via Gröbner bases. These steps are analyzed in Section 4.3.1 and Section 4.3.2 respectively. In Section 4.3.3, we also discuss the corresponding memory complexity.

Before we begin, note that the content of Section 4.2 also applies to pHFEv- with rank equal to $d' \stackrel{def}{=} d + p$. We simply have to replace the condition $n' \geqslant 2d + 1$ by $n' \geqslant 2d' + 1$ in the discussion at the end of Section 4.2.1. Moreover, this minimal value of n' already ensures $n_{c_T} \geqslant n_u$ for all the G*e*MSS and pHFEv- parameters (see Table 4.1). By Proposition 4.1, this means that Modeling 9 will be solved at degree 2. Independently, some of our estimates will assume that $v = o(n)$.

4.3.1 Kernel of Macaulay Matrix

The first step of the attack aims at obtaining the linear system $\mathcal{L}$ described in Section 4.2.2. In fact, it can be recovered from the right kernel of the first (affine) Macaulay matrix for Modeling 8. Note that such a kernel is also computed in standard XL. Here, we simply use it for different purposes.

A first method to obtain it is to rely on a row echelon form. The corresponding complexity in $\mathbb{F}_q$-operations is

$$\mathcal{O}\left((n+v)\binom{2d+1}{d}\left((n+v)\binom{2d+1}{d}\right)^{\omega-1}\right), \tag{4.8}$$

where $2 \leqslant \omega \leqslant 3$ is the constant of linear algebra. By setting $n_u = n - 1$ and $n_{c_T} = \binom{2d+1}{d} - 1$, this is a $\mathcal{O}\left(n_{c_T}^{\omega} n_u^{\omega}\right)$.

An alternative one is to apply Coppersmith's Block-Wiedemann algorithm (BW). Since our assumptions implied a dimension n for the kernel, we hope to find a basis of it with good probability by running BW roughly n times. Recalling that the weight of a SM equation is at most $(n+v)(d+1)$ (see Lemma 3.1), we get

$$\mathcal{O}\left(n \times (n+v)(d+1)\left((n+v)\binom{2d+1}{d}\right)^{2}\right) = \mathcal{O}\left(d n_{c_T}^2 n_u^4\right). \tag{4.9}$$

4.3.2 Gröbner Bases on Quadratic System

We have already discussed at the beginning of Section 4.3 that G*e*MSS and pHFEv- can yield instances of Modeling 9 which are solved in degree 2. The cost of the Gröbner basis step is thus the one of row reducing the affine Macaulay matrix at this degree. The number of columns is the number of initial monomials which is equal to $1 + n_u + \binom{n_u+1}{2}$ and there are more equations than monomials. The total complexity in $\mathbb{F}_q$-operations is then

$$\mathcal{O}\left(n_{c_T}(n+v-1)\left(1 + n_u + \binom{n_u+1}{2}\right)^{\omega-1}\right) = \mathcal{O}\left(n_{c_T} n_u^{2\omega-1}\right), \tag{4.10}$$

where $2 \leqslant \omega \leqslant 3$ is the exponent in the complexity of matrix multiplication. Note that the first step is expected to be more costly since $n_u \leqslant n_{c_T}$.

4.3.3 Memory Demand

This section contains details about the memory costs which are naturally associated to the attack. We restrict ourselves to Modeling 8 since the system given by Modeling 9 is significantly smaller. In Sections 4.3.3.1 and 4.3.3.2, we study the space complexity of the main step by describing two ways to store the Macaulay matrix $\mathcal{M}\mathrm{ac}(\mathcal{Q})$ when used within the BW algorithm. We choose $q = 2$ as in concrete parameters, which means that one element in $\mathbb{F}_q$ occupies one bit in memory. Finally, Section 4.3.3.3 provides a

comparison between these two approaches in the case of G*e*MSS and it also gives the space complexity of Strassen's algorithm.

Note that the analysis presented here is quite different from the one performed in the other part of [Bae+22]. There, we focus on the *memory access costs* which can be a bottleneck when applying BW to very large Macaulay matrices arising from SM-based attacks. In contrast to [Bar+20b; Beu21a] where they might be an issue, these costs should not be concerning to attack HFEv-. Indeed, we only deal with the bi-degree $(1, 1)$ Macaulay matrix which is very small in comparison. This can also be seen, to some extent, from the data given in Table 4.2. Even if these numbers do not tell about memory management and even if we did not describe state-of-the-art BW implementations (*e.g*, [CCNY12]), such small values should give enough confidence in the feasibility of our attack.

4.3.3.1 Naive Organization

This approach uses the sparsity of the matrix $\mathcal{M}\mathrm{ac}(\mathcal{Q})$ in the most standard way. Recall from Lemma 3.1 that every SM equation contains at most $(n + v)(d + 1)$ nonzero monomials. Thus, one way to store a single row of $\mathcal{M}\mathrm{ac}(\mathcal{Q})$ is to keep track of the indexes corresponding to nonzero positions. Hence we must store at most $(n+v)(d+1)$ column indexes per row. Since the Macaulay matrix has $(n+v)\binom{2d+1}{d}$ columns and since we usually drop several rows to get a square matrix, the space complexity is given by

$$\binom{2d+1}{d}(d+1)(n+v)^2 \log_2\left(\binom{2d+1}{d}(n+v)\right) = \mathcal{O}\left(dn_u^2 n_{c_T} \log_2(n_{c_T})\right). \tag{4.11}$$

4.3.3.2 Optimized Organization

A very simple way to improve upon the naive approach is to take advantage of the structure of Macaulay matrix. This was pioneered by Niederhagen [Nie12, §4.5.3] in the case of generic matrices. We adapt his techniques to the Macaulay matrix $\mathcal{M}\mathrm{ac}(\mathcal{Q})$ by noting that we can also use the SM structure.

Remark 4.1. This part of the paper was mostly Javier's contribution.

Before instantiating the G*e*MSS case, we describe the approach on an arbitrary MinRank problem with K matrices in $\mathbb{F}_2^{n_r \times n_c}$, target rank d and unknown vector $\boldsymbol{x}$. The core idea is to divide the Macaulay matrix into $\binom{n_c}{d+1}$ blocks $\mathcal{S}_J$ labelled by $J \subset \{1..n_c\}$, $\#J = d + 1$ such that $\mathcal{S}_J$ contains the equations $Q_{j,J}$ for $1 \leqslant j \leqslant n_r$. We have seen in Lemma 3.1 that all these equations have the same monomials, so that the set of columns potentially allocating nonzero entries are the same for each row in the block. This is the key fact to get a more efficient storage. Our approach then splits the storage of the matrix into four arrays V_1, V_2, V_3, and V_4:

V_1 This is a 2-dimensional array of size $n_r \times (Kn_c)$ which stores the coefficients of the linear forms which are the entries of $\boldsymbol{M} \in \mathbb{F}_2[\boldsymbol{x}]^{n_r \times n_c}$. The entry in position (i, j) in V_1 corresponds the coefficient of $x_{(j \bmod K)+1}$ in $\boldsymbol{M}_{i,\lceil (j-1)/K \rceil + 1}$.

V_2 This stores the indexes of the nonzero values of the Macaulay matrix for each block $\mathcal{S}_J,\ J = \{j_1, \ldots, j_{d+1}\}$. As seen in Lemma 3.1, the possibly nonzero coefficients of $Q_{j,J}$ only depend on J since they correspond to the monomials $u_i c_{J\setminus j_\ell},\ 1 \leqslant i \leqslant K,\ 1 \leqslant \ell \leqslant d+1$. Thus, we implement V_2 as an array of length $\binom{n_c}{d+1}$ such that each coordinate is enumerated by a set J and stores the $K(d+1)$ potential nonzero indexes. This requires

$$\binom{n_c}{d+1} K(d+1) \log_2 \left(\binom{n_c}{d} K \right) \tag{4.12}$$

bits of memory.

V_3 This indicates the columns of V_1 from which the nonzero coefficients of a given SM equation should be taken. These column indexes are the same for all the equations in one block $\mathcal{S}_J$ since they correspond to the elements of J. This data can be stored as an array of size $\binom{n_c}{d+1}$, where each coordinate contains a bit string of length $K(d+1)\log_2(Kn_c)$ bits of memory. So far, the only information missing to be able to read the nonzero coefficients of a given SM equation is the index of the row of V_1 from which they must be read. This is stored in V_4.

V_4 Since we usually drop several rows of the initial Macaulay matrix to end up with a square matrix, we have to keep track of the row of $\boldsymbol{M}$ from which a given SM equation comes from. Therefore, V_4 stores the indexes of the corresponding row in $\boldsymbol{M}$ for the $K\binom{n_c}{d}$ equations chosen to construct this square Macaulay matrix. This requires $\binom{n_c}{d} K \log_2(n_r)$ bits of memory.

Now we explain how the allocations of the vectors $V_1, \ldots, V_4$ fully store the Macaulay matrix. Basically, for a given row of the Macaulay matrix, we show how to get the coordinates and values of the potential nonzero entries by just accessing the memory allocated in V_1, V_2, V_3, and V_4. For the sake of clarity, let us assume that the coordinates of the vector V_4 are enumerated by elements of the set

$$\left\{ (a,b) : 0 \leqslant a \leqslant \binom{n_c}{d+1} \text{ and } 1 \leqslant b \leqslant n_r \right\}.$$

Then, for a given row (a_0, b_0) we know:

1. The indexes of the coordinates containing the potential nonzero positions by reading the bits in $V_2[a_0]$.
2. The values corresponding to the indexes in $V_2[a_0]$ are obtained by reading in $V_1[b_0]$ the coordinates indicated by $V_3[a_0]$.

In our attack, we apply this approach to Modeling 8 with $K = n + v$, $n_r = n + v$ and $n_c = 2d + 1$. In this case, one notices that the dominant cost is provided by Equation (4.12), which reads

$$\tbinom{2d+1}{d+1}(n+v)(d+1)\log_2\left(\tbinom{2d+1}{d}(n+v)\right) = \mathcal{O}\left(dn_u n_{c_T} \log_2(n_{c_T})\right), \tag{4.13}$$

where $n_u = n - 1 \leqslant n_{c_T} = \binom{2d+1}{d} - 1$.

4.3.3.3 Sum-up

Table 4.2 presents the space complexity of the first step of our attack. Keep in mind that the two approaches of Section 4.3.3.1 and Section 4.3.3.2 were tailored to Block-Wiedemann (BW) and that the memory demand for this algorithm should not be much more than the one to fully store the Macaulay matrix. It can even be significantly lower if rows are generated on-demand, but this would increase the time complexity. In contrast, the space complexity of Strassen's algorithm is dominated by the memory demand to store a square dense matrix of size $\binom{2d+1}{d}(n+v)$, see Column "Strassen".

Table 4.2: Memory ($\log_2$(#bytes)) needed to store the Macaulay matrix $\mathcal{M}\text{ac}(\mathcal{Q})$ to be used in BW or Strassen's algorithm.

Scheme	BW Standard	BW Optimized	Strassen
GeMSS128	38.665	34.553	48.935
BlueGeMSS128	34.332	30.258	41.263
RedGeMSS128	27.645	23.729	29.873
GeMSS192	39.930	35.213	50.166
BlueGeMSS192	35.586	30.917	42.478
RedGeMSS192	28.897	24.410	31.073
GeMSS256	40.836	35.686	51.049
BlueGeMSS256	36.488	31.389	43.353
RedGeMSS256	29.800	24.905	31.940

As we can see in Table 4.2, the Optimized organization requires only a few GigaBytes of shared memory to execute BW on any of the proposed parameters for GeMSS, whereas the Standard one requires up to a few TeraBytes. To perform the same step with Strassen's algorithm, one would need up to more than two Petabytes. To sum up, the amount of memory required by BW is small enough to be allocated even in a shared memory device, especially if one uses the Optimized storing.

4.4 Applications

We now evaluate the effect of the attack on the security of GeMSS and pHFEv-.

Application to the GeMSS scheme. In Table 4.3, we give the time complexity on the actual GeMSS parameters. We use Equation (4.8) or Equation (4.9) for the linear algebra step on Modeling 8 (Step 1) and Equation (4.10) for the Gröbner basis computation on Modeling 9 (Step 2). We use $\omega = 2.81$ and a conservative constant of 7 for the concrete complexity of Strassen's algorithm [Vol69], while a constant of 3 for the concrete complexity of BW [Kal95, Theorem 7]. One can check that for the specific

parameters proposed by the G*e*MSS team, the value $n' = 2d+1$ is high enough to ensure to solve Modeling 9 in degree 2, *i.e.*, $n_u \leqslant n_{c_T}$.

Table 4.3: Complexity of our attack ($\log_2$(#gates)) versus known attacks from [TPD21] for the G*e*MSS parameters.

Scheme	Minors [TPD21]	SM [TPD21]	Step 1 (Strassen/BW)	Step 2 (Strassen)	n'
G*e*MSS128	139	118	76/72	54	21
BlueG*e*MSS128	119	99	65/65	51	17
RedG*e*MSS128	86	72	49/53	45	11
G*e*MSS192	154	120	78/75	57	21
BlueG*e*MSS192	132	101	67/67	53	17
RedG*e*MSS192	95	75	51/55	48	11
G*e*MSS256	166	121	79/77	59	21
BlueG*e*MSS256	141	103	68/69	55	17
RedG*e*MSS256	101	76	52/57	50	11

The nature of our approach, although in theory similar to the one of [TPD21], allows us to reduce significantly the complexity of the Support-Minors attack performed by Tao *et al.* This is important since this improvement makes it completely infeasible to repair G*e*MSS by simply increasing the size of its parameters without turning it into an impractical scheme.

Our dominant cost is the initial linear algebra step on the SM equations, whereas in [TPD21] an attacker needs to multiply these equations by linear and/or minor variables to solve the system in expected degree 3. This explains why we obtain a much smaller cost than the one presented in the third column "SM [TPD21]". Another noticeable difference between [TPD21] and our work is that their estimate is purely conjectural.

Application to pHFEv-. The behaviour of our attack on pHFEv- is presented in Table 4.4. We keep the same choices and formulae as in G*e*MSS to compute the complexities. In [ØSV21], recall that the value of p was chosen such that the attack of [TPD21] based on the Minors modeling is just above the security level. We adopt the parameters of [ØSV21, Table 2] obtained with $\omega_2 = 2.81$. On these parameters, one notices that our attack always succeeds in solving Modeling 9 at degree 2 with $n' = 2d' + 1 = 2(d + p) + 1$. As before, for those parameters, the values of d' are indeed high enough to guarantee $n_u \leqslant n_{c_T}$.

The results from Table 4.4 also suggest that applying Projection to HFEv- will not be sufficient to repair the scheme as we have significantly broken the parameters given in [ØSV21]. To meet the new security levels, the value of p should be increased by a consequential amount, making the scheme inefficient. For example, to achieve security level 128 with the former G*e*MSS128 parameters, one should take $p = 14$, increasing the signing time by a factor q^{14}, which is considerable.

Table 4.4: Complexity of our attack ($\log_2$(#gates)) versus known attacks from [TPD21] for pHFEv-. The pHFEv- parameter set for level x consists of (q, n, v, D, a, p), where (q, n, v, D, a) is taken from GeMSSx and $p \geqslant 0$ is the smallest value such that the cost of the Minors attack of [TPD21] is just above x.

Scheme	p	Minors [TPD21; ØSV21]	Step 1 (Strassen/BW)	Step 2 (Strassen)	n'
GeMSS128	0	139	76/72	54	21
BlueGeMSS128	1	128	71/69	53	19
RedGeMSS128	4	128	71/69	53	19
GeMSS192	5	201	105/95	67	31
BlueGeMSS192	7	201	105/95	67	31
RedGeMSS192	10	205	105/95	67	31
GeMSS256	10	256	134/117	79	41
BlueGeMSS256	11	256	129/113	77	39
RedGeMSS256	14	263	129/113	77	39

4.5 Practical Experiments

We have performed experiments in Magma-2.23-8 to explore the feasibility of the attack on GeMSS. We only present the results for the first step to generate $\mathcal{L}$ because its cost dominates the total complexity. In fact, the second step was also much cheaper from a practical perspective. For these tests, we selected $a = v \approx n/10$, a small prime $q > 2$ and $d = \left\lceil \log_q (D) \right\rceil \geqslant 3$. We chose the number of columns n' to be the smallest integer such that $n_{c_T} \geqslant n_u$, *i.e.* $\binom{n'}{d} \geqslant n$, so that Modeling 9 is solved in degree 2.

Fig. 4.1 summarizes our results. In the graph, the theoretical value is the logarithm in base two of the time complexity given in Equation (4.8) with $n_u = n-1$, $n_{c_T} = \binom{n'}{d} - 1$, $\omega = 2.81$ and a hidden constant from the Strassen's algorithm taken equal to 7. The experimental complexity is measured in terms of clock cycles of the CPU given by the Magma command ClockCycles(). The matrix reduction was done via the Magma command GroebnerBasis($\mathcal{Q}$, 2), which is equivalent to Reduce($\mathcal{Q}$) in this context[4], yet more efficient.

Our goal here is to discuss how feasible an attack on GeMSS is. For example, the level I parameter set RedGeMSS128 is $(q, n, v, D, a) = (2, 177, 15, 17, 15)$, so that $d = 5$. According to our estimates, its complexity is upper bounded by 2^{49} as shown in Table 4.3. For this value of d, we have been able to run experiments up to $n = 160$, which is quite close to the goal of 177. Fig. 4.1 also shows that the estimated complexity is a good upper bound for the computation's complexity. Note that the jump in the $d = 4$ curves corresponds to a change in the value of n'. Indeed, one can solve Modeling 9 at

[4]The two procedures are equivalent because the system is bilinear, hence quadratic, and Gröbner bases are automatically reduced in Magma.

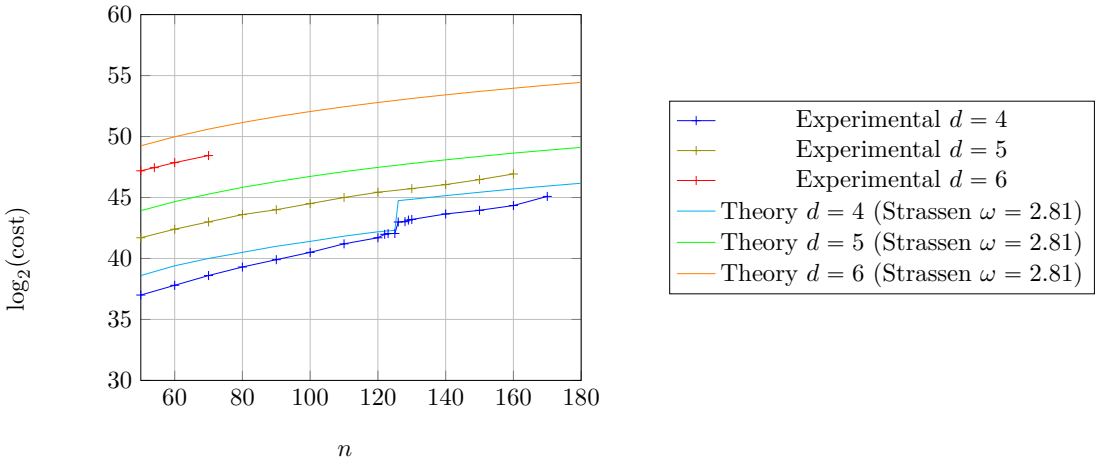


Figure 4.1: Experimental vs Theoretical value of the complexity of Step 1.

degree 2 with $n' = 2d + 1 = 9$ as long as $n \leqslant 126$, and otherwise one has to consider $n' > 2d + 1$, for instance $n' = 2d + 2$ for the rest of the data points in these curves.

A final note is that we also estimate the cost of Block-Wiedemann for this main step. Therefore, it could be interesting to use the XL implementation of Niederhagen provided in http://www.polycephaly.org/projects/xl/ in order to compute kernel vectors of $\mathcal{M}\text{ac}(\mathcal{Q})$.

Chapter 5
A Polynomial Attack on the Sidon Cryptosystem

In this chapter, we introduce the Sidon cryptosystem [RLT21] and we give our polynomial attack on the scheme. This work was published in [BTV21] with Jean-Pierre Tillich and Javier Verbel.

The proposal of [RLT21] is based on the theory of Sidon spaces, which correspond to $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$ with a multiplicative property. The core idea of the design already makes it vulnerable to a MinRank attack over $\mathbb{F}_{q^n}$ with target rank 1. Even though such a small rank might already be a sign of weakness, the authors remarked that the underlying instance had many solutions and that an arbitrary one will not necessarily lead to an attack.

We show that this particular feature is triggered by the explicit construction of a Sidon space used to instantiate the scheme. In this case, we highlight solutions over a subfield and from which we can efficiently recover an equivalent key.

Contents

5.1 The Sidon Cryptosystem

This sections presents the building blocks of the Sidon cryptosystem without giving the particular instantiation of [RLT21]. Of course, we need to define Sidon spaces.

5.1.1 Sidon Spaces

Sidon spaces were introduced in [BSZ15] while proving a theorem from pure mathematics. Explicit constructions tailored to network coding were later given in [RRT17].

For q a prime power and integers n and k, let $\mathcal{G}_q(n,k)$ be the set of all $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$ of dimension k. Sidon spaces of dimension k correspond to the elements of $\mathcal{G}_q(n,k)$ which satisfy the following condition.

Definition 5.1. A subspace $\mathcal{V} \in \mathcal{G}_q(n,k)$ is called a Sidon space if for all non-zero $a,b,c,d \in \mathcal{V}$, if $ab = cd$, then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$.

Definition 5.1 is equivalent to the fact that any product of two non-zero elements in $\mathcal{V}$ has unique factorization up to a constant factor in $\mathbb{F}_q$. In other words, Sidon spaces are the multiplicative counterpart of *Sidon sets* $\{a_1, a_2, \dots\} \subset \mathbb{N}$ from additive number theory, for which all sums $a_i + a_j,\ i \leqslant j$, are distinct. Even before discussing constructions, a rather natural question is whether there exist Sidon spaces of arbitrary dimension. A first upper bound on k is given by [BSZ15, Theorem 18] and [RRT17, Proposition 3], where it is proven that for a Sidon space $\mathcal{V} \in \mathcal{G}_q(n,k)$, the space $\mathcal{V}^2 \stackrel{def}{=} \mathrm{span}_{\mathbb{F}_q}\{uv : u,v \in \mathcal{V}\}$ is of dimension $\dim_{\mathbb{F}_q}(\mathcal{V}^2) \geqslant 2k$. Since $\mathcal{V}^2 \subset \mathbb{F}_{q^n}$, this implies that $k \leqslant n/2$. In particular, Sidon spaces for which this bound is an equality are referred to as *min-span*.

A crucial property for the applications of [RRT17] was the existence of an efficient *factoring algorithm*. Given a Sidon space $\mathcal{V}$ and a product $\pi = ab$ between non-zero elements $a,\ b \in \mathcal{V}$, this refers to any efficient method which recovers a pair $(\lambda a, \lambda^{-1} b),\ \lambda \in \mathbb{F}_q^*$.

5.1.2 Description of the Scheme

The proposal of [RLT21] calls for Sidon spaces which meet the same constraint. Indeed, it is a trapdoor-based scheme whose public key is an arbitrary description of such a space $\mathcal{V}$ while the private key is a factoring algorithm. More precisely, let us now present the standard PKE algorithms.

Keygen(1^λ):

- Pick $\mathcal{V} \in \mathcal{G}_q(n,k)$ a random Sidon space with an efficient factoring algorithm $\mathcal{A}$. Pick $\boldsymbol{\nu} \stackrel{def}{=} (\nu_1, \dots, \nu_k)$ a random basis of $\mathcal{V}$ and $\boldsymbol{\beta} \stackrel{def}{=} (\beta_1, \dots, \beta_n)$ a random basis of the extension field $\mathbb{F}_{q^n}$.

- Represent the matrix $\boldsymbol{M}(\boldsymbol{\nu}) \stackrel{def}{=} \boldsymbol{\nu}^{\mathsf{T}}\boldsymbol{\nu} \in \mathbb{F}_{q^n}^{k\times k}$ over the basis $\boldsymbol{\beta}$ by

$$\boldsymbol{M}(\boldsymbol{\nu}) = \boldsymbol{\nu}^{\mathsf{T}}\boldsymbol{\nu} \stackrel{def}{=} \sum_{i=1}^{n} \beta_i \boldsymbol{M}^{(i)}, \tag{5.1}$$

  where $\boldsymbol{M}^{(i)} \in \mathbb{F}_q^{k\times k}$ for $1 \leqslant i \leqslant n$.

- Output $\mathsf{sk} \stackrel{def}{=} (\boldsymbol{\beta}, \mathcal{A}, \boldsymbol{\nu})$ as secret key and $\mathsf{pk} \stackrel{def}{=} (\boldsymbol{M}^{(1)}, \ldots, \boldsymbol{M}^{(n)})$ as public key.

The message space corresponds to the equivalence class of pairs of elements $\{a, b\}$ in the Sidon space $\mathcal{V}$, two pairs $\{a, b\}$ and $\{c, d\}$ being equivalent if their product $ab = cd$ is the same. If one views an element a of $\mathcal{V}$ as a vector $\boldsymbol{a} \in \mathbb{F}_q^k$, *i.e.*, $a = \sum_{i=1}^{k} a_i\nu_i$, then the equivalence class associated to $\{\boldsymbol{a}, \boldsymbol{b}\}$ corresponds to all pairs $\{\boldsymbol{c}, \boldsymbol{d}\}$ such that either $\boldsymbol{a}^{\mathsf{T}}\boldsymbol{b} = \boldsymbol{c}^{\mathsf{T}}\boldsymbol{d}$ or $\boldsymbol{a}^{\mathsf{T}}\boldsymbol{b} = \boldsymbol{d}^{\mathsf{T}}\boldsymbol{c}$. The reason why the message space is defined in this way will become a bit more apparent from the decryption procedure described below.

Encrypt($\mathsf{pk} = (\boldsymbol{M}^{(i)})_{i=1}^{n}$, $\{\boldsymbol{a}, \boldsymbol{b}\}$):

- The ciphertext associated to (the equivalence class of) $\{\boldsymbol{a}, \boldsymbol{b}\}$ is

$$\boldsymbol{c} = (c_i)_{i=1}^{n} \stackrel{def}{=} (\boldsymbol{a}\boldsymbol{M}^{(i)}\boldsymbol{b}^{\mathsf{T}})_{i=1}^{n} \in \mathbb{F}_q^n.$$

Note that this definition is compatible with the way the plaintext is defined: the ciphertext does not depend on the particular pair $\{\boldsymbol{a}, \boldsymbol{b}\}$ chosen in the equivalence class of the message. An interesting property of the Sidon cryptosystem is that it is homomorphic under the addition on half of the plaintext. That is, for two given plaintexts $\{\boldsymbol{a}_1, \boldsymbol{b}\}$ and $\{\boldsymbol{a}_2, \boldsymbol{b}\}$, we have

$$\mathbf{Enc}(\mathsf{pk}, \{\boldsymbol{a}_1, \boldsymbol{b}\}) + \mathbf{Enc}(\mathsf{pk}, \{\boldsymbol{a}_2, \boldsymbol{b}\}) = \mathbf{Enc}(\mathsf{pk}, \{\boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{b}\}).$$

To decrypt, Bob starts by interpreting the ciphertext $\boldsymbol{c}$ as a product of two elements in $\mathcal{V}$ from the knowledge of $\boldsymbol{\beta}$. He can then recover its factors by applying Algorithm $\mathcal{A}$.

Decrypt($\mathsf{sk} = (\boldsymbol{\beta}, \mathcal{A}, \boldsymbol{\nu})$, $\boldsymbol{c}$):

- Compute

$$\begin{aligned}\sum_{i=1}^{n} \beta_i c_i &= \sum_{i=1}^{n} \beta_i \left(\boldsymbol{a}\boldsymbol{M}^{(i)}\boldsymbol{b}^{\mathsf{T}}\right) = \boldsymbol{a}\boldsymbol{M}(\boldsymbol{\nu})\boldsymbol{b}^{\mathsf{T}} \\ &= \boldsymbol{a}\boldsymbol{\nu}^{\mathsf{T}}\boldsymbol{\nu}\boldsymbol{b}^{\mathsf{T}} = \left(\sum_{i=1}^{k} a_i\nu_i\right)\left(\sum_{i=1}^{k} b_i\nu_i\right) = ab \in \mathcal{V}.\end{aligned}$$

- Use Algorithm $\mathcal{A}$ on ab to recover $\{a, b\}$ up to a multiplicative factor in $\mathbb{F}_q$.

- Finally, retrieve $\{\boldsymbol{a}, \boldsymbol{b}\}$ (up to a multiplicative factor) by representing $\{a, b\}$ over the basis $\boldsymbol{\nu}$. Such an $\{\boldsymbol{a}, \boldsymbol{b}\}$ defines the message in a unique way.

5.1.3 MinRank Problem

Our mere description of **Keygen** already gives a rather obvious MinRank instance.

Problem 5.1. *Let $\boldsymbol{M}_1, \dots, \boldsymbol{M}_n \in \mathbb{F}_q^{k\times k}$ denote the public key of the Sidon cryptosystem. Then, the vector $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ from the secret key is a solution over $\mathbb{F}_{q^n}$ to the homogeneous MinRank problem with target rank 1 defined by the $\boldsymbol{M}_i$'s for $1 \leqslant i \leqslant n$.*

This readily brings us to the following questions.

(1) Is Problem 5.1 difficult ?

(2) Can we recover an equivalent key from any solution to it ?

In HFE, MinRank was the bootleneck. On the contrary, retrieving a secret key from an arbitrary solution could be performed in polynomial time. The situation here will be quite different. For the first point, this already stems from the fact that we look for rank 1 matrices, which is unusual. For the second point, the variety of Problem 5.1 may actually depend a lot on the choice of a Sidon space. It turns out that the one adopted in [RLT21] yields a very large solution set.

5.2 Weakness of the Scheme

In this section, we present their construction and we study Problem 5.1 in this particular case. Our attack based on this analysis will be described in Sections 5.3 and 5.4.

5.2.1 Choice of the Sidon Space

The scheme considers a min-span Sidon space, *i.e.*, $n = 2k$, which is defined in terms the subfield $\mathbb{F}_{q^k} \subset \mathbb{F}_{q^n}$. It is chosen according to the following Construction 1. There, we denote by $W_{q-1} \stackrel{def}{=} \{u^{q-1} : u \in \mathbb{F}_{q^k}\}$ and $\overline{W_{q-1}} \stackrel{def}{=} \mathbb{F}_{q^k} \backslash W_{q-1}$.

Construction 1 (Construction 15, [RRT17]). *For $q \geqslant 3$ a prime power and $k \in \mathbb{N}^*$, let $n = 2k$ and let $\gamma \in \mathbb{F}_{q^n}^*$ be a root of an irreducible polynomial $x^2 + bx + c$ over $\mathbb{F}_{q^k}$ such that $c \in \overline{W_{q-1}}$ [1]. Then, the subspace $\mathcal{V} = \{u + u^q\gamma : u \in \mathbb{F}_{q^k}\} \subset \mathbb{F}_{q^n}$ is a Sidon space of dimension k.*

What justifies its use in [RLT21] is an efficient factoring procedure. The following Algorithm 2 relies on the knowledge of an element γ such that $(1, \gamma)$ is a basis of $\mathbb{F}_{q^n}$

[1] Such a polynomial is known to exist by [RRT17, Corollary 14].

over $\mathbb{F}_{q^k}$. For $x \in \mathbb{F}_{q^n}$, the notation $[1](x)$ and $[\gamma](x)$ stand for the components of x in this basis.

Algorithm 2: Factoring algorithm for $\mathcal{V}$ as in Construction 1.

Input: A product $\pi = \pi_1\pi_2$, where $\pi_1 = u + u^q\gamma$ and $\pi_2 = v + v^q\gamma \in \mathcal{V}$, the element $\gamma \in \mathbb{F}_{q^n}^*$ such that $\gamma^2 + b\gamma + c = 0$ from Construction 1.

Output: $\{\pi_1\mathbb{F}_q, \pi_2\mathbb{F}_q\}$.

Decompose π in the basis $(1, \gamma)$:

$q_0 \leftarrow [1](\pi)$; /* $q_0 = uv - c(uv)^q$ */

$q_1 \leftarrow [\gamma](\pi)$; /* $q_1 = uv^q + u^qv - b(uv)^q$ */

$A \leftarrow T^{-1}(q_0)$; /* where $T : x \mapsto x - cx^q$, $A = uv$ */

$B \leftarrow q_1 + bA^q$; /* $B = uv^q + u^qv$ */

Compute the roots α, β of $A + Bx + A^qx^2$, namely $(\alpha, \beta) = (-1/u^{q-1}, -1/v^{q-1})$

From α and β, recover $\{u\mathbb{F}_q, v\mathbb{F}_q\}$ uniquely and therefore $\{\pi_1\mathbb{F}_q, \pi_2\mathbb{F}_q\}$.

Finally, since such a primitive element is actually sufficient to devise the algorithm, one can assume a secret key of the form $(\boldsymbol{\beta}, \gamma, \boldsymbol{\nu})$ instead of $(\boldsymbol{\beta}, \mathcal{A}, \boldsymbol{\nu})$.

From now on, let $\mathcal{V}$ be a min-span Sidon space with random basis $\boldsymbol{\nu}$ as in Construction 1 as well as the matrices $\boldsymbol{M}^{(i)} \in \mathbb{F}_q^{k\times k}$ associated to a random basis $\boldsymbol{\beta}$. In the following, we study Problem 5.1 with this specific instantiation. For that purpose, we consider the matrix code of parameters $[k^2, n]_{q^n}$ endowed with the rank metric defined by

$$\mathcal{C}_{\text{mat}} \stackrel{def}{=} \left\langle \boldsymbol{M}^{(1)}, \ldots, \boldsymbol{M}^{(n)} \right\rangle_{\mathbb{F}_{q^n}}. \tag{5.2}$$

5.2.2 General Comments

The solutions to Problem 5.1 correspond to all codewords of weight 1 in $\mathcal{C}_{\text{mat}}$. Moreover, as the generators $\boldsymbol{M}^{(i)}$ are symmetric, all the elements in this code are symmetric. Thus, rank 1 matrices in $\mathcal{C}_{\text{mat}}$ will be of the form $\boldsymbol{x}^\mathsf{T}\boldsymbol{y} \in \mathbb{F}_{q^n}^{k\times k}$ for $\boldsymbol{x}$ collinear with $\boldsymbol{y}$.

In this section, we will outline general properties of these codewords which are not specific to Construction 1 and which even do not depend on the notion of Sidon space.

Linearity over $\mathbb{F}_{q^n}$. Since we are primarily interested in $\boldsymbol{\nu}^\mathsf{T}\boldsymbol{\nu} \in \mathcal{C}_{\text{mat}}$, we may want to focus on

$$\mathcal{Z}_{\mathbb{F}_{q^n}} \stackrel{def}{=} \left\{ \boldsymbol{x} \in \mathbb{F}_{q^n}^k : \boldsymbol{x}^\mathsf{T}\boldsymbol{x} \in \mathcal{C}_{\text{mat}} \right\}. \tag{5.3}$$

This set is clearly non-trivial as it contains $\boldsymbol{\nu}$. Also, there is still one degree of freedom coming from the $\mathbb{F}_{q^n}$-linearity of $\mathcal{C}_{\text{mat}}$. For instance, since $\nu_1 \neq 0$ in $\boldsymbol{\nu}$, the set

$$\mathcal{Z}_{\mathbb{F}_{q^n},s} \stackrel{def}{=} \left\{ \boldsymbol{x} \in \mathcal{Z}_{\mathbb{F}_{q^n}} : x_1 = s \right\}$$

is also non-trivial for $s \in \mathbb{F}_{q^n}^*$.

Stability under Frobenius. As already observed on Problem 4.1 in Chapter 4 (see Fact 1), applying the Frobenius morphism on a given solution provides another solution to the same instance. More interesting to us is that the subset $\mathcal{Z}_{\mathbb{F}_{q^n}}$ is also stable under this operation.

Notation 1. *For a matrix $\boldsymbol{M}$ over $\mathbb{F}_{q^n}$ and $p \in \mathbb{N}$, we use the same notation as for vectors by considering $\boldsymbol{M}^{[p]}$ the matrix obtained by applying the Frobenius map $x \mapsto x^q$ p times on each entry.*

Lemma 5.1. *Let $\mathcal{C}_{mat}$ be the code defined in Equation (5.2) and let $\mathcal{Z}_{\mathbb{F}_{q^n}}$ the set defined in Equation (5.3). If $\boldsymbol{\omega} \in \mathcal{Z}_{\mathbb{F}_{q^n}}$, then $\boldsymbol{\omega}^{[p]} \in \mathcal{Z}_{\mathbb{F}_{q^n}}$ for any $p \in \mathbb{N}$. More generally, if $\boldsymbol{M} \in \mathcal{C}_{mat}$, then $\boldsymbol{M}^{[p]} \in \mathcal{C}_{mat}$ for any $p \in \mathbb{N}$.*

Proof. Let $\boldsymbol{\omega} \in \mathbb{F}_{q^n}^k$ such that $\boldsymbol{\omega} \in \mathcal{Z}_{\mathbb{F}_{q^n}}$. By definition, there exists $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_n) \in \mathbb{F}_{q^n}^n$ such that

$$\boldsymbol{M}(\boldsymbol{\omega}) = \sum_{\ell=1}^{n} \eta_\ell \boldsymbol{M}^{(\ell)}.$$

Writing this for the entry in row i and column j for $1 \leqslant i, j \leqslant k$ gives

$$\omega_i \omega_j = \sum_{\ell=1}^{n} \eta_\ell \boldsymbol{M}_{i,j}^{(\ell)}.$$

Then, by iterating the Frobenius map p times on this equation for $p \in \mathbb{N}$ and by noting that $\boldsymbol{M}^{(\ell)} \in \mathbb{F}_q^{k \times k}$, one obtains

$$\omega_i^{[p]} \omega_j^{[p]} = \sum_{\ell=1}^{n} \eta_\ell^{[p]} \boldsymbol{M}_{i,j}^{(\ell)}.$$

This implies that the matrix

$$\boldsymbol{M}(\boldsymbol{\omega}^{[p]}) = \sum_{\ell=1}^{n} \eta_\ell^{[p]} \boldsymbol{M}^{(\ell)}$$

belongs to $\mathcal{C}_{\mathrm{mat}}$ for any $p \in \mathbb{N}$. The proof of the second statement is similar. □

So far, we have not used the fact that $\mathcal{V}$ is a Sidon space. More generally, all these results apply to a random subspace $\mathcal{W} \subset \mathbb{F}_{q^n}$ of dimension k generated by $\boldsymbol{\omega}$. In this case, the $\boldsymbol{M}^{(i)}$'s are still obtained from the decomposition of $\boldsymbol{M}(\boldsymbol{\omega})$ in an arbitrary basis of $\mathbb{F}_{q^n}$. Also, we keep the same definition for $\mathcal{C}_{\mathrm{mat}}$, $\mathcal{Z}_{\mathbb{F}_{q^n}}$ and $\mathcal{Z}_{\mathbb{F}_{q^n},s}$. For such a space, the only solutions to Problem 5.1 that we observe in practice are given by Lemma 5.1.

Experimental observation 1. *Let $\mathcal{W}$ be a random element in $\mathcal{G}_q(n,k)$ together with a basis $\boldsymbol{\omega}$ and let $s \in \mathbb{F}_{q^n}^*$. One has*

$$\#\mathcal{Z}_{\mathbb{F}_{q^n},s} = n.$$

Moreover, if $s \in \mathbb{F}_q^*$, then there exists $\boldsymbol{u} \in \mathbb{F}_{q^n}^k$ with $u_1 = s$ such that

$$\mathcal{Z}_{\mathbb{F}_{q^n},s} = \left\{ \boldsymbol{u}, \boldsymbol{u}^{[1]}, \ldots, \boldsymbol{u}^{[n-1]} \right\}.$$

5.2.3 Rank-One Matrices in a Subfield Subcode

The authors of the scheme had already noticed that the solution set to Problem 5.1 was unexpectedly large. However, they did not examine it in further details.

In the case of Construction 1, we show that the variety cannot be boiled down to the features exhibited in Section 5.2.2. This is because there exist specific solutions over the subfield $\mathbb{F}_{q^k}$, *i.e.*, weight 1 codewords in the $\mathbb{F}_{q^k}$-linear code

$$\mathcal{D}_{\text{mat}} \stackrel{def}{=} \mathcal{C}_{\text{mat}} \cap \mathbb{F}_{q^k}^{k\times k}.$$

Remark 5.1. One can view $\mathcal{D}_{\text{mat}}$ as a subfield subcode.

Let us start with the content of our experiments.

Experimental observation 2. *Let $\mathcal{V} \in \mathcal{G}_q(n,k)$ a random Sidon space as in Construction 1. For $s \in \mathbb{F}_{q^k}^*$, we observed that*

$$\#\mathcal{Z}_{\mathbb{F}_{q^k},s} = k(q^k - 1).$$

Moreover, if $t \in \mathbb{F}_{q^k}^*$, $t \notin \langle s\rangle_{\mathbb{F}_q}$, we observed that

$$\#\left\{\boldsymbol{x} \in \mathcal{Z}_{\mathbb{F}_{q^k},s} : x_2 = t\right\} = k.$$

To go beyond this observation, we will try to grasp some elements in $\mathcal{Z}_{\mathbb{F}_{q^k}}$. For $1 \leqslant i \leqslant k$, let $u_i \in \mathbb{F}_{q^k}$ such that

$$\nu_i = u_i + u_i^q\gamma. \tag{5.4}$$

Note that $\boldsymbol{u} \stackrel{def}{=} (u_1, \ldots, u_k)$ is necessarily a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Finally, let $\boldsymbol{M}(\boldsymbol{u}) \stackrel{def}{=} \boldsymbol{u}^\mathsf{T}\boldsymbol{u} \in \mathbb{F}_{q^k}^{k\times k}$.

Proposition 5.1. *Let $\mathcal{V} \in \mathcal{G}_q(n,k)$ a random Sidon space as in Construction 1 with basis $\boldsymbol{\nu}$ and let $\boldsymbol{u}$ the basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ associated to $\boldsymbol{\nu}$ by Equation (5.4). Let $\mathcal{C}_{mat}$ the $\mathbb{F}_{q^n}$-linear code generated by the matrices in pk and let $\mathcal{D}_{mat} = \mathcal{C}_{mat} \cap \mathbb{F}_{q^k}^{k\times k}$. Then, the matrix $\boldsymbol{M}(\boldsymbol{u})$ belongs to $\mathcal{D}_{mat}$. More generally, the same is true for $\boldsymbol{M}(\boldsymbol{u}^{[j]})$ for any integer $j \in \mathbb{N}$.*

Proof. We only do the proof for $\boldsymbol{M}(\boldsymbol{u}) = \boldsymbol{M}(\boldsymbol{u}^{[0]})$ since the rest easily follows from Lemma 5.1. By expressing the entries of $\boldsymbol{M}(\boldsymbol{\nu}) \in \mathbb{F}_{q^n}^{k\times k}$ in the basis $(1,\gamma)$, there exists a unique pair of matrices $(\boldsymbol{A},\boldsymbol{B}) \in \mathbb{F}_{q^k}^{k\times k} \times \mathbb{F}_{q^k}^{k\times k}$ such that $\boldsymbol{M}(\boldsymbol{\nu}) = \boldsymbol{A} + \gamma\boldsymbol{B}$. As we also have $\boldsymbol{M}(\boldsymbol{\nu}) = \sum_{i=1}^n \beta_i \boldsymbol{M}^{(i)}$ where $\boldsymbol{M}^{(i)} \in \mathbb{F}_q^{k\times k}$, it is in fact explicitly given by

$$\begin{cases} \boldsymbol{A} = \displaystyle\sum_{i=1}^n \delta_i \boldsymbol{M}^{(i)} \\ \boldsymbol{B} = \displaystyle\sum_{i=1}^n \eta_i \boldsymbol{M}^{(i)}, \end{cases} \tag{5.5}$$

where $\beta_i \overset{def}{=} \delta_i + \gamma\eta_i,\ \delta_i,\ \eta_i \in \mathbb{F}_{q^k}$ is the decomposition of β_i in $(1,\gamma)$ for $1 \leqslant i \leqslant n$. This definition shows that both $\boldsymbol{A}$ and $\boldsymbol{B}$ belong to $\mathcal{D}_{\text{mat}}$. Also, recall from Construction 1 that the primitive element γ is a root of the polynomial $x^2 + bx + c$ over $\mathbb{F}_{q^k}$. For $1 \leqslant i, j \leqslant k$, one thus obtains

$$\begin{aligned}\nu_i\nu_j &= (u_i + u_i^q\gamma)(u_j + u_j^q\gamma)\\ &= (u_iu_j - c(u_iu_j)^q) + \gamma(u_iu_j^q + u_i^qu_j - b(u_iu_j)^q). \end{aligned} \tag{5.6}$$

By (5.6), another expression for $\boldsymbol{A}$ is then $\boldsymbol{A} = \boldsymbol{M}(\boldsymbol{u}) - c\boldsymbol{M}(\boldsymbol{u}^{[1]})$. By (5.5), this matrix also belongs to $\mathcal{D}_{\text{mat}}$. More generally, using Lemma 5.1, the same is true for the matrices

$$\begin{aligned}\boldsymbol{A}^{[1]} &= \boldsymbol{M}(\boldsymbol{u}^{[1]}) - c^q\boldsymbol{M}(\boldsymbol{u}^{[2]})\\ \boldsymbol{A}^{[2]} &= \boldsymbol{M}(\boldsymbol{u}^{[2]}) - c^{q^2}\boldsymbol{M}(\boldsymbol{u}^{[3]})\\ &\vdots\\ \boldsymbol{A}^{[k-1]} &= \boldsymbol{M}(\boldsymbol{u}^{[k-1]}) - c^{q^{k-1}}\boldsymbol{M}(\boldsymbol{u}^{[k]}) = \boldsymbol{M}(\boldsymbol{u}^{[k-1]}) - c^{q^{k-1}}\boldsymbol{M}(\boldsymbol{u}).\end{aligned}$$

Then, by performing linear combinations over $\mathbb{F}_{q^k}$, one gets

$$\boldsymbol{A} + \sum_{i=1}^{k-1} c^{1+q+\cdots+q^{i-1}}\boldsymbol{A}^{[i]} = (1 - c^{1+q+\cdots+q^{k-1}})\boldsymbol{M}(\boldsymbol{u}) = (1 - c^{\frac{q^k-1}{q-1}})\boldsymbol{M}(\boldsymbol{u}).$$

Note finally that $c^{\frac{q^k-1}{q-1}} \neq 1$ since $c \in \overline{\mathcal{W}}_{q-1}$ in the construction. The matrix $\boldsymbol{M}(\boldsymbol{u})$ is thus a linear combination between the $\boldsymbol{A}^{[i]}$'s over $\mathbb{F}_{q^k}$, which proves $\boldsymbol{M}(\boldsymbol{u}) \in \mathcal{D}_{\text{mat}}$. □

In fact, it is easy to find other rank 1 matrices in $\mathcal{D}_{\text{mat}}$. First, Equation (5.6) shows that the matrix $\boldsymbol{B} \in \mathbb{F}_q^{k\times k}$ defined in Equation (5.5) satisfies $\boldsymbol{B}_{i,j} = u_iu_j^q + u_i^qu_j - b(u_iu_j)^q$ for $1 \leqslant i, j \leqslant k$, hence

$$\begin{aligned}\boldsymbol{B} &= \boldsymbol{u}^\mathsf{T}\boldsymbol{u}^{[1]} + \left(\boldsymbol{u}^{[1]}\right)^\mathsf{T}\boldsymbol{u} - b\left(\boldsymbol{u}^{[1]}\right)^\mathsf{T}\boldsymbol{u}^{[1]}\\ &= \boldsymbol{u}^\mathsf{T}\boldsymbol{u}^{[1]} + \left(\boldsymbol{u}^{[1]}\right)^\mathsf{T}\boldsymbol{u} - b\boldsymbol{M}(\boldsymbol{u}^{[1]}).\end{aligned} \tag{5.7}$$

Second, this matrix also belongs to $\mathcal{D}_{mat}$ by (5.5). Now, let $\lambda \in \mathbb{F}_{q^k}$ and consider

$$\begin{aligned}\boldsymbol{M}(\boldsymbol{u} + \lambda\boldsymbol{u}^{[1]}) &= \left(\boldsymbol{u} + \lambda\boldsymbol{u}^{[1]}\right)^\mathsf{T}\left(\boldsymbol{u} + \lambda\boldsymbol{u}^{[1]}\right)\\ &= \boldsymbol{u}^\mathsf{T}\boldsymbol{u} + \lambda^2\left(\boldsymbol{u}^{[1]}\right)^\mathsf{T}\boldsymbol{u}^{[1]} + \lambda\left\{\boldsymbol{u}^\mathsf{T}\boldsymbol{u}^{[1]} + \left(\boldsymbol{u}^{[1]}\right)^\mathsf{T}\boldsymbol{u}\right\}\\ &= \boldsymbol{M}(\boldsymbol{u}) + \lambda^2\boldsymbol{M}(\boldsymbol{u}^{[1]}) + \lambda\boldsymbol{B} + \lambda b\boldsymbol{M}(\boldsymbol{u}^{[1]}) \quad \text{(by (5.7))}.\end{aligned}$$

The last equality implies that the matrix $\boldsymbol{M}(\boldsymbol{u} + \lambda\boldsymbol{u}^{[1]})$ belongs to $\mathcal{D}_{\text{mat}}$. Since it is of rank 1, we have just proven the following generalization of Proposition 5.1.

Proposition 5.2. *Let* $\mathcal{Z}_{\mathbb{F}_{q^k}} = \left\{ \boldsymbol{x} \in \mathbb{F}_{q^k}^k : \boldsymbol{x}^\mathsf{T}\boldsymbol{x} \in \mathcal{D}_{mat} \right\}$ *and let* $\boldsymbol{u}$ *the basis of* $\mathbb{F}_{q^k}$ *over* $\mathbb{F}_q$ *associated to* $\boldsymbol{\nu}$ *by Equation (5.4). One has*

$$\left\{ \lambda \boldsymbol{u}^{[j]} + \mu \boldsymbol{u}^{[j+1]} : (\lambda, \mu) \in \mathbb{F}_{q^k}^2 \text{ and } 0 \leqslant j \leqslant k-1 \right\} \subset \mathcal{Z}_{\mathbb{F}_{q^k}}.$$

Assumption 4. *We assume that the inclusion from Proposition 5.2 is an equality.*

Assumption 4 implies that we have been able to characterize all the elements in $\mathcal{Z}_{\mathbb{F}_{q^k}}$. It is in particular supported by our Experimental observation 2. Based on this assumption, we will now describe our (equivalent) key-recovery attack which consists in 1. finding enough vectors in $\mathcal{Z}_{\mathbb{F}_{q^k}}$ (Section 5.3) 2. derive an equivalent key from these elements (Section 5.4).

5.3 MinRank over $\mathbb{F}_{q^k}$

In this section, our goal is to determine vectors in the set

$$\mathcal{Z}_{\mathbb{F}_{q^k}} = \left\{ \boldsymbol{x} \in \mathbb{F}_{q^k}^k : \boldsymbol{x}^\mathsf{T}\boldsymbol{x} \in \mathcal{D}_{\text{mat}} \right\}.$$

Rather than relying on the generic techniques recalled in [RLT21, §4], we found that it was more favorable to consider a dedicated algebraic modeling largely inspired by [DT18, §5.4]. This system is presented in Section 5.3.1. In Section 5.3.2, we show that it can be solved efficiently.

5.3.1 Parity-Check Modeling

The approach of [DT18, §5.4] simply exploits a parity-check matrix of $\mathcal{D}_{\text{mat}}$ when viewed as a linear code of length k^2. More explicitly, we use the linear isomorphism

$$\begin{aligned} \text{vec} : \ \mathbb{F}_{q^k}^{k \times k} &\to \mathbb{F}_{q^k}^{k^2} \\ \boldsymbol{M} &\mapsto \boldsymbol{m} \end{aligned}$$

such that $\boldsymbol{m}_{(i-1)k+j} = \boldsymbol{M}_{i,j}$ for $1 \leqslant i, j \leqslant k$ and we define

$$\text{vec}(\mathcal{D}_{\text{mat}}) \stackrel{def}{=} \{\text{vec}(\boldsymbol{M}) : \boldsymbol{M} \in \mathcal{D}_{\text{mat}}\}.$$

Let also

$$\boldsymbol{X} \stackrel{def}{=} \boldsymbol{x}^\mathsf{T}\boldsymbol{x} = \begin{bmatrix} x_1^2 & x_1x_2 & \cdots & x_1x_k \\ x_2x_1 & x_2^2 & \cdots & x_2x_k \\ \vdots & \vdots & \ddots & \vdots \\ x_kx_1 & x_kx_2 & \cdots & x_k^2 \end{bmatrix} \tag{5.8}$$

the matrix in the unknowns x_i used to model solutions $\boldsymbol{x} \in \mathcal{Z}_{\mathbb{F}_{q^k}}$. For an arbitrary parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^k}^{(k^2-2k)\times k^2}$, we consider the system containing $k^2 - 2k$ quadratic equations given by

$$\boldsymbol{H}\text{vec}(\boldsymbol{X})^\mathsf{T} = 0. \tag{5.9}$$

Lemma 5.2. *The sequence of Equation (5.9) contains at most* $k^2 - 2k - \binom{k}{2}$ *linearly independent quadratic polynomials over* $\mathbb{F}_{q^k}$.

Proof. Let $(\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_{k^2})$ be the canonical basis of $\mathbb{F}_{q^k}^{k^2}$. Due to the symmetry of the $\boldsymbol{M}^{(i)}$'s, the vector

$$\boldsymbol{\sigma}_{i,j} \stackrel{def}{=} \boldsymbol{\varepsilon}_{(i-1)k+j} - \boldsymbol{\varepsilon}_{(j-1)k+i}$$

belongs to the dual code $\mathrm{vec}(\mathcal{D}_{\mathrm{mat}})^{\perp}$ for any $1 \leqslant i < j \leqslant k$. This means that there exists a parity-check matrix of the form

$$\boldsymbol{H}' \stackrel{def}{=} \begin{bmatrix} \boldsymbol{U} \\ \boldsymbol{H}_{\sigma} \end{bmatrix}, \tag{5.10}$$

where the rows of $\boldsymbol{H}_{\boldsymbol{\sigma}} \in \mathbb{F}_{q^k}^{\binom{k}{2} \times k^2}$ are the $\boldsymbol{\sigma}_{i,j}$'s and where $\boldsymbol{U} \in \mathbb{F}_{q^k}^{(k^2-2k-\binom{k}{2}) \times k^2}$. Finally, since the equations coming from $\boldsymbol{H}_{\boldsymbol{\sigma}} \mathrm{vec}(\boldsymbol{X})^{\mathsf{T}} = 0$ all give the zero polynomial, the useful part of the system reduces to

$$\boldsymbol{U} \mathrm{vec}(\boldsymbol{X})^{\mathsf{T}} = 0.$$

This set of equations is of cardinality $k^2 - 2k - \binom{k}{2}$ equations. □

Modeling 10 (Parity-check modeling over $\mathbb{F}_{q^k}$). *Let* $\boldsymbol{X}$ *be the matrix of unknowns defined in Equation (5.8) and let* $\boldsymbol{H}' = \begin{bmatrix} \boldsymbol{U} \\ \boldsymbol{H}_{\boldsymbol{\sigma}} \end{bmatrix} \in \mathbb{F}_{q^k}^{(k^2-2k) \times k^2}$ *be a parity-check matrix for the code* $vec(\mathcal{D}_{mat})$ *as defined in Equation (5.10), where* $\mathcal{D}_{mat} = \mathcal{C}_{mat} \cap \mathbb{F}_{q^k}^{k \times k}$. *We consider the system* $\mathcal{F}$ *over* $\mathbb{F}_{q^k}$ *whose polynomials are the entries of the column vector* $\boldsymbol{U}\, vec(\boldsymbol{X})^{\mathsf{T}}$.

It is readily verified that the solutions to Modeling 10 are in one-to-one correspondence with the elements of $\mathcal{Z}_{\mathbb{F}_{q^k}}$. Experimentally, these solutions were also all of the form described in Proposition 5.2.

Fixing 2 variables. If one wants to find an element in $\mathcal{Z}_{\mathbb{F}_{q^k}}$ in practice, two unknowns can be fixed in Modeling 10 to reduce the number of solutions (the dimension of the ideal $\langle \mathcal{F} \rangle$ is at least 2). The corresponding variety over $\mathbb{F}_{q^k}$ has size $\geqslant k$ still by using Proposition 5.2, and Assumption 4 states that it is an equality (the system is a fortiori zero-dimensional). Since fixing more variables would result in a system with no solutions with high probability, we focus on this specialized version.

Modeling 11 (Recovering an element in $\mathcal{Z}_{\mathbb{F}_{q^k}}$). *Let* $(s,t) \in \mathbb{F}_{q^k}^2$ *such that* $t \notin \langle s \rangle_{\mathbb{F}_q}$. *We consider the sequence* $\mathcal{F}_{spec}$ *which is obtained by fixing* $x_{k-1} = s$ *and* $x_k = t$ *in Modeling 10.*

5.3.2 Solving the Specialized System

On $\mathcal{F}_{\text{spec}}$, we adopt the standard approach for zero-dimensional systems that was recalled in Section 2.2.3. First, note that the cost of FGLM can be considered polynomial in the parameters since we expect k distinct solutions by Proposition 5.2 and Assumption 4. Thus, we focus on the initial Gröbner basis step for which we will also prove a polynomial complexity. More precisely, we will show that – under the following Assumption 5 and Assumption 6 – the system $\mathcal{F}_{\text{spec}}$ can always be solved in degree 3 regardless of the value of k.

Coming back to Modeling 10, a first remark is that we can permute the coordinates of the row-vector $\text{vec}(\boldsymbol{X})$ and the columns of $\boldsymbol{U}$ accordingly so that the $\binom{k+1}{2}$ leftmost entries of $\text{vec}(\boldsymbol{X})$ correspond to all distinct monomials $x_i x_j$ for $1 \leqslant i \leqslant j \leqslant k$. This is equivalent to choosing a grevlex ordering on the variables to label the columns of $\boldsymbol{U}$. Furthermore, by adding rows of $\boldsymbol{H}_{\boldsymbol{\sigma}}$ to rows of $\boldsymbol{U}$ in $\boldsymbol{H}$, we can assume that the last $\binom{k}{2}$ columns of the matrix $\boldsymbol{U}$ are identically zero. Finally, we will rely on

Assumption 5. *We assume that the submatrix* $\boldsymbol{V} \overset{def}{=} \boldsymbol{U}_{*,\{1..\binom{k-1}{2}\}} \in \mathbb{F}_{q^k}^{\left(\binom{k-1}{2}-1\right)\times\binom{k-1}{2}}$ *is full-rank.*

On that hypothesis, we can construct $\binom{k-1}{2} - 1$ equations in the span of Modeling 10 with distinct leading monomials of the form $x_i x_j$, $1 \leqslant i \leqslant j \leqslant k-2$. Moreover, as we fix x_{k-1} and x_k to obtain $\mathcal{F}_{\text{spec}}$, these monomials remain the same in Modeling 11. Let us denote by $\mathcal{G}_{\text{spec}}$ the corresponding set of quadratic polynomials whose leading terms are all different. Since the total number of degree 2 monomials in $x_1, \ldots, x_{k-2}$ is equal to $\binom{k-1}{2}$, this means that all of them appear except one.

The rest of the discussion will prove that the Gröbner basis is either already computed or close to be computed if the set $\mathcal{G}_{\text{spec}}$ is known. We make the further assumption that

Assumption 6. *The algebraic system* $\mathcal{F}_{spec}$ *has exactly* k *distinct solutions which do not belong to a common hyperplane of* $\mathbb{F}_{q^k}^{k-2}$.

This hypothesis was investigated through experiments and it is natural when considering Proposition 5.2 together with Observation 2 (which suggests that the inclusion of Proposition 5.2 is an equality). Indeed, the shape of the variety we get from these results suggests that Assumption 6 should typically hold.

Under these assumptions, let us finally explain why the Gröbner basis computation terminates in degree $\leqslant 3$. There are two cases to consider.

Case 1. The missing leading monomial in $\mathcal{G}_{\text{spec}}$ is of the form $x_i x_j$ for distinct indexes $i \neq j$. Given arbitrary polynomials $g,\ h \in \mathcal{G}_{\text{spec}}$, Buchberger's second criterion (Proposition 3.1) shows that the only case when $S(g,h)$ were not reduced to 0 would be when the leading monomials of g and h have a common factor. In this situation, this S-polynomial is of degree at most 3 and since

(i) all cubic monomials appear as multiples of leading monomials in $\mathcal{G}_{\text{spec}}$,

(ii) all quadratic monomials appear as leading monomials except $x_i x_j$,

it will reduce to a polynomial of the form $f = \mu x_i x_j + L(\boldsymbol{x})$ for some scalar μ and $L \in \mathbb{F}_{q^k}[\boldsymbol{x}]$ of degree 1. It is impossible that $\mu = 0$ and $L \neq 0$ since this would imply that all k solutions to $\mathcal{F}_{\text{spec}}$ lie in the affine hyperplane $L(\boldsymbol{x}) = 0$, which contradicts Assumption 6. If $\mu \neq 0$, then it is clear by performing the same reasoning that all S-polynomials $S(f, g_i),\ g_i \in \mathcal{G}_{\text{spec}}$ would reduce to 0 (since they would this time reduce to affine forms which are necessarily 0 by the previous reasoning). By Theorem 2.1, we are thus left with a Gröbner basis.

Case 2. The missing leading monomial is of the form x_i^2. The difference with the previous case is that all degree 3 monomials appear as multiples of leading monomials in $\mathcal{G}_{\text{spec}}$ except x_i^3. In such a case, an S-polynomial $S(g, h)$ will reduce to a polynomial of the form $f = \lambda x_i^3 + \mu x_i^2 + L(\boldsymbol{x})$, where L is again an affine form and $\lambda,\ \mu \in \mathbb{F}_{q^k}$. It is readily seen that we cannot have $\lambda = \mu = 0$ without that $L = 0$ itself (this would contradict Assumption 6 in the same way as before). From this, it is readily seen that all S-polynomials $S(f, g_i),\ g_i \in \mathcal{G}_{\text{spec}}$ reduce to 0 and that we have a Gröbner basis again.

In both situations, this means that one needs to go up to degree 3 in the worst case to compute the Gröbner basis for $\mathcal{F}_{\text{spec}}$. The final complexity is then dominated by that of performing Gaussian elimination at degree 3 on a matrix of size $A \times B$ with $A \leqslant B \overset{def}{=} \binom{k-2+3}{3}$, namely

$$\mathcal{O}\left(\binom{k+1}{3}^{\omega}\right)$$

field operations. The cost of solving the system is thus in $\mathcal{O}\left(k^{3\omega}\right)$, which is clearly polynomial in the dimension of the Sidon space.

5.4 Finding an Equivalent Key

Retrieving elements in $\mathcal{Z}_{\mathbb{F}_{q^k}}$ can thus be performed in an efficient way. All that remains is to explain how this allows us to recover an equivalent key. Note that this second issue was not addressed in [RLT21]. There, they only evaluated the complexity of obtaining *arbitrary* solutions to Problem 5.1.

In our context, such equivalent keys will correspond to particular Sidon spaces.

Fact 2. *A Sidon space $\mathcal{V}' \in \mathcal{G}_q(n, k)$ with basis $\boldsymbol{\nu}' \in \mathbb{F}_{q^n}^k$ such that the matrix $\boldsymbol{M}(\boldsymbol{\nu}')$ is a solution to Problem 5.1 can be used as an equivalent key provided one has access to an efficient factoring algorithm $\mathcal{A}'$.*

Proof. Assume that $\boldsymbol{\nu}'$ is a basis of a Sidon space $\mathcal{V}'$ such that the matrix $\boldsymbol{M}(\boldsymbol{\nu}')$ is a linear combination between the $\boldsymbol{M}^{(i)}$'s. From the knowledge of $\boldsymbol{\nu}'$, one can construct $\boldsymbol{M}(\boldsymbol{\nu}')$ and then solve the linear system in the β_i''s given by $\boldsymbol{M}(\boldsymbol{\nu}') = \sum_{i=1}^n \beta_i' \boldsymbol{M}^{(i)}$. Finally, the quantity $\sum_{i=1}^n \beta_i' c_i$ is a product of elements in $\mathcal{V}'$ which can be factored using Algorithm $\mathcal{A}'$. □

We now show that we can efficiently find a Sidon space $\mathcal{V}'$ obtained by Construction 1 that meets the criteria of Fact 2 from a set of $k+1$ elements $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_{k+1}$ in $\mathcal{Z}_{\mathbb{F}_{q^k}}$ by applying the following procedure:

1. Using these vectors, we recover some $\boldsymbol{t} \stackrel{def}{=} (t_1, \cdots, t_k) = \lambda \boldsymbol{u}^{[j]},\ \lambda \in \mathbb{F}_{q^k},\ 0 \leqslant j \leqslant k-1$, where $\boldsymbol{u} = (u_1, \cdots, u_k)$ is defined by Equation (5.4) from the secret basis $\boldsymbol{\nu}$ of the genuine Sidon space $\mathcal{V}$.

2. From the knowledge of $\boldsymbol{t}$, we deduce the aforementioned Sidon space as

$$\mathcal{V}' \stackrel{def}{=} \left\langle t_1 + \gamma' t_1^q, \cdots, t_k + \gamma' t_k^q \right\rangle_{\mathbb{F}_q},$$

   where $\gamma' \in \mathbb{F}_{q^n}$ is generated like γ in **Keygen**, namely as a root of an irreducible polynomial $x^2 + ex + f$ over $\mathbb{F}_{q^k}$ such that $f \in \overline{W_{q-1}}$. Note that this γ' is sufficient to devise Algorithm 2 to factor in $\mathcal{V}'$.

These two steps are described in more depth in Sections 5.4.1 and 5.4.2 below.

5.4.1 Targeting the $\lambda \boldsymbol{u}^{[j]}$ Vector

Assuming that the inclusion in Proposition 5.2 is an equality, one obtains that the set $\mathcal{Z}_{\mathbb{F}_{q^k}}$ is equal to the union of vector spaces

$$\mathcal{Z}_{\mathbb{F}_{q^k}} = \bigcup_{i=1}^{k} \mathcal{W}_i, \quad \text{where } \mathcal{W}_i \stackrel{def}{=} \left\langle \boldsymbol{u}^{[i-1]}, \boldsymbol{u}^{[i]} \right\rangle_{\mathbb{F}_{q^k}}.$$

Let us notice that the components $\mathcal{W}_i$ satisfy the peculiar property that

$$\mathcal{W}_i \cap \mathcal{W}_i^{[1]} = \left\langle \boldsymbol{u}^{[i]} \right\rangle_{\mathbb{F}_{q^k}}, \tag{5.11}$$

where for a set S of vectors, $S^{[1]}$ stands for the set $\{\boldsymbol{x}^{[1]} : \boldsymbol{x} \in S\}$.

In other words, Equation (5.11) states that we can recover one of the $\boldsymbol{u}^{[i]}$'s up to multiplication by an element of $\mathbb{F}_{q^k}$ if we are able to produce one of those $\mathcal{W}_i$'s. This can be achieved thanks to the pigeonhole principle: two among the solutions $\boldsymbol{t}_i$ for $1 \leqslant i \leqslant k+1$ will fall into a same vector space $\mathcal{W}_{j_0}$. These considerations lead to the following Algorithm 3 for recovering one of those $\boldsymbol{u}^{[i]}$'s (up to a multiplicative constant):

Algorithm 3: Extracting the relevant vector.

Input: A set of $k+1$ non-collinear vectors $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_{k+1}$ in $\mathcal{Z}_{\mathbb{F}_{q^k}}$.

Output: A set $\mathcal{S}$ containing at least one element collinear with one of the $\boldsymbol{u}^{[i]}$'s.

```
for i = 1 to k do
    for j = i to k + 1 do
        V ← ⟨t_i, t_j⟩_{F_{q^k}}
        if dim V ∩ V^[1] = 1 then
            S ← S ∪ {x} ;          /* where x generates V ∩ V^[1] */
        end
    end
end
```

This algorithm is deterministic of complexity $\mathcal{O}(k^2)$. Note that we do not necessarily need $k+1$ non-collinear vectors $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_{k+1}$ in $\mathcal{Z}_{\mathbb{F}_{q^k}}$. Indeed, $\Theta(\sqrt{k})$ are sufficient by using the birthday paradox if we content ourselves with a probabilistic version of success probability $\Omega(1)$.

5.4.2 Deducing $\mathcal{V}'$

How a Sidon space $\mathcal{V}'$ with the right properties can be obtained from $\boldsymbol{t}$ collinear with some $\boldsymbol{u}^{[i]}$ is explained by the following proposition.

Proposition 5.3. *Let $\gamma' \in \mathbb{F}_{q^n}$ be a root of an irreducible polynomial $x^2 + ex + f$ over $\mathbb{F}_{q^k}$ such that $f \in \overline{W_{q-1}}$. Then, the $\mathbb{F}_q$-linear space $\mathcal{V}'$ generated by the ordered basis $\boldsymbol{\nu}' \stackrel{def}{=} \boldsymbol{t} + \gamma' \boldsymbol{t}^{[1]}$ is a Sidon space such that $\boldsymbol{M}(\boldsymbol{\nu}')$ belongs to the linear span of the $\boldsymbol{M}_i$'s.*

Proof. Without loss of generality, let us assume that $\boldsymbol{t} = \lambda \boldsymbol{u}$ for some $\lambda \in \mathbb{F}_{q^k}$. We then have

$$
\begin{aligned}
\boldsymbol{M}(\boldsymbol{\nu}') &= \boldsymbol{M}(\boldsymbol{t} + \gamma' \boldsymbol{t}^{[1]}) \\
&= \boldsymbol{t}^{\mathsf{T}} \boldsymbol{t} + \gamma'^2 \left(\boldsymbol{t}^{[1]}\right)^{\mathsf{T}} \boldsymbol{t}^{[1]} + \gamma' \boldsymbol{t}^{\mathsf{T}} \boldsymbol{t}^{[1]} + \gamma' \left(\boldsymbol{t}^{[1]}\right)^{\mathsf{T}} \boldsymbol{t} \\
&= \lambda^2 \boldsymbol{u}^{\mathsf{T}} \boldsymbol{u} + \lambda^{2q} \gamma'^2 \left(\boldsymbol{u}^{[1]}\right)^{\mathsf{T}} \boldsymbol{u}^{[1]} + \lambda^{1+q} \gamma' \left\{ \boldsymbol{u}^{\mathsf{T}} \boldsymbol{u}^{[1]} + \left(\boldsymbol{u}^{[1]}\right)^{\mathsf{T}} \boldsymbol{u} \right\} \quad \text{(using the definition of } \boldsymbol{t}\text{)} \\
&= \lambda^2 \boldsymbol{M}(\boldsymbol{u}) + \lambda^{2q} \gamma'^2 \boldsymbol{M}(\boldsymbol{u}^{[1]}) + \lambda^{1+q} \gamma' \left\{ (\boldsymbol{u} + \boldsymbol{u}^{[1]})^{\mathsf{T}} (\boldsymbol{u} + \boldsymbol{u}^{[1]}) - \boldsymbol{u}^{\mathsf{T}} \boldsymbol{u} - \left(\boldsymbol{u}^{[1]}\right)^{\mathsf{T}} \boldsymbol{u}^{[1]} \right\} \\
&= \lambda^2 \boldsymbol{M}(\boldsymbol{u}) + \lambda^{2q} \gamma'^2 \boldsymbol{M}(\boldsymbol{u}^{[1]}) + \lambda^{1+q} \gamma' \left\{ \boldsymbol{M}(\boldsymbol{u} + \boldsymbol{u}^{[1]}) - \boldsymbol{M}(\boldsymbol{u}) - \boldsymbol{M}(\boldsymbol{u}^{[1]}) \right\} \\
&\in \left\langle \boldsymbol{M}^{(1)}, \cdots, \boldsymbol{M}^{(n)} \right\rangle_{\mathbb{F}_{q^n}} \quad \text{(by Proposition 5.2).}
\end{aligned}
$$

□

More concretely, we will thus

1. find an element γ' satisfying the same constraints as γ, *i.e.*, γ' is a root of an irreducible polynomial $x^2 + ex + f$ over $\mathbb{F}_{q^k}$ such that $f \in \overline{W_{q-1}}$;
2. obtain $\mathcal{V}'$ as the $\mathbb{F}_q$-vector space generated by

$$\boldsymbol{\nu}' \stackrel{def}{=} (t_1 + \gamma' t_1^q, \ldots, t_k + \gamma' t_k^q).$$

The overall cost boils down to finding $\gamma' \in \mathbb{F}_{q^n}$ in Step 1., which can be performed in the same way as in **Keygen**. There, [RLT21] propose a random procedure whose success probability can be estimated using [RRT17, Lemma 13]. Heuristically, it works in constant expected time.

Part III
Cryptanalysis of Rank-Based Cryptography

Chapter 6
Rank Support Learning Problem

This chapter presents two attacks on the Rank Support Learning problem.

The first one is an algebraic approach which I published with Magali Bardet [BB21]. The main application at that time was the Durandal signature scheme. On a large zone of parameters relevant to this proposal, our work ourperforms the RD algorithms of [Bar+20b]. Interestingly, our proof technique also helped us to gain understanding on these previous methods. This will be a key ingredient in Chapter 7 where we describe [Bar+23].

The second one is a combinatorial approach due to Philippe Gaborit included in our joint work [BBBG23]. Even if it is slightly less efficient than [Bar+20b; BB21] when the number of syndromes is reduced, it allows to widen the parameter range for which a polynomial time algorithm exists on Problem 3.7.

Contents

6.1 Preliminaries

Section 6.1.1 details the current designs which rely on the hardness of RSL. The Durandal signature scheme [Ara+19b] was essentially the unique non-broken one when we published [BB21]. Since then, encryption mechanisms also based on Problem 3.7 have emerged [Agu+22; BBBG23; Ara+22]. In Section 6.1.2, we follow [GHPT17] by rewriting the problem in terms of low weight codeword search in a particular $\mathbb{F}_q$-linear code. This content will be used in both [BB21] and [BBBG23].

6.1.1 Cryptographic Applications

Let us recall that the Rank Support Learning problem was introduced for cryptographic purposes in order to build an IBE [GHPT17]. Even if this proposal was later shown to be insecure [DT18], this already illustrates the versatility of the assumption. In particular, RSL also allowed to devise a signature scheme [Ara+19b], which is known to be a challenging task in code-based cryptography.

6.1.1.1 Durandal Signature Scheme

We will first explain how Problem 3.7 appears within Durandal. We had briefly presented the scheme in Section 3.3.5.1. In this context, RSL can be viewed as the analogue of the Short Integer Solution (SIS) problem [Ajt96] used in Lyubashevsky's signature [Lyu09].

Durandal is based on an ideal structure. In [Ara+19b], the secret key sk consists of two matrices $(\boldsymbol{E}, \boldsymbol{E}') \in \mathbb{F}_{q^m}^{\ell \times 2k} \times \mathbb{F}_{q^m}^{\ell' \times 2k}$ whose entries lie in a subspace $\mathcal{V} \subset \mathbb{F}_{q^m}$ of small dimension r. The public key pk contains a random ideal double circulant matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{2k \times k}$ as well as $\boldsymbol{T}_1^\intercal \stackrel{def}{=} \boldsymbol{H}\boldsymbol{E}_1^\intercal \in \mathbb{F}_{q^m}^{k \times \ell}$ and $\boldsymbol{T}_2^\intercal \stackrel{def}{=} \boldsymbol{H}\boldsymbol{E}_2^\intercal \in \mathbb{F}_{q^m}^{k \times \ell'}$. Clearly, the pair $\left(\boldsymbol{H}, \boldsymbol{T} \stackrel{def}{=} \begin{bmatrix} \boldsymbol{T}_1 \\ \boldsymbol{T}_2 \end{bmatrix}\right)$ is an instance of Problem 3.7 with parameters $(m, 2k, k, r)$ and $\ell + \ell'$ syndromes. However, a more relevant one to cryptanalysis is $(\boldsymbol{H}, \boldsymbol{T}')$, where $\boldsymbol{T}' \in \mathbb{F}_{q^m}^{(\ell+\ell')k \times k}$ is publicly obtained from $\boldsymbol{T}$ by taking the ideal shifts of all the rows. In this way, key-recovery reduces to solving a structured instance with $N = k(\ell + \ell')$.

In addition to RSL, the scheme relies on the hardness of the *ad hoc* PSSI$^+$ problem [Ara+19b, Problem 5]. A recent attack by Aragon *et al.* [ADG23] has drastically reduced the security of this second assumption and it contributed to break all existing parameters. Thus, deriving new ones will require to take both [BB21] and [ADG23] into account. However, since the cryptanalysis of PSSI$^+$ is less mature and since the progress of [ADG23] was spectacular, one can expect that PSSI$^+$ attacks will be the limiting ones.

6.1.1.2 PKE/KEMs with Multiple Syndromes

More recently, [Agu+22] pioneered a new approach to improve the efficiency of RD-based cryptosystems. It was originally applied to ROLLO. A bit later, [BBBG23] and [Ara+22] revisited the same idea on RQC and Loidreau's [Loi17] respectively. As a result, all these works obtained unstructured rank-based schemes with more competitive sizes than those of similar Hamming-based or lattice-based proposals [Alb+20; Alk+20].

What matters here is that this leads to consider RSL in the security reduction. Indeed, the ciphertext now contains N syndromes $(\boldsymbol{s}_i)_{1 \leqslant i \leqslant N}$ associated to errors with the same support $\mathcal{V}$ of dimension r. Roughly speaking, the rationale is that the underlying decoder performs better when receiving several correlated syndromes instead of just one.

- In the case of an LDPC code with row weight d, the DFR decreases. Indeed, the standard one is close to $q^{rd-(n-k)-1}$ while [Agu+22] devise an algorithm for multiple syndromes with DFR approximately equal to $q^{rd-(n-k)N}$ [Agu+22, Proposition 2].

- In [Ara+22], the higher number of syndromes allows to improve the decoding capability. This stems from the fact that a horizontally interleaved Gabidulin code of order N can decode up to $\lfloor \frac{N}{N+1}(n-k) \rfloor$ errors if one accepts a non-zero DFR [SJB11, Equations (43),(44)].

As already mentioned in Section 3.3.5.2, the objective was to choose a higher rank r to limit the impact of algebraic attacks. What is also interesting is that the value of N is much smaller than in Durandal. In [Agu+22], the border condition $rd = n - k + o(1)$ is replaced by $(n-k)N = rd + o(1)$ (see the discussion after [Agu+22, Lemma 1]). In [Ara+22], the DFR formula inherited from [SJB11, Equation (44)] applies when the input weight is $\geqslant N$ and, a fortiori, when $N \leqslant \lfloor \frac{N}{N+1}(n-k) \rfloor$.

6.1.2 Rephrasing the Problem

Rather than elaborating on [GHPT17, §4.2] and [DT18] which are tailored to a large number of errors, we will describe the content of [GHPT17] that is used in our work.

Note that RSL with $N = 1$ is simply Problem 3.6. In this situation, it was relevant to consider the $\mathbb{F}_{q^m}$-linear code $\mathcal{C}_{\boldsymbol{y}} = \mathcal{C} \oplus \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}} = \mathcal{C} \oplus \langle \boldsymbol{e} \rangle_{\mathbb{F}_{q^m}}$. To tackle the general case, the issue with this method is that $\langle \boldsymbol{e}_1, \dots, \boldsymbol{e}_N \rangle_{\mathbb{F}_{q^m}}$ will quickly cover the full space $\mathbb{F}_{q^m}^n$. Thus, the authors of [GHPT17] attacked another code containing all these errors but which is simply $\mathbb{F}_q$-linear. If $\mathcal{T} \subset \mathbb{F}_{q^m}^{n-k}$ stands for the $\mathbb{F}_q$-linear space generated by the syndromes, a public description of this code is given by

Notation 2.

$$\mathcal{C}_{aug} \stackrel{def}{=} \left\{ \boldsymbol{x} \in \mathbb{F}_{q^m}^n : \boldsymbol{x}\boldsymbol{H}^\intercal \in \mathcal{T} \right\}. \tag{6.1}$$

The crux is that it contains both the code $\mathcal{C}$ and

$$\mathcal{E} \stackrel{def}{=} \langle \boldsymbol{e}_1, \dots, \boldsymbol{e}_N \rangle_{\mathbb{F}_q}. \tag{6.2}$$

This last observation shows that $\mathcal{C}_{\text{aug}}$ typically contains about q^N codewords of weight $\leqslant r$. The approach of [GHPT17] consisted in finding one of such vectors. If the weight is exactly r, its support will reveal $\mathcal{V}$. If the weight is smaller, it is a subspace but which yields enough information.

Since one can also view $\mathcal{C}_{\text{aug}}$ as a matrix code of parameters $[m \cdot n, \leqslant km + N]_q$, the above task can be rephrased as the one of solving a homogeneous MinRank problem with $km + N$ matrices in $\mathbb{F}_q^{m \times n}$ and target rank $\leqslant r$. Even though the code is not $\mathbb{F}_{q^m}$-linear, this instance has a lot of structure. Indeed, $\mathcal{C}_{\text{aug}}$ still admits a compact description over the extension field by Equation (6.1).

6.2 Restricting the Number of Solutions

The MinRank and RD algorithms that we have presented so far aimed at solving instances with essentially one solution. Since RSL can be seen as an in-between, we hope to be

able to use similar techniques. However, even if there is only one vector space $\mathcal{V}$, the number of weight $\leqslant r$ codewords in $\mathcal{C}_{\text{aug}}$ is exponential in N.

Thus, we will try to attack a related problem with roughly one solution. Of course, it should still allow to recover the initial support. Since what really matters is in fact a subspace, we may look for vectors of weight w strictly smaller than r. To reduce the number of such codewords even further, we may also work in a shortened code in the sense of Equation (2). Indeed, for such a code $\mathcal{S}_I(\mathcal{C}_{\text{aug}})$, weight $\leqslant r$ vectors should belong to $\mathcal{S}_I(\mathcal{E})$. We study the weight distribution of this latter code in Proposition 6.1.

Proposition 6.1. *Let $\mathcal{E}$ be the code defined by Equation (6.2) viewed as a matrix code, let $I \subset \{1..n\}$, $\#I = a$ and let $\mathcal{S}_I(\mathcal{E}) \subset \mathbb{F}_q^{m\times(n-a)}$ be the shortening at these positions (by considering columns with indexes in $\{1..n\}\backslash I$). We assume that its dimension is $N-ar$. For $w \leqslant r$, let $X_{\mathcal{S}_I(\mathcal{E}),w}$ be the random variable counting the number of codewords of weight w in $\mathcal{S}_I(\mathcal{E})$, where the randomness comes from the choice of a support $\mathcal{V}$ of dimension r and of the errors $\boldsymbol{e}_i$ with this support. The expectation and the variance of $X_{\mathcal{S}_I(\mathcal{E}),w}$ are respectively given by*

$$\begin{aligned}
\mathrm{E}\big[X_{\mathcal{S}_I(\mathcal{E}),w}\big] &= \frac{\mathcal{S}_{w,r,n-a,q}}{q^{rn-N}},\\
\mathrm{Var}\big[X_{\mathcal{S}_I(\mathcal{E}),w}\big] &= \mathcal{S}_{w,r,n-a,q} \times (q-1) \times \left(\frac{1}{q^{rn-N}} - \left(\frac{1}{q^{rn-N}}\right)^2\right),
\end{aligned}$$

where $\mathcal{S}_{w,r,n-a,q} \stackrel{def}{=} \#\{\boldsymbol{M} \in \mathbb{F}_q^{r\times(n-a)},\ \mathrm{rk}(\boldsymbol{M}) = w\}$. When q is a constant, this gives

$$\begin{aligned}
\mathrm{E}\big[X_{\mathcal{S}_I(\mathcal{E}),w}\big] &= \Theta(q^{w(n-a+r-w)-rn+N}) = \Theta(q^{N-ar-(r-w)(n-a-w)})\\
\mathrm{Var}\big[X_{\mathcal{S}_I(\mathcal{E}),w}\big] &= \Theta(q^{N-ar+1-(r-w)(n-a-w)}) = \Theta(q^{N-ar-(r-w)(n-a-w)}).
\end{aligned}$$

Proof. For $\boldsymbol{\beta} \in \mathbb{F}_{q^m}^m$ a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $\boldsymbol{S}_{\mathcal{V}} \in \mathbb{F}_q^{m\times r}$ a full-rank matrix such that $\boldsymbol{\beta}\boldsymbol{S}_{\mathcal{V}}$ is a basis of $\mathcal{V}$, let us remark that each element $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n-a}$ in $\mathcal{S}_I(\mathcal{E})$ can be written as $\boldsymbol{e} = \boldsymbol{\beta}\boldsymbol{S}_{\mathcal{V}}\boldsymbol{C}$ for some $\boldsymbol{C} \in \mathbb{F}_q^{r\times(n-a)}$. We consider the matrix code $\mathcal{D}$ of parameters $[r\cdot(n-a), N-ar]_q$ generated by these $\boldsymbol{C}$ matrices. Since $X_{\mathcal{S}_I(\mathcal{E}),w} = X_{\mathcal{D},w}$ for any $w \leqslant r$, the rest of the proof will focus on this latter code. For $\boldsymbol{C} \in \mathbb{F}_q^{r\times(n-a)}$, let us denote by $\mathbf{1}_{\boldsymbol{C}\in\mathcal{D}}$ the random variable equal to 1 if $\boldsymbol{C} \in \mathcal{D}$ and 0 otherwise, so that $X_{\mathcal{D},w} = \sum_{wt(\boldsymbol{C})=w} \mathbf{1}_{\boldsymbol{C}\in\mathcal{D}}$. By linearity of expectation, one obtains

$$\mathrm{E}[X_{\mathcal{D},w}] = \sum_{wt(\boldsymbol{C})=w} \mathrm{E}[\mathbf{1}_{\boldsymbol{C}\in\mathcal{C}}] = \sum_{wt(\boldsymbol{C})=w} \Pr[\boldsymbol{C} \in \mathcal{D}].$$

The probability that $\boldsymbol{C} \in \mathcal{D}$ is the one to satisfy $r(n-a)-(N-ar) = rn-N$ independent parity-check equations, hence $\Pr[\boldsymbol{C} \in \mathcal{D}] = \frac{1}{q^{rn-N}}$. The result follows by summing over all the codewords of weight w. For the variance, we start by computing the quantity

$$\mathrm{E}\big[X_{\mathcal{D},w}^2\big] = \sum_{wt(\boldsymbol{C}_1)=w} \sum_{wt(\boldsymbol{C}_2)=w} \mathrm{E}[\mathbf{1}_{\boldsymbol{C}_1\in\mathcal{D}}\mathbf{1}_{\boldsymbol{C}_2\in\mathcal{D}}].$$

We have $\mathrm{E}[1_{\boldsymbol{C}_1\in\mathcal{D}}1_{\boldsymbol{C}_2\in\mathcal{D}}] = \Pr[\boldsymbol{C}_1 \in \mathcal{D}, \boldsymbol{C}_2 \in \mathcal{D}]$ by definition. The code $\mathcal{D}$ being $\mathbb{F}_q$-linear, the events $\boldsymbol{C}_1 \in \mathcal{D}$ and $\boldsymbol{C}_2 \in \mathcal{D}$ are not independent when $\boldsymbol{C}_2 \in \langle \boldsymbol{C}_1 \rangle_{\mathbb{F}_q}$. In this case, one has

$$\Pr[\boldsymbol{C}_1 \in \mathcal{D}, \boldsymbol{C}_2 \in \mathcal{D} \mid \boldsymbol{C}_2 \in \langle \boldsymbol{C}_1 \rangle_{\mathbb{F}_q}] = \Pr[\boldsymbol{C}_1 \in \mathcal{D}] = \frac{1}{q^{rn-N}}.$$

Therefore

$$\begin{aligned}
\mathrm{E}\big[X^2_{\mathcal{D},w}\big] &= \sum_{wt(\boldsymbol{C}_1)=w} \sum_{\substack{\boldsymbol{C}_2\in\langle \boldsymbol{C}_1\rangle_{\mathbb{F}_q} \\ wt(\boldsymbol{C}_2)=w}} \frac{1}{q^{rn-N}} + \sum_{wt(\boldsymbol{C}_1)=w} \sum_{\substack{\boldsymbol{C}_2\notin\langle \boldsymbol{C}_1\rangle_{\mathbb{F}_q} \\ wt(\boldsymbol{C}_2)=w}} \left(\frac{1}{q^{rn'-N'}}\right)^2 \\
&= \mathcal{S}_{w,r,n-a,q}(q-1)\frac{1}{q^{rn-N}} + \mathcal{S}_{w,r,n-a,q}\left(\mathcal{S}_{w,r,n-a,q} - (q-1)\right)\left(\frac{1}{q^{rn-N}}\right)^2 \\
&= \mathrm{E}[X_{\mathcal{D},w}]^2 + \mathcal{S}_{w,r,n-a,q} \times (q-1) \times \left(\frac{1}{q^{rn-N}} - \left(\frac{1}{q^{rn-N}}\right)^2\right).
\end{aligned}$$

□

In other words, our method is a reduction to a smaller RSL instance. Recall that our goal is to attack one with a number of solutions which is essentially constant. This can be done by choosing parameters according to Proposition 6.1 or more simply to Equation (3.4) applied to $\mathcal{S}_I(\mathcal{E})$ since we mostly care about its minimum distance. More precisely, for a fixed weight $w \in \{1..r\}$, we will pick the code corresponding to the maximal value of $a \geqslant 0$ such that

$$N - ar > (r-w)(n-a-w) \Leftrightarrow aw < N - (r-w)(n-w).$$

To consider more cases in the optimization, we may also select slightly less syndromes and attack codes of the form $\mathcal{S}_I(\mathcal{E}')$, where $\mathcal{E}' \stackrel{def}{=} \langle \boldsymbol{e}'_1, \ldots, \boldsymbol{e}'_s \rangle_{\mathbb{F}_q} \subset \mathcal{E}$ is generated by the associated errors which is a subset of $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N\}$. Since this number of syndromes intervenes in our total amount of unknowns, there will be situations for which this addition makes sense.

6.3 An Algebraic Approach

In [BB21], we introduced a polynomial system to solve the subproblem. To simplify the notation, let us present it applied to the original RSL instance.

6.3.1 RSL-Minors Modeling

The point is to exploit the compact description of $\mathcal{C}_{\text{aug}}$ given in Equation (6.1). By definition, a codeword $\boldsymbol{e} \in \mathcal{C}_{\text{aug}}$ is such that $\boldsymbol{e}\boldsymbol{H}^\intercal \in \mathcal{T}$, *i.e.*, $\boldsymbol{e}\boldsymbol{H}^\intercal = \sum_{i=1}^N \lambda_i \boldsymbol{s}_i$ for coefficients $\lambda_i \in \mathbb{F}_q$, $1 \leqslant i \leqslant N$. Since we target one of weight $\leqslant r$, we can also write it

as in the MaxMinors case in the form $\boldsymbol{e} = \boldsymbol{\beta}\boldsymbol{S}_{\mathcal{V}}\boldsymbol{C}$, where $\boldsymbol{\beta}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, $\boldsymbol{S}_{\mathcal{V}} \in \mathbb{F}_q^{m\times r}$ and $\boldsymbol{C} \in \mathbb{F}_q^{r\times n}$. This yields the equation

$$\sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i = \boldsymbol{\beta}\boldsymbol{S}_{\mathcal{V}}\boldsymbol{C}\boldsymbol{H}^{\mathsf{T}}.$$

From there, the rest follows as in Support-Minors by noting that the vector $\sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i$ is a linear combination over $\mathbb{F}_{q^m}$ between the rows of $\boldsymbol{C}\boldsymbol{H}^{\mathsf{T}}$. This means that the matrix

$$\boldsymbol{\Delta} \stackrel{def}{=} \begin{bmatrix} \sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i \\ \boldsymbol{C}\boldsymbol{H}^{\mathsf{T}} \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{N} \lambda_i \boldsymbol{y}_i \\ \boldsymbol{C} \end{bmatrix} \boldsymbol{H}^{\mathsf{T}} \in \mathbb{F}_{q^m}^{(r+1)\times(n-k)}$$

has rank at most r. As in previous MinRank modelings, we can then adopt the system of all its $(r+1)\times(r+1)$ minors. In addition, computing them by Laplace expansion along the first row and by applying the Cauchy-Binet formula (Lemma 3.3) naturally leads to consider minor variables $c_T = |\boldsymbol{C}_{*,T}|$.

Modeling 12 (RSL-Minors). *The RSL-Minors modeling is the system in the λ_i variables and in the c_T variables, defined by $\{\boldsymbol{\Delta}_J\}_{J\subset\{1..n-k\},\ \#J=r+1}$, where*

$$\boldsymbol{\Delta}_J \stackrel{def}{=} |\boldsymbol{\Delta}_{*,J}| = \left| \begin{bmatrix} \sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i \\ \boldsymbol{C}\boldsymbol{H}^{\mathsf{T}} \end{bmatrix}_{*,J} \right|.$$

In the following, we will denote it by $\mathcal{U}$.

A bit more explicitly, we obtain

Lemma 6.1. *For an ordered subset $T \subset \{1..n\}$ and $t \in T$, let $Pos(t,T)$ denote the position of t in T. Let $J \subset \{1..n-k\}$ such that $\#J = r+1$. We have*

$$\boldsymbol{\Delta}_J = \sum_{i=1}^{N} \lambda_i \sum_{T\subset\{1..n\},\#T=r} c_T \sum_{t\notin T} y_{i,t}(-1)^{1+Pos(t,T\cup\{t\})} \left|\boldsymbol{H}_{J,T\cup\{t\}}\right|. \tag{6.3}$$

In other words, Modeling 12 is a bilinear system with $\binom{n-k}{r+1}$ equations and $N\binom{n}{r}$ monomials $\lambda_i c_T$ for $1 \leqslant i \leqslant N$ and $T \subset \{1..n\},\ \#T = r$.

Once again, the coefficients of the equations are over $\mathbb{F}_{q^m}$ while the unknowns λ_i and c_T are searched in $\mathbb{F}_q$. Thus, we can proceed as in the MaxMinors case to obtain Modeling 13 containing $m\binom{n-k}{r+1}$ equations.

Modeling 13 (RSL-Minors-$\mathbb{F}_q$). *Let $\boldsymbol{\beta}' = (\beta'_1, \ldots, \beta'_m)$ be an arbitrary $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Let Tr be the trace operation as in Equation (3.16) defined for polynomials in $\mathbb{F}_{q^m}[c_T, \boldsymbol{\lambda}]$. The RSL-Minors modeling over $\mathbb{F}_q$ is the system in the λ_i variables and in the c_T variables, defined by $\{\boldsymbol{\Delta}_{\ell,J}\}_{1\leqslant\ell\leqslant m,\ J\subset\{1..n-k\},\ \#J=r+1}$, where*

$$\boldsymbol{\Delta}_{\ell,J} \stackrel{def}{=} Tr(\beta'_\ell \boldsymbol{\Delta}_J) \ mod\ \{c_T^q - c_T, \lambda_i^q - \lambda_i\}.$$

In the following, we will denote it by $\mathcal{U}_{\mathbb{F}_q}$.

To solve this system, we use the same approach as in [Bar+20b] by multiplying the polynomials by all linear variables λ_i for $1 \leqslant i \leqslant N$. More precisely, we aim at recovering the low weight codeword from a vector in the right kernel of the Macaulay matrix $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{U}_{\mathbb{F}_q})$ at the relevant bi-degree. Since the subproblem is chosen to have roughly one solution, this corresponds to the least value such that the number of independent rows is greater than the number of columns minus one. Over $\mathbb{F}_2$ or more generally when $q \leqslant b$, this estimation has to take into account the field equations $\lambda_i^q - \lambda_i = 0$. Indeed, reduced modulo these polynomials, a homogeneous equation in bi-degree $(b, 1)$ may become affine and possibly involve monomials of degree $(b', 1)$ for any $1 \leqslant b' \leqslant b$. In this case, it will be favorable to consider the matrix $\mathcal{M}\mathrm{ac}_{\leqslant(b,1)}(\mathcal{U}_{\mathbb{F}_q})$ which contains all equations up to this bi-degree.

Remark 6.1. For two codes $\mathcal{S}_I(\mathcal{E}')$ and $\mathcal{S}_I(\mathcal{E})$ with $\mathcal{E}' \subset \mathcal{E}$ as presented above, the algebraic system for the same weight w should be solved at a lower degree on $\mathcal{S}_I(\mathcal{E})$ than on $\mathcal{S}_I(\mathcal{E}')$. We may prefer to consider $\mathcal{S}_I(\mathcal{E}')$ only when these degrees are equal. Indeed, since the code dimension is also the number of linear variables, the size of the Macaulay matrix will be smaller.

6.3.2 Analysis over the Extension Field

As in [Bar+20b], the complexity analysis calls for understanding the rank of the Macaulay matrices. However, for Modeling 13, we cannot obtain an exact formula regardless of the parameters. The situation is different with Modeling 12. There, indeed, the rank is always given by the number of independent rows. In particular, we can provide the precise value of $\mathrm{rk}\left(\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{U})\right)$ for any $b \geqslant 1$.

Let us start with the $b = 1$ case. Under the following elementary assumption on the matrix of syndromes, Theorem 6.1 shows that there are no linear relations in the initial system.

Assumption 7. *Let* $\boldsymbol{S} \stackrel{def}{=} \left[\boldsymbol{s}_1^\intercal \ \dots \ \boldsymbol{s}_N^\intercal\right] \in \mathbb{F}_{q^m}{}^{(n-k)\times N}$. *We assume that the matrix* $\boldsymbol{S}_{\{1..n-k-r\},*}$ *has rank* $n-k-r$.

Theorem 6.1. *Under Assumption 7, the equations of Modeling 12 are linearly independent over* $\mathbb{F}_{q^m}$.

Proof. The proof will consist in row reducing the Macaulay matrix for a particular term order. More precisely, we consider the grevlex monomial ordering on the variables λ_i and c_T such that

$$c_{\{t_1<\cdots<t_r\}} \prec c_{\{t'_1<\cdots<t'_r\}} \quad \text{if and only if} \quad t_i = t'_i \text{ for all } 1 \leqslant i < j \text{ and } t_j < t'_j,$$
$$c_T \prec \lambda_N \prec \lambda_{N-1} \prec \cdots \prec \lambda_1 \qquad \forall T \subset \{1..n\},\ \#T = r.$$

This means that $\lambda_i c_T \prec \lambda_j c_{T'}$ if and only if $c_T \prec c_{T'}$ or $c_T = c_{T'}$ and $\lambda_i \prec \lambda_j$. Using the systematic form of $\boldsymbol{H}$, we can sort the monomials in any equation as

Lemma 6.2. *For an ordered subset $T \subset \{1..n\}$ and $t \in T$, let $Pos(t,T)$ denote the position of t in T. For any subset $J \subset \{1..n-k\}$ such that $\#J = r+1$, we have*

$$\boldsymbol{\Delta}_J = \sum_{j\in J}\sum_{i=1}^{N}(-1)^{1+Pos(j,J)}s_{i,j}\lambda_i c_{(J\setminus\{j\})+k} + \text{ (smaller terms)},$$

where the smallest monomials $\lambda_i c_T$ are the ones with $T \cap \{1..k\} \neq \varnothing$ while the largest ones satisfy $T \subset J + k \subset \{k+1..n\}$.

Now, let $I = \{j_2 < \cdots < j_{r+1}\} \subset \{1..n-k\}$, $\#I = r$ and let $\mathcal{U}_I \overset{def}{=} \{\boldsymbol{\Delta}_{\{\ell\}\cup I} : 1 \leqslant \ell < j_2\}$. By Lemma 6.2, the Macaulay matrix reads

$$\mathcal{M}\mathrm{ac}^{\prec}_{(1,1)}(\mathcal{U}_I) = \begin{array}{c} \\ \boldsymbol{\Delta}_{\{1\}\cup I} \\ \boldsymbol{\Delta}_{\{j_1\}\cup I} \\ \boldsymbol{\Delta}_{\{j_2-1\}\cup I} \end{array} \begin{array}{c} \begin{array}{ccccc} \ldots & \lambda_1 c_{I+k} & \ldots & \lambda_N c_{I+k} & \ldots \end{array} \\ \begin{bmatrix} 0 & s_{1,1} & \ldots & s_{N,1} & \ldots \\ 0 & s_{1,j_1} & & s_{N,j_1} & \ldots \\ 0 & s_{1,j_2-1} & & s_{N,j_2-1} & \ldots \end{bmatrix} \end{array} = \begin{bmatrix} \mathbf{0} & \boldsymbol{S}_{\{1..j_2-1\},*} & \ldots \end{bmatrix}.$$

Then, using Assumption 7 and up to a permutation of the syndromes, there exists an invertible lower-triangular matrix $\boldsymbol{L} \in \mathbb{F}_{q^m}^{(n-k-r)\times(n-k-r)}$ and an upper-triangular matrix $\boldsymbol{U} \in \mathbb{F}_{q^m}^{(n-k-r)\times N}$ with ones on the main diagonal such that $\boldsymbol{L}\boldsymbol{S}_{\{1..n-k-r\},*} = \boldsymbol{U}$. Noting that $j_2 \leqslant n-k-r+1$, we obtain $\boldsymbol{L}_{\{1..j_2-1\},\{1..j_2-1\}}\mathcal{M}\mathrm{ac}^{\prec}_{(1,1)}(\mathcal{U}_I) = \begin{bmatrix}\mathbf{0} & \boldsymbol{U}_{\{1..j_2-1\},*} & \ldots\end{bmatrix}$, *i.e.*,

$$\boldsymbol{L}_{\{1..j_2-1\},\{1..j_2-1\}}\mathcal{M}\mathrm{ac}^{\prec}_{(1,1)}(\mathcal{U}_I) = \begin{array}{c} \begin{array}{ccccc} \ldots & \lambda_1 c_{I+k} & \ldots & \lambda_{j_2-1} c_{I+k} & \ldots \end{array} \\ \begin{bmatrix} 0 & 1 & \ldots & u_{1,j_2-1} & \ldots \\ 0 & 0 & \ddots & u_{j_1,j_2-1} & \ldots \\ 0 & 0 & 0 & 1 & \ldots \end{bmatrix} \end{array}.*$$

Any row in this echelon form corresponds to an equation with leading term $1 \cdot \lambda_{j_1} c_{I+k}$ for any $1 \leqslant j_1 < j_2$. Overall, we obtain distinct leading monomials by repeating the same operation on all subsystems $\mathcal{U}_I$ for $I = \{j_2 < \cdots < j_{r+1}\} \subset \{1..n-k\}$, $\#I = r$. This shows linear independence. □

From the proof of Theorem 6.1, we will also retain

Corollary 6.1. *Under Assumption 7, the linear span of Modeling 12 admits a basis of polynomials with distinct leading monomials, namely $\left\{\widetilde{\boldsymbol{\Delta}_J}\right\}_{J\subset\{1..n-k\},\ \#J=r+1}$ such that*

$$LM\left(\widetilde{\boldsymbol{\Delta}_J}\right) = \lambda_{j_1} r_{(J\setminus\{j_1\})+k},\ j_1 \overset{def}{=} \min(J).$$

At higher bi-degree, the shape of the system triggers combinatorial syzygies of the same nature as in [Bar+20b, Proposition 6]. However, we are in a better situation. Indeed, what is remarkable is that Assumption 7 used to control the $b = 1$ case still allows us to obtain linearly independent equations once we get rid of these relations. In the following Theorem 6.2, we reuse the basis $\left\{\widetilde{\boldsymbol{\Delta}_J}\right\}_{J\subset\{1..n-k\},\ \#J=r+1}$ of Corollary 6.1.

Theorem 6.2. *Under Assumption 7 and for any $b \geqslant 1$, a basis of the rowspace of $\mathcal{M}ac_{(b,1)}(\mathcal{U})$ is given by the polynomials*

$$\mathcal{B}_b \overset{def}{=} \left\{ \prod_{\min(J)\leqslant j\leqslant N} \lambda_j^{\alpha_j} \widetilde{\boldsymbol{\Delta}_J} : \sum_{j=1}^{N} \alpha_j = b-1 \text{ and } J \subset \{1..n-k\},\ \#J = r+1 \right\}. \quad (6.4)$$

This space is of dimension

$$N_b \overset{def}{=} \sum_{d=2}^{n-k-r+1} \binom{n-k-d}{r-1} \sum_{j=1}^{d-1} \binom{N-j+1+b-2}{b-1}. \quad (6.5)$$

Proof. Taking $b = 1$ is Theorem 6.1. Thus, we start from a complete proof of the $b = 2$ case. As the leading monomial of $\widetilde{\boldsymbol{\Delta}_J}$ is $\lambda_{\min(J)} c_{J\setminus\{\min(J)\})+k}$, the relations between the polynomials can only come from the pairs $\left(\lambda_j \widetilde{\boldsymbol{\Delta}_{\{i\}\cup I}}, \lambda_i \widetilde{\boldsymbol{\Delta}_{\{j\}\cup I}}\right)$ for all subsets $I \subset \{1..n-k\}$ of size r and all indexes $1 \leqslant i < j < \min(I)$. If we sort the rows of $\mathcal{M}\mathrm{ac}_{(2,1)}(\mathcal{U})$ in decreasing order with respect to the ordering $\ll$ defined by

$$\lambda_i \widetilde{\boldsymbol{\Delta}_J} \ll \lambda_{i'} \widetilde{\boldsymbol{\Delta}_{J'}} \text{ if and only if } (J \prec_{\text{lex}} J') \text{ or } (J = J' \text{ and } i > i'),$$
$$\text{where } J = \{j_1 < \cdots < j_{r+1}\} \prec_{\text{lex}} J' \text{ if and only if } j_t = j'_t\, \forall t > l \text{ and } j_l < j'_l,$$

then it is clear that when we compute a row echelon form without row pivoting, the only rows that can reduce to zero are the rows corresponding to the polynomials $\lambda_i \widetilde{\boldsymbol{\Delta}_{\{j\}\cup I}}$ with $I \subset \{1..n-k\}$, $\#I = r$ and $1 \leqslant i < j < \min(I)$. There are $\sum_{j_2=1}^{n-k-r+1} \binom{j_2-1}{2}\binom{n-k-j_2}{r-1} = \binom{n-k}{r+2}$ such rows. The complementary set is

$$\left\{ \lambda_j \widetilde{\boldsymbol{\Delta}_J} : J \subset \{1..n-k\},\ \#J = r+1 \text{ and } \min(J) \leqslant j \leqslant N \right\}$$

and this is exactly $\mathcal{B}_2$ from Equation (6.4). These equations are already linearly independent because their leading monomials are distinct. To finish the proof, we now construct $\binom{n-k}{r+2}$ independent relations which involve elements outside of $\mathcal{B}_2$.

Lemma 6.3. *For any subset $K \subset \{1..n-k\}$, $\#K = r+2$, we have*

$$\left| \begin{bmatrix} \boldsymbol{\Delta} \\ \sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i \end{bmatrix}_{*,K} \right| = 0. \quad (6.6)$$

Each of these $\binom{n-k}{r+2}$ equations is a relation between the $\lambda_j \boldsymbol{\Delta}_J$'s (hence the $\lambda_j \widetilde{\boldsymbol{\Delta}_J}$'s). Under Assumption 7, all these relations are linearly independent.

Proof. By definition of Modeling 12, the first and the last row of each matrix as in Equation (6.6) are the same. We thus obtain $\binom{n-k}{r+2}$ minors equal to zero. Then, by

Laplace expansion along the last row, the minor corresponding to $K \stackrel{def}{=} \{k_1 < k_2 < \cdots < k_{r+2}\}$ is also equal to

$$\sum_{i=1}^{N} \lambda_i \sum_{u=1}^{r+2} (-1)^{r+u} s_{i,k_u} \boldsymbol{\Delta}_{K\backslash\{k_u\}} = \sum_{u=1}^{r+2} \left((-1)^{w+u} \sum_{i=1}^{N} \lambda_i s_{i,k_u} \right) \boldsymbol{\Delta}_{K\backslash\{k_u\}}. \tag{6.7}$$

Let now $(\boldsymbol{\Delta}_J)_{J\subset\{1..n-k\},\#J=r+1}$ be the sequence associated to $\mathcal{U}$ by sorting the polynomials with respect to the lex ordering on the J's. Combining Equation (6.6) and Equation (6.7) gives the syzygy $\mathcal{G}^K$ such that $(\mathcal{G}^K)_J = 0$ if $J \not\subset K$ and $(\mathcal{G}^K)_J = (-1)^{r+Pos(u,K)} \sum_{i=1}^{N} s_{i,u}\lambda_i$ if $K\backslash J = \{u\}$. In particular, the leftmost non-zero coefficient corresponds to $J = K_1 \stackrel{def}{=} K\backslash\{k_1\}$ and it is equal to

$$(-1)^{r+1} \sum_{i=1}^{N} s_{i,k_1}\lambda_i = (-1)^{w+1} \left(s_{1,k_1} \ \ldots \ s_{N,k_1}\right) \left(\lambda_1 \ \ldots \ \lambda_N\right)^{\mathsf{T}}.$$

This leading position is the same for all syzygies $\mathcal{G}^{\{j\}\cup K_1}$ such that $1 \leqslant j < k_1$. Finally, let $\boldsymbol{L} \in \mathbb{F}_{q^m}^{(n-k-r)\times(n-k-r)}$ as in the proof of Theorem 6.1 and which exists thanks to Assumption 7. We obtain k_1 syzygies from the rows of

$$\boldsymbol{L}_{\{1..k_1\},\{1..k_1\}} \begin{bmatrix} \mathcal{G}^{\{1\}\cup K_1} \\ \vdots \\ \mathcal{G}^{\{k_1\}\cup K_1} \end{bmatrix}.$$

Since the coefficients in position K_1 are equal to the components of

$$(-1)^{r+1} \begin{bmatrix} 1 & \ldots & u_{1,k_1} & \ldots \\ & \ddots & \vdots & \ldots \\ 0 & & 1 & \ldots \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_N \end{bmatrix},$$

it is clear that these syzygies are linearly independent and so are the $\mathcal{G}^{\{j\}\cup K_1}$'s, for $1 \leqslant j \leqslant k_1$. The same eventually holds for the full set $\{\mathcal{G}^K\}_{K\subset\{1..n-k\},\#K=r+2}$. □

In the general case, note that the polynomials in

$$\mathcal{B}_b \stackrel{def}{=} \left\{ \prod_{\min(J)\leqslant j\leqslant N} \lambda_j^{\alpha_j} \widetilde{\boldsymbol{\Delta}_J} : \sum_{j=1}^{N} \alpha_j = b-1 \text{ and } J \subset \{1..n-k\},\ \#J = r+1 \right\}$$

have distinct leading monomials since

$$\mathrm{LM}(\lambda_{j_1}^{\alpha_{j_1}} \cdots \lambda_N^{\alpha_N} \widetilde{\boldsymbol{\Delta}_{\{j_1\}\cup I}}) = \lambda_{j_1}^{\alpha_{j_1}} \cdots \lambda_N^{\alpha_N} \mathrm{LM}(\widetilde{\boldsymbol{\Delta}_{\{j_1\}\cup I}}) = \lambda_{j_1}^{\alpha_{j_1+1}} \cdots \lambda_N^{\alpha_N} c_{I+k}.$$

On the contrary, the polynomials $\lambda_1^{\alpha_1} \cdots \lambda_N^{\alpha_N} \widetilde{\boldsymbol{\Delta}_{\{j_1\}\cup I}}$ such that $j_1 < \min(I)$, $\sum_{i=1}^{N} \alpha_i = b-1$ and $\sum_{i=1}^{j_1-1} \alpha_i \neq 0$ reduce to zero because they are divisible by some $\lambda_i \widetilde{\boldsymbol{\Delta}_J}$ with

$i < \min(J)$ and the latter reduces to zero. This means that $\mathcal{B}_b$ indeed gives a basis. Finally, its cardinality is

$$\sum_{j_2=2}^{n-k-r+1} \binom{n-k-j_2}{r-1} \sum_{j_1=1}^{j_2-1} \binom{N-j_1+1+b-2}{b-1},$$

which is the right-hand side of Equation (6.5). □

Assumption 7 has been used in all our proofs. A nice observation is that it actually holds in the Durandal case.

Lemma 6.4. *Let m a prime number and let $n \in \mathbb{N}$ such that $k = n/2$ is prime. Let $l \in \mathbb{N}$ and let $\boldsymbol{S} \stackrel{def}{=} \left[\boldsymbol{s}_1^\mathsf{T} \ \dots \ \boldsymbol{s}_{lk}^\mathsf{T}\right] \in \mathbb{F}_{q^m}{}^{k \times lk}$ whose columns are the ideal shifts modulo an irreducible polynomial $P \in \mathbb{F}_q[X]$ of l initial syndromes $\boldsymbol{\sigma}_1^\mathsf{T}, \dots, \boldsymbol{\sigma}_l^\mathsf{T}$. Then, there exists an invertible matrix $\boldsymbol{U} \in \mathbb{F}_{q^m}^{k \times k}$ such that*

$$\boldsymbol{U}\boldsymbol{S} = \left[\boldsymbol{I}_k \ *\right].$$

Proof. As $\boldsymbol{S}$ is publicly constructed, we can assume that $\boldsymbol{s}_1^\mathsf{T}, \dots, \boldsymbol{s}_k^\mathsf{T}$ are the ideal shifts of one unique vector $\boldsymbol{\sigma}^\mathsf{T}$. In this case, the leftmost block of size $k \times k$ in $\boldsymbol{S}$ is equal to the ideal matrix $\mathcal{IM}(\boldsymbol{\sigma})^\mathsf{T}$. We also have $\boldsymbol{\sigma} \neq 0$ with overwhelming probability because the double circulant ideal matrix $\boldsymbol{H}$ is generated as random in the scheme. Since P is irreducible over $\mathbb{F}_q$ and as both m and k are prime, [Ara+19c, Lemma 1] shows that there exists a vector $\boldsymbol{u} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{\sigma}\boldsymbol{u} = 1 \bmod P$. This implies that $\mathcal{IM}(\boldsymbol{\sigma})\mathcal{IM}(\boldsymbol{u}) = \boldsymbol{I}_k$ and we deduce Lemma 6.4 with $\boldsymbol{U} \stackrel{def}{=} \mathcal{IM}(\boldsymbol{u})^\mathsf{T}$. □

6.3.3 Coming Back to the Small Field

Similarly to the MaxMinors system over $\mathbb{F}_q$ (Modeling 7), we had difficulty proving results of independence for Modeling 13. Once again, this should not sound surprising because at some point the value of $\mathrm{rk}\left(\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{U}_q)\right)$ will no longer be obtained by a reasoning on the rows. Thus, we assumed that this rank was equal to m times the one of $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{U})$ as long as the latter is smaller than the number of columns and $b < q$. As already mentioned, the second condition is due to the field equations.

Analyzing their contribution remains an open problem. Before studying Modeling 13, an easier task is to consider Modeling 12 reduced modulo these polynomials. We focused on $q = 2$ and we proposed the following conjecture.

Conjecture 6.1. *In Modeling 12 reduced modulo the field equations, the number of linearly independent polynomials at bi-degree $(b, 1)$ when $b \leqslant r + 1$ is conjectured to be*

$$\begin{aligned} N_b^{\mathbb{F}_2} &\stackrel{def}{=} \sum_{d=1}^{b} \sum_{j=1}^{n-k} \binom{j-1}{d-1}\binom{n-k-j}{r-d+1}\binom{N-j}{b-d} \\ &= \sum_{d=1}^{b} (-1)^{d+1} \binom{n-k}{r+d}\binom{N}{b-d}. \end{aligned} \tag{6.8}$$

For any subset $J = \{j_1 < \dots j_{r+1}\} \subset \{1..n-k\}$, multiplying $\widetilde{\boldsymbol{\Delta}_J}$ by all squarefree monomials $\prod_{j_1<j\leqslant N} \lambda_j^{\alpha_j}$ with $\sum_j \alpha_j = b-1$ produces distinct leading monomials which are still squarefree since

$$\mathrm{LM}\left(\prod_{j_1<j\leqslant N} \lambda_j^{\alpha_j} \times \widetilde{\boldsymbol{\Delta}_J}\right) = \lambda_{j_1} \prod_{j_1<j\leqslant N} \lambda_j^{\alpha_j} \times c_{J\setminus\{j_1\}+k}.$$

This already gives a lower bound on $N_b^{\mathbb{F}_2}$. However, if we do the product by squarefree monomials $\lambda_{j_1} \prod_{j_1<j\leqslant N} \lambda_j^{\alpha'_j}$ with $\sum_j \alpha'_j = b-2$, the leading monomial before reduction is divisible by $\lambda_{j_1}^2$ and we do not grasp the one after reduction. Still, we have found experimentally that

- the leading monomial of $\lambda_{j_1} \cdots \lambda_{j_{b-1}} \widetilde{\boldsymbol{\Delta}_J}$ after reduction is $\lambda_{j_1} \cdots \lambda_{j_b} c_{J\setminus\{j_b\}}$,
- for $1 \leqslant d \leqslant b-1$ and $i_d < \cdots < i_{b-1}$ such that $j_{d-1} < i_d < j_d$ the polynomials

  $$\lambda_{j_1} \cdots \lambda_{j_{d-1}} \lambda_{i_d} \dots \lambda_{i_{b-1}} \widetilde{\boldsymbol{\Delta}_J}$$

  reduce to zero.

Conjecture 6.1 follows from these observations since the complementary set has size

$$\sum_{d=1}^{b} \sum_{j_d=1}^{n-k} \underbrace{\binom{j_d-1}{d-1}}_{\substack{\text{number of sets} \\ \{j_1<\cdots<j_{d-1}\} \\ \text{in } \{1..j_d-1\}}} \underbrace{\binom{n-k-j_d}{r+1-d}}_{\substack{\text{number of sets} \\ \{j_{d+1}<\cdots<j_{r+1}\} \\ \text{in } \{j_d+1..n-k\}}} \underbrace{\binom{N-j_d}{b-d}}_{\substack{\text{number of sets} \\ \{i_d<\cdots<i_{b-1}\} \\ \text{in } \{j_d+1..N\}}}.$$

We finish this section by giving the total complexity of our approach. As in Chapter 4, one can use dense or sparse linear algebra techniques to retrieve the kernel vector. Provided that the operating bi-degree $(b,1)$ is known, the cost of the latter can be obtained from Proposition 2.7. From now on, we will always assume that $\boldsymbol{H}_{*,\{k+1..n\}} = \boldsymbol{I}_{n-k}$. In this case, Lemma 6.1 shows that we can take $n_\mu = N\binom{k+1+r}{r}$. Moreover, the number of columns corresponds to the number of monomials, *i.e.*, $M_b \stackrel{def}{=} \binom{n}{r}\binom{N+b-1}{b}$ when $b < q$.

Proposition 6.2. *For $b \in \mathbb{Z}_{>0}$, let N_b as defined in Equation (6.5) and let $M_b = \binom{n}{r}\binom{N+b-1}{b}$. Under Assumption 7 and the hypothesis on the unfolded system stated at the beginning of this section, Modeling 13 can be solved in bi-degree $(b,1)$, $b < q$ whenever $mN_b \geqslant M_b - 1$. In this case, the global cost in $\mathbb{F}_q$-operations is*

$$\mathcal{O}\left(\min\left(N_b M_b^{\omega-1}, N\binom{k+1+r}{r} M_b^2\right)\right), \tag{6.9}$$

where ω is the linear algebra constant.

Over $q = 2$, recall that we consider the full affine Macaulay matrix. The relevant number of columns is thus $M_{\leqslant b}^{\mathbb{F}_2} \stackrel{def}{=} \binom{n}{r} \sum_{b'=1}^{b} \binom{N}{b'}$.

Proposition 6.3. *For $b \in \mathbb{Z}_{>0}$, let $N_b^{\mathbb{F}_2}$ as defined in Equation (6.8), let $N_{\leqslant b}^{\mathbb{F}_2} \stackrel{def}{=} \sum_{j=1}^{b} N_j^{\mathbb{F}_2}$ and let $M_{\leqslant b}^{\mathbb{F}_2} = \binom{n}{r} \sum_{b'=1}^{b} \binom{N}{b'}$. Based on Conjecture 6.1 and the hypothesis on the unfolded system stated at the beginning of this section, Modeling 13 can be solved in bi-degree $(b, 1)$ when $q = 2$ whenever $mN_{\leqslant b}^{\mathbb{F}_2} \geqslant M_{\leqslant b}^{\mathbb{F}_2} - 1$. In this case, the global cost in $\mathbb{F}_q$-operations is*

$$\mathcal{O}\left(\min\left(N_{\leqslant b}^{\mathbb{F}_2}\left(M_{\leqslant b}^{\mathbb{F}_2}\right)^{\omega-1}, N\binom{k+1+r}{r}\left(M_{\leqslant b}^{\mathbb{F}_2}\right)^2\right)\right), \tag{6.10}$$

where ω is the linear algebra constant.

Hybrid techniques can also be applied to Modeling 13. A first one is pretty similar to the strategy adopted by [Bar+20b] on the MaxMinors system (*e.g*, the first method in the underdetermined case given at the very end of Section 3.3.4.3). A second one which does not exploit the structure as strongly as this first method is to perform an exhaustive search on some λ_i variables. For the sake of simplicity, we keep this paragraph short and we refer to Chapter 7 for a more detailed description.

6.3.4 Application to Durandal

We now estimate the complexity of our (hybrid) attack on some parameters. First, note that we do not outperform [Bar+20b] on the original Durandal values which had already been broken by this prior work. However, they correspond to overdetermined RD cases and it is likely that future parameters will be chosen outside of this weak range.

To perform a broader comparison, we have constructed alternative parameters (m, n, k, r, N) which are immune to [Bar+20b] by taking into account the constraints from the Durandal scheme mentioned in [Ara+19b, §6.1]. The empirical ways to avoid the attack of [Bar+20b] seemed to increase the pair (n, k) compared to m or to increase the weight r. Our proposed values attempt to explore these two options. Contrary to [BB21, Table 2], there is no longer mention of the cost of the best attack on PSSI$^+$ because it has been significantly improved in [ADG23]. Note simply that [ADG23] would break the instantiation $d = r$, $\ell' = 1$ given in [BB21] since the best attack on PSSI$^+$ at the time of [Ara+19b] was close to the security target[1]. In other words, one must view this section as a mere comparison between attacks *on the RSL problem* and not as a cryptanalysis of Durandal. We compare ourselves with the RD attack of [Bar+20b] in Table 6.1 while combinatorial RSL techniques including the one of Section 6.4 are irrelevant in this regime.

In Table 6.1, Column "RD" gives the cost of the hybrid approach on Modeling 7 in the underdetermined case. The remaining columns correspond to our method. The three leftmost ones are associated to the strategy by targeting an error of maximal weight r and by shortening as much as possible. The rightmost columns concern the attack by looking for a word of weight $w < r$ and by shortening on a possibly non-maximal

[1] More precisely, the cost was a bit above 192 in a scenario where the adversary has access to 2^{64} signatures.

number $a \geqslant 0$ of columns. Thus, we give the pair (w, a) leading to the best complexity. In both cases, we also indicate the degree b to solve by linearization and the optimal quantities for the hybrid approach. A starred cost value is obtained with the Wiedemann algorithm, otherwise the Strassen algorithm is used. Finally, we write the value of the best strategy in bold text when it improves upon the RD attack.

Table 6.1: Comparison with the RD solver of [Bar+20b] on parameters akin to the ones used in Durandal.

$(m, n, k, r), N$	RD	$w = r$	b	$(\alpha_{\boldsymbol{C}}, \alpha_\lambda)$	$w < r$	b	Value of w	a	$(\alpha_{\boldsymbol{C}}, \alpha_\lambda)$
$(277, 358, 179, 7)$									
$N = k(r-3)$	130	173	2	(0,0)	174*	3	6	60	(0,0)
$N = k(r-2)$	130	147	1	(0,0)	**126**	1	5	37	(0,2)
$N = k(r-1)$	130	145	1	(0,0)	**125**	1	5	19	(0,1)
$(281, 242, 121, 8)$									
$N = k(r-2)$	159	170	2	(0,0)	170*	3	7	70	(0,0)
$N = k(r-1)$	159	144	1	(0,0)	**128**	1	5	27	(2,3)
$(293, 254, 127, 8)$									
$N = k(r-2)$	152	172	2	(0,0)	172*	3	7	73	(0,0)
$N = k(r-1)$	152	145	1	(0,0)	**125**	1	5	28	(1,4)
$(307, 274, 137, 9)$									
$N = k(r-2)$	251	187	2	(0,0)	**187***	3	8	86	(0,0)
$N = k(r-1)$	251	**159**	1	(0,0)	165*	2	8	103	(0,0)

We notice that our complexity is always below the one of the best RD attack of [Bar+20b] when $N = (k-1)r$ and it is very often the case for a slightly smaller number of syndromes. We want to stress that this general improvement is not associated to a precise value of N from which our attack will always be superior but it is particularly obvious when the system can be solved in bi-degree $(1, 1)$. Note also that it is significant on the set of parameters with $r = 9$, which suggests that our attack will probably be more efficient for larger parameter values as well.

6.4 A Combinatorial Approach

In [BBBG23], the smaller RSL instance is solved with combinatorial techniques. There, we focused on subproblems obtained by shortening as much as possible. This is mostly because the number N of syndromes in our proposal was not sufficient to target a weight $< r$ codeword.

Let $a \stackrel{def}{=} \left\lfloor \frac{N}{r} \right\rfloor$ and let $\boldsymbol{H}$ be the matrix of Problem 3.7 still assumed to be in systematic form on its last $n-k$ positions. Let $\widetilde{\boldsymbol{H}} \in \mathbb{F}_{q^m}^{(n-k)\times(n-a)}$ be a matrix obtained from it by deleting a columns outside of these positions. The discussion of Section 6.2

shows that the linear system in the unknowns $\widetilde{\boldsymbol{e}} \in \mathbb{F}_{q^m}^{n-a}$ and $\lambda_i \in \mathbb{F}_q$ given by

$$\widetilde{\boldsymbol{e}}\widetilde{\boldsymbol{H}}^{\mathsf{T}} = \sum_{i=1}^{N} \lambda_i \boldsymbol{s}_i$$

should have roughly one solution corresponding to a word of support $\mathcal{V}$.

To solve it with the weight constraint, we proceed as in Section 3.3.4.1 by guessing a larger subspace F of dimension $r_1 \geqslant r$. However, we cannot use more advanced techniques tailored to RD since our problem is not $\mathbb{F}_{q^m}$-linear. For instance, we can neither assume that $1 \in \mathcal{V}$ as in [GRS16] nor target an F containing a scalar multiple $\alpha\mathcal{V},\ \alpha \in \mathbb{F}_{q^m}^*$ as in [AGHT18]. The basic success probability is thus

$$\frac{\binom{r_1}{r}_q}{\binom{m}{r}_q} \approx q^{-r(m-r_1)}. \tag{6.11}$$

Then, expressing the coordinates of $\widetilde{\boldsymbol{e}}$ in a basis of F yields a linear system over $\mathbb{F}_{q^m}$ with $n-k$ equations and $r_1(n-a)+N$ unknowns searched in $\mathbb{F}_q$. As is standard in combinatorial attacks, the system projected over $\mathbb{F}_q$ is assumed to contain linearly independent equations. Finally, we pick the maximum r_1 to obtain an overdefined system, namely $r_1 \stackrel{def}{=} \min\left(\left\lfloor \frac{m(n-k)-N}{n-a} \right\rfloor, m\right)$ (as a value above m would not make sense). From Equation (6.11), it is then clear that the attack is polynomial if and only if this largest possible value is equal to m, *i.e.*, F is the full space $\mathbb{F}_{q^m}$ and the naive linear system is already overdefined. By recalling that $a = \left\lfloor \frac{N}{r} \right\rfloor$, this is equivalent to

$$\frac{m(n-k)-N}{n-a} \geqslant m \Leftrightarrow m(a-k) \geqslant N \Leftrightarrow \left\lfloor \frac{N}{r} \right\rfloor - \frac{N}{m} \geqslant k. \tag{6.12}$$

It readily implies $\frac{N}{r} - \frac{N}{m} \geqslant k$, hence $N \geqslant kr\frac{m}{m-r}$. However, the converse is not true as $N \geqslant kr\frac{m}{m-r}$ does not always imply Equation (6.12). A sufficient condition for it to hold is $\frac{N}{r} - 1 - \frac{N}{m} \geqslant k$, hence $N \geqslant (k+1)r\frac{m}{m-r}$.

Lemma 6.5. *The proposed combinatorial technique on an RSL instance with parameters (m,n,k,r,N) such that $N \geqslant (k+1)r\frac{m}{m-r}$ is expected to take polynomial time.*

Note that this condition for a polynomial complexity is more easily met than the former bound $N > nr$ given in [GHPT17] for most of the cryptographic parameters. In the general case, we obtain

Proposition 6.4. *The complexity in $\mathbb{F}_q$-operations to solve an RSL instance with parameters (m,n,k,r,N) is given by*

$$\widetilde{\mathcal{O}}\left(q^{r\left(m-\left\lfloor \frac{m(n-k)-N}{n-a} \right\rfloor\right)}\right),$$

where $a \stackrel{def}{=} \left\lfloor \frac{N}{r} \right\rfloor$.

Chapter 7
Rank Decoding Problem, MinRank and Hybrid Techniques

In this chapter, we apply the same proof technique as on Rank Support Learning to obtain more insight on algebraic methods for the RD problem. This lead to the paper [Bar+23].

Our work shows that the estimates of [Bar+20b] regarding the attack by combining the MaxMinors modeling and the Support-Minors modeling to solve underdetermined RD are too optimistic. Indeed, we exhibit linear dependencies between these equations and we introduce another system over $\mathbb{F}_{q^m}$. Finally, we propose an algebraic attack based on this new modeling as an alternative to the former approach of [Bar+20b]. This system has the advantage of being more compact but also easier to analyze.

Another contribution was to generalize the hybrid technique of [Bar+20b, §4.3] on MaxMinors to SM-like systems which still contain a block of minor variables. More precisely, we provide a generic reduction to a smaller MinRank/RD problem which can be used in combination with purely combinatorial techniques. In the context of generic MinRank instances over a small field, it significantly improves the complexity of the former SM approach.

Contents

7.1 Solving RD in the Underdetermined Case

On a Rank Decoding instance with parameters (m, n, k, r) such that $m\binom{n-k-1}{r} \geqslant \binom{n}{r} - 1$ and under Assumption 1, recall that the MaxMinors modeling over $\mathbb{F}_q$ (Modeling 7) can be solved by direct linearization. Since the initial ROLLO and RQC values were chosen in this range, this explains why the corresponding attack by [Bar+20b] strongly affected these schemes. In the underdetermined case, *i.e.*, $m\binom{n-k-1}{r} < \binom{n}{r}$, we had briefly mentioned right below Assumption 1 the two solving strategies considered in [Bar+20b]. The contributions of this chapter will call for a broader exposition.

7.1.1 Hybrid Approach on MaxMinors

The idea of [Bar+20b, §4.3] was to decrease the number of minor variables c_T in Modeling 7 but in a structured way. More precisely, they fix $a \geqslant 0$ columns in the matrix $\boldsymbol{C}$ in order to obtain only $\binom{n-a}{r}$ such unknowns. This is particularly obvious if these columns are set to zero because we only need to keep the $\binom{n-a}{r}$ minors $c_T = |\boldsymbol{C}|_{*,T}$ such that the set T does not meet these columns. In the general case, the number of variables will drop by the same amount if we assume that $\boldsymbol{C}$ is in systematic form on its first r columns as presented in Section 3.3.4.3 and if we fix columns in the $n - r$ rightmost positions. We will not elaborate more here and we refer to Section 7.4 for a more detailed explanation and a generalization of this technique.

Under an analogue of Assumption 1 on the specialized system, the new condition for linearization is now $m\binom{n-k-1}{r} \geqslant \binom{n-a}{r} - 1$. By picking the mininum number a_0 of columns for which it holds, the global complexity in $\mathbb{F}_q$-operations is

$$\mathcal{O}\left(q^{a_0 r} m \binom{n-k-1}{r} \binom{n-a_0}{r}^{\omega-1}\right), \tag{7.1}$$

where ω is the linear algebra constant.

7.1.2 Adding Support-Minors Equations

In addition to Modeling 7, the other method considers the Support-Minors modeling (Modeling 4). This is possible by viewing the RD instance as an inhomogeneous MinRank problem in $\mathbb{F}_q^{m \times n}$ with $K = km$ and with target rank r. The crux is that the blocks of minor variables in both modelings are identical since we put into equation the same low rank matrix. In spite of having a bigger system, another advantage of combining these equations is that we can exploit the sparsity of the SM Macaulay matrix.

A bit more precisely, the authors of [Bar+20b] perform the XL-Wiedemann approach that we have already encountered several times on a set of bi-degree $(b, 1)$ polynomials

obtained by multiplying the MaxMinors equations by degree b monomials in the linear unknowns and the Support-Minors equations by degree $b-1$ monomials in the same variables. This technique requires to grasp the rank of the Macaulay matrix $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{P}_{\mathbb{F}_q} \cup \mathcal{Q})$, where $\mathcal{P}_{\mathbb{F}_q}$ is Modeling 7 and $\mathcal{Q}$ is Modeling 4.

As long as this value is smaller than the number of columns, it is implicitly assumed in [Bar+20b] that

$$\mathrm{rk}\left(\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{P}_{\mathbb{F}_q} \cup \mathcal{Q})\right) = \mathrm{rk}\left(\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{P}_{\mathbb{F}_q})\right) + \mathrm{rk}\left(\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{Q})\right). \tag{7.2}$$

In other words, in this case, the MaxMinors and the Support-Minors systems are supposed to behave independently at higher degree. Still under Assumption 1, note that we trivially have $\mathrm{rk}(\mathcal{P}_{\mathbb{F}_q}) = \dim\langle\mathcal{P}_{\mathbb{F}_q}\rangle_{\mathbb{F}_q}\binom{K+b-1}{b} = m\binom{n-k-1}{r}\binom{K+b-1}{b}$ since the system $\mathcal{P}_{\mathbb{F}_q}$ is simply linear in the minor variables. For the other term in Equation (7.2), [Bar+20b] keep the same analysis used for non-structured MinRank problems.

7.2 Support-Minors Modeling over $\mathbb{F}_{q^m}$

The starting point was to observe that Equation (7.2) did not hold in my practical experiments. This lead me to study the Support-Minors modeling in light of the $\mathbb{F}_{q^m}$-linear structure and to propose another set of equations for the RD problem.

This system is obtained from a slight variation of the argument of [Bar+20b] to generate Support-Minors. We no longer consider the matrix version of

$$\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G} = (s_1, \ldots, s_r)\boldsymbol{C}$$

and we argue more directly that the vector $\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G}$ belongs to the row space of $\boldsymbol{C}$. We then adopt the equations given by the maximal minors of the matrix $\begin{bmatrix}\boldsymbol{x}\boldsymbol{G}+\boldsymbol{y}\\ \boldsymbol{C}\end{bmatrix}$. These polynomials still have an SM-like shape. Indeed, by performing Laplace expansion along the first row, we notice that each of them is affine bilinear in the entries x_i of $\boldsymbol{x}$ for $1 \leqslant i \leqslant k$ and in the maximal minors c_T of $\boldsymbol{C}$ for $T \subset \{1..n\}$, $\#T = r$. Note that the coefficients as well as these former variables are in the extension field.

Modeling 14 (Support-Minors over $\mathbb{F}_{q^m}$ (SM-$\mathbb{F}_{q^m}$)). *The Support-Minors modeling over $\mathbb{F}_{q^m}$ to solve an RD instance with noisy codeword $\boldsymbol{y}$, generator matrix $\boldsymbol{G}$, and target rank r is the system in the unknowns x_i (still referred to as linear variables) and in the maximal minors c_T of $\boldsymbol{C}$, with equations*

$$\left\{ Q_I = \left| \begin{bmatrix}\boldsymbol{x}\boldsymbol{G}+\boldsymbol{y}\\ \boldsymbol{C}\end{bmatrix}_{*,I} \right| : I \subset \{1..n\},\ \#I = r+1 \right\}.$$

This modeling presents the advantage of being much more compact than the original Support-Minors system: the number of linear variables is divided by m and the number of equations is also divided by m. This was in fact my initial motivation to introduce

these equations since I wanted to be able to run practical tests in Magma for higher parameter values.

Independently, we see that the structure of Modeling 14 is similar to the one of Modeling 12 for the RSL problem in the sense that these are bilinear equations which are maximal minors of only one matrix. This is in contrast with the former Support-Minors modeling where there were as many $\boldsymbol{C}_j$ matrices as the initial number of rows in the MinRank problem. In the same way as in Chapter 6, it will make it easier to understand the algebraic relations in our system than in general SM.

7.2.1 Analysis over the Extension Field

We now focus on the polynomials of Modeling 14 when multiplied by linear variables $x_i,\ i \in \{1..k\}$. This part is organized as Section 6.3.2 from the previous chapter by starting with the $b = 1$ case and then by studying equations at higher bi-degree $(b, 1)$. What will be remarkable is the relationship with the MaxMinors modeling over $\mathbb{F}_{q^m}$ (Modeling 6). Thus, let us first separate the polynomials from both systems into different sets by defining for nonnegative integers s and $i \in \{1..k\}$:

$$\begin{aligned}
\mathcal{Q}_s &\stackrel{def}{=} \{Q_I : I \subset \{1..n\},\ \#I = r+1 \text{ and } \#(I \cap \{1..k+1\}) = s\},\\
\mathcal{Q}_{\geqslant s} &\stackrel{def}{=} \{Q_I : I \subset \{1..n\},\ \#I = r+1 \text{ and } \#(I \cap \{1..k+1\}) \geqslant s\},\\
\mathcal{P} &\stackrel{def}{=} \mathcal{P}_{\mathbb{F}_{q^m}},\\
x_i\mathcal{P} &\stackrel{def}{=} \{x_i P : P \in \mathcal{P}\}.
\end{aligned}$$

Contrary to the RSL case where we relied on an assumption (Assumption 7), our results hold regardless of the RD instance. More precisely, we will only need

Fact 3. *The input instance is equivalent to an RD problem where the underlying code $\mathcal{C}$ has a generator matrix $\boldsymbol{G}$ in systematic form, i.e. $\boldsymbol{G} = \begin{bmatrix}\boldsymbol{I}_k & *\end{bmatrix}$, where $\boldsymbol{y} = \begin{pmatrix}\boldsymbol{0}_k & 1 & *\end{pmatrix}$ and where the extended code $\mathcal{C} + \langle \boldsymbol{y} \rangle$ has a parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$ in systematic form, i.e., $\boldsymbol{H}_{\boldsymbol{y}} = \begin{bmatrix} * & \boldsymbol{I}_{n-k-1}\end{bmatrix}$. Then, $\boldsymbol{H} \stackrel{def}{=} \begin{bmatrix}\boldsymbol{H}_{\boldsymbol{y}} \\ \boldsymbol{h}\end{bmatrix}$ is a parity-check matrix for $\mathcal{C}$ for a vector $\boldsymbol{h} = \begin{pmatrix} * & 1 & \boldsymbol{0}_{n-k-1}\end{pmatrix}$ lying in the dual $\mathcal{C}^\perp$. We have $\boldsymbol{y}\boldsymbol{h}^\mathsf{T} = 1$.*

Proof. Up to a permutation of the coordinates, we can assume that $\boldsymbol{G}$ is in systematic form $\boldsymbol{G} = \begin{bmatrix}\boldsymbol{I}_k & *\end{bmatrix}$, and up to the addition of an element in $\mathcal{C}$ that $\boldsymbol{y} = (\boldsymbol{0}_k\ *)$. As $\boldsymbol{y}$ contains an error of weight r, it is non-zero, so that up to a permutation of the coordinates of the code and up to the multiplication by a constant in $\mathbb{F}_{q^m}$, we assume that $\boldsymbol{y}$ has the given shape $\boldsymbol{y} = \begin{pmatrix}\boldsymbol{0}_k & 1 & *\end{pmatrix}$. Now, if $\widetilde{\boldsymbol{G}_{\boldsymbol{y}}} \stackrel{def}{=} \begin{bmatrix}\boldsymbol{I}_{k+1} & \boldsymbol{A}\end{bmatrix}$ is a generator matrix of $\mathcal{C}_{\boldsymbol{y}}$ in systematic form, then $\boldsymbol{H}_{\boldsymbol{y}} \stackrel{def}{=} \begin{bmatrix}-\boldsymbol{A}^\mathsf{T} & \boldsymbol{I}_{n-k-1}\end{bmatrix}$ is suitable. By considering an $\boldsymbol{h}$ linearly independent from the rows of $\boldsymbol{H}_{\boldsymbol{y}}$ and such that $\boldsymbol{y}\boldsymbol{h}^\mathsf{T} \neq 0$, any linear combination between $\boldsymbol{h}$ and the rows of $\boldsymbol{H}_{\boldsymbol{y}}$ still satisfies the same properties. Therefore, we may assume that $\boldsymbol{h} = \begin{pmatrix} * & \boldsymbol{0}_{n-k-1}\end{pmatrix}$, and moreover we have $\boldsymbol{y}\boldsymbol{h}^\mathsf{T} = h_{k+1} \neq 0$. Thus, the vector $h_{k+1}^{-1}\boldsymbol{h}$ is indeed of the form $\begin{pmatrix} * & 1 & \boldsymbol{0}_{n-k-1}\end{pmatrix}$. □

Lemma 7.1. *Let $\boldsymbol{H_y}$ be the matrix of Fact 3. For any subset $T \subset \{1..n-k-1\}$, we have*

$$\begin{aligned} |(\boldsymbol{H_y})_{T,T+k+1}| &= 1, \\ |(\boldsymbol{H_y})_{T,I}| &= 0 \ \text{ if } I \cap \{k+2..n\} \nsubseteq T+k+1. \end{aligned}$$

Proof. This immediately follows from the fact that $\boldsymbol{H_y}$ is in systematic form in its last $n-k-1$ columns. □

In affine bi-degree $(1,1)$, the following Propositions 7.1, 7.2 and 7.3 will show that

$$\mathcal{Q}_0 \subset \langle \mathcal{Q}_1, \mathcal{Q}_{\geqslant 2} \rangle_{\mathbb{F}_q},$$

$$\left\langle \mathcal{P}, \bigcup_{1 \leqslant i \leqslant k} x_i \mathcal{P}, \mathcal{Q}_{\geqslant 2} \right\rangle_{\mathbb{F}_q} = \langle \mathcal{Q}_1, \mathcal{Q}_{\geqslant 2} \rangle_{\mathbb{F}_q},$$

and that $\mathcal{P} \cup \bigcup_{1 \leqslant i \leqslant k} x_i \mathcal{P} \cup \mathcal{Q}_{\geqslant 2}$ is a basis of the latter space. These results can be seen as the analogue of Theorem 6.1 for Modeling 12. To state them, we will consider the same grevlex ordering as used in its proof, *i.e.*, such that $c_T \prec x_k \prec \cdots \prec x_1$ and where the c_T's are ordered with a reverse lexicographical order according to T.

Proposition 7.1. *The polynomials in $\mathcal{Q}_0$ can be obtained as linear combinations between the polynomials in $\mathcal{Q}_{\geqslant 1}$. More precisely, for any subset $T \subset \{1..n-k-1\}$, $\#T = r+1$, we have*

$$Q_{T+k+1} = - \sum_{Q_I \in \mathcal{Q}_{\geqslant 1}} |(\boldsymbol{H_y})_{T,I}| \, Q_I. \tag{7.3}$$

Proof. We first observe that any polynomial Q in $\mathcal{Q}_0$ is of the form Q_{T+k+1} for some $T \subset \{1..n-k-1\}$, $\#T = r+1$. Using the Cauchy-Binet formula gives

$$\left| \begin{bmatrix} \boldsymbol{xG} + \boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} (\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}})_{*,T} \right| = \sum_{\substack{I \subset \{1..n\} \\ \#I = r+1}} |(\boldsymbol{H_y})_{T,I}| \, Q_I,$$

and this minor is equal to zero as $(\boldsymbol{xG} + \boldsymbol{y})\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}} = 0$. Finally, we apply Lemma 7.1 to argue that $|(\boldsymbol{H_y})_{T,T+k+1}| = 1$ and that $|(\boldsymbol{H_y})_{T,I}| = 0$ for $I \subset \{k+2..n\}$, $I \neq T+k+1$. We obtain Equation (7.3) since the non-zero terms in the sum correspond to Q appearing with coefficient 1 and to the Q_I's in $\mathcal{Q}_{\geqslant 1}$. □

Proposition 7.2. *For any subset $I \subset \{1..n\}$, $\#I = r+1$ such that $Q_I \in \mathcal{Q}_{\geqslant 2}$ and $i_1 \stackrel{def}{=} \min(I)$, the leading term of Q_I is*

$$LT(Q_I) = x_{i_1} c_{I \setminus \{i_1\}}.$$

Moveover, for any subset $J \subset \{1..n-k-1\}$, $\#J = r$, we have

$$LT(P_J) = c_{J+k+1}.$$

Finally, the variable c_{J+k+1} only appears as the leading term of P_J and it is not present in any of the polynomials in $\mathcal{Q}_{\geqslant 2} \cup \mathcal{P} \setminus \{P_J\}$.

Proof. The statement on the MaxMinors polynomials P_J is already known so let us focus on the Q_I's. By definition of $\mathcal{Q}_{\geqslant 2}$, a subset I such that $Q_I \in \mathcal{Q}_{\geqslant 2}$ satisfies $i_1 = \min(I) \leqslant k$. Computing by Laplace expansion along the first row then gives

$$Q_I = \left| \begin{bmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix}_{*,I} \right| = \sum_{i_u \in I} (-1)^{1+u} \left(\boldsymbol{x}\boldsymbol{G}_{*,i_u} + y_{i_u} \right) c_{I\setminus\{i_u\}}.$$

If $\boldsymbol{G}$ and $\boldsymbol{y}$ are as in Fact 3 and for any $i_u \in I^- = I \cap \{1..k\}$ (and at least $i_1 \in I^-$ by assumption), we obtain $\boldsymbol{x}\boldsymbol{G}_{*,i_u} + \boldsymbol{y}_{i_u} = x_{i_u}$. Then, for $u \in \{1..r+1\}$, let $I_u \stackrel{def}{=} I\setminus\{i_u\}$, so that $I_1 > I_2 > \cdots > I_{r+1}$ according to the reverse lexicographical ordering. The ordered terms in Q_I are thus

$$Q_I = x_{i_1} c_{I_1} \underbrace{-\boldsymbol{x}\boldsymbol{G}_{*,i_2} c_{I_2} + \cdots + (-1)^r \boldsymbol{x}\boldsymbol{G}_{*,i_{r+1}} c_{I_{r+1}}}_{\text{smaller terms of degree 2}} \underbrace{-y_{i_2} c_{I_2} + \cdots + (-1)^r y_{i_{r+1}} c_{I_{r+1}}}_{\text{smaller terms of degree 1}}.$$

This shows in particular that $\mathrm{LT}(Q_I) = x_{i_1} c_{I_1}$. For the last point, we observe that $\{i_1 < i_2\} \subset \{1..k+1\}$ still by definition of $\mathcal{Q}_{\geqslant 2}$. This implies that for any $i_u \in I$, the set $I\setminus\{i_u\}$ is not included in $\{k+2..n\}$, and finally that the variables $\{c_{J+k+1}\}_{J\subset\{1..n-k-1\},\ \#J=r}$ do not appear in Q_I. □

Corollary 7.1. *The polynomials in $\mathcal{P} \cup \mathcal{Q}_{\geqslant 2}$ are linearly independent.*

Proposition 7.3. *For any subset $J \subset \{1..n-k-1\},\ \#J = r$ and for any $i \in \{1..k\}$, we have*

$$P_J = Q_{\{k+1\}\cup(J+k+1)} + \sum_{Q_I \in \mathcal{Q}_{\geqslant 2}} (-1)^r \left| \boldsymbol{H}_{J\cup\{n-k\},I} \right| Q_I, \tag{7.4}$$

$$x_i P_J = Q_{\{i\}\cup(J+k+1)} + \sum_{Q_I \in \mathcal{Q}_{\geqslant 2},\ i\in I} (-1)^{1+\mathrm{Pos}(i,I)} \left| (\boldsymbol{H}_{\boldsymbol{y}})_{J,I\setminus\{i\}} \right| Q_I, \tag{7.5}$$

where $\mathrm{Pos}(i_u, I) = u$ *for* $I = \{i_1, \ldots, i_{r+1}\}$ *such that* $i_1 < \cdots < i_{r+1}$.

Proof. Let us consider the minor $\left| \begin{bmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} (\boldsymbol{H}^{\mathsf{T}})_{*,J\cup\{n-k\}} \right|$. On the one hand, the Cauchy-Binet formula gives

$$\left| \begin{bmatrix} \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} (\boldsymbol{H}^{\mathsf{T}})_{*,J\cup\{n-k\}} \right| = \sum_{I\subset\{1..n\},\#I=r+1} \left| \boldsymbol{H}_{J\cup\{n-k\},I} \right| Q_I. \tag{7.6}$$

On the other hand, we use the particular shapes of $\boldsymbol{H}$, $\boldsymbol{y}$ and $\boldsymbol{h}$ given in Fact 3:

$$\begin{aligned} \boldsymbol{H} &= \begin{bmatrix} \boldsymbol{H}_{\boldsymbol{y}} \\ \boldsymbol{h} \end{bmatrix}, \\ \boldsymbol{y} &= \begin{pmatrix} \boldsymbol{0}_k & 1 & * \end{pmatrix}, \\ \boldsymbol{h} &= \begin{pmatrix} * & 1 & \boldsymbol{0}_{n-k-1} \end{pmatrix}, \end{aligned}$$

to obtain

$$\begin{bmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} \boldsymbol{H}^\intercal = \begin{bmatrix} \boldsymbol{yH}^\intercal \\ \boldsymbol{CH}^\intercal \end{bmatrix} = \begin{bmatrix} \boldsymbol{yH}_{\boldsymbol{y}}^\intercal & \boldsymbol{yh}^\intercal \\ \boldsymbol{CH}_{\boldsymbol{y}}^\intercal & \boldsymbol{Ch}^\intercal \end{bmatrix} = \begin{bmatrix} \boldsymbol{0}_{n-k-1} & 1 \\ \boldsymbol{CH}_{\boldsymbol{y}}^\intercal & \boldsymbol{Ch}^\intercal \end{bmatrix}.$$

This minor is thus also equal to

$$\left| \begin{bmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} \boldsymbol{H}^\intercal_{*,J\cup\{n-k\}} \right| = \left| \begin{bmatrix} \boldsymbol{0} & 1 \\ \boldsymbol{CH}_{\boldsymbol{y}}^\intercal & \boldsymbol{Ch}^\intercal \end{bmatrix}_{*,J\cup\{n-k\}} \right| = (-1)^r \left| \boldsymbol{C}(\boldsymbol{H}_{\boldsymbol{y}}^\intercal)_{*,J} \right| = (-1)^r P_J.$$

Then, we use

$$\left| \boldsymbol{H}_{J\cup\{n-k\},I} \right| = \begin{cases} 0 & \text{if } I \cap \{k+2..n\} \nsubseteq J+k+1, \\ (-1)^r & \text{if } I = \{k+1\} \cup (J+k+1), \end{cases}$$

to remove zero terms in Equation 7.6. We finally get

$$P_J = \underbrace{Q_{\{k+1\}\cup(J+k+1)}}_{\in\mathcal{Q}_1} + (-1)^r \sum_{Q_I\in\mathcal{Q}_{\geqslant 2}} \left| \boldsymbol{H}_{J\cup\{n-k\},I} \right| Q_I.$$

Let us now prove the second equation. For $i_1 \in \{1..k\}$, we denote by $\boldsymbol{g}_{i_1} \stackrel{def}{=} \boldsymbol{G}_{\{i_1\},*}$ the i_1-th row of the generator matrix $\boldsymbol{G}$. We then consider the matrix $\boldsymbol{H}_{i_1} \in \mathbb{F}_{q^m}^{(n-k-1)\times n}$ defined by $\boldsymbol{H}_{i_1}^\intercal = \left[\boldsymbol{H}_{\boldsymbol{y}}^\intercal \ \boldsymbol{\varepsilon}_{i_1}^\intercal\right]$, where $\boldsymbol{\varepsilon}_{i_1}$ is the i_1-th canonical basis vector in $\mathbb{F}_q^n$. This is a parity-check matrix for the $\mathbb{F}_{q^m}$-linear code $\mathcal{C}_{i_1}$ generated by $\left\{\boldsymbol{y}, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{i_1-1}, \boldsymbol{g}_{i_1+1}, \ldots, \boldsymbol{g}_k\right\}$. Since $\boldsymbol{g}_{i_1}\boldsymbol{\varepsilon}_{i_1}^\intercal = 1$, we have

$$\begin{bmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} \boldsymbol{H}_{i_1}^\intercal = \begin{bmatrix} x_{i_1}\boldsymbol{g}_{i_1}\boldsymbol{H}_{i_1}^\intercal \\ \boldsymbol{CH}_{i_1}^\intercal \end{bmatrix} = \begin{bmatrix} \boldsymbol{0} & x_{i_1} \\ \boldsymbol{CH}_{\boldsymbol{y}}^\intercal & \boldsymbol{C\varepsilon}_{i_1}^\intercal \end{bmatrix}.$$

For any $J \subset \{1..n-k-1\},\ \#J = r$, we then compute

$$\left| \begin{bmatrix} \boldsymbol{xG}+\boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix} (\boldsymbol{H}_{i_1}^\intercal)_{*,J\cup\{n-k\}} \right| = \left| \begin{bmatrix} \boldsymbol{0} & x_{i_1} \\ \boldsymbol{CH}_{\boldsymbol{y}}^\intercal & \boldsymbol{Ch}_{i_1}^\intercal \end{bmatrix}_{*,J\cup\{n-k\}} \right|$$

$$= \sum_{I\subset\{1..n\},\#I=r+1} \left| (\boldsymbol{H}_{i_1})_{J\cup\{n-k\},I} \right| Q_I = (-1)^r x_{i_1} \left| \boldsymbol{C}(\boldsymbol{H}_{\boldsymbol{y}}^\intercal)_{*,J} \right| = (-1)^r x_{i_1} P_J.$$

By Laplace expansion along the last row, we have $\left|(\boldsymbol{H}_{i_1})_{J\cup\{n-k\},I}\right| = 0$ if $i_1 \notin I$ and $\left|(\boldsymbol{H}_{i_1})_{J\cup\{n-k\},I}\right| = (-1)^{r+1+\mathrm{Pos}(i_1,I)} \left|(\boldsymbol{H}_{\boldsymbol{y}})_{J,I\setminus\{i_1\}}\right|$ if $i_1 \in I$, where $\mathrm{Pos}(i_1, I)$ denotes the position of i_1 in the ordered set I. From that, we can deduce:

$$\begin{aligned} x_{i_1} P_J &= \sum_{I\subset\{1..n\},\#I=r+1,i_1\in I} (-1)^{1+\mathrm{Pos}(i_1,I)} \left|(\boldsymbol{H}_{\boldsymbol{y}})_{J,I\setminus\{i_1\}}\right| Q_I \\ &= Q_{\{i_1\}\cup(J+k+1)} + \sum_{Q_I\in\mathcal{Q}_{\geqslant 2},i_1\in I} (-1)^{1+\mathrm{Pos}(i_1,I)} \left|(\boldsymbol{H}_{\boldsymbol{y}})_{J,I\setminus\{i_1\}}\right| Q_I. \end{aligned}$$

□

Corollary 7.2. *The polynomials in $\mathcal{Q}_1$ generate the same $\mathbb{F}_{q^m}$-vector space as the set of equations $\mathcal{P} \cup \bigcup_{i=1}^{k} x_i\mathcal{P}$ taken modulo the polynomials in $\mathcal{Q}_{\geqslant 2}$.*

The difference with Modeling 12 is that all equations are not linearly independent and that we observe degree falls. More precisely, there are $\binom{n-k-1}{r}$ degree falls from bi-degree $(1,1)$ to bi-degree $(0,1)$ that give the P_J polynomials. If we then eliminate c_T variables using those linear equations, we get new reductions to zero which correspond to the x_iP_J's.

Concretely, our discussion shows that the relevant system to start with is $\mathcal{Q}_{\geqslant 2}$. Note that it does not contain the variables c_{J+k+1} for $J \subset \{1..n-k-1\}$, $\#J = r$. The following Theorem 7.1 provides a basis in bi-degree $(b,1)$ which is of the same nature as the one we found for Modeling 12, see Theorem 6.2.

Theorem 7.1. *For any $b \geqslant 1$, the $\mathbb{F}_{q^m}$-vector space generated by the polynomials in $\mathcal{Q}_{\geqslant 2}$ augmented in bi-degree $(b,1)$ by multiplying by monomials of degree $b-1$ in the x_i variables has basis*

$$\mathcal{B}_b \stackrel{def}{=} \left\{ \left(\prod_{\min(I) \leqslant j \leqslant k} x_j^{\alpha_j} \right) Q_I : Q_I \in \mathcal{Q}_{\geqslant 2} \text{ and } \sum_{\min(I) \leqslant j \leqslant k} \alpha_j = b-1 \right\}. \tag{7.7}$$

This space is of dimension

$$N_b^{\mathbb{F}_{q^m}} \stackrel{def}{=} \sum_{i=1}^{k} \binom{n-i}{r} \binom{k+b-1-i}{b-1} - \binom{n-k-1}{r} \binom{k+b-1}{b}. \tag{7.8}$$

Proof. The set $\mathcal{B}_b$ defined by Equation (7.7) clearly contains linearly independent polynomials since the leading terms are all different. More precisely,

$$\mathrm{LT}({x_{i_1}}^{\alpha_{i_1}} \dots {x_k}^{\alpha_k} Q_I) = {x_{i_1}}^{\alpha_{i_1}+1} \dots {x_k}^{\alpha_k} c_{I\setminus\{i_1\}}.$$

Its cardinality is the number of sets I and $(\alpha_{i_1}, \dots, \alpha_k)$ with sum equal to $b-1$, hence

$$\sum_{i_1=1}^{k} \sum_{i_2=i_1+1}^{k+1} \binom{n-i_2}{r-1} \binom{k-i_1+1+b-2}{b-1}.$$

This gives Equation (7.8) by considering the identities $\sum_{i_2=i_1+1}^{k+1} \binom{n-i_2}{r-1} = \binom{n-i_1}{r} - \binom{n-k-1}{r}$ and $\sum_{i_1=1}^{k} \binom{k-i_1+1+b-2}{b-1} = \binom{k+b-1}{b}$.

It remains to see that $\mathcal{B}_b$ generates the desired vector space. As in the proof of Theorem 6.2, it will be sufficient to show that the polynomials x_jQ_I for $Q_I \in \mathcal{Q}_{\geqslant 2}$, $j \in \{1..\min(I)-1\}$ reduce to zero modulo $\mathcal{B}_2$. On the one hand, the number of such polynomials is equal to the number of subsets $K = \{k_1 < k_2 < \dots < k_{r+2}\} \subset \{1..n\}$ such that $k_3 \leqslant k+1$. On the other hand, we can construct the same number of independent

syzygies between the polynomials at bi-degree $(2,1)$. Note that for any such K, we have the relation

$$\left|\begin{bmatrix} \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{C} \end{bmatrix}_{*,K}\right| = 0.$$

By Laplace expansion along the first row, we also obtain

$$0 = x_{k_1} Q_{\{k_2,\ldots,k_{r+2}\}} - \sum_{u=2}^{r+2} (-1)^u \left(\sum_{j=1}^{k} x_j \boldsymbol{G}_{j,k_u} + y_{k_u}\right) Q_{K\setminus\{k_u\}}.$$

Since $|K \cap \{1..k+1\}| \geqslant 3$, these cancellations are syzygies between the relevant Q_I, *i.e.*, those such that $|I \cap \{1..k+1\}| \geqslant 2$. It remains to show that they are linearly independent. For that purpose, we keep the proof structure as the one of Lemma 6.3 and we order the Q_I's according to a grevlex order on the subsets I's. The syzygy associated to K is given by

$$\mathcal{G}^K \stackrel{def}{=} \left(\underbrace{0}_{I \not\subset K}, \underbrace{(-1)^{1+u} \sum_{j=1}^{k} x_j \boldsymbol{G}_{j,k_u} + \boldsymbol{y}_{k_u}}_{K\setminus I=\{k_u\}} \right)_{I\subset\{1..n\},\ \#I=r+1}.$$

The largest subset I such that the coefficient in front of Q_I in $\mathcal{G}^K$ is non-zero is $I = K_1 \stackrel{def}{=} K\setminus\{k_1\}$ and this coefficient is equal to x_{k_1}. The syzygies which have the same leading position Q_{K_1} as $\mathcal{G}^K$ are the $\mathcal{G}^{K_1\cup\{j\}}$'s for $j \in \{1..k_1-1\}$. Finally, the highest degree part in the coefficient in front of Q_{K_1} in $\mathcal{G}^{K_1\cup\{j\}}$ is x_j, which shows that all these syzygies are linearly independent. □

Since Theorem 7.1 holds regardless of the value of b, this means that the dimension $N_b^{\mathbb{F}_{q^m}}$ will always be *smaller than or equal to* the number of monomials

$$M_b^{\mathbb{F}_{q^m}} \stackrel{def}{=} \binom{k+b-1}{b}\left(\binom{n}{r} - \binom{n-k-1}{r}\right).$$

Alternatively, by a simple computation, we can prove that $\forall b \in \mathbb{Z}_{>0},\ N_b^{\mathbb{F}_{q^m}} < M_b^{\mathbb{F}_{q^m}} - 1$. A consequence is that the XL strategy cannot succeed on $\mathcal{Q}_{\geqslant 2}$. The deeper reason is because we have not taken into account the fact that the c_T variables are searched in $\mathbb{F}_q$ (the overall system is not zero-dimensional)

7.2.2 Coming Back to the Small Field

To obtain more equations, a natural idea is to unfold the system. However, in our case, the linear variables x_j belong to the extension field. Thus, we start by expressing them in the basis $\boldsymbol{\beta}$ as $x_j \stackrel{def}{=} \sum_{i=1}^{m} \beta_i x_{i,j}$, which yields m times more unknowns $x_{i,j}$'s over $\mathbb{F}_q$. Finally, for ease of exposition, we adopt the dual basis $\boldsymbol{\beta}' = \boldsymbol{\beta}^*$ in the unfolding procedure.

Modeling 15 (Support-Minors over $\mathbb{F}_q$ (SM-$\mathbb{F}_q$)). *Let $\boldsymbol{\beta}$ be an arbitrary $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ and let $\boldsymbol{\beta}^* = (\beta_1^\star, \dots, \beta_m^\star)$ be the dual basis. Let Tr be the trace operation defined in Section 3.3.4.3. The Support-Minors modeling over $\mathbb{F}_q$ is the system in the $x_{i,j}$ variables $x_j = \sum_{i=1}^m \beta_i x_{i,j}$ and in the c_T variables, defined by $\{R_{i,I}\}_{1\leqslant i\leqslant m,\ I\subset\{1..n\},\ \#I=r+1}$, where*

$$R_{i,I} \stackrel{def}{=} Tr(\beta_i^\star Q_I) \bmod \{c_T^q - c_T,\ x_{i,j}^q - x_{i,j}\}.$$

For the first time in this manuscript, we can control the rank of an unfolded system. This is in contrast with what we observed on both Modelings 7 and 13.

Proposition 7.4. *For any subset $I \subset \{1..n\}$, $\#I = r+1$, $i_1 \stackrel{def}{=} \min(I)$, such that $Q_I \in \mathcal{Q}_{\geqslant 2}$ and for any $i \in \{1..m\}$, we have*

$$LT(R_{i,I}) = x_{i,i_1} c_{I\setminus\{i_1\}}.$$

Proof. This directly follows from Proposition 7.2 showing that $\mathrm{LT}(Q_I) = x_{i_1} c_{I\setminus\{i_1\}}$ and from our new definition of linear variables yielding $x_{i_1} c_{I\setminus\{i_1\}} = \sum_{i=1}^m \beta_i x_{i,i_1} c_{I\setminus\{i_1\}}$. □

Corollary 7.3. *Unfolding $\mathcal{Q}_{\geqslant 2}$ gives linearly independent polynomials over $\mathbb{F}_q$.*

Finally, we show that Modelings 14 and 15 really deserve their names by proving that $R_{i,I} = Q_{i,I}$ for all $1 \leqslant i \leqslant m$ and all $I \subset \{1..n\}$, $\#I = r+1$, where $\{Q_{i,I}\}_{1\leqslant i\leqslant m,\ I\subset\{1..n\},\ \#I=r+1}$ is the genuine Support-Minors system of [Bar+20b] applied to the underlying MinRank problem. Let us recall its definition below. We consider the matrix code $\mathcal{C}_{\mathrm{mat}}$ isomorphic to $\mathcal{C}$ with basis $\{\boldsymbol{M}_{i,j}\}_{1\leqslant i\leqslant m,\ 1\leqslant j\leqslant k} \stackrel{def}{=} \{\mathrm{Mat}(\beta_i \boldsymbol{G}_{j,*})\}_{1\leqslant i\leqslant m,\ 1\leqslant j\leqslant k}$ together with the matrix $\boldsymbol{M}_0 \stackrel{def}{=} \mathrm{Mat}(\boldsymbol{y})$. As we have already seen, solving RD with weight r is equivalent to solving the inhomogeneous MinRank instance with target rank r, $K = km$ and matrices

$$(\boldsymbol{M}_0; \boldsymbol{M}_{1,1}, \dots, \boldsymbol{M}_{m,k}) \in \mathbb{F}_q^{m\times n}. \tag{7.9}$$

Notation 3. *For $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$, we denote by $\mathrm{Tr}(\boldsymbol{x})$ the vector $(\mathrm{Tr}(x_i))_{1\leqslant i\leqslant n}$ where the trace is applied componentwise. For a matrix $\boldsymbol{A}$, we denote by $\mathrm{Tr}(\boldsymbol{A})$ the matrix whose entry in row i and column j is equal to $\mathrm{Tr}(\boldsymbol{A}_{i,j})$.*

From the linearity of the trace over $\mathbb{F}_q$ and with these notation, we obtain

$$\forall i \in \{1..m\},\ \mathrm{Tr}(\beta_i^\star \boldsymbol{x}) = \mathrm{Mat}(\boldsymbol{x})_{i,*}, \tag{7.10}$$

$$\forall \boldsymbol{C} \in \mathbb{F}_q^{a\times b},\ \forall \boldsymbol{M} \in \mathbb{F}_{q^m}^{b\times c},\ \mathrm{Tr}(\boldsymbol{C}\boldsymbol{M}) = \boldsymbol{C}\,\mathrm{Tr}(\boldsymbol{M}). \tag{7.11}$$

Using Equation (7.10) and for $i \in \{1..m\}$, the i-th row of the MinRank solution associated to the low rank vector $\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G}$ is equal to

$$\boldsymbol{r}_i \stackrel{def}{=} \mathrm{Tr}\left(\beta_i^\star\,(\boldsymbol{y} + \boldsymbol{x}\boldsymbol{G})\right). \tag{7.12}$$

Proposition 7.5. *Let* $\{Q_{i,I}\}_{1\leqslant i\leqslant m,\ I\subset\{1..n\},\ \#I=r+1}$ *be the Support-Minors modeling of [Bar+20b] applied to the inhomogeneous MinRank problem with rank* r*,* $K = km$ *and with matrices given by Equation (7.9). Let* $\{R_{i,I}\}_{1\leqslant i\leqslant m,\ I\subset\{1..n\},\ \#I=r+1}$ *be Modeling 14. For any* $i \in \{1..m\}$ *and any* $I \subset \{1..n\}$*,* $\#I = r + 1$*, we have*

$$R_{i,I} = Q_{i,I}.$$

Proof. Let I_q be the ideal generated by the field equations $\{c_T^q - c_T,\ x_{i,j}^q - x_{i,j}\}$. We use the linearity of the determinant according to the first row and the properties of Tr to obtain

$$\begin{aligned} R_{i,I} = \mathrm{Tr}\left(\beta_i^\star \boldsymbol{Q}_I\right) \mod I_q &= \mathrm{Tr}\left(\left|\begin{bmatrix}\beta_i^\star\left(\boldsymbol{y}+\boldsymbol{x}\boldsymbol{G}\right)\\ \boldsymbol{C}\end{bmatrix}_{*,I}\right|\right) \mod I_q \\ &= \left|\begin{bmatrix}\mathrm{Tr}\left(\beta_i^\star\left(\boldsymbol{y}+\boldsymbol{x}\boldsymbol{G}\right)\right)\\ \boldsymbol{C}\end{bmatrix}_{*,I}\right| = \left|\begin{bmatrix}\boldsymbol{r}_i\\ \boldsymbol{C}\end{bmatrix}_{*,I}\right| = Q_{i,I}. \end{aligned}$$

The second last equality follows from Equation (7.12). □

7.3 New Combined Approach

This section presents another algebraic method for the RD problem based on Modeling 14. We will add to this system the MaxMinors equations unfolded over $\mathbb{F}_q$ (Modeling 7) as we have just observed that the mere P_J polynomials over the extension field were not enough to obtain a zero-dimensional ideal. Also, we will not unfold the equations of SM-$\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ to avoid dealing with a system with m times more linear unknowns. This increased compactness makes that even if our modeling were to be solved at higher degree than the former SM-$\mathbb{F}_q$, it may still perform better from a complexity point of view. Note finally that the analysis of this second system at arbitrary bi-degree $(b, 1)$, $b \geqslant 2$ remains an open problem.

In other words, we consider the set $\mathcal{T} \stackrel{def}{=} \left\{\widetilde{Q_I} : Q_I \in \mathcal{Q}_{\geqslant 2}\right\}$, where $\widetilde{Q_I}$ is the normal form of Q_I modulo the $P_{i,J}$ polynomials[1]. We may also refer to it as the SM-$\mathbb{F}_{q^m}^+$ system. Its elements do not involve any c_T variable which is a leading term in Modeling 7. As before, we construct and study the Macaulay matrix $\mathcal{M}\mathrm{ac}_{(b,1)}(\mathcal{T})$. Note that the sparsity of the initial equations Q_I's is destroyed by the reduction step. Thus, we will only try to apply dense linear algebra techniques. In this matrix, the relevant number of columns is equal to

$$M_b^{\mathbb{F}_q} = \binom{k+b-1}{b}\left(\binom{n}{r} - m\binom{n-k-1}{r}\right). \tag{7.13}$$

Proposition 7.6 contains our estimate for the dimension of its rowspace when the number of rows is smaller than $M_b^{\mathbb{F}_q}$. It is based on Assumption 1 and on a counting argument for the number of syzygies when we add the $P_{i,J}$ equations (Conjecture 7.1 below).

[1] Since they are linear, a Gröbner basis of them is simply an echelon form.

Proposition 7.6. *The rowspace of $\mathcal{M}ac_{(b,1)}(\mathcal{T})$ has generic dimension*

$$N_b^{\mathbb{F}_q} \stackrel{def}{=} N_b^{\mathbb{F}_{q^m}} - N_{b,syz}^{\mathbb{F}_q}$$

when $N_b^{\mathbb{F}_q} < M_b^{\mathbb{F}_q}$, where $N_b^{\mathbb{F}_{q^m}}$ is defined in Equation (7.8),

$$N_{b,syz}^{\mathbb{F}_q} \stackrel{def}{=} (m-1)\sum_{i=1}^{b}(-1)^{i+1}\binom{k+b-i-1}{b-i}\binom{n-k-1}{r+i}, \tag{7.14}$$

and where $M_b^{\mathbb{F}_q}$ is defined in Equation (7.13).

The $N_{b,\text{syz}}^{\mathbb{F}_q}$ term is the expected number of linearly independent syzygies due to the $P_{i,J}$'s. However, similarly to what we have seen in Modeling 13, we cannot obtain an exact value. This is because there is now a solving degree above which any attempt for a general estimate will fail. Our starting point are the following cancellations in bi-degree $(1,1)$:

Proposition 7.7. *For any subset $T \subset \{1..n-k-1\}$, $\#T = r+1$ and any $i \in \{1..m\}$, we have the relation with coefficients in $\mathbb{F}_q$:*

$$\mathrm{Tr}(\beta_i^\star)\widetilde{Q_{T+k+1}} + \sum_{\substack{I\subset\{1..n\}\\ \#I=r+1\\ I\cap\{k+1..n\}\subsetneq T+k+1}} \mathrm{Tr}(\beta_i^\star\,|(\boldsymbol{H_y})_{T,I}|)\widetilde{Q_I} = 0. \tag{7.15}$$

Proof. For a square matrix $\boldsymbol{M}$ over $\mathbb{F}_{q^m}$ and for $\ell \in \mathbb{N}$, we consider the matrix $\boldsymbol{M}^{[\ell]}$ obtained by iterating the Frobenius map ℓ times on the coefficients (see for instance Notation 1 in Chapter 5). Note that we have $\left|\boldsymbol{M}^{[\ell]}\right| = |\boldsymbol{M}|^{[\ell]}$. Given a MaxMinors equation P_J, $J \subset \{1..n-k-1\}$, $\#J = r$, we denote by $P_J^{[\ell]}$ the linear polynomial in the c_T's obtained by applying ℓ times the Frobenius map and then by reducing modulo $\{c_T^q - c_T\}$. Since $P_{i,J} = \mathrm{Tr}(\beta_i^\star P_J) = \sum_{\ell=0}^{m-1}(\beta_i^\star)^{[\ell]}P_J^{[\ell]}$ and $P_J^{[\ell]} = \sum_{i=1}^{m}\beta_i^{[\ell]}P_{i,J}$, we have

$$\langle P_{i,J} : 1 \leqslant i \leqslant m\rangle_{\mathbb{F}_{q^m}} = \langle P_J^{[\ell]} : 0 \leqslant \ell \leqslant m-1\rangle_{\mathbb{F}_{q^m}}. \tag{7.16}$$

For $\ell \in \{0..m-1\}$ and $T \subset \{1..n-k-1\}$, $\#T = r+1$, let

$$\Gamma_{\ell,T} \stackrel{def}{=} \left|\begin{bmatrix}\boldsymbol{xG}+\boldsymbol{y}\\ \boldsymbol{C}\end{bmatrix}(\boldsymbol{H_y}^{[\ell]})^{\mathsf{T}}_{*,T}\right|.$$

By Laplace expansion along the first row, this minor is a linear combination with coefficients in $\mathbb{F}_{q^m}[\boldsymbol{x}]$ between maximal minors of $\boldsymbol{C}(\boldsymbol{H_y}^{[\ell]})^{\mathsf{T}}_{*,T}$, more precisely the $P_J{}^{[\ell]}$'s such that $J \subset T$. By Equation (7.16), the normal form of $\Gamma_{\ell,T}$ modulo the unfolded MaxMinors polynomials is then equal to 0. Also, the Cauchy-Binet formula shows that $\Gamma_{\ell,T}$ is the linear combination between Q_I equations given by

$$\widetilde{Q_{T+k+1}} + \sum_{\substack{I\subset\{1..n\},\#I=r+1,\\ I\cap\{k+1..n\}\subsetneq T+k+1}} \left|(\boldsymbol{H_y}^{[\ell]})_{T,I}\right|\widetilde{Q_I}.$$

To conclude the proof, we use the fact that the set of previous equations for fixed T and for all $\ell \in \{0..m-1\}$ generate the same vector space over $\mathbb{F}_{q^m}$ as the one containing

$$\mathrm{Tr}(\beta_i^\star)\widetilde{Q_{T+k+1}} + \sum_{\substack{I\subset\{1..n\}\\ \#I=r+1\\ I\cap\{k+1..n\}\subsetneq T+k+1}} \mathrm{Tr}(\beta_i^\star\,|(\boldsymbol{H}_{\boldsymbol{y}})_{T,I}|)\widetilde{Q_I}$$

for all $i \in \{1..m\}$. □

This proposition gives $m\binom{n-k-1}{r+1}$ syzygies at bi-degree $(1,1)$ which include the ones from Proposition 7.1 (the $\ell = 0$ case in the proof). However, it does not tell about the independance of such relations. In bi-degree $(2,1)$, they are multiplied by all linear variables to generate new ones and this time we are certain that they are not independent. This is due to the identities

$$\left|\begin{bmatrix}\boldsymbol{x}\boldsymbol{G}+\boldsymbol{y}\\ \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y}\\ \boldsymbol{C}\end{bmatrix}(\boldsymbol{H}_{\boldsymbol{y}}^{[\ell]})^{\mathsf{T}}_{*,T_2}\right| = 0,$$

for any $\ell \in \{1..m-1\}$ and any subset $T_2 \subset \{1..n-k-1\},\ \#T_2 = r+2$. We obtain in this way $(m-1)\binom{n-k-1}{r+2}$ relations in degree $b=2$ between the syzygies of Proposition 7.7. If we assume that the whole syzygy module boils down to such cancellations, then a similar inclusion-exclusion argument as the one used to derive [Bar+20b, Heuristic 2] leads to the following Conjecture 7.1. We verified it experimentally on small underdetermined RD instances for $b=2,\ b=3$ and $b=4$.

Conjecture 7.1. *For $b \geqslant 1$, the number of independent syzygies is expected to be*

$$N_{b,syz}^{\mathbb{F}_q} = (m-1)\sum_{i=1}^{b}(-1)^{i+1}\binom{k+b-i-1}{b-i}\binom{n-k-1}{r+i},$$

provided that it is $< M_b^{\mathbb{F}_q}$.

We conclude this section with the total cost of our method. Note that it is always possible, whenever the ratio between equations and monomials is much larger than 1, to drop excess polynomials by taking punctured codes much in the same way as in [Bar+20b, §4.2]. Finally, we can also use the hybrid approach on the block of minor variables sketched in Section 7.1.1 to improve the solving degree. We will come back to it in the next section.

Corollary 7.4. *Under Assumption 1 and Conjecture 7.1 which yield Proposition 7.6, one can solve RD by applying dense linear algebra on the Macaulay matrix $\mathcal{M}ac_{(b,1)}(\mathcal{T})$ whenever*

$$N_b^{\mathbb{F}_q} \geqslant M_b^{\mathbb{F}_q} - 1.$$

In this case, the global complexity in $\mathbb{F}_q$-operations is

$$\mathcal{O}\left(m^2 N_b^{\mathbb{F}_q} (M_b^{\mathbb{F}_q})^{\omega-1}\right), \tag{7.17}$$

where ω is the linear algebra constant and where the m^2 factor accounts for expressing each $\mathbb{F}_{q^m}$-operation involved in terms of $\mathbb{F}_q$-operations.

7.4 Hybrid Technique on Minor Variables

In [Bar+23], we systematized the hybrid approach of Section 7.1.1 to any bilinear modeling involving a block of minors variables. Our method applies to the system of Section 7.3 for RD but also more generally to the Support-Minors modeling of the MinRank problem. This is in fact a reduction to a smaller instance which does not depend so much on the input system.

In the matrix $\boldsymbol{C}$ which yields the minor variables, the idea is still to set a columns to zero. Note that in the case of RD, this amounts to fixing a zero positions in the error vector $\boldsymbol{e}$. More precisely, we base ourselves on the following considerations.

1. If by chance these a positions are zero in the genuine RD solution and if they belong to an information set of the code, it is possible to reduce the problem with parameters (m, n, k, r) to a smaller one with parameters $(m, n-a, k-a, r)$;
2. The condition in 1. is met with probability $\frac{1}{q^{ar}}$ for a random instance;
3. It is possible to change the input problem into another one satisfying this constraint either by exhaustive search among all q^{ar} possible transformations or by using a rerandomizing trick that will succeed with probability $\mathcal{O}(q^{-ar})$.

Our method for RD is quite reminiscent of [GRS16, §5.2], where rerandomization is implicit (see the proof of Proposition 3 there). As we will see, this technique is also valid for generic MinRank.

In Section 7.4.1, we give a general presentation of the rerandomizing trick. In Section and, we apply it to RD and MinRank respectively. Finally, we provide a probabilistic description of our approach in Section.

7.4.1 Rerandomizing Trick

There is no reason a priori why a positions of the RD solution $\boldsymbol{e}$ nor a columns of the low rank matrix $\boldsymbol{M} = \boldsymbol{M}_0 + \sum_{i=1}^{K} \boldsymbol{M}_i$ would be equal to 0. To create such zeroes, we propose to multiply on the right by a square matrix $\boldsymbol{P}$ over $\mathbb{F}_q$ which is invertible so that the rank is preserved. Let us start with the RD case. If we make the following assumption on the input instance,

Assumption 8. *We assume that the first r positions of the solution $\boldsymbol{e}$ are independent over $\mathbb{F}_q$.*

then we can restrict ourselves to the q^{ar} matrices in

$$\mathcal{RM} \stackrel{def}{=} \left\{ \boldsymbol{P}_{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{I}_r & \boldsymbol{0}_{r\times(n-a-r)} & -\boldsymbol{A} \\ \boldsymbol{0}_{(n-a-r)\times r} & \boldsymbol{I}_{n-a-r} & \boldsymbol{0}_{(n-a-r)\times a} \\ \boldsymbol{0}_{a\times r} & \boldsymbol{0}_{a\times(n-a-r)} & \boldsymbol{I}_a \end{bmatrix} : \boldsymbol{A} \in \mathbb{F}_q^{r\times a} \right\}.$$

The point of multiplying by an element of $\mathcal{RM}$ is that it leaves the $(n-a)$ columns in the first two blocks unchanged but it adds to the last a positions of $\boldsymbol{e}$ or to the last a columns of $\boldsymbol{M}$ all possible linear combinations between the first r ones. Assumption 8 states that the product by one of these elements will yield an instance with the zero positions we want.

Finally, the knowledge of these coordinates allows to reduce the dimension of the underlying matrix code. This is easier to explain for RD because we will simply work in the code $\mathcal{C}_{\boldsymbol{A}} \stackrel{def}{=} \{\boldsymbol{c}\boldsymbol{P}_{\boldsymbol{A}} : \boldsymbol{c} \in \mathcal{C}\}$ shortened at $J \stackrel{def}{=} \{n-a+1..n\}$. Let us also denote the complementary subset by $\check{J} \stackrel{def}{=} \{1..n-a\}$.

7.4.2 Application to RD

In the Rank Decoding case, when $(\boldsymbol{e}\boldsymbol{P}_{\boldsymbol{A}})_J = \boldsymbol{0}$, we can reduce to the following smaller instance under a mild condition on the code shortened at J.

Proposition 7.8. *Let $\mathcal{C}' \stackrel{def}{=} \mathcal{S}_J(\mathcal{C})$ be the code $\mathcal{C}$ shortened at J. If this code is of maximal dimension $k-a$, then by Gaussian elimination on a generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ of $\mathcal{C}$, we can obtain a generator matrix of $\mathcal{C}$ in systematic form on the columns in J,* i.e.*,*

$$\boldsymbol{D}\boldsymbol{G} = \begin{array}{c} \begin{matrix} \check{J} & J \end{matrix} \\ \begin{bmatrix} \boldsymbol{G}' & \boldsymbol{0}_{(k-a)\times a} \\ \boldsymbol{B} & \boldsymbol{I}_a \end{bmatrix} \end{array} \in \mathbb{F}_{q^m}^{k\times n},$$

where $\boldsymbol{D} \in \mathbb{F}_{q^m}^{k\times k}$ is invertible and where $\boldsymbol{G}'$ is a generator matrix for $\mathcal{C}'$. If we further assume that $\boldsymbol{e}_J = \boldsymbol{0}$ and if we let $\boldsymbol{y}' \stackrel{def}{=} \boldsymbol{y}_{\check{J}} - \boldsymbol{y}_J\boldsymbol{B} \in \mathbb{F}_{q^m}^{n-a}$, then $(\boldsymbol{y}', \mathcal{C}', r)$ is a valid RD instance with parameters $(m, n-a, k-a, r)$ from which we can deduce a solution to the initial problem.

Proof. The first point is just standard linear algebra. For the second point, let $(\boldsymbol{c}, \boldsymbol{e} = \boldsymbol{y} - \boldsymbol{c}) \in \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n$ be the solution to the original instance and let

$$(\boldsymbol{x}',\ \boldsymbol{x}'') = \boldsymbol{x}\boldsymbol{D}^{-1} \in \mathbb{F}_{q^m}^{k-a} \times \mathbb{F}_{q^m}^{a}\ , \text{ where } \boldsymbol{c} = \boldsymbol{x}\boldsymbol{G}.$$

Observe now that

$$\begin{aligned} \boldsymbol{e}_J &= \boldsymbol{y}_J - \boldsymbol{c}_J \\ &= \boldsymbol{y}_J - (\boldsymbol{x}\boldsymbol{G})_J \\ &= \boldsymbol{y}_J - \left((\boldsymbol{x}',\ \boldsymbol{x}'')\,\boldsymbol{D}\boldsymbol{G}\right)_J \\ &= \boldsymbol{y}_J - \boldsymbol{x}''. \end{aligned}$$

If we assume that $\boldsymbol{e}_J = \mathbf{0}$, we obtain $\boldsymbol{y}_J = \boldsymbol{x}''$. Finally,

$$\begin{aligned}\boldsymbol{e}_{\check{J}} = \boldsymbol{y}_{\check{J}} - \boldsymbol{c}_{\check{J}} &= \boldsymbol{y}_{\check{J}} - \boldsymbol{x}'\boldsymbol{G}' - \boldsymbol{x}''\boldsymbol{B} \\ &= \underbrace{\boldsymbol{y}_{\check{J}} - \boldsymbol{y}_J\boldsymbol{B}}_{\boldsymbol{y}'} - \underbrace{\boldsymbol{x}'\boldsymbol{G}'}_{=\boldsymbol{c}'\in\mathcal{C}'},\end{aligned}$$

hence $\boldsymbol{y}' - \boldsymbol{c}'$ is of rank weight r and the desired result. □

Proposition 7.8 will be used as follows. Recall that we solve the RD instance $(\boldsymbol{y}, \mathcal{C}, r)$ with parameters (m, n, k, r) by considering the q^{ar} RD instances $(\boldsymbol{y}', \mathcal{C}', r)$ of parameters $(m, n-a, k-a, r)$ obtained from all $\boldsymbol{P}_{\boldsymbol{A}} \in \mathcal{RM}$ by computing a generator matrix $\boldsymbol{G}_{\boldsymbol{A}} \stackrel{def}{=} \boldsymbol{G}\boldsymbol{A}$ of $\mathcal{C}_{\boldsymbol{A}} = \{\boldsymbol{c}\boldsymbol{P}_{\boldsymbol{A}} : \boldsymbol{c} \in \mathcal{C}\}$ and then by putting it in (partial) systematic form on the columns in J by Gaussian elimination to get

$$\boldsymbol{G}'' \stackrel{def}{=} \begin{array}{c} \begin{matrix} \check{J} & J \end{matrix} \\ \begin{bmatrix} \boldsymbol{G}' & \mathbf{0}_{(k-a)\times a} \\ \boldsymbol{B} & \boldsymbol{I}_a \end{bmatrix} \end{array}. \tag{7.18}$$

Under Assumption 8, one of these instances has a solution. By solving it, Proposition 7.8 eventually shows that we can recover the solution to the original problem.

It remains to check under which condition the matrix $\boldsymbol{G}_{\boldsymbol{A}}$ admits a partial systematic form for any $\boldsymbol{A} \in \mathbb{F}_q^{r\times a}$ as required to obtain Equation (7.18). In other words, we have to examine when $\mathcal{S}_J(\mathcal{C}_{\boldsymbol{A}})$ is of dimension $k-a$ for any such matrix $\boldsymbol{A}$. There are two cases to consider:

Case $a + r \leqslant k$. In this situation, the relevant property holds under a very mild condition on the code $\mathcal{C}$.

Lemma 7.2. *Provided that there exists a systematic set for $\mathcal{C}$ that contains $\{1..r\} \cup J$, the code $\mathcal{S}_J(\mathcal{C}_{\boldsymbol{A}})$ is of dimension exactly $k-a$ for all matrices $\boldsymbol{A} \in \mathbb{F}_q^{r\times a}$.*

Proof. By reordering the positions, we may assume that the systematic set is $\{1..k\}$, that $J = \{r+1..r+a\}$ and that

$$\boldsymbol{P}_{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{I}_r & -\boldsymbol{A} & \mathbf{0}_{r\times(n-a-r)} \\ \mathbf{0}_{a\times r} & \boldsymbol{I}_a & \mathbf{0}_{a\times(n-a-r)} \\ \mathbf{0}_{(n-a-r)\times r} & \mathbf{0}_{(n-a-r)\times a} & \boldsymbol{I}_{n-a-r} \end{bmatrix}.$$

By hypothesis, we can also choose a generator matrix of $\mathcal{C}$ as

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_k & \boldsymbol{R} \end{bmatrix}.$$

A generator matrix for $\mathcal{C}_{\boldsymbol{A}}$ is then given by

$$\boldsymbol{G}\boldsymbol{P}_{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{I}_r & -\boldsymbol{A} & \mathbf{0}_{r\times(n-a-r)} & \boldsymbol{R}_1 \\ \mathbf{0}_{a\times r} & \boldsymbol{I}_a & \mathbf{0}_{a\times(k-a-r)} & \boldsymbol{R}_2 \\ \mathbf{0}_{(k-a-r)\times r} & \mathbf{0}_{(k-a-r)\times a} & \boldsymbol{I}_{k-a-r} & \boldsymbol{R}_3 \end{bmatrix},$$

which shows that this code is still systematic in its first k positions and finally that $\mathcal{S}_J(\mathcal{C}_{\boldsymbol{A}})$ has dimension $k-a$. □

Case $a + r > k$**.** This time, the $\mathbb{F}_{q^m}$-linear code $\mathcal{D}$ of parameters $[a + r, k]$ generated by the matrix $\boldsymbol{G}_{*,\{1..r\}\cup J} \in \mathbb{F}_{q^m}^{k\times(a+r)}$ cannot be the full code. Here, it will be helpful to notice that $\mathcal{S}_J(\mathcal{C}_{\boldsymbol{A}})$ has dimension $k - a$ if and only if the matrix $\boldsymbol{G}_{*,J} - \boldsymbol{G}_{*,\{1..r\}}\boldsymbol{A}$ is of rank a. To verify whether or not this property holds, we use

Lemma 7.3. *The existence of a matrix $\boldsymbol{A} \in \mathbb{F}_q^{r\times a}$ such that $\boldsymbol{G}_{*,J} - \boldsymbol{G}_{*,\{1..r\}}\boldsymbol{A}$ is rank defective is equivalent to the existence of a word of weight $\leqslant a$ in the dual of $\mathcal{D}$ whose support is spanned by the last a coordinates.*

Proof. Let us assume that the matrix $\boldsymbol{A} \in \mathbb{F}_q^{r\times a}$ satisfies $\mathrm{rk}\left(\boldsymbol{G}_{*,J} - \boldsymbol{G}_{*,\{1..r\}}\boldsymbol{A}\right) < a$. This means that there exists a vector $\boldsymbol{\lambda}_{\boldsymbol{A}} \in \mathbb{F}_{q^m}^{a}$ such that

$$-\boldsymbol{G}_{*,\{1..r\}}\boldsymbol{A}\boldsymbol{\lambda}_{\boldsymbol{A}}^{\mathsf{T}} + \boldsymbol{G}_{*,J}\boldsymbol{\lambda}_{\boldsymbol{A}}^{\mathsf{T}} = \boldsymbol{G}_{*,\{1..r\}\cup J}\underbrace{\begin{bmatrix} -\boldsymbol{A}\boldsymbol{\lambda}_{\boldsymbol{A}}^{\mathsf{T}} \\ \boldsymbol{\lambda}_{\boldsymbol{A}}^{\mathsf{T}} \end{bmatrix}}_{\stackrel{def}{=}\boldsymbol{v}_{\boldsymbol{A}}^{\mathsf{T}}} = 0.$$

In particular, the vector $\boldsymbol{v}_{\boldsymbol{A}} \in \mathbb{F}_{q^m}^{a+r}$ belongs to $\mathcal{D}^{\perp}$, its weight is $\leqslant a$ (as the entries of $\boldsymbol{A}$ belong to $\mathbb{F}_q$) and its support is spanned by the a last coordinates. The converse statement is similar by constructing an inverse of the map $\boldsymbol{A} \mapsto \boldsymbol{v}_{\boldsymbol{A}}$. □

Under the assumption that $\mathcal{D}$ behaves as a random code of parameters $[a + r, k]$, we can finally estimate the number of vectors as in Lemma 7.3.

Lemma 7.4. *The probability that there exists a non zero vector of weight $\leqslant a$ whose support is spanned by the last a coordinates in the dual of a random $\mathbb{F}_{q^m}$-linear code of parameters $[a + r, k]$ is upper-bounded by $\Theta\left(q^{(m+r)a-mk}\right)$ when q goes to infinity.*

Proof. This probability is upper-bounded by the simpler probability that there exists a non zero codeword of weight $\leqslant a$. Let X denote the number of such codewords. We use the fact that $\Pr[X \neq 0] \leqslant \mathrm{E}[X]$ and that the expected number $\mathrm{E}[X]$ of non-zero vectors of weight $\leqslant a$ in such a code is given by

$$\mathrm{E}[X] = \frac{\mathcal{B}_{m,a+r,a} - 1}{q^{mk}},$$

where $\mathcal{B}_{m,a+r,a}$ is the size of a ball of radius a in $\mathbb{F}_{q^m}^{a+r}$ in the rank metric. Finally, by [Loi14, Proposition 1], the size of such a ball is of the form $\Theta\left(q^{(m+a+r)a-a^2}\right) = \Theta\left(q^{(m+r)a}\right)$ for any nonnegative integer $a \leqslant m$ when q goes to infinity. □

7.4.3 Application to Generic MinRank

The reduction that we have just sketched for the RD problem also applies to MinRank. This time, the relevant assumption is

Assumption 9. *We assume the first d columns of the low rank matrix $\boldsymbol{M}$ are linearly independent.*

Under Assumption 9, we will restrict ourselves to the elements of

$$\mathcal{RM}_{\mathrm{MR}} \stackrel{def}{=} \left\{ \boldsymbol{P}_{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{I}_d & \boldsymbol{0}_{d\times(n_c-a-d)} & -\boldsymbol{A} \\ \boldsymbol{0}_{(n_c-a-d)\times d} & \boldsymbol{I}_{n_c-a-d} & \boldsymbol{0}_{(n_c-a-d)\times a} \\ \boldsymbol{0}_{a\times d} & \boldsymbol{0}_{a\times(n_c-a-d)} & \boldsymbol{I}_a \end{bmatrix} : \boldsymbol{A} \in \mathbb{F}_q^{d\times a} \right\}.$$

To explain the form taken by the reduced RD problems we got in Subsection 7.4.2, recall that it was convenient to put the generator matrix of the transformed code $\mathcal{C}_{\boldsymbol{A}} = \mathcal{C}\boldsymbol{P}_{\boldsymbol{A}}$ in systematic form. We start by introducing a similar formalism for Problem 3.1 from which we will derive analogous results (Proposition 7.9).

In the MinRank case, it will be worthwhile to view a matrix as the vector formed by the concatenation of its rows. To present the relevant systematic form that we will use, we bring in the invertible linear map

$$\begin{aligned} \varphi : \mathbb{F}_q^{n_r\times n_c} &\to \mathbb{F}_q^{n_r n_c} \\ \boldsymbol{A} &\mapsto (\boldsymbol{A}_{i,j})_{i\in\{1..n_r\},j\in\{1..n_c\}}, \end{aligned} \tag{7.19}$$

where the image of $\varphi(\boldsymbol{A})$ is formed by the entries of $\boldsymbol{A}$ in column-major order. We can now define

Definition 7.1. Let $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K$ be matrices in $\mathbb{F}_q^{n_r\times n_c}$ and let $\mathcal{L}$ be the linear code of length $n_r n_c$ generated by the vectors $\varphi(\boldsymbol{M}_i)$ for $i \in \{1..K\}$. We consider the generator matrix

$$\boldsymbol{L} \stackrel{def}{=} \boldsymbol{L}(\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K) \stackrel{def}{=} \begin{bmatrix} \varphi(\boldsymbol{M}_1) \\ \vdots \\ \varphi(\boldsymbol{M}_K) \end{bmatrix} \in \mathbb{F}_q^{K\times n_r n_c}.$$

As noted in [BESV22, §4.4], any elementary row operation on $\boldsymbol{L}$ corresponds to linear transformations of the variables x_i, *i.e.*, we can always replace the initial MinRank instance by an equivalent one with $\boldsymbol{L}$ in echelon form. A stronger constraint is

Definition 7.2. We say that a MinRank instance $(\boldsymbol{M}_0; \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K)$ is in systematic form if its associated generator matrix $\boldsymbol{L}(\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K)$ is. We denote by S the set of all systematic positions.

Remark 7.1. It is not always possible to put a MinRank instance in systematic form, as a permutation of the columns does not always preserve the rank of the $n_r \times n_c$ matrix associated to the row (this permutation must have a block structure so that it also acts as a permutation on the columns of the matrix). However, [BESV22] note that a random instance will be in systematic form with high probability.

Let us set $J \stackrel{def}{=} \{n_c - a + 1..n_c\}$, $\check{J} \stackrel{def}{=} \{1..n_c\}$, and let I be the elements in $\{1..n_r n_c\}$ that correspond to the columns indexed by the positions in J, that is $I \stackrel{def}{=} \cup_{j\in J}\{(j-1)n_r + 1..jn_r\}$.

Proposition 7.9. *Let $(\boldsymbol{M}_0; \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K) \in \mathbb{F}_q^{n_r \times n_c}$ be an inhomogeneous MinRank problem with rank d. Assume that the number a of fixed columns is such that $an_r \leqslant K$ and that the solution $\boldsymbol{x}$ satisfies $\boldsymbol{M}_{*,J} = \boldsymbol{0}_{n_r \times a}$, or equivalently $\varphi(\boldsymbol{M}_0)_I + \boldsymbol{x}\boldsymbol{L}_{*,I} = \boldsymbol{0}_{an_r}$. Let $\mathcal{L}' \stackrel{def}{=} \mathcal{S}_I(\mathcal{L})$ be the code $\mathcal{L}$ shortened at I. If we assume that $\mathcal{L}'$ is of dimension $K - an_r$, then the solution $\boldsymbol{x}$ can be deduced from the solution to a smaller MinRank instance $(\boldsymbol{M}'_0; \boldsymbol{M}'_1 \ldots, \boldsymbol{M}'_{K-an_r})$ in $\mathbb{F}_q^{n_r \times (n_c - a)}$ with target rank still equal to d.*

More precisely, by Gaussian elimination on $\boldsymbol{L}$, we can obtain a generator matrix of $\mathcal{L}$ in systematic form on the columns in I, i.e., *after permuting columns to bring these positions to the last an_r ones:*

$$\boldsymbol{D}\boldsymbol{L} = \begin{bmatrix} \boldsymbol{L}' & \boldsymbol{0}_{(K-an_r)\times an_r} \\ \boldsymbol{B} & \boldsymbol{I}_{an_r} \end{bmatrix},$$

where $\boldsymbol{D} \in \mathbb{F}_q^{K \times K}$ is invertible and where the matrix $\boldsymbol{L}' \in \mathbb{F}_q^{(K-an_r)\times n_r(n_c-a)}$ generates $\mathcal{L}'$. Finally, for every $i \in \{1..K - an_r\}$, we define $\boldsymbol{M}'_i$ to be the $n_r \times (n_c - a)$ matrix corresponding to the i-th row of $\boldsymbol{L}'$, and[2] *$\boldsymbol{M}'_0 \stackrel{def}{=} \varphi^{-1}(\varphi(\boldsymbol{M}_0)_{\check{I}} - \varphi(\boldsymbol{M}_0)_I \boldsymbol{B})$, where $\check{I} \stackrel{def}{=} \{1..n_r n_c\} \backslash I$. Then $(\boldsymbol{M}'_0; \boldsymbol{M}'_1, \ldots, \boldsymbol{M}'_{K-an_r}) \in \mathbb{F}_q^{n_r \times (n_c - a)}$ is a MinRank instance with target rank d whose arbitrary solution $\boldsymbol{x}'$ gives a solution $\boldsymbol{x} = \boldsymbol{D}(\boldsymbol{x}' \ \boldsymbol{x}'')$ to the initial problem with $\boldsymbol{x}'' = -\varphi(\boldsymbol{M}_0)_I$.*

Proof. To simplify the exposition, we assume that the positions in $\{1..n_r n_c\}$ have been permuted, so that the last an_r positions belong to I. By hypothesis, we have $\boldsymbol{D}\boldsymbol{L}_{*,I} = \begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{I}_{an_r} \end{bmatrix}$, so that if $\boldsymbol{x}\boldsymbol{D}^{-1} = (\boldsymbol{x}' \ \boldsymbol{x}'')$ with $\boldsymbol{x}'$ of size $K - an_r$, the hypothesis $\varphi(\boldsymbol{M}_0)_I + \boldsymbol{x}\boldsymbol{L}_{*,I} = \boldsymbol{0}$ is equivalent to $\boldsymbol{x}'' + \varphi(\boldsymbol{M}_0)_I = \boldsymbol{0}$. As $\boldsymbol{M}_J = \boldsymbol{0}$, the matrix $\boldsymbol{M}_{\check{J}}$ is of rank d. It is given by

$$\begin{aligned} \varphi(\boldsymbol{M}_{\check{J}}) = \varphi(\boldsymbol{M})_{\check{I}} &= \boldsymbol{x}'\boldsymbol{L}' + \boldsymbol{x}''\boldsymbol{B} + \varphi(\boldsymbol{M}_0)_{\check{I}} \\ &= \boldsymbol{x}'\boldsymbol{L}' - \varphi(\boldsymbol{M}_0)_I\boldsymbol{B} + \varphi(\boldsymbol{M}_0)_{\check{I}}, \\ \text{say } \boldsymbol{M}_{\check{J}} &= \boldsymbol{M}'_0 + \sum_{i=1}^{K-an_r} x'_i \boldsymbol{M}'_i. \end{aligned}$$

This is indeed the smaller MinRank problem described in the proposition. □

Finally, we give a simple case where the shortened code has maximal dimension when we do the product by all elements $\boldsymbol{P}_{\boldsymbol{A}} \in \mathcal{RM}_{\mathrm{MR}}$. Lemma 7.5 requires $(d + a)n_r \leqslant K$ and it is the MinRank counterpart of Lemma 7.2.

Lemma 7.5. *Let us assume the MinRank instance $(\boldsymbol{M}_0; \boldsymbol{M}_1, \ldots, \boldsymbol{M}_K)$ is in systematic form on a set of positions S that contains $\{1..dn_r\} \cup I$ and let $\mathcal{L}$ be the matrix code generated by $(\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K)$. For any $\boldsymbol{A} \in \mathbb{F}_q^{d \times a}$, the shortening of $\mathcal{L}\boldsymbol{P}_A$ at I has dimension $K - an_r$.*

[2] We abusively use the same name $\varphi : \mathbb{F}_q^{n_r \times n_c} \to \mathbb{F}_q^{n_r n_c}$ and $\mathbb{F}_q^{n_r \times (n_c - a)} \to \mathbb{F}_q^{n_r (n_c - a)}$.

Proof. For $i \in \{1..K\}$, the matrix $\boldsymbol{M}_i^{\boldsymbol{A}} \stackrel{def}{=} \boldsymbol{M}_i \boldsymbol{P}_{\boldsymbol{A}}$ is identical to $\boldsymbol{M}_i$ on the columns with indexes in $\check{J}$ and the other ones are such that $(\boldsymbol{M}_i^{\boldsymbol{A}})_{*,J} = (\boldsymbol{M}_i)_{*,J} - (\boldsymbol{M}_i)_{*,\{1..d\}}\boldsymbol{A}$. We may reorder the indices in $\{1..n_r n_c\}$ so that the systematic positions are the first K ones and such that $I = \{dn_r + 1..(d+a)n_r\}$. If the input instance is in systematic form, then for $u \in \{1..n_r\},\ v \in \{1..n_c\},\ i = (v-1)n_r + u \in \{1..n_r n_c\}$, the submatrix $(\boldsymbol{M}_i)_{*,\{1..d+a\}}$ has at most only one nonzero entry equal to 1 in position (u, v) if $v \leqslant d+a$ and it is all zero otherwise. This means that

$$(\boldsymbol{M}_i)_{*,\{1..d\}} = \boldsymbol{0}_{n_r \times d}, \text{ hence } \boldsymbol{M}_i^{\boldsymbol{A}} = \boldsymbol{M}_i \text{ if } i \geqslant dn_r + 1,$$

and that if $i \in \{1..dn_r\}$,

$$(\boldsymbol{M}_i^{\boldsymbol{A}})_{*,J} = \begin{bmatrix} \boldsymbol{0} \\ -\boldsymbol{A}_{v,*} \\ \boldsymbol{0} \end{bmatrix},$$

where the non-zero row is the u-th row. This eventually shows that the generator matrix

$$\boldsymbol{L}_{\boldsymbol{A}} = \begin{bmatrix} & \overset{\text{positions in } I}{} & & \\ \boldsymbol{I}_{dn_r} & \binom{\text{coefficients}}{\text{depending}}_{\text{on } \boldsymbol{A}} & \boldsymbol{0} & \boldsymbol{L}_{\{1..dn_r\},\{(d+a)n_r+1..n_r n_c\}} \\ \boldsymbol{0} & \boldsymbol{I}_{an_r} & \boldsymbol{0} & \boldsymbol{L}_{\{dn_r+1..(d+a)n_r\},\{(d+a)n_r+1..n_r n_c\}} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{K-(d+a)n_r} & \boldsymbol{L}_{\{(d+a)n_r+1..K\},\{(d+a)n_r+1..n_r n_c\}} \end{bmatrix}$$

for $\mathcal{L}\boldsymbol{P}_A$ is full rank on the columns in I and thus that the shortening at these positions has dimension $K - an_r$. □

7.4.4 Probabilistic Version

The deterministic approach presented in the previous sections does not work if the initial conditions on the solution $\boldsymbol{M}$ to the MinRank problem or on the solution $\boldsymbol{e}$ to the RD problem are not met, *i.e.*, the first d columns of $\boldsymbol{M}$ are not linearly independent nor the first r entries in $\boldsymbol{e}$ are not linearly independent over $\mathbb{F}_q$.

We propose to fix this by considering instead a randomized algorithm, which consists in multiplying the instance on the right by a random invertible matrix $\boldsymbol{P}$ over $\mathbb{F}_q$ (no longer in $\mathcal{RM}$ nor in $\mathcal{RM}_{\text{MR}}$), which produces a new problem instance which satisfies the right assumptions with constant probability and on which we can apply the former technique. Let us detail the case of MinRank. Once we have solved the new instance, we recover the solution to the original one simply by multiplying on the right by $\boldsymbol{P}^{-1}$. The plain idea might even be improved slightly by multiplying on the right each time by a new $\boldsymbol{P}$ and by directly including the bet on the a columns equal to 0 (in other words, we directly consider the smaller instance with parameters $(n_r, n_c - a, K - an_r, d)$). This has a probability of $\Omega\left(q^{-ad}\right)$ to happen.

7.5 Application to MinRank and to RD Instances

This section provides the bit complexity of our hybrid approach. In Section 7.5.1, we apply it to the SM solver on random MinRank problems. In Section 7.5.2, we present its results on the new RD modeling. In both cases, we compare ourselves to previous attacks.

7.5.1 Support-Minors on Generic MinRank

First, we obtain smaller complexities than the ones corresponding to the specialization of [Bar+20b] by fixing linear variables. This is because we exploit the MinRank structure and not only the bilinearity in the SM system. More interestingly, our technique offers a trade-off between combinatorial attacks (*e.g.*, Goubin's kernel search) and pure algebraic methods. Indeed, the bet that we make can be seen as guessing $a \geqslant 0$ vectors in the right kernel of the low rank matrix similarly to Section 3.1.3.1. The difference here is that we consider less vectors since we do not need to solve in degree 1.

Table 7.1 summarizes our results on the MR-DSS parameters [BESV22], where λ is the security level. Column "Kernel (a)" is the cost of kernel search given in Equation (3.5) with $a \stackrel{def}{=} \lceil \frac{K}{n_r} \rceil$. Column "Hybrid Kernel (a) [BESV22]" is the optimized kernel attack of [BESV22][3] which consists in guessing $a \leqslant \lceil \frac{K}{n_r} \rceil$ vectors instead of the maximum number and then in solving the resulting MinRank problem using standard kernel search. Its improvement upon Goubin's complexity is by a polynomial factor in Equation (3.5). Finally, regarding our attack, we report the triplet (b, a, n_{cols}) which leads to the best cost: the number of guessed columns is a, the number of columns in the reduced MinRank problem is $n_{\text{cols}} \leqslant n_c - a$, and b is the degree at which we solve via SM. Our values were obtained with $\omega = 2$ as in [BESV22] and with a hidden constant of 7 in Strassen's algorithm.

Table 7.1: Comparison to kernel search variants on the parameters of [BESV22].

(q, n_r, n_c, K, d)	λ	Kernel (a)	Hybrid Kernel (a) [BESV22]	Hybrid SM (b, a, n_{cols})
$(16, 16, 16, 142, 4)$	128	166 (9)	158 (8)	161 (5, 6, $n_c - a$)
$(16, 19, 19, 167, 6)$	192	238 (9)	231 (8)	231 (7, 6, $n_c - a$)
$(16, 22, 22, 254, 6)$	256	311 (12)	303 (11)	297 (1, 11, $n_c - a$)

Note that the parameters proposed in [BESV22] already take into account our attack. It is likely that it will also be the case in MinRank-based signatures submitted to NIST, including [ARV23].

7.5.2 Combined Approach on Rank Decoding

A motivation for introducing SM-$\mathbb{F}_{q^m}^+$ to solve the RD problem was also to have a system that we can better analyze than the combination between MM-$\mathbb{F}_q$ and SM-$\mathbb{F}_q$

[3]This attack is given in a revision of the paper which is subsequent to our work.

considered in [Bar+20b]. In particular, we start by correcting the underestimated values of [Bar+20b, Table 3] regarding the complexity of this former modeling, on ROLLO-I. In Table 7.2, they correspond to the struck out numbers. There, we give the binary logarithm of our attack cost and we keep track of the optimum values of a and b. We compare ourselves to the combinatorial attack of [AGHT18] ("comb") and to the hybrid MaxMinors attack ("MM-$\mathbb{F}_q$"). In contrast to [Bar+20b, Table 3] where all these numbers where obtained with $\omega = 2.81$, we adopt the optimistic choice $\omega = 2$.

Table 7.2: Comparison between known attacks on the new ROLLO-I parameters in [Bar+20b] and [Agu+20] after the 2021-04-21 update. The "*"-symbol indicates that the best attack is on the code of parameters $(m, 2k - \lfloor \frac{k}{d} \rfloor, k - \lfloor \frac{k}{d} \rfloor, d)$ used for key recovery, where d refers to the row weight of the LRPC code. Otherwise, it corresponds to solving an RD problem with parameters $(m, 2k, k, r)$.

Instance	q	k	m	r	d	MM-$\mathbb{F}_q$	a	p	SM-$\mathbb{F}_{q^m}^+$	b	a	comb
new2ROLLO-I-128	2	83	73	7	8	205	18	0	~~180~~ **202**	2	13	212
new2ROLLO-I-192	2	97	89	8	8	226*	17	0	~~197*~~ **223***	1	14	282*
new2ROLLO-I-256	2	113	103	9	9	371*	30	1	~~283*~~ **366***	1	27	375*
ROLLO-I-128-spe	2	83	67	7	8	212	19	0	214	2	15	**196**
ROLLO-I-192-spe	2	97	79	8	8	242*	19	0	**241***	2	15	251*
ROLLO-I-256-spe	2	113	97	9	9	380*	31	0	376*	2	27	**353***

Figure 7.1 and Figure 7.2 contain a broader comparison between the same RD attacks for $(m, n, k) = (31, 33, 15)$ and for a weight r between 2 and 10 which is the rank Gilbert-Varshamov distance when $q = 2$.

Figure 7.1 represents the case $q = 2$. In this setting, we can see that algebraic attacks seem to become less efficient than the combinatorial ones for large r. This confirms the observation made in Section 3.3.5.2 and which lead the designers of [Agu+22; Ara+22] to increase the rank of the error. Note also that in [Agu+22], choosing d of the same order as r increases the rank of the moderate weight codewords in the masked LRPC code and thus it may allow to gain confidence in the indistinguishability assumption.

Figure 7.2 represents the case $q = 2^8$, where the combinatorial attack becomes much slower. The complexity of the hybrid technique on MM-$\mathbb{F}_q$ and SM-$\mathbb{F}_{q^m}^+$ also worsens but by a lesser amount since the cost contains a part which is independent from q, for instance $\binom{n-a}{r}^\omega$ in MaxMinors. Independently, we notice that the approach based on SM-$\mathbb{F}_{q^m}^+$ starts being interesting compared to MM-$\mathbb{F}_q$ for small values of r when q increases. Since the hybrid component of the complexity is polynomial in q and since it is more in important in MM-$\mathbb{F}_q$ than in SM-$\mathbb{F}_{q^m}^+$ (we can solve the latter at a larger b by fixing less columns), the dependency in q is clear. The condition on r might be explained by the fact that SM-$\mathbb{F}_{q^m}^+$ yields bigger Macaulay matrices than MM-$\mathbb{F}_q$ due to the extra block of linear variables. These sizes may have even more impact when r is larger since the block of minor variables also becomes larger.

Finally, we plot in Figure 7.3 the optimal values of a for the hybrid approach on MM-$\mathbb{F}_q$ and SM-$\mathbb{F}_{q^m}^+$ for $q = 2$ and $q = 2^8$.

Figure 7.1: Binary logarithms of the complexities of MM-$\mathbb{F}_q$, SM-$\mathbb{F}_{q^m}^+$ and of the combinatorial attack on RD instances with fixed $(q, m, n, k) = (2, 31, 33, 15)$ as a function of the rank r. The rank Gilbert-Varshamov distance is 10.

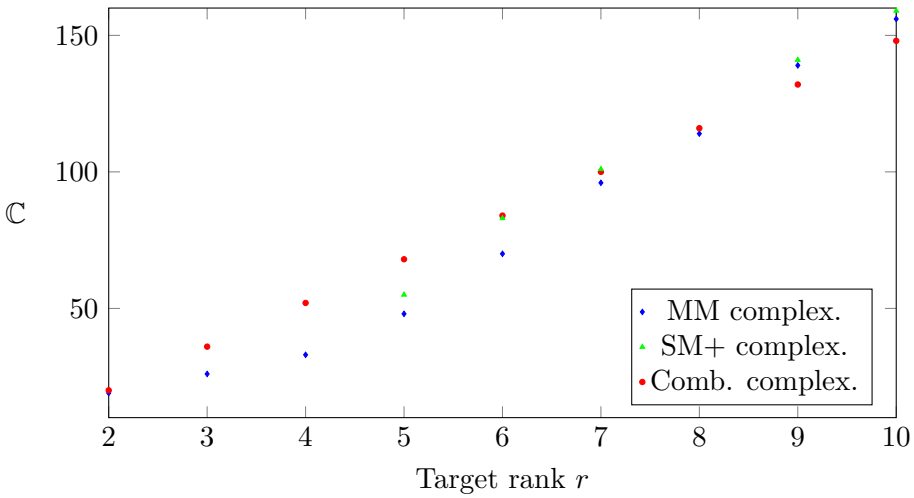
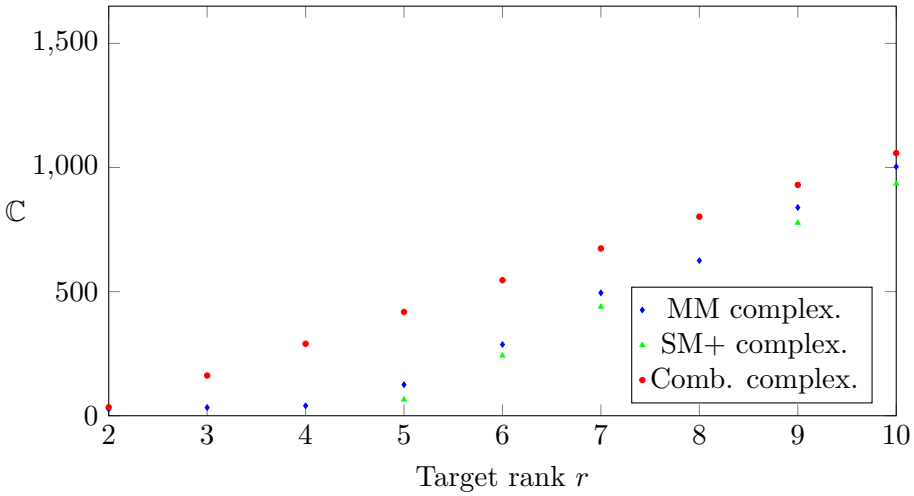


Figure 7.2: Same comparison as in Figure 7.1 but with $q = 2^8$.

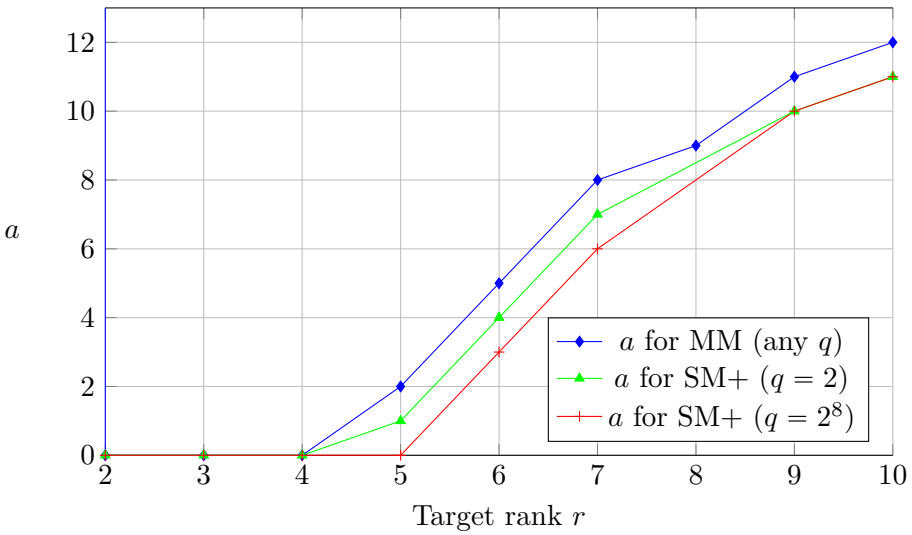


7.6 Application to the RSL Modeling

As announced at the end of Section 6.3.3 in the previous chapter, we finally come back to the hybrid approach on Modeling 13. Once again, we will multiply on the right by an invertible matrix $\boldsymbol{P} \in \mathbb{F}_q^{n \times n}$ of the desired shape to force zero positions in the target codeword $\boldsymbol{e}$. Let us recall that the number of syndromes is N. For any $i \in \{1..N\}$, we observe that

$$\boldsymbol{e}_i \boldsymbol{H}^\intercal = \boldsymbol{e}_i \boldsymbol{P} \boldsymbol{P}^{-1} \boldsymbol{H}^\intercal = \boldsymbol{e}_i \boldsymbol{P} (\boldsymbol{H} (\boldsymbol{P}^{-1})^\intercal)^\intercal = \boldsymbol{s}_i. \tag{7.20}$$

Figure 7.3: Optimal value of a in the hybrid approach on MM-$\mathbb{F}_q$ and SM-$\mathbb{F}_{q^m}^+$ for the parameters of Figure 7.1 and Figure 7.2.



Concretely, we use Equation (7.20) by keeping the same syndromes $\boldsymbol{s}_i$ for $i \in \{1..N\}$ but by considering the $\mathbb{F}_{q^m}$-linear code with parity-check matrix $\boldsymbol{H}(\boldsymbol{P}^{-1})^\intercal$ and which is simply $\mathcal{C}\boldsymbol{P}$. As in the RD case of above, we then shorten this code at the position $J \stackrel{def}{=} \{n-a+1..n\}$. Of course, we will need the same assumption regarding the dimension of $\mathcal{S}_J(\mathcal{C}\boldsymbol{P})$ for the analysis but there is nothing new compared to Section 7.4.2 in that respect. Contrary to what we have seen for MinRank and RD, note that this approach has no effect on the linear variables λ_i from Modeling 13.

Chapter 8
Rank Decoding Problem with Non-Homogeneous Errors

This chapter contains our results on the Non-Homogeneous Rank Decoding problem (NHRD, Problem 8.2). This work was initially motivated by its use in the Rank Quasi-Cyclic (RQC) cryptosystem [Agu+20] to mitigate the impact of the algebraic attacks of [Bar+20a; Bar+20b]. More importantly, it also helped to select the parameters of our new proposal [BBBG23], a more compact version of RQC.

First, we re-evaluate the complexity of the MaxMinors attack. We follow the specialization adopted by the RQC submitters [Agu+20, §6.2.2] and we correct their initial analysis by studying algebraic relations which occur in the system after fixing variables. Second, we propose a simple adaptation of combinatorial techniques to the non-homogeneous structure. There, the main technical point was the computation of the underlying success probability.

Contents

8.1 Preliminaries

We start by describing the basic RQC scheme submitted to NIST and by explaining the relevance of using non-homogeneous errors in this context. We then introduce our new RQC variant. Finally, we give details on the preliminary analysis of NHRD made in [Agu+20, §6.2.2].

8.1.1 RQC Cryptosystem

For positive integers m, n and w, let

$$\mathcal{S}_w^n(\mathbb{F}_{q^m}) = \{\boldsymbol{x} \in \mathbb{F}_{q^m}^n : |\boldsymbol{x}| = w\},$$
$$\mathcal{S}_{w,1}^n(\mathbb{F}_{q^m}) = \{\boldsymbol{x} \in \mathbb{F}_{q^m}^n : |\boldsymbol{x}| = w \text{ and } 1 \in \mathrm{Supp}(\boldsymbol{x})\},$$

and for a vector $\boldsymbol{g} \in \mathcal{S}_n^n(\mathbb{F}_{q^m})$ with necessarily $n \leqslant m$ and $k \leqslant n$, let $\mathcal{G}_{\boldsymbol{g}}(n,k,m)$ be the Gabidulin code of dimension k generated by $\boldsymbol{g}$ (see Definition 3.5). Recall that such a code can correct up to $\lfloor \frac{n-k}{2} \rfloor$ errors in an efficient manner. In particular, let $\mathcal{G}_{\boldsymbol{g}}.\mathsf{Decode}(.)$ denote a polynomial time decoding algorithm.

This section presents the PKE version of the scheme as it was before the update of [Agu+20]. In its name, the letters "QC" refer to the ideal structure. More precisely, quasi-cyclic codes have been replaced by ideal codes between the First and the Second Round due to the folding attack [HT15].

Setup(1^λ): Generates and outputs $\mathsf{param} = (n,k,\delta,w,w_1,P)$, where $(n,k,\delta,w,w_1) \in \mathbb{N}^4$ and where $P \in \mathbb{F}_q[X]$ is an irreducible polynomial of degree n.

Keygen(param): Samples $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$, $\boldsymbol{g} \in \mathcal{S}_n^n(\mathbb{F}_{q^m})$ and $(\boldsymbol{x},\boldsymbol{y}) \in \mathcal{S}_{w,1}^{2n}(\mathbb{F}_{q^m})$, computes $\mathbf{G} \in \mathbb{F}_{q^m}^{k\times n}$ a generator matrix of the Gabidulin code $\mathcal{G}_{\boldsymbol{g}}(n,k,m)$, sets $\mathsf{pk} = (\boldsymbol{g}, \boldsymbol{h}, \boldsymbol{s} = \boldsymbol{x} + \boldsymbol{h}\cdot\boldsymbol{y} \mod P)$ and $\mathsf{sk} = (\boldsymbol{x},\boldsymbol{y})$, returns $(\mathsf{pk},\mathsf{sk})$.

Encrypt($\mathsf{pk}, \mathbf{m}, \theta$): Uses randomness θ to generate $(\boldsymbol{r}_1, \boldsymbol{e}, \boldsymbol{r}_2) \in \mathcal{S}_{w_1}^{3n}(\mathbb{F}_{q^m})$, sets $\boldsymbol{u} = \boldsymbol{r}_1 + \boldsymbol{h}\cdot\boldsymbol{r}_2 \mod P$ and $\boldsymbol{r} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s}\cdot\boldsymbol{r}_2 + \boldsymbol{e} \mod P$, returns $\boldsymbol{c} = (\boldsymbol{u},\boldsymbol{v})$.

Decrypt($\mathsf{sk}, \boldsymbol{c}$): Returns $\mathcal{G}_{\boldsymbol{g}}.\mathsf{Decode}(\boldsymbol{v} - \boldsymbol{u}\cdot\boldsymbol{y} \mod P)$.

A first remark is that the code $\mathcal{G}_{\boldsymbol{g}}(n,k,m)$ is publicly known. Therefore, as already mentioned, the security is not related to masking a Gabidulin code. It turns out that the unique hardness assumption to prove IND-CPA is the difficulty of the ideal version of RD. More concretely, one can hope to attack two types of instances:

$$\begin{bmatrix}\boldsymbol{x} & \boldsymbol{y}\end{bmatrix}\begin{bmatrix}\boldsymbol{I}_n & \mathcal{IM}(\boldsymbol{h})\end{bmatrix}^{\mathsf{T}} = \boldsymbol{s}, \;\; |(\boldsymbol{x},\boldsymbol{y})| = w. \tag{8.1}$$

$$\begin{bmatrix}\boldsymbol{r}_1 & \boldsymbol{e} & \boldsymbol{r}_2\end{bmatrix}\begin{bmatrix}\boldsymbol{I}_n & 0 & \mathcal{IM}(\boldsymbol{h}) \\ 0 & \boldsymbol{I}_n & \mathcal{IM}(\boldsymbol{s})\end{bmatrix}^{\mathsf{T}} = \begin{bmatrix}\boldsymbol{u} & \boldsymbol{v} - \boldsymbol{m}\boldsymbol{G}\end{bmatrix}, \;\; |(\boldsymbol{r}_1,\boldsymbol{e},\boldsymbol{r}_2)| = w_1. \tag{8.2}$$

On the one hand, Equation (8.1) corresponds to an RD problem with parameters $(m, 2n, n, w)$ whose solutions lead to key-recovery. On the other hand, solving the instance of parameters $(m, 3n, n, w_1)$ given by Equation (8.2) allows to retrieve the message.

8.1.2 Non-Homogeneous Rank Decoding Problem

In RQC, the fact that these two instances do not come from masking a secret code is precisely why it was possible to replace the RD assumption by a more structured one. More precisely, [Agu+20] introduce the following problem:

Problem 8.1 ([Agu+20]). *Given a full-rank matrix* $\boldsymbol{H} \in \mathbb{F}_{q^m}^{2n\times 3n}$*, integers* $(w_1, w_2) \in \mathbb{N}^2$ *and* $\boldsymbol{s} \in \mathbb{F}_{q^m}^{2n}$*, find a vector* $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3) \in \mathbb{F}_{q^m}^{3n}$*,* $\boldsymbol{e}_1 \in \mathbb{F}_{q^m}^{n}$*,* $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n}$*,* $\boldsymbol{e}_3 \in \mathbb{F}_{q^m}^{n}$*, such that* $\boldsymbol{e}\boldsymbol{H}^\intercal = \boldsymbol{s}$*,* $|(\boldsymbol{e}_1, \boldsymbol{e}_3)| \leqslant w_1$*,* $|\boldsymbol{e}_2| \leqslant w_1 + w_2$ *and* $\mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_3) \subset \mathrm{Supp}(\boldsymbol{e}_2)$*.*

Concretely, instead of sampling a random $(\boldsymbol{r}_1, \boldsymbol{e}, \boldsymbol{r}_2) \in \mathcal{S}_{w_1}^{3n}(\mathbb{F}_{q^m})$, the new variant [Agu+20] picks a random $(\boldsymbol{r}_1, \boldsymbol{e}, \boldsymbol{r}_2) \in \mathbb{F}_{q^m}^{3n}$ such that $|(\boldsymbol{r}_1, \boldsymbol{r}_2)| = w_1$, $|\boldsymbol{e}| = w_1 + w_2$ and $\mathrm{Supp}(\boldsymbol{r}_1, \boldsymbol{r}_2) \subset \mathrm{Supp}(\boldsymbol{e})$, where $w_2 \in \mathbb{N}$ is an additional parameter. In this way, Equation (8.2) becomes an instance of Problem 8.1 where the error $\boldsymbol{e}$ has maximum weight. The rationale for using such an assumption was to have more flexibility when choosing the parameters. On the one hand, RD with parameters $(m, 3n, n, w_1)$ reduces to Problem 8.1 with $w_2 = 0$ [Agu+20, Proposition 2.1.1]. On the other hand, a non-homogeneous vector of weight (w_1, w_2) is both easier to decode and to store in practice than a random vector of weight $w_1 + w_2$ in $\mathbb{F}_{q^m}^{3n}$.

Problem 8.2 introduced in Section 3.3.5.2 and recalled below is a generalization of Problem 8.1 where the blocks $\boldsymbol{e}_1$, $\boldsymbol{e}_2$ and $\boldsymbol{e}_3$ do not have the same size. From now on, we will focus on this second version.

Problem 8.2 (Non-Homogeneous Rank Decoding (NHRD) problem). *Given a full-rank matrix* $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n+n_1)\times(2n+n_1)}$*, integers* $(w_1, w_2) \in \mathbb{N}^2$ *and* $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n+n_1}$*, find a vector* $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3) \in \mathbb{F}_{q^m}^{2n+n_1}$*,* $\boldsymbol{e}_1 \in \mathbb{F}_{q^m}^{n}$*,* $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n_1}$*,* $\boldsymbol{e}_3 \in \mathbb{F}_{q^m}^{n}$*, such that* $\boldsymbol{e}\boldsymbol{H}^\intercal = \boldsymbol{s}$*,* $|(\boldsymbol{e}_1, \boldsymbol{e}_3)| \leqslant w_1$*,* $|\boldsymbol{e}_2| \leqslant w_1 + w_2$ *and* $\mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_3) \subset \mathrm{Supp}(\boldsymbol{e}_2)$*.*

Remark 8.1. In the following, an instance of Problem 8.2 will be referred to as a NHRD instance of parameters (m, n, n_1, w_1, w_2).

8.1.3 Making RQC More Efficient

While NIST appreciated the absence of secret code in RQC, they pointed out slightly poorer performances compared to ROLLO [Ala+19, §3.16]. The need of greater efficiency was also increased by the recent algebraic attacks [Bar+20a; Bar+20b] since they lead to choose higher parameters.

In [BBBG23], we proposed a new version of the scheme with sizes reduced of the order of 50%. Moreover, similarly to [Agu+22], we managed to obtain a competitive variant without ideal structure. In this work, I was the sole contributor to the cryptanalysis of NHRD but I have not taken part in the design of the construction. Still, let us start by presenting the additions to [Agu+20] which explain why it can achieve such performance gains. First, we adopt the error distribution of Problem 8.2, namely $(\boldsymbol{r}_1, \boldsymbol{e}, \boldsymbol{r}_2)$ such that $|(\boldsymbol{r}_1, \boldsymbol{r}_2)| = w_1$, $|\boldsymbol{e}| = w_1 + w_2$ and $\mathrm{Supp}(\boldsymbol{r}_1, \boldsymbol{r}_2) \subset \mathrm{Supp}(\boldsymbol{e})$. The difference with Problem 8.1 is that we might consider $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n_1}$ with $n_1 \neq n$ if it is relevant.

Multiple syndromes. As pioneered in [Agu+22], several syndromes are packed in one ciphertext. For $n_1,\ n_2 \in \mathbb{N}$, let us denote by Fold(.) the linear map

$$\boldsymbol{v} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_{n_1}) \in \mathbb{F}_{q^m}^{n_1 n_2},\ \boldsymbol{v}_i \in \mathbb{F}_{q^m}^{n_2} \mapsto \left[\boldsymbol{v}_1^\mathsf{T} \dots \boldsymbol{v}_{n_1}^\mathsf{T}\right] \in \mathbb{F}_{q^m}^{n_2 \times n_1}.$$

Its inverse is denoted by Unfold(.). Let us also extend the dot product modulo P between vectors in $\mathbb{F}_{q^m}^{n_2}$ to the one by $\boldsymbol{M} \in \mathbb{F}_{q^m}^{n_2 \times n_1}$:

$$\boldsymbol{v} \cdot \boldsymbol{M} \stackrel{def}{=} \left[(\boldsymbol{v} \cdot \boldsymbol{M}_{*,1}^\mathsf{T})^\mathsf{T} \dots (\boldsymbol{v} \cdot \boldsymbol{M}_{*,n_1}^\mathsf{T})^\mathsf{T}\right].$$

The idea now is to consider n_2 non-homogeneous error vectors $(\boldsymbol{r}_1^{(j)}, \boldsymbol{e}^{(j)}, \boldsymbol{r}_2^{(j)})$ for $j \in \{1..n_2\}$ which have the same support. Here, the ideal structure requires to choose the three blocks $\boldsymbol{r}_1^{(j)},\ \boldsymbol{e}^{(j)}$ and $\boldsymbol{r}_2^{(j)}$ of the same size n_1. These errors are then grouped as the matrix $\left[\boldsymbol{R}_1\ \boldsymbol{E}\ \boldsymbol{R}_2\right] \in \mathbb{F}_{q^m}^{n_2 \times 3n_1}$ defined by

$$\forall j \in \{1..n_2\},\ (\boldsymbol{R}_1)_{j,*} \stackrel{def}{=} \boldsymbol{r}_1^{(j)},\ (\boldsymbol{E})_{j,*} \stackrel{def}{=} \boldsymbol{e}^{(j)} \text{ and } (\boldsymbol{R}_2)_{j,*} \stackrel{def}{=} \boldsymbol{r}_2^{(j)}.$$

For a message $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ of the same length as before, we pick $\boldsymbol{h} \in \mathbb{F}_{q^m}^{n_2}$ and we keep the definition $\boldsymbol{s} = \boldsymbol{x} + \boldsymbol{h} \cdot \boldsymbol{y} \in \mathbb{F}_{q^m}^{n_2}$, where $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{S}_{w,1}^{2n_2}(\mathbb{F}_{q^m})$. The new ciphertext is $(\boldsymbol{U}, \boldsymbol{V})$ with $\boldsymbol{U} = \boldsymbol{R}_1 + \boldsymbol{h} \cdot \boldsymbol{R}_2 \in \mathbb{F}_{q^m}^{n_2 \times n_1}$ and $\boldsymbol{V} = \text{Fold}(\boldsymbol{mG}) + \boldsymbol{s} \cdot \boldsymbol{R}_2 + \boldsymbol{E} \in \mathbb{F}_{q^m}^{n_2 \times n_1}$. Finally, decryption works as in the original scheme by decoding the vector $\text{Unfold}(\boldsymbol{V} - \boldsymbol{y} \cdot \boldsymbol{U})$ in the Gabidulin code generated by $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$. The crux is that this vector has the same weight as the n_2 individual errors because their supports have been taken equal.

This trick allows to significantly decrease the public key size. In the original scheme, recall that both public key and ciphertext could be seen as vectors whose length is a constant multiple of the code length n. This time, the ciphertext $(\boldsymbol{U}, \boldsymbol{V}) \in \mathbb{F}_{q^m}^{n_2 \times n_1} \times \mathbb{F}_{q^m}^{n_2 \times n_1}$ can be stored as a vector of length $2n_1 n_2$ (where $n_1 n_2$ plays the same role as n) but the quantities $\boldsymbol{h}$ and $\boldsymbol{s}$ which appear in pk have length n_2 instead of $n_1 n_2$. This represents a reduction by a factor of the order of n_1 compared to the size of the ciphertext.

Similarly to [Agu+22] where it was introduced, this technique comes at the price of relying on the RSL problem. More precisely, we require an ideal version with non-homogeneous errors, referred to as NHIRSL in [BBBG23, p. 9].

Changing the public code. Another contribution was to replace the public Gabidulin code by another one which can correct more errors under certain conditions. Its definition is as follows.

Definition 8.1 (Augmented Gabidulin code). Let $(k, n, n', m) \in \mathbb{N}^4$ such that $k \leqslant n' < m < n$. Let $\boldsymbol{g} = (g_1, \dots, g_{n'}) \in \mathcal{S}_{n'}^{n'}(\mathbb{F}_{q^m})$ and let $\overline{\boldsymbol{g}} \in \mathbb{F}_{q^m}^n$ which is equal to $\boldsymbol{g}$ padded with $n - n'$ extra zeroes on the right. The *Augmented Gabidulin code* $\mathcal{G}_{\overline{\boldsymbol{g}}}^+(n, n', k, m)$ is the code of parameters $[n, k]_{q^m}$ defined by

$$\mathcal{G}_{\overline{\boldsymbol{g}}}^+(n, n', k, m) \stackrel{def}{=} \left\{P(\overline{\boldsymbol{g}}) : \deg_q(P) < k\right\},$$

where P ranges through the set of q-polynomials, $\deg_q(.)$ is the q-degree and $P(\overline{\boldsymbol{g}}) \stackrel{def}{=} (P(g_1), \ldots, P(g_{n'}), 0, \ldots, 0)$.

The motivation is to go beyond the correction capacity $\lfloor \frac{n'-k}{2} \rfloor$ of a Gabidulin code of parameters $[n', k]_{q^m}$ for some noise patterns. Indeed, for any $\epsilon \in \{1..\min(n-n', n'-k)\}$, a code as in Definition 8.1 can decode in a deterministic way errors of weight $\leqslant \lfloor \frac{n'-k+\epsilon}{2} \rfloor$ whose last $n-n'$ coordinates span a vector space of dimension $\geqslant \epsilon$. In the general case, this gives an algorithm with non-zero DFR by making a bet on the dimension on this subspace [BBBG23, Proposition 2].

Removing ideal matrices. The gain in performance provided by these modifications has led us to propose a non-structured version which remains very efficient. Roughly speaking, the secret key now contains matrices $(\boldsymbol{X}, \boldsymbol{Y})$ and the dot products $\boldsymbol{h} \cdot \boldsymbol{R}_2$, $\boldsymbol{s} \cdot \boldsymbol{R}_2$ are replaced by a standard matrix products $\boldsymbol{R}_2\boldsymbol{H}$ and $\boldsymbol{R}_2\boldsymbol{S}$ respectively, where $\boldsymbol{H}$ is a random matrix and where $\boldsymbol{S} = \boldsymbol{X} + \boldsymbol{H}\boldsymbol{Y}$. Since we still want to keep n_2 syndromes and to decode in a code of length $n_1 n_2$, the number of columns in $\boldsymbol{S}$ and thus $\boldsymbol{X}$, $\boldsymbol{Y}$ must be n_1. However, there is no constraint on the number of rows apart from the fact that it is the same as the width of $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$. Concretely, the latter will be an integer denoted by n (be careful that the code length is $n_1 n_2$ here) which has no relationship with neither n_1 nor n_2. This flexibility justifies the use of Problem 8.2 with $n \neq n_1$ and it explains why our non-ideal variant can achieve competitive sizes.

8.1.4 Algebraic Analysis of NHRD

Already at the time of [Agu+20], the introduction of NHRD lead the RQC submitters to analyze the new modelings of [Bar+20b] in this structured context. In particular, they remarked that the shape of the error could be exploited to decrease the number of minor variables.

To see this, let us consider a non-homogeneous vector $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$ where $\boldsymbol{e}_1,\ \boldsymbol{e}_3 \in \mathbb{F}_{q^m}^n$, $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n_1}$, $|(\boldsymbol{e}_1, \boldsymbol{e}_3)| \leqslant w_1$, $|\boldsymbol{e}_2| \leqslant w_1 + w_2$ and $\mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_3) \subset \mathrm{Supp}(\boldsymbol{e}_2)$. In [Agu+20, §6.2.2], the row support of $\mathrm{Mat}(\boldsymbol{e}) \in \mathbb{F}_q^{m \times (2n+n_1)}$ is written as

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_1 & \boldsymbol{C}_2 & \boldsymbol{C}_3 \\ 0 & \boldsymbol{C}_2' & 0 \end{bmatrix} \in \mathbb{F}_q^{(w_1+w_2)\times(2n+n_1)},$$

where $\boldsymbol{C}_1,\ \boldsymbol{C}_3 \in \mathbb{F}_q^{w_1 \times n}$, $\boldsymbol{C}_2 \in \mathbb{F}_q^{w_1 \times n_1}$ and $\boldsymbol{C}_2' \in \mathbb{F}_q^{w_2 \times n_1}$. The point now is that all the minors $|\boldsymbol{C}|_{*,T}$, $\#T = w_1 + w_2$ such that $T \cap \{n+1..n+n_1\} \leqslant w_2 - 1$ vanish. As a consequence, [Agu+20, §6.2.2] suggest to fix the corresponding unknowns to zero in the MaxMinors and Support-Minors systems. This set of variables is given by

$$\zeta \stackrel{def}{=} \{c_T : \#T = w_1 + w_2 \text{ and } \#(T \cap \{n+1..n+n_1\}) \leqslant w_2 - 1\} \tag{8.3}$$

and it is of cardinality

$$M \stackrel{def}{=} \#\zeta = \sum_{i=0}^{w_2-1} \binom{n_1}{i} \binom{2n}{w_1+w_2-i}. \tag{8.4}$$

While the resulting modeling is clearly easier to solve since there are less variables, we noticed that there were linear dependencies in the specialized system that had not been taken into account in [Agu+20, §6.2.2].

8.2 Understanding MaxMinors on NHRD

In this section, we explain why we find less linearly indepedendent equations in the MaxMinors modeling when the abovementioned minor variables are fixed to zero. We then give a more realistic complexity formula for the MaxMinors attack.

As in the plain case, our analysis is on the system over $\mathbb{F}_{q^m}$ before projecting the equations. There, this system was referred to as the MaxMinors system over $\mathbb{F}_{q^m}$, MM-$\mathbb{F}_{q^m}$ or even Modeling 6. For the sake of simplicity, we will keep the same names in this structured setting. The final cost estimate will be deduced in the same way as in RD by assuming that there are no extra relations in the projected equations. Since NHRD does not rely more heavily on the extension field than RD, we believe that such an hypothesis is not significantly stronger than our assumption in the latter situation – Assumption 1 – stating that the equations of the projected MaxMinors modeling (*e.g.*, MM-$\mathbb{F}_q$ or Modeling 7) were as linearly independent as possible. Still, as there are less unknowns in the present case, the cancellation of few correlated coefficients (which is likely to happen over $\mathbb{F}_q$ for small q) may have more impact.

8.2.1 Effect of Fixing Variables

We now study the behaviour of the equations over $\mathbb{F}_{q^m}$ under the relevant specialization. First, let us recall the following result that we have already used in Chapter 7.

Lemma 8.1 (Proposition 2, [Bar+20b]). *With the notation of the MaxMinors modeling over $\mathbb{F}_{q^m}$ (Modeling 6), we have*

$$P_J = c_{J+n+1} + \sum_{\substack{T^- \subset \{1..n+1\}, T^+ \subset (J+n+1) \\ T = T^- \cup T^+,\ \#T = w_1+w_2,\ T^- \neq \varnothing}} c_T |\boldsymbol{H}_{\boldsymbol{y}}|_{J,T}. \tag{8.5}$$

Similarly, we will sort the minor variables c_T with reverse lexicographical order according to T. The leading term of P_J is then equal to c_{J+n+1}.

To analyze the system, Equation (8.3) lead us to separate the initial MaxMinors equations into several subsets in function of the presence or the absence of elements of ζ in such polynomials. More precisely, we consider the partition $\mathcal{P} = \mathcal{P}_{\text{lost}} \sqcup \mathcal{P}_{\text{rest}} \sqcup \mathcal{P}_{\text{indep}}$, where

$$\begin{aligned}
\mathcal{P}_{\text{lost}} &\overset{def}{=} \{P_J : \#J = w_1 + w_2 \text{ and } \#(J \cap \{1..(n_1-1)\}) \leqslant w_2 - 2\}, \\
\mathcal{P}_{\text{rest}} &\overset{def}{=} \{P_J : \#J = w_1 + w_2 \text{ and } \#(J \cap \{1..(n_1-1)\}) = w_2 - 1\}, \\
\mathcal{P}_{\text{indep}} &\overset{def}{=} \{P_J : \#J = w_1 + w_2 \text{ and } \#(J \cap \{1..(n_1-1)\}) \geqslant w_2\}.
\end{aligned}$$

Using Lemma 8.1, it is easy to grasp the shape of the equations from $\mathcal{P}_{\text{lost}}$ and $\mathcal{P}_{\text{indep}}$ after specialization.

Lemma 8.2. *By fixing the minor variables from ζ to zero in Modeling 6,*

1. *The equations in $\mathcal{P}_{lost}$ all become the zero polynomial.*
2. *The equations in $\mathcal{P}_{indep}$ keep the same leading terms so that they remain linearly independent. They generate a space of dimension*

$$\#\mathcal{P}_{indep} = \textstyle\sum_{i=w_2}^{w_1+w_2} \binom{n_1-1}{j}\binom{n}{w_1+w_2-j}.$$

Proof. For the first item, let us consider $J \subset \{1..n+n_1-1\}$, $\#J = w_1+w_2$ such that $P_J \in \mathcal{P}_{\text{lost}}$. By definition of $\mathcal{P}_{\text{lost}}$, the intersection of $J+n+1$ with $\{n+2..n+n_1\}$ is of size $\leqslant w_2-2$. Thus, any subset $T = T^- \cup T^+ \subset \{1..2n+n_1\}$ such that $T^- \subset \{1..n+1\}$ and $T^+ \subset J+n+1$ satisfies $\#(T \cap \{n+1..n+n_1\}) \leqslant w_2-1$ (because T^- might also contain $n+1$). By Equation (8.3), this means that $c_T \in \zeta$. The conclusion follows from the expression of P_J given in Equation (8.5).

For the second item, recall that the leading monomials in Modeling 6 are initially all different and that the one of P_J is equal to c_{J+n+1}. When $P_J \in \mathcal{P}_{\text{indep}}$, this variable does not belong to ζ since $\#(J+n+1 \cap \{n+2..n+n_1\}) = \#(J \cap \{1..n_1-1\}) \geqslant w_2$. Therefore, the leading terms are unchanged in $\mathcal{P}_{\text{indep}}$ and the equations are still linearly independent. The last statement on the dimension is obvious. □

Contrary to the ones in $\mathcal{P}_{\text{indep}}$, the equations in $\mathcal{P}_{\text{rest}}$ have their leading monomials included in ζ. Thus, in these polynomials, the leading term is affected by fixing variables. More precisely, using Lemma 8.1, an equation $P_J \in \mathcal{P}_{\text{rest}}$ becomes

$$\begin{aligned}\widetilde{P_J} &\stackrel{def}{=} \sum_{\substack{T^- \subset \{1..n+1\},\ T^+ \subset (J+n+1) \\ T=T^- \cup T^+,\ n+1 \in T^-,\ \#(T^+ \cap \{n+2..n+n_1\}) = w_2-1}} c_T |\boldsymbol{H_y}|_{J,T} \\ &= \sum_{\substack{T^- \subset \{1..n+1\},\ T^+ \subset (J+n+1) \\ T=T^- \cup T^+,\ n+1 \in T^-,\ T^+ \cap \{n+2..n+n_1\} = (J \cap \{1..(n_1-1)\})+n+1}} c_T |\boldsymbol{H_y}|_{J,T}. \end{aligned} \tag{8.6}$$

From now on, to simplify the notation, we still denote the specialized system by $\mathcal{P}_{\text{rest}} = \{\widetilde{P_J}\}_J$. We study it in Proposition 8.1.

Proposition 8.1. *The equations from the specialized system $\mathcal{P}_{rest}$ are independent from from the set of polynomials $\mathcal{P}_{indep}$. They generate an $\mathbb{F}_{q^m}$-vector space of dimension $\binom{n_1-1}{w_2-1}\binom{n-1}{w_1}$ and they contain at most $\binom{n_1-1}{w_2-1}\binom{2n}{w_1}$ variables.*

The first statement of Proposition 8.1 is clear. Using Equation (8.6), the leading monomial of $\widetilde{P_J} \in \mathcal{P}_{\text{rest}}$ is a c_T variable such that $n+1 \in T$ while the one of any $P_{J'} \in \mathcal{P}_{\text{indep}}$ is $c_{J'+n+1}$ which is necessarily greater. Thus, what is left to prove in Proposition 8.1 is that $\mathcal{P}_{\text{rest}}$ spans a space of dimension $\binom{n_1-1}{w_2-1}\binom{n-1}{w_1}$ and that the number of variables is $\binom{n_1-1}{w_2-1}\binom{2n}{w_1}$. For this we rely on the following results.

Lemma 8.3. *For any subset $A \subset \{n+2..n+n_1\}$ such that $\#A = w_2 - 1$, let*

$$\mathcal{P}_{rest,A} \stackrel{def}{=} \{P_J : P_J \in \mathcal{P}_{rest} \text{ and } J \cap \{1..n_1-1\} = A - (n+1)\}. \tag{8.7}$$

The polynomials in $\mathcal{P}_{rest,A}$ have their monomials included in a set μ_A of size $\binom{2n}{w_1}$. Moreover, for any $A \neq A'$, the sets μ_A and $\mu_{A'}$ are disjoint.

Lemma 8.4. *For any subset $A \subset \{n+2..n+n_1\}$ such that $\#A = w_2 - 1$, let $\mathcal{P}_{rest,A}$ as defined in Equation (8.7). We have*

$$\dim_{\mathbb{F}_{q^m}} \langle \mathcal{P}_{rest,A} \rangle \geqslant \tbinom{n-1}{w_1}. \tag{8.8}$$

Conjecture 8.1. *For any subset $A \subset \{n+2..n+n_1\}$ such that $\#A = w_2 - 1$, we will assume that Equation (8.8) is an equality.*

Before giving more details on the proofs, let us remark that Proposition 8.1 indeed follows. First, Lemma 8.3 shows that we have the direct sum of $\mathbb{F}_{q^m}$-vector spaces

$$\langle \mathcal{P}_{\text{rest}} \rangle = \bigoplus_{A \subset \{n+2..n+n_1\},\ \#A = w_2-1} \langle \mathcal{P}_{\text{rest},A} \rangle \tag{8.9}$$

and that the total number of monomials is at most

$$\tbinom{2n}{w_1} \times \#\{A : A \subset \{n+2..n+n_1\} \text{ and } \#A = w_2 - 1\} = \tbinom{2n}{w_1}\tbinom{n_1-1}{w_2-1}.$$

Then, the dimension $\langle \mathcal{P}_{\text{rest}} \rangle$ is obtained from the direct sum of Equation (8.9) and from that of the $\langle \mathcal{P}_{\text{rest},A} \rangle$'s provided by Conjecture 8.1.

Proof of Lemma 8.3. Equation (8.6) shows that we can take

$$\mu_A \stackrel{def}{=} \left\{c_T : T \subset \{1..2n+n_1\},\ \#T = w_1+w_2 \text{ and } n+1 \in T \text{ and } T \cap \{n+2..n+n_1\} = A\right\}.$$

This set is of size $\binom{2n}{w_1}$ and it satisfies $\mu_A \cap \mu'_A = \varnothing$ when $A \neq A'$. □

Proof of Lemma 8.4. Using Equation (8.6) once again, it is readily verified that the set of leading monomials of all equations in $\mathcal{P}_{\text{rest},A}$ is

$$\tau_A \stackrel{def}{=} \left\{c_{\{n+1\}\cup A\cup U} : U \subset \{(n+n_1+2)..(2n+n_1)\},\ \#U = w_1\right\}.$$

Since the equation P_{J_U} with $J_U + n + 1 = A \cup \{n+n_1+1\} \cup U$ has leading monomial $c_{\{n+1\}\cup A\cup U} \in \tau_A$, this shows that $\dim_{\mathbb{F}_{q^m}} \langle \mathcal{P}_{\text{rest},A} \rangle \geqslant \#\tau_A = \binom{n-1}{w_1}$. □

Before moving on to the next section, we give a sketch of reasoning for Conjecture 8.1. Note that a greater dimension than claimed in this conjecture for $\langle \mathcal{P}_{\text{rest},A} \rangle$ would be in the attacker's favour.

Argument for Conjecture 8.1. We implicitly use a randomness assumption on the entries of the P_J's in $\mathbb{F}_{q^m}$ that we will not formalize any further. More precisely, we want to argue that there is no element in $\langle \mathcal{P}_{\text{rest},A} \rangle$ whose leading term does not belong to τ_A. Let us consider $V_J \stackrel{def}{=} \left\{ v_1^{(J)} < \cdots < v_{w_1+1}^{(J)} \right\}$ such that $P_J \in \mathcal{P}_{\text{rest},A}$ with $J+n+1 \stackrel{def}{=} A \cup V_J$. The variables from P_J which belong to τ_A are the $c_{\{n+1\}\cup A \cup V_J \setminus \{v_j^{(J)}\}}$'s such that $1 \leqslant j \leqslant w_1+1$. To kill its leading monomial, we have to add an equation with the same one, namely some P'_J with $J' \neq J$, $J'+n+1 = A \cup V_{J'}$ and such that $V_{J \setminus \{v_1^{(J)}\}} = V_{J' \setminus \{v_1^{(J')}\}} = B$ for some subset B of size w_1+w_2-1. In this case, one can check that the only monomial from τ_A present in both P_J and $P_{J'}$ is $c_{\{n+1\}\cup A \cup B}$. This means that $P_J + \lambda_{J'} P_{J'}$ contains at least $2w_1$ monomials from τ_A. Similarly, by using a third subset J'', we can kill at most one extra monomial in P_J and in the worst case one in $P_{J'}$ as well. This implies that a linear combination of the form $P_J + \lambda_{J'} P_{J'} + \lambda_{J''} P_{J''}$ will contain at least $2(w_1-1) + (w_1+1-2) = 3(w_1-1)$ monomials from τ_A, the lower bound being reached if and only if those monomials in P_J and P'_J are killed at the same time by $\lambda_{J''} P_{J''}$. This is extremely unlikely if the coefficients of the MaxMinors equations are random in $\mathbb{F}_{q^m}$. Thus, we may assume instead that $P_J + \lambda_{J'} P_{J'} + \lambda_{J''} P_{J''}$ contains at least $(w_1-1) + w_1 + (w_1+1-1) = 3w_1 - 1$ monomials in τ_A. Relying on the same type of assumption, one can proceed by induction on the numbers of terms to show that a non-zero linear combination in $\langle \mathcal{P}_{\text{rest},A} \rangle$ always has a monomial in τ_A. □

8.2.2 Solving the Projected System

Since we keep the same method as in the non-structured case, we need to consider equations unfolded over the small field. More precisely, we will project the specialized systems $\mathcal{P}_{\text{indep}}$ and (a basis of) $\mathcal{P}_{\text{rest}}$ over $\mathbb{F}_q$. As already mentioned, we do not expect extra relations apart from those triggered by a too small number of monomials.

Assumption 10. *Let $\mathcal{P}_{indep,\mathbb{F}_q}$ (resp. $\mathcal{P}_{rest,\mathbb{F}_q}$) be the system over $\mathbb{F}_q$ obtained by projecting $\mathcal{P}_{indep}$ (resp. a basis of $\mathcal{P}_{rest}$), let $\mathcal{N}_{\mathbb{F}_q} \stackrel{def}{=} \dim_{\mathbb{F}_q} \langle \mathcal{P}_{indep,\mathbb{F}_q} \rangle$, let $\nu_{\mathbb{F}_q} \stackrel{def}{=} \dim_{\mathbb{F}_q} \langle \mathcal{P}_{rest,\mathbb{F}_q} \rangle$ and let M as defined in Equation (8.4). We assume that*

$$\mathcal{N}_{\mathbb{F}_q} = \min\left(m \sum_{i=w_2}^{w_1+w_2} \tbinom{n_1-1}{i} \tbinom{n}{w_1+w_2-i}, \tbinom{2n+n_1}{w_1+w_2} - M - 1 \right)$$

and

$$\nu_{\mathbb{F}_q} = m \dim_{\mathbb{F}_{q^m}} \langle \mathcal{P}_{rest} \rangle = m \tbinom{n_1-1}{w_2-1} \tbinom{n-1}{w_1},$$

provided that the latter is $\leqslant \binom{n_1-1}{w_2-1}\binom{2n}{w_1}$.

Remark 8.2. We chose not to give an estimation of $\nu_{\mathbb{F}_q}$ when $m\binom{n_1-1}{w_2-1}\binom{n-1}{w_1} > \binom{n_1-1}{w_2-1}\binom{2n}{w_1}$. For cryptographic parameters, we always had $m\binom{n-1}{w_1} \ll \binom{2n}{w_1}$. Interestingly enough, our Magma experiments were inconclusive in the other scenario.

Since the system $\mathcal{P}_{\text{rest},\mathbb{F}_q}$ is very underdetermined, one can imagine to use its equations to substitute $\nu_{\mathbb{F}_q}$ variables in the system $\mathcal{P}_{\text{indep},\mathbb{F}_q}$ to get a new system $\mathcal{P}'_{\text{indep},\mathbb{F}_q}$. As we do no longer control the leading terms in the projected modelings, we make an additional assumption.

Assumption 11. *Let $\mathcal{P}'_{indep,\mathbb{F}_q}$ the system constructed from $\mathcal{P}_{rest,\mathbb{F}_q}$ and $\mathcal{P}_{indep,\mathbb{F}_q}$ as described above. We assume that*

$$\dim_{\mathbb{F}_q}\langle \mathcal{P}'_{indep,\mathbb{F}_q}\rangle = \min\left(\dim_{\mathbb{F}_q}\langle \mathcal{P}_{indep,\mathbb{F}_q}\rangle, \tbinom{2n+n_1}{w_1+w_2} - M - \nu_{\mathbb{F}_q} - 1\right).$$

Theorem 8.1 (Under Assumptions 10 and 11). *Let $\mathcal{P}_{indep,\mathbb{F}_q}$ and $\mathcal{P}_{rest,\mathbb{F}_q}$ denote the projections of $\mathcal{P}_{indep}$ and a basis of $\mathcal{P}_{rest}$ respectively. We consider $\mathcal{P}'_{indep,\mathbb{F}_q}$ the linear system obtained from $\mathcal{P}_{indep,\mathbb{F}_q}$ by plugging $\nu_{\mathbb{F}_q}$ equations from the echelon form of $\mathcal{P}_{rest,\mathbb{F}_q}$ to substitute variables. When $\mathcal{N}_{\mathbb{F}_q} \geqslant \binom{2n+n_1}{w_1+w_2} - M - \nu_{\mathbb{F}_q} - 1$, we can solve the NHRD instance of parameters (m, n, n_1, w_1, w_2) by inverting $\mathcal{P}'_{indep,\mathbb{F}_q}$. The complexity in $\mathbb{F}_q$-operations is*

$$\mathcal{O}\left(\mathcal{N}_{\mathbb{F}_q}\left(\tbinom{2n+n_1}{w_1+w_2} - M - \nu_{\mathbb{F}_q}\right)^{\omega-1}\right),$$

where ω is a linear algebra constant.

When the condition of Theorem 8.1 does not hold, we propose a similar hybrid approach as in the RD case. In fact, like it was done in [Agu+20, p. 6.2.2], we can take advantage of the particular structure of $\boldsymbol{C}$ by fixing columns containing only w_1 non-zero coordinates in Equation (8.1.4). Indeed, this leads to a smaller exponential factor of q^{aw_1} in the final cost compared to the naive $q^{a(w_1+w_2)}$.

Corollary 8.1 (Under Assumptions 10 and 11). *Let $a \in \mathbb{N}$ be the smallest integer such that*

$$\mathcal{N}_{\mathbb{F}_q} \geqslant \tbinom{2n+n_1-a}{w_1+w_2} - M_a - \nu_{\mathbb{F}_q} - 1, \tag{8.10}$$

where $M_a \overset{def}{=} \sum_{i=0}^{\omega_2-1}\binom{n_1}{i}\binom{2n-a}{\omega_1+\omega_2-i}$. The complexity in $\mathbb{F}_q$ operations of the hybrid approach on $\mathcal{P}'_{indep,\mathbb{F}_q}$ by fixing $a \geqslant 0$ columns in $\{1..n\} \cup \{n+n_1+1..2n+n_1\}$ is

$$\mathcal{O}\left(q^{aw_1}\mathcal{N}_{\mathbb{F}_q}\left(\tbinom{2n+n_1-a}{w_1+w_2} - M_a - \nu_{\mathbb{F}_q}\right)^{\omega-1}\right),$$

where ω is a linear algebra constant.

Remark 8.3. In Theorem 8.1 and Corollary 8.1, it is possible to remove Assumption 11 if we simply attempt to invert the system $\mathcal{P}_{\text{indep},\mathbb{F}_q}$. Since we consider less equations, this will require a slightly stronger constraint on the parameters.

Finally, note that we have not tried to analyze Support-Minors (Modeling 4) in this particular case. From a practical perspective, finding non-homogeneous error patterns with rather small parameters to perform experiments but which do not lead to degenerated systems was more difficult than for RD. In addition, the new results presented in Chapter 7 were not known at that time.

8.3 New Combinatorial Attack on NHRD

We also proposed a combinatorial approach which exploits the specific shape of the error support. Recall that we are interested in noises of the form $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3) \in \mathbb{F}_{q^m}^{2n+n_1}$, $\boldsymbol{e}_1,\ \boldsymbol{e}_3 \in \mathbb{F}_{q^m}^{n}$ and $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n_1}$, such that $S_1 \stackrel{def}{=} \mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_3)$ is of dimension w_1, $S_2 \stackrel{def}{=} \mathrm{Supp}(\boldsymbol{e}_2)$ is of dimension $w_1 + w_2$ and $S_1 \subset S_2$.

The only change in our algorithm compared to the plain RD setting lies in the guessing step. For instance, we still make use of the parity-check equations from the augmented code $\mathcal{C}_{\boldsymbol{y}} \stackrel{def}{=} \mathcal{C} \oplus \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$ with full-rank parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}} \in \mathbb{F}_{q^m}^{(n+n_1-1)\times(2n+n_1)}$. Since the support of the entire vector $\boldsymbol{e}$ is S_2, applying the naive technique by forgetting the structure would consist in picking a candidate subspace V of dimension $r \geqslant w_1 + w_2$ containing S_2. To take advantage of the error pattern, our idea instead is to guess a V of dimension $r \geqslant w_1$ such that $S_1 \subset V$ and a tiny chunk Z of dimension $\rho \in \{1..m-r\}$ such that V and Z are linearly independent and $S_2 \subset V \oplus Z$. The motivation is to increase the success probability even if it may cause a higher number of variables in the linear system.

The rest of the approach is the same as in RD. Concretely, in the system $(\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)\boldsymbol{H}_{\boldsymbol{y}}^{\mathsf{T}} = \boldsymbol{0}$, we express the coordinates of $(\boldsymbol{e}_1, \boldsymbol{e}_3)$ in a fixed basis of V by introducing $2nr$ unknowns over $\mathbb{F}_q$ and those of $\boldsymbol{e}_2$ in a fixed basis of $V \oplus Z$ by adding $n_1(r+\rho)$ extra variables. Then, we project the equations over $\mathbb{F}_q$. Finally, as long as

$$m(n + n_1 - 1) \geqslant 2nr + n_1(r + \rho), \tag{8.11}$$

we can check the consistency of our guess by inverting the resulting linear system.

For values of $r,\ \rho$ such that Equation (8.11) holds, we give an estimate of the success probability in Section 8.3.1. We then deduce the cost of our technique in Sections 8.3.2 and 8.3.3.

8.3.1 Probability of a Correct Guess

Let us recall that $S_1 = \mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_3)$ and $S_2 = \mathrm{Supp}(\boldsymbol{e}_2)$ are such that $S_1 \subset S_2$. We consider $\Pi \stackrel{def}{=} \Pr_{V,Z}[S_1 \subset V,\ S_2 \subset V \oplus Z]$, where the randomness is taken over randomly sampled $\mathbb{F}_q$-subspaces $V,\ Z \subset \mathbb{F}_{q^m}$ which are in direct sum.

Lemma 8.5. *We have*

$$\begin{aligned}\Pi &= \Pr_{V,Z}[S_1 \subset V,\ S_2/S_1 \subset (V \oplus Z + S_1)/S_1] \\ &= \Pr_{V}[S_1 \subset V] \Pr_{V,Z}[S_2/S_1 \subset (V \oplus Z + S_1)/S_1 \mid S_1 \subset V].\end{aligned}$$

Proof. We prove the first equality since the second one is just the definition of conditional probability. Let π denote the projection $\mathbb{F}_{q^m} \to \mathbb{F}_{q^m}/S_1$ and let us consider the events $A \stackrel{def}{=}$ "$S_1 \subset V,\ S_2 \subset V \oplus Z$" and $B \stackrel{def}{=}$ "$S_1 \subset V,\ S_2/S_1 \subset (V \oplus Z + S_1)/S_1$". We show

$A = B$ by double-inclusion. By applying the projection map we already obtain $A \subset B$. If we take the inverse image we get $B \subset \pi^{-1}(B)$, where

$$\pi^{-1}(B) \stackrel{def}{=} \text{“}S_1 \subset V \text{ and } \pi^{-1}(\pi(S_2)) \subset \pi^{-1}(\pi(V \oplus Z + S_1))\text{”}. \tag{8.12}$$

Observe now that the event “$\pi^{-1}(\pi(S_2)) \subset \pi^{-1}(\pi(V \oplus Z + S_1))$” is more explicitly equal to

$$\begin{aligned}\text{“}S_2 \ + \ \ker(\pi) = S_2 \ + \ S_1 = S_2 \\ \subset V \oplus Z + S_1 \ + \ \ker(\pi) = V \oplus Z + S_1 + S_1 = V \oplus Z + S_1\text{.”}\end{aligned}$$

Hence $\pi^{-1}(B) = \text{“}S_1 \subset V,\ S_2 \subset V \oplus Z + S_1\text{”} = \text{“}S_1 \subset V,\ S_2 \subset V \oplus Z\text{”} = A$. □

In Π, the first factor $\Pr_V[S_1 \subset V]$ is easy to deal with so we will focus on the second one. We denote it by $\Pi_{\text{cond}} \stackrel{def}{=} \Pr_{V,Z}[S_2/S_1 \subset (V \oplus Z + S_1)/S_1 \mid S_1 \subset V]$. Note that we have the decomposition into disjoint events

$$\begin{aligned}\{S_2/S_1 \subset (V \oplus Z + S_1)/S_1 \mid S_1 \subset V\} &= \{S_2/S_1 \subset (V \oplus Z)/S_1\} \\ &= \coprod_{\ell=0}^{w_2} \left\{ \dim_{\mathbb{F}_q}(S_2/S_1 \cap V/S_1) = \ell,\ \frac{S_2/S_1}{S_2/S_1 \cap V/S_1} \subset \frac{(V \oplus Z)/S_1}{V/S_1} \right\} \\ &= \coprod_{\ell=0}^{w_2} \{A_\ell \cap B\},\end{aligned}$$

where $A_\ell \stackrel{def}{=} \text{“}\dim_{\mathbb{F}_q}(S_2/S_1 \cap V/S_1) = \ell\text{”}$ and $B \stackrel{def}{=} \text{“}\frac{S_2/S_1}{S_2/S_1 \cap V/S_1} \subset \frac{(V \oplus Z)/S_1}{V/S_1}\text{”}$. For $\ell \in \{0..w_2\}$, let $p_\ell \stackrel{def}{=} \Pr[A_\ell \cap B]$, let $s_\ell \stackrel{def}{=} \Pr[A_\ell]$ and let $t_\ell \stackrel{def}{=} \Pr[B \mid A_\ell]$ so that $p_\ell = s_\ell t_\ell$ and $\Pi_{\text{cond}} = \sum_{\ell=0}^{w_2} p_\ell$. To compute the first factor s_ℓ, we rely on

Lemma 8.6 (Lemma 9.3.2 p. 269, [BCN89]). *Let F be an $\mathbb{F}_q$-linear space of dimension n.*

1. *If X is a j-dimensional subspace of F, then there are $q^{ij}\binom{n-j}{i}_q$ i-dimensional subspaces Y such that $X \cap Y = 0$.*
2. *If X is a j-dimensional subspace of F, then there are $q^{(i-\ell)(j-\ell)}\binom{n-j}{i-\ell}_q\binom{j}{\ell}_q$ i-dimensional subspaces Y such that $X \cap Y$ has dimension ℓ.*

More precisely, we use item 2. with $F = \mathbb{F}_{q^m}/S_1$, fixed $X = S_2/S_1 \subset \mathbb{F}_{q^m}/S_1$ of dimension $j = w_2$ and random $Y = V/S_1 \subset \mathbb{F}_{q^m}/S_1$ of dimension $i = r - w_1$. We obtain

$$s_\ell = q^{(r-w_1-\ell)(w_2-\ell)} \frac{\binom{m-w_1-w_2}{r-w_1-\ell}_q \binom{w_2}{\ell}_q}{\binom{m-w_1}{r-w_1}_q}. \tag{8.13}$$

For the second factor t_ℓ, note that condionned on $\dim_{\mathbb{F}_q}(S_2/S_1 \cap V/S_1) = \ell$ the probability that $\frac{S_2/S_1}{S_2/S_1 \cap V/S_1} \subset \frac{(V \oplus Z)/S_1}{V/S_1}$ is the probability that a random subspace of dimension ρ

contains a fixed subspace of dimension $w_2 - \ell$ in the ambient space $\frac{\mathbb{F}_{q^m}/S_1}{V/S_1} \simeq \mathbb{F}_{q^m}/V$. From there we obtain

$$t_\ell = \frac{\binom{\rho}{w_2-\ell}_q}{\binom{m-r}{w_2-\ell}_q}. \tag{8.14}$$

Finally, by combining Equation (8.13) and Equation (8.14),

$$p_\ell = q^{(r-w_1-\ell)(w_2-\ell)} \frac{\binom{m-w_1-w_2}{r-w_1-\ell}_q \binom{w_2}{\ell}_q}{\binom{m-w_1}{r-w_1}_q} \frac{\binom{\rho}{w_2-\ell}_q}{\binom{m-r}{w_2-\ell}_q}. \tag{8.15}$$

Recall that we were interested in the sum $\Pi_{\text{cond}} = \sum_{\ell=0}^{w_2} p_\ell$. We show in Lemma 8.7 that we can approximate it by its first term.

Lemma 8.7. *Let $\Pi_{cond} = \sum_{\ell=0}^{w_2} p_\ell$, where p_ℓ is defined in Equation (8.15). We have*

$$p_0 < \Pi_{cond} < (q+3)p_0.$$

Proof. We only need to prove the upper bound on Π_{cond}. For $\ell \in \{0..w_2-1\}$, we consider the ratio $\Delta_\ell \stackrel{def}{=} p_{\ell+1}/p_\ell$. Using the identity $\binom{a+1}{b+1}_q = \frac{1-q^{a-b+1}}{1-q^{b+1}}\binom{a+1}{b}_q$, we compute explicitly

$$\begin{aligned}\Delta_\ell = q^{(r-w_1-\ell-1)(w_2-\ell-1)-(r-w_1-\ell)(w_2-\ell)} & \\ \times \frac{1-q^{r-w_1-\ell}}{1-q^{m-r-w_2+\ell+1}} \times \frac{1-q^{w_2-\ell}}{1-q^{\ell+1}} \times \frac{1-q^{w_2-\ell}}{1-q^{\rho-w_2+\ell+1}} \times \frac{1-q^{m-r-w_2+\ell+1}}{1-q^{w_2-\ell}} & \\ = q^{-(r-w_1-\ell)-(w_2-\ell-1)} \times \frac{(1-q^{r-w_1-\ell})(1-q^{w_2-\ell})}{(1-q^{\ell+1})(1-q^{\rho-w_2+\ell+1})}.\end{aligned}$$

Since $(1-q^{r-w_1-\ell})(1-q^{w_2-\ell}) < q^{r-w_1-\ell} \times q^{w_2-\ell}$, we then obtain

$$\begin{aligned}\Delta_\ell &\leqslant q^{-(r-w_1-\ell)-(w_2-\ell-1)} \times \frac{q^{r-w_1-\ell} \times q^{w_2-\ell}}{(1-q^{\ell+1})(1-q^{\rho-w_2+\ell+1})} = \frac{q}{(1-q^{\ell+1})(1-q^{\rho-w_2+\ell+1})} \\ &\leqslant \frac{q}{(q^{\ell+1}-1)^2} \leqslant q^{1-2\ell}.\end{aligned}$$

This gives $p_{\ell+1} \leqslant q^{1-2\ell} p_\ell$ and then by induction $p_\ell \leqslant q^{2\ell-\ell^2} p_0$ for any $\ell \in \{0..w_2-1\}$. By plugging this bound in the formula for Π_{cond}, this finally yields

$$\begin{aligned}\Pi_{\text{cond}} &< (1+q+1)p_0 + p_0 \sum_{j \geqslant 3} q^{2j-j^2} \\ &< (1+q+1)p_0 + p_0 \sum_{j \geqslant 3} q^{-j} = \left(2 + q + q^{-2}/(q-1)\right) p_0 < (q+3)p_0.\end{aligned}$$

□

Estimate 1. *We estimate the probability Π by $p_0 \Pr_V[S_1 \subset V]$, where p_0 is Equation (8.15) for $\ell = 0$ and where $\Pr_V[S_1 \subset V]$ is the probability that a randomly sampled r-dimensional subspace of $\mathbb{F}_{q^m}$ contains S_1.*

8.3.2 Complexity of the Approach

As in the case of standard combinatorial attacks on RD, the expression of the total cost is straightforward from the knowledge of the success probability. In fact, similarly to [AGHT18], we can take advantage of $\mathbb{F}_{q^m}$-linearity by considering a greater one of the form

$$\Pr_{V,Z}\left[\exists \alpha \in \mathbb{F}_{q^m}^*,\ \alpha S_1 \subset V,\ \alpha S_2 \subset V \oplus Z\right] \approx \frac{q^m-1}{q-1}\Pi. \tag{8.16}$$

Theorem 8.2. *As long as Equation (8.11) holds, the complexity of our algorithm in $\mathbb{F}_q$-operations can be estimated by*

$$\widetilde{\mathcal{O}}\left(q^{(w_1+w_2)(m-r)-w_2\rho-m}\right). \tag{8.17}$$

Proof. The polynomial factor coming from solving the final linear system is included in the $\widetilde{\mathcal{O}}$ notation. For the success probability, we use Equation (8.16) which gives a q^{-m} factor together with Estimate 1. Recall that

$$p_0 = q^{(r-w_1)w_2}\frac{\binom{m-w_1-w_2}{r-w_1}_q}{\binom{m-w_1}{r-w_1}_q}\frac{\binom{\rho}{w_2}_q}{\binom{m-r}{w_2}_q}.$$

Using $\binom{a}{b}_q = \Theta(q^{b(a-b)})$ when $\max(a,b) \to +\infty$ gives

$$p_0 = \Theta\left(q^{(r-w_1)w_2} \times q^{-(r-w_1)w_2} \times q^{-w_2(m-r-\rho)}\right) = \Theta(q^{-w_2(m-r-\rho)}).$$

The other term $\Pr_V[S_1 \subset V] = \binom{r}{w_1}_q / \binom{m}{w_1}_q$ is the classical one that is encountered in combinatorial attacks on RD. We obtain $\Theta\left(q^{-w_1(m-r)}\right)$ and the conclusion easily follows. □

The best cost obtained with such a strategy can be found by optimizing Equation (8.17) over values of (r,ρ) which yield an overdefined linear system. For this computation, we focus on the exponent of q and we neglect polynomial factors.

8.3.3 Optimization Problem

The problem of finding the minimum exponent subject to our constraints can be seen as a very small Integer Linear Program (ILP). More precisely, for $(r,\rho) \in \mathbb{N}^2$, we want to maximize the quantity

$$(w_1+w_2)r + w_2\rho$$

under the constraints

$$\begin{cases} (2n+n_1)r + n_1\rho & \leqslant m(n+n_1-1), \\ w_1 & \leqslant r, \\ w_2 & \leqslant \rho, \\ r+\rho & \leqslant m-1. \end{cases}$$

To derive the parameters of [BBBG23], we have performed a simple exhaustive search over the finite set of possible pairs (r, ρ).

What would be more interesting from a theoretical perspective is to find a closed form expression for the optimum provided it exists. We have addressed this question in the case of the basic RQC scheme, where $n_1 = n$. The relevant ILP becomes

$$\begin{cases} 3nr + n\rho & \leqslant (2n-1)m, \\ w_1 & \leqslant r, \\ w_2 & \leqslant \rho, \\ r + \rho & \leqslant m - 1. \end{cases}$$

The first inequality is equivalent to $3r + \rho \leqslant 2m - m/n$. Since we restrict ourselves to integer values for (r, ρ) and since $n < m < 2n$ in concrete parameters, we have replaced this constraint by $3r + \rho \leqslant 2m - 2$. A classical method to solve ILP is to remove the requirement that r and ρ are integers and to consider the associated relaxed Linear Program (LP). If we further assume that $1 + w_1/w_2 < 3$, an elementary geometrical argument shows that the LP solution is at the intersection of the lines $r + \rho = m - 1$ and $3r + \rho = 2m - 2$, *i.e.*, $r = (m-1)/2$ and $\rho = (m-1)/2$. Since m is always odd[1], this corresponds to an integer solution and thus it is also the optimal solution to the ILP.

The impact on the security on RQC is as follows:

Fact 4. *When $n < m < 2n$, $w_1 > w_2$ and $1 + w_1/w_2 < 3$, our approach improves the cost of the best known combinatorial attack on the scheme.*

Proof. The best attack on NHRD which does not exploit the structure corresponds to $\rho = 0$ in our strategy and thus we already outperform this technique. Since the security of RQC also reduces to this second problem [Agu+20, Theorem 5.1], let us now compare ourselves to the best combinatorial attack on an RD instance of parameters $(m, 2n, n, w_1)$. Using [AGHT18], its complexity is $\widetilde{\mathcal{O}}(q^{w_1(m-r_1)-m})$, where

$$r_1 \stackrel{def}{=} \left\lfloor \tfrac{m(n-1)}{2n} \right\rfloor = (m-1)/2 - \left\lceil \tfrac{m-n}{2n} \right\rceil = \tfrac{m-3}{2}.$$

The same cost exponent can also be obtained with our method by performing the free guess $S_2 \subset V \oplus Z = \mathbb{F}_{q^m}$. We can include it in the previous ILP if we replace $r + \rho \leqslant m - 1$ by $r + \rho \leqslant m$. As long as $1 + w_1/w_2 < 3$, the optimal solution to the new relaxed LP is such that $r + \rho = m$ and $3r + \rho = 2m - 2$, *i.e.*, $r = (m-2)/2$ and $\rho = (m+2)/2$. This time this is not an integer solution and the ILP solution may be obtained by rounding its entries to the nearest integer. In order not to violate the constraint $r + \rho = m$, possible roundings are $(r, \rho) = \left(\frac{m-1}{2}, \frac{m+1}{2}\right)$ and $(r, \rho) = \left(\frac{m-3}{2}, \frac{m+3}{2}\right)$. Note now that $\left(\frac{m-1}{2}, \frac{m+1}{2}\right)$ violates $3r + \rho = 2m - 2$ while $(r, \rho) = \left(\frac{m-3}{2}, \frac{m+3}{2}\right)$ corresponds to the pair

[1] In practice, it is chosen to be a prime greater than 2.

$(r_1, \rho_1 \stackrel{def}{=} r - r_1)$. The relevant comparison is thus between $(r_1, r - r_1)$ and the former $\left(\frac{m-1}{2}, \frac{m-1}{2}\right)$. For this we consider the difference

$$\begin{aligned}\delta &\stackrel{def}{=} \left(\frac{m-1}{2}(w_1 + w_2) + \frac{m-1}{2}w_2\right) - \left(\frac{m-3}{2}(w_1 + w_2) + \frac{m+3}{2}w_2\right) \\ &= (w_1 + w_2) - 2w_2 = w_1 - w_2.\end{aligned}$$

The expression of δ shows that our approach offers a better exponential factor compared to the one of solving $(m, 2n, n, w_1)$-RD when $w_1 > w_2$ but not when $w_1 \leqslant w_2$. This improvement is by a modest factor of $q^{w_1 - w_2}$. □

We finally provide a simple example of the situation in Figures 8.1 and 8.2 below, where $w_1 > w_2$ and $w_2 > w_1$ respectively. When $w_1 > w_2$, the red point $(r_1, m - r_1)$ is strictly below the blue line with slope $-(1 + w_1/w_2)$ which passes through the blue point $((m-1)/2, (m-1)/2)$, and in this case our approach is an improvement. The condition $1 + w_1/w_2 < 3$ reflects the fact that this blue line is always sandwiched between $x + y = m - 1$ and $3x + y = 2m - 2$. We have not considered the case $1 + w_1/w_2 \geqslant 3$ (*i.e.*, $w_1 \geqslant 2w_2$) since it does not seem relevant from an efficiency standpoint and as it does not correspond to any concrete parameters.

Figure 8.1: Parameter set $m = 29,\ n < m < 2n,\ w_1 = 5,\ w_2 = 3$.

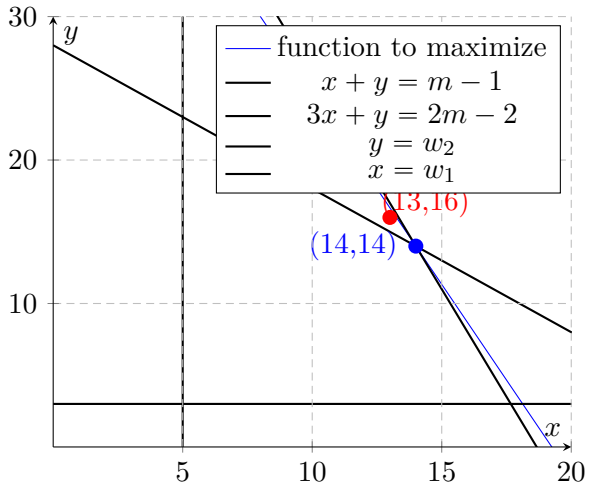
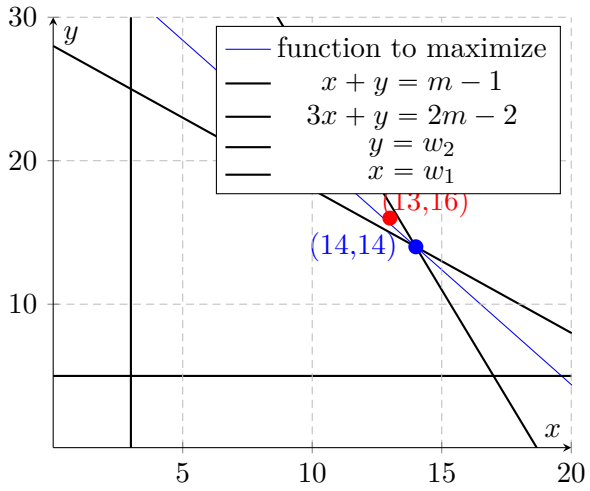


Figure 8.2: Parameter set $m = 29,\ n < m < 2n,\ w_1 = 3,\ w_2 = 5$.



Chapter 9
Assumption Underlying Loidreau's Scheme

The last chapter of this part is a joint work with Pierre Loidreau published at PQCrypto 2023 [BL23] about the cryptanalysis of schemes using distorted Gabidulin codes [Loi17; Ara+22]. It heavily relies on the constrained linear system that Loidreau introduced in an extended abstract presented at WCC 2022 and for which he proposed an enumeration approach. It was also observed that its equations can be rewritten as a bilinear modeling.

My contribution was to replace the initial solving method by a more efficient one which is directly borrowed from combinatorial attacks on RD. I have also tried to analyze algebraic techniques on Loidreau's bilinear polynomials. It turns out that the system shares similarities with the Ourivski-Johansson modeling [OJ02] and we can exhibit degree falls in a rather similar way as in [Bar+20a].

Contents

9.1 Preliminaries

This section gives some background on the scheme as presented at WCC 2022 and on the system that was proposed to distinguish the underlying Gabidulin code from a random one.

9.1.1 Loidreau's Cryptosystem

For integers $n \leqslant m$ and $k \leqslant n$, we consider a Gabidulin code $\mathcal{G}_{\boldsymbol{g}} \stackrel{def}{=} \mathcal{G}_{\boldsymbol{g}}(n,k,m)$ as in the previous chapter defined from a vector $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ whose coefficients are linearly independent over $\mathbb{F}_q$. We still denote by $\mathcal{G}_{\boldsymbol{g}}.\mathsf{Decode}(.)$ a polynomial time decoding algorithm that can decode errors of weight up to $\lfloor \frac{n-k}{2} \rfloor$ and we let $\mathrm{GL}_n(\mathbb{F}_{q^m})$ be the group of non-singular matrices of size n with entries in $\mathbb{F}_{q^m}$.

The scheme will also require an extra parameter $\lambda \in \mathbb{N}$ involved in the masking. Its value is taken such that $\lambda < \lfloor (n-k)/2 \rfloor$ for correctness but there are also extra constraints due to previous cryptanalysis. When $\lambda = 2$ and when the code rate k/n is $\geqslant 1/2$, Coggia and Couvreur gave a distinguisher which can be turned into an efficient attack [CC20]. Their distinguisher actually works for arbitrary λ as long as $k/n \geqslant 1 - 1/\lambda$ and there still exists an attack which is polynomial if $\lambda = 3$ [Gha22] and a priori exponential if $\lambda > 3$ [Gha22; LP21]. The cost of latter should remain threatening as [LP21] advised to choose values of $\lambda \geqslant 3$ such that $k/n < 1 - 1/\lambda$.

Keygen(1^ν):

- Pick a random element $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ whose support has dimension n and construct $\mathcal{G}_{\boldsymbol{g}}(n,k,m)$ the Gabidulin code of dimension k associated to $\boldsymbol{g}$.
- Select $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ an arbitrary full-rank generator matrix for this code. A standard method is to start from the matrix whose rows are the vectors $\boldsymbol{g}^{[j]}$ for $j \in \{0..k-1\}$ and then to multiply on the left by a random matrix in $\mathrm{GL}_k(\mathbb{F}_{q^m})$.
- Pick $\mathcal{V}$ a random $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension λ (by sampling λ random elements in $\mathbb{F}_{q^m}$ which are linearly independent) and sample $\boldsymbol{P}$ a random invertible matrix of size n whose entries belong to $\mathcal{V}$.
- Set $\mathsf{pk} \stackrel{def}{=} \boldsymbol{G}_{\mathrm{pub}} \stackrel{def}{=} \boldsymbol{G}\boldsymbol{P}^{-1}$ and $\mathsf{sk} \stackrel{def}{=} (\boldsymbol{G}, \boldsymbol{P})$.

Encrypt(pk, $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$):

- Sample $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ a random vector of weight $|\boldsymbol{e}| \leqslant \lfloor (n-k)/2\lambda \rfloor$.
- The ciphertext is $\boldsymbol{c} \stackrel{def}{=} \boldsymbol{m}\boldsymbol{G}_{\mathrm{pub}} + \boldsymbol{e}$.

Decrypt$(\mathsf{sk} = (\boldsymbol{G}, \boldsymbol{P}), \boldsymbol{c})$**:**

- Decode the noisy codeword $\boldsymbol{cP}$ using the algorithm $\mathcal{G}_{\boldsymbol{g}}.\mathsf{Decode}(.)$. Correctness follows from the fact that the weight of $\boldsymbol{eP}$ is upper bounded by

$$|\boldsymbol{e}| \times \lambda \leqslant \lfloor (n-k)/2\lambda \times \lambda \rfloor = \lfloor (n-k)/2 \rfloor.$$

9.1.2 Security

Let $\mathcal{C}_{\text{pub}}$ be the $\mathbb{F}_{q^m}$-linear code of parameters $[n, k]$ generated by the public matrix $\boldsymbol{G}_{\text{pub}}$. Even though no security proof is given, it is easy to see that IND-CPA is related to the difficulty of solving the following two problems:

- Distinguish the code $\mathcal{C}_{\text{pub}}$ from a random $\mathbb{F}_{q^m}$-linear code with the same parameters.
- Solve a generic RD instance of parameters $(m, n, k, t \stackrel{def}{=} \lfloor (n-k)/(2\lambda) \rfloor)$.

In this chapter, we will address the hardness of the first one.

9.1.3 A Constrained Linear System

We now describe the equations introduced by Loidreau in order to build a distinguisher. More precisely, its solutions allow to devise a polynomial time decryption algorithm for the public code $\mathcal{C}_{\text{pub}}$ (see Proposition 9.2).

Let $r \stackrel{def}{=} n-k$. In the following, we overline with a hat data that are publicly known. For instance, let $\widehat{\mathbf{H}}_{\text{pub}} \in \mathbb{F}_{q^m}^{r \times n}$ an arbitrary parity-check matrix for $\mathcal{C}_{\text{pub}}$ and for $\alpha \in \mathbb{F}_{q^m}$ a normal element, let $\widehat{\mathbf{H}}_{\text{norm}} \in \mathbb{F}_{q^m}^{r \times m}$ be the matrix whose entry in row i and column j is equal to $\alpha^{[i+j-2]}$ for any $i \in \{1..r\}$ and $j \in \{1..m\}$. Note that $\widehat{\boldsymbol{\alpha}} \stackrel{def}{=} \left(\alpha, \alpha^{[1]}, \ldots, \alpha^{[m-1]}\right)$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Since the dual of a Gabidulin code is again a Gabidulin code, there exists a vector $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$ whose coefficients are linearly independent over $\mathbb{F}_q$ such that a parity-check matrix for $\mathcal{G}_{\boldsymbol{g}}$ is

$$\mathbf{H} \stackrel{def}{=} \begin{bmatrix} \boldsymbol{h}^{[0]} \\ \vdots \\ \boldsymbol{h}^{[r-1]} \end{bmatrix} \in \mathbb{F}_{q^m}^{r \times n}. \tag{9.1}$$

Then, it is easy to see that there exists a unique matrix $\mathbf{S} \in \mathrm{GL}_r(\mathbb{F}_{q^m})$ such that

$$\mathbf{S}\widehat{\mathbf{H}}_{\text{pub}} = \mathbf{H}\mathbf{P}^{\mathsf{T}}. \tag{9.2}$$

This is because $\mathbf{H}\mathbf{P}^{\mathsf{T}}\boldsymbol{G}_{\text{pub}}^{\mathsf{T}} = \mathbf{H}\mathbf{P}^{\mathsf{T}}(\boldsymbol{P}^{\mathsf{T}})^{-1}\boldsymbol{G}^{\mathsf{T}} = \boldsymbol{H}\boldsymbol{G}^{\mathsf{T}} = \mathbf{0}$ and thus $\mathbf{H}\mathbf{P}^{\mathsf{T}}$ is a parity-check matrix for $\mathcal{C}_{\text{pub}}$. Equation (9.2) then follows since any parity-check matrix, a fortiori, $\widehat{\mathbf{H}}_{\text{pub}}$, is obtained by change of basis. Another straightforward proposition is

Proposition 9.1. *Let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{r\times n}$ be a parity-check matrix for $\mathcal{G}_{\boldsymbol{g}}$ as in Equation (9.1). There exists a matrix $\boldsymbol{M} \in \mathbb{F}_q^{m\times n}$ of rank n such that*

$$\boldsymbol{H} = \widehat{\boldsymbol{H}}_{norm}\boldsymbol{M}. \tag{9.3}$$

Proof. Let $\boldsymbol{h} = \boldsymbol{h}^{[0]} = (h_1, \ldots, h_n)$ denote the first row of $\boldsymbol{H}$. We consider the matrix $\boldsymbol{M} \in \mathbb{F}_q^{m\times n}$ whose i-th column corresponds to the vector of length m over $\mathbb{F}_q$ formed by the coordinates of h_i in the basis $\widehat{\boldsymbol{\alpha}}$, for $i \in \{1..n\}$. We have $\boldsymbol{H} = \widehat{\mathbf{H}}_{\mathrm{norm}}\mathbf{M}$ simply by construction. Finally, as $h_1, \ldots, h_n$ are linearly independent over $\mathbb{F}_q$ by definition of a Gabidulin code, the matrix $\boldsymbol{M}$ is necessarily of full rank. □

By combining Equation (9.2) and Equation (9.3) from Proposition 9.1, we obtain $\mathbf{S}\widehat{\mathbf{H}}_{\mathrm{pub}} = \widehat{\mathbf{H}}_{\mathrm{norm}}\left(\boldsymbol{M}\boldsymbol{P}^{\mathsf{T}}\right)$. It will be relevant to view this equality as a linear system in the entries of $\boldsymbol{S}$ and $\boldsymbol{T} \stackrel{def}{=} \boldsymbol{M}\boldsymbol{P}^{\mathsf{T}}$ under the constraint that the coefficients of $\boldsymbol{T}$ belong to a small $\mathbb{F}_q$-subspace of dimension λ. The following proposition indeed shows that any solution meeting this condition leads to a polynomial-time decryption algorithm.

Proposition 9.2. *Let $r = n - k$ and let $\widehat{\mathbf{H}}_{pub}$ be a parity-check matrix for $\mathcal{C}_{pub}$. Let $\alpha \in \mathbb{F}_{q^m}$ be a normal element and let $\widehat{\boldsymbol{H}}_{norm} \in \mathbb{F}_{q^m}^{r\times m}$ be the matrix whose entry in row i and column j is equal to $\alpha^{[i+j-2]}$ for $i \in \{1..r\}$ and $j \in \{1..m\}$. From the knowledge of any non-singular matrix $\boldsymbol{V} \in \mathbb{F}_{q^m}^{r\times r}$ and $\boldsymbol{W} \in \mathcal{W}^{m\times n}$ of rank n such that*

$$\mathbf{V}\widehat{\mathbf{H}}_{pub} = \widehat{\mathbf{H}}_{norm}\boldsymbol{W} \tag{9.4}$$

and where $\mathcal{W}$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ of dimension $\leqslant \lambda$, it is possible to decrypt any ciphertext in polynomial time.

Proof. We consider an arbitrary ciphertext $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{\mathrm{pub}} + \boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{e}| \leqslant \lfloor (n-k)/2\lambda \rfloor$ and also $\mathbf{V} \in \mathrm{GL}_r(\mathbb{F}_{q^m})$, $\mathbf{W} \in \mathcal{W}^{m\times n}$ as in the statement of the proposition. By definition of $\boldsymbol{c}$ we have $\widehat{\mathbf{H}}_{\mathrm{pub}}\boldsymbol{c}^{\mathsf{T}} = \widehat{\mathbf{H}}_{\mathrm{pub}}\boldsymbol{e}^{\mathsf{T}}$ and thus

$$\boldsymbol{V}\widehat{\mathbf{H}}_{\mathrm{pub}}\boldsymbol{e}^{\mathsf{T}} = \widehat{\mathbf{H}}_{\mathrm{norm}}\underbrace{\boldsymbol{W}\boldsymbol{e}^{\mathsf{T}}}_{\stackrel{def}{=}(\boldsymbol{e}')^{\mathsf{T}}}.$$

Since the vector space $\mathcal{W}$ is of dimension $\leqslant \lambda$, the error $\boldsymbol{e}'$ has weight $|\boldsymbol{e}'| \leqslant \lambda\,|\boldsymbol{e}| \leqslant \lfloor (n-k)/2 \rfloor$. We can therefore use an efficient decoder of the public Gabidulin code with parity-check matrix $\widehat{\mathbf{H}}_{\mathrm{norm}} \in \mathbb{F}_{q^m}^{r\times n}$ to recover this vector. Finally, the map $\boldsymbol{e} \mapsto \boldsymbol{e}\boldsymbol{W}^{\mathsf{T}}$ is injective as $\boldsymbol{W}$ has rank $n \leqslant m$. This allows to retrieve $\boldsymbol{e}$ and the vector $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ such that $\boldsymbol{m}\boldsymbol{G}_{\mathrm{pub}} = \boldsymbol{c} - \boldsymbol{e}$ in a unique way. □

To conclude this section, note that a naive approach would be to enumerate all solutions $(\mathbf{V}, \mathbf{W})$ to Equation (9.4) and to test if they satisfy the constraint, *i.e.*, the $\mathbf{W}$ matrix has its entries in a small dimensional $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$. This is clearly infeasible because the solution set without the imposed condition is an $\mathbb{F}_{q^m}$-vector space of dimension at least $r^2 + (m-r)n$.

9.2 Combinatorial Approach

To exploit the constraint added to Equation (9.4), the idea adopted at WCC 2022 was to enumerate candidate bases $\boldsymbol{\mu} \in \mathbb{F}_{q^m}^{\lambda}$ for the secret vector space $\mathcal{W}$. Any such candidate was then completed into a basis of $\mathbb{F}_{q^m}$ in which one could express the coefficients of the matrices $\boldsymbol{V}$ and $\boldsymbol{W}$. In such a way, Equation (9.4) can be rewritten as a linear system over $\mathbb{F}_q$. Since each entry in $\boldsymbol{W}$ is assumed to belong to the $\mathbb{F}_q$-vector space spanned by $\boldsymbol{\mu}$, only $\lambda \times mn$ unknowns over $\mathbb{F}_q$ are introduced for this matrix instead of the naive $m \times mn$. Finally, as one typically has $rmn \gg \lambda mn + mr^2$, this initial guess can be tested by solving the resulting linear equations over $\mathbb{F}_q$ to check if they have a non-zero solution. As is usual for this type of approach, the total cost contains two factors:

- an exponential one coming from enumerating the bases;
- a polynomial one which corresponds to the linear system solving over $\mathbb{F}_q$.

9.2.1 Proposed Algorithm

We can cheaply gain in the exponential factor by employing the general technique already used in combinatorial attacks on RD [OJ02; GRS16; AGHT18]. Indeed, it is sufficient to know (a basis for) a γ-dimensional vector space $\mathcal{U}$, $\gamma \geqslant \lambda$, which contains $\mathcal{V}$ to apply the same algorithm provided that γ is not too large. The advantage is that it is always easier to find such a $\mathcal{U}$ than to guess a basis of $\mathcal{V}$ directly, the extreme case being $\gamma = m$ for which we succeed with probability 1. Here, we even note that a vector space $\mathcal{U}$ which contains an arbitrary multiple $x\mathcal{V}$ for $x \in \mathbb{F}_{q^m}^*$ instead of simply $\mathcal{V}$ is enough for our purposes. This is because any pair $(x\boldsymbol{V}, x\boldsymbol{W})$ is a solution to the constrained linear system. The following Proposition 9.3 gives the precise upper bound on γ for our attack to succeed.

Proposition 9.3. *Assume that $\gamma \geqslant \lambda \in \mathbb{N}$ is such that*

$$rn \geqslant \gamma n + r^2. \tag{9.5}$$

If $\boldsymbol{\nu} \in \mathbb{F}_{q^m}^{\gamma}$ is a basis for a vector space $\mathcal{U}$ which contains a multiple $x\mathcal{V}$ for $x \in \mathbb{F}_{q^m}^*$, the linear system over $\mathbb{F}_q$ derived from Equation (9.4) by writing the coefficients of the secret matrix $\boldsymbol{W}$ in the basis $\boldsymbol{\nu}$ is expected to have a solution space of dimension 1. If $\boldsymbol{\nu}$ does not correspond to such a basis, this linear system will not have a non-zero solution with overwhelming probability.

From this proposition, we can then use the same algorithm as sketched at the beginning of Section 9.2 with γ instead of λ provided that $\gamma \leqslant r(1 - r/n)$.

9.2.2 Estimated Cost

The exponential factor is now given by the inverse of the probability that a fixed subspace $\mathcal{U}$ of dimension γ contains a subspace of the form $x\mathcal{V}$ for some $x \in \mathbb{F}_{q^m}^*$. According to

[AGHT18, §III.B.], this factor can be estimated by $\Theta(q^{\lambda(m-\gamma)-m}) = \Theta(q^{(\lambda-1)m-\lambda\gamma})$. We make the standard assumption that the optimum complexity corresponds to the highest success probability regardless of the polynomial factors. This means that we consider the largest possible value for γ, *i.e.*, $\gamma \stackrel{def}{=} \lfloor r(1-r/n) \rfloor$.

It is still worth discussing the complexity of solving the linear system over $\mathbb{F}_q$. This is especially relevant because it is bigger (by a polynomial factor) than the ones from the former combinatorial attacks on RD.

- On the matrix of size $rnm \times (\gamma n + r^2)m$ over $\mathbb{F}_q$ which is associated to it, a first approach is to apply Gaussian elimination. The corresponding cost in $\mathbb{F}_q$-operations can be estimated by $\mathcal{O}((\gamma n + r^2)m)^\omega)$, where $2 \leqslant \omega \leqslant 3$ is the linear algebra constant.

- However, checking that a linear system is consistent does not require to compute a row echelon form. Instead, we can make use of the Wiedemann algorithm which may offer an advantage since the input matrix is sparse. Note indeed that the equations have about $m(r+\gamma)$ non-zero coefficients while they contain $m(r^2 + \gamma n) \gg m(r+\gamma)$ unknowns. The standard estimate for this algorithm (*i.e.*, Equation (2.8) with $D = 1$) would then give a complexity of

$$\mathcal{O}\left(m^3(r+\gamma)(\gamma n + r^2)^2\right). \tag{9.6}$$

The final estimate at WCC 2022 was in fact a *lower bound* on the overall cost by replacing Equation (9.6) by the smaller value $m^3 r^5$ (without any constant in front of it). We follow exactly the same method so that the difference will only lie in the exponential factor. Recalling that $r = n - k$ and by introducing the code rate $R \stackrel{def}{=} k/n$, our lower bound reads

$$m^3(n-k)^5 q^{(\lambda-1)m-\lambda\lfloor n(1-R)R \rfloor}. \tag{9.7}$$

9.2.3 Applications

We instantiate Equation (9.7) with the parameters of the WCC 2022 paper and the ones of LowMS [Ara+22]. We believe that the comparison is fair since the latter have been obtained from the content presented at WCC 2022. In Table 9.1, Column "Lower bound" contains the value of the binary logarithm of the cost of Equation (9.7). Our results always improve the complexity of the structural attack simply because we have a better exponent. If this complexity becomes smaller than the cost of the best RD attack, this might lead to re-evaluate parameters in [Loi17] and [Ara+22].

9.3 A Bilinear System

Our second contribution was to partially analyze algebraic methods on the bilinear system that had been introduced by Loidreau (Modeling 16). It turns out that the original enumeration strategy corresponds to fixing the smallest block of variables as

Table 9.1: Cost estimate on the parameters of [Loi17] and [Ara+22].

(m, n, k, λ)	Security	Source	Lower bound	Former
$(128, 128, 20, 3)$	128	WCC 2022	263	311
$(128, 128, 44, 3)$	128	WCC 2022	225	308
$(59, 50, 25, 3)$	128	LowMS	**123**	158
$(67, 66, 33, 4)$	128	LowMS	180	244
$(83, 74, 37, 3)$	192	LowMS	**157**	211
$(79, 78, 39, 4)$	192	LowMS	206	282

described in Section 2.5.2.3 when mentioning techniques tailored to the bilinear structure. The same approach was also followed in [OJ02, §3.2. Strategy 2].

This section presents the input equations and it provides early comments. We refer to Section 9.4 for a more detailed analysis.

9.3.1 Statement of the Modeling

Let $\widehat{\boldsymbol{\beta}}$ denote an arbitrary basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For an element $a \in \mathbb{F}_{q^m}$, we consider $\vec{a} \in \mathbb{F}_q^m$ the m-dimensional vector of its coordinates over $\widehat{\boldsymbol{\beta}}$, so that $\widehat{\boldsymbol{\beta}}\vec{a}^{\mathsf{T}} = a$. For $\mu \in \mathbb{F}_{q^m}$, we also define $\boldsymbol{M}_\mu \in \mathbb{F}_q^{m\times m}$ the matrix of multiplication by μ in the basis $\widehat{\boldsymbol{\beta}}$. This matrix is such that

$$\forall a,\ b \in \mathbb{F}_{q^m},\ b = \mu a \Leftrightarrow \vec{b} = \vec{a}\boldsymbol{M}_\mu^{\mathsf{T}}.$$

Note that this choice of notation is implicit with respect to the basis. The claimed bilinear system is as follows.

Modeling 16. *Let $\widehat{\mathbf{H}}_{pub} = (\widehat{h}_{ij})_{i=1,j=1}^{r,n}$ and let $\widehat{\mathbf{H}}_{norm} = (\alpha^{[i+u-2]})_{i=1,u=1}^{r,m}$. We consider the bilinear equations over $\mathbb{F}_q$ in the non-zero unknowns $\vec{v_{iu}}$, $b_{ij}^{(\ell)}$ and linearly independent vectors $\vec{\mu_\ell} \in \mathbb{F}_q^m$ which are given by*

$$\begin{cases} \forall i \in \{1..r\} \\ \forall j \in \{1..n\} \end{cases}, \quad \sum_{u=1}^{r} \boldsymbol{M}_{\widehat{h}_{uj}} \vec{v_{iu}}^{\mathsf{T}} = \sum_{u=1}^{m}\sum_{\ell=1}^{\lambda} b_{uj}^{(\ell)} \boldsymbol{M}_{\alpha^{[i+u-2]}} \vec{\mu_\ell}^{\mathsf{T}}. \tag{9.8}$$

Modeling 16 contains mrn affine equations over $\mathbb{F}_q$. The linear parts involve mr^2 variables $\vec{v_{iu}}$ while the bilinear parts involve $\lambda mn + \lambda m$ variables $b_{uj}^{(\ell)}$ and $\vec{\mu_\ell}$ respectively. Proposition 9.4 states that its solutions are actually equivalent to the ones of the linear equations (9.4) with the relevant constraints added.

Proposition 9.4. *Let $\widetilde{\boldsymbol{V}} = (v_{ij}) \in \mathbb{F}_{q^m}^{r\times r}$ and let $\widetilde{\boldsymbol{W}} = (w_{ij}) \in \mathcal{W}^{m\times n}$ which satisfy the constrained linear equations (9.4), where $\mathcal{W}$ is a λ-dimensional subspace of $\mathbb{F}_{q^m}$ that contains the entries of $\widetilde{\boldsymbol{W}}$. We consider a basis $(\mu_1, \ldots, \mu_\lambda) \in \mathbb{F}_{q^m}^{\lambda}$ and we denote by*

$$w_{ij} \stackrel{def}{=} \sum_{\ell=1}^{\lambda} b_{ij}^{(\ell)} \mu_\ell \tag{9.9}$$

the unique decomposition of w_{ij} in this basis. Then, the values $\vec{v_{iu}}$, $b_{ij}^{(\ell)}$ and $\vec{\mu_\ell}$ correspond to a solution to Modeling 16. Conversely, any solution $\vec{v_{iu}}$, $b_{ij}^{(\ell)}$, $\vec{\mu_\ell}$ to Modeling 16 yields a pair of matrices $\widetilde{\boldsymbol{V}} = (v_{ij})$ and $\widetilde{\boldsymbol{W}} = (w_{ij})$ where w_{ij} is defined by Equation (9.9) for which Equation (9.4) holds and such that coefficients of $\widetilde{\boldsymbol{W}}$ lie in a λ-dimensional subspace.

If $(\boldsymbol{V}, \boldsymbol{W})$ stands for the genuine pair of matrices which is implicit from the description of the scheme, we have already seen that any $(\widetilde{\boldsymbol{V}}, \widetilde{\boldsymbol{W}}) = (x\boldsymbol{V}, x\boldsymbol{W})$, $x \in \mathbb{F}_{q^m}^*$ allows us to decrypt. Concretely, to reduce the number of solutions to Modeling 16, we will thus:

- fix μ_1 to 1 and choose a basis $\widehat{\boldsymbol{\beta}}$ whose first element is also equal to 1;
- target a basis in systematic form, *i.e.*,

$$(1, \mu_2, \ldots, \mu_\lambda)^\mathsf{T} \stackrel{def}{=} \begin{bmatrix} & \mathbf{0}_{1\times(m-\lambda)} \\ \boldsymbol{I}_\lambda & \\ & \boldsymbol{R}' \end{bmatrix} \widehat{\boldsymbol{\beta}}^\mathsf{T}, \tag{9.10}$$

  where $\boldsymbol{R}' \in \mathbb{F}_q^{(\lambda-1)\times(m-\lambda)}$. We cannot always guarantee to have a solution in this way but the success probability is constant.

Similar specializations have already been used in previous works, see for instance [CS96, §3.4] or [OJ02, §3.1.].

9.3.2 Particular Features

Our goal will be to understand the early steps of the generic Gröbner basis algorithm on Modeling 16. We start by describing the specificities in the equations that we have used in the analysis.

An obvious one is the bilinear shape. More precisely, we recover the matrix product structure as presented in Section 2.5.2.2. By that we mean equations which can be viewed as the entries of a matrix $\boldsymbol{M} = \boldsymbol{AXY}$, where $\boldsymbol{A}$ is a matrix of scalars and where $\boldsymbol{X}$ and $\boldsymbol{Y}$ are matrices of unknown coefficients. Using the notation from Modeling 16, we can indeed write each column $\boldsymbol{w}_j = (w_{1,j}, \ldots, w_{m,j}) \in \mathbb{F}_{q^m}^m$ of the unknown matrix $\boldsymbol{W}$ as $\boldsymbol{w}_j^\mathsf{T} = \boldsymbol{C}_j(\mu_1, \ldots, \mu_\lambda)^\mathsf{T} = \boldsymbol{C}_j\boldsymbol{R}\widehat{\boldsymbol{\beta}}^\mathsf{T}$, where $\boldsymbol{C}_j \stackrel{def}{=} (b_{i,j}^{(\ell)})_{i=1,\ell=1}^{m,\lambda}$ and where the rows of $\boldsymbol{R} \in \mathbb{F}_q^{\lambda\times m}$ are the vectors $\vec{\mu_\ell}$ for $\ell \in \{1..\lambda\}$. We then consider the system

Modeling 16-$\mathbb{F}_{q^m}$. *For $j \in \{1..n\}$, let $\widehat{\boldsymbol{h}_j} \in \mathbb{F}_{q^m}^r$ denote the j-th column in $\widehat{\mathbf{H}}_{pub}$. There are r bilinear equations in the entries of $\widetilde{\boldsymbol{V}}$, $\boldsymbol{R}$ and $\boldsymbol{C}_j$ from the equality*

$$\widetilde{\boldsymbol{V}}\widehat{\boldsymbol{h}_j}^\mathsf{T} = \widehat{\mathbf{H}}_{norm}\boldsymbol{C}_j\boldsymbol{R}\widehat{\boldsymbol{\beta}}^\mathsf{T}.$$

By considering all columns, we obtain an affine bilinear system containing rn equations over $\mathbb{F}_{q^m}$ in r^2 unknowns v_{ij} over $\mathbb{F}_{q^m}$ and $\lambda mn + \lambda m$ unknowns over $\mathbb{F}_q$.

Note that the former Modeling 16 captures exactly the same information as the system over $\mathbb{F}_q$ obtained from Modeling 16-$\mathbb{F}_{q^m}$ by taking as variables the coefficients of the vectors $\vec{v_{iu}}$ instead of the v_{ij}'s and then by unfolding over the small field. This operation has been employed several times in the previous chapters and it invites us to study the role of the extension field. So far, the analysis of the full system over $\mathbb{F}_q$ could be essentially boiled down to the one of the initial system over $\mathbb{F}_{q^m}$ under certain assumptions. Here, however, the situation is less simple. For instance, it will not be sufficient to analyze Modeling 16-$\mathbb{F}_{q^m}$ to understand the computation on Modeling 16 over $\mathbb{F}_q$. This may be due to the following simple fact: if we choose the normal basis $\widehat{\boldsymbol{\beta}} = \widehat{\boldsymbol{\alpha}}$ to unfold the equations, we recover the first row of $\widehat{\mathbf{H}}_{\text{norm}}$.

Our proofs will also make use of another related system. Its equations can be obtained from Modeling 16-$\mathbb{F}_{q^m}$ by iterating the Frobenius map and by reducing modulo the field equations of $\mathbb{F}_q$ involving the variables from $\boldsymbol{R}$ and $\boldsymbol{C}_j$ for $j \in \{1..n\}$ (see for example the proof of Proposition 7.7 in Chapter 7 for a similar construction). In that respect, it is essentially equivalent to Modeling 16.

Modeling 17. *For $j \in \{1..n\}$, let $\widehat{\boldsymbol{h}_j} \in \mathbb{F}_{q^m}^r$ denote the j-th column in $\widehat{\mathbf{H}}_{pub}$. For any $\ell \in \{0..m-1\}$, we consider the r polynomials obtained by applying the Frobenius map ℓ times on Modeling 16-$\mathbb{F}_{q^m}$ (the $^{[\ell]}$ notation for matrices and vectors is the same as in the previous chapters) and by reducing modulo the appropriate field equations. They are given by*

$$\boldsymbol{V}^{[\ell]} \left(\widehat{\boldsymbol{h}_j^{[\ell]}} \right)^{\mathsf{T}} = \widehat{\mathbf{H}}_{norm}^{[\ell]} \boldsymbol{C}_j \boldsymbol{R} \left(\widehat{\boldsymbol{\beta}}^{[\ell]} \right)^{\mathsf{T}}. \tag{9.11}$$

The main interest of Modeling 17 is theoretical. In particular, it would not be suitable to solve it using naive Gröbner basis algorithms because its equations have very high degree in the v_{ij} variables.

9.4 Degree Falls from Jacobians

We have tried to characterize the first degree fall polynomials in the affine bilinear modeling. Our results heavily rely on the content recalled in Section 2.5.2.1 about the connection between syzygies for homogeneous bilinear systems and kernels of Jacobians. More precisely, we can exploit the product structure described in Section 2.5.2.2 to show that these matrices have a specific shape. Using the above relationship, we can then deduce the existence of syzygies in degree $\lambda + 2$ for the bilinear parts and thus degree fall polynomials of degree $\lambda + 1$ for the affine equations.

Similarly to the MaxMinors system [Bar+20a] originally derived from degree fall polynomials in the Ourivski-Johansson's modeling [OJ02] and that can also be computed directly, the equations that we exhibit are minors of matrices of linear forms which are public. The main difference with this former work is that they come from the kernels of the two Jacobians which are naturally associated to Modeling 16 while only one of these matrices was relevant in [Bar+20a].

For the sake of simplicity, we give the results for the non-specialized version of our systems. They can be easily adapted if we fix μ_1 to 1 and if we choose a matrix $\boldsymbol{R}$ in systematic form as presented above.

9.4.1 Jacobian with Respect to $\boldsymbol{R}$

We start from the Jacobian matrices with respect to the unknowns which are the entries of $\boldsymbol{R}$. The situation for this block of variables is analogous to the one in [Bar+20a, §5.1]. As in their work, we observed that all degree falls over $\mathbb{F}_q$ from these matrices were obtained by projecting over $\mathbb{F}_q$ degree fall polynomials whose coefficients are in $\mathbb{F}_{q^m}$. This means that we can focus on Modeling 16-$\mathbb{F}_{q^m}$ rather than on Modeling 16 for this part of the analysis.

We restrict ourselves to the bilinear components in Modeling 16-$\mathbb{F}_{q^m}$ and we consider an arbitrary index $j \in \{1..n\}$. Recall that for a matrix $\boldsymbol{M}$, $\mathrm{row}(\boldsymbol{M})$ stands for the row vector formed by the concatenation of its rows. A direct application of Lemma 2.3 with $\boldsymbol{X} \stackrel{def}{=} \boldsymbol{R}$, $\boldsymbol{A} \stackrel{def}{=} \widehat{\mathbf{H}}_{\mathrm{norm}}\boldsymbol{C}_j$ and $\boldsymbol{Y} \stackrel{def}{=} \widehat{\boldsymbol{\beta}}^{\mathsf{T}}$ yields

$$\mathrm{Jac}_{\mathrm{row}(\boldsymbol{R})}\left(\mathrm{row}\left(\widehat{\mathbf{H}}_{\mathrm{norm}}\boldsymbol{C}_j\boldsymbol{R}\widehat{\boldsymbol{\beta}}^{\mathsf{T}}\right)\right) = \widehat{\mathbf{H}}_{\mathrm{norm}}\boldsymbol{C}_j \otimes \widehat{\boldsymbol{\beta}}. \tag{9.12}$$

The full system can also be viewed as the following matrix product

$$\left(\boldsymbol{I}_n \otimes \widehat{\mathbf{H}}_{\mathrm{norm}}\right)\begin{bmatrix}\boldsymbol{C}_1\\ \vdots \\ \boldsymbol{C}_n\end{bmatrix}\boldsymbol{R}\widehat{\boldsymbol{\beta}}^{\mathsf{T}}.$$

In the same manner, we can obtain

$$\mathrm{Jac}_{\mathrm{row}(\boldsymbol{R})}\left(\mathrm{row}\left(\left(\boldsymbol{I}_n \otimes \widehat{\mathbf{H}}_{\mathrm{norm}}\right)\begin{bmatrix}\boldsymbol{C}_1\\ \vdots \\ \boldsymbol{C}_n\end{bmatrix}\boldsymbol{R}\widehat{\boldsymbol{\beta}}^{\mathsf{T}}\right)\right) = \begin{bmatrix}\widehat{\mathbf{H}}_{\mathrm{norm}}\boldsymbol{C}_1\\ \vdots \\ \widehat{\mathbf{H}}_{\mathrm{norm}}\boldsymbol{C}_n\end{bmatrix} \otimes \widehat{\boldsymbol{\beta}}. \tag{9.13}$$

Using Lemma 2.1, vectors in the kernel of such Jacobians correspond to syzygies for the bilinear parts whose coefficients are polynomials in the $\boldsymbol{C}_j$ variables. They provide the following degree fall equations for the affine system:

Lemma 9.1. *In Modeling 16-$\mathbb{F}_{q^m}$, we find at least $\binom{nr}{\lambda+1}$ degree falls from degree $\lambda+2$ to $\lambda+1$. The ones coming from the Jacobian of Equation (9.13) are given by the maximal minors of the matrix*

$$\boldsymbol{N} \stackrel{def}{=} \begin{bmatrix}\widetilde{\boldsymbol{V}}\widehat{\boldsymbol{h}_1}^{\mathsf{T}} & \widehat{\mathbf{H}}_{norm}\boldsymbol{C}_1\\ & \vdots \\ \widetilde{\boldsymbol{V}}\widehat{\boldsymbol{h}_n}^{\mathsf{T}} & \widehat{\mathbf{H}}_{norm}\boldsymbol{C}_n\end{bmatrix}. \tag{9.14}$$

Among these minors and for $j \in \{1..n\}$, we may find in particular those of the matrix

$$\boldsymbol{N}^{(j)} \stackrel{def}{=} \boldsymbol{N}_{\{1+r(j-1)..rj\},*} = \left[\widetilde{\boldsymbol{V}}\widehat{\boldsymbol{h}_j}^{\mathsf{T}} \quad \widehat{\mathbf{H}}_{norm}\boldsymbol{C}_j\right].$$

These latter polynomials come from the Jacobian of Equation (9.12).

Even before giving the proof of Lemma 9.1, it is easy to see from the definition of Modeling 16-$\mathbb{F}_{q^m}$ that all the $\boldsymbol{N}^{(j)}$ matrices are not full-rank (a fortiori, $\boldsymbol{N}$) if and only if $(\widetilde{\boldsymbol{V}}, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_n)$ are components of a solution to Modeling 16-$\mathbb{F}_{q^m}$.

Proof. (Similar to in [Bar+20a, §5.1]). We do the proof for a single matrix $\boldsymbol{N}^{(j)}$. By Equation (9.12), it is sufficient to look at the left kernel of $\widehat{\mathbf{H}}_{\text{norm}}\boldsymbol{C}_j$. We then compute the kernel vectors $\boldsymbol{v}_J$ of Lemma 2.2 for this matrix of linear forms, namely

$$\boldsymbol{v}_J \stackrel{def}{=} \left(\underbrace{0}_{j\notin J}, \ldots, \underbrace{(-1)^{\ell+1}\left|\widehat{\mathbf{H}}_{\text{norm}}\boldsymbol{C}_j\right|_{J\setminus\{j\},*}}_{j=j_\ell\in J}, \ldots \right), \ \#J = \lambda+1, \ J \subset \{1..r\}.$$

Degree fall equations correspond to the multiplication by the linear parts. From the present vector $\boldsymbol{v}_J$, we obtain the degree $\lambda+1$ polynomial $(\boldsymbol{v}_J)\widetilde{\boldsymbol{V}}\widehat{\boldsymbol{h}_j}^{\mathsf{T}}$. Finally, it coincides with the maximal minor $\left|\boldsymbol{N}^{(j)}\right|_{J,*}$ by Laplace expansion along the first column. The reasoning is the same for $\boldsymbol{N}$ if we replace Equation (9.12) by Equation (9.13). □

Bilinear structure. The degree fall polynomials of Lemma 9.1 have degree $\lambda+1$. Perhaps more interestingly, Laplace expansion along the first column of $\boldsymbol{N}$ in Equation (9.14) also shows that they are *bilinear* in the entries of $\widetilde{\boldsymbol{V}}$ (which belong to $\mathbb{F}_{q^m}$) and in the maximal minors of the matrix $\boldsymbol{D}$ with coefficients in $\mathbb{F}_q$ defined by

$$\boldsymbol{D} \stackrel{def}{=} \begin{bmatrix} \boldsymbol{C}_1 \\ \vdots \\ \boldsymbol{C}_n \end{bmatrix}.$$

Similarly, the maximal minors of $\boldsymbol{N}^{(j)}$ are bilinear in the entries of $\widetilde{\boldsymbol{V}}$ and in the $\binom{m}{\lambda}$ maximal minors of $\boldsymbol{C}_j$. Such a structure has already been encountered in this manuscript, especially in SM-$\mathbb{F}_{q^m}$ (Modeling 14) which involves a block of linear variables over the extension field $\mathbb{F}_{q^m}$ and a block of minor variables over $\mathbb{F}_q$.

Unfolding over $\mathbb{F}_q$. In our experiments on Modeling 16, we found $m\binom{nr}{\lambda+1}$ (linearly independent) degree falls from degree $\lambda+2$ to degree $\lambda+1$ which contain these variables[1].

[1]Section 9.4.2 will give another type of degree fall polynomials in the same degree. As the tri-degree is different, it is still possible to distinguish these two sets of equations in Magma by considering several weighted orders.

Clearly, they should coincide with the unfolding over $\mathbb{F}_q$ of the degree fall polynomials described in Lemma 9.1 for Modeling 16-$\mathbb{F}_{q^m}$. To project the equations, note that we also need to express the entries of $\widetilde{\boldsymbol{V}}$ over $\mathbb{F}_q$. This yields r^2m variables $\vec{v_{iu}}$ and thus $r^2m\binom{mn}{\lambda}$ bilinear monomials appearing in these polynomials (but only $r^2m\binom{m}{\lambda}$ if we restrict ourselves to one matrix $\boldsymbol{C}_j$).

9.4.2 Jacobian with Respect to the C_j's

A particularity of Modeling 16 compared to the RD relevant systems is that the Jacobian with respect to the other block of variables provides degree fall polynomials of low degree, namely $\lambda + 1$. One cannot grasp them by studying Modeling 16-$\mathbb{F}_{q^m}$ only.

Absence of early degree falls in Modeling 16-$\mathbb{F}_{q^m}$. First, let us explain why we do not expect degree fall polynomials of small degree coming from this Jacobian for Modeling 16-$\mathbb{F}_{q^m}$. The set of bilinear components in this system can be written as $\mathcal{S} \stackrel{def}{=} \cup_{j=1}^{n}\mathcal{S}_j$, where the polynomials in $\mathcal{S}_j$ are defined as the entries of the matrix $\widehat{\mathbf{H}}_{\text{norm}}\boldsymbol{C}_j\boldsymbol{R}\widehat{\boldsymbol{\beta}}^{\mathsf{T}}$. Since the $\boldsymbol{R}\widehat{\boldsymbol{\beta}}^{\mathsf{T}}$ part does not depend on j, we have that $\text{Jac}_{\text{row}(\boldsymbol{C}_j)}\left(\text{row}(\mathcal{S}_j)\right) = \text{Jac}_{\text{row}(\boldsymbol{C}_1)}\left(\text{row}(\mathcal{S}_1)\right)$. The whole Jacobian then reads

$$\text{Jac}_{\text{row}(\boldsymbol{C})}\left(\text{row}(\mathcal{S})\right) = \boldsymbol{I}_n \otimes \text{Jac}_{\text{row}(\boldsymbol{C}_1)}\left(\text{row}(\mathcal{S}_1)\right).$$

Finally, to compute $\text{Jac}_{\text{row}(\boldsymbol{C}_1)}\left(\text{row}(\mathcal{S}_1)\right)$, we apply Lemma 2.3 once again this time with $\boldsymbol{X} \stackrel{def}{=} \widehat{\boldsymbol{H}}_{\text{norm}}$, $\boldsymbol{A} \stackrel{def}{=} \boldsymbol{C}_1$ and $\boldsymbol{Y} \stackrel{def}{=} \boldsymbol{R}\widehat{\boldsymbol{\beta}}^{\mathsf{T}}$. We obtain

$$\text{Jac}_{\text{row}(\boldsymbol{C}_1)}\left(\text{row}(\mathcal{S}_1)\right) = \widehat{\mathbf{H}}_{\text{norm}} \otimes \widehat{\boldsymbol{\beta}}\boldsymbol{R}^{\mathsf{T}}.$$

This matrix is of size $r \times m\lambda$ and its entries are linear forms in the $\boldsymbol{R}$ variables. However, we cannot pursue by applying Lemma 2.2 since $r < m\lambda$ in general. We expect a trivial left kernel for this matrix.

Additional degree falls for Modeling 16. We analyze the situation over $\mathbb{F}_q$ by studying Modeling 17 introduced in Section 9.3.2. From now on, we adopt the normal basis $\widehat{\boldsymbol{\beta}} = \widehat{\boldsymbol{\alpha}}$. As previously, we will reason in a similar way for all indexes $j \in \{1..n\}$. For $j \in \{1..n\}$ and $\ell \in \{0..m-1\}$, let us consider Equation (9.11) and for $u \in \{1..r\}$, let us denote by $g_{u,\ell,j}$ the bilinear polynomial

$$g_{u,\ell,j} \stackrel{def}{=} \left(\widehat{\boldsymbol{H}}_{\text{norm}}^{[\ell]}\right)_{u,*} \boldsymbol{C}_j\boldsymbol{R}\left(\widehat{\boldsymbol{\alpha}}^{[\ell]}\right)^{\mathsf{T}} = \left(\widehat{\boldsymbol{\alpha}}^{[\ell+u-1]}\right)\boldsymbol{C}_j\boldsymbol{R}\left(\widehat{\boldsymbol{\alpha}}^{[\ell]}\right)^{\mathsf{T}}.$$

We also keep track of the corresponding linear part $L_{u,\ell,j} \stackrel{def}{=} \boldsymbol{V}_{u,*}^{[\ell]}\left(\widehat{\boldsymbol{h}_j}^{[\ell]}\right)^{\mathsf{T}}$ so that the full equation reads $g_{u,\ell,j} - L_{u,\ell,j} = 0$. We then group the equations of Modeling

17 according to the value of $v \stackrel{def}{=} u + \ell - 1 \bmod m$. We obtain the following relations, where all ℓ indexes are modulo m and where $\widehat{\boldsymbol{H}}_{\text{inv}} \stackrel{def}{=} \begin{bmatrix} \widehat{\boldsymbol{\alpha}} \\ \dots \\ \widehat{\boldsymbol{\alpha}}^{-[r-1]} \end{bmatrix} \in \mathbb{F}_{q^m}^{m \times r}$:

$$\begin{aligned} \begin{bmatrix} L_{1,v,j} & L_{2,v-1,j} & \dots & L_{r,v-r+1,j} \end{bmatrix} &= \begin{bmatrix} g_{1,v,j} & \dots & g_{r,v-r+1,j} \end{bmatrix} \\ \widehat{\boldsymbol{h}_j}^{[\ell]} \left(\boldsymbol{V}^{[\ell]}\right)^{\mathsf{T}} &= \widehat{\boldsymbol{\alpha}}^{[v]} \boldsymbol{C}_j \boldsymbol{R} \left[\left(\widehat{\boldsymbol{\alpha}}^{[v]}\right)^{\mathsf{T}} \vdots \left(\widehat{\boldsymbol{\alpha}}^{[v-r+1]}\right)^{\mathsf{T}} \right] \\ &= \widehat{\boldsymbol{\alpha}}^{[v]} \boldsymbol{C}_j \boldsymbol{R} \left(\widehat{\boldsymbol{H}}_{\text{inv}}^{[v]}\right)^{\mathsf{T}}. \end{aligned}$$

Using Lemma 2.3 with $\boldsymbol{A} \stackrel{def}{=} \widehat{\boldsymbol{\alpha}}^{[v]}$, $\boldsymbol{X} \stackrel{def}{=} \boldsymbol{C}_j$ and $\boldsymbol{Y} \stackrel{def}{=} \boldsymbol{R} \left(\widehat{\boldsymbol{H}}_{\text{inv}}^{[v]}\right)^{\mathsf{T}}$ gives

$$\text{Jac}_{\text{row}(\boldsymbol{C}_j)} \left(g_{1,\ell_1,j} \ \dots \ g_{r,\ell_r,j}\right) = \widehat{\boldsymbol{\alpha}}^{[v]} \otimes \widehat{\boldsymbol{H}}_{\text{inv}}^{[v]} \boldsymbol{R}^{\mathsf{T}}.$$

Finally, the same proof technique used for Lemma 9.1 leads to

Lemma 9.2. *For $\widehat{\boldsymbol{\alpha}} \in \mathbb{F}_{q^m}^m$ a normal basis, let $\widehat{\boldsymbol{H}}_{inv} \in \mathbb{F}_{q^m}^{m \times r}$ be the matrix*

$$\widehat{\boldsymbol{H}}_{inv} \stackrel{def}{=} \begin{bmatrix} \widehat{\boldsymbol{\alpha}} \\ \dots \\ \widehat{\boldsymbol{\alpha}}^{-[r-1]} \end{bmatrix}.$$

For any fixed column $\boldsymbol{h}_j$ in $\boldsymbol{H}_{pub}$, $\ell \in \{0..m-1\}$ and $v \in \{0..m-1\}$, there are $\binom{r}{\lambda+1}$ degree falls from degree $\lambda+2$ to $\lambda+1$ given by the maximal minors of the matrix

$$\boldsymbol{N}_{(j,\ell,v)} \stackrel{def}{=} \begin{bmatrix} \widehat{\boldsymbol{h}_j}^{[\ell]} \left(\boldsymbol{V}^{[\ell]}\right)^{\mathsf{T}} \\ \boldsymbol{R} \left(\widehat{\boldsymbol{H}}_{inv}^{[v]}\right)^{\mathsf{T}} \end{bmatrix}.$$

The equations obtained in this way from all columns $\boldsymbol{h}_j$ in $\boldsymbol{H}_{\text{pub}}$, all indexes ℓ and all moduli v form a system of $nm^2\binom{r}{\lambda+1}$ polynomials of degree $\lambda+1$. They can also be seen as bilinear in the entries of the $\boldsymbol{V}^{[\ell]}$'s and in the maximal minors r_T of $\boldsymbol{R}$. If we come back to Modeling 16 over $\mathbb{F}_q$ which is the relevant one for a potential attack, this system corresponds to an extra set of $nm^2\binom{r}{\lambda+1}$ polynomials of degree $\lambda+1$ which are produced in degree $\lambda+2$ by the computation.

9.4.3 Solving a Degree Fall System

Instead of simply considering Modeling 16, our results provide another method by focusing on a system of degree fall polynomials of degree $\lambda+1$. It might be the one given by Lemma 9.1, Lemma 9.2 or a subset of such equations. As we have just seen,

this approach would benefit from the compactness of these polynomials due to the specific bilinear shape. Its analysis is left for future work, including the study of linear dependencies and the possibility of using hybrid techniques.

In the case of RD, solving the system given by the MaxMinors polynomials has led to a significant improvement over previous attacks based on Ourivski-Johansson. The same will not necessarily hold for Loidreau's. First, the ratio between equations and variables in Lemma 9.1 or Lemma 9.2 seems less favorable than in [Bar+20b]. Second, our tests suggest that the degree falls in degree $\lambda + 2$ do not mark the end of the computation when running F4 on Modeling 16 while it was often the case for RD [LP06; Bar+20a].

Part IV
Other Algebraic Systems

Chapter 10
Cryptanalysis of Regular Syndrome Decoding

This chapter contains a joint work with Morten Øygarden [BØ23] on a new algebraic attack on the Regular Syndrome Decoding problem (Problem 3.9).

We consider a folklore polynomial system containing the parity-check equations plus additional ones expressing the particular error distribution. Based on a careful theoretical analysis of this modeling, we show that the approach by solving this system may outperform standard decoding techniques on some concrete parameter sets used in PCGs. To the best of our knowledge, it is the first time that algebraic methods have appeared to be relevant in the Hamming setting.

Contents

10.1 Preliminaries

As we focus on applications to pseudorandom correlation generators, we will start by giving more details on the parameters of these primitives. We will then introduce the notion of witness degree that we use in our complexity analysis.

10.1.1 Relevant Parameters

In addition to regular errors, PCG constructions pick a structured code for better efficiency. Naturally, its choice must still yield secure decoding instances. It was for example proposed to use ℓ-local codes in the Primal case, *i.e.*, generator matrices $\boldsymbol{G}$ with column weight equal to a small integer ℓ [App+17]. Note however it would not be secure to reveal a parity-check matrix with constant locality in the Dual case, see [BCGI18; BBMS22]. In this case, other families such as quasi-cyclic codes or MDPC codes have been adopted.

All the corresponding variants of the Decoding Problem are conjectured to remain hard. In particular, known solving techniques have not been able to exploit the underlying structure. Since it is mostly aimed at modeling the regular distribution, our approach should not change this landscape. In fact, the equations depending on the code that we will consider are the same as in these previous attacks.

Table 10.1 contains typical parameters corresponding to [LWYY22, Table 1]. In their work, these values are obtained from [BCGI18, Table 1] by increasing the weight t and keeping the same code parameters k and n. The security of these instances would be 128 relying on [BCGI18] but they are thought to be much harder according to [LWYY22]. Even though the latter analysis might be flawed and even if we may not beat a more realistic complexity (ranging between 128 and the value of [LWYY22]), our goal will be to demontrate the feasibility of an algebraic attack in this parameter regime.

Table 10.1: PCG parameters in the Primal case [BCGI18; LWYY22].

n	k	t	Best $\mathbb{F}_2$ [LWYY22]	Best $\mathbb{F}_{2^{128}}$ [LWYY22]	Any field size [BCGI18]
2^{22}	64770	4788	147	156	128
2^{20}	32771	2467	143	155	128
2^{18}	15336	1312	139	153	128
2^{16}	7391	667	135	151	128
2^{14}	3482	338	132	150	128
2^{12}	1589	172	131	155	128
2^{10}	652	106	176	194	128

10.1.2 Witness Degree

On our modeling, one can obviously apply a general-purpose Gröbner basis algorithm. We also suggest to use XL-Wiedemann.

To estimate the parameter D in Proposition 2.7 and thus obtain the corresponding cost, we rely on the notion of *witness degree*. Its original definition was given in [BFSS13] for boolean systems.

Definition 10.1 (Witness degree, Definition 2, [BFSS13]). Let $\mathcal{F} = \{f_1, \dots f_m\}$ be an affine polynomial system over $\mathbb{F}_q$ and let $I = \langle \mathcal{F} \rangle$ be its associated ideal. For $d \in \mathbb{N}$, we consider the $\mathbb{F}_q$-vector spaces

$$I_{\leqslant d} \stackrel{def}{=} \{p \in I : \deg(p) \leqslant d\},$$
$$J_{\leqslant d} \stackrel{def}{=} \left\{ p \in I : p = \sum_{i=1}^{m} g_i f_i, \text{ and } \deg(g_i) \leqslant d - \deg(f_i) \text{ for } 1 \leqslant i \leqslant m \right\}.$$

Note that $J_{\leqslant d} \subset I_{\leqslant d}$. The *witness degree* d_{wit} of $\mathcal{F}$ is defined as the smallest integer d_0 such that $I_{\leqslant d_0} = J_{\leqslant d_0}$ and $\text{LM}(I_{\leqslant d_0}) = \text{LM}(I)$.

As explained in [BFSS13], the witness degree is the smallest integer d for which a row echelon form of the affine Macaulay matrix $\mathcal{M}\text{ac}_{\leqslant d}(\mathcal{F})$ yields a Gröbner basis.

If the input system does not have a solution, this value can be upper bounded by the degree of regularity of the homogenized ideal obtained by adding an extra homogenization variable[1]. In other words, we have

Proposition 10.1 (Proposition 5, [BFSS13]). *Let $\mathcal{F} = \{f_1, \dots, f_m, x_1^q - x_1, \dots, x_n^q - x_n\}$ be polynomial system in $\mathbb{F}_q[x_1, \dots, x_n]$ that admits no solutions, let $\mathcal{F}^{(z)}$ be the homogenized system and let $I^{(z)}$ be its associated ideal. Then $d_{wit}(\mathcal{F}) \leqslant d_{reg}\left(I^{(z)}\right)$.*

Remark 10.1. This statement was shown in the binary case but the same proof works over an arbitrary finite field.

Note that the requirement of $\mathcal{F}$ being non-consistent makes sense in [BFSS13] since they propose BooleanSolve which is a hybrid algorithm. For instance, the majority of calls to the system solver is made for equations without any solutions. Since we use hybrid techniques in Section 10.3, we will also rely on Proposition 10.1. However, on the plain systems, this result cannot be applied readily to bound d_{wit}. Instead, we will adopt a more direct approach of inspecting affine Macaulay matrices in Section 10.2.2.

10.2 Algebraic Modeling

This section introduces the polynomial systems that we consider for the RSD problem. We work over the polynomial ring $A \stackrel{def}{=} \mathbb{F}[\boldsymbol{e}]$, where each error entry $e_{i,j}$ is treated as an

[1] More formally, we apply the map given in Equation (2.5).

indeterminate to be solved for. Our equations are obtained from the $n-k$ parity-checks $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\mathsf{T}$ to which we add constraints coming from the regular structure. Modeling 18 is used to solve RSD over an arbitrary (large) field $\mathbb{F}_q$ while Modeling 19 is specific to the binary case.

Modeling 18 (Over a large field). *For a given RSD instance $(\boldsymbol{H}, \boldsymbol{s})$ over $\mathbb{F}_q$, $q \neq 2$, we consider the system $\mathcal{F} \stackrel{def}{=} \mathcal{P} \cup \mathcal{B}$, where*

i) $\mathcal{P}$ is the set of the $n-k$ linear polynomials given by the parity-check equations $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\mathsf{T}$;

ii) $\mathcal{B}$ is the set of quadratic polynomials that describe the regular form of the error vector $\boldsymbol{e}$, namely $e_{i,j_1}e_{i,j_2} = 0$ for $1 \leqslant i \leqslant t$ and $1 \leqslant j_1 < j_2 \leqslant N$.

We also include the field equations $e_{i,j}^q - e_{i,j} = 0$ to be certain that the ideal is zero-dimensional. However, they will not be useful for the computation due to their high degree. Note that this should not be a problem since our system is already very overdetermined in practice.

Modeling 18 only captures the fact that the Hamming weight in each block is at most 1 because we have no information on the non-zero entry. Over $\mathbb{F}_2$ however, we know that it is equal to 1. We will use this by adding linear equations expressing the fact that the sum of the coordinates within one block is equal to this value.

Modeling 19 (Over $\mathbb{F}_2$). *For a given binary RSD instance $(\boldsymbol{H}, \boldsymbol{s})$, we consider the system $\mathcal{F}_{\mathbb{F}_2} \stackrel{def}{=} \mathcal{P} \cup \mathcal{B} \cup \mathcal{Q}_{\mathbb{F}_2} \cup \mathcal{L}_{\mathbb{F}_2}$, where $\mathcal{P}$ and $\mathcal{B}$ are as in Modeling 18 and where*

i) $\mathcal{Q}_{\mathbb{F}_2}$ is the set of field equations $e_{i,j}^2 - e_{i,j} = 0$ for $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant N$;

ii) $\mathcal{L}_{\mathbb{F}_2}$ is the set of t linear equations $1 - \sum_{j=1}^{N} e_{i,j} = 0$ for $1 \leqslant i \leqslant t$.

Coming back to the PCG application, these systems can be employed regardless of the instantiation. Indeed, in the Primal case, one can trivially use the public data to reconstruct the RSD instance given in the dual form. For both modelings, let us also notice that the main contribution is the set $\mathcal{P}$ containing $n-k = n(1-k/n)$ parity-check equations. In particular, we expect our approach to be mostly relevant on small code rates $R = k/n$. This explains why we focused on Primal in our exposition. Finally, we see that the number of solutions is the same as in the original RSD problem. This makes it possible to apply XL since it is equal to 1 in this regime.

10.2.1 Hilbert Series

Hilbert series are known to be instrumental in obtaining the degree of regularity. Here, we use them to estimate the witness degree. First, we will give the ones of the homogeneous ideals $I \stackrel{def}{=} \langle \mathcal{F}^{(h)} \rangle$ and $I_{\mathbb{F}_2} \stackrel{def}{=} \langle \mathcal{F}_{\mathbb{F}_2}^{(h)} \rangle$ associated to Modeling 18 and Modeling 19 respectively.

Let us observe that these sequences cannot be analyzed as semi-regular systems. Indeed, consider the equations $f_1 \stackrel{def}{=} e_{1,1}e_{1,2}$ and $f_2 \stackrel{def}{=} e_{1,2}e_{1,3}$. Since $e_{1,1}f_2 = 0$ in $A/\langle f_1\rangle$, the polynomial f_2 is a non-trivial zero divisor in $A/\langle f_1\rangle$. This type of cancellation does not depend on the particular RSD instance but rather comes from the regular structure of $\boldsymbol{e}$. Thus, it still makes sense to compute Hilbert series that will be valid for generic instances of the RSD problem.

10.2.1.1 Hilbert Series of Modeling 18

We focus on $\mathcal{F} = \mathcal{P} \cup \mathcal{B}$, where $\mathcal{P}$ are the parity-check equations and where $\mathcal{B}$ describes the regular structure of the error vector. The first step will be to compute the Hilbert series $\mathcal{H}_S(z)$ by monomial counting, for $S \stackrel{def}{=} A/\langle \mathcal{B}^{(h)}\rangle$. Since S is not a polynomial ring, we will not formally speak about (semi-)regular sequences over S. Yet, we still want to capture the core idea of the remaining parity-check equations behaving nicely, by introducing the following assumption for Modeling 18.

Assumption 12. *Consider an instance $\mathcal{F} = \mathcal{P} \cup \mathcal{B}$ of Modeling 18 and let d_{reg} be the degree of regularity of $I = \langle \mathcal{F}^{(h)}\rangle$. Define the quotient ring $S = A/\langle \mathcal{B}^{(h)}\rangle$ and let $\mathcal{P}^{(h)} = \{p_1^{(h)}, \ldots, p_{n-k}^{(h)}\}$ denote the set of linear parity-check equations. We assume that for $1 \leqslant i \leqslant n-k$, $g_i p_i = 0$ in $S/\langle p_1, \ldots, p_{i-1}\rangle$ with $\deg(g_i p_i) < d_{reg}$ implies $g_i = 0$ in $S/\langle p_1, \ldots, p_{i-1}\rangle$.*

Relying on this assumption, we can obtain the Hilbert series for $I = \langle \mathcal{F}^{(h)}\rangle$.

Theorem 10.1. *Under Assumption 12, the Hilbert series of the homogeneous ideal $I = \langle \mathcal{F}^{(h)}\rangle$ associated to Modeling 18 is given by*

$$\mathcal{H}_{A/I}(z) = \left[(1-z)^{n-k}\left(1 + N\tfrac{z}{1-z}\right)^t\right]_+, \tag{10.1}$$

where $[.]_+$ means truncation after the first non-positive coefficient.

The proof of Theorem 10.1 easily follows from the following lemmata.

Lemma 10.1. *Let S denote the quotient ring $A/\langle \mathcal{B}^{(h)}\rangle$, where $\mathcal{B}^{(h)}$ consists of the quadratic parts of the structural equations from Modeling 18. We have*

$$\mathcal{H}_S(z) = \left(1 + N\tfrac{z}{1-z}\right)^t. \tag{10.2}$$

Proof. The quotient S can be seen as the set of polynomials whose monomials involve at most one $e_{i,j}$ variable in each block $1 \leqslant i \leqslant t$. For a given block, admissible monomials have only one variable but their degree can be arbitrary. Therefore, the Hilbert series "for one block" will be $1 + N\frac{z}{1-z}$. Finally, a general d monomial is a product of such monomials for distinct blocks and such that the sum of their degrees is equal to d. We finally obtain Equation (10.2) from the standard argument [FS09b, Equation (14)] giving the generating series of a Cartesian product of classes. □

Lemma 10.2. *Let I denote the homogeneous ideal associated to Modeling 18 by taking the top degree parts. Under Assumption 12, we have*

$$\mathcal{H}_{A/I}(z) = \Big[(1-z)^{n-k}\mathcal{H}_S(z)\Big]_+ .$$

Proof. This may be seen as a particular case of [Bar04, §3.3.2]. We give the proof here for the sake of completeness. To simplify notation, we write $\{f_1, \ldots, f_{n-k}\}$ for the set of homogeneous parity-check equations $\mathcal{P}^{(h)}$. For $1 \leqslant j \leqslant n-k$, we denote by $I(j)$ the ideal $\langle \mathcal{B}^{(h)}, f_1, \ldots, f_j \rangle$ in A and $I(0) = \langle \mathcal{B}^{(h)} \rangle$. For $1 \leqslant j \leqslant n-k$ and up to the degree of regularity of I, Assumption 12 states that we have the exact sequence of vector spaces when $d < d_{\text{reg}}$:

$$0 \to (A/I(j-1))_{d-1} \to (A/I(j-1))_d \to (A/I(j))_d \to 0.$$

This gives the following equality between Hilbert functions

$$\mathcal{HF}_{A/I(j-1)}(d-1) - \mathcal{HF}_{A/I(j-1)}(d) + \mathcal{HF}_{A/I(j)}(d) = 0. \tag{10.3}$$

Consider now the abstract sequence $h_{d,j}$ defined by $h_{d,j} = \dim_{\mathbb{F}_q}(S_d)$ if $j = 0$ or $d = 0$ and the induction relation

$$h_{d,j} = h_{d,j-1} - h_{d-1,j-1}. \tag{10.4}$$

Let $\mathcal{G}_j$ denote the generating series for $(h_{d,j})_{d \geqslant 0}$. From Equation (10.4) and by multiplying by z we easily obtain $\mathcal{G}_j(z) = (1-z)\mathcal{G}_{j-1}(z)$. The generating series for $(h_{d,0})_{d \geqslant 0}$ being $\mathcal{G}_0(z) \stackrel{def}{=} \mathcal{H}_S(z)$ we get $\mathcal{G}_{n-k}(z) = (1-z)^{n-k}\mathcal{H}_S(z)$. As long as the involved quantities are positive, Equation (10.3) and Equation (10.4) may be seen as the same relation. Therefore, the final Hilbert series is

$$\mathcal{H}_{A/I}(z) = \Big[(1-z)^{n-k}\mathcal{H}_S(z)\Big]_+ .$$

□

10.2.1.2 Hilbert Series of Modeling 19

Modeling 19 contains extra structural equations, starting from the field equations in $\mathcal{Q}_{\mathbb{F}_2}$. A difficulty arises when adding the last set of equations $\mathcal{L}_{\mathbb{F}_2}$ since it yields another type of cancellation. For $1 \leqslant i \leqslant t$ and $1 \leqslant j_0 \leqslant N$, we indeed have

$$e_{i,j_0}\left(-\sum_{j=1}^{N} e_{i,j}\right) = 0 \bmod \left\{e_{i,j_0}^2, \{e_{i,j_1}e_{i,j_2}\}_{j_1<j_2}\right\}. \tag{10.5}$$

In other words, any polynomial in $\mathcal{L}_{\mathbb{F}_2}^{(h)}$ is a zero divisor in $A/\langle \mathcal{B}^{(h)} \cup \mathcal{Q}_{\mathbb{F}_2}^{(h)} \rangle$. To keep the same type of analysis as with Modeling 18, we may use $\mathcal{L}_{\mathbb{F}_2}$ to remove t variables. More

formally, we define the graded ring homomorphism

$$\begin{aligned} \mathcal{L} : \mathbb{F}_2[\boldsymbol{e}] &\longrightarrow \mathbb{F}_2[\boldsymbol{x}] \\ e_{i,j} &\longmapsto x_{i,j}, \text{ for } 1 \leqslant i \leqslant t \text{ and } 1 \leqslant j < N \\ e_{i,N} &\longmapsto \sum_{j=1}^{N-1} x_{i,j} \text{ for } 1 \leqslant i \leqslant t. \end{aligned} \tag{10.6}$$

We also set $A' \stackrel{def}{=} \mathcal{L}(A)$, $I' \stackrel{def}{=} \mathcal{L}(I^{(h)})$, $\mathcal{B}' \stackrel{def}{=} \mathcal{L}(\mathcal{B}^{(h)})$, $\mathcal{Q}' \stackrel{def}{=} \mathcal{L}(\mathcal{Q}_{\mathbb{F}_2}^{(h)})$ and $S' \stackrel{def}{=} A'/\langle \mathcal{B}' \cup \mathcal{Q}' \rangle$. The following lemma shows that the image of A under $\mathcal{L}$ is still a polynomial ring and it describes the structure of S'.

Lemma 10.3. *The image of A is isomorphic to $\mathbb{F}_2[x_1, \ldots, x_{n-t}]$. Moreover, the ideal $\langle \mathcal{B}' \cup \mathcal{Q}' \rangle$ is generated by $\mathcal{G} \stackrel{def}{=} \{x_{i,j}x_{i,l} : 1 \leqslant i \leqslant t \text{ and } 1 \leqslant j, l < N\}$.*

Proof. The first statement is immediate from the definition of $\mathcal{L}$. For the second one, we note that $\mathcal{G}$ corresponds to the image of generators of $\mathcal{B}^{(h)} \cup \mathcal{Q}_{\mathbb{F}_2}^{(h)}$ that do not contain an element $e_{i,N}$. To see that the image of the rest of the generators of $\mathcal{Q}_{\mathbb{F}_2}^{(h)}$ does not add anything new, we get

$$\mathcal{L}(e_{i,N}^2) = \left(\sum_{j=1}^{N-1} x_{i,j}^2 \right) = 0 \bmod \mathcal{G}.$$

The cancellations of the remaining generators of $\mathcal{B}^{(h)}$ were already pointed out by Equation (10.5). □

We can furthermore use Lemma 10.3 to count the number of monomials in S'. Indeed, the possible monomials are squarefree and they contain only one variable per block due to the shape of $\mathcal{G}$. In particular, a degree d monomial defines a set of d blocks. Then, each block contains $N-1$ relevant variables instead of N since we reduce modulo $\mathcal{L}_{\mathbb{F}_2}$. This shows that there are $\binom{t}{d}(N-1)^d$ degree d monomials in S'.

The final Hilbert series will call for a similar hypothesis as with Modeling 18. Note the strong similarity between Definition 2.13 and the following Assumption 13.

Assumption 13. *Consider an instance $\mathcal{F}_{\mathbb{F}_2}$ of Modeling 19 and let d_{reg} be the degree of regularity of $I_{\mathbb{F}_2} = \langle \mathcal{F}_{\mathbb{F}_2}^{(h)} \rangle$. Let $\mathcal{L}$ denote the ring morphism of Equation (10.6) and let $A' \stackrel{def}{=} \mathcal{L}(A)$, $\mathcal{B}' \stackrel{def}{=} \mathcal{L}(\mathcal{B}^{(h)})$, $\mathcal{Q}' \stackrel{def}{=} \mathcal{L}(\mathcal{Q}_{\mathbb{F}_2}^{(h)})$ and $S' \stackrel{def}{=} A'/\langle \mathcal{B}' \cup \mathcal{Q}' \rangle$. For every parity-check equation p_i, write $p_i' = \mathcal{L}(p_i^{(h)})$. We assume that for $1 \leqslant i \leqslant n-k$, $g_i p_i' = 0$ in $S'/\langle p_1', \ldots, p_{i-1}' \rangle$ with $\deg(g_i p_i') < d_{reg}$ implies $g_i = 0$ in $S'/\langle p_1', \ldots, p_i' \rangle$.*

Theorem 10.2. *Under Assumption 13, the Hilbert series of the homogeneous ideal $I_{\mathbb{F}_2} = \langle \mathcal{F}_{\mathbb{F}_2}^{(h)} \rangle$ associated to Modeling 19 is given by*

$$\mathcal{H}_{A/I_{\mathbb{F}_2}}(z) = \left[\frac{(1+(N-1)z)^t}{(1+z)^{n-k}} \right]_+, \tag{10.7}$$

where $[.]_+$ means truncation after the first non-positive coefficient.

The structure of the proof is the same as for Theorem 10.1. We rely on Lemma 10.4 and Lemma 10.5 below, where the notation are those recalled in Assumption 13.

Lemma 10.4. *We have*

$$\mathcal{H}_{S'}(z) = (1 + (N-1)z)^t .$$

Proof. From the set of generators $\mathcal{G}$ described in Lemma 10.3, we observe that the admissible monomials of S' involve at most one variable from each block, with degree at most 1. From there, we proceed as in Lemma 10.1. □

Lemma 10.5. *Let $I_{\mathbb{F}_2}$ denote the homogeneous ideal associated to Modeling 19 by taking the top degree parts. Under Assumption 13, we have*

$$\mathcal{H}_{A/I_{\mathbb{F}_2}}(z) = \left[\mathcal{H}_{S'}(z)/(1+z)^{n-k}\right]_+ .$$

Proof (sketch). By construction and if $I' \stackrel{def}{=} \mathcal{L}(I_{\mathbb{F}_2})$, we clearly have $\mathcal{H}_{A/I}(z) = \mathcal{H}_{A'/I'}(z)$. As in the proof of Lemma 10.2, we simplify notation by writing $\{f_1, \ldots, f_{n-k}\}$ for the set of homogeneous parity-check equations $\mathcal{L}(\mathcal{P}^{(h)})$, and for $1 \leqslant j \leqslant n-k$, we denote by $I'(j)$ the ideal $\langle \mathcal{B}', \mathcal{Q}', f_1, \ldots, f_j \rangle$ in A' and $I'(0) = \langle \mathcal{B}', \mathcal{Q}' \rangle$. Assumption 13 ensures that the following sequence is exact for $d < d_{\text{reg}}$.

$$0 \to (A'/I'(j))_{d-1} \xrightarrow{\times f_j} (A'/I'(j-1))_d \xrightarrow{\pi} (A'/I'(j))_d \to 0.$$

The rest of the proof proceeds in the same way as [BFSY05, Proposition 9], starting from the equality between Hilbert functions

$$\mathcal{HF}_{A'/I'(j)}(d-1) - \mathcal{HF}_{A'/I'(j-1)}(d) + \mathcal{HF}_{A'/I'(j)}(d) = 0. \tag{10.8}$$

Similarly, we consider the sequence $c_{d,j}$ defined by $c_{d,j} = \dim_{\mathbb{F}_2}(S'_d)$ if $j = 0$ or $d = 0$ and the recurrent formula

$$c_{d,j} = c_{d,j-1} - c_{d-1,j}. \tag{10.9}$$

Let $\mathcal{C}_j$ denote the generating series for $(c_{d,j})_{d \geqslant 0}$. Multiplying by z in Equation (10.9) yields $(1+z)\mathcal{C}_j(z) = \mathcal{C}_{j-1}(z)$ and we have the border condition $\mathcal{C}_0(z) = \mathcal{H}_{A'/I'(0)}(z) = \mathcal{H}_{S'}(z)$. This finally gives

$$\mathcal{H}_{A/I}(z) = \mathcal{H}_{A'/I'}(z) = \left[\frac{\mathcal{H}_{S'}(z)}{(1+z)^{n-k}}\right]_+ .$$

□

10.2.2 Estimate for d_{wit}

In this section, we derive an upper bound on the witness degree of Modeling 18 (resp. Modeling 19). As explained at the end of Section 10.1, we cannot use Proposition 10.1 on systems which have a solution. In particular, our analysis assumes that the input

modeling has a single one. Note that a polynomial system that includes field equations[2] with unique solution $(a_1, \ldots, a_n)$ has reduced Gröbner basis $\{x_1 - a_1, \ldots, x_n - a_n\}$. Recalling the conditions in Definition 10.1 and if $I = \langle \mathcal{F} \rangle$, we have $\mathrm{LM}(I_{\leqslant 1}) = \mathrm{LM}(I)$ and $\dim(I_{\leqslant d}) = \dim(A_{\leqslant d}) - 1$. We can then say that $d_{\mathrm{wit}}(\mathcal{F})$ is the smallest degree such that the rank of the associated affine Macaulay matrix is equal to the number of columns minus one.

We will use this observation to provide an estimate of the witness degree. Note that semi-regularity can be seen as the assumption that the *homogeneous* Macaulay matrices have maximal rank. Here, we need the hypothesis that the *affine* Macaulay matrices achieve maximal rank. Under this assumption, we use the Hilbert series derived above. More precisely, we consider the generating functions in Equations (10.1) and (10.7) that have been truncated to obtain these series. The coefficient in a term of degree $d < d_{\mathrm{reg}}$ is positive and it coincides with the number of columns that cannot be reduced in the homogeneous Macaulay matrix $\mathcal{M}\mathrm{ac}_d(\mathcal{F}^{(h)})$. When $d \geqslant d_{\mathrm{reg}}$, the coefficient is non-positive and it measures the number of "excess" rows after full reduction of this matrix which should in general provide degree falls from the degree d for the affine system $\mathcal{F}$. Finally, we arrive at the following estimate for the witness degree by summing these coefficients.

Estimate 2 (Witness degree). *Let $\mathcal{F}$ be the polynomial system of Modeling 18 (resp. Modeling 19) and let $\mathcal{H}$ denote the generating series of Equation (10.1) (resp. Equation (10.7)). We estimate $d_{wit}(\mathcal{F})$ to be*

$$d_{wit,(0,0)} \stackrel{def}{=} \min \left\{ d \in \mathbb{Z}_{>0} : \sum_{j=0}^{d} [z^j] \left(\mathcal{H}(z) \right) \leqslant 0 \right\}, \tag{10.10}$$

where $[z^j] \left(\mathcal{H}(z) \right)$ denotes the coefficient of the monomial z^j in $\mathcal{H}$.

10.3 Hybrid Approach

As is standard in algebraic cryptanalysis, the complexity of our attack mainly depends on the value of d_{reg} or d_{wit}. However, for most of the parameter sets given in Table 10.1, these degrees seem too high for straightforward algebraic techniques to be competitive. To decrease these degrees and possibly improve the overall complexity, we propose to add new equations in the same $\boldsymbol{e}$ variables which hold with probability $\pi \in]0, 1[$. The idea is the same as in a standard hybrid approach and it has already been encountered several times in Part III.

Due to the tiny noise rate, a natural method is to fix linear constraints of the form $e_{i',j'} = 0$. Note that this is exactly what the Prange algorithm does by picking an information set I and then assuming that $\boldsymbol{e}_I = \mathbf{0}$. In our case, this allows to reduce the

[2] Field equations ensure that the ideal is radical and the result follows from the Nullstellensatz. In practice, the reliance on field equations can typically be eased for sufficiently overdetermined systems. We will thus assume that it also holds for Modeling 18.

number of non-zero monomials in degree $d \geqslant 1$ (even though the number of equations at hand also decreases) and thus we hope that the specialized system with these constraints will be solved at a smaller degree. In the following, we present this technique for Modeling 18, noting that the case of Modeling 19 is analogous. More precisely, we will give two structured ways to set variables to zero. In addition to being quite elementary, the interest of these specializations is that we still control the behaviour of the resulting system.

10.3.1 Error-Free Positions in All Blocks

A first strategy is to guess an equal number of noise-free coordinates in all portions $\boldsymbol{e}_i$. A similar approach was followed in [HOSS18, B.3] to adapt ISDs to the regular distribution. Each block in the RSD problem can be seen as a random vector of length N and weight 1. The success probability of guessing u error-free positions is $\binom{N-1}{u}/\binom{N}{u}$. By exploiting the regular structure, one may guess the same number of positions in each block with probability

$$\pi_{(u)} \stackrel{def}{=} \left(\frac{\binom{N-1}{u}}{\binom{N}{u}}\right)^t = (1-u/N)^t. \tag{10.11}$$

The improvement by using Equation (10.11) instead of the naive probability in Prange (or even in more involved ISD variants) was not really apparent in [HOSS18] ("ISD is always the most efficient attack and has roughly the same cost when considering SD and RSD" [HOSS18, p. 49]).

Still, we adopt the same technique on Modeling 18. In each block, we assume that the top part of size $u \in \{0..N\}$ is error-free. This should hold with probability $\pi_{(u)}$. The main difference with [HOSS18, B.3] is that we will consider $ut \ll k$. Indeed, we need to guess much fewer zero positions to decrease the solving degree of Modeling 18 while the Prange linear system "stays" in degree 1 and needs more equations. In case of failure, we pick a permutation matrix $\boldsymbol{P}_\sigma$ which permutes the coordinates in each block (so that the regular structure is preserved) and we try again on the RSD instance $(\boldsymbol{H}\boldsymbol{P}_\sigma^{-1}, \boldsymbol{s})$ which has error $\boldsymbol{\varepsilon}^\mathsf{T} = \boldsymbol{P}_\sigma \boldsymbol{e}^\mathsf{T}$. By fixing the $e_{i,j}$ variables to zero for $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant u$, the number of possible non-zero monomials in degree d is now given by the coefficient of z^d in $\left(1 + (N-u)\frac{z}{1-z}\right)^t$.

To derive the Hilbert series of the specialized modeling, we need to adapt Assumption 12 to ensure that zeroizing unknowns does not introduce unexpected cancellations at higher degree among the system of parity-check equations. Such an assumption is rather natural since we end up in this case with a reduced RSD instance with block size $N-u$ obtained by shortening the initial (random) code. On that new assumption, the Hilbert series of the hybrid system is

$$\mathcal{H}_{A/I,\mathrm{hyb1},u}(z) = \left[(1-z)^{n-k}\left(1 + (N-u)\frac{z}{1-z}\right)^t\right]_+. \tag{10.12}$$

Hence, while both the number of equations and monomials of degree $d \geqslant 1$ are affected by adding the zero constraints, they are still of a form that is captured by the series studied in Section 10.2.

In practice, we in fact require a weaker hypothesis. This is because the optimal choice of u is rather small for the parameters of Table 10.1. Heuristically, we are more confident that the resulting equations behave as expected when the number of fixed variables is reduced. Finally, we note that a similar statement for specialized systems is also present in the standard hybrid approach for semi-regular systems, see [BFP10, Hypothesis 3.3]. Starting from a semi-regular sequence $(f_1, \ldots, f_m)$, they assume that all the specialized versions

$$\Big\{(f_1(x_1, \ldots, x_{n-k}, \boldsymbol{v}), \ldots, f_m(x_1, \ldots, x_{n-k}, \boldsymbol{v})) : \forall \boldsymbol{v} \in \mathbb{F}_q^k \text{ and } \forall 0 \leqslant k \leqslant n\Big\}$$

are semi-regular.

10.3.2 Considering Less Blocks

A slightly more general approach is to guess $u \in \{0..N\}$ error-free coordinates in only $f \in \{0..t\}$ blocks so that the success probability becomes $\pi_{(f,u)} \stackrel{def}{=} (1 - u/N)^f$. We recover the previous strategy with $f = t$. To derive the Hilbert series, we adopt the following Assumption 14 (which encompasses Section 10.3.1 when $f = t$). For any invertible matrix $\boldsymbol{P}$, $u \in \{0..N\}$ and $f \in \{0..t\}$, let $\overline{\mathbf{P}^{-1}_{u,f}}$ denote the map that applies $\mathbf{P}^{-1}$ and then fixes the initial u variables to 0 in the last f blocks of the error.

Assumption 14. *Let $\mathcal{P}$ be the set of parity-check equations from an instance of Modeling 18. For every permutation matrix $\mathbf{P}$ which stabilizes each block, for $f \in \{0..t\}$ and for $u \in \{0..N\}$, we assume that $\mathcal{P}^{(h)} \circ \overline{\mathbf{P}^{-1}_{u,f}}$ satisfies Assumption 12 with ring $A \circ \overline{\mathbf{P}^{-1}_{u,f}}$ and quotient ring $S \circ \overline{\mathbf{P}^{-1}_{u,f}}$.*

On that hypothesis, we finally obtain

$$\mathcal{H}_{A/I,\mathrm{hyb2},f,u}(z) = \left[(1-z)^{n-k} \underbrace{\left(1 + (N-u)\frac{z}{1-z}\right)^f}_{\text{constraint}} \underbrace{\left(1 + N\frac{z}{1-z}\right)^{t-f}}_{\text{no constraint}}\right]_+ . \tag{10.13}$$

10.3.3 Witness Degree for the Hybrid Approach

Similary to what we did in Section 10.2.2 for the plain system, we now derive an estimate of the witness degree for the specialized polynomials. As the initial modeling has a unique solution, the majority of guesses will be wrong, *i.e.*, resulting in non-consistent systems. We can in this case use Proposition 10.1 to upper bound d_{wit} by the degree of regularity of the homogenized ideal. All that remains is to evaluate this latter quantity.

For that purpose, we assume that the hybrid systems form semi-regular sequences when homogenized. Based on this assumption, it is straightforward to adapt the Hilbert

series given by Equation (10.12) and Equation (10.13) to these homogenized versions in the following manner:

$$\mathcal{H}_{A/I,\mathrm{hyb}i,f,u}(z)/(1-z), \tag{10.14}$$

for $i \in \{1,2\}$. Note that this adaptation is in line with the earlier literature [BFSS13, Proposition 6] and that it has been accurate in our experiments (see). Finally, the degree of regularity is obtained in the usual way by computing the first non-positive coefficient in the associated generating series.

10.3.4 Complexity with XL Wiedemann

The cost of the hybrid approach is computed as follows. For each couple (f,u), $f \in \{0..t\}$, $u \in \{0..N\}$, we proceed as explained in Section 10.3.3 to obtain an upper-bound on the witness degree denoted by $d_{\mathrm{wit},(f,u)}$ and that we use as our estimate of the real witness degree. To apply Equation (2.8), we also need the number of columns which is the number of monomials of degree $\leqslant d_{\mathrm{wit},(f,u)}$ in the specialized system. It depends on both f, u and $d_{\mathrm{wit},(f,u)}$. For $\mathcal{H}_{(S,f,u)}(z) = \left(1+(N-u)\frac{z}{1-z}\right)^f \left(1+N\frac{z}{1-z}\right)^{t-f}$, it is indeed given by

$$M^{(f,u)}_{\leqslant d_{\mathrm{wit},(f,u)}} = \sum_{j=0}^{d_{\mathrm{wit},(f,u)}} [z^j]\left(\mathcal{H}_{(S,f,u)}(z)\right), \tag{10.15}$$

where we recall that $[z^j](\mathcal{H}(z))$ is the coefficient of the monomial z^j in the series $\mathcal{H}$. Finally, we have to estimate the quantity n_μ which is the number of non-zero terms in one row of the Macaulay matrix. This is directly related to the monomial content of the initial parity-check equations. We can assume that the matrix $\boldsymbol{H}$ is in systematic form, hence $n_\mu \leqslant k+1 = \mathcal{O}(k)$. For the specialized system, we can actually choose to fix the f bottom blocks of the error[3] to obtain the better factor $n_{\mu,(f,u)} \leqslant k+1-fu$. This allows to possibly gain a few bits in the final complexity.

Proposition 10.2. *Under Assumption 14 and the assumptions described in Section 10.3.3, the time complexity in $\mathbb{F}_q$-operations of the hybrid approach of Section 10.3.2 on Modeling 18 is estimated by*

$$\mathcal{O}\left(\min_{\substack{f\in\{0..t\}\\ u\in\{0..N\}}} (1-u/N)^{-f}\,(k+1-fu)\left(M^{(f,u)}_{\leqslant d_{\mathrm{wit},(f,u)}}\right)^2\right),$$

where $M^{(f,u)}_{\leqslant d_{\mathrm{wit},(f,u)}}$ is defined in Equation (10.15) and where $d_{\mathrm{wit},(f,u)}$ is the index of the first non-positive coefficient in the generating series given in Equation (10.14).

[3] There is no loss of generality: this can be seen as choosing a monomial ordering which favors the upper variables and then fixing somehow small variables

Remark 10.2. The cost of the hybrid approach on Modeling 19 is analogous and we refer to [BØ23, B.2, Propostion 7].

Finally, let us mention that the specializations proposed in Sections 10.3.1 and 10.3.2 are possibly the most naive ways to fix variables in the system. Even though they seem to lead to the best success probability as we take advantage of the distribution, other approaches might allow to decrease the solving degree faster.

10.3.5 Discussion on the Assumptions

Our working hypotheses are of the same type as those generally encountered in algebraic cryptanalysis. More specifically, in our systems, they concern the linear parts of the parity-check equations. Thus, they only depend on the matrix $\boldsymbol{H}$. Even though the underlying code is often structured, the parity-check matrix obtained from the public $\boldsymbol{G}$ has no reason to be special in a certain sense. Otherwise, such a property would probably be exploited by common attacks or suggest that this instantiation is weaker.

In a very similar context, the well-known Arora-Ge system [AG11] to solve LWE is generally assumed to be semi-regular [Alb+12; STA20]. In [ACFP14], some practical experiments have been performed to confirm this hypothesis ([ACFP14, §7.1]). We also note that they tried to prove (a weaker form of) it in some particular cases ([ACFP14, A.2]). Their experiments verify that the solving degree of Arora-Ge coincides with that of a random system of the same size.

Our experiments to test the assumptions made throughout Sections 10.2 and 10.3 can be found in Section 10.5.

10.4 Application to the Primal Setting in PCGs

This section gives the complexity of our hybrid technique on parameters sets used in the Primal case. We consider binary instances and ones over a larger field.

We focus on the values proposed in [LWYY22, Table 1] that we recalled in Table 10.1 together with the weaker ones of [BCGI18, Table 1] where the weight t is smaller. When n/t is not an integer, we set $N = \lfloor n/t \rfloor$ and we fix the last $n - tN$ coordinates to zero. Note that the number of parity-check equations at hand is still $n - k$.

We have also tested our methods on the parameters of [Yan+20] and [WYKW21]. While most of them seem resistant to the attack, a notable exception is the one-time parameter set $q = 2^{61} - 1$, $n = 642048$, $k = 19870$ and $t = 2508$ from [WYKW21, Table 2]. The authors claim to achieve 128 bits of security but [LWYY22] would suggest that this is too conservative. More precisely, the Python script provided in [LWYY22] gives a 154 bit security. For our part, we estimate that solving plain Modeling 18 in degree 3 yields a 126 bit cost.

10.4.1 Binary Case

In Tables 10.3 and 10.2, "Best" refers to the limiting attack according to the work of [LWYY22]. This corresponds to an advanced ISD algorithm. In our case, we report the couple (f, u) that leads to the optimal complexity and the associated estimate for the witness degree $d_{\text{conj}} = d_{\text{wit},(f,u)}$. This analysis was presented for Modeling 18, namely Estimate 2 when $f = u = 0$ and the content of Section 10.3.3 when we fix variables. We let the reader adapt it to Modeling 19. Note that the sparsity factor n_μ can be chosen as $\min(k + 1 - fu,\ k/2 + 1)$ over $\mathbb{F}_2$. The constant from the Wiedemann algorithm is taken equal to 3 as explained in Remark 2.1. Finally, for illustration, we give the plain witness degree of Modeling 19 in Column "d_{conj} plain".

Table 10.2: Hybrid approach on Modeling 19 (higher weight).

n	k	t	Best [LWYY22]	d_{conj} plain	(f, u)	d_{conj}	XL hybrid
2^{22}	64770	2735	104	2	$(0, 0)$	2	103
2^{20}	32771	1419	99	3	$(1159, 2)$	2	98
2^{18}	15336	760	95	3	$(657, 7)$	2	104
2^{16}	7391	389	91	4	$(373, 10)$	2	108
2^{14}	3482	198	86	6	$(197, 11)$	2	106
2^{12}	1589	98	83	8	$(88, 13)$	2	103
2^{10}	652	57	94	12	$(54, 9)$	2	101

Table 10.3: Hybrid approach on Modeling 19 (low weight).

n	k	t	Best [LWYY22]	d_{conj} plain	(f, u)	d_{conj}	XL hybrid
2^{22}	64770	4788	147	2	$(0, 0)$	2	103
2^{20}	32771	2467	143	3	$(2340, 4)$	2	125
2^{18}	15336	1312	139	4	$(676, 1)$	3	122
2^{16}	7391	667	135	5	$(604, 7)$	2	139
2^{14}	3482	338	132	7	$(322, 7)$	2	138
2^{12}	1589	172	131	11	$(154, 7)$	2	135
2^{10}	652	106	176	19	$(104, 4)$	3	145

10.4.2 Large Field Case

Following [LWYY22], we also consider the larger field $\mathbb{F}_{2^{128}}$. According to the authors, the best attack in this case is the most naive one. Indeed, their observation is that Prange and more involved ISDs perform equally. Note that this is reminiscent of the result of Canto-Torres [Can17] which states that all ISD variants converge to the same cost when the field size tends to infinity. Our results for this setting are summarized in Tables 10.4, 10.5 below, with the same notation as in Tables 10.3, 10.2.

Table 10.4: Hybrid approach on Modeling 18 over $\mathbb{F}_{2^{128}}$ (low weight).

n	k	t	Best [LWYY22]	d_{conj} plain	(f, u)	d_{conj}	XL hybrid
2^{22}	64770	2735	108	2	$(0, 0)$	2	104
2^{20}	32771	1419	107	3	$(1246, 3)$	2	102
2^{18}	15336	760	105	3	$(670, 8)$	2	107
2^{16}	7391	389	103	4	$(374, 11)$	2	111
2^{14}	3482	198	101	6	$(197, 12)$	2	110
2^{12}	1589	98	100	8	$(96, 13)$	2	107
2^{10}	652	57	111	14	$(55, 10)$	2	111

Table 10.5: Hybrid approach on Modeling 18 over $\mathbb{F}_{2^{128}}$ (higher weight).

n	k	t	Best [LWYY22]	d_{conj} plain	(f, u)	d_{conj}	XL hybrid
2^{22}	64770	4788	156	3	$(4237, 1)$	2	110
2^{20}	32771	2467	155	3	$(0, 0)$	3	131
2^{18}	15336	1312	153	4	$(995, 2)$	3	133
2^{16}	7391	667	151	6	$(613, 8)$	2	150
2^{14}	3482	338	150	8	$(324, 8)$	2	150
2^{12}	1589	172	155	12	$(157, 8)$	2	150
2^{10}	652	106	194	24	$(105, 5)$	3	179

10.4.3 Comments on the Results

A first remark is that a high witness degree for the plain system can be circumvented by the hybrid component of the attack which is analogous to Prange. Thus, we should not expect a too big gap in the complexity compared to the previous techniques in general.

By comparing Table 10.3 with Table 10.2 and Table 10.4 with Table 10.5, we notice that this difference is much reduced in the higher weight setting. We also observe that our attack is extremely efficient compared to ISDs when we can solve at degree 2, 3 without fixing a lot of variables (see for instance the first three rows in Tables 10.2 and 10.5). This may suggest a weak zone of parameters which is not encompassed by former methods.

Finally, the algebraic attack seems to compare better to known algorithms for larger fields. As mentioned above, the main reason may be that the advantage of ISDs over Prange worsens when the field size goes to infinity. In our case, even though the witness degree for plain Modeling 18 is slightly higher than the one of Modeling 19, the difference does not seem enough to expect a similar increase in the cost as we see in ISDs.

10.5 Practical Experiments

In this section, we present experiments that we have run on randomly generated instances[4] of the RSD problem in order to check the validity of our assumptions. All these tests have been performed using the computer algebra system Magma V2.27-1.

10.5.1 Hilbert Series

We give the parameter sets as $(t, N, k, f, u)_\nu$, where t, N and k describe the RSD problem, where f, u are the parameters of the hybrid approach and where ν is the number of times that we have repeated the experiment. For an affine ideal I, we have computed the Hilbert series of the ideal $I^{(h)}$ generated by the top degree parts. We used the built-in command `HilbertSeries`$(\cdot)$.

10.5.1.1 Experiments for Modeling 18

The systems we have tested for Modeling 18 are listed in Table 10.6 below, where we also give the associated degree of regularity d_{reg} of $I^{(h)}$. In all cases, the experimentally found Hilbert series was equal to the series of Equation (10.13), meaning, in particular, that Assumptions 12 and 14 have been true in all our experiments. For most of the hybrid systems, we have also computed the Hilbert series of the homogenized ideals $I^{(z)}$ and we give the associated degree of regularity $d_{\text{reg}}^{(z)}$. The Hilbert series in all of these tests have been equal to (the truncation of) those predicted by Equation (10.14).

Table 10.6: Tested Hilbert series from Hybrid Modeling 18 systems over $\mathbb{F}_{101}$.

System	d_{reg}	$d_{\text{reg}}^{(z)}$	System	d_{reg}	$d_{\text{reg}}^{(z)}$	System	d_{reg}	$d_{\text{reg}}^{(z)}$
$(5,6,15,0,0)_5$	3	-	$(5,6,20,0,0)_5$	4	-	$(5,8,20,0,0)_5$	3	-
$(5,8,30,0,0)_5$	4	-	$(7,7,30,0,0)_5$	4	-	$(8,6,30,0,0)_5$	5	-
$(10,4,25,0,0)_5$	6	-	$(12,7,50,3,2)_1$	5	-	$(7,8,30,2,3)_{10}$	3	3
$(7,8,30,6,3)_{10}$	2	3	$(10,7,40,5,2)_{10}$	4	4	$(10,7,40,5,3)_{10}$	3	4

10.5.1.2 Experiments for Modeling 19

Table 10.7 contains tests for the Hilbert series related to Modeling 19. The experimental series of the plain cases $f = u = 0$ were conform with Theorem 10.2. While the majority of hybrid cases we have tested were accurately described by our estimates (*e.g.*, [BØ23, B.2, Equation (21)]), we have been able to find a few discrepancies with the theoretical values. The systems marked by † both included a single case where the experimental Hilbert series deviated slightly from our prediction in one of its terms. The system marked by ‡ was another type of outlier, where the quotient $A/I^{(h)}$ contained a few

[4] we have not tried on structured codes

cubic elements in half of the tested cases. We note that for the system marked by ‡, the corresponding generating series of Equation [BØ23, B.2, Equation (21)] is exactly zero at term z^2. Thus, the homogeneous Macaulay matrix in degree 2 will be a square matrix over $\mathbb{F}_2$ (after removing trivial syzygies) and the quotient $A/I^{(h)}$ will contain cubic terms whenever this matrix fails to be of full rank. For the other tested cases, the series have a *negative* coefficient at the term corresponding to the degree of regularity, indicating that the homogeneous Macaulay matrices will be rectangular. We believe that this difference explains the peculiar behaviour observed for case ‡. Finally, we have performed the same experiments as in Modeling 18 for the homogenized ideals and we have obtained the same conclusive results regarding Equation (10.14).

Table 10.7: Tested Hilbert series from Hybrid Modeling 19 systems over $\mathbb{F}_2$.

System	d_{reg}	$d_{\text{reg}}^{(z)}$	System	d_{reg}	$d_{\text{reg}}^{(z)}$	System	d_{reg}	$d_{\text{reg}}^{(z)}$
$(10,6,30,0,0)_{10}$	3	-	$(10,6,30,3,3)_{10}$	2	2	$(10,6,40,0,0)_{10}$	4	-
$(10,6,40,6,2)_{10}^{\dagger}$	3	-	$(14,7,50,0,0)_{10}$	4	-	$(14,7,50,2,2)_{10}$	3	4
$(14,7,50,10,2)_{10}$	$2^{\ddagger}$	3	$(15,6,70,10,3)_{10}^{\dagger}$	5	-	$(20,6,70,5,3)_{10}$	4	4
$(20,6,70,10,3)_{10}$	3	3	$(15,6,60,2,1)_{1}$	5	-	$(20,20,150,0,0)_{1}$	3	-
$(20,20,150,15,4)_{10}$	2	3	$(20,20,100,0,0)_{10}$	2	-			

10.5.2 Witness Degree for the Plain System

We have also tested the witness degree of Modeling 18. To this end, we had to create the affine Macaulay matrix in degree 2 or 3 by hands and then to compute its rank to check if the system has a unique solution. The witness degree in all our tests was the same as the value estimated by Equation (10.10) in Section 10.2.2. Details are given in Table 10.8, where the parameters are listed as (t, N, k).

Table 10.8: Witness degree for Modeling 18 systems over $\mathbb{F}_{101}$.

System	d_{wit}	System	d_{wit}	System	d_{wit}	System	d_{wit}
$(8,8,18)$	2	$(4,12,21)$	2	$(15,8,27)$	2	$(12,7,20)$	2
$(7,5,16)$	3	$(8,4,13)$	3	$(4,8,20)$	3	$(8,5,18)$	3

10.6 Asymptotic Analysis

The purpose of this final section is to illustrate the concrete results of Section 10.4 with more theoretical considerations.

For the sake of simplicity, we restrict ourselves to Modeling 19. Moreover, we will focus on the degree of regularity rather than on the witness degree. Recall that we had

introduced the latter to analyze the Wiedemann algorithm, which is likely to be the best tool for linear algebra on the parameters we have discussed so far. However, there exist other techniques that may perform asymptotically better than Wiedemann (see for example [Le 14]). This justifies to study Gröbner basis strategies based on dense linear algebra and which require an estimate of d_{reg}.

In Section 10.6.1, we explore a possibly weak range of parameters where the RSD problem is solved in degree 2. In Section 10.6.2, we go on to obtain an asymptotic equivalent of the degree of regularity when the parameters grow to infinity.

10.6.1 Solving at Low Degree

From the generic complexity formulae given in Section 2.4, we see that having a constant d_{reg} is a sufficient condition for the Gröbner basis algorithm to run in polynomial time. Moreover, we noted in Section 10.4.3 that our techniques proved especially efficient in a parameter range where the plain system is solved at a small degree.

Thus, we start by focusing on a zone where the degree of regularity of Modeling 19 should be equal to 2. This will be the case whenever the coefficient in front of z^2 in the generating series of Equation (10.7) is non-positive. This coefficient reads

$$\kappa_2 \stackrel{def}{=} \binom{n-k+1}{2} + (N-1)^2\binom{t}{2} - (n-k)t(N-1). \tag{10.16}$$

In the following, we view it as a function of the length n, the code rate $R = k/n$ and the error rate $\rho = t/n$ and we will study its behaviour when n goes to infinity. First, let us rewrite κ_2 as

$$\kappa_2 = n\frac{\rho^3 n - 2nR\rho^2 + R^2\rho n - 1 + 3\rho - R\rho - \rho^2}{2\rho}.$$

Note that if the code rate R dominates over ρ, the possibly greatest term in the numerator of the fraction is either $R^2\rho n$ or -1. If the quantity $R^2\rho n$ tends to zero, then the value of κ_2 will be asymptotically negative since the main contribution in the numerator comes from -1.

Our goal now is to find such a parameter range where the Prange algorithm does not seem to be polynomial. We consider the work factor of the standard adaptation to the regular case by guessing k/t error-free coordinates per block, see [HOSS18, B.3 p. 55]. The success probability is easily seen to be $\pi = \left(1 - \frac{k/t}{n/t}\right)^t = (1-R)^t$, which gives a complexity exponential in $-t\log(1-R)$. Assuming that $R = o(1)$ when n goes to infinity, the main term in the development of this exponent is proportional to $tR = n\rho R$. If for instance $n\rho R \sim n^\alpha$ with $\alpha \in]0,1[$, then Prange should be subexponential. On the contrary, we can clearly find parameters for which $R^2\rho n$ tends to zero under this condition.

To simplify the analysis even further, we consider particular functions $R = \phi(n)$ and $\rho = \psi(n)$ and we view κ_2 as a mere function of n. From discussions with Geoffroy Couteau and upon inspection of the PCG parameters, we found it relevant to study two types of regime:

- noise rate $\rho = n^{-a}$ and code rate $R = \log(n)n^{-a}$ for some $a \in]0, 1[$ (Proposition 10.3),
- for $a \in]0, 1[$ and $b \in]0, a[$, $\rho = n^{-a}$ and $R = n^{-b}$ (Proposition 10.4).

Proposition 10.3. *When $\rho = n^{-a}$ and $R = \log(n)n^{-a}$, $a \in]1/3, 1/2[$ and when the length n is large enough, our approach is expected to be polynomial while the Prange algorithm is subexponential.*

The lower bound on a and the asymptotic constraint on n correspond to a zone where Modeling 8 should be solved in degree 2.

Lemma 10.6. *Let $a \in]0, 1[$. Under Assumption 13 which gives the Hilbert series of Equation (10.7), the degree of regularity of plain Modeling 19 for an RSD instance with $\rho = n^{-a}$ and $R = \log(n)n^{-a}$ is equal to 2 when $a > 1/3$ and when the length n tends to infinity.*

Proof of Lemma 10.6. In this regime, Equation (10.16) giving the coefficient in front of z^2 in the Hilbert series reads

$$\kappa_2(n) = -\frac{n^{a+1}}{2} + \frac{(\log(n)-1)^2 n^{2-2a}}{2} + \frac{3n}{2} - \frac{(\log(n)+1)n^{1-a}}{2}.$$

We see that the term $-\frac{n^{1+a}}{2}$ dominates when $a + 1 > 2 - 2a$, hence $a > 1/3$. In this case, the value $\kappa_2(n)$ will be negative when n is large enough. □

To prove Proposition 10.3 it remains to study the cost of the Prange decoder, which gives the upper bound on a.

Proof of Proposition 10.3. We base ourselves on the exponent $nR\rho$ equal to $n^{1-2a}\log(n)$ in this setting. When $a < 1/2 \Leftrightarrow 1 - 2a > 0$, the complexity of Prange should then be subexponential. □

The study of the second regime is analogous.

Proposition 10.4. *Let $a \in]0, 1[$ and let $b \in \left]\frac{1-a}{2}, \min(a, 1-a)\right[$. When $\rho = n^{-a}$ and $R = n^{-b}$ and when the length n is large enough, our approach is expected to be polynomial while the Prange algorithm is subexponential.*

We follow the same proof strategy as for Proposition 10.3 by focusing on a zone where the degree of regularity of Modeling 19 is asymptotically equal to 2.

Lemma 10.7. *Let $a \in]0, 1[$ and let $b \in]0, a[$. Under Assumption 13 which gives the Hilbert series of Equation (10.7), the degree of regularity of plain Modeling 19 for an RSD instance with $\rho = n^{-a}$ and $R = n^{-b}$ is asymptotically equal to 2 when $a + 2b > 1$ and when the length n is large enough.*

Proof of Lemma 10.7. In this case, Equation (10.16) becomes

$$\kappa_2(n) = \frac{n^{2-2a}}{2} + \frac{n^{2-2b}}{2} - n^{2-a-b} - \frac{n^{1+a}}{2} + \frac{3n}{2} - \frac{n^{1-a}}{2} - \frac{n^{1-b}}{2}.$$

This time, the main term is either $\frac{n^{2-2b}}{2}$ or $-\frac{n^{1+a}}{2}$. The second value dominates when $1 + a > 2 - 2b$, that is, $a + 2b > 1$. □

Lemma 10.7 imposes $b > \frac{1-a}{2}$ while the restriction $b < a$ came from the study of concrete parameters. The extra condition $b < 1 - a$ in Proposition 10.4 is due to the complexity exponent of the Prange algorithm.

Proof of Proposition 10.4. This exponent now reads $nR\rho = n^{1-a-b}$, so that the algorithm should be subexponential when $1 - a - b > 0 \Leftrightarrow b < 1 - a$. □

10.6.2 Equivalent of d_{reg} at Infinity

A more accurate complexity estimate ultimately requires an asymptotic analysis of the degree of regularity. For semi-regular systems, [Bar04, II,§4] gives the full asymptotic expansion in different parameter regimes. Related computations can also be found in [ACFP14, A.1, Proposition 2] or [BFSS13, §3.2, Proposition 7], where they contented themselves with an asymptotic equivalent.

For plain Modeling 19, we also restrict ourselves to the first term of the development. In some particular cases, we have obtained

Proposition 10.5. *When n goes to infinity, the degree of regularity d_{reg} of plain Modeling 19 behaves asymptotically as follows:*

1. *For constant code rate R and noise rate $\rho = o(1)$, let $\delta_R \stackrel{def}{=} 2 - R - 2\sqrt{1-R} > 0$. We have*
$$d_{reg} \sim \delta_R t.$$
2. *For $R = o(1)$ and $\rho = o(1)$ such that $\rho = o(R)$, we have*
$$d_{reg} + 1 \sim \frac{R^2}{4} t.$$
3. *Finally, for $R = o(1)$ and $\rho = o(1)$ such that $\rho = \lambda R$ is linear in R with $\lambda < 1$, we have*
$$d_{reg} + 1 \sim \frac{(1-\lambda)^2 R^2}{4} t. \tag{10.17}$$

The main tool for the proof is the so-called saddle-point method. For a detailed account of this technique in the context of Hilbert series, we refer to [Bar04, II,§4]. Each coefficient can be obtained as a Cauchy integral, *i.e.*,

$$[z^d]\mathcal{H}_{A/I_{\mathbb{F}_2}}(z) = \frac{1}{2i\pi} \oint \frac{1}{z^{d+1}} g_{A/I_{\mathbb{F}_2}}(z) dz,$$

where $g_{A/I_{\mathbb{F}_2}}(z)$ stands for the generating series in Equation (10.7). The saddle-point method allows to study the asymptotic behaviour of this quantity for fixed d. Since we are interested in the value of d such that the integral vanishes when $n \to +\infty$, we will cancel the main term in the resulting development in order to obtain the first term in the asymptotic expansion of d_{reg}.

Proof. Using Equation (10.7), we readily obtain

$$\mathcal{I}_d(n) \stackrel{def}{=} \frac{1}{2i\pi} \int \frac{1}{z^{d+1}} \frac{(1+(N-1)z)^t}{(1+z)^{n-k}} dz.$$

It is then standard to write the integrand as $e^{nf(z)}$, where here

$$f(z) \stackrel{def}{=} -\frac{d+1}{n} \ln(z) - (1-R)\ln(1+z) + \rho \ln(1+(\rho^{-1}-1)z).$$

We study the behaviour of this integral when n grows. Using Cauchy's integral theorem, we can make the path of integration to meet the saddle points so that the integral concentrates in the neighborhood of these saddle points when n tends to infinity. These saddle points are solutions to the equation

$$zf'(z) = -\frac{d+1}{n} - (1-R)\frac{z}{1+z} + (1-\rho)\frac{z}{1+(\rho^{-1}-1)z} = 0. \tag{10.18}$$

By clearing denominators, Equation (10.18) may be rewritten as a quadratic equation $P(z) = p_2 z^2 + p_1 z + p_0 = 0$ such that

$$\begin{aligned} p_2 &\stackrel{def}{=} (\rho-1)\left(d+1+(1-R-\rho)n\right), \\ p_1 &\stackrel{def}{=} \rho R n - n\rho^2 - d - 1, \\ p_0 &\stackrel{def}{=} -\rho(d+1). \end{aligned}$$

Then, the classical argument is that the polynomial P should have a double root, *i.e.* the saddle points *coalesce* (otherwise the integral is exponential, see for example [Bar04, p. 94], [ACFP14, A.1.] for details). Writing that the discriminant $p_1^2 - 4p_0p_2$ is equal to zero yields a new quadratic equation $Ad^2 + Bd + C = 0$, where

$$\begin{aligned} A &\stackrel{def}{=} (2\rho-1)^2, \\ B &\stackrel{def}{=} -4R\rho^2 n - 4\rho^3 n + 2R\rho n + 10n\rho^2 - 4\rho n + 8\rho^2 - 8\rho + 2, \\ C &\stackrel{def}{=} R^2\rho^2 n^2 + \rho^4 n^2 - 2R\rho^3 n^2 - 4R\rho^2 n - 4\rho^3 n + 2R\rho n + 10n\rho^2 - 4n\rho + (2\rho-1)^2. \end{aligned}$$

Solving for d finally gives

$$\begin{aligned} d &= \frac{-R\rho n - \rho^2 n + 2n\rho - 2\rho + 1 \pm \sqrt{\delta}}{1-2\rho} \\ &= -1 + \frac{\rho n\left(\pm 2\sqrt{1-R}\sqrt{1-\rho} + 2 - \rho - R\right)}{1-2\rho}, \end{aligned} \tag{10.19}$$

where $\sqrt{\delta} \stackrel{def}{=} 2n\sqrt{R\rho^3 - R\rho^2 - \rho^3 + \rho^2} = 2n\rho\sqrt{1-R}\sqrt{1-\rho}$. We want the smallest positive root which is given by the minus case of $\pm\sqrt{\delta}$, in the equation above. The end of the proof then consists in studying Equation (10.19) in the different regimes:

- For constant code rate R and $\rho = o(1)$, we obtain

$$-2\sqrt{1-R}\sqrt{1-\rho} + 2 - \rho - R = (2-R) - 2\sqrt{1-R} + o(1),$$

  hence $d_{\text{reg}} \sim \delta_R t$, where $\delta_R \stackrel{def}{=} (2-R) - 2\sqrt{1-R} > 0$.

- For $R = o(1)$ and $\rho = o(1)$ we have

$$\begin{aligned} -2\sqrt{1-R}\sqrt{1-\rho} &= -2\left(1 - \tfrac{R}{2} - \tfrac{R^2}{8} + o(R^2)\right)\left(1 - \tfrac{\rho}{2} - \tfrac{\rho^2}{8} + o(\rho^2)\right) \\ &= -2 + R + \rho + \tfrac{R^2}{4} + \tfrac{\rho^2}{4} - \tfrac{R\rho}{2} + o(R\rho), \end{aligned}$$

  hence $-2\sqrt{1-R}\sqrt{1-\rho} + 2 - \rho - R = \frac{R^2}{4} + \frac{\rho^2}{4} - \frac{R\rho}{2} + o(R\rho)$. This gives us $d_{\text{reg}} + 1 \sim \frac{R^2}{4}t$ if $r = o(R)$ and $d_{\text{reg}} + 1 \sim \frac{R^2}{4}(1-\lambda)^2 t$ if $\rho = \lambda R$ is linear in R with $\lambda < 1$.

□

10.6.3 Open Problems

Of course, one natural extension of this work would be to obtain the full development of d_{reg}. Another continuation would be to study the specialized systems. In theory, their analysis is feasible as we still know the Hilbert series. However, it may be more technical since we also have to find the best asymptotic trade-off between the cost of fixing variables and the one of the solving step. Note that this last question is not trivial even in the standard situation represented by quadratic semi-regular systems, see [BFP10, §3.3], [Bet12, §4.2].

From this study, the hope would be to perform a broader comparison to known attacks, for instance ISDs, Statistical Decoding, and potential variants tailored to the regular distribution.

Chapter 11 CICO Problem on the Anemoi Permutation

In this chapter, we present results of a rather more experimental nature which allowed to compute the parameters of the Anemoi permutation [Bou+23]. This function can be used to build efficient ZK-friendly hash and compression functions. It was designed to be well suited for several types of proof systems and it turns out to be more competitive than the state-of-the-art in many of them.

We studied this primitive by considering two polynomial systems. The first one is generic to the structure in rounds while the second one was inspired by the cryptanalysis of Griffin [Gra+23]. The parameters were derived from a conjecture on the solving degree of this first modeling. We also added experimental and theorerical data to compare both systems.

Contents

11.1 Preliminaries

11.1.1 Anemoi Permutation

In [Bou+23], we introduced the Anemoi permutation and a new mode of operation, Jive, in which it can be used. Instead of relying on a function of low degree or whose

inverse is of low degree as in Rescue [Aly+20], we considered a permutation which is *CCZ-equivalent* to an easily computable one. For a function $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$, let us denote by Γ_F the *graph*

$$\Gamma_F \stackrel{def}{=} \left\{(\boldsymbol{x}, F(\boldsymbol{x})) : \boldsymbol{x} \in \mathbb{F}_q^m\right\} \subset (\mathbb{F}_q^m)^2. \tag{11.1}$$

Definition 11.1 (CCZ-Equivalence [CCZ98]). Let F and G be two functions of $\mathbb{F}_q^m$. We say that they are CCZ-equivalent if there exists an affine permutation $\mathcal{L} : (\mathbb{F}_q^m)^2 \to (\mathbb{F}_q^m)^2$ such that $\Gamma_F = \mathcal{L}(\Gamma_G)$.

This definition encompasses Rescue's idea since a permutation and its inverse are known to be in the same CCZ-equivalence class [BCP06]. By considering $x \mapsto x^d$ for a small d and its inverse, we thus notice that it does not preserve the degree. Concretely, the hope will be to benefit from the same discrepancy between evaluation and verification times but for more general CCZ-equivalent functions. Another nice property for the analysis is that it will be enough to check the resistance against linear and differential attacks for only one representative in an equivalence class, for instance the low degree function we start with.

11.1.1.1 Description of the Sbox

Our proposal uses an SPN structure and we will first present the Sbox. We called it the *Flystel* because it combines ideas from Feistel networks and from the butterfly construction introduced in [PUB16].

More precisely, let $Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and let $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ be two quadratic functions and let $E : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation. We will consider the following pair of functions relying on Q_γ, Q_δ and E. The *open* `Flystel` is the permutation of $\mathbb{F}_q^2$ obtained using a 3-round Feistel network with Q_γ, E^{-1}, and Q_δ, as depicted in Figure 11.1. It is denoted $\mathcal{H}$, so that $\mathcal{H}(x, y) = (u, v)$ is evaluated as follows:

$$\begin{array}{l|l} 1.\ x \leftarrow x - Q_\gamma(y), & 3.\ x \leftarrow x + Q_\delta(y), \\ 2.\ y \leftarrow y - E^{-1}(x), & 4.\ u \leftarrow x,\ v \leftarrow y\ . \end{array}$$

The second function is $\mathcal{V} : (y, v) \mapsto (R_\gamma(y, v), R_\delta(y, v))$, where $R_\gamma : (y, v) \mapsto E(y - v) + Q_\gamma(y)$ and where $R_\delta : (y, v) \mapsto E(y - v) + Q_\delta(v)$, see Figure 11.2. We call it the *closed* `Flystel` over $\mathbb{F}_q^2$.

The crux of our construction lies in

Proposition 11.1. *For a given tuple (Q_γ, E, Q_δ), the corresponding closed and open* Flystel *are CCZ-equivalent.*

Proof. Let $(u, v) = \mathcal{H}(x, y)$. We observe that $v = y - E^{-1}(x - Q_\gamma(y))$, so that $x = E(y - v) + Q_\gamma(y)$. Similarly, we have that $u = Q_\delta(v) + E(y - v)$. Consider now the set $\Gamma_\mathcal{H} = \left\{((x, y), \mathcal{H}(x, y)) : (x, y) \in \mathbb{F}_q^2\right\}$. By definition, we have

$$\Gamma_\mathcal{H} = \left\{((x, y), (u, v)) : (x, y) \in \mathbb{F}_q^2\right\} = \mathcal{L}\left(\left\{((y, v), (x, u)) : (x, y) \in \mathbb{F}_q^2\right\}\right),$$

Figure 11.1: Open `Flystel`, $\mathcal{H}$.

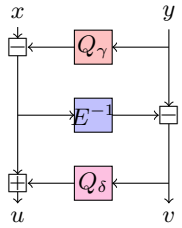
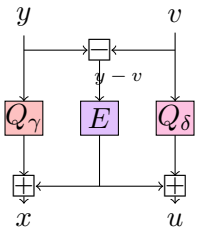


Figure 11.2: Closed `Flystel`, $\mathcal{V}$.



where $\mathcal{L}$ the permutation of $(\mathbb{F}_q^2)^2$ that satisfies $\mathcal{L}^{-1}((x,y),(u,v)) = ((y,v),(x,u))$. This map is indeed linear. Using the equalities of above we can then write

$$\begin{aligned}\mathcal{L}^{-1}(\Gamma_{\mathcal{H}}) &= \left\{((y,v),(x,u)) : (x,y) \in \mathbb{F}_q^2\right\} \\ &= \left\{((y,v),(E(y-v)+Q_\gamma(y), Q_\delta(v)+E(y-v))) : (y,v) \in \mathbb{F}_q^2\right\} = \Gamma_{\mathcal{V}}.\end{aligned}$$

We deduce that $\Gamma_{\mathcal{H}} = \mathcal{L}(\Gamma_{\mathcal{V}})$, so the two functions are CCZ-equivalent. □

Corollary 11.1. *Verifying that $(u,v) = \mathcal{H}(x,y)$ is equivalent to verifying that $(x,u) = \mathcal{V}(y,v)$.*

Concretely, we will encode the verification of a high degree open `Flystel` using the polynomial representation of the low degree closed `Flystel` that is CCZ-equivalent to it. Before coming to the presentation of the complete round function, we detail our instantiations of Q_γ, Q_δ and E in even and odd characteristics. The map E is always an exponentiation which is a permutation of $\mathbb{F}_q$ while the polynomials Q_γ and Q_δ have been selected to avoid classical attacks.

Even characteristic. When $q = 2^n$ for odd n, we take an exponent $\alpha = 2^i + 1$ such that i is coprime to n, $\alpha = 2^1 + 1 = 3$ in practice, and we adopt $E : x \mapsto x^3$. This is indeed a permutation that can be seen as quadratic with respect to the *algebraic degree*. Considerations related to linear and differential cryptanalysis led us to choose $Q_\gamma : x \mapsto gx^3 + g^{-1}$ and $Q_\delta : x \mapsto gx^3$, where g is a generator of the multiplicative subgroup $\mathbb{F}_q^*$.

Odd characteristic. When q is an odd prime, we pick an integer α coprime to $q-1$ and g an arbitrary generator of $\mathbb{F}_q^*$. We still consider $E : x \mapsto x^\alpha$ but this time the choice of α depends on the cost of the algebraic techniques. In the same flavour as in characteristic 2, we take $Q_\gamma : x \mapsto gx^2 + g^{-1}$ and $Q_\delta : x \mapsto gx^2$.

11.1.1.2 Full Round Function

In the general case, the input state is of size 2ℓ, $\ell \in \mathbb{Z}_{>0}$ and the Sbox is applied locally. For the moment, we limit ourselves to describing the situation when $\ell = 1$ because this is the only one for which we have been able to perform Gröbner basis experiments for sufficiently many rounds. For $i \in \{0..n_r - 1\}$ with $n_r \in \mathbb{N}$ the number of rounds, we consider the transformation

$$R_i = \mathcal{H} \circ \mathcal{M} \circ \text{AddConstants}_i, \tag{11.2}$$

where AddConstants_i corresponds to the addition of constants $(c_i, d_i) \in \mathbb{F}_q^2$, where $\mathcal{M}$ is the linear layer given by a 2 by 2 matrix over $\mathbb{F}_q$ and where $\mathcal{H}$ is the open `Flystel`. The Anemoi permutation finally reads

$$P = R_{n_r-1} \circ \cdots \circ R_0.$$

11.1.2 CICO Problem

The present chapter will discuss the security of Anemoi with respect to algebraic techniques. More precisely, we studied the hardness of the following problem stated in the case $\ell = 1$.

Problem 11.1 (Constrained Input/Constrained Output (CICO) Problem). *Let $P : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ be a permutation. The CICO problem consists in finding a pair $(y_{in}, y_{out}) \in \mathbb{F}_q^2$ such that $P(0, y_{in}) = (0, y_{out})$.*

It was introduced by the Keccak team in [Tea11, §8.2.4] due to its relevance for the security of sponge constructions. It is generally acknowledged that its difficulty gives enough confidence in the permutation. To encourage the analysis of ZK hash functions, the Ethereum Fundation proposed CICO challenges[1] for the permutations underlying several of these primitives. The goal there was to obtain *practical* attacks on round-reduced versions. Even though no preferred technique was mentioned, it turns out that the weakest instances were broken using algebraic methods [BBLP22]. More broadly, the study of such algorithms now appears as an essential ingredient to derive the number of rounds in an AO proposal.

[1] https://www.zkhashbounties.info/.

11.1.3 Standard Approaches

Several different techniques have already been proposed for the CICO problem. All of them rely on a modeling of the constraints together with a polynomial description of the primitive. In that respect, there is nothing new compared to the early attempts to attack block ciphers.

Univariate solving. The point is to set an unknown $x \in \mathbb{F}_q$ such that the initial state is $(0, x)$ and to evaluate the permutation on this input. Solving Problem 11.1 is then reduced to finding a root in $\mathbb{F}_q$ of a univariate polynomial $Q \in \mathbb{F}_q[x]$. In [BBLP22], this approach was shown to be successful on Feistel-MiMC and on Poseidon because the degree grows slowly. Indeed, these proposals use a round function derived from $x \mapsto x^d$ and the degree of Q is expected to be d^{n_r}. The authors of [BBLP22] are in fact able to side-step a few rounds (1 for Feistel-MiMC and 2 for Poseidon) by using *ad hoc* tricks, which was important for practical challenges.

The univariate strategy is however not feasible when the polynomial Q has a large degree (typically, greater than q). This was observed in the case in Rescue (since the scheme also uses the high degree map $x \mapsto x^{1/d}$) and more recently in Griffin [Gra+23]. We have not considered this method in our security analysis because the open `Flystel` is also of high degree.

Intermediate variables. In contrast to the former technique, the idea is to introduce equations and unknowns at each round to keep the degree low. It yields a multivariate system with a number of equations and variables which is roughly a multiple of n_r and where the degree of the polynomials only depends on the round function. This is essentially the historical approach of [CP02], applied to ZK-relevant ciphers in [BGL20; BBLP22; Gra+23; Bou+23], among many others.

Trade-off. Finally, the attacker can choose an in-between strategy based on a modeling with higher degree equations but fewer variables. This can be achieved by introducing new unknowns only at specific rounds. A more astute method relying on the properties of the cipher was proposed in [Gra+23, *Partial intermediate variables*, p. 24] and can also be applied to Anemoi.

11.2 Considered Modelings

11.2.1 Naive Equations

Our first algebraic system corresponds to the second strategy described above by introducing 2 equations and 2 variables at each round of the cipher. We denote the input state by (x_0, y_0) and by (x_{i+1}, y_{i+1}) the output of round R_i for $i \in \{0..n_r - 1\}$.

Fact 5. *For any $i \in \{0..n_r - 1\}$, there exist two polynomials f_i and g_i such that*

$$(x_{i+1}, y_{i+1}) = R_i(x_i, y_i) \Leftrightarrow \begin{cases} f_i(x_i, y_i, x_{i+1}, y_{i+1}) = 0 \\ g_i(x_i, y_i, x_{i+1}, y_{i+1}) = 0. \end{cases}$$

Proof. These equations are obtained as follows. We start from the following equality which holds for any $i \in \{0..n_r - 1\}$:

$$(x_{i+1}, y_{i+1}) = R_i(x_i, y_i) = \mathcal{H}(\mathcal{M}(x_i + c_i, y_i + d_i)[1], \mathcal{M}(x_i + c_i, y_i + d_i)[2]).$$

By Corollary 11.1, this is equivalent to

$$(\mathcal{M}(x_i + c_i, y_i + d_i)[1], x_{i+1}) = \mathcal{V}(\mathcal{M}(x_i + c_i, y_i + d_i)[2], y_{i+1}),$$

where $\mathcal{V}$ is the closed `Flystel`. Using the definition of this map yields

$$\begin{gathered}(\mathcal{M}(x_i + c_i, y_i + d_i)[2] - y_{i+1})^\alpha + Q_\gamma(\mathcal{M}(x_i + c_i, y_i + d_i)[2]) = \mathcal{M}(x_i + c_i, y_i + d_i)[1], \\ (\mathcal{M}(x_i + c_i, y_i + d_i)[2] - y_{i+1})^\alpha + Q_\delta(y_{i+1}) = x_{i+1}.\end{gathered}$$

We can thus set

$$\begin{aligned} f_i &= (\mathcal{M}(x_i + c_i, y_i + d_i)[2] - y_{i+1})^\alpha + Q_\gamma(\mathcal{M}(x_i + c_i, y_i + d_i)[2]) - \mathcal{M}(x_i + c_i, y_i + d_i)[1], \\ g_i &= (\mathcal{M}(x_i + c_i, y_i + d_i)[2] - y_{i+1})^\alpha + Q_\delta(y_{i+1}) - x_{i+1}. \end{aligned}$$

□

Modeling 20. *For $i \in \{0..n_r - 1\}$, let $f_i,\ g_i \in \mathbb{F}_q[x_0, \ldots, x_{n_r}, y_0, \ldots, y_{n_r}]$ be the two polynomials defined in Fact 5. Our first system to solve the CICO problem is*

$$\mathcal{F}_{naive} \stackrel{def}{=} \{f_0, g_0, \ldots, f_{n_r-1}, g_{n_r-1}\} \cup \{x_0, x_{n_r}\}.$$

This modeling can be seen as containing $2n_r$ equations and $2n_r$ variables if we get rid of the unknowns x_0 and x_{n_r}. We will assume that this system is zero-dimensional even if we do not add the field equations (they have very high degree). This behaviour was always observed in our experiments.

In characteristic 2, both f_i and g_i are of degree 3. In odd characteristic, they are of degree $\alpha \geqslant 3$ but their difference is a polynomial of degree 2. We will keep this feature in mind when analyzing the system. Another more general remark is that the shape of these polynomials highly depends on the instantations of $E,\ Q_\gamma,\ Q_\delta$, and $\mathcal{M}$.

11.2.2 Griffin-like Equations

In odd characteristic, we were invited by a reviewer to study another system derived in the same way as in [Gra+23, *Partial intermediate variables*, p. 24]. The inputs (x_0, y_0) are still seen as variables but then the idea is to introduce only one equation p_i and one variable v_i in the following rounds.

We still denote by (x_i, y_i) the output of round $i-1$ and we consider (x'_i, y'_i) the partial output defined by

$$(x'_i, y'_i) \stackrel{def}{=} (\mathcal{M}(x_i, y_i)[1] + c_i, \mathcal{M}(x_i, y_i)[2] + d_i).$$

It is clear that (x'_i, y'_i) are affine of degree 1 in (x_i, y_i) and that $\mathcal{H}(x'_i, y'_i) = (x_{i+1}, y_{i+1})$. We then set a new variable

$$v_i \stackrel{def}{=} y'_i - y_{i+1} \tag{11.3}$$

and we introduce the equation

$$p_i \stackrel{def}{=} v_i^\alpha - (x'_i - (\beta y_i'^2 + \gamma)) = 0. \tag{11.4}$$

Note that we also have $x_{i+1} = x'_i - \beta\gamma y_i'^2 + \beta y_{i+1}^2 + \delta$.

Lemma 11.1. *For any $i \in \{0..n_r - 1\}$, the polynomial p_i belongs to $\mathbb{F}_q[x_0, y_0, v_0, \ldots, v_i]$.*

Proof. Note first that for any $i \in \{0..n_r\}$, both x_i and y_i can be expressed as polynomials in x_0 and y_0. Recall also that (x'_i, y'_i) can be written in terms of x_i and y_i, so that $p_i \in \mathbb{F}_q[x_0, y_0, v_i]$. In practice, we can avoid high degree monomials in x_0, y_0 by also including variables v_j for $j \in \{0..i-1\}$. □

Modeling 21. *We consider the system $\{p_0, \ldots, p_{n_r-1}\}$ in the polynomial ring $\mathbb{F}_q[x_0, y_0, v_0, \ldots, v_{n_r-1}]$, where v_i is defined by Equation (11.3) and where p_i is defined by Equation (11.4). This set contains n_r equations in $n_r + 2$ variables. Our second modeling to solve the CICO problem, denoted $\mathcal{F}_{Griffin}$, is obtained from it by fixing $x_0 = 0$ and by adding the equation in $x_0, y_0, v_0, \ldots, v_{n_r-1}$ which corresponds to $x_{n_r} = 0$.*

A first apparent advantage of $\mathcal{F}_{\text{Griffin}}$ is that it contains half as many equations and variables as the system $\mathcal{F}_{\text{naive}}$. Even though we cannot avoid a degree growth in the p_i's through the rounds, the observation of the reviewer was that it only seems to be linear from round i such that v_i^α is not the term of maximal degree in p_i. This was in fact the initial motivation for studying $\mathcal{F}_{\text{Griffin}}$. Indeed, in the absence of specific structure, such a modeling usually contains polynomials whose degree increases exponentially with the number of rounds.

11.3 Results in Characteristic 2

We first derive our estimate for the cost of solving $\mathcal{F}_{\text{naive}}$ in even characteristic. Even though the initial system is not a DRL Gröbner basis, its computation appeared to be extremely cheap (this stems from Fact 6 below). For this reason, we derived the number of rounds only based on the FGLM algorithm.

Estimate 3. *We estimate the total cost of solving $\mathcal{F}_{naive}$ in even characteristic by the one of the change-of-order step. Using Equation (2.2), the latter has complexity*

$$\mathcal{O}(n_r 9^{\omega n_r}),$$

where $2 \leqslant \omega \leqslant 3$ is the linear algebra exponent.

This cost corresponds to the one of the dense variant[2] of FGLM [FGLM93] on a system of $2n_r$ cubic equations for which the Bézout bound of Proposition 2.2 is tight. This is what we observed in all our experiments.

We neglected the step to generate the DRL Gröbner basis due to the following result. Its proof can be seen as the result of computation since there are simply two polynomials per round.

Fact 6. *We consider the polynomial ring $\mathbb{F}_q[x_0, y_0, \ldots, x_{n_r}, y_{n_r}]$ endowed with the DRL ordering. For $i \in \{0..n_r - 1\}$, let f_i, g_i denote the two cubic equations at round i (which involve x_i, y_i, x_{i+1} and y_{i+1}). Then, the set of leading monomials in the reduced Gröbner basis of $\{f_i, g_i\}$ is*

$$\left\{y_{i+1}^5, x_i y_{i+1}^3, x_i^3, x_i y_{i+1}\right\}. \tag{11.5}$$

Moreover, the set of leading monomials in the reduced Gröbner basis of $\{x_0, f_0, g_0\}$ is

$$\left\{x_0, y_0^2 y_1, y_0^3, y_0 y_1^3, y_1^5\right\}. \tag{11.6}$$

All these individual Gröbner bases are obtained in degree 5.

We observe that the leading monomials in two distinct sets defined by Equation (11.5) for rounds $i \neq j \in \{1..n_r - 1\}$ are always coprime to each other. They are also coprime to those in Equation (11.6) and to x_{n_r} which corresponds to the second CICO constraint. We can thus use Proposition 3.1 to show that only computation to obtain the final Gröbner basis is to generate the partial bases considered in Fact 6. The corresponding complexity is essentially independent from the number of rounds.

11.4 Results in Odd Characteristic

The system $\mathcal{F}_{\text{naive}}$ behaves differently in odd characteristic since the main step seems to correspond to the Gröbner basis computation. We derived the number of rounds based on Conjecture 11.1, which gives a lower bound on the experimental solving degree $d_{\text{exp}}(n_r, \alpha)$ for n_r rounds when the exponent α is used.

Conjecture 11.1. *The experimental solving degree $d_{exp}(n_r, \alpha)$ of $\mathcal{F}_{naive}$ is such that*

$$d_{exp}(n_r, \alpha) \geqslant 2n_r + \kappa_\alpha, \tag{11.7}$$

where κ_α is a constant depending only on α. We found $\kappa_3 = 1$, $\kappa_5 = 2$, $\kappa_7 = 4, \kappa_9 = 7$ and $\kappa_\alpha = 9$ for[3] $\alpha \geqslant 11$.

[2] There exist improved algorithms by exploiting the sparsity of the multiplication matrices [FGHR14; FM17] or by viewing them as polynomial matrices [BNS22]. The latter requires assumptions on the input system and it is not clear that we can apply it to our case.

[3] We would expect the value of κ_α to keep increasing with α but the calculations needed to estimate it become too costly as α grows and thus we preferred to be conservative.

Estimate 4. *In odd characteristic, we adopt the lower bound*

$$\mathcal{O}\left(\binom{2n_r + \kappa_\alpha + 2n_r}{2n_r}^\omega\right), \tag{11.8}$$

where $2 \leqslant \omega \leqslant 3$ *is the linear algebra constant and where* κ_α *was derived from our experiments.*

Relying on Estimate 4 to choose the parameters α and n_r can be seen as a bit cavalier but it is common for AO primitives to use such lower bounds. We do not consider the cost of FGLM because it appears to be negligible[4] compared to the complexity in Equation (11.8). At the time of the submission, we conjectured a degree equal to $\deg(\langle \mathcal{F}_{\text{naive}} \rangle) = \deg(\langle \mathcal{F}_{\text{Griffin}} \rangle) = (\alpha+2)^{n_r}$. This result suggests that the Bézout bound[5] $\leqslant 2^{n_r}\alpha^{n_r}$ for $\mathcal{F}_{\text{naive}}$ is far from being sharp. Similarly to Jarvis in [BGL20, Appendix A], we realized while writing this manuscript that it corresponds to a case of equality for the *multi-homogeneous* Bézout bound:

Proposition 11.2 (Multi-homogeneous Bézout bound). *Let* $(f_1, \ldots, f_n) \subset \mathbb{K}[\boldsymbol{x}]$ *be a polynomial sequence in* n *variables and let* $X_1, \ldots, X_k$ *be a partition of the variable set* $\boldsymbol{x}$ *such that* $\#X_j = s_j$ *for* $j \in \{1..k\}$*. For* $i \in \{1..n\}$ *and* $j \in \{1..k\}$*, let* $d_{i,j}$ *be the degree of* f_i *in the variable set* X_j*. Then the number of solutions is bounded from above by the coefficient of the monomial* $z_1^{s_1} \ldots z_k^{s_k}$ *in*

$$\prod_{i=1}^{n} (d_{i,1}z_1 + \cdots + d_{i,n}z_k). \tag{11.9}$$

Remark 11.1. We recover Proposition 2.2 when $k = 1$ and $d_{i,1} = d_i$ for $i \in \{1..n\}$.

Lemma 11.2. *We have*

$$\deg(\langle \mathcal{F}_{naive} \rangle) \leqslant (\alpha + 2)^{n_r}.$$

Proof. Recall that the set of variables is $\{x_0, \ldots, x_{n_r}\} \cup \{y_0, \ldots, y_{n_r}\}$ and that the equations for round R_i, $i \in \{0..n_r - 1\}$ were given by

$$\begin{aligned} f_i &= (\mathcal{M}(x_i + c_i, y_i + d_i)[2] - y_{i+1})^\alpha + Q_\gamma(\mathcal{M}(x_i + c_i, y_i + d_i)[2]) \\ &\quad - \mathcal{M}(x_i + c_i, y_i + d_i)[1], \\ g_i &= (\mathcal{M}(x_i + c_i, y_i + d_i)[2] - y_{i+1})^\alpha + Q_\delta(y_{i+1}) - x_{i+1}. \end{aligned}$$

As observed above, their difference is quadratic corresponding to the polynomial

$$h_i \stackrel{def}{=} f_i - g_i = Q_\gamma(\mathcal{M}(x_i + c_i, y_i + d_i)[2]) - \mathcal{M}(x_i + c_i, y_i + d_i)[1] - Q_\delta(y_{i+1}) + x_{i+1}.$$

We now want to apply Proposition **??** to the pair $\{g_i, h_i\}$ using the *naive* partition of variables where the subsets X_j are singletons. This boils down to looking at the partial

[4] It is still worth studying as further progress on the first step might render it limiting.

[5] obtained from the generating set with n_r polynomials of degree 2 and n_r polynomials of degree α.

degree in each variable. The point is that the degree patterns are not generic. In the polynomial h_i, the partial degree is 2 for x_i, y_i and y_{i+1} but only 1 for x_{i+1}. Similarly in g_i we easily obtain α for x_i, y_i and y_{i+1} but only 1 for x_{i+1}. The polynomial P_{n_r-1} associated to the system $\{g_0, h_0, \ldots, g_{n_r-1}, h_{n_r-1}\}$ by Equation (**??**) is thus equal to

$$\begin{aligned} P_{n_r-1} &\stackrel{def}{=} (2y_{n_r} + x_{n_r} + 2y_{n_r-1} + 2x_{n_r-1})(\alpha y_{n_r} + x_{n_r} + \alpha y_{n_r-1} + \alpha x_{n_r-1})P_{n_r-2} \\ &\stackrel{def}{=} Q_{n_r-1}P_{n_r-2}, \end{aligned}$$

where P_{n_r-2} corresponds to the earliest rounds. It is easy to see that the coefficient of $\prod_{j=0}^{n_r} x_j y_j$ in P_{n_r-1} is equal to the one of $x_{n_r}y_{n_r}$ in Q_{n_r-1}, e.g., $\alpha + 2$, times the one of $\prod_{j=0}^{n_r-1} x_j y_j$ in P_{n_r-2}. We thus obtain $(\alpha+2)^{n_r}$ by induction. The conclusion regarding the degree follows from Proposition 2.2. □

Using Lemma **??** together with an agressive exponent of $\omega = 2$ in FGLM, a very rough upper-bound for the cost of the change-of-order step is $\mathcal{O}(n_r^2(\alpha+2)^{n_r})$. This complexity is quite below the value given in Estimate 4.

Experiments. Table 11.1 provides an experimental comparison to $\mathcal{F}_{\text{Griffin}}$ for the Gröbner basis step.

Table 11.1: DRL Gröbner basis for $\mathcal{F}_{\text{naive}}$ and $\mathcal{F}_{\text{Griffin}}$ (odd characteristic).

α	n_r	$d_{\text{exp}}(n_r, \alpha)$ $\mathcal{F}_{\text{naive}}$	Total Time $\mathcal{F}_{\text{naive}}$ (s)	α	n_r	Degrees	$d_{\text{exp}}(n_r, \alpha)$ $\mathcal{F}_{\text{Griffin}}$	Total Time $\mathcal{F}_{\text{Griffin}}$ (s)
3	3	7	**0.010**	3	3	3,4,6	7	**0.010**
	4	9	**0.040**		4	3,4,6,8	10	**0.040**
	5	11	**0.550**		5	3,4,6,8,10	11	**0.329**
	6	13	**11.429**		6	3,4,6,8,10,12	12	**6.639**
	7	15	**216.620**		7	3,4,6,8,10,12,14	15	**163.870**
	8	17	**14450.530**		8	3,4,6,8,10,12,14,16	16	**10575.610**
5	3	8	**0.040**	5	3	5,5,6	11	**0.049**
	4	10	**2.599**		4	5,5,6,8	15	**0.879**
	5	12	**226.330**		5	5,5,6,8,10	19	**19.129**
					6	5,5,6,8,10,12	23	**875.379**
7	3	10	**0.240**	7	3	7,7,7	12	**0.190**
	4	12	**55.420**		4	7,7,7,8	17	**16.870**
	5	14	**23042.180**		5	7,7,7,8,10	22	**3903.280**

In spite of a clear advantage in terms of timings especially for a small number of rounds when $\alpha = 3$ and for large values of α, we have not considered this system to derive Estimate 4 due to the high solving degree[6]. Note in particular that the general expression for the Gröbner basis complexity (*e.g.*, Equation (2.7)) indicates that this phenomenon should asymptotically prevail over a smaller number of variables (the initial purpose of $\mathcal{F}_{\text{Griffin}}$). Another reason is that this second modeling seemed more difficult to analyze. The shape of the equations is quite specific due to the way the system is generated and we have not grasped a clear pattern from the mere Table 11.1.

[6]Concretely, we have added 2 extra rounds on top of Estimate 4 to ensure that $\mathcal{F}_{\text{Griffin}}$ exploited in a more ingenious way will not jeopardize security.

Independently from these experiments, a very rough reasoning based on the Macaulay bound would suggest the same behaviour for the solving degrees of $\mathcal{F}_{\text{naive}}$ versus $\mathcal{F}_{\text{Griffin}}$. This is because the degree of the equations increases with the number of rounds in $\mathcal{F}_{\text{Griffin}}$ while it remains constant in $\mathcal{F}_{\text{naive}}$. The experimental degrees of the p_i's are provided in Column "Degrees" where they are listed as $\deg(p_0), \ldots, \deg(p_{n_r-1})$ for fixed (α, n_r). As initially claimed by the reviewer, our results suggest a linear increase.

From Table 11.1 and the following Table 11.2, we finally deduce the lower bound of Conjecture 11.1. Even for high values of α, theoretical considerations led us to think that the increase of the solving degree will be only by two after a few rounds. This explains the multiplicative constant of 2 in the lower bound of Equation (11.7).

Table 11.2: Solving degree of $\mathcal{F}_{\text{naive}}$ for higher values of α.

α	$d_{\text{exp}}(n_r, \alpha)$ $\mathcal{F}_{\text{naive}}$ when $n_r \in \{2, 3, 4\}$
9	10, 13, 15
11	12, 15, 18

11.5 Further Comments

11.5.1 General Case $\ell > 1$

We write the wider state as a vector $(\boldsymbol{X}, \boldsymbol{Y}) \in \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell$. In this setting, the Sbox consists in applying the open `Flystel` in parallel, *i.e.*,

$$\mathcal{S}(\boldsymbol{X}, \boldsymbol{Y}) \stackrel{def}{=} (\mathcal{H}(X_1, Y_1), \ldots, \mathcal{H}(X_\ell, Y_\ell)),$$

and the linear layer is of a different nature. The value of ℓ is typically $\ell \in \{1..8\}$, see [Bou+23, Table 1].

At round $i \in \{0..n_r - 1\}$, the straightforward generalization of $\mathcal{F}_{\text{naive}}$ contains 2ℓ polynomials $(f_{i,1}, \ldots, f_{i,\ell}, g_{i,1}, \ldots, g_{i,\ell})$ in 4ℓ variables $x_{u,v}$, $y_{u,v}$ for $u \in \{i, i+1\}$ and $v \in \{1..\ell\}$. The degree of the relevant equations is the same as before, *e.g.*, $(\alpha, \ldots, \alpha, 2, \ldots, 2)$ in odd characteristic. Since this modeling is about ℓ times bigger than the former one for the same number of rounds, we have not been able to perform a large range of experiments. For instance, we have tested at most 3 rounds when $\ell = 2$, which is probably not enough to make conjectures.

Even Characteristic. When $\ell = 1$, Fact 6 showed that the cost of the Gröbner basis computation on $\mathcal{F}_{\text{naive}}$ was mostly independent from n_r. However, the same does not necessarily hold when $\ell > 1$. In this situation, the individual Gröbner bases might be obtained at a degree larger than 5. More crucially, there may exist an overlap between the sets of leading terms in these bases so that the final one is not a simple gluing. The complexity would then clearly increase with the number of rounds.

Our experiments for $\ell = 2$ and $n_r \in \{1..3\}$ suggest the latter behaviour but we have not been able to draw a more precise conclusion. For this reason and since this choice is conservative, we have only considered FGLM in Estimate 3 even when $\ell > 1$ to set the concrete number of rounds.

Odd Characteristic. We have generalized Conjecture 11.1 and Estimate 4 to $\ell > 1$ by replacing $2n_r$ by $2\ell n_r$ everywhere, which is natural when considering the expression of the Macaulay bound. We would proceed in the same way if the change-of-order step were to be dominant because the Bézout bound is exponential in ℓ. Note that the cost of the algebraic attack of [BGL20, Appendix B][7] on Rescue also exhibits this extra ℓ factor in the exponent.

11.5.2 Precisions on the Experiments

Our tests were performed using the Sage code available at [Vel22] on top of which we have written additional Magma commands.

We have tried the DRL orders implicitly attached to the polynomial rings $\mathbb{F}_q[x_0, y_0, \ldots, x_{n_r}, y_{n_r}]$ and $\mathbb{F}_q[x_0, \ldots, x_{n_r}, y_0, \ldots, y_{n_r}]$ which seem to better capture the shape of the systems. We have also focused on one speficic round and plugged the associated leading terms, which was the starting point for Fact 6. More generally, we have tested the incremental strategy by computing a Gröbner basis for i rounds and by adding the polynomials of round $i+1$ only when this first calculation was complete. This can in fact be seen as a specific selection strategy in the naive Gröbner basis algorithm. We realized while writing this manuscript that this method had been formalized in [Alb08, §4.4.2] under the name of *Gröbner surfing*. Even though it may offer a practical improvement compared to the standard approach, it is difficult to translate this into a better theoretical complexity. This is especially true since there is no known result stating that a monomial order will be more efficient than another regardless of the system.

As already observed in previous works, the Magma implementation of FGLM can be the bottleneck even when this step seems to be cheaper than the one to obtain the first Gröbner basis. In most cases, the computation has not been completed but we could still obtain the dimension of the quotient ideal using Magma's verbosity.

[7] In this work, the main step is the FGLM algorithm.

Open Problems

We close our discussion with some research directions that appear natural from our contributions. Before detailing these perspectives for the three main parts of this thesis, note that the additional call for signature schemes recently launched by NIST[8] will be for sure a fruitful source of cryptanalysis projects involving algebraic techniques.

Multivariate cryptography. In Chapters 4 and 5, we gave attacks on two schemes which use an extension field. Apart from our work, the more high-profile breaks of GeMSS and Rainbow have shown that this type of construction or more generally a too large amount of added structure can clearly be detrimental to the security of multivariate cryptosystems. As a result, the community now favours more simple proposals built upon Unbalanced Oil and Vinegar (UOV) [KPG99] that are less structured than Rainbow. The hope is to rely on an old scheme which seems rather resistant to cryptanalysis.

Known techniques on UOV can be understood as a mix of ideas coming from combinatorial methods and from MQ algorithms. The application of rank attacks to UOV-type schemes has been proposed very recently [Beu+23, §4.5][FI23]. It is natural to expect improvements at this stage and it would be interesting to see if they can become the limiting attack. The answer may depend on the UOV variant [KPG99; FIKT21; Beu21b; FMPP22].

Rank-metric and MinRank-based schemes. Chapters 6 to 9 focused on the cryptanalysis of the MinRank problem and of assumptions underlying rank-based cryptography.

For MinRank, we introduced a hybrid technique that is compatible with known approaches on this problem. However, we have not addressed the issue of obtaining an asymptotic hierarchy between these different methods even in the random setting. This is important from a theoretical perspective and also to derive parameters for emerging proposals based on this assumption [Ara+23; Adj+23].

The same question naturally arises for rank-metric schemes. Independently, we can imagine more immediate progress on the algorithmic side. For instance, Chapter 7 did not analyze the former combined modeling of [Bar+20b] where all equations are over $\mathbb{F}_q$. Similarly, Chapter 8 on NHRD only studied the MaxMinors system. Finally, the cryptographically-relevant zone for RSL where the number of syndromes is limited

[8] https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals.

invites us to devise more efficient techniques. In this range, the algorithms that we have proposed do not outperform the RD solver.

Other systems. The approach followed in Chapter 10 by isolating a structured part in the system and by making an assumption on the rest of the equations is quite general and it may be used (at least, as a first step) in many other contexts. An interesting field of application is given by hard problems related to a secret permutation of $\{1..n\}$ such as the Permuted Equivalence Problem (PEP) and the Permuted Kernel Problem (PKP) [Sha90]. They are at the core of the NIST proposals [Bal+23] and [Aar+23] respectively. A bit before that, PKP was also used in [Beu+19]. The naive system suggested in [Sae17] to solve PEP is of the same shape as the one we studied for RSD. It combines structured polynomials modeling the secret permutation matrix together with linear equations provided by the input instance. However, no analysis has been performed. The goal would be to fill this gap as there should be a growing interest in the potential of algebraic attacks. Indeed, this type of cryptography is still at an early stage and parameters are far from being finalized.

The algebraic analysis of arithmetization-oriented primitives is another emerging topic and our work of Chapter 11 barely scratches the surface. We only studied one cipher and we restricted ourselves to the zero-dimensional strategy usually employed for public-key schemes. Regarding the first point, it may be interesting to adopt a more global approach no longer focused on one primitive especially because some existing modelings only depend on the structure in rounds and not really on particular design choices. Concerning the standard solving method, a first task would be to explain the gap between the generic bounds and the concrete quantities that we have observed (once again, this is not specific to Anemoi). Another route would be to find a suitable monomial order for which the input system is already a Gröbner basis. This is basically what happened for MiMC [Alb+19]. We have obviously no proof that such an ordering exists in general but this might be facilitated by the sparsity.

Bibliography

[Aar+23] Najwa Aaraj, Slim Bettaieb, Loïc Bidoux, Alessandro Budroni, Victor Dyseryn, Andre Esser, Philippe Gaborit, Mukul Kulkarni, Victor Mateu, Marco Palumbi, Luca Perin, and Jean-Pierre Tillich. *PERK*. NIST Round 1 submission to the Additional Call for Signature Schemes. 2023 (cit. on p. 200).

[ARV23] Gora Adj, Luis Rivera-Zamarripa, and Javier Verbel. "MinRank in the Head". In: *Progress in Cryptology - AFRICACRYPT 2023*. Ed. by Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne. Cham: Springer Nature Switzerland, 2023, pp. 3–27. ISBN: 978-3-031-37679-5 (cit. on pp. 31, 32, 127).

[Adj+23] Gora Adj, Stefano Barbero, Emanuele Bellini, Andre Esser, Luis Rivera-Zamarripa, Carlo Sanna, Javier Verbel, and Floyd Zweydinger. *MIRITH*. NIST Round 1 submission to the Additional Call for Signature Schemes. 2023 (cit. on p. 199).

[Agu+20] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Maxime Bros, Alain Couvreur, Jean-Christophe Deneuville, Philippe Gaborit, Gilles Zémor, and Adrien Hauteville. *Rank Quasi Cyclic (RQC)*. Second Round submission to NIST Post-Quantum Cryptography call. Apr. 2020 (cit. on pp. xii, 8, 46, 52, 128, 131–133, 135, 136, 140, 145).

[Agu+21] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and Jurjen Bos. *HQC*. Round 3 Submission to the NIST Post-Quantum Cryptography Call. https://pqc-hqc.org/doc/hqc-specification_2021-06-06.pdf. June 2021 (cit. on p. 46).

[Agu+22] Carlos Aguilar Melchor, Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, and Gilles Zémor. "LRPC Codes with Multiple Syndromes: Near Ideal-Size KEMs Without Ideals". In: *Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2022, 45–68. ISBN: 978-3-031-17233-5 (cit. on pp. 52, 91–93, 128, 133, 134).

[Ajt96] Miklós Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, 99–108. ISBN: 0897917855 (cit. on p. 92).

[Ala+19] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. en. 2019 (cit. on p. 133).

[Ala+22] Gorjan Alagic, David Cooper, Quynh Dang, Thinh Dang, John M. Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl A. Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Daniel Apon. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. en. 2022 (cit. on p. 8).

[Alb08] Martin Albrecht. "Algebraic Attacks on the Courtois Toy Cipher". In: *Cryptologia* 32 (July 2008), pp. 220–276 (cit. on p. 197).

[Alb+12] Martin Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. "On the complexity of the Arora-Ge Algorithm against LWE". In: *SCC 2012 – Third international conference on Symbolic Computation and Cryptography*. Castro Urdiales, Spain, July 2012, pp. 93–99 (cit. on p. 177).

[Alb+19] Martin Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. "Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC". In: Nov. 2019, pp. 371–397. ISBN: 978-3-030-34617-1 (cit. on p. 56).

[ACFP14] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. *Algebraic Algorithms for LWE*. Cryptology ePrint Archive, Paper 2014/1018. 2014 (cit. on pp. 177, 184, 185).

[Alb+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. "MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity". English. In: *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*. Lecture Notes in Computer Science. 2016 International Conference on the Theory and Application of Cryptology and Information Security : ASIACRYPT 2016, ASIACRYPT 2016 ; Conference date: 04-12-2016 Through 08-12-2016. 2016, pp. 191–219 (cit. on p. 55).

[Alb+20] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. *Classic McEliece: conservative code-based cryptography*. Round-3 submission to the NIST Post-Quantum Cryptography Standardization Project. https://cryptojedi.org/papers/#mceliecenistr3. 2020 (cit. on p. 92).

[Ale03] Michael Alekhnovich. "More on Average Case vs Approximation Complexity". In: vol. 20. Nov. 2003, pp. 298 –307. ISBN: 0-7695-2040-5 (cit. on p. 42).

[Alk+20] Erdem Alkim, Joppe W. Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, and Douglas Stebila. *FrodoKEM: Learning with errors key encapsulation*. https://frodokem.org/. Submission to the NIST Post-Quantum Cryptography standardization project, Round 3. 2020 (cit. on p. 92).

[Aly+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. "Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols". In: *IACR Trans. Symmetric Cryptol.* 2020 (2020), pp. 1–45 (cit. on pp. 55, 188).

[App+17] Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron. "Secure Arithmetic Computation with Constant Computational Overhead". In: *CRYPTO*. Springer, 2017, pp. 223–254 (cit. on p. 166).

[Ara+17a] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Güneysu, C. Aguilar Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, and G. Zémor. *BIKE*. NIST Round 1 submission for Post-Quantum Cryptography. Nov. 2017 (cit. on p. 43).

[Ara+19a] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Zémor. "Low Rank Parity Check Codes: New Decoding Algorithms and Application to Cryptography". In: 2019 (cit. on p. 45).

[ADG23] Nicolas Aragon, Victor Dyseryn, and Philippe Gaborit. "Analysis of the Security of the PSSI Problem and Cryptanalysis of the Durandal Signature Scheme". In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, 2023, pp. 127–149 (cit. on pp. 92, 103).

[AGHT18] 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 2018, Vail, CO, USA, June 17-22, 2018*. IEEE. 2018, pp. 2421–2425 (cit. on pp. 47, 48, 105, 128, 144, 145, 153, 154).

[Ara+17b] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. *LAKE – Low rAnk parity check codes Key Exchange*. First round submission to the NIST post-quantum cryptography call. NIST Round 1 submission for Post-Quantum Cryptography. Nov. 2017 (cit. on p. 45).

[Ara+17c] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. *LOCKER – LOw rank parity ChecK codes EncRyption*. First round submission to the NIST post-quantum cryptography call. NIST Round 1 submission for Post-Quantum Cryptography. Nov. 2017 (cit. on p. 46).

[Ara+19b] 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*. Vol. 11478. Springer, 2019, pp. 728–758 (cit. on pp. 51, 91, 92, 103).

[Ara+19c] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor, Carlos Aguilar Melchor, Slim Bettaieb, Loïc Bidoux, Bardet Magali, and Ayoub Otmani. *ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER)*. Second round submission to the NIST post-quantum cryptography call. NIST Round 2 submission for Post-Quantum Cryptography. Mar. 2019 (cit. on pp. 8, 46, 101).

[Ara+22] 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*. Cryptology ePrint Archive, Paper 2022/1596. https://eprint.iacr.org/2022/1596. 2022 (cit. on pp. 52, 91–93, 128, 149, 154, 155).

[Ara+23] Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesus-Javier Chi-Dominguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu, Mathieu Rivain, and Jean-Pierre Tillich. *MIRA*. NIST Round 1 submission to the Additional Call for Signature Schemes. 2023 (cit. on p. 199).

[AG11] Sanjeev Arora and Rong Ge. "New Algorithms for Learning in Presence of Errors". In: *Automata, Languages and Programming*. Ed. by Luca Aceto, Monika Henzinger, and Jiří Sgall. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 403–415. ISBN: 978-3-642-22006-7 (cit. on p. 177).

[Ars+04] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita. "Comparison Between XL and Gröbner Basis Algorithms". In: *Advances in Cryptology - ASIACRYPT 2004*. Ed. by Pil Joong Lee. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 338–353. ISBN: 978-3-540-30539-2 (cit. on pp. 23, 56).

[AD18] Tomer Ashur and Siemen Dhooghe. *MARVELlous: a STARK-Friendly Family of Cryptographic Primitives*. Cryptology ePrint Archive, Paper 2018/1098. https://eprint.iacr.org/2018/1098. 2018 (cit. on p. 55).

[AFS05] Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. "A Family of Fast Syndrome Based Cryptographic Hash Functions". In: *MYCRYPT 2005 : First International Conference on Cryptology in Malaysia*. Ed. by Dwason, Ed, Vaudenay, and Serge. Vol. 3715. Lecture Notes in Computer Science. Kuala Lumpur, Malaysia: Springer, Sept. 2005, pp. 64–83 (cit. on p. 53).

[BSZ15] Christine Bachoc, Oriol Serra, and Gilles Zémor. "An analogue of Vosper's Theorem for Extension Fields". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 163 (Jan. 2015) (cit. on p. 76).

[BV21] John Baena and Javier Verbel. *Sage tool for the GeMSS attack*. https://github.com/jbbaena/Attack_on_GeMSS/blob/main/Attack_on_GeMSS.ipynb. 2021 (cit. on p. 66).

[Bae+21] John Baena, Pierre, Daniel Cabarcas, Ray Perlner, Daniel Smith-Tone, and Javier Verbel. *Improving Support-Minors rank attacks: applications to GeMSS and Rainbow*. Cryptology ePrint Archive, Paper 2021/1677. https://eprint.iacr.org/2021/1677. 2021 (cit. on pp. 59, 60).

[Bae+22] John Baena, Pierre Briaud, Daniel Cabarcas, Ray A. Perlner, Daniel Smith-Tone, and Javier A. Verbel. "Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow". In: *CRYPTO 2022*. Vol. 13509. LNCS. Springer, 2022, pp. 376–405 (cit. on pp. xi, 59, 69).

[Bal+23] Jean-François Baldi, Alessandro Barenghi, Luke Beckwith, Jean-François Biasse, Andre Esser, Kris Gaj, Kamyar Mohajerani, Gerardo Pelosi, Edoardo Persichetti, Markku-Juhani O. Saarinen, Paolo Santini, and Robert Wallace. *LESS*. NIST Round 1 submission to the Additional Call for Signature Schemes. 2023 (cit. on p. 200).

[Bar04] Magali Bardet. "Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie". http://tel.archives-ouvertes.fr/tel-00449609/en/. PhD thesis. Université Paris VI, Dec. 2004 (cit. on pp. 19, 170, 184, 185).

[BB22] Magali Bardet and Manon Bertin. "Improvement of algebraic attacks for solving superdetermined MinRank instances". In: *PQCrypto 2022*. Vol. 13512. Lecture Notes in Computer Science. virtual, France: Springer, Sept. 2022 (cit. on p. 34).

[BB21] Magali Bardet and Pierre Briaud. "An Algebraic Approach to the Rank Support Learning Problem". In: *PQCrypto 2021*. Vol. 12841. LNCS. Springer, 2021, pp. 442–462 (cit. on pp. xii, xiii, 51, 91, 92, 95, 103).

[BFSY05] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. "Asymptotic behaviour of the index of regularity of quadratic semi-regular polynomial systems". In: *The Effective Methods in Algebraic Geometry Conference (MEGA'05)(P. Gianni, ed.)* 2005, pp. 1–14 (cit. on pp. 25, 172).

[BFS15] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. "On the complexity of the F5 Gröbner basis algorithm". In: *Journal of Symbolic Computation* 70 (2015), pp. 49–70. ISSN: 0747-7171 (cit. on p. 21).

[BFSS13] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Pierre-Jean Spaenlehauer. "On the complexity of solving quadratic Boolean systems". In: *Journal of Complexity* 29.1 (2013), pp. 53–75. ISSN: 0885-064X (cit. on pp. 167, 176, 184).

[BMT21] Magali Bardet, Rocco Mora, and Jean-Pierre Tillich. "Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach". In: *2021 IEEE International Symposium on Information Theory (ISIT)* (2021), pp. 872–877 (cit. on p. 25).

[BMT23] Magali Bardet, Rocco Mora, and Jean-Pierre Tillich. *Polynomial time key-recovery attack on high rate random alternant codes*. 2023. arXiv: 2304.14757 [cs.IT] (cit. on p. 43).

[Bar+20a] 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: *Advances in Cryptology - EUROCRYPT 2020 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020. Proceedings*. 2020 (cit. on pp. xi, 28, 49–51, 131, 133, 149, 157–159, 162).

[Bar+20b] 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: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by Shiho Moriai and Huaxiong Wang. Cham: Springer International Publishing, 2020, pp. 507–536. ISBN: 978-3-030-64837-4 (cit. on pp. x–xii, 34, 35, 49–51, 59, 62, 63, 69, 91, 97, 98, 103, 104, 107–109, 116, 117, 119, 127, 128, 131, 133, 135, 136, 162, 199).

[Bar+23] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. "Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem". In: *Designs, Codes and Cryptography* (2023) (cit. on pp. xi–xiii, 91, 107, 120).

[BBLP22] Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin. "Algebraic Attacks against Some Arithmetization-Oriented Primitives". In: *IACR Transactions on Symmetric Cryptology* 2022.3 (2022), 73–101 (cit. on pp. 190, 191).

[BBMS22] Carsten Baum, Lennart Braun, Alexander Munch-Hansen, and Peter Scholl. "MozZ2karella: Efficient Vector-OLE and Zero-Knowledge Proofs Over Z2k". In: *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part IV*. Santa Barbara, CA, USA: Springer-Verlag, 2022, 329–358. ISBN: 978-3-031-15984-8 (cit. on p. 166).

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. "Decoding Random Binary Linear Codes in 2n/20: How $1+1=0$ Improves Information Set Decoding". In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 520–536. ISBN: 978-3-642-29011-4 (cit. on p. 54).

[BM97] Mihir Bellare and Daniele Micciancio. "A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost". In: *Advances in Cryptology — EUROCRYPT '97*. Ed. by Walter Fumy. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 163–192. ISBN: 978-3-540-69053-5 (cit. on p. 54).

[BESV22] Emanuele Bellini, Andre Esser, Carlo Sanna, and Javier Verbel. "MR-DSS – Smaller MinRank-Based (Ring-)Signatures". In: *Post-Quantum Cryptography*. Ed. by Jung Hee Cheon and Thomas Johansson. Cham: Springer International Publishing, 2022, pp. 144–169. ISBN: 978-3-031-17234-2 (cit. on pp. 31, 124, 127).

[BGL20] Eli Ben-Sasson, Lior Goldberg, and David Levit. *STARK Friendly Hash – Survey and Recommendation*. Cryptology ePrint Archive, Paper 2020/948. https://eprint.iacr.org/2020/948. 2020 (cit. on pp. 56, 191, 197).

[Ber70] E. R. Berlekamp. "Factoring Polynomials Over Large Finite Fields". In: *Mathematics of Computation* 24.111 (1970), pp. 713–735. ISSN: 00255718, 10886842 (cit. on p. 38).

[BMT78] Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg. "On the inherent intractability of certain coding problems". In: 24.3 (May 1978), pp. 384–386 (cit. on p. 42).

[BBD08] Daniel J Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-Quantum Cryptography*. Dordrecht: Springer, 2008 (cit. on p. 23).

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. "Smaller Decoding Exponents: Ball-Collision Decoding". In: *Advances in Cryptology – CRYPTO 2011*. Ed. by Phillip Rogaway. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 743–760. ISBN: 978-3-642-22792-9 (cit. on p. 54).

[BLPS11] Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe. "Really Fast Syndrome-Based Hashing". In: *Progress in Cryptology – AFRICACRYPT 2011*. Ed. by Abderrahmane Nitaj and David Pointcheval. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 134–152. ISBN: 978-3-642-21969-6 (cit. on p. 53).

[BNS22] Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. "Faster change of order algorithm for Gröbner bases under shape and stability assumptions". In: *2022 International Symposium on Symbolic and Algebraic Computation*. Lille, France, July 2022 (cit. on p. 194).

[Bet12] Luk Bettale. "Cryptanalyse algébrique : outils et applications". PhD thesis. Université Pierre et Marie Curie - Paris 6, 2012 (cit. on p. 186).

[BFP10] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. "Hybrid approach for solving multivariate systems over finite fields". In: *Journal of Mathematical Cryptology* 3.3 (Jan. 2010), pp. 177–197 (cit. on pp. 24, 175, 186).

[BFP13] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. "Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic". In: *Designs, Codes and Cryptography* 69.1 (2013), pp. 1 –52 (cit. on pp. 39–41, 61, 63).

[BFP12] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. "Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach". In: July 2012, pp. 67–74 (cit. on p. 24).

[Beu20] Ward Beullens. "Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes". In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Cham: Springer International Publishing, 2020, pp. 183–211. ISBN: 978-3-030-45727-3 (cit. on pp. 31, 36).

[Beu21a] Ward Beullens. "Improved Cryptanalysis of UOV and Rainbow". In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by Anne Canteaut and François-Xavier Standaert. Cham: Springer International Publishing, 2021, pp. 348–373. ISBN: 978-3-030-77870-5 (cit. on pp. x, 28, 38, 59, 61, 63, 69).

[Beu21b] Ward Beullens. "MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps". In: *Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers*. Ed. by Riham AlTawy and Andreas Hülsing. Vol. 13203. Lecture Notes in Computer Science. Springer, 2021, pp. 355–376 (cit. on p. 199).

[Beu22] Ward Beullens. "Breaking Rainbow Takes a Weekend on a Laptop". In: *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*. Santa Barbara, CA, USA: Springer-Verlag, 2022, 464–479. ISBN: 978-3-031-15978-7 (cit. on p. 38).

[Beu+19] Ward Beullens, Jean-Charles Faugère, Eliane Koussa, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. "PKP-Based Signature Scheme". In: *Progress in Cryptology – INDOCRYPT 2019*. Vol. 11898. Lecture Notes in Computer Science. Hyderabad, India: Springer International Publishing, Dec. 2019, pp. 3–22 (cit. on p. 200).

[Beu+23] Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang. *Unbalanced Oil and Vinegar*. NIST Round 1 submission to the Additional Call for Signature Schemes. 2023 (cit. on pp. 61, 199).

[BBBG23] Loïc Bidoux, Pierre Briaud, Maxime Bros, and Philippe Gaborit. "RQC revisited and more cryptanalysis for Rank-based Cryptography". In: *IEEE Transactions on Information Theory* (2023) (cit. on pp. xii, xiii, 52, 91, 92, 104, 131, 133–135, 145).

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. "Short Group Signatures". In: *Advances in Cryptology – CRYPTO 2004*. Ed. by Matt Franklin. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 41–55. ISBN: 978-3-540-28628-8 (cit. on p. 5).

[BF01] Dan Boneh and Matt Franklin. "Identity-Based Encryption from the Weil Pairing". In: *Advances in Cryptology — CRYPTO 2001*. Ed. by Joe Kilian. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 213–229. ISBN: 978-3-540-44647-7 (cit. on p. 5).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171 (cit. on p. 22).

[Bou+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. "New Design Techniques For Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations

And Jive Compression Mode". In: *CRYPTO 2023*. Vol. 14085. LNCS. Springer, 2023, 507–539 (cit. on pp. xii, xiii, 187, 191, 196).

[BCGI18] Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai. "Compressing Vector OLE". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. Toronto, Canada: Association for Computing Machinery, 2018, 896–912. ISBN: 9781450356930 (cit. on pp. xiii, 53, 54, 166, 177).

[BGI15] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Function Secret Sharing". In: *Advances in Cryptology - EUROCRYPT 2015*. Ed. by Elisabeth Oswald and Marc Fischlin. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 337–367. ISBN: 978-3-662-46803-6 (cit. on p. 53).

[Boy+19a] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. "Efficient Pseudorandom Correlation Generators: Silent OT Extension and More". In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer International Publishing, 2019, pp. 489–518. ISBN: 978-3-030-26954-8 (cit. on p. 53).

[Boy+19b] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Rindal, and Peter Scholl. "Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. London, United Kingdom: Association for Computing Machinery, 2019, 291–308. ISBN: 9781450367479 (cit. on p. 53).

[BL23] Pierre Briaud and Pierre Loidreau. "Cryptanalysis of rank-metric schemes based on distorted Gabidulin codes". In: *PQCrypto 2023*. Vol. 14154. LNCS. Springer, 2023, pp. 38–56 (cit. on pp. xii, xiii, 149).

[BØ23] Pierre Briaud and Morten Øygarden. "A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions". In: *EUROCRYPT 2023*. Vol. 14008. LNCS. Springer, 2023, pp. 391–422 (cit. on pp. xii, xiii, 165, 177, 180, 181).

[BTV21] Pierre Briaud, Jean-Pierre Tillich, and Javier Verbel. "A Polynomial Time Key-Recovery Attack on the Sidon Cryptosystem". In: *SAC 2021*. Vol. 13203. LNCS. Springer, 2021, pp. 419–438 (cit. on pp. xii, 39, 75).

[BCN89] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. "The Families of Graphs with Classical Parameters". In: *Distance-Regular Graphs*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 255–293. ISBN: 978-3-642-74341-2 (cit. on p. 142).

[BV88] Winfried Bruns and Udo Vetter. "Preliminaries". In: *Determinantal Rings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 1–9. ISBN: 978-3-540-39274-3 (cit. on p. 35).

[Buc65] Bruno Buchberger. "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal". PhD thesis. Universitat Innsbruck, 1965 (cit. on p. 13).

[Buc76] Bruno Buchberger. "A Theoretical Basis for the Reduction of Polynomials to Canonical Forms". In: *SIGSAM Bull.* 10.3 (1976), 19–29. ISSN: 0163-5824 (cit. on pp. 14, 20).

[BPW06a] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. "A Zero-Dimensional Gröbner Basis for AES-128". In: *Fast Software Encryption*. Ed. by Matthew Robshaw. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 78–88. ISBN: 978-3-540-36598-3 (cit. on p. 56).

[BPW06b] Johannes A. Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. "Block Ciphers Sensitive to Gröbner Basis Attacks". In: *The Cryptographer's Track at RSA Conference*. 2006 (cit. on p. 56).

[BCP06] L. Budaghyan, C. Carlet, and A. Pott. "New classes of almost bent and almost perfect nonlinear polynomials". In: *IEEE Transactions on Information Theory* 52.3 (2006), pp. 1141–1152 (cit. on p. 188).

[BFS99] Jonathan F Buss, Gudmund S Frandsen, and Jeffrey O Shallit. "The Computational Complexity of Some Problems of Linear Algebra". In: *Journal of Computer and System Sciences* 58.3 (1999), pp. 572–596. ISSN: 0022-0000 (cit. on pp. x, 30).

[CG21] Alessio Caminata and Elisa Gorla. "Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra". In: *Arithmetic of Finite Fields*. Ed. by Jean Claude Bajard and Alev Topuzoğlu. Cham: Springer International Publishing, 2021, pp. 3–36. ISBN: 978-3-030-68869-1 (cit. on pp. 20, 24).

[CG23] Alessio Caminata and Elisa Gorla. "Solving degree, last fall degree, and related invariants". In: *Journal of Symbolic Computation* 114 (2023), pp. 322–335. ISSN: 0747-7171 (cit. on p. 26).

[Can17] Rodolfo Canto Torres. "Asymptotic Analysis of ISD algorithms for the $q-$ary case". In: *Proceedings of the Tenth International Workshop on Coding and Cryptography WCC 2017*. Sept. 2017 (cit. on pp. 54, 178).

[CS16] Rodolfo Canto Torres and Nicolas Sendrier. "Analysis of Information Set Decoding for a Sub-linear Error Weight". In: *Post-Quantum Cryptography*. Ed. by Tsuyoshi Takagi. Cham: Springer International Publishing, 2016, pp. 144–161. ISBN: 978-3-319-29360-8 (cit. on p. 54).

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. "Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems". In: *Designs, Codes and Cryptography* 15 (1998), pp. 125–156 (cit. on p. 188).

[CCJ23] Eliana Carozza, Geoffroy Couteau, and Antoine Joux. "Short Signatures From Regular Syndrome Decoding In The Head". In: *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*. Lyon, France: Springer-Verlag, 2023, 532–563. ISBN: 978-3-031-30588-7 (cit. on pp. 53, 54).

[CDMT22] Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. "Statistical decoding 2.0: Reducing decoding to LPN". In: *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*. Springer. 2022, pp. 477–507 (cit. on p. 54).

[CS17] Ryann Cartor and Daniel Smith-Tone. "An Updated Security Analysis of PFLASH". In: *Post-Quantum Cryptography*. Ed. by Tanja Lange and Tsuyoshi Takagi. Cham: Springer International Publishing, 2017, pp. 241–254. ISBN: 978-3-319-59879-6 (cit. on p. 38).

[CS19] Ryann Cartor and Daniel Smith-Tone. "EFLASH: A New Multivariate Encryption Scheme". In: *Selected Areas in Cryptography – SAC 2018*. Ed. by Carlos Cid and Michael J. Jacobson Jr. Cham: Springer International Publishing, 2019, pp. 281–299. ISBN: 978-3-030-10970-7 (cit. on p. 37).

[Cas+20] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, Ludovic Perret, and J. Ryckeghem. *GeMSS: A Great Multivariate Short Signature*. NIST CSRC. https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification_round2.pdf. 2020 (cit. on pp. 8, 37, 41).

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Cham: Springer Nature Switzerland, 2023, pp. 423–447. ISBN: 978-3-031-30589-4 (cit. on p. 8).

[CS96] Florent Chabaud and Jacques Stern. "The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes". In: *1996*. Vol. 1163. Kyongju, Korea: Springer, Nov. 1996, pp. 368–381 (cit. on pp. 47, 156).

[CYS15] Ming-Shing Chen, Bo-Yin Yang, and Daniel Smith-Tone. *PFLASH - Secure Asymmetric Signatures on Smart Cards*. Lightweight Cryptography Workshop 2015. http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf. 2015 (cit. on pp. 37, 42, 61).

[Che+18] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. "SOFIA: MQ-based signatures in the QROM". In: *Public Key Cryptography – PKC 2018*. Ed. by Michel Abdalla and Ricardo Dahab. Vol. 10770. Lecture Notes in Computer Science. Springer-Verlag Berlin Heidelberg, 2018, pp. 3–33 (cit. on p. 36).

[CCNY12] Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang. "Solving Quadratic Equations with XL on Parallel Architectures". In: *Cryptographic Hardware and Embedded Systems – CHES 2012*. Ed. by Emmanuel Prouff and Patrick Schaumont. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 356–373 (cit. on pp. 23, 69).

[CL05] Carlos Cid and Gaëtan Leurent. "An Analysis of the XSL Algorithm". In: *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*. Vol. 3788. Lecture Notes in Computer Science. Springer, 2005, pp. 333–352 (cit. on p. 56).

[CC20] Daniel Coggia and Alain Couvreur. "On the security of a Loidreau rank metric code based encryption scheme". In: *Des. Codes Cryptogr.* 88.9 (2020), pp. 1941–1957 (cit. on pp. 47, 150).

[Cop94] Don Coppersmith. "Solving homogeneous linear equations over GF (2) via block Wiedemann algorithm". In: *Mathematics of Computation* 62 (1994), pp. 333–350 (cit. on p. 23).

[CJ04] Jean-Sebastien Coron and Antoine Joux. *Cryptanalysis of a Provably Secure Cryptographic Hash Function*. Cryptology ePrint Archive, Paper 2004/013. https://eprint.iacr.org/2004/013. 2004 (cit. on p. 54).

[Cou01a] Nicolas Courtois. "La sécurité des primitives cryptographiques basées sur des problèmes algébriques multivariables MQ, IP, MinRank, HFE". In: 2001 (cit. on pp. 30–32).

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations". In: *Advances in Cryptology — EUROCRYPT 2000*. Ed. by Bart Preneel. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 392–407. ISBN: 978-3-540-45539-4 (cit. on p. 23).

[CM03] Nicolas Courtois and Willi Meier. "Algebraic Attacks on Stream Ciphers with Linear Feedback." In: vol. 2656. Jan. 2003, pp. 345–359 (cit. on p. ix).

[Cou01b] Nicolas T. Courtois. "Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank". In: *Advances in Cryptology — ASIACRYPT 2001*. Ed. by Colin Boyd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 402–421. ISBN: 978-3-540-45682-7 (cit. on pp. x, 30, 31, 34, 36).

[Cou01c] Nicolas T. Courtois. "The Security of Hidden Field Equations (HFE)". In: *Topics in Cryptology — CT-RSA 2001*. Ed. by David Naccache. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 266–281. ISBN: 978-3-540-45353-6 (cit. on pp. 34, 36).

[CP02] Nicolas T. Courtois and Josef Pieprzyk. "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". In: *Advances in Cryptology — ASIACRYPT 2002*. Ed. by Yuliang Zheng. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 267–287. ISBN: 978-3-540-36178-7 (cit. on pp. ix, 56, 191).

[CMT23] Alain Couvreur, Rocco Mora, and Jean-Pierre Tillich. "A new approach based on quadratic forms to attack the McEliece cryptosystem". In: Springer-Verlag, 2023 (cit. on p. 43).

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer International Publishing, 2015 (cit. on pp. 10, 13–15, 56).

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard (Information Security and Cryptography)*. 1st ed. Springer, 2002. ISBN: 3540425802 (cit. on p. 3).

[DT18] Thomas Debris-Alazard and Jean-Pierre Tillich. "Two attacks on rank metric code-based schemes: RankSign and an Identity-Based-Encryption scheme". In: *2018*. Vol. 11272. Brisbane, Australia: Springer, Dec. 2018, pp. 62–92 (cit. on pp. 51, 83, 92, 93).

[DH76] Whitfield Diffie and Martin E. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654 (cit. on pp. ix, 3).

[DCPS17] Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, and Dieter Schmidt. *Gui*. NIST CSRC. https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions. 2017 (cit. on p. 37).

[DH11] Jintai Ding and Timothy Hodges. "Inverting HFE Systems is Quasi-Polynomial for All Fields". In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference*. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, p. 721 (cit. on pp. xi, 41).

[DK12] Jintai Ding and Thorsten Kleinjung. "Degree of regularity for HFE Minus (HFE". In: 2012 (cit. on pp. xi, 41).

[DS05] Jintai Ding and Dieter Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme". In: *Applied Cryptography and Network Security*. Ed. by John Ioannidis, Angelos Keromytis, and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 164–175. ISBN: 978-3-540-31542-1 (cit. on p. 38).

[DS13] Jintai Ding and Dieter Schmidt. "Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields". In: *Number Theory and Cryptography*. 2013 (cit. on pp. 24, 25).

[DY13] Jintai Ding and Bo-Yin Yang. "Degree of Regularity for HFEv and HFEv-". In: *Post-Quantum Cryptography*. Ed. by Philippe Gaborit. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 52–66. ISBN: 978-3-642-38616-9 (cit. on pp. xi, 41).

[Din+20] Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, and Bo-Yin Yang. *Rainbow*. NIST CSRC. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions. 2020 (cit. on pp. 8, 38).

[DFSS07] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. "Practical Cryptanalysis of SFLASH". In: *Advances in Cryptology - CRYPTO 2007: 27th Annual International Cryptology Conference*. Ed. by Alfred Menezes. Vol. 4622. Lecture Notes in Computer Science. Santa Barbara, California, United States: Springer, 2007, pp. 1–12 (cit. on pp. 38, 61).

[DFS07] Vivien Dubois, Pierre-Alain Fouque, and Jacques Stern. "Cryptanalysis of SFLASH with Slightly Modified Parameters". In: *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Ed. by Moni Naor. Vol. 4515. Lecture Notes in Computer Science. Barcelona, Spain: Springer, 2007, pp. 264–275 (cit. on p. 38).

[EF17] Christian Eder and Jean-Charles Faugère. "A survey on signature-based algorithms for computing Gröbner bases". In: *Journal of Symbolic Computation* 80 (2017), pp. 719–784. ISSN: 0747-7171 (cit. on p. 22).

[Fau99] Jean-Charles Faugère. "A new efficient algorithm for computing Gröbner bases (F4)". In: *Journal of Pure and Applied Algebra* 139.1 (1999), pp. 61–88. ISSN: 0022-4049 (cit. on pp. xi, 22).

[Fau02] Jean Charles Faugère. "A New Efficient Algorithm for Computing GröBner Bases without Reduction to Zero (F5)". In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. ISSAC '02. Lille, France: Association for Computing Machinery, 2002, 75–83. ISBN: 1581134843 (cit. on pp. xi, 22).

[FGLM93] Jean-Charles Faugère, Patrizia M. Gianni, Daniel Lazard, and Teo Mora. "Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering". In: 16.4 (1993), pp. 329–344 (cit. on pp. 16, 194).

[FLP08] Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. "Cryptanalysis of MinRank". In: *Advances in Cryptology – CRYPTO 2008*. Ed. by David Wagner. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 280–296. ISBN: 978-3-540-85174-5 (cit. on pp. 33, 34).

[FM17] Jean-Charles Faugère and Chenqi Mou. "Sparse FGLM algorithms". In: *Journal of Symbolic Computation* 80.3 (May 2017), pp. 538 –569 (cit. on p. 194).

[FOPT10] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. "Algebraic Cryptanalysis of McEliece Variants with Compact Keys". In: *2010*. Vol. 6110. 2010, pp. 279–298 (cit. on p. 43).

[FSS10] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. "Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology". In: *ISSAC 2010 - 35th International Symposium on Symbolic and Algebraic Computation*. Munich, Germany: ACM, July 2010, pp. 257–264 (cit. on pp. x, 31, 33, 34).

[FSS13] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. "On the Complexity of the Generalized MinRank Problem". In: *Journal of Symbolic Computation* 55 (Mar. 2013), pp. 30–58 (cit. on p. 34).

[Fau+11] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. "A Distinguisher for High Rate McEliece Cryptosystems". In: *2011*. Paraty, Brasil, Oct. 2011, pp. 282–286 (cit. on p. 43).

[FGHR14] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault. "Sub-cubic Change of Ordering for Gröner Basis: A Probabilistic Approach". In: (July 2014) (cit. on p. 194).

[FMPP22] Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. *A New Perturbation for Multivariate Public Key Schemes such as HFE and UOV*. Cryptology ePrint Archive, Paper 2022/203. https://eprint.iacr.org/2022/203. 2022 (cit. on p. 199).

[FSS11] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity". In: *Journal of Symbolic Computation* 46.4 (2011), pp. 406–437. ISSN: 0747-7171 (cit. on pp. 24, 27, 33).

[Fen22] Thibauld Feneuil. *Building MPCitH-based Signatures from MQ, MinRank, Rank SD and PKP*. Cryptology ePrint Archive, Paper 2022/1512. https://eprint.iacr.org/2022/1512. 2022 (cit. on p. 31).

[FJR22] Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. "Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs". In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. Lecture Notes in Computer Science. Springer, 2022, pp. 541–572 (cit. on p. 53).

[FS87] Amos Fiat and Adi Shamir. "How To Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *Advances in Cryptology — CRYPTO' 86*. Ed. by Andrew M. Odlyzko. Berlin, Heidelberg: Springer Berlin Heidelberg, 1987, pp. 186–194. ISBN: 978-3-540-47721-1 (cit. on p. 31).

[FGS07] Matthieu Finiasz, Philippe Gaborit, and Nicolas Sendrier. "Improved Fast Syndrome Based Cryptographic Hash Functions". In: ECRYPT Hash Workshop 2007. 2007 (cit. on p. 53).

[FS09a] Matthieu Finiasz and Nicolas Sendrier. "Security Bounds for the Design of Code-Based Cryptosystems". In: *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*. Vol. 5912. Lecture Notes in Computer Science. Springer, 2009, pp. 88–105 (cit. on p. 54).

[FS09b] Philippe Flajolet and Robert Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009. ISBN: 978-0-521-89806-5 (cit. on p. 169).

[Frö85] Ralf Fröberg. "An inequality for Hilbert series of graded algebras". In: *Mathematica Scandinavica* 56.2 (1985), pp. 117–144. ISSN: 00255521, 19031807 (cit. on p. 19).

[Frö98] Ralf Fröberg. *An introduction to Gröbner bases*. Pure and applied mathematics. Wiley, 1998. ISBN: 978-0-471-97442-0 (cit. on p. 18).

[FI23] Hiroki Furue and Yasuhiko Ikematsu. "A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack". In: *Advances in Information and Computer Security*. Ed. by Junji Shikata and Hiroki Kuzuno. Cham: Springer Nature Switzerland, 2023, pp. 101–116. ISBN: 978-3-031-41326-1 (cit. on pp. 61, 199).

[FIKT21] Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. "A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV". In: Springer-Verlag, 2021 (cit. on p. 199).

[Gab85] E. M. Gabidulin. "Theory of codes with maximum rank distance". English. In: *Probl. Inf. Transm.* 21 (1985), pp. 1–12. ISSN: 0032-9460 (cit. on p. 45).

[GPT91] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. "Ideals over a Non-Commutative Ring and their Application in Cryptology". In: *Advances in Cryptology — EUROCRYPT '91*. Ed. by Donald W. Davies. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 482–489. ISBN: 978-3-540-46416-7 (cit. on pp. 43, 45).

[GHPT17] Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich. "Identity-based Encryption from Rank Metric". In: *2017*. Vol. 10403. Santa Barbara, CA, USA: Springer, Aug. 2017, pp. 194–226 (cit. on pp. 51, 91–93, 105).

[GRS16] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. "On the Complexity of the Rank Syndrome Decoding Problem". In: *IEEE Trans. Information Theory* 62.2 (2016), pp. 1006–1019 (cit. on pp. 47, 49, 105, 120, 153).

[GZ16] Philippe Gaborit and Gilles Zémor. "On the hardness of the decoding and the minimum distance problems for rank codes". In: 62(12) (2016), pp. 7245–7252 (cit. on p. 45).

[Gen09] Craig Gentry. "Fully Homomorphic Encryption Using Ideal Lattices". In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. STOC '09. Bethesda, MD, USA: Association for Computing Machinery, 2009, 169–178. ISBN: 9781605585062 (cit. on p. 7).

[Gha22] Anirban Ghatak. "Extending Coggia–Couvreur attack on Loidreau's rank-metric cryptosystem". In: *Designs, Codes and Cryptography* 90 (Jan. 2022) (cit. on p. 150).

[GM87] Patrizia Gianni and Teo Mora. "Algebraic Solution of Systems of Polynomial Equations Using Groebner Bases." In: vol. 356. Jan. 1987, pp. 247–257 (cit. on p. 15).

[GNS23] Sriram Gopalakrishnan, Vincent Neiger, and Mohab Safey El Din. "Refined F5 Algorithms for Ideals of Minors of Square Matrices". In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*. ISSAC '23. Tromsø, Norway: Association for Computing Machinery, 2023, 270–279. ISBN: 9798400700392 (cit. on p. 24).

[GC00] Louis Goubin and Nicolas Courtois. "Cryptanalysis of the TTM Cryptosystem". In: vol. 1976. Dec. 2000, pp. 44–57. ISBN: 978-3-540-41404-9 (cit. on p. 32).

[GKS23] Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. "Poseidon2: A Faster Version of the Poseidon Hash Function". In: *Progress in Cryptology - AFRICACRYPT 2023*. Ed. by Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne. Cham: Springer Nature Switzerland, 2023, pp. 177–203. ISBN: 978-3-031-37679-5 (cit. on p. 55).

[Gra+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. "Poseidon: A New Hash Function for Zero-Knowledge Proof Systems". In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 519–535. ISBN: 978-1-939133-24-3 (cit. on p. 55).

[Gra+23] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. "Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications". In: Springer-Verlag, 2023 (cit. on pp. 187, 191, 192).

[Gro96] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, 212–219. ISBN: 0897917855 (cit. on p. 7).

[HT15] Adrien Hauteville and Jean-Pierre Tillich. "New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem". In: (Apr. 2015) (cit. on pp. 47, 132).

[HOSS18] Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez. "TinyKeys: A New Approach to Efficient Multi-Party Computation". In: *Advances in Cryptology – CRYPTO 2018*. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 3–33 (cit. on pp. 53, 54, 174, 182).

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. "Zero-knowledge from secure multiparty computation". In: *Symposium on the Theory of Computing*. 2007 (cit. on p. 31).

[Jab01] A. Kh. Al Jabri. "A Statistical Decoding Algorithm for General Linear Block Codes". In: *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*. Ed. by Bahram Honary. Vol. 2260. Lecture Notes in Computer Science. Springer, 2001, pp. 1–8 (cit. on p. 54).

[Jac96] Nathan Jacobson. "Galois Descent and Generic Splitting Fields". In: *Finite-Dimensional Division Algebras over Fields*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 95–153. ISBN: 978-3-642-02429-0 (cit. on p. 36).

[Jao+17] David Jao, Reza Azarderakhsh, Matt Campagna, Craig Costello, Luca de Feo, Basil Hess, Amir Jalili, Brian Koziel, Brian Lamacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. *SIKE: Supersingular Isogeny Key Encapsulation*. Soumission à l'appel à candidatures "Post-Quantum Cryptography" du NIST. 2017 (cit. on p. 8).

[JDH07] Xin Jiang, Jintai Ding, and Lei Hu. "Kipnis-Shamir Attack on HFE Revisited". In: Aug. 2007, pp. 399–411. ISBN: 978-3-540-79498-1 (cit. on p. 61).

[JF03] Antoine Joux and Jean-Charles Faugère. "Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Grobner Bases". In: *CRYPTO 2003 - 23rd Annual International Cryptology Conference*. Vol. 2729. Lecture Notes in Computer Science. Santa Barbara, California, United States: Springer, Aug. 2003, pp. 44–60 (cit. on pp. xi, 38).

[KKS05] Gregory Kabatianskii, Evgenii Krouk, and Sergei Semenov. *Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept*. John Wiley & Sons, 2005 (cit. on p. 51).

[KKS97] Gregory Kabatianskii, Evgenii Krouk, and Ben. J. M. Smeets. "A Digital Signature Scheme Based on Random Error-Correcting Codes". In: *IMA Int. Conf.* Vol. 1355. Springer, 1997, pp. 161–167 (cit. on p. 51).

[Kal95] Erich Kaltofen. "Analysis of Coppersmith's Block Wiedemann Algorithm for the Parallel Solution of Sparse Linear Systems". In: *Mathematics of Computation* 64.210 (1995), pp. 777–806. ISSN: 00255718, 10886842 (cit. on p. 71).

[KKW18] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. Toronto, Canada: Association for Computing Machinery, 2018, 525–537. ISBN: 9781450356930 (cit. on p. 31).

[Ker83] A. Kerckhoffs. "La cryptographie militaire". In: *Journal des Sciences Militaires* (1883), pp. 161–191 (cit. on p. 5).

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. "Unbalanced Oil and Vinegar Signature Schemes". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by Jacques Stern. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 206–222. ISBN: 978-3-540-48910-8 (cit. on p. 199).

[KS99] Aviad Kipnis and Adi Shamir. "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization". In: *Advances in Cryptology — CRYPTO' 99*. Ed. by Michael Wiener. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 19–30. ISBN: 978-3-540-48405-9 (cit. on pp. 33, 34, 36, 39, 41, 61).

[Kir11] Paul Kirchner. *Improved Generalized Birthday Attack*. Cryptology ePrint Archive, Paper 2011/377. https://eprint.iacr.org/2011/377. 2011 (cit. on p. 54).

[Laz83] Daniel Lazard. "Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations". In: *Computer Algebra*. Ed. by J. A. van Hulzen. Berlin, Heidelberg: Springer Berlin Heidelberg, 1983, pp. 146–156. ISBN: 978-3-540-38756-5 (cit. on pp. 18, 20).

[Le 14] Francois Le Gall. "Powers of Tensors and Fast Matrix Multiplication". In: *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC* 2014 (Jan. 2014) (cit. on p. 182).

[LP06] Françoise Levy-dit-Vehel and Ludovic Perret. "Algebraic decoding of rank metric codes". In: *Talk at the Special Semester on Gröbner Bases - Workshop D1* (2006), pp. 1–19 (cit. on p. 162).

[LWYY22] Hanlin Liu, Xiao Wang, Kang Yang, and Yu Yu. *The Hardness of LPN over Any Integer Ring and Field for PCG Applications*. Cryptology ePrint Archive, Paper 2022/712. 2022 (cit. on pp. 54, 166, 177–179).

[Loi14] Pierre Loidreau. "Asymptotic behaviour of codes in rank metric over finite fields". In: 71.1 (2014), pp. 105–118 (cit. on p. 123).

[Loi17] Pierre Loidreau. "A New Rank Metric Codes Based Encryption Scheme". In: *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*. Ed. by Tanja Lange and Tsuyoshi Takagi. Vol. 10346. Lecture Notes in Computer Science. Springer, 2017, pp. 3–17 (cit. on pp. 46, 92, 149, 154, 155).

[LP21] Pierre Loidreau and Ba-Duc Pham. "An analysis of Coggia-Couvreur attack on Loidreau's rank-metric public key encryption scheme in the general case". In: *CoRR* abs/2112.12445 (2021). arXiv: 2112.12445 (cit. on p. 150).

[Lyu09] Vadim Lyubashevsky. "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2009, pp. 598–616 (cit. on pp. 51, 92).

[Mac02] F.S. Macaulay. "Some Formulæ in Elimination". In: *Proceedings of the London Mathematical Society* s1-35.1 (May 1902), pp. 3–27. ISSN: 0024-6115. eprint: https://academic.oup.com/plms/article-pdf/s1-35/1/3/4346649/s1-35-1-3.pdf (cit. on p. 18).

[Mac94] F.S. Macaulay. *The Algebraic Theory of Modular Systems*. Cambridge Mathematical Library. Cambridge University Press, 1994. ISBN: 9780521455626 (cit. on p. 20).

[Mai+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A Direct Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Cham: Springer Nature Switzerland, 2023, pp. 448–471. ISBN: 978-3-031-30589-4 (cit. on p. 8).

[MI88] Tsutomu Matsumoto and Hideki Imai. "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption". In: *Advances in Cryptology — EUROCRYPT '88*. Ed. by D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and Christoph G. Günther. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 419–453. ISBN: 978-3-540-45961-3 (cit. on p. 37).

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. "Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$". In: *ASIACRYPT*. Vol. 7073. Lecture Notes in Computer Science. Springer, 2011, pp. 107–124 (cit. on p. 54).

[MO15] Alexander May and Ilya Ozerov. “On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes”. In: *Advances in Cryptology – EUROCRYPT 2015*. Ed. by Elisabeth Oswald and Marc Fischlin. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 203–228. ISBN: 978-3-662-46800-5 (cit. on p. 54).

[McE78] Robert J. McEliece. “A Public-Key System Based on Algebraic Coding Theory”. In: DSN Progress Report 44. Jet Propulsion Lab, 1978, pp. 114–116 (cit. on p. 42).

[MDCE11] Mohammed Meziani, Özgür Dagdelen, Pierre-Louis Cayrel, and Sidi Mohamed El Yousfi Alaoui. “S-FSB: An Improved Variant of the FSB Hash Family”. In: *International Symposium on Algorithms*. 2011 (cit. on p. 53).

[Mic10] Daniele Micciancio. “A First Glimpse of Cryptography’s Holy Grail”. In: *Commun. ACM* 53.3 (2010), p. 96. ISSN: 0001-0782 (cit. on p. 7).

[MTSB13] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. “MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes”. In: *2013 IEEE International Symposium on Information Theory*. 2013, pp. 2069–2073 (cit. on p. 43).

[Moo+20] Dustin Moody, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Jacob Alperin-Sheriff. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. en. 2020 (cit. on p. 52).

[MR02] Sean Murphy and Matthew J. B. Robshaw. “Essential Algebraic Structure within the AES”. In: *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*. Vol. 2442. Lecture Notes in Computer Science. Springer, 2002, pp. 1–16 (cit. on p. 56).

[Nie12] Ruben Niederhagen. “Parallel Cryptanalysis”. http://polycephaly.org/thesis/index.shtml. PhD thesis. Eindhoven University of Technology, 2012 (cit. on p. 69).

[OJ02] Alexei V. Ourivski and Thomas Johansson. “New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications”. English. In: *Problems of Information Transmission* 38.3 (2002), pp. 237–246. ISSN: 0032-9460 (cit. on pp. 47–49, 149, 153, 155–157).

[Ove05] Raphael Overbeck. “A New Structural Attack for GPT and Variants”. In: *Progress in Cryptology – Mycrypt 2005*. Ed. by Ed Dawson and Serge Vaudenay. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 50–63. ISBN: 978-3-540-32066-1 (cit. on p. 45).

[ØSV21] Morten Øygarden, Daniel Smith-Tone, and Javier A. Verbel. "On the Effect of Projection on Rank Attacks in Multivariate Cryptography". In: *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings*. Ed. by Jung Hee Cheon and Jean-Pierre Tillich. Vol. 12841. Lecture Notes in Computer Science. Springer, 2021, pp. 98–113 (cit. on pp. xiii, 42, 60–62, 72, 73).

[Pai99] Pascal Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by Jacques Stern. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 223–238. ISBN: 978-3-540-48910-8 (cit. on p. 5).

[Par10] Keith Pardue. "Generic sequences of polynomials". In: *Journal of Algebra* 324.4 (2010), pp. 579–590. ISSN: 0021-8693 (cit. on p. 18).

[Pat95] Jacques Patarin. "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88". In: *Advances in Cryptology — CRYPT0' 95*. Ed. by Don Coppersmith. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 248–261. ISBN: 978-3-540-44750-4 (cit. on pp. 37, 38).

[Pat96] Jacques Patarin. "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms". In: *Advances in Cryptology — EUROCRYPT '96*. Ed. by Ueli Maurer. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 33–48. ISBN: 978-3-540-68339-1 (cit. on pp. xi, 37).

[PS20] Ray Perlner and Daniel Smith-Tone. *Rainbow Band Separation is Better than we Thought*. Cryptology ePrint Archive, Paper 2020/702. https://eprint.iacr.org/2020/702. 2020 (cit. on p. 28).

[PUB16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. "Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem". In: *Advances in Cryptology – CRYPTO 2016*. Ed. by Matthew Robshaw and Jonathan Katz. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 93–122. ISBN: 978-3-662-53008-5 (cit. on p. 188).

[Pet+15] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. "Design Principles for HFEv- Based Multivariate Signature Schemes". In: *Advances in Cryptology – ASIACRYPT 2015*. Ed. by Tetsu Iwata and Jung Hee Cheon. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 311–334. ISBN: 978-3-662-48797-6 (cit. on pp. 37, 38, 41).

[Pra62] Eugene Prange. "The use of information sets in decoding cyclic codes". In: *IRE Transactions on Information Theory* 8.5 (1962), pp. 5–9 (cit. on pp. 47, 54).

[Rab05] Michael O. Rabin. "How To Exchange Secrets with Oblivious Transfer". In: *IACR Cryptol. ePrint Arch.* 2005 (2005), p. 187 (cit. on p. 5).

[RLT21] Netanel Raviv, Ben Langton, and Itzhak Tamo. "Multivariate Public Key Cryptosystem from Sidon Spaces". In: *Public-Key Cryptography – PKC 2021*. Ed. by Juan A. Garay. Cham: Springer International Publishing, 2021, pp. 242–265. ISBN: 978-3-030-75245-3 (cit. on pp. xii, 37, 75, 76, 78, 83, 86, 88).

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (1978), 120–126. ISSN: 0001-0782 (cit. on p. 4).

[Rob23] Damien Robert. "Breaking SIDH in Polynomial Time". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Cham: Springer Nature Switzerland, 2023, pp. 472–503. ISBN: 978-3-031-30589-4 (cit. on p. 8).

[RRT17] Ron M. Roth, Netanel Raviv, and Itzhak Tamo. "Construction of Sidon Spaces With Applications to Coding". In: *IEEE Transactions on Information Theory* 64 (2017), pp. 4412–4422 (cit. on pp. 76, 78, 88).

[Saa07] Markku-Juhani O. Saarinen. "Linearization Attacks Against Syndrome Based Hashes". In: *Progress in Cryptology – INDOCRYPT 2007*. Ed. by K. Srinathan, C. Pandu Rangan, and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 1–9. ISBN: 978-3-540-77026-8 (cit. on p. 54).

[Sae17] Mohamed Ahmed Saeed. "Algebraic Approach for Code Equivalence". Theses. Normandie Université, Dec. 2017 (cit. on p. 200).

[SSH11a] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. "On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack". In: *Post-Quantum Cryptography*. Ed. by Bo-Yin Yang. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 68–82. ISBN: 978-3-642-25405-5 (cit. on p. 37).

[SSH11b] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. "Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials". In: *Advances in Cryptology – CRYPTO 2011*. Ed. by Phillip Rogaway. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 706–723. ISBN: 978-3-642-22792-9 (cit. on p. 36).

[Sch91] Claus-Peter Schnorr. "Efficient signature generation by smart cards". In: *Journal of cryptology* 4.3 (1991), pp. 161–174 (cit. on p. 51).

[Sem04] Igor A. Semaev. "Summation polynomials and the discrete logarithm problem on elliptic curves". In: *IACR Cryptol. ePrint Arch.* 2004 (2004), p. 31 (cit. on p. ix).

[Sha90] Adi Shamir. "An Efficient Identification Scheme Based on Permuted Kernels (extended abstract)". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by Gilles Brassard. New York, NY: Springer New York, 1990, pp. 606–609. ISBN: 978-0-387-34805-6 (cit. on p. 200).

[Sha49] C. E. Shannon. "Communication theory of secrecy systems". In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715 (cit. on p. 6).

[Sho94] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134 (cit. on pp. ix, 6).

[SJB11] Vladimir Sidorenko, Lan Jiang, and Martin Bossert. "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes". In: *Information Theory, IEEE Transactions on* 57 (Mar. 2011), pp. 621 –632 (cit. on p. 93).

[Smi10] Daniel Smith-Tone. "Properties of the Discrete Differential with Cryptographic Applications". In: *Post-Quantum Cryptography*. Ed. by Nicolas Sendrier. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–12. ISBN: 978-3-642-12929-2 (cit. on p. 38).

[Ste89] Jacques Stern. "A method for finding codewords of small weight". In: *Coding Theory and Applications*. Ed. by Gérard Cohen and Jacques Wolfmann. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 106–113. ISBN: 978-3-540-46726-7 (cit. on p. 54).

[Sto00] Arne Storjohann. "Algorithms for matrix canonical forms". en. Diss., Technische Wissenschaften ETH Zürich, Nr. 13922, 2001. Doctoral Thesis. Zürich: ETH Zurich, 2000 (cit. on p. 21).

[STA20] Chao Sun, Mehdi Tibouchi, and Masayuki Abe. "Revisiting the Hardness of Binary Error LWE". In: *Information Security and Privacy: 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 – December 2, 2020, Proceedings*. Perth, WA, Australia: Springer-Verlag, 2020, 425–444. ISBN: 978-3-030-55303-6 (cit. on p. 177).

[SAD20] Alan Szepieniec, Tomer Ashur, and Siemen Dhooghe. *Rescue-Prime: a Standard Specification (SoK)*. Cryptology ePrint Archive, Paper 2020/1143. https://eprint.iacr.org/2020/1143. 2020 (cit. on p. 55).

[TPD21] Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. "Efficient Key Recovery for All HFE Signature Variants". In: *Advances in Cryptology – CRYPTO 2021*. Ed. by Tal Malkin and Chris Peikert. Cham: Springer International Publishing, 2021, pp. 70–93. ISBN: 978-3-030-84242-0 (cit. on pp. x, xi, xiii, 41, 42, 59–63, 72, 73).

[Tea11] The Keccak Team. *Cryptographic sponge functions*. https://keccak.team/files/CSF-0.1.pdf. 2011 (cit. on p. 190).

[Tho02] Emmanuel Thomé. "Subquadratic Computation of Vector Generating Polynomials and Improvement of the Block Wiedemann Algorithm". In: *Journal of Symbolic Computation* 33.5 (2002), pp. 757–775. ISSN: 0747-7171 (cit. on p. 23).

[Tra96] Carlo Traverso. "Hilbert Functions and the Buchberger Algorithm". In: *Journal of Symbolic Computation* 22.4 (1996), pp. 355–376. ISSN: 0747-7171 (cit. on p. 24).

[VS17] Jeremy Vates and Daniel Smith-Tone. "Key Recovery Attack for All Parameters of HFE-". In: *Post-Quantum Cryptography*. Ed. by Tanja Lange and Tsuyoshi Takagi. Cham: Springer International Publishing, 2017, pp. 272–288. ISBN: 978-3-319-59879-6 (cit. on pp. 38, 61).

[Vel22] Vesselin Velichkov. *Design of Arithmetization-Oriented Hash Functions (zkcrypto)*. https://github.com/vesselinux/zkcrypto. 2022 (cit. on p. 197).

[Ver+19] Javier Verbel, John Baena, Daniel Cabarcas, Ray Perlner, and Daniel Smith-Tone. "On the Complexity of "Superdetermined" Minrank Instances". In: *Post-Quantum Cryptography*. Ed. by Jintai Ding and Rainer Steinwandt. Cham: Springer International Publishing, 2019, pp. 167–186. ISBN: 978-3-030-25510-7 (cit. on pp. 27, 33, 34).

[Vol69] Strassen Volker. "Gaussian Elimination is not Optimal". In: *Numerische Mathematik* 13 (1969), pp. 354–356 (cit. on p. 71).

[Wag02] David Wagner. "A Generalized Birthday Problem". In: *Advances in Cryptology — CRYPTO 2002*. Ed. by Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 288–304. ISBN: 978-3-540-45708-4 (cit. on p. 54).

[WYKW21] Chenkai Weng, Kang Yang, Jonathan Katz, and Xiao Wang. "Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits". In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 1074–1091 (cit. on pp. 53, 54, 177).

[Wie86] Doug Wiedemann. "Solving sparse linear equations over finite fields". In: *IEEE Transactions on Information Theory* 32.1 (1986), pp. 54–62 (cit. on p. 23).

[WP11] Christopher Wolf and Bart Preneel. "Equivalent Keys in Multivariate Quadratic Public Key Systems." In: *IACR Cryptology ePrint Archive* 2005 (Apr. 2011), p. 464 (cit. on pp. 39, 61).

[Yan+20] Kang Yang, Chenkai Weng, Xiao Lan, Jiang Zhang, and Xiao Wang. "Ferret: Fast Extension for Correlated OT with Small Communication". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. CCS '20. Virtual Event, USA: Association for Computing Machinery, 2020, 1607–1626. ISBN: 9781450370899 (cit. on pp. 53, 54, 177).

[Yao86] Andrew Chi-Chih Yao. "How to generate and exchange secrets". In: *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*. 1986, pp. 162–167 (cit. on p. 5).