Security Analysis of the Family of DME Schemes. Análisis de Seguridad de la Familia de Esquemas DME.

presentada por

Pilar Coscojuela Escanilla

Directores:

Martín Avendaño González, Ignacio Luengo Velasco

Facultad de Matemáticas, Universidad Complutense de Madrid

November 2025

Security Analysis of the Family of DME Schemes. Análisis de Seguridad de la Familia de Esquemas DME.

presentada por

Pilar Coscojuela Escanilla

Directores:

Martín Avendaño González, Ignacio Luengo Velasco

Programa de Doctorado en Investigación Matemática

Facultad de Matemáticas, Universidad Complutense de Madrid

November 2025

Acknowledgements

I would like to thank Ignacio Luengo for his work as advisor and supervisor; for having proposed an original thesis topic aligned with my interests, and for his involvement in designing variants, which has been extremely useful in gaining a broader perspective on the problem.

I am grateful to Martín Avendaño for accepting to be co-supervisor of this thesis and for his valuable help and advice on how to approach the problem.

I also wish to thank Ludovic Perret and Simona Samardjiska for their helpful comments, and them together with Alex Ryba for bringing to my attention the generalized MinRank problem, which was essential to the results of this thesis.

To the members of the project PID2020-114750GB-C32 for welcoming me warmly.

To the project and the Universidad Complutense for the financial support received.

Finally, I thank my parents, Jesús and Carmen, for their unconditional support throughout my studies. To Pablo, for listening and encouraging me whenever needed, and – oh yes – for recommending Visual Studio Code!

Contents

Abstract 1

1 Multivariate cryptography and Gröbner Bases 7
1.1 Post quantum era and Multivariate cryptography . . . 7
1.2 Padding in RSA . . . 10
1.3 Hilbert series and dimension of an ideal . . . 12
1.4 Orders on $\mathbb{T}^n$ and the Division Algorithm in $\mathbb{K}[X_1, \ldots, X_n]$ . . . 15
1.5 Gröbner Bases . . . 17
1.5.1 Computing Gröbner Bases . . . 21
1.5.2 Applications . . . 30
1.5.2.1 Elimination . . . 30
1.5.2.2 Solving systems of equations . . . 30

2 Complexity results 33
2.1 Complexity theory . . . 33
2.2 Complexity of computing Gröbner bases . . . 35
2.2.1 Degree, index of regularity and degree of regularity of an ideal. . . . 35
2.2.2 Complexity of Matrix F_5 algorithm . . . 37
2.3 Regular and Semi-regular Sequences . . . 38
2.4 MinRank Problem . . . 40
2.4.1 Complexity of the Generalized MinRank Problem and Determinantal ideals . . . 42

3 DME schemes 48
3.1 Mathematical setting . . . 48
3.2 NIST PQC 2017 version . . . 52
3.3 NIST PQC 2023 version . . . 53
3.3.1 Which data should be public and private? . . . 55
3.4 Reductions . . . 61
3.5 Padding . . . 62
3.6 New DME versions . . . 63
3.6.1 DME minus schemes . . . 63
3.6.2 DME plus scheme . . . 64
3.6.3 DME exponential over $\mathbb{F}_q$ . . . 65

3.6.4 DME$_{\mathrm{w}}$ . . . 66

4 Attacks 68
4.1 State of the art: structural attacks . . . 68
4.1.1 Attack to PQC NIST 2017 . . . 69
4.1.2 Reductions avoid the previous attack . . . 70
4.1.3 NIST algebraic structural attack . . . 71
4.2 Simplifying the private key . . . 73
4.3 Extended attack . . . 76
4.3.1 Modelling of the attack . . . 77
4.3.1.1 Removing collisions, case $k = 2$ . . . 79
4.3.1.2 Removing collisions, case $k > 2$ . . . 89
4.4 Reduction of the number of variables: DME 2023 . . . 94
4.5 Recovery of the variables before the exponential: DME 2023 . . . 97
4.6 Estimates on the number of variables when the maps are affine . . . 98

5 Attack on the DME minus 103
5.1 Modelling of the attack . . . 103
5.1.1 Removing collisions, case $k = 2$ . . . 109
5.2 Reduction of the number of variables: DME minus . . . 113
5.3 Recovery of the variables before the exponential: DME minus . . . 115
5.3.1 Simple example . . . 115
5.3.2 Using techniques of the extended attack . . . 119
5.3.2.1 On the preimage of a special family of points under the Kronecker product . . . 122

6 Variants 129
6.1 Other DME minus schemes . . . 129
6.2 DME^{+} . . . 135
6.3 DME over $\mathbb{F}_q$ . . . 136
6.4 DME$_{\mathrm{w}}$ . . . 137
6.4.1 Analysis . . . 137

7 Conclusions and future work 141
7.1 Future work . . . 142

Bibliography 144

Abstract

In this thesis, we propose a systematic approach to analyzing the security of the family of DME cryptosystems, which belong to the area of multivariate cryptography. As in many attacks on other multivariate cryptosystems, the bottleneck of the attack reduces to solving an instance of the MinRank problem of low rank, arising from the structure of the scheme.
All complexity estimates in this thesis are derived using the results of [1], and therefore rely on the assumption of genericity. Once the set of private keys is simplified – by specializing some of the variables – so that, for a given public key, there exists essentially a unique private key, the genericity assumption appears reasonable in light of the experimental results.
Our findings are consistent with those of [2] for the DME version introduced in [3]. Moreover, our analysis also applies to the DME minus, the minus variation of the scheme. While it can also be used to obtain estimates of the complexity of more general versions; this is future work.

Resumen

En esta tesis proponemos un modelo que permite analizar la seguridad de forma sistemática de la familia de esquemas DME; un tipo de esquemas multivariables. Como en muchos ataques algebraicos a otros esquemas de tipo multivariable, la parte que conlleva mayor complejidad es resolver una instancia del problema de MinRank con rango bajo que proviene de la estructura del criptosistema en cuestión. Todos los resultados de complejidad que se presentan en este trabajo se han obtenido usando los resultados de [1] y, por tanto, son válidos bajo hipótesis de genericidad. Tras reducir el conjunto de claves privadas – especializando alguna de sus variables – de forma que dada una clave pública, existe esencialmente una única clave privada, la hipótesis de genericidad parece razonable a la vista de los resultados experimentales. Nuestros resultados son consistentes con los obtenidos en [2] para la version del DME introducida en [3]. Además, nuestro análisis es válido para la versión DME minus. Aunque también puede utilizarse para deducir cotas de complejidad de otras versiones del DME; esto es trabajo futuro.

Introduction

The development by Shor in 1994 of an algorithm that can solve the underlying mathematical problems of the classical public-key cryptosystems – RSA and DSA —in polynomial time on a quantum computer, together with recent advances in building quantum hardware, has created an urgent need to develop new schemes that are resistant to quantum attacks.

The design of public-key schemes that remain secure against quantum computers is known as post-quantum cryptography. Its relevance beyond academia became evident when, in 2016, the National Institute of Standards and Technology (NIST) announced a call for proposals for quantum-resistant standards. Submissions to that call fall into five main classes: lattice-based, code-based, multivariate, isogeny-based and hash-based (the last only for digital signatures) public-key cryptography. Multivariate public-key cryptosystems are those in which the public key is given by a set of multivariate polynomials over a finite field. The fact that solving a system of randomly chosen multivariate polynomials over a finite field, with degree greater than one, is NP-hard, together with the expectation that quantum computers are unlikely to provide an advantage for this specific problem, makes multivariate schemes attractive candidates for post-quantum primitives. Compared to lattice-based schemes, multivariate schemes generally have larger public keys.

If

$$p_1, \dots, p_m \in \mathbb{F}_q[X_1, \dots, X_n],$$

where $\mathbb{F}_q$ is a finite field, are the public key polynomials of a multivariate scheme, then to send a message $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ to Bob, Alice computes

$$c_j = p_j(a_1, \dots, a_n) \qquad j = 1, \dots, m$$

and transmits the ciphertext $\mathbf{c} = (c_1, \dots, c_m) \in \mathbb{F}_q^m$ to Bob.

Bob's secret key is a trapdoor: information that allows him to recover $\mathbf{a}$ from $\mathbf{c}$ efficiently. Consequently, the system of polynomial equations formed by the public-key polynomials must have some special structure. The NP-hardness of solving random systems of polynomial equations of degree greater than one therefore does not guarantee that systems with the particular structure induced by a cryptosystem are also hard to solve.

Because the public key is a set of polynomials, *algebraic cryptanalysis*—attacks that attempt to solve systems of polynomial equations derived from the scheme's structure—is especially relevant to multivariate schemes. Gröbner-basis computation is a central tool for such attacks. Computing a lexicographic Gröbner basis of

$$I = \langle p_1 - c_1, \ldots, p_m - c_m \rangle$$

allows one to find the solutions – in the algebraic closure of $\mathbb{F}_q$ – of the system

$$p_1(X_1, \ldots, X_n) - c_1 = 0,\ \ldots,\ p_m(X_1, \ldots, X_n) - c_m = 0.$$

The solutions over $\mathbb{F}_q$ can be computed by adding the field equations $X_i^q - X_i$ to I. However, the average-case complexity of computing a Gröbner basis is exponential in the number of variables, and its worst-case complexity is doubly exponential.

This explains the interest in understanding the performance of Gröbner-basis algorithms on systems that arise in cryptography: complexity estimates are often given for generic systems and provide upper bounds for Gröbner-basis computation. Equations produced by concrete schemes typically exhibit additional algebraic structure that can be exploited; consequently, systems that appear intractable according to generic-parameter estimates may become solvable in practice.

In this thesis we focus on a family of multivariate schemes called DME schemes. They have a layered construction—typical of secret-key schemes—that combines linear (or affine) maps with a class of nonlinear maps known as *monomial maps* in algebraic geometry; we will refer to these as *exponential maps*. Unlike many other multivariate candidates, the public-key polynomials in DME have very high degree but are very sparse, which keeps the public-key size reasonable.

The first scheme in this family was submitted by I. Luengo, M. Avendaño and M. Marco to the NIST standardization competition as a full encryption and signature scheme. In 2021 a structural attack by [4] recovered a private key—often referred to as an *equivalent private key* because it may differ from the one originally used to compute the public key—from a given public key. In that version the nonlinear maps were public; the attack recovered the linear map of each layer (starting from the last) by exploiting syzygies that arose from the scheme's structure.

Contributions

In Sections 3.1, 3.3 and 3.4 we define a new DME variant. This version appeared in the publication:

Dme: a full encryption, signature and KEM multivariate public key cryptosystem. Ignacio Luengo, Martín Avendaño and Pilar Coscojuela. In International Conference on Post-Quantum Cryptography, pages 379–402. Springer, 2023.

We impose relations between the nonlinear maps of different layers; these relations eliminate the syzygies used by the previous attack. Additionally, only the structure of the matrices that define the nonlinear maps is public, not the exact values of their entries. A new structural attack on an instance of this version was later found in [2]. They were able to first compute equivalent matrices for the nonlinear maps and then recover the linear maps layer by layer by computing Gröbner bases of systems derived from the scheme.

This led us to consider further modifications: the DME-minus versions, which are obtained by applying the "minus" modification (used previously in schemes such as Imai–Matsumoto to prevent Patarin's linearization attack): some of the public polynomials are removed from the public key.

By construction, the N polynomials $p_1, \dots, p_N \in \mathbb{F}_q[X_1, \dots, X_N]$ that define the public key share their supports in pairs. Equivalently, we can view the public key as $n = N/2$ polynomials

$$P_1(X_1, \dots, X_N), \dots, P_n(X_1, \dots, X_N) \in \mathbb{F}_{q^2}[X_1, \dots, X_N], \qquad P_i = p_{2i-1} + u, p_{2i},\ i = 1, \dots, n,$$

where $\{1, u\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Different minus versions of DME arise depending on which public polynomials are removed. Analogous systems of equations—now over $\mathbb{F}_q$—can be derived from the public polynomials of the minus versions to recover an equivalent public key.

Although the systems are similar, the solving strategies must differ. In the original DME scheme, once $\mathbf{L}$ is recovered one can compute $(\mathbf{L} \circ \mathbf{E})^{-1}(\mathbf{c})$. In a DME-minus variant the ciphertext is $\mathbf{c}^-$, obtained from $\mathbf{c}$ by removing some components, so recovering $\mathbf{L}$ is not sufficient by itself; a different reconstruction strategy is required.

Our main contributions are:

- We define a framework to systematically study the complexity of structural attacks against different versions of DME. We show that the bottleneck in these attacks is the complexity of computing Gröbner bases of certain *generalized determinantal ideals*—ideals generated by all minors of a fixed order of a matrix whose entries are multivariate polynomials. We use these ideals to:

  - recover the values of what we call the *collision variables*. In Chapter 4 the generalized determinantal ideals correspond to minors of order 2, while in Chapter 5 they correspond to minors of order 3.
  - In Chapter 5 we also use these ideals to recover the coefficients of the missing polynomials. In that case we first compute the Gröbner basis over $\mathbb{F}_{q^2}$ of a generalized determinantal ideal and then compute the Gröbner basis of its Weil descent over $\mathbb{F}_q$.

    When the matrix defining the nonlinear map has exactly two nonzero entries per row, polynomials of degree up to $2^{\lfloor k/2 \rfloor}$ (for $q = 2^k$) can appear as entries of the matrix whose minors we consider; in such instances Gröbner-basis computations may not finish, and ad hoc modelling (as in Section 5.3.1) is necessary. However, as soon as there are more than two nonzero entries per row, large degrees do not appear, since we can treat each component separately. See Section 5.3 for details.

  Complexity results for computing Gröbner bases of generalized determinantal ideals are given in [1, Chapter 3]; those results hold for generic instances.

  Although one might expect generalized determinantal ideals arising from DME or DME-minus instances to be non-generic, in our experiments (where we specialized as many variables as possible to obtain a zero-dimensional ideal) the ideals exhibited the expected dimension. This specialization may explain the generic-like behaviour, but further study is needed.

- Building on [1], we observe that, in general, the complexity of computing a Gröbner basis of a generic generalized determinantal ideal is exponential in the number of equations and variables. For the systems arising from DME schemes we present a method that drastically reduces the support of the public-key polynomials. This reduction decreases both the number of variables and the number of equations in the derived systems. If the reduction is excessive, however, the generalized determinantal ideal may become positive-dimensional over $\overline{\mathbb{F}_q}$, making it difficult to extract solutions over $\mathbb{F}_q$. We therefore need to establish a trade-off between reducing the system size and preserving zero-dimensionality.

- In Proposition 2.34 and Proposition 2.35 we show that, for some parameter regimes, the complexity of computing a Gröbner basis of generalized determinantal ideals becomes polynomial. These result appears in:

  On the Complexity of the Relative Eigenvector Problem.
  P. Coscojuela, K. Mahavadi, L. Perret, A. Ryba and S. Samardjiska.
  Proceedings of the 50th International Symposium on Symbolic and Algebraic Computation (ISSAC 2025).

In the final chapter we present partial results obtained for other versions defined in Chapter 3, those are DME$^+$, DME over $\mathbb{F}_q$ and DME$_\mathrm{w}$. An analysis of the security of those schemes based on the techniques we have presented are future work.

Chapter 1

Multivariate cryptography and Gröbner Bases

In this chapter, we provide an overview of multivariate cryptography, one of the principal post-quantum alternatives to classical public-key cryptography. We also review the paddings used in the RSA scheme for encryption and digital signatures, since slight modifications of these will be used in the DME scheme. Moreover, we recall the definitions of the Hilbert function and the Hilbert series for both affine and homogeneous ideals. Finally, we present the classical theory of Gröbner bases and their computation, and explain how they can be used to solve systems of polynomial equations.

1.1 Post quantum era and Multivariate cryptography

The discovering of Shor's algorithm, a quantum algorithm that solves integer factorization and discrete logarithm problem in polynomial time, motivates the necessity to create new cryptosystem based on hard problems that, dislike factorization of integers and the discrete logarithm problem, are believed to remain safe in presence of a quantum computer. These new schemes are called post quantum schemes, and although they can be implemented on a classical computer, its security is not known to be undermined by a quantum computer. There exists five families of post quantum public key schemes:

- Code-based cryptosystems.
- Lattice-based cryptosystems.
- Multivariate cryptosystems.

- Isogeny-based cryptosystems.
- Hash-based signatures.

The property that characterizes multivariate primitives is that the public key is a set of multivariate polynomials over a finite field $\mathbb{F}_q$ of q elements. There are two main constructions of multivariate schemes: the bipolar construction and the mixed construction. We briefly describe them here; for a more detailed exposition, see [5, Chapter 2].

Bipolar construction

To construct a cryptographic primitive with the bipolar approach, a polynomial map

$$\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m,$$

whose components are multivariate (quadratic) polynomials in n variables, and two invertible affine maps,

$$\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m,\ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

are chosen and form the private key. The public key is the polynomial map

$$\mathcal{P} = \mathcal{S}\ o\ \mathcal{F}\ o\ \mathcal{T}.$$

Depending on whether the map $\mathcal{P}$ is injective, surjective or bijective it can be used to either an encryption scheme, digital signature scheme or both.

If $m \geq n$ then we get an encryption scheme. Given a message $\mathbf{a} \in \mathbb{F}_\mathbf{q}^\mathbf{n}$, one computes $\mathcal{P}(\mathbf{a}) = \mathbf{c}$, and $\mathbf{c} \in \mathbb{F}_\mathbf{q}^\mathbf{m}$ is the ciphertext of the message $\mathbf{a}$. To decrypt the ciphertext, one computes $\mathbf{x} = \mathcal{S}^{-\mathbf{1}}(\mathbf{c})$, then $\mathbf{y} = \mathcal{F}^{-\mathbf{1}}(\mathbf{x})$ and $\mathbf{a} = \mathcal{T}^{-\mathbf{1}}(\mathbf{y})$. The condition $m \geq n$ implies that $\mathbf{x}$ has unique preimage under $\mathcal{F}$.

To design a signature scheme we need $m \leq n$. To sign a message $\mathbf{a}$, we first hash it by using a hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{F}_q^m$, that is $\mathbf{h} = \mathcal{H}(\mathbf{a})$ and compute $\mathbf{x} = \mathcal{S}^{-\mathbf{1}}(\mathbf{h})$, $\mathbf{y} = \mathcal{F}^{-\mathbf{1}}(\mathbf{x})$, $\mathbf{s} = \mathcal{T}^{-\mathbf{1}}(\mathbf{y})$. And $\mathbf{s} \in \mathbb{F}_\mathbf{q}^\mathbf{n}$ is the signature of the message $\mathbf{a}$. Given a signature $\mathbf{s}$ for a message $\mathbf{a}$, to verify if it is a valid signature of $\mathbf{a}$, the verifier check if $\mathcal{P}(\mathbf{s}') = \mathbf{h}$ where $\mathbf{h} = \mathcal{H}(\mathbf{a})$. The hypothesis $m \leq n$ is needed to make sure that a preimage of $\mathbf{x}$ under $\mathcal{F}$ does exist.

Mixed construction

On the other hand, schemes of the mixed type take as private key a quadratic map $\mathcal{F} : \mathbb{F}_q^{n+m} \to \mathbb{F}_q^m$ such that for each $\mathbf{x} \in \mathbb{F}_q^n$, the map $\mathcal{F}(\mathbf{x}, \cdot)$ is linear and for each $\mathbf{y} \in \mathbb{F}_q^m$ the map $\mathcal{F}(\cdot,\mathbf{y})$ can be inverted efficiently, two affine maps $\mathcal{S}:\mathbb{F}_q^m\to\mathbb{F}_q^m,\mathcal{T}:\mathbb{F}_q^n\to\mathbb{F}_q^n$ and an invertible linear map $\mathcal{L}:\mathbb{F}_q^m\to\mathbb{F}_q^m$. The public key is

$$\mathcal{P}=\mathcal{L}\circ\mathcal{F}\circ(\mathcal{S}\times\mathcal{T}).$$

If $m\geq n$ we get an encryption scheme. To encrypt a message $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_q^n$, one solves the linear system

$$\mathcal{P}(a_1,\ldots,a_n,y_1,\ldots,y_m)=(0,\ldots,0).$$

The solution $\mathbf{c}=(c_1,\ldots,c_m)$ is the ciphertext of the message $\mathbf{a}$. To decrypt, one computes $\mathcal{T}(\mathbf{c})=\mathbf{y}$. Then one solves

$$\mathcal{F}(x_1,\ldots,x_n,y_1,\ldots,y_m)=(0,\ldots,0),$$

which can be done efficiently by construction of the scheme. Finally, one computes the plaintext as $\mathbf{a}=\mathcal{S}^{-1}(\mathbf{x})$ that is unique because $m\geq n$.

If $m\leq n$ then we get a signature scheme. Let $\mathbf{a}$ a message and $\mathbf{h}=\mathcal{H}(\mathbf{a})$ being $\mathcal{H}$ a hash function. First one computes $\mathbf{y}=\mathcal{T}(\mathbf{h})$ and solves

$$\mathcal{F}(x_1,\ldots,x_n,y_1,\ldots,y_m)=(0,\ldots,0).$$

By construction a solution $\mathbf{x}$ of this system can be efficiently found. The signature of the message $\mathbf{a}$ is $\mathbf{s}=\mathcal{S}^{-1}(\mathbf{x})$. To verify a signature $\mathbf{s}\in\mathbb{F}_q^n$, one computes the hash of $\mathbf{a}$, that is $\mathbf{d}=\mathcal{H}(\mathbf{a})$ and evaluates

$$\mathcal{P}(s_1,\ldots,s_n,h_1,\ldots,h_m).$$

If the result is $(0,\ldots,0)\in\mathbb{F}_q^m$, the signature is accepted, otherwise is rejected.

Security

The security of multivariate primitives rely on:

- Solving a random system of nonlinear multivariate polynomial equations over a finite field is NP-complete, even in the simple case of quadratic equations over the finite field $\mathbb{F}_2$ (see [6]).
- It is not clear how hard it is to solve the isomorphism problem that in its more general version can be formulated as: Fix a class $\mathcal{C}$ of nonlinear multivariate system and a

nonlinear multivariate system $\mathcal{P}$ which can be written as $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ where $\mathcal{S}, \mathcal{T}$ are affine maps and $\mathcal{F} \in \mathcal{C}$. Find a decomposition of $\mathcal{P}$ of the form $\mathcal{P} = \mathcal{S}' \circ \mathcal{F}' \circ \mathcal{T}'$ with $\mathcal{S}', \mathcal{T}'$ affine maps and $\mathcal{F}' \in \mathcal{C}$

Moreover, there is no hint that quantum computers can solve the problem efficiently.

Finally we argue the advantages and disadvantages of multivariate with respect to other families of post-quantum schemes. The main drawbacks are the large size of public and private key and the lack of security proofs for most of the schemes. This results in the fact that parameters are fixed to be secure against relevant attack. Nevertheless, this is a common feature of the chosen parameters in cryptographic applications. In the case of other types of primitives for which there are security reductions (usually not tight), choosing parameters to have security proof results in an inefficient performance.

1.2 Padding in RSA

Padding is applied before encryption or signing, and its purpose is to format the data so it can be used as input to an encryption or signature scheme. Because it adds randomness, the resulting scheme is non-deterministic, which is an essential security property. We describe here which are used for RSA : the OAEP is used for encryption and PSS000 for digital signature.

Encryption padding: Optimal Asymmetric Encryption Padding (OAEP)

If we zero padding to obtain the required message length, the resulting scheme is deterministic and therefore not even IND-CPA secure. To achieve CPA security, PKCS#1 v1.5 encryption padding was introduced. If IND-CCA security is required, RSA-OAEP should be used. The description given below is from [7, Section 12.8.4].

The OAEP padding scheme was proposed by Bellare and Rogaway in 1994. It is a pair of efficient algorithms (P, U),

$$P : \mathcal{M} \times \mathcal{R} \to \mathcal{X},\ U : \mathcal{X} \to \mathcal{M} \cup \{\text{reject}\},$$

where $\mathcal{R} := \{0,1\}^h$ and $\mathcal{X} := 0^8 \times \{0,1\}^{t-8}$ and $U(x) = m$ if $P(m,r)$ for some r and reject otherwise. We assume that t and h are multiples of eight so that lengths can be measured in bytes. In order to accommodate a t-bit RSA modulus, we insist that the left-most 8 bits of any element in $\mathcal{X}$ are zero. The message space $\mathcal{M}$ consists of all bit strings whose length is a multiple of 8, but at most $t - 2h - 16$.

The scheme also uses two hash functions H and W, where

$$H : \{0,1\}^{t-h-8} \times \mathcal{R} \longrightarrow \mathcal{R}, \qquad W : \mathcal{R} \longrightarrow \{0,1\}^{t-h-8}.$$

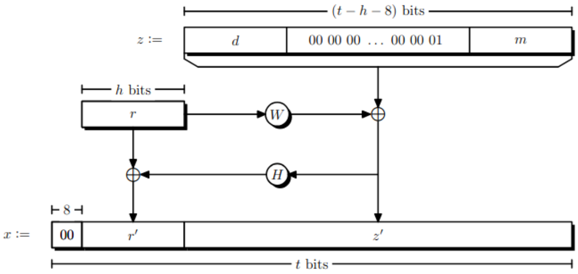
The set $\mathcal{R}$ should be sufficiently large to be beyond the range of a collision resistant hash. Typically, SHA256 is used as the function H and we set $h = 256$. The function W is derived from SHA256.

OAEP padding is used to build a public-key encryption scheme with associated data (see [7, Section 12.7]). As such, the padding algorithm P takes an optional input $d \in \mathcal{R} = \{0,1\}^h$, representing the associated data. To support associated data that is more than h bits long one can first hash the associated data using a collision resistant hash to obtain an element of $\mathcal{R}$. If no associated data is provided as input to P, then d is set to a constant that identifies the hash function H, as specified in the standard. For example, for SHA256, one sets d to the following 256-bit hex value:

$$d := \texttt{E3B0C442 98FC1C14 9AFBF4C8 996FB924 27AE41E4 649B934C A495991B 7852B855}.$$

Every pair of digits in the figure 1.1 represents one byte (8 bits). The variable length string of zeros in z is chosen so that the total length of z is exactly $(t - h - 8)$ bits. The algorithm outputs an $x \in \mathcal{X}$.

FIGURE 1.1: Algorithm P of OAEP from [7].



The inverse algorithm U: On input $x \in \mathcal{X}$ and $d \in \mathcal{R}$, proceed as follows:

1. Parse x as $(00 \,\|\, r' \,\|\, y)$ where $r' \in \mathcal{R}$ and $y \in \{0,1\}^{t-h-8}$. If x cannot be parsed this way, set $m \leftarrow \textsf{reject}$.

2. Compute $r \leftarrow r' \oplus H(y)$ and $z \leftarrow y \oplus W(r)$.

3. Parse z as $(d \,\|\, 00 \cdots 01 \,\|\, m)$ where $d \in \mathcal{R}$ and $m \in \mathcal{M}$. If z cannot be parsed this way, set $m \leftarrow \textsf{reject}$.

4. Output m.

Finally, the public-key encryption scheme RSA-OAEP is obtained by combining the RSA trapdoor function with the OAEP padding scheme, as follows:

- To encrypt a message m: choose $r \in \mathcal{R}$, compute $P(m, r) = x$ and encrypt x using RSA algorithm.
- To decrypt c: compute x with the inverse of RSA algorithm and then compute $m = U(x)$.

PSS00

The first version of RSA-Probabilistic Signature Scheme (RSA-PSS) as defined by Bellare and Rogaway is PSS96. The modified variant of PSS96 that was standardised by the IEEE is known as PSS00. While PSS00 has the same parameters as PSS96, there are some differences. The parameter ℓ_G is now defined as $\ell_G = \lambda - \ell_H - 9$. Additionally, due to the changes in the order of hash functions, we have $G_2(x) = \text{LSBs}(G(x), \ell_R + 1)$ and $G_1(x) = \text{MSBs}(G(x), \ell_G - \ell_R - 1)$. More details on this padding scheme can be found in [8].

1.3 Hilbert series and dimension of an ideal

The proofs of the results we state here can be found in [9]. We use the convention that the zero polynomial has degree -1 and that the zero ideal has Krull dimension -1.

Definition 1.1. Let $I \subset \mathbb{K}[X_1, \dots, X_n]$ be a proper ideal. We define the *dimension of* I as the Krull dimension of the ring $\overline{\mathbb{K}}[X_1, \dots, X_n]/I$.

For $d \in \mathbb{Z}_{\geq}0$, let

$$\mathbb{K}[X_1, \dots, X_n]_{\leq d} := \{f \in \mathbb{K}[X_1, \dots, X_n] \mid \deg(f) \leq d\}.$$

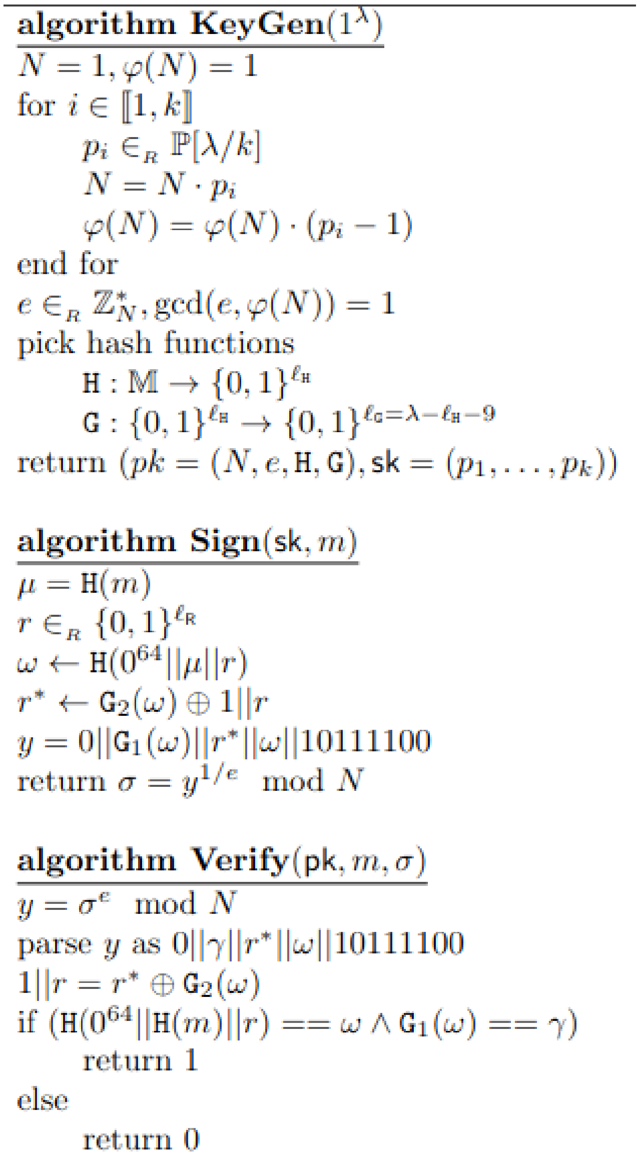
Then, given $I \subseteq \mathbb{K}[X_1, \dots, X_n]$ let

$$I_{\leq d} := I \cap \mathbb{K}[X_1, \dots, X_n]_{\leq d}.$$

$$I_{\leq d} := \{f \in I \mid f \in \mathbb{K}[X_1, \dots, X_n],\ \deg(f) \leq d\}.$$

Note that $\mathbb{K}[X_1, \dots, X_n]_{\leq d}$ is finite-dimensional as a $\mathbb{K}$-vector space and $I_{\leq d}$ is a subspace of $\mathbb{K}[X_1, \dots, X_n]_{\leq d}$.

Figure 1.2: Algorithm PSS00 from [8].



```
algorithm KeyGen($1^\lambda$)
$N = 1, \varphi(N) = 1$
for $i \in [\![1, k]\!]$
    $p_i \in_R \mathbb{P}[\lambda/k]$
    $N = N \cdot p_i$
    $\varphi(N) = \varphi(N) \cdot (p_i - 1)$
end for
$e \in_R \mathbb{Z}_N^*, \gcd(e, \varphi(N)) = 1$
pick hash functions
    $\mathtt{H} : \mathbb{M} \to \{0,1\}^{\ell_{\mathtt{H}}}$
    $\mathtt{G} : \{0,1\}^{\ell_{\mathtt{H}}} \to \{0,1\}^{\ell_{\mathtt{G}} = \lambda - \ell_{\mathtt{H}} - 9}$
return $(pk = (N, e, \mathtt{H}, \mathtt{G}), \mathsf{sk} = (p_1, \ldots, p_k))$

algorithm Sign($\mathsf{sk}, m$)
$\mu = \mathtt{H}(m)$
$r \in_R \{0,1\}^{\ell_{\mathtt{R}}}$
$\omega \leftarrow \mathtt{H}(0^{64}||\mu||r)$
$r^* \leftarrow \mathtt{G}_2(\omega) \oplus 1||r$
$y = 0||\mathtt{G}_1(\omega)||r^*||\omega||10111100$
return $\sigma = y^{1/e} \mod N$

algorithm Verify($\mathsf{pk}, m, \sigma$)
$y = \sigma^e \mod N$
parse $y$ as $0||\gamma||r^*||\omega||10111100$
$1||r = r^* \oplus \mathtt{G}_2(\omega)$
if $(\mathtt{H}(0^{64}||\mathtt{H}(m)||r) == \omega \wedge \mathtt{G}_1(\omega) == \gamma)$
    return 1
else
    return 0
```

Definition 1.2. The affine Hilbert function of I is defined as: $\mathrm{HF}^a_{\mathbb{K}[X_1,\ldots,X_n]/I} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$,

$$\mathrm{HF}^a_{\mathbb{K}[X_1,\ldots,X_n]/I}(d) = \dim_{\mathbb{K}}(\mathbb{K}[X_1,\ldots,X_n]_{\leq d}/I_{\leq d}) = \dim_{\mathbb{K}}(\mathbb{K}[X_1,\ldots,X_n]_{\leq d}) - \dim_{\mathbb{K}}(I_{\leq d}).$$

The affine Hilbert series of I is defined as the formal power series

$$\mathrm{HS}^a_{\mathbb{K}[X_1,\ldots,X_n]/I}(t) = \sum_{d=0}^{\infty} \mathrm{HF}^a_{\mathbb{K}[X_1,\ldots,X_n]/I}(d) t^d \in \mathbb{Z}[[t]].$$

Theorem 1.3. *Let $I \subseteq \mathbb{K}[X_1,\ldots,X_n]$ be an ideal. Then the Hilbert series can be written as*

$$HS^a_{\mathbb{K}[X_1,\ldots,X_n]/I} = \frac{N(t)}{(1-t)^{n+1}}, \quad \textit{for } N(t) = a_0 + a_1 t + \ldots + a_k t^k \in \mathbb{Z}[t].$$

Moreover, $HF^a_{\mathbb{K}[X_1,\ldots,X_n]/I}$ is a polynomial for large d. More precisely, the polynomial

$$p(X) = \sum_{i=0}^{k} a_i \binom{X+n-i}{n} \in \mathbb{Q}[X]$$

satisfies $HF^a_{\mathbb{K}[X_1,\ldots,X_n]/I}(d) = p(d)$ for all $d \geq d_0$, for some $d_0 \in \mathbb{Z}_{\geq 0}$.

Definition 1.4. The polynomial $p(X)$ defined in the previous theorem is called the affine Hilbert polynomial of I, and will be denoted as $\mathrm{HP}^a_{\mathbb{K}[X_1,\ldots,X_n]/I}$.

Although the affine Hilbert function and the affine Hilbert series depends on the generators of the ideal I, the degree of the affine Hilbert polynomials does not (cf. Lemma 11.12, [9])

Theorem 1.5. *Let $I \subseteq \mathbb{K}[X_1,\ldots,X_n]$. Then*

$$\deg(HP^a_{\mathbb{K}[X_1,\ldots,X_n]/I}) = \dim(I).$$

When the ideal $I \subseteq \mathbb{K}[X_1,\ldots,X_n]$ is homogeneous, we consider

$$\mathbb{K}[X_1,\ldots,X_n]_d := \{f \in \mathbb{K}[X_1,\ldots,X_n] :\ f \text{ is homogeneous and } \deg(f) = d\}$$

and $I_d = I \cap \mathbb{K}[X_1,\ldots,X_n]_d$.

Definition 1.6. The Hilbert function of I is defined as: $\mathrm{HF}_{\mathbb{K}[X_1,\ldots,X_n]/I} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$,

$$\mathrm{HF}_{\mathbb{K}[X_1,\ldots,X_n]/I}(d) = \dim_{\mathbb{K}}(\mathbb{K}[X_1,\ldots,X_n]_d/I_d) = \dim_{\mathbb{K}}(\mathbb{K}[X_1,\ldots,X_n]_d) - \dim_{\mathbb{K}}(I_d).$$

The Hilbert series of I is defined as the formal power series

$$\mathrm{HS}_{\mathbb{K}[X_1,\ldots,X_n]/I}(t) = \sum_{d=0}^{\infty} \mathrm{HF}_{\mathbb{K}[X_1,\ldots,X_n]/I}(d) t^d \in \mathbb{Z}[[t]].$$

Remark 1.7. Note that:

$$\mathbb{K}[X_1,\ldots,X_n]_{\leq d} = \bigoplus_{i=0}^{d} \mathbb{K}[X_1,\ldots,X_n]_i.$$

Then, if $I \subseteq \mathbb{K}[X_1,\ldots,X_n]$ is a homogeneous ideal, $\mathrm{HF}_{\mathbb{K}[X_1,\ldots,X_n]/I} = (1-t)\mathrm{HF}^a_{\mathbb{K}[X_1,\ldots,X_n]/I}$. Consequently $\dim(I) = deg(\mathrm{HP}_{\mathbb{K}[X_1,\ldots,X_n]/I}) - 1$ where $\mathrm{HP}_{\mathbb{K}[X_1,\ldots,X_n]/I} = (1-t)\mathrm{HP}^a_{\mathbb{K}[X_1,\ldots,X_n]/I}$.

1.4 Orders on $\mathbb{T}^n$ and the Division Algorithm in $\mathbb{K}[X_1, \dots, X_n]$

Definition 1.8. A monomial $\mathbf{X}^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ with $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ is called a *term*. The set of all terms of $\mathbb{K}[X_1, \dots, X_n]$ is denoted by $\mathbb{T}^n$. Given $f = \sum_\alpha c_\alpha \mathbf{X}^\alpha \in \mathbb{K}[X_1, \dots, X_n]$ we call the support of f, $\mathrm{Supp}(f)$, the set

$$\mathrm{Supp}(f) = \{\mathbf{X}^\alpha : c_\alpha \neq 0\}.$$

In $\mathbb{T}^1$ there is a natural order given by

$$X^i > X^j \iff i > j.$$

However, it is not so clear how to order the elements of $\mathbb{T}^n$ for $n > 1$.

Let us list some desirable properties:

- For any polynomial in $\mathbb{K}[X_1, \dots, X_n]$, we want to totally order its terms. That is, it should be a total order.

- It is a generalization of the order in $\mathbb{K}[X]$, so it is reasonable to ask that

$$\mathbf{X}^\alpha > \mathbf{X}^\beta \implies \mathbf{X}^\gamma \mathbf{X}^\alpha > \mathbf{X}^\gamma \mathbf{X}^\beta$$

Definition 1.9. A *term order* $>$ on $\mathbb{T}^n$ is a relation on $\mathbb{T}^n$ satisfying:

1. It is a total order on $\mathbb{T}^n$.

2. If $\mathbf{X}^\alpha > \mathbf{X}^\beta$ then $\mathbf{X}^\gamma \mathbf{X}^\alpha > \mathbf{X}^\gamma \mathbf{X}^\beta$.

3. It is a well-order, i.e., every non-empty subset of $\mathbb{T}^n$ has a minimal element with respect to $>$.

The following lemma will be key to proving that the algorithms terminate in a finite number of steps.

Lemma 1.10. *If $>$ is a term order on $\mathbb{T}^n$, then every strictly decreasing sequence of elements in $\mathbb{T}^n$ is finite.*

Proof. This follows from [10, Lemma 2, p. 56]. □

Remark 1.11. The concepts of monomial and term are frequently interchanged in the literature, so it is advisable to pay attention to the conventions used by each author. Accordingly, the notion defined in Definition 1.9 is referred to as term order or monomial order. We use the notation according to [11] and [12]. However, [10] and the MAGMA programming language use the opposite convention.

Example 1.1. *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n)$ and $|\alpha| = \sum_{i=1}^n \alpha_i$, $|\beta| = \sum_{i=1}^n \beta_i$. Some terms orders on $\mathbb{T}^n$ are:*

- ***Lexicographic Order:*** $\mathbf{X}^\alpha >_{\text{LEX}} \mathbf{X}^\beta$ *if* $\alpha_m - \beta_m > 0$ *where* $m = \min\{i \ : \ \alpha_i - \beta_i \neq 0\}$.
- ***Graded Lexicographic Order:*** $\mathbf{X}^\alpha >_{\text{DLEX}} \mathbf{X}^\beta$ *if*
$$\begin{aligned} &|\alpha| > |\beta| \quad \textit{or} \\ &|\alpha| = |\beta| \quad \textit{and} \quad \mathbf{X}^\alpha >_{\text{LEX}} \mathbf{X}^\beta \end{aligned}$$
- ***Graded Reverse Lexicographic Order:*** $\mathbf{X}^\alpha >_{\text{DRL}} \mathbf{X}^\beta$ *if*
$$\begin{aligned} &|\alpha| > |\beta| \quad \textit{or} \\ &|\alpha| = |\beta| \quad \textit{and} \quad \alpha_M - \beta_M < 0 \quad \textit{where} \quad M = \max\{i \ : \ \alpha_i - \beta_i \neq 0\} \end{aligned}$$

Once an order is fixed, we can extend the concepts of leading monomial and degree of a polynomial to the multivariate case.

Definition 1.12. Let $0 \neq f \in \mathbb{K}[X_1, \dots, X_n]$, $f = \sum_\alpha c_\alpha \mathbf{X}^\alpha$, and $<$ an order on $\mathbb{T}^n$.

- The *total degree of* f is $\deg(f) = \max\{|\alpha| \ : \ c_\alpha \neq 0\}$.
- The *multidegree of* f is $\text{multideg}(f) = \max_>\{\alpha : c_\alpha \neq 0\}$.
- The *leading monomial of* f is $\text{LM}(f) = \text{LC}(f) \cdot \text{LT}(f)$ where $\text{LC}(f) = c_{\text{multideg}(f)}$ and $\text{LT}(f) = \mathbf{X}^{\text{multideg}(f)}$.

We define now the notion of reduction of a polynomial modulo a set.

Definition 1.13. Let $f, g, p \in \mathbb{K}[X_1, \dots, X_n]$ with $f, p \neq 0$ and let $P = \{p_1, \dots, p_r\}$ be a subset of $\mathbb{K}[X_1, \dots, X_n]$.

1. f *reduces to* g *modulo* p, $f \underset{\text{p}}{\rightarrow} g$, if there exists t, a monomial of f, such that $t = s \cdot \text{LT}(p)$ and
$$g = f - \frac{\text{LC}(t)}{\text{LC}(p)} \cdot s \cdot p.$$
2. f *reduces to* g *modulo* P, $f \underset{\text{P}}{\rightarrow} g$, if $f \underset{\text{p}}{\rightarrow} g$ for some $p \in P$.

3. f is *reducible* modulo p (respectively, modulo P) if there exists $h \in \mathbb{K}[X_1, \ldots, X_n]$ such that $f \underset{\mathrm{p}}{\rightarrow} h$ (respectively, $f \underset{\mathrm{P}}{\rightarrow} h$).

   If f is not reducible modulo P it is said that f is in normal form modulo P. A *normal form* of f modulo P, denoted as $\overline{f}^P$, is a polynomial h that is in normal form modulo P such that $f - h \in \langle P \rangle$ and no term of h is in the ideal $\langle \mathrm{LT}(p_1), \ldots, \mathrm{LT}(p_r) \rangle$.

4. f is *top-reducible* modulo P if there exists $p \in P$ such that $\mathrm{LT}(f) = s \cdot \mathrm{LT}(p)$.

By $\overset{*}{\rightarrow}$ we denote the reflexive-transitive closure of $\rightarrow$.

In the univariate case, if we divide f by g and obtain remainder r, it holds that $r = \overline{f}^g$. Thus, the idea of reduction of a multivariate polynomial generalizes the division algorithm in one variable. There also exists a division algorithm in the multivariate case (cf. [12, p. 71]) which is also a particular case of reduction where the set modulo which we reduce is considered ordered and only top-reductions are allowed.

Proposition 1.14. *Given $f \in \mathbb{K}[X_1, \ldots, X_n]$ and $P \subset \mathbb{K}[X_1, \ldots, X_n]$. In a finite number of reductions of f modulo P we reach a normal form of f modulo P.*

Proof. It follows from the definition of reduction of a polynomial and Lemma 1.10. ([11], Theorem 5.21). □

1.5 Gröbner Bases

Historically, Gröbner basis were devised as an algorithmic approach to solve the ideal membership problem – that is, given an ideal over a polynomial ring, compute a system of generators that allow to determine in a systematic way if a polynomial belongs to the ideal. More generally, to give a basis of the ring $\mathbb{K}[x_1, \ldots, X_n]/I$ regarded as a $\mathbb{K}$-vector space.

In the univariate polynomial ring $\mathbb{K}[X]$, the solutions to both problems are immediate consequence of:

Theorem 1.15. *Let $\mathbb{K}$ be a field, $f, g \in \mathbb{K}[X]$ with $g \neq 0$. Then, there exist unique $q, r \in \mathbb{K}[X]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$ if $r \neq 0$, which can be computed efficiently by the Euclidean algorithm.*

Proposition 1.16. *The ring $\mathbb{K}[X]$ is a principal ideal domain. Given an ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[X]$, then $I = \langle gcd(f_1, \ldots, f_s) \rangle$. The $\gcd$ can be computed efficiently with the extended Euclidean Algorithm.*

Thus, for $f \in \mathbb{K}[X]$, in order that $f \in I$ it is necessary and sufficient that $f = q{\cdot}\gcd(f_1, \ldots, f_s)$.

A basis of $\mathbb{K}[X]/I$ regarded as a $\mathbb{K}$-vector space is

$$\{X + I, \ldots, X^{d-1} + I\}$$

where $d = \deg(\gcd(f_1, \ldots, f_s))$.

When considering $\mathbb{K}[X_1, \ldots, X_n]$, the ring is Noetherian – every ideal is finitely generated – but it is no longer a principal ideal domain; therefore, the univariate strategy to determine polynomial membership does not generalize immediately. A Gröbner basis of I is a generating set of this ideal, that allows to solve those problems in the multivariate setting.

Given $I = \langle f_1, \ldots, f_s \rangle$ a sufficient condition for a polynomial f to be in I is that a normal form of f modulo $\{f_1, \ldots, f_s\}$ is 0. However, it is not necessary as normal forms are not unique.

Example 1.2. *Let $I = \langle F \rangle \subset \mathbb{K}[X_1, \ldots, X_n]$, $f \in \mathbb{K}[X_1, \ldots, X_n]$.*
Consider $f = XY^2 - X, f_1 = XY - 1, f_2 = Y^2 - 1$. Then

$$f = Yf_1 + (-X + Y), \; f = Xf_2$$

therefore $-X + Y, 0$ are both normal forms of f modulo $\{f_1, f_2\}$.

Definition-Proposition 1.17. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$, $I \neq 0$, and fix an order on $\mathbb{T}^n$. We define*

$$LT(I) := \{\mathbf{X}^\alpha : \text{ there exists } 0 \neq f \in I \text{ with } LT(f) = \mathbf{X}^\alpha\}.$$

And $\langle LT(I) \rangle$, the ideal of $\mathbb{K}[X_1, \ldots, X_n]$ generated by the elements of $LT(I)$, is a monomial ideal.

Proposition 1.18. *Let $I = \langle \mathbf{X}^\alpha \; : \; \alpha \in A \rangle$ be a monomial ideal. Then*

$$\mathbf{X}^\beta \in I \iff \mathbf{X}^\beta \text{ is divisible by some } \mathbf{X}^\alpha \text{ with } \alpha \in A.$$

Moreover, the following are equivalent:

1. *f is a polynomial belonging to I.*

2. *Every monomial of f is in I, i.e., f is a $\mathbb{K}$-linear combination of monomials in I.*

Proof. The proof can be found in [10, pp. 70–71]. □

Let $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[X_1, \ldots, X_n]$, $I \neq 0$. Suppose we obtain two representations

$$f = g + r, f = g' + r'$$

with r and r' normal forms of f modulo $\{f_1, \ldots, f_s\}$ and $r \neq r'$. Then

$$r - r' = g - g' \in I \text{ and } \mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle.$$

If we impose

$$\langle \mathrm{LT}(I) \rangle \subseteq \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle,$$

then $\mathrm{LT}(r-r')$ will be in $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$, contradicting the properties that r and r' have for being normal forms of f.

This motivates the following definition:

Definition 1.19. Let $>$ be an order on $\mathbb{T}^n$ and $0 \neq I \subset \mathbb{K}[X_1, \ldots, X_n]$ an ideal. A finite subset $G = \{g_1, \ldots, g_t\}$, $G \subset I$, is a *Gröbner basis of* I if $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$. By convention, $\{\emptyset\}$ is the Gröbner basis of the ideal $\langle 0 \rangle$.

The following theorem guarantees the existence of Gröbner bases for any ideal.

Theorem 1.20. *Fix an order on $\mathbb{T}^n$ and let I be an ideal of $\mathbb{K}[X_1, \ldots, X_n]$. Then there exists a Gröbner basis of I.*

Proof. We can write $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. It suffices to see that $I = \langle g_1, \ldots, g_t \rangle$. Since $g_1, \ldots, g_t \in I$, $\langle g_1, \ldots, g_t \rangle \subset I$. For the other inclusion, let $f \in \langle g_1, \ldots, g_t \rangle$. If we compute a normal forms of f modulo $\{g_1, \ldots, g_t\}$, we obtain $f = q_1 g_1 + \ldots + q_s g_s + r$ with no term of r in $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ if $r \neq 0$. Note that $r = f - q_1 g_1 - \ldots - q_s g_s \in I$, so $\mathrm{LT}(r) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. By Proposition 1.18, $\mathrm{LT}(r)$ is divisible by $\mathrm{LT}(g_i)$ for some $1 \leq i \leq s$. Therefore, $r = 0$ and thus $f \in \langle g_1, \ldots, g_t \rangle$. □

Remark 1.21. In the proof of Theorem 1.20, we have shown that a Gröbner basis of I in particular is a set of generators of I.

From the above, we deduce the following proposition.

Proposition 1.22. *Let $I \subseteq \mathbb{K}[X_1, \ldots, X_n]$ be an ideal and $G = \{g_1, \ldots, g_t\}$ a Gröbner basis of I. Then, given $f \in \mathbb{K}[X_1, \ldots, X_n]$, there exists a unique $r \in \mathbb{K}[X_1, \ldots, X_n]$ satisfying:*

- *No monomial of r is in $\langle LT(g_1), \ldots, LT(g_t) \rangle$.*
- *There exists $g \in I$ such that $f = g + r$.*

In particular, there exists only a normal form of f modulo $\{g_1, \dots, g_t\}$.

Proposition 1.23. *The normal form of a polynomial modulo a Groebner basis does not depend on the Groebner basis.*

Proof. See [12, Proposition 2.4.7]. □

Corollary 1.24. *Let I be a nonzero ideal in $\mathbb{K}[X_1, \dots, X_n]$, $G = \{g_1, \dots, g_s\}$ a Gröbner basis of I and $f \in \mathbb{K}[X_1, \dots, X_n]$. Then f belongs to I if and only if the normal form f modulo G is zero.*

Let $0 \neq I \subset \mathbb{K}[X_1, \dots, X_n]$. If $G = \{g_1, \dots, g_t\} \subset \mathbb{K}[X_1, \dots, X_n] \setminus \{0\}$, denote $\mathrm{LT}(G) = \{\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t)\}$.

Definition 1.25. A Gröbner basis G with respect to $>$ of I is said to be *minimal* if for any $g_i, g_j \in G$ with $g_i \neq g_j$ it holds that $\mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$.

Given a fixed order and an ideal, there exist different minimal Gröbner bases; therefore, for uniqueness, we must impose more conditions. This leads to the notion of reduced Gröbner basis.

Definition 1.26. A Gröbner basis of I with respect to $>$ is reduced if for every $p \in G$, $\mathrm{LT}(p) = 1$ and no monomial of p is in $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Theorem 1.27. *Let $I \neq 0$ be an ideal. Then, for a given order on $\mathbb{T}^n$, there exists a unique* reduced *Gröbner basis of I.*

Proof. See [10, p. 93]. □

To complete this section we state the result that tells us how to compute basis of $\mathbb{K}[X_1, \dots, X_n]/I$.

Theorem 1.28 (Basis Theorem). *Let $I \subset \mathbb{K}[X_1, \dots, X_n]$ be an ideal and $<$ an order on $\mathbb{T}^n$. Let B be the set of all terms in $\mathbb{T}^n \setminus \langle LT(I) \rangle$. Then $\{b + I : b \in B\}$ is a basis of the $\mathbb{K}$-vector space $\mathbb{K}[X_1, \dots, X_n]/I$.*

Proof. See [12, pp. 62–63]. □

Let $f \in \mathbb{K}[X_1, \dots, X_n]$, $I = \langle f_1, \dots, f_s \rangle$ and we want to find the coordinates of $f + I$ with respect to B. We imitate the univariate case, divide f by $(f_1, \dots, f_s)$ and obtain $f = q_1 f_1 + \dots + q_s f_s + r$ where r satisfies that none of its terms are in $\langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s) \rangle$. Let B' be the set of those elements in $\mathbb{T}^n \setminus \langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s) \rangle$. In general, only $\langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s) \rangle \subset \langle \mathrm{LT}(I) \rangle$ holds. Thus, r is a $\mathbb{K}$-linear combination of elements from B' but not necessarily from B. This is true if $\{f_1, \dots, f_s\}$ is a Gröbner basis of I, since in that case $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s) \rangle$. This proves:

Proposition 1.29. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ an ideal, $G = \{g_1, \ldots, g_t\}$ a Gröbner basis of I and $B(G)$ the set of all terms in $\mathbf{t} \in \mathbb{T}^n$ that are not multiples of $LT(g_1), \ldots, LT(g_s)$. Then the set $\{b + I : b \in B(G)\}$ is a basis of the $\mathbb{K}$-vector space $\mathbb{K}[X_1, \ldots, X_n]/I$.*

1.5.1 Computing Gröbner Bases

In the previous section we discussed that Gröbner bases exist. However, since we have to consider every polynomial in I to check Definition 1.19 and Theorem 1.20 is not constructive, we need algorithms to verify when a set of generators of an ideal is indeed a Gröbner basis and to compute a Gröbner basis of an ideal.

To verify whether a set of generators of an ideal is a Gröbner basis, it suffices to check that certain polynomials, called S-polynomials, reduce to zero.

Definition 1.30. Let $f, g \in \mathbb{K}[X_1, \ldots, X_n]$ be non-zero polynomials with $\alpha = \text{multideg}(f), \beta = \text{multideg}(g) \in \mathbb{Z}^n_{\geq 0}$. If we denote $\gamma = \text{lcm}(\text{multideg}(f), \text{multideg}(g))$, we define the *S-polynomial of f and g* as

$$S(f, g) := \text{LC}(g)\frac{\mathbf{X}^\gamma}{\text{LT}(f)}f - \text{LC}(f)\frac{\mathbf{X}^\gamma}{\text{LT}(g)}g.$$

Theorem 1.31 (Buchberger's Criterion)**.** *Let $I \subseteq \mathbb{K}[X_1, \ldots, X_n]$ be an ideal. A system of generators $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if the remainder of the division of $S(g_i, g_j)$ by G is zero for all $1 \leq i < j \leq t$.*

The first algorithm to compute from a set of generator of an ideal a Gröbner Basis is the Buchberger's Algorithm 1. Let $I = \langle f_1, \ldots, f_s \rangle$ an ideal in $\mathbb{K}[X_1, \ldots, X_n]$. The essence of Buchberger's algorithm is as follows: given a subset $G \subset I$ such that $I = \langle G \rangle$, let $g_1, g_2 \in G$ and assume that $\overline{S(g_1, g_2)}^G \neq 0$. Note that by definition $S(g_1, g_2) \in I$ and $S(g_1, g_2) = p + \overline{S(g_1, g_2)}^G$ with $p \in I$, then $\overline{S(g_1, g_2)}^G \in I$. If we add $\overline{S(g_1, g_2)}^G$ to the set G, and denote G_{new} this new set, that is, $G_{\text{new}} = G \cup \{\overline{S(g_1, g_2)}^G\}$, then it holds that $\langle G_{\text{new}} \rangle = I$ and $\overline{S(g_1, g_2)}^{G_{\text{new}}} = 0$.

```
Input: An ordered set $F = \{f_1, \dots, f_s\}$.
Output: A Gröbner basis $G$ of $I = \langle F \rangle$.
$G := F$;
while $G' \neq G$ do
    $G' := G$;
    for every pair $\{f, g\}$ with $f, g \in G'$, $f \neq g$ do
        $r := \overline{S(f,g)}^{G'}$;
        if $r \neq 0$ then
            $G := G \cup \{r\}$;
        end
    end
end
return $G$;
```

Algorithm 1: Buchberger's Algorithm

The termination of the algorithm uses the following result of Noetherian rings:

Theorem 1.32. *Let $I_1 \subsetneq I_2 \subsetneq \dots$ be a sequence of ideals in $\mathbb{K}[X_1, \dots, X_n]$, then there exists a natural number $N \geq 1$ such that $I_j = I_{j+1}$ for all $j \geq N$.*

Some of the reductions to zero can be predicted with the following two criteria:

Lemma 1.33 (First Buchberger's criterion). *Let $f, g \in \mathbb{K}[X_1, \dots, X_n]$ such that*

$$gcd(LT(f), LT(g)) = 1$$

then $S(f,g) \xrightarrow[\{f,g\}]{*} 0$.

Lemma 1.34 (Second Buchberger's criterion). *Let $F \subset \mathbb{K}[X_1, \dots, X_n]$ a finit subset and $g_1, p, g_2 \in \mathbb{K}[X_1, \dots, X_n]$ such that*

1. *$LT(p) \mid lcm(LT(g_1), LT(g_2))$*

2. *$S(g_i, p) \xrightarrow{*} 0$ for $i = 1, 2$.*

Then, it is unnecessary to consider the S-polynomial $S(g_1, g_2)$.

Proof. Implied by [11, Proposition 5.70]. □

When the input $F = \{f_1, \dots, f_s\}$ of Buchberger's Algorithm is a set of homogeneous polynomials, if a graded order of $\mathbb{T}^n$ is chosen, the algorithm computes a d-Gröbner basis, that is, a

Gröbner basis of $I_{\leq d} = I \cap \mathbb{K}[X_1, \ldots, X_n]_{\leq d}$. By Theorem 1.32 there exists $D_0 \in \mathbb{N}$ such that $G_d = G_{D_0}$ for every $d \geq D_0$. Then, G_{D_0} is a Gröbner basis of the ideal.

In the homogeneous case, if $f \xrightarrow{F} r$ and $r \neq 0$ then $\deg(r) = \deg(f)$. Moreover, the property of being homogeneous is also preserved in the computation of the S-polynomial:

Proposition 1.35. *Let f and g homogeneous polynomials. Then, if $S(f,g) \neq 0$, $S(f,g)$ is homogenous of degree* $\deg(lcm(LT(f), LT(g)))$.

From these last two propositions, we deduce that if Buchberger's algorithm is started with a set of homogeneous polynomials F, then all nonzero S-polynomials generated throughout the execution of the algorithm are homogeneous, as well as their remainders upon reduction modulo the current set G at each step.

Moreover, in the homogeneous case, the degree of the S-polynomials allows us to order the pairs in Buchberger's algorithm.

Definition 1.36. Let $F = \{f_1, \ldots, f_s\}$ a set of homogeneous polynomials. Let $i < j$, we define $\deg(i,j) := \deg(\text{lcm}(\text{LT}(f_i), \text{LT}(f_j)))$. Note that if $S(f_i, f_j)$ is non-zero then $\deg(i,j) = \deg(S(f_i, f_j))$.

Definition 1.37. Let $I = \langle f_1, \ldots, f_s \rangle$ with $f_1, \ldots, f_s$ homogeneous polynomials. A finite subset $G \subset I$ satisfying that for every $f \in I$ with $\deg(f) \leq d$, there exists $g \in G$ such that $\text{LT}(g) \mid \text{LT}(f)$, is called a *$d$-Gröbner basis.*

Let F be an ordered set as before. We consider a graded order and the normal selection strategy for pairs in P, that is, choosing the pair $(i,j) \in P$ for which $\text{lcm}(\text{LT}(f_i), \text{LT}(f_j))$ is minimal. Since the order is graded, it follows that such a minimum corresponds exactly to the pair $(i,j) \in P$ for which $\deg(i,j)$ is minimal. Algorithm 2 computes a Gröbner basis of $\langle F \rangle$; moreover, the value taken by m increases at each iteration. Finally, upon completing an iteration for some m the set G obtained is an m-Gröbner basis.

```
**Input:** An ordered set $F = \{f_1, \dots, f_s\}$ of homogeneous polynomials.
**Output:** A Gröbner basis $G$ of $I = \langle F \rangle$.
$P := \{\{f_i, f_j\} : f_i, f_j \in F, f_i \neq f_j, i < j\}$;
$G := F$;
$l := s$;
while $P \neq \emptyset$ do
    $m := \min\{\deg(i,j) : \{f_i, f_j\} \in P\}$;
    $P' := \{\{f_i, f_j\} \in P : \deg(i,j) = m\}$;
    $P := P \setminus P'$;
    while $P' \neq \emptyset$ do
        $\{f_i, f_j\} :=$ first element in $P'$;
        $P' := P' \setminus \{\{f_i, f_j\}\}$;
        $S := \overline{S(f_i, f_j)}^G$;
        if $S \neq 0$ then
            $l := l + 1, f_l := S$;
            $G := G \cup \{f_l\}$;
            $P := P \cup \{\{f_i, f_l\} : 1 \leq i \leq l - 1\}$;
        end
    end
end
return $G$;
```

Algorithm 2: Homogeneous Buchberger's Algorithm

Requiring the ideals we work with to be homogeneous is quite restrictive. Therefore, the next question is: can we adapt or leverage these methods in some way to compute Gröbner bases of ideals generated by arbitrary, not necessarily homogeneous polynomials?

One possibility is to homogenize the generators of the ideal, compute a Gröbner basis— with respect to an *appropriate* order—of the homogeneous ideal they generate using the studied methods, and then dehomogenize that basis. If we want to compute a Gröbner basis with respect to an order $>$, and we homogenize with the variable X_0, the *appropriate* order is the $>_h$ defined in Definition 1.39.

Definition 1.38. Given a polynomial $f \in \mathbb{K}[X_1, \dots, X_n]$, we define the *homogenization of f* as $f^* := X_0^d \cdot f\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right)$, where $d := \deg(f)$.

Given a polynomial $F \in \mathbb{K}[X_0, \dots, X_n]$, we define its *dehomogenization* as $F_* := F(1, X_1, \dots, X_n)$.

For an ideal $I \subset \mathbb{K}[X_1, \dots, X_n]$, we denote by I^* the homogeneous ideal $I^* = \langle f^* : f \in I \rangle$.

If $I = \langle f_1, \ldots, f_s \rangle$, it holds that $\langle f_1^*, \ldots, f_s^* \rangle \subset I^*$, but in general this inclusion is strict. Let $J = \langle f_1^*, \ldots, f_s^* \rangle$. If we compute the reduced Gröbner basis of J with respect to an appropriate order, then dehomogenizing it yields a Gröbner basis of I.

Definition 1.39. Let $>$ be an order on $\mathbb{T}^n$. We define the order $>_h$ as $\mathbf{X}^\alpha X_0^a >_h \mathbf{X}^\beta X_0^b \iff \mathbf{X}^\alpha > \mathbf{X}^\beta \quad \text{or} \quad \big(\mathbf{X}^\alpha = \mathbf{X}^\beta \text{ and } a > b\big)$.

Proposition 1.40. *Let G be the reduced Gröbner basis of $J = \langle f_1^*, \ldots, f_s^* \rangle$ with respect to the order $>_h$. Then, the dehomogenization G_* is a Gröbner basis of $I = \langle f_1, \ldots, f_s \rangle$ with respect to the order $>$.*

Proof. See [11, Lemma 10.57]. □

Algorithms using linear algebra and Matrix F_5

This section shows that the homogeneous Buchberger's Algorithm can be seen as performing row operations in certain matrices, called Macaulay matrices.

Lemma 1.41. *Let $I = \langle f_1, \ldots, f_s \rangle$ with f_i, $i = 1, \ldots, s$ homogeneous polynomials and let $m \in \mathbb{Z}_{\geq 0}$ be fixed. Then every element of I_m is a linear combination with coefficients in $\mathbb{K}$ of polynomials of the form $\mathbf{X}^\alpha f_i$ with $|\alpha| + \deg(f_i) = m$.*

That is, $S_m := \{\mathbf{X}^\alpha f_i : |\alpha| + \deg(f_i) = m\}$ is a generating set of I_m viewed as a $\mathbb{K}$-vector space. We fix an order on $\mathbb{T}^n$, denote by T_m the set of all terms of total degree m, and order them in decreasing order with respect to the fixed order.

Remark 1.42. Let $\mathbf{X}^\alpha f_i$ with $|\alpha| + \deg(f_i) = m$. Since f_i is homogeneous of degree $\deg(f_i)$, f_i can be uniquely written as a sum of distinct monomials all of degree $\deg(f_i)$. Therefore, $\mathbf{X}^\alpha f_i$ can be uniquely written as a $\mathbb{K}$-linear combination of terms in T_m.

For each m, we construct a matrix with entries in $\mathbb{K}$ of size $|S_m| \times |T_m|$, called the Macaulay matrix of $F = (f_1, \ldots, f_s)$ of degree m with respect to $>$.

Definition 1.43 (Macaulay matrix)**.** Let $>$ be an order on $\mathbb{T}^n$, and let $F = (f_1, \ldots, f_m) \in (\mathbb{K}[X_1, \ldots, X_n])^m$ be homogeneous polynomials of degrees $(d_1, \ldots, d_m)$. The *Macaulay matrix* of F of degree D is the matrix $\mathrm{Mac}_{<,D}(F)$ with entries in $\mathbb{K}$ such that:

- The matrix has $\sum_{i=1}^{m} \binom{n+D-d_i-1}{n-1}$ rows. Each row corresponds to a polynomial of the form $\mathbf{X}^\alpha f_i$, with $|\alpha| + \deg(f_i) = D$. Equivalently, each row corresponds to tf_i where t is a monomial of total degree $D - \deg(f_i)$. We define the *signature* of a row tf_i as the pair (t, f_i). We order the rows as follows:

$$(t, f_i) > (s, f_j) \iff i < j \quad \text{or} \quad \big(i = j \text{ and } s < t\big).$$

- The number of columns is $\binom{n+D-1}{D}$, where the columns correspond to all monomials of total degree D, ordered in decreasing order with respect to $<$.
- The entry of $\mathrm{Mac}_{<,D}(F)$ at the intersection of the row (t, f_i) and the column corresponding to the monomial m is the coefficient of the monomial m in the polynomial tf_i.

To simplify notation, in what follows we denote $M_m := \mathrm{Mac}_{<,m}(f_1, \ldots, f_s)$.

By Gaussian elimination, we can transform the matrix M_m to reduced row echelon form N_m. We know that the $\mathbb{K}$-vector space generated by the rows of M_m and N_m is the same. In particular, each row of N_m represents a polynomial g that is a $\mathbb{K}$-linear combination of the polynomials in S_m, which form a generating system of I_m. That is, $g \in I_m$. Moreover, the rows of N_m are linearly independent because N_m is in reduced row echelon form. It follows that the nonzero rows of N_m, viewed as polynomials, form a basis of the $\mathbb{K}$-vector space I_m.

Remark 1.44. The S-polynomials of a pair of homogeneous polynomials of degree m are either zero or homogeneous of degree m. Moreover, if the remainder of the division is nonzero, it remains homogeneous of degree m, and is given by $r = S(f_i, f_j) - q_1 f_1 - \cdots - q_s f_s \in I_m$. Therefore, the remainder of each S-polynomial of degree m is a $\mathbb{K}$-linear combination of the rows of N_m.

Recall that Buchberger's algorithm incorporates the remainder r of the reduction into G if no monomial of r lies in $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$, iterating until for all $g_i, g_j \in G$ it holds that $\overline{S(g_i, g_j)}^G = 0$, i.e., that the leading terms of all the remainders of all S-polynomials lie in the ideal $\langle \mathrm{LT}(G)\rangle$.

Proposition 1.45. *Let $I = \langle f_1, \ldots, f_s\rangle$ with f_i homogeneous polynomials. Let $g_1, \ldots, g_t$ be the polynomials corresponding to the nonzero rows of the matrix N_m. If $0 \neq g \in I_m$, then $LT(g) = LT(g_i)$ for some $1 \leq i \leq t$.*

Proof. The set $\{g_1, \ldots, g_t\}$ is a basis of the $\mathbb{K}$-vector space I_m. For any $g \in I_m$, there exist unique $c_1, \ldots, c_t \in \mathbb{K}$ such that $g = \sum_{j=1}^{t} c_j g_j$. Since N_m is in reduced row echelon form, it follows that $\mathrm{LT}(g) = \mathrm{LT}(g_i)$, where $i = \max\{j : 1 \leq j \leq t, c_j \neq 0\}$. □

By Lemma 1.41 and the previous remark, reducing S-polynomials of degree m is equivalent to performing row operations on the matrix M_m.

Indeed, let $F = \{f_1, \ldots, f_s\}$ be homogeneous polynomials. Suppose we want to reduce $S(f_1, f_2)$, and set $d = \deg(S(f_1, f_2))$ and $\mathbf{X}^\gamma = \mathrm{lcm}(\mathrm{LT}(f_1), \mathrm{LT}(f_2))$. By Remark 1.44, $\overline{S(f_1, f_2)}^F = S(f_1, f_2) - \sum_{\substack{\mathbf{X}^\alpha f_i \in S_d \\ \mathbf{X}^\alpha f_i \neq \mathbf{X}^\gamma}} c_{\alpha,i} \mathbf{X}^\alpha f_i, \quad c_{\alpha,i} \in \mathbb{K}$.

The terms $\mathrm{LT}(g_i) \notin \langle \mathrm{LT}(S_m) \rangle$ play the role of remainders r in Buchberger's algorithm (cf. Remark 1.46). The nonzero remainder of an S-polynomial of degree m lies in I_m, and thus its leading term is one of the $\mathrm{LT}(g_i)$ for some row g_i of N_m.

Remark 1.46. If $t \mid t'$, then $t' = mt$ for some $m \geq 1$, and thus $t \leq t'$. Therefore, if the leading term of g_i is smaller than those of $\mathrm{LT}(S_m)$, the same holds for all other terms of g_i. Hence, no term of g_i lies in $\langle \mathrm{LT}(S_m) \rangle$.

Corollary 1.47. *The nonzero rows of N_j, for $0 \leq j \leq d$, viewed as polynomials, form a d-Gröbner basis of $I = \langle f_1, \ldots, f_s \rangle$.*

Proof. Let $t \in \mathrm{LT}(I)$ with $\deg(t) \leq d$. Then there exists some $f \in I$ such that $\mathrm{LT}(f) = t$. Let $\hat{f}$ be the homogeneous part of f of degree $\deg(t)$. Note that $\hat{f} \in I_{\deg(t)}$ and $\mathrm{LT}(\hat{f}) = t$. Applying Proposition 1.45, we have that $\mathrm{LT}(\hat{f})$ equals the leading term of a nonzero row of $N_{\deg(t)}$. □

Let $F = \{f_1, \ldots, f_m\}$. Both the S-polynomials and the polynomials added to F during Buchberger's algorithm to construct a Gröbner basis of $I = \langle F \rangle$ lie in the ideal I; thus, they can be expressed as $a_1 f_1 + \cdots + a_m f_m$ for certain polynomials $a_1, \ldots, a_m$. This relation can be written as $(a_1, \ldots, a_m) \cdot (f_1, \ldots, f_m)$.

Definition 1.48. An element $s \in (\mathbb{K}[X_1, \ldots, X_n])^m$ is called a *syzygy* with respect to the tuple $F = (f_1, \ldots, f_m)$ in $\mathbb{K}[X_1, \ldots, X_n]$ if $\sum_{i=1}^m s_i f_i = 0$. If $m \geq 2$, then for each pair f_i, f_j with $1 \leq i < j \leq m$, we have trivial relations $f_i f_j - f_j f_i = 0$, which give rise to the so-called *principal syzygies* $\pi_{ij} = f_i \mathbf{e}_j - f_j \mathbf{e}_i$, where $\mathbf{e}_k$ is the k-th canonical basis vector of $\mathbb{K}^m$. The set of syzygies of F, denoted $\mathrm{Syz}(F)$, is a $\mathbb{K}[X_1, \ldots, X_n]$-submodule of $(\mathbb{K}[X_1, \ldots, X_n])^m$.

Example 1.3. *A zero reduction in Buchberger's algorithm corresponds to a syzygy. Starting from $F = (f_1, \ldots, f_m)$, let G be the set returned by the algorithm. Suppose that $s = S(g_k, g_l) = h_1 g_k - h_2 g_l$ reduces to zero modulo G. This means there is a reduction chain*

$$s \to s - m_1 g_{i_1} \to s - m_1 g_{i_1} - m_2 g_{i_2} \to \cdots \to s - \sum_{j=1}^{k} m_j g_{i_j} = 0,$$

and the following conditions hold:

$$LT(m_j g_{i_j}) \leq LT(s) < LT(h_1 g_k) = LT(h_2 g_k).$$

Note that each $g_j \in G$ lies in $\langle F \rangle$, so it can be written as

$$g_j = \sum_{i=1}^{m} g_{i,j} f_i.$$

From this, we get

$$0 = s - \sum_{j=1}^{k} m_j g_{i_j} = h_1 g_k - h_2 g_l - \sum_{j=1}^{|G|} p_j g_j$$
$$= \sum_{i=1}^{m} \big(h_1 g_{i,k} - h_2 g_{i,l} - \sum_{j=1}^{|G|} p_j g_{i,j} \big) f_i.$$

The Matrix F_5 algorithm described in [13] uses a criterion to eliminate rows of Macaulay matrices that will reduce to zero due to trivial relations $f_i f_j - f_j f_i$.

Let $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]$ be homogeneous polynomials and $I \subseteq \mathbb{K}[X_1, \dots, X_n]$ the ideal they generate. Fix an integer $D \geq 1$ and an order on $\mathbb{T}^n$. The Matrix F_5 algorithm computes a Gröbner basis of I up to degree D with respect to the fixed order.

Given $d \geq 1$, a Gröbner basis up to degree d of $I_i = \langle f_1, \dots, f_i \rangle$ can be obtained as follows: construct the Macaulay matrices of degree $l \leq d$ of $f_1, \dots, f_i$, denoted $M_{l,i}$, and compute their row echelon forms $\tilde{M}_{l,i}$. The nonzero rows of $\tilde{M}_{l,i}$ form the desired Gröbner basis. For $i < m$, the next step is to compute a Gröbner basis up to degree d of I_{i+1}. The idea is to compute triangular bases of $\mathbb{K}[X_1, \dots, X_n]_d \cap I_i$ for $1 \leq i \leq m$, $1 \leq d \leq D$; that is, to efficiently compute row echelon forms of Macaulay matrices.

The key for this is given by the F_5 criterion, which reveals *a priori* (that is, before computing the reduced form of a Macaulay matrix) some rows that will be zero after reduction.

Remark 1.49. We call the *row echelon form* of a matrix M, denoted $\tilde{M}$, the matrix obtained by applying Gaussian elimination to M without row permutations.

Theorem 1.50 (F_5 Criterion)**.** *Let (t, f_i) be the signature of a row of* $\mathrm{Mac}_d(F)$. *If $t \in$ LT$(\langle f_1, \dots, f_{i-1} \rangle)$, then the row (t, f_i) is a linear combination of previous rows.*

Remark 1.51. Let $f_1, f_2, f_3 \in \mathbb{K}[X_1, \dots, X_n]$. Suppose t is a term with $t \in \mathrm{LT}\langle f_1, f_2 \rangle$. Using the notations of Theorem 1.50, we want to check if tf_3 will reduce to zero in the matrix reduction. There exists $\hat{h} \in \langle f_1, f_2 \rangle$ such that $\mathrm{LT}(\hat{h}) = t$. Then, $\hat{h} = uf_1 + vf_2$, and the relation

$$\hat{h} f_3 - u f_3 f_1 - v f_3 f_2 = u(f_1 f_3 - f_3 f_1) + v(f_2 f_3 - f_3 f_2) = 0$$

holds. This allows expressing tf_3 as a linear combination of previous rows. This illustrates the close relation between the F_5 criterion and principal syzygies.

Corollary 1.52. *With the notations of Theorem 1.50, let t be the leading term of a row in $\tilde{M}_{d-d_i,i-1}$ with signature (t', f_j) for some j with $1 \leq j \leq i-1$. Then the row of $M_{d,i}$ with signature (t, f_i) is a linear combination of previous rows.*

```
**Input:** $(t, f_i)$ the signature of a row, $M$ a matrix in echelon form.
**Output:** A boolean variable.
if $t$ is the leading term of a row in $M$ then
    TRUE;
else
    FALSE;
end
```

Algorithm 3: Matrix F_5 Criterion

```
Input: $f_1, \dots, f_m$ homogeneous polynomials of degrees $d_1 \leq d_2 \leq \dots \leq d_m$, $D$ an integer
  $\geq 1$ and an order $>$ in $\mathbb{T}^n$.
Output: A $D$-Gröbner basis of $\langle f_1, \dots, f_m \rangle$ with respect to $>$.
$G := \emptyset$;
for $d$ from $d_1$ to $D$ do
    $\tilde{M}_{d,0} := \emptyset$;
    for $i$ from 1 to $m$ do
        build $M_{d,i}$ adding to $\tilde{M}_{d,i-1}$ the following rows:
        if $d_i = d$ then
            add the row $f_i$ with signature $(1, f_i)$;
        end
        if $d > d_i$ then
            for every $f$ of $\tilde{M}_{d-1,i}$ with signature $(e, f_i)$ such that $x_j$ is the largest variable
              of $e$, add $n - j + 1$ rows $x_j f, x_{j+1} f, \dots, x_n f$ with signatures
              $(x_j e, f_i), (x_{j+1} e, f_i), \dots, (x_n e, f_i)$ except for those that satisfy:
              Matrix$F_5$Criterion($(x_{j+k} e, f_i), \tilde{M}_{d-d_i,i-1}$) =TRUE;
        end
        Compute $\tilde{M}_{d,i}$ the echelon form of $M_{d,i}$;
        Add to $G$ the polynomials that correspond to the rows of $\tilde{M}_{d,i}$ whose leading
          terms differ from the leading terms of the rows with the same signatures in $M_{d,i}$;
    end
end
return $G$;
```

Algorithm 4: Matrix F_5 Algorithm

Let us see how F_5 Criterion works within the algorithm. Fix i and assume that $e = X_1^{\alpha_1} \dots X_j^{\alpha_j}$. We want to determine which of the rows $eX_{j+k} f_i$ with $0 \leq k \leq n - j$ will be zero. By Corollary 1.52 we have that $ex_j f_i$ is zero if ex_j is the leading term of a polynomial corresponding to a row of $\tilde{M}_{d-d_i,i-1}$.

Remark 1.53. In the affine case, that $I = \langle f_1, \ldots, f_s \rangle$, with $f_1, \ldots, f_s$ polynomials non necessarily homogeneous, we use Matrix F_5 to compute a Gröbner basis G^* of I^* with respect to the order $>_h$ of Definition 1.39 and then G_* is a Gröbner basis of I.

1.5.2 Applications

Gröbner bases are also useful for describing the projection of an algebraic set and for computing implicit equations from a rational parametrization (see [10, Chapter 3] for details). Moreover, they provide an effective tool for finding solutions to multivariate systems of equations (see [12, Section 3.7] for details).

1.5.2.1 Elimination

Definition 1.54. Let $I = \langle f_1, \ldots, f_s \rangle$. The *$l$-th elimination ideal*, I_l is the ideal of $\mathbb{K}[X_{l+1}, \ldots, X_n]$ defined as $I_l = I \cap \mathbb{K}[X_{l+1}, \ldots, X_n]$.

Computing a set of generator of I_l can be made as follows:

Theorem 1.55. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ be an ideal and G a Gröbner basis of I with respect to the* LEX *order $X_1 > \ldots > X_n$. Then, for each $0 \leq l \leq n$, the set $G_l := \{g \in G : g \in \mathbb{K}[X_{l+1}, \ldots, X_n]\}$ is a Gröbner basis of I_l.*

Proof. The proof can be found in [10, p. 123]. □

This has as an important consequence the following result:

Theorem 1.56. *Let $\mathbb{K}$ be an infinite field*

$$F : \mathbb{K}^n \to \mathbb{K}^m, \ (x_1, \ldots, x_n) \mapsto (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$$

a polynomial map and $I = \langle Y_1 - f_1(X_1, \ldots, X_n), \ldots, Y_m - f_m(X_1, \ldots, X_n) \rangle \subseteq \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Then $V_{\mathbb{K}}(I_n)$ is the smallest algebraic set in $\mathbb{K}^m$ containing the image of F.

1.5.2.2 Solving systems of equations

Given $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$ polynomials over $\mathbb{K}$. Consider the system of equations

$$S = \{f_1(X_1, \ldots, X_n) = 0, \ldots, f_m(X_1, \ldots, X_n) = 0\}.$$

The set of solutions of S over $\overline{\mathbb{K}}$ is the algebraic set

$$V_{\overline{\mathbb{K}}}(f_1,\dots,f_m)=\{(x_1,\dots,x_n)\in\mathbb{A}_{\overline{\mathbb{K}}}\mid f_1(x_1,\dots,x_n)=0,\dots,f_m(x_1,\dots,x_n)=0\}.$$

Let $I=\langle f_1,\dots,f_m\rangle\subseteq\mathbb{K}[X_1,\dots,X_n]$ the ideal generated by $f_1,\dots,f_m$, then it is well-known that

$$V_{\overline{\mathbb{K}}}(f_1,\dots,f_m)=V_{\overline{\mathbb{K}}}(I).$$

Remark 1.57. If $\mathbb{K}=\mathbb{F}_q$ is the finite field of q elements, then

$$V_{\mathbb{F}_q}(f_1,\dots,f_m)=V_{\overline{\mathbb{F}_q}}(f_1,\dots,f_m,X_1^q-X_1,\dots,X_m^q-X_m).$$

A Gröbner basis of the ideal I gives information about the solutions of S over $\overline{\mathbb{K}}$ such as the dimension and the degree of $V_{\overline{\mathbb{K}}}(I)$ or the number of solutions if it is finite. Moreover, in the case that S has a finite number of solutions over $\overline{\mathbb{K}}$, i.e. $V_{\overline{\mathbb{K}}}(I)$ is finite, the lexicographical Gröbner basis of I is a set of generators from which the solutions over $\overline{\mathbb{K}}$ can be read off easily. The ideals such that $V_{\overline{\mathbb{K}}}(I)$ is finite are precisely those with $\dim I=0$ (cf. [10, Proposition 6, §4, Chapter 9]). Here we list some properties they have:

Theorem 1.58. *Let $<$ be an order. The following are equivalent:*

1. *I is a zero dimensional ideal*
2. *For $1\le i\le n$, $I\cap\mathbb{K}[X_i]\neq\{0\}$.*
3. *The $\mathbb{K}$-vector space $\mathbb{K}[X_1,\dots,X_n]/I$ has finite dimension.*
4. *The set $\mathbb{T}^n\setminus\langle LT(I)\rangle$ is finite.*
5. *For each i, $1\le i\le n$, there exists $\alpha_i\ge 0$ such that $X_i^{\alpha_i}\in\langle LT(I)\rangle$.*

Definition-Proposition 1.59. *Let $I=\langle f_1,\dots,f_m\rangle$ be a zero-dimensional ideal. Then, by Theorem 1.58, $\dim_{\mathbb{K}}(\mathbb{K}[X_1,\dots,X_n]/I)$ is finite. The degree of the ideal I, is defined as $DEG(I)=\dim_{\mathbb{K}}(\mathbb{K}[X_1,\dots,X_n]/I)$. The number of solutions to the system*

$$f_1=0,\dots,f_m=0$$

in $\overline{\mathbb{K}}^n$ is $\le DEG(I)$.

Hence, for a zero dimensional ideal the degree of an ideal bounds the number of solutions of the system. In addition, if the field $\mathbb{K}$ is perfect and the ideal is radical [12, Theorem 3.7.19], then DEG(I) coincides with the number of solutions of the system.

If we work with a zero-dimensional ideal I as in Theorem 1.58, then $I \cap \mathbb{K}[X_i, \ldots, X_n] \neq \{0\}$ for all $i = 1, \ldots, n$, so if we compute a Gröbner basis G with respect to LEX with $X_1 > \ldots > X_n$, each G_l is nonempty with $1 \leq l \leq n$, where G_l is the set defined in Theorem 1.55. Note that $I_{n-1} \subset \mathbb{K}[X_n]$, so I_{n-1} will be a principal ideal; thus $G_{n-1} = \{g\}$ for some $g \in \mathbb{K}[X_n]$. This is described in detail in the following proposition.

Proposition 1.60. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ be a zero-dimensional ideal and $G = \{g_1, \ldots, g_t\}$ a minimal basis of I with respect to the* LEX *order such that*

$$LT(g_t) < \cdots < LT(g_1).$$

Then $g_t \in \mathbb{K}[X_n]$ and there exists a strictly increasing sequence

$$1 = i_1 < i_2 < \cdots < i_n = t$$

such that for every $j \in \{1, \ldots, n-1\}$ and every $k \in \{i_j, \ldots, i_{j+1} - 1\}$, it holds that

$$g_k \in \mathbb{K}[X_j, \ldots, X_n] \quad \textit{and} \quad g_k \notin \mathbb{K}[X_{j+1}, \ldots, X_n].$$

To find $V_{\overline{\mathbb{K}}}(G)$ we start by solving the equation $g_t = 0$, then substitute the obtained values for x_n into the equations that depend on X_n and X_{n-1} and compute the possible values for X_{n-1}. We continue this process until we calculate the values of X_1.

If, in addition, we work with radical ideals and the field $\mathbb{K}$ is perfect and has sufficiently many elements, an even better situation can be achieved. The assumption that $\mathbb{K}$ has sufficiently many elements is necessary to apply [12, Proposition 3.7.22]. How many elements are enough and the proof of the following theorem can be found in [12, 3.7.C Solving Systems Effectively].

Theorem 1.61 (Shape Lemma)**.** *Let $\mathbb{K}$ be a perfect field with sufficiently many elements, and let $I = \langle h_1, \ldots, h_s \rangle \subset P$ be a zero-dimensional ideal. Let g_n be a monic generator of the ideal $I \cap \mathbb{K}[x_n]$ and set $d = \deg(g_n)$. Then the reduced Gröbner basis of I with respect to* LEX *order is of the form*

$$\{X_1 - g_1, \ldots, X_n - g_n\},$$

with $g_1, \ldots, g_{n-1} \in \mathbb{K}[x_n]$. Moreover, the polynomial g_n has d distinct roots $c_1, \ldots, c_d \in \overline{\mathbb{K}}$. The solutions of the system

$$h_1 = 0, \ldots, h_s = 0$$

are exactly

$$\{(g_1(c_i), \ldots, g_{n-1}(c_i), c_i) : i = 1, \ldots, d\}.$$

Chapter 2

Complexity results

To give complexity estimates, we introduce notions from commutative algebra such as the Hilbert function, dimension, degree, and index of regularity of a homogeneous ideal.

Finally, we present known complexity results for computing Gröbner bases of determinantal ideals. These ideals appear when solving the MinRank problem, which is especially relevant in multivariate cryptography, as many algebraic attacks on multivariate schemes reduce to solving instances of MinRank.

2.1 Complexity theory

We recall here some basic notions in complexity theory, which focuses on classifying computational problems according to their resources usage (e.g time, storage space).

The running time of an algorithm, that is, the number of steps executed, is given in terms of the size of its inputs. Usually, a step is a bit operation and the size is the number of bits to represent the inputs in ordinary bit notation. Occasionally, a step can be a more complex operation or a machine instruction; the size can also be the number of items in the input. The worst-case running time is an upper bound on the running time of any input. On the other hand, the average-case running time is the average running time over all inputs of a fix size. Both, the worst-case and the average-case running time are expressed as functions of the input size. In cryptography, it is relevant the average-case running time as the underlying mathematical problems used to construct cryptographic schemes must be hard to solve on average.

It is often difficult to derive the exact running time of an algorithm for every input. Therefore, one studies how the running time of an algorithm behaves asymptotically. For that, the order notation is used.

Definition 2.1 (Order notation)**.** Let $f, g : \mathbb{Z}_{\leq 0} \to \mathbb{R}$ that are always positive from some point onwards.

- Asymptotic upper bound $f(n) = O(g(n)$: if there exists a positive constant c and a positive integer n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$.
- Asymptotic lower bound $f(n) = \Omega(g(n))$: if there exists a positive constant c and a positive integer n_0 such that $0 \leq cg(n) \leq f(n)$ for all $n \geq n_0$.
- Asymptotic tight bound $f(n) = \Theta(g(n))$: if there exist positive constants c_1 and c_2, and a positive integer n_0 such that $c_1 g(n) \leq f(n) \leq c_2 g(n)$ for all $n \geq n_0$.
- o-notation $f(n) = o(g(n))$ if for any positive constant $c > 0$ there exists a constant $n_0 > 0$ such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$.

Example 2.1. *Gaussian elimination in a matrix $n \times n$ has an asymptotic running time $O(n^3)$ assuming an arithmetic operation takes a unit of time.*

Algorithms can be classified according to its running time:

Definition 2.2. A polynomial-time algorithm is an algorithm whose worst-case running time function is of the form $O(n^k)$, where n is the input size and k is a constant positive integer. Any algorithm whose running time whose running time cannot be so bounded is called an exponential-time algorithm.

An intermediate class of algorithms are the subexponential-time algorithms:

Definition 2.3. A subexponential-time algorithm is an algorithm whose worst case running time function is of the form $e^{o(n)}$ where n is the size of the input.

We finally recall the main complexity classes of decision problems, those are, problems with answer yes or no.

Definition 2.4. The complexity class **P** is the set of all decision problems that are solvable in polynomial time.

Definition 2.5. The complexity class **NP** is the set of all decision problems for which a yes answer can be verified in polynomial time given some extra information, called a certificate.

To compare the difficulties of two problems, the notion of reducibility is useful.

Definition 2.6. Let L_1 and L_2 be two decision problems. The problem L_1 is said to polytime reduce to L_2, written $L_1 \leq_P L_2$, if there is an algorithm that solves L_1 which uses as a subroutine an algorithm for solving L_2, and which runs in polynomial time if the algorithm for L_2 does.

NP-complete problems are as hard as other problems in **NP**:

Definition 2.7. A decision problem L is **NP**-complete if is **NP** and $L_1 \leq_P L$ for every $L_1 \in \mathbf{NP}$.

Definition 2.8. A problem either in decision or in search form is **NP**-hard if there exists some **NP**-complete problem that polytime reduces to it.

2.2 Complexity of computing Gröbner bases

The worst-case complexity of computing a Gröbner basis of an ideal in $\mathbb{K}[X_1, \dots, X_n]$ is doubly exponential in n. By [14, Theorem 3], for ideals such that the solutions of the homogenized system– as points of $(x_0 : \dots : x_n) \in \mathbb{P}^n$ – is a finite set; the largest degree of a polynomial that appear in the computation of a DRL Gröbner basis of the ideal is $\sum_{i=0}^{n+1} d_i + n - 1$ and the computation of the DRL Gröbner basis is upper bounded by $O(\max\{d_i\}^{n+1})$.

To derive an upper bound on the complexity of computing a Gröbner basis of an ideal I with the Matrix F_5, we need to know for which D a D-Gröbner basis is indeed a Gröbner basis of I. For zero dimensional homogeneous ideals, such D can be taken as the index or regularity of the ideal.

2.2.1 Degree, index of regularity and degree of regularity of an ideal.

In Section 1.3 we defined the Hilbert series of an homogeneous ideal, which analogously to the affine Hilbert series, corresponds to power series expansions of rational functions.

Proposition 2.9. *Let $I \subset \mathbb{K}[X_1, \dots, X_n]$ be a homogeneous ideal. Then there exists a polynomial $N(t) \in \mathbb{Z}[t]$ such that*

$$HS_{\mathbb{K}[X_1,\dots,X_n]/I}(t) = \frac{N(t)}{(1-t)^n}.$$

Proof. It follows from Remark 1.7 and Theorem 1.3. □

Proposition 2.10. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ be a proper homogeneous ideal and*

$$HS_{\mathbb{K}[X_1,\ldots,X_n]/I}(t) = \frac{P(t)}{(1-t)^d}$$

with $P(1) \neq 0$. Then $\dim(I) = d$. If, furthermore, I is zero-dimensional, then $HS_{\mathbb{K}[X_1,\ldots,X_n]/I}(t)$ is a polynomial and

$$DEG(I) = HS_{\mathbb{K}[X_1,\ldots,X_n]/I}(1).$$

Proof. See [1, Proposition 1.43]. □

The degree of an ideal, together with the index of regularity of an ideal (concept introduced below), are key to giving bounds on the complexity of algorithms computing Gröbner bases. With the convention that the zero polynomial has degree -1, we have:

Definition-Proposition 2.11. *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ be a homogeneous ideal. There exists a polynomial $HP_{\mathbb{K}[X_1,\ldots,X_n]/I}(t) \in \mathbb{Q}[t]$ of degree $\dim(I) - 1$ and some $d_0 \in \mathbb{N}$ such that for all $d \geq d_0$,*

$$HF_{\mathbb{K}[X_1,\ldots,X_n]/I}(d) = HP_{\mathbb{K}[X_1,\ldots,X_n]/I}(d).$$

The least $d_0 \in \mathbb{Z}_{\geq 0}$ verifying the above is called the index of regularity of I*, $i_{reg}(I)$.*

Proof. It follows from Remark 1.7 and Theorem 1.3. □

If the ideal is zero-dimensional, by Proposition 2.10, the Hilbert series is a polynomial. In that case, we have:

Corollary 2.12. *If $I \subset \mathbb{K}[X_1, \ldots, X_n]$ is a zero-dimensional homogeneous ideal, then $i_{reg}(I) = \deg(HS_{\mathbb{K}[X_1,\ldots,X_n]/I}) + 1$. Moreover, $i_{reg}(I)$ is an upper bound for the degree of all polynomials in any minimal homogeneous Gröbner basis of I.*

Proof. See [1, Corollary 1.66]. □

Theorem 2.13. *Let $f_1, \ldots, f_n$ be homogeneous polynomials such that $I = \langle f_1, \ldots, f_n \rangle$ is zero-dimensional and $d_i = \deg(f_i) \in \mathbb{N}^n$ for $1 \leq i \leq n$. Then*

$$HS_{\mathbb{K}[X_1,\ldots,X_n]/I}(t) = HS_{\mathbb{K}[X_1,\ldots,X_n]}(t) \cdot \prod_{i=1}^{n}(1 - t^{d_i})$$

and

$$HS_{\mathbb{K}[X_1,\ldots,X_n]/I}(t) = \frac{\prod_{i=1}^{n}(1 - t^{d_i})}{(1-t)^n}.$$

Proof. See [1, Proposition 1.67]. This is based on the two preceding propositions. □

Corollary 2.14. *Under the hypotheses of the previous theorem:*

- *The degree of I is $DEG(I) = \prod_{j=1}^{n} d_j$ (Bézout Bound).*
- *The index of regularity of I is $i_{reg}(I) = 1 + \sum_{j=1}^{n}(d_j - 1)$ (Macaulay Bound).*

Proof. Since I is zero-dimensional, $\mathrm{HS}_{\mathbb{K}[X_1,\dots,X_n]/I}$ is a polynomial. Moreover, by Theorem 2.13

$$\mathrm{HS}_{\mathbb{K}[X_1,\dots,X_n]/I}(t) = \frac{\prod_{j=1}^{n}(1-t^{d_j})}{(1-t)^n}.$$

Therefore

$$\mathrm{DEG}(I) = \dim_k(\mathbb{K}[X_1,\dots,X_n]/I) = \mathrm{HS}_{\mathbb{K}[X_1,\dots,X_n]/I}(1) = \prod_{j=1}^{n} d_j.$$

and

$$i_{\mathrm{reg}}(I) = 1 + \deg(\mathrm{HS}_{\mathbb{K}[X_1,\dots,X_n]/I}(t)) = 1 + \sum_{j=1}^{n}(d_j - 1).$$

□

Definition 2.15. Let $F = \{f_1, \dots, f_m\}$ with f_i non-necessarily homogeneous and $I = \langle F \rangle$. Define $F^{(h)} = \{f_1^{(h)}, \dots, f_m^{(h)}\}$ where $f_i^{(h)}$ is the highest-degree homogeneous part of f_i, $i = 1, \dots, m$. If

$$\dim(\langle F^{(h)} \rangle) = 0,$$

then $\dim I = 0$ and the degree of regularity of F, $d_{\mathrm{reg}}(F)$, is $i_{reg}(F^{(h)})$.

2.2.2 Complexity of Matrix F_5 algorithm

By Corollary 2.12, if I is a zero dimensional ideal and run Matrix F_5 algorithm with $D \geq i_{\mathrm{reg}}(I)$ then output, that is a D-Gröbner basis of I, is indeed a Gröbner basis of I. This allows us to give an upper bound on the minimum number of arithmetic operations necessary to compute a Gröbner basis.

Proposition 2.16. *Let $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]$ be homogeneous polynomials that generate a zero-dimensional ideal $I = \langle f_1, \dots, f_m \rangle$. The complexity of computing a Gröbner basis with respect to any term order is bounded above by*

$$O\left(m \binom{n + i_{reg}(I)}{n}^{\omega}\right).$$

By ω we denote the exponent of matrix multiplication, that is, ω is the smallest positive number such that the product of two $N \times N$ matrices can be performed with $O(N^{\omega})$ arithmetic operations.

Proof. The complexity of computing the row echelon form of an $M \times N$ matrix is bounded by

$$O(MN^{\omega-1}).$$

By Corollary 2.12 it is enough to consider the Macaulay matrix of degree $i_{\text{reg}}(I)$. Its number of columns is the number of terms in $\mathbb{T}^n$ of degree $i_{\text{reg}}(I)$, that is, $\binom{n+i_{\text{reg}}(I)-1}{n-1}$, and its number of rows is bounded by $m\binom{n+i_{\text{reg}-1}(I)}{n-1}$. □

If additionally $m = n$, by Corollary 2.14 we have $i_{\text{reg}}(I) = 1 + \sum_{i=1}^{n}(d_i - 1)$.

An analogous result holds for ideals that are not necessarily homogeneous, provided that the ideal generated by the highest-degree homogeneous components of the generators is zero-dimensional.

Proposition 2.17. *Let $I = \langle f_1, \ldots, f_m \rangle \in \mathbb{K}[X_1, \ldots, X_n]$ an ideal such that $\langle F^{(h)} \rangle$ is zero-dimensional. The complexity of computing a Gröbner basis of I is upper-bounded by*

$$O\left(m\binom{n + d_{reg}(F)}{n}^{\omega} + n\text{DEG}(I)^3\right).$$

Proof. The complexity of computing a Gröbner basis with respect to a graded ordering is upper-bounded by

$$O\left(m\binom{n + d_{\text{reg}}(F)}{n}^{\omega}\right).$$

Changing the term order in the zero dimensional case has complexity $O(n\text{DEG}(I)^3)$, see Remark 2.18 below. □

Remark 2.18. The summand $n\text{DEG}(\langle F^{(h)} \rangle)^3$ in the estimate of Proposition 2.17 accounts for the complexity of the FGLM algorithm. This algorithm takes as input a Gröbner basis of a zero-dimensional ideal with respect to one term order, together with a target term order, and outputs a Gröbner basis of the same ideal with respect to the target order.

2.3 Regular and Semi-regular Sequences

In the most general case, the Hilbert series of an ideal is difficult to compute and the cost of this task is essentially the same as computing a Gröbner basis of the associated system. For systems of equations that satisfy a certain notion of regularity, the Hilbert series can be predicted.

Definition 2.19. A sequence $(f_1, \ldots, f_m)$ of non-zero homogeneous polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ is said to be *regular* if for all $i \in \{1, \ldots, m-1\}$, f_{i+1} is not a zero divisor in the ring $\mathbb{K}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_i \rangle$.

Proposition 2.20. *Let $F = (f_1, \ldots, f_m)$ be a sequence of homogeneous polynomials $f_1, \ldots, f_m$ with $m \leq n$ and $d_i = \deg(f_i)$ for $i = 1, \ldots, m$. Then the following are equivalent:*

- *F is regular.*
- *The Hilbert function is*

$$HF_{\mathbb{K}[X_1,\ldots,X_n]/\langle F \rangle}(t) = \frac{\prod_{j=1}^{m}(1 - t^{d_j})}{(1-t)^n}.$$

- $\dim(\langle F \rangle) = n - m$.

Moreover, for regular sequences i_{reg} is the Macaulay bound.

Being regular is a generic property:

Proposition 2.21. *Let $m \leq n$ and $d_1, \ldots, d_m \geq 1$. Then there exists a non-empty Zariski open set U of the vector space $\mathbb{K}[X_1, \ldots, X_n]_{d_1} \times \ldots \times \mathbb{K}[X_1, \ldots, X_n]_{d_m}$ such that every $F = (f_1, \ldots, f_m) \in U$ is a regular sequence.*

The notion of semi-regular sequence extends the definition of regular sequence to the case where $m > n$.

Definition 2.22. Let $f_1, \ldots, f_m$ be homogeneous polynomials, $I = \langle f_1, \ldots, f_m \rangle$ a proper ideal and let D_{reg} be the smallest d such that $\mathbb{K}[X_1, \ldots, X_n]_d = I_d$. Then $f_1, \ldots, f_m$ is semi-regular if for $i \in \{1, \ldots, m-1\}$, if $g_i f_{i+1} = 0$ in the ring $\mathbb{K}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_i \rangle$ and $\deg(g_i f_{i+1}) < D_{reg}$, then $g_i = 0$ in $\mathbb{K}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_i \rangle$.

Definition 2.23. Let $f_1, \ldots, f_m$ be homogeneous polynomials of degrees $d_1, \ldots, d_m$ respectively. The sequence is semi-regular if the Hilbert series of $\mathbb{K}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_m \rangle$ is

$$\mathrm{HS}_{\mathbb{K}[X_1,\ldots,X_n]/\langle f_1,\ldots,f_m \rangle}(t) = \left[\frac{\prod_{i=1}^{m}(1 - t^{d_i})}{(1-t)^n} \right]_+$$

where $[P(t)]_+$ denotes the polynomial obtained by truncating the negative powers of t in the Laurent expansion of $P(t)$.

For regular sequences, all algebraic relations can be expressed in terms of the trivial relations $f_i f_j - f_j f_i$.

Proposition 2.24. *Let $F = \{f_1, \ldots, f_m\}$ a set of polynomials. If F is a semi-regular sequence then $Syz(F) = \langle \pi_{ij} \rangle$, where π_{ij} are the principal syzygies.*

Proof. The proof can be found in [1, Proposition 1.47]. □

Therefore, regular sequences (and semi-regular sequences) are those for which the F_5 criterion detects *a priori* all the rows of the Macaulay matrices that will reduce to zero during the algorithm. Equivalently, this means that all the matrices $M_{d,i}$ have full rank.

Experimentally, semi-regularity appears to be a generic property (in fact, it is proven in some cases, e.g., when $m = n + 1$). Random systems behave as predicted by the results for semi-regular sequences. Since no general proof exists, this remains a conjecture:

Proposition 2.25 (Fröberg's conjecture)**.** *Let $d_1, \ldots, d_m \geq 0$. Then there exists a non-empty Zariski open set U of the vector space $\mathbb{K}[X_1, \ldots, X_n]_{d_1} \times \ldots \times \mathbb{K}[X_1, \ldots, X_n]_{d_m}$ such that every $F = (f_1, \ldots, f_m) \in U$ is a semi-regular sequence.*

2.4 MinRank Problem

MinRank is a well-known hard problem whose complexity has been the topic of intense research in computer algebra, e.g. [1, 15–18], with many applications in cryptography, e.g. [19–24], or real algebraic geometry [17, 25]. It is defined as follows.

Problem 1 (MinRank problem)**.** *Given a set of k matrices $\mathbf{A}_1, \ldots, \mathbf{A}_k \in \mathcal{M}_{m\times n}(\mathbb{K})$, where we assume $n \leq m$, and an integer $r <$ min$(m, n) = n$, the* MinRank *problem asks to find – if any – $(\beta_1, \ldots, \beta_k) \in \mathbb{K}^k$ such that:*

$$\text{Rank}\left(\sum_{i=1}^{k} \beta_i \mathbf{A}_i\right) \leq r.$$

Although the problem is NP-Hard [26] (when $\mathbb{K}$ is a finite field), efficient methods have been proposed to solve MinRank. Up to now, the best algorithms are algebraic, i.e. they reduce the problem to solving a set of algebraic equations. They fall largely under three different approaches – the Kipnis-Shamir modeling [19], the Minors modeling [15, 20] and the Support-Minors modeling [22].

Kipnis-Shamir Modeling.

Kipnis and Shamir [19] proposed to model the MinRank problem as a bilinear system of equations of the form

$$\begin{pmatrix} 1 & & & x_{1,1} & \dots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{m-r,1} & \dots & x_{m-r,r} \end{pmatrix} \cdot \sum_{i=1}^{k} \beta_i \, \mathbf{A}_i = \mathbf{0}_{(m-r)\times n}. \tag{2.1}$$

where the matrix on the left represents an unknown basis of the left kernel of $\sum_{i=1}^{k} \beta_i \, \mathbf{A}_i$, which is of dimension $m-r$. This basis is typically given in systematic form to ensure independence of the found vectors and to reduce the number of variables and can be shown it exists with high probability. Initially, [19] used linearization to solve this algebraic system. The approach was later improved using the results from [1, 20] for solving generic affine bilinear zero-dimensional systems, which upper bounded its complexity by $O\left(\binom{d_{\text{reg}}+(m-r)r+k}{d_{\text{reg}}}^{\omega}\right)$ where d_{reg} is bounded by $\min((m-r)r, k)+1$.

Verbel et al. [27] significantly improve upon this bound in the so called "superdetermined" case when $m < rn$. They show that the equations in the Kipnis-Shamir model contain additional structure by explicitly constructing syzygies that lead to degree falls and subsequently to improved complexity. For example, when $n = m = k$ their analysis provides quadratic speedup compared to previous results.

Minors Modelling.

Alternatively, MinRank is equivalent to finding a vector $(\beta_1, \dots, \beta_k) \in \mathbb{K}^k$ such that all minors of size $r+1$ of the matrix $\sum_{i=1}^{k} \beta_i \mathbf{A}_i$ are zero. We then have to solve a multivariate polynomial system of $\binom{m}{r+1}\binom{n}{r+1}$ equations in m variables as shown in [15, 20]. The system has more equations and less variables than the Kipnis-Shamir modeling but the degree of the equations is $r+1$.

In particular, the authors [15, 16] consider determinantal ideals, i.e. ideals generated by the minors of rank $(r+1)$ of a matrix $\mathbf{M}(x_1, \dots, x_k) \in \mathcal{M}_{m\times n}(\mathbb{K}[x_1, \dots, x_k])$. They give precise formulas for computing the degree and degree of regularity of determinantal ideals, by providing explicitly their Hilbert series.

Support-Minors modelling

In [22], inspired by techniques in coding theory, the following algebraic model was proposed.

Suppose $\mathbf{C}$ is an (unknown) $r \times n$ basis matrix of the row space of $\sum_{i=1}^{k} \beta_i \mathbf{A}_i$ (assuming the MinRank problem has a solution). Assume further that $\mathbf{C}_i$, where $i \in C(n, r)$ are all (unknown) minors of order r of $\mathbf{C}$.

Then the matrix $\mathbf{M}_i = \binom{\mathbf{a}_i}{\mathbf{C}}$, for all $1 \leqslant i \leqslant m$, has rank r, and we can make equations by equating all $r+1$ minors of $\mathbf{M}_i$ to 0. Considering $\mathbf{C}_i$, $i \in C(n, r)$ and $\beta_j, 1 \leq j \leq k$ as unknowns, we obtain $m\binom{n}{r+1}$ bilinear equations in the two sets of unknowns.

It can be noticed, that the number of monomials, that amounts to $k\binom{n}{r}$ is quite small compared to the number of equations. This means that for a wide range of parameters, we can determine an upper bound of the complexity by posing conditions for direct linearization at a different degree. For example, if we expect a unique solution of the MinRank problem, we expect to be able to solve the Support-minors modeling by direct linearization if $m\binom{n}{r+1} \geq k\binom{n}{r} - 1$.

2.4.1 Complexity of the Generalized MinRank Problem and Determinantal ideals

By Section 2.2 we have an upper bound on the complexity of computing a LEX Gröbner basis of a zero dimensional ideal. Here, we focus on giving more precise bounds to the case of determinantal ideals. In this section we will assume that $n \leq m$.

Definition-Proposition 2.26. *Let* $\mathbf{M}$ *be a generic matrix:*

$$\mathbf{M} = \begin{pmatrix} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{m1} & \dots & u_{mn} \end{pmatrix} \in \mathbb{K}[u_{11}, u_{12}, \dots, u_{mn}].$$

Then, the ideal of minors of order $r \geq 1$*, denoted as* $\mathcal{I}_{\text{Minors}(r)}$*, is called a determinantal ideal. We have:*

- *The Hilbert series is* $\frac{\det(C_r^{m,n})}{t^{r/2}(1-t)^{r(m+n-r))}}$*, where* $C_r^{m,n}$ *is the matrix whose element* i, j *is* $\sum_{\ell \geq 0} \binom{m-i}{\ell}\binom{n-i}{\ell}$
- $\dim(\mathcal{I}_{\text{Minors}(r)}) = mn - (m-r)(n-r) = r(m+n-r)$.
- *DEG*$(\mathcal{I}_{\text{Minors}(r)}) = \frac{\prod_{i=0}^{n-r-1} i!(m+i)!}{(n-1+i)!(m-r+i)!}$.

In [1] it is showed that these properties can be transferred to the case where the entries of the matrix $\mathbf{M}$ are polynomials of degree D in a a set of variables with generic coefficients. Generic means that there exists a polynomial $h \neq 0$ such that the results we deduce holds when this polynomial does not vanish on the coefficients of the polynomials that are the entries of the matrix. Such matrices appear in the Generalized MinRank Problem (see matrix $\mathbf{M}(x_1, \dots, x_k)$ in Problem 2 below). Assuming that Fröberg's conjecture holds, by a matrix with entries generic polynomials we may think of a matrix whose entries form a semi-regular sequence.

Remark 2.27. We make a slight abuse of notation, denoting also by $\mathcal{I}_{\text{Minors}(r+1)}$ the ideal of minors of order $r+1$ of the matrix $\mathbf{M}(x_1, \dots, x_k)$, defined below.

Problem 2 (Homogeneous Generalized MinRank problem)**.** *Given a matrix* $\mathbf{M}(x_1, \dots, x_k) \in \mathcal{M}_{m \times n}(\mathbb{K}[x_1, \dots, x_k])$ *whose entries are homogeneous polynomials of degree D and an integer $r < min(m, n)$, the* MinRank *problem asks to find – if any –* $(x_1, \dots, x_k) \in \mathbb{K}^k$ *such that:*

$$\text{Rank}\left(\mathbf{M}(x_1, \dots, x_k)\right) \leq r. \tag{2.2}$$

Proposition 2.28. *Let* $\mathbf{M}$ *be a matrix whose entries are homogeneous polynomials of degree D in* $\mathbb{K}[x_1, \dots, x_k]$ *with generic coefficients. Let*

$$\sum_{\mathbf{t} \in \mathbb{K}[x_1, \dots, x_k]_D} a_{\mathbf{t}}^{(i,j)} \mathbf{t}$$

be the entry (i, j) of $\mathbf{M}$*. Then, the Krull dimension of the ring* $\mathbb{K}(\mathbf{a})[x_1, \dots, x_k]/\mathcal{I}_{\text{Minors}(r+1)}$ *is*

$$\max\{k - (m-r)(n-r), 0\}.$$

Proof. See [1]. □

Following [1, 15, 16, 20], we have to distinguish three cases:

- Case $k > (m-r)(n-r)$. This is the positive dimension case. Under a genericity assumption on the entries of the matrix $\mathbf{M}(x_1 \dots, x_k)$, the dimension of the set of solutions is positive and expected to be $k - (m-r)(n-r)$.

- Case $k = (m-r)(n-r)$. This is the well-defined case where the problem has finitely many solutions under a genericity assumption.

- Case $k < (m-r)(n-r)$. This is the over-determined case where we get an explicit formulas for the Hilbert series if we assume a determinantal variant of Fröberg's Conjecture 2.25. The exact statement can be found in [1, Conjecture 4.11].

In the second and third cases, the set of solutions is finite, so we first compute a DRL Gröbner and then convert it to a LEX basis by using the FGLM algorithm.

Theorem 2.29. *Let $k \leq (m-r)(n-r)$. If the entries of the matrix $\mathbf{M}(x_1,\dots,x_k) \in \mathcal{M}_{m\times n}(\mathbb{K}[x_1,\dots,x_k])$ are generic homogeneous polynomials of degree D, then the arithmetic complexity of computing a* LEX *Gröbner basis of $\mathcal{I}_{\mathrm{Minors}(r+1)}$ is bounded by :*

$$O\left(\binom{m}{r+1}\binom{n}{r+1}\binom{d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{Minors}(r+1)})+k}{k}^{\omega} + k(\mathrm{DEG}(\mathcal{I}_{\mathrm{Minors}(r+1)}))^3\right),$$

where $2 \leq \omega \leq 3$ is a feasible exponent for the matrix multiplication. Also :

- *if $k = (m-r)(n-r)$, then*

$$d_{reg} = deg(\boldsymbol{HS}_{K[x_1,\dots,x_k]/\mathcal{I}_{\mathrm{Minors}(r+1)}}(t)) + 1 = Dr(n-r) + (D-1)k + 1$$

  and

$$DEG(\mathcal{I}_{\mathrm{Minors}(r+1)}) = (\boldsymbol{HS}_{K[x_1,\dots,x_k]/\mathcal{I}_{\mathrm{Minors}(r+1)}}(1)) = D^{(m-r)(n-r)}\prod_{i=0}^{n-r-1}\frac{i!(m+1)!}{(n-1-i)!(m-r+i)!}.$$

- *if $k < (m-r)(n-r)$ and assuming the variant of Fröberg's conjecture is true,*

$$d_{reg} = deg(\boldsymbol{HS}_{K[x_1,\dots,x_k]/I}(t)) + 1$$

  and

$$DEG(\mathcal{I}_{\mathrm{Minors}(r+1)}) = \boldsymbol{HS}_{K[x_1,\dots,x_k]/\mathcal{I}_{\mathrm{Minors}(r+1)}}(1)$$

  where

$$\boldsymbol{HS}_{K[x_1,\dots,x_k]/\mathcal{I}_{\mathrm{Minors}(r+1)}}(t) = \left[(1-t^D)^{(m-r)(n-r)}\frac{det\ C_r^{m,n}(t^D)}{t^{D\binom{r}{2}}(1-t)^k}\right]_+$$

  and $C_r^{m,n}$ denotes the matrix $r \times r$ whose (i,j)-entry is $\sum_{\ell\geq 0}\binom{m-i}{\ell}\binom{n-j}{\ell}t^\ell$.

In the case of positive dimension the degree of regularity is not a bound of the maximal degree of polynomials in a reduced Gröbner basis of the ideal, but we have

Lemma 2.30. *If $k > (m-r)(n-r)$ then the maximal degree in a reduced Gröbner basis is*

$$Dr(n-r) + (D-1)(m-r)(n-r) + 1.$$

From this result, the following complexity bound can be deduced in the case of positive dimension

Theorem 2.31. *Using the same notations as in Theorem 2.29. If $k > (m-r)(n-r)$ then the arithmetic complexity of computing a graded reverse lexicographical of $\mathcal{I}_{\mathrm{Minors}(r+1)}$ is bounded* *by*

$$O\left(\binom{m}{r+1}\binom{n}{r+1}\binom{Dr(n-r)+(D-1)(m-r)(n-r)+1+k}{k}^{\omega}\right), \tag{2.3}$$

In the case entries of $\mathbf{M}(x_1,\dots,x_k)$ are affine polynomials, complexity results can be derived from the homogeneous case [16].

Proposition 2.32. *Let $\mathbf{M}(x_1,\dots,x_k) \in \mathcal{M}_{m\times n}(\mathbb{K}[x_1,\dots,x_k])$ be generic affine polynomials of degree D.*

- *If $k=(m-r)(n-r)$, then $d_{reg}(\mathcal{I}_{\mathrm{Minors}(r+1)}) \leq Dr(n-r)+(D-1)k+1$.*
- *If $k<(m-r)(n-r)$, then*

  $$d_{reg}(\mathcal{I}_{\mathrm{Minors}(r+1)}) \leq deg(\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_k]/\mathcal{I}^{(h)}_{\mathrm{Minors}(r)}}(t))+1.,$$

  where $\mathcal{I}^{(h)}_{\mathrm{Minors}(r+1)}$ is the ideal generated by the homogeneous components of highest degree in $\mathcal{I}_{\mathrm{Minors}(r+1)}$.

Remark 2.33. Note that for affine polynomials with generic coefficients, the ideal $\mathcal{I}^{(h)}_{\mathrm{Minors}(r+1)}$ is the ideal of minors of order $r+1$ of the matrix $\mathbf{M}^{(h)}(x_1,\dots,x_k)$ with entry (i,j) the homogeneous part of highest degree of the (i,j)-entry of $\mathbf{M}(x_1,\dots,x_k)$.

The following proposition is a contribution that will appear in [28].

Proposition 2.34. *Let a generic instance of generalized* MinRank *with target rank $r=1$. Assume that $m,n\geq 3$, $(m-1)(n-1)-k\geq 2$ and:*

$$\binom{k+1}{2}+\binom{m-1}{2}\binom{n-1}{2}<\binom{(m-1)(n-1)}{2},$$

then $d_{\mathrm{reg}}(\mathcal{I}_{\mathrm{Minors}(2)})=2$ as soon as a determinantal variant of Fröberg's conjecture holds. Under these conditions, MinRank *with target rank 1 can be solved in polynomial-time.*

Proof. In the overdetermined case, we know from Theorem 2.29 that d_{reg} can be computed as $\deg(\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_k]/\mathcal{I}_{\mathrm{REP}}})+1$ where

$$\mathbf{HS}_{\mathbb{K}[x_1,\dots,x_k]/\mathcal{I}_{\mathrm{REP}}}=[(1-t)^{(m-1)(n-1)-k}\,\mathbf{C}^{m,n}(t)]_{+}.$$

Therefore, the degree of regularity is 2 if and only if the coefficient of t^2 is the first non-positive coefficient.

Since $m-1 \geq 2, n-1 \geq 2$ and $(m-1)(n-1)-k \geq 2$, we have

$$\begin{aligned}&(1-t)^{(m-1)(n-1)-k}\ \mathbf{C}^{m,n}(t) = \big[1-\big((m-1)(n-1)-k\big)t\\ &+\big((m-1)(n-1)-(k+1)\big)t^2+o(t^3)\big]\cdot\big[1+(m-1)(n-1)t\\ &+\frac{1}{4}(m-1)(m-2)(n-1)(n-2)t^2+o(t^3)\big]\end{aligned}$$

Consequently, the coefficient of t is

$$(m-1)(n-1)-\big((m-1)(n-1)-k\big) > 0.$$

The coefficient of t^2 is

$$\begin{aligned}&\frac{1}{4}(m-1)(m-2)(n-1)(n-2)\\ &+\frac{1}{2}\big((m-1)(n-1)-k\big)\cdot\big((m-1)(n-1)-(k+1)\big)\\ &-(m-1)(n-1)\big((m-1)(n-1)-k\big) = (m-1)(n-1)\\ &\Bigg[\frac{1}{4}(m-2)(n-2)+\frac{1}{2}\big((m-1)(n-1)-2k-1\big)\\ &-\big((m-1)(n-1)-k\big)\Bigg]+\frac{1}{2}k(k+1) = (m-1)(n-1)\\ &\cdot\left[\frac{1}{4}(m-2)(n-2)-\frac{1}{2}(m-1)(n-1)-\frac{1}{2}\right]+\frac{1}{2}k(k+1).\end{aligned}$$

Note that $\frac{1}{4}(m-2)(n-2)-\frac{1}{2}(m-1)(n-1)-\frac{1}{2} < 0$ for all $m,n \geq 2$. Then the coefficient of t^2 is non-positive if and only if

$$k(k+1) < (m-1)(n-1)\big[-\frac{1}{2}(m-2)(n-2)+(m-1)(n-1)+1\big].$$

□

Proposition 2.35. *Let a generic instance of generalized* MinRank *with target rank* 1 *and assume* $k+1=(m-1)(n-1)$*. If*

$$n\binom{k+1}{2}-1 \leq \binom{n}{2}mk-\binom{n}{3}\binom{m+1}{2},$$

then the system of equations corresponding to the minors of order one can be solved in time

$$O\left(\left(n\binom{k+1}{2}\right)^{\omega}\right)$$

Proof. The inequality of the hypothesis corresponds to the condition of having more equations than variables when using linearization of the equations obtained by the supports minors modeling. □

Chapter 3

DME schemes

Notation

Throughout the thesis, if $\mathbb{K}$ is a field, we denote its multiplicative group by $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. For $q = 2^k$, with $k > 0$, $\mathbb{F}_q$ denotes the finite field of q elements. Moreover, for any integer $\ell \geq 1$, $\mathbb{Z}_\ell$ stands for the ring of integers modulo ℓ. Vectors are denoted in boldface, and unless otherwise specified, they are to be understood as column vectors.

Although we will be working over fields of characteristic two, all results in this chapter hold for arbitrary fields of positive characteristic.

Most of the results in 3.1, 3.3 and 3.4 appear in [3].

3.1 Mathematical setting

The family of DME schemes belongs to the class of multivariate cryptographic schemes and follows a layered construction commonly used to build secret-key schemes. Specifically, each round consists of a composition of a suitably chosen linear or affine transformation and a nonlinear transformation, the exponential map, which we will define precisely below.

It is natural to ask whether adding multiple rounds result in additional security or merely increases the complexity of attacks by a polynomial factor in the number of rounds. The latter would be consistent with the conclusions of [29], which addressed this question for the family of HFE-like schemes. The structural attacks we study work by independently inverting one round at a time, resulting in an overall complexity that grows polynomially with the number of rounds.

Fix integers $m > 0,\ n > 0$ and let $\mathbf{E} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^m-1})$. We define the *exponential map* $F_{\mathbf{E}}$ as follows:

$$F_{\mathbf{E}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n,$$

$$\mathbf{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \mapsto \mathbf{z}^{\mathbf{E}} = \begin{pmatrix} \prod_{j=1}^n z_j^{a_{1j}} \\ \vdots \\ \prod_{j=1}^n z_j^{a_{nj}} \end{pmatrix}$$

The fact that entries of the matrix $\mathbf{E}$ are in $\mathbb{Z}_{q^m-1}$ introduces no loss of generality in the definition since the domain of the map $F_{\mathbf{E}}$ is $\mathbb{F}_{q^m}^n$.

Remark 3.1. By abuse of notation, we will use $\mathbf{E}$ both to denote the matrix that define $F_{\mathbf{E}}$ and the map itself. Which one we refer to will be clear by the context.

The following two lemmas are useful to find exponential maps that are invertible:

Lemma 3.2. *Let* $F_{\mathbf{E}_1}, F_{\mathbf{E}_2} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ *be exponential maps then*

$$F_{\mathbf{E}_2}\ o\ F_{\mathbf{E}_1} = F_{\mathbf{E}_2 \cdot \mathbf{E}_1}.$$

Lemma 3.3. *If* $\mathbf{E} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^m-1})$ *satisfies* $\gcd(\det(\mathbf{E}), q^m-1) = 1$*, then* $\mathbf{E}^{-1} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^m-1})$ *exists.*

Proof. As $\gcd(\det(\mathbf{E}), q^m - 1) = 1$, then $\det(\mathbf{E})$ is a unit in $\mathbb{Z}_{q^m-1}$. Hence, we define $\mathbf{E}^{-1} = (\det(\mathbf{E}))^{-1}\mathrm{Adj}(\mathbf{E})$. □

Proposition 3.4. *Let* $\mathbf{E} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^m-1})$ *satisfies* $\gcd(\det(\mathbf{E}), q^m - 1) = 1$ *and* $V = (\mathbb{F}_{q^m}^*)^n$. *Then the restriction*

$$F_{\mathbf{E}}\big|_V : V \longrightarrow V$$

is a bijection, with inverse $F_{\mathbf{E}^{-1}}$.

In the context of multivariate schemes, the role of linear maps is often to hide structure and make the public key polynomials appear as random as possible. In our case, since exponents allow us to distinguish components, and to obtain a public key of reasonable size, we work with component-wise $\mathbb{F}_q$-linear maps of the form:

$$\begin{aligned} \mathbf{L} : (\mathbb{F}_{q^m})^n &\longrightarrow (\mathbb{F}_{q^m})^n \\ \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} &\mapsto \begin{pmatrix} \sum_{i=1}^m \alpha_{i,1} \cdot z_1^{q^{i-1}} \\ \vdots \\ \sum_{i=1}^m \alpha_{i,n} \cdot z_n^{q^{i-1}} \end{pmatrix}, \end{aligned} \tag{3.1}$$

with $\alpha_{i,j} \in \mathbb{F}_{q^m},\ 1 \leq i \leq m, 1 \leq j \leq n.$

We aim to construct a primitive that is as versatile as possible; ideally, we want a bijective polynomial map to be used both for encryption and signing. To achieve this, we require that both the $\mathbb{F}_q$-linear map $\mathbf{L}$ and the exponential map $F_{\mathbf{E}}$ are bijective. From this point forward, unless otherwise stated, we consider $F_{\mathbf{E}}$ with $\gcd(\det(\mathbf{E}), q^m - 1)$ to be restricted to the Zariski open subset $V = (\mathbb{F}_{q^m}^*)^n$, where it is bijective.

It is well-known that elements over $\mathbb{F}_{q^m}$ are in bijection with m-tuples over $\mathbb{F}_q$.

Proposition 3.5. *Fix a basis $\{u_1, \dots, u_m\}$ of $\mathbb{F}_{q^m}$ regarded as an extension field of degree m of $\mathbb{F}_q$. The map*

$$\phi : \mathbb{F}_q^m \to \mathbb{F}_{q^m},\ (x_1, \dots, x_m) \mapsto \sum_{i=0}^{m-1} x_i u_i$$

is a bijection.

Each of the components of a linear map $\mathbf{L}$ defined as in (3.1) can be regarded as a linear map of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^m$. Such correspondence is also a bijection.

Proposition 3.6. *Let $\mathbf{L} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a linear map. Then there are coefficients $\alpha_0, \dots, \alpha_{m-1}$ such that for any two $\mathbf{X}, \mathbf{y} \in \mathbb{F}_q^m$,*

$$\mathbf{L} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

if and only if

$$w = \sum_{i=0}^{m-1} \alpha_i z^{q^i},$$

where

$$z = \sum_{i=1}^{m} x_i u_i \text{ and } w = \sum_{i=1}^{m} y_i u_i$$

being $\{u_1, \ldots, u_m\}$ an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. That is, there exists a bijection between linear maps from $\mathbb{F}_q^m$ to itself and $\mathbb{F}_q$- linear maps from $\mathbb{F}_{q^m}$ to itself of the form

$$z \mapsto \sum_{i=0}^{m-1} \alpha_i z^{q^i} \tag{3.2}$$

Proof. Fix a basis of $\mathbb{F}_q^m$ as $\mathbb{F}_q$-vector space and a basis of $\mathbb{F}_{q^m}$ as an extension field of degree m of $\mathbb{F}_q$. An endomorphism is determined by its matrix $m \times m$ in a basis, therefore it depends on m^2 parameters over $\mathbb{F}_q$. On the other hand an $\mathbb{F}_{q^m}$ linear maps of the form

$$z \mapsto \sum_{i=0}^{m-1} \alpha_i z^{q^i}$$

is determined by m parameters over $\mathbb{F}_{q^m}$ or, equivalently by m^2 parameters over $\mathbb{F}_q$. This proves that both sets has the same number of elements. Hence, a map between them is a bijection if and only if it is injective. Assume there are two $\mathbb{F}_q$-linear maps of the form (3.2) that are mapped to the same linear map from $\mathbb{F}_q^m$ to itself, then their difference will be a non zero $\mathbb{F}_q$-linear map of degree q^{m-1} with q^m roots, which is a contradiction. □

Let $N = mn$, from Proposition 3.6 the map $\mathbf{L}$ can be represented as a block matrix

$$\left(\begin{array}{c|c|c|c} \mathbf{L}_{i1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{L}_{i2} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \ddots & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{L}_{in} \end{array}\right) \tag{3.3}$$

of size $N \times N$, where each block $\mathbf{L}_{ij}, j = 1, \ldots, n$ has size $m \times m$.

Remark 3.7. We use the same symbol $\mathbf{L}$ for both the big-field representation (over $\mathbb{F}_{q^m}$) and the small-field representation (over $\mathbb{F}_q$) of a linear map; which one we refer to will be clear from the context. Specifically, we will use the big-field representation when the input is an element of $(\mathbb{F}_{q^m})^n$, and the small-field representation when the input is an element of $\mathbb{F}_q^{mn}$.

A $\mathbf{DME}_r$ map will be the composition of r interleaved exponential maps and $r+1$ linear maps/affine maps.

In order to be fast computing the public key and get reasonable public key, we ask for the entries of the exponential map to be of the form 2^s, $0 \leq s \leq \lfloor log_2(q^2 - 1) \rfloor$.

Remark 3.8. If a row of the exponential matrix has exactly two nonzero entries and they are a power of q then $x_i^{q^a} \cdot x_j^{q^b}$ is the quadratic polynomial $x_i \cdot x_j$. However, when the nonzero entries can be taken a power of the characteristic p (here $q = p^k$) then the degree of the polynomials in x_i is up to $q-1$.

In addition, entries of the matrices $\mathbf{E}_j$, $1 \leq j \leq r$ are chosen such that at least one of the $\mathbf{E}_j^{-1}$ has large binary Hamming weight to avoid the recovering of the map $\mathbf{DME}_r^{-1}$ just by interpolating in several $\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ and the corresponding $\begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix} = \mathbf{DME}_r \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ since low Hamming weight causes a low number of monomials in the map $\mathbf{DME}_r^{-1}$.

3.2 NIST PQC 2017 version

For the NIST PQC 2017 call, I. Luengo, M. Avendaño and M. Marco submitted a KEM cryptosystem called $\mathbf{DME} - (3,2,k)$ [30] which consisted in two fixed exponential maps $F_{\mathbf{E_1}} : (\mathbb{F}_{q^2})^3 \longrightarrow (\mathbb{F}_{q^2})^3$ and $F_{\mathbf{E_2}} : (\mathbb{F}_{q^3})^2 \longrightarrow (\mathbb{F}_{q^3})^2$ interleaved between three linear maps over the finite field $\mathbb{F}_q$ with $q = 2^k$. The first two linear maps consist of three 2×2 blocks and the last of two 3×3 blocks. The integer matrices that define the exponential maps are:

$$\mathbf{E}_1 = \begin{pmatrix} 2^{24} & 2^{59} & 0 \\ 2^{21} & 0 & 2^{28} \\ 0 & 2^{29} & 2^{65} \end{pmatrix}, \ \mathbf{E}_2 = \begin{pmatrix} 2^{50} & 2^{24} \\ 2^{7} & 2^{88} \end{pmatrix}$$

The $\mathbf{DME} - (3,2,k)$ polynomial map is:

$$\mathbb{F}_q^6 \xrightarrow{\mathbf{L}_0} \mathbb{F}_q^6 \xrightarrow{\hat{\phi}_1} (\mathbb{F}_{q^2})^3 \xrightarrow{F_{\mathbf{E_1}}} (\mathbb{F}_{q^2})^3 \xrightarrow{\hat{\phi}_1^{-1}} \mathbb{F}_q^6 \xrightarrow{\mathbf{L}_1} \mathbb{F}_q^6 \xrightarrow{\hat{\phi}_2} (\mathbb{F}_{q^3})^2 \xrightarrow{F_{\mathbf{E_2}}} (\mathbb{F}_{q^3})^2 \xrightarrow{\hat{\phi}_2^{-1}} \mathbb{F}_q^6 \xrightarrow{\mathbf{L}_2} \mathbb{F}_q^6,$$

where $\hat{\phi}_1 = \phi_1 \times \phi_1 \times \phi_1$, $\hat{\phi}_2 = \phi_2 \times \phi_2$ with ϕ_1, ϕ_2 defined in Proposition 3.5.

Some care is required in defining $\mathbf{L}_1$ to ensure that a vector $\mathbf{x} \in (\mathbb{F}_{q^2}^*)^3$ is mapped to a vector $\mathbf{L}_1(\mathbf{x}) \in (\mathbb{F}_{q^3}^*)^2$.

Public Key: Matrices that define the exponential map. Padding as described in [30]. Output polynomials of the map $\mathbf{DME} - (2,3,k)$, that is, 6 polynomials over the ring $\mathbb{F}_q[X_1, \ldots, X_6]$.

Private Key: Linear maps given by matrices $\mathbf{L}_0, \mathbf{L}_1, \mathbf{L}_2$ over $\mathbb{F}_q$ where $\mathbf{L}_0, \mathbf{L}_2$ are matrices of the form (3.3) with blocks of size 2×2. For the definition of $\mathbf{L}_1$ see [30].

Encrypt: Given a random message $\mathbf{a} \in (\mathbb{F}_q^*)^6$, split it into two parts $\mathbf{a} = (\mathbf{a}_1 || \mathbf{a}_2)$, apply a padding $h : \mathbb{F}_q^3 \to \mathbb{F}_q^6$ that add nonzero fixed values in the even coordinates. In this way, $h(\mathbf{a}_i)$, $i = 1, 2$ is in the domain where the encryption map is a bijection, that is, $(\mathbb{F}_{q^2}^*)^3$. The encrypted message is

$$\mathbf{b} = (\mathbf{b}_1||\mathbf{b}_2) = (\mathbf{DME} - (3,2,k)(\mathbf{a}_1)||\mathbf{DME} - (3,2,k)(\mathbf{a}_2))\,.$$

Sign: Some messages do not have a signature, they are exactly those that are not in the image of the map $\mathbf{DME} - (3,2,k)$. The probability for that is $\frac{1}{q^2}$. To fix it add some randomness using a padding in the image (see [30]). Assuming the hash $\mathbf{d}$ of a message $\mathbf{a}$ in the image, then $\mathbf{DME}^{-1} - (3,2,k)(\mathbf{d})$ is a signature of $\mathbf{a}$.

In the next sections, the parameter m will be taken to be 2 and all the exponential maps are given by matrices of the same size.

3.3 NIST PQC 2023 version

The scheme we define here correspond to the one presented in [3].

Definition 3.9 (DME scheme of r rounds)**.** Let $\mathbf{E}_1, \ldots, \mathbf{E}_r$ be matrices in $\mathcal{M}_{n\times n}(\mathbb{Z}_{q^2-1})$ with $\gcd(\det(\mathbf{E}_i), q^2-1) = 1,\ i = 1, \ldots, r$ whose non zero entries are of the form $2^s, 0 \leq s \leq \lfloor log_2(2k-1)\rfloor$ and such that the determinant of $\mathbf{E}_j^{-1}$, for some $j = 1, \ldots, n$, has a large Hamming weight. Moreover, let $\mathbf{L}_0, \ldots, \mathbf{L}_r \in GL_{N\times N}(\mathbb{F}_q)$ where $N = 2n$ are matrices of the form (3.3) with blocks of size 2×2. An r-th round DME is the map

$$\mathbf{DME}_r : (\mathbb{F}_q^2 \setminus \{(0,0)\})^n \longrightarrow \mathbb{F}_q^N$$

defined as:

$$\mathbf{DME}_r = \mathbf{L}_r\ o\ F_{\mathbf{E}_r}\ o\ \mathbf{L}_{r-1}\ o\ \cdots\ o\ F_{\mathbf{E}_2}\ o\ \mathbf{L}_1\ o\ F_{\mathbf{E}_1}\ o\ \mathbf{L}_0,$$

$$\begin{tikzcd}
(\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{L}_0"] & (\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{E}_1"] & (\mathbb{F}_{q^2}^*)^n \arrow[dll, "\mathbf{L}_1"] & & \\
(\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{E}_2"] & (\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{L}_2"] & (\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{E}_3"] & (\mathbb{F}_{q^2}^*)^n \arrow[dlll, "\mathbf{L}_3"] & \\
\vdots & \vdots & \vdots & \vdots & \\
(\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{E}_{r-1}"] & (\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{L}_{r-1}"] & (\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{E}_r"] & (\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{L}_r"] & (\mathbb{F}_{q^2}^*)^n
\end{tikzcd}$$

The map $\mathbf{DME}_r$ is a bijection so it is a potential candidate for both encryption and digital signature scheme.

Public Key: Output polynomials $\mathcal{P} = (p_1, \ldots, p_N)$ where $p_i \in \mathbb{F}_q[X_1, \ldots, X_N]$, $i = 1, \ldots, n$. Structure of the linear maps and of the matrices that define the exponential maps. Padding as described in Section 3.5.

Private Key: Entries of the matrices that define the exponential maps and entries of the linear maps.

Encrypt: To encrypt a message $\mathbf{a} \in \mathbb{F}_q^N$ we compute

$$b_1 = p_1(\mathbf{a}), \ldots, b_N = p_N(\mathbf{a})$$

and $\mathbf{b} = (b_1, \ldots, b_N)$ is the encrypted message. The desired property for security is that only the trusted party can recover the plaintext $\mathbf{a}$ from the ciphertext $\mathbf{b}$ as inverting the public key is infeasible unless you know the simple maps, *i.e.* the linear and exponential maps, that were used to compute the public key.

Sign: To sign a message $\mathbf{a}$, we compute the hash of the message $\mathbf{d} = H(\mathbf{a})$ and $\mathbf{s} = \mathbf{DME}_r^{-1}(\mathbf{d})$ is the signature for $\mathbf{a}$. The fact that it is difficult to compute $\mathbf{DME}_r^{-1}$ solely having access to the public polynomials implies that only the author of the message can sign it.

To simplify notation, in the following, a matrix

$$\mathbf{E} = \begin{pmatrix} 2^{c_{11}} & \cdots & 2^{c_{1n}} \\ \vdots & \ddots & \vdots \\ 2^{c_{n1}} & \cdots & 2^{c_{nn}} \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^2-1})$$

will be simply represented as

$$\mathbf{E} = \begin{pmatrix} [c_{11}] & \cdots & [c_{1n}] \\ \vdots & \ddots & \vdots \\ [c_{n1}] & \cdots & [c_{nn}] \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^2-1}).$$

In the case that some entry of the original matrix is zero then in the simplified version it will appear a 0 without brackets in that entry.

Considering affine maps

We will add affine shifts to some of the layers –that is, to consider affine instead of linear maps – in order to avoid forgery attacks. A possible forgery attack works as follows: let $\mathcal{P} = (p_1, \ldots, p_N) \in (\mathbb{F}_q[X_1, \ldots, X_N])^N$ be the public key of an instance of $\mathbf{DME}_r$. Take $\mathbf{s} = (s_1, \ldots, s_N)$ the signature of the hash of a message, $\mathbf{d}$, that is, $\mathcal{P}(\mathbf{s}) = \mathbf{d}$. Then the image of $\lambda\mathbf{s} = (\lambda_1 s_1, \lambda_1 s_2, \dots, \lambda_n s_{N-1}, \lambda_n s_N)$ under $\mathbf{DME}_r$ is $\gamma\mathbf{d} = (\gamma_1 d_1, \gamma_1 d_2, \dots, \gamma_n d_{N-1}, \gamma_n d_N)$, being $\lambda = (\lambda_1, \dots, \lambda_n)$ with $\lambda_i \in \mathbb{F}_q^*$ and $\gamma = \lambda^{\mathbf{E}_r \cdot \dots \cdot \mathbf{E}_1}$. Therefore, for all $\mathbf{d}'$ such that

$$\frac{d'_{2i}}{d'_{2i-1}} = \frac{d_{2i}}{d_{2i-1}} \tag{3.4}$$

we can find $\mathbf{s}'$ such that $\mathcal{P}(\mathbf{s}') = \mathbf{d}'$, that is valid signature for $\mathbf{d}'$. Explicitly, from equation (3.4) we have that $(d'_1, \dots, d'_N) = (\gamma_1 d_1, \gamma_1 d_2, \dots, \gamma_n d_{N-1}, \gamma_n d_N)$. Thus λ such that $\lambda^{\mathbf{E}_r \cdots \mathbf{E}_1} = \gamma$ will give $\mathbf{s}' = \lambda\mathbf{s}$ that is a signature of $\mathbf{d}'$.

Affine maps will be denoted by $\mathbf{A}$. Its big field representation is:

$$\begin{aligned} \mathbf{A} : (\mathbb{F}_{q^m})^n &\longrightarrow (\mathbb{F}_{q^m})^n \\ \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} &\mapsto \begin{pmatrix} \sum_{i=1}^m \alpha_{i,1} \cdot z_1^{q^{i-1}} + \beta_1 \\ \vdots \\ \sum_{i=1}^m \alpha_{i,n} \cdot z_n^{q^{i-1}} + \beta_n \end{pmatrix}, \end{aligned}$$

where $\alpha_{i,j}, \beta_j \in \mathbb{F}_{q^m}$. And the small field one is:

$$\begin{aligned} \mathbf{A} : \mathbb{F}_q^{mn} &\longrightarrow \mathbb{F}_q^{mn} \\ \begin{pmatrix} x_1 \\ \vdots \\ x_m \\ x_{m+1} \\ \vdots \\ x_{2m} \\ \vdots \\ x_{mn} \end{pmatrix} &\longmapsto \mathbf{L} \begin{pmatrix} x_1 \\ \vdots \\ x_m \\ x_{m+1} \\ \vdots \\ x_{2m} \\ \vdots \\ x_{mn} \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_m \\ b_{m+1} \\ \vdots \\ b_{2m} \\ \vdots \\ b_{mn} \end{pmatrix} \end{aligned}$$

where $\mathbf{L}$ is as in (3.3) and $b_j \in \mathbb{F}_q,\ j = 1, \dots, mn$. We denote by $\mathbf{A}_i,\ i = 1 \dots, n$ the i-th component of $\mathbf{A}$.

Remark 3.10. When we consider affine maps, the domain of the map $\mathbf{DME}_r$ where it is a bijection, is not simply $(\mathbb{F}_{q^2}^*)^n$.

3.3.1 Which data should be public and private?

It is not relevant whether the polynomial that define the extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ are publicly known or not because changing the choice corresponds to modify the linear maps. More in detail, assume that $p_1, \ldots, p_N \in \mathbb{F}_q[X_1, \ldots, X_N]$ is a public key computed by using a polynomial $a + bx + cx^2$ irreducible over $\mathbb{F}_q$. To find an equivalent public key the attacker wants to compute linear and exponential maps that give the polynomials of the public key. If they do not know the polynomial that defines the extension, they choose a polynomial and write the equations of the last round to recover the last linear map.

Remark 3.11. Let p, q two irreducible polynomials over $\mathbb{F}_{q^2}$ of degree two, then $\mathbb{F}_{q^2} \cong \mathbb{F}_q/\langle p\rangle \cong \mathbb{F}_q/\langle q\rangle$ and $u = x + \langle p\rangle, w = y + \langle q\rangle$ then there exists $\mathbf{L} \in GL_{2\times 2}(\mathbb{F}_q)$ such that

$$(L\ o\ \phi_u^{-1})(A + uB)^{2^a} = \phi_w^{-1}((A + wB)^{2^a}).$$

In the specification document that can be found in [31], the public key is given as a set of monomials together with a list of exponents, which are denoted as f's. Moreover, the symbolic expression of each of the f's in terms of the entries of the exponential matrices is also given. Such expressions of the f's can be obtained symbolically easily:

Example 3.1. *Assume* $\mathbf{E}_1 = \begin{pmatrix} [a_1] & [a_2] \\ [a_3] & [a_4] \end{pmatrix}$, $\mathbf{E}_2 = \begin{pmatrix} [b_1] & [b_2] \\ [b_3] & [b_4] \end{pmatrix}$. *Then the* f_i'*s – that are such that* 2^{f_i} *are the exponents of the variables* $x_1, \ldots, x_N$ *in the public key –of a 2-round DME scheme with exponential matrices* $\mathbf{E}_1, \mathbf{E}_2$ *can be represented in a matrix*

$$\mathbf{E}_2 \star \mathbf{E}_1 = \begin{pmatrix} (2^{a_1+b_1}, 2^{a_3+b_2}) & (2^{a_2+b_1}, 2^{a_4+b_2}) \\ (2^{a_1+b_3}, 2^{a_3+b_4}) & (2^{a_2+b_3}, 2^{a_4+b_4}) \end{pmatrix} = \begin{pmatrix} [a_1+b_1, a_3+b_2] & [a_2+b_1, a_4+b_2] \\ [a_1+b_3, a_3+b_4] & [a_2+b_3, a_4+b_4] \end{pmatrix} \quad (3.5)$$

where the entries of $\mathbf{E}_2 \star \mathbf{E}_1$ *are computed by a kind of multiplication* $\mathbf{E}_2$ *by* $\mathbf{E}_1$ *in which products and sums are replaced by sums and commas respectively. This matrix encode the following information:*

- *the public polynomials* p_1, p_2 *will have* $[a_1 + b_1, a_3 + b_2]$ *as exponents of the variables* x_1, x_2*; and* $[a_2 + b_1, a_4 + b_2]$ *as exponents of the variables* x_3, x_4*. Moreover, the support of* p_1, p_2 *will be the same and equal to*

$$[x_1^{[f_1]}x_1^{[f_2]}, x_1^{[f_1]}x_2^{[f_2]}, x_2^{[f_1]}x_1^{[f_2]}, x_2^{[f_1]}x_2^{[f_2]}] \otimes [x_3^{[f_3]}x_3^{[f_4]}, x_4^{[f_3]}x_3^{[f_4]}, x_3^{[f_3]}x_4^{[f_4]}, x_4^{[f_3]}x_4^{[f_4]}]$$

  where $f_1 = a_1 + b_1,\ f_2 = a_3 + b_2,\ f_3 = a_2 + b_1,\ f_4 = a_4 + b_2$.

- *the public polynomials* p_3, p_4 *will have* $[a_1 + b_3, a_3 + b_4]$ *as exponents of the variables* x_1, x_2*; and* $[a_2 + b_3, a_4 + b_4]$ *as exponents of the variables* x_3, x_4*. Moreover, the support of* p_3, p_4 *will be the same and equal to*

$$[x_1^{[f_5]}x_1^{[f_6]}, x_1^{[f_5]}x_2^{[f_6]}, x_2^{[f_5]}x_1^{[f_6]}, x_2^{[f_5]}x_2^{[f_6]}] \otimes [x_3^{[f_7]}x_3^{[f_8]}, x_4^{[f_7]}x_3^{[f_8]}, x_3^{[f_7]}x_4^{[f_8]}, x_4^{[f_7]}x_4^{[f_8]}]$$

where $f_5 = a_1 + b_3,\ f_6 = a_3 + b_2,\ f_7 = a_2 + b_3,\ f_8 = a_4 + b_4.$

The star product is an operation on the exponents of the exponential matrices that reflects the output that one obtains when computing the components of the $\mathbf{DME}_r$ map. Let us define the star product in general:

Definition 3.12. Given $\mathbf{E}_1 = (a_{ij})_{1\le i,j\le n}, \mathbf{E}_2 = (b_{ij})_{1\le i,j\le n}$ the matrices of the exponential maps of a **DME** scheme, $\mathbf{E}_2 \star \mathbf{E}_1$ is the $n \times n$ matrix whose (i,j) entry is the vector $(b_{i1} \cdot a_{1j}, \dots, b_{in} \cdot a_{nj})$. For $r \geq 2$, the star product $\mathbf{E}_r \star \cdots \star \mathbf{E}_1$ is defined recursively.

Now we discuss why knowing the values of the $f's$ is enough to compute exponential matrices, non necessarily equal to the original matrices, for which there exist linear maps that all together will give an equivalent private key. This proves that hiding the values of the entries of the exponential matrices is not crucial.

The result is the following:

Proposition 3.13. *Let* $\mathbf{E}_1, \dots, \mathbf{E}_r \in \mathcal{M}_{n\times n}(\mathbb{F}_q)$ *with* $r \geq 2$ *a set of matrices whose entries are of the form* $[c] = 2^c$ *with* $0 \le c \le \lfloor log_2(q^2 - 1)\rfloor$*. Denote by* f_ℓ *the entries* $[.]$ *that appear in* $\mathbf{E}_r \star \ldots \star \mathbf{E}_1$*. Then* $\mathbf{E}_r \cdot \ldots \cdot \mathbf{E}_1$ *can be written as a product of* $\mathbf{G}_r \cdot \ldots \cdot \mathbf{G}_1$ *where the entries* $[.]$ *of* $\mathbf{G}_i$ *are linear combinations of the* f_ℓ*'s.*

Proof. Let I be the ideal generated by all the f_ℓ's and we consider the polynomial ring $\mathbb{Q}[\mathcal{S}]$ where $\mathcal{S}$ is the union of the set of variables that appear in each matrix $\mathbf{E}_i$. Consider the term order given by $[e] > [e']$ if $[e] \in \mathbf{E}_i$, $[e'] \in \mathbf{E}_j$, and $i > j$ or if $i = j$ and $[e]$ appear later than $[e']$ in the matrix $\mathbf{E}_i$. By appearing before we mean it appear with a lower index in the vector obtained by concatenating the rows of a matrix.

We claim that the number of elements in the reduced Gröbner basis G of I with respect to this order has $s_r + \sum_{i=1}^{r-1}(s_i - n)$ elements where S_j is the number of variables on $\mathbf{E}_j$ for $j = 1, \dots, r$. Moreover, if we denote $G := \{g_0, \dots g_{s_k-1}, \dots, g_t\}$ we have $\mathbf{E}_r \cdot \ldots \cdot \mathbf{E}_1 = \tilde{\mathbf{E}}_r \cdot \ldots \cdot \tilde{\mathbf{E}}_1$ where $\tilde{\mathbf{E}}_r$ is built by replacing all non-zero entries by $g_0, \dots, g_{s_k-1}$ starting from the right upper corner and going row by row and $\tilde{\mathbf{E}}_j$ in the same way but writing a 1 in the most left nonzero entry of each row. Now notice that I is an ideal generated by linear combinations of elements of $\mathcal{S}$ so the Groebner basis is obtained just by performing Gaussian elimination on the Macaulay matrix of degree 1 associated to I with the order defined above. Then g's are linear combinations of the f's and the matrices $\tilde{\mathbf{E}}_j$ depend only on the f's. □

Let us illustrate this with an example:

Example 3.2. *Let*

$$\mathbf{E}_1 := \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{bmatrix}, \ \mathbf{E}_2 := \begin{bmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{bmatrix}, \ \mathbf{E}_3 := \begin{bmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{bmatrix}$$

then the exponents are

```
[x1,x2],[c0 + b0 + a0,c1 + b2 + a1],
[x3,x4],[c1 + b2 + a2],
[x5,x6],[c0 + b1 + a4],
[x7,x8],[c0 + b1 + a5],

[x1,x2],[c2 + b2 + a1],
[x3,x4],[c2 + b2 + a2],
[x5,x6],[c3 + b5 + a4],
[x7,x8],[c3 + b5 + a5]

[x1,x2],[c4 + b2 + a1],
[x3,x4],[c4 + b2 + a2],
[x5,x6],[c5 + b5 + a4],
[x7,x8],[c5 + b5 + a5]

[x1,x2],[c6 + b3 + a1],
[x3,x4],[c6 + b3 + a2],
[x5,x6],[c6 + b4 + a3,c7 + b5 + a4],
[x7,x8],[c7 + b5 + a5]
```

So the f's are

```
   f_0:= c0 + b0 + a0,
   f_1:= c0 + b1 + a4,
   f_2:=  c0 + b1 + a5,
   f_3:=  c1 + b2 + a1,
   f_4:=  c1 + b2 + a2,
   f_5:=  c2 + b2 + a1,
   f_6:=  c2 + b2 + a2,
   f_7:=  c3 + b5 + a4,
   f_8:=  c3 + b5 + a5,
   f_9:=  c4 + b2 + a1,
   f_10:=  c4 + b2 + a2,
   f_11:=  c5 + b5 + a4,
   f_12:=  c5 + b5 + a5,
   f_13:=  c6 + b3 + a1,
   f_14:=  c6 + b3 + a2,
   f_15:=  c6 + b4 + a3,
   f_16:=  c7 + b5 + a4,
   f_17:=  c7 + b5 + a5
```

Let I be the ideal generated by the f's, then the reduced Groebner basis with respect to the term order $c_7 > \ldots > c_0 > b_5 > \ldots > b_0 > a_5 > \ldots > a_0$ is

```
g_0:= c7 + b5 + a4,
g_1:= c6 + b3 + a1,
g_2:= c5 + b5 + a4,
g_3:= c4 + b2 + a1,
g_4:= c3 + b5 + a4,
g_5:= c2 + b2 + a1,
g_6:= c1 + b2 + a1,
g_7:= c0 + b0 + a0,
g_8:= b4 - b3 + a3 - a1,
g_9:= b1 - b0 + a4 - a0,
g_10:= a5 - a4,
g_11:= a2 - a1
```

We show that

$$\mathbf{E}_3 \cdot \mathbf{E}_2 \cdot \mathbf{E}_1 = \begin{bmatrix} 2^{g_0} & 2^{g_1} & 0 & 0 \\ 0 & 2^{g_2} & 0 & 2^{g_3} \\ 0 & 2^{g_4} & 0 & 2^{g_5} \\ 0 & 0 & 2^{g_6} & 2^{g_7} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 2^{g_8} \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2^{g_9} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 2^{g_{10}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2^{g_{11}} \end{bmatrix}$$

Computing Gaussian elimination in the Macaulay matrix is equivalent to do the following

$$\mathbf{E}_3 \cdot \mathbf{E}_2 \cdot \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 0 & 2^{a_1} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 0 & 2^{a_4} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 2^{a_2-a_1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2^{a_5-a_4} \end{bmatrix} \overset{\text{def}}{=} \mathbf{E}_3 \cdot \mathbf{E}_2 \cdot \mathbf{D}_1 \cdot \tilde{\mathbf{E}}_1$$

$$= \mathbf{E}_3 \cdot \begin{bmatrix} 2^{b_0+a_0} & 0 & 0 & 2^{b_1+a_4} \\ 0 & 2^{b_2+a_1} & 0 & 0 \\ 0 & 2^{b_3+a_1} & 2^{b_4+a_3} & 0 \\ 0 & 0 & 0 & 2^{b_5+a_4} \end{bmatrix} \cdot \tilde{\mathbf{E}}_1$$

$$= \mathbf{E}_3 \cdot \begin{bmatrix} 2^{b_0+a_0} & 0 & 0 & 0 \\ 0 & 2^{b_2+a_1} & 0 & 0 \\ 0 & 0 & 2^{b_3+a_1} & 0 \\ 0 & 0 & 0 & 2^{b_5+a_4} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 2^{b_1+a_4-(b_0+a_0)} \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2^{b_4+a_3-(b_2+a_1)} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \tilde{\mathbf{E}}_1$$

$$\overset{\text{def}}{=} \mathbf{E}_3 \cdot \mathbf{D}_2 \cdot \tilde{\mathbf{E}}_2 \cdot \tilde{\mathbf{E}}_1 = \begin{bmatrix} 2^{c_0+b_0+a_0} & 2^{c_1+b_2+a_1} & 0 & 0 \\ 0 & 2^{c_2+b_2+a_1} & 0 & 2^{c_3+b_5+a_4} \\ 0 & 2^{c_4+b_2+a_1} & 0 & 2^{c_5+b_5+a_4} \\ 0 & 0 & 2^{c_6+b_3+a_1} & 2^{c_7+b_5+a_4} \end{bmatrix} \cdot \tilde{\mathbf{E}}_2 \cdot \tilde{\mathbf{E}}_1 \overset{\text{def}}{=} \tilde{\mathbf{E}}_3 \tilde{\mathbf{E}}_2 \tilde{\mathbf{E}}_1.$$

Thus $\mathbf{E}_1 = \mathbf{D}_1 \cdot \tilde{\mathbf{E}}_1$, $\mathbf{D}_2 \cdot \tilde{\mathbf{E}}_2 = \mathbf{E}_2 \cdot \mathbf{D}_1$ and $\tilde{\mathbf{E}}_3 = \mathbf{E}_3 \cdot \mathbf{D}_2$. where $\mathbf{D}_1 := \begin{bmatrix} 2^{a_0} & 0 & 0 & 0 \\ 0 & 2^{a_1} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 0 & 2^{a_4} \end{bmatrix}$ and

$$\mathbf{D}_2 := \begin{bmatrix} 2^{b_0+a_0} & 0 & 0 & 0 \\ 0 & 2^{b_2+a_1} & 0 & 0 \\ 0 & 0 & 2^{b_3+a_1} & 0 \\ 0 & 0 & 0 & 2^{b_5+a_4} \end{bmatrix}.$$

Remark 3.14. To compute the reduced Gröbner basis of I with respect to the term order defined by $a_5 > \ldots > a_0 > b_5 > \ldots > b_0 > c_7 \ldots > c_0$ is equivalent to start by putting ones on the uppermost element of each column of $\mathbf{E}_3$.

Remark 3.15. It is worth noticing that the equivalent factorization has been achieved multiplying the original matrices by diagonal matrices. This fact will be essential in the proof of the commuting lemmas.

Following the method explained in Example 3.2 we get exponential matrices that gives as public key polynomials with the same monomials as the ones originally used to generate the public key.

Note that as the public key is given over $\mathbb{F}_q$, if we take to set of exponential matrices $\mathbf{E}_1 = (e^1_{ij}), \ldots, \mathbf{E}_r = (e^r_{ij})$ and $\hat{\mathbf{E}}_1 = (\hat{e}^1_{ij}), \ldots, \hat{\mathbf{E}}_r = (\hat{e}^r_{ij})$ such that $[e^k_{ij} + q] = [\hat{e}^k_{ij}]$ for all $1 \leq i, j \leq n$,

$k = 1, \dots, r$, then the supports of the polynomials in $\mathcal{P}$ are equal to the supports of the polynomials in $\hat{\mathcal{P}}$. Moreover, changing the choice corresponds to modify a linear map. This means that the entries of the new exponential matrices can be taken $[c]$, $0 \leq c < \lfloor log_2(q-1) \rfloor$.

Proposition 3.16. *Let $q = 2^k, z, w \in \mathbb{F}_{q^2}$ and $c_0, c_1 \in \mathbb{Z}$ with $0 \leq c_0, c_1 < 2k$ and $\mathbf{L}_0$ the identity map over $\mathbb{F}_{q^2}$ and $\mathbf{L}_1$ the Frobenius map. Then, there exist $\hat{c}_0, \hat{c}_1 \in \mathbb{Z}$ with $0 \leq c_0, c_1 < k$ such that*

$$z^{2^{c_0}} w^{2^{c_1}} = \mathbf{L}_i(z)^{2^{\hat{c}_0}} \mathbf{L}_j(w)^{2^{\hat{c}_1}}$$

for some $i, j = 0, 1$.

Proof. Let $\hat{c}_0$ and $\hat{c}_1$ the remainders of the division of c_0, c_1 by n, respectively. Note that since $0 \leq c_0, c_1 < 2k$ the quotient of the division is 0 or 1. If both quotients are zero then $c_0 = \hat{c}_0, c_1 = \hat{c}_1$ and the equality in the proposition holds taking $\mathbf{L}_i = \mathbf{L}_j = \mathbf{L}_0$. Suppose that one of the quotients is one and assume that it is the first one, then $c_0 = k + \hat{c}_0$, thus $2^{c_0} = 2^k 2^{\hat{c}_0}$ and $z^{2^{c_0}} = (z^q)^{2^{\hat{c}_0}} = \mathbf{L}_1(z)^{2^{\hat{c}_0}}$. This result guarantees that by modifying the linear maps we can assume that the entries of the exponential matrices are of the form 2^c with $0 \leq c < k$. □

This shows that there is no need to choose the entries of the exponential maps over $\mathbb{Z}_{q^2-1}$.

3.4 Reductions

In order to avoid the structural attack in [4], the exponential matrices for DME version 2023 and the new variants of DME we present below, we require the existence of reductions.

Definition 3.17 (Reduction)**.** Let the f's of a **DME** instance be arranged in a matrix as (3.5). Fix i, j and suppose the (i, j)-entry, which is list, contains $\ell > 1$ elements.

If all the ℓ elements are pairwise distinct, we will say that there are no reduction in the (i, j)-entry Otherwise we say that there are reductions in the (i, j)-entry.

The effect of the reductions is the following:

With the notations of Definition 3.17. Fix j, and for each $i = 1, \dots, n$ let ℓ_i the length of the list in the entry (i, j). If the are no reductions in (i, j)-entry for all $i = 1, \dots, n$, then the support of the j-th public-key (over $\mathbb{F}_{q^2}$) component contains 2^{ℓ_i} distinct terms in the variables x_{2i-1}, x_{2i} for $i = 1, \dots, n$. If there are reductions, the number of terms in the variables x_{2i-1}, x_{2i} is less than 2^{ℓ_i}. We compute the exact value in Section 4.3.

To build a scheme with reductions, we need to impose relations between the f's. Let us explain this with an example:

Example 3.3. *Consider matrices of example 3.1. Then the possible reductions are $a_1 + b_1 = a_3 + b_2$, $a_2 + b_1 = a_4 + b_2$, $a_1 + b_3 = a_3 + b_4$, $a_2 + b_3 = a_4 + b_4$.*

However if we want that the exponential matrices are invertible, we cannot do all the reductions. In this example, if we do $a_1 + b_1 = a_3 + b_2$, $a_2 + b_1 = a_4 + b_2$, then $[a_1 + a_4] = [a_2 + a_3]$ and hence $\det(\mathbf{E}_1) = 0$.

The reason why reductions avoid the attack in [4] will be detailed in Section 4.3.

3.5 Padding

For encryption, we want that a generated random value can be shared to the other party, is called key encapsulation mechanism. The padding we use in this case is the OAEP algorithm. We describe below how it is used specifically in DME, assuming $q = 2^{64}$.

1. Take a randomly generated shared secret denoted as ss and a random vector rr, both of size 32 bytes.

2. Compute
$$gr = \text{SHA-3}(rr) \text{ and } pt_{low} = gr[1 \dots 32] \oplus ss.$$

3. Apply SHA-3 to pt_{low} which is a 32 byte-array to get hs that has 64 bytes length.
$$hs = \text{SHA-3}(pt_{low})$$

4. Then compute
$$pt_{high} = hs[1 \dots 32] \oplus rr.$$

5. The plaintext is the concatenation of pt_{high} and pt_{low},
$$pt = (pt_{low}||pt_{high})$$

This plaintext has 64 bytes so it is converted to 8 elements of $\mathbb{F}_q$ and the DME encryption function is applied to compute the ciphertext. Note that the shared secret ss can be recovered from the plaintext.

The padding for signature schemes is different, it is called PSS. To illustrate how it works let $q = 2^{128}$ and $\mathbf{m}$ a message of arbitrary length that we want to sign.

1. Let r be random vector of 16 bytes. Compute $w = \text{SHA-3}(m||r)$ which has 64 bytes.

2. Then
$$g = \text{SHA-3}(w[1 \dots 32]) \text{ and } \tilde{g} = g[1 \dots 16] \oplus r$$

3. Finally, a vector $\mathbf{d}$ of 128 bytes is built. Let $\mathbf{d} = (d_1||\ldots||d_8)$ where every block d_i, $i = 1, \ldots, 8$ has length 16 bytes. Then the blocks d_2, d_4, d_6, d_6 take random values while the blocks d_1, d_3, d_5, d_7 contains parts of $\tilde{g}, g$ and w. Specifically, d_1 stores $\tilde{g}$; the second stores the second quarter of g, $g[17\ldots32]$; the third has the first quarter of w, $w[1\ldots16]$; and the fourth one has the second quarter of $w[17\ldots32]$.

The DME signature function applied to d produces the signature of the message $\mathbf{m}$.

3.6 New DME versions

Here we explain variants of the version of Subsection 3.3 that lead to different schemes either for signing or for encryption.

3.6.1 DME minus schemes

The public key in this version is obtained by removing some components of the DME map $\mathcal{P}$. As a result the map is no longer injective and therefore it can be use to define a signature scheme but not an encryption scheme. The precise formulation is:

Definition 3.18 (DME minus scheme)**.** Let $\mathbf{E}_1, \ldots, \mathbf{E}_r$ be matrices in $\mathcal{M}_{n\times n}(\mathbb{Z}_{q^2-1})$ with

$$\gcd(\det(\mathbf{E}_i), q^2-1) = 1,\ i = 1, \ldots, r$$

whose non zero entries are of the form $2^s, 0 \leq s \leq \lfloor log_2(2k-1)\rfloor$ and such that the determinant of $\mathbf{E}_j^{-1}$, for some $j = 1, \ldots, n$, has a large Hamming weight. Moreover, let $\mathbf{L}_0, \ldots, \mathbf{L}_r \in \mathrm{GL}_{N\times N}(\mathbb{F}_q)$ where $N = 2n$ are matrices of the form (3.3) with blocks of size 2×2. Fixed $t \in \mathbb{Z}_{>0}$, an r round DME minus is the map

$$\mathbf{DME}_r^- : (\mathbb{F}_q^2 \setminus \{(0,0)\})^n \longrightarrow \mathbb{F}_q^{N-t}$$

defined as:

$$\mathbf{DME}_r^- = \pi\ o\ \mathbf{L}_r\ o\ F_{\mathbf{E}_r}\ o\ \mathbf{L}_{r-1}\ o\ \cdots\ o\ F_{\mathbf{E}_2}\ o\ \mathbf{L}_1\ o\ F_{\mathbf{E}_1}\ o\ \mathbf{L}_0,$$

where $\pi : \mathbb{F}_q^N \to \mathbb{F}_q^{N-t}$, $\pi(x_1, \ldots, x_N) = (x_{i_1}, \ldots, x_{i_{N-t}})$, with $i_1, \ldots, i_{N-t} \in \{1, \ldots, N\}$ and for $1 \leq j, k \leq N,\ i_j \neq i_k$ if $j \neq k$.

Public Key: Output polynomials $\mathcal{P}^- = (p_{i_1}, \ldots, p_{i_{N-t}})$ where $p_i \in \mathbb{F}_q[X_1, \ldots, X_N]$, $i = 1, \ldots, N-t$. Structure of the linear maps and of the matrices that define the exponential maps. Padding as described in Section 3.5.

Private Key: Entries of the matrices defining the exponential maps and the linear maps.

Sign: To sign a message $\mathbf{a}$, we compute the hash of the message $\mathbf{d} = H(\mathbf{a}) \in \mathbb{F}_q^{N-t}$, complete it adding t random values over $\mathbb{F}_q$ to $\hat{\mathbf{d}}$, and $\mathbf{s} = \mathbf{DME}_r^{-1}(\hat{\mathbf{d}})$ is a signature for $\mathbf{a}$ and the fact that it is difficult to compute $\mathbf{DME}_r^{-1}$ solely having access solely to the public polynomials implies that only the author of the message can sign. To verify the signature, the verifier checks if $\mathbf{DME}_r^-(\mathbf{s}) = \mathbf{d}$.

Finally, we want to add affine shifts to some of the layers in order to avoid forgery attacks, that can be performed more easily that in DME 2023 version. Note that there are several signatures for a message.

Note that scheme of Definition 3.18 depends on the value t, which give the number of polynomials from $\mathcal{P}$ that have been removed. Because of that, we adopt the convention that when we just say DME minus without specifying π we will refer to the scheme obtained with π defined as $\pi : \mathbb{F}_q^N \to \mathbb{F}_q^n,\ \pi(x_1, \ldots, x_N) = (x_1, x_3, x_5, \ldots, x_{N-1})$. If we want to consider other π, we will specify it explicitly.

Considering affine maps

Replacing some of the linear maps by affine maps is essential in DME minus schemes in order to avoid forgery attacks. Let $\mathcal{P}^- = (p_1, \ldots, p_{N-t}) \in (\mathbb{F}_q[X_1, \ldots, X_N])^N$ be the public key of a $\mathbf{DME}_r^-$. Take $\mathbf{s} = (s_1, \ldots, s_N)$ the signature of the hash of a message, $\mathbf{d}$, that is, $\mathcal{P}^-(\mathbf{s}) = \mathbf{d}$. Then the image under $\mathbf{DME}_r^-$ of $\lambda\mathbf{s} = (\lambda_1 s_1, \lambda_1 s_2, \ldots, \lambda_n s_{N-1}, \lambda_n s_N)$ is $\pi(\gamma\hat{\mathbf{d}}) \in \mathbb{F}_q^n$, being $\lambda = (\lambda_1, \ldots, \lambda_n)$ with $\lambda_i \in \mathbb{F}_q^*$ and $\gamma = \lambda^{\mathbf{E}_r \cdot \ldots \cdot \mathbf{E}_1}$. Therefore, for all $\mathbf{d}' \in \mathbb{F}_q^n$ we can find $\mathbf{s}'$ such that $\mathcal{P}^-(\mathbf{s}') = \mathbf{d}'$, that is valid signature for $\mathbf{d}'$. Explicitly, we can write $(d_1', \ldots, d_N') = (\gamma_1 d_1, \gamma_2 d_3, \ldots, \gamma_n d_{N-1})$. Thus λ such that $\lambda^{\mathbf{E}_r \cdots \mathbf{E}_1} = \gamma$ will give $\mathbf{s}' = \lambda\mathbf{s}$ that is a signature of $\mathbf{d}'$.

3.6.2 DME plus scheme

We now define a version that can be used for encryption.

Definition 3.19 (DME plus scheme)**.** Let $\mathbf{E}_1, \ldots, \mathbf{E}_r$ be matrices in $\mathcal{M}_{n\times n}(\mathbb{Z}_{q^2-1})$ with $\gcd(\det(\mathbf{E}_i), q^2-1) = 1,\ i = 1, \ldots, r$ whose non zero entries are of the form $2^s, 0 \le s \le \lfloor log_2(2k-1)\rfloor$ and such that the determinant of $\mathbf{E}_j^{-1}$, for some $j = 1, \ldots, n$, has a large Hamming weight. Moreover, let $\mathbf{L}_0, \ldots, \mathbf{L}_{r-1} \in GL_{N\times N}(\mathbb{F}_q)$ where $N = 2n$ are matrices of the form (3.3) with blocks of size 2×2. and

$$\mathcal{P} : (\mathbb{F}_q^2 \setminus \{(0,0)\})^n \longrightarrow \mathbb{F}_q^n$$

defined as:

$$\mathcal{P} = (P_1, \ldots, P_n) = F_{\mathbf{E}_r}\ o\ \mathbf{L}_{r-1}\ o\ \cdots\ o\ F_{\mathbf{E}_2}\ o\ \mathbf{L}_1\ o\ F_{\mathbf{E}_1}\ o\ \mathbf{L}_0.$$

Fixed $s_1, \ldots, s_n \in \mathbb{Z}_{>0}$, denote by $\mathcal{Q}_i : \mathbb{F}_q^2 \to \mathbb{F}_q^{2+s_i}$ a random polynomial map such that every of its component are polynomials with the same support as the i-th component, $i = 1, \ldots, n$, of the polynomial map $\mathcal{F}$. An r round DME plus is the map

$$\mathbf{DME}_r^+ : (\mathbb{F}_q^2 \setminus \{(0,0)\})^n \longrightarrow \mathbb{F}_q^{N+s}$$

defined as:

$$\mathbf{DME}_r^+ = \mathbf{L}_r \ o \ (P_1||\mathcal{Q}_1||\ldots||P_n||\mathcal{Q}_n)$$

where $\mathbf{L}_r \in GL_{(N+\sum_{i=1}^n s_i)\times(N+\sum_{i=1}^n s_i)}(\mathbb{F}_q)$ of the form

$$\mathbf{L}_r = \left(\begin{array}{c|c|c|c} \mathbf{L}_r^{s_1} & 0 & 0 & 0 \\ \hline 0 & \mathbf{L}_r^{s_2} & 0 & 0 \\ \hline 0 & 0 & \ddots & 0 \\ \hline 0 & 0 & 0 & \mathbf{L}_r^{s_n} \end{array}\right)$$

with $\mathbf{L}_r^{s_i}$ is a matrix of size $(2+s_i)\times(2+s_i)$.

Public Key: Output polynomials $\mathcal{P} = (p_1,\ldots,p_{N+s})$ where $p_i \in \mathbb{F}_q[X_1,\ldots,X_N]$. Structure of the linear maps and of the matrices that define the exponential maps.

Private Key: Entries of the matrices defining the exponential maps and the linear maps.

Encrypt: To encrypt a message $\mathbf{a} \in \mathbb{F}_q^N$ we compute

$$b_1 = p_1(\mathbf{a}),\ldots,b_{N+s} = p_{N+s}(\mathbf{a})$$

and $\mathbf{b} = (b_1,\ldots,b_{N+s})$ is the encrypted message. The desired property for security is that only the trusted party can recover the plaintext $\mathbf{a}$ from the ciphertext $\mathbf{b}$ as inverting the public key is infeasible unless you know the simple maps, *i.e.* the linear and exponential maps, that were used to compute the public key. To decrypt the message, given $\mathbf{b} \in \mathbb{F}_q^{N+s}$, compute $\mathbf{c} = \mathbf{L}_r^{-1}(\mathbf{b})$. Remove the components c_i that correspond to the added polynomials to get $\hat{\mathbf{c}} \in \mathbb{F}_q^N$ and compute $\mathcal{F}^{-1}(\hat{\mathbf{c}})$.

3.6.3 DME exponential over $\mathbb{F}_q$

Let $\mathbf{E} \in \mathcal{M}(\mathbb{Z}_{q^2-1})$ and $F_{\mathbf{E}} : \mathbb{F}_{q^2}^n \to \mathbb{F}_{q^2}^n, \mathbf{z} \mapsto \mathbf{z}^{\mathbf{E}}$. Then we can define a new exponential map as follows:

$$G_{\mathbf{E}} : \mathbb{F}_q^n \to \mathbb{F}_q^n,\ \mathbf{x} \mapsto \mathbf{x}^{\mathbf{E}\otimes\mathbf{I_2}},$$

where $\otimes$ denotes the Kronecker product.

If $(\det(\mathbf{E}), q^2-1) = 1$ then $(\det(\mathbf{E}), q-1) = 1$. Since $\det(\mathbf{E}\otimes\mathbf{I}_2) = \det(\mathbf{E})^2$ we have that $(\det(\mathbf{E}\otimes\mathbf{I}_2), q-1) = 1$ and therefore $G_{\mathbf{E}}$ is a bijection restricted to $\mathbb{F}_q^*$.

Definition 3.20 (**DME** over $\mathbb{F}_q$)**.** Let $\mathbf{E}_1,\ldots,\mathbf{E}_r$ be matrices in $\mathcal{M}_{N\times N}(\mathbb{Z}_{q-1})$ with $\gcd(\det(\mathbf{E}_i), q-1) = 1,\ i = 1,\ldots,r$ whose non zero entries are of the form $2^s, 0 \le s \le \lfloor log_2(k-1)\rfloor$ and such that the determinant of $\mathbf{E}_j^{-1}$, for some $j = 1,\ldots,n$, has a large Hamming weight. Moreover, let $\mathbf{L}_0,\ldots,\mathbf{L}_r \in GL_{N\times N}(\mathbb{F}_q)$ where $N = 2n$ are matrices of the form (3.3) with blocks of size 2×2. An r-th round DME is the map

$$\mathbf{DME}_r : (\mathbb{F}_q^2 \setminus \{(0,0)\})^n \longrightarrow \mathbb{F}_q^N$$

defined as:

$$\mathbf{DME}_r = \mathbf{L}_r \ o \ G_{\mathbf{E}_r} \ o \ \mathbf{L}_{r-1} \ o \ \cdots \ o \ G_{\mathbf{E}_2} \ o \ \mathbf{L}_1 \ o \ G_{\mathbf{E}_1} \ o \ \mathbf{L}_0.$$

Note that $\mathbf{E}_r \otimes \mathbf{I}_2$ gives a matrix of size $2n \times 2n$. This idea can be generalized as follows: Let $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$ then it lead to 2^n vectors of size $2n$ constructed by choosing to place a_i in the $(2i-1)$-th position or in the $2i$-th position. This 2^n vectors will be called associated vector of $\mathbf{v}$ Therefore instead of simply take $\mathbf{E} \otimes \mathbf{I}_2$, we can decide to choose a set of associated vectors of each of vectors that define the rows of the matrix $\mathbf{E}_r$. If we choose exactly k_1 associated to the first row,...,k_n vectors associated to the last row, the matrix, $\mathbf{E}^{\mathrm{ass}(k_1,\dots,k_n)}$, whose rows are these vectors is of size $(k_1 + \ldots + k_n) \times N$. We do not know how to predict the rank of $\mathbf{E}^{\mathrm{ass}(k_1,\dots,k_n)}$. The case when $\mathbf{E}^{\mathrm{ass}(k_1,\dots,k_n)}$ square and invertible can be analyzed with the techniques seen for DME over $\mathbb{F}_q$ with the only modification that now the block of the linear matrices can be bigger than 2×2. The other cases lead to a new version $\mathrm{DME}_{\mathrm{w}}$.

3.6.4 $\mathbf{DME}_{\mathbf{w}}$

As we mention this version can be understood as a generalization of DME over $\mathbb{F}_q$.

Definition 3.21. Let $\mathbf{E}_1^{\mathrm{ass}(k_1^1,\dots,k_n^1)}, \dots, \mathbf{E}_r^{\mathrm{ass}(k_1^r,\dots,k_n^r)}$ matrices. Define

$$\mathcal{F}_{\mathbf{E}^{\mathrm{ass}}} : \mathbb{F}_q^n \to \mathbb{F}_q^n, \ \mathbf{x} \mapsto \mathbf{x}^{\mathbf{E}^{\mathrm{ass}}}$$

and linear matrices $\mathbf{L}_0, \mathbf{L}_1, \dots, \mathbf{L}_r$ where

$$\mathbf{L}_i = \left(\begin{array}{c|c|c|c} \mathbf{L}_{i1} & 0 & 0 & 0 \\ \hline 0 & \mathbf{L}_{i2} & 0 & 0 \\ \hline 0 & 0 & \ddots & 0 \\ \hline 0 & 0 & 0 & \mathbf{L}_{in} \end{array}\right)$$

with $\mathbf{L}_{ij}$ is a block of size $k_j^i \times k_j^i, \ j = 1, \dots, n, \ i = 1, \dots j.$

The map $\mathbf{DME}_{\mathrm{w}}$ is defined as:

$$\mathbf{DME}_{\mathrm{w}} = \mathbf{L}_r \circ \mathbf{E}_r^{\mathrm{ass}(k_1^r,\dots,k_n^r)} \circ \ldots \circ \mathbf{L}_1 \circ \mathbf{E}_1^{\mathrm{ass}(k_1^1,\dots,k_n^1)} \circ \mathbf{L}_0.$$

Note that if $\mathbf{E}^{\mathrm{ass}}$ is full rank of size $m \times n$, then if $m \geq n$ is injective whereas if $m \leq n$ it is surjective. On the other hand if we consider $\mathbf{E}^{\mathrm{ass}}$ square $N \times N$ with Rank($\mathbf{E}^{\mathrm{ass}}$) $= r < N$ then our map is nor injective nor surjective. For proving this, we know that two matrices are equivalent if and only if they have the same rank, therefore there exists $\mathbf{P}, \mathbf{Q}$ invertible matrices $N \times N$ such that $\mathbf{E}^{\mathrm{ass}} = \mathbf{P} \left(\begin{array}{c|c} \mathbf{I}_r & 0 \\ \hline 0 & 0 \end{array}\right) \mathbf{Q} = \mathbf{PSQ}$ and now use that $\mathbf{x}^{\mathbf{E}^{\mathrm{ass}}} = \mathbf{x}^{\mathbf{PSQ}}$.

However, when we restrict the map to its image, it is, by definition, surjective onto that image. Note that the defining equations of the variety containing the image can be obtained from Theorem 1.56. Consequently, to sign a message we must ensure that its hash lies in the image. Moreover, the intermediate values produced during signing must lie in the images of the preceding rounds: in particular, the output must belong to the image of the second-to-last round, and so on. Whether this can be done efficiently is future work.

Chapter 4

Attacks

In this chapter $\mathbb{F}_q$ is a finite field with $q = 2^k,\ k \geq 0$. We analyze the DME scheme of Definition 3.9. Following notation of the previous chapter, from a private key $\mathbf{E}_1, \ldots, \mathbf{E}_r$ and $\mathbf{L}_0, \mathbf{A}_1, \ldots, \mathbf{A}_r$ let $\mathcal{P} = (P_1, \ldots, P_n) \in (\mathbb{F}_{q^2}[X_1, \ldots, X_N])^n$ be the corresponding $\mathbf{DME}_r$ public key. By $\mathbf{A}_1, \ldots, \mathbf{A}_r$ we denote the affine map derived from $\mathbf{L}_1, \ldots, \mathbf{L}_r$ adding a shift vector. Moreover, given a polynomial map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m,\ (x_1, \ldots, x_n) \to (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n))$ we write $F_i(X_1, \ldots, X_n),\ i = 1, \ldots, m$ when its components are regarded as polynomials. We first summarize the two known structural attacks to the DME versions 3.2 and 3.3 respectively. Structural attacks consist in recovering a private key from a given public key. We refer to this private key as an equivalent private key, as it is disticnt to the private key chosen by the trusted party to compute the public key. Although the target of the first attack is the DME version of Section 3.2, still some ideas are general and can be applied for the DME of Definition 3.9. In Section 4.2, we prove some results that will simplify the structure of the equivalent private key. In Section 4.3 we describe an structural attack to the DME version 3.3 – assuming the affine maps $\mathbf{A}_0, \ldots, \mathbf{A}_r$ are linear – that combine techniques from both of the former two attacks and applies to a broader scenario. The complexity of the attack depend on the attack depend on the number of equations and variables of a system of equations. Therefore, in Section 4.4 we describe a method to reduce the size of such systems. Finally, we describe the general case where the maps $\mathbf{A}_0, \ldots, \mathbf{A}_r$ are affine.

4.1 State of the art: structural attacks

The following result will be used to describe the structural attacks to DME version 2017 [4] and 2023 [2].

Proposition 4.1. *Given polynomials $p, q \in \overline{\mathbb{F}_q}[X_1, \ldots, X_N]$ with $p = \sum_{\mathbf{t} \in \mathbb{T}^N} a_{\mathbf{t}} \mathbf{t}, q = \sum_{\mathbf{t} \in \mathbb{T}^N} b_{\mathbf{t}} \mathbf{t}$. Then the maps*

$$f : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q},\ (x_1, \ldots, x_N) \to p(x_1, \ldots, x_N)$$

$$g : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q},\ (x_1, \ldots, x_N) \to q(x_1, \ldots, x_N)$$

are equal if and only if $a_{\mathbf{t}} = b_{\mathbf{t}}$ *for all* $\mathbf{t} \in \mathbb{T}^N$.

Proof. See [10, Proposition 5, Sec.1, Ch. 1] □

4.1.1 Attack to PQC NIST 2017

The structural attack proposed in [4] exploits the malleability of the private key and the highly structured final map. Firstly, it is shown that given a public key, there are several equivalent private keys, and that the set of equivalent private keys can be reduced by specializing some of the unknowns. Specifically, it is shown that the linear maps of the private key can be always assumed to have a very specific structure.

After this specialization, it is easy to compute a candidate for the last linear by noticing the existence of some syzygies coming from the structure of the last exponential map.

To be precise, let

$$\mathbf{L}_2 \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} s_1 z_1 + t_1 z_1^q + u_1 z_1^{q^2} \\ s_2 z_2 + t_2 z_2^q + u_2 z_2^{q^2} \end{pmatrix},$$

and denote by $Q_1, Q_2 \in \mathbb{F}_{q^3}[X_1, \ldots, X_6]$ the polynomials that define the components of the map

$$\mathbf{L}_1 \circ \mathbf{E}_1 \circ \mathbf{L}_0.$$

Then

$$F_{\mathbf{E}_2} \begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} = \mathbf{L}_2^{-1} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}. \tag{4.1}$$

From the entries of the exponential matrices (cf. Example 3.1), we know the support of $Q_i,\ 1 \le i \le 2$, we write

$$Q_1 = \sum_{i=1}^{\#\mathrm{Supp}(Q_1)} A_i \mathbf{t}_{1i}, Q_2 = \sum_{i=1}^{\#\mathrm{Supp}(Q_2)} B_i \mathbf{t}_{2i}$$

where $A_i, B_j \in \mathbb{F}_{q^3}$. By Proposition 4.1, polynomial maps on both sides of (4.1) are equal if and only if their components are equal as polynomials, that is, they have the same coefficients. Hence, for each of the two components, we obtain a system of equations by equaling those terms that have the same terms. In particular, for the first component the system is

$$\{A_i^{[50]} B_j^{[24]} + s_1 c_{ij} + t_1 c_{ij}^q\}$$

in the unknowns A_i, B_j and s_1, t_1, u_1 and s_1 can be specialized to $s_1 = 1$. Therefore, for every $1 \leq i, j \leq \#\mathrm{Supp}(Q_1)$, $1 \leq k, l \leq \#\mathrm{Supp}(Q_2)$ we have

$$\begin{aligned} 0 &= A_i^{[50]} B_j^{[24]} A_k^{[50]} B_l^{[24]} + A_i^{[50]} B_l^{[24]} A_k^{[50]} B_j^{[24]} \\ &= (c_{ij} + t_1 c_{ij}^q + u_1 c_{ij}^{q^2}) \cdot (c_{kl} + t_1 c_{kl}^q + u_1 c_{kl}^{q^2}) + (c_{il} + t_1 c_{il}^q + u_1 c_{il}^{q^2}) \cdot (c_{kj} + t_1 c_{kj}^q + u_1 c_{kj}^{q^2}). \end{aligned} \tag{4.2}$$

which leads to quadratic equations in the variables $c_{ij}, c_{il}, c_{kj}, c_{kl}$.

4.1.2 Reductions avoid the previous attack

If the values of the entries of the matrices are chosen at random, then it is unlikely that there are reductions (see Definition 3.17). In Example 3.3 we described how reductions are obtained: taking the entries of the exponential matrices of a specific form. As a consequence, the cardinality of the support of the polynomials in the public key is reduced. Doing reductions produces collisions, which we define here:

Definition 4.2 (Collision)**.** Let $\mathcal{P} = (P_1(\mathbf{x}), \ldots, P_n(\mathbf{x}))$ the public key and denote by $Q_1(\mathbf{x}), \ldots, Q_n(\mathbf{x})$ the components of the polynomial map $\mathbf{L}_{r-1} \circ \ldots \circ \mathbf{L}_1 \circ \mathbf{E}_1 \circ \mathbf{L}_0$. Fix i, $1 \leq i \leq n$ and assume that the columns with nonzero entries in the ith-row of $\mathbf{E}_r$ are $\mathrm{Indices}_{P_i} = \{j_1, j_2, \ldots, j_k\} \subseteq \{1, \ldots, n\}$ then for every $\mathbf{t} \in \mathrm{Supp}(P_i)$ we define the set

$$\mathrm{Terms}_{P_i,\mathbf{t}} = \{(\mathbf{s}_1, \ldots, \mathbf{s}_k) \in \mathrm{Supp}(Q_{j_1}) \times \ldots \times \mathrm{Supp}(Q_{j_k}) \mid \mathbf{s}_1^{[a_{ij_1}]} \cdot \ldots \cdot \mathbf{s}_k^{[a_{ij_k}]} = \mathbf{t}\}.$$

If $\exists \mathbf{t} \in \mathrm{Supp}(P_i)$ such that $\mathrm{Terms}_{P_i,\mathbf{t}}$ has more than one element we say that P_i has collisions in term $\mathbf{t}$.

Given $\mathcal{P} = (P_1, \ldots, P_n)$ the public key and $\mathbf{L}_r^{-1}$ the inverse of the last linear map then $\mathrm{Supp}(P_i) = \mathrm{Supp}(\mathbf{L}_{ri}^{-1}(P_i))$ for $i = 1, \ldots, n$. Therefore, collisions are independent of the last linear map. Denote by $Q_1(\mathbf{x}), \ldots, Q_n(\mathbf{x})$ the components of the polynomial map

$$\mathbf{L}_{r-1} \circ \ldots \circ \mathbf{L}_1 \circ \mathbf{E}_1 \circ \mathbf{L}_0.$$

By Example 3.1, we know the support of $Q_1, \ldots, Q_n$.

Consequently, the system of equations derived from the i-th component of the equality

$$\mathbf{E}_r \begin{pmatrix} Q_1 \\ \vdots \\ Q_n \end{pmatrix} = \mathbf{L}_r^{-1} \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix}$$

is

$$\{\alpha \cdot \mathrm{Coeff}_{\mathbf{t},P_i} + \beta \cdot \mathrm{Coeff}_{\mathbf{t},P_i}^q = \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k) \in \mathrm{Terms}_{P_i,\mathbf{t}}} C_{\mathbf{s}_1,Q_{j_1}}^{[a_{ij_1}]} \cdot \ldots \cdot C_{\mathbf{s}_k,Q_{j_k}}^{[a_{ij_k}]}\}_{\mathbf{t} \in \mathrm{Supp}(P_i)} \tag{4.3}$$

where $\mathbf{E}_r = (a_{ij})_{1\leq i,j\leq n}$,

$$Q_1 = \sum_{i=1}^{\#\mathrm{Supp}(Q_1)} C_{1i}\mathbf{t}_{1i}, \ldots, Q_n = \sum_{i=1}^{\#\mathrm{Supp}(Q_n)} C_{ni}\mathbf{t}_{ni}$$

with $C_{ki} \in \mathbb{F}_{q^2}$ and

$$\alpha \cdot P_i(\mathbf{x}) + \beta \cdot P_i(\mathbf{x})^q = \mathbf{L}_{ri}^{-1}(P_i(\mathbf{x})),\ \alpha, \beta \in \mathbb{F}_{q^2}$$

Note that the analogue over $\mathbb{F}_{q^2}$ to syzygy (4.2) is only obtained if there are four terms $\mathbf{t}_{1i_1}, \ldots, \mathbf{t}_{1i_4}$ such that

$$\mathbf{t}_{1i_1}\mathbf{t}_{1i_2} = \mathbf{t}_{1i_3}\mathbf{t}_{1i_4}$$

and for $j = i_1, \ldots, i_4$, the sets $\mathrm{Terms}_{P_i,\mathbf{t}_{1j}}$ have one element.

This property is not true in general when there are reductions.

Example 4.1. *Consider the matrices of Example 3.1 with the reduction $a_1 + b_1 = a_3 + b_2$. Then the system of equations we obtain for the first component is:*

$$A_1B_1 + sC_1 + tC_1^q = 0$$
$$A_2B_1 + A_1B_2 + sC_2 + tC_2^q = 0$$
$$A_2B_2 + sC_3 + tC_3^q = 0$$

where $L_{21} : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2},\ z_1 \mapsto sz_1 + tz_1^q$ and the analogue over $\mathbb{F}_{q^2}$ to syzygy of (4.2) does not give an equation that only involves the variables s, t.

4.1.3 NIST algebraic structural attack

To consider for each polynomial of the public key a system of equations was done by [2]. We will follow their set-up which we briefly describe here. Recall that only the structure of the matrices defining the exponential maps are known but not their entries. Given a public key, the first step is to compute entries for the exponential matrices that lead to an equivalent private key, the main result for this is Lemma 4.3 (or Lemma 5 of [2]). We propose a more general alternative to Algorithm 1 of [2], described in Example 3.2. Secondly, recall that the knowledge of the exponential matrices completely determines the support of the polynomials in each round (cf. Example 3.1). Therefore, the only private information we still have to compute is the affine maps. This is the motivation in [2] to consider systems of equations as in (4.3) – generalized to the case where the last map is $\mathbf{A}_r$ – to compute a candidate for $\mathbf{A}_r$. Specifically, let

$$\mathbf{A}_r = \begin{pmatrix} s_1 z_1 + t_1 z_1^q + d_1 \\ s_2 z_2 + t_2 z_2^q + d_2 \\ \vdots \\ s_n z_n + t_n z_n^q + d_n \end{pmatrix}, \tag{4.4}$$

and $Q_1(\mathbf{x}), \ldots, Q_n(\mathbf{x})$ the components of the polynomial map

$$\mathbf{A}_{r-1} \circ \ldots \circ \mathbf{A}_1 \circ \mathbf{E}_1 \circ \mathbf{A}_0.$$

To compute $s_i, t_i, d_i \in \mathbb{F}_{q^2}$ consider the system of equations

$$\{s_i \cdot \mathrm{Coeff}_{\mathbf{t},P_i} + t_i \cdot \mathrm{Coeff}_{\mathbf{t},P_i}^q = \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k) \in \mathrm{Terms}_{P_i,\mathbf{t}}} C_{\mathbf{s}_1,Q_{j_1}}^{[a_{ij_1}]} \cdot \ldots \cdot C_{\mathbf{s}_k,Q_{j_k}}^{[a_{ij_k}]} \}_{\mathbf{t} \neq 1, \mathbf{t} \in \mathrm{Supp}(P_i)} \tag{4.5}$$

The coefficients of the term $\mathbf{t} = 1$ give an equation where the variable d_i appears.

The equations of these system become bilinear when each of the variables $C_{\mathbf{s}_1,Q_{j_1}}^{[a_{ij_1}]}, \ldots, C_{\mathbf{s}_1,Q_{j_1}}^{[a_{ij_k}]}$ is renamed as new variable. In [2], the authors propose an ad hoc modelling with two notable features: renaming variables to reduce the degree – leading to quadratic equations – and specializing as many variables as possible before computing a Gröbner basis. Specialization reduces the number of private keys equivalent to a given public key by fixing the values of some variables. This translates in reducing the dimension of the ideal that corresponds to the system of equations we want to solve. We aim to get a zero dimensional ideal, that is, that the remaining variables after specialization can only takes a finite number of values (over $\overline{\mathbb{F}_q}$ which can be read off from a LEX Gröbner basis.

It is important to note that, after specialization, we may not obtain a unique solution over $\mathbb{F}_{q^2}$. This was the case in the instance attacked in [2] (where $r = 3$ and $n = 8$). In this instance, the last exponential map is given by:

$$\mathbf{E}_3 = \begin{pmatrix} [c_0] & [c_1] & 0 & 0 \\ 0 & [c_2] & 0 & [c_3] \\ 0 & [c_4] & 0 & [c_5] \\ 0 & 0 & [c_6] & [c_7] \end{pmatrix}.$$

Moreover, the parameters $s_1, \ldots, s_4$ of $\mathbf{A}_3$ can be specialized simultaneously to 1, under the assumption that the chosen

$$\mathbf{A}_3$$

in the private key is random and therefore, generically, has nonzero coefficients.

$$\begin{aligned} Q_1^{[c_0]}Q_2^{[c_1]} &= P_1 + t_1P_1^q, \\ Q_2^{[c_2]}Q_4^{[c_3]} &= P_2 + t_2P_2^q, \\ Q_2^{[c_4]}Q_4^{[c_5]} &= P_3 + t_3P_3^q, \\ Q_3^{[c_6]}Q_4^{[c_7]} &= P_4 + t_4P_4^q. \end{aligned}$$

If there exists a solution (Q_1, Q_2, Q_3, Q_4) and $t_1, \ldots, t_4$, then there is another solution: by raising the last equation to the q-th power and dividing by t_4^q, we obtain

$$\left(Q_3/t_4\right)^{[kc_6]} Q_4^{[kc_7]} \;=\; P_4 \;+\; t_4^{-q}P_4^q.$$

Moreover, $\mathbf{L}_2$ can be modified so that its output is $\left(Q_1^{[k]},\, Q_2^{[k]},\, (Q_3/t_4)^{[k]},\, Q_4^{[k]}\right)$ where $q = 2^k$, which – together with the parameters $t_1^q, t_2^q, t_3^q, t_4^{-q}$ – also yields a solution.

4.2 Simplifying the private key

Given $\mathcal{P}$ a public key of $\mathbf{DME}_r$, our goal is to compute an equivalent private key, that is, $\tilde{\mathbf{E}}_1, \ldots, \tilde{\mathbf{E}}_r$ and $\tilde{\mathbf{A}}_0$, $\tilde{\mathbf{A}}_1, \ldots, \tilde{\mathbf{A}}_r$ such that the public key $\tilde{\mathcal{P}}$ coincides with $\mathcal{P}$. Such attacks are known as structural attacks.

Inspired by the works [4] and [2] we first study the malleability of the private key to reduce the number of equivalent keys, this will give a system of equations at the end that will be zero dimensional over the algebraic closure of $\mathbb{F}_q$. In other words, we are going to reduce the set of private keys that leads to a given public key. This is done by finding those parameters whose specialization to some fixed values are allowed, in the sense that the set of private keys with such constraints is not empty. If we are able to identify exactly those parameters, the resulting system is expected to be zero dimensional and therefore more chance are it can be solved efficiently using Gröbner basis techniques for zero dimensional affine systems.

In Example 3.2 we explained an algorithm to write $\mathbf{E}_r \cdot \ldots \cdot \mathbf{E}_1$ as $\tilde{\mathbf{E}}_r \cdot \ldots \cdot \tilde{\mathbf{E}}_1$ with $\tilde{\mathbf{E}}_1, \ldots, \tilde{\mathbf{E}}_r$ depending only on the f's which explicitly appear in the linear part of the public key. By linear part of the public key we refer to the public key we would obtained by changing $\mathbf{A}_0, \ldots, \mathbf{A}_r$ by just the linear part of them. Indeed, we found diagonal matrices $\mathbf{D}_1, \ldots, \mathbf{D}_{r-1}$ such that

$$\mathbf{E}_1 = \mathbf{D}_1 \cdot \tilde{\mathbf{E}}_1, \mathbf{E}_2 = \mathbf{D}_2 \cdot \tilde{\mathbf{E}}_2 \cdot \mathbf{D}_1^{-1}, \ldots, \mathbf{E}_r = \tilde{\mathbf{E}}_r \cdot \mathbf{D}_{r-1}^{-1}.$$

As a result $\mathbf{DME}_r$ can be written as

$$\begin{tikzcd}
(\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{L}_0"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\tilde{\mathbf{E}}_1"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_1"] & (\mathbb{F}^*_{q^2})^n \arrow[dlll, "\mathbf{A}_1"] \\
(\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_1^{-1}"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\tilde{\mathbf{E}}_2"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_2"] & (\mathbb{F}^*_{q^2})^n \arrow[dlll, "\mathbf{A}_2"] \\
(\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_2^{-1}"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\tilde{\mathbf{E}}_3"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_3"] & (\mathbb{F}^*_{q^2})^n \arrow[dlll, "\mathbf{A}_3"] \\
\vdots & \vdots & \vdots & \vdots \\
(\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_{r-2}^{-1}"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\tilde{\mathbf{E}}_{r-1}"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_{r-1}"] & (\mathbb{F}^*_{q^2})^n \arrow[dlll, "\mathbf{A}_{r-1}"] \\
(\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{D}_{r-1}^{-1}"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\tilde{\mathbf{E}}_r"] & (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{A}_r"] & (\mathbb{F}^*_{q^2})^n
\end{tikzcd}$$

We would like to swap $\mathbf{A}_i$ with $\mathbf{D}_i^{-1}$, $i = 1, \dots, r-1$. In Lemma 5 of [2], they mention that exponential diagonal maps nearly commute with linear maps. We rephrase this as:

Lemma 4.3. *Let $\mathbf{A} : (\mathbb{F}_{q^2})^n \to (\mathbb{F}_{q^2})^n$ a map of the form 4.4 and $\mathbf{D}$ a diagonal matrix,*

$$\mathbf{D} = \begin{pmatrix} [d_0] & & \\ & \ddots & \\ & & [d_{n-1}] \end{pmatrix}, \ 0 \leq d_i < 2k - 1.$$

Then there is a unique affine map $\tilde{\mathbf{A}}$ that makes the diagram

$$\begin{tikzcd}
(\mathbb{F}^*_{q^2})^n \arrow[r, "\tilde{\mathbf{A}}"] \arrow[d, "\mathbf{D}"] & (\mathbb{F}^*_{q^2})^n \arrow[d, "\mathbf{D}"] \\
(\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{A}"] & (\mathbb{F}^*_{q^2})^n
\end{tikzcd}$$

commutative.

Proof. Since $\gcd(\det(\mathbf{D}), q^2 - 1) = 1$, the map

$$\begin{aligned} \mathbf{D} : (\mathbb{F}^*_{q^2})^n &\to (\mathbb{F}^*_{q^2})^n \\ \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} &\mapsto \begin{bmatrix} z_1^{[\delta_0]} \\ z_2^{[\delta_1]} \\ \vdots \\ z_n^{[\delta_{n-1}]} \end{bmatrix} \end{aligned}$$

is invertible with inverse

$$\mathbf{D}^{-1} : (\mathbb{F}_{q^2}^*)^n \to (\mathbb{F}_{q^2}^*)^n$$
$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \mapsto \begin{bmatrix} z_1^{[-\delta_0+2k]} \\ z_2^{[-\delta_1+2k]} \\ \vdots \\ z_4^{[-\delta_{n-1}+2k]} \end{bmatrix}$$

Hence we simply define $\tilde{\mathbf{A}} := \mathbf{D}^{-1} \circ \mathbf{A} \circ \mathbf{D}$ that explicitly is

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_4 \end{bmatrix} \xrightarrow{\tilde{\mathbf{A}}} \begin{bmatrix} s_1^{[-\delta_0+2k]} z_1 + t_1^{[-\delta_0+2k]} z_1^q + d_1^{[-\delta_0+2k]} \\ s_2^{[-\delta_1+2k]} z_2 + t_2^{[-\delta_1+2k]} z_2^q + d_2^{[-\delta_1+2k]} \\ \vdots \\ s_n^{[-\delta_{n-1}+2k]} z_n + t_n^{[-\delta_{n-1}+2k]} z_n^q + d_n^{[-\delta_{n-1}+2k]} \end{bmatrix}$$

□

This result allows us to rewrite $\mathbf{DME}_r$ as

$$(\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{L}_0} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\tilde{\mathbf{E}}_1} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\tilde{\mathbf{A}}_1} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\tilde{\mathbf{E}}_2} \cdots \xrightarrow{\tilde{\mathbf{A}}_{r-1}} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\tilde{\mathbf{E}}_r} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{A}_r} (\mathbb{F}_{q^2}^*)^n.$$

In the sequel we will assume that the structure is

$$(\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{L}_0} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{E}_1} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{A}_1} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{E}_2} \cdots \xrightarrow{\mathbf{A}_{r-1}} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{E}_r} (\mathbb{F}_{q^2}^*)^n \xrightarrow{\mathbf{A}_r} (\mathbb{F}_{q^2}^*)^n.$$

where $\mathbf{E}_i$ for $i = 1, \ldots, r$ are known.

Moreover, affine maps can be assumed without loss of generality to have this simpler structure:

$$(\mathbf{A}_j)^{-1} : (\mathbb{F}_{q^2})^n \to (\mathbb{F}_{q^2})^n, \quad \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \mapsto \begin{bmatrix} z_1 + t_{j1} z_1^q + d_{j1} \\ z_2 + t_{j2} z_2^q + \delta_{j2} \\ \vdots \\ z_n + t_{jn} z_n^q + d_{jn} \end{bmatrix}, \quad j = 1, \ldots, r \tag{4.6}$$

Now we consider the inverse of the last round of the DME scheme, that is

$$(\mathbb{F}_{q^2}^*)^n \xleftarrow{\mathbf{E}_r^{-1}} (\mathbb{F}_{q^2}^*)^n \xleftarrow{\mathbf{A}_r^{-1}} (\mathbb{F}_{q^2}^*)^n.$$

and define the map

$$\begin{aligned} \mathbf{M}_{(S_1,\ldots,S_n)} : (\mathbb{F}_{q^2})^n &\to (\mathbb{F}_{q^2})^n \\ \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} &\mapsto \begin{bmatrix} S_1 z_1 \\ S_2 z_2 \\ \vdots \\ S_n z_n \end{bmatrix} \end{aligned}$$

where $(S_1, \ldots, S_n) \in (\mathbb{F}^*_{q^2})^n$ are such that $\mathbf{M}_{(S_1,\ldots,S_n)} \circ \mathbf{A}_m^{-1}$ has the simplified form. Now we call $\hat{\mathbf{A}}_r^{-1} := \mathbf{M}_{(S_1,\ldots,S_n)} \circ \mathbf{A}_r^{-1}$ and as a result we get that $\mathbf{A}_r^{-1} = M_{(S_1^{-1},\ldots,S_n^{-1})} \circ \hat{\mathbf{A}}_r^{-1}$ and $\hat{\mathbf{A}}_r^{-1}$ has that simple structure.

Lemma 4.4. *Let* $\mathbf{M}_{(S_1,\ldots,S_n)}$ *with* $(S_1, \ldots, S_n) \in (\mathbb{F}^*_{q^2})^n$ *defined as above. The diagram*

$$\begin{tikzcd} (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{E}^{-1}"] \arrow[d, "\mathbf{M}_{(S_1^{-1},\ldots,S_n^{-1})}"] & (\mathbb{F}^*_{q^2})^n \arrow[d, "\mathbf{M}_{(\tilde{S}_1,\ldots,\tilde{S}_n)}"] \\ (\mathbb{F}^*_{q^2})^n \arrow[r, "\mathbf{E}^{-1}"] & (\mathbb{F}^*_{q^2})^n \end{tikzcd}$$

is commutative.

Proof. Define $\begin{bmatrix} \tilde{S}_1 \\ \tilde{S}_2 \\ \vdots \\ \tilde{S}_n \end{bmatrix} := \mathbf{E}^{-1} \begin{bmatrix} S_1^{-1} \\ S_2^{-1} \\ \vdots \\ S_n^{-1} \end{bmatrix}$. □

With this lemma we get the simple form for $\mathbf{A}_r^{-1}$. After that, we redefine $\mathbf{A}_{r-1}^{-1} := \mathbf{A}_{r-1}^{-1} \circ \mathbf{M}_{(\tilde{S}_1,\ldots,\tilde{S}_n)}$, that is still affine, and repeat the same reasoning now with

$$\begin{tikzcd} (\mathbb{F}^*_{q^2})^n & (\mathbb{F}^*_{q^2})^n \arrow[l, "\mathbf{E}_{r-1}^{-1}"'] & (\mathbb{F}^*_{q^2})^n \arrow[l, "\mathbf{A}_{r-1}^{-1}"'] \end{tikzcd}$$

and so on.

4.3 Extended attack

In this section we will assume that given a public key, the entries of the exponential matrices have been computed (with the algorithm described in 3.2) and that the form of the affine maps have the simplified form (4.6).

The attack described in Section 4.1.3 is over the big field because the variables of the system of equations are in $\mathbb{F}_{q^2}$. Note that to compute these equations it is not necessary to write the polynomials entirely over the big field, but only the variables that are involved in the equations. To be precise, this means that to get the system of equations we do not have to lift the public key polynomials to the big field, it is enough to write it as $\mathcal{P} = (P_1(\mathbf{X}), \dots, P_n(\mathbf{X}))$ where $P_j = \sum_{\mathbf{t}\in\mathrm{Supp}(P_j)} C_{\mathbf{t},P_j}\mathbf{t}(\mathbf{X})$ and $C_{\mathbf{t},P_j} \in \mathbb{F}_{q^2}$, $\mathbf{X} = (X_1, \dots, X_N)$. When we use the small representation, the public key is written as $\mathcal{P} = (p_1(\mathbf{X}), \dots, p_N(\mathbf{X}))$ where

$$p_j = \sum_{\mathbf{t}\in\mathrm{Sup}(p_j)} c_{\mathbf{t},p_j}\mathbf{t}(\mathbf{X})$$

and $c_{\mathbf{t},p_j} \in \mathbb{F}_q$. There is a simple relation between variables over the big and small field:

$$C_{\mathbf{t},P_j} = c_{\mathbf{t},p_{2j-1}} + u \cdot c_{\mathbf{t},p_{2j}}$$

for $j = 1, \dots, n$.

We are interested in knowing over which field is better to work at different points of the structural attack. When looking at a round of the $\mathbf{DME}_r$, over the big field the output of the exponential map have less variables than in the case of the small field. On the other hand, each component of the affine map viewed over the big field $\mathbb{F}_{q^2}$ is of the form $z \mapsto \alpha z + \beta z^q + \gamma$, so they have a large exponent q. so it involves the large exponent q. This is not the case over the small field $\mathbb{F}_q$, where the components are given by $(x, y) \mapsto (a_1x + a_2y + c_1, a_3x + a_4y + c_2)$. However, if we consider the inverse of the affine map, the large exponent q is not an exponent of any of the unknown. Both facts explain why the attack proposed was over the big field and aimed to recover the inverse of the linear map. The simpler structure reduces the number of variables and the large exponent q of the linear map does not have relevance because its input is the public key.

To be able to give estimates on the complexity of the attack of Section 4.1.3 and to generalize it to other versions we consider the same systems of equations as in [2] but we adopt a different perspective to solve them.

Remark 4.5. The incorporation of collisions was to avoid the attack of [4], since the syzygy obtained there was no longer existing. We observed that although it removes that syzygies of low degree, still syzygies of larger degree can be found, but in some cases MAGMA does not complete the task.

The fact that attack in [2] was so efficient along with Remark 4.5, we suspected that such an efficient Gröbner basis computation means that the structure is still present and that the collisions do not seem to increase the security.

4.3.1 Modelling of the attack

In the following, we restrict to the case where $\mathbf{A}_r$ is a linear map. Consider the system of equations (4.5) with $s_i = 1$ – which can be done by Lemma 4.4. Our goal is to show that collisions can be removed, that is, every equation in

$$\{\mathrm{Coeff}_{\mathbf{t},P_i} + t_i \cdot \mathrm{Coeff}^{q}_{\mathbf{t},P_i} = \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}} C^{[a_{ij_1}]}_{\mathbf{s}_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}_k,Q_{j_k}}\}_{\mathbf{t}\neq 1,\mathbf{t}\in \mathrm{Supp}(P_i)} \tag{4.7}$$

that corresponds to $\mathbf{t}$ with $\#\mathrm{Terms}_{P_i,\mathbf{t}} = r > 1$ can be rewritten as

$$\begin{aligned}&\{H_{\mathbf{s}_1,\ldots,\mathbf{s}_k} = C^{[a_{ij_1}]}_{\mathbf{s}_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}_k,Q_{j_k}}\}_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}\setminus(\mathbf{s}'_1,\ldots,\mathbf{s}'_k)},\\ &\mathrm{Coeff}_{\mathbf{t},P_i} + t_i \cdot \mathrm{Coeff}^{q}_{\mathbf{t},P_i} + \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}\setminus(\mathbf{s}'_1,\ldots,\mathbf{s}'_k)} H_{\mathbf{s}_1,\ldots,\mathbf{s}_k} = C^{[a_{ij_1}]}_{\mathbf{s}'_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}'_k,Q_{j_k}}\end{aligned} \tag{4.8}$$

with $H_{\mathbf{s}_1,\ldots,\mathbf{s}_k} \in \mathbb{F}_{q^2}$ known. Let us illustrate with an example what removing collision means.

Example 4.2. *For the system of equations in Example 4.1, with $s = 1$, we say we have removed the collisions if we are able to compute $H_1 \in \mathbb{F}_{q^2}$ such that*

$$\begin{aligned}&A_1B_1 + C_1 + \beta C_1^q = 0\\ &A_2B_1 + H_1 = 0\\ &A_1B_2 + C_2 + \beta C_2^q + H_1 = 0\\ &A_2B_2 + C_3 + \beta C_3^q = 0.\end{aligned}$$

Then we want to compute β and to remove the collisions. We will split the study in several cases, according to k and the form of the analogue to the matrix (3.5). First of all, let us introduce a notation that is closely related to the $\star$ operation of Example 3.1.

Definition 4.6. Given $\mathbf{E}_1, \ldots, \mathbf{E}_2$ the matrices of exponential maps of a $\mathbf{DME}_r$ scheme. We define

$$\mathbf{E}_2 \odot \mathbf{E}_1$$

as the matrix $n \times n$ whose element (i, j) is the vector obtained from the (i, j)-entry of $\mathbf{E}_2 \star \mathbf{E}_1$ (which is also a vector) by summing up the entries that are equal. For r matrices $\mathbf{E}_r \odot \ldots \odot \mathbf{E}_r$ is defined recursively.

Let see an example:

Example 4.3. *Consider the matrices of Example 3.1 and impose that $b_2 = a_1 + b_1 - a_3$. Then*

$$\mathbf{E}_2 \odot \mathbf{E}_1 = \begin{pmatrix} (2 \cdot 2^{a_1+b_1}) & (2^{a_2+b_1}, 2^{a_4+a_1+b_1-a_3}) \\ (2^{a_1+b_3}, 2^{a_3+b_4}) & (2^{a_2+b_3}, 2^{a_4+b_4}) \end{pmatrix}$$

The simplest instances to count how many collision variables corresponds to the cases where every entry of the analogue matrix to (3.5) is a list with only one element. For such instances,

$$\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} e_{11} \cdot 2^{c_{11}} & \ldots & e_{1n} \cdot 2^{c_{1n}} \\ \vdots & \ddots & \vdots \\ e_{n1} \cdot 2^{c_{n1}} & \ldots & e_{nn} \cdot 2^{c_{nn}} \end{pmatrix}$$

and the i-th row of $\mathbf{E}_r \odot \ldots \odot \mathbf{E}_1$ is

$$\big((e_{j_1 1} + \ldots + e_{j_k 1}) \cdot 2^{f_{11}}, \ldots, (e_{j_1 n} + \ldots + e_{j_k n}) \cdot 2^{f_{1n}}\big). \tag{4.9}$$

where the f_{ij} are the f's that are part of the public key (see discussion after Remark 3.11). We refer to this instances as: instances where all the possible reductions are done.

4.3.1.1 Removing collisions, case $k = 2$

We will use the following:

Proposition 4.7. *Let $k_1 = \#Supp(Q_1), k_2 = \#Supp(Q_2)$. Define*

$$\sigma : \mathbb{K}^{k_1} \times \mathbb{K}^{k_2} \longrightarrow \mathbb{K}^{k_1 k_2},$$
$$(A_1, \ldots, A_{k_1}), (B_1, \ldots, B_{k_2}) \longmapsto (C_{11}, C_{12}, \ldots, C_{k_1 k_2})$$

with $C_{ij} = A_i B_j,\ 1 \leq i \leq k_1,\ 1 \leq j \leq k_2$. Then, $Im(\sigma)$ is the algebraic set $V_{\mathbb{K}}(\mathcal{I}_{\text{Minors}(2),\mathbf{C}})$ where $\mathcal{I}_{\text{Minors}(2),\mathbf{C}}$ is the minors of order two of the matrix

$$\mathbf{C} = \begin{pmatrix} C_{11} & \ldots & C_{1k_2} \\ \vdots & \ddots & \vdots \\ C_{k_1 1} & \ldots & C_{k_1 k_2} \end{pmatrix}$$

Our goal is to derive a sufficient condition that, assuming genericity of the equations, allows us to remove the collisions. We start by a simpler case: fix i, $\text{Indices}_{P_i} = \{1, 2\}$ and assume $\mathbf{L}_{ri}$ is the identity:

Let $k_1 = \#\text{Supp}(Q_1), k_2 = \#\text{Supp}(Q_2)$,

$$\sigma : \overline{\mathbb{F}_q}^{k_1} \times \overline{\mathbb{F}_q}^{k_2} \longrightarrow \overline{\mathbb{F}_q}^{k_1 k_2},$$
$$(A_1, \ldots, A_{k_1}), (B_1, \ldots, B_{k_2}) \longmapsto (A_1 B_1, A_1 B_2, \ldots, A_{k_1} B_{k_2})$$

and $\mathbf{S} : \overline{\mathbb{F}_q}^{k_1 k_2} \to \overline{\mathbb{F}_q}^{k}, (x_{11}, \ldots, x_{1k_2}, \ldots, x_{k_1 1}, \ldots, x_{k_1 k_2}) \mapsto (l_1, \ldots, l_k)$ a surjective linear map verifying that every x_{ij}, $i = 1, \ldots, k_1$, $j = 1, \ldots, k_2$ is only in one l_r, $r = 1, \ldots, k$. Then, given $\mathbf{d} \in \text{Im}(\mathbf{S} \circ \sigma)$

we have

$$\begin{aligned}\mathbf{S}^{-1}(\mathbf{d}) \cap \operatorname{Im}(\sigma) &= \{\mathbf{x} \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{C}}) \mid \mathbf{S}(\mathbf{x}) = \mathbf{d}\}\\ &= \{\mathbf{p} + \mathbf{q} \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{C}}) \mid \mathbf{q} \in \ker(\mathbf{S})\}.\end{aligned}$$

where $\mathbf{p}$ is a point in $\mathbf{S}^{-1}(\mathbf{d}) \cap \operatorname{Im}(\sigma)$. As $\mathbf{S}$ is surjective $\dim(\ker(\mathbf{S})) = k_1k_2 - k$, therefore $\mathbf{S}^{-1}(\mathbf{d}) \cap \operatorname{Im}(\sigma)$ is

$$\{(x_{11}(H_1, \dots, H_{k_1k_2-k}), \dots, x_{k_1k_2}(H_1, \dots, H_{k_1k_2-k})) \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{C}}) \mid H_1, \dots, H_{k_1k_2-k} \in \overline{\mathbb{F}_q}\}$$

where $x_{ij}(H_1, \dots, H_{k_1k_2-k})$, $1 \leq i \leq k_1,\ 1 \leq j \leq k_2$ are polynomials of degree ≤ 1 in the variables $H_1, \dots, H_{k_1k_2-k}$. Denote by $\mathcal{I}_{\text{Minors}(2),\mathbf{M}}$ the ideal generated by the minors of order two of the matrix

$$\mathbf{M}(H_1, \dots, H_{k_1k_2-k}) = \begin{pmatrix} x_{11}(H_1, \dots, H_{k_1k_2-k}) & \dots & x_{k_11}(H_1, \dots, H_{k_1k_2-k}) \\ \vdots & \ddots & \vdots \\ x_{1k_2}(H_1, \dots, H_{k_1k_2-k}) & \dots & x_{k_1k_2}(H_1, \dots, H_{k_1k_2-k}) \end{pmatrix}.$$

and $\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}$ the minors of order two of the matrix

$$\mathbf{M}^{(h)}(H_1, \dots, H_{k_1k_2-k}) = \begin{pmatrix} x^{(h)}_{11}(H_1, \dots, H_{k_1k_2-k}) & \dots & x^{(h)}_{k_11}(H_1, \dots, H_{k_1k_2-k}) \\ \vdots & \ddots & \vdots \\ x^{(h)}_{1k_2}(H_1, \dots, H_{k_1k_2-k}) & \dots & x^{(h)}_{k_1k_2}(H_1, \dots, H_{k_1k_2-k}) \end{pmatrix}.$$

Then, $\mathbf{S}^{-1}(\mathbf{d}) \cap \operatorname{Im}(\sigma) = V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{M}})$.

Proposition 4.8. *With the notations above. Assume the following:*

- *the entries of $\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}$ behave as homogeneous polynomials of degree one with generic coefficients,*
- $\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}} = \mathcal{I}^{(h)}_{\text{Minors}(2)}$,
- *the entries of $\mathcal{I}_{\text{Minors}(2)}$ behave as affine polynomials of degree one with generic coefficients.*

Then, $\dim(\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}) = (k_1k_2 - k) - (k_1 - 1)(k_2 - 1)$. *Moreover, if $\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}$ is zero dimensional then $\mathcal{I}_{\text{Minors}(2)}$ is zero dimensional and the set $\mathbf{S}^{-1}(\mathbf{c}) \cap Im(\sigma)$ is finite.*

Proof. By Proposition 2.28, $\dim(\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}) = (k_1k_2 - k) - (k_1 - 1)(k_2 - 1)$. Now, if $\mathcal{I}^{(h)}_{\text{Minors}(2)}$ is zero dimensional, it follows immediately that $\mathcal{I}_{\text{Minors}(2)}$ is zero dimensional. As $\mathcal{I}^{(h)}_{\text{Minors}(2)} = \mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}$ by hypothesis, the claim holds. □

Remark 4.9. We refer to the three hypothesis of Proposition 4.8 as genericity conditions.

Example 4.4. *Let $k_1 = 2$ and $k_2 = 3$ and $\mathbf{S} \circ \sigma((\alpha_1, \alpha_2), (\beta_1, \beta_2, \beta_3)) = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_1\beta_3, \alpha_2\beta_1 + \alpha_2\beta_2 + \alpha_2\beta_3)$. Then,*

$$\begin{aligned}
&\mathbf{S}^{-1}(\mathbf{d}) \cap Im(\sigma) = \{\mathbf{x} \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2)}) \mid \mathbf{S}(\mathbf{x}) = \mathbf{d}\} \\
&= \{(x_1, \ldots, x_6) \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2)}) \mid x_1 = d_1, x_2 = d_2, x_3 = d_3, x_4 + x_5 + x_6 = d_4\} \\
&= \{(d_1, d_2, d_3, H_1, H_2, d_4 + H_1 + H_2) \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2)}) \mid H_1, H_2, H_3 \in \overline{\mathbb{F}_q}\}.
\end{aligned}$$

Let

$$\mathbf{M}(H_1, H_2) = \begin{pmatrix} d_1 & d_2 & d_3 \\ H_1 & H_2 & d_4 + H_1 + H_2 \end{pmatrix},$$

assuming that the genericity conditions holds, we have

$$\dim(\mathcal{I}^{(h)}_{\text{Minors}(2),\mathbf{M}}) = (3 \cdot 2 - 4) - (3 - 1)(2 - 1) = 0$$

and therefore $\mathbf{S}^{-1}(\mathbf{d}) \cap Im(\sigma)$ is finite.

In the case we are in the scenario where the previous result holds we can compute the set of finite points in $\mathbf{S}^{-1}(\mathbf{c})$ and for each $\mathbf{d} = (\alpha_{11}, \ldots, \alpha_{k_1k_2}) \in \mathbf{S}^{-1}(\mathbf{c})$, we have that

$$\sigma^{-1}(\mathbf{d}) = \{((A_1, \frac{\alpha_{21}A_1}{\alpha_{11}}, \ldots, \frac{\alpha_{k_11}A_1}{\alpha_{11}}), (\frac{\alpha_{11}}{A_1}, \frac{\alpha_{12}}{A_1}, \ldots, \frac{\alpha_{1k_2}}{A_1})) \mid A_1 \neq 0\}.$$

We generalize this result by adding a new parameter β: Let $k_1 = \#\text{Supp}(Q_1), k_2 = \#\text{Supp}(Q_2)$, and σ and $\mathbf{S}$ as before. Then, for $\mathbf{d} \in \text{Im}(\mathbf{S} \circ \sigma)$,

$$\left(\bigcup_{\beta \in \overline{\mathbb{F}_q}} \mathbf{S}^{-1}(\mathbf{c} + \beta\mathbf{c}^q)\right) \bigcap \text{Im}(\sigma)$$

$$= \{(x_{11}(H_1, \ldots, H_{k_1k_2-k}, \beta), \ldots, (x_{k_1k_2}(H_1, \ldots, H_{k_1k_2-k}, \beta)) \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{C}}) \mid H_1, \ldots, H_{k_1k_2-k}, \beta \in \overline{\mathbb{F}_q}\}.$$

Therefore,

$$\left(\bigcup_{\beta \in \overline{\mathbb{F}_q}} \mathbf{S}^{-1}(\mathbf{d} + \beta\mathbf{d}^q)\right) \bigcap \text{Im}(\sigma) = V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{M}})$$

where

$$\mathbf{M}(H_1, \ldots, H_{k_1k_2-k}, \beta) = \begin{pmatrix} x_{11}(H_1, \ldots, H_{k_1k_2-k}, \beta) & \ldots & x_{k_11}(H_1, \ldots, H_{k_1k_2-k}, \beta) \\ \vdots & \ddots & \vdots \\ x_{1k_2}(H_1, \ldots, H_{k_1k_2-k}, \beta) & \ldots & x_{k_1k_2}(H_1, \ldots, H_{k_1k_2-k}, \beta) \end{pmatrix}. \quad (4.10)$$

Proposition 4.10. *With the notations above and let $\mathbf{M} = \mathbf{M}(H_1, \ldots, H_{k_1k_2-k}, \beta)$. Assume the genericity conditions holds for $\mathbf{M}$. Then, $\dim(\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}) = (k_1k_2 - k) + 1 - (k_1 - 1)(k_2 - 1)$.*

Moreover, if $\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}$ is zero dimensional then $\mathcal{I}_{\text{Minors}(2)}$ is zero dimensional and the set

$$\left(\bigcup_{\beta\in\overline{\mathbb{F}_q}} \mathbf{S}^{-1}(\mathbf{c}+\beta\mathbf{c}^q)\right)\bigcap Im(\sigma)$$

is finite.

Example 4.5. *Let σ and $\mathbf{S}$ as in the previous example.*

$$\left(\bigcup_{\beta\in\overline{\mathbb{F}_q}} \mathbf{S}^{-1}(\mathbf{d}+\beta\mathbf{d}^q)\right)\bigcap Im(\sigma)$$
$$= \{(d_1+\beta d_1^q, d_2+\beta d_2^q, d_3+\beta d_3^q, H_1, H_2, d_4+\beta d_4^q+H_1+H_2) \in V_{\overline{\mathbb{F}_q}}(\mathcal{I}_{\text{Minors}(2),\mathbf{C}}) \mid H_1, H_2\beta \in \overline{\mathbb{F}_q}\}.$$

Let

$$\mathbf{M}(H_1,H_2) = \begin{pmatrix} d_1+\beta d_1^q & d_2+\beta d_2^q & d_3+\beta d_3^q \\ H_1 & H_2 & d_4+\beta d_4^q+H_1+H_2 \end{pmatrix}.$$

Assuming that the genericity conditions holds

$$\dim(\mathcal{I}^{(h)}_{\text{Minors}(2),\mathbf{M}}) = (3\cdot 2-4)+1-(3-1)(2-1) = 1 > 0.$$

Systems of equations (4.3) have the structure described in Proposition 4.10, the map $\mathbf{S}$ is implicitly defined by the reductions that has the **DME** map we are considering. Saying that the set

$$\left(\bigcup_{\beta\in\overline{\mathbb{F}_q}} \mathbf{S}^{-1}(\mathbf{c}+\beta\mathbf{c}^q)\right)\bigcap \text{Im}(\sigma)$$

is finite is equivalent to saying that there only exist a finite number of possible values for β and the H_i's. Therefore, we can build a matrix $\mathbf{M}$ as in Proposition 4.10 and consider the ideal $\mathcal{I}_{\text{Minors}(2),\mathbf{M}}$. If such ideal is zero dimensional then β and the H_i's variables can only take a finite number of values. In the following, we refer to variables H_i's as collision variables.

Example 4.6. *As a toy example let*

$$\mathbf{E}_1 = \begin{pmatrix} [a_1] & [a_2] \\ [a_3] & [a_4] \end{pmatrix} \text{ and } \mathbf{E}_2 = \begin{pmatrix} [b_1] & [b1+a1-a3] \\ [b_3] & [b3+a2-a4] \end{pmatrix}.$$

Then the system of equations corresponding to P_1 is obtained from

$$Q_1^{[b_1]}Q_2^{[b_1+a_1-a_3]} = P_1+\beta P_1^q.$$

By Proposition 4.10, assuming the genericity conditions holds: if the number of collisions that we get plus one, which comes from the unknown linear map, is lower or equal than $(k_1-1)(k_2-1)$

being $k_1 = \#Supp(Q_1), k_2 = \#Supp(Q_2)$ *then* $\mathcal{I}_{\text{Minors}(2),\mathbf{M}}$ *is zero dimensional. Therefore, the value of collision variables and* β *can be determined (meaning that the variety where the solutions are is zero dimensional over* $\overline{\mathbb{F}_q}$*).*

Explicitly, the system of equations is the following:

$$
\begin{aligned}
&A_1^{[b_1]}B_1^{[b1+a1-a3]} = R_1 + \beta \cdot R_1^q\\
&A_1^{[b_1]}B_2^{[b1+a1-a3]} + A_2^{[b_1]}B_1^{[b1+a1-a3]} = R_2 + \beta \cdot R_2^q\\
&A_1^{[b_1]}B_3^{[b1+a1-a3]} = R_3 + \beta \cdot R_3^q\\
&A_1^{[b_1]}B_4^{[b1+a1-a3]} + A_2^{[b_1]}B_3^{[b1+a1-a3]} = R_4 + \beta \cdot R_4^q\\
&A_2^{[b_1]}B_2^{[b1+a1-a3]} = R_5 + \beta \cdot R_5^q\\
&A_2^{[b_1]}B_4^{[b1+a1-a3]} = R_6 + \beta \cdot R_6^q\\
&A_3^{[b_1]}B_1^{[b1+a1-a3]} = R_7 + \beta \cdot R_7^q\\
&A_3^{[b_1]}B_2^{[b1+a1-a3]} + A_4^{[b_1]}B_1^{[b_2]} = R_8 + \beta \cdot R_8^q\\
&A_3^{[b_1]}B_3^{[b1+a1-a3]} = R_9 + \beta \cdot R_9^q\\
&A_3^{[b_1]}B_4^{[b1+a1-a3]} + A_4^{[b_1]}B_3^{[b1+a1-a3]} = R_{10} + \beta \cdot R_{10}^q\\
&A_4^{[b_1]}B_2^{[b1+a1-a3]} = R_{11} + \beta \cdot R_{11}^q\\
&A_4^{[b_1]}B_4^{[b1+a1-a3]} = R_{12} + \beta \cdot R_{12}^q
\end{aligned}
\tag{4.11}
$$

In this example we have 4 *collisions and* 1 *unknown parameter,* β*, coming from the linear* $\mathbf{L}_{21}^{-1}$ *so we obtain* 5 *variables which is lower than* $(4-1)(4-1)$ *therefore we expect a finite number of ways of split the equations that involve collisions.*

All the reductions done

Let us move to a more general scenario and explain how we can get the number of collisions without writing the system of equations. Then,

$$
\begin{aligned}
\#\text{Supp}(Q_{j_1}) &= (e_{j_1 1}+1)\dots(e_{j_1 n}+1)\\
\#\text{Supp}(Q_{j_2}) &= (e_{j_2 1}+1)\dots(e_{j_2 n}+1)\\
&\vdots\\
\#\text{Supp}(Q_{j_k}) &= (e_{j_k 1}+1)\dots(e_{j_k n}+1).
\end{aligned}
$$

Recall that $\text{Supp}(Q_{j_1}),\dots,\text{Supp}(Q_{j_k})$ is the number of variables $C_{\mathbf{t},Q_{j_1}},\dots,C_{\mathbf{t},Q_{j_k}}$ – which represent the coefficients of $Q_{j_1},\dots,Q_{j_k}$– respectively. Consequently, if applying $\mathbf{E}_r$ had caused no collisions we would have obtained a system of $\#\text{Supp}(Q_{j_1})\cdot\dots\cdot\#\text{Supp}(Q_{j_k})$ equations. However, the assumption of (4.9) means that all the possible collisions have been occurred and therefore the number of equations (that is equal to $\#\text{Supp}(P_i)$) is

$$(e_{j_1 1} + \ldots + e_{j_k 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + \ldots + e_{j_k n} + 1)$$

In the case $k = 2$ we can build a matrix $\mathbf{M}$ as in the proof of Proposition (4.10). Under genericity conditions, a sufficient condition to obtain only a finite number of possible values for the collisions variables and β is that the ideal $\mathcal{I}^h_{\text{Minors}(2),\mathbf{M}}$ is zero-dimensional. The following result proves that $\mathcal{I}_{\text{Minors}(2),\mathbf{M}^{(h)}}$ – which is equal to $\mathcal{I}^h_{\text{Minors}(2),\mathbf{M}}$ by genericity conditions – has dimension zero, under some light extra assumptions.

Proposition 4.11. *Let $n \geq 2$ and assume $e_{j_1 k_1}, e_{j_2 k_2} \geq 1$ where $k_1 \neq k_2$, $1 \leq k_1, k_2, \leq n$, then*

$$\begin{aligned} &MN - (e_{j_1 1} + e_{j_2 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1) + 1 \\ &\leq (M-1) \cdot (N-1) \end{aligned} \tag{4.12}$$

where $M = \#Supp(Q_{j_1}), N = \#Supp(Q_{j_2})$

Proof. (Case $k = 2$ all collisions done) Assume without loss of generality that $j_1 = 1, j_2 = 2, k_1 = 1, k_2 = 2$. To prove that

$$MN \ - \ \prod_{i=1}^{n} \big(e_{1i} + e_{2i} + 1\big) \ + \ 1 \ \leq \ (M-1)\,(N-1)$$

setting

$$P = \prod_{i=1}^{n} (e_{1i} + e_{2i} + 1),$$

we need to show

$$MN - P + 1 \ \leq \ (M-1)(N-1) \quad \Longleftrightarrow \quad P \ \geq \ M + N.$$

By induction on $n > 1$.

For $n = 2$, write

$$X_i = e_{1i}, \quad Y_i = e_{2i}.$$

We must prove

$$(X_1 + Y_1 + 1)(X_2 + Y_2 + 1) \ \geq \ (X_1 + 1)(X_2 + 1) \ + \ (Y_1 + 1)(Y_2 + 1).$$

The left hand side is:

$$X_1X_2 + X_1Y_2 + Y_1X_2 + Y_1Y_2 + X_1 + X_2 + Y_1 + Y_2 + 1.$$

The right hand side is:

$$X_1X_2 + X_1 + X_2 + 1 + Y_1Y_2 + Y_1 + Y_2 + 1 \;=\; X_1X_2 + Y_1Y_2 + X_1 + X_2 + Y_1 + Y_2 + 2.$$

Subtracting them,

$$(X_1Y_2 + Y_1X_2) - 1 \;\geq\; 1 - 1 = 0,$$

since $X_1, Y_2 \geq 1$.

Assume the claim holds for $n-1$; we show it for n. Write

$$M = M'\,(X_n + 1), \quad N = N'\,(Y_n + 1), \quad P = P'\,(X_n + Y_n + 1),$$

where

$$M' = \prod_{i=1}^{n-1}(X_i + 1),\; N' = \prod_{i=1}^{n-1}(Y_i + 1),\; P' = \prod_{i=1}^{n-1}(X_i + Y_i + 1).$$

By the inductive hypothesis,

$$P' \;\geq\; M' + N'.$$

We must show

$$P'\,(X_n + Y_n + 1) \;\geq\; M'\,(X_n + 1) \;+\; N'\,(Y_n + 1).$$

That is,

$$P'\,(X_n + Y_n + 1) \;-\; M'(X_n + 1) \;-\; N'(Y_n + 1) \;\geq\; 0.$$

Use $P' \geq M' + N'$:

$$\begin{aligned} P'(X_n + Y_n + 1) &\geq (M' + N')(X_n + Y_n + 1) \\ &= M'X_n + M'Y_n + M' + N'X_n + N'Y_n + N' \\ &= \big[M'(X_n + 1) + N'(Y_n + 1)\big] \;+\; \big[N'X_n + M'Y_n\big]. \end{aligned}$$

Since $M', N' \geq 2$,

$$N'X_n + M'Y_n \geq 0.$$

Hence

$$P'(X_n + Y_n + 1) \ \geq \ M'(X_n + 1) + N'(Y_n + 1),$$

completing the induction. □

Case arbitrary number of reductions done

To finish we show that the previous computations can be done for the more general setting where not all the collisions have been done because, for example, they prevent the last exponential from being invertible.

We restrict for the sake of clarity the exposition to the case $k = 2$.

Recall that in the case analyzed above we had

$$\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} (e_{11} \cdot 2^{c_{11}}) & \cdots & (e_{1n} \cdot 2^{c_{1n}}) \\ \vdots & \vdots & \vdots \\ (e_{n1} \cdot 2^{c_{n1}}) & \cdots & (e_{nn} \cdot 2^{c_{nn}}) \end{pmatrix}$$

where $e_{ij} \in \mathbb{Z}_{\geq 0}$. However, in the actual setting

$$\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} (e^{\ell}_{11} \cdot 2^{c^{\ell}_{11}})_{1 \leq \ell \leq k_{11}} & \cdots & (e^{\ell}_{1n} \cdot 2^{c^{\ell}_{1n}})_{1 \leq \ell \leq k_{1n}} \\ \vdots & \ddots & \vdots \\ (e^{\ell}_{n1} \cdot 2^{c^{\ell}_{n1}})_{1 \leq \ell \leq k_{n1}} & \cdots & (e^{\ell}_{nn} \cdot 2^{c^{\ell}_{nn}})_{1 \leq \ell \leq k_{nn}} \end{pmatrix}.$$

When the $2^{c_{ij}}$ are not relevant, we will simply write

$$\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} \mathbf{e}_{11} & \cdots & \mathbf{e}_{1n} \\ \vdots & \vdots & \vdots \\ \mathbf{e}_{n1} & \cdots & \mathbf{e}_{nn} \end{pmatrix}$$

where $\mathbf{e}_{ij} = (e^1_{ij}, \ldots, e^{k_{ij}}_{ij}), 1 \leq i, j \leq n.$

The result in this setting is:

Proposition 4.12. *Let* $\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} \mathbf{e}_{11} & \cdots & \mathbf{e}_{1n} \\ \vdots & \vdots & \vdots \\ \mathbf{e}_{n1} & \cdots & \mathbf{e}_{nn} \end{pmatrix}$. *Then the number of terms that came from* $\mathbf{e}_{ij}$ *is* $\prod_{\ell=1}^{k_{ij}} (e_{ij}^{\ell} + 1)$. *Consequently,*

$$\#Supp(Q_i) = \prod_{j=1}^{n} \prod_{\ell=1}^{k_{ij}} (e_{ij}^{\ell} + 1).$$

Proof. Fix i, j, then the number of terms that result from $\mathbf{e}_{ij} = (e_{ij}^{\ell})_{1 \leq \iota \leq k_{ij}}$ are

$$[x_{2i-1}, x_{2i}], [e_{ij}^{1}, \ldots, e_{ij}^{k_{ij}}]$$

which is the ways of putting $\sum_{\ell=1}^{k_{ij}} e_{ij}^{\ell}$ balls of k_{ij} different types into two boxes.

$$\prod_{\iota=1}^{l} \binom{e_{ij}^{(\iota)} + 2 - 1}{2 - 1}$$

□

To understand the difference with the previous setting: if the first row of $\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1$ is $(2, 1, 0, 0)$ there are several options for the matrices: if the first row of $\mathbf{E}_{r-1} \cdot \ldots \cdot \mathbf{E}_1$ is

$$((2^{c_1}, 2^{c_2}), 2^{c_3}, 0, 0)$$

then $\mathbf{e}_{11} = [1, 1]$ and $\mathbf{e}_{12} = [1]$ whereas if the first row of $\mathbf{E}_{r-1} \cdot \ldots \cdot \mathbf{E}_1$ is

$$(2 \cdot 2^{c_1}, 2^{c_3}, 0, 0)$$

then $\mathbf{e}_{11} = [2]$ and $\mathbf{e}_{12} = [1]$. Consequently, in the first case the number of variables is $(1 + 1) \cdot (1 + 1) \cdot (1 + 1)$ while in the second is $(2 + 1) \cdot (1 + 1)$.

General setting $k = 2$ proof. Assume that $j_1 = 1, j_2 = 2$, and $\mathbf{E}_r = ([a_{ij}])_{1 \leq i,j \leq n}$ and let $\mathbf{e}_{1j} = (e_{1j}^{(\iota_j)})_{1 \leq \iota_j \leq k_{1j}}$ for $1 \leq j \leq n$ and $\mathbf{e}_{2j} = (e_{2j}^{(\tau_j)})_{1 \leq \tau_j \leq k_{2j}}$ for $1 \leq j \leq n$. If there exists j in which a collision appear, there exist unique ι_0, τ_0 such that $c_{1j}^{(\iota_j)} + a_{1j} = c_{2j}^{(\tau_j)} + a_{2j}$. Consequently, for such j the number of variables before $\mathbf{E}_r$ in the first component is

$$\prod_{\iota_j=1}^{k_{1j}} (e_{1j}^{(\iota_j)} + 1)$$

and in the second

$$\prod_{\tau_j=1}^{k_{2j}=1} (e_{2j}^{(\tau_j)} + 1).$$

And after $\mathbf{E}_r$ the resulting component has

$$\prod_{\iota_j\neq\iota_0}(e_{1j}^{(\iota_j)}+1)\prod_{\tau_j\neq\tau_0}(e_{2j}^{(\tau_j)}+1)(e_{1j}^{(\iota_0)}+e_{2j}^{(\tau_0)}+1).$$

Now, assume that scenario described for a fix j happens only once, say for j_0. In such a case our claim is that defining

$$M=\prod_{j=1}^{n}\prod_{\iota_j}(e_{1j}^{(\iota)}+1),$$

$$N=\prod_{j=1}^{n}\prod_{\tau_j}(e_{2j}^{(\tau)}+1),$$

$$P=(\prod_{j\neq j_0}\prod_{\iota_j}(e_{1j}^{(\iota)}+1)\prod_{j\neq j_0}\prod_{\tau_j}(e_{2j}^{(\tau)}+1))\prod_{\iota_{j_0}\neq\iota_0}(e_{1j}^{(\iota)}+1)\prod_{\tau_{j_0}\neq\tau_0}(e_{2j_0}^{(\tau)}+1)(e_{1j_0}^{(\iota_0)}+e_{2j_0}^{(\tau_0)}+1).$$

we have

$$MN-P+1\leq(M-1)(N-1).$$

Setting

$$M=M_1(e_{1j_0}^{\iota_0}+1),N=N_1(e_{2j_0}^{\tau_0}+1)$$

we have that

$$P=M_1N_1(e_{1j_0}^{\iota_0}+e_{2j_0}^{\tau_0}+1).$$

Therefore we only need to prove that

$$M_1N_1(e_{1j_0}^{\iota_0}+1)(e_{2j_0}^{\tau_0}+1)-M_1N_1(e_{1j_0}^{\iota_0}+e_{2j_0}^{\tau_0}+1)+1\leq(M_1(e_{1j_0}^{\iota_0}+1)-1)(N_1(e_{2j_0}^{\tau_0}+1)-1)$$

or equivalently

$$M_1N_1(e_{1j_0}^{\iota_0}+e_{2j_0}^{\tau_0}+1)\geq M_1(e_{1j_0}^{\iota_0}+1)+N_1(e_{2j_0}^{\tau_0}+1).$$

Assuming $M_1,N_1\geq 2$ we have $M_1N_1\geq M_1+N_1$ and then

$$M_1(e_{1j_0}^{\iota_0}+1)+N_1(e_{2j_0}^{\tau_0}+1)\leq(M_1+N_1)(e_{1j_0}^{\iota_0}+e_{2j_0}^{\tau_0}+1)\leq M_1N_1(e_{1j_0}^{\iota_0}+e_{2j_0}^{\tau_0}+1).$$

On the other hand, if there are collisions for more than one j, let say $j_1,\ldots,j_k,k>1$. Then we can repeat the reasoning but now we get

$$\begin{aligned}M&=M_1(e_{1j_1}^{\iota_1}+1)\cdot\ldots\cdot(e_{1j_k}^{\iota_k}+1),\\N&=N_1(e_{2j_1}^{\tau_1}+1)\cdot\ldots\cdot(e_{2j_k}^{\tau_k}+1),\\P&=M_1N_1(e_{1j_1}^{\iota_1}+e_{2j_1}^{\tau_1}+1)\cdot\ldots\cdot(e_{1j_k}^{\iota_k}+e_{2j_k}^{\tau_k}+1)\end{aligned}$$

and need to prove that

$$MN - P + 1 \leq (M-1)(N-1)$$

or equivalently

$$P \geq M + N$$

The fact that the $k > 1$ allows us to use Proposition 4.11 to get that

$$\frac{P}{M_1 N_1} \geq \frac{M}{M_1} + \frac{N}{N_1}.$$

Multiplying by $M_1 N_1 > 0$ we get

$$P \geq N_1 M + M_1 N \geq M + N.$$

□

4.3.1.2 Removing collisions, case $k > 2$

When $k > 2$, we can arrange the entries in a k-order hypermatrix whose edges are indexed by the variables $C_{\mathbf{t},Q_{j_1}}, C_{\mathbf{t},Q_{j_2}}, \ldots, C_{\mathbf{t},Q_{j_k}}$, which we recall are the coefficients of polynomials before the last exponential $\mathbf{E}_r$ – which is the natural generalization of a matrix as in the proof of Proposition 4.10. In order to get a result similar to Proposition 4.11, we would like to obtain matrices from the hyper-matrix.

This leads us to introduce the notion of flattening of a hypermatrix.

Definition 4.13. Let $\mathbf{A} = (a_{i_1,\ldots,i_k})_{(i_1,\ldots,i_k)\in I_1\times I_2\times\ldots\times I_k} \in \overline{\mathbb{K}}^{I_1\times I_2\times\ldots\times I_k}$ a k-order hypermatrix. For $1 \leq m \leq k$, the mode-$[m]$ flattening of $\mathbf{A}$, denoted as $\mathbf{A}_{[m]}$, is defined as the $I_m \times (I_1 \cdot \ldots \cdot I_{m-1} \cdot \check{I}_m \cdot I_{m+1} \cdot \ldots I_k)$ matrix whose entry (r,s) is the element $a_{i_1,\ldots,i_k}$ of $\mathbf{A}$ such that

$$r = i_m$$

and

$$s = 1 + \sum_{n=1, n\neq m}^{k} (i_n - 1) \prod_{l=1, l\neq m}^{n-1} I_l$$

with the convention that $\prod_{l=1,l\neq m}^{n-1} I_l = 1$ if $\{l : 1 \leq l \leq n-1, l \neq m\} = \emptyset$.

Let us illustrate with an example that the notion of mode-$[m]$ flattening is intuitive.

Example 4.7. *Assume we have $k = 3$ and let $A = (a_{ij\ell})_{1\leq i,j\leq 2, 1\leq \ell\leq 3}$.*

Then, the mode-$[1]$ *flattening is the matrix*

$$A_{[1]} = \begin{pmatrix} a_{111} & a_{121} & a_{131} & a_{112} & a_{122} & a_{132} & a_{113} & a_{123} & a_{133} \\ a_{211} & a_{221} & a_{231} & a_{212} & a_{222} & a_{232} & a_{213} & a_{223} & a_{233} \end{pmatrix}.$$

Let us illustrate the process of removing collisions for $k = 3$.

Example 4.8. *Assume we have the following system of equations*

$$\begin{aligned}
&A_1B_1C_1 = c_1 + \beta c_1^q\\
&A_1B_1C_2 = c_2 + \beta c_2^q\\
&A_1B_2C_1 + A_2B_1C_1 = c_3 + \beta c_3^q\\
&A_1B_2C_2 + A_2B_1C_2 = c_4 + \beta c_4^q\\
&A_2B_2C_1 = c_5 + \beta c_5^q\\
&A_2B_2C_2 = c_6 + \beta c_6^q.
\end{aligned}$$

Then, by adding the collision variables we obtain

$$\begin{aligned}
&A_1B_1C_1 = c_1 + \beta c_1^q\\
&A_1B_1C_2 = c_2 + \beta c_2^q\\
&A_1B_2C_1 = H_1\\
&A_2B_1C_1 = c_3 + \beta c_3^q + H_1\\
&A_1B_2C_2 = H_2\\
&A_2B_1C_2 = c_4 + \beta c_4^q + H_2\\
&A_2B_2C_1 = c_5 + \beta c_5^q\\
&A_2B_2C_2 = c_6 + \beta c_6^q.
\end{aligned}$$

We can describe 3*-order hypermatrix,* $\mathbf{M} = (m_{ij\ell})_{1\leq i,j,\ell\leq 2}$*, associated with this system by listing its elements:*

$$\begin{gathered}
m_{111} = c_1 + \beta c_1^q,\ m_{112} = c_2 + \beta c_2^q,\ m_{121} = H_1,\ m_{211} = c_3 + \beta c_3^q + H_1\\
m_{122} = H_2,\ m_{212} = c_4 + \beta c_4^q + H_2,\ m_{221} = c_5 + \beta c_5^q,\ m_{222} = c_6 + \beta c_6^q
\end{gathered}$$

Then we consider the mode-[1] *flattening*

$$\mathbf{M}_{[1]} = \begin{pmatrix} c_1 + \beta c_1^q & H_1 & c_2 + \beta c_2^q & H_2 \\ c_3 + \beta c_3^q + H_1 & c_5 + \beta c_5^q & c_4 + \beta c_4^q + H_2 & c6 + \beta c_6^q \end{pmatrix} \tag{4.13}$$

If the ideal generated by the minors of order two of $\mathbf{M}_{[1]}$ *is zero dimensional we get a finite number of possible values for* H_1, H_2, β*.*

The matrices of which we consider the minors of order two will not be the mode-$[m]$ flattenings but a reduction. We do this to reduce the number of collision variables as well as the size of the matrices.

Definition 4.14 (Reduced mode-m flattening)**.** Let $\mathbf{M}_{[m]}$ be a matrix of the form (4.13) coming from a system (4.7). then the reduced mode-$[m]$ flattening is obtained from $M_{[m]}$ by summing up those columns for which the elements with the same row index have a collision variable in common.

Example 4.9. *Continuing with the previous example:*

- *The reduced mode-*$[1]$ *flattening of* $\mathbf{M}_{[1]}$ *is itself.*
- *The mode-*$[3]$ *flattening is*

$$\mathbf{M}_{[3]} = \begin{pmatrix} c_1 + \beta c_1^q & H_1 & c_3 + \beta c_3^q + H_1 & c_5 + \beta c_5^q \\ c_2 + \beta c_2^q & c_4 + \beta c_4^q + H_2 & H_2 & c_6 + \beta c_6^q \end{pmatrix}$$

and therefore the reduced mode-$[3]$ *flattening is*

$$\begin{pmatrix} c_1 + \beta c_1^q & c_3 + \beta c_3^q & c_5 + \beta c_5^q \\ c_2 + \beta c_2^q & c_4 + \beta c_4^q & c_6 + \beta c_6^q \end{pmatrix}$$

Example 4.10. *Consider the system of equations from*

```
https://github.com/pilarcoscojuela/Thesis/blob/DME_minus_3_entries/
components_1_and_2.txt
```

Compare magma example with reduced mode-$[1]$ *and mode-*$[1]$*: the reduced mode-*$[1]$ *is a matrix* 4×2 *with row indices*

```
[
R1*K1+R2*K2,
R2*K3,
R1*K3+R2*K1,
R1*K2
]
```

and column indices

```
[
X1,
X2
]
```

while the mode-$[1]$ *is a matrix* 2×6 *with columns indices*

```
[
R1,
R2
]
```

and row indices

```
[
K1*X1,
K2*X1,
K3*X1,
K1*X2,
K2*X2,
K3*X2
]
```

Assume $k = 3$, if we split the summands that have different variables of Q_{j_3} – that is, we are considering the reduced mode-[3] flattening – we obtain a matrix of size

$$\#\mathrm{Supp}(Q_{j_3}) \times ((e_{j_1 1} + e_{j_2 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1)).$$

The number of equations without any collision is now

$$(e_{j_1 1} + e_{j_2 1} + 1) \cdot (e_{j_3 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1) \cdot (e_{j_3 n} + 1)$$

because we do not count collisions coming from $Q_{j_1}^{[a_{ij_1}]} Q_{j_2}^{[a_{ij_2}]}$. Moreover, the number of equations when we split them according to different variables of Q_{j_3} is

$$(e_{j_1 1} + e_{j_2 1} + e_{j_3 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + e_{j_3 n} + 1)$$

Therefore, under genericity assumptions, the ideal $\mathcal{I}_{\mathrm{Minors}(2)}$ will be zero dimensional if

$$\begin{aligned}
&(e_{j_1 1} + e_{j_2 1} + 1) \cdot (e_{j_3 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1) \cdot (e_{j_3 n} + 1) \\
&- (e_{j_1 1} + e_{j_2 1} + e_{j_3 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + e_{j_3 n} + 1) + 1 \\
&\leq ((e_{j_1 1} + e_{j_2 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1) - 1) \cdot (\#\mathrm{Supp}(Q_{j_3}) - 1)
\end{aligned}$$

Proposition 4.15. *Assume $n \geq 2$ and $e_{j_1 k_1}, e_{j_3 k_2} \geq 1$ with $k_1 \neq k_2$, $1 \leq k_1, k_2 \leq n$ then*

$$\begin{aligned}
&((e_{j_1 1} + e_{j_2 1} + 1) \cdot (e_{j_3 1} + 1)) \cdot \ldots \\
&\cdot ((e_{j_1 n} + e_{j_2 n} + 1) \cdot (e_{j_3 n} + 1)) \\
&- (e_{j_1 1} + e_{j_2 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1) + 1 \\
&\leq ((e_{j_1 1} + e_{j_2 1} + 1) \cdot \ldots \cdot (e_{j_1 n} + e_{j_2 n} + 1) - 1) \cdot (\#\mathit{Supp}(Q_{j_3}) - 1)
\end{aligned}$$

Proof. For each coordinate $i = 1, \ldots, n$ set

$$A_i \;=\; e_{j_1 i} + e_{j_2 i}, \quad B_i \;=\; e_{j_3 i}.$$

Then

- $\displaystyle\prod_{i=1}^{n}(A_i + 1) = (e_{j_1 1} + e_{j_2 1} + 1) \cdots (e_{j_1 n} + e_{j_2 n} + 1)$,
- $\displaystyle\prod_{i=1}^{n}(B_i + 1) = \#\mathrm{Supp}\, q_{j_3}$,
- $\displaystyle\prod_{i=1}^{n}(A_i + B_i + 1) = (e_{j_1 1} + e_{j_2 1} + 1) \cdots (e_{j_1 n} + e_{j_2 n} + 1)$.

But we already proved for any sequences $\{A_i\}$, $\{B_i\}$ such that there exists $A_{k_1}, B_{k_2} \geq 1$ with $k_1 \neq k_2$, $1 \leq k_1, k_2 \leq n$, the inequality

$$\prod_{i=1}^{n}(A_i + 1) \prod_{i=1}^{n}(B_i + 1) \;-\; \prod_{i=1}^{n}(A_i + B_i + 1) + 1 \;\leq\; \Big(\prod_{i=1}^{n}(A_i + 1) - 1\Big) \Big(\prod_{i=1}^{n}(B_i + 1) - 1\Big).$$

□

Remark 4.16. Experimentally, to solve the system as (4.7) with $k = 3$, we got that it is enough to consider first the reduced mode-$[m]$ for a $m \in \{1, 2, 3\}$. This gives a matrix from which, assuming genericity, we will obtain that the ideal of minors of order two if zero dimensional by Proposition 4.15. Hence, a finite number of possible values for the collision variables (that appear in this matrix) and the parameter of the linear. Substitute these values to simplify the original system of equations we want to solve. Then, we take $m' \in \{1, 2, 3\}$, $m' \neq m$ and repeat the process. Finally, do it one last time with $m'' \in \{1, 2, 3\}$, $m'' \neq m'$, $m'' \neq m$. In this way collision variables are not recover at once but in three steps. This is useful (cf. Example 4.10) when the number of collision variables is big to reduce the complexity (see 2.17). However, if the number of collision variables is small, it is enough to consider the matrix of a mode-$[m]$ flattening, for a $m \in \{1, 2, 3\}$, and compute a Gröbner basis of the ideal of minors of order two of this matrix.

Remark 4.17. For the case $k \geq 4$ similar techniques can be used but the combinatorics become more complicated.

We have proven that the ideal we get for examples of $\mathbf{DME}_r$ is zero dimensional, assuming genericity conditions, as soon as some light technical assumptions on the entries of the exponential matrices hold.

By Proposition 2.17 the complexity of computing a DRL Gröbner basis of $\mathcal{I}_{\mathrm{Minors}(2)}$ is upper-bounded by:

$$O\left(\binom{m}{2}\binom{n}{2}\binom{k + \mathrm{d_{reg}}(\mathcal{I}_{\mathrm{Minors}(2),\mathbf{M}})}{k}^{\omega}\right)$$

where $\binom{m}{2}\binom{n}{2}$ is the number of equations we have and k are the number of variables. Moreover, as the matrix of which we take the minors has entries that are affine polynomials of degree one, by Theorem 2.29 we have that the degree of regularity when compute a DRL Gröbner basis of $\mathcal{I}_{\mathrm{Minors}(2),\mathbf{M}}$, associated with a matrix $\mathbf{M}(x_1,\ldots,x_k)$ of size $m \times n$, is bounded by $\min(m,n)$. Therefore, we want to reduce the number of variables k and the size of matrices so that the complexity bound is not so high. This leads to consider weights.

Remark 4.18. Note that $\mathrm{d}_{\mathrm{reg}} \leq \min(m,n)$ provides an upper bound, but for specific parameter configurations we can compute the exact value. For instance, in the instance attacked in [2], we obtain $\mathrm{d}_{\mathrm{reg}} = 2$, since the hypotheses of Proposition 2.34 are satisfied.

4.4 Reduction of the number of variables: DME 2023

We want to keep the size of the matrix relatively small so that we can compute the collision variables fast. That is the reason why we present here a method that allows to reduce drastically the number of variables $C_{\mathbf{t}Q_{j_1}},\ldots,C_{\mathbf{t}Q_{j_k}}$ and consequently the size of the matrices.

By construction of the scheme note that the terms that form the support of the public key polynomials are symmetric within every pair of variables $[x_{2i-1},x_{2i}]$, meaning that if $\mathbf{t}(x_1,x_2,\ldots,x_N) \in \mathrm{Supp}(P_j)$ then all the terms obtained by flipping $[x_{2i-1},x_{2i}]$ are also in the support of P_j. Indeed, all such terms are mapped to the same term via the following map

$$\sigma : \mathbb{F}_q[x_1,\ldots,x_N] \to \mathbb{F}_q[t_1,\ldots,t_n], \quad x_{2i-1} \mapsto t_i, x_{2i} \mapsto t_i,\ i = 1,\ldots,n.$$

To have more flexibility, we define the σ map more generally.

Definition 4.19 (Weight-reduction map)**.** Take $j_1,\ldots,j_k \in \{1,\ldots,n\}$ pairwise distinct. The weight-reduction map σ associated to $j_1,\ldots,j_k$ is defined as:

$$\begin{aligned} \sigma_{j_1,\ldots,j_k} : \mathbb{F}_{q^2}[x_1,\ldots,x_N] &\longrightarrow \mathbb{F}_{q^2}[t_1,\ldots,t_{k+2(n-k)}], \\ (x_1,\ldots,x_N) &\longmapsto (y_1,\ldots,y_N) \end{aligned}$$

where $y_{2j-1} = t_{2j-1}, y_{2j} = t_{2j}$ if $j \neq j_1,\ldots,j_k$ and $y_{2j-1} = y_{2j} = t_j$ otherwise.

Therefore, the system of equations we will consider will be derived from

$$\mathbf{E}_r(\hat{\mathcal{Q}}) = \mathbf{L}_r^{-1}(\hat{\mathcal{P}}) \tag{4.14}$$

where $\hat{\mathcal{Q}} = (\hat{Q}_1,\ldots,\hat{Q}_n) = (\sigma_{j_1,\ldots,j_k}(Q_1),\ldots,\sigma_{j_1,\ldots,j_k}(Q_n))$ and

$$\hat{\mathcal{P}} = (\hat{P}_1,\ldots,\hat{P}_n) = (\sigma_{j_1,\ldots,j_k}(P_1),\ldots,\sigma_{j_1,\ldots,j_k}(P_n)).$$

Specifically, for $1 \leq j \leq n$ we write the system of equations obtained from equation (4.14) by equaling these terms that have the same terms $\mathbf{t}(t_1, \ldots, t_n)$. The effect of the map σ is that it reduces the number of terms. Let's see how big is this reduction. Following the notations of the previous section, we consider the matrix

$$\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} (e_{11}^{\ell} \cdot 2^{c_{11}^{\ell}})_{1\leq \ell \leq k_{11}} & \cdots & (e_{1n}^{\ell} \cdot 2^{c_{1n}^{\ell}})_{1\leq \ell \leq k_{1n}} \\ \vdots & \ddots & \vdots \\ (e_{n1}^{\ell} \cdot 2^{c_{n1}^{\ell}})_{1\leq \ell \leq k_{n1}} & \cdots & (e_{nn}^{\ell} \cdot 2^{c_{nn}^{\ell}})_{1\leq \ell \leq k_{nn}} \end{pmatrix}.$$

Then the equivalent to Proposition 4.12 is:

Proposition 4.20. *Let* $\mathbf{E}_{r-1} \odot \ldots \odot \mathbf{E}_1 = \begin{pmatrix} \mathbf{e}_{11} & \cdots & \mathbf{e}_{1n} \\ \vdots & \vdots & \vdots \\ \mathbf{e}_{n1} & \cdots & \mathbf{e}_{nn} \end{pmatrix}$. *Then the number of terms that result from* $\mathbf{e}_{ij}$ *after applying* $\sigma_{j_1,\ldots,j_k}$ *is* 1 *if* $j \in \{j_1, \ldots, j_k\}$ *and* $\prod_{v \in \mathbf{e}_{ij}}(v+1)$ *otherwise.*

Fix a row index i, in the case $\#\mathbf{e}_{ij} = 1,\ \forall j = 1, \ldots, n$, and the weight-reduction map is chosen to be $\sigma_{1,\ldots,n}$, the system of equations for the i-th component has only one equation, which is not enough to recover the parameter of $\mathbf{L}_r^{-1}$. This explain why we define σ (cf. Definition 4.19) so that we can consider intermediate scenarios where some pairs $[x_{2i-1}, x_{2i}]$ are reduced while for other pairs each of the variables are mapped to two different variables. This causes a drop in the number of collision variables but does not remove them completely.

The computation of the number of terms in this case can be done using Propositions 4.12 and 4.20. If the weight-reduction map drop a lot the number of terms it might well happen that the ideal $\mathcal{I}_{\text{Minors}(2)}$ was not zero dimensional and therefore, we need to change the chosen weight-reduction map to one that leads to an ideal $\mathcal{I}_{\text{Minors}(2)}$ that is zero dimensional.

Note that the weight-reduction maps reduce the number of variables and hence we can a new one each time we want to solve a system of equations corresponding to a row of $\mathbf{E}_r$.

Going back to equation (4.14), let $\sigma = \sigma_{j_1,\ldots,j_k}$ and write

$$\mathcal{Q} = \left(\sum_{\mathbf{t} \in \text{Supp}(Q_1)} C_{\mathbf{t},Q_1}\mathbf{t}, \ldots, \sum_{\mathbf{t} \in \text{Supp}(Q_n)} C_{\mathbf{t},Q_n}\mathbf{t} \right)$$

,

$$\hat{Q} = \sigma(\mathcal{Q}) = \left(\sum_{\mathbf{t} \in \text{Supp}(\hat{Q}_1)} \hat{C}_{\mathbf{t},\hat{Q}_1}\mathbf{t}, \ldots, \sum_{\mathbf{t} \in \text{Supp}(\hat{Q}_n)} \hat{C}_{\mathbf{t},\hat{Q}_n}\mathbf{t} \right)$$

Fix $i,\ 1 \leq i \leq n$, a way to compute $C_{\mathbf{t},Q_i},\ \mathbf{t} \in \text{Supp}(Q_i),\ i = 1, \ldots, n$, would be to compute first values for those $\hat{C}_{\mathbf{t}',\hat{Q}_i}$ such that $\mathbf{t}' \in \text{Supp}(\hat{Q}_i))$ and $\sigma(\mathbf{t}) = \mathbf{t}'$ and then use that:

$$\hat{C}_{\mathbf{t}',\hat{Q}_i} = \sum_{\mathbf{t} \in \text{Supp}(Q_i) | \sigma(\mathbf{t}) = \mathbf{t}'} C_{\mathbf{t},Q_i}. \tag{4.15}$$

This is a linear system of equations that it is not injective as soon as the right-hand side has more than one summand, therefore values of $C_{\mathbf{t},Q_j}$ cannot be computed, in general, from the values of $\tilde{C}_{\mathbf{t}',\hat{Q}_j}$. To deal with that, we want to get various systems of linear equations as (4.15). The fact of having more than one allows us to recover the values of $C_{\mathbf{t},Q_j}$.

Definition 4.21. Let $j_1, \dots, j_k \in \{1, \dots, n\}$ and $(a_1, \dots, a_N) \in \mathbb{F}_q^N$. Define

$$\begin{aligned} \sigma_{\mathbf{a},j_1,\dots,j_k} : \mathbb{F}_{q^2}[x_1, \dots, x_N] &\longrightarrow \mathbb{F}_{q^2}[t_1, \dots, t_{k+2(n-k)}], \\ (x_1, \dots, x_N) &\longmapsto (y_1, \dots, y_N) \end{aligned}$$

where $y_{2j-1} = t_{2j-1}a_{2j-1}, y_{2j} = t_{2j}a_{2j}$ if $j \neq j_1, \dots, j_k$ and $y_{2j-1} = t_j a_{2j-1}, y_{2j} = t_j a_{2j}$ otherwise.

For every choice of $\mathbf{a} = (a_1, \dots, a_N)$ we get a system of equations as (4.14).

To recover the coefficients $C_{\mathbf{t},Q_i}$ from the values $\hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}}(Q_i)}$ we consider several linear systems in the unknowns $C_{\mathbf{t},Q_i}$, obtained by varying $\mathbf{a}$. Each system has the form

$$\hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}}(Q_i)} = \sum_{\substack{\mathbf{t} \in \mathrm{Supp}(Q_i) \\ \sigma_{\mathbf{a}}(\mathbf{t}) = \mathbf{t}'}} \mathbf{t}(a_1, \dots, a_N)\, C_{\mathbf{t},Q_i}. \tag{4.16}$$

Note that for each choice $\mathbf{a} = (a_1, \dots, a_N)$ the left-hand side of (4.16) is different because the values $\hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}}(Q_i)}$ depend on $\mathbf{a}$. Thus we obtain a family of linear systems with the same unknowns $C_{\mathbf{t},Q_i}$ but with different left-hand sides.

This dependence on $\mathbf{a}$ creates a potential problem when a single system (for a fixed $\mathbf{a}$) admits multiple solutions for the unknowns $\hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}}(Q_i)}$. If one picks, for each $\mathbf{a}$, an arbitrary solution among the several admissible ones, the choices may be incompatible: the combined system formed by all equations (4.16) for different $\mathbf{a}$ might then have no common solution. Hence it is important that the linear system be (generically) uniquely solvable, or that we have a rule to select the correct solution consistently across different $\mathbf{a}$.

Experimentally, for the DME version in [3], we observe the following: whenever the ideal $\mathcal{I}_{\mathrm{Minors}(2)}$ corresponding to the equations of a public-key component is zero-dimensional, there are exactly two possible values for the parameter $\beta \in \mathbb{F}_{q^2}$ that defines the linear map in that component. Once one of these two values of β is fixed, all remaining coefficients $C_{\mathbf{t},\sigma_{\mathbf{a}}(Q_i)}$ are determined uniquely. Therefore, in these instances the ambiguity described above does not occur in practice. These two values of β are related as shown in [2] and discussed at the end of Section 4.1.3.

4.5 Recovery of the variables before the exponential: DME 2023

In this section, we discuss how the coefficients $C_{\mathbf{t},Q_j}$ of the polynomials of $\mathcal{Q}$ can be recovered, assuming that there are no collision variables and the linear or affine map has already been computed. We also assumed that, as it was argued before, we have grouped some variables by weights, so what we are going to recover are the coefficients $\hat{C}_{\mathbf{t},\hat{Q}_j}$ from which the original coefficients $C_{\mathbf{t},Q_j}$ can be computed by solving an overdetermined system of linear equations (see Section 4.4).

Since we have already computed the last affine map, we know $\mathbf{A}^{-1}(\mathcal{P})$. Its i-th component that is the result of a product of $Q_{j_1}^{[a_{ij_1}]}, Q_{j_2}[a_{ij_2}], \ldots, Q_{j_k}^{[a_{ij_k}]}$ when we equal the coefficients leads to the system of equations

$$C_{\mathbf{s}_1,Q_{j_1}}^{[a_{ij_1}]} \ldots C_{\mathbf{s}_k,Q_{j_k}}^{[a_{ij_k}]} + \alpha_{\mathbf{s}_1,Q_{j_1}\ldots\mathbf{s}_k,Q_{j_k}}$$

where $\mathbf{s}_1$ runs over $\mathrm{Supp}(Q_{j_1}), \ldots, \mathbf{s}_k$ runs over $\mathrm{Supp}(Q_{j_k})$ with $j_1, \ldots, j_k \in \{1,..,n\}$ and $\alpha_{\mathbf{s}_1,Q_{j_1}\ldots\mathbf{s}_k,Q_{j_k}} \in \mathbb{F}_{q^2}$ are known. The exponents are also known as we are considering the exponential maps defined by the exponential matrices got in Algorithm of Example 3.2. To simplify a bit notation assume that $k = 2, \#\mathrm{Supp}(Q_{j_1}) = m, \#\mathrm{Supp}(Q_{j_2}) = n$. Denote $[a_{ij_1}] = [a], [a_{ij_2}] = [b]$, $\{C_{\mathbf{s},Q_{j_1}}\}_{\mathbf{s}\in\mathrm{Supp}(Q_{j_1})} = \{A_i\}_{1\leq i\leq m}, \{C_{\mathbf{s}'Q_{j_2}}\}_{\mathbf{s}'\in\mathrm{Supp}(Q_{j_2})} = \{B_j\}_{1\leq j\leq n}$ and let $\alpha_{ij} = A_i^{[a]}B_j^{[b]}$. Then the set of solutions, assuming $A_1 \neq 0$, can be parametrized as

$$(A_1^{[a]} : \frac{\alpha_{21}A_1^{[a]}}{\alpha_{11}} : \ldots : \frac{\alpha_{m1}A_1^{[a]}}{\alpha_{11}}), (\frac{\alpha_{11}}{A_1{}^{[a]}} : \frac{\alpha_{12}}{A_1{}^{[a]}} : \ldots : \frac{\alpha_{1n}}{A_1{}^{[a]}}).$$

Now if $\mathbf{E}_r$ is invertible, the polynomials in $\mathcal{Q}$ are unique. For example, given $\mathbf{s}_1 \in \mathrm{Supp}(Q_{j_1}), \ldots, \mathbf{s}_n \in \mathrm{Supp}(Q_{j_n})$, to compute $\begin{pmatrix} C_{\mathbf{s}_1,Q_{j_1}} \\ \vdots \\ C_{\mathbf{s}_n,Q_{j_n}} \end{pmatrix}$ we have to search the coefficients in $\mathbf{A}^{-1}(\mathcal{P})$, call them $(c_1, \ldots, c_n)$, that verify

$$\mathbf{E}_r \begin{pmatrix} C_{\mathbf{s}_1,Q_{j_1}} \\ \vdots \\ C_{\mathbf{s}_n,Q_{j_n}} \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}. \tag{4.17}$$

Note that we can search them because we know the support of the polynomials in $\mathcal{Q}$ and in $\mathbf{A}^{-1}(\mathcal{P})$ (the latter is the same that the support of $\mathcal{P}$).

From Equation (4.17) it directly follows that

$$\begin{pmatrix} C_{\mathbf{s}_1,Q_{j_1}} \\ \vdots \\ C_{\mathbf{s}_n,Q_{j_n}} \end{pmatrix} = \mathbf{E}_r^{-1} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

as we want to show.

It is clear that what we showed for the case $k = 2$ can be easily generalized to an arbitrary $k, 2 \leq k \leq n$. In this case equations are:

$$C^{[a_{ij_1}]}_{\mathbf{s}_1,Q_{j_1}} \dots C^{[a_{ij_k}]}_{\mathbf{s}_k,Q_{j_k}} + \alpha_{\mathbf{s}_1,Q_{j_1}\dots\mathbf{s}_k,Q_{j_k}}.$$

4.6 Estimates on the number of variables when the maps are affine

We assume that we know which of the linear maps have affine shifts. This is not a significant restriction, since the number of monomials and the structure of the matrices $\mathbf{E}_1, \dots, \mathbf{E}_r$ are publicly available. In the worst case, there might be more than one distribution of affine shifts leading to the correct number of terms, in which case the attack must be run for all possible distributions. However, it is unlikely that several distributions produce the correct number of terms. Because the components appear well mixed, it is reasonable to expect that only one choice of affine shifts yields the correct number of monomials in the end.

In what follows, we show how to systematically compute the number of terms when there are affine shifts. To illustrate this, we consider the example proposed in [3] and attacked in [2]. The matrices are

$$\mathbf{E}_1 = \begin{pmatrix} [a_0] & 0 & 0 & 0 \\ [a_1] & [a_2] & 0 & 0 \\ 0 & 0 & [a_3] & 0 \\ 0 & 0 & [a_4] & [a_5] \end{pmatrix}, \quad \mathbf{E}_2 = \begin{pmatrix} [b_0] & 0 & 0 & [b_1] \\ 0 & [b_2] & 0 & 0 \\ 0 & [b_3] & [b_4] & 0 \\ 0 & 0 & 0 & [b_5] \end{pmatrix}, \quad \mathbf{E}_3 = \begin{pmatrix} [c_0] & [c_1] & 0 & 0 \\ 0 & [c_2] & 0 & [c_3] \\ 0 & [c_4] & 0 & [c_5] \\ 0 & 0 & [c_6] & [c_7] \end{pmatrix}.$$

with the reductions

$$[c_1] = [a_0 + b_0 + c_0 - a_1 - b_2],$$
$$[c_7] = [a_3 + b_4 + c_6 - a_4 - b_5]$$

We show that if affine shifts are added to all but the first linear maps, we obtain the correct number of terms in the first component. Analogously, it can be verified that we obtain the correct number of terms in all components of the public key, namely $65, 25, 25, 65$.

Following the notation of chapter 3, we have that

$$\mathbf{E}_2 \odot \mathbf{E}_1 = \begin{pmatrix} 2^{b_0+a_0} & 0 & 2^{b_1+a_4} & 2^{b_1+a_5} \\ 2^{b_2+a_1} & 2^{b_2+a_2} & 0 & 0 \\ 2^{b_3+a_1} & 2^{b_3+a_2} & 2^{b_4+a_3} & 0 \\ 0 & 0 & 2^{b_5+a_4} & 2^{b_5+a_5} \end{pmatrix}.$$

and similarly

$$\mathbf{E}_3 \odot \mathbf{E}_2 \odot \mathbf{E}_1 = \begin{pmatrix} 2\cdot 2^{c_0+b_0+a_0} & 2^{c_1+b_2+a_2} & 2^{c_0+b_1+a_4} & 2^{c_0+b_1+a_5} \\ 2^{c_2+b_2+a_1} & 2^{c_2+b_2+a_2} & 2^{c_3+b_5+a_4} & 2^{c_3+b_5+a_5} \\ 2^{c_4+b_2+a_1} & 2^{c_4+b_2+a_2} & 2^{c_5+b_5+a_4} & 2^{c_5+b_5+a_5} \\ 2^{c_6+b_3+a_1} & 2^{c_6+b_3+a_2} & 2\cdot 2^{c_6+b_4+a_3} & 2^{c_7+b_5+a_5} \end{pmatrix}.$$

Recall that the first row of $\mathbf{E}_3 \odot \mathbf{E}_2 \odot \mathbf{E}_1$ means that: the support of first component of the output polynomials after $\mathbf{E}_3$ is:

$$\begin{aligned} &(x_1^{2\cdot 2^{c_0+b_0+a_0}}, x_1^{2^{c_0+b_0+a_0}} \cdot x_2^{2^{c_0+b_0+a_0}}, x_1^{2\cdot 2^{c_0+b_0+a_0}}) \otimes (x_3^{2^{c_1+b_2+a_2}}, x_4^{2^{c_1+b_2+a_2}}) \\ &\otimes (x_5^{2^{c_0+b_1+a_4}}, x_5^{2^{c_0+b_1+a_4}}) \otimes (x_7^{2^{c_0+b_1+a_5}}, x_8^{2^{c_0+b_1+a_5}}) \end{aligned}$$

If we ignore the exponents we can write the first row of $\mathbf{E}_3 \odot \mathbf{E}_2 \odot \mathbf{E}_1$ as $(2,1,1,1)$. With this notation the support of the first, second, third and fourth component after $\mathbf{L}_0$ can be represented as $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$, respectively.

The support of the first component after $\mathbf{E}_1$ is $(x_1^{2^{a_0}}, x_2^{2^{a_0}})$, of the second is $(x_1^{2^{a_1}}, x_2^{2^{a_1}}) \otimes (x_3^{2^{a_2}}, x_4^{2^{a_2}})$, of the third is $(x_5^{2^{a_3}}, x_6^{2^{a_3}})$ and of the fourth is $(x_5^{2^{a_4}}, x_6^{2^{a_4}}) \otimes (x_7^{2^{a_5}}, x_8^{2^{a_5}})$.

Note that they can be obtained simply as follows: for example, the support of the second component is $(1,1,0,0)$ that is $(1,0,0,0)+(0,1,0,0)$ where $(1,0,0,0)$ and $(0,1,0,0)$ are the support of the first and second components of the previous step. These are the components we have to sum because in the second row of $\mathbf{E}_1$ the non-zero entries are in the first and second position.

Now, we apply $\mathbf{A}_1$ that has shifts in all its components. Note that the linear part does not modify the support of the input polynomials but the shifts add an independent term that we will denote by a 1. Then, we represent the support of the first component after $\mathbf{A}_1$ as:

$(1,0,0,0),1$. Similarly, the support for the second, third and fourth components is

$$\begin{gathered} (1,1,0,0),1, \\ (0,0,1,0),1, \\ (0,0,1,1),1 \end{gathered}$$

respectively. The reason why we write the 1 corresponding to the independent term outside the parenthesis will be clear in the next step. We now have to compute the support of the components after $\mathbf{E}_2$. By looking at the first row of $\mathbf{E}_2$ we have that the first component after $\mathbf{E}_2$ is computed by multiplying the first and the fourth input polynomials (powered to some exponents). As the input polynomials are affine, the first component after $\mathbf{E}_2$ is

$$((x_1^{2^{b_0+a_0}}, x_2^{2^{b_0+a_0}}), 1) \otimes ((x_3^{2^{b_1+a_4}} x_5^{2^{b_1+a_5}}, x_4^{2^{b_1+a_4}} x_5^{2^{b_1+a_5}}, x_3^{2^{b_1+a_4}} x_6^{2^{b_1+a_5}}, x_4^{2^{b_1+a_4}} x_6^{2^{b_1+a_5}}), 1)$$

that with the simplified notation is simply

$$(1,0,0,0) + (0,0,1,1), (1,0,0,0), (0,0,1,1), 1$$

Therefore, the support of the components after $\mathbf{E}_2$ can be represented as:

$$\begin{aligned}
&(1,0,1,1), (1,0,0,0), (0,0,1,1), 1\\
&(1,1,0,0), 1\\
&(1,1,1,0), (1,1,0,0), (0,0,1,0), 1\\
&(0,0,1,1), 1
\end{aligned}$$

The map $\mathbf{A}_2$ does not modify the support as they already have an independent term.

Finally, the first component after applying $\mathbf{E}_3$ can be represented as

$$(1,0,1,1)+(1,1,0,0), (1,0,1,1), (1,0,0,0)+(1,1,0,0), (1,1,0,0), (0,0,1,1)+(1,1,0,0), (1,1,0,0), 1$$

that gives the following distributions of terms

$$(2,1,1,1), (1,0,1,1), (2,1,0,0), (1,0,0,0), (1,1,1,1), (0,0,1,1), (1,1,0,0), 1. \qquad (4.18)$$

where the vector $(2,1,1,1)$ means

$$(2 \cdot 2^{c_0+b_0+a_0}, 2^{c_1+b_2+a_2}, 2^{c_0+b_1+a_4},\ 1 \cdot 2^{c_0+b_1+a_5}),$$

the vector $(1,0,1,1)$ means

$$(2^{c_0+b_0+a_0},\ 0,\ 2^{c_0+b_1+a_4}, 2^{c_0+b_1+a_5}),$$

and so on. Therefore, from (4.18), the support of the first component after $\mathbf{E}_3$ has:

- $(2+1)\cdot(1+1)\cdot(1+1)\cdot(1+1) = 24$ terms coming from the vector $(2,1,1,1)$.
- $(1+1)\cdot(0+1)\cdot(1+1)\cdot(1+1) = 8$ terms coming from the vector $(1,0,1,1)$.
- $(2+1)\cdot(1+1)\cdot(0+1)\cdot(0+1) = 6$ terms coming from the vector $(2,1,0,0)$.
- $(1+1)\cdot(0+1)\cdot(0+1)\cdot(0+1) = 2$ terms coming from the vector $(1,0,0,0)$.

- $(1+1)\cdot(1+1)\cdot(1+1)\cdot(1+1) = 16$ terms coming from the vector $(1,1,1,1)$.
- $(0+1)\cdot(0+1)\cdot(1+1)\cdot(1+1) = 4$ terms coming from the vector $(0,0,1,1)$.
- $(1+1)\cdot(1+1)\cdot(0+1)\cdot(0+1) = 4$ terms coming from the vector $(1,1,0,0)$.
- one independent coming from 1.

in total $24+8+6+2+16+4+4+1 = 65$ terms.

Remark 4.22. With the notation of the Section 4.3, in this example all the possible collisions have been done. This can be deduced from $\mathbf{E}_3 \odot \mathbf{E}_2 \odot \mathbf{E}_1$, as the entries are single elements instead of vectors. In the general setting, of an arbitrary number of collisions, a similar reasoning can be done. As the notation is more complicated, we do not give the details.

We now explain how the terms of the first component (over $\mathbb{F}_{q^2}$) can be split into blocks and how the collision variables are distributed. Recall that in the linear case, a necessary condition for the i-th component, $1 \leq i \leq 4$, of the public key to have a collision was that the i-th row of $\mathbf{E}_3 \odot \mathbf{E}_2 \odot \mathbf{E}_1$ had an entry greater of the form $e \cdot 2^c$ with $e > 1$. In this example, collisions in the first component occur only when computing the linear part $(1,0,1,1)+(1,1,0,0)$ and the affine part $(1,0,0,0)+(1,0,0,0)$.

The matrix $\mathbf{M}$ constructed as in equation (4.10) that corresponds to the first component of the public key has as row indices the terms of the first component in $\mathcal{Q}$ and as column indices the terms of the second component in $\mathcal{Q}$:

$$\left[\begin{array}{c|c} 8\times 4 & 8\times 1 \\ \hline 4\times 4 & 4\times 1 \\ \hline 2\times 4 & 2\times 1 \\ \hline 1\times 4 & 1\times 1 \end{array}\right].$$

Since the vectors in (4.18) are pairwise distinct, collision variables of different blocks are also distinct, and we can apply the results of the previous section to each block separately (provided the parameters of the block satisfy the required hypotheses). This improves the efficiency of the method. If a block does not satisfy the hypotheses, it can be treated as part of a larger block where the hypotheses do hold.

Not all matrices can be split into blocks as above. To do so, we require the following assumption: no two vectors in the distribution of terms share the same exponents. The following example illustrates a case where this assumption fails.

Example 4.11. *We consider a very simple example, which cannot be used because* $\det(\mathbf{E}_1) = 0$ *but it serves us for what we want to illustrate. Let* $\mathbf{E}_1 = \begin{pmatrix} [a_1] & [a_2] \\ [a_3] & [a_4] \end{pmatrix}, \mathbf{E}_2 = \begin{pmatrix} [b_1] & [b_2] \\ [b_3] & [b_4] \end{pmatrix}$ *with* $b_1 + a_1 = b_2 + a_3, b_1 + a_2 = b_2 + a_4$. *Then,* $\mathbf{E}_1^* = \mathbf{E}_2^* = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ *and assume that* $\mathbf{A}_1$ *has affine shifts* *in all the components. Then the distribution of the terms after* $\mathbf{E}_2$ *in the first component will be*

$$(2,2),(1,1),(1,1),1.$$

We see the vector $(1,1)$ *appear twice in the distribution. Looking at the matrices* $\mathbf{E}_1, \mathbf{E}_2$ *we can write the exponents that corresponds to these vectors, these are* $([a_1+b_1],[a_2+b_1])$ *and* $([a_1+b_1],[a_2+b_1])$*. As the vectors of exponents are equals this gives collision variables in distinct blocks, being in this case the block structure:*

$$\left[\begin{array}{c|c} 4\times 4 & 4\times 1 \\ \hline 1\times 4 & 1\times 1 \end{array}\right]. \tag{4.19}$$

Even when this assumption does not hold, the collision variables of the linear part remain separated from the rest. Hence, we can still apply the modelling of Section 4.3 to compute these variables and the linear part of the affine map.

In practice, we have not encountered any example where $\mathcal{I}_{\text{Minors}(2)}$ is not zero-dimensional in the affine case. However, we have not been able to prove this property in general, since for instances that do not satisfy the assumption we lack a method to estimate the number of collision variables. This prevents us from establishing a theoretical guarantee that $\mathcal{I}_{\text{Minors}(2)}$ remains zero-dimensional in those cases.

It is also worth emphasizing that with affine shifts, it may not be necessary to recover all collision variables in order to invert the last round. For example, in the matrix above, computing the collision variables of all blocks except the 8×4 block, together with the parameters of the linear part of the affine map, suffices, since the coefficients of all polynomials in $\mathcal{Q}$ can then be recovered.

Remark 4.23. The affine case introduces one new parameter from the affine shift, which only appears in the 1×1 block. The proofs of Section 4.3 can be extended with minor modifications, since the bounds were not completely tight.

Chapter 5

Attack on the DME minus

In this section we explain how the model of Section 4.3 can be adapted to the setting where only the odd components of $\mathcal{P}$ are made public, that will be denoted as $\mathcal{P}^-$.

5.1 Modelling of the attack

We first prove that given $\mathcal{P}^- = (p_1, p_3, \dots, p_{2n-1})$ there exists an equivalent private key such that the linear part of $\mathbf{A}_r$ is the identity:

Lemma 5.1. *Given a* $\boldsymbol{DME}_r^-$*, there exist* $\tilde{\mathbf{L}}$ *such that*

$$\pi \circ \mathbf{E}_r \circ \tilde{\mathbf{L}} = \pi \circ \mathbf{L}_r \circ \mathbf{E}_r.$$

Proof. Let the matrix of $\mathbf{L}_{ri}$ in the canonical basis $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Let $\lambda = \alpha + u\beta$ and $u^2 = A + u \cdot B$, then the map

$$M_\lambda : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2},\ z \mapsto \lambda z$$

can be seen as the following liner map:

$$\mathbf{L}_\lambda : \mathbb{F}_q^2 \to \mathbb{F}_q^2, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \alpha & A \cdot \beta \\ \beta & \alpha + B \cdot \beta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Hence solving the system $\alpha = a, A \cdot \beta = b$ we find λ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ *_1 & *_2 \end{pmatrix} \cdot \begin{pmatrix} \alpha & A \cdot \beta \\ \beta & \alpha + B \cdot \beta \end{pmatrix}.$$

The matrix of $\mathbf{L}_{ri} \circ \mathbf{L}_{\lambda^{-1}}$ has the form $\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}$. The result follows by taking $\tilde{\mathbf{L}}$ the map such that $\mathbf{E}_r \circ \tilde{\mathbf{L}} = \mathbf{E}_r \circ \mathbf{L}_{\lambda^{-1}}$. The existence of such $\tilde{\mathbf{L}}$ is guaranteed by Lemma 4.4.

□

For the i-th polynomial of the public key $\mathcal{P}^-$, i.e. p_{2i-1}, the system of equations we have to solve is:

$$\{\mathrm{Coeff}_{\mathbf{t},p_{2i-1}} + d_{2i-1} = \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}} [C^{[a_{ij_1}]}_{\mathbf{s}_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}_k,Q_{j_k}}]_1\}_{\mathbf{t}\in \mathrm{Supp}(P_i)}$$

in the variables d_{2i-1} and the $C_{\mathbf{s}_\ell,Q_{j_\ell}}$, $1 \le \ell \le k$. The parameter d_{2i-1} comes from the affine map, which is assumed to have the simplified form given in Lemma 5.1,

$$\mathbf{A}_{ri} : \mathbb{F}_q^2 \to \mathbb{F}_q^2,\ (x_{2i-1}, x_{2i}) \mapsto (x_{2i-1} + d_{2i-1}, x_{2i} + d_{2i})$$

for some $d_{2i-1}, d_{2i} \in \mathbb{F}_q$. Moreover, the notation $[.]_1$ means the coordinate of 1 when we represent the element in $\mathbb{F}_{q^2}$ as an element of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^2$ with basis $\{1, u\}$. We follow the setup of the previous chapter, and aim to build matrices that allow to compute the collision variables. Now, collision variables appear in every equation

$$\mathrm{Coeff}_{\mathbf{t},p_{2i-1}} + d_{2i-1} = \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}} [C^{[a_{ij_1}]}_{\mathbf{s}_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}_k,Q_{j_k}}]_1$$

with $\mathbf{t} \neq 1, \mathbf{t} \in \mathrm{Supp}(P_i)$ such that $\mathrm{Terms}_{P_i,\mathbf{t}} = r > 1$ when we write it as

$$\begin{aligned}
&\{H_{\mathbf{s}_1,\ldots,\mathbf{s}_k} = [C^{[a_{ij_1}]}_{\mathbf{s}_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}_k,Q_{j_k}}]_1\}_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}\setminus(\mathbf{s}'_1,\ldots,\mathbf{s}'_k)},\\
&\mathrm{Coeff}_{\mathbf{t},p_{2i-1}} + \sum_{(\mathbf{s}_1,\ldots,\mathbf{s}_k)\in \mathrm{Terms}_{P_i,\mathbf{t}}\setminus(\mathbf{s}'_1,\ldots,\mathbf{s}'_k)} H_{\mathbf{s}_1,\ldots,\mathbf{s}_k} = [C^{[a_{ij_1}]}_{\mathbf{s}'_1,Q_{j_1}} \cdot \ldots \cdot C^{[a_{ij_k}]}_{\mathbf{s}'_k,Q_{j_k}}]_1
\end{aligned}$$

Asume $k = 2$ and let explain how an analogue to the matrix $\mathbf{M}$ – which will be denoted also by $\mathbf{M}$ – of equation (4.10) can be defined.

Example 5.1. *We consider the example 4.6. We use a slight abuse of notation and the variables $A_i \in \mathbb{F}_{q^2}$ and $B_i \in \mathbb{F}_{q^2}$ of Example 4.6 are in this example $A_i + uB_i$ and $C_i + uD_i$, respectively where now $A_i, B_i, C_i, D_i \in \mathbb{F}_q$. With this notation, the minus version of the system of equations 4.11 of the previous chapter is:*

$$\begin{aligned}
&[(A_1+uB_1)^{[b_1]}(C_1+uD_1)^{[b_1+a_1-a_3]}]_1 = r_1\\
&[(A_1+uB_1)^{[b_1]}(C_2+uD_2)^{[b_1+a_1-a_3]} + (A_2+uB_2)^{[b_1]}(C_1+uD_1)^{[b_1+a_1-a_3]}]_1 = r_2\\
&[(A_1+uB_1)^{[b_1]}(C_3+uD_3)^{[b_1+a_1-a_3]}]_1 = r_3\\
&[(A_1+uB_1)^{[b_1]}(C_4+uD_4)^{[b_1+a_1-a_3]} + (A_2+uB_2)^{[b_1]}(C_3+uD_3)^{[b_1+a_1-a_3]}]_1 = r_4\\
&[(A_2+uB_2)^{[b_1]}(C_2+uD_2)^{[b_1+a_1-a_3]}]_1 = r_5\\
&[(A_2+uB_2)^{[b_1]}(C_4+uD_4)^{[b_1+a_1-a_3]}]_1 = r_6\\
&[(A_3+uB_3)^{[b_1]}(C_1+uD_1)^{[b_1+a_1-a_3]}]_1 = r_7\\
&[(A_3+uB_3)^{[b_1]}(C_2+uD_2)^{[b_1+a_1-a_3]} + (A_4+uB_4)^{[b_1]}(C_1+uD_1)^{[b_1+a_1-a_3]}]_1 = r_8\\
&[(A_3+uB_3)^{[b_1]}(C_3+uD_3)^{[b_1+a_1-a_3]}]_1 = r_9\\
&[(A_3+uB_3)^{[b_1]}(C_4+uD_4)^{[b_1+a_1-a_3]} + (A_4+uB_4)^{[b_1]}(C_3+uD_3)^{[b_1+a_1-a_3]}]_1 = r_{10}\\
&[(A_4+uB_4)^{[b_1]}(C_2+uD_2)^{[b_1+a_1-a_3]}]_1 = r_{11}\\
&[(A_4+uB_4)^{[b_1]}(C_4+uD_4)^{[b_1+a_1-a_3]}]_1 = r_{12}
\end{aligned} \tag{5.1}$$

where $r_i = [R_i]_1,\ i = 1, \dots, 12$.

Note that

$$\begin{aligned}
&[(A_i+uB_i)^{[b_1]}(C_j+uD_j)^{[b_1+a_1-a_3]}]_1\\
&= [(A_i^{[b_1]} + (\alpha_1+u\beta_1)B_i^{[b_1]})(C_j^{[b_1+a_1-a_3]} + (\alpha_2+u\beta_2)D_j^{[b_1+a_1-a_3]})]_1\\
&= (A_i^{[b_1]} + \alpha_1 B_i^{[b_1]})(C_j^{[b_1+a_1-a_3]} + \alpha_2 D_j^{[b_1+a_1-a_3]}) + \alpha\beta_1 B_i^{[b_1]}\beta_2 D_j^{[b_1+a_1-a_3]}
\end{aligned}$$

where $u = \alpha + u\beta$, $u^{[b_1]} = \alpha_1 + u\beta_1,\ u^{[b_1+a_1-a_3]} = \alpha_2 + u\beta_2$, can be written as:

$$\begin{pmatrix} A_i & B_i \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_j \\ D_j \end{pmatrix}$$

beind $\mathbf{W}_1 = \begin{pmatrix} 1 & \alpha_2 \\ \alpha_1 & \alpha_1\alpha_2 + \alpha\beta_1\beta_2 \end{pmatrix}$. We can arrange this into a matrix whose element (i,j) is

$$\begin{pmatrix} A_i & B_i \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_j \\ D_j \end{pmatrix}$$

$$\mathbf{M} = \begin{pmatrix} r_1 & H_1 & r_3 & H_2 \\ r_2 + H_1 & r_5 & r_4 + H_2 & r_6 \\ r_7 & H_3 & r_9 & H_4 \\ r_8 + H_3 & r_{11} & r_{10} + H_4 & r_{12} \end{pmatrix}.$$

Imposing in this setting that the minors of order 2 of $\mathbf{M}$ *vanish will imply that*

$$\begin{pmatrix} A_1 & B_1 \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_1 \\ D_1 \end{pmatrix} \cdot \begin{pmatrix} A_2 & B_2 \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_2 \\ D_2 \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_2 \\ D_2 \end{pmatrix} \cdot \begin{pmatrix} A_1 & B_1 \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_2 \\ D_2 \end{pmatrix}$$

which does not hold in general.

We prove that it is not the minors of order 2 but rather the minors of order 3 of the matrix $\mathbf{M}$ that vanish. Denote $k_1 = \#\mathrm{Supp}(Q_{j_1}),\ k_2 = \#\mathrm{Supp}(Q_{j_2})$ and let

$$Q_{j_1} = \sum_{i=1}^{k_1} (A_i + uB_i)\mathbf{s}_i,\ Q_{j_2} = \sum_{i=1}^{k_2} (C_i + uD_i)\mathbf{s}'_i.$$

We then consider the matrix

$$\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1k_2} \\ x_{21} & x_{22} & \dots & x_{2k_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{k_1 1} & x_{k_1 2} & \dots & x_{k_1 k_2} \end{pmatrix} \tag{5.2}$$

where $x_{ij} = \begin{pmatrix} A_i & B_i \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_j \\ D_j \end{pmatrix}$ where $\mathbf{W}_1 = \begin{pmatrix} 1 & \alpha_2 \\ \alpha_1 & \alpha_1\alpha_2 + \alpha\beta_1\beta_2 \end{pmatrix}$ with $u = \alpha + u\beta,\ u^a = \alpha_1 + u\beta_1,\ u^b = \alpha_2 + u\beta_2$ and write a matrix $\mathbf{Y}$ of size $\binom{m}{2}\binom{n}{2}$

$$\mathbf{Y} = \begin{pmatrix} \begin{pmatrix} A_1^a & B_1^a \\ A_2^a & B_2^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_1^b & C_2^b \\ D_1^b & D_2^b \end{pmatrix} & \begin{pmatrix} A_1^a & B_1^a \\ A_2^a & B_2^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_1^b & C_3^b \\ D_1^b & D_3^b \end{pmatrix} & \cdots & \begin{pmatrix} A_1^a & B_1^a \\ A_2^a & B_2^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{k_2-1}^b & C_{k_2}^b \\ D_{k_2-1}^b & D_{k_2}^b \end{pmatrix} \\ \begin{pmatrix} A_1^a & B_1^a \\ A_3^a & B_3^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_1^b & C_2^b \\ D_1^b & D_2^b \end{pmatrix} & \begin{pmatrix} A_1^a & B_1^a \\ A_3^a & B_3^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_1^b & C_3^b \\ D_1^b & D_3^b \end{pmatrix} & \cdots & \begin{pmatrix} A_1^a & B_1^a \\ A_3^a & B_3^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{k_2-1}^b & C_{k_2}^b \\ D_{k_2-1}^b & D_{k_2}^b \end{pmatrix} \\ \vdots & \vdots & \ddots & \vdots \\ \begin{pmatrix} A_{k_1-1}^a & B_{k_1-1}^a \\ A_{k_1}^a & B_{k_1}^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_1^b & C_2^b \\ D_1^b & D_2^b \end{pmatrix} & \begin{pmatrix} A_{m-1}^a & B_{m-1}^a \\ A_m^a & B_m^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_1^b & C_3^b \\ D_1^b & D_3^b \end{pmatrix} & \cdots & \begin{pmatrix} A_{k_1-1}^a & B_{k_1-1}^a \\ A_{k_1}^a & B_{k_1}^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{k_2-1}^b & C_{k_2}^b \\ D_{k_2-1}^b & D_{k_2}^b \end{pmatrix} \end{pmatrix}. \tag{5.3}$$

For each $i, i', j, j' \in \{1, \dots, k_1\},\ r, r', s, s' \in \{1, \dots, k_2\}$ with $i \neq j, i' \neq j', r \neq s, r' \neq s'$ (and assuming that the matrices are invertible, which is true for generic matrices) the following relation holds:

$$\begin{aligned} &\left[\begin{pmatrix} A_i^a & B_i^a \\ A_j^a & B_j^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_r^b & C_s^b \\ D_r^b & D_s^b \end{pmatrix}\right]^{-1} \cdot \begin{pmatrix} A_i^a & B_i^a \\ A_j^a & B_j^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{r'}^b & C_{s'}^b \\ D_{r'}^b & D_{s'}^b \end{pmatrix} \\ &= \left[\begin{pmatrix} A_{i'}^a & B_{i'}^a \\ A_{j'}^a & B_{j'}^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_r^b & C_s^b \\ D_r^b & D_s^b \end{pmatrix}\right]^{-1} \cdot \begin{pmatrix} A_{i'}^a & B_{i'}^a \\ A_{j'}^a & B_{j'}^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{r'}^b & C_{s'}^b \\ D_{r'}^b & D_{s'}^b \end{pmatrix}. \end{aligned} \tag{5.4}$$

If the entries of the matrix (5.3) were integers, this relation would be the same as the vanishing of minors of order two. However, once the entries are matrices the condition is no longer equivalent to the vanishing of the minors of order two. What we are going to prove is that it is equivalent to the vanishing of the minors of order 3 of $\mathbf{X}$.

Proposition 5.2. *Let* $\mathbf{Y} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{C} & \mathbf{D} \end{array}\right)$ *be a block matrix. Then,*

- *if* $\mathbf{A}$ *is invertible,* $\det(\mathbf{Y}) = \det(\mathbf{A})\det(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B})$*.*
- *if* $\mathbf{D}$ *is invertible* $\det(\mathbf{Y}) = \det(\mathbf{D})\det(\mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C})$*.*

Proof. If $\mathbf{A}$ is invertible we have that $\mathbf{Y}$ can be written as:

$$\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{C}\mathbf{A}^{-1} & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I} & \mathbf{A}^{-1}\mathbf{B} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}.$$

The result follows by taking determinants.

If $\mathbf{D}$ is invertible, the factorization we use is:

$$\mathbf{Y} = \begin{pmatrix} \mathbf{I} & \mathbf{B}\mathbf{D}^{-1} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{D} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{D}^{-1}\mathbf{C} & \mathbf{I} \end{pmatrix}.$$

□

Proposition 5.3. *For every* $1 < i, i', j, j' < k_1$ *pairwise distinct and* $1 < r, r', s, s' < k_2$ *pairwise distinct let* $I_1 = \{i, j\}, I_2 := \{i', j'\}, I_3 := \{r, s\}, I_4 := \{r', s'\}$ *. Then if relation* (5.4) *holds, we have that*

$$\det\left(\mathbf{X}_{(I_1 \cup I_2)\times(J_1 \cup J_2)}\right) = 0$$

where $\mathbf{X}_{(I_1 \cup I_2)\times(J_1 \cup J_2)}$ *is the minor of order* 4 *of the matrix* $\mathbf{X}$ *corresponding to choose the row indices* $I_1 \cup I_2 = \{i, j, i', j'\}$ *and the column indices* $J_1 \cup J_2 = \{r, s, r', s'\}$*.*

Proof. It is very simple from Proposition 5.2. Let $\mathbf{Y} = \mathbf{X}_{(I_1 \cup I_2)\times(J_1 \cup J_2)}$. Note that

$$\mathbf{Y} = \begin{pmatrix} \begin{pmatrix} A_i^a & B_i^a \\ A_j^a & B_j^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_r^b & C_s^b \\ D_r^b & D_s^b \end{pmatrix} & \begin{pmatrix} A_i^a & B_i^a \\ A_j^a & B_j^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{r'}^b & C_{s'}^b \\ D_{r'}^b & D_{s'}^b \end{pmatrix} \\ \begin{pmatrix} A_{i'}^a & B_{i'}^a \\ A_{j'}^a & B_{j'}^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_r^b & C_s^b \\ D_r^b & D_s^b \end{pmatrix} & \begin{pmatrix} A_{i'}^a & B_{i'}^a \\ A_{j'}^a & B_{j'}^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_{r'}^b & C_{s'}^b \\ D_{r'}^b & D_{s'}^b \end{pmatrix} \end{pmatrix} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{C} & \mathbf{D} \end{array}\right)$$

and therefore $\det(\mathbf{Y}) = \det(\mathbf{A})\det(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B})$. Now equation (5.4) holds is equivalent to $\mathbf{A}^{-1}\mathbf{B} = \mathbf{C}^{-1}\mathbf{D}$ that can be rewritten as $\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B} = 0$ – assuming that $\mathbf{C}$ is invertible– and hence $\det(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}) = 0$. □

Define $\mathbf{Y}_\Delta = \begin{pmatrix} \Delta_{\{1,2\}\times\{1,2\}} & \Delta_{\{1,2\}\times\{1,3\}} & \cdots & \Delta_{\{1,2\}\times\{n-1,n\}} \\ \Delta_{\{1,3\}\times\{1,2\}} & \Delta_{\{1,3\}\times\{1,3\}} & \cdots & \Delta_{\{1,3\}\times\{n-1,n\}} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{\{k_1-1,k_1\}\times\{1,2\}} & \Delta_{\{k_1-1,k_1\}\times\{1,3\}} & \cdots & \Delta_{\{k_1-1,k_1\}\times\{k_2-1,k_2\}} \end{pmatrix}$ where

$$\Delta_{\{i,j\}\times\{r,s\}} = \det\left(\begin{pmatrix} A_i^a & B_i^a \\ A_j^a & B_j^a \end{pmatrix} \mathbf{W}_1 \begin{pmatrix} C_r^b & C_s^b \\ D_r^b & D_s^b \end{pmatrix}\right).$$

Observe that taking determinants in equation 5.4, we obtain that the minors of order two of $\mathbf{Y}_\Delta$ vanish. In particular:

$$\det\begin{pmatrix} \Delta_{\{i,j\}\times\{r,s\}} & \Delta_{\{i,j\}\times\{r',s\}} \\ \Delta_{\{i',j'\}\times\{r,s\}} & \Delta_{\{i',j'\}\times\{r',s\}} \end{pmatrix} = 0, \tag{5.5}$$

$$\det\begin{pmatrix} \Delta_{\{i,j\}\times\{r,s\}} & \Delta_{\{i,j\}\times\{s',s\}} \\ \Delta_{\{i',j'\}\times\{r,s\}} & \Delta_{\{i',j'\}\times\{s',s\}} \end{pmatrix} = 0, \tag{5.6}$$

$$\det\begin{pmatrix} \Delta_{\{i,j\}\times\{r,s\}} & \Delta_{\{i,j\}\times\{r,r'\}} \\ \Delta_{\{i',j'\}\times\{r,s\}} & \Delta_{\{i',j'\}\times\{r,r'\}} \end{pmatrix} = 0, \tag{5.7}$$

$$\det\begin{pmatrix} \Delta_{\{i,j\}\times\{r,s\}} & \Delta_{\{i,j\}\times\{r,s'\}} \\ \Delta_{\{i',j'\}\times\{r,s\}} & \Delta_{\{i',j'\}\times\{r,s'\}} \end{pmatrix} = 0. \tag{5.8}$$

The following proposition shows that these equations correspond to the minors of order 3 of the matrix $\mathbf{X}$.

Proposition 5.4. *For every $1 < i, j, j' < k_1$ pairwise distinct and $1 < r, r', s < k_2$ pairwise distinct let $I_1 = \{i, j\}, I_2 := \{i, j'\}, J_1 := \{r, s\}, J_2 := \{r', s\}$. Then relation (5.5) –taking $i' = i$– holds is equivalent to*

$$\det\left(\mathbf{X}_{(I_1\cup I_2)\times(J_1\cup J_2)}\right) = 0$$

where $\mathbf{X}_{(I_1\cup I_2)\times(J_1\cup J_2)}$ is the minor of order 3 of the matrix $\mathbf{X}$ corresponding to choose the row indices $I_1 \cup I_2 = \{i, j, j'\}$ and the column indices $J_1 \cup J_2 = \{r, r', s\}$. Therefore, all minors of order 3 of $\mathbf{X}$ vanish is equivalent to (5.4) –with $i' = i, s' = s$ – holds for all $\{i, j, j'\}, \{r, r', s\}$.

Proof. Let $\mathbf{Y} = \mathbf{X}_{(I_1\cup I_2)\times(J_1\cup J_2)}$. We prove that the ideal $I = \langle \det(\mathbf{Y})\rangle \subseteq \mathbb{K}[x_{i,j}, 1 < i < k_1, 1 < j < k_2]$ contains the polynomial

$$\Delta_{I_1\times J_1}\Delta_{I_2\times J_2} - \Delta_{I_1\times J_2}\Delta_{I_2\times J_1},$$

which is exactly (5.5). Let $\mathbf{Y} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ then

$$\det(\mathbf{Y}) = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{31}a_{12}a_{23} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{33}a_{12}a_{21}$$

and

$$\begin{aligned}&\Delta_{I_1\times J_1}\Delta_{I_2\times J_2}-\Delta_{I_1\times J_2}\Delta_{I_2\times J_1}\\&=(a_{11}a_{22}-a_{21}a_{12})(a_{22}a_{33}-a_{23}a_{32})-(a_{12}a_{23}-a_{22}a_{13})(a_{21}a_{32}-a_{22}a_{31})\\&=a_{22}\det(\mathbf{Y}).\end{aligned}$$

Therefore

$$\langle\det(\mathbf{Y})\rangle=\langle\Delta_{I_1\times J_1}\Delta_{I_2\times J_2}-\Delta_{I_1\times J_2}\Delta_{I_2\times J_1}\rangle$$

seen as ideals in field of fractions $\mathbb{K}(x_{i,j}, 1<i<k_1, 1<j<k_2)$.

To prove the last part of the proposition, note that equations (5.5),(5.6),(5.7),(5.8) can be simplified to (5.5),(5.7) when we impose $i'=i, s'=s$ because (5.6) and (5.8) are trivially true and (5.7) correspond to the same minor of $\mathbf{X}$ as (5.5) (just with a different J_2, $J_2=\{r,s\}$). □

Corollary 5.5. *Equations* (5.4) *for* $i,i',j,j'\in\{1,\ldots,k_1\}$, $r,r',s,s'\in\{1,\ldots,k_2\}$ *are equivalent to minors of order three of* $\mathbf{X}$ *vanish.*

The matrices that appear in the modelling of **DME** minus, are not generic as $\mathbf{X}$ of (5.2), their entries are affine polynomials of degree one:

$$\mathbf{M}(H_1,\ldots,H_\ell)=\begin{pmatrix}x_{11}(H_1,\ldots,H_\ell)&\ldots&x_{1k_2}(H_1,\ldots,H_\ell)\\\vdots&\ddots&\vdots\\x_{k_11}(H_1,\ldots,H_\ell)&\ldots&x_{k_1k_2}(H_1,\ldots,H_\ell)\end{pmatrix}\tag{5.9}$$

(e.g. see M of Example 5.1). Analogously as we reason in Chapter 4, to assure that $\mathcal{I}_{\text{Minors}(3),\mathbf{M}}$ is zero dimensional, we need some genericity conditions. The genericity conditions required for $\mathcal{I}_{\text{Minors}(3),\mathbf{M}}$ are analogous to those imposed on $\mathcal{I}_{\text{Minors}(2),\mathbf{M}}$ in Section 4.3. These are:

- the entries of $\mathcal{I}_{\text{Minors}(3),\mathbf{M}^{(h)}}$ behave as homogeneous polynomials of degree one with generic coefficients,
- $\mathcal{I}_{\text{Minors}(3),\mathbf{M}^{(h)}}=\mathcal{I}^{(h)}_{\text{Minors}(3),\mathbf{M}}$,
- the entries of $\mathcal{I}_{\text{Minors}(3),\mathbf{M}}$ as affine polynomials of degree one with generic coefficients.

Example 4.1. (continued) From Section 2.4.1 we know that under genericity assumptions the ideal $\mathcal{I}_{\text{Minors}(3),\mathbf{M}}$ of minors of order 3 of $\mathbf{M}$ is zero dimensional if $4=\#\{H_i\}\leq(k_1-2)(k_2-2)=(4-2)(4-2)=4$. Therefore, we expect a finite set of possible values of the collision variables over $\overline{\mathbb{F}_q}$. A small subset of them live in $\mathbb{F}_q$, this are which interest us.

5.1.1 Removing collisions, case $k=2$

In general we cannot prove an analogue of Proposition 4.11. If we define M,N and P in the same way as there, one can check that the base case $n=2$ of the proof does not hold in general. In those cases it holds, we can removing collision variables in one component. However, when it does not hold, we have to consider a matrix

$$\mathbf{M}^* = \begin{pmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \end{pmatrix}$$

which is the vertical concatenation of matrices of the form (5.9), each one corresponding to the system of equations of a polynomial in the public key $\mathcal{P} = p_1, p_3, \ldots, p_{2n-1}$. To construct such a matrix, it is necessary that if $\mathbf{M}_1$ and $\mathbf{M}_2$ correspond to p_{2i-1} and $p_{2i'-1}$ respectively with $i \neq i'$, then there must exist a column index j such that the entries (i, j) and (i', j) of $\mathbf{E}_r$ are both nonzero. This situation occurs as soon as we choose a row with more than one nonzero entry. If a row of the exponent matrix has a nonzero entry only in column j and no other row has a nonzero entry in that column, then this row is "free" and no collision variables appear in the corresponding system of equations. However, once a row has at least two nonzero entries, the key point is the following: if a row has nonzero entries in columns $j_1, \ldots, j_k$ with $k \geq 2$, and no other row has a nonzero entry in any of these columns, then the determinant of the matrix is zero. Consequently, we can assume that for any row we select, there exists another row with at least one nonzero entry in a column where the chosen row also has a nonzero entry.

Case $k = 2$ all collisions done.

Assume we choose two components of the public key $\mathcal{P}^-$ that correspond to two rows, $i, i', i \neq i'$ of $\mathbf{E}_r$ such that

$$p_{2i-1} = Q_{j_1}^{[a_{ij_1}]} Q_{j_2}^{[a_{ij_2}]}$$

$$p_{2i'-1} = Q_{j_1}^{[a_{i'j_1}]} Q_{j_3}^{[a_{i'j_3}]}.$$

The coefficients of Q_{j_1} are common variables to both system of equations, however they appear with different exponents. To obtain the same exponents we consider the second equation to be

$$p_{2i'-1}^{[a_{ij_1} - a_{i'j_1}]} = Q_{j_1}^{[a_{ij_1}]} Q_{j_3}^{[a_{i'j_3} + a_{ij_1} - a_{i'j_1}]}$$

instead.

Then we can build a matrix $\mathbf{M}_1$ and a matrix $\mathbf{M}_2$ for the system of equations derived from equation

$$p_{2i-1} = Q_{j_1}^{[a_{ij_1}]} Q_{j_2}^{[a_{ij_2}]}$$

$$p_{2i'-1}^{[a_{ij_1} - a_{i'j_1}]} = Q_{j_1}^{[a_{ij_1}]} Q_{j_3}^{[a_{i'j_3} + a_{ij_1} - a_{i'j_1}]}$$

respectively.

Lemma 5.6. *Let $K = \#Supp(Q_{j_1}), M = \#Supp(Q_{j_2})$ and $N = \#Supp(Q_{j_3})$. The inequality*

$$MN - \prod_{i=1}^{n}(e_{1i} + e_{2i} + 1) + MK - \prod_{i=1}^{n}(e_{1i} + e_{3i} + 1) \leq (M-2)\,(N+K-2)$$

holds as soon as $e_{1i_1}, e_{2i_2}, e_{3i_3} \geq 1$ for some $1 \leq i_1 \neq i_2 \neq i_3 \leq n$ and $n \geq 3$.

Proof. Set for each $i = 1, \dots, n$

$$A_i = e_{1i} + 1, \quad B_i = e_{2i} + 1, \quad C_i = e_{3i} + 1,$$

so

$$M = \prod_{i=1}^{n} A_i, \quad N = \prod_{i=1}^{n} B_i, \quad K = \prod_{i=1}^{n} C_i,$$

and define the two "mixed" products

$$P = \prod_{i=1}^{n}(A_i + B_i - 1), \quad Q = \prod_{i=1}^{n}(A_i + C_i - 1).$$

Then the inequality to prove is equivalently

$$MN - P + MK - Q \leq (M-2)\,(N+K-2).$$

- The right hand side expands to

  $$(M-2)(N+K-2) = MN + MK - 2M - 2N - 2K + 4.$$

  So the inequality

  $$MN - P + MK - Q \leq MN + MK - 2M - 2N - 2K + 4$$

  is equivalent to

  $$-P - Q \leq -2M - 2N - 2K + 4 \quad \Longleftrightarrow \quad P + Q \geq 2\,(M + N + K) - 4.$$

  Thus we must show

  $$\prod_{i=1}^{n}(A_i + B_i - 1) + \prod_{i=1}^{n}(A_i + C_i - 1) \geq 2\Big(\prod_i A_i + \prod_i B_i + \prod_i C_i\Big) - 4.$$

- Fix all but one coordinate, say the k-th. View

  $$F(A_k,B_k,C_k)=\prod_{i\neq k}(A_i{+}B_i{-}1)\cdot(A_k{+}B_k{-}1)+\prod_{i\neq k}(A_i{+}C_i{-}1)\cdot(A_k{+}C_k{-}1)-\big[\,2(M{+}N{+}K){-}4\,\big]$$

  as a function of the single triple (A_k,B_k,C_k), with all other A_i,B_i,C_i held fixed at ≥ 1. We get

  $$\frac{\partial}{\partial A_k}F=\prod_{i\neq k}(A_i+B_i-1)+\prod_{i\neq k}(A_i+C_i-1)-2\prod_{i\neq k}A_i.$$

  Now

  $$2\prod_{i\neq k}A_i=\prod_{i\neq k}A_i+\prod_{i\neq k}A_i\leq\prod_{i\neq k}(A_i+B_i-1)+\prod_{i\neq k}(A_i+C_i-1)$$

  for $A_i,B_i,C_i\geq 1$. Hence $\partial F/\partial B_k\geq 0$ Analogous estimates show $\partial F/\partial B_k\geq 0$ and $\partial F/\partial C_k\geq 0$. In other words, raising any one of the three entries A_k,B_k,C_k do not decrease the left minus right side F.

- Because each $e_{ij}\geq 0$, each $A_i,B_i,C_i\geq 1$ and there exist i_1,i_2,i_3 such that $A_{i_1},B_{i_2},C_{i_3}\geq 2$, we have $P\geq 3,Q\geq 3,M,N,K\geq 2$. Hence expression

  $$P+Q-2(M+N+K)+4$$

  reach the minimal value when $P=Q=3,M=N=K=2$, that is $P{+}Q{-}2(M{+}N{+}K){+}4=4+4-2(2+2+2)+4=0$

In conclusion:

Since increasing any coordinate A_i,B_i,C_i makes $P+Q-[2(M+N+K)-4]$ do not decrease, and its minimal value is 0 , it follows that for A_i,B_j,C_k satisfying the hypothesis

$$P+Q\geq 2(M+N+K)-4.$$

Equivalently the original inequality holds. □

Remark 5.7. With minor modification on the hypothesis, the proposition holds if we add +4 on the left hand side which accounts for the parameters corresponding to the affine shifts.

Example: case $k>2$.

In the case there are more than two entries per row. The key point is that the reduced mode-$[m]$ flattenings can be also applied to a matrix $\mathbf{M}$ that is a concatenation of several components. We do not prove a general statement but let us give an example:

Example 5.2 (Case 3 entries)**.** *Consider the systems of equations in*

https://github.com/pilarcoscojuela/Thesis/blob/DME_minus_3_entries/components_1_and_2.txt

These systems of equations correspond to the first and second components of the example in

https://github.com/pilarcoscojuela/Thesis/blob/DME_minus_3_entries/initial_setup.txt

We can build a matrix 4×8 *where rows are indexed by*

```
[
    Rt1*Kt2,
    Rt2*Kt3,
    Rt1*Kt1 + Rt2*Kt2,
    Rt1*Kt3 + Rt2*Kt1
]
```

and columns by

```
[
    Zt4,
    Zt3,
    Zt1,
    Zt2,
    Xt1,
    Xt2
]
```

The matrix is:

```
mat_tot_zx:= [[T^26   z[52] + T^308   z[53]   T^640   T^919   T^801],
[z[49]   T^139   T^449   z[54] + T^770   T^950   T^700],
[z[52]   z[51] + T^299   z[50]   z[53] + T^691   T^923   T^782],
[z[51]   z[49] + T^19   z[54]   z[50] + T^507   T^141   T^557]]
```

5.2 Reduction of the number of variables: DME minus

The weight-reduction maps of Section 4.4 can also be applied in the DME-minus setting to reduce the number of terms. There are, however, two points require discussion; we comment on them below.

- In the DME version 3.3 we could use a fresh weight-reduction map each time we solve the system corresponding to a row of $\mathbf{E}_r$. In the DME-minus version, however, the computation of collision variables requires two components simultaneously; consequently, the same weights must be used in the systems of equations corresponding to both components.
- At the end of Section 4.4 we noted the drawback that the reduced systems for the variables $\hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}}(Q_i)}$ may fail to have a unique solution. This issue does indeed arise in the DME-minus setting where each system of equations

$$\left\{ \hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}}(Q_j)} = \sum_{\substack{\mathbf{t}\in\mathrm{Supp}(Q_i)\\ \sigma_{\mathbf{a}}(\mathbf{t})=\mathbf{t}'}} \mathbf{t}(a_1,\dots,a_N)\, C_{\mathbf{t},Q_i} \right\}_{\substack{\mathbf{t}'\in\mathrm{Supp}(\sigma_{\mathbf{a}}(Q_j))\\ j=1,3,\dots,n-1}}. \tag{5.10}$$

  admits a finite set of solutions rather than a single solution. Empirically we observe that all unknowns depend linearly on a single distinguished variable, which itself can take two possible values. We denote this distinguished variable by

$$\hat{C}_{\mathbf{t}'_0,\sigma_{\mathbf{a}}(Q_{n-1})}(x_1,\dots,x_N)$$

  to emphasize its dependence on $(x_1,\dots,x_N)$.

  To resolve the ambiguity described above, we evaluate the identities of type (5.10) at several distinct sampling points $\mathbf{a}_1,\dots,\mathbf{a}_r \in \mathbb{K}^N$. We choose these points so that, for every monomial $\mathbf{t} \in \mathrm{Supp}(Q_{n-1})$ satisfying $\sigma(\mathbf{t}) = \mathbf{t}'_0$, the evaluations $\mathbf{t}(\mathbf{a}_i)$ are equal for all i. Under this condition the value of the distinguished variable $\hat{C}_{\mathbf{t}'_0,\sigma_{\mathbf{a}_i}(Q_{n-1})}(\mathbf{a}_i)$ is the same for every sampling point $\mathbf{a}_i$. Fixing one of the two admissible values of this variable for one sampling point then allows us to form as many independent linear combinations as needed to recover the remaining unknowns $C_{\mathbf{t},Q_j}$ for $j = 1,3,5,\dots,n-1$.

There is a small technical caveat, which we have confirmed experimentally but whose validity appears to depend on the instance. The question is:

In the DME-minus case, can one always find sufficiently many sampling points $\mathbf{a}_i$ such that all unknowns $C_{\mathbf{t},Q_j}$ are recoverable from the weighted variables $\hat{C}_{\mathbf{t}',\sigma_{\mathbf{a}_i}(Q_j)}$?

So far, our experiments indicate that this strategy succeeds for the examples we tested, but we do not have a general theoretical proof guaranteeing the existence of the required sampling points for every instance.

5.3 Recovery of the variables before the exponential: DME minus

This section is devoted to see how we can compute $\mathcal{Q} = (Q_1, \ldots, Q_n) \subset \mathbb{F}_{q^2}[X_1, \ldots, X_N]$ that verifies

$$\pi(\mathbf{E}_r(\mathcal{Q})) = \mathcal{P}^-. \tag{5.11}$$

We assume that we do not have collisions as we have already compute the values of the collision variables as shown in the previous chapter and the affine shifts $d_1, \ldots, d_n$ of $\mathbf{A}_r^{-1}$. In the case of the DME minus, recovery is more subtle as the equations we have are of the form

$$[(A_{\mathbf{t}Q_{j_1}} + uB_{\mathbf{t}Q_{j_1}})^{[a]}(C_{\mathbf{t}'Q_{j_2}} + uD_{\mathbf{t}'Q_{j_2}})^{[b]}]_1 + \alpha_{\mathbf{t}Q_{j_1}\mathbf{t}'Q_{j_2}} \tag{5.12}$$

where $\alpha_{\mathbf{t}Q_{j_1}\mathbf{t}'Q_{j_2}} \in \mathbb{F}_q$.

A priori it is not clear why given $\mathcal{P}^-$, we should expect that there exists only a finite set of possibles $\mathcal{Q}$ verifying (5.11). Experimental results shows that this is the case for the exponential maps we consider in **DME**$^-$. Although we could not prove this in general, we will explain what occurs in an example.

5.3.1 Simple example

Consider the following matrices:

$$E_1 = \begin{pmatrix} 2^{a_0} & 0 & 0 & 0 \\ 2^{a_1} & 2^{a_2} & 0 & 0 \\ 0 & 0 & 2^{a_3} & 0 \\ 0 & 0 & 2^{a_4} & 2^{a_5} \end{pmatrix}, E_2 = \begin{pmatrix} 2^{b_0} & 0 & 0 & 2^{b_1} \\ 0 & 2^{b_2} & 0 & 0 \\ 0 & 2^{b_3} & 2^{b_4} & 0 \\ 0 & 0 & 0 & 2^{b_5} \end{pmatrix}, E_3 = \begin{pmatrix} 2^{c_0} & 2^{c_1} & 0 & 0 \\ 0 & 2^{c_2} & 0 & 2^{c_3} \\ 0 & 2^{c_4} & 0 & 2^{c_5} \\ 0 & 0 & 2^{c_6} & 2^{c_7} \end{pmatrix}$$

We want to compute $\mathcal{Q} = (Q_1, \ldots, Q_4)$ with

$$Q_1 = \sum_{i=1}^{\#\mathrm{Supp}(Q_1)} (A_i + uB_i)\mathbf{t}_{1i},\ Q_2 = \sum_{i=1}^{\#\mathrm{Supp}(Q_2)} (C_i + uD_i)\mathbf{t}_{2i},$$
$$Q_3 = \sum_{i=1}^{\#\mathrm{Supp}(Q_3)} (E_i + uF_i)\mathbf{t}_{3i},\ Q_4 = \sum_{i=1}^{\#\mathrm{Supp}(Q_4)} (G_i + uH_i)\mathbf{t}_{4i}.$$

where the variables are $A_i, B_i, C_j, D_j, E_k, F_k, G_\ell, H_\ell$ such that

$$\begin{aligned}[Q_1^{[c_0]}Q_2^{[c_1]}]_1 &= p_1\\ [Q_2^{[c_2]}Q_4^{[c_3]}]_1 &= p_3\\ [Q_2^{[c_4]}Q_4^{[c_5]}]_1 &= p_5\\ [Q_3^{[c_6]}Q_4^{[c_7]}]_1 &= p_7\end{aligned}$$

By powering this equations to $[-c_0], [-c_2], [-c_4], [-c_6]$ respectively we obtain

$$\begin{aligned}[Q_1Q_2^{[c_1-c_0]}]_1 &= p_1^{[-c_0]}\\ [Q_2Q_4^{[c_3-c_2]}]_1 &= p_3^{[-c_2]}\\ [Q_2Q_4^{[c_5-c_4]}]_1 &= p_5^{[-c_4]}\\ [Q_3Q_4^{[c_7-c_6]}]_1 &= p_7^{[-c_6]}.\end{aligned} \tag{5.13}$$

This four equations leads to four systems of equations:

$$\begin{cases}\alpha_{1,1} = \text{1st coordinate with respect to the base } 1, u \text{ of } (A_1 + u\cdot B_1)\cdot(C_1 + u\cdot D_1)^{e_1}\\ \alpha_{1,2} = \text{1st coordinate with respect to the base } 1, u \text{ of } (A_1 + u\cdot B_1)\cdot(C_2 + u\cdot D_2)^{e_1}\\ \vdots\\ \alpha_{i,j} = \text{1st coordinate with respect to the base } 1, u \text{ of } (A_i + u\cdot B_i)\cdot(C_j + u\cdot D_j)^{e_1}\end{cases}$$

$$\begin{cases}\beta_{1,1} = \text{1st coordinate with respect to the base } 1, u \text{ of } (C_1 + u\cdot D_1)\cdot(G_1 + u\cdot H_1)^{e_2}\\ \beta_{1,2} = \text{1st coordinate with respect to the base } 1, u \text{ of } (C_1 + u\cdot D_1)\cdot(G_2 + u\cdot H_2)^{e_2}\\ \vdots\\ \beta_{j,l} = \text{1st coordinate with respect to the base } 1, u \text{ of } (C_j + u\cdot D_j)\cdot(G_l + u\cdot H_l)^{e_2}\end{cases}$$

$$\begin{cases}\gamma_{1,1} = \text{1st coordinate with respect to the base } 1, u \text{ of } (C_1 + u\cdot D_1)\cdot(G_1 + u\cdot H_1)^{e_3}\\ \gamma_{1,2} = \text{1st coordinate with respect to the base } 1, u \text{ of } (C_1 + u\cdot D_1)\cdot(G_2 + u\cdot H_2)^{e_3}\\ \vdots\\ \gamma_{j,l} = \text{1st coordinate with respect to the base } 1, u \text{ of } (C_j + u\cdot D_j)\cdot(G_l + u\cdot H_l)^{e_3}\end{cases}$$

$$\begin{cases}\delta_{1,1} = \text{1st coordinate with respect to the base } 1, u \text{ of } (E_1 + u\cdot F_1)\cdot(G_1 + u\cdot H_1)^{e_4}\\ \delta_{1,2} = \text{1st coordinate with respect to the base } 1, u \text{ of } (E_1 + u\cdot F_1)\cdot(G_2 + u\cdot H_2)^{e_4}\\ \vdots\\ \delta_{k,l} = \text{1st coordinate with respect to the base } 1, u \text{ of } (E_k + u\cdot F_k)\cdot(G_l + u\cdot H_l)^{e_4}\end{cases}$$

being $e_1 = 2^{c_0-c_1}, e_2 = 2^{c_3-c_2}, e_3 = 2^{c_5-c_4}, e_4 = 2^{c_7-c_6}$. These systems can be rewritten as

$$\begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,j} \\ \vdots & \ddots & \vdots \\ \alpha_{i,1} & \cdots & \alpha_{i,j} \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ \vdots & \vdots \\ A_i & B_i \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_1^{e_1} & \cdots & C_j^{e_1} \\ D_1^{e_1} & \cdots & D_j^{e_1} \end{pmatrix}$$

$$\begin{pmatrix} \beta_{1,1} & \cdots & \beta_{1,l} \\ \vdots & \ddots & \vdots \\ \beta_{j,1} & \cdots & \beta_{j,l} \end{pmatrix} = \begin{pmatrix} C_1 & D_1 \\ \vdots & \vdots \\ C_j & D_j \end{pmatrix} \cdot \mathbf{W}_2 \cdot \begin{pmatrix} G_1^{e_2} & \cdots & G_l^{e_2} \\ H_1^{e_2} & \cdots & H_l^{e_2} \end{pmatrix}$$

$$\begin{pmatrix} \gamma_{1,1} & \cdots & \gamma_{1,l} \\ \vdots & \ddots & \vdots \\ \gamma_{j,1} & \cdots & \gamma_{j,l} \end{pmatrix} = \begin{pmatrix} C_1 & D_1 \\ \vdots & \vdots \\ C_j & D_j \end{pmatrix} \cdot \mathbf{W}_3 \cdot \begin{pmatrix} G_1^{e_3} & \cdots & G_l^{e_3} \\ H_1^{e_3} & \cdots & H_l^{e_3} \end{pmatrix}$$

$$\begin{pmatrix} \delta_{1,1} & \cdots & \delta_{1,l} \\ \vdots & \ddots & \vdots \\ \delta_{k,1} & \cdots & \delta_{k,l} \end{pmatrix} = \begin{pmatrix} E_1 & F_1 \\ \vdots & \vdots \\ E_k & F_k \end{pmatrix} \cdot \mathbf{W}_4 \cdot \begin{pmatrix} G_1^{e_4} & \cdots & G_l^{e_4} \\ H_1^{e_4} & \cdots & H_l^{e_4} \end{pmatrix}$$

We start by solving

$$\begin{cases} \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ A_2 & B_2 \end{pmatrix} \cdot \mathbf{W}_1 \cdot \begin{pmatrix} C_1^{e_1} & C_2^{e_1} \\ D_1^{e_1} & D_2^{e_1} \end{pmatrix} \\ \begin{pmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{pmatrix} = \begin{pmatrix} C_1 & D_1 \\ C_2 & D_2 \end{pmatrix} \cdot \mathbf{W}_2 \cdot \begin{pmatrix} G_1^{e_2} & G_2^{e_2} \\ H_1^{e_2} & H_2^{e_2} \end{pmatrix} \\ \begin{pmatrix} \gamma_{1,1} & \gamma_{1,2} \\ \gamma_{2,1} & \gamma_{2,2} \end{pmatrix} = \begin{pmatrix} C_1 & D_1 \\ C_2 & D_2 \end{pmatrix} \cdot \mathbf{W}_3 \cdot \begin{pmatrix} G_1^{e_3} & G_2^{e_3} \\ H_1^{e_3} & H_2^{e_3} \end{pmatrix} \\ \begin{pmatrix} \delta_{1,1} & \delta_{1,2} \\ \delta_{2,1} & \delta_{2,2} \end{pmatrix} = \begin{pmatrix} E_1 & F_1 \\ E_2 & F_2 \end{pmatrix} \cdot \mathbf{W}_4 \cdot \begin{pmatrix} G_1^{e_4} & G_2^{e_4} \\ H_1^{e_4} & H_2^{e_4} \end{pmatrix} \end{cases} .$$

Assuming that the matrices are invertible,from the second and the third equations we obtain

$$\mathbf{W}_2 \cdot \begin{pmatrix} G_1^{e_2} & G_2^{e_2} \\ H_1^{e_2} & H_2^{e_2} \end{pmatrix} \cdot \begin{pmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{pmatrix}^{-1} = \begin{pmatrix} C_1 & D_1 \\ C_2 & D_2 \end{pmatrix}^{-1} = \mathbf{W}_3 \cdot \begin{pmatrix} G_1^{e_3} & G_2^{e_3} \\ H_1^{e_3} & H_2^{e_3} \end{pmatrix} \cdot \begin{pmatrix} \gamma_{1,1} & \gamma_{1,2} \\ \gamma_{2,1} & \gamma_{2,2} \end{pmatrix}^{-1} \tag{5.14}$$

which is a system of four equations in four variables G_1, G_2, H_1, H_2. As the exponents are power of two, each of these equations is equivalent to k, being $q = 2^k$, linear equations in $4k$ variables over

$\mathbb{F}_2$. All together they give a linear system of $4k$ equations in $4k$ variables, that can be solved by Gaussian elimination with a complexity $O(64k^3)$.

Due to the structure of the equations we can do better, we can compute a LEX Gröbner basis efficiently. Define $G_{3a} := G_3^{e_2}, G_{4a} := G_4^{e_2}, G_{3b} := G_3^{e_3}, G_{4b} := G_4^{e_3}$, $H_{3a} := H_3^{e_2}, H_{4a} := H_4^{e_2}, H_{3b} := H_3^{e_3}, H_{4b} := H_4^{e_3}$ and consider the previous system of equations as a linear system of four equations in eight variables $G_{3a}, G_{4a}, G_{3b}, G_{4b}, H_{3a}, H_{4a}, H_{3b}, H_{4b}$.

To simplify this system of equations we are going to compute the row echelon form of the associate Macaulay matrix of degree 1 with the variables ordered as $G_{3a} > G_{4a} > G_{3b} > G_{4b} > H_{3a} > H_{4a} > H_{3b} > H_{4b}$. To explicitly write such matrix, let $W_2 = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, W_3 = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ and $\mathbf{B}^T = \begin{pmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{pmatrix}^{-1}, \mathbf{C}^T = \begin{pmatrix} \gamma_{1,1} & \gamma_{1,2} \\ \gamma_{2,1} & \gamma_{2,2} \end{pmatrix}^{-1}$.

Then by making the computations it can be verified that the Macaulay matrix of degree 1 of the system of equations from (5.14) with respect to $G_{3a} > G_{4a} > G_{3b} > G_{4b} > H_{3a} > H_{4a} > H_{3b} > H_{4b}$ is the 4×8 matrix:

$$\mathrm{Mac}_{<,1} = \left(\begin{array}{c|c|c|c} a_1\mathbf{B} & b_1\mathbf{C} & a_2\mathbf{B} & b_2\mathbf{C} \\ \hline a_3\mathbf{B} & b_3\mathbf{C} & a_4\mathbf{B} & b_4\mathbf{C} \end{array}\right)$$

Let

$$\mathbf{P} = \left(\begin{array}{c|c} a_1\mathbf{B} & b_1\mathbf{C} \\ \hline a_3\mathbf{B} & b_3\mathbf{C} \end{array}\right)$$

be the submatrix of $\mathrm{Mac}_{<,1}$ consisting of the first four rows. As $\mathbf{B}$ is invertible, then by Proposition 5.2 we know an explicit expression for $\mathbf{P}^{-1}$. Then, it can be checked that

$$\mathbf{P}^{-1} \cdot \mathrm{Mac}_{<,1} = \left(\begin{array}{c|c|c|c} \mathbf{I}_{2\times 2} & \mathbf{0} & \lambda\mathbf{I}_{2\times 2} & * \\ \hline \mathbf{0} & \mathbf{I}_{2\times 2} & * & \lambda'\mathbf{I}_{2\times 2} \end{array}\right)$$

where λ, λ' are depending on $a_i, b_i,\ i = 1, \ldots, 4$ and $*$ represent some matrices.

The system of linear equations given by

$$\mathbf{P}^{-1}\mathrm{Mac}_{<,1} = \mathbf{0}$$

has the same solutions as

$$\mathrm{Mac}_{<,1} = \mathbf{0}$$

but its structure is much simpler. The polynomials associated to their rows are LEX Groebner basis, $G = \{g_1, \ldots, g_4\}$ for the system of four linear equations in eight variables We describe here an Algorithm that computes from G a LEX Gröbner basis of the ideal generated by the equations of (5.14).

```
**Ensure:** $e_2 < e_3$.
    $G1a \leftarrow G_1^{e_2}, G2a \leftarrow G_2^{e_2}, H1a \leftarrow H_1^{e_2}, H2a \leftarrow H_2^{e_2}$.
    $G1b \leftarrow G_1^{e_3}, G2b \leftarrow G_2^{e_3}, H1b \leftarrow H_1^{e_3}, H2b \leftarrow H_2^{e_3}$.
**Require:** The Gröbner basis $G$ defined above where $G_{1b}, G_{2b}, H_{1b}, H_{2b}$ have been replaced by
    $G_{1a}^d, G_{2a}^d, H_{1a}^d, H_{1a}^d$ where $d = e_3/e_2$.
    Note that $\mathrm{LM}(g_1^d) = \mathrm{LM}(g_3), \mathrm{LM}(g_2^d) = \mathrm{LM}(g_4)$.
    $p_1 \leftarrow g_1^d + g_3, p_2 \leftarrow g_2^d + g_4$
    $p_1 \leftarrow (\mathrm{LC}(p_1))^{-1} \cdot p_1$;
    $p_2 \leftarrow (\mathrm{LC}(p_2))^{-1} \cdot p_2$;
    $p_3 \leftarrow p_1 + p_2$;
    $p_3 \leftarrow (\mathrm{LC}(p_3))^{-1} \cdot p_3$;
    $p_4 \leftarrow (p_1 + p_3^d)$;
    $p_4 \leftarrow (\mathrm{LC}(p_4))^{-1} \cdot p_4$;
    $p_5 \leftarrow p_4 + p_3$;
    $p_5 \leftarrow (\mathrm{LC}(p_5))^{-1} \cdot p_5$;
    $p_6 \leftarrow p_4^d + p_1$;
    $p_6 \leftarrow (\mathrm{LC}(p_6))^{-1} \cdot p_6$;
    $p_7 \leftarrow p_6 + p_3$;
    $p_7 \leftarrow (\mathrm{LC}(p_7))^{-1} \cdot p_7$;
    The polynomial $p_5 + p_7$ is univariate in the variable $H_{2a}$.
```

Algorithm 5: Univariate polynomial

Experimentally we obtain that $p_5 + p_7$ is of the form:

$$p_5 + p_7 = \sum_{i=0}^{4} c_i H_{2a}^{d^i}$$

for some $c_i \in \mathbb{F}_q$ and $d = e_3/e_2$. As d is a power of 2 we can see the univariate polynomial as k linear equations over $\mathbb{F}_2$. The arithmetic complexity of solving it is $O(k^3)$.

5.3.2 Using techniques of the extended attack

The second approach is to use the techniques explained in Chapter 3 to recover candidates to complete the public key $\mathcal{P}^-$ to a public key $\mathcal{P}$ of a full DME (i.e. version DME 2023). Recall that polynomials in $\mathcal{P}^- = (p_1, p_3, \ldots, p_{2n-1})$ are obtained from a public key $\mathcal{P} = (p_1 + up_2, \ldots, p_{2n-1} + up_{2n})$. Since in the DME minus version the last linear map can be assumed to be the identity and the affine shift can be recovered with the results of Chapter 4, the equations say for the i-th component (over $\mathbb{F}_{q^2}$) are

$$\left[\left(\sum_{\mathbf{s}_1 \in Supp(Q_{j_1})} C_{\mathbf{s}_1 Q_{j_1}}\right) \cdot \ldots \cdot \left(\sum_{\mathbf{s}_k \in Supp(Q_{j_k})} C_{\mathbf{s}_k Q_{j_k}}\right)\right]_1 = d_{\mathbf{s}_1 Q_{j_1} \ldots \mathbf{s}_k Q_{j_k}}$$

$$\left[\left(\sum_{\mathbf{s}_1 \in Supp(Q_{j_1})} C_{\mathbf{s}_1 Q_{j_1}}\right) \cdot \ldots \cdot \left(\sum_{\mathbf{s}_k \in Supp(Q_{j_k})} C_{\mathbf{s}_k Q_{j_k}}\right)\right]_u = e_{\mathbf{s}_1 Q_{j_1} \ldots \mathbf{s}_k Q_{j_k}}$$

being $C_{\mathbf{s}_\ell Q_{j_\ell}}$ and $e_{\mathbf{s}_1 Q_{j_1} \ldots \mathbf{s}_k Q_{j_k}}$ unknowns, where

$$p_{2i-1} = \sum_{\mathbf{s}_i \in Supp(Q_{j_i}), 1 \le i \le k} d_{\mathbf{s}_1 Q_{j_1} \ldots \mathbf{s}_k Q_{j_k}}$$

and

$$p_{2i} = \sum_{\mathbf{s}_i \in Supp(Q_{j_i}), 1 \le i \le k} e_{\mathbf{s}_1 Q_{j_1} \ldots \mathbf{s}_k Q_{j_k}}$$

Assume that $k = 2$, then to compute $e_{\mathbf{s}_1 Q_{j_1} s_2 Q_{j_2}}$ where $\mathbf{s}_i \in Supp(Q_{j_i})$ we can build a matrix $\mathbf{M}$ as in Section 4.3 of size $k_1 \times k_2$ where $k_1 = \text{Supp}(Q_{j_1})$ and $k_2 = \text{Supp}(Q_{j_2})$ such that the $\mathbf{s}_1, \mathbf{s}_2$ entry is $d_{\mathbf{s}_1 Q_{j_1} \mathbf{s}_2 Q_{j_2}} + u e_{\mathbf{s}_1 Q_{j_1} \mathbf{s}_2 Q_{j_2}}$ where $d_{\mathbf{s}_1 Q_{j_1} \mathbf{s}_2 Q_{j_2}}$ are known and $e_{\mathbf{s}_1 Q_{j_1} \mathbf{s}_2 Q_{j_2}}$ unknown. Note that under genericity conditions,

$$\dim(\mathcal{I}_{\text{Minors}(2), \mathbf{M}^{(h)}}) = m + n - 1$$

as entries of the matrix $\mathbf{M}^{(\mathbf{h})}$ are polynomials in mn variables. From there we cannot get an estimate on $\dim(\mathcal{I}_{\text{Minors}(2)})$. As we are interested in the solutions over $\mathbb{F}_q$, to compute it we will prove that solutions over $\mathbb{F}_q$ can be parametrized with two parameters (see Section 5.3.2.1). This implies that although over the algebraic closure we do not know $\dim(\mathcal{I}_{\text{Minors}(2)})$, this is not the case when we restrict to solutions over $\mathbb{F}_q$. This aligns with the fact that we obtain zero dimensional ideal when we consider equations corresponding to all the rows of $\mathbf{E}_r$ together.

Here we experimentally show how to recover the values $C_{\mathbf{s}_\ell, Q_\ell}$ by first computing the values of $e_{\mathbf{s}_1 Q_{j_1} \ldots \mathbf{s}_k Q_{j_k}}$, we restrict to the cases $k = 2$ and k=3.

The case when $\mathbf{E}_r$ has only nonzero entries per row is modelled as follows: assume

$$\mathbf{E}_r = \begin{pmatrix} [a_{11}] & 0 & 0 & [a_{14}] \\ 0 & [a_{22}] & [a_{23}] & 0 \\ [a_{31}] & 0 & [a_{33}] & 0 \\ 0 & [a_{42}] & 0 & [a_{44}] \end{pmatrix}$$

and we want to compute

$$\mathcal{Q} = \begin{pmatrix} \sum_{i=1}^{n_1} A_i \mathbf{t}_1(x_1, \ldots, x_N) \\ \sum_{i=1}^{n_2} B_i \mathbf{t}_2(x_1, \ldots, x_N) \\ \sum_{i=1}^{n_3} C_i \mathbf{t}_3(x_1, \ldots, x_N) \\ \sum_{i=1}^{n_4} D_i \mathbf{t}_4(x_1, \ldots, x_N) \end{pmatrix}$$

where $A_i, B_j, C_k, D_l,\ 1 \le i \le n_1, 1 \le j \le n_2, 1 \le k \le n_3, 1 \le l \le n_4$ where unknowns such that

$$\mathbf{E}_r(\mathcal{Q}) = \mathcal{P}^-$$

where $\mathcal{P}^- = (p_1, p_3, p_5, p_7)$ with

$$p_1 = \sum_{t_1,t_4} e_{t_1t_4}\mathbf{t}_1\mathbf{t}_4, \quad p_2 = \sum_{t_2,t_3} e_{t_2t_3}\mathbf{t}_2\mathbf{t}_3$$

$$p_3 = \sum_{t_1,t_3} e_{t_1t_3}\mathbf{t}_1\mathbf{t}_3, \quad p_4 = \sum_{t_2,t_4} e_{t_2t_4}\mathbf{t}_2\mathbf{t}_4.$$

We build the matrices:

- A matrix M_1 of size $n_1 \times n_4$ such that its entry $\mathbf{t}_1, \mathbf{t_4}$ is $(d_{\mathbf{t}_1\mathbf{t}_4} + ue_{\mathbf{t}_1\mathbf{t}_4})^{[-a_{11}]}$.
- A matrix M_2 of size $n_2 \times n_3$ such that its entry $\mathbf{t}_2, \mathbf{t_3}$ is $(d_{\mathbf{t}_2\mathbf{t}_3} + ue_{\mathbf{t}_2\mathbf{t}_3})^{[a_{33}-a_{31}-a_{23}]}$.
- A matrix M_3 of size $n_1 \times n_3$ such that its entry $\mathbf{t}_1, \mathbf{t_3}$ is $(d_{\mathbf{t}_1\mathbf{t}_3} + ue_{\mathbf{t}_1\mathbf{t}_3})^{[-a_{31}]}$.
- A matrix M_4 of size $n_2 \times n_4$ such that its entry $\mathbf{t}_2, \mathbf{t_4}$ is $(d_{\mathbf{t}_2\mathbf{t}_4} + ue_{\mathbf{t}_2\mathbf{t}_4})^{[a_{31}-a_{33}-a_{22}-a_{42}]}$.
- A matrix M_5 of size $n_2 \times n_4$ such that its entry $\mathbf{t}_2, \mathbf{t_4}$ is $(d_{\mathbf{t}_2\mathbf{t}_4} + ue_{\mathbf{t}_2\mathbf{t}_4})^{[a_{14}-a_{11}-a_{44}]}$.

Now we build four matrices by join $M_1, \dots, M_5$ as follows:

- Let N_1 the matrix obtained by join horizontally M_1 and M_3.
- Let N_2 the matrix obtained by join horizontally M_2 and M_4
- Let N_3 the matrix obtained by join horizontally M_2 and M_3
- Let N_4 the matrix obtained by join horizontally M_1 and M_5.

Then for each matrix $V_{\mathbb{F}_q}(\mathcal{I}^{N_i}_{\text{Minors}(2)})$ can be parametrized by two parameters, and

$$V_{\mathbb{F}_q}\left(\sum_{1\le i\le 4} \mathcal{I}^{N_i}_{\text{Minors}(2)}\right)$$

is a finite set. To compute it we first get the Gröbner basis of the minors (over $\mathbb{F}_{q^2}$) and then the Gröbner basis of the Weil descent of $J = \sum_{1\le i\le 4} \mathcal{I}^{N_i}_{\text{Minors}(2)}$ over $\mathbb{F}_q$. Note that this algorithm is easily modified to deal with any $\mathbf{E}_r$ that has two non-zero entries per row.

Finally, we describe how it can be adapted to the case of three entries per row. Interestingly in this case it is enough to consider only one component to get a finite set of solutions over $\mathbb{F}_q$. The way to proceed is to build two matrices:

- A matrix N_1 of size $n_1 \times (n_2 \cdot n_3)$ such that the $\mathbf{t}_1, \mathbf{t_2}\mathbf{t}_3$ element is $d_{\mathbf{t}_1\mathbf{t}_2\mathbf{t}_3} + ue_{\mathbf{t}_1\mathbf{t}_2\mathbf{t}_3}$.
- A matrix N_2 of size $n_2 \times (n_1 \cdot n_3)$ such that the $\mathbf{t}_2, \mathbf{t_1}\mathbf{t}_3$ element is $d_{\mathbf{t}_1\mathbf{t}_2\mathbf{t}_3} + ue_{\mathbf{t}_1\mathbf{t}_2\mathbf{t}_3}$.

Now we have $V_{\mathbb{F}_q}(\mathcal{I}^{N_i}_{\text{Minors}(2)})$ can be parametrized by two parameters (see next section), and

$$V_{\mathbb{F}_q}\left(\sum_{1\leq i\leq 2}\mathcal{I}^{N_i}_{\text{Minors}(2)}\right)$$

is a finite set. To compute it we first get the Gröbner basis of $\mathcal{I}^{N_i}_{\text{Minors}(2)}$ (over $\mathbb{F}_{q^2}$) and then the Gröbner basis of the Weil descent of $J = \sum_{1\leq i\leq 2}\mathcal{I}^{N_i}_{\text{Minors}(2)}$ over $\mathbb{F}_q$.

5.3.2.1 On the preimage of a special family of points under the Kronecker product

Let $n, m \geq 2$, $\mathbf{a} \in \mathbb{C}^n$, $\mathbf{b} \in \mathbb{C}^m$, and $\mathbf{c} = \mathbf{a}\otimes\mathbf{b} = (a_1b_1, a_1b_2, \ldots, a_nb_m) \in \mathbb{C}^{nm}$. Assume that only the real part of the entries of $\mathbf{c}$ are known. The main question that we discuss in this article is whether it is possible or not to recover the imaginary part of $\mathbf{c}$.

To simplify notation, we use a double index to refer to the entries of $\mathbf{c}$, i.e. we write $c_{ij} = a_ib_j$ with $i = 1, \ldots, n$ and $j = 1, \ldots, m$.

Lemma 5.8. *Let $\mathbf{c} \in \mathbb{C}^{nm}$. The following are equivalent:*

1. $\mathbf{c} = \mathbf{a}\otimes\mathbf{b}$ *for some* $\mathbf{a} \in \mathbb{C}^n$ *and* $\mathbf{b} \in \mathbb{C}^m$.
2. $c_{ij}c_{kl} = c_{il}c_{kj}$ *for any* $i, k = 1, \ldots, n$ *and* $j, l = 1, \ldots, m$.

Proof. $(1 \Rightarrow 2)$ $c_{ij}c_{kl} = a_ib_ja_kb_l = a_ib_la_kb_j = c_{il}c_{kj}$.

$(2 \Rightarrow 1)$ Suppose that $c_{i_0j_0} \neq 0$. Define $a_i = c_{ij_0}$ for $i = 1, \ldots, n$ and $b_j = c_{i_0j}/c_{i_0j_0}$ for $j = 1, \ldots, m$. Using our assumption (2), we have

$$a_ib_j = \frac{c_{ij_0}c_{i_0j}}{c_{i_0j_0}} = c_{ij},$$

so $\mathbf{c} = \mathbf{a}\otimes\mathbf{b}$. Finally, the case where $\mathbf{c}$ is the zero vector is trivial. □

Note that the equations with $i = k$ or $j = l$ in (2) are trivial. Moreover, by the symmetry of this system of equations, we can reduce (2) to only the cases where $i < k$ and $j < l$. This gives a total of $\binom{n}{2}\binom{m}{2}$ quadratic equations in nm unknowns.

None of these equations can be removed in Lemma 5.8. Indeed, assume without loss of generality that the equation $c_{11}c_{22} = c_{12}c_{21}$ corresponding to $i = k = 1$ and $j = l = 2$ can be removed. The vector $\mathbf{c}$ whose entries are defined by

$$c_{ij} = \begin{cases} 0 & \text{if } i = 1 \wedge j = 1 \\ 1 & \text{if } i = 1 \wedge j = 2 \\ 1 & \text{if } i = 2 \wedge j = 1 \\ 1 & \text{if } i = 2 \wedge j = 2 \\ 0 & \text{otherwise} \end{cases}$$

satisfies all the remaining equations, but cannot be expressed as $\mathbf{c} = \mathbf{a} \otimes \mathbf{b}$ for any $\mathbf{a} \in \mathbb{C}^n$ and $\mathbf{b} \in \mathbb{C}^m$, since otherwise, by lemma 5.8, it would also satisfy the equation that we removed. This means that the implication $(2 \Rightarrow 1)$ is no longer valid as soon as a single equation is removed.

If we restrict to vectors $\mathbf{c} \in \mathbb{C}^{nm}$ with $c_{i_0 j_0} \neq 0$, we can reduce the number of equations to $(n-1)(m-1)$. The proof of $(2 \Rightarrow 1)$ in Lemma 5.8 only requires the equations $c_{i_0 j_0} c_{kl} = c_{i_0 l} c_{k j_0}$ for $k \neq i_0$ and $l \neq j_0$.

Lemma 5.9. *Let $\mathbf{c} \in (\mathbb{C})^{nm}$ such that $c_{i_0 j_0} \neq 0$. The following are equivalent:*

1. *$\mathbf{c} = \mathbf{a} \otimes \mathbf{b}$ for some $\mathbf{a} \in \mathbb{C}^n$ and $\mathbf{b} \in \mathbb{C}^m$ with $a_{i_0} \neq 0$ and $b_{j_0} \neq 0$.*

2. *$c_{i_0 j_0} c_{kl} = c_{i_0 l} c_{k j_0}$ for any $k \neq i_0$ and $l \neq j_0$.*

Moreover, if $\mathbf{c} = \mathbf{a} \otimes \mathbf{b} = \mathbf{a}' \otimes \mathbf{b}'$ with $\mathbf{a}, \mathbf{a}' \in (\mathbb{C}^*)^n$ and $\mathbf{b}, \mathbf{b}' \in (\mathbb{C}^*)^m$, there exists $\lambda \in \mathbb{C}^*$ such that $\mathbf{a}' = \lambda \mathbf{a}$ and $\mathbf{b}' = \lambda^{-1} \mathbf{b}$.

Proof. $(1 \Leftrightarrow 2)$ is proven as in Lemma 5.8, except that $i_0 = j_0 = 1$ must be chosen for the second implication.

For the other part, assume that $\mathbf{c} = \mathbf{a} \otimes \mathbf{b} = \mathbf{a}' \otimes \mathbf{b}'$. Since $c_{i_0 j_0} \neq 0$, we have that $a_{i_0}, a'_{i_0}, b_{j_0}, b'_{j_0} \neq 0$. Define $\lambda = a'_{i_0}/a_{i_0} \in \mathbb{C}^*$. From $c_{i_0 j} = a_{i_0} b_j = a'_{i_0} b'_j$ for any $j = 1, \ldots, m$, we get $b' = \lambda^{-1} b$ and in particular $\lambda = b_{j_0}/b'_{j_0}$. By repeating the reasoning with $c_{i j_0} = a_i b_{j_0} = a'_i b'_{j_0}$, we conclude that $\mathbf{a}' = \lambda \mathbf{a}$. □

The polynomial map $\mathbb{C}^n \times \mathbb{C}^m \to \mathbb{C}^{nm}$ given by $(\mathbf{a}, \mathbf{b}) \mapsto \mathbf{a} \otimes \mathbf{b}$ sends the Zariski open set $(\mathbb{C}^*)^n \times (\mathbb{C}^*)^m$ to an open set in $\mathbb{C}^{nm}$ of dimension $n + m - 1$, since the fibers over any point in the image have dimension 1 by Lemma 5.9. This proves that none of the $(n-1)(m-1)$ equations in (2) can be removed.

Now, we decompose the entries of $\mathbf{c}$ in real and imaginary part, that is, we write $c_{ij} = d_{ij} + i e_{ij}$ with $d_{ij}, e_{ij} \in \mathbb{R}$. Our original question asks for a method to recover the vector $\mathbf{e} = (e_{ij}) \in \mathbb{R}^{nm}$ when given the vector $\mathbf{d} = (d_{ij}) \in \mathbb{R}^{nm}$.

For simplicity, assume first that $d_{11} \neq 0$, which in particular implies that $c_{11} \neq 0$. According to Lemma 5.9, the problem reduces to the $(n-1)(m-1)$ quadratic equations

$$(d_{11} + ie_{11})(d_{kl} + ie_{kl}) = (d_{1l} + ie_{1l})(d_{k1} + ie_{k1})$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. Splitting these equations into real and imaginary part, we get

$$d_{11}d_{kl} - e_{11}e_{kl} = d_{1l}d_{k1} - e_{k1}e_{1l}$$
$$d_{11}e_{kl} + d_{kl}e_{11} = d_{1l}e_{k1} + d_{k1}e_{1l}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. From the second row of equations, we can express e_{kl} linearly in terms of e_{11}, e_{1l} and e_{k1}. Doing so, we get

$$e_{kl} = \frac{d_{1l}}{d_{11}} e_{k1} + \frac{d_{k1}}{d_{11}} e_{1l} - \frac{d_{kl}}{d_{11}} e_{11}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots m$. Plugging these expressions back into the first row of the equations above (the ones coming from the real part), we get

$$d_{11}d_{kl} - e_{11}\left(\frac{d_{1l}}{d_{11}} e_{k1} + \frac{d_{k1}}{d_{11}} e_{1l} - \frac{d_{kl}}{d_{11}} e_{11}\right) = d_{1l}d_{k1} - e_{k1}e_{1l}$$

which can be reformulated as

$$\frac{d_{kl}}{d_{11}} e_{11}^2 + e_{k1}e_{1l} - \frac{d_{k1}}{d_{11}} e_{11}e_{1l} - \frac{d_{1l}}{d_{11}} e_{11}e_{k1} = d_{1l}d_{k1} - d_{11}d_{kl}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. At this point, we have $(n-1)(m-1)$ quadratic equations in $n + m - 1$ unknowns.

To simplify the equations, we make the change of variables

$$e_{1l} = \tilde{e}_{1l} + \frac{d_{1l}}{d_{11}} e_{11}$$
$$e_{k1} = \tilde{e}_{k1} + \frac{d_{k1}}{d_{11}} e_{11}$$

for $k, l \geq 2$, but we keep e_{11}. This reduces our equations to

$$\frac{d_{11}d_{kl} - d_{1l}d_{kl}}{d_{11}^2} e_{11}^2 + \tilde{e}_{k1}\tilde{e}_{1l} = d_{1l}d_{k1} - d_{11}d_{kl}$$

for $k, l \geq 2$. Moving the term with e_{11}^2 to the right side, we get

$$\tilde{e}_{k1}\tilde{e}_{1l} = (d_{1l}d_{k1} - d_{11}d_{kl})\left(1 + \frac{e_{11}^2}{d_{11}^2}\right) = -\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k1} & d_{kl} \end{pmatrix} \underbrace{\left(1 + \frac{e_{11}^2}{d_{11}^2}\right)}_{=|1+ie_{11}/d_{11}|^2 \neq 0}$$

for $k, l \geq 2$.

Note that if we define $\mathbf{v} = (\tilde{e}_{k1})_{k\geq 2} \in \mathbb{R}^{n-1}$ and $\mathbf{w} = (\tilde{e}_{1l})_{l\geq 2} \in \mathbb{R}^{m-1}$, the left side of the equation above is just $\mathbf{v} \otimes \mathbf{w}$. We have already studied a system like that before (the analysis over $\mathbb{C}$ can also be done over any field). The necessary and sufficient condition for the existence of a solution is that

$$\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k1} & d_{kl} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k'1} & d_{k'l'} \end{pmatrix} = \det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k1} & d_{kl'} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k'1} & d_{k'l} \end{pmatrix}$$

for all $k, k' = 2, \dots, n$ and $l, l' = 2, \dots, m$. Of course, only the cases with $2 \leq k < k' \leq n$ and $2 \leq l < l' \leq m$ are necessary, by the symmetry of the equations. Moreover, since we are assuming that $\tilde{e}_{21}\tilde{e}_{12} \neq 0$, we can reduce the set of equations to only those with $k = l = 2$ and $k', l' \geq 3$.

Proposition 5.10. *Let $\mathbf{d} \in \mathbb{R}^{nm}$ be such that $d_{11} \neq 0$ and $d_{11}d_{22} \neq d_{12}d_{21}$. The following are equivalent:*

1. *$\mathbf{d}$ is the real part of $\mathbf{a} \otimes \mathbf{b}$ for some $\mathbf{a} \in \mathbb{C}^n$ and $\mathbf{b} \in \mathbb{C}^m$.*

2. *For any $k, k' = 2, \dots, n$ and $l, l' = 2, \dots, m$,*

$$\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k1} & d_{kl} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k'1} & d_{k'l'} \end{pmatrix} = \det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k1} & d_{kl'} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k'1} & d_{k'l} \end{pmatrix}.$$

3. *For any $k' = 3, \dots, n$ and $l' = 3, \dots, m$,*

$$\det\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k'1} & d_{k'l'} \end{pmatrix} = \det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{21} & d_{2l'} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{k'1} & d_{k'2} \end{pmatrix}.$$

In this case, the imaginary part $\mathbf{e} \in \mathbb{R}^{nm}$ of $\mathbf{a} \otimes \mathbf{b}$ is given by the following equations

$$e_{k1} = -\lambda \det\begin{pmatrix} d_{11} & d_{12} \\ d_{k1} & d_{k2} \end{pmatrix}\left(1 + \frac{e_{11}^2}{d_{11}^2}\right) + \frac{d_{k1}}{d_{11}}e_{11}$$

$$e_{1l} = \lambda^{-1}\frac{\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{21} & d_{2l} \end{pmatrix}}{\det\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}} + \frac{d_{1l}}{d_{11}}e_{11}$$

$$e_{kl} = \frac{d_{1l}}{d_{11}}e_{k1} + \frac{d_{k1}}{d_{11}}e_{1l} - \frac{d_{kl}}{d_{11}}e_{11}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$ where $\lambda \in \mathbb{R}^*$ and $e_{11} \in \mathbb{R}$ are free parameters. Vectors $\mathbf{a} \in \mathbb{C}^n$ and $\mathbf{b} \in \mathbb{C}^m$ can be reconstructed as

$$a_i = \mu(d_{i1} + ie_{i1})$$
$$b_j = \mu^{-1} \frac{d_{1j} + ie_{1j}}{d_{11} + ie_{11}}$$

for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ where $\mu \in \mathbb{C}^*$ is a free parameter. All solutions are included in this parametrization.

This results generalizes, with some minor changes, to any quadratic extension

$$\mathbb{L} = \mathbb{K}[u]/\langle u^2 + \alpha u + \beta \rangle$$

of a field $\mathbb{K}$. Note that the irreducibility of the minimal polynomial of u implies that $\beta \neq 0$. Any element of $\mathbb{L}$ can be expressed as $d + ue$ with $d, e \in \mathbb{K}$. We define real and imaginary part of $x = d + ue \in \mathbb{L}$ as $\mathrm{Re}(x) = d$ and $\mathrm{Im}(x) = e$.

Recall that our main problem is to recover the vector $\mathbf{e} = \mathrm{Im}(\mathbf{a} \otimes \mathbf{b}) \in \mathbb{K}^{nm}$ when given $\mathbf{d} = \mathrm{Re}(\mathbf{a} \otimes \mathbf{b}) \in \mathbb{K}^{nm}$ where $\mathbf{a} \in \mathbb{L}^n$ and $\mathbf{b} \in \mathbb{L}^m$ are unknown. As in the previous case, we will see that also $\mathbf{a}$ and $\mathbf{b}$ can be reconstructed.

For simplicity, we assume that $d_{11} \neq 0$, which in turn implies that $a_1 \neq 0$ and $b_1 \neq 0$. By Lemma 5.9, it is enough to consider the $(n-1)(m-1)$ quadratic equations

$$(d_{11} + ue_{11})(d_{kl} + ue_{kl}) = (d_{1l} + ue_{1l})(d_{k1} + ue_{k1})$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. Separating the real and imaginary parts, we get

$$d_{11}d_{kl} - \beta e_{11}e_{kl} = d_{1l}d_{k1} - \beta e_{1l}e_{k1}$$
$$d_{11}e_{kl} + d_{kl}e_{11} - \alpha e_{11}e_{kl} = d_{1l}e_{k1} + d_{k1}e_{1l} - \alpha e_{1l}e_{k1}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. We can eliminate the quadratic part in the second row by subtracting the first row multiplied by α/β. Doing so, the system of equations becomes

$$d_{11}d_{kl} - \beta e_{11}e_{kl} = d_{1l}d_{k1} - \beta e_{1l}e_{k1}$$
$$d_{11}e_{kl} + d_{kl}e_{11} - \frac{\alpha}{\beta} d_{11}d_{kl} = d_{1l}e_{k1} + d_{k1}e_{1l} - \frac{\alpha}{\beta} d_{1l}d_{k1}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. Using the second row of equations, we write e_{kl} in terms of e_{11}, e_{1l} and e_{k1}, as follows:

$$e_{kl} = \frac{d_{1l}}{d_{11}} e_{k1} + \frac{d_{k1}}{d_{11}} e_{1l} - \frac{d_{kl}}{d_{11}} e_{11} + \frac{\alpha}{\beta} \frac{d_{11}d_{kl} - d_{1l}d_{k1}}{d_{11}}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. Replacing the expressions for e_{kl} into the first row of equations above, we get

$$d_{11}d_{kl} - \beta e_{11}\left(\frac{d_{1l}}{d_{11}}e_{k1} + \frac{d_{k1}}{d_{11}}e_{1l} - \frac{d_{kl}}{d_{11}}e_{11} + \frac{\alpha}{\beta}\frac{d_{11}d_{kl} - d_{1l}d_{k1}}{d_{11}}\right) = d_{1l}d_{k1} - \beta e_{1l}e_{k1}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. After some algebraic manipulation, we obtain

$$\frac{d_{kl}}{d_{11}}e_{11}^2 + e_{1l}e_{k1} - \frac{d_{k1}}{d_{11}}e_{11}e_{1l} - \frac{d_{1l}}{d_{11}}e_{11}e_{k1} - \frac{\alpha}{\beta}\frac{d_{11}d_{kl} - d_{1l}d_{k1}}{d_{11}}e_{11} = \frac{d_{1l}d_{k1} - d_{11}d_{kl}}{\beta}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. To simplify the equations, we perform the substitutions

$$\begin{aligned} e_{1l} &= \tilde{e}_{1l} + \frac{d_{k1}}{d_{11}}e_{11} \\ e_{k1} &= \tilde{e}_{k1} + \frac{d_{1l}}{d_{11}}e_{11} \end{aligned}$$

and we get

$$\tilde{e}_{1l}\tilde{e}_{k1} = -\frac{1}{\beta}\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k1} & d_{kl} \end{pmatrix} \underbrace{\left(1 - \alpha\frac{e_{11}}{d_{11}} + \beta\frac{e_{11}^2}{d_{11}^2}\right)}_{=N_{\mathbb{L}/\mathbb{K}}(1+ue_{11}/d_{11})\neq 0}$$

for $k = 2, \ldots, n$ and $l = 2, \ldots, m$. Now, we have all the ingredients to state the generalization of proposition 5.10 to the field extension $\mathbb{L}/\mathbb{K}$.

Proposition 5.11. *Let $\mathbf{d} \in \mathbb{K}^{nm}$ be such that $d_{11} \neq 0$ and $d_{11}d_{22} \neq d_{12}d_{21}$. The following are equivalent:*

1. *$\mathbf{d}$ is the real part of $\mathbf{a} \otimes \mathbf{b}$ for some $\mathbf{a} \in \mathbb{L}^n$ and $\mathbf{b} \in \mathbb{L}^m$.*

2. *For any $k, k' = 2, \ldots, n$ and $l, l' = 2, \ldots, m$,*

$$\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k1} & d_{kl} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k'1} & d_{k'l'} \end{pmatrix} = \det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k1} & d_{kl'} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k'1} & d_{k'l} \end{pmatrix}.$$

3. *For any $k' = 3, \ldots, n$ and $l' = 3, \ldots, m$,*

$$\det\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{k'1} & d_{k'l'} \end{pmatrix} = \det\begin{pmatrix} d_{11} & d_{1l'} \\ d_{21} & d_{2l'} \end{pmatrix}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{k'1} & d_{k'2} \end{pmatrix}.$$

In this case, the imaginary part $\mathbf{e} \in \mathbb{K}^{nm}$ *of* $\mathbf{a} \otimes \mathbf{b}$ *is given by the following equations*

$$\begin{aligned}
e_{k1} &= -\frac{\lambda}{\beta}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{k1} & d_{k2} \end{pmatrix}\left(1 - \alpha\frac{e_{11}}{d_{11}} + \beta\frac{e_{11}^2}{d_{11}^2}\right) + \frac{d_{k1}}{d_{11}}e_{11} \\
e_{1l} &= \lambda^{-1}\frac{\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{21} & d_{2l} \end{pmatrix}}{\det\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}} + \frac{d_{1l}}{d_{11}}e_{11} \\
e_{kl} &= \frac{d_{1l}}{d_{11}}e_{k1} + \frac{d_{k1}}{d_{11}}e_{1l} - \frac{d_{kl}}{d_{11}}e_{11} + \frac{\alpha}{\beta}\frac{\det\begin{pmatrix} d_{11} & d_{1l} \\ d_{k1} & d_{kl} \end{pmatrix}}{d_{11}}
\end{aligned}$$

for $k = 2, \ldots, n$ *and* $l = 2, \ldots, m$ *where* $\lambda \in \mathbb{K}^*$ *and* $e_{11} \in \mathbb{K}$ *are free parameters. Vectors* $\mathbf{a} \in \mathbb{L}^n$ *and* $\mathbf{b} \in \mathbb{L}^m$ *can be reconstructed as*

$$\begin{aligned}
a_i &= \mu(d_{i1} + ue_{i1}) \\
b_j &= \mu^{-1}\frac{d_{1j} + ue_{1j}}{d_{11} + ue_{11}}
\end{aligned}$$

for $i = 1, \ldots, n$ *and* $j = 1, \ldots, m$ *where* $\mu \in \mathbb{L}^*$ *is a free parameter. All solutions are included in this parametrization.*

Both a_i and b_j in proposition 5.11 can be reparametrized in terms of the $\tilde{u} = \mu(1 + ue_{11}/d_{11}) \in \mathbb{L}^*$.

$$\begin{aligned}
a_i &= \mu(d_{i1} + ue_{i1}) \\
&= \mu\left[d_{i1} - \frac{\lambda u}{\beta}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{i1} & d_{i2} \end{pmatrix} N_{\mathbb{L}/\mathbb{K}}\left(1 + u\frac{e_{11}}{d_{11}}\right) + \frac{d_{i1}}{d_{11}}ue_{11}\right] \\
&= \mu\left[d_{i1}\left(1 + u\frac{e_{11}}{d_{11}}\right) - \frac{\lambda u}{\beta}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{i1} & d_{i2} \end{pmatrix}\left(1 + u\frac{e_{11}}{d_{11}}\right)\left(1 + \overline{u}\frac{e_{11}}{d_{11}}\right)\right] \\
&= \tilde{\mu}\left[d_{i1} - \frac{\lambda u}{\beta}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{i1} & d_{i2} \end{pmatrix}\left(1 + \overline{u}\frac{e_{11}}{d_{11}}\right)\right] \\
&= \tilde{\mu}\left[d_{i1} - \frac{\lambda e_{11}}{d_{11}}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{i1} & d_{i2} \end{pmatrix} - \frac{\lambda u}{\beta}\det\begin{pmatrix} d_{11} & d_{12} \\ d_{i1} & d_{i2} \end{pmatrix}\right] \\
b_j &= \mu^{-1}\frac{d_{1j} + ue_{1j}}{d_{11} + ue_{11}} = \frac{d_{1j} + ue_{1j}}{\tilde{\mu}d_{11}} \\
&= \tilde{\mu}^{-1}d_{11}^{-1}\left[d_{1j}\left(1 + \frac{e_{11}}{d_{11}}u\right) + \lambda^{-1}\frac{\det\begin{pmatrix} d_{11} & d_{1j} \\ d_{21} & d_{2j} \end{pmatrix}}{\det\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}}u\right]
\end{aligned}$$

Chapter 6

Variants

6.1 Other DME minus schemes

In Chapter 5 we studied the security of the DME minus scheme given by Definition 3.18 when π is defined as:

$$\pi : (\mathbb{F}_q[x_1, \dots, x_N])^N \longrightarrow (\mathbb{F}_q[x_1, \dots, x_N])^n, \ \pi(p_1, \dots, p_N) = (p_1, p_3, \dots, p_{N-1}),$$

where $N = 2n$. The goal of this section is to study if results from Chapter 5 can be applied for other choices of π.

First we consider

$$\pi : (\mathbb{F}_q[x_1, \dots, x_N])^N \longrightarrow (\mathbb{F}_q[x_1, \dots, x_N])^n, \ \pi(p_1, \dots, p_N) = (p_1, p_2, \dots, p_{N/2}) = (p_1, p_2, \dots, p_n),$$

as $N = 2n$.

Assuming n is even, to analyze this case note that $\mathcal{P}^-$ is formed of polynomials that can be regarded over $\mathbb{F}_{q^2}$ as both coordinates in the $\mathbb{F}_q$-basis $\{1, u\}$ of $\mathbb{F}_{q^2}$ are known. Specifically, $\mathcal{P}^-$ can be seen over $\mathbb{F}_{q^2}$:

$$\begin{aligned} P_1 &= p_1 + up_2 \\ P_2 &= p_3 + up_4 \\ &\vdots \\ P_{n/2} &= p_{(n-1)} + up_n \end{aligned}$$

Remark 6.1. If n is odd, we get

$$\begin{aligned} P_1 &= p_1 + up_2 \\ P_2 &= p_3 + up_4 \\ &\vdots \\ P_{(n-1)/2} &= p_{n-2} + up_{n-1} \\ P_{(n+1)/2} &= p_n + u(\text{unknown}) \end{aligned}$$

Hence, the procedure is:

- With Algorithm of Example 3.2 compute $\tilde{\mathbf{E}}_1, \ldots, \tilde{\mathbf{E}}_{r-1} \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^2-1})$ and the first $n/2$ rows of $\mathbf{E}_r$. Denote this map $\mathbf{E}_r^-$
- From Lemma 4.4 we can assume that the first $n/2$ components of $\mathbf{A}_r^{-1}$ depend only on two parameters, i.e. are of the form $z \in \mathbb{F}_{q^2} \mapsto z + \gamma z^q + \delta$ for some $\gamma, \delta \in \mathbb{F}_{q^2}$. Let denote this map $(\mathbf{A}_r^{-1})^-$

With this setting, the first $n/2$ components of the affine map $\mathbf{A}_r^{-1}$, that is $(\mathbf{A}_r^{-1})^-$, can be computed each one independently as we explained in Chapter 4 and collision variables can also be removed independently in each component (over $\mathbb{F}_{q^2}$) of the public key, maybe after a reduction of the number of variables by considering weights – as explained in Section 4.4. The task has been reduced to determine a preimage, $\hat{\mathcal{Q}}$, of $\mathbf{A}_r^-(\mathcal{P}^-)$ under $\mathbf{E}_r^-$ that lies in the image of the map $\mathbf{DME}_{r-1} = \mathbf{A}_{r-1} \circ \ldots \circ \mathbf{E}_1 \circ \mathbf{A}_0$.

Lemma 6.2. *With the notations above, assume* $(\mathbf{E}_r^-)^* = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ *and denote* $(\mathbf{A}_r^-)^{-1}(\mathcal{P}^-) = (P_1', \ldots, P_{n/2}')$. *Let*

$$\hat{\mathcal{Q}} = (\hat{Q}_1, \ldots, \hat{Q}_4) = (\sigma(Q_1), \ldots, \sigma(Q_4)) \subseteq \mathbb{F}_{q^2}[x_1, \ldots, x_n]$$

a set of polynomials – with known support determined by $\tilde{\mathbf{E}}_1, \ldots, \tilde{\mathbf{E}}_{r-1}$ *and the structure of* $\mathbf{A}_0, \ldots, \mathbf{A}_{r-1}$ *– that verifies*

- $\mathbf{E}_r^-(\hat{\mathcal{Q}}) = (\mathbf{A}_r^-)^{-1}(\mathcal{P}^-)$
- $\hat{\mathcal{Q}}$ *is in the image of* $\boldsymbol{DME}_{r-1}$.

Then $\tilde{\mathcal{Q}} = (\tilde{Q}_1, \tilde{Q}_2, \tilde{Q}_3, \tilde{Q}_4)$ *where* $\tilde{Q}_1$ *has one of the coefficients equal to 1 and the others completely determined by* $\tilde{Q}_1\tilde{Q}_2 = P_1', \tilde{Q}_1\tilde{Q}_3 = P_2'$ *also verifies those conditions.*

Proof. Let

$$\hat{Q}_1 = \sum_{\mathbf{t}_1 \in Supp(\hat{Q}_1)} \hat{A}_{\mathbf{t}_1} \mathbf{t}_1(t_1, \ldots, t_s),$$
$$\hat{Q}_2 = \sum_{\mathbf{t}_2 \in Supp(\hat{Q}_2)} \hat{B}_{\mathbf{t}_2} \mathbf{t}_2(t_1, \ldots, t_s),$$
$$\hat{Q}_3 = \sum_{\mathbf{t}_3 \in Supp(\hat{Q}_3)} \hat{C}_{\mathbf{t}_3} \mathbf{t}_3(t_1, \ldots, t_s).$$

The map

$$\mathbf{M}_\lambda : z \in \mathbb{F}_{q^2}^* \to \lambda z \in \mathbb{F}_{q^2}^*, \ \lambda \in \mathbb{F}_{q^2}^*$$

commutes with exponential maps (see Lemma 4.4). Then, we take $\mathbf{t}_1^0 \in Supp(\hat{Q}_1)$, set $\lambda = \hat{A}_{\mathbf{t}_1^0}^{-1}$ and define $\tilde{\mathcal{Q}}$ as

$$\tilde{Q}_1 = \lambda \hat{Q}_1, \ \tilde{Q}_2 = \lambda^{-1} \hat{Q}_2, \ \tilde{Q}_3 = \lambda^{-1} \hat{Q}_3.$$

Hence, $\mathbf{E}_r^-(\tilde{\mathcal{Q}}) = \mathbf{E}_r^-(\hat{\mathcal{Q}})$. Then we have the following commutative diagram

$$\begin{tikzcd}
(\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{A}_{r-1}"] \arrow[d, "\tilde{\mathbf{L}} \circ \mathbf{A}_{r-1}"] & (\mathbb{F}_{q^2}^*)^n \arrow[d, "\mathbf{E}_r^-"] \\
(\mathbb{F}_{q^2}^*)^n \arrow[r, "\mathbf{E}_r^-"] & (\mathbb{F}_{q^2}^*)^n
\end{tikzcd}$$

where $\tilde{\mathbf{L}} = M_{(\lambda, \lambda^{-1}, \lambda^{-1}, 1)}$ which proves that $\tilde{Q}$ satisfy the two conditions of the proposition.

Let

$$\tilde{Q}_1 = \sum_{\mathbf{t}_1 \in Supp(\hat{Q}_1)} \tilde{A}_{\mathbf{t}_1} \mathbf{t}_1(t_1, \ldots, t_s),$$
$$\tilde{Q}_2 = \sum_{\mathbf{t}_2 \in Supp(\hat{Q}_2)} \tilde{B}_{\mathbf{t}_2} \mathbf{t}_2(t_1, \ldots, t_s),$$
$$\tilde{Q}_3 = \sum_{\mathbf{t}_3 \in Supp(\hat{Q}_3)} \tilde{C}_{\mathbf{t}_3} \mathbf{t}_3(t_1, \ldots, t_s).$$

As collision variables have been removed, the equations we get from

$$\mathbf{E}_r^-(\tilde{\mathcal{Q}}) = (P_1', P_2')$$

when we equal those monomials that have the same term $\mathbf{t}_1 \mathbf{t}_2$ are

$$\{\tilde{A}_{\mathbf{t}_1} \tilde{B}_{\mathbf{t}_2} = \Lambda_{\mathbf{t}_1 \mathbf{t}_2}\}_{\mathbf{t}_1 \in Supp(\hat{Q}_1), \mathbf{t}_2 \in Supp(\hat{Q}_2)} \tag{6.1}$$

where $\Lambda_{\mathbf{t}_1\mathbf{t}_2} \in \mathbb{F}_{q^2}$ are known as they are the coefficients of P'_1. Similarly for the second component we have

$$\{\tilde{A}_{\mathbf{t}_1}\tilde{C}_{\mathbf{t}_3} = \Lambda_{\mathbf{t}_1\mathbf{t}_3}\}_{\mathbf{t}_1 \in Supp(\hat{Q}_1), \mathbf{t}_3 \in Supp(\hat{Q}_3)} \tag{6.2}$$

where $\Lambda_{\mathbf{t}_1\mathbf{t}_3} \in \mathbb{F}_{q^2}$ are known as they are the coefficients of P'_2. Since by construction $\tilde{A}_{\mathbf{t}_1^0} = 1$, we can compute $\tilde{Q}_2, \tilde{Q}_3$ from equations 6.1,6.2 and finally the remaining coefficients of $\tilde{Q}_1$.

□

To be able to recover an equivalent public key it is not enough to have $\hat{\mathcal{Q}}$ but $\mathcal{Q}$, where $\hat{\mathcal{Q}} = \sigma(\mathcal{Q})$. To compute $\mathcal{Q}$ recall that for each $(a_1, \ldots, a_8)$ we have

$$\sum_{\mathbf{s}_1 | \sigma(\mathbf{s}_1) = \mathbf{t}_1} A_{\mathbf{s}_1}(a_1, \ldots, a_8) = \hat{A}_{\mathbf{t}_1}$$

where $Q_1 = \sum_{\mathbf{s}_1 \in Supp(Q_1)} A_{\mathbf{s}_1}\mathbf{s}_1(x_1, \ldots, x_8)$ and analogous equations are for Q_2, Q_3 Since in the previous result we have fixed $\tilde{A}_{\mathbf{t}_1^0} = 1$ we have to assure that, for each $\mathbf{s}_1$ such that $\mathrm{Supp}(\sigma(\mathbf{s}_1)) = \mathbf{t}_1^0$, $A_{\mathbf{s}_1}(a_1, \ldots, a_8)$ have the same value for every choice we made of $(a_1, \ldots, a_8)$.

What we have described is applied when we know some of the components of $\mathcal{P}$ seen over $\mathbb{F}_{q^2}$. In the case that we know some components over $\mathbb{F}_{q^2}$ but for other only one of its two coordinates in $\mathbb{F}_q$ (see e.g. Remark 6.1) we have to combine the results from Chapters 4 and 5.

We finally study a scenario where recover $\mathcal{Q}$ from several $\hat{\mathcal{Q}}$ is not as easy.

The setting is the following:

Let $\mathbf{E}_1 = \mathbf{E}_2 = \mathbf{E}_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ and take $\mathbf{A}_0, \ldots, \mathbf{A}_3$ with $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_3$ linear maps and $\mathbf{A}_2$ that is a linear map with two affine shifts, in the first and fourth – seen over $\mathbb{F}_{q^2}$– components. We define

$$\pi : (\mathbb{F}_q[x_1, \ldots, x_8])^8 \ldots (\mathbb{F}_q[x_1, \ldots, x_8])^2, \; \pi(p_1, \ldots, p_8) = (p_1, p_7).$$

Let $\mathcal{P} = (p_1, \ldots, p_8)$ the public key of $\mathbf{DME}_3$ and let $\mathcal{P}^- = \pi(\mathcal{P}) = (p_1, p_7)$. We describe here the steps to be followed according previous chapters:

- We can assume that $\mathbf{A}_3$ is the identity as the first and fourth – seen over $\mathbb{F}_{q^2}$– components of $\mathcal{P}$ has a minus structure while the second and third components are completely unknown.
- Denote $\mathbf{E}_r^- = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, compute

  $$\mathcal{Q} \subseteq (\mathbb{F}_{q^2}[x_1, \ldots, x_8])^4$$

  such that:

- Firstly, $\mathbf{E}_r^-(\mathcal{Q}) = (H_1, H_2) \subseteq (\mathbb{F}_{q^2}[x_1, \ldots, x_8])^2$ and $[H_1]_1 = p_1, [H_2]_1 = p_7$ where $[.]_1$ means the first coordinate of an element of $\mathbb{F}_{q^2}$ written in a $\mathbb{F}_q$-basis $\{1, u\}$.
- Secondly, $\mathcal{Q}$ is in the image of $\mathbf{DME}_2$ with the entries of the matrices $\mathbf{E}_1, \mathbf{E}_2$ and the structure of the affine maps being known.

If we revise how we found such a preimage $\mathcal{Q}$ in the case of DME minus, we saw that in the case of two non zero entries per row, we first removed collisions and then we had to use several of the rows of the $\mathbf{E}_r$ (here $r = 3$) to get only a finite number of candidates $\mathcal{Q}$.

When we try to imitate it in our setting, we can consider two different approaches:

- Assume we do not take weights to reduce the number of variables. Hence we get that $\mathcal{Q}$ has $\#Supp(Q_1) = \#Supp(Q_4) = 13$ and $\#Supp(Q_2) = \#Supp(Q_3) = 12$. Moreover the number of collision variables in p_1 is 80 and in p_4 is also 80 and these collision variables come all from the linear part. An upper bound of computing a LEX Gröbner basis using results in Chapter 2 is:
$$O\left(\binom{12}{3}\binom{12}{3}\binom{80 + \mathrm{d_{reg}}(\mathcal{I}_3)}{80}^{\omega} + 80 \cdot \mathrm{DEG}(\mathcal{I}_3)^3\right)$$
and
$$\binom{12}{3}^2 \binom{80+5}{80}^{\omega} + 80 \cdot (108900)^3 \sim 2^{90}$$

- The second approach is to reduce variables using weights. For example if we take
$$x_1 = t_1 a_1, x_2 = t_2 a_2, x_3 = t_3 a_3, x_4 = t_3 a_4,$$
$$x_5 = t_4 a_5, x_6 = t_5 a_6, x_7 = t_6 a_7, x_8 = t_7 a_8$$
then for $\#Supp(Q_1) = \#Supp(Q_4) = 7, \#Supp(Q_2) = \#Supp(Q_3) = 4$ and the number of collision in p_1 is 8. As $8 < (7-2)(4-2)$ collisions variables can be removed. Now we see an analogous of Lemma 6.2.

Lemma 6.3. *With the notations above, assume* $(\mathbf{E}_3^-)^* = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$. *Let*
$$\hat{\mathcal{Q}} = (\hat{Q}_1, \ldots, \hat{Q}_4) = (\sigma(Q_1), \ldots, \sigma(Q_4)) \subseteq \mathbb{F}_{q^2}[t_1, \ldots, t_7]$$
a set of polynomials – with known support determined by $\tilde{\mathbf{E}}_1, \ldots, \tilde{\mathbf{E}}_{r-1}$*, the structure of* $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$ *and* σ *– that verifies the two conditions above. Then* $\tilde{\mathcal{Q}} = (\tilde{Q}_1, \tilde{Q}_2, \tilde{Q}_3, \tilde{Q}_4)$ *where*
$$\tilde{Q}_i = \sum_{\mathbf{t}_i \in Supp(\hat{Q}_i)} (\tilde{a}_{\mathbf{t}_i} + u\tilde{b}_{\mathbf{t}_i})\mathbf{t}_i(t_1, \ldots, t_7), \ i = 1, \ldots, 4$$
and $\tilde{a}_{\mathbf{t}_1^0} = 1, \tilde{b}_{\mathbf{t}_1^0} = 0, \tilde{b}_{\mathbf{t}_2^0} = 1, \tilde{b}_{\mathbf{t}_2^1} = 0, \tilde{a}_{\mathbf{t}_3^0} = 1, \tilde{b}_{\mathbf{t}_3^0} = 0, \tilde{b}_{\mathbf{t}_4^0} = 1, \tilde{b}_{\mathbf{t}_4^1} = 0$ *also verifies those conditions.*

Proof. From Section 5.3.2.1 we know that the system

$$\{[(\hat{a}_{\mathbf{t}_1} + u\hat{b}_{\mathbf{t}_1})(\hat{a}_{\mathbf{t}_2} + u\hat{b}_{\mathbf{t}_2})]_1 = \alpha_{\mathbf{t}_1\mathbf{t}_2}\}_{\mathbf{t}_1 \in \mathrm{Supp}(\hat{Q}_1), \mathbf{t}_2 \in \mathrm{Supp}(\hat{Q}_2)}$$

still has a solution if we take $\hat{a}_{\mathbf{t}_1^0} = 1, \hat{b}_{\mathbf{t}_1^0} = 0, \hat{b}_{\mathbf{t}_2^0} = 1, \hat{b}_{\mathbf{t}_2^1} = 0$. Then if we define $\lambda = (\hat{a}_{\mathbf{t}_1^0} + u\hat{b}_{\mathbf{t}_1^0})^{-1}$ and a linear map $\mathbf{L} = \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix}$ such that

$$\mathbf{L}\begin{pmatrix} [\lambda^{-1}(\hat{a}_{\mathbf{t}_2^0} + u\hat{b}_{\mathbf{t}_2^0})]_1 & [\lambda^{-1}(\hat{a}_{\mathbf{t}_2^1} + u\hat{b}_{\mathbf{t}_2^1})]_1 \\ [\lambda^{-1}(\hat{a}_{\mathbf{t}_2^0} + u\hat{b}_{\mathbf{t}_2^0})]_u & [\lambda^{-1}(\hat{a}_{\mathbf{t}_2^1} + u\hat{b}_{\mathbf{t}_2^1})]_u \end{pmatrix} = \begin{pmatrix} * & * \\ 1 & 0 \end{pmatrix}$$

then $\tilde{Q}_1 = \lambda\hat{Q}_1, \tilde{Q}_2 = \mathbf{L}([\lambda^{-1}\hat{Q}_2]_1, [\lambda^{-1}\hat{Q}_2]_u)$ satisfy the conditions. As $\hat{Q}_3, \hat{Q}_4$ have disjoint supports with $\hat{Q}_1, \hat{Q}_2$, we can get analogous results for $\hat{Q}_3, \hat{Q}_4$.

□

Since we have been working with weights we need to be able to recover the $\mathcal{Q}$. But in this example we have fixed several of the weight variables, so it is not clear that we can get many $(a_1, \ldots, a_8)$ that preserve the definition of the variables we fixed, i.e. $\tilde{a}_{\mathbf{t}_1^0} = 1, \tilde{b}_{\mathbf{t}_1^0} = 0, \tilde{b}_{\mathbf{t}_2^0} = 1, \tilde{b}_{\mathbf{t}_2^1} = 0, \tilde{a}_{\mathbf{t}_3^0} = 1, \tilde{b}_{\mathbf{t}_3^0} = 0, \tilde{b}_{\mathbf{t}_4^0} = 1, \tilde{b}_{\mathbf{t}_4^1} = 0$. We explain here an approach that we think may allow to recover original collision variables from the values of collision variables when considering weights. Let denote H_ℓ collision variables that appear in the system of equations corresponding to p_1 and Ht_m collision variables in the system of equations corresponding to $\sigma_{\mathbf{a}}(p_1)$. Then if $p_1 = \sum_{\mathbf{t} \in \mathrm{Supp}(p_1)} c_{\mathbf{t}}\mathbf{t}$, we have $\hat{p}_1 = \sigma_{\mathbf{a}}(p_1) = \sum_{\mathbf{t} \in \mathrm{Supp}(\hat{p}_1)} \hat{c}_{\mathbf{t}}\mathbf{t}(t_1, \ldots, t_s)$ where

$$\hat{c}_{\mathbf{t}} = \sum_{\mathbf{t}' \in \mathrm{Supp}(p_1) | \mathbf{t}'(t_1, \ldots, t_s) = \mathbf{t}} c_{\mathbf{t}'}\mathbf{t}'(a_1, \ldots, a_8)$$

for every $\mathbf{t} \in \mathrm{Supp}(\hat{p}_1)$. Note that collision variables H_ℓ came from splitting the $c_{\mathbf{t}'}, \mathbf{t}' \in \mathrm{Supp}(p_1)$ and collision variables Ht_m came from splitting the $c_{\mathbf{t}}, \mathbf{t} \in \mathrm{Supp}(\hat{p}_1)$. Since we had computed Ht_m we get linear equations that allow to compute H_ℓ. To get sufficiently many equations note that $\mathbf{a} \in \mathbb{F}_q^8$ can be changed and also the value of s that defines the number of weighted variables.

6.2 DME^{+}

Let $\mathbf{E}_1, \ldots, \mathbf{E}_r \in \mathcal{M}_{n\times n}$, $\mathbf{L}_0, \ldots, \mathbf{L}_{r-1} \in \mathcal{M}_{N\times N}(\mathbb{F}_q)$ as in Definition 3.19. Then, each $\mathbf{L}_i$ is of the form

$$\mathbf{L}_i = \left(\begin{array}{c|c|c|c} \mathbf{L}_{i1} & 0 & 0 & 0 \\ \hline 0 & \mathbf{L}_{i2} & 0 & 0 \\ \hline 0 & 0 & \mathbf{L}_{i3} & 0 \\ \hline 0 & 0 & 0 & \mathbf{L}_{i4} \end{array}\right)$$

and let $\mathbf{L}_r \in \mathcal{M}(\mathbb{F}_q)_{(N+s)\times(N+s)}$. Note that with Algorithm of Example 3.2 we can compute $\tilde{\mathbf{E}}_1 \ldots, \tilde{\mathbf{E}}_r$. Then we have to compute the linear maps.

Proposition 6.4. *Assume $\mathbf{L}_{ri}$ is an invertible matrix over $\mathbb{F}_q$ of sizer $s_i \times s_i$ and that is i-th block of the linear map $\mathbf{L}_r$ of a* ***DME***$^{+}$*. We can write it as a block matrix*

$$\mathbf{L}_{ri} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{C} & \mathbf{D} \end{array}\right)$$

where $\mathbf{A}$ is a 2×2 matrix, $\mathbf{B}$ is a $2 \times s_i$ matrix, $\mathbf{C}$ is a $s_i \times 2$ matrix and $\mathbf{D}$ has size $s_i \times s_i$. With the notations of Definition 3.19, denote $P_i = p_1 + up_2$. Let $\mathbf{v} = (p_1, p_2)$ and $\mathbf{w} = (q_1, \ldots, q_{s_i})$ the components of Q_i. Then

- *If $s_i = 2$, define $\tilde{\mathbf{w}} = \mathbf{A}\mathbf{v} + \mathbf{B}\mathbf{w}$ and*

  $$\tilde{\mathbf{L}}_{ri} = \left(\begin{array}{c|c} \mathbf{0}_{2\times 2} & \mathbf{I}_2 \\ \hline \mathbf{C} - \mathbf{D}\mathbf{B}^{-1}\mathbf{A} & \mathbf{D}\mathbf{B}^{-1} \end{array}\right)$$

  verifies

  $$\mathbf{L}_{ri}\left(\begin{array}{c} \mathbf{v} \\ \hline \mathbf{w} \end{array}\right) = \tilde{\mathbf{L}}_{ri}\left(\begin{array}{c} \mathbf{v} \\ \hline \tilde{\mathbf{w}} \end{array}\right)$$

- *If $s_i \geq 3$ and assuming Rank$(B) = 2$, let $\mathbf{B}^{+}$ a right inverse of $\mathbf{B}$, i.e. $\mathbf{B}\mathbf{B}^{+} = \mathbf{I}_2$. Define $\tilde{\mathbf{w}} = \mathbf{B}^{+}\mathbf{A}\mathbf{v} + \mathbf{w}$ and*

  $$\tilde{\mathbf{L}}_{ri} = \left(\begin{array}{c|c} \mathbf{0}_{2\times 2} & \mathbf{B} \\ \hline \mathbf{C} - \mathbf{D}\mathbf{B}^{+}\mathbf{A} & \mathbf{D} \end{array}\right)$$

  verifies

  $$\mathbf{L}_{ri}\left(\begin{array}{c} \mathbf{v} \\ \hline \mathbf{w} \end{array}\right) = \tilde{\mathbf{L}}_{r}\left(\begin{array}{c} \mathbf{v} \\ \hline \tilde{\mathbf{w}} \end{array}\right)$$

Proof. It is a simple computation. □

This proposition allows us to simplify $\mathbf{L}_{ri}$, not $\mathbf{L}_{ri}^{-1}$.

6.3 DME over $\mathbb{F}_q$

This is the analogue of Lemma 5.1 in the setting over $\mathbb{F}_q$.

Proposition 6.5. *In a DME over $\mathbb{F}_q$ (see Definition 3.20) let*

$$\mathbf{L}_r = \left(\begin{array}{c|c|c|c} \mathbf{L}_{r1} & 0 & 0 & 0 \\ \hline 0 & \mathbf{L}_{r2} & 0 & 0 \\ \hline 0 & 0 & \ddots & 0 \\ \hline 0 & 0 & 0 & \mathbf{L}_{iN} \end{array}\right)$$

be the last linear map with

$$\mathbf{L}_{ri} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

Assuming that $a_i, b_i \neq 0,\ i = 1, \dots, n$, there exists

- $\tilde{\mathbf{L}}_r$ *with the same block structure as* $\mathbf{L}_r$ *with* $\tilde{\mathbf{L}}_{ri} = \begin{pmatrix} 1 & 1 \\ a_i^{-1}c_i & b_i^{-1}d_i \end{pmatrix}$, $i = 1, \dots, N$,
- *A map*

  $$\mathbf{M}_{\mathbf{D}} : \mathbb{F}_q^N \to \mathbb{F}_q^N,\ \mathbf{x} \mapsto \mathbf{D}\mathbf{x}$$

  where $\mathbf{D}$ *is the $N \times N$ diagonal matrix with diagonal* $(a_1, b_1, \dots, a_N, b_N)^{\mathbf{E}^{-1}}$

such that

$$\begin{tikzcd} (\mathbb{F}_q^*)^n \arrow[r, "\mathbf{L}_{r-1}"] \arrow[d, "\mathbf{M}_{\mathbf{D}} \circ \mathbf{L}_{r-1}"] & (\mathbb{F}_q^*)^n \arrow[d, "\mathbf{L}_r \circ \mathbf{E}_r"] \\ (\mathbb{F}_q^*)^n \arrow[r, "\tilde{\mathbf{L}}_r \circ \mathbf{E}"] & (\mathbb{F}_q^*)^n \end{tikzcd}$$

is commutative.

In the DME minus version the $\tilde{\mathbf{L}}_{ri}$ *can be taken* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proof. It is very similar to proof of Lemma 4.4. Note that $\mathbf{L}_r \circ \mathbf{M}_{\tilde{D}} = \tilde{\mathbf{L}}_r$ where $\tilde{D}$ is the diagonal matrix with diagonal $(a_1, b_1, \dots, a_N, b_N)$. Now $\tilde{\mathbf{D}} \circ \mathbf{E}_r = \mathbf{E}_r \circ \mathbf{D}$. In the minus case the c_i, d_i can be chosen arbitrarily – keeping the matrix invertible – as the second component is not public. □

This is the kind of results we have for the generalization, assuming $\mathbf{E}_r$ is invertible.

Remark 6.6. Assume the first four components of the **DME** over $\mathbb{F}_q$ generalized have the same support. Then the first block of $\mathbf{L}_r$ can be taken 4×4. Analogously to previous proposition we can prove that there exists $\tilde{\mathbf{L}}_r$ with its first block 4×4 of the form $\begin{pmatrix} 1 & 1 & a & b \\ * & * & * & * \\ c & d & 1 & 1 \\ * & * & * & * \end{pmatrix}$ where a, b, c, d, e, f, g, h can be computed and if we want a complete public key the values of the asterisks must be chosen to make the matrix invertible.

Proof. Use first lemma to simplify the two by two block of the up left side and the two by two block of the down right side. □

6.4 DME$_\mathbf{w}$

We give some partial results about how to use the studied techniques in this version, in which linear maps can be taken completely full without a block structure. A collateral consequence is that these exponential matrices have not in general full rank. This leads to a careful definition of the signature scheme to get consistency. To sign a message $\mathbf{m}$, we first compute a hash $\mathbf{d} = H(\mathbf{m})$. In order to be able to compute a preimage of $\mathbf{d}$ under $\mathbf{E}_r \circ \mathbf{L}_r$, the vector $\mathbf{d}$ must be in the image of $\mathbf{E}_r \circ \mathbf{L}_r$. For this, by Proposition 1.56 it is necessary that $\mathbf{d}$ lies in the algebraic set where the image $\mathbf{E}_r \circ \mathbf{L}_r$ is contained. But it is not sufficient. We have not come up with an efficient method to do it.

6.4.1 Analysis

In a previous section we already considered the scenario where the exponential matrices are over $\mathbb{F}_q$. Due to how they were constructed this version behave much as the version over $\mathbb{F}_{q^2}$. The modification we consider here is to generalize the matrix $\mathbf{E} \otimes \mathbf{I}_2$ to $\mathbf{E}^{\text{ass}}$.

We do not have results that show that an equivalent private key can be recovered efficiently. However we got some experimental results for a specific example. As always we start by writing the system of equations derived from

$$\mathbf{E}^{\text{ass}}(\mathcal{Q}) = \mathbf{L}_3^{-1}(\mathcal{P}) \tag{6.3}$$

by equal coefficients that share the same term $\mathbf{t}(x_1, \ldots, x_8)$. For our example, we work over $\mathbb{F}_q$ with $q = 2^8$ and the matrices are

$$E_1 = \begin{bmatrix} 16384 & 0 & 16 & 0 & 0 & 0 & 0 & 0 \\ 0 & 16384 & 0 & 16 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 32 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 32 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 & 32768 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & 32768 \\ 0 & 0 & 0 & 0 & 2 & 0 & 8192 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 8192 \end{bmatrix},$$

$$E_2 = \begin{bmatrix} 512 & 0 & 0 & 32 & 0 & 0 & 0 & 0 \\ 0 & 512 & 32 & 0 & 0 & 0 & 0 & 0 \\ 512 & 0 & 32 & 0 & 0 & 0 & 0 & 0 \\ 0 & 512 & 0 & 32 & 0 & 0 & 0 & 0 \\ 2048 & 0 & 0 & 0 & 0 & 4096 & 0 & 0 \\ 0 & 2048 & 0 & 0 & 4096 & 0 & 0 & 0 \\ 2048 & 0 & 0 & 0 & 4096 & 0 & 0 & 0 \\ 0 & 2048 & 0 & 0 & 0 & 4096 & 0 & 0 \end{bmatrix},$$

$$E_3 = \begin{bmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 8 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 8 & 2 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 8 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & 2 \end{bmatrix}$$

To get $\tilde{\mathbf{L}}_3^{-1}$ that has a simplified form we want to compute $\mathbf{C}$ a matrix with the same structure as $\mathbf{L}_2$ such that $\mathbf{L}_3 \circ \mathbf{E}_3 = \tilde{\mathbf{L}}_3 \circ \mathbf{E}_3 \circ \mathbf{C}$. Experimentally, we got that the if $\tilde{\mathbf{L}}_3^{-1}$ can be taken with all the entries of the last column identically zero.

Lemma 6.7. *If $\mathbf{E}_3$ has the structure of this example, $\mathcal{Q}' = \mathbf{M}_{(1,1,\beta,1,1,1,1,1)}\mathcal{Q}$, where β is such that $\beta^8 = \lambda a_{77}^{-1}$, satisfies $\mathbf{E}_3(\mathcal{Q}') = \mathbf{L}_3'^{-1}(\mathcal{P})$ with $\mathbf{L}_3'^{-1}$ such that its element $7,7$ is $\lambda \in \mathbb{F}_q$ (assuming the element $7,7$ of $\mathbf{L}_3^{-1}$ is non zero).*

Proof. Note that the variables C_i, F_j only appear in the system of equations corresponding to the third and the seventh row of $\mathbf{E}_3$. The third and seventh component of 6.3 are

$$\sum C_i^8 F_j^2 \mathbf{t}(x_1, \ldots, x_8) = \sum_{k=1}^{8} a_{3,k} p_k(x_1, \ldots, x_8)$$
$$\sum C_i^8 F_j^2 \mathbf{t}(x_1, \ldots, x_8) = \sum_{k=1}^{8} a_{7,k} p_k(x_1, \ldots, x_8)$$

where $\mathcal{P} = (p_1, \ldots, p_8)$ is the public key and $\mathbf{L}_3^{-1} = (a_{ij})_{1 \leq i,j \leq 8}$ Then, if $a_{77} \neq 0$, multiplying by $\lambda \cdot a_{77}^{-1}$ we have

$$\sum \frac{\lambda C_i^8}{a_{77}} F_j^2 \mathbf{t}(x_1, \ldots, x_8) = \sum_{k=1}^{8} \frac{\lambda a_{3,k}}{a_{77}} p_k(x_1, \ldots, x_8)$$
$$\sum \frac{\lambda C_i^8}{a_{77}} F_j^2 \mathbf{t}(x_1, \ldots, x_8) = \sum_{k=1}^{8} \frac{\lambda a_{7,k}}{a_{77}} p_k(x_1, \ldots, x_8)$$

□

Lemma 6.8. *Assume we have*

$$\mathcal{Q} = \begin{pmatrix} \sum_{i=1}^{\#Supp(q_1)} A_i \mathbf{t}_i \\ \sum_{i=1}^{\#Supp(q_2)} B_i \mathbf{t}_i \\ \vdots \\ \sum_{i=1}^{\#Supp(q_8)} H_i \mathbf{t}_i \end{pmatrix}$$

such that

$$\mathbf{L}_3 \circ \mathbf{E}_3(\mathcal{Q}) = (\mathcal{P}).$$

Then, assuming that $A_1, B_1, \ldots, H_1 \neq 0$, $\mathcal{Q}' = \mathbf{M}_{(A_1^{-1}, B_1^{-1}, \ldots, G_1^{-1}, H_1^{-1})}(\mathcal{Q})$ satisfies that $\mathbf{L}_3' \circ \mathbf{E}_3(\mathcal{Q}') = \mathcal{P}$ where $\mathbf{L}_3' = \mathbf{L}_3 \circ \mathbf{M}_{\mathbf{E}_3(A_1, B_1, \ldots, H_1)}$.

Corollary 6.9. *Under the hypothesis of the previous lemmas. When we solve the system of equations derived from* (6.3) *we can assume that*

- *the last column of $\mathbf{E}_3^{-1}$ is zero.*
- *the element $7, 7$ of $\mathbf{L}_3^{-1}$ can be fix to a random value.*
- *$A_1 = 1, \ldots, H_1 = 1$.*

Proof. We take $\mathbf{L}_3^{-1}$ to have its last column zero by changing the original $\mathbf{L}_2$ by $\mathbf{C} \circ \mathbf{L}_2$. Then to get that element $7, 7$ of $\mathbf{L}_3^{-1}$ is $\lambda = G_1^{-1}$ we change $\mathbf{C} \circ \mathbf{L}_2$ by $\mathbf{M}_{(1,1,\beta,1,1,1,1,1)} \circ \mathbf{C} \circ \mathbf{L}_2$ with β defined in Lemma 6.7. Finally, by Lemma 6.8, changing $\mathbf{M}_{(1,1,\beta,1,1,1,1,1)} \circ \mathbf{C} \circ \mathbf{L}_2$ by $\mathbf{M}_{(A_1^{-1}, \ldots, H_1^{-1})} \circ \mathbf{M}_{(1,1,\beta,1,1,1,1,1)} \circ \mathbf{C} \circ \mathbf{L}_2$; and changing $\mathbf{L}_3^{-1}$ by $\mathbf{M}_{\mathbf{E}_3(A_1^{-1}, B_1^{-1}, \ldots, H_1^{-1})} \circ \mathbf{L}_3^{-1}$ we get the desired properties.

□

The linear map is not completely determined, to know the equations for the variables we have to choose we can make an example for which we know the private and the public key and compare the structure of the solutions.

To recover the $\mathbf{L}_2$ we repeat the process.

Chapter 7

Conclusions and future work

The Magma code used for the experimental work in this thesis is available at:

`https://github.com/pilarcoscojuela/Thesis.git`

Magma does not allow exponents larger than 2^{30}. To avoid exponent overflow, our experiments are reported for fields $\mathbb{F}_q$ with $q = 2^k$ with k up to 8 and, in some cases, up to $k = 14$. For larger finite fields Magma does not make the computations and therefore we cannot print the system of polynomial equations. Nevertheless, in those cases polynomials may be represented as lists (as in [2]) and the collision variables can be renamed so that they do not have exponents. The only case where large exponents can occur is in the modeling of Section 5.3.2 when $k = 2$. In such a case we think that an ad-hoc modeling is necessary.

In this thesis we have proposed a structural attack that aims to recover an equivalent private key from a given public key for the DME schemes of Definition 3.9 and Definition 3.18. The attack combines ideas from the two previously known attacks against versions of DME. For the DME 2023 version (see [2]), from the equation

$$\mathbf{E}_r(\mathcal{Q}) = \mathbf{A}_r^{-1}(\mathcal{P})$$

we derive n systems of equations (one for each component of the public key) over the field $\mathbb{F}_{q^2}$. The variables are the coefficients of the polynomials $\mathcal{Q} = (Q_1, \ldots, Q_n)$ together with the parameters defining $\mathbf{A}_r^{-1}$. To estimate the complexity of solving such a system, in which there may be reductions caused by algebraic relations between the entries of the exponential maps, we introduce a new set of variables — the *collision variables* — that allow us to express syzygies between the collision variables and the parameters of the linear/affine maps. These syzygies generalize those described in [4] to the case where reductions occur.

This attack can be adapted to the DME-minus version. In that case, although the linear part of the last affine map can be assumed to be the identity, the public key $\mathcal{P}^-$ contains only one of the two

$\mathbb{F}_q$-coordinates of each polynomial over $\mathbb{F}_{q^2}$ that defines $\mathcal{P}$. We consider the analogous equation

$$\pi \circ \mathbf{E}_r(\mathcal{Q}) = \mathcal{P}^- + \begin{pmatrix} d_1 \\ d_3 \\ d_5 \\ \vdots \\ d_{N-1} \end{pmatrix}.$$

In the DME-minus setting we again introduce collision variables as additional unknowns. However, the resulting syzygies correspond to minors of order 3 of a matrix rather than minors of order 2. Moreover, to compute the values of the collision variables in the minus setting one typically needs to consider simultaneously the systems corresponding to more than one component, since those systems are over $\mathbb{F}_q$.

Assuming the number of collision-variable solutions is finite, the complexity of computing their values is upper-bounded by the complexity of computing a Gröbner basis of the ideals generated by the minors of order 2 or 3 of a matrix. Under genericity assumptions, upper bounds for this complexity are given in [1]. Additionally, if the hypothesis of Proposition 2.34 holds, a LEX Gröbner basis can be computed in polynomial time.

7.1 Future work

The final chapter discusses additional DME variants that remain under study. For the DME$^+$ variant, which is an encryption scheme, we do not believe our current modeling is sufficient to break it.

Nevertheless, it worth noticing that if we consider a system of equations derived from a component from

$$\mathbf{L} \circ \mathbf{E}(\mathcal{Q}) = \mathcal{P}$$

then:

- We cannot use the matrix over the big field of Chapter 4 because the linear map make that the minors of order two of this matrix does not vanish.

- We can consider matrices as in Chapter 5, but now the entries are

$$\begin{pmatrix} A_i^a & B_i^a \\ A_j^a & B_j^a \end{pmatrix} (a \cdot \mathbf{W}_1 + b\mathbf{W}_u) \begin{pmatrix} C_r^b & C_s^b \\ D_r^b & D_s^b \end{pmatrix}$$

  being $\mathbf{W}_u$ the matrix that correspond to the u-part. There exist similar syzygies to which we obtain in Chapter 5.

Future work includes the following directions:

- A rigorous analysis of the complexity of the method proposed in Section 5.3.2 for recovering the coefficients of the missing polynomials in the DME-minus case.
- A deeper study of the genericity assumptions that underlie many of our complexity estimates. While our experiments support these assumptions for the examples we tested, their validity in general remains unproven and deserves further investigation.
- Exploring alternative modeling strategies to handle in general the cases in which $\mathbf{E}_r$ has two non zero entries per row. We only presented an ad hoc modeling for a specific example in 5.3.1.
- Studying the implications of these structural attacks to the versions DME$^+$, DME over $\mathbb{F}_q$ and DME$_\mathrm{w}$.

Addressing these points will help clarify the scope and limits of the structural attacks introduced here, and will contribute to a better understanding of the security of DME-family schemes.

Bibliography

[1] Pierre-Jean Spaenlehauer. *Solving multi-homogeneous and determinantal systems: algorithms, complexity, applications.* PhD thesis, Université Pierre et Marie Curie (Univ. Paris 6), 2012.

[2] Pierre Briaud, Maxime Bros, Ray Perlner, and Daniel Smith-Tone. Practical attack on all parameters of the dme signature scheme. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–29. Springer, 2024.

[3] Ignacio Luengo, Martín Avendaño, and Pilar Coscojuela. Dme: a full encryption, signature and kem multivariate public key cryptosystem. In *International Conference on Post-Quantum Cryptography*, pages 379–402. Springer, 2023.

[4] Martin Avendaño and Miguel Marco. A structural attack to the dme-(3, 2, q) cryptosystem. *Finite Fields and Their Applications*, 71:101810, 2021.

[5] Jintai Ding, Jason E Gower, and Dieter S Schmidt. *Multivariate public key cryptosystems.* Springer, 2006.

[6] Michael R Garey, David S Johnson, et al. A guide to the theory of np-completeness. *Computers and intractability*, pages 37–79, 1990.

[7] Dan Boneh and Victor Shoup. A graduate course in applied cryptography. *Version 0.6*, 2023.

[8] Saqib A Kakvi. On the security of rsa-pss in the wild. In *Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop*, pages 23–34, 2019.

[9] Gregor Kemper. *Hilbert Series and Dimension*, pages 151–164. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011. ISBN 978-3-642-03545-6. doi: 10.1007/978-3-642-03545-6_12. URL https://doi.org/10.1007/978-3-642-03545-6_12.

[10] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics.* Springer-Verlag, New York,, 2015.

[11] V Weispfenning and T Becker. Groebner bases: a computational approach to commutative algebra, vol. 141 of. *Graduate Texts in Mathematics: readings in mathematics*, 1993.

[12] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra*, volume 1. Springer, 2008.

[13] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the f5 gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015.

[14] Daniel Lazard. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In *European Conference on Computer Algebra*, pages 146–156. Springer, 1983.

[15] 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 Wolfram Koepf, editor, *Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings*, pages 257–264. ACM, 2010. doi: 10.1145/1837934.1837984. URL https://doi.org/10.1145/1837934.1837984.

[16] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. On the complexity of the generalized minrank problem. *J. Symb. Comput.*, 55:30–58, 2013. doi: 10.1016/J.JSC.2013.03.004. URL https://doi.org/10.1016/j.jsc.2013.03.004.

[17] Sriram Gopalakrishnan, Vincent Neiger, and Mohab Safey El Din. Optimized gröbner basis algorithms for maximal determinantal ideals and critical point computations. In Jonathan D. Hauenstein, Wen-shin Lee, and Shaoshi Chen, editors, *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation, ISSAC 2024, Raleigh, NC, USA, July 16-19, 2024*, pages 400–409. ACM, 2024. doi: 10.1145/3666000.3669713. URL https://doi.org/10.1145/3666000.3669713.

[18] Sriram Gopalakrishnan. On the arithmetic complexity of computing gröbner bases of comaximal determinantal ideals. *CoRR*, abs/2403.02160, 2024. doi: 10.48550/ARXIV.2403.02160. URL https://doi.org/10.48550/arXiv.2403.02160.

[19] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[20] Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. Cryptanalysis of minrank. In David A. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008. doi: 10.1007/978-3-540-85174-5_16. URL https://doi.org/10.1007/978-3-540-85174-5_16.

[21] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Algebraic attacks for solving the rank decoding and minrank problems without gröbner basis. *arXiv preprint arXiv:2002.08322*, 2020.

[22] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier A. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 507–536. Springer, 2020. doi: 10.1007/978-3-030-64837-4_17. URL https://doi.org/10.1007/978-3-030-64837-4_17.

[23] Magali Bardet and Manon Bertin. Improvement of algebraic attacks for solving superdetermined minrank instances. In *International Conference on Post-Quantum Cryptography*, pages 107–123. Springer, 2022.

[24] Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret, Simona Samardjiska, and Enrico Thomae. A polynomial-time key-recovery attack on MQQ cryptosystems. In Jonathan Katz, editor, *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings*, volume 9020 of *Lecture Notes in Computer Science*, pages 150–174. Springer, 2015. doi: 10.1007/978-3-662-46447-2_7. URL https://doi.org/10.1007/978-3-662-46447-2_7.

[25] Didier Henrion, Simone Naldi, and Mohab Safey El Din. Real root finding for determinants of linear matrices. *J. Symb. Comput.*, 74:205–238, 2016. doi: 10.1016/J.JSC.2015.06.010. URL https://doi.org/10.1016/j.jsc.2015.06.010.

[26] Jonathan F Buss, Gudmund S Frandsen, and Jeffrey O Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572–596, 1999.

[27] Javier Verbel, John Baena, Daniel Cabarcas, Ray Perlner, and Daniel Smith-Tone. On the complexity of "superdetermined" minrank instances. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, pages 167–186, Cham, 2019. Springer International Publishing. ISBN 978-3-030-25510-7.

[28] Pilar Coscojuela, Krishna Mahavadi, Ludovic Perret, Alex Ryba, and Simona Samardjiska. On the complexity of the relative eigenvector problem. In *Proceedings of the 50th International Symposium on Symbolic and Algebraic Computation (ISSAC 2025)*, 2025.

[29] Jean-Charles Faugère and Ludovic Perret. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *Journal of Symbolic Computation*, 44(12): 1676–1689, 2009.

[30] I Luengo, M Avendano, and M Marco. Dme a public key, signature and kem system based on double exponentiation. *NIST proposal*, 2017.

[31] Martín Avendaño. The dme cryptosystem. https://blogs.mat.ucm.es/dme/ [Accessed: 2025-02-14].