Efficiency and security of ZHFE

por

Javier Alfonso Verbel Herrera

Trabajo presentado como requisito parcial para optar por al título de:

Magister en Ciencias Matemáticas

Director
Ph.D Daniel Cabarcas Jaramillo

Universidad Nacional de Colombia
Sede Medellín

Facultad de Ciencias
Escuela de Matemáticas

Medellín, Colombia
2015

Dedicated with all my love
to my parents Angel and Julia.

Acknowledgements

Firstly, I want to acknowledge to God for letting me achieve this goal. Also I am so grateful with my advisor Prof. Daniel Carbarcas Jaramillo for the continuous support of my master study, for his patience, motivation, and immense knowledge.

Additionally, I would like to expressed my gratitude with Jhon Baena, Daniel Carbarcas, Daniel Escudero and Jaibeth Porras for their useful participation in the paper entitled "Efficient ZHFE key generation", from which it is extracted the Chapter 2 of this thesis. I want to say thank to the Facultad de Ciencias of the Universidad Nacional de Colombia sede Medellín for granting us access to the Enlace server, where we execute most of the experiments of this thesis.

Abstract

In this thesis we describe the hidden structure in the key generation process for the multivariate public key cryptosystem ZHFE. Based on such structure, we propose a new method for the mentioned process. We compare the time and memory required between our new method and the original key generation process.

We also analyze the security of ZHFE with respect to the MinRank Attack. We show that with high probability there exist a linear combination of Frobenious power of the core polynomials F and $\tilde{F}$ of low rank. Furthermore, we show that such linear combination can be extracted from the public key.

Resumen

En esta tesis describimos la estructura oculta en el proceso de generación de llave para el criptosistema de llave pública multivariada ZHFE. Basados en tal estructura, proponemos un nuevo método para tal proceso. Comparamos los tiempo y memoria requerida entre nuestro nuevo método y el método original de generación.

También analizamos las seguridad de ZHFE respecto al Ataque del MinRank. Demostramos que con alta probabilidad existe de una combinanción lineal de las potencias de Frobenious de los polinomios centrales F y $\tilde{F}$ de rango pequeño. Más aún, demostramos que tal combinación puede ser extraída de la llave pública.

Contents

Introduction

In the last years, multivariate public key cryptosystems (**MPKCs**, [2]) have been study as alternative to replace current public key cryptosystems, which would be insecure in a world with large quantum computers. In 2014, Porras et al. proposed ZHFE, an **MPKCs** inspired in the HFE cryptosystem [9]. The key difference is that in ZHFE there are two high degree core polynomials F and $\tilde{F}$, whose associated matrices also have high rank. Furthermore, a low degree function Ψ is used as a trapdoor for decryption.

Although ZHFE is a very interesting approach, it still have some issues that we improve in this thesis. On the one hand, the key generation procedure is very slow, because to construct the function Ψ, it is necessary to find the null space of a big matrix over a finite field. On the other hand, it is not known if the existence of two linear combinations of the Frobenius power of F and $\tilde{F}$ such that its matrix associated has low rank is a threat for the ZHFE's security.

In this thesis we describe the structure of the big matrix necessary to build the low degree function Ψ. Based on that structure, we propose a method to find a random element in its whole null space. We also want to show that there exist two linear combinations of the Frobenius power of the core polynomials such that their associated matrices have low rank and at least one of them can be extracted from the public key.

Chapter 1

Preliminaries

Cryptography is a branch of mathematics which, among other things, provides solutions to confidentiality and authenticity in data transmition. In order to avoid that no authorized people get access to transmitted information. *Cryptosystems* are designed to allow to *encrypt* messages before they are sent, then *decrypt* the encrypted messages and recover the original messages. To encrypt and decrypt messages is necessary that authorized people share a secret information (a *private key*) before they communicate with each other. But, in several very important communication media, (like the Internet) sharing a private key in advance is not practical. This was the principal reason for developing *public key cryptosystems*. In a public key cryptosystem, only one user knows both keys, a *public key* used to encrypt and a *private key* only known by the the owner and used to decrypt.

The public key cryptosystems more commonly used in communications today are RSA, whose security is based on the difficulty of factoring integers in classic computers and Diffie-Hellman whose security is based on the difficulty of solving the *Discrete Logarithm Problem* (DLP) [14].

In 1994, Peter Shor introduced a *quantum algorithm* that factors integers modulo n and solve the DLP in polynomial time on the size of the problem [13]. Although there exists no large enough quantum computer to break RSA today, great efforts are being made to construct one [2]. For that reason, alternative secure cryptosystems in a postquatum world must be constructed (*postquantum cryptosystems*).

One of the most interesting postquantum cryptosystems are the so called Multivariate Public Key Cryptosystems (**MPKCs**) [5]). In general terms, a **MPKC** is a public key cryptosystem such that the public key is an order set of multivariate polynomials $(p_1, \ldots, p_m)$ with coefficients in a finite field. The private key is some secret information about the construction of the public key which allows to easily find pre-images of the function $P = (p_1, \ldots, p_m)$. The security of **MPKCs** is based on the fact that the problem of directly solving a random system of multivariates polynomials is an $\mathcal{NP}$-hard problem [6]. Even more, this problem is believed to be hard even in the presence of large quantum computers.

1.1 Hidden field equation cryptosystem

In 1996, Patarin proposed one of the most important **MPKCs** called Hidden Fields Equation (HFE, [9]). To give a formal description of HFE let us introduce first some notation. Let $\mathbb{F}$ be a finite field with q elements, denote by $\mathbb{K}$ a field extension of degree n generated by an irreducible polynomial $g(x) \in \mathbb{F}[x]$. We say that $F \in \mathbb{K}[X]$ is an HFE polynomial if F is a polynomial with the shape

$$F(X) = \sum_{i=0}^{b} \sum_{j=0}^{i} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{n} b_i X^{q^i} + c,$$

where $a_{ij}, b_i, c \in \mathbb{K}$. If φ denotes the natural isomorphism from $\mathbb{K}$ to $\mathbb{F}^n$, i.e, $\varphi(a_0+a_1y+\ldots+a_{n-1}y^{n-1}) = (a_0, \ldots, a_{n-1})$, then $\varphi \circ F \circ \varphi^{-1}(x_1, \ldots x_n)$ is an ordered set of n quadratic polynomials over $\mathbb{F}^n$ [5]. For simplicity, throughout this thesis we write p instead of $p(x_1, \ldots, x_n)$ to make reference to a polynomial in the variables $x_1, \ldots, x_n$. We say that a polynomial $F(X) \in \mathbb{K}[X]$ has q-Hamming-weight-W if the maximum of the q-Hamming weights of all its exponents is W. The q-Hamming weight of a non-negative integer is the sum of the q-digits of its q-ary expansion. Also we donote by $\mathbf{F} \in \mathcal{M}_{n\times n}(\mathbb{K})$ the matrix associated with the q-Hamming-weight-two part of F (for short, matrix associated with F) if

$$F(X) = \underline{X}\mathbf{F}\underline{X}^t + \sum_{i=0}^{n-1} b_i X^{q^i} + c,$$

where $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$. The public key of an HFE cryptosystem is a set of degree two multivariate polynomials $P = (p_1, \ldots, p_n)$ in $(\mathbb{F}[x_1, \ldots, x_n])^n$ given by

$$P = T \circ \varphi \circ F \circ \varphi^{-1} \circ S.$$

Here T and S are invertible affine transformations, F is a uniformly random chosen HFE polynimial of degree less than an integer D and φ is the natural isomorphism from $\mathbb{K}$ to $\mathbb{F}^n$ [5]. The private key is formed by the polynomial F and the two invertible affine transformations S, T.

As in most **MPKCs**, the *ciphertext* of a *plaintext* $\mathbf{x} \in \mathbb{F}^n$ (message to be encrypted) is the element $\mathbf{y} = P(\mathbf{x}) \in \mathbb{F}^n$. To decrypt a chiphertext $\mathbf{y}$ it is necessary to do the following steps

1. To compute $\mathbf{z} = (T \circ \varphi)^{-1}(\mathbf{y})$, then
2. to find $K = \{\mathbf{w} |\ F(\mathbf{w}) = \mathbf{z}\}$, next
3. for each element $\mathbf{w} \in K$ compute $(\varphi^{-1} \circ S)^{-1}(\mathbf{w})$.

Clearly, the process to decrypt a HFE ciphertext may have several outputs, so some redundant information must be placed in the paintext allowing to choose the correct output. One important issue, in the decryption process is the inversion of the HFE polynomial F. One of the most efficient algorithm to invert a univariate polynomial is Berlekamp's Algorithm,

whose complexity $O(nd^3)$ [5] is polynomial in the polynomial degree (D in our case). For this reason, the parameter D must be small enough. But Kipnis and Shamir found out in this fact the principal problem for HFE security.

In 1999, Kipnis and Shamir proposed a key recovery attack [7], i.e., they designed a method to find a private key from the public key. Several years later, Bettale, Faugère and Perret improved this attack [3] making the key recovery attack faster than Kipnis and Shamir. In their paper, they show that the principal weaknesses of HFE are the following facts:

- the low rank of the matrix associated with the nolinear part of the polynomial F, which allows recover the transformation T solving an instance of the MinRank problem (see Definition 1.1.1),
- the low degree and randomness of the core polynomial F. This fact allows recover the transformation S by solving a linear equation system.

Definition 1.1.1. *(MinRank Problem from HFE) Given $n \times n$ matrices $A_1, \ldots, A_n$ over a finite field $\mathbb{F}$ and $r < n$, find a non-trivial linear combination*

$$A = \alpha_1 A_1 + \cdots + \alpha_n A_n$$

such that the rank of A is less than or equal to r.

Bettale, Faugère and Perret showed in [3] that the complexity of MiniRank from a HFE cryptosystem is $O(n^{(r+1)w})$, where r is less than 11 and n is the number of polynomials in the public key ($2 \leq w < 3$ is a linear algebra constant).

1.2 ZHFE cryptosystem

In 2014, Porras, Baena and Ding, made a attempt to correct the weakness of HFE and proposed a cryptosystem called ZHFE [11]. It has two high degree core polynomial F, $\tilde{F}$ and a private low degree function Ψ used for invertion of the polynomials F and $\tilde{F}$. They show that that the matrices associated with the core polynomial have high rank.

Let $\mathbb{F}$, $\mathbb{K}$ and φ be as in the last section, T and S invertible affine transformation from $\mathbb{F}^{2n}$ to $\mathbb{F}^{2n}$ and from $\mathbb{F}^n$ to $\mathbb{F}^n$, respectively. Furthermore, suppose F and $\tilde{F}$ are HFE polynomials such that for some $\alpha_1, \ldots, \alpha_{2n}, \beta_1, \ldots, \beta_{2n}$ in $\mathbb{K}$, the q-Hamming-weight-three $\Psi = \Psi_0 + \Psi_1$ has degree lower than a "small" integer D, where

$$\begin{aligned} \Psi_0 &= X\left(\alpha_1 F_0 + \cdots + \alpha_n F_{n-1} + \beta_1 \tilde{F}_0 + \cdots + \beta_n \tilde{F}_{n-1}\right) \text{ and} \\ \Psi_1 &= X^q\left(\alpha_{n+1} F_0 + \cdots + \alpha_{2n} F_{n-1} + \beta_{n+1} \tilde{F}_0 + \cdots + \beta_{2n} \tilde{F}_{n-1}\right). \end{aligned}$$

Similarly to HFE decrytion, in ZHFE for decryption it is necessary to invert the core function $G := (F, \tilde{F})$. However, the high degree of the core polynomials makes it inefficient to find directly preimagens from F and $\tilde{F}$. At this point, the function Ψ plays an important role. The following proposition was proven in [12] and shows how Ψ is used to invert the core polynomials

Proposition 1.2.1. *Let (Y_1, Y_2) be an element in $Im(G) \subseteq \mathbb{K}\times\mathbb{K}$. Then the set of pre-images of (Y_1, Y_2) under the map $G = (F, \tilde{F})$ is a subset of the roots of the low degree polynomial*

$$\Psi' = \Psi - \sum_{j=1}^{2} X^{q^{j-1}} \sum_{i=1}^{n} \alpha_{i+n(j-1)} Y_1^{q^{i-1}} + \beta_{i+n(j-1)} Y_2^{q^{i-1}}.$$

The ZHFE's public key is formed by the structure of the field $\mathbb{F}$ and an ordered set of $2n$ degree two polynomials in n variables $P = (p_1, \ldots, p_{2n})$ constructed as

$$P = (p_1, \ldots, p_{2n}) = T \circ (\varphi \times \varphi) \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S.$$

The core polynomials F and $\tilde{F}$ have high degree and their associated matrices, high rank. This is in order to avoid the so called Kipnis and Shamir attack.

The ZHFE's private key is formed by the invertible affine transformations S and T, the function Ψ and the scalars α_i's and β_i's.

As in HFE, to encryp a message $\mathbf{x} \in \mathbb{F}^n$ using the ZHFE cryptosystem, simply we compute $\mathbf{y} = P(\mathbf{x}) \in \mathbb{F}^{2n}$. To decrypt a chipertext $\mathbf{y}$ we do the following steps

1. compute $\mathbf{w} = T^{-1}(\mathbf{y})$, next
2. calculate $(Y_1, Y_2) = \varphi_2^{-1}(\mathbf{w})$, where $\varphi_2 := (\varphi \times \varphi)$
3. Now we need to find the set of pre-images of Y_1, Y_2 under $(F, \tilde{F})$, i.e., the elements $X \in \mathbb{K}$ such that $(F(X), \tilde{F}(X)) = (Y_1, Y_2)$. From Proposition 1.2.1 that set is a subset of the set $\mathcal{Z}$ of roots of Ψ', i.e.,

   $$\mathcal{Z} = \{X \in \mathbb{K} |\ \Psi'(X) = 0\}.$$

   So, finding $\mathcal{Z}$ and for each element $X \in \mathcal{Z}$ computing $(F(X), \tilde{F}(X))$, we can find the set of pre-images of Y_1, Y_2 under $(F, \tilde{F})$.
4. Finally, apply $(\varphi^{-1} \circ S)^{-1}$ for each pre-image found in the previous step. To know which of the outputs is the original plaintext, some redundant information must be added to he plaintext.

1.3 ZHFE's key generation

In a public key cryptosystem, the key generation algorithm is the set of steps whereby the private and public key are constructed. In ZHFE case it is necessary to find two HFE polynomials F and $\tilde{F}$, and scalars $\alpha_1, \ldots, \alpha_{2n}, \beta_1, \ldots, \beta_{2n}$ such that the polynomial Ψ defined as in the previous section has degree less than a small integer D. Next, choose uniformly at random the invertible transformations S and T. Then, construct the public key P and the low degree polynomial Ψ.

The hard part of the key generation process is to find the polynomials F, $\tilde{F}$ and the scalars α_i's, β_i's, such that the polynomial

$$\Psi = X\left(\sum_{i=1}^{n} \alpha_i F_{i-1} + \sum_{i=1}^{n} \beta_i \tilde{F}_{i-1}\right) + X^q \left(\sum_{i=1}^{n} \alpha_{n+i} F_{i-1} + \sum_{i=1}^{n} \beta_{n+i} \tilde{F}_{i-1}\right),$$

has degree less than D. To accomplish this, Porras et al. proposed in [12] to determine the coefficients of F and $\tilde{F}$, also the scalars α_i's, β_i's so that the coefficients of terms in Ψ of degree greater than D are zero. This results in a vanishing equation system $\mathcal{S}$ where the coefficients of F and $\tilde{F}$, together with the scalars α_i's and β_i's are variables in the big field $\mathbb{K}$. Each equation represents the coefficient of one term in Ψ with degree greater than D. Since each polynomial has $\frac{n(n+1)}{2} + n + 1$ coefficients, if q (the size of the small field $\mathbb{F}$) is different from two, and it is equal to $\frac{n(n-1)}{2} + n + 1$ if $q = 2$, then the number of variables in this system is

$$N = \begin{cases} 2\left(\frac{n(n+1)}{2} + n + 1\right) + 4n & \text{if} \quad q \neq 2 \\ 2\left(\frac{n(n-1)}{2} + n + 1\right) + 4n & \text{if} \quad q = 2. \end{cases}$$

The number of equation depends on the parameter D and it is the number t of terms in Ψ having degree greater than D. Therefore, we get an equation system with N variables and t equations. Solving this system of equation we can get the coefficients of F and $\tilde{F}$, plus the scalars α_i's and β_i's necessary to build a low degree polynomial Ψ. The problem with this system is that it is not a linear system because several variables are raised to one q-power.

To make $\mathcal{S}$ a linear equation system, Porras et al. proposed in [12] choosing uniformly at random the scalars α_i's and β_i's, and writing each variable Z (coefficient of F or $\tilde{F}$) in terms of the basis $\{1, y, \ldots, y^{n-1}\}$, i.e.,

$$Z = u_0 + u_1 y + \cdots + u_{n-1} y^{n-1},$$

where $u_0, \ldots, u_{n-1}$ are new variables over the small field $\mathbb{F}$. Notice that, by linearity of Frobenius powers,

$$Z^{q^i} = u_0 + u_1 y^{q^i} + \cdots + u_{n-1} y^{q^i(n-1)}.$$

Writing each power of y as a linear combination of the basis $\{1, y, \ldots, y^{n-1}\}$ we get

$$Z^{q^i} = h_0(u_0, \ldots, u_{n-1}) + h_1(u_0, \ldots, u_{n-1}) y + \ldots + h_{n-1}(u_0, \ldots, u_{n-1}) y^{n-1},$$

where $h_i(u_0, \ldots, u_{n-1})$ is a linear combination of the variables u_i's. In this sense, each equation in $\mathcal{S}$ can be seen as n equations (one by each power of y) and Nn variables (n by each coefficient from F or $\tilde{F}$). Therefore, the non linear system $\mathcal{S}$ with variables in the big field $\mathbb{K}$ can be seen as a linear system with tn equations and Nn variables in the small field $\mathbb{F}$, called $\mathcal{T}$. Since F and $\tilde{F}$ have the same terms, then for any D, the number of equations t is less than or equal to two times the number of coefficients in F, i.e., $t \leq N$. The equality is only obtained when $D = 0$, which implies that Ψ is a constant. This makes no sense in ZHFE, so we can assume that D is always greater than 1. For any D, we have $t < N$ and the linear system has more variables (Nn) than equations (tn), so that, in general the linear system $\mathcal{T}$ has nontrivial solutions.

Porras et al. suggested in [12] to find a basis for the null space associated with the linear system $\mathcal{T}$ and then choose a uniformly random element to build the polynomials F and $\tilde{F}$. The problem with this approach is that for realistic parameters the size of the matrix is very big, thus finding a null space basis is very slow and then the key generation process is not practical. The information in Table 1.1 is subtracted from [12] and shows the computational

n	CPU time [s]	Memory[MB]	Number of rows	Number of columns
20	109.38	416	8500	9200
23	272.96	778	12880	13754
26	560.41	1361	18538	19604
29	1148.27	2333	25636	26912
32	2019.73	3609	34336	35840
35	3661.46	5813	44800	46550

Table 1.1: Private key generation for $q = 7$ and $D = 105$

time, memory resources, size of the matrix necessary to create one ZHFE private key for different parameters.

In this thesis we describe the structure behind the big system $\mathcal{T}$ used in private key generation and we propose an efficient method to find an element in that null space.

Chapter 2

A faster key generation method

In this chapter we describe a new method to build the function Ψ necessary to create the private key in ZHFE. First, we enumerate adequately the coefficients of the polynomial F and $\tilde{F}$ in order to show the hidden structure of the matrix associated with the vanishing equation system. Next, we propose a method to solve efficiently the structured vanishing equation system. This chapter was adapted from the paper entitled Efficient ZHFE Key Generation, which was accept for publication in Post-Quantum Cryptography 7-th International Conference [1].

2.1 Structure of the Matrix

The vanishing equation system arises from equating to zero the coefficients of terms in $\Psi = \Psi_0 + \Psi_1$ of degree greater than or equal to D. We carefully explain the combinatorial structure of the Frobenius powers of F and $\tilde{F}$. We explain how they match and mismatch when raised to q-Hamming-weight-three through multiplication by q-Hamming-weight-one monomials.

We will consider the case when n is even. The case when n is odd is similar and even easier. Our analysis focuses on the q-Hamming-weight-three terms of Ψ, because q-Hamming-weight-two terms lead to an independent and much simpler system. For $k \in \{0, \ldots, \frac{n}{2}\}$ let $\mathcal{A}_k$ be the subset of $\mathbb{Z}_n \times \mathbb{Z}_n$

$$\mathcal{A}_k := \begin{cases} \{(i, (k+i) \mod n) |\ 0 \leq i < n\} & \text{if } 0 \leq k < \frac{n}{2}, \\ \left\{(i, k+i) |\ 0 \leq i < \frac{n}{2}\right\} & \text{if } k = \frac{n}{2}. \end{cases}$$

Let $\mathcal{A}$ be the union of the $\mathcal{A}_i'$s. Each element (i, j) from $\mathcal{A}$ represents the q-Hamming-weight-two term $X^{q^i+q^j}$ of an HFE polynomial. Note that each possible q-Hamming-weight-two term $X^{q^i+q^j}$ appears on a single $\mathcal{A}_i$. Moreover, if $(i, j) \in \mathcal{A}$ then $(j, i) \notin \mathcal{A}$.

Consider two HFE polynomials F and $\tilde{F}$. We denote by Z_h the coefficient of $X^{q^i+q^j}$ in F or $\tilde{F}$, where $h \in \mathbb{Z}^+$ depends on (i, j) and on which polynomial the term $Z_h X^{q^i+q^j}$ belongs to. We aim to sort these terms according to the partition $\{\mathcal{A}_k\}_{k=0}^{\frac{n}{2}}$ of $\mathcal{A}$. For $(i, j) \in \mathcal{A}_k$, the coefficient of $X^{q^i+q^j}$ in F will be indexed by $2nk + i$ so that they range from $2nk$ to $2nk + n - 1$, and we will index the coefficient of $X^{q^i+q^j}$ in $\tilde{F}$ by $2nk + n + i$ so that they range from $2nk + n$ to $2nk + 2n - 1$.

Similarly, we index the coefficients of the q-Hamming-weight-one monomials by setting $Z_{n(n+1)+i}$ and $Z_{n(n+1)+n+i}$ to be the coefficients of X^{q^i} in F and $\tilde{F}$, respectively. With the terms indexed in this fashion, F and $\tilde{F}$ are as follows

$$\begin{aligned} F(X) &= \sum_{k=0}^{\frac{n}{2}} \left(\sum_{(i,j)\in\mathcal{A}_k} Z_{2nk+i} X^{q^i+q^j} \right) + \sum_{i=1}^{n-1} Z_{n(n+1)+i} X^{q^i} + C, \\ \tilde{F}(X) &= \sum_{k=0}^{\frac{n}{2}} \left(\sum_{(i,j)\in\mathcal{A}_k} Z_{2nk+n+i} X^{q^i+q^j} \right) + \sum_{i=1}^{n-1} Z_{n(n+1)+n+i} X^{q^i} + \tilde{C}. \end{aligned}$$

For $0 \leq k \leq \frac{n}{2}$, we define **the $k-$th part of** F as ${}_kF(X) := \sum_{(i,j)\in\mathcal{A}_k} Z_{2nk+i} X^{q^i+q^j}$. For $(i,j) \in \mathcal{A}_k$, the Frobenius powers of $X^{q^i+q^j} \mod \left(X^{q^n} - X\right)$ fall within a set indexed by $\mathcal{A}_k$, moreover, the $k-$th part of F^{q^ℓ} is equal to the $k-$th part of F, raised to the power q^ℓ. In order to prove this, we introduce the following definition.

Definition 2.1.1. *For $(i,j) \in \mathcal{A}_k$, and $\ell \in \mathbb{Z}_n$ we define*

$$i \ominus \ell := \begin{cases} i - \ell \ mod\ n & if \quad k \neq \frac{n}{2} \\ i - \ell \ mod\ \frac{n}{2} & if \quad k = \frac{n}{2}. \end{cases}$$

Proposition 2.1.2. *For $0 \leq \ell \leq n-1$, ${}_k\left[F(X)^{q^\ell}\right] = [{}_kF(X)]^{q^\ell}$.*

Proof. In this proof we start taking $\ell = 1$ and after we iterate ℓ times the same process.

$$\begin{aligned} [{}_kF(X)]^q &= \left(\sum_{(i,j)\in\mathcal{A}_k} Z_{2nk+i} X^{q^i+q^j} \right)^q \mod (X^{q^n} - X) \\ &= \left(\sum_{(i,j)\in\mathcal{A}_k} Z^q_{2nk+i} X^{q^{i+1}+q^{j+1}} \right) \mod (X^{q^n} - X) \\ &= \sum_{(i,j)\in\mathcal{A}_k} Z^q_{2nk+(i\ominus 1)} X^{q^i+q^j}. \end{aligned}$$

So, by iterating this ℓ times, we obtain

$${}_k\left[F(X)^{q^\ell}\right] = \sum_{(i,j)\in\mathcal{A}_k} Z^{q^\ell}_{2nk+(i\ominus\ell)} X^{q^i+q^j} = [{}_kF(X)]^{q^\ell}.$$

□

Using the notation for the $\ell-$th Frobenius power of F as F_ℓ, we have ${}_k[F_\ell] = [{}_kF]_\ell$. Since the $\mathcal{A}_k$'s are mutually disjoint, if $2 < q$ and $(i,j) \in \mathcal{A}_k$, the only term in F_ℓ that has the monomial $X^{q^i+q^j}$ is $Z^{q^\ell}_{2nk+(i\ominus\ell)} X^{q^i+q^j}$. We thus get the following result.

Corolary 2.1.3. *If $(i,j) \in \mathcal{A}_k$ and $s \in \{0,1\}$, then the coefficient of $X^{q^s+q^i+q^j}$ in Ψ_s is*

$$\sum_{\ell=0}^{n-1} \alpha_{ns+\ell+1} Z_{2nk+(i\ominus\ell)}^{q^\ell} + \sum_{\ell=0}^{n-1} \beta_{ns+\ell+1} Z_{2nk+n+(i\ominus\ell)}^{q^\ell}.$$

This corollary determines the coefficients of the q-Hamming-weight-three monomials in Ψ_0 and Ψ_1. Since $\Psi = \Psi_0 + \Psi_1$, in order to determine the coefficients of the q-Hamming-weight-three monomials of Ψ, we only need to find the q-Hamming-weight-three monomials that Ψ_0 and Ψ_1 share. The following lemma gives the conditions under which this holds

Lemma 2.1.4. *Assume $2 < q$, $(i,j) \in \mathcal{A}_k$ and $(s,t) \in \mathcal{A}$.*

1. *For $0 \le k < \frac{n}{2}$, $q^0 + q^i + q^j = q^1 + q^s + q^t$ if and only if*
   (a) *$i = 1$, $s = 0$ and $j = t$, or*
   (b) *$j = 1$, $t = 0$ and $i = s$.*
2. *For $k = \frac{n}{2}$, $q^0 + q^i + q^j = q^1 + q^s + q^t$ if and only if $i = 1, s = j = \frac{n}{2} + 1$ and $t = 0$.*

Proof. Throughout this proof we will use the uniqueness of the q-ary expansion of integers. Suppose $q^0 + q^i + q^j = q^1 + q^s + q^t$. If $i = j$, then $q^0 + 2q^i = q^1 + q^s + q^t$, but this is absurd since $q > 2$ and q^1 does not appear in the q-ary expansion of $q^0 + 2q^i$. Now, if $i \neq j$, the uniqueness of the q-ary expansion of $q^0 + q^i + q^j$ shows us that one of the following cases must hold:

1. $i = 1, s = 0$ and $j = t$
2. $j = 1, t = 0$ and $i = s$
3. $i = 1, t = 0$ and $j = s$
4. $j = 1, s = 0$ and $i = t$.

Suppose $0 \le k < \frac{n}{2}$. We now show that cases 3 and 4 are not possible. Suppose $i = 1, t = 0$ and $j = s$, then $(s,0) \in \mathcal{A}$ and therefore $s > \frac{n}{2}$, but $j = s$, then $(1,j) \in \mathcal{A}_k$ with $0 \le k < \frac{n}{2}$ and $j > \frac{n}{2}$, but this is a contradiction since in this case $\frac{n}{2} > k = j - 1 > \frac{n}{2} - 1$, so case 3 is not possible. Now, if case 4 holds, i.e., if $j = 1, s = 0$ and $i = t$, proceeding as before we see that $(0,t) \in \mathcal{A}$ and so $t \le \frac{n}{2}$, but then $(i,1) \in \mathcal{A}_k$ with $0 \le k \le \frac{n}{2}$ and $i = t \le \frac{n}{2}$, which is absurd since $(1,i) \in \mathcal{A}_k$ (note this also shows that case 4 is not possible when $k = \frac{n}{2}$). It is straightforward to see that cases 1 and 2 are actually achievable.

Now suppose $k = \frac{n}{2}$. We claim that only case 3 is possible. Indeed, case 4 is not possible as we pointed out in the previous paragraph. Suppose case 1 holds, then $i = 1, s = 0$ and $j = t$ and therefore $(1,j) \in \mathcal{A}_{\frac{n}{2}}$, then $j = \frac{n}{2} + 1 = t$ so $\left(0, \frac{n}{2} + 1\right) \in \mathcal{A}$, which is absurd since $\left(\frac{n}{2} + 1, 0\right) \in \mathcal{A}_{\frac{n}{2}-1} \subseteq \mathcal{A}$. If case 2 holds, i.e., $j = 1, t = 0$ and $i = s$, we would then have $(i,1) \in \mathcal{A}_{\frac{n}{2}}$, but this is absurd since there is no element of this form in $\mathcal{A}_{\frac{n}{2}}$. Finally, the only possibility left is case 3, which is only achievable by taking $i = 1, s = j = \frac{n}{2} + 1$ and $t = 0$.

□

We can now precisely describe the coefficients of the q-Hamming-weight-three monomials in Ψ.

Proposition 2.1.5. *If $2 < q$ and $(i,j) \in \mathcal{A}_k$, then the coefficient of $X^{q^0+q^i+q^j}$ in Ψ is one of the following:*

i) $$\sum_{p=0}^{1}\left[\sum_{\ell=0}^{n-1}\left(\alpha_{pn+\ell+1}Z^{q^\ell}_{2n(k+p)+((i-p)\ominus\ell)}+\beta_{pn+\ell+1}Z^{q^\ell}_{2n(k+p)+n+((i-p)\ominus\ell)}\right)\right]$$

ii) $$\sum_{p=0}^{1}\left[\sum_{\ell=0}^{n-1}\left(\alpha_{pn+\ell+1}Z^{q^\ell}_{2n(k-p)+((\frac{n}{2}p+1)\ominus\ell)}+\beta_{pn+\ell+1}Z^{q^\ell}_{2n(k-p)+n+((\frac{n}{2}p+1)\ominus\ell)}\right)\right]$$

iii) $$\sum_{p=0}^{1}\left[\sum_{\ell=0}^{n-1}\left(\alpha_{pn+\ell+1}Z^{q^\ell}_{2n(k-p)+(i\ominus\ell)}+\beta_{pn+\ell+1}Z^{q^\ell}_{2n(k-p)+n+(i\ominus\ell)}\right)\right]$$

iv) $$\sum_{\ell=0}^{n-1}\alpha_{\ell+1}Z^{q^\ell}_{2nk+(i\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{\ell+1}Z^{q^\ell}_{2nk+n+(i\ominus\ell)}$$

Moreover, i) holds if $i = 1$ and $k \neq \frac{n}{2}$, ii) holds if $i = 1$ and $k = \frac{n}{2}$, iii) holds if $j = 1$ and iv) holds otherwise.

Proof. Let $(i,j) \in \mathcal{A}_k$. Suppose at first that $i = 1$ and $k \neq \frac{n}{2}$. Note that in this case $(0,j) \in \mathcal{A}_{k+1}$. By Corollary 2.1.3, the coefficient of $X^{q^0+q^1+q^j}$ in Ψ_0 is

$$\sum_{\ell=0}^{n-1}\alpha_{\ell+1}Z^{q^\ell}_{2nk+(1\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{\ell+1}Z^{q^\ell}_{2nk+n+(1\ominus\ell)}.$$

By Lemma 2.1.4, the only monomial in Ψ_1 equal to $X^{q^0+q^1+q^j}$ is $X^{q^1+q^0+q^j}$, whose coefficient by Corollary 2.1.3 is

$$\sum_{\ell=0}^{n-1}\alpha_{n+\ell+1}Z^{q^\ell}_{2n(k+1)+(0\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{n+\ell+1}Z^{q^\ell}_{2n(k+1)+n+(0\ominus\ell)}.$$

Since $\Psi = \Psi_0 + \Psi_1$, the coefficient of $X^{q^0+q^1+q^j}$ in Ψ is

$$\sum_{\ell=0}^{n-1}\alpha_{\ell+1}Z^{q^\ell}_{2nk+(1\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{\ell+1}Z^{q^\ell}_{2nk+n+(1\ominus\ell)} + \sum_{\ell=0}^{n-1}\alpha_{n+\ell+1}Z^{q^\ell}_{2n(k+1)+(0\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{n+\ell+1}Z^{q^\ell}_{2n(k+1)+n+(0\ominus\ell)},$$

i.e.,

$$\sum_{p=0}^{1}\left[\sum_{\ell=0}^{n-1}\left(\alpha_{pn+\ell+1}Z^{q^\ell}_{2n(k+p)+((1-p)\ominus\ell)}+\beta_{pn+\ell+1}Z^{q^\ell}_{2n(k+p)+n+((1-p)\ominus\ell)}\right)\right].$$

Now suppose $i=1$ and $k=\frac{n}{2}$, i.e. $i=1$ and $(i,j)\in\mathcal{A}_k$. Clearly $j=\frac{n}{2}+1$. By Corollary 2.1.3, the coefficient of $X^{q^0+q^1+q^{\frac{n}{2}+1}}$ in Ψ_0 is

$$\sum_{\ell=0}^{n-1}\alpha_{\ell+1}Z^{q^\ell}_{2nk+(1\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{\ell+1}Z^{q^\ell}_{2nk+n+(1\ominus\ell)}.$$

By lemma 2.1.4, the only monomial in Ψ_1 equal to $X^{q^0+q^1+q^{\frac{n}{2}+1}}$ is $X^{q^1+q^{\frac{n}{2}+1}+q^0}$, and by Corollary 2.1.3, its coefficient is

$$\sum_{\ell=0}^{n-1}\alpha_{n+\ell+1}Z^{q^\ell}_{2n(k-1)+((\frac{n}{2}+1)\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{n+\ell+1}Z^{q^\ell}_{2n(k-1)+n+((\frac{n}{2}+1)\ominus\ell)}.$$

Then, the coefficient of $X^{q^1+q^{\frac{n}{2}+1}+q^0}$ in Ψ is

$$\sum_{\ell=0}^{n-1}\alpha_{\ell+1}Z^{q^\ell}_{2nk+(1\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{\ell+1}Z^{q^\ell}_{2nk+n+(1\ominus\ell)}$$
$$+\sum_{\ell=0}^{n-1}\alpha_{n+\ell+1}Z^{q^\ell}_{2n(k-1)+((\frac{n}{2}+1)\ominus\ell)}+\sum_{\ell=0}^{n-1}\beta_{n+\ell+1}Z^{q^\ell}_{2n(k-1)+n+((\frac{n}{2}+1)\ominus\ell)},$$

i.e.,

$$\sum_{p=0}^{1}\left[\sum_{\ell=0}^{n-1}\left(\alpha_{pn+\ell+1}Z^{q^\ell}_{2n(k-p)+((\frac{n}{2}p+1)\ominus\ell)}+\beta_{pn+\ell+1}Z^{q^\ell}_{2n(k-p)+n+((\frac{n}{2}p+1)\ominus\ell)}\right)\right].$$

The other cases are obtained in a similar fashion. □

Recall that the polynomial Ψ is constructed so that its degree is smaller than an adequate parameter D. Therefore, we get a system $\mathcal{S}$ of vanishing equations, where the variables are the coefficients of the polynomials F and $\tilde{F}$, and each equation corresponds to the coefficient of every term in Ψ of degree higher than D equated to zero. From now on, we refer to the variables of the form $Z^{q^\ell}_{2nk+pn+(i\ominus\ell)}$, with $p\in\{0,1\}$, as the variables associated with the group $\mathcal{A}_k$; and to the coefficient of $X^{q^s+q^i+q^j}$ in Ψ equated to zero as the (s,i,j) equation. The matrix associated with this system has a very distinct structure as stated in the following theorem.

Teorema 2.1.6. *Let n,q, and D be positive integers such that $2<q$, $1<r=\lceil\log_q D\rceil<\frac{n}{2}$, and $q+2q^{r-1}<D\leq q^r$. Then, we can reorganize adequately the rows of the matrix associated*

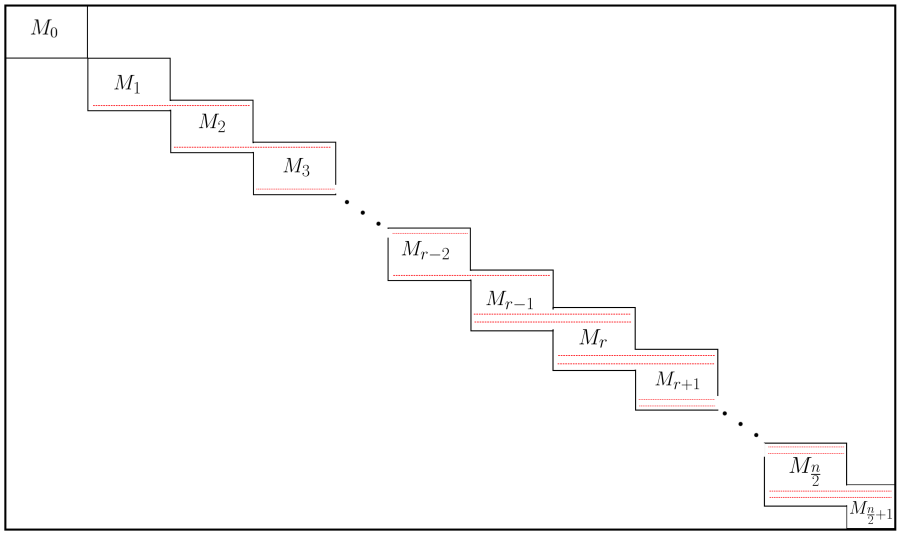

Figure 2.1: Hidden structure of the matrix associated with the system $\mathcal{S}$.

with $\mathcal{S}$ so that it has the form shown in Fig. 2.1, and for $0 \leq k \leq \frac{n}{2}$, the size of the submatrix M_k is $a \times b$, with

$$a = \begin{cases} 2(n-r+k) & \text{if} \quad k < r \\ 2n & \text{if} \quad r \leq i < \frac{n}{2} \\ n & \text{if} \quad k = \frac{n}{2} \end{cases} \qquad \text{and} \qquad b = \begin{cases} 2n^2 & \text{if} \quad k \neq \frac{n}{2} \\ n^2 & \text{if} \quad k = \frac{n}{2} \end{cases} .$$

Proof. Note first that the condition $q + 2q^{r-1} < D \leq q^r$ guarantees that for each $(i,j) \in \mathcal{A}$, $D \leq q + q^i + q^j$ if and only if $D \leq q^0 + q^i + q^j$, and they are both true only if $i \geq r$ or $j \geq r$. So given $0 \leq k \leq \frac{n}{2}$, the number of (s,i,j) equations such that $D \leq q^s + q^i + q^j$, where $s \in \{0,1\}$ and $(i,j) \in \mathcal{A}_k$, is equal to twice the number of elements $(i,j) \in \mathcal{A}_k$ such that $i \geq r$ or $j \geq r$, i.e

$$\begin{cases} 2(n-r+k) & \text{if} \quad k < r \\ 2n & \text{if} \quad r \leq k < \frac{n}{2} \\ 2\frac{n}{2} & \text{if} \quad k = \frac{n}{2}. \end{cases}$$

For $0 < k \leq \frac{n}{2}$, we have $(0,k) \in \mathcal{A}_k$ and $(1,k) \in \mathcal{A}_{k-1}$, so by Proposition 2.1.5 the $(0,1,k)$ equation only contains variables associated with the groups $\mathcal{A}_{k-1}$ and $\mathcal{A}_k$. On the other hand, for $0 \leq k < \frac{n}{2} - 1$ and $(i,0) \in \mathcal{A}_k$, $(i,1) \in \mathcal{A}_{k+1}$ and by the Proposition 2.1.5 the $(0,i,1)$ equation only contains variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k+1}$. Furthermore, note that $(\frac{n}{2}+1, 0) \in \mathcal{A}_{\frac{n}{2}-1}$ and $(1, \frac{n}{2}+1) \in \mathcal{A}_{\frac{n}{2}}$, so the $(0,1,\frac{n}{2}+1)$ equation contains only variables associated with $\mathcal{A}_{\frac{n}{2}-1}$ and $\mathcal{A}_{\frac{n}{2}-1}$.

According to Lemma 2.1.4 and Corollary 2.1.3, if $(i,j) \in \mathcal{A}_k$ and $i,j \notin \{0,1\}$, then the $(0,i,j)$, $(1,i,j)$ equations only contain variables associated with $\mathcal{A}_k$. Then, for each k the elements of the form $(0,j)$, $(1,j+1)$, $(i,0)$ and $(i+1,0)$ are the only ones that have elements associated with a group different to $\mathcal{A}_k$. So, given $0 < k < \frac{n}{2}$, the number of equations in $\mathcal{S}$ that contain variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k+1}$ is equal to the number of elements

$(i,j) \in \mathcal{A}_k$ such that $i = 1$ and $j \geq r$; or $j = 0$ and $i \geq r$. Similarly, the number of equations in $\mathcal{S}$ that contain variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k-1}$ is equal to the number of elements $(i,j) \in \mathcal{A}_k$ such that $i = 0$ and $j \geq r$; or $j = 1$ and $i \geq r$. Finally, the number of equations in $\mathcal{S}$ that only contain variables associated with $\mathcal{A}_k$ is equal to the number of elements $(i,j) \in \mathcal{A}_k$, such that $i, j \notin \{0,1\}$.

Clearly, for each $(i,i) \in \mathcal{A}_0$ with $i \geq r$, the $(0,i,i)$ and $(1,i,i)$ equations appear in the system $\mathcal{S}$ and only have variables associated with $\mathcal{A}_0$. So, for any equation of the system $\mathcal{S}$ there are two possibilities, either it does not contain variables associated with $\mathcal{A}_0$ or it only contains variables associated with $\mathcal{A}_0$.

Suppose $1 < k \leq r-2$. Even though by Proposition 2.1.5 the $(1,0,k)$ equation contains variables associated with $\mathcal{A}_{k-1}$ and $\mathcal{A}_k$, that equation does not appear in the system because $k \leq r$. Analogously, we conclude that the $(0,1,k+1)$ equation does not appear in the system. On the other hand, $(n-k,0),(n-k+1,1) \in \mathcal{A}_k$, and since $1 < k \leq r-2$ and $r < \frac{n}{2}$, then $r < n-k < n-1$ and so the $(1,n-k,0)$ equation appears in the system; and by Proposition 2.1.5 it has variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k+1}$. Also, since $r < n-k+1 \leq n-1$, the $(0,n-k+1,1)$ equation appears in the system and contains variables associated with $\mathcal{A}_{k-1}$ and $\mathcal{A}_k$. Consequently, for $1 < k \leq r-2$ the system $\mathcal{S}$ only has one equation that contains variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k-1}$, and $\mathcal{S}$ only has one equation that contains variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k+1}$. For every other equation in $\mathcal{S}$, either it only contains variables associated with A_k or it does not contain variables associated with A_k at all.

Now, if $k = r-1$, then $(0,r-1),(1,r) \in \mathcal{A}_{r-1}$. The $(1,0,r-1)$ equation has variables associated with $\mathcal{A}_{r-1}$ and $\mathcal{A}_{r-2}$, but it does not appear in the system. Clearly, the $(0,1,r)$ equation is the only one in $\mathcal{S}$ that contains variables associated with $\mathcal{A}_{r-1}$ and $\mathcal{A}_r$. If in particular $2 < r < \frac{n}{2}$, then $r < \frac{n}{2}+1 < n-(r-1) < n-1$. Thus, $r < n-(r-1)+1 \leq n-1$ and finally we have that

$$\begin{aligned}(n-(r-1),0) &= (0+(n-(r-1)),(r-1)+(n-(r-1)) \bmod n)\,, \text{ and}\\ (n-(r-1)+1,1) &= (0+(n-(r-1))+1,(r-1)+(n-(r-1)+1) \bmod n)\,.\end{aligned}$$

Therefore, $(n-(r-1),0),(n-(r-1)+1,1) \in \mathcal{A}_{r-1}$ and, by Proposition 2.1.5, the $(1,n-(r-1),0)$ equation appears in the system and contains variables associated with $\mathcal{A}_r$ and $\mathcal{A}_{r-1}$. Likewise, the $(0,n-(r-1)+1,1)$ equation appears in the system and has variables associated with $\mathcal{A}_{r-1}$ and $\mathcal{A}_{r-2}$. Notice that, if $r = 2$, then $A_{r-1} = A_1$, and $(0,1)$ is the unique element of the form $(i,1)$ in A_1. Consequently, and since $0,1 < r$, no equation contains variables associated with A_{r-1} and A_{r-2} in the system; in contrast, if $r > 2$, there is only one equation in $\mathcal{S}$ that contains variables associated with A_{r-1} and A_{r-2}, namely, the $(0,n-(r-1)+1,1)$ equation.

If $r \leq k < \frac{n}{2}$, then $\frac{n}{2} \leq n-k < n-k+1 \leq n-1$. By similar reasons as above, the $(1,0,k)$ and $(0,n-k+1,1)$ equations are the only ones in $\mathcal{S}$ that have variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k-1}$. Furthermore, the $(0,1,k+1)$ and $(1,n-k,0)$ equations are the only ones in $\mathcal{S}$ that have variables associated with $\mathcal{A}_k$ and $\mathcal{A}_{k-1}$. All equations of the form (s,i,j) with $(i,j) \in \mathcal{A}_k$ are in $\mathcal{S}$, and they only contain variables associated with $\mathcal{A}_k$.

For $k = \frac{n}{2}$, the $(1,0,\frac{n}{2})$ and $(0,1,\frac{n}{2}+1)$ equations are the only ones that contain variables associated with $\mathcal{A}_{\frac{n}{2}-1}$ and $\mathcal{A}_{\frac{n}{2}}$. Moreover, the (s,i,j) equations with $s \in \{0,1\}$ and $(i,j) \in \mathcal{A}_{\frac{n}{2}}$ are the only ones in $\mathcal{S}$ that contain variables associated with $\mathcal{A}_{\frac{n}{2}}$.

r	**without** the restriction	**with** the restriction
2	$7 < D \leq 49$	$21 < D \leq 49$
3	$49 < D \leq 343$	$105 < D \leq 343$
4	$343 < D \leq 2401$	$693 < D \leq 2401$

Table 2.1: Possible values of D for $q = 7$ and $n = 56$.

Therefore, we can reorganize the rows of the matrix associated with the vanishing equation system $\mathcal{S}$ so that it has the desired structure.

□

Remark 2.1.7. *The conditions* $1 < r < \frac{n}{2}$ *and* $q + 2q^{r-1} < D \leq q^r$ *in Theorem 2.1.6 are merely technical. If we omit these conditions, the matrix is still quite structured but it is a bit harder to describe. Moreover, these conditions do not restrict much the values* D *can take. For example, if we choose the parameters suggested in [11] for a practical implementation of ZHFE,* $q = 7$ *and* $n = 56$*, then* r *could be in the interval* $[1, 28]$ *and the possible values for* D *are as shown in Table 2.1.*

2.2 The Matrix over the Small Field

Recall that we aim at determining the coefficients Z_k such that the polynomial Ψ has degree less than D. Initially, each coefficient Z_k is seen as a variable. In that way, every term of the form $\alpha_{ns+\ell+1} Z_k^{q^\ell}$ in Ψ can be seen as an $\mathbb{F}$-linear transformation from $\mathbb{K}$ to $\mathbb{K}$. Since the big field $\mathbb{K}$ is a vector space over the small field $\mathbb{F}$, any $\mathbb{F}$-linear transformation $\mathbb{K} \to \mathbb{K}$ can be seen as an $\mathbb{F}$-linear transformation $\mathbb{F}^n \to \mathbb{F}^n$. Let $A_{ns+\ell}$ be the matrix over $\mathbb{F}$ that represents the $\mathbb{F}$-linear transformation $Z \mapsto \alpha_{ns+\ell+1} Z^{q^\ell}$ with respect to the canonical basis.

Let (i, j) be an element in $\mathcal{A}_k$ for some $k \neq \frac{n}{2}$. We know that the coefficient of $X^{q^s+q^i+q^j}$ in Ψ_s is

$$\sum_{\ell=0}^{n-1} \alpha_{ns+\ell+1} Z_{2nk+(i \ominus \ell)}^{q^\ell} + \sum_{\ell=0}^{n-1} \beta_{ns+\ell+1} Z_{2nk+n+(i \ominus \ell)}^{q^\ell}. \tag{2.1}$$

We can see the expression in (2.1) as an $\mathbb{F}$-linear transformation $T_{s,i}^k : \mathbb{K}^{2n} \to \mathbb{K}$, such that its $(ns + i)$-th variable is $Z_{2nk+ns+i}$, where $s \in \{0, 1\}$ and $i = 0, \ldots n - 1$. In that way, the matrix that represents $T_{s,i}^k$ is $[A|B]$ with

$$A = \left[\; A_{ns+i} \;\middle|\; A_{ns+i-1} \;\middle|\; \cdots \;\middle|\; A_{ns} \;\middle|\; A_{ns+n-1} \;\middle|\; \cdots \;\middle|\; A_{ns+(i+1)} \; \right],$$
$$B = \left[\; B_{ns+i} \;\middle|\; B_{ns+i-1} \;\middle|\; \cdots \;\middle|\; B_{ns} \;\middle|\; B_{ns+n-1} \;\middle|\; \cdots \;\middle|\; B_{ns+(i+1)} \; \right],$$

where $A_{ns+\ell}$ and $B_{ns+\ell}$ are the matrices that represent the $\mathbb{F}$-linear transformations $\alpha_{ns+\ell+1} Z^{q^\ell}$ and $\beta_{ns+\ell+1} Z^{q^\ell}$, respectively. Furthermore, the matrix that represents the $\mathbb{F}$-linear transformation T_k from $\mathbb{K}^{2n}$ to $\mathbb{K}^{2n}$, defined by

$$T_k = (T_{0,0}^k, \cdots, T_{0,n-1}^k, T_{1,0}^k, \cdots T_{1,n-1}^k),$$

$$\left[\begin{array}{ccccc|ccccc}
A_0 & A_{n-1} & A_{n-2} & \cdots & A_1 & B_0 & B_{n-1} & B_{n-2} & \cdots & B_1 \\
A_1 & A_0 & A_{n-1} & \cdots & A_2 & B_1 & B_0 & B_{n-1} & \cdots & B_2 \\
A_2 & A_1 & A_0 & \cdots & A_3 & B_2 & B_1 & B_0 & \cdots & B_3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
A_{n-2} & A_{n-3} & A_{n-4} & \cdots & A_{n-1} & B_{n-2} & B_{n-3} & B_{n-4} & \cdots & B_{n-1} \\
A_{n-1} & A_{n-2} & A_{n-3} & \cdots & A_0 & B_{n-1} & B_{n-2} & B_{n-3} & \cdots & B_0 \\
\hline
A_n & A_{2n-1} & A_{2n-2} & \cdots & A_{n+1} & B_n & B_{2n-1} & B_{2n-2} & \cdots & B_{n+1} \\
A_{n+1} & A_n & A_{2n-1} & \cdots & A_{n+2} & B_{n+1} & B_n & B_{2n-1} & \cdots & B_{n+2} \\
A_{n+2} & A_{n+1} & A_n & \cdots & A_{n+3} & B_{n+2} & B_{n+1} & B_n & \cdots & B_{n+3} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
A_{2n-2} & A_{2n-3} & A_{2n-4} & \cdots & A_{2n-1} & B_{2n-2} & B_{2n-3} & B_{2n-4} & \cdots & B_{2n-1} \\
A_{2n-1} & A_{2n-2} & A_{2n-3} & \cdots & A_n & B_{2n-1} & B_{2n-2} & B_{2n-3} & \cdots & B_n
\end{array}\right]$$

Figure 2.2: Matrix representation of $T_k : \mathbb{K}^{2n} \to \mathbb{K}^{2n}$.

is as shown in Fig. 2.2.

Similarly, for $(i,j) \in \mathcal{A}_{\frac{n}{2}}$, we can define the $\mathbb{F}$-linear transformation $T_{s,i}^{\frac{n}{2}}$ from $\mathbb{K}^n$ to $\mathbb{K}$, so that the matrix that represents $T_{s,i}^{\frac{n}{2}}$ is $[A|B]$ with

$$A = \left[\begin{array}{c|c|c|c|c} A_{ns+i} + A_{ns+\frac{n}{2}+i} & \cdots & A_{ns} + A_{ns+\frac{n}{2}} & A_{ns+n-1} + A_{ns+\frac{n}{2}-1} & \cdots & A_{ns+(i+1)} + A_{ns+\frac{n}{2}+(i+1)} \end{array}\right],$$
$$B = \left[\begin{array}{c|c|c|c|c} B_{ns+i} + B_{ns+\frac{n}{2}+i} & \cdots & B_{ns} + B_{ns+\frac{n}{2}} & B_{ns+n-1} + B_{ns+\frac{n}{2}-1} & \cdots & B_{ns+(i+1)} + B_{ns+\frac{n}{2}+(i+1)} \end{array}\right].$$

The matrix that represents the $\mathbb{F}$-linear transformation $T_{\frac{n}{2}} = (T_{0,1}^{\frac{n}{2}}, \ldots, T_{0,\frac{n}{2}-1}^{\frac{n}{2}}, T_{1,0}^{\frac{n}{2}}, \ldots, T_{1,\frac{n}{2}-1}^{\frac{n}{2}})$ is presented Fig. 2.3.

Recall that the homogeneous system $\mathcal{S}$ contains all (s,i,j) equations such that $q^s + q^i + q^j \geq D$, where $s \in \{0,1\}$ and $(i,j) \in \mathcal{A}$. Theorem 2.1.6 explains the hidden structure of the matrix associated with $\mathcal{S}$. We now consider $\mathcal{S}$ with the order given in Theorem 2.1.6, so that the $i-$th equation in $\mathcal{S}$ can be seen as $L_i(Z_0, \ldots, Z_N) = \mathbf{0}$, where L_i is an $\mathbb{F}$-linear transformation from $\mathbb{K}^N$ to $\mathbb{K}$ and N is two times the number of variables of the polynomial F. In that way, $\mathcal{S}$ can be seen as $L(Z_1, \ldots, Z_N) = \mathbf{0}$, where $L = (L_1, \ldots, L_t)$ and t is the number of equations in the system $\mathcal{S}$.

Teorema 2.2.1. *Let n, q, and D be positive integers such that $q > 2$, $1 < r = \lceil \log_q D \rceil < \frac{n}{2}$ and $q + 2q^{r-1} < D \leq q^{r-1}$. Then, the matrix $\tilde{M}$ that represents the $\mathbb{F}$-linear transformation L is formed by $\frac{n}{2}+1$ submatrices $\tilde{M}_0, \ldots, \tilde{M}_{\frac{n}{2}}$ arranged in the same way as in the matrix in Fig. 2.1. For $0 \leq i \leq \frac{n}{2}$, the size of the submatrix $\tilde{M}_i$ is $a \times b$, where*

$$a = \begin{cases} 2n(n-r-i) & \text{if } i < r \\ 2n^2 & \text{if } r \leq i < \frac{n}{2} \\ n^2 & \text{if } i = \frac{n}{2} \end{cases}, \qquad b = \begin{cases} 2n^2 & \text{if } i \neq r \\ n^2 & \text{if } i = \frac{n}{2}. \end{cases}$$

Remark 2.2.2. *The blocks $\tilde{M}_i$ and $\tilde{M}_{i+1}$ overlap in a block of pn rows if and only if the blocks M_i and M_{i+1} overlap in p rows.*

A_0 $+A_{\frac{n}{2}}$	$A_{\frac{n}{2}-1}$ $+A_{\frac{n}{2}-1}$	$\cdots$	A_1 $+A_{\frac{n}{2}+1}$	B_0 $+B_{\frac{n}{2}}$	$B_{\frac{n}{2}-1}$ $+B_{\frac{n}{2}-1}$	$\cdots$	B_1 $+B_{\frac{n}{2}+1}$
A_1 $+A_{\frac{n}{2}+1}$	A_0 $+A_{\frac{n}{2}}$	$\cdots$	A_2 $+A_{\frac{n}{2}+2}$	B_1 $+B_{\frac{n}{2}+1}$	B_0 $+B_{\frac{n}{2}}$	$\cdots$	B_2 $+B_{\frac{n}{2}+2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$A_{\frac{n}{2}-1}$ $+A_{\frac{n}{2}+\frac{n}{2}-1}$	$A_{\frac{n}{2}-2}$ $+A_{\frac{n}{2}+\frac{n}{2}-2}$	$\cdots$	A_0 $+A_{\frac{n}{2}}$	$B_{\frac{n}{2}-1}$ $+B_{\frac{n}{2}+\frac{n}{2}-1}$	$B_{\frac{n}{2}-2}$ $+B_{\frac{n}{2}+\frac{n}{2}-2}$	$\cdots$	B_0 $+B_{\frac{n}{2}}$
A_n $+A_{n+\frac{n}{2}}$	$A_{n+\frac{n}{2}-1}$ $+A_{n+\frac{n}{2}-1}$	$\cdots$	A_{n+1} $+A_{n+\frac{n}{2}+1}$	B_n $+B_{n+\frac{n}{2}}$	$B_{n+\frac{n}{2}-1}$ $+B_{n+\frac{n}{2}-1}$	$\cdots$	B_{n+1} $+B_{n+\frac{n}{2}+1}$
A_{n+1} $+A_{n+\frac{n}{2}+1}$	A_n $+A_{n+\frac{n}{2}}$	$\cdots$	A_{n+2} $+A_{n+\frac{n}{2}+2}$	B_{n+1} $+B_{n+\frac{n}{2}+1}$	B_n $+B_{n+\frac{n}{2}}$	$\cdots$	B_{n+2} $+B_{n+\frac{n}{2}+2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$A_{n+\frac{n}{2}-1}$ $+A_{n+\frac{n}{2}+\frac{n}{2}-1}$	$A_{n+\frac{n}{2}-2}$ $+A_{n+\frac{n}{2}+\frac{n}{2}-2}$	$\cdots$	A_n $+A_{n+\frac{n}{2}}$	$B_{n+\frac{n}{2}-1}$ $+B_{n+\frac{n}{2}+\frac{n}{2}-1}$	$B_{n+\frac{n}{2}-2}$ $+B_{n+\frac{n}{2}+\frac{n}{2}-2}$	$\cdots$	B_n $+B_{n+\frac{n}{2}}$

Figure 2.3: Matrix representation of $T_{\frac{n}{2}} : \mathbb{K}^n \to \mathbb{K}^n$.

Remark 2.2.3. *The submatrices $\tilde{M}_0, \ldots, \tilde{M}_{\frac{n}{2}}$ are small modifications of the matrix in Fig. 2.2. More precisely, for $r \leq k < \frac{n}{2}$, $\tilde{M}_k$ can be obtained simply by permuting the rows of the matrix in Fig. 2.2, placing in the upper part the rows that come from equations in $\mathcal{S}$ with variables associated with both $\mathcal{A}_k$ and $\mathcal{A}_{k-1}$. Also, for $0 \leq k \leq r-1$, $\tilde{M}_k$ can be obtained by removing the blocks of rows that represent expressions with $(i,j) \in A_k$, $i < r$ and $j < r$, and adequately permuting rows as above.*

Note that Theorem 2.2.1, together with the description of the submatrices above, provide a direct and fast algorithm to construct the matrix $\tilde{M}$. Given α_i's and β_i's we construct $A_{ns+\ell}$ and $B_{ns+\ell}$ as the matrices that represent the $\mathbb{F}$-linear transformations $Z \mapsto \alpha_{ns+\ell+1} Z^{q^\ell}$ and $Z \mapsto \beta_{ns+\ell+1} Z^{q^\ell}$, respectively. Then, we assemble the matrices in Fig. 2.2 and Fig. 2.3 for all k's, and sort their rows according to Remark 2.2.3. Finally, we put them together as described in Theorem 2.2.1. However, as we will see in the next section, we never really have to construct the whole matrix $\tilde{M}$. Since we just aim at finding a non-trivial element in its null space, we can exploit its structure to do so more efficiently.

2.3 An Algorithm to Solve the System

In this section, we will first describe an algorithm for finding random elements in the null space of the matrix $\tilde{M}$. The algorithm is based on the hidden structure of the matrix unveiled in Theorem 2.2.1. Then, we will discuss the probability that this algorithm terminates.

As seen in Section 2.2, the matrix $\tilde{M}$ is almost block diagonal, with blocks $\tilde{M}_1, \ldots, \tilde{M}_{\frac{n}{2}}$ overlapping in a few rows. In order to illustrate the method, suppose we have only two

blocks $\tilde{M}_1, \tilde{M}_2$. We first split each block in two blocks U_i and L_i so that the matrix has the form

$$\tilde{M} = \begin{bmatrix} U_1 & 0 \\ L_1 & U_2 \\ 0 & L_2 \end{bmatrix}.$$

Next we find an element $\mathbf{y}_2$ in the null space of L_2. Then, we compute $\mathbf{r} = U_2\mathbf{y}_2$. Then we find an element $\mathbf{y}_1$ such that $\begin{bmatrix} U_1 \\ L_1 \end{bmatrix} \mathbf{y}_1 = \begin{bmatrix} 0 \\ -\mathbf{r} \end{bmatrix}$. It is easy to see that $\tilde{M} \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} = 0$. This process can be iterated through the whole matrix regardless of the number of blocks.

To formally describe the algorithm, we introduce the following notation. For $r \leq i \leq \frac{n}{2}$, let L_i be the matrix that results from removing the first $2n$ rows from $\tilde{M}_i$, and let L_i be the matrix that results from removing the first n rows from $\tilde{M}_i$, for $2 \leq i < r$. For each $2 \leq i \leq \frac{n}{2}$, U_i is the matrix such that $\tilde{M}_i = \begin{bmatrix} U_i \\ \hline L_i \end{bmatrix}$ (for $i = 1$, we define $U_1 = \tilde{M}_1$). The expression $\mathbf{y} \xleftarrow{\$} W$ denotes that $\mathbf{y}$ is an element chosen uniformly at random from the set W. Algorithm 1 describes an algorithm to find a solution of the equation $\tilde{M}\mathbf{y} = 0$.

Algorithm 1: Finds an element in the null space of $\tilde{M}$

Input: $\tilde{M}_0, \tilde{M}_1, \ldots, \tilde{M}_{\frac{n}{2}}$, blocks of $\tilde{M}$ as described in Theorem 2.2.1

1: $W := \left\{\mathbf{z} \mid L_{\frac{n}{2}}\mathbf{z} = \mathbf{0}\right\}$
2: **for** $i = \frac{n}{2}, \ldots, 1$ **do**
3: $\quad \mathbf{y}_i \xleftarrow{\$} W$
4: $\quad \mathbf{r}_i := U_i\mathbf{y}_i$
5: $\quad W := \left\{\mathbf{z} \mid L_i\mathbf{z} = \left[\begin{array}{c} \mathbf{0} \\ \hline -\mathbf{r}_i \end{array}\right]\right\}$
6: $\quad$ **if** $W = \emptyset$ **then**
7: $\quad\quad$ **stop algorithm**
8: $W := \left\{\mathbf{z} \mid \tilde{M}_0\mathbf{z} = \mathbf{0}\right\}$
9: $\mathbf{y}_0 \xleftarrow{\$} W$
10: **return** $\mathbf{y} = \begin{bmatrix} \mathbf{y}_0 \\ \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_{\frac{n}{2}} \end{bmatrix}$

It is easy to see that if this algorithm terminates, the output $\mathbf{y}$ is an element in the null space of $\tilde{M}$. Moreover, the converse is also true.

Proposition 2.3.1. *If $\boldsymbol{x}$ is a vector in the null space of the matrix $\tilde{M}$, then $\boldsymbol{x}$ can be the output of Algorithm 1.*

Proof. Let $\mathbf{x}$ be an element in the null space of $\tilde{M}$, say

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{t-1} \\ x_t \end{bmatrix}, \qquad t = n^2(n+1).$$

For $0 < i \leq \frac{n}{2}$, we define

$$\mathbf{x}_i = \begin{bmatrix} x_{t_{i-1}+1} \\ x_{t_{i-1}+2} \\ \vdots \\ x_{t_i} \end{bmatrix},$$

where $t_i := 2in^2$, for $0 < i < \frac{n}{2}$, $t_0 := 0$ and $t_{\frac{n}{2}} := t$. Since $\mathbf{x}$ is an element in the null space of $\tilde{M}$ and $\tilde{M}_i = \left[\frac{U_i}{L_i}\right]$, then

$$L_{\frac{n}{2}}\mathbf{x}_{\frac{n}{2}} = \mathbf{0}.$$

Let us define the vector $\mathbf{r}_{\frac{n}{2}}$ as

$$\mathbf{r}_{\frac{n}{2}} = U_{\frac{n}{2}}\mathbf{x}_{\frac{n}{2}}.$$

Since $\mathbf{x}$ is a element in the null space of $\tilde{M}$, we must have that

$$L_{\frac{n}{2}-1}\mathbf{x}_{\frac{n}{2}-1} = \left[\frac{\mathbf{0}}{-\mathbf{r}_{\frac{n}{2}}}\right].$$

So, $\mathbf{x}_{\frac{n}{2}-1}$ belongs to the solution set of the equation

$$L_{\frac{n}{2}-1}\mathbf{z} = \left[\frac{\mathbf{0}}{-\mathbf{r}_{\frac{n}{2}}.}\right]$$

In general, for $0 \leq i < \frac{n}{2}$, $\mathbf{x}_{i-1}$ belongs to the solution set of the equation

$$L_i\mathbf{z} = \left[\frac{\mathbf{0}}{-\mathbf{r}_{i+1},}\right]$$

where $\mathbf{r}_i = U_i\mathbf{x}_i$. □

The above proposition shows that every element in the null space of $\tilde{M}$ can be output by Algorithm 1. However, at this point is not clear what is the distribution of probability over the null space of $\tilde{M}$ given by Algorithm 1. That is a very important issue because if the distribution changes, then the *degree of regularity*[1] may change too.

In the following, we prove that the distribution over the null space of $\tilde{M}$ is still uniform when we use Algorithm 1 to find an element in the null space of $\tilde{M}$. First, we show that

[1]The degree of regularity is a very important parameter associated with a multivariate public key cryptosystem. Its importance lies in the fact that the complexity of the best known algorithm to find preimages in a multivariate polynomial systems is exponential in the degree of regularity

every element in such null space has the same probability to be an output for an execution of Algorithm 1. Indeed, let $\mathbf{x} = [x_1 x_2 \cdots x_{t-1} x_t]^T$, be an element in the null space of $\tilde{M}$, with $t = n^2(n+1)$, U_i's, L_i's and $\mathbf{x}_i'$s as in the proof of Proposition 2.3.1. Let us define the random variable V_i as the result of the i-th partial output in one run of Algorithm 1. Let V be the random variable denoting the complete output. Clearly, the probability that V takes the value $\mathbf{x}$ (denoted by $P(V = \mathbf{x})$) is given by

$$\begin{aligned} P(V = \mathbf{x}) &= P(V_0 = \mathbf{x}_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} P(V_i = \mathbf{x}_{\frac{n}{2}-i} \mid V_{i-1} = \mathbf{x}_{\frac{n}{2}-(i-1)}, \ldots, V_0 = \mathbf{x}_{\frac{n}{2}}) \\ &= P(V_0 = \mathbf{x}_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} P(V_i = \mathbf{x}_{\frac{n}{2}-i} \mid V_{i-1} = \mathbf{x}_{\frac{n}{2}-(i-1)}) \\ &= \frac{1}{\mid W_{\frac{n}{2}} \mid} \prod_{i=1}^{\frac{n}{2}} \frac{1}{\mid W_{\frac{n}{2}-i} \mid}, \end{aligned}$$

where $W_{i-1} = \left\{ \mathbf{z} \mid L_i \mathbf{z} = \left[\begin{array}{c} \mathbf{0} \\ \hline -\mathbf{r}_i \end{array}\right] \right\}$ and $\mathbf{r}_i = U_i \mathbf{x}_i$. It is easy see that $\mid W_{i-1} \mid$ is equal to the number of element in the null space of L_{i-1} (denoted by $\mid \mathrm{Ker}(L_{i-1}) \mid$). Therefore,

$$P(V = \mathbf{x}) = \prod_{i=0}^{\frac{n}{2}} \frac{1}{\mid \mathrm{Ker}(L_{\frac{n}{2}-i}) \mid}.$$

Consequently, each $\mathbf{x}$ in the null space of $\tilde{M}$ is equality probable to be output by Algorithm 1. Finally, we claim that if we execute Algorithm 1 as many times as necessary until it terminates, then the distribution over the null space of $\tilde{M}$ is the uniform distribution.

Algorithm 1 does not always terminate. In case it fails, we would have to run it again. However, we claim that the probability of failure is very small. Note that the termination of the Algorithm 1 depends on W not being empty for each $i = \frac{n}{2}, \ldots, 1$. So, a sufficient condition to guarantee that the Algorithm 1 terminates is that each matrix L_i be of full rank. Therefore, for a uniformly random instance of ZHFE, the probability that the Algorithm 1 terminates is greater than the probability that for each i the rank of L_i is equal to its number of rows. In order to give an estimate for this probability, we ran extensive experiments for different values of n and computed the rank of L_i for $i = r, \ldots, \frac{n}{2}$ (see Table 2.2). For every single instance and for each $i = r, \ldots, \frac{n}{2}$, the matrix L_i was full rank.

2.4 Complexity

The new method finds an element in the null space of an almost-block diagonal matrix with $\frac{n}{2}+1$ blocks, as depicted in Fig. 2.1. The size of each block is at most $2n^2 \times 2n^2$, so reducing each block to its echelon form has complexity $\mathcal{O}\left((n^2)^\omega\right)$, where the parameter $2 \leq \omega \leq 3$ is a constant that depends on the specific Gaussian elimination algorithm used (e.g., $\omega = 3$ for a classical Gaussian elimination algorithm and $\omega < 2.376$ for an asymptotically improved algorithm). Therefore, the complexity of the new method is $\mathcal{O}\left(n\,(n^2)^\omega\right) = \mathcal{O}\left(n^{2\omega+1}\right)$. This

n	Number of Instances
8	80000000
16	4000000
32	100000
56	5000

Table 2.2: Computation of the rank of the L_i's with $q = 7$ and $D = 106$. For every generated instance, the matrices are full rank.

improves the naive approach used in [11], which costs $\mathcal{O}\left((n^3)^\omega\right) = \mathcal{O}\left(n^{3\omega}\right)$, if a dense Gaussian elimination algorithm is used. Since the matrix of the vanishing equation system is sparse, even the old method could take advantage of its sparsity. Although the complexity of sparse algorithms is harder to compare with, our experiments confirm a significant improvement against sparse methods too.

We performed experiments in order to compare the new method with the one used in [11] for solving the vanishing equation system. We built different ZHFE private keys using both methods. In Table 2.3 we present these results for different sets of parameters. All the experiments were performed using Magma v2.21-1 [4] on a server with a processor Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz, running Linux CentOS release 6.6. It is important to notice that the experiments for the old method where performed on Magma using the *Nullspace* command. Magma's *Nullspace* implementation exploits the matrix sparsity using the Markowitz Pivot Strategy. Hence, in practice, we are comparing our new method with an sparse matrix solving algorithm.

		Nuevo Método			Viejo Método		
q	D	n	Tiempo [s]	Memoria [MB]	n	Tiempo [s]	Memoria [MB]
7	106	8	0.07	≤ 32	8	0.43	≤ 32
7	106	16	1.46	≤ 32	16	25.41	131
7	106	32	67.29	64	32	2285.44	3452
7	106	56	1111.26	235	55*	216076.27	53619
17	106	8	0.08	≤ 32	8	0.45	≤ 32
17	106	16	2.02	68	16	26.63	160
17	106	32	122.86	93	32	2095.94	3785
17	595	56	2712.63	353	55*	226384.28	59658

* Experiments run on a different machine: Magma V2.20-2 on a Sun X4440 server, with four Quad-Core AMD OpteronTM Processor 8356 CPUs running at 2.3 GHz.

Table 2.3: Private key generation: comparison between the new and old methods.

Note the significant reduction in the time needed to construct the keys for ZHFE. It is also evident that, for the new method, the memory needed to build the ZHFE keys is considerably less than the memory needed in [11].

Chapter 3

Security of ZHFE

In this chapter we analyze the security of ZHFE with respect to the MinRank Attack. We first show that with high probability there exists a linear combination of Frobenius powers of the core polynomials F and $\tilde{F}$ of low rank. Then, we show that such linear combination can be extracted from the public key.

3.1 Existence of a low rank equivalent key

In this section, we will show that given a instance of ZHFE with public key $P = T \circ (\varphi \times \varphi) \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S$, with high probability there are two invertible affine transformations T', S', and two HFE polynomial F', $\tilde{F}'$ with low rank associated matrices such that

$$P = T' \circ (\varphi \times \varphi) \circ (F', \tilde{F}') \circ \varphi^{-1} \circ S'.$$

Throughout this section we use the following notation, the capital bold font letter denotes a matrix, e.g. $\mathbf{M}$, underline letter denotes a vector, e.g. $\underline{v} = (v_1, \ldots, v_n)$ and φ_2 for $\varphi \times \varphi$. In this section we say that (G, S, T), where $G = (F, \tilde{F})$ is a private key of ZHFE. We only consider linear transformations and homogeneous polynomials. This case can be easily adapted to affine transformations and general HFE polynomial (See [3] section 6.2).

Two private keys are equivalent if they build the same public key. That is:

Definition 3.1.1. *Let (G, S, T) be a private key for ZHFE. We say that (G', S', T'), $G' = (F', \tilde{F}')$ is an equivalent key to (G, S, T) if the polynomials in G' have HFE shape, and*

$$T' \circ \varphi_2 \circ (F', \tilde{F}') \circ \varphi^{-1} \circ S' = T \circ \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S.$$

In terms of above definition, our purpose in this section is to show that given a ZHFE private key, with high probability, there exists an equivalent private key (G', S', T') such that the matrices associated with the polynomials in the core map G' have low rank. To see how this is possible, remember that for each ZHFE private key (G, S, T), $G = (F, \tilde{F})$, there are scalars $\alpha_1, \ldots, \alpha_{2n}, \beta_1, \ldots, \beta_{2n}$ in the big field $\mathbb{K}$ such that the function

$$\begin{aligned} \Psi &= X\left(\alpha_1 F_0 + \cdots + \alpha_n F_{n-1} + \beta_1 \tilde{F}_0 + \cdots + \beta_n \tilde{F}_{n-1}\right) \\ &+ X^q\left(\alpha_{n+1} F_0 + \cdots + \alpha_{2n} F_{n-1} + \beta_{n+1} \tilde{F}_0 + \cdots + \beta_{2n} \tilde{F}_{n-1}\right), \end{aligned}$$

has degree less than a small integer D. Notice that for $s \in \{0,1\}$ the polynomial,

$$\alpha_{sn+1}F_0 + \cdots + \alpha_{sn+n}F_{n-1} + \beta_{sn+1}\tilde{F}_0 + \cdots + \beta_{sn+n}\tilde{F}_{n-1}$$

has HFE shape and by Lemma 2.1.4 in Chapter 2, its non zero monomials with degree greater than D have the form $ZX^{q^0+q^1+q^j}$, with $Z \in \mathbb{K}$ and j an integer. Consequently, in each case the matrix associated with that polynomial has rank less than or equal to $\lceil \log_q D \rceil + 1$ and the following form:

$$\begin{pmatrix} * & * & * & & * & & & \\ * & * & * & \cdots & * & * & \cdots & * \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ & * & & & & & & \\ & \vdots & & & & & & \\ & * & & & & & & \end{pmatrix} \qquad \begin{pmatrix} * & * & * & & * & * & \cdots & * \\ * & * & * & \cdots & * & & & \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ * & & & & & & & \\ \vdots & & & & & & & \\ * & & & & & & & \end{pmatrix}$$

Case $s = 0$. Case $s = 1$.

Let L be the function from $\mathbb{K}^2$ to $\mathbb{K}^2$ given by $L(X,Y) = (L_1(X,Y), L_2(X,Y))$, such that

$$L_1(X,Y) = \sum_{i=1}^{n} \alpha_i X^{q^{i-1}} + \sum_{i=1}^{n} \beta_i Y^{q^{i-1}},\ L_2(X,Y) = \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}}.$$

Notice that L is a linear transformation of the vector space $\mathbb{K}^2$ over $\mathbb{F}$. From the above observation, the matrices associated with the polynomials in $L \circ G$ are of low rank (less than or equal to $r+1 = \lceil \log_q D \rceil + 1$). Furthermore, if L is invertible, then $(L \circ G, S, T \circ R)$ is an equivalent key to (G, S, T), with $R = \varphi_2 \circ L^{-1} \circ \varphi_2^{-1}$ and the matrices associated with the core polynomials $L \circ G$ are of low rank. Indeed

$$\begin{aligned} (T \circ R) \circ \varphi_2 \circ (L \circ G) \circ \varphi^{-1} \circ S &= T \circ \varphi_2 \circ (L^{-1} \circ \varphi_2^{-1} \circ \varphi_2 \circ L) \circ G \circ \varphi^{-1} \circ S \\ &= T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S. \end{aligned}$$

For the above assertion to make sense, the function R must be an invertible linear transformation from $\mathbb{F}^{2n}$ to $\mathbb{F}^{2n}$, and this is only possible if L^{-1} is well defined. For this reason, we will study some properties of the function L taken into the small field $\mathbb{F}$, i.e., properties of the function $\varphi_2 \circ L \circ \varphi_2^{-1}$. To do that, we start introducing the following change of basis matrix $\mathbf{M}_n \in \mathcal{M}_{n\times n}(\mathbb{K})$ defined by

$$M_n = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ y & y^q & & y^{q^{n-1}} \\ \vdots & & \ddots & \\ y^{n-1} & y^{(n-1)q} & & y^{(n-1)q^{n-1}} \end{pmatrix}.$$

It is well known that the matrix M_n is invertible (see [8]). The following proposition is a particular case of Proposition 4 in [3]. We include its proof for completeness.

Proposition 3.1.2. *Let $\boldsymbol{M}_{2n} \in \mathcal{M}_{2n\times 2n}(\mathbb{K})$ be the matrix defined by*

$$\boldsymbol{M}_{2n} = \begin{pmatrix} \boldsymbol{M}_n & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{M}_n \end{pmatrix}.$$

Then the function $\varphi_2 = \mathbb{K}^2 \to \mathbb{F}^{2n}$ can be expressed as

$$(X, Y) \mapsto (X, X^q, \ldots, X^{q^{n-1}}, Y, Y^q, \ldots, Y^{q^{n-1}})\boldsymbol{M}_{2n}^{-1}$$

and its inverse $\varphi_2^{-1} : \mathbb{F}^{2n} \to \mathbb{K}^2$ as

$$(x_1, \ldots, x_{2n}) \mapsto (X_1, X_{n+1}),$$

where $(X_1, \ldots, X_{2n}) = (x_1, \ldots, x_{2n})\boldsymbol{M}_{2n}$

Proof. Assume that $X = x_1 + x_2 y + \cdots + x_n y^{n-1}$ and $Y = y_1 + y_2 y + \cdots + y_n y^{n-1}$. Clearly,

$$(x_1, \ldots, x_n)\mathbf{M}_n = (X, X^q, \ldots, X^{q^{n-1}}),$$

and

$$\begin{aligned} (x_1, \ldots, x_n, y_1, \ldots, y_n)\mathbf{M}_{2n} &= ((x_1, \ldots, x_n)\mathbf{M}_n, (y_1, \ldots, y_n)\mathbf{M}_n \\ &= (X, X^q, \ldots, X^{q^{n-1}}, Y, Y^q, \ldots, Y^{q^{n-1}}). \end{aligned}$$

Consequently,

$$\begin{aligned} \varphi_2(X, Y) &= (\varphi(X), \varphi(Y)) \\ &= (x_1, \ldots, x_n, y_1, \ldots, y_n) \\ &= (X, X^q, \ldots, X^{q^{n-1}}, Y, Y^q, \ldots, Y^{q^{n-1}})\mathbf{M}_{2n}^{-1} \end{aligned}$$

and its inverse

$$\varphi_2^{-1}(x_1, \ldots, x_{2n}) = (X_1, X_{n+1}),$$

where $(X_1, \ldots, X_{2n}) = (x_1, \ldots, x_{2n})\mathbf{M}_{2n}$ □

In the following, we use the change of basis matrix $\mathbf{M}_{2n}$ to show that, if the elements $\alpha_1, \ldots, \alpha_{2n}$, $\beta_1, \ldots, \beta_{2n}$ are chosen following a uniform distribution, then the probability that L is invertible is equal to the probability that a uniformly chosen matrix $A \in \mathcal{M}_{2n\times 2n}(\mathbb{F})$ is invertible. This implies that, given an instance of ZHFE with a high probability there is an equivalent key such that the matrices associated with the core polynomials are of low rank. First we show that if L is as above, then $\varphi_2 \circ L \circ \varphi_2^{-1}$ is a linear transformation from $\mathbb{F}^{2n}$ to $\mathbb{F}^{2n}$, and explicitly reveal the shape of its matrix.

Proposition 3.1.3. *Let $\alpha_1, \ldots, \alpha_{2n}$, $\beta_1, \ldots, \beta_{2n}$ be elements in $\mathbb{K}$, L be the function from $\mathbb{K}^2$ to $\mathbb{K}^2$ given by $L(X, Y) = (L_1(X, Y), L_2(X, Y))$, with*

$$L_1(X, Y) = \sum_{i=1}^{n} \alpha_i X^{q^{i-1}} + \sum_{i=1}^{n} \beta_i Y^{q^{i-1}},\ L_2(X, Y) = \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}}.$$

It holds that $\varphi_2 \circ L \circ \varphi_2^{-1}$ is a linear transformation with matrix associated $\boldsymbol{M}_{2n}\boldsymbol{J}\boldsymbol{M}_{2n}^{-1}$, where

$$\boldsymbol{J} = \begin{pmatrix} \alpha_1 & \alpha_n^q & \dots & \alpha_2^{q^{n-1}} & \alpha_{n+1} & \alpha_{2n}^q & \dots & \alpha_{n+2}^{q^{n-1}} \\ \alpha_2 & \alpha_1^q & & \alpha_3^{q^{n-1}} & \alpha_{n+2} & \alpha_{n+1}^q & & \alpha_{n+3}^{q^{n-1}} \\ & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ \alpha_n & \alpha_{n-1}^q & \dots & \alpha_1^{q^{n-1}} & \alpha_{2n} & \alpha_{2n-1}^q & \dots & \alpha_{n+1}^{q^{n-1}} \\ \beta_1 & \beta_n^q & \dots & \beta_2^{q^{n-1}} & \beta_{n+1} & \beta_{2n}^q & \dots & \beta_{n+2}^{q^{n-1}} \\ \beta_2 & \beta_1^q & & \beta_3^{q^{n-1}} & \beta_{n+2} & \beta_{n+1}^q & & \beta_{n+3}^{q^{n-1}} \\ & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ \beta_n & \beta_{n-1}^q & \dots & \beta_1^{q^{n-1}} & \beta_{2n} & \beta_{2n-1}^q & \dots & \beta_{n+1}^{q^{n-1}} \end{pmatrix}$$

Proof. Suppose that $\varphi_2 \circ L \circ \varphi_2^{-1}(\underline{x}, \underline{y}) = (z_1, \dots, z_{2n})$ and set $X = x_1 + x_2 y + \cdots + x_n y^{n-1}$, $Y = y_1 + y_2 y + \cdots + y_n y^{n-1}$, $Z_1 = z_1 + z_2 y + \cdots + z_n y^{n-1}$ and $Z_2 = z_{n+1} + z_{n+2} y + \cdots + z_{2n} y^{n-1}$, so that $L(X, Y) = (Z_1, Z_2)$. Then, from the definition of L

$$(Z_1, Z_2) = \left(\sum_{i=1}^{n} \alpha_i X^{q^{i-1}} + \sum_{i=1}^{n} \beta_i Y^{q^{i-1}}, \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}} \right),$$

and clearly, for each integer k, $0 \leq k < n$,

$$\left(Z_1^{q^k}, Z_2^{q^k} \right) = \left(\sum_{i=1}^{n} \alpha_{i-k}^{q^k} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{i-k}^{q^k} Y^{q^{i-1}}, \sum_{i=1}^{n} \alpha_{n+(i-k)}^{q^k} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+(i-k)}^{q^k} Y^{q^{i-1}} \right).$$

Equivalently,

$$Z_1^{q^k} = \left(X, \dots, X^{q^{n-1}}, Y, \dots, Y^{q^{n-1}} \right) \begin{pmatrix} \alpha_{1-k}^{q^k} \\ \vdots \\ \alpha_{n-k}^{q^k} \\ \beta_{1-k}^{q^k} \\ \vdots \\ \alpha_{n-k}^{q^k} \end{pmatrix}, \text{ and}$$

$$Z_2^{q^k} = \left(X, \dots, X^{q^{n-1}}, Y, \dots, Y^{q^{n-1}} \right) \begin{pmatrix} \alpha_{n+(1-k)}^{q^k} \\ \vdots \\ \alpha_{n+(n-k)}^{q^k} \\ \beta_{n+(1-k)}^{q^k} \\ \vdots \\ \alpha_{n+(n-k)}^{q^k} \end{pmatrix},$$

where the index operation $i - k$ is modulo n if $i - k \neq 0$, else $i - j$ is equal to n. From the previous equation we get that

$$(Z_1, \dots, Z_1^{q^{n-1}}, Z_2, \dots, Z_2^{q^{n-1}}) = (X, \dots, X^{q^{n-1}}, Y, \dots, Y^{q^{n-1}})\mathbf{J}.$$

Furthermore, we know that

$$\begin{aligned}(z_1, \dots z_{2n})\,\mathbf{M}_{2n} &= \left(Z_1, \dots, Z_1^{q^{n-1}}, Z_2, \dots, Z_2^{q^{n-1}}\right), \\ (x_1, \dots x_n, y_1, \dots y_n)\,\mathbf{M}_{2n} &= \left(X, \dots, X^{q^{n-1}}, Y, \dots, Y^{q^{n-1}}\right).\end{aligned}$$

Putting everything together, we get

$$\begin{aligned}(z_1, \dots z_{2n})\,\mathbf{M}_{2n} &= \left(Z_1, \dots, Z_1^{q^{n-1}}, Z_2, \dots, Z_2^{q^{n-1}}\right) \\ &= \left(X, \dots, X^{q^{n-1}}, Y, \dots, Y^{q^{n-1}}\right)\mathbf{J} \\ &= (x_1, \dots x_n, y_1, \dots y_n)\,\mathbf{M}_{2n}\mathbf{J}.\end{aligned}$$

Therefore, $(z_1, \dots z_{2n}) = (x_1, \dots x_n, y_1, \dots y_n)\,\mathbf{M}_{2n}\mathbf{J}\mathbf{M}_{2n}^{-1}$ □

By Proposition 3.1.3, we know that $\varphi_2 \circ L \circ \varphi_2^{-1}$ is a linear transformation with associated matrix $\mathbf{M}_{2n}\mathbf{J}\mathbf{M}_{2n}^{-1}$. Since $\mathbf{M}_{2n}$ is an invertible matrix, L is an invertible function if and only if $\mathbf{M}_{2n}\mathbf{J}\mathbf{M}_{2n}^{-1}$ is an invertible matrix over $\mathbb{F}$. Even more, the map from the set of functions like L to $\mathcal{M}_{2n\times 2n}(\mathbb{F})$, given by $L \mapsto \mathbf{M}_{2n}\mathbf{J}\mathbf{M}_{2n}^{-1}$ is clearly a bijection. Therefore, the number of invertible functions like L is equal to the number of invertible matrices in $\mathcal{M}_{2n\times 2n}(\mathbb{F})$. As a direct consequence of the last analysis we have the next theorem.

Teorema 3.1.4. *If $\alpha_1, \dots, \alpha_{2n}$, $\beta_1, \dots, \beta_{2n} \in \mathbb{K}$ are chosen uniformly, the probability that L defined by*

$$L(X, Y) = (\sum_{i=1}^{n} \alpha_i X^{q^{i-1}} + \sum_{i=1}^{n} \beta_i Y^{q^{i-1}}, \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}})$$

is invertible, is given by

$$\frac{\prod_{i=0}^{2n-1}(q^{2n} - q^i)}{q^{4n^2}}$$

Proof. The number of invertible matrices in $\mathcal{M}_{2n\times 2n}(\mathbb{F})$ is $\prod_{i=0}^{2n-1}(q^{2n} - q^i)$. The total number of matrices in $\mathcal{M}_{2n\times 2n}(\mathbb{F})$ is q^{4n^2}. □

The principal conclusion in this section is that given an instance for ZHFE with private key (G, S, T), with a high probability there is an equivalent key (G', S, T') such that the matrices associated with the polynomials in G' have low rank.

3.2 Finding a low rank core polynomial

In the previous section we saw that, with high probability a ZFHE public key P has at least one private key (G', S, T') such that the matrices associated with the polynomials in G' have low rank. The principal goal in this section is to explain how from P, we can get one of those private keys.

Let P be a ZHFE public key with low rank core polynomial, e.g.

$$P = T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S,$$

where $G = (F, \tilde{F})$, and the matrices $\mathbf{F}$, $\tilde{\mathbf{F}}$ associated with F, $\tilde{F}$ have low rank ($r+1$, with $r = \lceil \log_q D \rceil$). Let $\mathbf{F}^{*k} \in \mathcal{M}_{n\times n}(\mathbb{F})$ be the matrix associated with the k-th Frobenius power of the polynomial F.

Proposition 3.2.1. *Let $\boldsymbol{F} = [a_{i,j}]$ be the matrix associated with an HFE polynomial F. Then, the (i,j)-th element in $\boldsymbol{F}^{*k}$ is $a_{i-k,j-k}^{q^k}$ (indexes are modulo n).*

Now we use the property on the matrices $\mathbf{M}_n$ and $\mathbf{M}_{2n}$ to deduce a useful relation between the matrices associated with the secret polynomials $\varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1}$ and the matrices $\mathbf{F}^{*k\prime}$s. The following Lemma is very similar to Lemma 2 in [3], the only difference is that here we use φ^{-1} instead of φ_2^{-1}.

Lemma 3.2.2. *Let $(\boldsymbol{H}_1, \ldots, \boldsymbol{H}_{2n}) \in (\mathcal{M}_{2n\times 2n}(\mathbb{F}))^{2n}$ be the matrices associated with the secret quadratic polynomials $\varphi_2 \circ G \circ \varphi^{-1} = (h_1, \ldots, h_{2n}) \in (\mathbb{F}[x_1, \ldots, x_n])^{2n}$, i.e. $h_i = \underline{x}\boldsymbol{H}_i\underline{x}^t$ for all i, $1 \le i \le n$. It holds that*

$$(\boldsymbol{H}_1, \ldots, \boldsymbol{H}_{2n}) = (\boldsymbol{M}_n\boldsymbol{F}^{*0}\boldsymbol{M}_n^{-1}, \ldots, \boldsymbol{M}_n\boldsymbol{F}^{*n-1}\boldsymbol{M}_n^{-1}, \boldsymbol{M}_n\tilde{\boldsymbol{F}}^{*0}\boldsymbol{M}_n^{-1}, \ldots, \boldsymbol{M}_n\tilde{\boldsymbol{F}}^{*n-1}\boldsymbol{M}_n^{-1})\boldsymbol{M}_{2n}^{-1}$$

Proof. Let $\underline{v} = (v_1, \ldots, v_n)$ be an element in $\mathbb{F}^n$. Since $(h_1, \ldots, h_{2n}) = \varphi_2 \circ G \circ \varphi^{-1}$,

$$\begin{aligned}(h_1(\underline{v}), \ldots, h_{2n}(\underline{v})) &= \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1}(\underline{v}) \\ &= \varphi_2(F(\varphi^{-1}(\underline{v})), \tilde{F}(\varphi^{-1}(\underline{v}))) \\ &= (F^{q^0}(\varphi^{-1}(\underline{v})), \ldots, F^{q^{n-1}}(\varphi^{-1}(\underline{v})), \tilde{F}^{q^0}(\varphi^{-1}(\underline{v})), \ldots, \tilde{F}^{q^{n-1}}(\varphi^{-1}(\underline{v})))\mathbf{M}_{2n}^{-1}.\end{aligned}$$

If $V = \varphi^{-1}(\underline{v})$ and $\underline{V} = \underline{v}\mathbf{M}_n$, then

$$(\underline{v}\mathbf{H}_1\underline{v}^t, \ldots, \underline{v}\mathbf{H}_{2n}\underline{v}^t) = (\underline{V}\mathbf{F}^{*0}\underline{V}^t, \ldots, \underline{V}\mathbf{F}^{*n-1}\underline{V}^t, \underline{V}\tilde{\mathbf{F}}^{*0}\underline{V}^t, \ldots, \underline{V}\tilde{\mathbf{F}}^{*n-1}\underline{V}^t)\mathbf{M}_{2n}^{-1}.$$

Since $\underline{V}^t = \mathbf{M}_n^t\underline{v}^t$, we have

$$(\mathbf{H}_1, \ldots, \mathbf{H}_{2n}) = (\mathbf{M}_n\mathbf{F}^{*0}\mathbf{M}_n^t, \ldots, \mathbf{M}_n\mathbf{F}^{*n-1}\mathbf{M}_n^t, \mathbf{M}_n\tilde{\mathbf{F}}^{*0}\mathbf{M}_n^t, \ldots, \mathbf{M}_n\tilde{\mathbf{F}}^{*n-1}\mathbf{M}_n^t)\mathbf{M}_{2n}^{-1}.$$

□

Let $\mathfrak{F} \in (\mathbb{F}[x_1, \ldots, x_n])^{2n}$ be the secret quadratic polynomials, i.e, $\mathfrak{F} = \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1}$. Assume also that $(\mathbf{G}_1, \ldots, \mathbf{G}_{2n}) \in (\mathcal{M}_{n\times n}(\mathbb{F}))^{2n}$ are the matrices associated with the quadratic public polynomials. So,

$$\begin{aligned}P(\underline{x}) &= T(\mathfrak{F}(S(\underline{x}))) \\ (\underline{x}\mathbf{G}_1\underline{x}^t, \ldots, \underline{x}\mathbf{G}_{2n}\underline{x}^t) &= (h_1(\underline{x}\mathbf{S}), \ldots, h_{2n}(\underline{x}\mathbf{S}))\mathbf{T} \\ (\underline{x}\mathbf{G}_1\underline{x}^t, \ldots, \underline{x}\mathbf{G}_{2n}\underline{x}^t) &= (\underline{x}\mathbf{S}\mathbf{H}_1\mathbf{S}^t\underline{x}^t, \ldots, \underline{x}\mathbf{S}\mathbf{H}_{2n}\mathbf{S}^t\underline{x}^t)\mathbf{T}.\end{aligned}$$

So by Lemma 3.2.2,

$$(\mathbf{G}_1, \ldots, \mathbf{G}_{2n})\mathbf{U} = (\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t, \mathbf{W}\tilde{\mathbf{F}}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\tilde{\mathbf{F}}^{*n-1}\mathbf{W}^t), \tag{3.1}$$

where, $\mathbf{W} = \mathbf{S}\mathbf{M}_n \in \mathcal{M}_{n\times n}(\mathbb{K})$ and $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{2n} \in \mathcal{M}_{2n\times 2n}(\mathbb{K})$. If $\mathbf{U} = [u_{i,j}]$, by (3.1) we get the following useful equations

$$\sum_{i=0}^{2n-1} u_{i,0}\mathbf{G}_{i+1} = \mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t = \mathbf{W}\mathbf{F}\mathbf{W}^t,\ \sum_{i=0}^{2n-1} u_{i,n}\mathbf{G}_{i+1} = \mathbf{W}\tilde{\mathbf{F}}^{*0}\mathbf{W}^t = \mathbf{W}\tilde{\mathbf{F}}\mathbf{W}^t. \tag{3.2}$$

Since $\mathbf{F}$, $\tilde{\mathbf{F}}$ have rank $r+1$ and $\mathbf{W}$ is an invertible matrix, the rank of $\mathbf{W}\mathbf{F}\mathbf{W}^t$ is also $r+1$ (similarly for $\tilde{\mathbf{F}}$). Consequently, the last equation implies that the vectors $(u_{0,0}, \ldots, u_{2n-1,0})$ and $(u_{0,n}, \ldots, u_{2n-1,n})$ are solutions for the MinRank problem associated with the public symmetric matrices $(\mathbf{G}_1, \ldots, \mathbf{G}_{2n})$ and the integer $r+1$. Therefore, if we solve that MinRank problem we get the matrix associated with a linear combination of the Frobenius powers of F and $\tilde{F}$ composed with $\varphi^{-1} \circ S$. More precisely, we have the next result.

Teorema 3.2.3. *Given a ZHFE public key $P = T \circ \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S$. We can find the matrix associated with a polynomial in the form*

$$\mathsf{F} \circ \varphi^{-1} \circ S,$$

where F is a linear combination of the Frobenius power for F and $\tilde{F}$.

Proof. We know that the MinRank problem associated with the public matrices $(\mathbf{G}_1, \ldots, \mathbf{G}_{2n})$ and the integer $r+1$ has at least one solution. So, by solving the MinRank problem we can find scalars $u'_0, \ldots, u'_{2n-1}$ in the big field such that

$$\operatorname{Rank}\left(\sum_{j=0}^{2n-1} u'_j\mathbf{G}_{j+1}\right) \leq r+1.$$

On the other hand, if $\mathbf{U}^{-1} = [u^{-1}_{i,j}]$, by equation (3.2) we have that

$$\mathbf{G}_{j+1} = \sum_{i=0}^{n-1} u^{-1}_{i,j}(\mathbf{W}\mathbf{F}^{*i}\mathbf{W}^t) + \sum_{i=0}^{n-1} u^{-1}_{i+n,j}(\mathbf{W}\tilde{\mathbf{F}}^{*i}\mathbf{W}^t) = \mathbf{W}\left(\sum_{i=0}^{n-1} u^{-1}_{i,j}\mathbf{F}^{*i} + \sum_{i=0}^{n-1} u^{-1}_{i+n,j}\tilde{\mathbf{F}}^{*i}\right)\mathbf{W}^t.$$

Therefore,

$$\begin{aligned}
\mathbf{G}' &= \sum_{j=0}^{2n-1} u'_j \mathbf{G}_{j+1} \\
&= \sum_{j=0}^{2n-1} u'_j \mathbf{W} \left(\sum_{i=0}^{n-1} u_{i,j}^{-1} \mathbf{F}^{*i} + \sum_{i=0}^{n-1} u_{i+n,j}^{-1} \tilde{\mathbf{F}}^{*i} \right) \mathbf{W}^t \\
&= \sum_{j=0}^{2n-1} \mathbf{W} \left(u'_j \sum_{i=0}^{n-1} u_{i,j}^{-1} \mathbf{F}^{*i} + u'_j \sum_{i=0}^{n-1} u_{i+n,j}^{-1} \tilde{\mathbf{F}}^{*i} \right) \mathbf{W}^t \\
&= \mathbf{W} \sum_{j=0}^{2n-1} \left(u'_j \sum_{i=0}^{n-1} u_{i,j}^{-1} \mathbf{F}^{*i} + u'_j \sum_{i=0}^{n-1} u_{i+n,j}^{-1} \tilde{\mathbf{F}}^{*i} \right) \mathbf{W}^t \\
&= \mathbf{W} \left[\sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} u'_j u_{i,j}^{-1} \right) \mathbf{F}^{*i} + \sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} u'_j u_{i+n,j}^{-1} \right) \tilde{\mathbf{F}}^{*i} \right] \mathbf{W}^t \\
&= \mathbf{S}\mathbf{M}_n \left[\sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} u'_j u_{i,j}^{-1} \right) \mathbf{F}^{*i} + \sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} u'_j u_{i+n,j}^{-1} \right) \tilde{\mathbf{F}}^{*i} \right] \mathbf{M}_n^t \mathbf{S}^t.
\end{aligned}$$

And finally, define F as the polynomial with coefficient in the big field $\mathbb{K}$ given by the symmetric matrix

$$\sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} u'_j u_{i,j}^{-1} \right) \mathbf{F}^{*i} + \sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} u'_j u_{i+n,j}^{-1} \right) \tilde{\mathbf{F}}^{*i}$$

. □

By Theorem 3.2.3 and equation (3.2), we could find another low rank linear combination $\tilde{G}$ of the public matrices $(\mathbf{G}_1, \ldots, \mathbf{G}_{2n})$ such that the polynomial with associated matrix $\tilde{G}$ is in the form $\tilde{\mathsf{F}} \circ \varphi^{-1} \circ S$. This may represent a weakness of ZHFE.

Recently, in parallel with our work and independetly, Perlner and Smith-Tone analyzed the security of ZHFE [10]. They argue that if $L_{11} = \sum_{i=1}^{n} \alpha_i X^{q^{i-1}}$, $L_{12} = \sum_{i=1}^{n} \beta_i Y^{q^{i-1}}$, $L_{21} = \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}}$ and $L_{22} = \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}}$ are chosen so that each $\varphi \circ L_{ij} \circ \varphi^{-1}$ has corank s greater than zero, then the rank of the matrix associated with $L_i(F, \tilde{F})$ is $2s$, and with this simple restriction on the L_{ij} maps is enough to avoid a MinRank attack. They assure, that this is the case because the complexity of the attack is exponential in the rank of the matrix associate with $L_i(F, \tilde{F})$.

Chapter 4

Conclutions and future works

In Chapter 2 we have proposed a novel way to solve the vanishing equation system necessary to construct keys in ZHFE. By exposing its almost-block diagonal structure, we unleashed a series of improvements in ZHFE key generation. We can now construct the matrix associated with the system faster, and store it more efficiently. Moreover, we can find solutions to the system asymptotically faster. These improvements turn ZHFE from an only theoretical proposal, into a viable Post-Quantum public key encryption scheme.

We think that future improvements are possible in ZHFE derived from this work. In Section 2.3, we exposed the structure by blocks of the L_i matrices in Algorithm 1. We believe that it is possible to exploit its structure to compute the set W faster.

In Chapter 3 we have found out that given a ZHFE pulic key P, if the function L is invertible, there exist two affine transformations T' and S' and a core polynomials F', $\tilde{F}'$ with associated matrix of low rank shuch that $P = T' \circ \varphi_2 \circ (F', \tilde{F}') \circ \varphi^{-1} \circ S'$. We also showed that L is invertible with very high probability. Then we show that it is possible to extract a linear combination of the public matrices from the public key, whereby we can get T'.

As future works, we consider interesting studying if it is possible to find both affine transformations T' and S from the public key. Also, verify if with the resulting HFE core polynomials F' and $\tilde{F}'$ we can bulit a polynomial as Ψ of low degree. Finally, a crucial question is whether it is posible to prevent this attack by choosing the function L not invertible.

Bibliography

[1] Baena, J., Cabarcas, D., Escudero, D., Porras, J., Verbel, J.: Efficient ZHFE key generation. In: Post-Quantum Cryptography - 7th International Conference, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016. Proceedings (2016), accepted for publication

[2] Bernstein, D.J., Buchmann, J., Dahmen, E.: Post-Quantum Cryptography. Springer Publishing Company, Incorporated, 1st edn. (2008)

[3] Bettale, L., Faugère, J.C., Perret, L.: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Designs, Codes and Cryptography 69(1), 1–52 (2013)

[4] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24(3-4), 235–265 (1997), http://dx.doi.org/10.1006/jsco.1996.0125, computational algebra and number theory (London, 1993)

[5] Ding, J., Gower, J.E., Schmidt, D.S.: Multivariate public key cryptosystems, Advances in Information Security, vol. 25. Springer, New York (2006)

[6] Garey, M.R., Johnson, D.S.: Computers and Intractability; A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., New York, NY, USA (1990)

[7] Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Advances in cryptology—CRYPTO '99 (Santa Barbara, CA), Lecture Notes in Computer Science, vol. 1666, pp. 19–30. Springer, Berlin (1999)

[8] Lids, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge Univesity Pres, New York (1986)

[9] Patarin, J.: Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms. In: Maurer, U. (ed.) Advances in Cryptology—EUROCRYPT 96. Lecture Notes in Computer Science, vol. 1070, pp. 33–48. Springer-Verlag (1996)

[10] Perlner, R.A., Smith-Tone, D.: Security analysis and key modification for ZHFE. In: Post-Quantum Cryptography - 7th International Conference, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016. Proceedings (2016), accepted for publication

[11] Porras, J., Baena, J., Ding, J.: ZHFE, a new multivariate public key encryption scheme. In: Mosca, M. (ed.) Post-Quantum Cryptography, Lecture Notes in Computer Science, vol. 8772, pp. 229–245. Springer International Publishing (2014)

[12] Porras, J., Baena, J., Ding, J.: New candidates for multivariate trapdoor functions. Revista Colombiana de Matemáticas 49, 57–76 (06 2015)

[13] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 41(2), 303–332 (electronic) (1999)

[14] Stamp, M.: Information Security: Principles and Practice. Wiley Publishing, New York (2011)