Efficient ZHFE Key Generation

John B. Baena[1], Daniel Cabarcas[1], Daniel E. Escudero[1],
Jaiberth Porras-Barrera[2], and Javier A. Verbel[1](✉)

[1] Universidad Nacional de Colombia, Sede Medellín, Medellín, Colombia
{jbbaena,dcabarc,deescuderoo,javerbelh}@unal.edu.co
[2] Facultad de Ingeniería, Tecnológico de Antioquia, Medellín, Colombia
jporras6@tdea.edu.co

Abstract. In this paper we present a new algorithm to construct the keys of the multivariate public key encryption scheme ZHFE. Constructing ZHFE's trapdoor involves finding a low degree polynomial of q-Hamming-weight-three, as an aid to invert a pair of q-Hamming-weight-two polynomials of high degree and high rank. This is done by solving a large sparse linear system of equations. We unveil the combinatorial structure of the system in order to reveal the hidden structure of the matrix associated with it. When the system's variables and equations are organized accordingly, an almost block diagonal shape emerges. We then exploit this shape to solve the system much faster than when ZHFE was first proposed. The paper presents the theoretical details explaining the structure of the matrix. We also present experimental data that confirms the notable improvement of the key generation complexity, which makes ZHFE more suitable for practical implementations.

Keywords: Multivariate public key cryptography · Encryption schemes · ZHFE · Block diagonal matrix

1 Introduction

The eventual construction of large quantum computers has triggered the creation and development of research in Post-Quantum Cryptography (PQC) [1]. PQC is the branch of cryptography that is dedicated to the study of cryptosystems that have the potential to resist quantum computer attacks. If such computers were built, Shor's algorithm could be used to factorize integers and solve the Discrete Logarithm Problem (DLP) in polynomial time [14]. This scenario would annihilate most of our current security protocols, causing a worldwide catastrophe.

Multivariate Public Key Cryptography (MPKC) [4] is an appealing Post-Quantum alternative. The public key in an MPKC is usually a set of multivariate quadratic polynomials over a finite field. A direct attack is to solve a system of multivariate quadratic equations. Solving a random such system is an $\mathcal{NP}$-hard problem [8], and at the moment there is no known quantum algorithm that can solve this problem efficiently. On the other hand, the computations on MPKC's are usually very efficient.

T. Takagi (Ed.): PQCrypto 2016, LNCS 9606, pp. 213–232, 2016.
DOI: 10.1007/978-3-319-29360-8_14

Although efficient and secure MPK signature schemes do exist (cf. [5]), no MPK encryption scheme has prevailed. One of the most researched alternative for PKC encryption is the HFE cryptosystem, proposed in 1996 by Patarin [10]. The idea behind HFE is to hide a core low degree polynomial over a large field by means of two invertible affine transformations over a small field. The composition of these maps, via a vector space isomorphism, yields the public key polynomials. The restriction on the core polynomial degree is necessary to make decryption possible. However, this restriction introduces a weakness in HFE exploited by Faugère and Joux [7] to break HFE over the binary field through a direct algebraic attack. The case of odd characteristic remained open until Faugère et al. [2] improved the Kipnis-Shamir attack [9] and broke some related HFE schemes.

Porras et al. [13] recently proposed an alternative to avoid both the direct algebraic attack [6] and the Kipnis-Shamir attack [2]. They proposed a reduction method to construct and invert pairs of q-Hamming-weight-two polynomials of high degree and high rank. Using these polynomials they introduced a new family of multivariate trapdoor functions. The trapdoor information includes a low degree polynomial Ψ of q-Hamming weight three, used to invert the multivariate trapdoor function consisting of two polynomials F and $\tilde{F}$ of q-Hamming weight two. The polynomial Ψ is a linear combination of Frobenius powers of F and $\tilde{F}$ lifted to q-Hamming weight three by multiplying by X and X^q. Ψ can be found by solving a large sparse linear system of equations resulting from vanishing the high degree terms.

Based on the new trapdoor function, they proposed an HFE-type encryption scheme named ZHFE [12]. They presented theoretical and practical evidence that supports their claim that ZHFE resists the main attacks against this kind of schemes, namely, the direct algebraic attack [6] and the Kipnis-Shamir attack [2]. They also showed that encryption and decryption speed are comparable with their counterparts in the HFE challenge 1 [10]. The main drawback of ZHFE is that the vanishing equation system is very large. Solving it directly requires a lot of time and memory. This situation represents an obstacle to consider ZHFE for practical security protocols.

Our Contribution

In this paper we propose a new method for generating the ZHFE private key efficiently. The main idea of this method is to conveniently sort the variables and equations of the vanishing equation system coming from the reduction method introduced in [12,13], in order to unveil its hidden structure. With this suitable order, the matrix associated with this system presents a shape close to a block diagonal matrix, as shown in Fig. 1.

The math required to expose the matrices' hidden structure is important in its own right. We carefully explain the combinatorial structure of Frobenius powers of q-Hamming-weight-two univariate polynomials. We explain how they match and mismatch when raised to q-Hamming weight three through multiplication by q-Hamming-weight-one monomials.

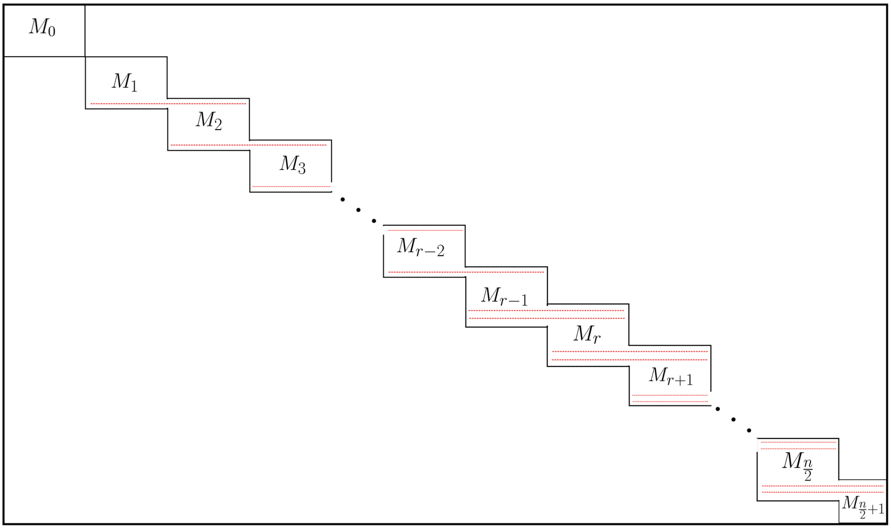

Fig. 1. Hidden structure of the matrix associated with the system $\mathcal{S}$.

Understanding the vanishing equation system leads in the first place to a direct and fast algorithm to construct its matrix. Moreover, we propose an algorithm to solve the vanishing equation system very efficiently. More precisely, the algorithm finds an element in the null space of an almost block diagonal matrix over a finite field. We improved the asymptotic complexity from $\mathcal{O}(n^{3\omega})$ in a naive approach to $\mathcal{O}(n^{2\omega+1})$, where n is the number of variables of the public ZHFE polynomials and $2 \leq \omega \leq 3$ is a constant that depends on the specific Gaussian elimination algorithm used. Moreover, for practical parameters, our experiments show that the proposed key generation algorithm is much faster than the one proposed in [12,13]. We reduced key generation time from a couple of days to only a few minutes.

Another important contribution of this paper is that the new method for solving the vanishing equation system does not require as much memory as the method used in [12,13]. This is because we do not need to work with the complete matrix of Theorem 2, but instead we now work with each block separately. Moreover, once a block is used, it can be deleted, thus in total we are significantly reducing the memory usage.

All these improvements turn ZHFE into an interesting alternative as a Post-Quantum public key encryption scheme.

The paper is organized as follows. In Sect. 2, we review the main features of the ZHFE encryption scheme. In Sect. 3, we present the new method for solving the vanishing equation system, and in Sect. 4, we discuss the complexity of the new method and present experimental data that confirms the efficiency of the new algorithm. In Sect. 5 we discuss some remarks about security, and we finalize giving some conclusions in Sect. 6.

2 The ZHFE Encryption Scheme

The authors in [13] introduced a special reduction method to construct new candidates for multivariate trapdoor functions using q-Hamming-weight-two polynomials of high degree and high rank. The idea of their construction is as follows. Let n be a positive integer, $\mathbb{F}$ a finite field of size q, and $g(y) \in \mathbb{F}[y]$ a degree n irreducible polynomial. Consider the field extension $\mathbb{K} = \mathbb{F}[y]/\left(g(y)\right)$ and the vector space isomorphism $\varphi\colon \mathbb{K} \to \mathbb{F}^n$ defined by $\varphi\left(u_1 + u_2 y + \ldots + u_n y^{n-1}\right) = (u_1, u_2, \ldots, u_n)$. Take two HFE polynomials over $\mathbb{K}$ of the form

$$\begin{aligned} F(X) &= \sum a_{ij} X^{q^i+q^j} + \sum b_i X^{q^i} + c, \text{ and} \\ \tilde{F}(X) &= \sum \tilde{a}_{ij} X^{q^i+q^j} + \sum \tilde{b}_i X^{q^i} + \tilde{c}. \end{aligned}$$

Denote by $F_0, F_1, \cdots, F_{n-1}$ the Frobenius powers of F, and by $\tilde{F}_0, \tilde{F}_1, \cdots, \tilde{F}_{n-1}$ the Frobenius powers of $\tilde{F}$. Let Ψ_0 and Ψ_1 be the q-Hamming-weight-three polynomials defined by

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

Fix a positive integer D such that every univariate polynomial equation over $\mathbb{K}$ of degree less than D is solved efficiently using Berlekamp's algorithm. Choose the scalars $\alpha_i, \beta_i \in \mathbb{K}$ uniformly at random. Then, determine coefficients $a_{ij}, b_i, c, \tilde{a}_{ij}, \tilde{b}_i, \tilde{c} \in \mathbb{K}$, such that the q-Hamming-weight-three polynomial $\Psi = \Psi_0 + \Psi_1$ has degree less than D. This leads to a sparse linear equation system over the small field $\mathbb{F}$ with more variables than equations and thus with nontrivial solutions. This vanishing equation system has about n^3 variables, so finding its solution via the Gaussian elimination process has complexity $\mathcal{O}(n^{3\omega})$, where $2 \leq \omega \leq 3$ is a constant that depends on the specific Gaussian elimination algorithm used.

The multivariate trapdoor function is built in a similar way as the HFE public key is constructed. Choose $G = (F, \tilde{F})$ as the core map, and then select two invertible affine transformations $S : \mathbb{F}^n \to \mathbb{F}^n$ and $T : \mathbb{F}^{2n} \to \mathbb{F}^{2n}$. The multivariate trapdoor function is the map $P : \mathbb{F}^n \to \mathbb{F}^{2n}$ given by

$$P(x_1, \cdots, x_n) = \left(T \circ (\varphi \times \varphi) \circ G \circ \varphi^{-1} \circ S\right)(x_1, \cdots, x_n).$$

Porras et al. used this multivariate trapdoor function to introduce a new encryption scheme named ZHFE [12]. The ZHFE public key includes the field $\mathbb{F}$ and its structure, and the trapdoor function $P(x_1, \cdots, x_n)$. The private key includes the low degree polynomial Ψ, the two invertible affine transformations S and T, and the scalars $\alpha_1, \cdots, \alpha_{2n}, \beta_1, \cdots, \beta_{2n}$. The inversion of the core map G is accomplished by means of the low degree polynomial Ψ, the scalars $\alpha_1, \cdots, \alpha_{2n}, \beta_1, \cdots, \beta_{2n}$, and Berlekamp's algorithm.

3 New Method

In this section 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.

3.1 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 and independent and much simpler system. For $k \in \{0, \dots, \frac{n}{2}\}$ let $\mathcal{A}_k$ be the subset of $\mathbb{Z}_n \times \mathbb{Z}_n$

$$\mathcal{A}_k := \begin{cases} \{(i, (k+i) \mod n) |\ 0 \leq i < n\} & \text{if } 0 \leq k < \frac{n}{2}, \\ [5pt]\ \{(i, k+i) |\ 0 \leq i < \frac{n}{2}\} & \text{if } k = \frac{n}{2}. \end{cases}$$

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

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

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

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

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

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

Proof.

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

So, by iterating this ℓ times, we obtain

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

Using the notation for the ℓ−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.

Corollary 1. *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*

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

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 1. *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. *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:*

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

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

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

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

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 1, the coefficient of $X^{q^0+q^1+q^j}$ in Ψ_0 is

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

By Lemma 1, 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 1 is

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

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

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

i.e.,

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

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 1, the coefficient of $X^{q^0+q^1+q^{\frac{n}{2}+1}}$ in Ψ_0 is

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

By Lemma 1, 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 1, its coefficient is

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

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

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

i.e.,

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

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 $Z_{2nk+pn+(i\ominus\ell)}^{q^\ell}$, 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.

Theorem 1. *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 with $\mathcal{S}$ so that it has the form shown in Fig. 1, and for $0 \leq k \leq \frac{n}{2}$, the size of the submatrix M_k is $a \times b$, with*

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

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.

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

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 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 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 contain only variables associated with $\mathcal{A}_{\frac{n}{1}-1}$ and $\mathcal{A}_{\frac{n}{2}-1}$.

According to Lemma 1 and Corollary 1, 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 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 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

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

Therefore, $(n - (r - 1), 0), (n - (r - 1) + 1, 1) \in \mathcal{A}_{r-1}$ and, by Proposition 2, 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 $\mathcal{A}_{\frac{n}{2}}$.

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 1. The conditions $1 < r < \frac{n}{2}$ and $q + 2q^{r-1} < D \leq q^r$ in Theorem 1 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 [12] 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 1.

Table 1. Possible values of D for $q = 7$ and $n = 56$.

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	$343 < D \leq 2401$	$693 < D \leq 2401$

3.2 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

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

We can see the expression in (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

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

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

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

is as shown in Fig. 2.

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

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

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

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

The matrix that represents the $\mathbb{F}$-linear transformation

$$T_{\frac{n}{2}} = (T^{\frac{n}{2}}_{0,1}, \ldots, T^{\frac{n}{2}}_{0,\frac{n}{2}-1}, T^{\frac{n}{2}}_{1,0}, \ldots, T^{\frac{n}{2}}_{1,\frac{n}{2}-1})$$

is presented in Fig. 3.

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

Fig. 3. Matrix representation of $T_{\frac{n}{2}} : \mathbb{K}^n \rightarrow \mathbb{K}^n$.

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 1 explains the hidden structure of the matrix associated with $\mathcal{S}$. We now consider $\mathcal{S}$ with the order given in Theorem 1, 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 $\mathcal{S}$.

Theorem 2. *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. 1. For $0 \leq i \leq \frac{n}{2}$, the size of the submatrix $\tilde{M}_i$ is $a \times b$, where*

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

Remark 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.

Remark 3. The submatrices $\tilde{M}_0, \ldots, \tilde{M}_{\frac{n}{2}}$ are small modifications of the matrix in Fig. 2. More precisely, for $r \le k < \frac{n}{2}$, $\tilde{M}_k$ can be obtained simply by permuting the rows of the matrix in Fig. 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 $0 \le k \le r-1$, $\tilde{M}_k$ 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, 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 Figs. 2 and 3 for all k's, and sort their rows according to Remark 3. Finally, we put them together as described in Theorem 2. However, as we will see in the next subsection, 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.

3.3 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. Then, we will discuss the probability that this algorithm terminates.

As seen in Sect. 3.2, 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 $\tilde{M}_i = \left[\frac{U_i}{L_i}\right]$ (for $i = 1$, we define $U_1 = \tilde{M}_1$). The expression $\mathbf{y} \overset{\$}{\longleftarrow} W$ 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
W := $\left\{\mathbf{z} \mid L_{\frac{n}{2}}\mathbf{z} = \mathbf{0}\right\}$
for $i = \frac{n}{2}, \ldots, 1$ do
    $\mathbf{y}_i \overset{\$}{\longleftarrow} W$
    $\mathbf{r}_i := U_i\mathbf{y}_i$
    $W := \left\{\mathbf{z} \mid L_i\mathbf{z} = \left[\frac{\mathbf{0}}{-\mathbf{r}_i}\right]\right\}$
    if $W = \emptyset$ then
        stop algorithm
$W := \left\{\mathbf{z} \mid \tilde{M}_0\mathbf{z} = \mathbf{0}\right\}$
$\mathbf{y}_0 \overset{\$}{\longleftarrow} W$
return $\mathbf{y} = [\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n}{2}}]^T$
```

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 3. *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 $\mathbf{x} = [x_1, x_2, \ldots, x_t]^T$, with $t = n^2(n+1)$. For $0 < i \leq \frac{n}{2}$, we define $\mathbf{x}_i = [x_{t_{i-1}+1}, x_{t_{i-1}+2}, \ldots, x_{t_i}]^T$, 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

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

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

$$L_i\mathbf{z} = \left[\begin{array}{c}\mathbf{0}\\ \hline -\mathbf{r}_{i+1},\end{array}\right]$$

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

This proposition shows that every element of the null space of $\tilde{M}$ can be output by Algorithm 1. Moreover, the element in the null space is still chosen with uniform distribution. This is because Algorithm 1 obtains each element $\mathbf{x}$ by finding its projections $\mathbf{x}_i$, and this is performed uniformly.

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). For every single instance and for each $i = r, \ldots, \frac{n}{2}$, the matrix L_i was full rank.

Table 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.

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

4 Complexity of the New Method

The new method introduced in this paper to solve the vanishing equation system finds an element in the null space of an almost-block diagonal matrix with $\frac{n}{2} + 1$ blocks, as depicted in Fig. 1. The size of each block is at most $2n^2 \times 2n^2$, so reducing each block to its echelon form has complexity $\mathcal{O}\left(\left(n^2\right)^{\omega}\right)$, 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 $\mathcal{O}\left(n\left(n^2\right)^{\omega}\right) = \mathcal{O}\left(n^{2\omega+1}\right)$. This improves the naive approach used in [12], which costs $\mathcal{O}\left(\left(n^3\right)^{\omega}\right) = \mathcal{O}\left(n^{3\omega}\right)$, 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 [12] for solving the vanishing equation system. We built different ZHFE private keys using both methods. In Table 3 we present these results for different sets of parameters. All the experiments were performed using Magma v2.21-1 [3] 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.

Table 3. Private key generation: comparison between the new and old methods.

Method		New method			Old method		
q	D	n	CPU time [s]	Memory [MB]	n	CPU time [s]	Memory [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[a]	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[a]	226384.28	59658

[a] 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.

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 [12].

5 Remarks About Security

Although a more rigorous study of the security of ZHFE is out of the scope of this paper, this aspect is not affected by the proposed key generation improvement. The matrix $\widetilde{M}$ is simply a rearrangement of the sparse matrix used in the original approach to construct the ZHFE private key. Moreover, Proposition 3 guarantees that the new algorithm would not miss any solution of the system and as remarked in Sect. 3, the solution is chosen under the same uniform distribution. This matrix $\tilde{M}$ has about n^2 free variables, so the size of its null space is about q^{n^2}. This number is huge for practical values of the parameters. Thus, in principle, the unveiled structure of the matrix $\tilde{M}$ does not represent an obvious threat to the security of ZHFE. Nevertheless, this aspect should be considered more deeply and will be part of future research.

The security of ZHFE was studied in detail in [12], and we base the pertinence of this paper on those arguments. Nevertheless, it recently came to our attention new works exposing a rank weakness on the original ZHFE [11,15]. Perlner and Smith-Tone prove that if we write $\Psi(X) = X(L_{11}F + L_{12}\tilde{F}) + X^q(L_{21}F + L_{22}\tilde{F})$, and the L_{ij} maps have full rank, then the rank of ZHFE is no larger than $\lceil \log_q D \rceil + 2$ [11]. They also argue that if we select the L_{ij} maps to have reasonable corank c, then the Q-rank does not appear to be a weakness for ZHFE. They further propose a "minus" modification of ZHFE, called ZHFE$^-$, which adds a projection to the original ZHFE, by removing r polynomials from the public key. They recommend the following parameters for this new proposal:

$$\text{ZHFE}^- : \qquad (q, n, D, r, c) = (7, 55, 105, 2, 6).$$

They claim that with these parameters the public key Q-rank is about 12, and the degree of regularity is estimated to be 9, which implies a security level of at least 80 bits.

We performed extensive experiments to see how our new key generation method behaves for the parameters proposed in [11]. We found that for the parameters $(q, n, D, r, c) = (7, 55, 105, 2, 6)$, both the new and old methods produce only the trivial solution $\Psi(X) = 0$, even though the kernel is not trivial. We also found that for those parameters, c must be chosen in $\{1, 2\}$ for a nontrivial $\Psi(X)$ to exist. Using a different value for q, we realised that for $(q, n, D, r) = (3, 55, 105, 2)$, the corank c must be chosen in $\{1, 2, 3\}$ for a nontrivial $\Psi(X)$ to exist. We also found that if we want to obtain a nontrivial $\Psi(X)$ for $(q, n, D, r) = (3, 55, 170, 2)$, the corank c must be chosen in $\{1, 2, 3, 4\}$. Again, in all these cases both the new and old methods work fine. In order to construct a ZHFE key using L_{ij} maps with corank $c = 6$, the parameter D must be increased. We discovered for instance that the new and old methods work for $(q, n, D, r, c) = (3, 56, 1462, 2, 6)$. Table 4 shows the results of the experiments run for some choices of the parameters.

According to our extensive experiments, we can say that our new algorithm works flawlessly, when we use L_{ij} maps with positive corank, including the case $c = 6$. Moreover, we can say that for any fixed set of parameters, the original method finds a nontrivial $\Psi(X)$ if and only if the new algorithm finds a nontrivial $\Psi(X)$.

Table 4. Computation of ZHFE keys for $(q, D, c) = (3, 1462, 6)$, $(q, D, c) = (3, 490, 5)$ and $(q, D, c) = (3, 170, 4)$. For every generated instance, the algorithm terminated successfully

n	Number of instances
16	400000
32	5000
56	400

6 Conclusions

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.

In order to achieve these, we had to understand the combinatorial structure of Frobenius powers of q-Hamming-weight-two univariate polynomials. We expect this understanding will serve as a tool to explore a bigger family of encryption schemes, i.e., generalizations of ZHFE in which the polynomial Ψ is obtained multiplying by more than two powers of the form X^{q^i}.

We also found that, in terms of success, our new algorithm works just as good as the original method, when considering L_{ij} maps with positive corank, as proposed in [11].

We foresee further improvements in ZHFE derived from this work. Since the vanishing equation system has several free variables, we can fix some variables for all instances of the trapdoor function. Knowing the structure of the matrix allows us to do so in a way that further speeds up key generation, and reduces secret key size.

We must not discard the theoretical results of this paper as a useful tool to get a better understanding of the security of ZHFE.

Acknowledgements. This work was partially supported by “Fondo Nacional de Financiamiento para la Ciencia, la Tecnología y la Innovación Francisco José de Caldas”, Colciencias (Colombia), Project No. 111865842333 and Contract No. 049-2015. We would like to thank Jintai Ding, Ludivic Perret, and Felipe Cabarcas for useful discussions. We would also like to thank the reviewers of PQCrypto 2016 for their constructive reviews and suggestions. And last but not least, we thank the Facultad de Ciencias of the Universidad Nacional de Colombia sede Medellín for granting us access to the Enlace server, where we ran most of the experiments of this paper.

References

1. Bernstein, D.J., Buchmann, J., Dahmen, E.: Post-quantum Cryptography, 1st edn. Springer, Heidelberg (2009)
2. Bettale, L., Faugère, J.C., Perret, L.: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Des. Codes Crypt. **69**(1), 1–52 (2013)
3. 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)
4. Ding, J., Gower, J.E., Schmidt, D.S.: Multivariate Public Key Cryptosystems. AISC, vol. 25. Springer, New York (2006)
5. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005)
6. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F_4). J. Pure Appl. Algebra **139**(1–3), 61–88 (1999). Effective methods in algebraic geometry (Saint-Malo, 1998)
7. Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
8. Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., New York (1990)
9. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
10. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
11. Perlner, R.A., Smith-Tone, D.: Security analysis and key modification for ZHFE. In: Proceedings of the 7th International Conference Post-Quantum Cryptography, PQCrypto 2016, 24–26 February 2016, Fukuoka, Japan (2016, to appear)
12. Porras, J., Baena, J., Ding, J.: ZHFE, a new multivariate public key encryption scheme. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 229–245. Springer, Heidelberg (2014)
13. Porras, J., Baena, J., Ding, J.: New candidates for multivariate trapdoor functions. Rev. Colomb. Matemáticas **49**, 57–76 (2015)
14. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. **41**(2), 303–332 (1999). (Electronic)
15. Zhang, W., Tan, C.H.: Personal communication (2015)