Practical Key Recovery Attack for ZHFE

Daniel Cabarcas[1], Daniel Smith-Tone[2,3], and Javier A. Verbel[1]

[1]Universidad Nacional de Colombia, Sede Medellín, Colombia: dcabarc@unal.edu.co
[2]University of Louisville, USA: daniel-c.smith@louisville.edu
[3]National Institute of Standards and Technology, USA: daniel.smith@nist.gov

Abstract. At PQCRYPTO 2014, Porras, Baena and Ding introduced ZHFE, an interesting new technique for multivariate post-quantum encryption. The scheme is a generalization of HFE in which a single low degree polynomial in the central map is replaced by a pair of high degree degree polynomials with a low degree cubic polynomial contained in the ideal they generate. ZHFE was constructed with the philosophy that a statistically injective multivariate expansion map may have less rigid a structure than a bijection, and may be more resistant to cryptanalysis. We show that in the case of ZHFE, this intuition is false.

We present a practical key recovery attack for ZHFE based on the independent discoveries of the low rank property of ZHFE by Verbel and by Perlner and Smith-Tone. Thus, although the two central maps of ZHFE have high degree, their low rank property makes ZHFE vulnerable to the Kipnis-Shamir(KS) rank attack. We adapt the minors modeling approach to the KS attack pioneered by Bettale, Faugère and Perret in application to HFE, and break ZHFE for practical parameters. Specifically, our attack recovers a private key for ZHFE$(7, 55, 105)$ in approximately 2^{64} operations.

Keywords: Multivariate public key cryptography, encryption schemes, ZHFE

1 Introduction

The fundamental problem of solving systems of nonlinear equations is thousands of years old and has been very influential in the development of algebra and number theory. In the realm of cryptography, the task of solving systems of nonlinear, often quadratic, equations is a principal challenge which is relevant in the analysis of many primitives, both in the symmetric and asymmetric setting. This basic problem is the basis of numerous public key schemes, which, in principle, add to the diversity of public key options. The subdiscipline of cryptography concerned with this family of cryptosystems is usually called Multivariate Public Key Cryptography (MPKC).

In addition to the benefit of creating a more robust toolkit of public key primitives, the advent of MPKC offers a potential solution to the problem of securing communication against quantum adversaries, adversaries with access to a sophisticated quantum computer. Since Peter Shor discovered in the mid

90s, see [27], algorithms for factoring and computing discrete logarithms on a quantum computer, a dedicated community has been emmersed in the challenge of securing data from quantum adversaries. In December 2016 the National Institute of Standards and Technology (NIST) published a call for proposals for post-quantum standards from the international community, putting a figurative spotlight on public key cryptography useful in an era with quantum computing technology. In light of this focus from NIST, the cryptometry and cryptanalysis of post-quantum schemes is not simply an academic matter.

While there are several secure, performant, and well-studied multivariate signature schemes, see [9,5,16,21], for example, there are very few unbroken multivariate encryption schemes in the current cryptonomy. Surprisingly, this general absence of secure and long-lived encryption schemes is primarily due to a small array of extremely effective cryptanalytic techniques.

Broadly, we can categorize attacks on multivariate cryptosystems as either direct algebraic, directly inverting the multivariate public key via Gröbner basis calculation, differential, exploiting some symmetric or invariant structure exhibited by the differential of the private key, or rank, recovering a low rank equivalent private key structure by solving an instance of MinRank, i.e. finding a low rank map in a space of linear maps derived from the public key. These basic tools form the core of modern multivariate cryptanalysis and the algebraic objects related to them are of great interest, not only theoretically, but also for use in cryptometry, see for example, [4,13,6,18,2,22,28,11,7,10].

In the last few years, a few novel techniques for the construction of multivariate encryption schemes have been proposed. The idea is to retain statistical injectivity while relaxing the structure of the public key by doubling the dimension of the codomain. The schemes *ABC* Simple Matrix, and Cubic Simple Matrix, proposed in [30,8], are based on a large matrix algebra over a finite field. The ZHFE scheme, proposed in [25] (with a significant key generation improvement from [1]) is based on high degree polynomials F and $\tilde{F}$ over an extension field. Decryption in the later is possible, by the existence of a low degree polynomial Ψ in the ideal generated by F and $\tilde{F}$.

The *ABC* Simple Matrix and Cubic Simple Matrix encryption schemes have been shown vulnerable to differential attacks, see [18,19]. Moreover, in [23] and independently in [31] a trivial upper bound on the Q-rank, or quadratic rank, of ZHFE is provided, further calling into question whether the design strategy of enlarging the dimension of the codomain of the public key is an effective way of achieving multivariate encryption.

On the other hand, in [32], a new security estimate is provided for the original parameters of ZHFE. The paper not only purports to prove the security of ZHFE against the attack methodology of Kipnis and Shamir on low Q-rank schemes, see [17], it also improves the estimate of the degree of regularity of the public key of ZHFE, indicating that the security level of the original parameters is at least 2^{96} instead of the original claim of 2^{80}. In particular, their bound on the complexity of the KS attack on ZHFE is 2^{138}, placing this attack well out of the realm of possibility.

In this paper, we make the impossible practical. We detail a full key recovery attack, that works with high probability from the public key alone, and test its effectiveness for small parameters. Our attack adapts the techniques first introduced in [17] and later improved in [2], to recover low rank central maps. Furthermore, we show how to recover a low degree polynomial equivalent to Ψ, that can be used to decrypt.

Our complexity analysis of the attack demonstrates that ZHFE is also asymptotically broken, revealing an error in the analysis of [32]. Specifically, we find that the expected complexity of the Kipnis-Shamir attack on this scheme is $\mathcal{O}\left(n^{(\lceil log_q(D)\rceil+2)\omega}\right)$, where D is the degree bound in ZHFE and ω is the linear algebra constant, instead of the complexity $\mathcal{O}\left(n^{2(\lceil log_q(D)\rceil+2)\omega}\right)$ as reported in [32]. Our empirical data from an implementation of this attack support our complexity estimate. This correction in the complexity estimate reveals that the attack is feasible for the original parameters; instead of a complexity of 2^{138} as claimed in [32], we find the complexity is 2^{64} (A.3). We thus consider ZHFE to be broken.

The article is organized as follows. In the next section, we describe the ZHFE construction and discuss the encryption scheme. In the subsequent section, we outline our attack, describing our notation, our proof of the existence of a low rank equivalent private key, reduce the task of recovering a low rank central polynomial to a MinRank problem, and state how to construct a fully functional equivalent key from it. In the following section, we derive the complexity of our attack, and present our experimental data supporting our complexity bound. A detailed comparison of our analysis to previous MinRank analysis and a toy example are provided in the appendices for space reasons. In the last section, we conclude that ZHFE is broken and discuss the current landscape of multivariate public key encryption.

2 The ZHFE encryption scheme

The ZHFE encryption scheme was introduced in [25] based on the idea that a high degree central map may resist cryptanalysis in the style of [2]. The hope of the authors was that having a high degree central map may result in high Q-rank.

Let $\mathbb{F}$ be a finite field of order q. Let $\mathbb{K}$ be a degree n extension of $\mathbb{F}$. Large Roman letters near the end of the alphabet denote indeterminants over $\mathbb{K}$. Small Roman letters near the end of the alphabet denote indeterminants over $\mathbb{F}$. An underlined letter denotes a vector over $\mathbb{F}$, e.g. $\underline{v} = (v_1, \dots, v_n)$. A small bold letter denotes a vector over $\mathbb{K}$, e.g. $\mathbf{u} = (u_0, \dots, u_{n-1})$. Small Roman letters near $f, g, h, \dots$ denote polynomials over $\mathbb{F}$. Large Roman letters near $F, G, H, \dots$ denote polynomials over $\mathbb{K}$. Large bold letters denote matrices; the field in which coefficients reside will be specified, but may always be considered to be included in $\mathbb{K}$. The function $\text{Frob}_k()$ takes as argument a polynomial or a matrix. For polynomials it returns the polynomial with its coefficient raised to k-th Frobenius power, and for matrices it raises each entry of the matrix to k-th Frobenius power.

Fix an element $y \in \mathbb{K}$ whose orbit under the Frobenius map $y \mapsto y^q$ is of order n. We define the canonical $\mathbb{F}$-vector space isomorphism $\phi : \mathbb{F}^n \to \mathbb{K}$ defined by $\phi(\underline{a}) = \sum_{i=0}^{n-1} a_i y^{q^i}$. We further define $\phi_2 = \phi \times \phi$.

The construction of the central map of ZHFE is quite simple. Without loss of the generality of analysis, we focus on the homogeneous case. One formally declares the following relation over $\mathbb{K}$:

$$\begin{aligned}\varPsi = {} & X\left(\alpha_1 F^{q^0} + \cdots + \alpha_n F^{q^{n-1}} + \beta_1 \tilde{F}^{q^0} + \cdots + \beta_n \tilde{F}^{q^{n-1}}\right)\Bigg(\\ & + X^q\left(\alpha_{n+1} F^{q^0} + \cdots + \alpha_{2n} F^{q^{n-1}} + \beta_{n+1} \tilde{F}^{q^0} + \cdots + \beta_{2n} \tilde{F}^{q^{n-1}}\right)\Bigg(\end{aligned}$$

where juxtaposition represents multiplication in $\mathbb{K}$ and where $\varPsi$ is constrained to have degree less than a bound D. By its construction, $\varPsi$ has the form

$$\varPsi(x) = \sum_{i=0}^{1} \sum_{\substack{i \le j \le k \\ q^i + q^j + q^k \le D}} \Bigg(a_{i,j,k} x^{q^i + q^j + q^k}.$$

One may then arbitrarily choose the coefficients α_i and β_i and solve the resulting linear system for the unknown coefficients of F and $\tilde{F}$. Even making an arbitrary selection of the coefficients $a_{i,j,k}$ of $\varPsi$, we have an underdefined system and have a large solution space for maps F and $\tilde{F}$.

The private key is given by $\varPi = (G, S, T)$ where $G = (F, \tilde{F})$, $S \in End(\mathbb{F}^n)$ and $T \in End(\mathbb{F}^{2n})$. The public key is constructed via

$$P = T \circ \phi_2 \circ G \circ \phi^{-1} \circ S.$$

Encryption is accomplished by simply evaluating P at the plaintext $\underline{x} \in \mathbb{F}^n$. The interesting step in decryption is inverting the central map, G. Notice that if $G(X) = (Y_1, Y_2)$ then the following relation holds:

$$\begin{aligned}\varPsi(X) = {} & X(\alpha_1 Y_1 + \alpha_2 Y_1^q + \cdots \alpha_n Y_1^{q^{n-1}} + \beta_1 Y_2 + \cdots + \beta_n Y_2^{q^{n-1}} \\ & + X^q(\alpha_{n+1} Y_1 + \alpha_{n+2} Y_1^q + \cdots \alpha_{2n} Y_1^{q^{n-1}} + \beta_{n+1} Y_2 + \cdots + \beta_{2n} Y_2^{q^{n-1}}.\end{aligned}$$

Since this equation is of degree bounded by D, solutions X can be found efficiently using Berlekamp's Algorithm. While it is possible that there may be multiple solutions to this equation, it is very unlikely; furthermore, the public key can be used to determine the actual preimage.

3 Key Recovery Attack for ZHFE

In this section describe a key recovery attack for ZHFE using the MinRank approach. We first show that with high probability there exist linear combinations of Frobenius powers of the core polynomials F and $\tilde{F}$ of low rank. Then, we show that such linear combinations can be efficiently extracted from the public key. Finally, we describe how to construct a low degree polynomial $\varPsi'$ from those low rank polynomials.

3.1 Existence of a low rank equivalent key

Fix the representation $a \overset{\Phi}{\mapsto} (a, a^q, \dots, a^{q^{n-1}})$ of $\mathbb{K}$. Then the image $\Phi(\mathbb{K}) = \mathbb{A} = \{(a, a^q, \dots, a^{q^{n-1}}) : a \in \mathbb{K}\}$ is a one-dimensional $\mathbb{K}$-algebra. We define $\mathbf{M}_n$ by $\mathbf{M}_n = \Phi \circ \phi$. Using the element y defined in Section 2, we recover an explicit representation of $\mathbf{M}_n \in \mathcal{M}_{n\times n}(\mathbb{K})$:

$$\mathbf{M}_n = \begin{pmatrix} 1 & 1 & \dots & 1 \\ y & y^q & & y^{q^{n-1}} \\ \vdots & & \ddots & \\ y^{n-1} & y^{(n-1)q} & & y^{(n-1)q^{n-1}} \end{pmatrix}.$$

It is well known that the matrix $\mathbf{M}_n$ is invertible. The following proposition is a particular case of Proposition 4 in [2].

Proposition 1. *Let* $\boldsymbol{M}_{2n} = \begin{pmatrix} \boldsymbol{M}_n & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{M}_n \end{pmatrix}$. *Then the function* $\varphi_2 = \mathbb{K}^2 \to \mathbb{F}^{2n}$ *can be expressed as* $(X, Y) \mapsto (X, X^q, \dots, X^{q^{n-1}}, Y, Y^q, \dots, Y^{q^{n-1}})\boldsymbol{M}_{2n}^{-1}$*, and its inverse* $\varphi_2^{-1} : \mathbb{F}^{2n} \to \mathbb{K}^2$ *as* $(x_1, \dots, x_{2n}) \mapsto (X_1, X_{n+1})$*, where* $(X_1, \dots, X_{2n}) = (x_1, \dots, x_{2n})\boldsymbol{M}_{2n}$

Two private keys are equivalent if they build the same public key, that is:

Definition 1. *Let* $\Pi = (G, S, T)$*, and* $\Pi' = (G', S', T')$ *be private ZHFE keys. We say that* Π *and* Π' *are equivalent if*

$$T' \circ \varphi_2 \circ G' \circ \varphi^{-1} \circ S' = T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S.$$

We show that given an instance of ZHFE with public key $P = T \circ (\varphi \times \varphi) \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S$ and private key $\Pi = (G, S, T)$, with high probability, there exists an equivalent key $\Pi' = (G', S', T')$, where the polynomials $G' = (F', \tilde{F}')$ have low rank associated matrices. We only consider linear transformations and homogeneous polynomials. This case can be easily adapted to affine transformations and general HFE polynomial.

It was noted by Perlner and Smith-Tone [23] and independently by Verbel [31] that there exists a linear transformation of ZHFE's core map $G = (F, \tilde{F})$ with low rank associated matrices. Recall that for each ZHFE private key (G, S, T), $G = (F, \tilde{F})$, there are scalars $\alpha_1, \dots, \alpha_{2n}, \beta_1, \dots, \beta_{2n}$ in the big field $\mathbb{K}$ such that the function

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

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

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

has HFE shape and 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 a particular form of tail shown in A.2.

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. It is easy to see that if the coefficients $\alpha_1, \ldots, \alpha_{2n}, \beta_1, \ldots, \beta_{2n}$ are chosen uniformly at random in $\mathbb{K}$, the probability that L is invertible is very high (see [31] for more details).

Were L singular as suggested in [24], a different approach is also possible. Defining the linear transformation $R' = \varphi_2 \circ L \circ \varphi_2^{-1} \circ T^{-1}$ and with the public key $P = T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S$, we have $R' \circ P = \varphi_2 \circ (L \circ G) \circ \varphi^{-1} \circ S$. Thus, $R' \circ P$ has low rank core polynomials $L \circ G$, hence we can attack $R' \circ P$ and find R' in the process. We do not further discuss this approach, and instead, from now on, we assume L is invertible which happens with high probability for the scheme as originally proposed.

3.2 Finding a low rank core polynomial

In the previous section we saw that, with high probability a ZHFE 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. We now discuss how from the public key P, we can obtain such an equivalent key and how to further exploit it to decrypt without knowing the secret key.

Let P be a ZHFE public key and let us assume there exists an equivalent key (G', S', T'), with low rank core map $G' = (H, \tilde{H})$, so that $P = T' \circ \varphi_2 \circ G' \circ \varphi^{-1} \circ S'$. Let $\mathbf{H}$ and $\tilde{\mathbf{H}}$ be the low rank ($r + 1$, with $r = \lceil \log_q D \rceil$) matrices associated with H and $\tilde{H}$.

Note that the above relation implies that, algebraically, ZHFE is similar to a high degree (but still low rank) version of multi-HFE. Thus, we may suspect that all of the consequences of low rank derived in [2] apply. In fact, our attack on ZHFE, though related, has some subtle but significant distinctions from the cryptanalysis of multi-HFE. The details of the MinRank attack follow.

Using the notation $\mathbf{H}^{*k} \in \mathcal{M}_{n\times n}(\mathbb{K})$ to represent the matrix associated with the k-th Frobenius power of a polynomial H with matrix $\mathbf{H} = [a_{i,j}]$, it is easy to see that the (i, j)-th entry of $\mathbf{H}^{*k}$ is $a^{q^k}_{i-k,j-k}$ (indices 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 low rank polynomials $\mathfrak{H} = \varphi_2 \circ (H, \tilde{H}) \circ \varphi^{-1} = (h_1, \ldots, h_{2n})$ and the matrices $\mathbf{H}^{*k}$'s. The following Lemma follows from Lemma 2 in [2].

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

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

Let $(\mathbf{P}_1, \ldots, \mathbf{P}_{2n}) \in (\mathcal{M}_{n\times n}(\mathbb{F}))^{2n}$ be the matrices associated with the quadratic public polynomials. Then,

$$\begin{aligned} P(\underline{x}) &= T(\mathfrak{H}(S(\underline{x}))) \\ (\underline{x}\mathbf{P}_1\underline{x}^\top, \ldots, \underline{x}\mathbf{P}_{2n}\underline{x}^\top) &= (h_1(\underline{x}\mathbf{S}), \ldots, h_{2n}(\underline{x}\mathbf{S}))\mathbf{T} \qquad (1) \\ (\underline{x}\mathbf{P}_1\underline{x}^\top, \ldots, \underline{x}\mathbf{P}_{2n}\underline{x}^\top) &= (\underline{x}\mathbf{S}\mathbf{H}_1\mathbf{S}^\top\underline{x}^\top, \ldots, \underline{x}\mathbf{S}\mathbf{H}_{2n}\mathbf{S}^\top\underline{x}^\top)\mathbf{T}, \end{aligned}$$

where $\mathbf{S} \in \mathcal{M}_{n\times n}(\mathbb{F})$ and $\mathbf{T} \in \mathcal{M}_{2n\times 2n}(\mathbb{F})$. Using this relation and Lemma 1, we can derive a simultaneous MinRank problem on the matrices associated with the public polynomials, which lie in $\mathcal{M}_{n\times n}(\mathbb{F})$, the solutions of which lie in the extension field $\mathbb{K}$. This result is similar to, but has consequential differences from, [2, Theorem 2].

Theorem 1. *Given the notation above, for any instance of ZHFE, calculating* $\boldsymbol{U} = \boldsymbol{T}^{-1}\boldsymbol{M}_{2n} \in \mathcal{M}_{2n\times 2n}(\mathbb{K})$ *for some equivalent key* (G', S', T') *reduces to solving a MinRank instance with rank* $r + 1$ *and* $k = 2n$ *on the public matrices* $(\boldsymbol{P}_1, \ldots, \boldsymbol{P}_{2n}) \in \mathcal{M}_{n\times n}(\mathbb{F})$. *The solutions of this MinRank instance lie in* $\mathbb{K}^n$.

Proof. By Equation (1) and Lemma 1,

$$(\mathbf{P}_1, \ldots, \mathbf{P}_{2n})\mathbf{U} = (\mathbf{W}\mathbf{H}^{*0}\mathbf{W}^\top, \ldots, \mathbf{W}\mathbf{H}^{*n-1}\mathbf{W}^\top, \mathbf{W}\tilde{\mathbf{H}}^{*0}\mathbf{W}^\top, \ldots, \mathbf{W}\tilde{\mathbf{H}}^{*n-1}\mathbf{W}^\top), \quad (2)$$

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 (2) we get the following equations

$$\sum_{i=0}^{2n-1} u_{i,0}\mathbf{P}_{i+1} = \mathbf{W}\mathbf{H}\mathbf{W}^\top, \text{ and } \sum_{i=0}^{2n-1} u_{i,n}\mathbf{P}_{i+1} = \mathbf{W}\tilde{\mathbf{H}}\mathbf{W}^\top. \quad (3)$$

Since $\mathbf{H}$ has rank $r+1$ and $\mathbf{W}$ is an invertible matrix, the rank of $\mathbf{W}\mathbf{H}\mathbf{W}^\top$ is also $r+1$ (similarly for $\tilde{\mathbf{H}}$). Consequently, the last equation implies that the vectors $\mathbf{u} = (u_{0,0}, \ldots, u_{2n-1,0})$ and $\mathbf{v} = (u_{0,n}, \ldots, u_{2n-1,n})$ are solutions (called the original solutions) for the MinRank problem associated with the $k = 2n$ public symmetric matrices $(\mathbf{P}_1, \ldots, \mathbf{P}_{2n})$ and the integer $r+1$.

An immediate consequence of Theorem 1 is that if we solve that MinRank problem we get the matrix associated with a linear combination of the Frobenius powers of H and $\tilde{H}$ composed with $\varphi^{-1} \circ S$. We must next analyze the space of solutions of the MinRank problem for ZHFE and complete the key extraction.

3.3 Finding solution from a MinRank problem

From the previous section we know that there are at least two solution $\mathbf{u}$ and $\mathbf{v}$ (the original solutions) for the MinRank problem associated with ZHFE. In this part we show that every nonzero linear combination of a Frobenius power of the original solutions, i.e, $\alpha\mathbf{u}^{q^k} + \beta\mathbf{v}^{q^k}$, is also solution for the MinRank problem associated with ZHFE.

First of all, note that for each nonzero vector $(a_{00}, a_{10}) \in \mathbb{K} \times \mathbb{K}$ there is another vector $(a_{01}, a_{11}) \in \mathbb{K} \times \mathbb{K}$ such that the matrix $A^* = \begin{bmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \end{bmatrix}$ is an invertible matrix. If $\mathcal{A}$ is the linear transformation associated with A^*, the private key (G'', S'', T'') with

$$\begin{aligned} G'' &= \text{Frob}_{\ k} \circ \mathcal{A} \circ (H, \tilde{H}) \circ \text{Frob}_{\ n-k} \\ T'' &= T' \circ \varphi_2 \circ \mathcal{A}^{-1} \circ \text{Frob}_{n-k} \circ \varphi_2^{-1} \\ S'' &= \varphi \circ \text{Frob}_k \circ \varphi^{-1} \circ S', \end{aligned}$$

is equivalent to (G', S', T'). From Proposition 8 in [2], we know that the matrix associated with $\varphi_2 \circ \mathcal{A} \circ \varphi_2^{-1}$ is $\mathbf{M}_{2n}\widehat{A^*}\mathbf{M}_{2n}^{-1}$, where $\widehat{A^*} = \left[\begin{array}{c|c} A_{00} & A_{01} \\ \hline A_{10} & A_{11} \end{array}\right]$ and $A_{ij} = \text{Diag}(a_{ij}, a_{ij}^q, \ldots, a_{ij}^{q^{n-1}})$.

Also, from Proposition 10 in [2], the matrix associated with $\varphi_2 \circ \text{Frob}_{\ n-k} \circ \varphi_2^{-1}$ is $\mathbf{M}_{2n}\mathbf{P}_{2,n-k}\mathbf{M}_{2n}^{-1}$, where $\mathbf{P}_{N,k} = \text{Diag}(\mathbf{R}_{n,k}, ..., \mathbf{R}_{n,k})(N$ times), and $\mathbf{R}_{n,k}$ is the $n \times n$ matrix of a k positions left-rotation. So the matrices associated with H', $\tilde{H}'$(where $G'' := (H', \tilde{H}')$), T''^{-1} and S'' are respectively

$$\begin{aligned} \mathbf{H}' &= a_{00}\,\text{Frob}_k(\mathbf{H}) + a_{01}\,\text{Frob}_k(\tilde{\mathbf{H}}), \\ \tilde{\mathbf{H}}' &= a_{10}\,\text{Frob}_k(\mathbf{H}) + a_{11}\,\text{Frob}_k(\tilde{\mathbf{H}}), \\ \mathbf{T}''^{-1} &= \mathbf{T}'^{-1}\mathbf{M}_{2n}\mathbf{P}_{2,k}\widehat{A^*}\mathbf{M}_{2n}^{-1}, \\ \mathbf{S}'' &= \mathbf{S}'\mathbf{M}_{2n}\mathbf{P}_{1,k}\mathbf{M}_{2n}^{-1}. \end{aligned}$$

As $\text{Rank}(\mathbf{H}') \leq r+1$, (similarly for $\tilde{\mathbf{H}}'$), from equation (3) we get that all columns of $\mathbf{T}''^{-1}\mathbf{M}_{2n}$ are solutions of the MinRank problem associated with the public matrices $(\mathbf{P}_1, \ldots, \mathbf{P}_{2n})$ and $r+1$. Note that $\mathbf{T}''^{-1}\mathbf{M}_{2n} = \mathbf{U}\mathbf{P}_{2,k}\widehat{A^*}$, so the first column of $\mathbf{UP}_{2,k}\widehat{A^*}$, namely $a_{00}\mathbf{u}^{q^k} + a_{10}\mathbf{v}^{q^k}$, is in particular a solution for such MinRank problem. Moreover, we expect most solutions to be of this form because the system is very overdetermined. Our experiments confirm this latest claim (see Section 4).

So far we know that there are many equivalent keys like (G'', T'', S''). In the following, we explain how we can find one of them. First, we solve the MinRank problem, and use the vector solution $\mathbf{u}' = a_{00}\mathbf{u}^{q^k} + a_{10}\mathbf{v}^{q^k} = (u'_1, \ldots, u'_{2n})$ to compute $\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u'_i\mathbf{P}_{i+1}\right)$. Next, we find another solution $\mathbf{v}' = (v'_0, \ldots, v'_{2n-1})$ to the MinRank problem by solving the linear system,

$$\mathbf{K}' \left(\sum_{i=0}^{2n-1} x_i\mathbf{P}_{i+1}\right) = \mathbf{0}_{(n-r)\times n}.$$

Again, we expect that the new solution $\mathbf{v}'$ preserves the form as a linear combination of the Frobenius power of the original solutions, i.e, $\mathbf{v}' = a_{01}\mathbf{u}^{q^{k_1}} + a_{11}\mathbf{v}^{q^{k_1}}$. Moreover, we claim that both founded solutions come from the same Frobenius power, i.e, $k_1 = k$. Indeed, if $\mathbf{u} = (u_0, \ldots, u_{2n-1})$ (one of the original solutions) and we set $\mathbf{K} = \ker\left(\sum_{i=0}^{2n-1} u_i\mathbf{P}_{i+1}\right)$, Theorem 6 in [2] give us $\mathbf{K}' = \mathrm{Frob}_k(\mathbf{K}) = \mathrm{Frob}_{k_1}(\mathbf{K})$, hence, if $\mathbf{K}$ has at least one entry in $\mathbb{K} \setminus \mathbb{F}$, then $k_1 = k$.

It is easy to see that the probability that $\mathbf{A} = [a_{ij}]$, $i, j = 0, 1$ is invertible is high. In that case, we already know that the matrix $\mathbf{T}''$, such that, $\mathbf{T}''^{-1} = \mathbf{U"M}_{2n}^{-1}$, with $\mathbf{U}'' := [\mathbf{u}'|\cdots|\mathbf{u}'^{q^{n-1}}|\mathbf{v}'|\cdots|\mathbf{v}'^{q^{n-1}}]$ is part of an equivalent key. In the rest of this section we show how to find the other two elements of the already fixed equivalent key.

Once an equivalent key has been fixed, our second target is to find $\mathbf{W}'' := \mathbf{S}''\mathbf{M}_n$. Keeping in mind that $\sum_{i=0}^{2n-1} u'_i\mathbf{P}_{i+1} = \mathbf{W}''\mathbf{H}'\mathbf{W}''^\top$, and $\mathbf{W}''$ is invertible, we get $\ker(\mathbf{H}') = \mathbf{K}'\mathbf{W}''$. Assuming $\mathbf{H}'$ has the shape

$$\left[\begin{array}{c|c} \mathbf{A} & \mathbf{B}^T \\ \hline \mathbf{B} & 0_{(n-r)\times(n-r)} \end{array}\right],$$

where $\mathbf{A}$ is a full rank $r \times r$ matrix, and $\mathbf{B}$ is a rank one $(n-r) \times r$ matrix, it is easy to see that $\ker(\mathbf{H}')$ is of the form $\left[0_{(n-r-1)\times r} \mid \mathbf{C}\right]$, where $\mathbf{C}$ is a full rank $(n-r-1) \times (n-r)$ matrix. Thus $\mathbf{K}'\mathbf{W}''$ has its first r columns set to zero. In particular, if $\mathbf{w}$ is the first column of $\mathbf{W}''$, then $\mathbf{K}'\mathbf{w} = 0$ leads to a linear system of $n-r-1$ equations in n variables. Such a system might have spurious solutions that do not correspond to a matrix of the form $\mathbf{W}'' = \mathbf{S}''\mathbf{M}_n$. In order to get more equations we can use Frobenius powers of $\mathbf{K}'$. For $j = 0, \ldots, n-1$,

$$\mathrm{Frob}_j(\mathbf{K}') = \ker\left(\sum_{i=0}^{2n-1} u_{i,j}\mathbf{P}_{i+1}\right) = \ker\left(\mathbf{W}''\mathbf{H}'^{*j}\mathbf{W}''^\top\right) = \ker\left(\mathbf{W}''\mathbf{H}'^{*j}\right)$$

hence $\ker(\mathbf{H}'^{*j}) = \mathrm{Frob}_j(\mathbf{K}')\mathbf{W}''$. Moreover, $\ker(\mathbf{H}'^{*j})$ has r zero columns indexed by $j+1, \ldots, j+r+1 \mod n$. Therefore, for $j = n-r, \ldots, n-1$,

$\mathrm{Frob}_j(\mathbf{K}')\mathbf{w} = 0$ and each of these contributes $n - r - 1$ equations in the same n variables. Note that we only need one column of $\mathbf{W}''$ to build the rest of the matrix.

Once $\mathbf{U}''$ and $\mathbf{W}''$ are recovered, we might find the core polynomials by using the following equations

$$\mathbf{H}' = \mathbf{W}''^{-1} \left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1} \right) \mathbf{W}''^{-t} \text{ and } \tilde{\mathbf{H}}' = \mathbf{W}''^{-1} \left(\sum_{i=0}^{2n-1} v'_i \mathbf{P}_{i+1} \right) \mathbf{W}''^{-t}.$$

At this point, we are not able to decrypt a ciphertext because the recovered core polynomials $\mathbf{H}'$ and $\tilde{\mathbf{H}}'$ would have high degree. But fortunately $\mathbf{H}'$ and $\tilde{\mathbf{H}}'$ satisfy the following equations

$$\begin{aligned} a_{11}\mathbf{H}' - a_{01}\tilde{\mathbf{H}}' &= (a_{11}a_{00} - a_{01}a_{10}) \,\mathrm{Frob}_k(\mathbf{H}) = \det(A^*) \,\mathrm{Frob}_k(\mathbf{H}), \text{ and} \\ -a_{10}\mathbf{H}' + a_{00}\tilde{\mathbf{H}}' &= (-a_{01}a_{10} + a_{11}a_{00}) \,\mathrm{Frob}_k(\tilde{\mathbf{H}}) = \det(A^*) \,\mathrm{Frob}_k(\tilde{\mathbf{H}}), \end{aligned}$$

where the a'_{ij}s are the ones given by the equivalent key already fixed by $\mathbf{T}''$. Consequently, if we would know the a'_{ij}s, we could derive a low degree polynomial (useful to invert H' and $\tilde{H}'$) as shown in the next equation

$$\begin{aligned} X(a_{11}H' - a_{01}\tilde{H}') + X^q(-a_{10}H' + a_{00}\tilde{H}') = \\ \det(A^*) \left[X \,\mathrm{Frob}_k(H) + X^q \,\mathrm{Frob}_k(\tilde{H}) \right] = \\ \det(A^*) \,\mathrm{Frob}_k(\Psi). \end{aligned}$$

Setting $\mathbf{H}' = [h_{ij}]$ and $\tilde{\mathbf{H}}' := [\tilde{h}_{ij}]$, we try to find a_{00}, a_{01}, a_{10}, and a_{11} by first solving the overdetemined systems

$$\begin{bmatrix} h_{1,r+1} & h_{1,r+2} & \cdots & h_{1,n-1} & h_{1,n} \\ \tilde{h}_{1,r+1} & \tilde{h}_{1,r+2} & \cdots & \tilde{h}_{1,n-1} & \tilde{h}_{1,n} \end{bmatrix}^{\top} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \mathbf{0} \text{ , and}$$

$$\begin{bmatrix} h_{2,r+1} & h_{2,r+2} & \cdots & h_{2,n-1} & h_{2,n} \\ \tilde{h}_{2,r+1} & \tilde{h}_{2,r+2} & \cdots & \tilde{h}_{2,n-1} & \tilde{h}_{2,n} \end{bmatrix}^{\top} \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \mathbf{0}.$$

For n large enough we expect that both solution spaces are one-dimensional, i.e, our expected solution are of the form

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \alpha \begin{bmatrix} a_{11} \\ -a_{01} \end{bmatrix}, \quad \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \beta \begin{bmatrix} -a_{10} \\ a_{00} \end{bmatrix}$$

for some $\alpha, \beta \in \mathbb{K}$. Then, we compute

$$\begin{aligned} \alpha a_{11}H' - \alpha a_{01}\tilde{H}' &= \alpha \det(A^*) \,\mathrm{Frob}_k(H), \quad \text{and} \\ -\beta a_{10}H' + \beta a_{00}\tilde{H}' &= \beta \det(A^*) \,\mathrm{Frob}_k(\tilde{H}), \end{aligned}$$

and by solving a linear system, we can get α, β, and our low degree polynomial

$$\Psi'' := \gamma \det(A^*) \,\mathrm{Frob}_k(\Psi), \quad \text{with } \gamma \in \mathbb{K}.$$

4 Experimental Results and Complexity

In order to experimentally verify our attack, we generated ZHFE instances for different parameters and carried out the full attack. We were able to solve the MinRank problem associated with each instance of ZHFE and then we recovered an equivalent key for every solved MinRank problem. We also recovered the low degree polynomial Ψ''. Every time we successfully solved the MinRank problem, we were able to carry out the rest of the attack. This confirms that most solutions for such MinRank problem are of the form $a_{00}\mathbf{u}^{q^k} + a_{10}\mathbf{v}^{q^k}$. For these experiments we used the fast key generation method proppposed by Baena, et al. [26], so we need to keep in mind that n must be even and the relation $q + 2q^{r-1} < D \leq q^r$ must be satisfied. 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.

			Minors		KS	
q	r	n	CPU time [s]	Memory [MB]	CPU time [s]	Memory [MB]
7	2	8	255	4216	280	439
7	2	12	3111	59651	1272	752
7	2	16			5487	2537
17	2	8	277	5034	299	503
17	2	12	3584	68731	1330	817
17	2	16			6157	2800

Table 1. MinRank attack to ZHFE

Table 1 shows the time and memory required for the attacks using either the Kipnis-Shamir modeling or the minors modeling for solving the MinRank. These few data measures suggests that the Kipnis-Shamir modeling is more efficient. The Kipnis-Shamir modeling yields a bilinear system of $n(n-r-1)$ equations in $(n-r-1)(r+1)+2n$ variables. The Groebner Basis computation on every reported instance with $r=2$ had a falling degree of 4. It follows that under this modeling the resulting system is not bi-regular as defined in [14]. To the best of our knowledge, there is no tight bound in the literature for the falling degree for the system that arises from the Kipnis-Shamir modeling.

Alternatively, the minors modeling yields a system of $\binom{n}{r+2}^2$ equations in $2n$ variables, whose complexity can be studied as in [2]. Assuming the conjecture about regularity in [12], the Hilbert series of the minors model ideal is

$$HS(t) = (1-t)^{(n-R)^2-2n} \frac{\det A(t)}{t^{\binom{R}{2}}},$$

where R is the target matrix rank (in our case $R = r+1$) and $A(t) = [a_{i,j}(t)]$ is the $R \times R$ matrix defined by $a_{i,j} = \sum_{\ell=0}^{n-\max(i,j)} \binom{n-i}{\ell}\binom{n-j}{\ell} t^{\ell}$. The degree of regularity is then given by the index of the first negative coefficient of $HS(t)$.

In comparison to the Hilbert Series in the multi-HFE case discussed in [2], the only difference is the $2n$ term in the exponent of $1-t$ (simply n in their case). This does not affect significantly the analysis thereafter. For example, if we define $H_R(t) = (1-t)^{(n-R)^2-2n} \det A(t)$, we can compute

$$H_1(t) = 1 + nt - \frac{1}{4}n(n-4)(n+1)^2t^2 + \mathcal{O}(t^3).$$

Note that the coefficient of 1 and t are positive and that the coefficient of t^2 is negative for $n > 4$. So the degree of regularity is $2 = R+1 = r+2$. Similarly, with $r = 1$, $R = 2$, the degree of regularity is $3 = R+1 = r+2$ for $n > 5.88$, with $r = 2$, $R = 3$, the degree of regularity is 4 for $n > 7.71$, and with $r = 3$, $R = 4$, the degree of regularity is 5 for $n > 9.54$. We thus adventure to claim that the degree of regularity of the minors modeling of the min-rank problem arising from the attack on ZHFE is less or equal to $r+2$ for all cases of interest. It follows that the complexity is $\mathcal{O}\left(\binom{2n+r+2}{r+2}\right)^{\omega} \sim \mathcal{O}\left(n^{(r+2)\omega}\right)$, where $2 < \omega < 3$ is the linear algebra constant. This is polynomial in n for r constant. Even if r is a logarithmic function of n, the complexity is barely superpolynomial in n.

It is worth spelling out the practical consequences of the above analysis. The expected degree of regularity $r+2$ is also the degree of the minors. Thus, for n large enough, these minors span the whole degree $r+2$ polynomial ring's subspace. Therefore, to solve this system it suffices to gather enough minors and linearly reduce them among themselves. No Groebner basis algorithm is necessary. Moreover, in practice two variables can be fixed to 0 and 1, thus we just need to row-reduce a $\binom{2n+r}{r+2}$ square matrix.

5 Conclusion

We have shown a practical and asymptotic key recovery attack on the ZHFE encryption scheme. The details provided leave no doubt about its effectiveness. The asymptotic analysis shows the scheme vulnerable even for larger parameters. The rank structure of the central polynomials has proven too difficult to mask. Though the concept of ZHFE was directly inspired by a desire to avoid rank weakness, ZHFE succombed to rank weaknesses.

Nevertheless, the idea of an injective multivariate trapdoor function may be viable, though ZHFE is not the correct technique. The landscape for multivariate public key encryption remains fairly bleak at this time. Fundamentally new ideas must emerge to realize the goal of secure multivariate encryption.

References

1. Baena, J.B., Cabarcas, D., Escudero, D.E., Porras-Barrera, J., Verbel, J.A.: Efficient ZHFE key generation. In: Takagi [29], pp. 213–232, http://dx.doi.org/10.1007/978-3-319-29360-8_14

2. 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)
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. Cartor, R., Gipson, R., Smith-Tone, D., Vates, J.: On the differential security of the hfev- signature primitive. In: Takagi [29], pp. 162–181, http://dx.doi.org/10.1007/978-3-319-29360-8_11
5. Chen, M.S., Yang, B.Y., Smith-Tone, D.: Pflash - secure asymmetric signatures on smart cards. Lightweight Cryptography Workshop 2015 (2015), http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf
6. Daniels, T., Smith-Tone, D.: Differential properties of the HFE cryptosystem. In: Mosca [20], pp. 59–75, http://dx.doi.org/10.1007/978-3-319-11659-4_4
7. Ding, J., Hodges, T.J.: Inverting HFE systems is quasi-polynomial for all fields. In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6841, pp. 724–742. Springer (2011), http://dx.doi.org/10.1007/978-3-642-22792-9_41
8. Ding, J., Petzoldt, A., Wang, L.: The cubic simple matrix encryption scheme. In: Mosca [20], pp. 76–87, http://dx.doi.org/10.1007/978-3-319-11659-4_5
9. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3531, pp. 164–175 (2005), http://dx.doi.org/10.1007/11496137_12
10. Ding, J., Yang, B.Y.: Degree of regularity for hfev and hfev-. In: Gaborit [15], pp. 52–66, http://dx.doi.org/10.1007/978-3-642-38616-9
11. Dubois, V., Gama, N.: The degree of regularity of HFE systems. In: Abe, M. (ed.) Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6477, pp. 557–576. Springer (2010), http://dx.doi.org/10.1007/978-3-642-17373-8_32
12. Faugère, J.C., El Din, M.S., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using grÖbner bases and applications to cryptology. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. pp. 257–264. ISSAC '10, ACM, New York, NY, USA (2010)
13. Faugère, J., Gligoroski, D., Perret, L., Samardjiska, S., Thomae, E.: A polynomial-time key-recovery attack on MQQ cryptosystems. In: Katz, J. (ed.) Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings. Lecture Notes in Computer Science, vol. 9020, pp. 150–174. Springer (2015), http://dx.doi.org/10.1007/978-3-662-46447-2_7
14. FaugÃ¨re, J.C., Din, M.S.E., Spaenlehauer, P.J.: GrÃ¶bner bases of bihomogeneous ideals generated by polynomials of bidegree : Algorithms and complexity. Journal of Symbolic Computation 46(4), 406 – 437 (2011)
15. Gaborit, P. (ed.): Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings, Lecture Notes

in Computer Science, vol. 7932. Springer (2013), http://dx.doi.org/10.1007/978-3-642-38616-9

16. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Lecture Notes in Computer Science, vol. 1592, pp. 206–222. Springer (1999), http://dx.doi.org/10.1007/3-540-48910-X_15
17. 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)
18. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In: Mosca [20], pp. 180–196, http://dx.doi.org/10.1007/978-3-319-11659-4_11
19. Moody, D., Perlner, R.A., Smith-Tone, D.: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme. Springer (2017)
20. Mosca, M. (ed.): Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings, Lecture Notes in Computer Science, vol. 8772. Springer (2014), http://dx.doi.org/10.1007/978-3-319-11659-4
21. Patarin, J., Courtois, N., Goubin, L.: Quartz, 128-bit long digital signatures. In: Naccache, D. (ed.) Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2020, pp. 282–297. Springer (2001), http://dx.doi.org/10.1007/3-540-45353-9_21
22. Perlner, R.A., Smith-Tone, D.: A classification of differential invariants for multivariate post-quantum cryptosystems. In: Gaborit [15], pp. 165–173, http://dx.doi.org/10.1007/978-3-642-38616-9
23. Perlner, R.A., Smith-Tone, D.: Security analysis and key modification for ZHFE. In: Takagi [29], pp. 197–212, http://dx.doi.org/10.1007/978-3-319-29360-8_13
24. 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)
25. Porras, J., Baena, J., Ding, J.: Zhfe, a new multivariate public key encryption scheme. In: Mosca [20], pp. 229–245, http://dx.doi.org/10.1007/978-3-319-11659-4_14
26. 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)
27. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 41(2), 303–332 (electronic) (1999)
28. Smith-Tone, D.: On the differential security of multivariate public key cryptosystems. In: Yang, B.Y. (ed.) PQCrypto. Lecture Notes in Computer Science, vol. 7071, pp. 130–142. Springer (2011)
29. Takagi, T. (ed.): Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings, Lecture Notes in Computer Science, vol. 9606. Springer (2016), http://dx.doi.org/10.1007/978-3-319-29360-8
30. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In: Gaborit [15], pp. 231–242, http://dx.doi.org/10.1007/978-3-642-38616-9

31. Verbel, J.A.: Efficiency and Security of ZHFE. Master's thesis, Universidad Nacional de Colombia, sede Medellín (2016)
32. Zhang, W., Tan, C.H.: On the security and key generation of the zhfe encryption scheme. In: Advances in Information and Computer Security - 11th International Workshop on Security, IWSEC 2016, Tokyo, Japan, September 12-14, 2016, Proceedings (2015)

A Appendix

A.1 Toy Example

We provide a small example of the MinRank attack for ZHFE with parameters $n = 8$, $q = 3$ and $D = 9$. The small field is $\mathbb{F} = \mathbb{F}_q$, the extension field is $\mathbb{K} = \mathbb{F}/\langle g(y)\rangle$, where $g(y) = y^8 + 2y^5 + y^4 + 2y^2 + 2y + 2 \in \mathbb{F}[y]$, and b is a primitive root of the irreducible polynomial $g(y)$.

For ease of presentation, we consider a homogeneous public key and linear transformations. An easy adaptation for the general case can be done following the ideas expressed in [2].

The matrices associated with our private key $\left((F, \tilde{F}), S, T\right)$ are

$$\mathbf{F} = \begin{pmatrix} b^{827} & b^{487}3 & b^{3298} & b^{211} & b^{1824} & b^{5374} & b^{6155} & b^{2404} \\ b^{4873} & b^{5172} & b^{1526} & b^{1317} & b^{2727} & b^{1863} & b^{3546} & b^{5876} \\ b^{3298} & b^{1526} & b^{1842} & b^{3540} & b^{2647} & b^{2349} & b^{4599} & b^{2987} \\ b^{211} & b^{1317} & b^{3540} & b^{5242} & b^{5758} & b^{4705} & b^{2663} & b^{4097} \\ b^{1824} & b^{2727} & b^{2647} & b^{5758} & b^{4629} & b^{5792} & b^{5196} & b^{666} \\ b^{5374} & b^{1863} & b^{2349} & b^{4705} & b^{5792} & b^{6318} & b^{4937} & b^{6150} \\ b^{6155} & b^{3546} & b^{4599} & b^{2663} & b^{5196} & b^{4937} & b^{2275} & b^{1436} \\ b^{2404} & b^{5876} & b^{2987} & b^{4097} & b^{666} & b^{6150} & b^{1436} & b^{4721} \end{pmatrix}, \mathbf{S} = \begin{pmatrix} 0 & 0 & 2 & 2 & 2 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 & 0 & 2 & 2 & 2 \\ 1 & 2 & 2 & 1 & 1 & 1 & 0 & 2 \\ 0 & 2 & 1 & 2 & 0 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 & 2 & 1 & 0 & 0 \\ 2 & 1 & 0 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

$$\tilde{\mathbf{F}} = \begin{pmatrix} b^{5574} & b^{2257} & b^{4540} & b^{880} & b^{2073} & b^{4932} & b^{3441} & b^{5482} \\ b^{2257} & b^{301} & b^{5824} & b^{5391} & b^{1155} & b^{1678} & b^{572} & b^{3108} \\ b^{4540} & b^{5824} & b^{5208} & b^{3763} & b^{6074} & b^{2097} & b^{3074} & b^{139} \\ b^{880} & b^{5391} & b^{3763} & b^{125} & b^{2055} & b^{1763} & b^{1168} & b^{4512} \\ b^{2073} & b^{1155} & b^{6074} & b^{2055} & b^{5080} & b^{1720} & b^{5820} & b^{5832} \\ b^{4932} & b^{1678} & b^{2097} & b^{1763} & b^{1720} & b^{5850} & b^{1822} & b^{5443} \\ b^{3441} & b^{572} & b^{3074} & b^{1168} & b^{5820} & b^{1822} & b^{2857} & b^{939} \\ b^{5482} & b^{3108} & b^{139} & b^{4512} & b^{5832} & b^{5443} & b^{939} & b^{1665} \end{pmatrix}$$

and $\mathbf{T} = [\mathbf{T}_1|\mathbf{T}_2]$, where

$$\mathbf{T1} = \begin{pmatrix} 0&2&2&1&0&1&0&1&1&0&1&1&0&1&1&1 \\ 2&2&0&2&2&1&2&2&2&2&0&1&2&2&0&0 \\ 2&0&2&0&2&0&2&2&2&1&1&0&1&2&1&0 \\ 1&1&0&0&0&1&1&1&1&1&1&0&1&0&1&1 \\ 1&0&1&2&2&1&2&0&2&2&1&0&0&0&1&2 \\ 0&1&1&1&2&1&2&0&0&0&1&2&1&1&0&0 \\ 0&1&2&2&1&0&2&2&1&2&2&1&0&2&2&1 \\ 2&0&0&1&2&2&2&2&2&2&1&0&1&1&0&1 \end{pmatrix}^{\top}, \mathbf{T2} = \begin{pmatrix} 2&1&0&2&0&0&1&1&0&1&1&0&0&0&1&0 \\ 2&0&0&0&1&0&2&2&1&1&1&1&1&2&0&0 \\ 1&2&2&2&2&0&0&2&0&0&2&1&1&1&1&2 \\ 2&0&1&1&1&2&1&2&1&1&2&2&1&2&0&1 \\ 0&1&1&1&1&0&0&1&0&0&1&2&2&0&1&0 \\ 0&1&0&1&2&2&0&1&0&0&2&2&0&1&0&1 \\ 1&2&0&0&2&0&0&0&0&1&1&0&2&0&0&1 \\ 0&2&0&0&2&0&2&2&2&0&2&0&2&1&2&0 \end{pmatrix}^{\top}.$$

This private key gives us a public key represented by the matrices $\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_{2n}$.

$$\mathbf{P}_1 = \begin{pmatrix} 0&0&2&0&2&1&0&2 \\ 0&2&1&2&2&2&0&1 \\ 2&1&0&1&0&0&0&1 \\ 0&2&1&1&2&2&1&2 \\ 2&2&0&2&0&2&2&0 \\ 1&2&0&2&2&0&0&2 \\ 0&0&0&1&2&0&0&0 \\ 2&1&1&2&0&2&0&0 \end{pmatrix}, \mathbf{P}_2 = \begin{pmatrix} 2&1&0&1&1&0&2&0 \\ 1&0&2&0&0&0&0&2 \\ 0&2&0&2&0&0&2&1 \\ 1&0&2&1&1&0&0&1 \\ 1&0&0&1&1&0&0&1 \\ 0&0&0&0&0&2&1&0 \\ 2&0&2&0&0&1&0&1 \\ 0&2&1&1&1&0&1&2 \end{pmatrix}, \mathbf{P}_3 = \begin{pmatrix} 1&0&0&0&2&1&1&1 \\ 0&2&1&2&1&1&2&1 \\ 0&1&1&2&0&1&1&2 \\ 0&2&2&1&2&2&1&1 \\ 2&1&0&2&2&0&0&2 \\ 1&1&1&2&0&0&1&0 \\ 1&2&1&1&0&1&2&2 \\ 1&1&2&1&2&0&2&0 \end{pmatrix}, \mathbf{P}_4 = \begin{pmatrix} 0&1&2&2&2&1&1&0 \\ 1&0&0&2&0&2&0&2 \\ 2&0&1&0&2&0&2&2 \\ 2&2&0&0&2&2&2&2 \\ 2&0&2&2&0&2&1&0 \\ 1&2&0&2&2&0&1&0 \\ 1&0&2&2&1&1&1&0 \\ 0&2&2&2&0&0&0&1 \end{pmatrix},$$

$$\mathbf{P}_5 = \begin{pmatrix} 2&0&1&1&1&0&2&1 \\ 0&1&2&0&0&0&2&1 \\ 1&2&2&0&0&0&1&0 \\ 1&0&0&1&2&1&0&0 \\ 1&0&0&2&1&1&2&1 \\ 0&0&0&1&1&0&0&1 \\ 2&2&1&0&2&0&0&2 \\ 1&1&0&0&1&1&2&0 \end{pmatrix}, \mathbf{P}_6 = \begin{pmatrix} 0&1&1&0&0&2&1&1 \\ 1&2&2&2&2&2&1&2 \\ 1&2&0&1&1&2&0&2 \\ 0&2&1&0&2&1&2&0 \\ 0&2&1&2&0&2&0&1 \\ 2&2&2&1&2&2&1&2 \\ 1&1&0&2&0&1&2&0 \\ 1&2&2&0&1&2&0&2 \end{pmatrix}, \mathbf{P}_7 = \begin{pmatrix} 0&1&2&2&1&2&2&0 \\ 1&1&2&2&0&1&0&0 \\ 2&2&0&1&2&1&1&0 \\ 2&2&1&1&0&1&1&2 \\ 1&0&2&0&0&2&2&2 \\ 2&1&1&1&2&0&0&1 \\ 2&0&1&1&2&0&0&0 \\ 0&0&0&2&2&1&0&0 \end{pmatrix}, \mathbf{P}_8 = \begin{pmatrix} 1&2&0&0&0&2&0&2 \\ 2&1&0&2&1&1&0&1 \\ 0&0&2&1&0&1&1&1 \\ 0&2&1&0&1&0&0&1 \\ 0&1&0&1&1&1&0&1 \\ 2&1&1&0&1&2&2&1 \\ 0&0&1&0&0&2&2&1 \\ 2&1&1&1&1&1&1&0 \end{pmatrix},$$

$$\mathbf{P}_9 = \begin{pmatrix} 2&0&2&1&2&0&1&0 \\ 0&0&0&1&1&2&1&2 \\ 2&0&1&2&1&2&2&2 \\ 1&1&2&1&2&2&2&0 \\ 2&1&1&2&0&1&0&1 \\ 0&2&2&2&1&2&2&1 \\ 1&1&2&2&0&2&0&2 \\ 0&2&2&0&1&1&2&2 \end{pmatrix}, \mathbf{P}_{10} = \begin{pmatrix} 0&2&0&0&0&0&1&1 \\ 2&2&2&2&0&1&1&1 \\ 0&2&1&2&2&0&1&0 \\ 0&2&2&1&1&1&0&1 \\ 0&0&2&1&1&0&1&1 \\ 0&1&0&1&0&1&1&0 \\ 1&1&1&0&1&1&2&0 \\ 1&1&0&1&1&0&0&1 \end{pmatrix}, \mathbf{P}_{11} = \begin{pmatrix} 0&0&0&2&2&2&0&1 \\ 0&0&2&0&1&2&0&1 \\ 0&2&2&0&1&2&2&1 \\ 2&0&0&0&2&2&1&0 \\ 2&1&1&2&2&1&1&1 \\ 2&2&2&2&1&0&0&1 \\ 0&0&2&1&1&0&1&2 \\ 1&1&1&0&1&1&2&2 \end{pmatrix}, \mathbf{P}_{12} = \begin{pmatrix} 0&2&1&0&2&1&1&0 \\ 2&1&0&1&2&1&1&2 \\ 1&0&0&1&0&0&1&2 \\ 0&1&1&2&2&2&1&1 \\ 2&2&0&2&2&0&2&2 \\ 1&1&0&2&0&0&2&2 \\ 1&1&1&1&2&2&0&2 \\ 0&2&2&1&2&2&2&0 \end{pmatrix},$$

$$\mathbf{P}_{13} = \begin{pmatrix} 2&0&0&0&2&1&1&0 \\ 0&1&1&2&0&1&1&0 \\ 0&1&1&0&2&1&2&1 \\ 0&2&0&2&1&1&2&2 \\ 2&0&2&1&2&0&2&2 \\ 1&1&1&1&0&2&1&2 \\ 1&1&2&2&2&1&1&0 \\ 0&0&1&2&2&2&0&0 \end{pmatrix}, \mathbf{P}_{14} = \begin{pmatrix} 1&0&0&1&0&2&1&0 \\ 0&0&2&2&0&1&0&0 \\ 0&2&0&2&1&0&1&1 \\ 1&2&2&2&0&1&0&2 \\ 0&0&1&0&0&0&0&2 \\ 2&1&0&1&0&2&0&1 \\ 1&0&1&0&0&0&1&2 \\ 0&0&1&2&2&1&2&0 \end{pmatrix}, \mathbf{P}_{15} = \begin{pmatrix} 1&0&2&2&2&1&1&0 \\ 0&2&2&0&2&1&0&2 \\ 2&2&2&1&2&1&2&0 \\ 2&0&1&1&2&1&2&0 \\ 2&2&2&2&0&0&2&0 \\ 1&1&1&1&0&2&0&2 \\ 1&0&2&2&2&0&1&2 \\ 0&2&0&0&0&2&2&0 \end{pmatrix}, \mathbf{P}_{16} = \begin{pmatrix} 1&1&0&0&1&1&0&0 \\ 1&1&2&1&0&1&0&1 \\ 0&2&1&2&1&0&1&2 \\ 0&1&2&2&0&2&1&0 \\ 1&0&1&0&1&0&0&0 \\ 1&1&0&2&0&2&1&0 \\ 0&0&1&1&0&1&2&1 \\ 0&1&2&0&0&0&1&1 \end{pmatrix}.$$

Recovering *T*: The first and harder step to recover an equivalent linear transformation T is to solve the MinRank problem associated with the public matrices $\mathbf{P}_1, \ldots, \mathbf{P}_{16}$ and $r+1$, with $r = \lceil \log_q D \rceil = 2$. Using the minors modeling, we construct a degree 4 polynomial system in $2n$ variables. We can fix the two first coordinates of the vector $\mathbf{u}'' = (u'_0, u'_1, \ldots, u'_7)$ as 1 and 0 respectively. A solution for this system is

$$\mathbf{u}' = (1, 0, b^{5854}, b^{4879}, b^{2843}, b^{2676}, b^{6279}, b^{1845}, b^{6102}, b^{5619}, b^{5448}, b^{6022}, b^{1721}, b^{2632}, b^{3738}, b^{6170}).$$

Next we compute

$$\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right) = \begin{pmatrix} 1&0&0&0&0&b^{6158}&b^{1567}&b^{6415} \\ 0&1&0&0&0&b^{3943}&b^{4591}&b^{95} \\ 0&0&1&0&0&b^{4461}&b^{4216}&b^{3027} \\ 0&0&0&1&0&b^{3577}&b^{5899}&b^{1096} \\ 0&0&0&0&1&b^{6554}&b^{4266}&b^{907} \end{pmatrix},$$

and by solving the linear system

$$\mathbf{K}'\left(\sum_{i=0}^{2n-1} x_i \mathbf{P}_{i+1}\right) = \mathbf{0}_{(n-r)\times n},$$

we get another solution

$$\mathbf{v}' := (b^{1519}, b^{4750}, b^{4454}, b^{3326}, b^{2077}, b^{4519}, b^{3525}, b^{1978}, b^{5511}, b^{315}, b^{715}, b^{4722}, b^{5003}, b^{1895}, b^{2665}, b^{4505}).$$

Once we have two solution for the MinRank problem we compute

$$\mathbf{T}''^{-1} = \mathbf{U}\text{”}\mathbf{M}_{16}^{-1},$$

with $\mathbf{U}'' := [\mathbf{u}'|\cdots|\mathbf{u}'^{q^{n-1}}|\mathbf{v}'|\cdots|\mathbf{v}'^{q^{n-1}}]$, invert the output matrix to obtain $\mathbf{T}'' = [\mathbf{T}''_1|\mathbf{T}''_2]$, with

$$\mathbf{T}''_1 = \begin{pmatrix} 2&0&2&1&1&0&1&0\\ 1&2&2&2&0&2&0&0\\ 1&1&0&2&0&0&0&2\\ 2&2&1&2&0&1&0&0\\ 0&2&2&0&2&0&0&0\\ 2&1&0&1&1&2&0&0\\ 2&1&1&1&1&1&0&0\\ 2&2&1&0&2&1&0&1\\ 0&0&2&0&0&1&2&0\\ 1&2&2&0&0&0&0&1\\ 0&1&1&2&2&2&2&2\\ 2&2&0&1&0&1&2&1\\ 1&0&0&1&1&0&0&1\\ 1&2&2&1&1&2&1&0\\ 1&0&0&1&1&0&1&0\\ 0&0&2&0&2&2&1&1 \end{pmatrix}, \mathbf{T}''_2 = \begin{pmatrix} 1&1&0&0&2&1&1&1\\ 1&0&0&1&0&2&1&1\\ 2&1&1&2&2&1&1&0\\ 1&2&2&1&2&2&0&0\\ 0&1&1&2&0&1&2&1\\ 2&0&2&1&2&0&1&2\\ 2&0&2&2&2&0&2&1\\ 2&2&1&0&2&2&0&1\\ 2&1&0&1&2&1&1&0\\ 0&1&2&1&0&2&1&1\\ 2&2&2&1&1&0&1&2\\ 0&0&0&0&1&2&2&0\\ 0&2&0&0&2&1&1&0\\ 0&1&2&0&1&1&2&1\\ 1&2&0&2&0&1&2&1\\ 1&2&0&0&0&1&1&0 \end{pmatrix}$$

Recovering *S*: To find $\mathbf{W}'' := \mathbf{S}''\mathbf{M}_n = [\mathbf{w}''|\mathbf{w}''^q|\cdots|\mathbf{w}''^{q^{n-1}}]$, we find its first column $\mathbf{w}''$, which satisfy $\mathrm{Frob}_{j+1}(\mathbf{K}')\mathbf{w}'' = \mathbf{0}$, for $j = n-r, \ldots, n-1 = 7, 8$. By solving the overdetermined system

$$\begin{pmatrix} \mathbf{K}' \\ \mathrm{Frob}_7(\mathbf{K}') \end{pmatrix} \mathbf{w}'' = \begin{pmatrix} 1&0&0&0&0&b^{6158}&b^{1567}&b^{6415}\\ 0&1&0&0&0&b^{3943}&b^{4591}&b^{95}\\ 0&0&1&0&0&b^{4461}&b^{4216}&b^{3027}\\ 0&0&0&1&0&b^{3577}&b^{5899}&b^{1096}\\ 0&0&0&0&1&b^{6554}&b^{4266}&b^{907}\\ 1&0&0&0&0&b^{6426}&b^{2709}&b^{4325}\\ 0&1&0&0&0&b^{3501}&b^{3717}&b^{4405}\\ 0&0&1&0&0&b^{1487}&b^{3592}&b^{1009}\\ 0&0&0&1&0&b^{3379}&b^{4153}&b^{2552}\\ 0&0&0&0&1&b^{6558}&b^{1422}&b^{2489} \end{pmatrix} \mathbf{w}'' = \mathbf{0},$$

we obtain $\mathbf{w}'' = (b^{929}, b^{2174}, b^{2323}, b^{4231}, b^{3677}, b^{6313}, b^{2372}, b^{3245})$. We then compute

$$\mathbf{W}'' = \begin{pmatrix} b^{929} & b^{2787} & b^{1801} & b^{5403} & b^{3089} & b^{2707} & b^{1561} & b^{4683} \\ b^{2174} & b^{6522} & b^{6446} & b^{6218} & b^{5534} & b^{3482} & b^{3886} & b^{5098} \\ b^{2323} & b^{409} & b^{1227} & b^{3681} & b^{4483} & b^{329} & b^{987} & b^{2961} \\ b^{4231} & b^{6133} & b^{5279} & b^{2717} & b^{1591} & b^{4773} & b^{1199} & b^{3597} \\ b^{3677} & b^{4471} & b^{293} & b^{879} & b^{2637} & b^{1351} & b^{4053} & b^{5599} \\ b^{6313} & b^{5819} & b^{4337} & b^{6451} & b^{6233} & b^{5579} & b^{3617} & b^{4291} \\ b^{2372} & b^{556} & b^{1668} & b^{5004} & b^{1892} & b^{5676} & b^{3908} & b^{5164} \\ b^{3245} & b^{3175} & b^{2965} & b^{2335} & b^{445} & b^{1335} & b^{4005} & b^{5455} \end{pmatrix},$$

and

$$\mathbf{S}'' = \mathbf{W}''\mathbf{M}_8^{-1} = \begin{pmatrix} 2 & 2 & 2 & 1 & 2 & 0 & 0 & 2 \\ 1 & 2 & 1 & 1 & 2 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 & 0 & 2 & 1 & 0 \\ 2 & 2 & 1 & 1 & 2 & 1 & 2 & 2 \\ 0 & 2 & 1 & 2 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 & 2 & 2 & 0 \\ 0 & 1 & 1 & 0 & 2 & 2 & 0 & 1 \end{pmatrix}$$

Recovering core polynomials: To find our equivalent core polynomials H' and $\tilde{H}'$ we calculate $\mathbf{H}' = \mathbf{W}''^{-1}\left(\sum_{i=0}^{7} u'_i \mathbf{P}_{i+1}\right)\mathbf{W}''^{-t}$ as well as the value of $\tilde{\mathbf{H}}' = \mathbf{W}''^{-1}\left(\sum_{i=0}^{7} v'_i \mathbf{P}_{i+1}\right)\mathbf{W}''^{-t}$ and obtain

$$\mathbf{H}' = \begin{pmatrix} b^{2287} & b^{992} & b^{5159} & b^{4953} & b^{4144} & b^{6518} & b^{3920} & b^{4127} \\ b^{992} & b^{5165} & b^{5229} & b^{5023} & b^{4214} & b^{28} & b^{3990} & b^{4197} \\ b^{5159} & b^{5229} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{4953} & b^{5023} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{4144} & b^{4214} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{6518} & b^{28} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{3920} & b^{3990} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{4127} & b^{4197} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \ \tilde{\mathbf{H}}' = \begin{pmatrix} b^{87} & b^{1874} & b^{3075} & b^{2869} & b^{2060} & b^{4434} & b^{1836} & b^{2043} \\ b^{1874} & b^{6189} & b^{1832} & b^{1626} & b^{817} & b^{3191} & b^{593} & b^{800} \\ b^{3075} & b^{1832} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{2869} & b^{1626} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{2060} & b^{817} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{4434} & b^{3191} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{1836} & b^{593} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{2043} & b^{800} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Recovering the low degree polynomial: Once the core polynomials $\mathbf{H}' = [h_{ij}]$, $\tilde{\mathbf{H}}' = [\tilde{h}_{ij}]$ are recovered, our target is to build the low degree polynomial Ψ'' fundamental for the attacker to be able decrypt. So, we solve the following overdetermined systems

$$\begin{bmatrix} h_{1,r+1} & h_{1,r+2} & \cdots & h_{1,n-1} & h_{1,n} \\ \tilde{h}_{1,r+1} & \tilde{h}_{1,r+2} & \cdots & \tilde{h}_{1,n-1} & \tilde{h}_{1,n} \end{bmatrix}^{\top} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \begin{bmatrix} b^{5159} & b^{4953} & b^{4144} & b^{6518} & b^{3920} & b^{4127} \\ b^{3075} & b^{2869} & b^{2060} & b^{4434} & b^{1836} & b^{2043} \end{bmatrix}^{\top} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \mathbf{0},$$

$$\begin{bmatrix} h_{2,r+1} & h_{2,r+2} & \cdots & h_{2,n-1} & h_{2,n} \\ \tilde{h}_{2,r+1} & \tilde{h}_{2,r+2} & \cdots & \tilde{h}_{2,n-1} & \tilde{h}_{2,n} \end{bmatrix}^{\top} \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} b^{5229} & b^{5023} & b^{4214} & b^{28} & b^{3990} & b^{4197} \\ b^{1832} & b^{1626} & b^{817} & b^{3191} & b^{593} & b^{800} \end{bmatrix}^{\top} \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \mathbf{0},$$

and we obtain the solutions $[x_0, x_1]^\top = [b^{1418},\ b^{222}]^\top$ and $[y_0, y_1]^\top = [b^{2162},\ b^{2279}]^\top$. Then, we compute $b^{1418}\mathbf{H}' + b^{222}\tilde{\mathbf{H}}'$ and $b^{2162}\mathbf{H}' + b^{2279}\tilde{\mathbf{H}}'$ obtaining respectively

$$\begin{pmatrix} b^{106} & b^{6092} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{6092} & b^{3643} & b^{4437} & b^{4231} & b^{3422} & b^{5796} & b^{3198} & b^{3405} \\ 0 & b^{4437} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b^{4231} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b^{3422} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b^{5796} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b^{3198} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b^{3405} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} b^{1294} & b^{536} & b^{3144} & b^{2938} & b^{2129} & b^{4403} & b^{1905} & b^{2112} \\ b^{536} & b^{844} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{3144} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{2938} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{2129} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{4503} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{1905} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{2112} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Finally, we form the system

$$\begin{bmatrix} b^{4437} & b^{4231} & b^{3422} & b^{5796} & b^{3198} & b^{3405} \\ b^{3144} & b^{2938} & b^{2129} & b^{4403} & b^{1905} & b^{2112} \end{bmatrix}^\top \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} = \mathbf{0},$$

we a solution $[z_0,\ z_1]^\top = [b^{1024},\ b^{5597}]^\top$, and we use it to compute our low degree polynomial,

$$\begin{aligned} \Psi'' &= b^{1024}X(b^{1418}H' + b^{222}\tilde{H}') + X^q(b^{2162}H' + b^{2279}\tilde{H}') \\ &= b^{6441}X^9 + b^{2097}X^7 + b^{852}X^5 + b^{1130}X^3 \end{aligned}$$

A.2 Low rank matrix forms

$$\begin{pmatrix} * & * & * & & * & & \\ * & * & * & \dots & * & * & \dots & * \\ * & * & * & & * & & \\ & \vdots & & \ddots & & & \\ * & * & * & & * & & \\ & * & & & & & \\ & \vdots & & & & & \\ & * & & & & & \end{pmatrix}$$

Case $s = 0$.

$$\begin{pmatrix} * & * & * & & * & * & \dots & * \\ * & * & * & \dots & * & & & \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ * & & & & & & & \\ \vdots & & & & & & & \\ * & & & & & & & \end{pmatrix}$$

Case $s = 1$.

A.3 Comparison to Previous MinRank Analysis

It has been noted in [26] and [32], for example, that we may consider ZHFE to be a high degree instance of multi-HFE with two branches, i.e. $(X_1, X_2) \mapsto (F_1(X_1), F_2(X_2))$. This intuition is, however, mistaken. If we regard ZHFE as an instance of multi-HFE with $N = 2$, we must impose the relation $X_1 = X_2$, which considerably changes the rank analysis. This fact is missing from the discussion of the KS-attack complexity in both [26], before the low Q-rank property was discovered and in [32] after the low Q-rank property of ZHFE was announced in [23].

Although our complexity analysis is quite similar to the analysis of the multi-HFE attack of [2], there are, however, a few important distinctions that arise and elucidate the disparity between the complexity reported in [32] and our derived complexity. First, in multi-HFE, with N branches, the number of variables over the extension field required to express the quadratic function is N; thus the dimension of matrices required to construct a matrix representation for the central map is Nn, see [2, Proposition 5]. In ZHFE, a single variable is required over the extension field, and thus dimension n matrices are all that is required. Another distinction is that the rank bound for multi-HFE is due to a simultaneous degree bound in each of N variables over the extension field, producing a rank bound on the dimension Nn matrices of NR, where R is the rank, see [2, Lemma 3]. In ZHFE, the rank bound is due to the degree bound on Ψ, and only applies to a single variable; thus the rank bound is merely $R = r + 1$ where $r = \lceil log_q(D) \rceil$. Moreover, the minrank instance involves twice as many matrices in relation to the dimension of the matrices when compared with the minrank instances arising in multi-HFE. A final important distinction is that after the simultaneous MinRank is solved, an extra step, the derivation of an equivalent Ψ map, is required to recover a full private key.

These distinctions lead to vastly different complexity estimates on the KS-attack with minors modeling for ZHFE. In [32], the complexity of the KS-attack is reported as $\mathcal{O}(n^{2(R+1)\omega})$ citing the complexity estimate in [2]. Indeed, the complexity would be $\mathcal{O}(n^{(2R+1)\omega})$ for the KS-attack on a multi-HFE instance with Q-rank R according to [2, Proposition 13]. We are uncertain where the extra power of ω enters the analysis of [32]. We note that in [32] they claim that with an unrealistic linear algebra constant of $\omega = 2$ they obtain from this formula a complexity of 2^{138} for the KS-attack; however, computing $n^{2(R+1)\omega} = 55^{2(4+1)(2)} \approx 2^{115}$, whereas using the more realistic value $\omega = 2.3766$ we obtain 2^{138} as reported. This is apparently a minor editing mistake.

The reality is that the analysis in [2, Proposition 13] is related but not directly applicable to ZHFE since ZHFE does *not* correspond to multi-HFE with $N = 2$. Using an analysis analogous to the techniques in [2, Section 7], we derive above, using rank $R = r+1$, an estimate of $\mathcal{O}(n^{(r+2)\omega})$. Using the proposed parameters $q = 7$, $n = 55$, and $D = 105$ which imply $r = 3$, we obtain an attack complexity of 2^{64}. We thus conclude that ZHFE is broken.