On the Security and Key Generation of the ZHFE Encryption Scheme

Wenbin Zhang and Chik How Tan

Temasek Laboratories
National University of Singapore
tslzw@nus.edu.sg and tsltch@nus.edu.sg

Abstract. At PQCrypto'14 Porras, Baena and Ding proposed a new interesting construction to overcome the security weakness of the HFE encryption scheme, and called their new encryption scheme ZHFE. They provided experimental evidence for the security of ZHFE, and proposed the parameter set $(q, n, D) = (7, 55, 105)$ with claimed security level 2^{80} estimated by experiment. However there is an important gap in the state-of-the-art cryptanalysis of ZHFE, i.e., a sound theoretical estimation for the security level of ZHFE is missing. In this paper we fill in this gap by computing upper bounds for the Q-Rank and for the degree of regularity of ZHFE in terms of $\log_q D$, and thus providing such a theoretical estimation. For instance the security level of ZHFE(7,55,105) can now be estimated theoretically as at least 2^{96}. Moreover for the inefficient key generation of ZHFE, we also provide a solution to improve it significantly, making almost no computation needed.

Keywords: post-quantum cryptography, multivariate public key cryptography, HFE, ZHFE

1 Introduction

Multivariate public key cryptography (MPKC) [DGS06] is a candidate of post-quantum cryptography to resist future quantum computers. MPKC uses multivariate polynomials to represent its public key, and its security is backed on the fact that solving a random multivariate quadratic polynomial system is NP-hard [GJ79]. Since 1980's there have been many multivariate public key schemes constructed, but unfortunately most of them have been broken. One of the most important schemes is Patarin's Hidden Field Equations (HFE) encryption scheme [Pat96] which uses a low degree univariate polynomial F over the degree n extension field of $\mathbb{F}_q$ to construct the public key $P = T \circ F \circ S$ where S, T are two invertible affine transformations over $\mathbb{F}_q^n$. Though Patarin's original HFE has been broken [KS99, Cou01, FJ03, GJS06, DH11, BFP13], it has been developed into a big family. Some of its variants remain unbroken till now, for example HFEv for encryption and HFEv- for signature [PCG01, DY13, PCY$^+$15].

In 2014 Porras, Baena and Ding [PBD14a, PBD14b] proposed a very interesting extension of HFE for encryption to overcome the security weakness of HFE. The public key of their construction is $P = T \circ (F_1, F_2) \circ S$, where the central map (F_1, F_2) consists of two *high* degree univariate polynomials F_1, F_2 with a built-in

trapdoor. The trapdoor is that two linear combinations of all the Frobenius powers $(F_1)^{q^i}, (F_2)^{q^i}$, $0 \le i \le n-1$, are shifted by X, X^q respectively and then added up to a secret *low* degree polynomial Ψ. They called their encryption scheme ZHFE and showed that it is relatively efficient on decryption, but is very inefficient to generate the private key.

ZHFE uses a low degree polynomial Ψ as the trapdoor function and thus belongs to the HFE family. So those attacks on HFE, including direct algebraic attack [FJ03] and the Kipnis-Shamir MinRank attack (KS attack) [KS99, BFP13], might also be applicable to ZHFE and should be investigated carefully. In [PBD14a, PBD14b], experimental method was used to verify the security of ZHFE against the two types of attacks by looking at the computation time and memory consumed for relatively small parameters. The experiment also computed two important characters, the degree of regularity [DG10] and the quadratic rank (Q-Rank) [DH11], of the polynomial system which can determine the security. Based on the experiment results, they found that for relatively small parameters, instances of ZHFE match well with random instances, and thus concluded by guessing that both the degree of regularity and Q-Rank increases as the number of variables increases so that ZHFE is secure. They also recommended a practical parameter set ZHFE(7,55,105) and guessed that its security level is greater than 2^{80}.

Later on Perlner and Smith-Tone [PST16] at PQCrypto'16 provided an additional cryptanalysis for ZHFE. They considered differential attack and Isomorphism of Polynomials attack [WP05], and found that the two attacks are not applicable to ZHFE. They also tried to consider the degree of regularity and the Q-Rank, but the "Q-Rank" they defined is simply the usual rank rather than the one of [DH11, PBD14a, PBD14b]. Due to this issue of terminology, they did not came out a valid theoretical estimation for the two important characters.

Hence it is still missing in the state-of-the-art cryptanalysis of ZHFE the very much desired theoretical estimation for the degree of regularity, Q-Rank and thus for the security level of ZHFE. In this paper we fill in this gap by first computing an upper bound for the Q-Rank of ZHFE which is $\lfloor \log_q D \rfloor + 3$ if $q > 2$ and $\lfloor \log_2 D \rfloor + 4$ if $q = 2$. We then use this upper bound to compute an upper bound for the degree of regularity of ZHFE which is $\frac{1}{2}(q-1)(\lfloor \log_q D \rfloor + 3) + 2$ if $q > 2$ and $\frac{1}{2}\lfloor \log_2 D \rfloor + 4$ if $q = 2$. Hence we obtain the missing theoretical result for the security of ZHFE, and as a consequence, we improve the guessed security level 2^{80} of ZHFE(7,55,105) to a theoretically estimated level 2^{96}. In addition, we find that the Q-Rank and the degree of regularity of the instances in the experiment of [PBD14a, PBD14b] are still (much) less than the upper bound. This explains why the tested ZHFE instances performed the same as random instances.

In this paper we also consider the key generation of ZHFE. The original method for generating the private key of ZHFE [PBD14a, PBD14b] need to solve a large linear system for the about n^3 coefficients of the secret F_1, F_2, and is very time-consuming with complexity $O(n^{3\omega})$. Recently a new paper of Baena et al [BCE+16]

at PQCrypto'16 was devoted to improve the generation method and reduced the complexity to $O(n^{2\omega+1})$ by carefully studying the structure in the coefficients of F_1, F_2. However we find a very simple solution to the key generation which requires only very little computation, i.e., $O(\log_q D)$ $\mathbb{F}_q$-additions, and thus we can generate the private key almost immediately.

This paper is organized as follows. We first review the design of ZHFE in Section 2 and its state-of-the-art cryptanalysis in Section 3. We then present our new security analysis in Section 4 and our efficient solution to the key generation in Section 5. Finally we conclude this paper in Section 6.

2 The ZHFE Encryption Scheme

In this section, we shall recall Porras et al's novel encryption scheme ZHFE [PBD14a, PBD14b].

2.1 Design of the Core Map

Let $\mathbb{K}$ be a degree n extension of $\mathbb{F}_q$ and $\phi : \mathbb{K} \to \mathbb{F}_q^n$ the canonical isomorphism of vector spaces over $\mathbb{F}_q$. Firstly, we describe how to generate the core map of the scheme which consists of two high degree polynomials over $\mathbb{K}$,

$$F_1(X) = \sum a_{ij} X^{q^i+q^j} + \sum b_i X^{q^i} + c, \quad F_2(X) = \sum a'_{ij} X^{q^i+q^j} + \sum b'_i X^{q^i} + c'$$

whose coefficients will be determined later. Pick four linearized polynomials $L_{kl}(Y) = \sum_{i=0}^{n-1} u_{kl;i} Y^{q^i}$, $(1 \le k, l \le 2)$, with coefficients chosen randomly from $\mathbb{K}$. Then define

$$\Psi(X, F_1, F_2) = X \cdot [L_{11}(F_1) + L_{12}(F_2)] + X^q \cdot [L_{21}(F_1) + L_{22}(F_2)]. \tag{1}$$

Choose a positive integer D. The coefficients of F_1, F_2 are required to satisfy

$$\deg \Psi(X, F_1(X), F_2(X)) \le D. \tag{2}$$

By this degree restriction, a very large linear system can be obtained for the coefficients of F_1, F_2, and any nonzero solution gives a pair of F_1, F_2. Then compute

$$\begin{aligned} \Psi_D(X) &= \Psi(X, F_1(X), F_2(X)) \\ &= \sum_{0 \le i \le 1} \sum_{q^i+q^j+q^k \le D} a''_{ijk} X^{q^i+q^j+q^k} \sum_{q^i+q^j \le D} b''_{ij} X^{q^i+q^j} + \sum_{q^i \le D} c''_i X^{q^i}. \end{aligned} \tag{3}$$

Secondly, we describe how to invert the central map (F_1, F_2). Given any $Y_1, Y_2 \in \mathbb{K}$, since F_1, F_2 are of high degree, it is expected infeasible in general to solve

$$\begin{cases} F_1(X) = Y_1 \\ F_2(X) = Y_2 \end{cases} \tag{4}$$

directly. It is shown in [PBD14a, PBD14b] that Equations (4) can be solved with the help of $\Psi_D(X) = \Psi(X, Y_1, Y_2)$; i.e., solutions to (4) are also solutions to

$$\Psi_D(X) - \Psi(X, Y_1, Y_2) = 0. \tag{5}$$

Since the degree of Equation (5) is bounded by a relatively small D, Equation (5) can be solved efficiently using Berlekamp's algorithm, then each solution can be checked whether it is also a solution to the original equation (4).

2.2 The ZHFE Encryption Scheme

We can now describe the ZHFE encryption scheme. Its public map is

$$P = T \circ (\phi \times \phi) \circ (F_1, F_2) \circ \phi^{-1} \circ S : \mathbb{F}_q^n \to \mathbb{F}_q^{2n}$$

where $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $T : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{2n}$ are two randomly chosen invertible affine transformations.

Public Key The public key includes $\mathbb{F}_q$ and the polynomial map $P(x_1, \ldots, x_n)$.
Private Key The private key includes Ψ, D, Ψ_D and S, T.
Encryption The ciphertext of a plaintext $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is obtained by computing $(y_1, \ldots, y_{2n}) = P(x_1, \ldots, x_n)$.
Decryption A given ciphertext $\mathbf{y}$ is decrypted as follows:

1. Compute $(w_1, \ldots, w_{2n}) = T^{-1}(\mathbf{y})$.
2. Compute $(Y_1, Y_2) = (\phi^{-1}(w_1, \ldots, w_n), \phi^{-1}(w_{n+1}, \ldots, w_{2n}))$;
3. Substitute (Y_1, Y_2) into Equation (5), solve it by Berlekamp's algorithm, and let $\mathcal{Z}$ be the set of solutions.
4. For each $X \in \mathcal{Z}$, compute $S^{-1}(\phi(X))$ and check whether it is a solution to $P(\mathbf{x}) = \mathbf{y}$. Each solution is a candidate for the plaintext — additional redundant information must be added to determine which candidate is the correct plaintext.

In [PBD14b], parameters $(q, n, D) = (7, 55, 105)$ is suggested for ZHFE and its security level is claimed to be greater than 2^{80} with more features listed below.

Public Key	Private Key	Encryption Time	Decryption Time	Claimed Security
66 KB	11 KB	0.024 s	0.427 s	2^{80}

A drawback of ZHFE is the low efficiency of generating the secret F_1, F_2. In the rest of this paper, we will discuss the security and key generation of ZHFE.

3 Review of Cryptanalysis of ZHFE

ZHFE uses a low degree polynomial over the extension field $\mathbb{K}$ over $\mathbb{F}_q$ as the trapdoor, and thus it belongs to the HFE family. It may further be regarded as a Multi-HFE with two branches, but there is a significant difference. The usual HFE and

Multi-HFE use one or more polynomials over the extension field $\mathbb{K}$ which are of low degree (thus of low rank) as the core map. This low degree (low rank) is exactly the weakness of HFE and Multi-HFE. To overcome this weakness, ZHFE [PBD14a, PBD14b] is designed to use two high degree polynomial maps F_1, F_2 over $\mathbb{K}$ as its core map. The trapdoor is that, F_1, F_2 are related to a secret low degree map Ψ (1), which will be inverted, instead of inverting F_1, F_2, for decryption. This design is intended to increase the degree and rank of the core map to improve its security.

There are two types of attacks on the family of HFE schemes, i.e. direct algebraic attack [FJ03] and the Kipnis-Shamir MinRank Attack (KS attack) [KS99, BFP13]. The security of ZHFE against the two attacks was analyzed in [PBD14a, PBD14b], and then a few other attacks were also considered in [PST16]. In this section, we shall review the cryptanalysis of ZHFE from [PBD14a, PBD14b, PST16] and point out an important gap which is missing there.

3.1 Direct Algebraic Attacks

Direct algebraic attacks, such as F_4 [Fau99], F_5 [Fau02] and XL [CKPS00] try to solve the polynomial equation $P(\mathbf{x}) = \mathbf{y}$ directly, where P is the public polynomial map, and is applicable to all multivariate public key cryptosystems. The complexity of direct algebraic attacks is characterized by the degree of regularity of the polynomial system which is informally the highest degree achieved in the process of computing the Gröbner basis, cf. [DG10]. The degree of regularity has been a powerful tool for investigating the security of the HFE family [DG10, DH11, DY13, PCY$^+$15] and it has deep connection with another notion, the quadratic rank of the polynomial system [DH11].

We shall recall the notion of quadratic rank (Q-Rank for short) [DH11] in the following. The rank $\mathrm{Rank}(f)$ of a quadratic function $f = \sum a_{ij}x_ix_j + \sum b_ix_i + c : \mathbb{F}_q^n \to \mathbb{F}_q$ is defined as the rank of its associated quadratic form $\sum a_{ij}x_ix_j$. For a polynomial map $F = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, its Q-Rank is defined as the minimal rank of all nonzero linear combination of $f_1, \ldots, f_m$,

$$\text{Q-Rank}(F) = \min\{\mathrm{Rank}(f) \mid f \in Span_{\mathbb{F}_q}(f_1, \ldots, f_m), f \neq 0\}$$

where $Span_{\mathbb{F}_q}(f_1, \ldots, f_m)$ is the linear space over $\mathbb{F}_q$ spanned by $f_1, \ldots, f_m$. For polynomial

$$F(X) = \sum a_{ij}X^{q^i+q^j} + \sum b_iX^{q^i} + c,$$

over $\mathbb{K}$, its rank is also defined as the rank of its associated quadratic form $\sum a_{ij}X_iX_j$ where $X_i = X^{q^i}$. In addition, its Q-Rank is defined as the minimal rank of all its nonzero linear combinations of all the Frobenius powers F^{q^i} of F. Noting the equivalence between the multivariate representation and univariate representation of a polynomial, the two definitions of rank and Q-Rank are also equivalent [BFP13].

Ding and Hodges [DH11] found that the degree of regularity d_{reg} of a polynomial F is bounded by

$$d_{reg}(F) \leq \frac{(q-1)\text{Q-Rank}(F)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2 \qquad (6)$$

if Q-Rank$(F) > 1$. As a consequence, they [DH11] found that inverting HFE systems is polynomial on n if D, q are fixed, and is quasi-polynomial on n if D is of the scale $O(n^{\alpha})$. Therefore, to estimate the security level of ZHFE against direct algebraic attacks, it is very important to understand well its degree of regularity and Q-Rank.

A practical experimental approach to test the security strength of a scheme against direct algebraic attacks is to compute some instances and compare with random instances for relatively small parameters. One can do so by computing the Gröbner basis and comparing the time and memory needed, and calculating the degree of regularity and see how it changes as the parameters change. In [PBD14a, PBD14b], experiments were conducted to compute the Gröbner bases of instances of ZHFE and random instances using the F_4 function of MAGMA. Their experiments included instances with $q = 2$, $n \leq 40$ and $q = 7$, $n \leq 25$. They found that those relatively small instances of ZHFE match very well with random instances on time, memory and the degree of regularity. Based on the experiment results they concluded that ZHFE would perform generally as random instances against direct algebraic attack, and especially the degree of regularity would grow as n grows.

However, only experiments is not sufficient to guarantee the security level as only a small range of parameters are tested. Theoretical estimation of the degree of regularity and thus of the complexity is necessary, as it can ensure what will happen for parameters beyond the range that can be practically tested. Unfortunately such theoretical estimation is missing in [PBD14a, PBD14b]. This is an important gap which should be filled in.

3.2 The Kipnis-Shamir MinRank Attack

In 1999 Kipnis and Shamir [KS99] proposed an attack to recover the secret key of HFE. Their attack relies on the fact that the core map of HFE has a small rank and thus can be converted into the MinRank Problem.

The MinRank Problem: Let $\mathbb{K}$ be a finite field and $M_1, \ldots, M_m$ $t \times t$ matrices over $\mathbb{K}$. Given a positive integer $r \leq t$, find scalars $\lambda_1, \ldots, \lambda_m$, not all zero, such that

$$\text{Rank}(\lambda_1 M_1 + \cdots + \lambda_m M_m) \leq r.$$

It is well known that this is generally an NP-hard problem, but if r is small, then the MinRank problem is not too hard to compute. Kipnis and Shamir [KS99] proposed a method to solve the MinRank problem for small r and thus gave an attacking method to HFE though not breaking it.

In 2013, Bettale, Faugère and Perret improved the KS attack significantly and break HFE and multi-HFE [BFP13]. They showed that the rank of HFE also gives the Q-Rank of the public polynomial map, then reduced the MinRank problem from the extension field $\mathbb{K}$ to the much smaller field $\mathbb{F}_q$ and thus reduced the complexity considerably. The complexity of their improved KS attack is estimated as $O(n^{(r+1)\omega})$ where r is the Q-Rank of the HFE scheme, and thus breaks HFE with practical parameters. Their attack also breaks multi-HFE with k branches with complexity $O(n^{k(r+1)\omega})$. Therefore the Q-Rank of the polynomial system is not only important for the degree of regularity and direct algebraic attack, but also determines the security level against Bettale, Faugère and Perret's (BFP's for short) KS attack.

In [PBD14b], the Q-Rank of the suggested parameter set ZHFE(7,55,105) is showed by experiments to be greater than 3. However for the case that whether the Q-Rank is 4, their experiment did not stop but reached the set time limit and memory limit. Based on this experiment result, it was then guessed in [PBD14b] that for ZHFE: 1) *the Q-rank grows as n grows*; 2) *the Q-rank is independent of D*; 3) *in principle there seems no obvious way to recover* Ψ.

Later on [PST16] tried to analyze the Q-Rank of ZHFE for $q > 2$. However, it should be clarified that the "Q-Rank" of a polynomial $F = \sum a_{ij} X^{q^i+q^j}$ over $\mathbb{K}$ in [PST16, Section 3] is defined as the rank of the matrix of the associated quadratic form, while the "Q-Rank" of F defined here and in [PBD14a, PBD14b] is the minimal rank of all nonzero linear combinations of all the Frobenius powers F^{q^i} of F. Namely the "Q-Rank" of [PST16] is *NOT* the "Q-Rank" defined here and in [PBD14a, PBD14b]. In [PST16, Subsection 3], they noticed that the rank of $L_{11}(F_1) + L_{12}(F_2)$ is no more than $\lceil \log_q D \rceil + 2$, and then claimed that the rank of (F_1, F_2) is bounded by $\lceil \log_q D \rceil + 2$ if L_{ij} are nonsingular, and can be increased easily by choosing singular L_{ij} with small co-rank; but due to their definition, they did not conclude the Q-Rank of ZHFE. Therefore, theoretical analysis of the Q-Rank of ZHFE and the security of ZHFE against BFP' KS attack is still missing in [PST16].

3.3 Other Attacks

[PST16] also considered a few other attacks. They computed the differential symmetry of the secret Ψ and found no evidence to attack ZHFE by the symmetry. They then further proved that Ψ does not have nontrivial differential invariant and thus differential attack is not applicable to ZHFE. The number of equivalent and nonequivalent keys are estimated in [PST16], and found to be large enough to prevent the IP-basded equivalent key attacks [WP05].

4 New Security Analysis of ZHFE

From the preceding review on current cryptanalysis of ZHFE, [PBD14a, PBD14b] showed convincing experimental results to support that ZHFE is like random systems against direct algebraic attack for relatively small parameters, but lacked a

theoretical analysis. For BFP's KS attack, their experiment results only showed that the Q-Rank of ZHFE(7,55,105) is greater than 3, and again theoretical analysis on the Q-Rank is lacked. [PST16] found that a few other attacks are not applicable to ZHFE and also considered the rank of ZHFE — but unfortunately not the Q-Rank. Therefore a thorough theoretical analysis on the Q-Rank of ZHFE is still missing in the cryptanalysis of ZHFE, but is necessary to ensure the security level of ZHFE.

In this section, we shall fill this gap. We will first deduce a linear system determining the two maps

$$\bar{F}_1 = L_{11}(F_1) + L_{12}(F_2), \quad \bar{F}_2 = L_{21}(F_1) + L_{22}(F_2).$$

which unexpectedly turns out to be so simple that no computation is needed to solve it. We then apply this technical result to give an upper bound for the Q-Rank of ZHFE. Finally we apply this upper bound to give the missing theoretical estimation on the security of ZHFE against direct algebraic attack and BFP's KS attack.

4.1 Computing $L_{11}(F_1) + L_{12}(F_2)$ and $L_{21}(F_1) + L_{22}(F_2)$

Here we shall compute the conditions for the coefficients of

$$\bar{F}_1 = L_{11}(F_1) + L_{12}(F_2), \quad \bar{F}_2 = L_{21}(F_1) + L_{22}(F_2)$$

to satisfy the degree restriction (2) on Ψ. Since the two cases 1) $q > 2$ and 2) $q = 2$ are different, we shall deal with them separately.

First Case: $q > 2$. Write

$$\begin{aligned}
\bar{F}_1(X) &= \sum_{0\le i\le j\le n-1} \bar{a}_{ij} X^{q^i+q^j} + \sum_{0\le i\le n-1} \bar{b}_i X^{q^i} + \bar{c} \\
\bar{F}_2(X) &= \sum_{0\le i\le j\le n-1} \bar{a}'_{ij} X^{q^i+q^j} + \sum_{0\le i\le n-1} \bar{b}'_i X^{q^i} + \bar{c}'
\end{aligned}$$

Then by calculation, we have

$$\begin{aligned}
\Psi(X, F_1, F_2) = &\sum_{1\le i\le j\le n-1} \bar{a}'_{ij} X^{q+q^i+q^j} + \sum_{2\le i\le j\le n-1} \bar{a}_{ij} X^{1+q^i+q^j} + \sum_{1\le i\le n-1} \bar{b}'_i X^{q+q^i} \\
&+ \sum_{1\le j\le n-1} (\bar{a}_{1j} + \bar{a}'_{0j}) X^{1+q+q^j} + \sum_{1\le j\le n-1} \bar{a}_{0j} X^{2+q^j} + \sum_{2\le i\le n-1} \bar{b}_i X^{1+q^i} \\
&+ \bar{a}'_{00} X^{2+q} + (\bar{b}_1 + \bar{b}'_0) X^{1+q} + \bar{c}' X^q + \bar{a}_{00} X^3 + \bar{b}_0 X^2 + \bar{c} X. \qquad (7)
\end{aligned}$$

Notice that the highest degree is of the form $q+2q^{n-1}$. So we shall separate the degree range by $q + 2q^{s-1} < D \le q + 2q^s$, $1 \le s \le n-1$. Then $\deg \Psi(X, F_1, F_2) \le q + 2q^s$ if and only if

$$\begin{cases}
\bar{a}_{ij} = 0, & 2 \le i < j,\ j > s \\
\bar{a}'_{ij} = 0, & 1 \le i < j,\ j > s \\
\bar{a}_{0j} = 0, \bar{a}'_{0j} = -\bar{a}_{1j}, & j > s \\
\bar{b}_i = 0, \bar{b}'_i = 0, & i > s
\end{cases} \qquad (8)$$

Therefore, to find $\bar{F}_1, \bar{F}_2$, we just need to solve this system of linear equations whose solution is already obvious and does not need any computation. In other words, the two secret maps are

$$\bar{F}_1 = \sum_{1\le j\le n-1} \bar{a}_{1j} X^{q+q^j} + \sum_{0\le i\le j\le s, i\neq 1} \bar{a}_{ij} X^{q^i+q^j} + \sum_{0\le i\le s} \bar{b}_i X^{q^i} + \bar{c} \tag{9}$$

$$\bar{F}_2 = \sum_{0\le j\le n-1} \bar{a}'_{0j} X^{1+q^j} + \sum_{1\le i\le j\le s} \bar{a}'_{ij} X^{q^i+q^j} + \sum_{0\le i\le s} \bar{b}'_i X^{q^i} + \bar{c}' \tag{10}$$

where the coefficients can be arbitrarily chosen with the only restriction

$$\bar{a}'_{0j} = -\bar{a}_{1j}, \quad j > s.$$

The secret Ψ_D is then computed by (7) requiring only $s+1 \approx \log_q D$ $\mathbb{F}_q$-additions.

Second Case: $q = 2$. Write

$$\bar{F}_1(X) = \sum_{0\le i<j\le n-1} \bar{a}_{ij} X^{2^i+2^j} + \sum_{0\le i\le n-1} \bar{b}_i X^{2^i} + \bar{c}$$

$$\bar{F}_2(X) = \sum_{0\le i<j\le n-1} \bar{a}'_{ij} X^{2^i+2^j} + \sum_{0\le i\le n-1} \bar{b}'_i X^{2^i} + \bar{c}'$$

Notice that there is no $\bar{a}_{ii}, \bar{a}'_{ii}$ since $X^{2^i+2^i} = X^{2^{i+1}}$. By computation,

$$\begin{aligned}\Psi(X, F_1, F_2) = &\sum_{1\le i<j<n} \bar{a}'_{ij} X^{2+2^i+2^j} + \sum_{2\le i<j<n} \bar{a}_{ij} X^{1+2^i+2^j} + \sum_{2\le i<n} (\bar{a}_{1i} + \bar{a}'_{0i}) X^{1+2+2^i} \\ &+ \sum_{2\le i\le n-1} (\bar{a}_{0i} + \bar{b}'_i) X^{2+2^i} + \sum_{3\le i\le n-1} \bar{b}_i X^{1+2^i} + (\bar{a}'_{01} + \bar{b}_2) X^5 \\ &+ (\bar{a}_{01} + \bar{b}'_1) X^4 + (\bar{b}_1 + \bar{b}'_0) X^3 + (\bar{b}_0 + \bar{c}') X^2 + \bar{c} X. \end{aligned} \tag{11}$$

The highest degree is of the form $2 + 2^{n-2} + 2^{n-1}$. So we shall separate the degree range by $2+2^{s-2}+2^{s-1} < D \le 2+2^{s-1}+2^s$, $2 \le s \le n-1$. Then $\deg \Psi(X, F_1, F_2) \le 2 + 2^{s-1} + 2^s$ if and only if

$$\begin{cases} \bar{a}_{ij} = 0, & 2 \le i < j,\ j > s \\ \bar{a}'_{ij} = 0, & 1 \le i < j,\ j > s \\ \bar{a}'_{0j} = \bar{a}_{1j}, \bar{b}'_j = \bar{a}_{0j}, \bar{b}_j = 0, & j > s \end{cases} \tag{12}$$

So we already solve the two secret maps

$$\bar{F}_1 = \sum_{j=2}^{n-1} \bar{a}_{1j} X^{2+2^j} + \sum_{j=1}^{n-1} \bar{a}_{0j} X^{1+2^j} + \sum_{2\le i<j\le s} \bar{a}_{ij} X^{2^i+2^j} + \sum_{0\le i\le s} \bar{b}_i X^{2^i} + \bar{c} \tag{13}$$

$$\bar{F}_2 = \sum_{j=0}^{n-1} \bar{a}'_{0j} X^{1+2^i} + \sum_{j=0}^{n-1} \bar{b}'_j X^{2^j} + \sum_{1\le i<j\le s} \bar{a}'_{ij} X^{2^i+2^j} + \bar{c}' \tag{14}$$

where the coefficients are arbitrarily chosen with the only restriction

$$\bar{a}'_{0j} = \bar{a}_{1j}, \quad \bar{b}'_j = \bar{a}_{0j}, \quad j > s$$

The secret Ψ_D is then computed by (11) requiring only $2s+2 \approx 2\log_2 D$ $\mathbb{F}_2$-additions.

4.2 Upper Bound for the Q-Rank of ZHFE

Notice that $\bar{F}_1, \bar{F}_2$ can have maximum degree $q + q^{n-1}$ and $1 + q^{n-1}$ respectively. Although their maximum degree can be this high, their ranks are still small.

Theorem 1. *We have the following upper bound on the Q-Rank of ZHFE(q, n, D):*

1. *If $q > 2$, $D \leq q + 2q^s$, then*

$$\textit{Q-Rank } (\textit{ZHFE}) \leq s + 2 \leq \lfloor \log_q D \rfloor + 3.$$

2. *If $q = 2$, $D \leq 2 + 2^{s-1} + 2^s$, then*

$$\textit{Q-Rank } (\textit{ZHFE}) \leq s + 3 \leq \lfloor \log_2 D \rfloor + 4,$$

Proof. From the calculation in Subsection 4.1, if $q > 2$ is odd, the associated symmetric matrices of the quadratic forms of $\bar{F}_1, \bar{F}_2$ are

$$\begin{pmatrix} \bar{a}_{00} & \bar{a}_{01}/2 & \cdots & \bar{a}_{0s}/2 & & \\ \bar{a}_{01}/2 & \bar{a}_{11} & \cdots & \bar{a}_{1s}/2 & \cdots & \bar{a}_{1,n-1}/2 \\ \vdots & \vdots & & \vdots & & \\ \bar{a}_{0s}/2 & \bar{a}_{1s}/2 & \cdots & \bar{a}_{ss} & & \\ & \vdots & & & & \\ & \bar{a}_{1,n-1}/2 & & & & \end{pmatrix}, \quad \begin{pmatrix} \bar{a}'_{00} & \cdots & \bar{a}'_{0s}/2 & \cdots & \bar{a}'_{0,n-1}/2 \\ \vdots & & \vdots & & \\ \bar{a}'_{0s}/2 & \cdots & \bar{a}'_{ss} & & \\ \vdots & & & & \\ \bar{a}'_{0,n-1}/2 & & & & \end{pmatrix}$$

respectively. If $q > 2$ even, the two matrices are

$$\begin{pmatrix} 0 & \bar{a}_{01} & \cdots & \bar{a}_{0s} & & \\ \bar{a}_{01} & 0 & \cdots & \bar{a}_{1s} & \cdots & \bar{a}_{1,n-1} \\ \vdots & \vdots & & \vdots & & \\ \bar{a}_{0s} & \bar{a}_{1s} & \cdots & 0 & & \\ & \vdots & & & & \\ & \bar{a}_{1,n-1} & & & & \end{pmatrix}, \quad \begin{pmatrix} 0 & \cdots & \bar{a}'_{0s} & \cdots & \bar{a}'_{0,n-1} \\ \vdots & & \vdots & & \\ \bar{a}'_{0s} & \cdots & 0 & & \\ \vdots & & & & \\ \bar{a}'_{0,n-1} & & & & \end{pmatrix}$$

respectively, with zero diagonal. It is then obvious that

$$\mathrm{Rank}(\bar{F}_1) \leq s + 2 \quad \text{and} \quad \mathrm{Rank}(\bar{F}_2) \leq s + 2.$$

If $q = 2$, the two matrices are

$$\begin{pmatrix} 0 & \bar{a}_{01} & \cdots & \bar{a}_{0s} & \cdots & \bar{a}_{0,n-1} \\ \bar{a}_{01} & 0 & \cdots & \bar{a}_{1s} & \cdots & \bar{a}_{1,n-1} \\ \vdots & \vdots & & \vdots & & \\ \bar{a}_{0s} & \bar{a}_{1s} & \cdots & 0 & & \\ \vdots & \vdots & & & & \\ \bar{a}_{0,n-1} & \bar{a}_{1,n-1} & & & & \end{pmatrix}, \quad \begin{pmatrix} 0 & \cdots & \bar{a}'_{0s} & \cdots & \bar{a}'_{0,n-1} \\ \vdots & & \vdots & & \\ \bar{a}'_{0s} & \cdots & 0 & & \\ \vdots & & & & \\ \bar{a}'_{0,n-1} & & & & \end{pmatrix}$$

respectively. Then it is also obvious that their ranks are $\leq s+3$ and ≤ 2 respectively.

$$\text{Rank}(\bar{F}_1) \leq s+3 \quad \text{and} \quad \text{Rank}(\bar{F}_2) \leq s+2.$$

Since $\bar{F}_1, \bar{F}_2$ are linear combinations of the Frobenius powers of F_1, F_2, the Q-Rank of (F_1, F_2) is bounded above by the ranks of $\bar{F}_1, \bar{F}_2$. Therefore we have the first part of the claimed upper bound for the Q-Rank of ZHFE.

Notice that for $q+2q^{s-1} < D \leq q+2q^s$ or $2+2^{s-2}+2^{s-1} < D \leq 2+2^{s-1}+2^s$, we have $s-1 < \log_q D < s+1$, thus $\lfloor \log_q D \rfloor = s-1$ or $\lfloor \log_q D \rfloor = s$. So $s \leq \lfloor \log_q D \rfloor + 1$ and the second part of the claimed upper bound follows immediately.

As an example, for ZHFE(7,55,105), $105 = q + 2q^s$ where $q = 7$ and $s = 2$, so its Q-Rank $r \leq 4$. From [PBD14b], the Q-Rank of ZHFE(7,55,105) $r > 3$, so $r = 4$. This example shows that the above estimation is tight.

From this result, we see that the Q-rank of ZHFE is independent on n, but dependent on the degree D of the secret Ψ. Moreover, we will show next how to apply BFP's KS attack [BFP13] to recover the secret Ψ. Therefore the three guesses of [PBD14b] on the Q-Rank, summarized in Subsection 3.2 of this paper, are incorrect. In addition, we remark that the upper bound on the rank of $\bar{F}_1, \bar{F}_2$ when $q > 2$ was also noticed in [PST16], but they did not use it to conclude an upper bound for the Q-Rank of ZHFE. Instead, they concluded that they can choose L_{ij} and F_1, F_2 to make (F_1, F_2) have high rank. The reason is that they defined the Q-Rank as the usual rank.

4.3 BFP's KS Attack

As pointed out in [PBD14b], ZHFE can be regarded as a simple case of multi-HFE with two branches, i.e., $\mathbb{K}^2 \to \mathbb{K}^2$, $(X_1, X_2) \mapsto (F_1(X_1), F_2(X_2))$. Based on this viewpoint, we next sketch how to apply BFP's KS attack [BFP13] to attack ZHFE by recovering $\bar{F}_1, \bar{F}_2$ and Ψ, and estimate its complexity.

$\bar{F}_1$ has high degree $q + q^{n-1}$ but small Q-Rank (bounded by $s+2$ if $q = 2$ and $s+3$ if $q > 3$), and $\bar{F}_2$ also has high degree $1 + q^{n-1}$ but small Q-Rank bounded by $s+2$. So the first step is to apply BFP's KS attack to compute $\bar{F}_1, \bar{F}_2$. Since there are two branches, the complexity is $O(n^{2(r+1)\omega})$ in terms of $\mathbb{F}_q$ operations. So the

complexity of the first step is, $O(n^{(2s+6)\omega})$ if $q > 2$ for small q, and $O(n^{(2s+8)\omega})$ if $q = 2$.

Next recovering Ψ can be done with the simple relation

$$\Psi = X\bar{F}_1 + X^q\bar{F}_2.$$

More explicitly, once we have found two linearly independent G_1, G_2 with rank $s+2$ (if $q > 2$ and $s+3$ if $q > 3$) and $s+2$ respectively, then $\bar{F}_1, \bar{F}_2$ are linear combinations of the Frobenius powers of G_1, G_2, and thus there are coefficients such that

$$\Psi(X, G_1, G_2) = X(u_1G_1 + u_2G_1^q + \cdots + u_nG_1^{q^{n-1}} + v_1G_2 + v_2G_2^q \cdots + v_nG_2^{q^{n-1}})$$
$$+X^q(u_{n+1}G_1 + u_{n+2}G_1^q + \cdots + u_{2n}G_1^{q^{n-1}} + v_{n+1}G_2 + v_{n+2}G_2^q + \cdots + v_{2n}G_2^{q^{n-1}})$$

satisfies the degree condition $\deg \Psi \leq D$. So to recover Ψ, we can just find these coefficients by solving an overdefined linear system with $4n$ variables. Such a linear system can be solved using only part of its relations, say $8n$ of them, and thus the complexity is $O(n^3)$.

Therefore the complexity of BFP's KS attack is dominated by the first step of recovering $\bar{F}_1, \bar{F}_2$, and thus is estimated as

$$O(n^{2(r+1)\omega}) = \begin{cases} O(n^{(2s+6)\omega}) \approx O(n^{(2\lfloor \log_q D \rfloor + 8)\omega}), & \text{if } q > 2, \\ O(n^{(2s+8)\omega}) \approx O(n^{(2\lfloor \log_2 D \rfloor + 10)\omega}), & \text{if } q = 2, \end{cases}$$

in terms of $\mathbb{F}_q$ operations. Notice that this complexity is polynomial on n but exponential on $\log_q D$. This seems not so satisfying as it is not exponential on n and that D is small in practice, but it is still secure enough for practical parameters. For example, if choosing $\omega = 2$, the security level of ZHFE(7,55,105) against BFP's KS attack is estimated as at least 2^{138}. As comparison, the HFE system with the same set of parameters $(q, n, D) = (7, 55, 105)$ has Q-Rank 3 and its security level against BFP's KS attack is $n^{(r+1)\omega} = 55^{4\omega} = 2^{46}$. The key improvement of ZHFE is that it has bigger Q-Rank 4 and it has two branches, i.e. its number of equations double that of HFE.

4.4 Direct Algebraic Attacks

By Ding and Hodges' formula [DH11] for the degree of regularity, we have the following consequence of Theorem 1.

Theorem 2. *Let d_{reg} be the degree of regularity of the public polynomial map P of ZHFE(q, n, D).*

1. *If $q > 2$, $D \leq q + 2q^s$, then*

$$d_{reg} \leq \frac{(q-1)(s+2)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q D \rfloor + 3)}{2} + 2.$$

2. If $q = 2$, $D \leq 2 + 2^{s-1} + 2^s$, then

$$d_{reg} \leq \frac{s+3}{2} + 2 \leq \frac{\lfloor \log_2 D \rfloor + 4}{2} + 2 = \frac{1}{2}\lfloor \log_2 D \rfloor + 4.$$

For instance, the degree of regularity of ZHFE(2,n,500) is bounded by 8, and the one of ZHFE(7,n,105) is bounded by 14. In the experiment of [PBD14a, PBD14b], the highest degree of regularity achieved for the tested instances is 5 for ZHFE(2,n,500) in [PBD14a] and 6 for ZHFE(7,n,105) in [PBD14b], both of which are only about half of our upper bounds. This explains why the tested instances were like random instances when being solved by direct algebraic attack, and suggests that if bigger parameters exceeding the upper bound were tested, we might see significant drop on computation time compared to random instances. This will require more powerful computer and/or more time to do the experiment, but such bigger parameters should be tested in the future.

Comparing with the upper bound for the degree of regularity of HFE (6),

$$d_{reg}(\text{HFE}) \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2,$$

we see the upper bound for ZHFE is more than the one for HFE with difference

$$(q-1) \quad \text{if } q > 2, \quad \text{and} \quad \frac{3}{2} \quad \text{if } q = 2.$$

Therefore ZHFE(q, n, D) can be more secure than HFE(q, n, D) if q is bigger. It should be noted that a little change of the degree of regularity can result a difference on the complexity by a factor of a few thousand. For instance, following [DY13, PCY+15], the security of HFE(7,55,105) and ZHFE(7,55,105) against direct algebraic attacks F_4, F_5 can be estimated as

$$C_{F_4/F_5}(\text{HFE } (7,55,105)) \geq 3\tau T^2 = 3\binom{55}{2}\binom{55}{11}^2 \geq 2^{85.7}$$
$$C_{F_4/F_5}(\text{ZHFE } (7,55,105)) \geq 3\tau T^2 = 3\binom{55}{2}\binom{55}{14}^2 \geq 2^{96}$$

respectively. Namely both HFE(7,55,105) and ZHFE(7,55,105) are practically secure against direct algebraic attacks. However it should be noted that their security level against BFP's KS attack is 2^{46} and 2^{138} respectively. Hence our theoretical estimation for the security level of ZHFE(7,55,105) is at least 2^{96}.

5 Improving the Key Generation of ZHFE

The private key F_1, F_2, Ψ of ZHFE are defined subject to the following condition

$$\deg \Psi = \deg(X \cdot [L_{11}(F_1) + L_{12}(F_2)] + X^q \cdot [L_{21}(F_1) + L_{22}(F_2)]) \leq D.$$

Thus to generate F_1, F_2, one need to solve a large linear system derived from the vanishing coefficients of Ψ. Notice that this linear system has the coefficients of F_1, F_2 as the variables whose number is about n^3. The method of [PBD14a, PBD14b] solves F_1, F_2 with complexity $O(n^{3\omega})$ which is very high as it may take several days to generate a practical key. Later on another paper [BCE+16] is devoted to improve the key generation and reduces the complexity to $O(n^{2\omega+1})$. Here we shall propose a solution to improve the key generation which requires only little computation and is almost immediate.

Recall that in Subsection 4.1, we have computed

$$\bar{F}_1 = L_{11}(F_1) + L_{12}(F_2), \quad \bar{F}_2 = L_{21}(F_1) + L_{22}(F_2).$$

and expressed them in terms of (9), (10) if $q > 2$, and (13), (14) if $q = 2$, whose coefficients can be arbitrarily chosen *without* any computation. In addition, the secret Ψ_D is computed by (7) if $q > 2$ and (11) if $q = 2$ which requires only very *little* computation, i.e., about $\log_q D$ if $q > 2$, or $2\log_2 D$ if $q = 2$, additions of $\mathbb{F}_q$ elements.

Our solution then is to forget F_1, F_2, L_{ij}, but regard $\bar{F}_1, \bar{F}_2$ as two individual maps, and use the pair $(\bar{F}_1, \bar{F}_2)$ as the core map of ZHFE instead of (F_1, F_2). So the public map becomes

$$P = T \circ (\phi \times \phi) \circ (\bar{F}_1, \bar{F}_2) \circ \phi^{-1} \circ S : \mathbb{F}_q^n \to \mathbb{F}_q^{2n}$$

and in the decryption step, we solve the following equation

$$\Psi_D(X) - (XY_1 + X^q Y_2) = 0$$

instead of Equation (5), while the rest of the scheme remain the same. Namely we redesign the Ψ of ZHFE as

$$\Psi = X\bar{F}_1 + X^q \bar{F}_2.$$

instead of (1), and use $(\bar{F}_1, \bar{F}_2)$ as the core map instead of (F_1, F_2). With this simple change, the original time-consuming key generation of ZHFE now becomes almost immediate with very little computation, i.e., about $\log_q D$ $\mathbb{F}_q$-additions if $q > 2$, or $2\log_2 D$ $\mathbb{F}_2$-additions if $q = 2$. We remark that our new design may be regarded as equivalent to the original one. This is because that $(\bar{F}_1, \bar{F}_2)$ is a linear transformation of (F_1, F_2), and if this linear transformation is nonsingular, then (F_1, F_2) is also a linear combination of $(\bar{F}_1, \bar{F}_2)$. If one still wants to compute (F_1, F_2) then just compute the inverse of the linear transformation with complexity $O(n^\omega)$, better than the improvement $O(n^{2\omega+1})$ of [BCE+16].

One may concern if this change affects the security of ZHFE, but we claim that it does not. From the security analysis in the preceding section, we see that to attack ZHFE, one actually does not need to recover F_1, F_2 and the four linear maps L_{ij}, but only need $\bar{F}_1, \bar{F}_2$ which are sufficient to recover the secret Ψ. Namely the two maps F_1, F_2 and the four linear maps L_{ij} actually do not matter, and what matters is $\bar{F}_1, \bar{F}_2$. So the security analysis is not changed and thus our redesign of ZHFE does not change the security.

6 Conclusion

ZHFE is a new novel extension of the HFE encryption scheme and is designed to overcome the security weakness of HFE. There has been cryptanalysis of ZHFE and especially experimental evidence for its security, however a sound theoretical estimation of its security is still missing. We filled in this gap in this paper by providing such a theoretical estimation for the security of ZHFE. We achieved this goal by first computing for the Q-Rank of ZHFE(q, n, D) an upper bound which is $\lfloor \log_q D \rfloor + 3$ if $q > 2$ and $\lfloor \log_2 D \rfloor + 4$ if $q = 2$. We then estimated the security level, in terms of $\mathbb{F}_q$ operations, of ZHFE against Bettale, et al's improved Kipnis-Shamir MinRank attack as $O(n^{(2\lfloor \log_q D \rfloor + 8)\omega})$ for small $q > 2$, and $O(n^{(2\lfloor \log_2 D \rfloor + 10)\omega})$ for $q = 2$, where $2 \leq \omega \leq 3$ depends on the Gaussian elimination algorithm chosen. For instance the security level of ZHFE(7,55,105) against this attack is estimated as at least 2^{138}. We further applied our upper bound on the Q-Rank to give an upper bound for the degree of regularity of ZHFE which is $\frac{(q-1)(\lfloor \log_q D \rfloor + 3)}{2} + 2$ if $q > 2$ and $\frac{1}{2}\lfloor \log_2 D \rfloor + 4$ if $q = 2$. Consequently the security level of ZHFE(7,55,105) against the direct algebraic attack F_4 is estimated as at least 2^{96}. Therefore we conclude that ZHFE does increase the degree of regularity and Q-Rank of HFE and thus improve the security to have practical and secure parameters. The security estimation here may still be improved, and more refined analysis and experiment should be carried out in the future to have a more solid estimation.

Moreover we also provided a solution to improve the inefficient key generation of ZHFE. The original key generation of ZHFE is very time-consuming with complexity $O(n^{3\omega})$ and is later improved to $O(n^{2\omega+1})$ by Baena et al. However our solution requires very little computation, i.e., $O(\log_q D)$ $\mathbb{F}_q$-additions, and thus can generate the private key almost immediately.

Acknowledgment

The authors would like to thank the anonymous reviewers of PQCrypto'16 for their valuable comments on an early version of this paper, and the anonymous reviewers of IWSEC'16 for their helpful comments on this paper. The first author would like to thank the financial support from the National Natural Science Foundation of China (Grant No. 61572189).

References

[BCE+16] John B. Baena, Daniel Cabarcas, Daniel E. Escudero, Jaiberth Porras-Barrera, and Javier A. Verbel. Efficient ZHFE Key Generation. In T. Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 213–232. Springer, 2016.

[BFP13] L. Bettale, J. C. Faugère, and L. Perret. Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Des. Codes Cryptography*, 69(1):1–52, 2013.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In B. Preneel, editor, *EUROCRYPT 2000*, volume 1807, pages 392–407. Springer-Verlag Berlin Heidelberg, 2000.

[Cou01] N. T. Courtois. The Security of Hidden Field Equations (HFE). In D. Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 266–281. Springer, 2001.

[DG10] Vivien Dubois and Nicolas Gama. The Degree of Regularity of HFE Systems. In M. Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 557–576. Springer, 2010.

[DGS06] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt. *Multivariate public key cryptosystems*, volume 25 of *Advances in Information Security*. Springer, 2006.

[DH11] Jintai Ding and Timothy J. Hodges. Inverting HFE Systems Is Quasi-Polynomial for All Fields. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 724–742. Springer, 2011.

[DY13] Jintai Ding and Bo-Yin Yang. Degree of Regularity for HFEv and HFEv-. In P. Gaborit, editor, *PQCrypto 2013*, volume 7932 of *LNCS*, pages 52–66. Springer, 2013.

[Fau99] Jean-Charles Faugére. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

[Fau02] Jean-Charles Faugére. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *ISSAC '02 Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83. ACM New York, 2002.

[FJ03] J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In D. Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.

[GJ79] Michael R. Garey and David S. Johnson. *Computers and intractability: A guide to the theory of NP-completeness*. W. H. Freeman, 1979.

[GJS06] L. Granboulan, A. Joux, and J. Stern. Inverting HFE is Quasipolynomial. In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 345–356. Springer, 2006.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In M. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 19–30. Springer, 1999.

[Pat96] Jacques Patarin. Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms. In U. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.

[PBD14a] Jaiberth Porras, John Baena, and Jintai Ding. New Candidates for Multivariate Trapdoor Functions. Cryptology ePrint Archive, Report 2014/387, 2014. `http://eprint.iacr.org/2014/387`.

[PBD14b] Jaiberth Porras, John Baena, and Jintai Ding. ZHFE, a New Multivariate Public Key Encryption Scheme. In M. Mosca, editor, *PQCrypto 2014*, volume 8772 of *LNCS*, pages 229–245. Springer, 2014.

[PCG01] Jacques Patarin, Nicolas Courtois, and Louis Goubin. QUARTZ, 128-bit long digital signatures. In D. Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 282–288. Springer, 2001.

[PCY+15] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design Principles for HFEv- Based Multivariate Signature Schemes. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015*, volume 9452 of *LNCS*, pages 311–334. Springer, 2015.

[PST16] Ray Perlner and Daniel Smith-Tone. Security Analysis and Key Modification for ZHFE. In T. Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 197–212. Springer, 2016.

[WP05] Christopher Wolf and Bart Preneel. Equivalent Keys in HFE, C^*, and Variations. In E. Dawson and S. Vaudenay, editors, *Mycrypt 2005*, volume 3715 of *LNCS*, pages 33–49. Springer-Verlag Berlin Heidelberg, 2005.