The Distinguishing Attack on HFE

Josh Deaton and Jintai Ding

University of Cincinnati, OH, USA
jdeaton1995@gmail.com jintai.ding@gmail.com

Abstract. Often times, the ability to distinguish between random data and a public key can leads to attack against the cryptosystem itself. In this paper, we will show experimentally a very efficient distinguisher based on the distribution of ranks of the symmetric matrices associated with the central map in the multivariate cryptosystem HFE when the degree D of the central map is very small.

1 Introduction

Ever since Shor [21] introduced his algorithm which can break most modern cryptosystem like RSA efficiently given a sufficiently powerful quantum computer, there has been a great push to introduce new public key cryptosystems which can both be efficient to implement as well as secure against quantum attack. Currently, four of the most promising types of quantum secure cryptosystems are [3] Code-based, Lattice-based, Hash-based, and Multivariate. In this paper, we present experimentally a distinguisher for the multivariate cryptosystem HFE. For a brief overview of current multivariate schemes, see the paper [6]. Let us first describe what a multivariate cryptosystem is.

A multivariate cryptosystem is based a system of m multivariate polynomials in n variables

$$\mathscr{P} = \left(p^{(1)}(x_1, x_2, \ldots, x_n), p^{(2)}(x_1, x_2, \ldots, x_n), \ldots, p^{(m)}(x_1, x_2, \ldots, x_n)\right)$$

over a finite field $\mathbb{F}_q$ of size q. When convenient, we will write vectors by underlining them $(x_1, x_2, \ldots, x_n) = \underline{x}$. As quadratic systems are easier to store and evaluate, almost all multivariate cryptosystems use a quadratic system, though there are exceptions like the hashing scheme [8], and thus rely on the difficulty of the MQ (Multivariate Quadratic) problem:

MQ Problem For a given quadratic system of m polynomials in n variables $\mathscr{P}$, find a vector $\underline{x} \in \mathbb{F}_q^n$ such that $\mathscr{P}\left(\underline{x}\right) = 0$.

This problem is believed to be hard in the average case and has been proven to be NP-hard [12]. Multivariate cryptography can be used both for encryption if $m \geq n$ (to be injective) and signature generation if $n \geq m$ (to be surjective). In both cases, the public key $\mathscr{P}$ is a seemingly random system of quadratic polynomials, and the

secret key is hidden knowledge that always an efficient method for finding a pre-image $\underline{x} \in \mathbb{F}_q^n$ for a given message $\underline{y} \in \mathbb{F}_q^m$. It is common to write

$$\mathscr{P}^{-1}\left(\underline{y}\right) = \underline{x}$$

to mean that $\underline{x}$ is such an pre-image (but not necessarily that $\mathscr{P}$ is an invertible function).

The standard bi-polar construction of a multivariate scheme is for the secret key to be a triple $(\mathscr{S}, \mathscr{F}, \mathscr{T})$ where $\mathscr{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathscr{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ are invertible affine maps, and $\mathscr{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is a quadratic map which $\mathscr{F}^{-1}\left(\underline{y}\right)$ is efficient to find for each $\underline{y} \in \mathbb{F}_q^m$. The public key is the composition

$$\mathscr{P} := \mathscr{S} \circ \mathscr{F} \circ \mathscr{T}$$

which serves to hid the structure of $\mathscr{F}$. Depending on the scheme in question, the map $\mathscr{F}$ might be public knowledge like in the Matsumoto-Imai cryptosystem (also called C^*) [15], or the map $\mathscr{S}$ might be redundant and thus not included if $\mathscr{S} \circ \mathscr{F}$ has the same structure as $\mathscr{F}$ as in the Oil and Vinegar Scheme by Patarin [17]. Given a secret key $(\mathscr{S}, \mathscr{F}, \mathscr{T})$, one can efficiently find $\underline{x} = \mathscr{P}^{-1}\left(\underline{y}\right)$ by computing in turn $\underline{w} = \mathscr{S}^{-1}\left(\underline{y}\right)$, $\underline{z} = \mathscr{F}^{-1}\left(\underline{w}\right)$, and $\underline{x} = \mathscr{T}^{-1}\left(\underline{z}\right)$. In the case that $((\mathscr{S}, \mathscr{F}, \mathscr{T}), \mathscr{P})$ is an encryption scheme, a message $\underline{x}$ is encrypted by computing $\mathscr{P}\left(\underline{x}\right) = \underline{y}$ which is decrypted using the secret key by computing $\mathscr{P}^{-1}\left(\underline{y}\right) = \underline{x}$. In the case that $((\mathscr{S}, \mathscr{F}, \mathscr{T}), \mathscr{P})$ is signature scheme, a hash $\underline{y}$ of a message is signed using the secret key by computing $\mathscr{P}^{-1}\left(\underline{y}\right) = \underline{x}$ which is verified by computing $\mathscr{P}\left(\underline{x}\right) = \underline{y}$.

Multivariate cryptography has proven to be very competitive with the other fields of cryptography as can be seen with one of the three finalist for signature schemes in the NIST post-quantum cryptography competition being the multivariate Rainbow cryptosystem by Ding et al. [7].

2 HFE and HFEv-

2.1 Description of the Private Key

The HFE scheme was originally proposed by Patarin in 1996 [16] as a generalization of the Matsumoto-Imai cryptosystem [15]. A further generalization is the 2001 scheme HFEv- [18] which we will now describe. HFEv- uses a parameter set (q, n, v, a, D) and the standard bi-polar construction where the private key public key pair is given by $((\mathscr{S}, \mathscr{F}, \mathscr{T}), \mathscr{P})$ where $\mathscr{T} : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$ is an invertible affine map, $\mathscr{S} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-a}$ is an affine map of rank $n-a$, and $\mathscr{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is an easily inverted map to be described shortly. The public key is the composition

$$\mathscr{P} := \mathscr{S} \circ \mathscr{F} \circ \mathscr{T}.$$

We note that as the number of equations $n-a$ is less than the number of variables $n+v$, HFEv- is only appropiate for a signature scheme. In order to construct $\mathscr{F}$ such

that is it both quadratic and easy to find pre-images for, HFEv- utilizes a vector space isomorphism between $\mathbb{F}_q^n$ and the degree n extension $\mathbb{F}_{q^n} := \mathbb{F}_q[t]/\langle \mu(t) \rangle$ for some degree n irreducible polynomial μ in $\mathbb{F}_q[t]$. The standard isomorphism $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ is defined by

$$\phi(a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}) = (a_0, a_1, \ldots, a_{n-1}).$$

We also define the vector space isomorphism $\psi : \mathbb{F}_q^{n+v} \to \mathbb{F}_{q^n} \times \mathbb{F}_q^v$ by

$$\psi(x_1, x_2, \ldots, x_{n+v}) = \phi^{-1}(x_1, x_2, \ldots, x_n) \times id_v(x_{n+1}, x_{n+2}, \ldots, x_{n+v})$$

HFEv- first generates a map $\overline{\mathscr{F}} : \mathbb{F}_{q^n} \times \mathbb{F}_q^v \to \mathbb{F}_{q^n}$ which will determine the central map $\mathscr{F}$. $\overline{\mathscr{F}}$ is defined by

$$\overline{\mathscr{F}}(X, \underline{x}) = \sum_{\substack{i,j \in \mathbb{N}_0 \\ q^i + q^j \leq D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{i \in \mathbb{N}_0 \\ q^i \leq D}} \beta_i(\underline{x}) X^{q^i} + \gamma(\underline{x})$$

where one randomly selects $\alpha_{i,j}, \in \mathbb{F}_{q^n}$, $\beta_i : \mathbb{F}_q^v$ as random linear maps, and $\gamma : \mathbb{F}_q^v$ as a random quadratic. The positive integer D limits the degree of $\overline{\mathscr{F}}$. Notice that for any *fixed* $\underline{v} \in \mathbb{F}_q^v$, the map $\overline{\mathscr{F}}(X, \underline{v})$ is a univariate polynomial of degree at most D. So, using Berlekamp's algorithm [1], $\overline{\mathscr{F}}(X, \underline{v})$ we will find a pre-image with complexity [20]

$$\mathscr{O}(D^3 + nD^2)$$

if such a pre-image exists for a given element in the range. So this is efficient if D is sufficiently small.

We define the q-Hamming weight of an integer e as the sum of the coefficients in the base-q expansion of e. As the q-Hamming weight of the exponents of X in $\overline{\mathscr{F}}(X)$ is at most two and we are working over a ground field of size q, by using the field equations $x_i^q = x_i$ for $x_i \in \mathbb{F}_q$ the composition

$$\mathscr{F}(\underline{x}) := (\phi \circ \overline{\mathscr{F}} \circ \psi)(\underline{x})$$

is a quadratic system of n polynomials in $n + v$ variables. Notice that $\mathscr{F}$ is also easy to invert by inverting each of the three maps ϕ, $\overline{\mathscr{F}}$, and ψ in turn.
So now we have an efficient way to generate signatures for a hash $\underline{y} \in \mathbb{F}) q^{n-a}$.

1. Compute $\underline{z} = \mathscr{S}^{-1}(\underline{y})$.
2. Let $Z = \phi^{-1}(\underline{z})$ to lifted it to the extension field.
3. Repeat guess $\underline{v} \in \mathbb{F}_q^v$ until $\overline{\mathscr{F}}(X, \underline{v}) = Z$ has a solution found by Berlekamp's algorithm. Call such a solution $(W, \underline{v})$.
4. Let $\underline{w} = \psi^{-1}(W, \underline{v})$.
5. Finally, $x = \mathscr{T}^{-1}(\underline{w})$ is the signature for $\underline{y}$.

HFEv- is the basis of many cryptosystems such as QUARTZ [18], Gui [19], and the Nist Round three alternate candidate GeMSS [4]. We note that one recovers the original HFE scheme when $v = a = 0$.

2.2 Attacks on HFEv-

There have been many attacks against HFEv-, with the most damaging being direct attacks and MinRank attacks [19].

In the direct attack, one attempt to solve the MQ-problem

$$\mathscr{P}(\underline{x}) = \underline{y}$$

directly using algebraic techniques such as Faugére's F4/F5 algorithm [10, 11]. These algorithm's complexities depend on what is called the degree of regularity of the system D_{reg}. For an HFEv- public key, D_{reg} is lower than for a random system making it easier to solve the system directly [9].

In minrank attacks, one attempts to solve the minrank problem in which one attempts to find a matrix of rank at most a set value r from the span of a finite amou nt of matrices. These matrices are associated to the public key in various ways so that the recovery of one of that small rank will allow one to construct an equivalent secret key to the public key use by HFEv-. Often this is done by examining what is called the min-Q-rank of the quadratic form of $\mathscr{P}$ over the extension field $\mathbb{F}_{q^n}$. Examples include Kipnis and Shamir's attack [13] which was improved by Bettale et al's paper. [2] Here recently, a very strong attack was made by Tao et al. in [22] which does not depend at all on the value of a and the value of v creates only a polynomial factor. This attack has successfully beaten the parameters of GeMSS. This will force future parameters of HFEv- to more heavily rely on a large D to remain secure.

Another attack on HFEv- is a distinguisher of HFEv- by Ding et al. [5] which can tell how many vinegar variables there are by examining the step degrees in the before mentioned F4 algorithm. This is different for different values for v with a HFEv- system as well when compared with a a random system, so by examining the step degrees after projecting the variables into subspaces the authors found a way to find and kill the set of vinegar variables in the public key.

3 The Distinguishing Attack

Here we present a simple and efficient distinguishing attack on HFE when the degree D is small. We may associate to to the component $p^{(k)}$ of $\mathscr{P} = \left(p^{(1)}, \ldots, p^{(n)}\right)$ a symmetric matrix $Q_k = \left(q_{i,j}^{(k)}\right)$ where, if q is odd,

$$q_{i,j}^{(k)} = \begin{cases} \text{MonomialCoefficient}(P^{(k)}, x_i x_j) & \text{if } i = j \\ \text{MonomialCoefficient}(P^{(k)}, x_i x_j)/2 & \text{if } i \neq j \end{cases},$$

and, if q is even,

$$q_{i,j}^{(k)} = \begin{cases} 0 & \text{if } i = j \\ \text{MonomialCoefficient}(P^{(k)}, x_i x_j) & \text{if } i \neq j \end{cases}.$$

We note that in the add case the quadratic parts of $p^{(k)}$ correspond exactly to $\underline{x}^T Q_k \underline{x}$, but as it is impossible to divide by two in characteristic two we cannot have such a

close match in this case. The associated the latter associated matrix is often used as a substitute.

What we noticed experimentally is that when D in a HFE public key is small and one examines the distribution ranks of the linear combinations of the Q_k, there were less matrices of both full rank than expected and matrices of lower rank than expected. If these were acting like a random system, we would expect that they would follow the distribution of the ranks of symmetric matrices over $\mathbb{F}_q$ in general (with zeros in the diagonal for characteristic two). This distribution is well understood, and in 1969 MacWilliams [14] calculated by elementary methods that if we denote by $N(n,r,q)$ the number of symmetric matrices of size $n \times n$ with rank r over the finite field $\mathbb{F}_q$ and $N_0(n,r,q)$ the number of $n \times n$ symmetric matrices with zeros on the diagonal of rank r over the finite field $\mathbb{F}_q$ with $\mathrm{char}(q) = 2$ then

$$N(n,r,q) = \begin{cases} \prod_{i=1}^{r/2} \frac{q^{2i}}{q^{2i}-1} \prod_{i=0}^{r-1} (q^{n-i}-1) & \text{if r is even,} \\ \prod_{i=1}^{(r-1)/2} \frac{q^{2i}}{q^{2i}-1} \prod_{i=0}^{r-2} (q^{n-i}-1) & \text{if r is odd,} \end{cases}$$

and

$$N_0(n,r,q) = \begin{cases} \prod_{i=1}^{r/2} \frac{q^{2i-2}}{q^{2i}-1} \prod_{i=0}^{r-1} (q^{n-i}-1) & \text{if r is even,} \\ 0 & \text{if r is odd.} \end{cases}$$

Using this we can calculate exactly the probability of choosing a symmetric matrix of rank r that could be associate to a public key when choosing one uniformly from all such symmetric matrices. We conjectured that is we had a random system, the distribution of the ranks of the span of this system would follow the true uniform distribution fairly closely.

To this end we tested the chi-square goodness of fit test on both a randomly generated sets of polynomials as well as HFEv- public keys. To recall this, in the chi-squared test one selects a number of r categories from a known probability distribution called the expected outcomes $E_1, E_2, \ldots E_r$ after so many trials of the experiment. Then one records the number of observed outcomes there are in each category $O_1, O_2, \ldots, O_r$ for that number of trials. Then one calculates the test statistic

$$\chi^2 = \sum_{i=1}^{r} \frac{(O_i - E_i)^2}{E_i}$$

which can be compare to a chi-squared distribution with degree of freedom $r-1$. This later fact we will ignore as we only will examine if the values of χ^2 are different for random polynomials than HFEv- public keys.

As this test works best when each category has many expected observations and the ranks of most matrices are high, we choose a small number of categories in each case. For the case that q is odd we had the four categories for rank r: $r = n + v$,

$r = n+v-1$, $r = n+v-2$, and $r \leq n+v-3$. For the case that both $n+v$ and q are even we also had four categories for the rank r: $r = n+v$, $r = n+v-2$, $r = n+v-4$, and $r \leq n+v-6$ where we notice we skip matrices of odd rank as none such exists. For the case that q is even and $n+v$ is odd, there are very few matrices of low rank, so we choose three categories for the rank r: $r = n+v-1$, $r = n+v-3$, and $r \leq n+v-5$.

In each case of a parameter set we performed the chi-squared test with five times sets of systems of polynomials with those parameters. For each system we calculated the ranks of 2^{16} random linear combinations of the symmetric matrices and recorded the value of χ^2. Then we took the average of the five.

In Table 1 we record our results for a random polynomials with $q \in \{2,3\}$, $n \in \{20,35,50\}$, $v \in \{0,1,2\}$ and $a \in \{0,1,2\}$. In Tables 2 and 3 where we record our observations for HFEv- public keys. We keep the same choices for n, v, a as before and let Table 2 have $q = 2$ and $D \in \{5,7,9\}$ and Table 3 have $q = 3$ and $D \in \{7,9,11\}$. For each parameter choice we performed the test five times, recorded the value of χ^2, and then took the average.

Examining these tables shows that when $q = 2$, $D \in \{5,7\}$, and $v = 0$ we can easily distinguish, as well when $q = 3$, $D \in \{7,9\}$, and $v = 0$. But any vinegar variables makes the system seem random. The amount of equations a removed had no effect in either case.

(q,n,v,a)	Recorded χ^2 values	Average χ^2
$(2,20,0,0)$	4.044, 4.153, 4.594, 5.756, 6.344	4.978
$(2,20,0,1)$	3.939, 3.999, 4.019, 4.762, 7.963	4.937
$(2,20,0,2)$	3.406, 3.576, 4.449, 5.754, 7.134	4.864
$(2,20,1,0)$	1.133, 1.913, 3.498, 6.440, 8.384	4.273
$(2,20,1,1)$	0.1367, 0.4006, 0.7286, 0.9982, 3.419	1.137
$(2,20,1,2)$	0.005187, 0.2598, 1.926, 3.901, 7.940	2.806
$(2,35,0,0)$	0.2332, 1.495, 3.017, 3.420, 5.839	2.801
$(2,35,0,1)$	0.2030, 0.6624, 2.565, 2.956, 7.669	2.811
$(2,35,0,2)$	0.1405, 0.2389, 0.2639, 4.890, 5.744	2.255
$(2,35,1,0)$	2.899, 3.308, 3.921, 4.448, 7.226	4.360
$(2,35,1,1)$	2.901, 3.433, 4.388, 4.962, 6.915	4.520
$(2,35,1,2)$	3.021, 3.090, 3.137, 3.925, 9.724	4.579
$(2,50,0,0)$	2.948, 3.360, 3.665, 3.792, 5.551	3.863
$(2,50,0,1)$	2.986, 3.136, 3.163, 4.101, 5.143	3.706
$(2,50,0,2)$	4.075, 4.792, 5.069, 5.559, 6.716	5.242
$(2,50,1,0)$	0.5572, 1.002, 1.069, 1.651, 1.952	1.246
$(2,50,1,1)$	0.4164, 1.956, 1.995, 2.108, 5.470	2.389
$(2,50,1,2)$	0.02453, 0.06370, 0.1788, 1.731, 1.879	0.7753
$(3,20,0,0)$	0.5995, 1.507, 1.521, 6.139, 9.552	3.864
$(3,20,0,1)$	1.884, 3.161, 3.403, 4.689, 5.905	3.809
$(3,20,0,2)$	0.5038, 0.9148, 1.397, 2.554, 4.015	1.877
$(3,20,1,0)$	0.5208, 0.6498, 2.750, 3.346, 3.762	2.206
$(3,20,1,1)$	2.477, 2.765, 3.016, 3.544, 6.625	3.685
$(3,20,1,2)$	0.5717, 0.9815, 1.235, 1.599, 4.697	1.817
$(3,35,0,0)$	0.07915, 0.6830, 1.377, 6.146, 6.366	2.930
$(3,35,0,1)$	1.247, 1.275, 2.059, 2.461, 3.400	2.088
$(3,35,0,2)$	0.4974, 1.544, 2.666, 4.521, 8.579	3.562
$(3,35,1,0)$	1.137, 2.394, 2.766, 5.928, 10.20	4.484
$(3,35,1,1)$	0.1549, 0.5222, 2.279, 2.897, 4.314	2.034
$(3,35,1,2)$	0.2609, 0.2627, 0.7047, 4.117, 6.936	2.456
$(3,50,0,0)$	0.3723, 0.8345, 1.064, 2.091, 2.559	1.384
$(3,50,0,1)$	0.2228, 1.753, 3.412, 5.190, 8.719	3.859
$(3,50,0,2)$	0.03812, 0.9194, 1.066, 2.459, 4.261	1.749
$(3,50,1,0)$	1.263, 2.103, 4.288, 6.585, 7.601	4.368
$(3,50,1,1)$	0.5659, 2.646, 2.697, 6.408, 8.103	4.084
$(3,50,1,2)$	0.9360, 2.987, 3.255, 5.762, 15.16	5.620

Table 1: The χ^2 Values of Various Random Systems of $n-a$ quadratics with $n+v$ Variables

(q,n,v,a,D)	Recorded χ^2 values	Average χ^2
$(2,20,0,0,5)$	124.5, 130.1, 132.5, 135.7, 150.7	134.7
$(2,20,0,0,7)$	103.3, 117.9, 124.6, 153.7, 174.6	134.8
$(2,20,0,0,9)$	2.875, 2.932, 3.623, 3.917, 6.315	3.932
$(2,20,0,1,5)$	112.6, 128.8, 133.1, 144.4, 144.8	132.7
$(2,20,0,1,7)$	125.2, 127.4, 130.5, 133.4, 134.7	130.2
$(2,20,0,1,9)$	2.955, 4.349, 4.420, 5.344, 6.184	4.650
$(2,20,0,2,5)$	99.71, 125.6, 129.8, 154.1, 197.4	141.3
$(2,20,0,2,7)$	119.9, 132.4, 138.7, 142.2, 144.9	135.6
$(2,20,0,2,9)$	2.889, 2.909, 3.506, 4.769, 5.869	3.988
$(2,20,1,0,5)$	0.1241, 8.497, 9.300, 10.13, 13.87	8.385
$(2,20,1,0,7)$	0.07668, 7.989, 8.532, 10.80, 11.51	7.780
$(2,20,1,0,9)$	0.1465, 0.9952, 1.161, 1.176, 3.882	1.472
$(2,20,1,1,5)$	2.712, 3.747, 7.054, 9.186, 11.10	6.759
$(2,20,1,1,7)$	3.707, 5.106, 7.612, 12.04, 18.31	9.355
$(2,20,1,1,9)$	0.04622, 1.340, 3.002, 3.177, 3.679	2.249
$(2,20,1,2,5)$	5.764, 7.391, 8.573, 13.45, 14.75	9.983
$(2,20,1,2,7)$	0.5318, 2.597, 5.236, 5.612, 9.592	4.714
$(2,20,1,2,9)$	0.1529, 1.586, 1.620, 4.494, 6.322	2.835
$(2,35,0,0,5)$	100.4, 102.7, 104.8, 118.2, 122.7	109.8
$(2,35,0,0,7)$	98.24, 108.4, 112.0, 115.9, 135.0	113.9
$(2,35,0,0,9)$	0.3707, 2.005, 3.088, 4.446, 8.229	3.627
$(2,35,0,1,5)$	104.5, 110.6, 112.7, 117.3, 122.9	113.6
$(2,35,0,1,7)$	103.8, 106.9, 116.4, 131.5, 135.7	118.9
$(2,35,0,1,9)$	1.036, 1.104, 1.222, 2.195, 2.410	1.594
$(2,35,0,2,5)$	96.80, 99.69, 106.2, 109.7, 117.7	106.0
$(2,35,0,2,7)$	105.2, 105.3, 107.5, 108.5, 125.7	110.5
$(2,35,0,2,9)$	0.8652, 1.019, 1.209, 1.967, 2.454	1.503
$(2,35,1,0,5)$	3.187, 3.206, 7.492, 8.940, 9.047	6.374
$(2,35,1,0,7)$	2.988, 3.542, 4.133, 5.781, 12.78	5.846
$(2,35,1,0,9)$	3.072, 3.428, 3.437, 4.248, 4.530	3.743
$(2,35,1,1,5)$	3.657, 4.314, 7.350, 9.971, 12.04	7.466
$(2,35,1,1,7)$	3.468, 5.347, 5.952, 6.499, 6.698	5.593
$(2,35,1,1,9)$	3.246, 3.351, 3.378, 3.513, 3.561	3.410
$(2,35,1,2,5)$	3.125, 3.600, 4.708, 8.538, 8.635	5.722
$(2,35,1,2,7)$	2.891, 3.790, 4.269, 5.347, 9.939	5.247
$(2,35,1,2,9)$	3.411, 3.516, 3.721, 3.883, 6.875	4.281
$(2,50,0,0,5)$	103.1, 131.6, 135.0, 154.4, 162.5	137.3
$(2,50,0,0,7)$	100.8, 108.1, 132.0, 137.3, 151.6	126.0
$(2,50,0,0,9)$	3.454, 3.492, 3.778, 4.202, 5.198	4.025
$(2,50,0,1,5)$	128.7, 133.8, 144.6, 148.5, 161.9	143.5
$(2,50,0,1,7)$	120.4, 129.2, 133.3, 136.9, 147.1	133.4
$(2,50,0,1,9)$	2.928, 3.142, 3.790, 3.950, 5.683	3.899
$(2,50,0,2,5)$	110.4, 121.5, 141.6, 147.8, 160.8	136.4
$(2,50,0,2,7)$	103.2, 116.4, 122.9, 127.9, 171.1	128.3
$(2,50,0,2,9)$	2.909, 3.197, 3.206, 3.310, 6.034	3.731
$(2,50,1,0,5)$	0.5502, 3.346, 10.29, 11.19, 11.32	7.341
$(2,50,1,0,7)$	2.237, 3.653, 5.679, 7.133, 14.08	6.556
$(2,50,1,0,9)$	0.3119, 0.9134, 0.9244, 1.295, 2.758	1.240
$(2,50,1,1,5)$	0.9327, 1.391, 7.078, 8.629, 8.961	5.398
$(2,50,1,1,7)$	6.014, 8.750, 9.525, 9.587, 11.44	9.062
$(2,50,1,1,9)$	1.196, 1.453, 2.183, 2.516, 6.641	2.798
$(2,50,1,2,5)$	2.940, 5.216, 10.49, 11.97, 16.51	9.425
$(2,50,1,2,7)$	1.248, 5.008, 6.925, 6.944, 9.300	5.885
$(2,50,1,2,9)$	0.4251, 0.9306, 0.9431, 4.939, 5.110	2.470

Table 2: The χ^2 values on various HFEv- Parameters for $q = 2$

(q,n,v,a,D)	Recorded χ^2 values	Average χ^2
$(3,20,0,0,7)$	143.0, 144.2, 162.2, 166.6, 173.3	157.9
$(3,20,0,0,9)$	159.9, 164.5, 170.0, 177.6, 180.9	170.6
$(3,20,0,0,11)$	1.766, 2.806, 3.176, 3.471, 4.463	3.136
$(3,20,0,1,7)$	155.6, 165.7, 171.8, 178.8, 188.9	172.2
$(3,20,0,1,9)$	165.4, 166.4, 176.1, 177.1, 200.0	177.0
$(3,20,0,1,11)$	0.1130, 0.8573, 3.969, 5.553, 5.603	3.219
$(3,20,0,2,7)$	157.5, 159.9, 162.4, 181.1, 182.3	168.6
$(3,20,0,2,9)$	156.8, 159.5, 172.5, 175.5, 187.4	170.3
$(3,20,0,2,11)$	1.352, 1.374, 1.439, 4.801, 8.654	3.524
$(3,20,1,0,7)$	1.860, 3.046, 4.654, 5.098, 17.90	6.513
$(3,20,1,0,9)$	0.4120, 1.342, 1.831, 4.080, 4.660	2.465
$(3,20,1,0,11)$	1.787, 2.646, 3.691, 3.935, 5.597	3.531
$(3,20,1,1,7)$	0.3343, 1.181, 3.559, 6.293, 11.19	4.512
$(3,20,1,1,9)$	0.6513, 1.190, 4.427, 6.740, 14.60	5.521
$(3,20,1,1,11)$	0.7447, 2.163, 2.766, 3.817, 5.733	3.044
$(3,20,1,2,7)$	1.107, 1.143, 1.674, 2.824, 3.256	2.001
$(3,20,1,2,9)$	0.9177, 1.968, 2.959, 2.959, 4.238	2.608
$(3,20,1,2,11)$	0.8658, 0.9041, 0.9318, 0.9970, 1.835	1.107
$(3,35,0,0,7)$	141.6, 172.2, 174.9, 178.0, 191.4	171.6
$(3,35,0,0,9)$	151.4, 152.8, 156.8, 157.5, 185.1	160.7
$(3,35,0,0,11)$	0.5800, 2.007, 3.379, 4.221, 5.240	3.085
$(3,35,0,1,7)$	145.9, 178.2, 181.8, 182.4, 199.7	177.6
$(3,35,0,1,9)$	153.4, 155.5, 164.0, 179.2, 190.3	168.5
$(3,35,0,1,11)$	2.150, 2.515, 3.913, 6.792, 11.22	5.317
$(3,35,0,2,7)$	150.6, 158.7, 172.6, 175.9, 183.8	168.3
$(3,35,0,2,9)$	146.9, 152.8, 155.6, 164.9, 168.8	157.8
$(3,35,0,2,11)$	0.4238, 3.266, 5.331, 6.034, 8.240	4.659
$(3,35,1,0,7)$	0.2299, 1.176, 1.536, 1.979, 2.306	1.445
$(3,35,1,0,9)$	0.4943, 1.754, 2.024, 3.612, 5.875	2.752
$(3,35,1,0,11)$	1.814, 3.210, 3.543, 4.537, 8.801	4.381
$(3,35,1,1,7)$	1.671, 2.574, 7.164, 9.162, 11.33	6.380
$(3,35,1,1,9)$	0.9097, 1.511, 1.660, 2.885, 7.497	2.892
$(3,35,1,1,11)$	1.036, 1.097, 1.448, 1.880, 9.921	3.077
$(3,35,1,2,7)$	0.1023, 1.868, 2.476, 2.662, 12.42	3.905
$(3,35,1,2,9)$	0.1321, 0.3956, 0.6979, 2.622, 2.799	1.329
$(3,35,1,2,11)$	0.7589, 0.8359, 1.351, 1.366, 4.765	1.815
$(3,50,0,0,7)$	137.0, 168.6, 175.0, 186.2, 196.0	172.6
$(3,50,0,0,9)$	164.8, 169.8, 179.6, 185.1, 185.8	177.0
$(3,50,0,0,11)$	0.1621, 1.873, 2.258, 6.190, 11.56	4.409
$(3,50,0,1,7)$	162.2, 163.6, 166.0, 169.0, 192.8	170.7
$(3,50,0,1,9)$	151.8, 156.2, 168.8, 170.2, 173.4	164.1
$(3,50,0,1,11)$	0.6886, 1.242, 1.562, 2.755, 4.057	2.061
$(3,50,0,2,7)$	152.6, 167.8, 169.2, 172.5, 172.7	167.0
$(3,50,0,2,9)$	164.2, 165.6, 175.0, 179.6, 180.5	173.0
$(3,50,0,2,11)$	0.7302, 0.7725, 1.302, 3.150, 5.671	2.325
$(3,50,1,0,7)$	0.5854, 1.010, 1.101, 4.272, 9.603	3.314
$(3,50,1,0,9)$	0.03689, 0.4790, 0.6195, 1.076, 2.863	1.015
$(3,50,1,0,11)$	1.109, 1.498, 2.627, 5.803, 9.572	4.122
$(3,50,1,1,7)$	0.2952, 0.8565, 1.282, 2.194, 5.468	2.019
$(3,50,1,1,9)$	0.9932, 1.794, 1.969, 5.085, 5.721	3.113
$(3,50,1,1,11)$	0.4366, 2.356, 2.464, 3.702, 9.121	3.616
$(3,50,1,2,7)$	3.105, 4.224, 6.753, 8.171, 8.523	6.155
$(3,50,1,2,9)$	1.163, 1.222, 1.430, 1.580, 3.340	1.747
$(3,50,1,2,11)$	0.9080, 1.078, 1.082, 1.619, 3.536	1.645

Table 3: The χ^2 values on various HFEv- Parameters with $q = 3$

Bibliography

[1] Elwyn R Berlekamp. Factoring polynomials over finite fields. *Bell System Technical Journal*, 46(8):1853–1859, 1967.

[2] Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.

[3] Matthew Campagna, Lidong Chen, Özgür Dagdelen, Jintai Ding, Jennifer K Fernick, Nicolas Gisin, Donald Hayford, Thomas Jennewein, Norbert Lütkenhaus, Michele Mosca, et al. Quantum safe cryptography and security. *ETSI White Paper*, 8, 2015.

[4] Antoine Casanova, Jean-Charles Faugere, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. Gemss: A great multivariate short signature. *Submission to NIST*, 2017.

[5] Jintai Ding, Ray Perlner, Albrecht Petzoldt, and Daniel Smith-Tone. Improved cryptanalysis of hfev-via projection. In *International Conference on Post-Quantum Cryptography*, pages 375–395. Springer, 2018.

[6] Jintai Ding and Albrecht Petzoldt. Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4):28–36, 2017.

[7] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *International Conference on Applied Cryptography and Network Security*, pages 164–175. Springer, 2005.

[8] Jintai Ding and Bo-Yin Yang. Multivariates polynomials for hashing. In *International Conference on Information Security and Cryptology*, pages 358–371. Springer, 2007.

[9] Jintai Ding and Bo-Yin Yang. Degree of regularity for hfev and hfev-. In *International Workshop on Post-Quantum Cryptography*, pages 52–66. Springer, 2013.

[10] Jean-Charles Faugere. A new efficient algorithm for computing gröbner bases (f4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[11] Jean Charles Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (f 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.

[12] Michael R Garey and David S Johnson. *Computers and intractability*, volume 174. freeman San Francisco, 1979.

[13] Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In *Annual International Cryptology Conference*, pages 19–30. Springer, 1999.

[14] Jessie MacWilliams. Orthogonal matrices over finite fields. *The American Mathematical Monthly*, 76(2):152–164, 1969.

[15] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.

[16] Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer, 1996.

[17] Jacques Patarin. The oil and vinegar algorithm for signatures. In *Dagstuhl Workshop on Cryptography, 1997*, 1997.

[18] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Quartz, 128-bit long digital signatures. In *Cryptographers' Track at the RSA Conference*, pages 282–297. Springer, 2001.

[19] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design principles for hfev-based multivariate signature schemes. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 311–334. Springer, 2015.

[20] Chelsea Richards. *Algorithms for factoring square-free polynomials over finite fields*. PhD thesis, Master thesis, Simon Fraser University, Canada, 2009.

[21] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[22] Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Improved key recovery of the hfev-signature scheme.