Degree of Regularity for HFEv and HFEv-

Jintai Ding[1,2,⋆] and Bo-Yin Yang[3,⋆⋆]

[1] University of Cincinnati, Cincinnati OH, USA
[2] Chongqing University, China,
jintai.ding@gmail.com
[3] Academia Sinica, Taipei, Taiwan,
by@crypto.tw

Abstract. In this paper, we first prove an explicit formula which bounds the degree of regularity of the family of HFEv ("HFE with vinegar") and HFEv- ("HFE with vinegar and minus") multivariate public key cryptosystems over a finite field of size q. The degree of regularity of the polynomial system derived from an HFEv- system is less than or equal to

$$\begin{array}{c} \frac{(q-1)(r+v+a-1)}{2}+2 \text{ if } q \text{ is even and } r+a \text{ is odd,} \\ \frac{(q-1)(r+v+a)}{2}+2 \text{ otherwise,} \end{array}$$

where the parameters v, D, q, and a are parameters of the cryptosystem denoting respectively the number of vinegar variables, the degree of the HFE polynomial, the base field size, and the number of removed equations, and r is the "rank" paramter which in the general case is determined by D and q as $r = \lfloor \log_q(D-1) \rfloor + 1$. In particular, setting $a = 0$ gives us the case of HFEv where the degree of regularity is bound by

$$\begin{array}{c} \frac{(q-1)(r+v-1)}{2}+2 \text{ if } q \text{ is even and } r \text{ is odd,} \\ \frac{(q-1)(r+v)}{2}+2 \text{ otherwise.} \end{array}$$

This formula provides the first solid theoretical estimate of the complexity of algebraic cryptanalysis of the HFEv- signature scheme, and as a corollary bounds on the complexity of a direct attack against the QUARTZ digital signature scheme. Based on some experimental evidence, we evaluate the complexity of solving QUARTZ directly using F_4/F_5 or similar Gröbner methods to be around 2^{92}.

Keywords: Degree of regularity, HFE, HFEv, HFEv-.

⋆ Partially sponsored by National Science Foundation of China, Grant #60973131 and U1135004, and the Charles Phelps Taft Research Center.

⋆⋆ Partially sponsored by Taiwan's National Science Council project #100-2628-E-001-004-MY3 and 101-2915-I-001-019.

P. Gaborit (Ed.): PQCrypto 2013, LNCS 7932, pp. 52–66, 2013.

1 Introduction

1.1 Questions

HFE (Hidden Field Equations) and its derivatives form one of the best known families of multivariate quadratic public-key cryptosystems. It was invented by Patarin as a modification of the Matsumoto-Imai cryptosystem C^* in 1997.

Shor's algorithm from 1994 and its extensions [30,34] will break RSA and ECC when large quantum computers became available. In this context, multivariate PKCs and in particular HFE [28] had been viewed as a possible candidate to replace RSA. Although it was shown by Faugère and Joux [19] that the basic form can be cryptanalyzed by a direct algebraic attack, simple HFE variations had already been designed to guard against known attacks. The best known of these is probably QUARTZ, a very conservatively designed HFE variant over $\mathbb{F}_2$ using both the "Vinegar" and "Minus" modifications [29]. QUARTZ (and all HFEv variants) have never been credibly cryptanalyzed.

We want to give a solid theoretical bound on the degree of regularity of HFEv and associated systems, such as QUARTZ, and thereby obtain a good estimate on the complexity of attacking HFEv, HFEv-, and ipHFE cryptosystems using Gröbner Bases.

1.2 Answers

One usually solves $p_1(x_1, \ldots, x_n) = p_2(x_1, \ldots, x_n) = \cdots = p_m(x_1, \ldots, x_n) = 0$ over $\mathbb{F}_q$ using Gröbner basis algorithms such as F_4/F_5. The critical parameter which determines the complexity is known as "the degree of regularity", which is the maximum degree of monomials that appear in the computation. If we denote by $(p_i)^h$ the homogeneous leading part of p_i, the degree of regularity of the system is the first degree at which we find non-trivial relations among the $(p_i)^h$'s, or if we set as the graded ring $B := \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q, \ldots, x_n^q \rangle$ and B_d its degree-d slice, we may state a definition as follows for the case of degree-2 equations (generalizable to higher/mixed degrees):

Definition 1.1. *For homogeneous quadratic polynomials $(\lambda_1, \ldots, \lambda_m) \in B_2^m$, let $\psi_d : B_d^m \to B_{d+2}$ be the map defined as $\psi(b_1, \ldots, b_m) = \sum_{i=1}^m b_i \lambda_i$. Then $R_d(\lambda_1, \ldots, \lambda_m) := \ker \psi_d$ defines the subspace of relations $\sum_{i=1}^m b_i \lambda_i = 0$. Further let $T_d(\lambda_1, \ldots, \lambda_n)$ be the subspace of trivial relations generated by elements*

$$\{b(\lambda_i e_j - \lambda_j e_i) | 1 \leq i < j \leq m,\, b \in B_{d-2}\},\ \textit{and}$$

$$\{b(\lambda_i^{q-1} - 1)e_i | 1 \leq i \leq m,\, b \in B_{d-2(q-1)}\}.$$

Here e_i means the i-th unit vector consisting of all zeros except one 1 at the i-th position. The degree of regularity of a homogeneous quadratic set is then

$$D_{reg}(\lambda_1, \ldots, \lambda_m) := \min\{d | R_{d-2}(\lambda_1, \ldots, \lambda_m)/T_{d-2}(\lambda_1, \ldots, \lambda_m) \neq \{0\}\},$$

and $D_{reg}(p_1, \ldots, p_m) := D_{reg}((p_1)^h, \ldots, (p_m)^h)$ for polynomials in general.

We find an upper bound to D_{reg} for HFEv and HFEv-, which like in earlier studies depends on the size of the base field q, the rank of the HFE polynomial r, the number of removed equations a (if "minus" is used), and additionally the number of vinegar variables v, but in general on not the number of variables n:

$$D_{\text{reg}} \leq \frac{(q-1)(r+v+a-1)}{2} + 2, \quad \text{if } q \text{ is even and } r+a \text{ is odd,}$$
$$D_{\text{reg}} \leq \frac{(q-1)(r+v+a)}{2} + 2, \quad \text{otherwise.}$$

For small numbers we evaluated D_{reg} of random tests for HFEv and HFEv- using MAGMA and in each case the bound is relatively tight (see Section 4.1) which lends credence to predictions using our bound above for the Gröbner bases complexity.

As an example, substituting the actual parameters of QUARTZ we get $D_{\text{reg}} \leq 9$. Assuming that it is indeed 9, we can compute the number of bit-operations required to break it as $\approx 2^{92}$ (see Section 4.1), so QUARTZ should be reasonably secure for now.

This also shows that the break of an instance of internally perturbed HFE in [18], which is very much related to HFEv, is likely a case of overly aggressive parameters rather than of systematic problems.

1.3 Related Work

The C^* cryptosystem can be seen as a simple case of an HFE cryptosystem, and [14] noted that Patarin's linearization attack [27] was equivalent to the degree of regularity of C^* being three (in line with the formula in that paper).

The Square cryptosystem [7] is a C^* system with rank 1 and an odd base field. [14] proves a *lower* bound on its degree of regularity, showing a direct algebraic attack with Gröbner basis to be infeasible. However, such a result does not mean that the system is secure, because Square is actually broken by a different attack.

[9] was the first to claim to "break" HFE (cryptanalyze in significantly under design security), and [10] the earliest to mention HFEv- and HFE- specifically. But neither was followed up with a concrete implementation, and all interest was attracted to the news of Faugère's actually breaking HFE Challenge 1 [19].

[21] started to investigate algebraically the degree of regularity of HFE, but [17] seems to be the first rigorous study of the subject, which is continued by [14, 15].

2 Background

In the standard formulation of a multivariate public-key cryptosystem over a finite field $\mathbb{F}$, the public-key $P : \mathbb{F}^n \mapsto \mathbb{F}^m = T \circ Q \circ S$ is a composition of two invertible affine maps $S : \mathbb{F}^n \mapsto \mathbb{F}^n$ and $T : \mathbb{F}^m \mapsto \mathbb{F}^m$, and a quadratic map (possibly with some parameters) $Q : \mathbb{F}^n \mapsto \mathbb{F}^m$ which is easily invertible

when all parameters are given. The maps S and T are part of the secret key, and properties of the central map Q determines most of the properties of the cryptosystem.

2.1 The HFEv, ipHFE and HFEv- Cryptosystems

Let $\mathbb{F} \cong \mathbb{F}_q$ be a finite field of order q and $\mathbb{K}$ a degree-n extension of $\mathbb{F}$, with a "canonical" isomorphism ϕ identifying $\mathbb{K}$ with the vector space $\mathbb{F}^n$. That is, $\mathbb{F}^n \xrightarrow{\phi} \mathbb{K}$, $\mathbb{K} \xrightarrow{\phi^{-1}} \mathbb{F}^n$. Any function or map F from $\mathbb{K}$ to $\mathbb{K}$ can be expressed *uniquely* as a polynomial function with coefficients in $\mathbb{K}$ and degree less than q^n, namely

$$F(X) = \sum_{i=0}^{q^n-1} a_i X^i, \quad a_i \in \mathbb{K}.$$

Denote by $\deg_{\mathbb{K}}(F)$ the degree of $F(X)$ for any map F. Using ϕ, we can build a new map $F' : \mathbb{F}^n \to \mathbb{F}^n$

$$P(x_1, .., x_n) = (p_1(x_1, .., x_n), \ldots, p_n(x_1, .., x_n)) = \phi^{-1} \circ F \circ \phi(x_1, .., x_n),$$

which is essentially F but viewed from the perspective of $\mathbb{F}^n$. We can identify F and F' unless there is a chance of confusion.

An $\mathbb{F}$-degree-2 or $\mathbb{F}$-quadratic function from $\mathbb{K}$ to $\mathbb{K}$ can in this framework be seen to be a polynomial all of whose monomials have exponent $q^i + q^j$ or q^i or 0 for some i and j. The general form of this $\mathbb{F}$-quadratic function is $Q(X) = \sum_{i,j=0}^{n-1} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{n-1} b_i X^{q^i} + c.$, the *extended Dembowski-Ostrom polynomial map*. Such a $Q(X)$ with a fixed low $\mathbb{K}$-degree is used to build the HFE multivariate public key cryptosystems, as in the following

$$Q(X) = \sum_{i,j=0}^{q^i+q^j \le D, j \le i} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{q^i \le D} b_i X^{q^i} + c;$$

Note that the coefficients are values in $\mathbb{K}$, and all coefficients $a_{ii} = 0$ if $q = 2$, since those are covered by the b-part of the coefficients.

For a recent overview of multivariate cryptosystems, including all the common modifiers such as "minus", "internal perturbation", and "vinegar" see [16]. It gives this formulation of HFEv, which uses the vinegar modification [23], built from this polynomial:

$$Q(X, \bar{X}) := \sum_{i,j} a_{ij} X^{q^i+q^j} + \sum_{i,j} b_{ij} X^{q^i} \bar{X}^{q^j} + \sum_{i,j} \alpha_{ij} \bar{X}^{q^i+q^j} + \sum_i b_i X^{q^i} + \sum_i \beta'_i \bar{X}^{q^i} + c \tag{1}$$

where the auxiliary variable $\bar{X}$ occupies only a subspace of small rank v in $\mathbb{K} \cong \mathbb{F}^n$. The function Q is quadratic in the components of X and $\bar{X}$, and so is $P = T \circ Q \circ S$ for affine bijections T and S in $\mathbb{F}^n$ and $\mathbb{F}^{n+v}$. We hope that P is hard to invert to the adversary, while the legitimate user, with the knowledge of

(S, T) can compute X by substituting a random $\bar{X}$, then solving for X via root-finding algorithms such as Berlekamp (or Cantor-Zassenhaus, if $q \neq 2$). To limit the effort of Berlekamp, we restrict the maximum degree D of the polynomial. QUARTZ has the parameter set $(q, n, D, v, a) = (2, 103, 129, 4, 3)$.

We note that to verify in QUARTZ, one invokes the public map multiple times, but the ability to defeat QUARTZ still principally rests on inverting an HFEv- public map.

In an HFEv- cryptosystem, the public key P becomes P^-, that is, it is released minus the last a equations. Again we hope that inverting P^- is intractible without the trapdoor. The legitimate user can invert P^- simply by appending a random numbers from $\mathbb{F}_q$ to to the ciphertext or signature before inverting P.

Another closely related scheme to HFEv is ipHFE (internally perturbed HFE). Suppose in Eq. 1, $\bar{X}$ is not a free variable, but is instead the image of ℓ, a map from $\mathbb{F}^n$ onto $\mathbb{F}^v$. So the central map is really $Q'(X) := Q(X, \ell(X))$. To invert Q', the legitimate user would *guess* the values at positions in $V = \ell(X)$, solve for X, and then check whether $V = \ell(X)$. So the inversion process becomes less efficient in the sense that it takes in the worst case q^v tries to get one answer. From this description, we can see that ipHFE is the same as HFEv with the prefix modification (i.e., one or more limbs of the plaintext in a multivariate scheme becomes pre-determined).

2.2 Conventional Wisdom about HFE Security

There is no "proof of security" for any variant of HFE or any of the usual multivariate PKC proposals that reduce to a difficult computational problem commonly used for cryptography. However, similarly the security of NTRU depends on the hardness of lattice problems, but does not reduce to them. There are lattice-based systems which reduce to hard lattice problems, but these are much less efficient than NTRU. Analogously, there are multivariate PKCs that are "provably secure" in the sense that a break of such a PKC would imply an advance in the solution to an MQ-related computational problem [22,32,33], which happen to be much less efficient. Hence we take the approach that only careful study of cryptanalytic techniques can determine the security of a cryptosystem.

It is unfortunate, then, that HFE Challenge 1 was proposed when we understood the algebra behind it much less. It is even more unfortunate that some of the proposed HFE variants were overly aggressive and were promptly broken [3, 4, 18] just like many other multivariate schemes, because the public perception became biased against the HFE family.

HFE variants also gained a further reputation for being flimsy, more specifically poly-time-solvable [17, 21] with further mathematical studies. In particular [21] sketched a way to bound the degree of regularity for HFE when $q = 2$, using an approach to lift the problem back to the extension $\mathbb{K}$, an idea first suggested by Kipnis-Shamir [24]. They managed to describe a connection of the degree of regularity of the HFE system to the degree of regularity of a lifted system over the big field. Heuristic asymptotic bounds were found when $q = 2$

leading to the conclusion that if $D = O(n)$ the complexity of Gröbner basis solvers for the corresponding HFE systems is quasi-polynomial.

In some ways, this reputation is actually somewhat unfair, since simple HFE variations such as QUARTZ have resisted known attacks for a long time, and it is actually known in various contexts how the degree of operations in an algebraic attack varies (cf. [14]). We hope to achieve a more realistic evaluation of the security of HFE-related schemes. In particular we hope that better understanding of the degree of regularity under algebraic attcks can establish some HFE variants as fundamentally sound cryptosystems which had previously been proposed with overly aggressive parameters, rather than fundamentally broken systems (like C^*-).

2.3 Algebraic Cryptanalysis

Aside from cases in which brute-force enumeration [5] seems to the best *practical* way to solve systems, almost all of today's algebraic algorithms to solve

$$p_1(x_1, \ldots, x_n) = p_2(x_1, \ldots, x_n) = \cdots = p_m(x_1, \ldots, x_n) = 0$$

over $\mathbb{F}_q$ go back to Buchberger's algorithm for computing Gröbner bases [6]. Lazard proposed the following critical simplification (later reinvented as the XL Method): multiply the equations with monomials to form a collection of relations up to a some degree d. Linearize (i.e., treat each individual monomial as a variable), and use well-studied matrix algorithms over $\mathbb{F}_q$ on the resulting matrix (the *extended Macaulay matrix*) [11,25].

The Degree of Regularity. The critical concept in the complexity analysis of algebraic polynomial solving algorithms is the concept of *degree of regularity*. As given in Definition 1.1, the degree of regularity of the polynomial system is the lowest degree where we find a *non-trivial* degree drop. Conventional wisdom has it that in general this is the degree at which $\mathrm{F}_4/\mathrm{F}_5$ and similar algorithms usually terminate. Therefore D_{reg} is used to characterize the complexity of the algorithms.

We first note that almost all modern Gröbner Bases methods improve on XL as follows: suppose we fix a degree d and multiply each p_i with all monomials of degree $d - \deg p_i$ to create a large collection of relations of degree d. Order the monomials and linearize these equations to obtain the Macaulay matrix $\mathrm{Mac}^{(d)}(p_1, \ldots, p_m)$. Try to eliminate the highest degree monomials from $\mathrm{Mac}^{(d)}(p_1, \ldots, p_m)$ to create relations of degree $d-1$ or lower.

After we find such polynomials with degree drop, we multiply them by individual variables, and we obtain equations of at most degree d, which are effectively elimination remnants from higher-degree relations. If necessary, we can repeat this process many times until we can solve for all the variables. This describes MutantXL or XL2 [13,36] which will terminate at the same degree as $\mathrm{F}_4/\mathrm{F}_5$ [36]. Any superiority of the latter comes from having fewer redundant equations being generated or going through the elimination.

In Definition 1.1, we can see that the subspace T_d of trivial syzygies represents a "known-to-be-useless" degree drop in the following sense: Let $p_i = c^{(i)} + \sum_k b_k^{(i)} x_k + \sum_{k \leq \ell} a_{k\ell}^{(i)} x_k x_\ell$. For a polynomial p, let $(p)^h$ represent the homogeneous highest degree part of the polynomial p, and (p) a corresponding row in a Macaulay-type matrix. Clearly $(p_j)^h (p_i)^h - (p_i)^h (p_j)^h = 0$ is a trivial syzygy, which is equivalent to the combination of degree-4 rows $\left(\sum_{k\ell} a_{k\ell}^{(i)} (x_k x_\ell p_j)\right) - \left(\sum_{k\ell} a_{k\ell}^{(j)} (x_k x_\ell p_i)\right)$ being of degree-3 (or fewer). Equally clearly this "degree-drop" will not give us anything useful since

$$\left(c^{(i)}(p_j) + \sum_k b_k^{(i)} (x_k p_j) + \sum_{k\ell} a_{k\ell}^{(i)} (x_k x_\ell p_j)\right)$$
$$= \left(c^{(j)}(p_i) + \sum_k b_k^{(j)} (x_k p_i) + \sum_{k\ell} a_{k\ell}^{(j)} (x_k x_\ell p_i)\right),$$

given that both give $(p_i p_j)$. Thus we just "found" a linear combination of polynomials we already have at degree 3. So a trivial or *principal* syzygy between the top-degree parts $(p_i)^h$ leads to a *trivial* degree drop useless for generating new equations. We must verify that a degree-drop is non-trivial before we can claim that we have reached the degree of regularity.

Issue of Terminology. There is some confusion about the term "the degree of regularity". The rank of Macaulay matrices at a given degree can be derived as the coefficients of certain generating functions, with the heuristic assumption that there are no non-trivial syzygies. A system where this holds for all degrees is called *regular*. However this can be the case only for underdetermined systems over characteristic zero fields. Otherwise at a sufficiently high degree the generating function eventually has a non-positive coefficient, and regularity becomes impossible. Systems for which the rank of the Macaulay matrices follows the heuristic for as long as possible are called "semi-regular" [12]. Definition 1.1 follows [17] in that the degree of regularity is defined as "the first appearance of non-trivial degree fall", i.e., where the system ceases to behave as semi-regular.

The heuristic formulas that have since long been known to hold for the degree of regularity of most random systems (including asymptotics) are given by Bardet et al [1,2,37]. However, this formula does not hold for most systems with structure.

Conventional wisdom also accepts that when $m/n = h + o(1)$ where h is a constant not far removed from 1, solving m "generic" or "random" equations in n variables is exponential in time and space in n. We can do a tiny bit better. That is, for sufficiently large h we may solve the system faster than just guessing variables first (cf. e.g. [8, 35]), but it is still exponential time and space in m (and/or n).

Invariance of Degree of Regularity. The degree of regularity is invariant under invertible linear transformation in both the domain and the codomain.

So if $P = T \circ Q \circ S$ is the public map of a multivariate PKC with the central map Q with both S and T invertible affine transformations, then the degree of regularity in solving X from $P(X) = Y$ depends only on Q, and can be written $D_{\text{reg}}(Q)$.

3 Main Results

To recap, suppose we wish to solve an HFEv system with $\mathbb{K} \cong \mathbb{F}^n$, where $\mathbb{F} = \mathbb{F}_q$, with degree D and v vinegar variables. We would have then $n + v$ variables and n equations. However, MutantXL or F_4/F_5 algorithms deal with determined or overdetermined equations. The standard way to get around this problem is to guess some v variables and bring it down to a system with n variables. As noted earlier, we have now an ipHFE instance. We try to analyze the direct attack as in [14,15,17]. First, let us present our main results.

Theorem 3.1. *Let r be the rank of the HFE polynomial and v the number of vinegar variables. We may bound the degree of regularity of HFEv as follows:*

$$D_{\text{reg}} \leq \frac{(q-1)(r+v-1)}{2} + 2, \quad \textit{if } q \textit{ is even and } r \textit{ is odd,} \tag{2}$$

$$D_{\text{reg}} \leq \frac{(q-1)(r+v)}{2} + 2, \quad \textit{otherwise.} \tag{3}$$

This result is sufficient to bound the complexity of a direct algebraic attack against HFEv. If we assume that the direct algebraic attack is the best attack on HFEv systems, this would be the most important bound required to evaluate the security of odd-field HFEv and derivatives.

However, QUARTZ is an instance of HFEv-, not just HFEv. We recall that HFEv-, of which QUARTZ is a special case is derived from HFEv by removing a few public key polynomials. We normally have $n+v$ variables and $n-a$ equations. To solve a HFEv- case, we again first guess v-values. Then we have n variables and $n-a$ equations. As we mentioned, this is essentially an ipHFE system. Now we need to bound the degree of regularity of a direct algebraic attack on HFEv on such a system.

Theorem 3.2. *Let r be the rank of the HFE polynomial, v the number of vinegar variables, and a the number of "minus" equations, then we may bound the degree of regularity as follows:*

$$D_{\text{reg}} \leq \frac{(q-1)(r+a+v-1)}{2} + 2, \quad \textit{if } q \textit{ is even and } r+a \textit{ is odd,}$$

$$D_{\text{reg}} \leq \frac{(q-1)(r+a+v)}{2} + 2, \quad \textit{otherwise.}$$

We will now show how our main results is proved.

To prove Equation (3) in Theorem 3.1, we must use a result that link the degree of regularity on a big-field multivariate to the rank of the central map.

Proposition 3.3. *[14, Theorem 4.1] For central maps Q that corresponds to quadratic maps, we have*

$$D_{reg}(Q) \leq \frac{(q-1)\,\mathrm{Rank}(Q)}{2} + 2.$$

We now need to show that the rank of an HFEv central polynomial with v vinegar variables is no higher than that of the original HFE polynomial plus v. First, we rewrite the HFEv polynomial so that it is more easily handled.

Proposition 3.4. *The associated polynomial when solving an HFEv or an ipHFE system over the big field $\mathbb{K}$ can be written as:*

$$\begin{aligned}\bar{P}(X) = &\sum_{i=0}^{q^i<D} \Big((\sum_{j=0}^{q^i+q^j \leq D, j\leq i} a_{ij} X^{q^i+q^j}) + (\sum_{l=0}^{v-1} a'_{il} X^{q^i} \bar{X}_l) \Big) \\ &+ \sum_{i=0}^{v-1} \sum_{j=i}^{v-1} a''_{ij} \bar{X}_i \bar{X}_j + \sum_{i=0}^{q^i \leq D} b_i X^{q^i} + \sum_{i=0}^{v-1} u_i \bar{X}_i + c, \qquad (4)\end{aligned}$$

where $\bar{X}_i := \mathrm{Tr}(\alpha_i X)$ for suitably chosen α_i. The map Tr *is the trace function, which is also given by* $\mathrm{Tr}(X) := \sum_{j=0}^{n-1} (X)^{q^j}$.,

Proof. We note that Tr is a nontrivial linear map of $\mathbb{F}^n \to \mathbb{F}$. For some representation of $\mathbb{F}^n \cong \mathbb{K}$, we can write it as a projection into the first component. With a suitably chosen α_i, we can make the first component of $\alpha_i X$ any nontrivial linear map of the components of X. So we can express each of the components of $\bar{X} = \ell(X)$ in Eq. 1 as $\mathrm{Tr}(\alpha_i X)$ for some α_i.

So Theorem 3.1 can be proved if we can show that:

Proposition 3.5. *The rank of the quadratic form associated with the polynomial $\bar{P}$ above, written $R(\bar{P})$, is bounded by:*

$$R(\bar{P}) \leq R(P) + v.$$

To obtain this we need this result about quadratic forms:

Proposition 3.6. *[26, Chapter 6] The rank of a quadratic form F is less than or equal to the minimum number of linear forms one needs to express F as a quadratic function in them. That is, if one can write F as a quadratic function of linear forms $\ell_1, \ldots, \ell_r$, then* $\mathrm{Rank}\, F \leq r$.

Definition 3.7. *Let F be a quadratic form over a field k, and $F(X,Y) := X^t F Y$ be the bilinear (symmetric) form associated with F over the field k^n. Let*

$$N_F = \{X \in k^n | F(X,Y) = 0, \quad \textit{for any} \quad Y \in k^n\}.$$

N_F as linear subspace is called the radical for the bilinear form F.

Note that for any F of rank r, we can write F in the linear forms $\ell_1, \ldots, \ell_r$, and any X with $\ell_1(X) = \cdots = \ell_r(X) = 0$ is in N_F. So by using the following observation, we see that the dimension of N_F is $n - r$.

Proposition 3.8. *Let z_ℓ, $\ell = 0, \ldots, v-1$, be linear functions from $\mathbb{F}^n$ to $\mathbb{F}$, i.e., $z_\ell : (x_1, \ldots, x_n) \mapsto \sum \beta_i^{(\ell)} x_i$. Then the dimension of the intersection of kernels $K(z_i) := \{X \in \mathbb{F}^n | z_i(X) = 0\}$ is bounded by*

$$\dim\left(\bigcap_i^{v-1} K(z_i)\right) \geq n - v.$$

Proposition 3.9. *Under the conditions and notation of Definition 3.7 and Proposition 3.8,*

$$\dim(N_F \bigcap K(Z)) \geq n - r - v.$$

The last proposition follows from 3.7 and 3.8, basically by inclusion-exclusion.

Proposition 3.10. *Let $F(x_0, ..x_{n-1})$ be a quadratic form (or polynomial) whose rank is r. Here each variable x_i can additionally be considered as a linear map or function from $\mathbb{F}^n$ to $\mathbb{F}$. In this manner it would be viewed the i-th component map $x_i(u_0, \ldots, u_{n-1}) = u_i$, for $(u_0, \ldots, u_{n-1}) \in \mathbb{F}^n$. Let $A : \mathbb{F}^n \to \mathbb{F}^n$ be an invertible linear transformation (with A^{-1} its inverse), such that*

$$F(A(x_0), \ldots, A(x_{n-1}))) = \sum_{i=0}^{r} \sum_{j=i}^{r} a_{ij} x_i x_j,$$

where $A(x_i)$ is the function from $\mathbb{F}^n$ to $\mathbb{F}$ derived from $x_i \circ A$. Let

$$\bar{F}(x) = F(x_0, ..x_{n-1}) + \sum_{i=0}^{r} (\sum_{\ell=0}^{v-1} a'_{i\ell} A^{-1}(x_i) z_\ell),$$

where each z_ℓ is a linear function from $\mathbb{F}^n$ to $\mathbb{F}$, i.e., $z_\ell : (x_0, \ldots, x_{n-1}) \mapsto \sum \beta_i^{(\ell)} x_i$. Then

$$\text{Rank}(\bar{F}) \leq \text{Rank}(F) + v.$$

This follows from Proposition 3.9.

Now we further note that the process of fixing v variables to get a determined system corresponds to introducing v linear relations of the form

$$\sum_i a_i X^{q^i} + \sum_{j=1}^{v} b_j \overline{X}_j = 0.$$

From this we can substitute for each of the $\overline{X}_j$, a linear combination of the X^{q^i} (which is itself linear in X), which shows that the quadratic form $\overline{P}$ of HFEv or ipHFE can be expressed using v extra linear forms than the Dembowski-Ostrom polynomial map P (that is, without the v forms $\overline{X}_i$). Then since the rank of a quadratic form is bounded by the number of linear forms used to express it, we have Proposition 3.5, and Equation (3) then follows.

We note that the above line of reasoning is good only for odd q because in binary fields the rank of the associated matrix to a symmetric form is always even, creating various off-by-one errors in the above process, we may go through steps akin to that in [14] to patch those off-by-one problems (to be included in a full journal version), and account for the binary field cases in Theorem 3.1.

A note on HFE over tower fields. An HFE-derivative cryptosystem built over $\mathbb{F}_{q^k}$ is also one over $\mathbb{F}_q$. So we can (for example) attack an HFE-type instance built over $\mathbb{F}_{16}$ by solve it as a system over $\mathbb{F}_2$. However, in this situation the rank parameter r would usually be $\lfloor \log_{16}(D-1) \rfloor + 1$, not $\lfloor \log_2(D-1) \rfloor + 1$. The reason is that the central Dembowski-Ostrom polynomial, and therefore the rank r, is an entity in the big field and does not vary according to our viewpoint.

Proving Theorem 3.2 Again let us examine only odd characteristic cases for now. From the definition of HFEv-, it may be viewed as (HFE-)v. I.e., just as a central map of HFEv is one of HFE *plus a quadratic function with the extra variables in the form of a vector in an unknown subspace of dimension v (the "vinegar subspace")*, in exactly the fashion, HFEv- is HFEv plus a quadratic function with extra unknowns in that same vinegar subspace.

Put another way, let $\hat{P}^-$ be the public key of an HFEv- instance which is derived from the corresponding public key of an HFEv instance:

$$\hat{P}^-(x_1, \ldots, x_n) = (\hat{p}_1(x_1, \ldots, x_n), \ldots, \hat{p}_{n-a}(x_1, \ldots, x_n), 0, ..0).$$

We can then depict $\hat{P}^-$ as the vinegar form of an HFE- instance with central map Q^-. Q^- is a quadratic map, and can hence expressible as an extended Dembowski-Ostrom map. In other words, Q^- is also the central map of an HFE instance.

Now, according to [15, Section 4, Proposition 1] we have $\text{Rank}(Q) \leq \text{Rank}(Q) + a$, where a is the number of "minus" equations. This holds because all the arguments there depend only on rank and not on exponents in the formulas.

Finally, we use Proposition 3.10 with $\hat{P}^-$ as the central map of an HFEv instance. We conclude that $\text{Rank}(P^-) < \text{Rank}(Q) + r + a$ which leads to the odd-q half of Theorem 3.2.

4 Testing, Implication and Discussion

Having given a bound for the degree of regularity for HFEv- (and ipHFE) systems, we give some experimental results and discuss what this means for QUARTZ.

4.1 Tests and Results

We ran MAGMA-2.7.12 on random systems for each parameter $n \leq 13$, $r \leq 4$, $a, v \leq 2$, and $q \leq 5$, on a workstation (with 2x Opteron 6212 and 32GB of RAM) to find D_{reg} on 4–20 randomly generated HFEv and HFEv- systems, and for $q = 2$ further for 1 random system each up to $n = 29$. We added $x_i^q - x_i$ for each i as part of the system of equations, so as to trigger field-specific optimizations that MAGMA might have for $q = 2$. In each case, D_{reg} proves to be the *smaller* of *either* the minimum of the bound in the formula above *or*, if we use $[u]S$ to mean the coefficient of the term u in a corresponding series expansion of S:

$$\min \left\{ d : [x^d] \left(\left(\frac{1-x^q}{1-x} \right)^n \left(\frac{1-x^2}{1-x^{2q}} \right)^m \right) < 0 \right\},$$

for m equations and n variables in $\mathbb{F}_q$. The cryptic expression above denotes the smallest d such that the coefficient of x^d in the Maclaurin expansion of $\left(\frac{1-x^q}{1-x}\right)^n \left(\frac{1-x^2}{1-x^{2q}}\right)^m$ becomes negative. It is actually the usual heuristic expression for D_{reg} for random systems, such as those found in [1] (for $q = 2$ only).

The numbers may seem too small to be conclusive, but for 13 variables and equations over $\mathbb{F}_7$ or 14 variables and equations over $\mathbb{F}_5$ MAGMA is already running out of memory, and these results lend credence to predictions using our bound for the Gröbner Bases complexity for HFEv and HFEv- systems. We can now try to justify the predictions for QUARTZ given in Section 1.

4.2 Implications for QUARTZ

We have obtained a bound on the degree of regularity of 9 for QUARTZ (which has $q = 2$, $n = 103$, $r = 7$, $a = 3$, $v = 4$), which represents a big drop already compared to degree 13 for a random system of that size (cf. formula above). However, if the bound is reasonably tight, the number of columns (monomials) involved in the elimination should be roughly the number of top-level monomials, which are $T := \binom{n}{D_{\text{reg}}} = \binom{100}{9} \gtrsim 2^{40}$ in total. A dense-matrix elimination would require 2^{80} bits of storage which is clearly not feasible.

Let us assume an extremely optimistic scenario for the attacker, such that a putative sparse-matrix-enabled $\mathrm{F}_4/\mathrm{F}_5$ attack is possible. Since each row has $\tau = \binom{100}{2} \geq 2^{12}$ terms, we will require about 2^{52} bits of memory. This is very large still, but not impossible in the mid-term future. We further use the number of bit-operations in the most time-consuming Wiedemann or Block Wiedemann type elimination methods as the estimate of the attack complexity, then we get the evaluation of the complexity given in Section 1:

$$C_{\mathrm{F}_4/\mathrm{F}_5} \geq 3\tau T^2 \gtrsim 3 \cdot 2^{12} \cdot (2^{40})^2 \geq 2^{92}.$$

Note: This evaluation above is highly optimistic in that it makes the implicit assumption that there is no penalty for accessing large memory. This may be very wrong in two ways:

- There is a very perceptible cost penalty in assembling a large amount of RAM which is either accessible on one machine or is networked using high speed interconnect to every other machine.
- Accessing a large amount of memory is slower; most server motherboards takes a speed penalty when using the maximum number of memory modules, and accessing memory on other machines of course incurs terrible latency.

What this might mean practically is that *it might be more advantageous to attack QUARTZ by brute-force [5]*, which imposes no communication requirements (i.e., networking and memory bandwidth and latencies) and is embarassingly parallelizable (hence perfectly scalable).

Final Remark: In some of the cases previously studied, we can *prove* tightness of the bounds. Clearly more of this type of work is needed, where theoretical bounds for attacks are given, just like the studies of theoretical bounds on differential probabilities in AES.

References

1. Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving, pp. 71–74 (2004); Previously INRIA report RR-5049
2. Bardet, M., Faugère, J.-C., Salvy, B., Yang, B.-Y.: Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In: Gianni, P. (ed.) MEGA 2005 Sardinia, Italy (2005)
3. Bettale, L., Faugère, J.-C., Perret, L.: Cryptanalysis of multivariate and odd-characteristic HFE variants. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 441–458. Springer, Heidelberg (2011)
4. Billet, O., Macario-Rat, G.: Cryptanalysis of the square cryptosystems. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 451–468. Springer, Heidelberg (2009)
5. Bouillaguet, C., Chen, H.-C., Cheng, C.-M., Chou, T., Niederhagen, R., Shamir, A., Yang, B.-Y.: Fast exhaustive search for polynomial systems in $\mathbb{F}_2$. In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010. LNCS, vol. 6225, pp. 203–218. Springer, Heidelberg (2010)
6. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, Innsbruck (1965)
7. Clough, C., Baena, J., Ding, J., Yang, B.-Y., Chen, M.-S.: Square, a new multivariate encryption scheme. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 252–264. Springer, Heidelberg (2009)
8. Courtois, N., Goubin, L., Meier, W., Tacier, J.-D.: Solving underdefined systems of multivariate quadratic equations. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 211–227. Springer, Heidelberg (2002)
9. Courtois, N.T.: The security of hidden field equations (HFE). In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 266–281. Springer, Heidelberg (2001)
10. Courtois, N.T., Daum, M., Felke, P.: On the security of HFE, HFEv- and Quartz. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 337–350. Springer, Heidelberg (2002)
11. Courtois, N.T., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000), `http://www.minrank.org/xlfull.pdf`
12. Diem, C.: The XL-algorithm and a conjecture from commutative algebra. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 323–337. Springer, Heidelberg (2004)
13. Ding, J., Buchmann, J., Mohamed, M.S.E., Mohamed, W.S.A.E., Weinmann, R.-P.: Mutant XL. Talk at the First International Conference on Symbolic Computation and Cryptography (SCC 2008), Beijing (2008)
14. Ding, J., Hodges, T.J.: Inverting HFE systems is quasi-polynomial for all fields. In: Rogaway [31], pp. 724–742
15. Ding, J., Kleinjung, T.: Degree of regularity for HFE−. Cryptology ePrint Archive, Report 2011/570 (2011), `http://eprint.iacr.org/`

16. Ding, J., Yang, B.-Y.: Multivariate public key cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post Quantum Cryptography, 1st edn., pp. 193–241. Springer, Berlin (2008) ISBN 3-540-88701-6
17. Dubois, V., Gama, N.: The degree of regularity of HFE systems. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 557–576. Springer, Heidelberg (2010)
18. Dubois, V., Granboulan, L., Stern, J.: Cryptanalysis of HFE with internal perturbation. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 249–265. Springer, Heidelberg (2007)
19. Faugère, J.-C., Joux, A.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
20. Fischlin, M., Buchmann, J., Manulis, M. (eds.): PKC 2012. LNCS, vol. 7293. Springer, Heidelberg (2012)
21. Granboulan, L., Joux, A., Stern, J.: Inverting HFE is quasipolynomial. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 345–356. Springer, Heidelberg (2006)
22. Huang, Y.-J., Liu, F.-H., Yang, B.-Y.: Public-key cryptography from new multivariate quadratic assumptions. In: Fischlin et al. [20], pp. 190–205
23. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999)
24. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999), `http://www.minrank.org/hfesubreg.ps`
25. Lazard, D.: Gröbner-bases, Gaussian elimination and resolution of systems of algebraic equations. In: van Hulzen, J.A. (ed.) ISSAC 1983 and EUROCAL 1983. LNCS, vol. 162, pp. 146–156. Springer, Heidelberg (1983)
26. Lidl, R., Niederreiter, H.: Finite Fields, 2nd edn. Encyclopedia of Mathematics and its Application, vol. 20. Cambridge University Press (2003)
27. Patarin, J.: Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995)
28. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996), `http://www.minrank.org/hfe.pdf`
29. Patarin, J., Courtois, N.T., Goubin, L.: QUARTZ, 128-bit long digital signatures. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 282–288. Springer, Heidelberg (2001)
30. Proos, J., Zalka, C.: Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Information & Computation 3(4), 317–344 (2003)
31. Rogaway, P. (ed.): Advances in Cryptology – CRYPTO 2011. LNCS, vol. 6841. Springer, Heidelberg (2011)
32. Sakumoto, K.: Public-key identification schemes based on multivariate cubic polynomials. In: Fischlin et al. [20], pp. 172–189
33. Sakumoto, K., Shirai, T., Hiwatari, H.: Public-key identification schemes based on multivariate quadratic polynomials. In: Rogaway [31], pp. 706–723

34. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26(5), 1484–1509 (1997)
35. Thomae, E., Wolf, C.: Solving underdetermined systems of multivariate quadratic equations revisited. In: Fischlin et al. [20], pp. 156–171.
36. Yang, B.-Y., Chen, J.-M.: All in the XL family: Theory and practice. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2005)
37. Yang, B.-Y., Chen, J.-M.: Theoretical analysis of XL over small fields. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 277–288. Springer, Heidelberg (2004)