The Degree of Regularity of HFE Systems*

Vivien Dubois[1] and Nicolas Gama[2]

[1] DGA-MI, France
vivien.dubois@m4x.org
[2] EPFL, Switzerland
nicolas.gama@ens.fr

Abstract. HFE is a public key scheme introduced by Patarin in 1996. An HFE public key is a large system of polynomials in many variables over a small finite field. This system results from some secret composition, based on which the owner can solve it to any arbitrary vector. While the security of the cryptosystem relies on the difficulty of solving the public system without the trapdoor information, in 2002 Faugère found experimentally that Gröbner basis computations perform much better on certain HFE instances than on random systems. More specifically, Faugère observed that the regular behaviour of the Gröbner basis computation collapses at a much lower degree than expected for random systems, letting the computation finish much earlier. Accounting for this distinctive property, Faugère and Joux showed in 2003 that mapping HFE systems to some other multivariate ring exhibits the particular algebraic structure of these systems. Nevertheless, they did not offer the actual computation of the degree of regularity of HFE systems. Later, in 2006, Granboulan, Joux and Stern showed an asymptotic upper bound on the degree of regularity of HFE systems over $GF(2)$ using independent results on overdetermined systems of equations. The case of larger ground fields has remained however completely unsolved. In this paper, we exhibit an additional property of HFE systems that is increasingly significant as the size of the ground field grows. Using this property with a standard combinatorial calculation yields an arguably tight numerical bound on the degree of regularity of HFE systems for any parameters.

Keywords: multivariate polynomials, HFE, algebraic cryptanalysis.

1 Introduction

Solving large systems of multivariate equations over a finite field is one of the most recurrent problems in computer science. Although achieving this task seems very hard in general and can only be tackled for small sizes by current best algorithms, sparse classes of systems exist that can be solved efficiently. In the last fifteen years, attempts have been made at exploiting this gap to build asymmetric cryptographic primitives. In a nutshell, the issue has been to find secure ways of masking structured systems of polynomials.

* This paper is an extended abstract. The full version is available from the authors.

M. Abe (Ed.): ASIACRYPT 2010, LNCS 6477, pp. 557–576, 2010.

The HFE Cryptosystem. One of the most prominent proposals in this area has been the *Hidden Field Equation* cryptosystem, introduced by Patarin in 1996. HFE is based on an elegant idea introduced by Matsumoto and Imai in 1988 of deriving a set of multivariate equations from a single variable equation over a large extension field; this makes use of the vector space structure of this extension field. When the single variable equation can be solved efficiently the same holds for the multivariate system, and access to the large field equation is restricted by applying secret linear bijections on the variables and equations.

More formally, let $\mathbb{F}_q$ denote the finite field with q elements and let ϕ be some linear bijection from $\mathbb{F}_{q^n}$, the degree n extension of $\mathbb{F}_q$, to $(\mathbb{F}_q)^n$. Such a linear bijection is defined by a choice of a linear basis of $\mathbb{F}_{q^n}$. To any polynomial function $P(X)$ on $\mathbb{F}_{q^n}$, one associates the function $\phi \circ P \circ \phi^{-1}$ on $(\mathbb{F}_q)^n$. In HFE, polynomials P have a small degree to ensure efficient root finding. Also, they have a special shape which ensures that $\phi \circ P \circ \phi^{-1}$ is quadratic. This function is then composed with secret linear bijections $S, T : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$, $T \circ (\phi \circ P \circ \phi^{-1}) \circ S$ and the result is released as the public function. HFE can be used as a signature scheme and also, with some minor arrangements, as an encryption scheme [16]. Many variations exist and offer potential enhancements.

The Security of HFE. The fundamental issue is whether the public function is a one-way function. Finding a preimage by the public function is the same as finding a solution to the corresponding system of quadratic equations. Denote by $\mathrm{MQ}(q, n)$ the set of systems of n quadratic equations in n variables over $\mathbb{F}_q$, and by $\mathrm{HFE}(q, n, D)$ the subset of HFE systems where D is the parameter that controls the degree of the internal polynomial P. Two lines of work have so far been able to distinguish HFE systems from random MQ systems. One line of work, proposed in [8], targets so called differential properties of HFE functions and was able to produce a distinguisher with proven complexity for all parameters (q, n, D). The other line of work, proposed in [4,9,15], directly targets the difficulty of the preimage problem on HFE systems. It produced experimental evidence that for some parameters the preimage problem is much easier on HFE systems than on random MQ instances [12]. Since the difficulty of the preimage problem on HFE systems is ultimately the issue, one wishes to clarify what property is disclosed by the methods used in the second line of work and how this property depends on the parameters (q, n, D). So far, the available information has been the following.

1. The experimental evidence has been obtained by using algorithms for computing Gröbner bases [12,17]. These algorithms proceed through combinations with polynomial coefficients of a given set of polynomials and generate additional polynomials that can be used to solve the system.
2. The attacks have only concerned systems over $\mathbb{F}_2$. Experiments for various values of n and D evidenced that the degree of combinations needed to compute a Gröbner basis (for a graded ordering of terms) on HFE systems only depends on D for large enough n [12]. Unfortunately, no extension of this property to larger values of q has been reported. In fact, some authors [7]

argued that the size of the field should have a strong negative impact the computation and observed it on experiments using the Magma package [18].
3. On the theoretical side, a qualitative account was given in [9] on how the combinations performed on the public polynomials correspond to related operations on the internal polynomial. Although this clearly initiated a way of investigating HFE systems, it has not been followed with the computation of theoretical complexity bounds. Nevertheless, the authors in [15] showed that when $q = 2$, complexity bounds can be heuristically derived from results on overdetermined MQ systems.

We note that quantitative information has only been obtained from experiments and on systems over $\mathbb{F}_2$. The theoretical connections have not permitted to derive quantitative information beyond practical reach. Notably, how the phenomenon that is observed experimentally varies as q increases has remained unknown. The gain of potential enhancements also has, incidentally, remained unclear.

Our contribution. Recent studies on the complexity of Gröbner basis algorithms focus on the notion of degree of regularity of a system of polynomials [2,1]. Roughly speaking, the degree of regularity is the smallest degree at which a non-trivial degree fall among algebraic combinations of the input polynomials occurs. The degree of regularity of HFE systems over $\mathbb{F}_2$ was experimentally found within some parameter range in [9] and asymptotically upper bounded in [15] using the results of [2,1]. In this paper, we give a way to compute a numerical bound on the degree of regularity of HFE systems over any field and for any parameters. This is achieved by using previous ideas and methods present in [9,15,1,6] in combination with an apparently unnoticed additional property of HFE systems which is increasingly significant as the size of the ground field grows.

Organization of the paper. In Section 2, we define the degree of regularity of a system of polynomials and relate this notion to the computation of a Gröbner basis. In Section 3, we define HFE systems in greater detail and set a few notations. In Section 4, we map the problem of computing the degree of regularity to some other multivariate ring where the algebraic structure of HFE systems is apparent. This is only a more precise statement of a property used in [9,15] and our upper bound derives from the same observation that the degree of regularity is upper bounded by the degree of regularity of any subsystem. In Section 5, we show how to compute the degrees of regularity of these subsystems by using classical methods such as used in [1,6] but with the specific properties of the polynomials at hand. We deduce numerical bounds for many parameters. In Section 6, we derive estimates on the complexity of algebraic attacks on HFE.

2 Algebraic Properties of a System of Polynomials

We first give an informal presentation of the notions that will be used in the sequel and then give precise definitions and statements for our particular setting.

2.1 Solving a System of Multivariate Equations

Suppose we face the problem of finding the common roots of a system of polynomials $p_1, \ldots, p_k$ in a multivariate ring R over a field. Would this system be in few enough variables to be tried by hand, one would probably try to combine the given polynomials to derive "simpler" ones, that is, that make it easier to discover the space of solutions. For instance, one may try to obtain a polynomial in fewer variables, or with a smaller total degree. In any case, combining the given polynomials always comes down to consider polynomials of the shape $m_1p_1 + \cdots + m_kp_k$ for some polynomial multiples $m_1, \ldots, m_k$. Hence, these polynomials are linear combinations of $p_1, \ldots, p_k$ with coefficients in R. And the goal is then to find such a linear combination within some target subspace of R.

To do this mechanically, one may consider two main strategies. Either one chooses *a priori* search spaces for the m_i (for instance, polynomials with degree under some bound) and one performs linear algebra on their coefficients. (This is the basic idea of XL algorithms [5,19].) Or one defines a priority list among terms to be eliminated (called an ordering) and one performs systematic leading term reductions on polynomials $p_1, \ldots, p_k$ and the new polynomials that are generated by this process, until it can be predicted that any further combination will reduce to zero. (This is the basic idea of Gröbner bases algorithms [3,14,10,11].) These two strategies are not as different as it could seem. Indeed, to reduce the head terms of polynomials $p_1, \ldots, p_k$ the ones by the others, one determines the respective sets of multipliers $\{m_1\}, \ldots, \{m_k\}$ that are needed to do so. Then it remains to perform linear algebra on the resulting combinations and iterate with polynomials with new head terms that may be found in this process. Both strategies therefore have a clear intersection although Gröbner bases algorithms are natively more careful with the number of combinations to be dealt with.

In any case, it is convenient to arrange the available combinations with respect to their total degree. For any integer $d \geq 1$, let V_d denote the set of combinations of degree d multiples of $p_1, \ldots, p_k$. It is a linear subspace of all polynomials of degree at most d. This paper focuses on an intrinsic parameter of polynomials, which we call degree of regularity. This parameter was introduced in [2,1]. It is commonly considered as the main complexity parameter for the following intuitive reasons. Let $\mathcal{A}$ be an algorithm that computes such combinations, and indexing its execution steps by t, one may consider the subspace $V_d[\mathcal{A}(t)]$ of combinations of degree d multiples that are computed through $\mathcal{A}$ up to t. Obviously, $V_d[\mathcal{A}(t)] \subseteq V_d \subseteq R_{\leq d}$. Now, choose a target subspace $W_d \subseteq R_{\leq d}$. There exists an element of W_d among combinations in degree d when the intersection of V_d and W_d is not zero and such a combination is found by the algorithm $\mathcal{A}$ before step t if $V_d[\mathcal{A}(t)] \cap W_d \neq \{0\}$. When the polynomials $p_1, \ldots, p_k$ are not too specific, the intersection of V_d and W_d is expected to be non-zero only when the sum of their respective dimensions exceeds the dimension of $R_{\leq d}$ itself. In this case, any algorithm $\mathcal{A}$ can just consider combinations in degree d to find a non-zero element of W_d. It is assured to find one at step t if $V_d[\mathcal{A}(t)] = V_d$. On the other hand, should the intersection of V_d and W_d be non-zero at a significantly lower degree than expected for a random subspace V_d would suggest that the

polynomials $p_1, \ldots, p_k$ are not random. Interesting choices of a target subspace W_d are polynomials of low degree. For instance, one may consider whether there exists a non-zero polynomial of degree strictly lower than d among combinations in degree d. Such a combination is called a degree fall and the smallest degree at which such a degree fall occurs is essentially the degree of regularity. A precise definition will be given in the sequel. An algorithm $\mathcal{A}$ finds the degree of regularity when at some step t its subspace of combinations in degree d contains a degree fall. At this point, it is worth noting that when using a Gröbner basis algorithm it is best to use an ordering that refines the degree. Indeed in this case new head terms are confined among the smallest degree monomials.

The degree of regularity permits to distinguish a system of polynomials from random. Furthermore, any degree fall can give a new whole set of multiples in degree d or even below, which can be further combined with the existing combinations. Moreover, the dimension of $V_d^{\mathcal{A}}$ usually takes large steps as one increments d and then, many degree falls appear at once. These degree falls in turn help the appearance of new degree falls in lower degrees. Either these degree falls are low enough to solve the system (e.g. linear polynomials) or one pushes the computation until obtaining a complete Gröbner basis.

2.2 Systems with Field Equations over a Finite Field

In the setting of cryptographic schemes, the coefficient field is a finite field $\mathbb{F}_q$ (with q elements) and the solutions are searched with coordinates in this finite field. Let $x_1, \ldots, x_n$ denote the variables of R. Then one actually searches for the solutions of the system $\{p_1 = 0, \ldots, p_k = 0\}$ with the additional equations $\{x_1^q - x_1 = 0, \ldots, x_n^q - x_n = 0\}$. Equivalently, since the x_i describe values in $\mathbb{F}_q$, all monomials in R can be reduced according to the rules $x_i^q = x_i$, $i = 1, \ldots, n$. Then, all combinations of the polynomials $p_1, \ldots, p_k$ can be considered in the reduced ring $R_q = \mathbb{F}_q[x_1, \ldots, x_n]/\{x_1^q - x_1, \ldots, x_n^q - x_n\}$.

While in the sequel we compute the degree of regularity of underdetermined systems ($k \leq n$) in a reduced ring, it serves in upperbounding the degree of regularity of a public HFE system with exactly n polynomials. In this case, the expected number N of solutions is hardly more than one and it can be shown that any Gröbner basis for any ordering that refines the degree contains at least $n - N$ linearly independent degree-1 polynomials (*cf* full version). Hence, our setting makes it particularly easy to derive the solutions from a Gröbner basis.

Since in the sequel we only encounter systems of quadratic polynomials, for convenience sake we specialize the following definitions to this case. Let $p_1, \ldots, p_k$ be a system of quadratic polynomials in R_q. For any integer $d \geq 2$, consider the subspace of combinations $m_1 p_1 + \cdots + m_k p_k$ where the m_i have degree at most $d - 2$ in R_q. By definition, it is the image space of the map

$$\sigma_d(p_1, \ldots, p_k) : (m_1, \ldots, m_k) \in ((R_q)_{\leq d-2})^k \longmapsto m_1 p_1 + \cdots + m_k p_k.$$

An important observation is that the kernel of $\sigma_d(p_1, \ldots, p_k)$ always contains predictible non-zero tuples called *trivial syzygies*. Examples of trivial syzygies are the combinations over R_q of the k-tuples with $m_i = p_j$, $m_j = -p_i$ for some i, j

and 0 otherwise. A formal definition of **trivial syzygies** is the following. For indeterminates $y_1, \ldots, y_k$, let $T_q(y_1, \ldots, y_k)$ denote the set of k-tuples $(m_1, \ldots, m_k)$ over $R_q[y_1, \ldots, y_k]/\{y_1^q - y_1, \ldots, y_k^q - y_k\}$ such that $m_1 y_1 + \cdots + m_k y_k = 0$. For any polynomials $p_1, \ldots, p_k$ over R_q, we call trivial syzygies of $p_1, \ldots, p_k$ the evaluations of the k-tuples in $T_q(y_1, \ldots, y_k)$ at $(p_1, \ldots, p_k)$.

When searching for degree falls, we are only interested in the subspace V_d spanned by the highest degree homogeneous part of the image of $\sigma_d(p_1, \ldots, p_k)$. This subspace is spanned by the degree d homogeneous parts of the combinations $m_1 p_1 + \cdots + m_k p_k$ where $m_1, \ldots, m_k$ are homogeneous polynomials of degree $d-2$. We define a **degree fall** in degree d of $p_1, \ldots, p_k$ as a k-tuple $(m_1, \ldots, m_k)$ of degree $d-2$ homogeneous polynomials such that the degree d homogeneous part of $m_1 p_1 + \cdots + m_k p_k$ is zero. The degree $d-2$ homogeneous parts of the trivial syzygies of $p_1, \ldots, p_k$ in degree $d-2$ are trivially degree falls and we call them *trivial degree falls*. We call the **degree of regularity** of $p_1, \ldots, p_k$ the smallest d such that a non trivial degree fall of $p_1, \ldots, p_k$ exists in degree d.

3 Definition of HFE Systems

The construction of HFE systems is based on the linear isomorphism between $(\mathbb{F}_q)^n$ and $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Recall that $\mathbb{F}_{q^n}$ is a degree n polynomial extension over $\mathbb{F}_q$ and as a consequence is an n dimensional vector space over $\mathbb{F}_q$. Any choice of a basis of $\mathbb{F}_{q^n}$ defines a linear bijection S from $(\mathbb{F}_q)^n$ to $\mathbb{F}_{q^n}$, and extends to a linear bijection ψ_S from functions on $\mathbb{F}_{q^n}$ to functions on $(\mathbb{F}_q)^n$ by:

$$\psi_S : P \mapsto S^{-1} \circ P \circ S$$

Recall that functions on $(\mathbb{F}_q)^n$ are uniquely represented by n-tuples of polynomials in $R_q = \mathbb{F}_q[x_1, \ldots, x_n]/\{x_1^q - x_1, \ldots, x_n^q - x_n\}$ and that functions on $\mathbb{F}_{q^n}$ are uniquely represented by polynomials in $\mathbb{F}_{q^n}[X]/\{X^{q^n} - X\}$. This gives an expression of ψ_S on polynomials: $\psi_S : \mathbb{F}_{q^n}[X]/\{X^{q^n} - X\} \longrightarrow (R_q)^n$. Also recall that raising to a power of q is linear over $\mathbb{F}_q$ and that the n distinct q-powerings on $\mathbb{F}_{q^n}$ are called the **Frobenius maps**. More generally, for any power function X^a in $\mathbb{F}_{q^n}[X]/\{X^{q^n} - X\}$, we call **$q$-degree** of X^a the sum $a_0 + \cdots + a_{n-1}$, where $(a_0, a_1, \ldots, a_{n-1})$ is the decomposition of a in base q. In particular, constants have q-degree 0 and Frobenius maps have q-degree 1. Since any function in $\mathbb{F}_{q^n}[X]/\{X^{q^n} - X\}$ is a linear combination of power functions, we define q-degree as the maximal q-degree of its terms. The following proposition ensures that ψ_S maps q-degree in $\mathbb{F}_{q^n}[X]/\{X^{q^n} - X\}$ to degree in $(R_q)^n$.

Proposition 1. *Let S be an arbitrary linear bijection from $(\mathbb{F}_q)^n$ to $\mathbb{F}_{q^n}$. For any integer $d \geq 0$, ψ_S defines a bijection from polynomials in $\mathbb{F}_{q^n}[X]/\{X^{q^n} - X\}$ with q-degree d to n-tuples over R_q with degree d.*

Please refer to the full version for a proof. We are now ready to define HFE systems. Recall from the introduction that an HFE public key is the data of the n coordinate polynomials of a composition $T \circ P \circ S$ where S is a linear bijection

from $(\mathbb{F}_q)^n$ to $\mathbb{F}_{q^n}$, T is a linear bijection from $\mathbb{F}_{q^n}$ to $(\mathbb{F}_q)^n$ and P is a function on $\mathbb{F}_{q^n}$ which as a polynomial in $\mathbb{F}_{q^n}[X]/\{X^{q^n} - X\}$ has the shape

$$P(X) = \sum_{i,j \leq D} p_{ij} X^{q^i+q^j} + \sum_{k \leq D} \lambda_k X^{q^k} + c$$

where D is a parameter of the scheme. For any linear bijection S, we call **HFE systems** the systems in $(R_q)^n$ which are the images by ψ_S of the polynomials $P(X)$ of the above shape. We see from the above proposition that HFE systems are quadratic and that their only particularity in this class is to correspond to a polynomial $P(X)$ of degree upper bounded by $2q^D$. Since T is a linear bijection, an HFE public key has all the algebraic properties of an HFE system.

4 Combinations of HFE Polynomials

In this section, we map combinations of HFE systems to related operations on the defining polynomial in $\mathbb{F}_{q^n}[X]/(X^{q^n}-X)$. This mapping was outlined in [9] and is made precise here. Incidentally, it is independent of the particular shape of HFE defining polynomials and hence is valid for any cryptosystem following a similar construction. To lighten the notation, we now denote $\mathcal{R}_{q^n} = \mathbb{F}_{q^n}[X]/(X^{q^n} - X)$. This section is a chain of technical points which are necessary to make the mapping complete. For a quick reading, one may jump directly to subsection 4.4.

4.1 From Combinations in R_q to Combinations in $\mathcal{R}_{q^n}$

Let P be any polynomial in $\mathcal{R}_{q^n}$ and $(p_1, \ldots, p_n) = \psi_S(P)$. We have defined combinations of $p_1, \ldots, p_n$ as linear combinations of $p_1, \ldots, p_n$ with coefficients in R_q. Hence, n-tuples of linear combinations over R_q are products by $n \times n$ matrices over R_q. Proposition 1 implies that ψ_S^{-1} is a linear bijection from linear maps on $(\mathbb{F}_q)^n$ to linear combinations over $\mathbb{F}_{q^n}$ of the Frobenius maps. We extend this result when coefficients are in R_q and $\mathcal{R}_{q^n}$ instead of $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$.

Proposition 2. *Let S be an arbitrary linear bijection from $(\mathbb{F}_q)^n$ to $\mathbb{F}_{q^n}$. There exists an $\mathbb{F}_q$-linear bijection ψ_S^* from $(\mathcal{R}_{q^n})^n$ to $n \times n$ matrices over R_q, such that for any $M_0, \ldots, M_{n-1}$ and P in $\mathcal{R}_{q^n}$,*

$$\psi_S^*(M_0, \ldots, M_{n-1})\psi_S(P) = \psi_S(M_0 P^{q^0} + \cdots + M_{n-1} P^{q^{n-1}}). \tag{1}$$

Proof. We simply construct ψ_S^* by hand by considering the above identity over the set of constant functions $P = a$ with a in $\mathbb{F}_{q^n}$. Since ψ_S is linear we only need to consider $P = a$ for a over a basis of $\mathbb{F}_{q^n}$. For any $i = 1, \ldots, n$, let $e_i \in \mathbb{F}_{q^n}$ denote the image by S of the i-th canonical vector of $(\mathbb{F}_q)^n$. For any $M_0, \ldots, M_{n-1}$, $\psi_S^*(M_0, \ldots, M_{n-1})\psi_S(e_i)$ is the i-th column of $\psi_S^*(M_0, \ldots, M_{n-1})$ and must be set to $\psi_S(\sum_{k=0}^{n-1} M_k(e_i)^{q^k})$. ψ_S^* is linear by the linearity of ψ_S. Consider $(M_0, \ldots, M_{n-1})$ whose image by ψ_S^* is zero. Then, ψ_S being a linear bijection, for any $i = 1, \ldots, n$, we have $\sum_{k=0}^{n-1} (e_i)^{q^k} . M_k = 0$. The only solution to this invertible system is $M_0 = \cdots = M_{n-1} = 0$, which proves that ψ_S^* is injective. Surjectivity follows ψ_S^* mapping subspaces of identical dimension over $\mathbb{F}_q$. □

Equation (1) over the constants e_i also shows that the q-degree of $(M_0, \ldots, M_{n-1})$ equals the degree of $\psi_S^*(M_0, \ldots, M_{n-1})$. In particular, for any P of q-degree 2 and $d \geq 2$, we define

$$U_{\leq d}(P) = \left\{ M_0 P^{q^0} + \cdots + M_{n-1} P^{q^{n-1}} \,|\, q\text{-deg}(M_i) \leq d-2,\, i = 0, \ldots, n-1 \right\}$$

and on the other hand, for $(p_1, \ldots, p_n) = \psi_S(P)$,

$$V_{\leq d}(p_1, \ldots, p_n) = \{ m_1 p_1 + \cdots + m_n p_n \,|\, \deg(m_i) \leq d-2,\, i = 1, \ldots, n \}.$$

Property 1. For any $d \geq 2$, ψ_S is a bijection from $U_{\leq d}(P)$ to $(V_{\leq d}(p_1, \ldots, p_n))^n$.

Proof. ψ_S^* transforms n-tuples of q-degree $\leq d-2$ to $n \times n$ matrices of degree $\leq d-2$. Both spans have the same dimension over $\mathbb{F}_q$ by Proposition 1, hence ψ_S^* is a bijection from the one to the other. Finally, the property holds by the identity satisfied by ψ_S^* and evaluated at the particular P. □

Since the dimension of $(V_{\leq d})^n$ is n times the dimension of $V_{\leq d}$ and the dimension of $U_{\leq d}$ over $\mathbb{F}_q$ is n times its dimension over $\mathbb{F}_{q^n}$, the property implies

$$\dim_{\mathbb{F}_q} (V_{\leq d}(p_1, \ldots, p_n)) = \dim_{\mathbb{F}_{q^n}} (U_{\leq d}(P)).$$

4.2 From Degree Falls in R_q to q-Degree Falls in $\mathcal{R}_{q^n}$

When considering degree falls, one is really interested in the subspace spanned by the highest degree homogeneous part of a bounded degree combination space. For any quadratic polynomials $p_1, \ldots, p_n$ in R_q and any integer $d \geq 2$, let $V_d^h(p_1, \ldots, p_n)$ denote the subspace generated by the degree d homogeneous parts of polynomials in $V_{\leq d}(p_1, \ldots, p_n)$. Similarly, for any polynomial P of q-degree 2 in $\mathcal{R}_{q^n}$ and any integer $d \geq 2$, let $U_d^h(P)$ denote the subspace of q-degree d homogeneous parts of polynomials in $U_{\leq d}(P)$. Quite expectably, we have:

Property 2. Let P in $\mathcal{R}_{q^n}$ and $(p_1, \ldots, p_n) = \psi_S(P)$. Then, for any $d \geq 2$, there exists an $\mathbb{F}_q$-linear bijection from $U_d^h(P)$ to $(V_d^h(p_1, \ldots, p_n))^n$.

Proof. The highest degree homogeneous part of a polynomial p in R_q with degree $d \geq 2$ is its class mod $(R_q)_{\leq d-1}$. Hence, $V_d^h(p_1, \ldots, p_n)$ is $V_{\leq d}(p_1, \ldots, p_n)$ mod $(R_q)_{\leq d-1}$. Similarly $U_d^h(P)$ is $U_{\leq d}(P)$ mod $(\mathcal{R}_{q^n})_{\leq d-1}$. Let Q and Q' be arbitrary polynomials in $\mathcal{R}_{q^n}$ such that $Q = Q'$ mod $(\mathcal{R}_{q^n})_{\leq d-1}$. Then, $Q - Q'$ has q-degree at most $d-1$. Since ψ_S preserves the degree, $\psi_S(Q - Q')$ has degree at most $d-1$. Hence, since ψ_S is linear, $\psi_S(Q) = \psi_S(Q')$ mod $((R_q)_{\leq d-1})^n$. Therefore, ψ_S induces an $\mathbb{F}_q$-linear map from $\mathcal{R}_{q^n}$ mod $(\mathcal{R}_{q^n})_{\leq d-1}$ to $(R_q)^n$ mod $((R_q)_{\leq d-1})^n$. Since ψ_S is a bijection from $U_{\leq d}(P)$ to $(V_{\leq d}(p_1, \ldots, p_n))^n$, the induced map is a bijection from $U_d^h(P)$ to $(V_d^h(p_1, \ldots, p_n))^n$. □

Let R_q^h denote the set of homogeneous polynomials of R_q. For any polynomial p in R_q and any integer $d \geq 0$, let $[p]_d$ denote the degree d homogeneous part of

p. For any system $p_1, \ldots, p_n$ of quadratic polynomials in R_q and any $d \geq 2$, the degree falls of $p_1, \ldots, p_n$ in degree d are the kernel of the map

$$\sigma_d^h(p_1, \ldots, p_n) : (m_1, \ldots, m_n) \in ((R_q^h)_{d-2})^n \longmapsto [m_1 p_1 + \cdots + m_n p_n]_d.$$

With completely transposed notations, for any P of q-degree 2 in $\mathcal{R}_{q^n}$ and any $d \geq 2$, we define the q-degree falls of P in degree d as the kernel of the map

$$\Sigma_d^h(P) : (M_0, \ldots, M_{n-1}) \in ((\mathcal{R}_{q^n}^h)_{d-2})^n \mapsto [M_0 P + M_1 P^q + \cdots + M_{n-1} P^{q^{n-1}}]_d$$

The image spaces $\sigma_d^h(p_1, \ldots, p_n)$ and $\Sigma_d^h(P)$ respectively are $V_d^h(p_1, \ldots, p_n)$ and $U_d^h(P)$. Property 2 ensures that when $(p_1, \ldots, p_n) = \psi_S(P)$ the image spaces of $(\sigma_d^h(p_1, \ldots, p_n))^n$ and $\Sigma_d^h(P)$ have the same cardinality. Besides, Proposition 1 ensures that the same holds for their input spaces. Therefore, the kernels of $(\sigma_d^h(p_1, \ldots, p_n))^n$ and $\Sigma_d^h(P)$ have the same cardinality. Finally,

$$\dim_{\mathbb{F}_q}(\ker \sigma_d^h(p_1, \ldots, p_n)) = \dim_{\mathbb{F}_{q^n}}(\ker \Sigma_d^h(P)). \tag{2}$$

4.3 Trivial Syzygies and Trivial Degree Falls

Trivial syzygies of $p_1, \ldots, p_n$ are n-tuples over R_q such that $m_1 p_1 + \cdots + m_n p_n = 0$ even when $p_1, \ldots, p_n$ are indeterminates. They are precisely defined the following way. Let $\bar{R}_q$ denote the extension of R_q with additional variables $y_1, \ldots, y_n$, $\bar{R}_q = R_q[y_1, \ldots, y_n]/\{y_1^q - y_1, \ldots, y_n^q - y_n\}$. Let $T_q(y_1, \ldots, y_n)$ denote the set of n-tuples $(m_1, \ldots, m_n)$ over $\bar{R}_q$ such that $m_1 y_1 + \cdots + m_n y_n = 0$. For any polynomials $p_1, \ldots, p_n$ in R_q, we define its trivial syzygies as the evaluations of the n-tuples in $T_q(y_1, \ldots, y_n)$ at $(p_1, \ldots, p_n)$. As a shorthand, let $T_q(p_1, \ldots, p_n)$ denote the set of trivial syzygies of $p_1, \ldots, p_n$.

Elements of $\bar{R}_q$ are polynomials in both $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$. For any monomial in $\bar{R}_q$, let d_x, d_y denote its degrees in $x_1, \ldots, x_n$ and in $y_1, \ldots, y_n$ respectively. Since variables $y_1, \ldots, y_n$ are intended to be specialized at quadratic polynomials $p_1, \ldots, p_n$ in R_q, we define the $(1,2)$**-degree** of a monomial in $\bar{R}_q$ as $d_x + 2d_y$, and the $(1,2)$-degree of a polynomial in $\bar{R}_q$ as the maximum of the $(1,2)$-degree of its monomials. Hence, any element of $T_q(y_1, \ldots, y_n)$ with $(1,2)$-degree d yields an element of $T_q(p_1, \ldots, p_n)$ with degree $\leq d$. We call trivial syzygies of $p_1, \ldots, p_n$ with designed degree d the elements of $T_q(p_1, \ldots, p_n)$ whose corresponding element of $T_q(y_1, \ldots, y_n)$ has $(1,2)$-degree d. The trivial syzygies with designed degree $\leq d$ are denoted by $T_q(p_1, \ldots, p_n)_{\preceq d}$. On the other hand, one may analogously consider the extension of $\mathcal{R}_{q^n}$ with additional variable Y, $\bar{\mathcal{R}}_{q^n} = \mathcal{R}_{q^n}[Y]/(Y^{q^n} - Y)$, and define $\mathcal{T}_{q^n}(Y)$ as the n-tuples $(M_0, \ldots, M_{n-1})$ over $\bar{\mathcal{R}}_{q^n}$ such that $M_0 Y + M_1 Y^q + \cdots + M_{n-1} Y^{q^{n-1}} = 0$. For any P in $\mathcal{R}_{q^n}$, let $\mathcal{T}_{q^n}(P)$ denote the evaluations of the n-tuples in $\mathcal{T}_{q^n}(Y)$ at P. Finally, for any P of q-degree 2 and any $d \geq 0$, we let $\mathcal{T}_{q^n}(P)_{\preceq d}$ denote the elements whose corresponding elements in $\mathcal{T}_{q^n}(Y)$ have $(1,2)$-q-degree d. By a series of simple extensions of the previous results, we can show (*cf* full version)

Property 3. Let P in $\mathcal{R}_{q^n}$ of q-degree 2 and $(p_1, \ldots, p_n) = \psi_S(P)$. For any $d \geq 0$,

$$\dim_{\mathbb{F}_q}(T_q(p_1, \ldots, p_n)_{\preceq d}) = \dim_{\mathbb{F}_{q^n}}(\mathcal{T}_{q^n}(P)_{\preceq d}).$$

The polynomials $p_1, \ldots, p_n$ being quadratic, for any $d \geq 2$, we call trivial degree falls of $p_1, \ldots, p_n$ in degree d the homogeneous parts of (actual) degree $d-2$ of the elements in $T_q(p_1, \ldots, p_n)_{\preceq d-2}$ and denote them (with a slight abuse of notation) by $T_q(p_1, \ldots, p_n)^h_{d-2}$. Similarly, for P of q-degree 2, we call trivial q-degree falls of P in q-degree d the homogeneous parts of q-degree $d-2$ of the elements in $\mathcal{T}_q(P)_{\preceq d-2}$ and denote them by $\mathcal{T}_q(P)^h_{d-2}$. We have (*cf* full version)

Property 4. Let P in $\mathcal{R}_{q^n}$ of q-degree 2 and $(p_1, \ldots, p_n) = \psi_S(P)$. For any $d \geq 2$,

$$\dim_{\mathbb{F}_q}(T_q(p_1, \ldots, p_n)^h_{d-2}) = \dim_{\mathbb{F}_{q^n}}(\mathcal{T}_{q^n}(P)^h_{d-2}).$$

4.4 Mapping the Degree of Regularity from R_q to $\mathcal{R}_{q^n}$

Recall that the degree of regularity of a system of quadratic polynomials $p_1, \ldots, p_n$ is the smallest integer d such that a non-trivial degree fall exists in degree d. With the previous notation, this is the smallest d such that the kernel of $\sigma^h_d(p_1, \ldots, p_n)$ is strictly larger than $T_q(p_1, \ldots, p_n)^h_{d-2}$. Now, let S be an arbitrary linear bijection from $(\mathbb{F}_q)^n$ to $\mathbb{F}_{q^n}$ and P in $\mathcal{R}_{q^n}$ such that $\psi_S(P) = (p_1, \ldots, p_n)$. Then, P has q-degree 2 and, by Equality 2 and Property 3,

Property 5. the degree of regularity of $p_1, \ldots, p_n$ is the smallest d such that the kernel of $\Sigma^h_d(P)$ is strictly larger than $\mathcal{T}_{q^n}(P)^h_{d-2}$.

Hence, we obtain an equivalent characterization of the degree of regularity of $p_1, \ldots, p_n$ in term of the associated polynomial P in $\mathcal{R}_{q^n}$. In the remainder of this section, we slightly modify the above characterization to make it more conveniently usable in the analysis of the next section.

Multivariate representation of $\mathcal{R}_{q^n}$. Our first step is a simple alternative notation for the elements $\mathcal{R}_{q^n}$. This notation was proposed in [9]. As already seen, we can split any power of X according to the decomposition in base q of the exponent. Now simply introduce a distinct notation for the Frobenius of X: for $i = 0, \ldots, n-1$, let X_i denote X^{q^i}. Observe that for any $i = 0, \ldots, n-1$, $X_i^q - X_{i+1} = 0$ where the indices are taken modulo n. Using these relations, any power of X corresponds to a unique multivariate monomial in $X_0, \ldots, X_{n-1}$. It extends trivially to all polynomials in $\mathcal{R}_{q^n}$. Addition and multiplication are compatible with this notation. Therefore, $\mathcal{R}_{q^n}$ identifies as a ring with $\mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]/\{X_0^q - X_1, \ldots, X_{n-1}^q - X_0\}$. Along with this identification, q-degree becomes degree in the multivariate ring. Also, for any polynomial P in $\mathcal{R}_{q^n}$, let $P_0, \ldots, P_{n-1}$ denote its successsive Frobenius. For any $i = 0, \ldots, n-1$, $P_i^q - P_{i+1} = 0$ where indices are modulo n. When P has q-degree 2, its Frobenius are multivariate quadratic polynomials. Since the P-termed sets really express in terms of the Frobenius of P, they are conveniently rewritten with the above notation. Hence, $\Sigma^h_d(P)$ rewrites to

$$\Sigma^h_d(P_0, \ldots, P_{n-1}) : (M_0, \ldots, M_{n-1}) \in (\mathcal{R}^h_{q^n})_{d-2} \mapsto [M_0 P_0 + \cdots + M_{n-1} P_{n-1}]_d.$$

The ring $\bar{\mathcal{R}}_{q^n} = \mathcal{R}_{q^n}[Y]/(Y^{q^n} - Y)$ rewrites to $\mathcal{R}_{q^n}[Y_0, \ldots, Y_{n-1}]/\{Y_0^q - Y_1, \ldots, Y_{n-1}^q - Y_0\}$. The set $\mathcal{T}_{q^n}(Y)$ rewrites to $\mathcal{T}_{q^n}(Y_0, \ldots, Y_{n-1})$, the n-tuples $(M_0, \ldots, M_{n-1})$ over $\bar{\mathcal{R}}_{q^n}$ such that $M_0Y_0 + \cdots + M_{n-1}Y_{n-1} = 0$. Hence, $\mathcal{T}_{q^n}(P)$ identifies with $\mathcal{T}_{q^n}(P_0, \ldots, P_{n-1})$. And the elements of $\mathcal{T}_{q^n}(P_0, \ldots, P_{n-1})_d^h$ are the degree d homogeneous parts of the elements of $\mathcal{T}_{q^n}(P_0, \ldots, P_{n-1})_{\preceq d}$. Finally, our characterization (Property 5) rewrites to, when $(p_1, \ldots, p_n) = \psi_S(P)$,

Property 6. the degree of regularity of $p_1, \ldots, p_n$ equals the degree of regularity of $P_0, \ldots, P_{n-1}$, the n Frobenius of P in the multivariate representation of $\mathcal{R}_{q^n}$.

At this point, our task is reduced to studying the degree of regularity of the quadratic polynomials $P_0, \ldots, P_{n-1}$ in $\mathcal{R}_{q^n}$, and we do not need to address the polynomials $p_1, \ldots, p_n$ any further. The next paragraph is devoted to refining the characterization of the degree of regularity of $P_0, \ldots, P_{n-1}$.

Characterizing the Degree of Regularity of Systems of $\mathcal{R}_{q^n}$. Our first observation is a simple one: the highest degree terms of combinations in degree d of $P_0, \ldots, P_{n-1}$ only depends on their highest degree terms $\hat{P}_0, \ldots, \hat{P}_{n-1}$.

Property 7. The degree of regularity of quadratic polynomials in $\mathcal{R}_{q^n}$ equals the degree of regularity of their degree 2 homogeneous parts.

Proof. For any degree $d-2$ homogeneous polynomials $M_0, \ldots, M_{n-1}$, the associated combinations of $P_0, \ldots, P_{n-1}$ and $\hat{P}_0, \ldots, \hat{P}_{n-1}$ have the same degree d homogeneous part. Hence, degree falls in degree d are the same for both systems of polynomials. On the other hand, the trivial syzygies of $P_0, \ldots, P_{n-1}$ of designed degree $d-2$ have the same degree $d-2$ homogeneous parts as the trivial syzygies of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ of designed degree $d-2$. The property follows. □

Our second observation is more subtle: when considering combinations of the quadratic homogeneous polynomials $\hat{P}_0, \ldots, \hat{P}_{n-1}$ with degree $d-2$ homogeneous coefficients, terms of degree smaller than d can only appear with reductions modulo the polynomials $X_i^q - X_{i+1}$, $i = 0, \ldots, n-1$. Since all terms with degree smaller than d are discarded, the same result is obtained as when performing combinations in the ring $\boldsymbol{\mathcal{R}}_{q^n} = \mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]/\{X_0^q, \ldots, X_{n-1}^q\}$. Considering combinations in $\boldsymbol{\mathcal{R}}_{q^n}$ rather than in $\mathcal{R}_{q^n}$, the map $\Sigma_d^h(\hat{P}_0, \ldots, \hat{P}_{n-1})$ simply rewrites to $\boldsymbol{\Sigma}_d^h(\hat{P}_0, \ldots, \hat{P}_{n-1})$:

$$(M_0, \ldots, M_{n-1}) \in ((\boldsymbol{\mathcal{R}}_{q^n}^h)_{d-2})^n \mapsto M_0\hat{P}_0 + M_1\hat{P}_1 + \cdots + M_{n-1}\hat{P}_{n-1}.$$

Furthermore, we can equivalently characterize the trivial degree falls using the ring structure of $\boldsymbol{\mathcal{R}}_{q^n}$. Consider $\bar{\boldsymbol{\mathcal{R}}}_{q^n} = \boldsymbol{\mathcal{R}}_{q^n}[Y_0, \ldots, Y_{n-1}]/\{Y_0^q, \ldots, Y_{n-1}^q\}$ and the associated set $\boldsymbol{\mathcal{T}}_{q^n}(Y_0, \ldots, Y_{n-1})$. For any $d \geq 0$, we can define the sets $\boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{n-1})_{\preceq d}$ and $\boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{n-1})_d^h$, exactly as before.

Property 8. For any $d \geq 0$, the sets $\mathcal{T}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{n-1})_d^h$ and $\boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{n-1})_d^h$ are identical. Therefore, for any $d \geq 2$, the trivial degree falls of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ in degree d are the elements of $\boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{n-1})_{d-2}^h$.

Proof. For any $(M_0, \ldots, M_{n-1})$ in $\boldsymbol{\mathcal{T}}_{q^n}(Y_0, \ldots, Y_{n-1})$, let Q denote the combination $M_0Y_0 + \cdots + M_{n-1}Y_{n-1}$ in $\mathcal{R}_{q^n}[Y_0, \ldots, Y_{n-1}]$. Since Q is zero modulo $Y_0^q, \ldots, Y_{n-1}^q$, any of its term is divisible by at least one of $Y_0^q, \ldots, Y_{n-1}^q$. Since $M_0, \ldots, M_{n-1}$ have degree at most $q-1$ in any Y_i, any term of Q can have degree q in only one single indeterminate and at most $q-1$ in all the others. Therefore, any term of Q exactly has degree q is one indeterminate and at most $q-1$ in all the others. Hence, Q admits a unique decomposition $A_0Y_0^q + \cdots + A_{n-1}Y_{n-1}^q$. Using the unique polynomials $A_0, \ldots, A_{n-1}$ associated to $(M_0, \ldots, M_{n-1})$, we construct an element $(M'_0, \ldots, M'_{n-1})$ of $\mathcal{T}_{q^n}(Y_0, \ldots, Y_{n-1})$ by setting for all $i = 0, \ldots, n-1$, $M'_i = M_i - A_{i-1}$ (indices are modulo n). Now, observe that the terms of $A_0, \ldots, A_{n-1}$ consist of terms of $M_0, \ldots, M_{n-1}$ divided by one indeterminate to the power of $q-1$. As a consequence, each of them has a total degree in the Y_i variables smaller (by $q-1$) than the one it originates from. In particular, when $M_0, \ldots, M_{n-1}$ have $(1,2)$-degree at most d, $M'_0, \ldots, M'_{n-1}$ respectively have the same terms of $(1,2)$-degree d as $M_0, \ldots, M_{n-1}$ because they differ by terms of strictly smaller $(1,2)$-degree. □

Hence, we end up with the following characterization which we use in the sequel.

Property 9. Let $\hat{P}_0, \ldots, \hat{P}_{n-1}$ be homogeneous quadratic polynomials in $\mathcal{R}_{q^n}$. The degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ can be computed in $\boldsymbol{\mathcal{R}}_{q^n}$ as the smallest $d \geq 2$ such that degree $d-2$ homogeneous n-tuples $(M_0, \ldots, M_{n-1})$ satisfying $M_0\hat{P}_0 + \cdots + M_{n-1}\hat{P}_{n-1} = 0$ exist besides the elements of $\boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{n-1})_d^h$.

5 Bounding the Degree of Regularity of HFE Systems

We first describe the proof principle of our upper bound and then perform the combinatorial computations that convey the result.

5.1 Upper Bounding the Degree of Regularity

First consider arbitrary homogeneous quadratic polynomials $\hat{P}_0, \ldots, \hat{P}_{k-1}$ in $\boldsymbol{\mathcal{R}}_{q^n}$ where $k \leq n$. The dimensions of the kernel and the image of the map

$$\begin{aligned} \boldsymbol{\Sigma}_d^h(\hat{P}_0, \ldots, \hat{P}_{k-1}) : \quad ((\boldsymbol{\mathcal{R}}_{q^n})_{d-2}^h)^k &\longrightarrow (\boldsymbol{\mathcal{R}}_{q^n})_d^h \\ (M_0, \ldots, M_{k-1}) &\longmapsto M_0\hat{P}_0 + M_1\hat{P}_1 + \cdots + M_{k-1}\hat{P}_{k-1} \end{aligned}$$

relate to each other by

$$k \dim(\boldsymbol{\mathcal{R}}_{q^n})_{d-2}^h - \dim \ker \boldsymbol{\Sigma}_d^h(\hat{P}_0, \ldots, \hat{P}_{k-1}) = \dim \operatorname{Im}(\boldsymbol{\Sigma}_d^h(\hat{P}_0, \ldots, \hat{P}_{k-1})).$$

Not knowing what the degree of regularity of the system is, one can assume that it is not reached while incrementing d. In this case, the kernel is assumed to contain only the trivial elements of $\boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{k-1})_{d-2}^h$. Since the image is confined in $(\boldsymbol{\mathcal{R}}_{q^n})_d^h$, a contradiction to this assumption appears as soon as

$$k \dim(\boldsymbol{\mathcal{R}}_{q^n})_{d-2}^h - \dim \boldsymbol{\mathcal{T}}_{q^n}(\hat{P}_0, \ldots, \hat{P}_{k-1})_{d-2}^h > \dim(\boldsymbol{\mathcal{R}}_{q^n})_d^h$$

and then we know that the degree of regularity was reached before. The smallest d satisfying this "saturation" condition is therefore an upper bound on the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{k-1}$. Since it is valid for any homogeneous quadratic polynomials, we refer to it as the *MQ bound.*

We now show how in the case of HFE systems better bounds can be obtained.

5.2 The Case of HFE Systems

It was noted in [15] that when $\hat{P}_0, \ldots, \hat{P}_{n-1}$ are obtained from the Frobenius of an HFE polynomial P, they express over small shifted sets of consecutive variables: $\hat{P}_0$ expresses over X_0 to X_D, $\hat{P}_1$ expresses over X_1 to X_{D+1}, ..., $\hat{P}_{n-1}$ expresses over X_{n-1} to X_{D-1} (indices are modulo n). Then, the authors noted that a consequence of this property is that small subsystems of consecutive polynomials only involve a small subset of the available variables. Consecutive subsystems of a prescribed size being all equivalent up to a cyclic shift, we focus on the n subsystems $\mathcal{S}_k = \{\hat{P}_0, \ldots, \hat{P}_{k-1}\}$ for $k = 1, \ldots, n$. The subsystem $\mathcal{S}_k$ expresses over the first m_k variables, where $m_k = D + k$ for all $k \leq n - D$ and $m_k = n$ beyond. The degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ is upper bounded by the respective degrees of regularity d_k of the subsystems $\mathcal{S}_k$ for all $k = 1, \ldots, n$. Indeed the degree falls of $\mathcal{S}_k$ identify with the degree falls of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ with zero on the last $n-k$ coordinates. On the other hand we will show in Section 5.3 (Property 11) that whenever a degree fall is non-trivial for $\mathcal{S}_k$, its completion with zero on the last $n - k$ coordinates is non-trivial for $\hat{P}_0, \ldots, \hat{P}_{n-1}$. At this point, the authors of [15] estimated the degree of regularity of any subsystem $\mathcal{S}_k$ by using an asymptotic formula from [2]. This needed restricting to $q = 2$ and assuming that the quadratic polynomials $\hat{P}_0, \ldots, \hat{P}_{k-1}, X_0^2, \ldots, X_{m_k-1}^2$ satisfy the condition for which the formula holds. Instead, we use the previous saturation bound: we upper bound the degree of regularity of $\mathcal{S}_k$ by applying the MQ bound to $\hat{P}_0, \ldots, \hat{P}_{k-1}$. Hence it is upper bounded by the smallest d such that

$$k \dim(\boldsymbol{\mathcal{R}}_{q^n|m_k})_{d-2}^h - \dim \boldsymbol{\mathcal{T}}_{q^n|m_k}(\hat{P}_0, \ldots, \hat{P}_{k-1})_{d-2}^h > \dim(\boldsymbol{\mathcal{R}}_{q^n|m_k})_d^h \quad (3)$$

where $\boldsymbol{\mathcal{R}}_{q^n|m_k}$ denotes the restriction of $\boldsymbol{\mathcal{R}}_{q^n}$ to the first m_k variables. Since this upper bound uses a property showed in [15], we refer to it as the *GJS bound.*

We now observe an additional property of HFE systems. Since polynomials $\hat{P}_0, \ldots, \hat{P}_{n-1}$ write over monomials $X_i X_{i+\ell}$ with $\ell \leq D$, combinations of these polynomials necessarily write over the monomials which are divisible by $X_i X_{i+\ell}$ for some i and $\ell \leq D$. Let $\boldsymbol{\mathcal{M}}_q^D$ denote the subspace spanned by such monomials. For any subsystem $\mathcal{S}_k$, we improve the GJS bound by the smallest d such that

$$k \dim(\boldsymbol{\mathcal{R}}_{q^n|m_k})_{d-2}^h - \dim \boldsymbol{\mathcal{T}}_{q^n|m_k}(\hat{P}_0, \ldots, \hat{P}_{k-1})_{d-2}^h > \dim(\boldsymbol{\mathcal{M}}_q^D|m_k)_d^h \quad (4)$$

where $(\boldsymbol{\mathcal{M}}_q^D|m_k)_d^h$ denotes the subspace spanned by degree d monomials of $\boldsymbol{\mathcal{M}}_q^D$ in the first m_k variables. The distinction between $\boldsymbol{\mathcal{M}}_q^D$ and $\boldsymbol{\mathcal{R}}_{q^n}^h$ is increasingly significant as q grows. Indeed, at fixed n and d, the average Hamming weight of multidegrees in degree d decreases as q grows. Then, the proportion of monomials

containing two variables distant by at most D indices (mod n) grows thiner. We call *HFE bound* the upper bound on the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ obtained from the latter improvement.

We now compute for any $d \geq 2$ and any $k = 1, \ldots, n$, the above dimensions by means of induction formulae and deduce the related numerical upper bound.

5.3 Induction Formulae for Computing Our Upper Bound

We show how to compute the dimensions of $(\boldsymbol{\mathcal{R}}_{q^n|m})_d^h$, $(\boldsymbol{\mathcal{M}}_q^D|m)_d^h$ and $\boldsymbol{\mathcal{T}}_{q^n|m}(\hat{P}_0, \ldots, \hat{P}_{k-1})_d^h$, for any $m, k = 1, \ldots, n$.

The dimension $H(m, d)$ of $(\boldsymbol{\mathcal{R}}_{q^n|m})_d^h$ is simply the number of homogeneous monomials of degree d in m variables, where all exponents are bounded between 0 and $q-1$. Obviously, it equals $H(m, d) = 0$ for $d < 0$, or $d > 0$ and $m \leq 0$, we have $H(m, 0) = 1$ for all m, and when $d > 0, m > 0$ it satisfies the induction $H(m, d) = \sum_{\alpha=0}^{q-1} H(m-1, d-\alpha)$. Equivalently, $H(m, d)$ is the d-th term of the series $((1-z^q)/(1-z))^u$ of term z. In particular, for $q = 2$, $H(u, d) = \binom{u}{d}$.

The Number of Monomials Arising in Combinations of HFE. For any $d \geq 0$, and $u = 1, \ldots, n$, let $C(u, d)$ denote the dimension the complement of $(\boldsymbol{\mathcal{M}}_q^D|u)_d^h$ in $(\boldsymbol{\mathcal{R}}_{q^n|u})_d^h$. This is the number of monomials of degree d in u consecutive variables, with exponents modulo q, such that all variables with non-zero exponents have indices (modulo n) distant by at least $D+1$ positions. First, ignore that distance between indices is taken modulo n, and that we allow for instance X_0 and X_{u-1} to have both a non-zero power. Then, $C'(u, d)$ is given by the simple "Pascal's triangle" formula $C'(u, d) = C'(u-1, d) + \sum_{\alpha=1}^{q-1} C'(u-D-1, d-\alpha)$ for any $u = 1, \ldots, n$, where $C(u, 0) = 1$ and $C(u, d) = 0$ whenever $d < 0$ or $u \leq 0$. When u is lower than $n-D$, then the requested dimension $C(u, d)$ is there equal to $C'(u, d)$ since the last D variables have zero exponents. Otherwise, when $u > n-D$, the distance must be taken modulo n, so we deduce all values of $C(n, d)$ by considering the partitions defined by monomials containing X_0, plus monomials containing X_1, ..., plus monomials containing X_{D-1}, plus monomials containing none of them. Hence, $C(u, d) = C'(u-D, d) + D\sum_{\alpha=1}^{q-1} C'(n-1-2D, d-\alpha)$. Finally, $\dim(\boldsymbol{\mathcal{M}}_q^D|u)_d^h = H(u, d) - C(u, d)$.

The Dimension of Trivial Syzygies in Degree *d*. Simply denote $\boldsymbol{\mathcal{R}}_{q^n|m}$ by $\boldsymbol{\mathcal{R}}_m$. Our first step is to exhibit generators for the module $\boldsymbol{\mathcal{T}}_m(Y_0, \ldots, Y_{k-1})$.

Property 10. An n-tuple $(M_0, \ldots, M_{k-1})$ is an element of $\boldsymbol{\mathcal{T}}_m(Y_0, \ldots, Y_{k-1})$ if and only if it is a combination with polynomial coefficients of the n-tuples

$$\begin{cases} \Gamma_{ij} = (0, \ldots, 0, M_i = Y_j, 0, \ldots, 0, M_j = -Y_i, 0, \ldots, 0), & i, j = 0, \ldots, k-1, \\ \Phi_i = (0, \ldots, 0, M_i = Y_i^{q-1}, 0, \ldots, 0), & i = 0, \ldots, k-1. \end{cases}$$

Proof. For any n-tuple $(M_0, \ldots, M_k)$, decompose M_i into $\bar{M}_i Y_i^{q-1} + M_i'$. An n-tuple $(M_0, \ldots, M_k)$ is an element of $\boldsymbol{\mathcal{T}}_{q^n}(Y_0, \ldots, Y_k)$ if and only if $M_0 Y_0 + \cdots +$

M_kY_k is zero modulo $Y_0^q, \ldots, Y_k^q$. This is equivalent to $M'_0Y_0 + \cdots + M'_kY_k = 0$ (without modulo). We prove that this latter equality implies that $(M'_0, \ldots, M'_k)$ is a combination of (Γ_{ij}). We do this through induction on k. If $k = 1$ then, if M'_0 or M'_1 is zero they are both zero, otherwise $M'_0 = M''Y_1$ and $M'_1 = -M''Y_0$ and $(M'_0, M'_1) = M''(Y_1, -Y_0)$. Assume the property holds up to $k-1$. Then, if M'_k is zero, we fall on the property at $k-1$, otherwise all M'_i, $i = 0, \ldots, k-1$ must contain Y_k and denoting by M''_i the quotient, we have $M'_k = -(M''_0Y_0 + \cdots + M''_{k-1}Y_{k-1})$, from which we get $(M'_0, \ldots, M'_k) = M''_0\Gamma_{0,k} + \cdots + M''_{k-1}\Gamma_{k-1,k}$. Coming back to the main proof, we get$(M_0, \ldots, M_k) = \bar{M}_0\Phi_0 + \cdots + \bar{M}_k\Phi_k + (M'_0, \ldots, M'_k)$where the last n-tuple decomposes over (Γ_{ij})'s. □

Since Γ_{ij}'s and Φ_i's are homogeneous in the variables $Y_0, \ldots, Y_{k-1}$, the $(1,2)$-degree d parts of the elements of $\boldsymbol{\mathcal{T}}_m(Y_0, \ldots, Y_{k-1})$ themselves decompose over these generators. Replacing variables $Y_0, \ldots, Y_{k-1}$ respectively by $\hat{P}_0, \ldots, \hat{P}_{k-1}$, trivial syzygies in degree d of $\hat{P}_0, \ldots, \hat{P}_{k-1}$ write

$$\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})^h_d = (\boldsymbol{\mathcal{R}}_m)^h_{d-2}\{\Gamma_{ij}\}_{0\le i<j\le k-1} + (\boldsymbol{\mathcal{R}}_m)^h_{d-2(q-1)}\{\Phi_i\}_{0\le i\le k-1},$$

where we again denote by Γ_{ij}'s and Φ_i's their specializations at $(\hat{P}_0, \ldots, \hat{P}_{k-1})$. Unfortunately, decomposition over the above generators is not unique. Therefore, the dimension of $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})^h_d$ can not be directly read from the above formula. However, we see that this dimension follows a simple induction.

Let $\partial\Gamma_{d,k}$ denote the subspace spanned by $\Gamma_{i,k}$, $i = 0, \ldots, k-1$ $(k \ge 1)$ and $\partial\Phi_{d,k}$ denote the subspace spanned by Φ_k. Then, for $k \ge 1$,

$$\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_d = \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})^h_d + (\partial\Gamma_{d,k} + \partial\Phi_{d,k}). \tag{5}$$

For $k = 1$, we simply have $\boldsymbol{\mathcal{T}}_m(\hat{P}_0)^h_d = \partial\Phi^1_d$. For all $k \ge 1$, the increase of dimension when adding $\partial\Gamma_{d,k} + \partial\Phi_{d,k}$ is the dimension of the quotient space $(\partial\Gamma_{d,k} + \partial\Phi_{d,k}) \bmod \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})^h_d$. Now we use the following property.

Property 11. For d up to the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_k$,

$$\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_d \cap \{(*, \ldots, *, 0)\}_d = \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})^h_d.$$

(Hence, the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_k$ is upper-bounded by the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{k-1}$ because a cancellation of $\hat{P}_0, \ldots, \hat{P}_{k-1}$ which is non-trivial in the sense of $\hat{P}_0, \ldots, \hat{P}_{k-1}$ is non-trivial in the sense of $\hat{P}_0, \ldots, \hat{P}_k$.)

Proof. First recall that Γ_{ij}'s have degree 2 and ϕ_i's have degree $2(q-1) \ge 2$. As a consequence $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})$ has no element in degree 0 or 1.

For any $1 \le \alpha \le q$ and $d \ge 0$, define the set

$$\boldsymbol{\mathcal{T}}^{*\alpha}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_d = \left\{ (M_0, \ldots, M_{k-1}, 0) \;\middle|\; \begin{array}{r} \exists M_k^{(\alpha)}, (M_0, \ldots, M_{k-1}, M_k^{(\alpha)} P_k^{q-\alpha}) \\ \in \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_d \end{array} \right\}$$

Observe that for $\alpha = 1$, this set is exactly $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_d \cap \{(*, \ldots, *, 0)\}_d$. We show that for d up to the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_k$, and $\alpha \le q-1$,

$$\boldsymbol{\mathcal{T}}^{*\alpha}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_d \subseteq \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})^h_d + P_k\boldsymbol{\mathcal{T}}^{*(\alpha+1)}_m(\hat{P}_0, \ldots, \hat{P}_k)^h_{d-2}. \tag{6}$$

Indeed, let $(M_0, \ldots, M_{k-1}, 0)$ belong to the left handside. By definition, there exists M_k^α such that $(M_0, \ldots, M_{k-1}, M_k^\alpha P_k^\alpha)$ is in $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)_d^h$. Refer to the decomposition 5 of this set. Hence there exists an element T_k of $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})_d^h$ (with its last coordinate to zero) and coefficients $\mu_0, \ldots, \mu_{k-1}, \nu_k$ such that $(M_0, \ldots, M_{k-1}, M_k^\alpha P_k^\alpha) = T_k + \mu_0 \Gamma_{0k} + \cdots + \mu_{k-1}\Gamma_{k-1,k} + \nu_k \phi_k$. Coordinate-wise identity writes

$$\begin{cases} (M_0, \ldots, M_{k-1}, 0) = T_k + P_k(\mu_0, \ldots, \mu_{k-1}, 0), \\ -M_k^\alpha P_k^\alpha = \mu_0 P_0 + \cdots + \mu_{k-1} P_{k-1} - \nu_k P_k^{q-1}. \end{cases}$$

The second equation implies that $(\mu_0, \ldots, \mu_{k-1}, M_k^\alpha P_k^{\alpha-1} - \nu_k P_k^{q-2})$ lies in $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)_{d-2}^h$, which shows (6). Now by using (6), from 1 to $\alpha \leq q-1$,

$$\boldsymbol{\mathcal{T}}_m^{*1}(\hat{P}_0, \ldots, \hat{P}_k)_d^h \subseteq \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})_d^h + P_k^\alpha \boldsymbol{\mathcal{T}}_m^{*(\alpha+1)}(\hat{P}_0, \ldots, \hat{P}_k)_{d-2\alpha}^h.$$

The second summand is zero as soon as $d - 2\alpha \leq 1$. As α increases to $q-1$, one either encounters this case or ends up with $P_k^{q-1}\boldsymbol{\mathcal{T}}_m^{*q}(\hat{P}_0, \ldots, \hat{P}_k)_{d-2(q-1)}^h$. But again any $(M_0, \ldots, M_{k-1}, 0)$ of the set in factor writes $T_k + P_k(\mu_0, \ldots, \mu_{k-1}, 0)$. In the product set, the second summand vanishes by $P_k^q = 0$. □

By Property 11, two n-tuples of $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_k)_d^h$ are equivalent modulo $\boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})_d^h$ if and only if they have the same $(k+1)$-th coordinate. Hence, the marginal dimension of the second summand in 5 is the dimension of $(\boldsymbol{\mathcal{R}}_m)_{d-2}^h\{\hat{P}_i\}_{0\leq i\leq k-1} + (\boldsymbol{\mathcal{R}}_m)_{d-2(q-1)}^h \hat{P}_k^{q-1}$. Let $\tau_{k,d} = \dim \boldsymbol{\mathcal{T}}_m(\hat{P}_0, \ldots, \hat{P}_{k-1})_d^h$ and let $\delta_{k+1,d}^{q-1}$ be the dimension of the above. So far, $\tau_{k+1,d} = \tau_{k,d} + \delta_{k+1,d}^{q-1}$. Furthermore, iterating this process, we can show (*cf* full version for a proof)

Lemma 1. *For any $1 \leq \alpha \leq q-1$, let $\delta_{k+1,d}^\alpha$ denote the dimension of $(\boldsymbol{\mathcal{R}}_m)_{d-2}^h\{\hat{P}_i\}_{0\leq i\leq k-1} + (\boldsymbol{\mathcal{R}}_m)_{d-2\alpha}^h \hat{P}_k^\alpha$. For d up to the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_k$, this dimension follows the induction*

$$\delta_{k+1,d}^\alpha = k \dim(\boldsymbol{\mathcal{R}}_m)_{d-2}^h - \tau_{k+1,d-2} + \delta_{k+1,d-2}^{\alpha-1},$$

for any $\alpha \geq 2$, and $\delta_{k+1,d}^1 = (k+1)\dim(\boldsymbol{\mathcal{R}}_m)_{d-2}^h - \tau_{k+1,d-2}$.

Using this lemma we finally find the induction defining $\tau_{k,d}$ for any $k \leq n$ and d up to the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{n-1}$,

$$\tau_{k+1,d} = \tau_{k,d} + \textstyle\sum_{i=1}^{q-1} \left(k \dim(\boldsymbol{\mathcal{R}}_m)_{d-2i}^h - \tau_{k+1,d-2i}\right) + \dim(\boldsymbol{\mathcal{R}}_m)_{d-2(q-1)}^h. \quad (7)$$

5.4 Numerical Computation of the Upper Bounds

We numerically computed the above induction formulas using a dynamic programming approach. A simple complexity analysis can be found in the full version. Figure 1 below represents the upper bounds on the degree of regularity of HFE systems for many parameters q, n. The corresponding value of D was set

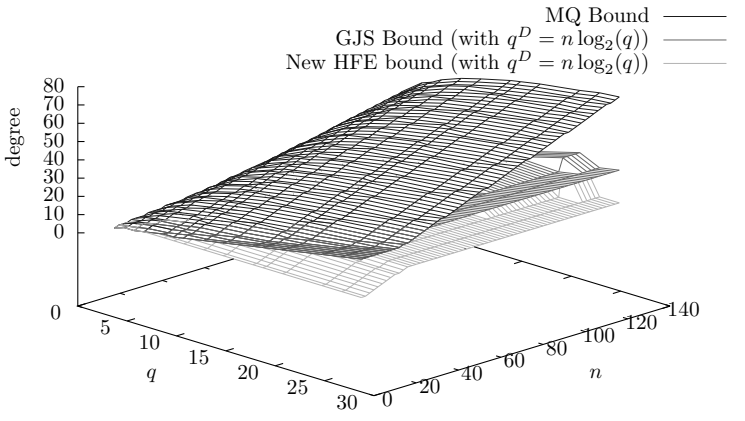

Fig. 1. Overview of the three upper bounds for many HFE parameters: MQ, GJS, HFE

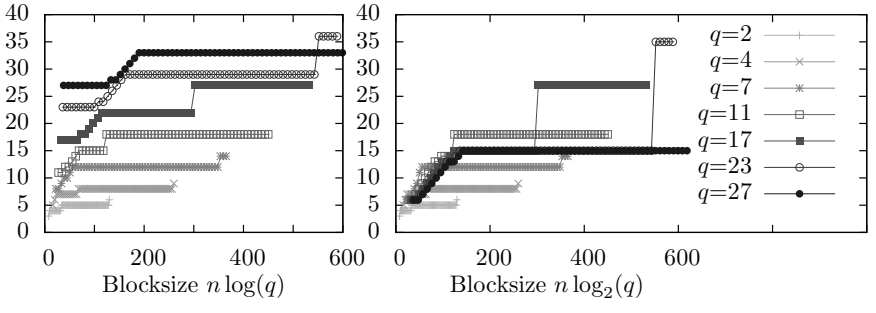

Fig. 2. Comparing the two upper bounds specific to HFE: GJS, HFE bounds

to satisfy $q^D = n \log_2 q$, that is, the degree of the internal HFE polynomial is indexed on the block size. This choice lets schemes operating on the same block size have comparable complexity of the secret operations (roughly $(\log_2 q)^3 n^5$ using the algorithms suggested in [16]). One can note that the surface rendering the GJS bound initially coincides with the MQ surface while our bound ensures a much smaller degree of regularity. Figure 2 below renders (*cf* full version for colorful figures) the improvement of the HFE bound over the GJS bound as q grows. One can perceive the significance of this improvement from the curves being massively pulled down. This is especially true for small blocksizes where the GJS bound is lower bounded by q while the corresponding value of the HFE bound is roughly independent of the value of q.

6 Application to the Security of HFE

The previous discussion has led to the ability to compute an upper bound on the degree of regularity of HFE systems for any parameters. In this section, we describe applications of this parameter to the security of HFE.

6.1 Computing the Degree of Regularity in Practice

We consider a simple algorithm which given the n quadratic polynomials and a prescribed degree $d \geq 2$ computes a generator basis of combinations in degree d of these polynomials (given by monomial multiples of each polynomial) and puts them in row echelon form (any ordering of terms can be used). It is then trivial to obtain the dimension spanned by these combinations. As a consequence, using this algorithm with d incrementing from 2, one can compare the experimental dimension of combinations with the one predicted until the degree of regularity is found. As soon as these dimensions disagree, current d is the degree of regularity of the system. Hence, this simple procedure allows to compute the degree of regularity is practice. Denote by $M_q(n, d)$ the number of monomials of degree d in n variables with exponents modulo q. In degree d, the canonical generator basis has size $M_q(n, d-2)n$. Each such vector has at most $n(n+1)/2$ non-zero coefficients. Computing a row echelon form of these vectors therefore has time complexity about $M_q(n, d-2)^2 n^4$ and space complexity at most $S_q(n, d) = M_q(n, d-2)^2 n^2$. When making d range from 2 to some prescribed d_{max}, the complexity of the iteration is dominated by the complexity at $d = d_{max}$ because $M_q(n, d-2)$ grows exponentially with d. In particular, for HFE(q, n, D) systems, the complexity of computing the degree of regularity is upper bounded by the latter complexity at d set to the HFE bound $\delta(q, n, D)$ computed previously. Since the degree of regularity of random MQ systems is expected very closely tied to the MQ bound (which is much higher for practical parameters), the degree of regularity provides a way to algorithmically distinguish HFE systems from random MQ instances. This distinguisher was already addressed in [4,9,15] and we refer to it as the algebraic distinguisher. Our result makes it possible to compute its complexity for any parameters. Comparing this complexity with the complexity of the differential distinguisher presented in [8], it turns out the latter is almost always far more efficient (*cf* full version of the paper).

6.2 Estimated Upper Bound for Solving HFE Systems

A more critical application uses the heuristic that the degree of regularity originates from the saturation of a subspace of combinations, yielding many degree falls at once. These degree falls in turn contribute to further saturations and further degree falls in smaller degree. When computing a Gröbner basis with a graded ordering, this initiates a process of new head terms appearing with decreasing degree and precipitates the end of the computation. Due to these heuristics, it is commonly taken that the degree of regularity estimates the maximal degree needed in the computation of a Gröbner basis for a graded ordering. In our case, this heuristic is supported by our upper bound on the degree of regularity of HFE closely matching the experimental maximal degree given for $q = 2$ in [12]. As to the complexity of the Gröbner basis computation, it is also commonly estimated as the cost of row echelon form on the combinations matrix at the maximal degree. Although, some algorithms offer improvements to reduce the combinations matrix by removing trivial syzygies [11,13], we keep on

the simple analysis of the precedent paragragh. When a more detailed analysis is available for a particular algorithm our upper bound on the degree of regularity can be readily plugged into it to obtain tighter complexity upper bounds. Figure 3 below represents the obtained upper bound for many HFE parameters, where the degree of the internal parameter is again indexed on the block size by $q^D = n \log_2 q$. Within the limits of the above heuristics, parameters that do not emerge from the 80-bits security level should not be considered secure.

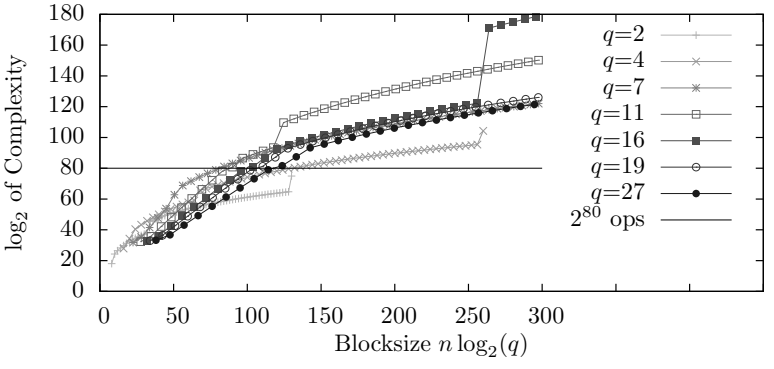

Fig. 3. Estimated Upper Bounds on the Complexity of Algebraic Attacks on HFE

7 Conclusion

In this paper, we provide a rigourous analysis of the degree of regularity of HFE systems. Under commonly used heuristics, this analysis allows to derive estimates for the complexity of algebraic attacks on the public key. In particular, using these estimates, hardly any HFE cryptosystem with block size 80 bits can achieve 80 bits security. HFE over $GF(2)$ with blocksize 128 does not achieve 80 bits security. On the other hand, our work can not be used to infer the security of HFE parameters, because our estimates are only complexity upper bounds and focus on a particular type of attack. Finally, we point out that the first part of our work – shifting the analysis to the internal polynomial – can be used for any cryptosystem following a similar construction to HFE. In particular, it potentially offers a useful framework to the analysis of variations of HFE.

References

1. Bardet, M.: Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et ála cryptographie. PhD thesis, UniversitéParis 6 (2004)
2. Bardet, M., Faugére, J.-C., Salvy, B.: On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations. In: ICPSS International Conference on Polynomial System Solving (2004)
3. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassnringes nach einem nulldimensionalen Polynomideal. PhD thesis, Innsbruck (1965)

4. Courtois, N.: The Security of Hidden Field Equations (HFE). In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 266–281. Springer, Heidelberg (2001)
5. Courtois, N., 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)
6. 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)
7. Ding, J., Schmidt, D., Werner, F.: Algebraic attack on hfe revisited. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 215–227. Springer, Heidelberg (2008)
8. Dubois, V., Granboulan, L., Stern, J.: An Efficient Provable Distinguisher for HFE. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 156–167. Springer, Heidelberg (2006)
9. 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)
10. Faugére, J.-C.: A New Efficient Algorithm for Computing Gröbner Bases (F4). Journal of Pure and Applied Algebra 139, 61–88 (1999)
11. Faugére, J.-C.: A New Efficient Algorithm for Computing Gröbner Bases without Reductions to Zero $F5$. In: ISSAC, pp. 75–83 (2002)
12. Faugére, J.-C.: Algebraic Cryptanalysis of HFE using Gröbner Bases. Technical Report 4738, INRIA (2003)
13. Kunz-Jacques, S.: Preuves de sécurité et problémes difficiles en cryptologie: étude de cas. PhD thesis, Université Paris 7 (2007)
14. 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)
15. 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)
16. 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)
17. Steel, A.: Allan Steel's Groebner Basis Timings Page (2004), `magma.maths.usyd.edu.au/users/allan/gb`
18. University of Sydney Computational Algebra Group. The MAGMA Computational Algebra System
19. Yang, B.-Y., Chen, J.-M.: All in the xl family: Theory and practice. In: Park, C., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2005)