# Inverting HFE Systems Is Quasi-Polynomial for All Fields

Jintai Ding[1,2] and Timothy J. Hodges[2]

[1] South China University of Technology, Guangzhou, China
[2] Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221-0025, USA
jintai.ding@gmail.com, timothy.hodges@uc.edu

**Abstract.** In this paper, we present and prove the first closed formula bounding the degree of regularity of an HFE system over an arbitrary finite field. Though these bounds are not necessarily optimal, they can be used to deduce

1. *if D, the degree of the corresponding HFE polynomial, and q, the size of the corresponding finite field, are fixed, inverting HFE system is polynomial for all fields;*
2. *if D is of the scale $O(n^\alpha)$ where n is the number of variables in an HFE system, and q is fixed, inverting HFE systems is quasi-polynomial for all fields.*

We generalize and prove rigorously similar results by Granboulan, Joux and Stern in the case when $q = 2$ that were communicated at Crypto 2006.

## 1 Introduction

The security of cryptosystems such as RSA, ECC, and Diffie-Hellman key exchange scheme, depends on assumptions about the hardness of certain number theory problems, such as the Integer Prime Factorization Problem or the Discrete Logarithm Problem. However, in 1994 Peter Shor [19] showed that quantum computers could break all public key cryptosystems that are based on these hard number theory problems. People realize that we need to look ahead to a possible future of quantum computers. In recent years significant effort has been put into the search for alternative public key cryptosystems, now called post-quantum cryptosystems, which would remain secure in an era of quantum computers. Multivariate public key cryptosystems (MPKC) [5] are one of the main families of cryptosystems that have the potential to resist quantum computer attacks.

An MPKC is a cryptosystem whose public key is given as a set of multivariate polynomials over a normally small finite field. The security of such systems is suggested by the fact that solving a system of multivariate polynomial equations over a finite field is in general NP-complete [11]. A quantum computer has not yet been shown to be efficient in solving this problem. Furthermore, computations in a finite field are more efficient than the manipulation of large integers

P. Rogaway (Ed.): CRYPTO 2011, LNCS 6841, pp. 724–742, 2011.

which is required by the systems based on hard number theory problems. Thus MPKC's can be less computationally intense than these systems and therefore have potential for application in small ubiquitous computing devices with limited resources.

Research into MPKC's started in the middle of 1980s in work of Diffie, Fell, Tsujii, Shamir. However the success of this work was limited and the real breakthrough in this direction was the cryptosystem proposed by Matsumoto and Imai [16]. Their scheme used a simple quadratic function on an extension field whose field structure was kept hidden. Unfortunately this efficient scheme was proved to be insecure by Patarin using his linearization equation attack [18]. Hidden Field Equation (HFE) cryptosystems are a family of cryptosystems proposed by Patarin based on the same fundamental idea of quadratic functions on extension fields [18].

Fixing a finite field $\mathbb{F}$ of characteristic 2 and cardinality $q$, Matsumoto and Imai suggested using a bijective map $P$ defined over $\mathbb{K}$, an extension field of degree $n$ over $\mathbb{F}$. By identifying $\mathbb{K}$ with $\mathbb{F}^n$, one sees that $P$ induces a multivariate polynomial map $\tilde{P}\colon \mathbb{F}^n \longrightarrow \mathbb{F}^n$. One can "hide" this map by composing on the left by $L_1$ and on the right by $L_2$, where the $L_i : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ are invertible affine maps. This composition gives a map $\bar{P} : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ defined by

$$\bar{P}\,(x_1, \ldots, x_n) = L_1 \circ \tilde{P} \circ L_2\,(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \quad .$$

For a Hidden Field Equation (HFE) system [18], $P$ is given as a univariate polynomial in the form:

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

where the coefficients are randomly chosen. Here the total degree $D$ of $P$ should not be too large since the decryption process involves solving the system of single variable polynomial equations given by $P(X) = Y'$ for a given $Y'$ using the Berlekamp-Massey algorithm.

Faugère and Joux showed that these systems can be broken rather easily in the case when $q = 2$ and $D$ is small [10] using the Gröbner basis algorithm $F_4$. Furthermore the experimental results suggested that such algorithms will finish at degree of order $\log_q(D)$ (by which we mean that the highest degree polynomials encountered are of degree of order $\log_q(D)$) and, therefore, that the complexity of the algorithm is $O(n^{\log_q(D)})$.

A key concept in the analysis of the complexity of these algorithms is that of *degree of regularity*. The degree of regularity of the component functions of $P$, $p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)$ is the lowest degree at which non-trivial polynomial relations between the $p_i$ occur (we also talk about this as the degree of regularity of $P$ or of the associated HFE system). Experimental evidence has shown that this is the point at which the algorithm will terminate. Here we mean by "*termination at a certain degree*", that the large matrices, whose entries are coefficients of multivariate polynomials, and on which the algorithm performs Gaussian eliminations, contain polynomials at most of the designated degree.

The largest size of all such matrices essentially determines the complexity of the algorithm. Bardet, Faugère and Salvy defined (in a different notation) the degree of regularity of random or generic systems and found an asymptotic formula for this degree. However since the systems arising from HFE polynomials were far from generic, the BFS bound does not yield useful information about the complexity of HFE systems. Granboulan, Joux and Stern [12] outlined a new way to bound the degree of regularity in the case $q = 2$. Their approach was to lift the problem back up to the extension field $\mathbb{K}$, an idea that originated in the work of Kipnis and Shamir [13] and Faugère and Joux [10]. They sketched that one can connect the degree of regularity of an HFE system to the degree of regularity of a lifted system over the big field. Assuming this assertion, the semi-regularity of a subsystem of the lifted system, and that the degree of regularity of a subsystem is greater than that of the original system, and using some asymptotic analysis of the degree of regularity of random systems found in [1], they derived heuristic asymptotic bounds for the case $q = 2$, which implied that if $D$ is chosen to be $O(n^\alpha)$ for $\alpha \geq 1$, then the complexity of Gröbner basis attacks is quasi-polynomial. While the results derived from this method match well with experimental results, the asymptotic bound formula has not yet been proven rigorously. It relies on a formula that holds for a class of overdetermined generic systems but it is not yet clear how to prove their systems belong to this class. Therefore to derive any definitive general bounds on the degree of regularity for general $q$ and $n$, or on the asymptotic behavior of the degree of regularity remained an open problem.

The security of HFE systems in the case when the characteristic of the field is odd has been the subject of much less study. The notions of degree of regularity and semi-regularity in [1] can be generalized to the case when $q$ is odd. However, the asymptotic analysis on which the results of [12] depend has not yet been generalized to this situation. The work in [8] seemed to suggest that HFE systems over a field of odd characteristic could resist the attack of Gröbner basis algorithms even when $D$ is small. When $q$ is large the field equations $X_1^q - X_2, \ldots, X_n^q - X_1$ cannot be used effectively and this limits the efficiency of the Gröbner basis algorithms. A breakthrough in the case of general $q$ came in the recent work of Dubois and Gama [9]. They first refined and gave a rigorous mathematical foundation for the arguments in [12]. They then derived a new method to compute the degree of regularity over any field similar to that in [1]. This led to an algorithm that can be used to calculate a bound for the degree of regularity for any choice of $q$, $n$ and $D$. However it is not clear how to derive a closed form for their bound from their algorithm and therefore they were not able to answer the question of whether the complexity was quasi-polynomial in this case.

**The contributions of this Paper.** In this article we answer the above questions by giving a global bound on the degree of regularity (in the sense of [9]) of an HFE system. We begin with a similar idea to that used in [12] - roughly that one can bound the degree of regularity of a system by finding a bound for certain simpler subsystems. However we obtain our bound using a very different

approach. Previously all estimates on the degree of regularity were based on a dimension counting argument. At some point the assumption that there are no trivial relations would imply that the space of linear combinations of the functions $p_1, \ldots, p_n$ by polynomials of degree $k$ would be greater than the dimension of the space of all polynomials of degree $k+2$. Dubois and Gama were able to improve on earlier bounds by observing that the subspace of linear combinations has to lie in a special subspace of the space of all polynomials of a fixed degree. Unfortunately the dimension of this space is given by a recursive formula which does not have a known closed form. In contrast our approach is to find explicit non-trivial relations. Surprisingly, it is enough to do this for the case of a single polynomial. Moreover, we can find an explicit formula for the degree in which these non-trivial relations occur. This gives the degree of regularity as an explicit function of $q$ and $D$ (it does not depend on $n$ unless the degree $D$ is a function of $n$). Such explicit formulas enable us to draw conclusions about the complexity of inverting the system using Gröbner basis methods. Our conclusions rely on no heuristic assumptions beyond the standard assumption that the Gröbner basis algorithms terminate at or shortly after the degree of regularity.

Specifically, we give a closed formula bound for the degree of regularity of a multivariate quadratic polynomial of the form

$$P(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c \ .$$

This bound depends on the rank of $P$ (in a sense defined below); since the restriction $q^i + q^j \leq D$ implies a strong restriction on the rank of $P$, we are able to deduce a sharp bound for the degree of regularity of $P$ over a field of any order $q$. When $q$ is odd, these bounds are comparable with those found computationally by Dubois and Gama when the block size $n \log_2(q)$ is less than 700. Interestingly this formula also yields the degree of regularity of the Matsumoto-Imai system when $q = 2$ to be 3. This is precisely the statement that Patarin's linearization attack works in this case. Thus we believe that the notion of rank is a key new ingredient in the analysis of multivariate quadratic cryptosystems.

A crucial step in our approach is to look at the single polynomial

$$P_0(X_1, ..., X_n) = \sum_{i,j} a_{ij} X_i X_j$$

considered as an element of the graded algebra $\mathbb{K}[X_1, \ldots, X_n]/(X_i^q)$. Using methods from [9], the degree of regularity of the whole system is bounded by the degree of regularity of this single polynomial. This problem was studied in detail by the authors and their collaborators in [6,7] in the cases $q = 2$ and 3. Drawing on the ideas from this work we are able to find explicit relations which give us bounds on the degree of regularity of $P_0$ for any $q$ (which we believe are sharp when $q$ is odd). Specifically we show that the degree of regularity of the system defined by $P$ is bounded by

$$\frac{\mathrm{Rank}(P_0)(q-1)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2$$

if $\text{Rank}(P_0) > 1$. Here $\text{Rank}(P_0)$ is the rank of the quadratic form associated to $P_0$. by It is important to note that these are universal bounds that require no assumption that the polynomials are of "generic type".

There are two very critical points in the formula. First, the degree of regularity depends only on the rank of $P_0$, not the degree of $P$; while the rank is bounded by $\log_q D + 1$, there are many situations (such as the Matsumoto-Imai operators or sparse HFE polynomials) where the rank is much smaller than can be predicted by looking at the degree; thus we believe that the rank of a HFE operator to be a more important invariant than its degree. Second, while we do not expect our formula to give sharp bounds, it yields similar results to those obtained in [9] for prime $q$. It also explains many of the jump discontinuities in their data, since jumps in the degree of regularity should be expected to occur when the degree reaches a value which allows the rank of $P$ to increase.

The formulas above enable us to draw the following conclusions about the complexity of inverting an HFE polynomial using a Gröbner basis algorithm.

1. If $D$, the degree of the corresponding HFE polynomial, and $q$, the size of the corresponding finite field, are fixed, then the degree of regularity is bounded by a fixed integer $(q-1)(\lfloor \log_q(D-1) \rfloor + 1)/2 + 2$ or $q$. Therefore inverting HFE systems is polynomial for all fields;
2. If $q$ is fixed and $D$ is of the scale $O(n^\alpha)$, then inverting HFE systems is quasi-polynomial.

If, on the other hand, $q$ is of the scale $O(n)$, then our results are inconclusive and the possibility remains that inverting HFE systems is actually exponential with respect to this parameter. Comparisons with the results of [9,12], suggest that our formulas asymptotically may be proportional to the degree of regularity at least for the case where $q$ is a prime.

This paper is organized as follows. We first briefly introduce HFE cryptosystems in the section below. In Section 3, we review the definition and basic properties of the degree of regularity from [9]. In Section 4, we show how the notion of rank can give a useful closed formula bound on the degree of regularity and apply this to the analysis of the complexity of the Gröbner basis attacks on HFE systems.

In the appendix, we develop the key ideas of [9] in a more abstract mathematical framework using the language of graded algebras. This allows us to create different but abstractly more transparent proofs for the main theorems that we use in the paper.

After the present paper was submitted, a paper by Bettale, Faugère and Perret [2] was published that has some commonality with ours. In this article, the authors come to similar conclusions on the security of the HFE systems, but with respect only to the Kipnis-Shamir attack. They conjecture that if $D$ is fixed the complexity of the Kipnis-Shamir attack is polynomial in $n$, the degree of the extension. Their experimental data backs up this conjecture.

## 2 HFE Systems

### 2.1 Quadratic Operators

Denote by $\mathbb{F}$ a finite field of order $q$ and let $\mathbb{K}$ be an extension of $\mathbb{F}$ of degree $n$. Any function from $\mathbb{K}$ to $\mathbb{K}$ can be expressed as a polynomial with coefficients in $\mathbb{K}$ and degree less than $q^n$. Thus it has the general form

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

There are two distinct notions of degree for $P$, the degree over $\mathbb{K}$ and the degree over $\mathbb{F}$. The degree over $\mathbb{K}$, denoted by $\deg_{\mathbb{K}}(P)$ is the degree in the usual sense of degree of a polynomial function. On the other hand, the functions $X^{q^i}$ are all linear over $\mathbb{F}$. Thus the degree of the monomial $X^d$ will be the sum of the digits in the base $q$ expansion of $d$; that is, if $d = \sum_i d_i q^i$, $\deg_{\mathbb{F}}(X^d) = \sum_i d_i$. When $q = 2$, this is the Hamming weight of the binary representation of $d$. The degree of $P$ over $\mathbb{F}$, denoted $\deg_{\mathbb{F}}(P)$ is the maximum of the degree of the monomial terms.

An $\mathbb{F}$-quadratic function from $\mathbb{K}$ to $\mathbb{K}$ is thus a polynomial all of whose monomial terms have exponent $q^i + q^j$ or $q^i$ for some $i$ and $j$. The general form of an $\mathbb{F}$-quadratic function is

$$P(X) = \sum_{i,j=0}^{n-1} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{n-1} b_i X^{q^i} + c \ .$$

### 2.2 HFE Systems

In an HFE cryptosystem, plaintext from $\mathbb{F}^n$ is encrypted using an identification of $\mathbb{F}^n$ with $\mathbb{K}$ and an $\mathbb{F}$-quadratic map $P$. The nature of $P$ is further hidden by pre- and post-composition with invertible affine linear maps $L_1, L_2 \colon \mathbb{F}^n \to \mathbb{F}^n$. Thus if $\phi \colon \mathbb{F}^n \to \mathbb{K}$ is the chosen linear isomorphism, the encryption is performed by the function $\bar{P} = L_1 \circ \phi^{-1} \circ P \circ \phi \circ L_2$. Decryption is performed by inverting the maps $L_1$ and $L_2$ and applying a standard root-finding algorithm for $P$. The public key is the function $\bar{P}$ expressed in terms of its quadratic component functions $\bar{p}_1, \ldots, \bar{p}_n \colon \mathbb{F}^n \to \mathbb{F}$. Provided the degree of $P$ is not too high the decryption process will be manageable. However the direct solution of a system of quadratic multivariate equations

$$\bar{p}_1 = b_1, \ldots, \bar{p}_n = b_n$$

is a hard problem which provides the system with a certain level of security.

### 2.3 Gröbner Basis Attacks

One of the most successful attacks on HFE systems is to apply the refined Gröbner basis algorithms $F_4$ (and maybe $F_5$ if we do know how to make it work

as efficiently as claimed) to convert the system of equations $\bar{p}_1 = b_1, \ldots, \bar{p}_n = b_n$ to a simpler system that can be solved quickly. From the point of view of security analysis it is sufficient to consider the system $p_1 = 0, \ldots, p_n = 0$ where the $p_i$ are the component functions of $\phi^{-1} \circ P \circ \phi$ with respect to the given basis. From this point on, we restrict our attention to this case.

Implementation of the Gröbner basis algorithm involves searching through combinations of multiples of the $p_i$ by polynomials of a fixed degree for polynomials of smaller degree. If the combination $\sum_i g_i p_i$ has smaller degree then the corresponding combination of leading components $\sum_i g_i^h p_i^h$ is zero. Here, by the leading component of a multivariate polynomial $g$ we mean the multivariate polynomial $g^h$ derived from removing all the monomial terms of $g$ with degree lower than the degree of $g$, or the highest homogeneous component of $g$. In general, the decisive moment in the calculation is when *non-trivial* such combinations occur. These non-trivial relations will very likely generate what is called mutants [3,4,15], which are instrumental in solving the system. Obviously the combinations $p_i^h p_j^h - p_j^h p_i^h$ are tautologically zero and the equation $((p_i^h)^{q-1} - 1)p_i^h = 0$ is a result of the identity $a^q = a$ in $\mathbb{F}$. A non-trivial relation is one that does not follow from these trivial identities. The degree at which the first non-trivial relation occurs is called the *degree of regularity*. Extensive experimental evidence has shown that the algorithm will terminate at or shortly after the degree of regularity. Thus the calculation of the degree of regularity is crucial to understanding the complexity of the algorithm.

## 3 Degree of Regularity

We begin with the formal definition of degree of regularity as given in [9] and we summarize the key results from that paper. More abstract versions of these results are also given in the appendix. Let

$$A = \mathbb{F}[X_1, \ldots, X_n] / \langle X_1^q - X_1, \ldots, X_n^q - X_n \rangle \ .$$

This is the algebra of functions from $\mathbb{F}^n$ to $\mathbb{F}$. Let $p_1, \ldots, p_n$ be quadratic elements of $A$. Denote by $A_k$ the subspace of $A$ consisting of functions representable by a polynomial of degree less than or equal to $k$. For all $j$ we have a natural map $\psi_j \colon A_j^n \to \sum_i A_j p_i$ given by

$$\psi_j(a_1, \ldots, a_n) = \sum_i a_i p_i \ .$$

We are interested in 'degree falls'; a degree fall occurs when the $a_i$ have degree $j$ but $\sum_i a_i p_i$ has degree less than degree $j+2$. Obviously we can have trivial degree falls of the form $p_j p_i + (-p_i)p_j$ or $(p_i^{q-1} - 1)p_i$. The *degree of regularity* of the set $\{p_1, \ldots, p_n\}$ is the first degree (measured as $\deg a_i + \deg p_i$) at which a non-trivial degree fall occurs. Obviously we can restrict our attention to the highest degree terms in the $a_i$ and work modulo terms of smaller degree. Mathematically this means working in the associated graded ring $B = \mathbb{F}[X_1, \ldots, X_n] / \langle X_1^q, \ldots, X_n^q \rangle$.

The degree of regularity of the $\{p_1, \ldots, p_n\}$ in $A$ will be the first degree at which we find non-trivial relations among the leading components $p_1^h, \ldots, p_n^h$ (considered as elements of $B$).

Denote by $B_k$ the subspace of $B$ consisting of homogeneous elements of degree $k$. Consider an arbitrary set of homogeneous quadratic elements $\{\lambda_1, \ldots, \lambda_n\} \in B_2$. For all $j$ we have a natural map $\psi_j \colon B_j^n \to B_{j+2}$ given by

$$\psi_j(b_1, \ldots, b_n) = \sum_i b_i \lambda_i \ .$$

Let $R_j(\lambda_1, \ldots, \lambda_n) = \ker \psi_j$; this is the subspace of relations of the form $\sum_i b_i \lambda_i = 0$. Inside $R_j(\lambda_1, \ldots, \lambda_n)$ is the subspace of trivial relations, $T_j(\lambda_1, \ldots, \lambda_n)$ generated by elements of the form:

1. $b(0, \ldots, 0, \lambda_j, 0, \ldots, 0, -\lambda_i, 0 \ldots, 0)$ for $1 \leq i < j \leq n$ and $b \in B_{j-2}$; where $\lambda_j$ is in the $i$-th position and $-\lambda_i$ is in the $j$-th position;
2. $b(0, \ldots, 0, \lambda_i^{q-1} - 1, 0 \ldots, 0)$ for $1 \leq i \leq n$ and $b \in B_{j-2(q-1)}$; where $\lambda_i^{q-1}$ is in the $i$-th position;

The space of non-trivial relations is the quotient space $R_j(\lambda_1, \ldots, \lambda_n)/T_j(\lambda_1, \ldots, \lambda_n)$.

**Definition 3.1.** *The* degree of regularity *of* $\{\lambda_1, \ldots, \lambda_n\}$ *is defined by*

$$D_{\mathrm{reg}}(\{\lambda_1, \ldots, \lambda_n\}) = \min\{j \mid R_{j-2}(\{\lambda_1, \ldots, \lambda_n\})/T_{j-2}(\{\lambda_1, \ldots, \lambda_n\}) \neq 0\}$$

It turns out that the degree of regularity is dependent only on the subspace generated by the $\lambda_i$ so we can simplify the notation a little by denoting the space generated by the $\lambda_i$ by $V$ and writing $D_{\mathrm{reg}}(V)$ for $D_{\mathrm{reg}}(\{\lambda_1, \ldots, \lambda_n\})$.

Two important properties of the degree of regularity were observed in [9]. First, the degree of regularity of a space is less than or equal to the degree of regularity of a subspace.

*Property 3.2.* [9, Property 11] Let $V'$ be a subspace of $V$. Then $D_{\mathrm{reg}}(V) \leq D_{\mathrm{reg}}(V')$.

Second, the degree of regularity is invariant under field extension. Let $\mathbb{K}$ be an extension of $\mathbb{F}$. Define $B_{\mathbb{K}} = \mathbb{K}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle$ and denote by $V_{\mathbb{K}}$ be the $\mathbb{K}$-subspace of $B_{\mathbb{K}}$ generated by the $\lambda_i$.

*Property 3.3.* [9, §4.4] Let $\mathbb{K}$ be an extension of $\mathbb{F}$. Then $D_{\mathrm{reg}}(V_{\mathbb{K}}) = D_{\mathrm{reg}}(V)$.

Returning to the situation where $P$ is a quadratic map with component functions $p_1, \ldots, p_n \in A$. Let $V$ and $V^h$ be the vector spaces generated by the $p_1, \ldots, p_n$ and their leading components $p_1^h, \ldots, p_n^h$ (considered as elements of $B$). Our goal is to find a bound for $D_{\mathrm{reg}}(V^h)$. We begin by extending the base field to $\mathbb{K}$. When we extend the base field in $A$, we pass from functions from $\mathbb{F}^n$ to $\mathbb{F}$ to functions from $\mathbb{F}^n$ to $\mathbb{K}$. Via the linear isomorphism $\phi^{-1} \colon \mathbb{K} \to \mathbb{F}^n$, this algebra is isomorphic to the algebra of functions from $\mathbb{K}$ to $\mathbb{K}$ which is simply $\mathbb{K}[X]/\langle X^{q^n} - X \rangle$.

It follows from elementary Galois theory that the space $V_{\mathbb{K}}$ corresponds under this identification with the space generated by $P, P^q, \ldots, P^{q^{n-1}}$. If we filter the algebra $\mathbb{K}[X]/\left\langle X^{q^n} - X \right\rangle$ by degree of functions over $\mathbb{F}$, then the linear component is spanned by $X, X^q, \ldots, X^{q^{n-1}}$. The associated graded ring will then be the algebra $B_{\mathbb{K}} = \mathbb{K}[X_0, \ldots, X_{n-1}]$ where $X_i$ corresponds to $X^{q^i}$ and $X_i^q = 0$. This is naturally isomorphic to the algebra $B$ with coefficients extended to $\mathbb{K}$ (proofs in Appendix B). Thus the processes of extending the base field and taking the associated graded ring commute.

Let $P_i$ denote the leading component of $P^{q^i}$ in $B_{\mathbb{K}}$. Thus for instance if $P$ is defined as above, then

$$P_0 = \sum_{i,j=0}^{n-1} a_{ij} X_i X_j \ .$$

The space generated by the $P_i$ is exactly $V_{\mathbb{K}}^h$, the subspace of $B_{\mathbb{K}}$ generated by the $p_i^h$. Putting all the above together we get the following important theorem. A brief proof is given in Appendix B.

**Theorem 3.4 ([9])**

$$D_{\text{reg}}(\{p_1, \ldots, p_n\}) = D_{\text{reg}}(\{p_1^h, \ldots, p_n^h\}) = D_{\text{reg}}(\{P_0, \ldots, P_{n-1}\})$$

Using Property 2, we get the following immediate corollary.

**Corollary 3.5.** $D_{\text{reg}}(\{p_1, \ldots, p_n\}) \leq \min\{D_{\text{reg}}(Q) \mid Q \in V_{\mathbb{K}}^h\}$

## 4 Bounding the Degree of Regularity Using Q-Rank

Up to this point we have been following the ideas of [12,9]. In particular, the proofs of all the above results are given in [9], which is the basis for this work. We now, however, take a significant change of direction. The bounds on the degree of regularity in [12,9] and previous authors are all found by counting dimensions. The basic idea going back to [21,1] is that if $\dim B_j^n - \dim T_j > \dim B_j^{n+2}$, then $R_j \supsetneq T_j$ and the degree of regularity has been reached. This approach was refined in [12] by using Property 1 to reduce to subsets $\{P_0, \ldots, P_s\}$ which, for HFE systems, involve significantly fewer variables. It was further refined in [9] where the authors observed that the space on the right hand side of the inequality could be replaced by a significantly smaller space, allowing a more accurate computational estimate of the degree of regularity. The disadvantage of the approach in [9] was that no general formula for the degree of regularity could be derived.

Our approach is completely different. Instead of counting and comparing dimensions we actually find non-trivial relations in specific dimensions. Surprisingly, an important bound can be found by restricting to the case of a single polynomial. We begin by giving a bound on the degree of regularity of a single polynomial in terms of its rank. Applying this formula to $P_0$ yields a bound on the degree of regularity of an HFE system in terms of its degree.

The degree of regularity of a single polynomial has been studied in great detail in the cases where $q = 2$ and 3 [6,7]. In order to obtain the desired bound, we do not need the kind of exact information found in those papers. We merely need to demonstrate the existence of non-trivial relations. This we can do explicitly using the classification of quadratic forms. Recall that $P_0$ is a homogeneous quadratic polynomial in the algebra $\mathbb{K}[X_0, \ldots, X_{n-1}]/\left\langle X_0^q, \ldots, X_{n-1}^q \right\rangle$. Using the classification theorem of quadratic forms over finite fields, we are able to explicitly construct nontrivial relations and hence derive a simple bound for the degree of regularity of $P_0$ in terms of its rank.

We now briefly review the classification of quadratic forms over a finite field. We begin with the case when $q$ is odd. A quadratic form in $n$ indeterminates is a homogeneous quadratic polynomial in the polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$. Two forms $P$ and $Q$ are said to be equivalent (written $P \sim Q$) if there is an invertible linear change of variables $L$ which transforms $P$ into $Q$:

$$P \circ L(X_1, ..., X_n) = Q(X_1, ..., X_n).$$

Pick an element $c \in \mathbb{K}$ that is not a square. Then a quadratic form is equivalent to one of the two types

1. $X_1^2 + \cdots + X_{r-1}^2 + X_r^2$
2. $X_1^2 + \cdots + X_{r-1}^2 + cX_r^2$

for some $r \leq n$ [17, §62]. The same classification applies to quadratic elements of the quotient ring $\mathbb{K}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle$.

When $q$ is even, the situation is complicated by the fact that $X^2$ is linear rather than quadratic when $q = 2$. It is shown in [14, Theorem 6.30] that a quadratic polynomial in the polynomial algebra $\mathbb{K}[X_1, \ldots, X_n]$ is equivalent to an polynomial of one of the following forms for some $r \leq n$:

1. $X_1X_2 + ... + X_{r-1}X_r$
2. $X_1X_2 + ... + X_{r-2}X_{r-1} + X_r^2$
3. $X_1X_2 + ... + X_{r-1}X_r + X_{r-1}^2 + cX_r^2$ where $c \in \mathbb{K}\backslash\{0\}$ satisfies $\mathrm{TR}_{\mathbb{K}}(c) = 1$.

For $q > 2$ this classification carries over to the quotient ring $\mathbb{K}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle$. When $q = 2$, all quadratic elements of the quotient ring are equivalent to an element of the first type. In all cases the number $r$ is known as the rank of $Q$. Note that if $q = 2$, the rank of a quadratic element must be at least 2.

When $r = 1$ (in which case $q > 2$), $Q$ is actually equal to $aX_1^2$ for some $a \in \mathbb{K}$. It is easily verified that the smallest non-trivial relation is $X^{q-2}(aX^2) = 0$ and hence that $D_{\mathrm{reg}}(Q) = q$. More generally we have the following inequality.

**Theorem 4.1.** *Let $Q$ be quadratic of rank $r$. If $r > 1$,*

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

*Proof.* In the case of a single polynomial, the definition of degree of regularity can be expressed in terms of non-trivial annihilators. Let $Q$ be an arbitrary quadratic element of $B = \mathbb{K}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle$. The annihilators of $Q$ are the elements of $\mathrm{Ann}(Q) = \{f \in B \mid fQ = 0\}$. The trivial annihilators are the multiples of $Q^{q-1}$. The degree of regularity is the first $k$ such that there is a non-trivial annihilator of $Q$ of degree $k-2$. The degree of regularity is invariant under a linear change of variables, so it is sufficient to prove the result by exhibiting explicit non-trivial annihilators for each of the above types of quadratic elements.

Because of the different types of standard forms we need to consider separately the cases when $q$ is odd and even. We also need to divide these cases into the cases when $r$ is odd or even.

– Case 1: $q$ odd, $r$ even

Set $s = r/2$. In this case $Q$ is of the form

$$Q = X_1^2 + X_2^2 + \cdots + X_{2s-1}^2 + aX_{2s}^2$$

for some $a \in \mathbb{K}$. Let

$$K_i = X_{2i-1}^{q-1} - X_{2i}^2 X_{2i-1}^{q-3} + X_{2i}^4 X_{2i-1}^{q-5} + \cdots + (-1)^{(q-1)/2} X_{2i}^{q-1}$$

for $i = 1, \ldots, s-1$; and

$$K_i = X_{2s-1}^{q-1} - aX_{2s}^2 X_{2s-1}^{q-3} + a^2 X_{2s}^4 X_{2s-1}^{q-5} + \cdots + (-a)^{(q-1)/2} X_{2s}^{q-1}$$

Set

$$K = K_1 K_2 \ldots K_s \ .$$

It is clear that

$$K_i(X_{2i-1}^2 + X_{2i}^2) = X_{2i-1}^{q+1} - (-1)^{(q+1)/2} X_{2i}^{q+1} = 0 \ ,$$

for $i = 1, ..., s-1$; and

$$K_s(X_{2s-1}^2 + aX_{2s}^2) = X_{2s-1}^{q+1} - (-a)^{(q+1)/2} X_{2s}^{q+1} = 0 \ .$$

Hence $KQ = 0$. Thus $K \in \mathrm{Ann}(Q) \cap B_{s(q-1)}$. We claim that $K \notin \langle Q^{q-1} \rangle$. Consider the quotient algebra

$$\bar{B} = B/\left\langle X_{2i-1}^2 + X_{2i}^2, i = 1, ..., s-1;\ X_{2s-1}^2 + aX_{2s}^2 \right\rangle \ .$$

The algebra $\bar{B}$ has a basis consisting of monomials with the powers of the variables $X_2, X_4, \ldots, X_{2s}$ at most 1. It is clear that the image of $Q$ (and hence also $Q^{q-1}$) in $\bar{B}$ is zero, whereas the image of $K$ is

$$\prod_i^s X_{2i-1}^{q-1} \left(\frac{q+1}{2}\right)^s$$

which is non-zero. Therefore $K$ is not in the ideal generated by $Q^{q-1}$. Hence $D_{\mathrm{reg}}(Q) \leq r(q-1)/2 + 2$.

– Case 2: $q$ odd, $r$ odd

Set $s = (r-1)/2$. In this case $Q$ is of the form

$$Q = X_1^2 + X_2^2 + \cdots + X_{2s-1}^2 + X_{2s}^2 + aX_{2s+1}^2$$

for some $a \in \mathbb{K}$. From the classification of quadratic forms [20] we have

$$X_{2s-1}^2 + X_{2s}^2 + aX_{2s+1}^2 \sim X_{2s-1}^2 - X_{2s}^2 - aX_{2s+1}^2 \sim X_{2s-1}X_{2s} - aX_{2s+1}^2$$

so $Q$ can be taken to be of the form:

$$Q = X_1^2 + X_2^2 + \cdots + X_{2s-2}^2 + X_{2s-1}X_{2s} - aX_{2s+1}^2 \ .$$

Let

$$K_i = X_{2i-1}^{q-1} - X_{2i}^2 X_{2i-1}^{q-3} + X_{2i}^4 X_{2i-1}^{q-5} + \cdots + (-1)^{(q-1)/2} X_{2i}^{q-1}$$

for $i = 1, \ldots, s-1$; and

$$K' = \frac{(X_{2s-1}X_{2s})^{(q+1)/2} - a^{(q+1)/2} X_{2s+1}^{(q+1)}}{X_{2s-1}X_{2s} - aX_{2s+1}^2} X_{2s-1}^{(q-1)/2} \ .$$

Note that

$$K'(X_{2s-1}X_{2s} - aX_{2s+1}^2) = (X_{2s-1}X_{2s})^{(q+1)/2} X_{2s-1}^{(q-1)/2} = 0 \ .$$

Set

$$K = K_1 K_2 \ldots K_{s-1} K'.$$

Note that the degree of $K$ is $(s-1)(q-1) + 3(q-1)/2 = r(q-1)/2$. Again we see that $KQ = 0$ and so $K \in \mathrm{Ann}(Q) \cap B_{r(q-1)/2}$. Consider the quotient algebra

$$\bar{B} = B/\left\langle X_{2i-1}^2 + X_{2i}^2, i = 1, ..., s-1;\ X_{2s-1}X_{2s} - aX_{2s+1}^2 \right\rangle \ ,$$

Then $\bar{B}$ has a basis consists of monomials in which the powers of the variables $X_2, X_4, \ldots, X_{2(s-1)}, X_{2s+1}$ are at most one. The image of $Q$ in $\bar{B}$ is zero, but that of $K$ is

$$\prod_{i=1}^{s-1} X_{2i-1}^{q-1} \left(\frac{q+1}{2}\right)^{s-1} X_{2s-1}^{q-1} X_{2s}^{(q-1)/2} \left(\frac{q+1}{2}\right)$$

which is non-zero. Hence $K$ is not in the ideal generated by $Q^{q-1}$ and $D_{\mathrm{reg}}(Q) \leq r(q-1)/2 + 2$.

– Case 3: $q$ even, $r$ even (Q of type (1) or (3))

First suppose that $Q$ is of the form $Q = X_1X_2 + \cdots + X_{2s-1}X_{2s}$ where $r = 2s$. Set $H = X_1^{q-1} X_3^{q-1} \ldots X_{2s-1}^{q-1}$. Then it is easily seen that $H \in \mathrm{Ann}(Q) \cap B_{s(q-1)}$. Consider the quotient algebra

$$\bar{B} = B/\left\langle X_1 - X_2, \ldots, X_{2s-1} - X_{2s} \right\rangle \ .$$

The image of $Q$ in $\bar{B}$ is

$$\bar{Q} = X_1^2 + X_3^2 + \cdots + X_{2s-1}^2 = (X_1 + X_3 + \cdots + X_{2n-1})^2$$

so the image of $Q^{q-1}$ is $\bar{Q}^{q-1} = 0$. On the other hand the image of $H$ is

$$X_1^{q-1} X_3^{q-1} \ldots X_{2s-1}^{q-1}$$

which is non-zero. Thus $H \notin \langle Q^{q-1} \rangle$ Hence $D_{\text{reg}}(Q) \leq r(q-1)/2 + 2$.

Next suppose that $Q$ is of the form $Q = X_1X_2 + \cdots + X_{2s-1}X_{2s} + X_{2s-1}^2 + \alpha X_{2s}^2$. Let $\mathbb{L}$ be a finite extension field of $\mathbb{K}$ in which the equation $1 + X + aX^2$ has a root. In $\mathbb{L}[X_1, \ldots, X_r]$, $Q$ is equivalent to $X_1X_2 + \cdots + X_{2s-1}X_{2s}$. Since the degree of regularity is invariant under extensions of the base field by Property 2, it follows from the first part that $D_{\text{reg}}(Q) \leq r(q-1)/2 + 2$.

– Case 4: $q$ even, $r$ odd (Q of type (2))

Note that in this case we must have $q > 2$. We may assume that $Q$ is of the form $Q = X_1X_2 + \cdots + X_{2s-1}X_{2s} + X_{2s+1}^2$ where $r = 2s + 1$. Set

$$H = X_1^{q-1} X_3^{q-1} \ldots X_{2s-3}^{q-1} X_{2s-1}^{q/2} (X_{2s-1}X_{2s} + X_{2s+1}^2)^{(q-2)/2} \ .$$

Note that $\deg H = r(q-2)/2$ and

$$HQ = (X_{2s-1}X_{2s} + X_{2s+1}^2)^{q/2} X_{2s-1}^{q/2} = X_{2s-1}^q X_{2s}^{q/2} + X_{2s+1}^q X_{2s-1}^{q/2} = 0 \ .$$

Consider the quotient algebra

$$\bar{B} = B/\langle X_1 - X_2, \ldots, X_{2s-1} - X_{2s} \rangle \ .$$

The image of $Q$ in $\bar{B}$ is $\bar{Q} = X_1^2 + X_3^2 + \cdots + X_{2s-1}^2 + X_{2s+1}^2 = (X_1 + X_3 + \cdots + X_{2s-1} + X_{2s+1})^2$ so the image of $Q^{q-1}$ is $\bar{Q}^{q-1} = 0$. On the other hand the image of $H$ is $X_1^{q-1} X_3^{q-1} \ldots X_{2s-3}^{q-1} X_{2s-1}^{q/2} (X_{2s-1}^2 + X_{2s+1}^2)^{(q-2)/2}$ which is non-zero. Thus $H \notin \langle Q^{q-1} \rangle$ Hence $D_{\text{reg}}(Q) \leq r(q-1)/2 + 2$.

Note that for $q$ odd, these bounds were conjectured to be optimal in [7]. Experimental evidence suggests that this is not the case when $q$ is even.

Let us define the Q-Rank of a quadratic operator $P(X)$ to be the minimal rank of elements of the space $V_{\mathbb{K}}^h$ generated by $P_0, \ldots, P_{n-1}$.

$$\text{Q-Rank}\, P = \min\{\text{Rank}\, Q \mid Q \in V_{\mathbb{K}}^h\}$$

Note in particular that $\text{Q-Rank}(P) \leq \text{Rank}(P_0)$.

**Theorem 4.2.** *Let $P$ be a quadratic operator of degree $D$. If* $\text{Q-Rank}(P) > 1$, *the degree of regularity of the associated system is bounded by*

$$\frac{(q-1)\,\text{Q-Rank}(P)}{2} + 2 \ .$$

*In particular, this is less than or equal to*

$$\frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2 \ .$$

*If* $\text{Q-Rank}(P) = 1$, *then the degree of regularity is less than or equal to $q$.*

*Proof.* The first assertion follows from Theorem 4.1 and Corollary 3.5. Suppose that

$$P(X) = \sum_{q^i+q^j \le D} a_{ij} X^{q^i+q^j} + \sum_{q^i \le D} b_i X^{q^i} + c \ .$$

Then

$$P_0 = \sum_{q^i+q^j \le D} a_{ij} X_i X_j \ .$$

Let $k$ be the largest subscript of a variable $X_k$ that occurs non-trivially in $P_0$ (that is, $a_{ik} \neq 0$ for some $i$). The rank of $P_0$ is bounded by the number of variables involved in its expression which is at most $k+1$. On the other hand, by our assumption on $D$, $D \geq q^k + 1$ or equivalently, $k \leq \lfloor \log_q(D-1) \rfloor$. Thus the rank of $P_0$ is at most $\lfloor \log_q(D-1) \rfloor + 1$.

*Example 4.3.* Consider a Matsumoto-Imai operator of the form $P(X) = X^{1+2^\theta}$ over the field $GF(2)$. Then $P_0 = X_0 X_\theta$ has rank 2. So our theorem implies that the degree of regularity is less than or equal to three. This is precisely the statement that linearization equations exist in this case [18]. On the other hand if we consider a Matsumoto-Imai operator over a field of order $q = 2^m$, then the degree of regularity remains 3 but our bound is $2^m + 1$. Therefore our estimate formula needs to be improved when $q$ is not a prime.

For fixed $q$ the degree of regularity is $O(\log_q D)$. Consider now a Gröbner basis attack on an HFE system of degree $D$. We continue to make the assumption that these algorithms will terminate at degree equal to the degree of regularity or shortly after this. The runtime of this algorithm will be $O(n^{3D_{\text{reg}}})$. Assuming that the security parameter is chosen in such a way that $D = O(n^\alpha)$, the runtime for the Gröbner basis attack on an HFE system over any base field will be $2^{O(\log(n)^2)}$; that is, it will be quasi-polynomial.

On the other hand, suppose that $q$ itself is a component of the security parameter and is taken to be of scale $O(n)$ (this assumption is reasonable since it will only increase the computation complexity for HFE systems by the scale of $O(\log_2 n)$). If the bound above is asymptotically sharp then the degree of regularity will be at least of the scale $O(n)$, and therefore inverting HFE systems will be exponential.

We do not expect or believe the bound obtained in Theorem 4.2 to be optimal in any degree of generality. We compare the bound $(q-1)(\lfloor \log_q(D-1) \rfloor + 1)/2 + 2$ with that obtained by Dubois and Gama for a large number of values of $n$ and $D$ and prime $q$ from [9]. The tables Appendix C give a detailed comparison of our bound with the bound calculated in [9]. As $n$ becomes large relative to $q$, the two bounds appear to be getting closer, though ours are frequently slightly higher. It seems possible that there may be a tighter upper bound of the form $cq \log_q(D)$ for some scalar $c$ when $q$ is a prime. The discontinuities in the Dubois-Gama data are close to the discontinuities of $\lfloor \log_q(D-1) \rfloor$ and the jump size seems proportional to $q$.

## 5 Conclusion

By finding explicit non-trivial relations, we prove that the degree of regularity of a multivariate quadratic cryptosystem over a field of arbitrary characteristic $q$ is bounded above by a simple linear function of its Q-Rank and $q$. These universal estimate formulas for the degree of regularity for HFE systems for all finite fields allow us to show that if the degree $D$ of the HFE formula is fixed and the number of variables increased, the complexity of a Gröbner basis attack on this system will grow as a polynomial function in $n$; if, on the other hand, the degree of the HFE polynomial is $O(n^{\alpha})$, then the algorithm will take quasi-polynomial time, as was observed in the case $q = 2$ in [12].

Our bounds on the degree of regularity are not likely to be optimal even for large $n$ - we look for relations involving a single polynomial rather than the whole polynomial systems to prove our estimates. We expect in general that there will be some non-trivial relations resulting from relations between polynomials in subsystems, which have smaller degree than relations coming from single polynomials. On the other hand there is a surprising similarity between our bounds and those found by Dubois and Gama using a very different approach. Of course, it is possible that neither bound is close to being optimal and it would be interesting to run experimental trials for large values of $n$, $D$ and $q$. However, memory limitations prevent us from being able to do this at sufficiently large values. Taking all this into account, we conjecture that our formulas should give a good asymptotic estimate (up to a linear factor) of the degree of regularity in the case $q$ when is prime. If this is true, this would imply that inverting an HFE system with $q$ of size $O(n)$ is actually exponential.

**Acknowledgments.** J. Ding would like to thank V. Dubois and N. Gama for sending him their paper [9] before its publication and for sending him their data and their program to compute the estimated bound of the degree of regularity in terms of their formulation. J. Ding would like to thank V. Dubois for many stimulating and insightful discussions, without which this paper will not be possible. J. Ding would like to thank C. Christensen and J. Buchmann for useful discussions. J. Ding would also like to thank many years' crucial support of the **Charles Phelps Taft Foundation** and the support of the **National Science Foundation of China** under the grant #60973131.

## References

1. Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: International Conference on Polynomial System Solving - ICPSS, pp. 71–75 (November 2004)
2. 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)
3. Ding, J.: Mutants and its impact on polynomial solving strategies and algorithms. Privately distributed research note, University of Cincinnati and Technical University of Darmstadt (2006)

4. Ding, J., Buchmann, J., Mohamed, M., Mohamed, W., Weinmann, R.-P.: Mutant XL. In: First International Conference on Symbolic Computation and Cryptography – SCC (2008)
5. Ding, J., Gower, J., Schmidt, D.: Multivariate Public Key Cryptography. Advances in Information Security series. Springer, Heidelberg (2006)
6. Ding, J., Hodges, T.J., Kruglov, V.: Growth of the ideal generated by a quadratic boolean function. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS, vol. 6061, pp. 13–27. Springer, Heidelberg (2010)
7. Ding, J., Hodges, T.J., Kruglov, V., Schmidt, D., Tohaneanu, S.: Growth of the ideal generated by a multivariate quadratic function over GF(3), preprint
8. 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)
9. 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)
10. 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)
11. Garey, M.R., Johnson, D.S.: Computers and intractability, A Guide to the theory of NP-completeness. W.H. Freeman, San Francisco (1979)
12. 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)
13. 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)
14. Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
15. Mohamed, M., Cabarcas, D., Ding, J., Buchmann, J., Bulygin, S.: $\mathrm{MXL}_3$: An Efficient Algorithm for Computing Gröbner Bases of Zero-Dimensional Ideals. In: Lee, D., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 87–100. Springer, Heidelberg (2010)
16. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
17. O'Meara, O.T.: Introduction to Quadratic Forms. Springer, Berlin (1963)
18. 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)
19. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 41(2), 303–332 (1999)
20. Wan, Z.-X.: Lectures on Finite Fields and Galois Rings. World Scientific Publishing, Singapore (2003)
21. 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)

## A Degree of Regularity

Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q$. Denote by $B = \bigoplus_{k=0}^{N} B_k$ a graded finite dimensional algebra over $\mathbb{F}$. Let $V \subset B_d$ be a homogeneous subspace. Then for

all $j$ we have a natural map $\phi_j : B_j \otimes V \to B_j V$ given by $\phi(\sum b_i \otimes v_i) = \sum b_i v_i$. Let $R_j(V) = \ker \phi_j$. Inside $R_j(V)$ there is a subspace of "trivial relations" $T_j(V)$ spanned by the elements

1. $b(v \otimes w - w \otimes v)$ where $v, w \in V$ and $b \in B_{j-d}$;
2. $b(v^{q-1} \otimes v)$ where $v \in V$ and $b \in B_{j-(q-1)d}$.

A similar basis-dependent definition of trivial relations was give in [9]. It can be shown that these two definitions coincide.

Following Dubois and Gama [9], we define the degree of regularity of $V$ to be the degree of the first space $B_j V$ in which non-trivial relations occur.

**Definition A.1.** *For a homogeneous subspace $V \subset B_d$, the* degree of regularity *of $V$ is defined to be*

$$D_{\mathrm{reg}}(V) = \min\{j \mid T_{j-d}(V) \subsetneq R_{j-d}(V)\}$$

Let $A$ be a filtered algebra over $\mathbb{F}$ and let $\mathrm{Gr}A = \bigoplus_j A_j/A_{j+1}$. Let $V$ be a subspace of $A_j$. We denote by $\bar{V}$ its image in $\mathrm{Gr}A$; that is, $\bar{V} = V + A_{j-1} \subset A_j/A_{j-1}$.

**Definition A.2.** *For a subspace $V \subset A_d$, we define the* degree of regularity *of $V$ by*

$$D_{\mathrm{reg}}(V) = \begin{cases} d & \text{if} \quad \dim \bar{V} < \dim V \\ D_{\mathrm{reg}}(\bar{V}) & \text{otherwise} \end{cases}$$

Extension of the base field does not affect the degree of regularity.

**Theorem A.3.** *Let $B$ be a graded algebra over $\mathbb{F}$, let $\mathbb{K}$ be an extension field of $\mathbb{F}$ and let $\tilde{B} = \mathbb{K} \otimes_{\mathbb{F}} B$. Let $\tilde{V} = \mathbb{K} \otimes V \subset \tilde{B}$. Then $D_{\mathrm{reg}}(V) = D_{\mathrm{reg}}(\tilde{V})$.*

Secondly, the degree of regularity of a subspace is at least that of the original space.

**Theorem A.4.** *Let $B$ be a graded algebra. Let $V$ be a homogeneous subspace and let $V'$ be a subspace of $V$. Then $D_{\mathrm{reg}}(V) \leq D_{\mathrm{reg}}(V')$.*

## B Quadratic Operators

Let $\mathbb{K}$ be an extension of $\mathbb{F}$ of degree $n$; hence $|\mathbb{K}| = q^n$. An $\mathbb{F}$-quadratic function $P\colon \mathbb{K} \to \mathbb{K}$ takes the form

$$P(X) = \sum_{i,j} a_{ij} X^{q^i} X^{q^j} + \sum_i b_i X^{q^i} + c$$

for some $a_{ij}, b_i, c \in \mathbb{K}$.

Fix a dual basis $\{e_i \in \mathbb{K}, x_i \in \mathbb{K}^* = Hom_{\mathbb{F}}(\mathbb{K}, \mathbb{F})\}$ for $\mathbb{K}$ over $\mathbb{F}$. Define

$$A = \mathrm{Fun}(\mathbb{K}, \mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]$$

Note that $x_i^q = x_i$ and $A$ is naturally isomorphic to $\mathbb{F}[T_1, \ldots, T_n]/(T_1^q - T_1, \ldots, T_n^q - T_n)$. Note also that $\dim_{\mathbb{F}} A = q^n$ and a basis for $A$ is given by all monomials of the form

$$x_1^{i_1} \ldots x_n^{i_n}, \quad \text{where } 0 \le i_j \le q-1.$$

Analogously we have that

$$\tilde{A} = \mathrm{Fun}(\mathbb{K}, \mathbb{K}) = \mathbb{K}[X]$$

where $X^{q^n} = X$. It can be easily verified that

$$\tilde{A} \cong \mathbb{K} \otimes_{\mathbb{F}} A = \mathbb{K}[x_1, \ldots, x_n]$$

This isomorphism identifies $X$ with the element $\sum_i e_i x_i$.

We can filter both of these algebra by degree over $\mathbb{F}$. Thus for $A$ we define

$$A_0 = \mathbb{F}, \quad A_1 = \sum_i \mathbb{F} x_i + \mathbb{F}, \quad A_{i+1} = A_1 A_i$$

For $\tilde{A}$ we note that the maps $X^{q^i}$ are $\mathbb{F}$-linear and that they span the $\mathbb{K}$-space of $\mathbb{F}$-linear maps from $\mathbb{K}$ to $\mathbb{K}$. Thus we define

$$\tilde{A}_0 = \mathbb{K}, \quad \tilde{A}_1 = \sum_i \mathbb{K} X^{q^i} + \mathbb{K}, \quad \tilde{A}_{i+1} = \tilde{A}_1 \tilde{A}_i$$

Recall from basic Galois theory that $\sum_i \mathbb{K} X^{q^i} = \sum_i \mathbb{K} x_i$. From this it follows easily that $\tilde{A}_i \cong \mathbb{K} \otimes_{\mathbb{F}} A_i$ and that

$$\tilde{B} = \mathrm{Gr}\tilde{A} \cong \mathbb{K} \otimes_{\mathbb{F}} \mathrm{Gr} A = \mathbb{K} \otimes_{\mathbb{F}} B.$$

Define $\bar{X}_i = X^{q^i} + \tilde{A}_0 \in \tilde{B}_1$ and $\bar{x}_i = x_i + A_0 \in B_1$. Note that $\bar{X}^q = 0$ and $\bar{x}^q = 0$ for all $i$. Note also that $\bar{X}_i = \sum_i e_i^{q^i} \bar{x}_i$ and that $\tilde{B}_1 = \sum \mathbb{K} \bar{x}_i$. Hence

$$\tilde{B} = \mathbb{K}[\bar{X}_1, \ldots, \bar{X}_n] = \mathbb{K}[\bar{x}_1, \ldots, \bar{x}_n].$$

Now consider a quadratic operator $P$. Let $p_i = x_i \circ P$ and let $V = \sum \mathbb{F} p_i$.

**Theorem B.1.** $\sum \mathbb{K} p_i = \sum \mathbb{K} P^{q^i}$.

*Proof.* Note that

$$\begin{aligned} \sum \mathbb{K} p_i &= \{L \circ P \mid L \in \sum \mathbb{K} x_i\} \\ &= \{L \circ P \mid L \in \sum \mathbb{K} X^{q^i}\} \\ &= \sum \mathbb{K} P^{q^i} \end{aligned}$$

since $X^{q^i} \circ P = P^{q^i}$.

Let $\bar{P}_i$ be the image of $P^{q^i}$ in $\tilde{B}$; that is, $\bar{P}_i = P^{q^i} + \tilde{A}_1$ .

**Corollary B.2.** $\sum \mathbb{K} \bar{p}_i = \sum \mathbb{K} \bar{P}_i$.

*Proof.*

$$\sum \mathbb{K} \bar{p}_i = \sum \mathbb{K}(p_i + A_1) = \sum \mathbb{K} p_i + \tilde{A}_1 = \sum \mathbb{K}(P^{q^i} + \tilde{A}_1) = \sum \mathbb{K} \bar{P}_i.$$

## C Comparison with Dubois-Gama Bounds

The following tables give a detailed comparison of our bound with the bound calculated in [9].

In these tables, the symbol $\mathcal{D}$ stands for the bound on the degree of the HFE polynomial used in [9]. Rather than restrict by the total degree $D$ of the HFE operator, their restriction is given by

$$P(X) = \sum_{i,j \le \mathcal{D}} a_{ij} X^{q^i+q^j} + \sum_{q^i \le D} b_i X^{q^i} + c \ .$$

Thus $\mathcal{D}$ is one less than the number of variables involved in the polynomial $P_0$ and so Q-Rank $\le \mathcal{D}+1$. In the same row as $\mathcal{D}$, DG Dreg stands for the bound on the degree of regularity given in [9], and DH Dreg stands for the bound obtained from Theorem 4.2 using $\mathcal{D}+1$ in place of Q-Rank. Thus DH Dreg $= (q-1)(\mathcal{D}+1)/2+2$.

The authors would like to thank Vivien Dubois and Nicolas Gama for providing the detailed data that made this comparison possible.

**Table 1.** Comparison with Dubois-Gama bound

| | $q=3$ | | | $q=5$ | | | $q=7$ | | | $q=11$ | | | $q=13$ | | | $q=17$ | | | $q=19$ | | | $q=23$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | | | $D_{\text{reg}}$ | |
| $n$ | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH | $\mathcal{D}$ | DG | DH |
| 8 | 3 | 5 | 6 | 2 | 6 | 8 | 2 | 6 | 11 | 2 | 6 | 17 | 2 | 6 | 20 | 2 | 6 | 26 | 2 | 6 | 29 | 2 | 6 | 35 |
| 12 | 3 | 5 | 6 | 3 | 7 | 10 | 2 | 7 | 11 | 2 | 7 | 17 | 2 | 7 | 20 | 2 | 7 | 26 | 2 | 7 | 29 | 2 | 7 | 35 |
| 16 | 3 | 6 | 6 | 3 | 9 | 10 | 2 | 9 | 11 | 2 | 9 | 17 | 2 | 9 | 20 | 2 | 9 | 26 | 2 | 9 | 29 | 2 | 9 | 35 |
| 20 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 12 | 14 | 2 | 11 | 17 | 2 | 11 | 20 | 2 | 11 | 26 | 2 | 11 | 29 | 2 | 11 | 35 |
| 24 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 13 | 14 | 2 | 13 | 17 | 2 | 13 | 20 | 2 | 13 | 26 | 2 | 13 | 29 | 2 | 13 | 35 |
| 28 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 14 | 14 | 2 | 14 | 17 | 2 | 14 | 20 | 2 | 14 | 26 | 2 | 14 | 29 | 2 | 14 | 35 |
| 32 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 14 | 14 | 2 | 16 | 17 | 2 | 16 | 20 | 2 | 16 | 26 | 2 | 16 | 29 | 2 | 16 | 35 |
| 36 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 14 | 14 | 3 | 21 | 22 | 2 | 18 | 20 | 2 | 18 | 26 | 2 | 18 | 29 | 2 | 18 | 35 |
| 40 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 14 | 14 | 3 | 22 | 22 | 2 | 20 | 20 | 2 | 20 | 26 | 2 | 20 | 29 | 2 | 20 | 35 |
| 44 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 14 | 14 | 3 | 22 | 22 | 2 | 21 | 20 | 2 | 21 | 26 | 2 | 21 | 29 | 2 | 21 | 35 |
| 48 | 4 | 7 | 7 | 3 | 10 | 10 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 23 | 26 | 2 | 23 | 29 | 2 | 23 | 35 |
| 52 | 5 | 8 | 8 | 3 | 10 | 10 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 24 | 26 | 2 | 25 | 29 | 2 | 25 | 35 |
| 56 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 24 | 26 | 2 | 25 | 29 | 2 | 25 | 35 |
| 60 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 24 | 26 | 2 | 25 | 29 | 2 | 25 | 35 |
| 64 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 24 | 26 | 2 | 25 | 29 | 2 | 25 | 35 |
| 68 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 24 | 26 | 2 | 25 | 29 | 2 | 25 | 35 |
| 72 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 2 | 24 | 26 | 2 | 25 | 29 | 2 | 25 | 35 |
| 76 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 2 | 25 | 29 | 2 | 25 | 35 |
| 80 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 2 | 25 | 29 | 2 | 25 | 35 |
| 84 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 2 | 25 | 29 | 2 | 25 | 35 |
| 88 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 92 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 96 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 100 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 104 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 108 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 112 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 116 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 120 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 2 | 25 | 35 |
| 124 | 5 | 8 | 8 | 4 | 12 | 12 | 3 | 14 | 14 | 3 | 22 | 22 | 3 | 25 | 26 | 3 | 32 | 34 | 3 | 36 | 38 | 3 | 42 | 46 |