INVERTING SQUARE SYSTEMS ALGEBRAICALLY IS EXPONENTIAL

JINTAI DING

Abstract. In this paper, we prove that the degree of regularity of the family of Square systems, an HFE type of systems, over a prime finite field of odd characteristics q is exactly q, and therefore prove that

- inverting Square systems algebraically is exponential, when $q = O(n)$, where n is the number of variables of the system.

1. Introduction

In 1994 Peter Shor [21] showed that quantum computers could break all public key cryptosystems based on these hard number theory problems. Recently significant efforts have been put into the search for alternative public key cryptosystems, post-quantum cryptosystems, which would remain secure in an era of quantum computers. Multivariate public key cryptosystems (MPKC)[7] are one of the main families of cryptosystems that have the potential to resist quantum computer attacks.

Research into MPKC's started in the middle of 1980s in the works of Diffie, Fell, Tsujii, Shamir. However the success of this work was limited and the real breakthrough was the cryptosystem proposed by Matsumoto and Imai [19], which however was broken by Patarin [20]. The 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 [20].

Fixing a finite field $\mathbb{F}$ of characteristic 2 and cardinality q, they suggested using an almost bijective map P defined over $\mathbb{K}$, an extension field of degree n over $\mathbb{F}$. By identifying $\mathbb{K}$ with $\mathbb{F}^n$, P induces a multivariate polynomial map $P' \colon \mathbb{F}^n \longrightarrow \mathbb{F}^n$. One then "hides" 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

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

For the Hidden Field Equations (HFE) [20], P is given as a univariate polynomial in the form:

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

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 single variable polynomial equation given by $P(X) = Y'$ for a given Y' using 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 [13] using the Gröbner basis algorithm F_4. Furthermore the experimental results suggested that such algorithms will finish at degree of order $O(\log_q(D))$, where the highest degree polynomials we deal with are of the degree of order $O(\log_q(D))$, and, therefore that the complexity of the algorithm is $n^{O(\log_q(D))}$. *Even though, the authors did not say it explicitly, the claims seem to imply such a statement is valid for any q even or odd, and therefore one can break any HFE cryptosystems with small D or asymptotically for any fixed D,* which we will disprove in this paper.

Key words and phrases. Square, HFE, degree of regularity.

A key concept in the complexity analysis of these algorithms is that of *degree of regularity*. The degree of regularity of the component functions of P, $p_1(x_1,\dots,x_n),\dots,p_n(x_1,\dots,x_n)$ is the lowest degree at which non-trivial polynomial relations between the p_i occur. Experiments show that this is the degree at which the algorithm will terminate and therefore determines the complexity. Bardet, Faugère and Salvy defined (in a different interpretation) the degree of regularity of random or generic systems and gave an asymptotic estimate 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 solving HFE systems algebraically, which is based on counting of dimensions of spaces with linear independence assumptions. Granboulan, Joux and Stern 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 [16] and Faugère and Joux [13]. They **sketched** that one can connect the degree of regularity of the 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 [2], 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 over-determined 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 [2] can be generalized to the case when q is odd. However, the asymptotic analysis on which the results of [15] depend, has not yet been generalized to this situation. The work in [11] 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. Their rational is that when q is large the field equations $X_1^q - X_2, ..., X_n^q - X_1$ cannot be used effectively and this limits the efficiency of the Gröbner basis algorithms, because one actually tries to solve the equations over the algebraic closure of the finite field. A breakthrough in case of general q came in the recent work of Dubois and Gama [12]. They first refined and gave a rigorous mathematical foundation for the arguments in [15]. They then derived a new method to compute the degree of regularity over any field similar to that in [2]. 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.

Inspired by the work of [12], and using a similar idea to that used in [15] - roughly that one can bound the degree of regularity of a system by finding a bound for certain simpler subsystems, in [8], a new closed formula was found for the degree regularities for all HFE systems for any field. However this bound is derived using a very different approach. Previously all estimates on the degree of regularity were based on a dimension counting argument, while the new approach constructively proves the upper bound of the degree of regularity as an explicit function of q and D. Such explicit formulas enable [8] to draw conclusions about the upper bound complexity of inverting the system using Gröbner basis methods.

1.1. The contribution of this paper.

In the paper[8], a very strong conjecture was presented on the lower bound of the degree of regularity for the case of that q is odd and q is the size of $\Omega(n)$, which implies that to invert the related systems algebraically is actually exponential.

Follows the same mathematical approach, we actually prove in this paper that in the case of the Square system, which was proposed in [3], namely, when the HFE system is given by:

$$P(X) = X^2,$$

the degree of regularity is exactly q for odd prime q.

This theorem therefore allow us to draw the following conclusions about the complexity of inverting an Square polynomial using a Gröbner basis algorithm.

Inverting Square systems algebraically is exponential, when $q = \Omega(n)$, where n is the number of variables of the system.

This proves the conjecture in [8], though it does not answer the question about the cases other than Square systems. However the common senses tells us that the conjecture is very likely to be true for all generic HFE cases, since Square systems are the simplest among all.

As far as we know, our work is the first to give a lower bound for degree of regularity for HFE cryptosystems and therefore show a lower bound for the complexity of the related algebraic attacks. Clearly from the point view of cryptography, this result could have profound impact in many related areas, in particular, in understanding the complexity of algebraic attacks and in designing new cryptosystems.

The results of this paper strongly suggest, as speculated in [11] that using odd characteristics is indeed a very good idea to resist algebraic attacks, and therefore confirms the idea that we should move to filed of odd characteristics. Also this works points the possibility to provide certain provablely secure property for MPKCs. Indirectly, this work also points to new directions in terms of algebraic immunity for function that should be used in symmetric cryptosystems.

Here, we would also like to point out that Square scheme itself is broken[1]*, but with a totally different method than algebraic attacks. Algebraic attacks were considered as the most powerful tool in attack the HFE systems before due to its effectiveness in breaking the HFE Challenge 1. The result of this paper, however, shows that algebraic attacks is not something we should worry too much about in general for the HFE family once we use odd characteristics q and $q = \Omega(n)$.*

This paper is organized as follows. We will first introduce briefly HFE and Square cryptosystems in the section below. In Section 3, we review the definition and basic properties of the degree of regularity from [12][8]. In Section 4, we will prove and main theorem that degree of regularity of Square systems is indeed q and derive that the complexity of the Gröbner basis attacks on Square systems is indeed exponential.

2. Square systems

2.1. **HFE systems and Square systems.**

In this paper, the cases we will study are that q is an odd prime number, which also implies that $q > 2$.

Let $\mathbb{F}$ be a finite field of order q and $\mathbb{K}$ an degree n extension of $\mathbb{F}$.

Any map P from $\mathbb{K}$ to $\mathbb{K}$ can be expressed **uniquely** as a polynomial function with coefficients in $\mathbb{K}$ and degree less than q^n, namely

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

The degree of $P(X)$ is the highest degree of the monomial above with non-zero coefficients.

There is an standard map ϕ, which identifies $\mathbb{K}$ as $\mathbb{F}^n$:

$$\mathbb{F}^n \overset{\phi}{\to} \mathbb{K},$$

$$\mathbb{K} \overset{\phi^{-1}}{\to} \mathbb{F}^n.$$

Then we can build a new map

$$P'(x_0, .., x_{n-1}) = (p_0(x_0, .., x_{n-1}), ..., p_{n-1}(x_0, .., x_{n-1})) = \phi^{-1} \circ P \circ \phi(x_0, .., x_{n-1}),$$

which is essentially P but viewed from the perspective of $\mathbb{F}^n$.

In this case, again each component $p_i(x_0, ..., x_{n-1})$ can be expressed **uniquely** as a polynomial of the variables x_i such that the highest power of $x_i (i = 0, ..., n-1)$ is not more than q, which is due to the fact that $x_i^q = x_i$ over $\mathbb{F}$. Then the degree of the map P' is the highest degree of all the p_i' components.

In some way, we can say that these are two different way of defining the 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 of $P(X)$.The degree of P over $\mathbb{F}$, denoted $\deg_{\mathbb{F}}(P)$ is the degree of P'. For example, the functions X^{q^i} are all linear viewed from the point of $\mathbb{F}^n$. Thus

$$\deg_{\mathbb{F}}(P) = 1.$$

The degree of the monomial X^d will be the sum of the digits in the base q expansion of d. The degree of P over $\mathbb{F}$, denoted $\deg_{\mathbb{F}}(P)$ is the same as the maximum of the Hamming weight of the degree of the monomial terms of $P(X)$.

An $\mathbb{F}$-degree 2 or $\mathbb{F}$-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

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

The function $P(X)$ with a fixed low $\mathbb{K}$ degree is used to build the HFE multivariate public key cryptosystems and originally the q is selected as 2, which is very different from what considered here, namely q is an odd primes.

The simplest form of an $\mathbb{F}$-quadratic function is

$$P(X) = X^2,$$

which is what we will study in this paper. Surely if $q = 2$, this map is of actually degree one over $\mathbb{F}$ as explained above.

In a Square HFE-type of system, just like an HFE system itself, we build a system $\bar{P}$ from an $\mathbb{F}$-quadratic map P, where the nature of P is further hidden by pre- and post-composition with invertible affine linear maps $L_1, L_2 \colon \mathbb{F}^n \to \mathbb{F}^n$:

$$\bar{P} = L_1 \circ P' \circ L_2.$$

2.2. Algebraic solvers – Gröbner basis attacks.

The question we will address here is how difficult it is to find directly the solution of a system of quadratic multivariate equations

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

The most successful attacks on HFE systems is to apply the improved Gröbner basis algorithms F_4 and F_5 to solve the system $\bar{p}_1 = b_1, \dots, \bar{p}_n = b_n$.

Without loss of generality, and due to the fact that what L_1 does is an transformation of deriving a set of new polynomials from linear combination of the old ones and what L_2 does is nothing but a change of basis of the variables of the polynomials, and those transformations do not change the degree of regularity of the systems, therefore we only need to consider the case $p_1 = 0, \dots, p_n = 0$ where the p_i are the component functions of $P' = \phi \circ P \circ \phi^{-1}$.

A key component of the Gröbner basis algorithm involves searching through combinations of multiples of the p_i by polynomials of a fixed degree for new polynomials of lower degree that this fixed degree. If the combination $\sum_i g_i p_i$ has smaller degree then the corresponding combination of leading terms $\sum_i g_i^h p_i^h$ is zero. The key moment in the calculation is when *non-trivial* such combinations occur. These non-trivial relations will very likely generate what is called mutant [6, 18, 18], 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

$$((p_i^h)^{q-1}-1)p_i=0$$

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 (see details in Section 3 below). 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, in particular, for the case of HFE. The algorithm will never finish before dealing with polynomials at 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 will present the definition of degree of regularity as defined in [12] and and the main results in [12][8]. Let

$${}_nA=\mathbb{F}[x_1,\dots,x_n]/\left\langle x_1^q-x_1,\dots,x_n^q-x_n\right\rangle.$$

This is the algebra of functions over $\mathbb{F}^n$. Let $p_1,\dots,p_n$ be a set of quadratic polynomials in ${}_nA$. Denote by ${}_nA_k$ the subspace of ${}_nA$ consisting of functions representable by a polynomial of degree less than or equal to k.

For all j we have a natural map $\psi_j\colon {}_nA_j{}^n\to{}_nA_{j+2}$ given by

$$\psi_j(a_1,\dots,a_n)=\sum_i a_ip_i,$$

where

$${}_nA_j{}^n={}_nA_j\times{}_nA_j\times\ldots\times{}_nA_j.$$

The key here is the non-trivial "degree falls"; a degree fall occurs when the a_i have degree j but $\sum_i a_ip_i$ has degree less than degree $j+2$. Obviously we can have trivial degree falls of the form

$$p_jp_i+(-p_i)p_j=0$$

or

$$(p_i^{q-1}-1)p_i=0.$$

The *degree of regularity* of the set $\{p_1,\dots,p_n\}$ is the first degree at which such a degree fall occurs. Obviously we can restrict our attention to the highest degree terms in the polynomials, namely the highest degree homogeneous components of the polynomials. Mathematically this means working in the associated graded ring

$${}_n\mathcal{B}=\mathbb{F}[x_1,\dots,x_n]/\left\langle x_1^q,\dots,x_n^q\right\rangle.$$

The degree of regularity of the $\{p_1,\dots,p_n\}$ in ${}_nA$ will be the first degree at which we find non-trivial relations among the leading component $p_1^h,\dots,p_n^h$ (considered as elements of ${}_n\mathcal{B}$). By leading component, we mean the highest degree homogeneous component of a multivariate polynomial.

Denote by ${}_n\mathcal{B}_k$ the subspace of ${}_n\mathcal{B}$ consisting of homogeneous elements of degree k. Consider an arbitrary set of homogeneous quadratic elements $\{\lambda_1,\dots,\lambda_n\}\in\mathcal{B}_2$, which are linear independent. For all j we have a natural map $\psi_j\colon{}_n\mathcal{B}_j^n\to{}_n\mathcal{B}_{j+2}$ given by

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

where

$${}_n\mathcal{B}_j^n={}_n\mathcal{B}_j\times{}_n\mathcal{B}_j\times\ldots\times{}_n\mathcal{B}_j,$$

the direct product of n copies of ${}_n\mathcal{B}_j$.

Let ${}_nR_j(\lambda_1,\ldots,\lambda_n)=\ker\phi_j$; this is the subspace of relations of the form:

$$\sum_i b_i\lambda_i=0.$$

The key here is that ${}_nR(\lambda_1,\ldots,\lambda_n)=\cup_j {}_nR_j(\lambda_1,\ldots,\lambda_n)$ as usual is also a module of the ring ${}_nB$, where each elements of ${}_nB$ acts on the module by multiplying to each component of elements in ${}_n\mathcal{B}$:

$$a(b_1,...,b_n)=(ab_1,...,ab_n),$$

where $a\in {}_n\mathcal{B}$ and $(b_1,...,b_n)\in {}_nR$. Inside ${}_nR_j(\lambda_1,\ldots,\lambda_n)$,${}_nZ_j(\lambda_1,\ldots,\lambda_n)$ is the subspace of trivial relations, which is a submodule generated by elements of the form:

(1) $b(0,\ldots,0,\lambda_j,\ldots,0-\lambda_i,0\ldots,0)$ for $1\leq i<j\leq n$ where $b\in {}_n\mathcal{B}_{j-2}$; λ_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 $b\in {}_n\mathcal{B}_{j-2(q-1)}$; where λ_i^{q-1} is in the i-th position;

The space of non-trivial relations is the quotient space ${}_nR_j(\lambda_1,\ldots,\lambda_n)/{}_nZ_j(\lambda_1,\ldots,\lambda_n)$.

Following standard definition, we have

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

$$D_{\text{reg}}(\{\lambda_1,\ldots,\lambda_n\})=\min\{j\mid {}_nZ_{j-2}(\{\lambda_1,\ldots,\lambda_n\})\subsetneq {}_nR_{j-2}(\{\lambda_1,\ldots,\lambda_n\})\}$$

The degree of regularity is dependent only on the subspace generated by the λ_i assuming that the linear independence of λ_i, so we can simplify the notation a little by denoting the space generated by the λ_i by V and writing $D_{\text{reg}}(V)$ for $D_{\text{reg}}(\{\lambda_1,\ldots,\lambda_n\})$.

There are two important properties of the degree of regularity were observed in [12].

Property 1. Let V' be a subspace of V. Then $D_{\text{reg}}(V)\leq D_{\text{reg}}(V')$.

Property 2. Let $\mathbb{K}$ be an extension of $\mathbb{F}$. Then $D_{\text{reg}}(V_{\mathbb{K}})=D_{\text{reg}}(V)$.

Here $V_{\mathbb{K}}$ corresponding to the space of polynomials spanned by elements in V but over the extension field $\mathbb{K}$ as the base field.

The second property tells us that the degree of regularity is invariant under field extension.

Define $B_{\mathbb{K}}=\mathbb{K}[x_1,\ldots,x_n]$ and let $V_{\mathbb{K}}$ be the $\mathbb{K}$-vector space generated by the λ_i. If we look at the situation where P be a quadratic map with component functions $p_1,\ldots,p_n\in A$ from it associated map P'. Let V and V^h be the vector spaces generated by the $p_1,\ldots,p_n$ and their leading component, namely the component of all their respective quadratic terms: $p_1^h,\ldots,p_n^h$. Our goal is to find a bound for $D_{\text{reg}}V^h$. We begin by extending the base field to $\mathbb{K}$. When we extend the base field in ${}_nA$, we pass from functions from $\mathbb{F}^n$ to $\mathbb{F}$ to functions from $\mathbb{F}^n$ to $\mathbb{K}$:

$$\mathbb{F}^n\overset{p_i}{\to}\mathbb{F}\overset{emdedding}{\to}\mathbb{K}.$$

Then via the linear isomorphism $\phi^{-1}\colon\mathbb{K}\to\mathbb{F}^n$, we can show that this algebra is isomorphic to the algebra of functions from $\mathbb{K}$ to $\mathbb{K}$ which is simply $\mathbb{K}[X]/\left\langle X^{q^n}-X\right\rangle$[8].

From elementary Galois theory [8] we know that the space $V_{\mathbb{K}}$ corresponds under this identification with the space generated by $P,P^q,\ldots,P^{q^{n-1}}$.

Further more, 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 $X,X^q,\ldots,X^{q^{n-1}}$. We then can show easily [8] that the associated graded ring will then be the algebra ${}_nB_{\mathbb{K}}=\mathbb{K}[X_0,\ldots,X_{n-1}]$ where X_i corresponds to X^{q^i} and $X_i^q=0$. This is naturally isomorphic to the algebra ${}_n\mathcal{B}_{\mathbb{K}}$ with coefficients extended to $\mathbb{K}$: ${}_n\mathcal{B}_{\mathbb{K}}={}_n\mathcal{B}\otimes_{\mathbb{F}}\mathbb{K}$.

We will denote this new ring as:

$${}_nB_{\mathbb{K}}=\mathbb{K}[X_1,\ldots,X_n]/\left\langle X_1^q,\ldots,X_n^q\right\rangle.$$

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

$$P_i = X_i^2.$$

The space generated by the P_i is exactly $V_{\mathbb{K}}^h$, the subspace of ${}_nB_{\mathbb{K}}$ generated by the p_i^h, which is the highest degree homogeneous component of p_i. Putting all the above together we get the following important theorem.

Theorem 3.2. [12] $D_{reg}(\{p_1, \dots, p_n\}) = D_{reg}(\{p_1^h, \dots, p_n^h\}) = D_{reg}(\{P_0, \dots, P_{n-1}\})$

In [8], inspired the work by [12], for the first time, there is a rigorous proof for the following much expected important theorem:

Theorem 3.3. *Let P be a quadratic operator of degree D. If* Q-Rank$(P) > 1$*, the degree of regularity of the associated system is bounded by*

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

where Q-Rank(P) *of a quadratic operator $P(X)$ is the minimal rank of all quadratic forms spanned by $V_{\mathbb{K}}^h$ generated by $P_0, \dots, P_{n-1}$. If* Q-Rank$(P) = 1$*, then the degree of regularity is less than or equal to q.*

It is clear that this theorem gives an **upper bound** of the degree of regularity, and with some reasonable assumptions on the termination conditions, this gives us the upper bound of the complexity ot break the related HFE systems algebraically. But to ensure the security of the systems from algebraic attacks, what we actually need is a lower bound, which is what we are going to prove in the next section for Square systems.

4. The Degree of regularity of Square systems

To prove the main theorems, we will first present some basic results on ${}_nB$.

Lemma 4.1. *In*

$${}_nB = \mathbb{K}[X_0, \dots, X_{n-1}] / \langle X_1^q, \dots, X_n^q \rangle ,$$

the monomials

$$\prod_i^{n-1} X_i^{a_i}, \quad a_i < q, \quad \sum_i^n a_i = k,$$

are linearly independent and form a basis of ${}_nB_k$.

This follows from definition.

Lemma 4.2. *There is a natural ring embedding of ${}_nB$ into ${}_{n+1}B$, which we denote as E_n, where*

$$E_n(X_i) = X_i,$$

for i=0,...,n-1.

The proof also follows from definition and the lemma above.

Lemma 4.3. *${}_{n+1}B$ is a direct sum of two subspaces:*

$${}_{n+1}B = {}_nB^* \oplus C_{n+1},$$

where

$${}_nB^* = E_n({}_nB),$$

which is the image space of ${}_nB$ in ${}_{n+1}B$ under E_n; and

$${}_{n+1}C = \{\textit{The space spanned by monmials, which must include a nonzero power of } X_n \textit{ in } {}_{n+1}B\}.$$

We call this lemma the inductive decomposition lemma.

This is a very natural decomposition of the ring namely into the sum a space contains monomials of variable $X_0, .., X_{n-1}$, which is ${}_nB^*$, and the space of monomials involving X_n, which is ${}_{n+1}C$.

This lemma can be easily proved by showing that the following ring homomorphism sequence is exact:

$$0 \to C_{n+1} \overset{I_n}{\to} {}_{n+1}B \overset{P_n}{\to} {}_nB \to 0,$$

where I_n is a ring embedding, P_n is a ring homomorphism such that

$$P_n(X_i) = X_i, i = 0, ..., n-1; \quad P_n(X_n) = 0,$$

and

$$P_n \circ E_n = Id,$$

where Id stands for identity map on ${}_nB$.

Theorem 4.4. *Let $f_i(X_0, ..., X_{n-1}), i = 0, .., n-1$ be elements in ${}_nB_j, j < q-2$, if*

$$\phi_j(f_0(X_0, ..., X_{n-1}), ..., f_{n-1}(X_0, ..., X_{n-1})) = \sum f_i(X_0, ..., X_{n-1})X_i^2 = 0,$$

then

$$F = (f_0(X_0, ..., X_{n-1}), ..., f_{n-1}(X_0, ..., X_{n-1}))$$

belongs to

$${}_nZ_j(X_0^2, \dots, X_{n-1}^2),$$

the subpage of degree j elements in the space of trivial syzygies.

We prove this by induction on n.

First, it is straightforward that when $n = 1$, the claim is true,since

$$X_0^2 \times f(X_0) = 0,$$

implies that

$$f(X_0) = X_0^{q-2}F'(x_0).$$

Now, let us **assume** that the statement is true for **the case** n, we will try to show **the case** $n+1$ is also true.

Assume that $j < q-2$ and

$$\phi_j(f_0(X_0, ..., X_n, X_n), ..., f_n(X_0, ..., X_n)) = \sum_1^n f_i(X_0, ..., X_n)X_i^2 = 0,$$

where $f_i(X_0, ..., X_n)$ are homogeneous of degree j.

Then we will rewrite for each $i < n$:

$$f_i(X_0, ..., X_n) = f_i^*(X_0, ..., X_n) + X_n f'(X_0, ..., X_n),$$

which follows from decomposition lemma above and

$$f_i^*(X_0, ..., X_n) = E_n \circ P_n(f_i(X_0, ..., X_n)).$$

Then we have that

$$\sum_0^n f_i(X_0, ..., X_{n-1})X_i^2 = \sum_0^{n-1} f *_i (X_0, ..., X_{n-1})X_i^2 + X_n \sum_0^{n-1} X_i^2 f_i'(X_0, ..., X_n) + X_n^2 f_n(X_0, ..., X_n) = 0,$$

where

$$\sum_1^{n-1} f *_i (X_0, ..., X_{n-1})X_i^2 = E_n \circ P_n(\sum_1^n f_i(X_0, ..., X_{n-1})X_i^2).$$

Due to the Inductive Decomposition lemma, this implies that

$$\sum_0^{n-1} f_i^*(X_0, ..., X_{n-1})X_i^2 = 0,$$

and

$$X_n \sum_1^{n-1} X_i^2 f_i'(X_0, ..., X_n) + X_n^2 f_n(X_0, ..., X_n) = 0,$$

Due to the induction assumption, we know that

$$(f_0^*(X_0, ..., X_{n-1}), ..., f_{n-1}^*(X_0, ..., X_{n-1})) \in {}_nZ_j(X_0^2, \dots, X_{n-1}^2)$$

and therefore we have **(I)**:

$$(f_0^*(X_0, ..., X_{n-1}), ..., f_{n-1}^*(X_0, ..., X_{n-1}), 0) \in {}_{n+1}Z_j(X_0^2, \dots, X_{n-1}^2, X_n^2).$$

Follow further decomposition by using the Inductive Decomposition lemma, we have that

$$\begin{array}{c} X_n \sum_1^{n-1} X_i^2 f_i'(X_0, ..., X_n) + X_n^2 f_n(X_0, ..., X_n) \\ = X_n(\sum_1^{n-1} X_i^2(f_i^{'*}(X_0, ..., X_{n-1}) + X_n f_i''(X_0, ..., X_n)) \\ +X_n^2 f_n(X_0, ..., X_n) = 0, \end{array}$$

where

$$f_i^{'*}(X_0, ..., X_{n-1}) = E_n \circ P_n(f_i'(X_0, ..., X_n)).$$

This induces that

$$X_n(\sum_1^{n-1} X_i^2(f_i^{'*}(X_0, ..., X_{n-1}) + X_n^2(\sum_1^{n-1} X_i^2 f_i''(X_0, ..., X_n) + f_n(X_0, ..., X_n)) = 0.$$

Then from the first lemma in this section, we know that

$$X_n(\sum_1^{n-1} X_i^2(f_i^{'*}(X_0, ..., X_{n-1})) = 0$$

and

$$X_n^2(\sum_1^{n-1} X_i^2 f_i''(X_0, ..., X_n) + f_n(X_0, ..., X_n)) = 0.$$

$$X_n(\sum_1^{n-1} X_i^2(f' *_i (X_0, ..., X_{n-1})) = 0$$

implies that

$$(\sum_1^{n-1} X_i^2(f' *_i (X_0, ..., X_{n-1})) = 0$$

following from the first lemma in this section.

Since the degree of $f' *_i (X_0, ..., X_{n-1})$ for $i < n$ is $j - 1 < q - 2$, following from induction assumption, therefore we have

$$(f_0^{'*}(X_0, ..., X_{n-1}), ..., f_{n-1}^{'*}(X_0, ..., X_{n-1})) \in {}_nZ_{j-1}(X_0^2, \dots, X_{n-1}^2)$$

and therefore we have **(II)**

$$(f_0^{'*}(X_0, ..., X_{n-1}), ..., f_{n-1}^{'*}(X_0, ..., X_{n-1}), 0) \in {}_{n+1}Z_{j-1}(X_0^2, \ldots, X_{n-1}^2, X_n^2),$$

and therefore we have **(II)**:

$$(X_n f_0^{'*}(X_0, .., X_{n-1}), .., X_n f^{'*} *_{n-1} (X_0, .., X_{n-1}), 0) \in {}_{n+1}Z_j(X_0^2, \ldots, X_{n-1}^2, X_n^2).$$

Then again following from the first lemma in this section and the fact that the annihilator of X_n^2 is generated by X_n^{q-2}, we have that

$$X_n^2(\sum_1^{n-1} X_i^2 f_i''(X_0, ..., X_n) + f_n(X_0, ..., X_n)) = 0,$$

imples

$$\sum_1^{n-1} f_i'' X_i^2(X_0, ..., X_n) + f_n(X_0, ..., X_n) = 0,$$

and therefore

$$f_n(X_0, ..., X_n) = -\sum_1^{n-1} X_i^2 f_i''(X_0, ..., X_n).$$

This means that

$$\begin{gathered}
(X_n^2 f_0''(X_0, ..., X_n), ..., X_n^2 f_{n-1}''(X_0, ..., X_n), f_n(X_0, ..., X_n)) \\
= (X_n^2 f_0''(X_0, ..., X_n), ..., X_n^2 f_0''(X_0, ..., X_n), -\textstyle\sum_1^{n-1} X_i^2 f_i''(X_0, ..., X_n)) \\
= (X_n^2 f_0''(X_0, ..., X_n), 0, ..., 0, -X_0^2 f_0''(X_0, ..., X_n)) + \\
(0, X_n^2 f_1''(X_0, ..., X_n), 0, ..., 0, -X_1^2 f_1''(X_0, ..., X_n)) + ... + \\
(0, .., 0, X_n^2 f_{n-1}''(X_0, ..., X_n), -X_{n-1}^2 f_1''(X_0, ..., X_n)) \\
= f_0''(X_0, ..., X_n)(X_n^2, 0, ..., 0, -X_0^2) + \\
f_1''(X_0, ..., X_n)(0, X_n^2, 0, ..., 0 - X_1^2) + ... + \\
f_{n-1}''1(X_0, ..., X_n)(0, .., X_n^2, -X_{n-1}^2).
\end{gathered}$$

This means that **(III)**:

$$(X_n^2 f_0''(X_0, .., X_n), .., X_n^2 f_{n-1}''(X_0, .., X_n), f_n(X_0, .., X_n) \in {}_{n+1}Z_j(X_0^2, \ldots, X_{n-1}^2, X_n^2).$$

Since

$$\begin{gathered}
(f_0(X_0, ..., X_{n-1}, X_n), ..., f_n(X_0, ..., X_n)) \\
= (f_0^*(X_0, ..., X_{n-1}), ..., f_{n-1}^*(X_0, ..., X_{n-1}), 0) + \\
(X_n f_0^{'*}(X_0, ..., X_{n-1}), ..., X_n f_{n-1}^{'*}(X_0, ..., X_{n-1}), 0) + \\
(X_n^2 f_0''(X_0, ..., X_n), ..., X_n^2 f_{n-1}''(X_0, ..., X_n), f_n(X_0, ..., X_n)),
\end{gathered}$$

with (I), (II), (III), we have that

$$(f_0(X_0, ..., X_n, X_n), ..., f_n(X_0, ..., X_n)) \in {}_{n+1}Z_j(X_0^2, \ldots, X_{n-1}^2, X_n^2).$$

This gives us the proof for our theorem.

Lemma 4.5. $(X_0^{q-2}, 0..., 0)$ *does not belong to* $Z_{q-2}(X_0^2, \ldots, X_{n-1}^2, X_n^2)$.

This surely follows from the main theorem above ffrom [8]
But, we give a different but direct proof also by induction.
It is obvious that for n=1, the case is true since $Z_{q-2}(X_0^2, \dots, X_{n-1}^2, X_n^2)$. contains only the zero element.
Assume our claims is true for the case n, we now proceed to prove the case for $n+1$.
Assume that $(X_0^{q-2}, 0..., 0)$ does belong to $Z_{q-2}(X_0^2, \dots, X_{n-1}^2, X_n^2)$, since $2(q-1) > q-2$ then we have

$$(X_0^{q-2}, 0..., 0) = \sum_{i<j}^{n} f_{ij}(X_0, ..., X_n)(0, .., X_i^2, 0, ..., 0, -X_j^2, 0, ..., 0).$$

Then we have

$$\begin{gathered} E_n \circ P_n(X_0^{q-2}, 0..., 0) = (X_0^{q-2}, 0..., 0) \\ = E_n \circ P_n(\textstyle\sum_{i<j}^{n} f_{ij}(X_0, ..., X_n)(0, .., X_j^2, 0, ..., 0, -X_i^2, 0, ..., 0)) = \\ (\textstyle\sum_{i<j}^{n-1} f_{ij}^*(X_0, ..., X_{n-1})(0, .., X_j^2, 0, ..., 0, -X_i^2, 0, ..., 0)) + \\ (\textstyle\sum_{i<n}^{n-1} f_{i,n}^*(X_0, ..., X_{n-1})(0, .., 0, ..., 0, 0, 0, ..., -X_i^2)). \end{gathered}$$

Then if we only look at the first n components, we have

$$(X_0^{q-2}, 0..., 0) = \sum_{i<j}^{n-1} f *_{ij} (X_0, ..., X_{n-1})(0, .., X_j^2, 0, ..., 0, -X_i^2, 0, ..., 0)),$$

where $(X_0^{q-2}, 0..., 0)$ is of size n. This implies that all $f*_{ij}$ are zero follows from induction assumption.

We therefore have that

$$f_{ij}(X_0, ..., X_n) = X_n f'_{ij}(X_0, ..., X_n)$$

for $i < j < n$.

Then have that

$$\begin{gathered} (X_0^{q-2}, 0..., 0) = \\ \textstyle\sum_{i<j}^{n-1} X_n f'_{ij}(X_0, ..., X_n)(0, .., X_j^2, 0, ..., 0, -X_i^2, 0, ..., 0) + \\ (\textstyle\sum_{i<n}^{n-1} f_{i,n}(X_0, ..., X_{n-1})(0, .., X_n^2, ..., 0, 0, 0, ..., -X_i^2)) = \\ \textstyle\sum_{i<j}^{n-1} X_n f'_{ij}(X_0, ..., X_n)(0, .., X_j^2, 0, ..., 0, -X_i^2, 0, ..., 0) + \\ (f_{0,n}(X_0, ..., X_{n-1})X_n^2, .., 0, ..., 0, 0, 0, ..., -f_{0,n}(X_0, ..., X_{n-1})X_i^2) + \\ (\textstyle\sum_{0<i<n}^{n-1} f_{i,n}(X_0, ..., X_{n-1})(0, .., X_n^2, ..., 0, 0, 0, ..., -X_i^2)). \end{gathered}$$

Let us look at the first component, we have

$$X_0^{q-2} = X_n(\sum^{n-1} n_{0<j} X_n f'_{0j}(X_0, ..., X_n)X_j^2) + X_n^2 f_{0,n}(X_0, ..., X_{n-1}),$$

which is impossible since the LHS can factor our X_n, while the right can not.

This prove our lemma.

This lemma implies that

$$D_{\text{reg}}(\{P_0, \dots, P_{n-1}\}) \leq q,$$

while the theorem above implies that

$$D_{\text{reg}}(\{P_0, \dots, P_{n-1}\}) \geq q,$$

therefore we have

Theorem 4.6. *For a Square system,*

$$D_{reg}(\{P_0, \dots, P_{n-1}\}) = q$$

Theorem 4.7. *For a square systems,*

$$D_{reg}(\{p_1, \dots, p_n\}) = q$$

There is also a possibility to prove this theorem in a more abstract way. This proof can be sketched as follows:

1) the first step is to prove that:

over the polynomial ring $A = \mathbb{K}[X_1, ..., X_n]$, the polynomial system $\{X_1^2, .., X_n^2\}$ does not have any non-trivial syzygies, due to the fact that $\{X_1^2, .., X_n^2\}$ are algebraically independent over A ;

2) let ψ be the map: ψ: $A^n \rightarrow {}_n\mathcal{B}$ given by

$$\psi(b_1, \dots, b_n) = \sum_i b_i X_i^2,$$

where

$$A^n = A \times A \times ... \times A,$$

the direct product of n copies of A, then the second step is to prove that:

the syzygy module of the polynomial system $\{X_1^12, .., X_n^2\}$ over ${}_nB_{\mathbb{K}} = \mathbb{K}[X_1, \dots, X_n]/\langle X_1^q, \dots, X_n^q\rangle$ is isomorphic to kernal$(\psi)/T$, where $T = (t_1, .., t_n)$, where $t =$ Ideal $< X_1^q, ..., x_n^q >$;

3) the last step is to use a filtration of module argument to show that there is no non-trivial syzygies before the degree of $q - 1$ and this proves also our main theorem.

We omit the details of this proof since the detailed proof in this paper is straightforward and easy to understand.

Theorem 4.8. *For a Square systems with n variables and $q = \Omega(n)$, the complexity to invert the system algebraically is exponential.*

If we look at a Gröbner basis attack on a Square system with the assumption that these algorithms will terminate at degree equal to the degree of regularity or shortly after this, the running time of this algorithm will be roughly $n^{3D_{\text{reg}}}/6$, which is clearly exponential.

Remark *If one pays close attention, one can reach an easy conclusion that our theorems works also in the case of any odd characteristic field including composite field, however the situation of composite field is a little subtle in terms of complexity analysis due to the fact that we can work on smaller filed (the prime field) with more variables. We will deal with this case in a subsequent paper.*

5. Conclusion

Following the previous works of [15], [12],[8], this paper proves that in the case of the Square system, which was proposed in [3], namely, when the HFE system is given by:

$$P(X) = X^2,$$

the degree of regularity is exactly q.

This theorem proves a very strong conjecture in [8] on the lower bound of the degree of regularity for the case of q is odd and q is the size of $\Omega(n)$, which implies that to invert the related systems algebraically is actually exponential.

This work is the first ever to give a lower bound for degree of regularityof HFE systems and therefore show a lower bound for the complexity of the related algebraic attacks. Clearly from the point view of cryptography, this result could have profound impacts in many related areas, in particular, in understanding the complexity of algebraic attacks and in designing new cryptosystems. The results of this paper strongly suggest, as speculated in [11], that using odd characteristics is indeed a very good idea to resist algebraic attacks, and therefore confirms the idea that we should move to filed of odd characteristics. Also this works points to the possibility to design provablely secure MPKCs. Indirectly, this work also points to new directions in terms of algebraic immunity for function that should be used in symmetric cryptosystems.

References

[1] Olivier Billet and Gilles Macario-Rat, Cryptanalysis of the Square Cryptosystems. In Advances in Cryptology ASIACRYPT 2009 Lecture Notes in Computer Science, 2009, Volume 5912, 451-468, Springer, 2009

[2] M. Bardet, J.-C. Faugère, and B. Salvy, On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In International Conference on Polynomial System Solving - ICPSS, pages 71 -75, Nov 2004

[3] Crystal Clough, John Baena, Jintai Ding, Bo-Yin Yang, Ming-Shing Chen Square, a New Multivariate Encryption Scheme, CT-RSA, 2009, pages 252-264, Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings, Springer, Lecture Notes in Computer Science, V. 5473,

[4] Crystal Clough, Jintai Ding, Secure Variants of the Square Encryption Scheme, PQCrypto 2010– The Third International Workshop on Post-Quantum Cryptography Darmstadt, Germany, May 25-28, 2010, P. 153-164, Lecture Notes in Computer Science, V. 6061 Springer 2010

[5] Jintai Ding. Mutants and its impact on polynomial solving strategies and algorithms. Privately distributed research note, University of Cincinnati and Technical University of Darmstadt, 2006.

[6] Jintai Ding, Johannes Buchmann, Mohamed Saied Emam Mohamed, Wael Said Abdel Mageed Mohamed, Ralf-Philipp Weinmann, *Mutnat XL*, First International Conference on Symbolic Computation and Cryptography – SCC 2008

[7] Jintai Ding, Jason Gower, Dieter Schmidt, *Multivariate Public Key Cryptography*, Advances in Information Security series, Springer, 2006.

[8] J. Ding, T. Hodges, *Inverting the HFE System is Quasi-polynomial for All Fields*, accepted for Crypto 2011

[9] J. Ding, T. Hodges, V. Kruglov, *Growth of the ideal generated by a quadratic boolean function*, PQCrypto 2010, Lecture Notes in Computer Science 6061, Springer, 13-27.

[10] J. Ding, T. Hodges, V. Kruglov, D. Schmidt, S. Tohaneanu, *Growth of the ideal generated by a multivariate quadratic function over GF(3)*, preprint.

[11] J. Ding, D. Schmidt, and F. Werner. Algebraic attack on HFE revisited. Information Security, 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008.,Lecture Notes in Computer Science, V. 5222, P. 215-227 Springer, 2008
In *The 11th Information Security Conference*. Springer-Verlag, 2008.

[12] V. Dubois and N. Gama, *The degree of regularity of HFE systems.* ,Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010, LNCS, v. 6477, 557-576, Springer, 2010

[13] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In Dan Boneh, editor, *Advances in cryptology – CRYPTO 2003, LNCS*, volume 2729, pages 44–60. Springer, 2003.

[14] M. R. Garey and D. S. Johnson. *Computers and intractability, A Guide to the theory of NP-completeness.* W.H. Freeman, 1979.

[15] L. Granboulan, A. Joux and J. Stern, Inverting HFE Is Quasipolynomial. CRYPTO 2006, LNCS, V. 4117, P. 345-356, Springer, 2006

[16] A. Kipnis and A. Shamir: *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.* CRYPTO 1999: 19-30, Lecture Notes in Computer Science,V. 1666, Springer 1999

[17] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, 1997.

[18] Mohamed Saied Emam Mohamed, Daniel Cabarcas, Jintai Ding, Johannes Buchmann, Stanislav Bulygin: MXL3: An Efficient Algorithm for Computing Grbner Bases of Zero-Dimensional Ideals. ICISC 2009: 87-100

[19] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature verification and message encryption. In C. G. Guenther, editor, *Advances in cryptology – EUROCRYPT '88, LNCS*, volume 330, pages 419–453. Springer, 1988.

[20] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In D. Coppersmith, editor, *Advances in Cryptology – Crypto '95, LNCS*, volume 963, pages 248–261, 1995.

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

[22] Zhe-Xian Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing Co. Ltd., 2003

[23] B.-Y. Yang, J.-M. Chen, *Theoretical Analysis of XL over Small Fields*, in: Proc. 9th Australasian Conference on Info. Sec. and Privacy, Lecture Notes in Computer Science 3108, Springer, Berlin, 2004, pp. 277-288.

1: Southern Chinese University of Technology, Guangzhou, China, Department of Mathematical Sciences, University of Cincinnati , USA

E-mail address: `jintai.ding@uc.edu`