Finite Fields and Their Applications 26 (2014) 32–48

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Inverting square systems algebraically is exponential

Jintai Ding[a,b,*], Crystal Clough[b], Roberto Araujo[c]

[a] *CPS Lab, Chongqing University, China*
[b] *Department of Mathematical Sciences, University of Cincinnati, USA*
[c] *Faculdade de Computação, Universidade Federal do Pará, Brazil*

ARTICLE INFO

Article history:
Received 9 October 2012
Received in revised form 29 August 2013
Accepted 1 October 2013
Available online 26 November 2013
Communicated by S. Gao

MSC:
94A60
14G50
13P15
03D15

Keywords:
Square
HFE
Degree of regularity

ABSTRACT

In this paper, we prove that the degree of regularity of square systems, a subfamily of the HFE systems, over a prime finite field of odd characteristic q is exactly q and, therefore, prove that inverting square systems algebraically using Gröbner basis algorithm is exponential, when $q = \Omega(n)$, where n is the number of variables of the system.

1. Introduction

In 1994 Peter Shor [16] showed that quantum computers could break all public key cryptosystems based on hard number-theoretic problems like the integer prime factorization problem and the discrete logarithm problem. Recently significant efforts have been put into the search for alternative post-quantum cryptosystems which would remain secure in an era of quantum computers. Multivariate public key cryptosystems (MPKCs) are one of the main families of cryptosystems that have the potential to resist future quantum computer attacks.

Research on MPKCs started in the 1980s with the works of Diffie, Fell, Tsujii, and Shamir. The real breakthrough came in 1988 with the cryptosystems proposed by Matsumoto and Imai [14]. The

[*] Corresponding author at: Department of Mathematical Sciences, University of Cincinnati, USA.
E-mail address: jintai.ding@gmail.com (J. Ding).

1071-5797/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ffa.2013.10.004

schemes were broken by Patarin, who later developed Hidden Field Equation (HFE) cryptosystems based on the same fundamental idea of quadratic functions derived from special functions on large extension fields [15].

Fixing a finite field $\mathbb{F}$ of characteristic 2 and cardinality q, Patarin 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 $P' : \mathbb{F}^n \longrightarrow \mathbb{F}^n$. One then "hides" this map by composing with invertible affine maps. The resulting map, $\bar{P} : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ defined by

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

where the $L_i : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ are the invertible affine maps, is the public key of the encryption scheme.

For a Hidden Field Equation system (HFE) [15], P is given as a univariate polynomial in the form:

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

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 the Berlekamp–Massey algorithm.

Faugère and Joux [10] showed that these systems can be broken rather easily in the case when $q = 2$ and D is small using the Gröbner basis algorithm F_4. A good measure of how quickly and efficiently these algorithms run is the degree at which they terminate; that is, the highest degree of polynomials that are generated during the algorithm involved in non-trivial computations. (At this degree, the step to compute the reduction of polynomials becomes a process of Gaussian elimination, and this step of computation involves matrices of the largest size and consumes the largest number of computations.) In [10], the experimental results suggested that such algorithms will finish at the degree of order $\log_q(D)$, meaning the highest degree polynomials that the algorithm will generate have degree of order $\log_q(D)$. Therefore they claim that the complexity of the algorithm is $O(n^{\log_q(D)})$.

A key concept in the complexity analysis of these algorithms is that of *degree of regularity*. Bardet, Faugère and Salvy (BFS) defined the degree of regularity for semi-regular systems (like random or generic systems) and gave an asymptotic estimate formula for this degree, which is based on counting of dimensions of spaces with linear independence assumptions [2,17]. Experiments show that this is the degree at which the algorithm will terminate and therefore determines the complexity. However, since the systems arising from HFE polynomials are far from generic, the BFS bound does not yield useful information about the complexity of solving HFE systems algebraically.

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 [12] and Faugère and Joux [10]. They **sketched** how 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 $q = 2$. These bounds suggest that if D is chosen to be $O(n^\alpha)$ for $\alpha \geqslant 1$, 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 that HFE systems belong to this class. Therefore, to derive 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.

A breakthrough in case of general q came in the recent work of Dubois and Gama [9]. They formulate a different definition of the degree of regularity. The degree of regularity of a polynomial system:

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0, \\ &\vdots \\ p_n(x_1, \ldots, x_n) &= 0 \end{aligned}$$

is the lowest degree at which non-trivial polynomial relations between the polynomial p_i occur. They refined and gave a rigorous mathematical foundation for the arguments in [11]. They derived a new method to compute the degree of regularity over any field similar to that in [2]. This leads 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 bounds from their algorithm.

Inspired by the work of [9], and using a similar idea to that used in [11] – roughly that one can bound the degree of regularity of a system by finding a bound for certain simpler subsystems, a new closed formula was found for the degree regularity for all HFE systems for any field in [7]. However, this bound is derived using a very different approach. All previous 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 them to draw conclusions about the upper bound of the complexity of inverting the system using Gröbner basis methods, assuming that the polynomial solving algorithm will terminate at this degree.

It is clear that these two definitions of degree of regularity are not exactly the same. The definition of degree of regularity of BFS is not general in the sense that it is restricted only to semi-regular cases and thus does not apply to any system that is not semi-regular, e.g. an HFE system. To simplify our exposition, we will call the degree of regularity defined by BFS the restricted degree of regularity.

Though we cannot prove that polynomial solving algorithms terminate at the degree of regularity, we do know:

(1) for semi-regular systems, these two definitions of degree of regularity are identical;
(2) for HFE systems, experiments show that Gröbner basis solvers indeed terminate at the degree of regularity or one degree above it;
(3) a Gröbner basis solver cannot terminate below the degree of regularity for an HFE system, since a non-trivial degree fall needs to occur before solvers finish;
(4) if a polynomial system has only one solution, the Gröbner basis solvers will never terminate below the degree of regularity, since to get the solution requires non-trivial degree fall. Here, by non-trivial degree fall, we mean the situation that linear combinations of multiples of the generators of an ideal produce polynomial of lower degree than usually expected. (Mathematical definition is given in Section 3.)

Therefore the degree of regularity of an HFE system at least tells us a lower bound of the degree below which Gröbner basis solvers will not terminate. Therefore, it enables us to derive a lower bound of the complexity of Gröbner basis solvers and related mutant XL solvers [5,6,13].

1.1. The contribution of this paper

In the paper [7], the authors presented a conjecture 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.

Following the same mathematical approach as in [7], we actually prove in this paper that in the case of the square system, which was proposed in [3,4], 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 allows us to draw the following conclusions about the complexity of inverting a 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 [7]. Though it does not answer the question about cases other than square systems, common sense 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 an HFE system and accordingly a lower bound for the complexity of the related algebraic attacks. Clearly from the point of view of cryptography, this result could have significant impact in many related areas, in particular, in understanding the complexity of algebraic attacks and in designing practical parameters for cryptosystems.

The results of this paper strongly suggest that, as speculated in [8], using odd characteristics of a reasonable size is a good idea to resist algebraic attacks, and therefore confirms the idea that we should move to fields of odd characteristic.

We would also like to point out that the square scheme itself is broken [1], but by a totally different method from the direct algebraic attacks by solving the public equations. Algebraic attacks were considered as the most powerful tool in attacking the HFE systems before due to their effectiveness in breaking the HFE Challenge 1. *The result of this paper, however, shows that algebraic attacks are not something we should worry too much about in general for the HFE family once we use odd characteristics $q = \Omega(n)$.*

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 definitions and basic properties of the degree of regularity from [7,9]. In Section 4, we will prove the main theorem that the 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, we will consider the case that q is an odd prime number, which also implies that $q > 2$.

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

We will, in general, use x_i to denote variables over $\mathbb{F}$ and use X_i as variables over $\mathbb{K}$.

Any map P from $\mathbb{K}$ to $\mathbb{K}$ can be expressed **uniquely** as a polynomial function with coefficients in $\mathbb{K}$ and its 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 a standard map ϕ, which identifies $\mathbb{K}$ as $\mathbb{F}^n$:

$$\mathbb{F}^n \xrightarrow{\phi} \mathbb{K},$$

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

Then we can build a new map

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

which is essentially P but viewed as a function over $\mathbb{F}^n$.

In this case, again each component $p_i(x_0, \dots, x_{n-1})$ can be expressed **uniquely** as polynomials of the variables x_i such that the highest power of x_i $(i = 0, \dots, n-1)$ 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.

We can say that these are two different ways of defining the degree for P, the degree over $\mathbb{K}$ and the degree over $\mathbb{F}$. The degree over $\mathbb{K}$ is the degree of $P(X)$. The degree of P over $\mathbb{F}$ is the degree of P'. For example, the functions X^{q^i} are linear over $\mathbb{F}$. Thus, the degree of X^{q^i} over $\mathbb{K}$ is q^i while the degree of this map over $\mathbb{F}$ is 1. The degree of any monomial X^d over $\mathbb{F}$ is the sum of the digits in the base q expansion of d (i.e. the q-Hamming weight of d). In general, the degree of $P(X)$ over $\mathbb{F}$ is the maximum of the q-Hamming weights associated to the monomial terms of $P(X)$.

A map from $\mathbb{K}$ to $\mathbb{K}$ has $\mathbb{F}$-degree 2 if all of its monomial terms have exponents of the form $q^i + q^j$ or q^i for some i and j. The general form of such 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 degree over $\mathbb{F}$ is used to build the HFE multivariate public key cryptosystems and originally the q is selected as 2, which is very different from what we consider here, namely q is an odd prime.

The simplest form of a quadratic function over $\mathbb{F}$ is

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

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

In a square system, just like any HFE system, we build the public key $\bar{P}$ 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 $L_1, L_2 : \mathbb{F}^n \to \mathbb{F}^n$:

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

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

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

where

$$\bar{P}(x_1, \dots, x_n) = \bigl(\bar{p}_1(x_1, \dots, x_n), \dots, \bar{p}_n(x_1, \dots, x_n)\bigr).$$

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

Since L_1 performs a transformation of deriving a set of new polynomials from linear combination of the old ones, and L_2 performs a change of basis of the variables of the polynomials, and neither transformation changes the degree of regularity, without loss of generality we only need to consider the case $p_1 = 0, \dots, p_n = 0$ where the p_i are the component functions of $P' = \phi \circ P \circ \phi^{-1}$.

Implementation of the Gröbner basis algorithm implicitly involves searching through combinations of multiples of the p_i by polynomials of a fixed degree for polynomials of smaller degree than expected. If the combination $\sum_i g_i p_i$ has degree which is smaller than the maximum $(\deg g_i + \deg p_i)$, then the corresponding combination of highest degree terms $\sum_i g_i^h p_i^h$ is zero, where f^h stands for the highest degree homogeneous component of a function f (we will also call f^h the leading component of f). The key moment in the calculation is when *non-trivial* combinations of this type occur. These non-trivial relations will very likely generate what is called mutant [5,6,13], which is 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

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

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. As discussed earlier, the degree at which the first non-trivial relation occurs is called the *degree of regularity*. Extensive experiments have shown that the algorithm will terminate at or shortly after the degree of regularity for the case of HFE systems. The algorithm does not finish before dealing with polynomials at the degree of regularity. Thus the calculation of the degree of regularity is crucial in understanding the complexity of the algorithm.

3. Degree of regularity

We will present the definition of degree of regularity as defined in [9] and the main results in [7,9].

Let

$$A^{(n)} = \mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[x_1, \ldots, x_n] / \left\langle x_1^q - x_1, \ldots, x_n^q - x_n \right\rangle.$$

This is the algebra of functions over $\mathbb{F}^n$. Let $p_1, \ldots, p_n$ be a set of quadratic polynomials in $A^{(n)}$. Denote by $A_l^{(n)}$ the subspace of $A^{(n)}$ consisting of functions representable by a polynomial of degree less than or equal to l.

For all j we have a natural map $\psi_j : (A_j^{(n)})^n \to A_{j+2}^{(n)}$ given by

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

where

$$\left(A_j^{(n)}\right)^n = A_j^{(n)} \times A_j^{(n)} \times \cdots \times A_j^{(n)}.$$

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

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

or

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

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

$$\mathcal{B}^{(n)} = \mathbb{F}[x_1, \dots, x_n] / \langle x_1^q, \dots, x_n^q \rangle.$$

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

Denote by $\mathcal{B}_l^{(n)}$ the subspace of $\mathcal{B}^{(n)}$ consisting of homogeneous elements of degree l. Consider an arbitrary set of homogeneous quadratic elements $\{\lambda_1, \dots, \lambda_n\} \in \mathcal{B}_2^{(n)}$, which are linearly independent. For all j we have a natural map $\psi'_j : (\mathcal{B}_j^{(n)})^n \to \mathcal{B}_{j+2}^{(n)}$ given by

$$\psi'_j(b_1, \dots, b_n) = \sum_i b_i \lambda_i,$$

where

$$\left(\mathcal{B}_j^{(n)}\right)^n = \mathcal{B}_j^{(n)} \times \mathcal{B}_j^{(n)} \times \dots \times \mathcal{B}_j^{(n)},$$

the direct product of n copies of $\mathcal{B}_j^{(n)}$.

Let $R_j^{(n)}(\lambda_1, \dots, \lambda_n) = \ker \psi'_j$, and this comes from the subspace of relations of the form:

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

The key here is that

$$R^{(n)}(\lambda_1, \dots, \lambda_n) = \bigcup_j \left(R_j^{(n)}(\lambda_1, \dots, \lambda_n)\right)$$

is also a module of the ring $\mathcal{B}^{(n)}$, where each element of $\mathcal{B}^{(n)}$ acts on the module by multiplying it to each component of elements:

$$a(b_1, \dots, b_n) = (ab_1, \dots, ab_n),$$

where $a \in \mathcal{B}^{(n)}$ and $(b_1, \dots, b_n) \in R^{(n)}$. Inside $R_j^{(n)}(\lambda_1, \dots, \lambda_n)$ is the subspace of trivial relations, $Z_j^{(n)}(\lambda_1, \dots, \lambda_n)$, which a submodule generated by elements of the form:

(1) $b(0, \dots, 0, \lambda_j, \dots, 0, -\lambda_i, 0, \dots, 0)$ for $1 \leqslant i < j \leqslant n$ where $b \in \mathcal{B}_{j-2}^{(n)}$; λ_j is in the i-th position and $-\lambda_i$ is in the j-th position;
(2) $b(0, \dots, 0, \lambda_i^{q-1}, 0, \dots, 0)$ for $1 \leqslant i \leqslant n$ and $b \in \mathcal{B}_{j-2(q-1)}^{(n)}$; where λ_i^{q-1} is in the i-th position.

The space of non-trivial relations is the quotient space $R_j^{(n)}(\lambda_1, \dots, \lambda_n) / Z_j^{(n)}(\lambda_1, \dots, \lambda_n)$.

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

$$D_{\text{reg}}\left(\{\lambda_1, \dots, \lambda_n\}\right) = \min\left\{j \mid Z_{j-2}^{(n)}(\lambda_1, \dots, \lambda_n) \subsetneq R_{j-2}^{(n)}(\lambda_1, \dots, \lambda_n)\right\}.$$

If the λ_i are linearly independent, the degree of regularity is dependent only on the subspace generated by the λ_i. So we can simplify the notation by denoting the space generated by the λ_i by V and writing $D_{\text{reg}}(V)$ for $D_{\text{reg}}(\{\lambda_1, \dots, \lambda_n\})$.

There are two important properties of the degree of regularity observed in [9].

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

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

Here $V_{\mathbb{K}} = \mathbb{K} \otimes_{\mathbb{F}} V$. The second property tells us that the degree of regularity is invariant under field extension.

Let $B_{\mathbb{K}}^{(n)} = \mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}[x_1, \dots, x_n]$. $V_{\mathbb{K}}$ can be viewed as the $\mathbb{K}$-vector space generated by the λ_i. We will look at the situation where P is a quadratic map with component functions $p_1, \dots, p_n \in A^{(n)}$, which comes from an associated map P'. Let V and V^h be the vector spaces generated by $p_1, \dots, p_n$ and their leading components, namely the component of all their respective quadratic terms: $p_1^h, \dots, p_n^h$. 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 $A^{(n)}$, we pass from functions from $\mathbb{F}^n$ to $\mathbb{F}$ to functions from $\mathbb{F}^n$ to $\mathbb{K}$:

$$\mathbb{F}^n \xrightarrow{p_i} \mathbb{F} \xrightarrow{\text{embedding}} \mathbb{K}.$$

Then via the linear isomorphism $\phi^{-1}: \mathbb{K} \to \mathbb{F}^n$, we can show that this algebra is isomorphic to the algebra of functions from $\mathbb{K}$ to $\mathbb{K}$ which is simply $\mathbb{K}[X]/\langle X^{q^n} - X \rangle$ [7].

From elementary Galois theory [7], we know that the space $V_{\mathbb{K}}$ corresponds, under this identification, to the space generated by $P, P^q, \dots, P^{q^{n-1}}$.

Furthermore, if we **filter** the algebra $\mathbb{K}[X]/\langle X^{q^n} - X \rangle$ by degree of functions over $\mathbb{F}$, then the linear component is spanned by $X, X^q, \dots, X^{q^{n-1}}$. We then can show easily [7] that the associated graded ring will then be the algebra

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

where X_i corresponds to X^{q^i}. This is naturally isomorphic to the algebra $\mathcal{B}^{(n)}$ with coefficients extended to $\mathbb{K}$: $\mathcal{B}^{(n)} \otimes_{\mathbb{F}} \mathbb{K}$.

We will denote this new ring as:

$$B^{(n)} = \mathbb{K}[X_0, \dots, X_{n-1}]/\langle X_1^q, \dots, X_{n-1}^q \rangle.$$

Let P_i denote the leading component of P^{q^i} in $B^{(n)}$. 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 $V_{\mathbb{K}}^h$, which corresponds to the subspace of $\mathcal{B}^{(n)} \otimes_{\mathbb{F}} \mathbb{K}$ generated by the p_i^h, the homogeneous highest degree part of p_i. Putting all the above together we get the following important theorem.

Theorem 3.2. *(See [9].)* $D_{\text{reg}}(\{p_1, \dots, p_n\}) = D_{\text{reg}}(\{p_1^h, \dots, p_n^h\}) = D_{\text{reg}}(\{P_0, \dots, P_{n-1}\})$.

In [7], inspired by the work [9], 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 $P_0, \ldots, P_{n-1}$. 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 an upper bound of the complexity to 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 $B^{(n)}$.

Denote by $B_l^{(n)}$ the subspace of $B^{(n)}$ consisting of homogeneous elements of degree l.

Lemma 4.1. *In $B^{(n)} = \mathbb{K}[X_0, \ldots, X_{n-1}]/\langle X_0^q, \ldots, X_{n-1}^q\rangle$, the monomials*

$$\prod_{i=0}^{n-1} X_i^{a_i}, \quad a_i < q, \ \sum_{i=0}^{n} a_i = k,$$

are linearly independent and form a basis of $B_k^{(n)}$.

This follows from definition.

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

$$E_n(X_i) = X_i,$$

for $i = 0, \ldots, n-1$.

The proof also follows from definition and the lemma above.

Lemma 4.3 *(Inductive decomposition lemma). $B^{(n+1)}$ is a direct sum of two subspaces:*

$$B^{(n+1)} = B^{(n)*} \oplus C^{(n+1)},$$

where

$$B^{(n)*} = E_n\big(B^{(n)}\big),$$

which is the image space of $B^{(n)}$ in $B^{(n+1)}$ under E_n; and

$$C^{(n+1)} = \big\{\textit{The space spanned by monomials in } B^{(n+1)}, \textit{ which are divisible by } X_n\big\}.$$

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

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

$$0 \to C^{(n+1)} \xrightarrow{I_n} B^{(n+1)} \xrightarrow{Pr_n} B^{(n)} \to 0,$$

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

$$Pr_n(X_i) = X_i, \quad i = 0, \dots, n-1; \qquad Pr_n(X_n) = 0,$$

and

$$Pr_n \circ E_n = Id,$$

where Id stands for identity map on $B^{(n)}$.

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

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

If

$$\Phi_j\big(f_0(X_0, \dots, X_{n-1}), \dots, f_{n-1}(X_0, \dots, X_{n-1})\big) = 0$$

then

$$F = \big(f_0(X_0, \dots, X_{n-1}), \dots, f_{n-1}(X_0, \dots, X_{n-1})\big)$$

belongs to

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

the subspace of degree j elements in the space of trivial syzygies corresponding to the system: $\{X_0^2, \dots, X_{n-1}^2\}$.

Here, $Z_j^{(n)}(X_0^2, \dots, X_{n-1}^2)$ follows the same definition as that of $Z_j^{(n)}(\lambda_1, \dots, \lambda_n)$ in Section 3, namely, it is a subspace of degree j elements in the module generated by

$$b\big(0, \dots, 0, X_{j-1}^2, \dots, 0, -X_{i-1}^2, 0, \dots, 0\big)$$

for $0 \leqslant i < j \leqslant n-1$, where $b \in B_{j-2}^{(n)}$, X_{j-1}^2 is in the i-th position and $-X_{i-1}^2$ is in the j-th position.

Note here that

$$\big(0, \dots, 0, \big(X_i^2\big)^{q-1}, 0, \dots, 0\big) = (0, \dots, 0).$$

Note also that this theorem implies that for $j < q-2$, $Z_{j-2}^{(n)} = R_{j-2}^{(n)}$ and thus the degree of regularity must be at least q.

We prove this by induction on n.

1. *The case, when* $n = 1$.

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

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

if the degree of $f(X_0) < q - 2$, since this equation implies that

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

for some polynomial $F'(X_0)$.

2. *Prove the case* $n + 1$ *with the assumption that the statement is true for the case* n.

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

$$\Phi_j\big(f_0(X_0, \ldots, X_{n-1}, X_n), \ldots, f_n(X_0, \ldots, X_n)\big) = \sum_0^n f_i(X_0, \ldots, X_n) X_i^2 = 0,$$

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

Lemma 4.3, the inductive decomposition lemma, allows us to rewrite for each $i < n$:

$$f_i(X_0, \ldots, X_n) = f_i^*(X_0, \ldots, X_{n-1}) + X_n f_i'(X_0, \ldots, X_n),$$

where

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

Then we have that

$$\begin{aligned}&\sum_0^n f_i(X_0, \ldots, X_n) X_i^2 \\ &\quad = \sum_0^{n-1} f_i^*(X_0, \ldots, X_{n-1}) X_i^2 + X_n \sum_0^{n-1} X_i^2 f_i'(X_0, \ldots, X_n) + X_n^2 f_n(X_0, \ldots, X_n) = 0,\end{aligned}$$

where

$$\sum_0^{n-1} f_i^*(X_0, \ldots, X_{n-1}) X_i^2 = E_n \circ Pr_n\left(\sum_0^{n-1} f_i(X_0, \ldots, X_{n-1}) X_i^2\right).$$

From Lemma 4.3, the inductive decomposition lemma, this leads to

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

and

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

Due to the induction assumption, we know that

$$\bigl(f_0^*(X_0,\dots,X_{n-1}),\dots,f_{n-1}^*(X_0,\dots,X_{n-1})\bigr) \in Z_j^{(n)}\bigl(X_0^2,\dots,X_{n-1}^2\bigr)$$

and therefore we have:

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

Using further decomposition according to Lemma 4.3, the inductive decomposition lemma, we have that

$$\begin{aligned} & X_n \sum_0^{n-1} X_i^2 f_i'(X_0,\dots,X_n) + X_n^2 f_n(X_0,\dots,X_n) \\ &\quad = X_n\left(\sum_0^{n-1}\bigl(X_i^2 f_i'^*(X_0,\dots,X_{n-1}) + X_n f_i''(X_0,\dots,X_n)\bigr)\right) \\ &\quad\quad + X_n^2 f_n(X_0,\dots,X_n) = 0, \end{aligned}$$

where

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

Then we have that

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

Then, from Lemma 4.1 in this section, we know that

$$X_n\left(\sum_0^{n-1} X_i^2 f_i'^*(X_0,\dots,X_{n-1})\right) = 0 \tag{2}$$

and

$$X_n^2\left(\sum_0^{n-1} X_i^2 f_i''(X_0,\dots,X_n) + f_n(X_0,\dots,X_n)\right) = 0.$$

Eq. (2) implies that

$$\left(\sum_0^{n-1} X_i^2\bigl(f_i'^*(X_0,\dots,X_{n-1})\bigr)\right) = 0,$$

which is a direct consequence of Lemma 4.1 in this section.

Since the degree of $f_i'^*(X_0,\dots,X_{n-1})$ for $i<n$ is $j-1<q-2$, according to the induction assumption, we have

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

and, therefore, we have

$$\big(f_0'^*(X_0,\dots,X_{n-1}),\dots,f_{n-1}'^*(X_0,\dots,X_{n-1}),0\big)\in Z_{j-1}^{(n+1)}\big(X_0^2,\dots,X_{n-1}^2,X_n^2\big),\tag{3}$$

and therefore we have:

$$\big(X_nf_0'^*(X_0,\dots,X_{n-1}),\dots,X_nf_{n-1}'^*(X_0,\dots,X_{n-1}),0\big)\in Z_{j}^{(n+1)}\big(X_0^2,\dots,X_{n-1}^2,X_n^2\big).\tag{4}$$

Then again with Lemma 4.1 and the fact that the annihilator of X_n^2 is generated by X_n^{q-2}, we have that

$$X_n^2\left(\sum_0^{n-1}X_i^2f_i''(X_0,\dots,X_n)+f_n(X_0,\dots,X_n)\right)=0$$

implies

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

Therefore

$$f_n(X_0,\dots,X_n)=-\sum_0^{n-1}X_i^2f_i''(X_0,\dots,X_n).$$

This means that

$$\begin{aligned}
&\big(X_n^2f_0''(X_0,\dots,X_n),\dots,X_n^2f_{n-1}''(X_0,\dots,X_n),f_n(X_0,\dots,X_n)\big)\\
&\quad=\left(X_n^2f_0''(X_0,\dots,X_n),\dots,X_n^2f_{n-1}''(X_0,\dots,X_n),-\sum_0^{n-1}X_i^2f_i''(X_0,\dots,X_n)\right)\\
&\quad=\big(X_n^2f_0''(X_0,\dots,X_n),0,\dots,0,-X_0^2f_0''(X_0,\dots,X_n)\big)\\
&\qquad+\big(0,X_n^2f_1''(X_0,\dots,X_n),0,\dots,0,-X_1^2f_1''(X_0,\dots,X_n)\big)\\
&\qquad+\dots+\big(0,\dots,0,X_n^2f_{n-1}''(X_0,\dots,X_n),-X_{n-1}^2f_{n-1}''(X_0,\dots,X_n)\big)\\
&\quad=f_0''(X_0,\dots,X_n)\big(X_n^2,0,\dots,0,-X_0^2\big)\\
&\qquad+f_1''(X_0,\dots,X_n)\big(0,X_n^2,0,\dots,0-X_1^2\big)\\
&\qquad+\dots+f_{n-1}''(X_0,\dots,X_n)\big(0,\dots,X_n^2,-X_{n-1}^2\big).
\end{aligned}$$

This gives:

$$\big(X_n^2 f_0''(X_0,\dots,X_n),\dots,X_n^2 f_{n-1}''(X_0,\dots,X_n), f_n(X_0,\dots,X_n)\big) \in Z_j^{(n+1)}\big(X_0^2,\dots,X_{n-1}^2,X_n^2\big). \quad (5)$$

Since

$$\begin{aligned}&\big(f_0(X_0,\dots,X_{n-1},X_n),\dots,f_n(X_0,\dots,X_n)\big)\\&\quad=\big(f_0^*(X_0,\dots,X_{n-1}),\dots,f_{n-1}^*(X_0,\dots,X_{n-1}),0\big)\\&\qquad+\big(X_n f_0'^*(X_0,\dots,X_{n-1}),\dots,X_n f_{n-1}'^*(X_0,\dots,X_{n-1}),0\big)\\&\qquad+\big(X_n^2 f_0''(X_0,\dots,X_n),\dots,X_n^2 f_{n-1}''(X_0,\dots,X_n), f_n(X_0,\dots,X_n)\big),\end{aligned}$$

with (1), (4), (5), we have that

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

This finishes the proof for the theorem.

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

This surely follows from the main theorem above from [7].

But, we give a different but direct proof also by induction.

It is obvious that for $n=0$ (the base case of one variable), the lemma is true since $Z_{q-2}^{(n)}(X_0^2,\dots,X_{n-1}^2,X_n^2)$ contains only the zero element.

Assume our claim is true for the case n, we now proceed to prove the case for $n+1$.

Assume that $(X_0^{q-2},0,\dots,0)$ does belong to $Z_{q-2}^{(n)}(X_0^2,\dots,X_{n-1}^2,X_n^2)$, since $2(q-1)>q-2$ then we have

$$\big(X_0^{q-2},0,\dots,0\big)=\sum_{1\leqslant i<j\leqslant n} f_{ij}(X_0,\dots,X_n)\big(0,\dots,X_i^2,0,\dots,0,-X_j^2,0,\dots,0\big)$$

for some $f_{ij}\in\mathcal{B}^{(n)}$.

Then we have

$$\begin{aligned}&E_n\circ Pr_n\big(X_0^{q-2},0,\dots,0\big)=\big(X_0^{q-2},0,\dots,0\big)\\&\quad=E_n\circ Pr_n\Bigg(\sum_{1\leqslant i<j\leqslant n} f_{ij}(X_0,\dots,X_n)\big(0,\dots,X_j^2,0,\dots,0,-X_i^2,0,\dots,0\big)\Bigg)\\&\quad=\Bigg(\sum_{1\leqslant i<j\leqslant n-1} f_{ij}^*(X_0,\dots,X_{n-1})\big(0,\dots,X_j^2,0,\dots,0,-X_i^2,0,\dots,0\big)\Bigg)\\&\qquad+\Bigg(\sum_{1\leqslant i<j\leqslant n-1} f_{i,n}^*(X_0,\dots,X_{n-1})\big(0,\dots,0,\dots,0,0,0,\dots,-X_i^2\big)\Bigg).\end{aligned}$$

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

$$\big(X_0^{q-2},0,\dots,0\big)=\sum_{1\leqslant i<j\leqslant n-1} f_{ij}^*(X_0,\dots,X_{n-1})\big(0,\dots,X_j^2,0,\dots,0,-X_i^2,0,\dots,0\big),$$

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

We therefore have that

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

for $i < j < n$.

Then we have that

$$\begin{aligned}
&\big(X_0^{q-2}, 0, \dots, 0\big) \\
&\quad = \sum_{1 \leqslant i < j \leqslant n-1} X_n f'_{ij}(X_0, \dots, X_n)\big(0, \dots, X_j^2, 0, \dots, 0, -X_i^2, 0, \dots, 0\big) \\
&\qquad + \left(\sum_{1 \leqslant i < j \leqslant n-1} f_{i,n}(X_0, \dots, X_{n-1})\big(0, \dots, X_n^2, \dots, 0, 0, 0, \dots, -X_i^2\big) \right) \\
&\quad = \sum_{1 \leqslant i < j \leqslant n-1} X_n f'_{ij}(X_0, \dots, X_n)\big(0, \dots, X_j^2, 0, \dots, 0, -X_i^2, 0, \dots, 0\big) \\
&\qquad + \big(f_{0,n}(X_0, \dots, X_{n-1})X_n^2, \dots, 0, \dots, 0, 0, 0, \dots, -f_{0,n}(X_0, \dots, X_{n-1})X_i^2\big) \\
&\qquad + \left(\sum_{1 \leqslant i < j \leqslant n-1} f_{i,n}(X_0, \dots, X_{n-1})\big(0, \dots, X_n^2, \dots, 0, 0, 0, \dots, -X_i^2\big) \right).
\end{aligned}$$

Let us look at the first component, we have

$$X_0^{q-2} = X_n \left(\sum_{1 \leqslant i < j \leqslant n-1} X_n f'_{0j}(X_0, \dots, X_n) X_j^2 \right) + X_n^2 f_{0,n}(X_0, \dots, X_{n-1}),$$

which is impossible since the LHS can factor out X_n, while the RHS does not.

This proves our lemma.

This lemma implies that

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

while the theorem above implies that

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

therefore, we have

Theorem 4.6. *For a square system,*

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

Theorem 4.7. *For a square systems,*

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

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 $A = \mathbb{K}[X_0, \dots, X_{n-1}]$, the polynomial system $\{X_0^2, \dots, X_{n-1}^2\}$ does not have any non-trivial syzygies, due to the fact that $\{X_0^2, \dots, X_{n-1}^2\}$ are algebraically independent over A.

(2) Let Φ be the map: $A^n \to B^{(n)}$ given by

$$\Phi(b_0, \dots, b_n) = \sum_0^{n-1} b_i X_i^2,$$

where

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

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

the syzygy module of the polynomial system $\{X_1^2, \dots, X_{n-1}^2\}$ *over*

$$B^{(n)} = \mathbb{K}[X_0, \dots, X_{n-1}]/\langle X_0^q, \dots, X_{n-1}^q \rangle$$

is isomorphic to $\mathrm{kernel}(\Phi)/T^n$, *where* $T = \mathrm{Ideal}\langle X_0^q, \dots, X_n^q \rangle$.

(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 proof in this paper is straightforward and easier 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.*

Since Gröbner basis attacks on a square system will terminate at degree equal to or above the degree of regularity, the running time of this algorithm will be clearly exponential.

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

5. Conclusion

Following the previous works of [7,9,11], this paper proves that in the case of a square system, which was proposed in [3], namely, when the system is given by:

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

the degree of regularity is exactly q.

This theorem proves a conjecture in [7] 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 using Gröbner basis algorithms is actually exponential.

This work is the first to give a lower bound for degree of regularity for an HFE system based on theoretical proofs, and, therefore, shows a lower bound for the complexity of the related algebraic attacks. Clearly from the point view of cryptography, this result could have significant impacts in many related areas, in particular, in understanding the complexity of algebraic attacks and in designing practical parameters for various cryptosystems. The results of this paper strongly suggest that, as speculated in [8], using odd characteristics of a reasonable size for cryptosystems is indeed a good idea to resist algebraic attacks.

Acknowledgments

The authors would like to thank V. Dubois for many stimulating and insightful discussions, without which this paper will not be possible. We would also like to thank many years' crucial support of the Charles Phelps Taft Foundation and the partial support of the National Science Foundation of China under the grant #60973131, and the grant MMJJ201201001. We would like to thank the anonymous referees for valuable suggestions.

References

[1] O. Billet, G. Macario-Rat, Cryptanalysis of the square cryptosystems, in: Advances in Cryptology ASIACRYPT 2009, in: Lect. Notes Comput. Sci., vol. 5912, Springer, 2009, pp. 451–468.

[2] M. Bardet, J.-C. Faugère, B. Salvy, On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, in: International Conference on Polynomial System Solving, ICPSS, November 2004, pp. 71–75.

[3] C. Clough, J. Baena, J. Ding, B.-Y. Yang, M.-S. Chen, Square, a new multivariate encryption scheme, in: CT-RSA, in: Lect. Notes Comput. Sci., vol. 5473, Springer, 2009, pp. 252–264.

[4] C. Clough, J. Ding, Secure variants of the square encryption scheme, in: PQCrypto 2010 – The Third International Workshop on Post-Quantum Cryptography, Darmstadt, Germany, May 25–28, 2010, in: Lect. Notes Comput. Sci., vol. 6061, Springer, 2010, pp. 153–164.

[5] J. 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] J. Ding, J. Buchmann, M.S.E. Mohamed, W.S.A.M. Mohamed, R.-P. Weinmann, in: Mutant XL, First International Conference on Symbolic Computation and Cryptography, SCC, 2008.

[7] J. Ding, T. Hodges, Inverting the HFE system is quasi-polynomial for all fields, in: CRYPTO, 2011, pp. 724–742.

[8] J. Ding, D. Schmidt, F. Werner, Algebraic attack on HFE revisited, in: Information Security, 11th International Conference, ISC 2008, Taipei, Taiwan, September 15–18, 2008, in: Lect. Notes Comput. Sci., vol. 5222, Springer, 2008, pp. 215–227.

[9] V. Dubois, N. Gama, The degree of regularity of HFE systems, in: Advances in Cryptology, 16th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2010, Singapore, December 5–9, 2010, in: Lect. Notes Comput. Sci., vol. 6477, Springer, 2010, pp. 557–576.

[10] J.-C. Faugère, A. Joux, Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases, in: Dan Boneh (Ed.), Advances in Cryptology, CRYPTO 2003, in: Lect. Notes Comput. Sci., vol. 2729, Springer, 2003, pp. 44–60.

[11] L. Granboulan, A. Joux, J. Stern, Inverting HFE is quasipolynomial, in: CRYPTO 2006, in: Lect. Notes Comput. Sci., vol. 4117, Springer, 2006, pp. 345–356.

[12] A. Kipnis, A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, in: CRYPTO 1999, in: Lect. Notes Comput. Sci., vol. 1666, Springer, 1999, pp. 19–30.

[13] M.S.E. Mohamed, D. Cabarcas, J. Ding, J. Buchmann, S. Bulygin, MXL3: An efficient algorithm for computing Gröbner bases of zero-dimensional ideals, in: ICISC, 2009, pp. 87–100.

[14] T. Matsumoto, H. Imai, Public quadratic polynomial-tuples for efficient signature verification and message encryption, in: C.G. Guenther (Ed.), Advances in Cryptology, EUROCRYPT'88, in: Lect. Notes Comput. Sci., vol. 330, Springer, 1988, pp. 419–453.

[15] J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88, in: D. Coppersmith (Ed.), Advances in Cryptology, Crypto'95, in: Lect. Notes Comput. Sci., vol. 963, 1995, pp. 248–261.

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

[17] B.-Y. Yang, J.-M. Chen, Theoretical analysis of XL over small fields, in: Proc. 9th Australasian Conference on Info. Sec. and Privacy, in: Lect. Notes Comput. Sci., vol. 3108, Springer, Berlin, 2004, pp. 277–288.