Degree of regularity for HFE Minus (HFE-)

Ding, Jintai

Kleinjung, Thorsten

丁, 津泰

出版情報：Journal of Math-for-Industry (JMI). 4 (B), pp.97-104, 2012-10. Faculty of Mathematics, Kyushu University
バージョン：
権利関係：

Journal of Math-for-Industry, Vol. 4 (2012B-3), pp. 97–104

Math-for-industry
Education & Research Hub

Degree of regularity for HFE Minus (HFE-)

Jintai Ding and Thorsten Kleinjung

Received on February 29, 2012 / Revised on August 7, 2012

Abstract. In this paper, we prove a closed formula for the degree of regularity of the family of HFE- (HFE Minus) multivariate public key cryptosystems over a finite field of size q. The degree of regularity of the polynomial system derived from an HFE- system is less than or equal to

$$\begin{cases} \frac{(q-1)(\lfloor \log_q(D-1)\rfloor + a)}{2} + 2 & \text{if } q \text{ is even and } r+a \text{ is odd,} \\ \frac{(q-1)(\lfloor \log_q(D-1)\rfloor + a + 1)}{2} + 2 & \text{otherwise.} \end{cases}$$

Here q is the base field size, D the degree of the HFE polynomial, $r = \lfloor \log_q(D-1)\rfloor + 1$ and a is the number of removed equations (Minus number).
This allows us to present an estimate of the complexity of breaking the HFE Challenge 2:

- the complexity to break the HFE Challenge 2 directly using algebraic solvers is about 2^{97}.

Keywords. HFE, degree of regularity, Minus

1. Introduction

In 1994, Peter Shor [25] showed that all public key cryptosystems based on hard number theory problems, like the factoring problem or the discrete logarithm problem, can be broken by a large quantum computer. Since then, people around the world have devoted significant effort looking for new types of public key cryptosystems, post-quantum cryptosystems which could resist future quantum computers attacks. Multivariate public key cryptosystems (MPKC) [8] are one of the four main groups of cryptosystems that have the potential to accomplish this goal.

MPKC started in the 1980s via the attempts of Diffie, Fell, Tsujii, Shamir, Matsumoto, Imai etc, but without much progress. The first real MPKC should be credited to the cryptosystem proposed by Matsumoto and Imai [21], which however was defeated by Patarin [22] 7 years later. After that Patarin developed the Hidden Field Equation (HFE) cryptosystems, which use the same fundamental mathematical idea via special functions over large extension fields [22].

Let $\mathbb{F}$ be a finite field with cardinality q. The key component is a nearly bijective map P (called an HFE polynomial) over an extension field $\mathbb{K}$ of degree n over $\mathbb{F}$. We can identify $\mathbb{K}$ with $\mathbb{F}^n$, which allows P to induce a multivariate polynomial map $P' \colon \mathbb{F}^n \longrightarrow \mathbb{F}^n$. We then "hide" this core map by composing it on the left and the right by two invertible affine maps L_1 and L_2 over $\mathbb{F}^n$ respectively. This construction yields a new map $\bar{P} \colon \mathbb{F}^n \longrightarrow \mathbb{F}^n$:

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

In order to obtain a quadratic system, we choose a degree D and a univariate polynomial P of 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 selected. Since the decryption process involves solving the single variable polynomial equation $P(X) = Y'$ for a given Y' using the standard Berlekamp-Massey algorithm, we require that the degree D of P should not be too high.

However, Faugère and Joux demonstrated that we can solve and break these systems easily in the case when $q = 2$ and D small [15] using the Gröbner basis algorithm F_4. Furthermore their experimental results imply that such algorithms should finish at a degree of order $\log_q(D)$, such that the highest degree polynomials we need to process are of a degree of order $\log_q(D)$. Therefore they conclude that the complexity of the algorithm is roughly $O(n^{\log_q(D)})$.

The critical concept in the complexity analysis of polynomial solving algorithms is the concept of *degree of regularity*. The degree of regularity of the polynomial system of P consisting of polynomials $p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)$ is the lowest degree at which we have non-trivial polynomial relations between the p_i components. It is commonly accepted that in general this is the degree at which the solving algorithm will terminate and therefore

it is used to parameterize the complexity of the algorithm. Bardet, Faugère and Salvy [1] gave an asymptotic estimate formula for the degree of regularity of random or generic systems. Granboulan, Joux and Stern sketched a new way to bound the degree of regularity in the case $q = 2$ using an approach to lift the problem back to the extension field $\mathbb{K}$, an idea, which first appeared in the works of Kipnis and Shamir [18] and Faugère and Joux [15]. They managed to describe a connection of the degree of regularity of the HFE system to the degree of regularity of a lifted system over the big field. With additional assumptions, they obtained heuristic asymptotic bounds in the case $q = 2$, which leads to the conclusion that for $D = O(n^\alpha)$, $\alpha \geq 1$, the complexity of Gröbner basis solvers for the corresponding HFE systems is quasi-polynomial. Due to the additional assumptions, the problem 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 was not resolved.

The work in [13] seems to suggest that HFE systems over a field of odd characteristic could resist the attack of Gröbner basis algorithms even when D is very small. Their rationale is supported by some abstract algebraic geometry argument related to the usage of field equations. This suggests that the previous results are not necessarily right for fields other than $GF(2)$.

In the case of general q, Dubois and Gama [14] made a big step by setting a rigorous mathematical foundation for the arguments in [17]. They also derived a new inductive method to compute the degree of regularity over any field. Following the work of [14], and using a similar idea as in [17] — roughly that one can bound the degree of regularity of a system by finding a bound for certain simpler subsystems — in [9], a new simple closed formula was found for the degree of regularity for all HFE systems for any field using a completely new constructive proof method. They constructively proved 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 complexity of inverting the system using Gröbner basis methods.

In the paper [9], a strong conjecture is presented on the lower bound of the degree of regularity for the case of odd q of size $\Omega(n)$, which implies that to invert the related systems algebraically is actually exponential.

Following the same mathematical approach [5], it is actually proven that in the case of the Square system, i.e., $P(X) = X^2$, for an odd prime q which was proposed in [2], the degree of regularity is exactly q.

This theorem therefore allows to draw the conclusion: **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 [9], though it does not answer the question about the cases other than Square systems. However 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.

1.1. Our contribution in this paper

We consider the so called HFE- system, where the public key is derived by removing a polynomials:

$$\bar{P}^- = (p_1, \ldots, p_{n-a}).$$

Such a variant is normally used for signatures like in the case of Sflash but can be used for encryption if a is small.

The main contribution of this paper is a closed mathematical formula for the degree of regularity for the HFE- systems. This work is closely related to the new method used in studying the security of Sflash-V3 [12].

We prove that: *The degree of regularity of the HFE- system above is at most*

1)

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

if q is even and $r + a$ is odd (where $r = \lfloor \log_q(D-1) \rfloor + 1$);

2)

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

otherwise.

As far as we know, our work is the first to give a bound for degree of regularity for HFE- systems (or any Minus system), and therefore shows a bound for the complexity of the related algebraic attacks on HFE- systems. Clearly from the point of view of cryptography, this result should have significant implications in many related areas. Furthermore, we use this estimate to give an estimate of algebraic attacks on the HFE Challenge 2 designed by Patarin. We conclude that *the complexity to break HFE Challenge 2 directly using algebraic solvers is about* 2^{97}. Furthermore our results demonstrate that the claims in [3] are far from being correct.

This paper is organized as follows. We will first introduce HFE and Square cryptosystems in the section below. In Section 3, we review the definition and basic properties of the degree of regularity from [14, 9]. In Section 4, we will prove the main theorem that gives the upper bounds for the degree of regularity of HFE- systems and derive the complexity of the Gröbner basis attacks on the HFE Challenge 2.

2. Previous results

2.1. HFE systems and Square systems

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

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

Denote by $\deg_{\mathbb{K}}(P)$ the degree of $P(X)$.

Let ϕ be a map which identifies $\mathbb{K}$ and $\mathbb{F}^n$:

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

Then we can build a new map $P'\colon \mathbb{F}^n \to \mathbb{F}^n$

$$\begin{aligned} P'(x_1,\ldots,x_n) &= (p_1(x_1,\ldots,x_n),\ldots,p_n(x_1,\ldots,x_n)) \\ &= \phi^{-1}\circ P\circ\phi(x_1,\ldots,x_n), \end{aligned}$$

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

In this case, again each component $p_i(x_1,\ldots,x_n)$ can be expressed **uniquely** as a polynomial in the x_j such that the highest power of x_j $(j=1,\ldots,n)$ is not more than q. This is due to the fact that $x_j^q = x_j$ over $\mathbb{F}$. Denote by $\deg_{\mathbb{F}}(P)$ the maximum of the degrees of the components p_i of P'.

In some way, we can say that these are two different ways of defining the degree for P, the degree over $\mathbb{K}$ and the degree over $\mathbb{F}$. For example, the functions X^{q^i}, $i<n$, are all linear viewed from the point of $\mathbb{F}^n$. Thus

$$\deg_{\mathbb{F}}(X^{q^i}) = 1 \quad \text{while} \quad \deg_{\mathbb{K}}(X^{q^i}) = q^i.$$

In general the degree over $\mathbb{F}$ of the monomial X^d will be the sum of the coefficients in the base q expansion of d or the q-Hamming weight of d. Therefore the degree of P over $\mathbb{F}$ is the same as the maximum of the Hamming weights of all 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 or 0 for some i and j. The general form of an $\mathbb{F}$-quadratic function is

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

The function $P(X)$ with a fixed low $\mathbb{K}$-degree is used to build the HFE multivariate public key cryptosystems. Originally the case $q=2$ was considered, which is very different from general q, especially, when q is an odd prime.

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

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

which will give us the so called Square system. Surely if $q=2$, this map is actually of degree one over $\mathbb{F}$ as explained above.

For constructing a system of Square HFE-type, just as in the case of an HFE system itself, we build a map $\bar{P}$ from an $\mathbb{F}$-quadratic map P, where the nature of P is 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 most successful attack on HFE systems is to apply the improved Gröbner basis algorithms F_4 and F_5 to solve the system

$$\bar{p}_1 = y_1,\ldots,\bar{p}_n = y_n.$$

In general, the transformations L_1 and L_2 do not change the degree of regularity (see below) of the system, therefore we only need to consider the case $p_1=0,\ldots,p_n=0$ where the p_i are the component functions of $P' = \phi\circ P\circ\phi^{-1}$.

A key step of the Gröbner basis algorithm consists in searching combinations $\sum_i g_ip_i$, $g_i\in\mathbb{F}[x_1,\ldots,x_n]$, such that the degrees of the summands g_ip_i are equal and the degree of this combination is lower than the degrees of its summands. Denoting by g_i^h the highest degree term of g_i and analogously for p_i we get that the combination of highest degree terms $\sum_i g_i^hp_i^h$ is zero. The key moment in the calculation occurs when such combinations are *non-trivial*. These non-trivial relations will very likely generate mutants (see [6, 7, 20]), which are instrumental in solving the system. Obviously the combinations

$$p_i^hp_j^h - p_j^hp_i^h$$

are tautologically zero and the equation

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

is just a result of the identity $x^q = x$ in $\mathbb{F}$. A non-trivial relation is one that does not arise 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 in general will terminate at or shortly after the degree of regularity, in particular, for the case of HFE systems. 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 the degree of regularity as defined in [14] and the main results in [14, 9]. Let

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

This is the algebra of functions over $\mathbb{F}^n$. Let $p_1,\ldots,p_n$ be a set of quadratic polynomials in ${}_nA$. Denote by ${}_nA_{\le k}$ 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 $\psi_j\colon {}_nA_{\le j}{}^n \to {}_nA_{\le j+2}$ given by

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

where

$${}_nA_{\le j}{}^n = {}_nA_{\le j}\times {}_nA_{\le j}\times\cdots\times {}_nA_{\le j}.$$

If at least one of the a_i has degree j but $\sum_i a_i p_i$ has degree less than $j+2$, we say that a "degree fall" occurs. Obviously we can have trivial degree falls of the form

$$p_j p_i + (-p_i)p_j = 0 \qquad \text{or} \qquad (p_i^{q-1} - 1)p_i = 0.$$

The *degree of regularity* of the set $\{p_1, \ldots, p_n\}$ is the smallest degree 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

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

The degree of regularity of the $\{p_1, \ldots, p_n\}$ in ${}_nA$ 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 ${}_n\mathcal{B}$). 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 $\{\lambda_1, \ldots, \lambda_n\} \subset {}_n\mathcal{B}_2$, which are linearly independent. For all k we have a natural map $\phi_k \colon {}_n\mathcal{B}_k^n \to {}_n\mathcal{B}_{k+2}$ given by

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

where

$${}_n\mathcal{B}_k^n = {}_n\mathcal{B}_k \times {}_n\mathcal{B}_k \times \cdots \times {}_n\mathcal{B}_k,$$

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

Let ${}_nR_k(\lambda_1, \ldots, \lambda_n) = \ker \phi_k \subset {}_n\mathcal{B}_k^n$. The key here is that

$${}_nR(\lambda_1, \ldots, \lambda_n) = \bigoplus_k {}_nR_k(\lambda_1, \ldots, \lambda_n) \subset {}_n\mathcal{B}^n$$

is also a module of the ring ${}_n\mathcal{B}$. The subspace of trivial relations ${}_nZ_k(\lambda_1, \ldots, \lambda_n) \subset {}_n\mathcal{B}$ is generated by relations of the form:

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

The space of non-trivial relations is the quotient space ${}_nR_k(\lambda_1, \ldots, \lambda_n)/{}_nZ_k(\lambda_1, \ldots, \lambda_n)$. From previous work, we know

Definition 1. The *degree of regularity* of $\{\lambda_1, \ldots, \lambda_n\}$ is defined by

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

Assuming the linear independence of the λ_i, the degree of regularity depends only on the subspace V generated by the λ_i, so we can simplify the notation by writing $D_{\text{reg}}(V)$ for $D_{\text{reg}}(\{\lambda_1, \ldots, \lambda_n\})$.

There are two important properties of the degree of regularity which were observed in [14].

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

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

Coming back to the case of an HFE system, let P be a quadratic map, P' its associated map with component functions $p_1, \ldots, p_n \in {}_nA$, and let V resp. V^h be the vector spaces generated by $p_1, \ldots, p_n$ resp. their leading components $p_1^h, \ldots, p_n^h$. 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 ${}_nA$ to ${}_nA \otimes_{\mathbb{F}} \mathbb{K}$, we pass from functions from $\mathbb{F}^n$ to $\mathbb{F}$ to functions from $\mathbb{F}^n$ to $\mathbb{K}$. Via the linear isomorphism $\phi^{-1} \colon \mathbb{K} \to \mathbb{F}^n$, we can show that this algebra is isomorphic to the algebra of functions from $\mathbb{K}$ to $\mathbb{K}$ which is simply $\mathbb{K}[X] / \langle X^{q^n} - X \rangle$ [9].

From elementary Galois theory [9] we know that the space $V_{\mathbb{K}}$ corresponds under this identification with the space generated by $P, P^q, \ldots, P^{q^{n-1}}$.

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 $X, X^q, \ldots, X^{q^{n-1}}$. We can show easily [9] that *the associated graded ring will be the algebra* ${}_n\mathcal{B}_{\mathbb{K}} = \mathbb{K}[X_1, \ldots, X_n] / \langle X_1^q, \ldots, X_n^q \rangle$ *where* X_i *corresponds to* $X^{q^{i-1}}$.

Let P_i denote the leading component of P^{q^i} in ${}_n\mathcal{B}_{\mathbb{K}}$. The space generated by the P_i is exactly $V_{\mathbb{K}}^h$, the subspace of ${}_n\mathcal{B}_{\mathbb{K}}$ generated by the p_i^h. Putting all the above together we get the following theorem.

Theorem 1 ([14])**.** *We have* $D_{reg}(\{p_1, \ldots, p_n\}) = D_{reg}(\{p_1^h, \ldots, p_n^h\}) = D_{reg}(\{P_0, \ldots, P_{n-1}\})$.

In [9], inspired by [14], there is a rigorous proof of the following theorem:

Theorem 2. *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* $V_{\mathbb{K}}^h$*. 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 against algebraic attacks, we actually need a lower bound. This one can prove in the case of Square systems [5].

Theorem 3. *Let* P *be a quadratic operator for the square system for a finite field of odd characteristic* q*. Then the degree of regularity of the associated system is equal to* q*.*

In the next section, we will deal with the HFE Minus systems.

4. The Degree of regularity of HFE-

Here, we assume that the polynomials p_i are linearly independent. Since the coefficients of P are randomly chosen, it is extremely unlikely that the p_i are linearly dependent.

Now let us recall the HFE Minus system. It is derived from an HFE system by removing a components and thus given by a set of $n-a$ polynomials in n variables:

$$\bar{P}^- = (\bar{p}_1, \ldots, \bar{p}_{n-a}).$$

Such a variant is normally used for signatures but can be used for encryption if a is small. We would like to study the degree of regularity of this new system.

To reconnect with the original system, we will build a new system $\bar{P}^o$ by amending zeroes to $\bar{P}^-$:

$$\bar{P}^o = (\bar{p}_1, \ldots, \bar{p}_{n-a}, 0, \ldots, 0).$$

Since the zero polynomials have no impact on the degree of regularity, we get

Lemma 1. *The degree of regularity of the system defined by $\bar{P}^o$ is the same as the degree of regularity of the system defined by $\bar{P}^-$.*

Let E be the standard forgetting map from $\mathbb{F}^n \to \mathbb{F}^{n-a} \hookrightarrow \mathbb{F}^n$ defined as

$$E(x_1, \ldots, x_n) = (x_1, \ldots, x_{n-a}, 0, \ldots, 0).$$

Then we have that

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

Unlike in the case of HFE, $E \circ L_1$ is no longer invertible, but L_2 is still invertible. Therefore we consider

$$P^- = \phi \circ E \circ L_1 \circ \phi^{-1} \circ P = E_1^- \circ P$$

where $E_1^- = \phi \circ E \circ L_1 \circ \phi^{-1}$ and we know that the degree of regularity is determined by this system.

From [9] we know that

Lemma 2. *The degree of regularity of the system of $\bar{P}^-$ is the same as the degree of regularity of the system formed by*

$$P_0^-, P_1^-, \ldots, P_{n-1}^-,$$

where

$$P_i^- = (P^-)^{q^i}.$$

Let $W^- \subset \mathbb{K}[X]/\left\langle X^{q^n} - X \right\rangle$ be the linear space (over $\mathbb{K}$) spanned by $P_0^-, P_1^-, \ldots, P_{n-1}^-$. Since the dimension of the kernel of E is $a > 0$ we get

Lemma 3. *The dimension of W^- over $\mathbb{K}$ is $n-a$.*

For each element of W^-, we can naturally associate a quadratic form and therefore a rank, which is the rank of the corresponding quadratic form. We define the Q-Rank of P^- to be the minimal rank of all elements in W^-.

Furthermore, from [9] we have that

Lemma 4. *The degree of regularity of the system formed by*

$$P_0^-, P_1^-, \ldots, P_{n-1}^-$$

is less than or equal to

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

or q if $\text{Q-Rank}(P^-) = 1$ *for odd q.*

This means that the key problem is to find the Q-Rank of P^- or the minimum rank (Minrank) of the (non-trivial) matrices spanned by matrices associated with all P_i^-.

Let $R(P)$ be the rank of the quadratic form associated with a polynomial P. First we know that

$$R(P) \leq \lfloor \log_q(D-1) \rfloor + 1 = r,$$

if q is odd or r is even; and

$$R(P) \leq \lfloor \log_q(D-1) \rfloor = r - 1,$$

if q is even and r is odd, which is due to the facts that

- The $n \times n$ matrix associated to the quadratic form corresponding to P has the following shape:
$$\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix},$$
where $*$ is an $r \times r$ submatrix
- If q is even the symmetric matrix associated to the polynomial has zero diagonal entries and therefore can only be of even rank.

Let $P_i = P^{q^i}$ and

$$W^a = \text{Span}(P_0, \ldots, P_a).$$

Then the dimension of W^a is exactly $a+1$ since the p_i are assumed to be linearly independent polynomials.

Following the argument of the attack of Sflash^{v-3} of Ding and Schmidt [12], we have that

Lemma 5. *Let $r = \lfloor \log_q(D-1) \rfloor + 1$. The maximum rank of the matrix systems associated to W^a is less than or equal to: 1) $r+a$, if q is odd; 2) $r+a$, if q is even and $r+a$ is even; 3) $r+a-1$, if q is even and $r+a$ is odd.*

Proof. First we know that the matrix associated to the quadratic form corresponding to P_i is in the following shape:

$$\begin{pmatrix} O_i & 0 & 0 \\ 0 & *' & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

where $*'$ is a submatrix of size $r \times r$ and O_i is a zero matrix of size $i \times i$. Namely we shift the position of matrix of P_0 by i positions down and to the right since the Frobenius map $F(X) = X^{q^i}$ is actually $\mathbb{F}$ linear.

Therefore the matrix associated to any elements of W^a is in the shape of

$$\begin{pmatrix} *'' & 0 \\ 0 & 0 \end{pmatrix},$$

where $*''$ is a submatrix of size $(r+a) \times (r+a)$. This gives us the proof. □

Proposition 1. *Let $r = \lfloor \log_q(D-1) \rfloor + 1$. The minrank of the matrix systems associated to $\{P_0^-, P_1^-, \ldots, P_{n-1}^-\}$ is less than or equal to: 1) $r+a$, if q is odd; 2) $r+a$, if q is even and $r+a$ is even; 3) $r+a-1$, if q is even and $r+a$ is odd.*

Proof. Since the dimension of W^a is $a+1$ and the dimension of W^- is $n-a$, we have that

$$W^- \cap W^a \neq \emptyset.$$

This means that there is a nonzero element of W^a in W^-. Then the lemma above gives us the proof. □

Therefore we have

Theorem 4. *Let $r = \lfloor \log_q(D-1) \rfloor + 1$. The degree of regularity of the system formed by*

$$P_0^-, P_1^-, \ldots, P_{n-1}^-$$

is less than or equal to

1)

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

if q is odd or if q is even and $r+a$ is even;

2)

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

if q is even and $r+a$ is odd.

This is the main theorem of this paper.

4.1. Application of the main theorem

Using the main theorem we will discuss the complexity of attacking some multivariate public key cryptosystems.

First, let us look at the case of the HFE Challenge 2. It is an HFE- system, which is defined over $GF(q) = GF(2^4) = GF(16)$, where $n = 36$, $D = 4352$ and $a = 4$.

Since

$$D = 4352 = 16^4 + 16^2 = 4096 + 256,$$

we have that

$$P_0(X) = \sum_{i,j,i\neq j, q^i+q^j \leq D} a_{i,j} X^{16^i+16^j} + \sum_{i \leq 4} b_i X^{16^i} + C,$$

which means that the corresponding matrix for P_0 is in the form:

$$\begin{pmatrix} 0 & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & 0 \\ a_{1,0} & 0 & a_{1,2} & a_{1,3} & a_{1,4} & 0 \\ a_{2,0} & a_{2,1} & 0 & a_{2,3} & a_{2,4} & 0 \\ a_{3,0} & a_{3,1} & a_{3,2} & 0 & a_{3,4} & 0 \\ a_{4,0} & a_{4,1} & a_{4,2} & a_{4,3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

Therefore $r = \lfloor \log_q(D-1) \rfloor + 1 = 4 + 1 = 5$ and the degree of regularity of the challenge over $GF(16)$ is less than or equal to

$$15 \times 8/2 + 2 = 62,$$

and the complexity of an algebraic attack is more than 2^{280}, which is worse than an exhaustive search.

We can also try to solve the system over $GF(2)$. Namely we look at the system

$$W^- = \mathrm{Span}(P_0^-, \ldots, P_{35}^-),$$

as a system over a field which is viewed as a degree $4 \times 36 = 144$ extension over $GF(2)$ instead of a degree 36 extension over $GF(2^4)$. Following the same argument of the main theorem above we conclude that the degree of regularity of the system is less than or equal to

$$(2-1) \times 8/2 + 2 = 6.$$

Remark 1. Here we would like to make a very critical remark, namely we are looking at the system deduced from the HFE Challenge 2 over the field of $GF(2^4)$, which is very **different** from the case of an HFE- system over $GF(2)$, where $n = 4 \times 36 = 144$, $D = 4352$ and $a = 4 \times 4 = 16$, whose corresponding polynomial over the large field would have much more terms than the one from the original HFE Challenge 2.

In the case of the HFE Challenge 2, we now look at solving a system of 128 equations with 144 variables with degree of regularity at most 6. Therefore we expect to solve the system of equations at most degree 6. We can guess 16 variables, thus reducing the number of variables to 128. Since the number of monomials up to degree 6 in these 128 variables is

$$\binom{134}{6} \approx 2^{33}$$

the complexity of solving the system of equations is essentially the same as solving a linear system of this size (number of rows). If we solve it directly using Gaussian elimination, the complexity is estimated to be about $\binom{134}{6}^3/3 \approx 2^{97}$.

However, there are two ways that might reduce the complexity. If we are able to reduce the degree of regularity to 5 by guessing a few more variables the matrix size will be roughly

$$\binom{133}{5} \approx 2^{28}.$$

We can also try to use solvers for sparse matrices, e.g., the Wiedemann algorithm, which have a lower complexity but generate less solutions. This can be done either directly on the degree 6 system or in combination with further guessing of variables. It is not clear how much these approaches affect the complexity.

Finally, let us look at the case of Sflash [24], where $q = 2^7$, $n = 37$ and $r = 11$. If we follow the same argument as above, we can conclude that

1) the degree of regularity of the system over $GF(2^7)$ is roughly $127 \times 6 + 2 = 764$ with 27 variables;

2) the degree of regularity of the system over $GF(2)$ is roughly $6 + 2 = 8$ with 189 variables.

This means that the complexity to solve these systems algebraically is extremely high. The results above show that the claims in [3] about the HFE Challenge 2 and Sflash far from being correct.

5. Conclusion and Discussion

Following previous work [9], we prove a closed formula for the degree of regularity for the family of HFE Minus systems over a finite field of size q. This allows us to obtain an estimate of the complexity of breaking the HFE Challenge 2: *the complexity to break the HFE Challenge 2 directly using algebraic solvers is about* 2^{97}. The mathematical method used in this paper is based on the estimate of certain Minrank problems.

In a subsequent paper, we are now working to extend this work to the case of HKFv and HFEv-, which should lead to much better understanding of the security of related cryptosystems such as Quartz.

References

[1] M. Bardet, J.-C. Faugère, and B. Salvy, *On the complexity of Gröbner Basis Computation of Semi-regular Overdetermined Algebraic Equations*, International Conference on Polynomial System Solving - ICPSS, pp. 71–75, 2004.

[2] C. Clough, J. Baena, J. Ding, B.-Y. Yang, and M.-S. Chen, *Square, a New Multivariate Encryption Scheme*, Topics in Cryptology - CT-RSA 2009, LNCS 5473, pp. 252–264, 2009.

[3] N. Courtois, *Algebraic Attacks over* $GF(2^k)$*, Cryptanalysis of HFE Challenge 2 and Sflash-v2*, Public Key Cryptography - PKC 2004, LNCS 2947, pp. 201–217, 2004.

[4] C. Clough and J. Ding, *Secure Variants of the Square Encryption Scheme*, PQCrypto 2010–The Third International Workshop on Post-Quantum Cryptography, LNCS 6061, pp. 153–164, 2010.

[5] J. Ding, *Inverting Square Systems Algebraically is Exponential*, Cryptology ePrint Archive, Report 2011/275, 2011, eprint.iacr.org

[6] 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.

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

[8] J. Ding, J. Gower, and D. Schmidt, *Multivariate Public Key Cryptography*, Advances in Information Security series, 2006.

[9] J. Ding and T. Hodges, *Inverting the HFE System is Quasi-polynomial for All Fields*, CRYPTO 2011, LNCS 6841, pp. 724–742, 2011.

[10] J. Ding, T. Hodges, and V. Kruglov, *Growth of the Ideal Generated by a Quadratic Boolean Function*, PQCrypto 2010, LNCS 6061, pp. 13–27, 2010.

[11] J. Ding, T. Hodges, V. Kruglov, D. Schmidt, and S. Tohaneanu, *Growth of the Ideal Generated by a Multivariate Quadratic Function over GF(3)*, preprint.

[12] J. Ding and D. Schmidt, *Cryptanalysis of SFlash v3*, Cryptology ePrint Archive, Report 2004/103, 2004, eprint.iacr.org

[13] J. Ding, D. Schmidt, and F. Werner, *Algebraic Attack on HFE Revisited*, Information Security, 11th International Conference, ISC 2008, LNCS 5222, pp. 215–227, 2008.

[14] V. Dubois and N. Gama, *The degree of Regularity of HFE systems*, ASIACRYPT 2010, LNCS 6477, pp. 557–576, 2010.

[15] J.-C. Faugère and A. Joux, *Algebraic Cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases*, CRYPTO 2003, LNCS 2729, pp. 44–60, 2003.

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

[17] L. Granboulan, A. Joux and J. Stern, *Inverting HFE Is Quasipolynomial*, CRYPTO 2006, LNCS 4117, pp. 345–356, 2006.

[18] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, CRYPTO 1999, LNCS 1666, pp. 19–30, 1999.

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

[20] M. S. E. Mohamed, D. Cabarcas, J. Ding, J. Buchmann, and S. Bulygin, *MXL3: An Efficient Algorithm for Computing Gröbner Bases of Zero-Dimensional Ideals*, ICISC 2009, LNCS 5984, pp. 87–100, 2010.

[21] T. Matsumoto and H. Imai, *Public Quadratic Polynomial-tuples for Efficient Signature Verification and Message Encryption*, EUROCRYPT 1988, LNCS 330, pp. 419–453, 1988.

[22] J. Patarin, *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, CRYPTO 1995, LNCS 963, pp. 248–261, 1995.

[23] J. Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, EUROCRYPT 1996, LNCS 1070, pp. 33–48, 1996.

[24] J. Patarin, L. Goubin, and N. Courtois, *C*-+ and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai*, ASIACRYPT 1998, LNCS 1514, pp. 35–49, 1998.

[25] P. Shor, *Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Rev. 41(2), pp. 303–332, 1999.

[26] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing Co. Ltd., 2003.

[27] B.-Y. Yang and J.-M. Chen, *Theoretical Analysis of XL over Small Fields*, ACISP 2004, LNCS 3108, pp. 277–288, 2004.

Jintai Ding
University of Cincinnati, USA; Chongqing University, China
E-mail: jintai.ding(at)uc.edu

Thorsten Kleinjung
EPFL IC LACAL, Lausanne, Switzerland
E-mail: thorsten.kleinjung(at)epfl.ch