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
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: