Computer Security Symposium 2020
26 - 29 October 2020

On the Weil Descent Attack against the Multivariate Quadratic Problem

Yacheng Wang[1,a)] Tsuyoshi Takagi[1,b)]

Abstract: Among candidates for post-quantum cryptography, multivariate cryptography is known for constructing good signature schemes with short signature length. Its security depents on the hardness of solving a set of multivariate polynomials that are used as public key in a multivariate cryptographic scheme, which is often referred to as multivariate quadratic problem (MQ problem). In this paper, we investigate a method for solving the MQ problem, which first transforms a set of multivariate polynomials over a finite field into a new set of multivariate polynomials over its subfield, and then solve it by using algebraic tools like XL, F4 or F5. We investigate the complexity of using such method by analyzing the non-trivial syzygies and the first fall degree of this resulting new polynomial system. Through this, we give a concrete formula for estimating this first fall degree and verify its correctness through some experiments on some small parameters. For a given multivariate quadratic polynomial system $f_1, \ldots, f_n$ over a finite field $\mathbb{F}_{2^q}$, we show the first fall degree of the polynomial system obtained from applying the Weil Descent on $f_1, \ldots, f_n$ is independent from the choice of q being

$$\min\left\{ d \;\middle|\; n\binom{n}{d-2} > \binom{n}{d} \right\}.$$

Moreover, we discuss the possible improvements on this method by coupling it with the hybrid approach of exhaustive search and Gröbner basis techniques.

Keywords: Weil Descent, Multivariate quadratic, First fall degree, Syzygies

1. Introduction

With currently widely used cryptosystems, RSA [18] and ECC [16], being threatened by the development of quantum computers because of Shor's quantum algorithm [19], research on the post-quantum cryptography has become more urgent. NIST [1], [6] anticipated a realization of quantum computers that are capable enough of breaking 2048-bit RSA by the year of 2030, and they have taken actions on standardizing post-quantum cryptosystems. Currently, their project has entered Round 3 of screening.

Multivariate cryptography is considered one of the candidates for post-quantum cryptography because of the hardness of solving the multivariate quadratic problem. Multivaraite public key cryptosystems use a set of multivariate quadratic polynomials as its public key, hence solving the polynomials in a public key is equivalent to breaking a multivariate cryptosystem. Fukuoka MQ challenge [21] is dedicated to understanding the hardness of the multivariate quadratic problem.

One of the most efficient way to solve the multivariate quadratic problem is through computing a Gröbner basis [5] of the ideal generated by the given set of polynomials, which is proposed along with an algorithm called Buchberger's algorithm. Later on, new algorithms F4 [12] and F5 [13], which use linear algebra to do polynomial reduction, are proposed. This really changed the security analysis on multivariate cryptography. For example, Gröbner bases are used to break the first HFE [17] challenge [14].

The Weil descent attack [15] was first proposed to break the discrete logarithm problem on algebraic curve over composite fields, and it can also be applied to the multivariate quadratic problem. When a set of multivariate quadratic polynomials over a field are given, through the Weil descent, a new polynomial system over its subfield can be obtained. Adding the relation on the new variables in the subfield to this new polynomial system will give us a very large polynomial system. However, it is still unclear whether this Weil Descent transformation will solve the given polynomial system faster, and we want to fill in this gap in our work.

1.1 Contribution

The main contribution of this paper is giving a complexity analysis on the Weil Descent against the MQ problem. More specifically, we analyze the first fall degree of the polynomial system obtained from the Weil descent against the MQ problem by considering its non-trivial syzy-

[1] Department of Mathematical Informatics
University of Tokyo
[a)] yacheng_wang@mist.i.u-tokyo.ac.jp
[b)] takagi@mist.u-tokyo.ac.jp

gies. For a given polynomial system $f_1, \ldots, f_n$ over a finite field $\mathbb{F}_{2^q}$, the Weil descent transforms it into a new polynomial system $f'_{1,1}, \ldots, f'_{1,q}, \ldots, f'_{n,1}, \ldots, f'_{n,q}$ over $\mathbb{F}_2$ in variables $y_{1,1}, \ldots, y_{1,q}, \ldots, y_{n,1}, \ldots, y_{n,q}$. Since those variables are over $\mathbb{F}_2$, they all hold $y_{i,j}^2 - y_{i,j}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, q$. We find that the first fall degree of $f'_{1,1}, \ldots, f'_{n,q}$ is independent from the choice of q and is only determined by n :

$$\min \left\{ d \;\middle|\; n\binom{n}{d-2} > \binom{n}{d} \right\}.$$

Moreover, we think solving $f'_{1,1}, \ldots, f'_{n,q}$ works well with the hybrid approach of exhaustive search and Gröbner basis techniques, since variables $y_{1,1}, \ldots, y_{n,q}$ are over $\mathbb{F}_2$, which makes them easy to be specified. Specifying every variable cost a complexity of 2.

1.2 Organization

The paper is organized as follows. Section 2 explains about multivariate quadratic (MQ) problem, complexity of solving the MQ problem using Gröbner basis techniques, the degree of regularity, the first fall degree and computing syzygies of a set of polynomial using linear algebra. In section 3, we introduce the Weil descent transformation on a set of multivariate quadratic polynomials and its complexity. In section 4, we run some experiments on the Weil descent against the MQ problem under some small parameters and we compare the complexity of directly solving the MQ problem using Gröbner basis technique with applying the Weil descent on the MQ problem, and discuss a possible improvement. In section 5, we conclude this paper.

2. The Multivariate Quadratic Problem

In this section, we review the multivariate quadratic problem, a mathematical tool used for solving it called Gröbner bases and the complexity for computing a Gröbner basis.

2.1 Multivariate Quadratic Problem

Let $\mathbb{F}$ be a finite field of order q, $m, n \in \mathbb{N}$, and $R := \mathbb{F}[x_1, \ldots, x_n]$ be the polynomial ring in variables $x_1, \ldots, x_n$ over $\mathbb{F}$.

Problem 1 (Multivariate Qudratic Problem) Given a set of quadratic polynomials $f_1, \ldots, f_m \in R$ and a vector $\mathbf{y} = (y_1, \ldots, y_m) \in \mathbb{F}^m$, find $\mathbf{z} \in \mathbb{F}^n$ such that $f_1(\mathbf{z}) = y_1, \ldots, f_m(\mathbf{z}) = y_m$.

An effective method for solving this problem is through Gröbner basis computation [5]. Efficient algorithms for computing a Gröbner basis include XL [7], F4 [12] and F5 [13]. The complexity of using those algorithms for computing a Gröbner basis depends on polynomials involved during this computation, hence the polynomial degree at which an algorithm terminates can be used to estimate this complexity. This degree is often referred to as *solving degree,* denoted by d_{sol}. This complexity mainly comes from a computation of the row echelon form of a Macaulay matrix of degree d_{sol}. Suppose such a Macaulay matrix has size $R_{d_{sol}} \times C_{d_{sol}}$, then the complexity of the fast algorithm proposed in [20] for computing its row echelon form is given by $O(R_{d_{sol}} C_{d_{sol}}^{\omega-1})$, where $2 \leq \omega \leq 3$ is the linear algebra constant. However, the solving degree of a polynomial system is an experimental value, it can be difficult to be precisely known. Therefore, an approximation value, which is related to the mathematical property of the given polynomial system, is often used. It is called *degree of regularity* (d_{reg}) [3], which is defined as follows.

Definition 1 (Degree of regularity (d_{reg})) Monomials of degree d of R forms a vector space, denoted by R_d. Given $f_1, \ldots, f_m \in R$, denote their homogeneous components of the highest degree by $f_1^h, \ldots, f_m^h \in R$ and let $\langle f_1^h, \ldots, f_m^h \rangle_d$ be the ideal generated by the polynomials in $\langle f_1, \ldots, f_m \rangle$ of degree d. Then the degree of regularity of $\{f_1, \ldots, f_m\}$, if it exists, is the smallest value of

$$\{d \mid \langle f_1^h, \ldots, f_m^h \rangle_d = R_d\}.$$

The degree of regularity d_{reg} for random systems can be precisely evaluated, but hard to estimate for specific families of polynomial systems. Therefore, in cryptographical studies, d_{reg} is often approximated by the *first fall degree* (d_{ff}). To define the first fall degree, we need to be familiar with a notion called non-trivial syzygies.

Definition 2 (Syzygy) Let $\{f_1, \ldots, f_m\} \in R$ be a set of polynomials. A syzygy of $(f_1, \ldots, f_m)$ is an m-tuple $(s_1, \ldots, s_m) \in R^m$ such that $\sum_{i=1}^m s_i f_i = 0$. The degree of a syzygy $\mathbf{s} = (s_1, \ldots, s_m)$, in this paper, is defined as $\deg(\mathbf{s}) = \max_{1 \leq i \leq m} \deg(s_i)$.

The linear combinations of m-tuples $(s_1, \ldots, s_m) \in R^m$ with $s_i = h_j, s_j = -h_i$ for some i, j $(i \neq j)$ and $s_t = 0$ for $t \neq i, j$ are called *trivial syzygies.* The syzygies that are not linear combinations of the trivial syzygies are called *non-trivial syzygies.* Non-trivial syzygies of the homogeneous components of the highest degree of $f_1, \ldots, f_m$ account for the non-trivial degree falls during a Gröbner basis computation.

Definition 3 (First fall degree (d_{ff})) Given a set of polynomials $\{f_1, \ldots, f_m\} \subset R$, let $\{f_1^h, \ldots, f_m^h\} \subset R$ be their homogeneous component of the highest degree. Its first fall degree is the smallest degree d_{ff} such that there exist non-trivial syzygies $(s_1, \ldots, s_m) \in R^m$ of $(f_1^h, \ldots, f_m^h)$ with $\max_i(\deg(s_i f_i^h)) = d_{ff}$, satisfying $\deg(\sum_{i=1}^m s_i f_i) < d_{ff}$ but $\sum_{i=1}^m s_i f_i \neq 0$.

Many results on multivariate cryptosystems are based on analyzing d_{ff} [8], [9], [10], [11], although it is not always true that d_{ff} and d_{reg} are very close, experimental and theoreti-

cal evidences in these results have shown it seems to be true for some cryptographic schemes.

2.2 Computing Syzygies Using Linear Algebra

In this subsection, we exploit the method for computing syzygies of a set of homogeneous polynomials using linear algebra.

Given homogeneous polynomials $f_1, \ldots, f_m \in R$, its degree 0 syzygies $(s_1^{(0)}, \ldots, s_m^{(0)})$ satisfies

$$(f_1, \ldots, f_m) \cdot \begin{pmatrix} s_1^{(0)} \\ \vdots \\ s_m^{(0)} \end{pmatrix} = 0.$$

Let $\mathbf{m}_0$ be the set of all monomials appeared in $f_1, \ldots, f_m$, and $\mathbf{c}_i \in \mathbb{F}^{|\mathbf{m}_0|}$ for $i = 1, \ldots, m$ be coefficients of f_i with respect to $\mathbf{m}_0$. Then we have

$$\mathbf{m}_0 \cdot \begin{pmatrix} \mathbf{c}_1^\top & \mathbf{c}_2^\top & \cdots & \mathbf{c}_1^\top \end{pmatrix} \cdot \begin{pmatrix} s_1^{(0)} \\ \vdots \\ s_m^{(0)} \end{pmatrix} = 0.$$

Therefore, $(s_1^{(0)}, \ldots, s_m^{(0)})$ can be obtained from the right kernel of the matrix $\begin{pmatrix} \mathbf{c}_1^\top & \mathbf{c}_2^\top & \cdots & \mathbf{c}_1^\top \end{pmatrix}$.

For degree 1 syzygies $(s_1^{(1)}, \ldots, s_m^{(1)})$, we assume $s_i^{(1)} = \sum_{j=1}^{n} a_{i,j} x_n$ for $a_{i,j} \in \mathbb{F}$. Let $\mathbf{m}_1$ be the set of all monomials appeared in $x_i f_1, \ldots, x_i f_m$ for $i = 1, \ldots, n$ and $\mathbf{c}_{k,l} \in \mathbb{F}^{|\mathbf{m}_0|}$ be coefficients of $x_k f_l$ with respect to $\mathbf{m}_1$. Then we have

$$\mathbf{m}_1 \cdot \begin{pmatrix} \mathbf{c}_{1,1}^\top & \mathbf{c}_{2,1}^\top & \cdots & \mathbf{c}_{n,m}^\top \end{pmatrix} \cdot \begin{pmatrix} a_{1,1} \\ a_{1,2} \\ \vdots \\ a_{m,n} \end{pmatrix} = 0.$$

Therefore, $(s_1^1, \ldots, s_m^1)$ can be obtained from the right kernel of the matrix $\begin{pmatrix} \mathbf{c}_{1,1}^\top & \mathbf{c}_{2,1}^\top & \cdots & \mathbf{c}_{n,m}^\top \end{pmatrix}$.

Similarly, for degree d syzygies $(s_1^{(d)}, \ldots, s_m^{(d)})$, we first find the set of degree d monomials $\mathbf{b} = (b_1, \ldots, b_t)$ in $\mathbb{F}[x_1, \ldots, x_n]$. Then consider polynomials $b_i f_j$. Let $\mathbf{m}_d$ be all monomials appeared in $b_i f_j$ and $\mathbf{c}_{k,j} \in \mathbb{F}^{|\mathbf{m}_d|}$ be coefficients of $b_k f_l$. Then $(s_1^{(d)}, \ldots, s_{(d)}^m)$ can be obtained from the left kernel of the matrix $\begin{pmatrix} \mathbf{c}_{1,1}^\top & \mathbf{c}_{2,1}^\top & \cdots & \mathbf{c}_{t,m}^\top \end{pmatrix}$.

3. The Weil descent against the MQ Problem

In this section, we describe the Weil descent transformation on the MQ problem, which first transforms a set of multivariate polynomials over a finite field to a new set of multivariate polynomials over its subfields and then solve it using algebraic methods. We especially focus on finite fields with characteristic 2.

3.1 The Weil descent Transformation on the MQ Problem

Let $\mathbb{F}_{2^q}$ be a finite field of characteristic 2 with a cardinality 2^q, $\mathbb{F}_{2^q}[x_1, \ldots, x_n]$ be the polynomial ring in variables $x_1, \ldots, x_n$ over $\mathbb{F}_{2^q}$. Let $\{\theta_1, \ldots, \theta_{\frac{q}{d}}\} \subset \mathbb{F}_{2^q}$ be a basis for $\mathbb{F}_{2^q}/\mathbb{F}_{2^d}$ where $d|q$ holds. Let $\mathbb{F}_{2^d}[y_{1,1}, y_{1,2}, \ldots, y_{1,\frac{q}{d}}, \ldots, y_{m,\frac{q}{d}}]$ be the polynoimal ring in $y_{1,1}, \ldots, y_{m,\frac{q}{d}}$ over the finite field $\mathbb{F}_{2^d}$. Then $x_i = \sum_{j=1}^{\frac{q}{d}} y_{i,j}\theta_j$ holds for $i = 1, \ldots, n$.

In the MQ problem, a polynomial system

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

is asked to be solved. If we substitute $\sum_{j=1}^{\frac{q}{d}} y_{i,j}\theta_j$ in this polynomial system for x_i, we obtain a new system given by

$$\begin{cases} f'_{1,1}\theta_1 + \cdots + f'_{1,\frac{q}{d}}\theta_{\frac{q}{d}} = 0 \\ \vdots \\ f'_{m,1}\theta_1 + \cdots + f'_{m,\frac{q}{d}}\theta_{\frac{q}{d}} = 0 \\ y_{1,1}^{2^d} - y_{1,1} = 0 \\ \vdots \\ y_{n,\frac{q}{d}}^{2^d} - y_{n,\frac{q}{d}} = 0 \end{cases} \Rightarrow \begin{cases} f'_{1,1} = 0 \\ f'_{1,2} = 0 \\ \vdots \\ f'_{1,\frac{q}{d}} = 0 \\ \vdots \\ f'_{m,\frac{q}{d}} = 0 \\ y_{1,1}^{2^d} - y_{1,1} = 0 \\ \vdots \\ y_{n,\frac{q}{d}}^{2^d} - y_{n,\frac{q}{d}} = 0 \end{cases}.$$

Note that equations

$$\begin{cases} y_{1,1}^{2^d} - y_{1,1} = 0 \\ \vdots \\ y_{n,\frac{q}{d}}^{2^d} - y_{n,\frac{q}{d}} = 0 \end{cases}$$

are trivial relations over the field $\mathbb{F}_{2^d}$ and are also commonly referred to as *field equations.*

3.2 Complexity Analysis

In this subsection, we will investigate the complexity of solving the polynomial system obtain from the Weil descent transformation on a set of multivariate polynomial system through Gröbner bases computation. We will focus on the case of $d = 1$.

When $d = 1, f_1, \ldots, f_m \in \mathbb{F}_{2^q}[x_1, \ldots, x_n]$ transforms into $f'_{1,1}, f'_{1,2}, \ldots, f'_{1,q}, f'_{2,1}, \ldots, f'_{m,q}, y_{1,1}^2 - y_{1,1}, \ldots, y_{n,q}^2 - y_{n,q} \in \mathbb{F}_2[y_{1,1}, \ldots, y_{1,q}, y_{2,1}, \ldots, y_{n,q}]$, and we want to know the complexity of solving this new polynomial system using Gröbner basis techniques. In the following discussions, we assume $m = n$, and we try to analyze its first fall degree by investigating its syzygies.

Since the first fall degree depends only on the homogeneous components of the highest degree of a polynomial system, we assume polynomials $f_1, \ldots, f_n$ are all homogeneous of degree 2 since multivariate quadratic polynomials are used in multivariate cryptography. In this case, we need to analyze the first fall degree of

$$\left\{\begin{array}{c} f_1(x_1,\ldots,x_n)=0 \\ \vdots \\ f_n(x_1,\ldots,x_n)=0 \\ x_1-\sum_{j=1}^{q} y_{1,j}\theta_j=0 \\ \vdots \\ x_n-\sum_{j=1}^{q} y_{n,j}\theta_j=0 \\ y_{1,1}^2-y_{1,1}=0 \\ \vdots \\ y_{n,q}^2-y_{n,q}=0 \end{array}\right\} = \left\{\begin{array}{c} f'_{1,1}=0 \\ \vdots \\ f'_{n,q}=0 \\ y_{1,1}^2-y_{1,1}=0 \\ \vdots \\ y_{n,q}^2-y_{n,q}=0 \end{array}\right\}. \quad (1)$$

Since $f_1,\ldots,f_n$ are all homogeneous quadratic polynomials, $f'_{1,1},\ldots,f'_{n,q}$ are also homogeneous quadratic polynomials. To know the first fall degree of (1), we need to only consider its homogeneous components of the highest degree, namely, we need to consider the syzygies of the system

$$\{f'_{1,1}=0,\ldots,f'_{n,q}=0,y_{1,1}^2=0,\ldots,y_{n,q}^2=0\}. \quad (2)$$

The speciality about the system (2) is that during a Gröbner basis computation, any monomials that contain $y_{i,j}^2$ for $i=1,\ldots,n$ and $j=1,\ldots,q$ vanish. Moreover, we know

$$\left\{\begin{array}{c} x_1^2=\sum_{j=1}^{q} y_{1,j}^2\theta_j^2 \\ \vdots \\ x_n^2=\sum_{j=1}^{q} y_{n,j}^2\theta_j^2 \end{array}\right. \quad (3)$$

due to Frobenius endomorphism, which implies any monomials that contain x_i^2 for $i=1,\ldots,n$ vanish during a Gröbner basis computation.

Next we try to analyze the first fall degree of the system (2) starting from the case $n=m=2$, then increase to larger cases.

Case $n=m=2$

When $n=m=2$, monomials involved in f_1 and f_2 can only be x_1^2, x_1x_2 and x_2^2 since f_1 and f_2 are homogeneous of quadratic polynomials, and we want to find a Gröbner basis for the ideal generated by f_1, f_2.

Assume we have

$$\begin{cases} f_1=a_{1,1}x_1^2+a_{1,2}x_1x_2+a_{2,2}x_2^2, \\ f_2=b_{1,1}x_1^2+b_{1,2}x_1x_2+b_{2,2}x_2^2. \end{cases}$$

By extracting the coefficients of f_1 and f_2, we form a Macaulay matrix

$$\begin{array}{c} \\ f_1 \\ f_2 \end{array}\begin{array}{c} \begin{array}{ccc} x_1^2 & x_1x_2 & x_2^2 \end{array} \\ \begin{pmatrix} a_{1,1} & a_{1,2} & a_{2,2} \\ b_{1,1} & b_{1,2} & b_{2,2} \end{pmatrix} \end{array}.$$

Performing row operations on this matrix is equivalent to doing operations on f_1 and f_2. Now if we do not consider $y_{1,1},\ldots,y_{2q}$, the echelon form of this matrix remains the same shape. However, if $y_{1,1}^2=0,\ldots,y_{2,q},x_1^2=0,x_2^2=0$ are considered, entries $a_{1,1},a_{2,2},b_{1,1},b_{2,2}$ vanish and this matrix turns into

$$\begin{array}{c} \\ f_1 \\ f_2 \end{array}\begin{array}{c} \begin{array}{ccc} x_1^2 & x_1x_2 & x_2^2 \end{array} \\ \begin{pmatrix} 0 & a_{1,2} & 0 \\ 0 & b_{1,2} & 0 \end{pmatrix} \end{array},$$

and associated polynomials are $\hat{f}_1=a_{1,2}x_1x_2$ and $\hat{f}_2=b_{1,2}x_1x_2$. Since $\hat{f}_1$ and $\hat{f}_2$ are scalar times to each other, when the Weil descent transformation are applied on them, among the obtained new polynomials, some polynomials are scalar times to each other. Assume applying the Weil descent on $\hat{f}_1$ and $\hat{f}_2$ gives us $f'_{1,1},\ldots,f'_{1,q},f'_{2,1},\ldots,f'_{2,q}$ and $y_{1,1}^2,\ldots,y_{2,q}^2$. We know $f'_{1,1},\ldots,f'_{1,q}$ and $f'_{2,1},\ldots,f'_{2,q}$ are scalar times to each other. There exist degree 0 syzygies of the system $f'_{1,1},\ldots,f'_{2,q},y_{1,1}^2,\ldots,y_{2,q}^2$ since the right kernel of the coefficient matrix of this polynomial system has dimension q, and they are not trivial syzygies since their degree is 0. Hence the first fall degree of this polynomial system is 2 no matter the choice of q.

Case $n=m=3$

When $n=m=3$, f_1,f_2,f_3 can only possibly have monomials $x_1^2,x_1x_2,x_1x_3,x_2^2,x_2x_3,x_3^2$. We can assume polynomial f_1,f_2,f_3 are

$$\begin{cases} f_1=a_{1,1}x_1^2+a_{1,2}x_1x_2+a_{1,3}x_1x_3+a_{2,2}x_2^2+ \\ \qquad a_{2,3}x_2x_3+a_{3,3}x_3^2, \\ f_2=b_{1,1}x_1^2+b_{1,2}x_1x_2+b_{1,3}x_1x_3+b_{2,2}x_2^2+ \\ \qquad b_{2,3}x_2x_3+b_{3,3}x_3^2, \\ f_3=c_{1,1}x_1^2+c_{1,2}x_1x_2+c_{1,3}x_1x_3+c_{2,2}x_2^2+ \\ \qquad c_{2,3}x_2x_3+c_{3,3}x_3^2, \end{cases}$$

where $a_{i,j},b_{i,j},c_{i,j}\in\mathbb{F}_{2^q}$. Its corresponding Macaulay matrix is

$$\begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \end{array}\begin{array}{c} \begin{array}{cccccc} x_1^2 & x_1x_2 & x_1x_3 & x_2^2 & x_2x_3 & x_3^2 \end{array} \\ \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{2,2} & a_{2,3} & a_{3,3} \\ b_{1,1} & b_{1,2} & b_{1,3} & b_{2,2} & b_{2,3} & b_{3,3} \\ c_{1,1} & c_{1,2} & c_{1,3} & c_{2,2} & c_{2,3} & c_{3,3} \end{pmatrix} \end{array}.$$

When considering $y_{1,1}^2=0,\ldots,y_{3,q}^2=0$, this matrix reduces to

$$\begin{array}{c} \\ \bar{f}_1 \\ \bar{f}_2 \\ \bar{f}_3 \end{array}\begin{array}{c} \begin{array}{cccccc} x_1^2 & x_1x_2 & x_1x_3 & x_2^2 & x_2x_3 & x_3^2 \end{array} \\ \begin{pmatrix} 0 & a_{1,2} & a_{1,3} & 0 & a_{2,3} & 0 \\ 0 & b_{1,2} & b_{1,3} & 0 & b_{2,3} & 0 \\ 0 & c_{1,2} & c_{1,3} & 0 & c_{2,3} & 0 \end{pmatrix} \end{array}.$$

Performing Gaussian Elimination on this matrix gives us

$$\begin{array}{c} \\ \hat{f}_1 \\ \hat{f}_2 \\ \hat{f}_3 \end{array}\begin{array}{c} \begin{array}{cccccc} x_1^2 & x_1x_2 & x_1x_3 & x_2^2 & x_2x_3 & x_3^2 \end{array} \\ \begin{pmatrix} 0 & \hat{a}_{1,2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \hat{b}_{1,3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \hat{c}_{2,3} & 0 \end{pmatrix} \end{array}.$$

The ideal generated by f_1,f_2,f_3 is the same as the ideal generated by $\hat{f}_1=\hat{a}_{1,2}x_1x_2,\hat{f}_2=\hat{b}_{1,3}x_1x_3,\hat{f}_3=\hat{c}_{2,3}x_2x_3$.

Let $f'_{1,1},\ldots,f'_{1,q},\ldots,f'_{3,1},\ldots,f'_{3,1},y_{1,1}^2-y_{1,1},\ldots,y_{3,q}^2-$

$y_{3,q}$ be the new polynomial system obtained after the Weil descent transformation. For degree 0 syzygies of $\{f'_{1,1},\ldots,f'_{3,1},y^2_{1,1},\ldots,y^2_{3,1}\}$ to exist, there need to exist some dependent relations between polynomials $\hat{f}_1,\hat{f}_2,\hat{f}_3$, which can only happen when any of $\hat{a}_{1,2},\hat{b}_{1,3},\hat{c}_{2,3}$ is 0. This happens with probability $\frac{1}{q}$. Therefore, the first fall degree of $\{f'_{1,1},\ldots,f'_{1,q},\ldots,f'_{3,1},\ldots,f'_{3,1},y^2_{1,1}-y_{1,1},\ldots,y^2_{3,q}-y_{3,q}\}$ with probability $\frac{1}{q}$ is 2.

Before considering degree 1 syzygies, we first perform the Weil descent transformation on $\hat{f}_1,\hat{f}_2,\hat{f}_3$ with

$$\begin{cases} x_1 = \sum_{j=1}^{q} y_{1,j}\theta_j, \\ x_2 = \sum_{j=1}^{q} y_{2,j}\theta_j, \\ x_3 = \sum_{j=1}^{q} y_{2,j}\theta_j. \end{cases}$$

Let $\Delta = \begin{pmatrix}\theta_1 & \ldots & \theta_q\end{pmatrix}^\top \cdot \begin{pmatrix}\theta_1 & \ldots & \theta_q\end{pmatrix}$, we have

$$\begin{cases} \hat{f}_1 = \hat{a}_{1,2}\cdot\begin{pmatrix}y_{1,1},\ldots,y_{1,q}\end{pmatrix}\cdot\Delta\cdot\begin{pmatrix}y_{2,1},\ldots,y_{2,q}\end{pmatrix}, \\ \hat{f}_2 = \hat{b}_{1,3}\cdot\begin{pmatrix}y_{1,1},\ldots,y_{1,q}\end{pmatrix}\cdot\Delta\cdot\begin{pmatrix}y_{3,1},\ldots,y_{3,q}\end{pmatrix}, \\ \hat{f}_3 = \hat{c}_{2,3}\cdot\begin{pmatrix}y_{2,1},\ldots,y_{2,q}\end{pmatrix}\cdot\Delta\cdot\begin{pmatrix}y_{3,1},\ldots,y_{3,q}\end{pmatrix}. \end{cases}$$

To find the degree 1 syzygies of $\{\hat{f}_1,\hat{f}_2,\hat{f}_3\}$, we only need to find the right kernel of the coefficient matrix of $\{y_{1,1}\hat{f}_1,\ldots,y_{3,q}\hat{f}_1,y_{1,1}\hat{f}_2,\ldots,y_{3,q}\hat{f}_2,y_{1,1}\hat{f}_3,\ldots,y_{3,q}\hat{f}_3\}$. We also need to consider the fact that all monomials that contain $y^2_{1,1},\ldots,y^2_{3,q}$ vanish. However, it seems like a very difficult task and we consider another path for this problem.

As we have discussed before, we showed x_1^2,x_2^2,x_3^2 all vanish due to $y^2_{1,1},\ldots,y^2_{3,q}$ (see (3)), which can be easily obtained from Frobeneius endomorphism. Therefore, instead of multiplying $y_{1,1},\ldots,y_{3,q}$ with $\hat{f}_1,\hat{f}_2,\hat{f}_3$, we multiply x_1,x_2,x_3 with $\hat{f}_1,\hat{f}_2,\hat{f}_3$. We obtain

$$\begin{cases} g_1 &= x_1\hat{f}_1 = \hat{a}_{1,2}x_1^2x_2 = 0, \\ g_2 &= x_2\hat{f}_1 = \hat{a}_{1,2}x_1x_2^2 = 0, \\ g_3 &= x_3\hat{f}_1 = \hat{a}_{1,2}x_1x_2x_3, \\ g_4 &= x_1\hat{f}_2 = \hat{b}_{1,3}x_1^2x_3 = 0, \\ g_5 &= x_2\hat{f}_2 = \hat{b}_{1,3}x_1x_2x_3, \\ g_6 &= x_3\hat{f}_2 = \hat{b}_{1,3}x_1x_3^2 = 0, \\ g_7 &= x_1\hat{f}_3 = \hat{c}_{2,3}x_1x_2x_3, \\ g_8 &= x_2\hat{f}_3 = \hat{c}_{2,3}x_2^2x_3 = 0, \\ g_9 &= x_3\hat{f}_3 = \hat{c}_{2,3}x_2x_3^2 = 0. \end{cases}$$

Now we observe $g_1,\ldots,g_9$. Take $g_1 = x_1\hat{f}_1 = 0$ for example. Since $x_1 = \sum_{j=1}^{q} y_{1,j}\theta_j$, we have

$$g_1 = \theta_1 y_{1,1}\hat{f}_1 + \cdots \theta_q y_{1,q}\hat{f}_1 = 0,$$

which means $(\sum_{j=1}^{q}\theta_j y_{1,j},0,0)$ is a degree 1 syzygy of $\{\hat{f}_1,\hat{f}_2,\hat{f}_3\}$. Similarly, from g_2,g_4,g_6,g_7,g_8,g_9 we can also obtain degree 1 syzygies. Moreover, we have

$$\begin{cases} g_3 &= x_3\hat{f}_1 = \hat{a}_{1,2}x_1x_2x_3, \\ g_5 &= x_2\hat{f}_2 = \hat{b}_{1,3}x_1x_2x_3, \\ g_7 &= x_1\hat{f}_3 = \hat{c}_{2,3}x_1x_2x_3, \end{cases}$$

which are linearly dependent to each other. Therefore, g_5 and g_7 can also be reduced to 0 by g_3, which give two more syzygies. Therefore, in total we get 8 degree 1 syzygies of $\hat{f}_1,\hat{f}_2,\hat{f}_3$, and the first fall degree of $\{f'_{1,1},\ldots,f'_{3,q},y^2_{1,1}-y_{1,1},\ldots,y^2_{3,q}-y_{3,q}\}$ is 3 with a probability of $1-\frac{1}{q}$.

Case $n=m>3$

Armed with results from case $n=m=2$ and $n=m=3$, we generalize those results to higher parameter cases.

Consider homogeneous quadratic polynomials $f_1,\ldots,f_n$. After the Weil descent transformation, suppose we have polynomials

$$f'_{1,1},\ldots,f'_{1,q},\ldots,f'_{n,1},\ldots,f'_{n,q}, \tag{4}$$

$$y^2_{1,1}-y_{1,1},\ldots,y^2_{n,q}-y_{n,q}. \tag{5}$$

Because of (5), we have $x_i^2=0$ for $i=1,\ldots,n$. Therefore, monomials x_i^2 involved in $f_1,\ldots,f_n$ will vanish after the Weil descent transformation, which means total number of monomials remained are $\binom{n}{2}$.

For degree 0 syzygies, polynomials $f_1,\ldots,f_n$ have to be linear dependent, which is highly improbable. As for syzygies with degree d, we simply multiply monomials of degree d in variables $x_1,\ldots,x_n$ with polynomials $f_1,\ldots,f_n$ and observe its coefficient matrix.

For $n=m=3$, if we consider degree 1 syzygies, we multiply $x_1,\ldots,x_n$ with $f_1,\ldots,f_n$ which gives us n^2 new polynomials. To get its coefficient matrix, we need to know the total number of monomials involved. Among new polynomials, monomials can not contain $x_1^2,\ldots,x_n^2$ as they will vanish. Therefore, we will have $\binom{n}{3}$ monomials. Therefore, this coefficient matrix is a $n^2\times\binom{n}{3} = 9\times 1$ matrix, which has a dimension 8 kernel space, and this is consistent with our results in $n=m=3$ case.

For $n=m>3$, if we consider degree d syzygies, we multiply monomials of degree d with square free in variables $x_1,\ldots,x_n$ with $f_1,\ldots,f_n$, which results in $n\cdot\binom{n}{d}$ new polynomials of degree $d+2$. To know about the size of the coefficient matrix of those new polynomials, we need to count the total number of monomials involved. Considering they are all degree $d+2$ polynomials with square free monomials, the total number of monomials should be $\binom{n}{d+2}$. Therefore, its coefficient matrix should be in size $n\binom{n}{d}\times\binom{n}{d+2}$. When

$$n\binom{n}{d} > \binom{n}{d+2},$$

this matrix will have a nonzero kernel space. From this kernel space, non-trivial syzygies of

$$f'_{1,1},\ldots,f'_{1,q},\ldots,f'_{n,1},\ldots,f'_{n,q},$$

$$y^2_{1,1}-y_{1,1},\ldots,y^2_{n,q}-y_{n,q},$$

can be constructed, and its first fall degree is $d+2$.

From the aforementioned discussions, we know the first fall degree of $f'_{1,1},\ldots,f'_{1,q},\ldots,f'_{n,1},\ldots,f'_{n,q},y^2_{1,1}-$

$y_{1,1}, \ldots, y_{n,q}^2 - y_{n,q}$ is independent from the choice of q and only depends on n. And for different choice of m, its d_{ff} is listed in Table 1 have the following results.

Table 1 Estimated first fall degree of the polynomial system $f_1, \ldots, f_n$ over $\mathbb{F}_{2^q}$ after the Weil descent transformation to polynomials over $\mathbb{F}_2$

n	$d_{ff}(f_1, \ldots, f_n)$ after the Weil descent
2	2
$3, \ldots, 8$	3
$9, \ldots, 16$	4
$17, \ldots, 26$	5
$27, \ldots, 38$	6
$39, \ldots, 52$	7
$53, \ldots, 68$	8
$69, \ldots, 86$	9
$87, \ldots, 106$	10
$107, \ldots, 128$	11
$129, \ldots, 152$	12
$153, \ldots, 178$	13
$179, \ldots, 206$	14
$207, \ldots, 236$	15
$237, \ldots, 268$	16
$269, \ldots, 302$	17
$303, \ldots, 338$	18
$339, \ldots, 376$	19
$378, \ldots, 416$	20

4. Experiments and Comparison

In this section, we first verify the results obtained from last section by performing some experiments on different polynomial system after the Weil descent transformation. Then evaluate the effect of the Weil descent on $f_1, \ldots, f_n$ by comparing with solving it directly using Gröbner basis.

4.1 Experiments

We run some experiments on the actual first fall degree and solving degree of $f_1, \ldots, f_n$ after the Weil descent transformation. The results are listed in Table 2. From these results, our theoretical estimation on the first fall degree of $\{f'_{1,1}, \ldots, f'_{1,q}, \ldots, f'_{n,q}, \ldots, f'_{n,q}, y_{1,1}^2 - y_{1,1}, \ldots, y_{n,q}^2 - y_{n,q}\}$ is verified. However, there are cases when the solving degree is larger than the first fall degree such as $n = 7, 8$ case.

Table 2 Experimented first fall degree and solving degree of the polynomial system $f_1, \ldots, f_n$ over $\mathbb{F}_{2^q}$ after the Weil descent Transformation to polynomials over $\mathbb{F}_2$

n	$q=3$		$q=4$		$q=5$		$q=6$		$q=7$	
	d_{ff}	d_{sol}	d_{ff}	d_{sol}	d_{ff}	d_{sol}	d_{ff}	d_{sol}	d_{ff}	d_{sol}
2	2/3	3	2/3	3	2/3	3	2/3	3	2/3	3
3	3	3	3	3	3	3	3	3	3	3
4	3	3	3	3	3	3	3	3	3	3
5	3	3	3	3	3	3	3	3	3	3
6	3	3	3	3	3	3	3	3	3	3
7	3	4	3	4	3	4	3	4	3	4
8	3	4	3	4	3	4	3	4	3	4
9	4	4	4	4	4	4	4	4	4	4
10	4	4	4	4	4	4	4	4	4	4
11	4	4	4	4	4	4	4	4	4	4
12	4	5	4	5	4	5	4	5	4	5
13	4	5	4	5	4	5	4	5	4	5

4.2 Comparison with Direct Solving

Since when the Weil descent transformation is applied to a set of polynomial system $f_1, \ldots, f_n$ over a finite field $\mathbb{F}_{2^q}$ and results in a new polynomial system $f'_{1,1}, \ldots, f' - 1, q, \ldots, f'_{n,1}, \ldots, f'_{n,q}$ over the finite field $\mathbb{F}_2$, new informations

$$\begin{cases} y_{1,1}^2 - y_{1,1}, \\ \quad \vdots, \\ y_{n,q}^2 - y_{n,q} \end{cases}$$

can be added, and it may change the behavior of computing a Gröbner basis. In this subsection, we compare the complexity between with the Weil descent transformation and without it.

For a given random polynomial system $f_1, \ldots, f_n$ in variables $x_1, \ldots, x_n$ over a finite field $\mathbb{F}_{2^q}$, it is supposed to be regular, and its degree of regularity is supposed to $n+1$ [3]. The complexity for computing a Gröbner basis using F4/F5 algorithm [12], [13] is estimated to be

$$\left(\binom{n + d_{reg}}{d_{reg}}^{\omega} \right) \text{ [2]}, \tag{6}$$

where d_{reg} is degree of regularity and $2 \leq \omega \leq 3$ is the linear algebra constant.

As for the polynomial system obtained from applying the Weil descent transformation on $f_1, \ldots, f_n$, we know it is not random, and its degree of regularity can not be estimated using the results in [3], we use its first fall degree as an approximation to its degree of regularity. The complexity hence is

$$\left(\binom{nq + d_{ff}}{d_{ff}}^{\omega} \right), \tag{7}$$

where d_{ff} is the first fall degree.

Both of (6) and (7) mean the approximated number of field operations, since (6) is for $\mathbb{F}_{2^q}$ and (7) is for $\mathbb{F}_2$. Suppose an operation over $\mathbb{F}_{2^q}$ is equivalent to q^2 operations over $\mathbb{F}_2$, we then have to multiply (6) with q^2.

Take $n = 11$ for example, assume $\omega = 2.8$, then direct solving requires a complexity of

$$\binom{11 + 12}{12}^{2.8} \cdot q^2 \approx 2^{57.0 + 2lg(q)},$$

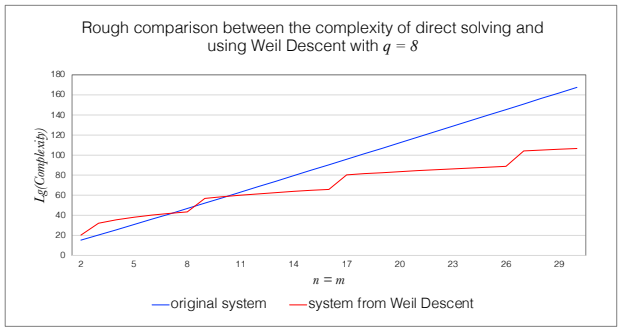
which are $2^{59.03}, 2^{60.20}, 2^{61.03}, 2^{61.67}, 2^{62.20}, 2^{62.64}, 2^{63.03}$ for $q = 2, 3, 4, 5, 6, 7, 8$. For the system derived from the Weil descent, we have a complexity of

$$\binom{11q + 4}{4}^{2.8},$$

which are $2^{38.83}, 2^{44.83}, 2^{49.20}, 2^{52.63}, 2^{55.46}, 2^{57.86}, 2^{60.00}$ for $q = 2, \ldots, 8$. In this case, the polynomial system from the Weil descent requires less complexity than direct solving.

To give a rough comparison between the complexity of the direct solving and using the Weil descent, we fix $q = 8$ and compare their complexity with different values of n from 2 to 30 using d_{ff} we estimated in Table 1 and plot the results in Figure 1.

Fig. 1 Comparison between the complexity of directly solving $f_1, \ldots, f_n$ over $\mathbb{F}_{2^8}$ using Gröbner basis techniques with the complexity of solving a new polynomial system over $\mathbb{F}_2$ obtained from applying the Weil descent transformation on $f_1, \ldots, f_n$



4.3 Further Imporvement with the Hybrid Approach

When solving $f_1, \ldots, f_n$ over a finite field $\mathbb{F}_{2^q}$ with large q with Gröbner basis techniques, applying the hybrid approach [4] does not bring any positive results, as specifying every variable in $\mathbb{F}_{2^q}$ requires a complexity of 2^q. However, when the Weil descent transformation is applied to $f_1, \ldots, f_n$, a new polynomial system

$$\begin{cases} f'_{1,1}(y_{1,1}, \ldots, y_{1,q}, \ldots, y_{n,1}, \ldots, y_{n,q}), \\ \vdots \\ f'_{1,q}(y_{1,1}, \ldots, y_{1,q}, \ldots, y_{n,1}, \ldots, y_{n,q}), \\ \vdots \\ f'_{n,1}(y_{1,1}, \ldots, y_{1,q}, \ldots, y_{n,1}, \ldots, y_{n,q}), \\ \vdots \\ f'_{n,q}(y_{1,1}, \ldots, y_{1,q}, \ldots, y_{n,1}, \ldots, y_{n,q}), \\ y_{1,1}^2 - y_{1,1}, \\ \vdots \\ y_{n,q}^2 - y_{n,q} \end{cases}$$

over $\mathbb{F}_2$ can be obtained. All new variables are over $\mathbb{F}_2$, which means specifying every variable only requires a complexity of 2. Moreover, if we observe Figure 1, the complexity for systems from the Weil descent grows like a staircase, not as flat as the original system. This can possibly be fixed by coupling the hybrid approach of polynomial solving with the Weil descent transformation. Further analysis on the behavior of the first fall degree of this approach is left for a future work.

5. Conclusion

In this paper, we investigated a method of polynomial solving through the Weil descent transformation on a polynomial system. This method first transforms a polynomial system over a finite field into a new polynomial system over its subfield. The resulting polynomial system ends up having more variables and equations, but trivial relations on those variables can be added to this new polynomial system, which possibly can be solved faster.

We specifically investigated the complexity of this method by theoretically analyzing the syzygies and the first fall degree of the system obtained from the Weil descent. We gave a concrete formula for its first fall degree, and verified our analysis through some experiments on small parameters. Since our analysis are purely theoretical, our results should hold for large parameters as well. However, we acknowledge the complexity of polynomial solving using Gröbner basis computing algorithms are mainly determined by the solving degree rather than the first fall degree. Therefore, the actual solving degree for large parameters may be slightly higher than its first fall degree, and more research should be conducted on this regard. Nevertheless, we think this method of polynomial solving is better than simple direct solving, and it may bring a threat to current multivariate cryptography.

Moreover, we believe when the Weil descent approach couples with the hybrid approach of polynomial solving, even better results can possibly be obtained and we plan to do more investigations on this.

Acknowledgments This work was supported by JSPS KAKENHI Grant Number JP18J20866 and JST CREST Grant Number JPMJCR14D6.

References

[1] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. Status report on the first round of the nist post-quantum cryptography standardization process. NIST Internal Report 8240, National Institute of Standards and Technology, 2018.

[2] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the f5 gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49 – 70, 2015.

[3] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. Asymptotic behavior of the index of regularity of quadratic semi-regular polynomial systems. In *8th International Symposium on Effective Methods in Algebraic Geometry –MEGA'05*, 2005.

[4] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3:177–197, 2009.

[5] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universitat Innsbruck, 1965.

[6] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography. NIST Interagency Report 8105, National Institute of Standards and Technology, 2016.

[7] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 392–407. Springer, 2000.

[8] Jintai Ding and Timothy J. Hodges. Inverting HFE system is quasi-polynomial for all fields. In *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *LNCS*, pages 724–742. Springer, 2011.

[9] Jintai Ding and Thorsten Kleinjung. Degree of regularity for hfe-. Cryptology ePrint Archive, Report 2011/570, 2011. `https://eprint.iacr.org/2011/570`.

[10] Jintai Ding and Thorsten Kleinjung. Degree of regularity for HFE-. In *Cryptology ePrint Archieve, Report 2011/570*, 2011. `http://eprint.iacr.org/2011/570`.

[11] Jintai Ding and Bo-Yin Yang. Degree of regularity for HFEv and HFEv-. In *Post-Quantum Cryptography 2013*, volume 7932 of *LNCS*, pages 52–66. Springer, 2013.

[12] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1):61 – 88, 1999.

[13] Jean Charles Faugère. A new efficient algorithm for computing Gröbner Bases without reduction to zero (F5). In *ISSAC 2002*, pages 75–83. ACM, 2002.

[14] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In *CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.

[15] G. Frey and H.-G. Ruck. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[16] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[17] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.

[18] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[19] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[20] A. Stothers. *On the Complexity of Matrix Multiplication*. PhD thesis, University of Edinburgh, 2010.

[21] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai. Mq challenge: Hardness evaluate of solving multivariate quadratic problems. *Eprint*, 2015.