On The Method of "XL" And Its Inefficiency to TTM

T. Moh*

January 28, 2000

1 Introduction

In the article [2], Nicolas Courtois, Adi Shamir, Jacques Patarin and Alexander Klimov propose a method named "XL" which gives an "*efficient algorithm for solving overdefined systems of multivariate polynomial equations*". In the abstract, they state "*we then develop an improved algorithm called XL which is both simpler and more powerful than relinearization*".

We will use the notations of [2]. Let K be a field, and let A be a system of multivariate **quadratic** equations $\ell_k = 0$ $(1 \leq k \leq m)$. Let D be a positive integer. We consider all polynomials $\prod x_{i_j} * \ell_i$ of total degree $\leq D$. Then for a fixed D. We do the following,

Definition 3.0.1 [2](**The XL algorithm**) Execute the following steps:

1. **Multiply:** Generate all the products $\prod x_{i_j} * \ell_i$ of total degree $\leq D$.
2. **Linearize:** Consider each monomial in x_i of degree $\leq D$ as a new variable and perform Gaussian elimination on the equation obtained.

   The ordering on the monomials must be such that all the terms containing one variable (say x_i) are eliminated last.
3. **Solve:** Assume that step 2 yields at least one univariate equation in the powers of x_1. Solve the equation over the finite fields (e.q., with Berlekamp's algorithm).
4. **Repeat:** Simplify the equations and repeat the process to find the values of the other variables.

■

In [2], the authors mention that "*we are interested in the problem of solving overdefined systems of multivariate polynomial equations in which the number of equautions m exceeds the number of variables n.*", and call them "*cryptographically important case(s)*". The cryptographic scheme TTM[1] is one of the important cases. The authors wish to study those cases. However, as pointed out in an e-mail to us by one of the authors of [2]: "*but still your algorithm TTM has nothing to fear directly of XL*". It will be interesting to test this scheme on the various versions of TTM to find their securities.

*Math Department, Purdue University, West Lafayette, Indiana 47907-1395. tel: (765)-494-1930, e-mail ttm@math.purdue.edu

[1]Tame Transformation Method, see [3], [4] or the section 5.

The above XL algorithm is very nature and is a folk lore of experienced algebraic geometers. Every algebraic geometer apply it with intuition and caution. Traditionally, algebraic geometers work only on small number of variables, say 4 or less. In those cases, usually $D < 10$ suffices. It is a real good service to systemize the scheme.

From mathematical view, *relinearization* is about the ring $K[\ell_1, \cdots, \ell_m] \subset K[x_1, \cdots, x_n]$ and XL is about the ideal $(\ell_1, \cdots, \ell_m) \subset K[x_1, \cdots, x_n]$. Let α be a polynomial equation of degree d. Let $V(\alpha, D)$ be the vector space of all polynomials of degree D or less which are multiples of α, and $dim(V(\alpha, D))$ be its dimension. It is easy to see that

$$dim(V(\alpha, D)) = C_{D-d}^{n+D-d}$$

Given a system of *quadratic polynomial equations* ℓ_i for $i = 1, \cdots, m$, it is easy to see that the number of linearly independent equations of degree $\leq D$ which are generated by the step (1) (**multiply**), $H(I, D)$, is $dim(\sum_i V(\ell_i, D))$.

In the section 2, we will show that the function $H(I, D)$ of D is the *compliment* of a well-known function, the *characteristic function*, of the ideal I. From the theory of Hilbert-Serre, we may deduce that the XL program works for many interesting cases for D **large enough**. In general, the XL program will not work as established by Example 4. In the section 3, we show that about $1/m$ of the equations generated by step (1) are linearly independent if D is **large enough**. We summerize the simulations of [2] into a table. In the section 4, we prove an exact formula for $H(I, D)$ for some interesting cases. In the section 5, we apply the previous results to the encryption system TTM, and show that it is *strong*.

We wish to express our thanks to J. Patarin and L. Goubin for correspondences, and W. Heinzer for discussions.

2 Characteristic Function of an Ideal

The function $H(I, D)$ is closely related to the *characteristic function* of the ideal $(\ell_1, \cdots, \ell_m) \subset K[x_1, \cdots, x_n]$ which is defined as follows (cf [1], [5]): Let $I = (\ell_1, \cdots, \ell_m) \subset K[x_1, \cdots, x_n]$ be an ideal with the generators $\ell_1, \cdots, \ell_m$ and $I^\natural$ be the homogenization of I, i.e., $I^\natural = (\ell_1^\natural, \cdots, \ell_m^\natural) \subset K[x_0, x_1, \cdots, x_n]$ where $\ell_i^\natural = x_0^{d_i} \ell_i(x_1/x_0, \cdots, x_n/x_0)$ with $d_i =$ degree of ℓ_i. Note that $I^\natural$ changes if we change the generators. We shall fix the set of generators in the following discussions. The *characteristic function*, $\chi(I^\natural, D)$, is defined as the dimension of all polynomials in $K[x_0, x_1, \cdots, x_n]$ which are of degree D and are linearly independent modulo the ideal $I^\natural$. Since $I^\natural$ is uniquely determined by the generators of the ideal I. we may simply define that $\chi(I, D) = \chi(I^\natural, D)$. We have

Proposition 1: It is easy to see that $H(I, D) + \chi(I, D) = C_D^{n+D}$.

Proof. The dimension of the vector space U of all homogeneous polynomials of degree D in $K[x_0, \cdots, x_n]$ is C_D^{n+D}. All polynomials in $\sum_i V(\ell_i, D)$ can be homogenized to degree D. Therefore $H(I, D) =$ dimension of the vector space V of all homogeneous polynomials of degree D in $I^\natural$. We have $\chi(I^\natural, D) =$ dimension of the quotient space of U modulo $V = \chi(I, D)$.

■

Corollary 1; We have $H(I, D) \leq C_D^{n+D}$. ■

To apply the XL program, we will first locate D with $H(I,D) \geq C_D^{n+D} - D - 1$, and then convert the problem of solving polynomial equations to solving linear equations.

Corollary 2; We have $H(I,D) \geq C_D^{n+D} - D - 1 \Longleftrightarrow \chi(I,D) \leq D+1$. Therefore, the XL program works for $D \Longleftrightarrow \chi(I,D) \leq D+1$. ■

In general, it is difficult to understand the characteristic function $\chi(I^\natural, D)$ exactly. However, there is a polynomial $\bar{\chi}(I^\natural, D)$, the *characteristic polynomial*, which equals to $\chi(I^\natural, D)(= \chi(I,D))$ for D **large enough**[2] (Hilbert-Serre Theorem). The characteristic polynomial gives many important geometric properties of the projective variety defined by $I^\natural$. For the characteristic polynomial $\bar{\chi}(I^\natural, D)$ we have the following formula,

$$\bar{\chi}(I^\natural, D) = a_0 C_r^D + a_1 C_{r-1}^D + \cdots + a_{r-1} C_1^D + a_r$$

where a_i are integers, r is the *projective* dimension of the variety defined by $I^\natural$ and a_0 is the *degree* of the ideal $I^\natural, a_r$ determines the *arithmetic genus*, $p_a(I^\natural)$, of $I^\natural$ by the formula $p_a(I^\natural) = (-1)^r(a_r - 1)$.

Example:

(1) Let $I = (x_1) \subset K[x_1, x_2]$. Then $H(I,0) = 0$ and for $D > 0$, it is easy to see

$$\begin{aligned} H(I,D) &= C_{D-1}^{2+D-1} = D(D+1)/2 \\ \chi(I^\natural, D) &= C_D^{2+D} - H(I,D) = D+1 \\ &= C_1^D + 1 \\ &= \bar{\chi}(I^\natural, D) \end{aligned}$$

Note that the projective variety defined by $x_1 = 0$ is of dimension 1, degree 1 and arithmetic genus 0.

(2) Let $I = (x_1^2) \subset K[x_1, x_2]$. Then $H(I,0) = H(I,1) = 0$, and for $D > 1$, it is easy to see

$$\begin{aligned} H(I,D) &= C_{D-2}^{2+D-2} = D(D-1)/2 \\ \chi(I^\natural, D) &= C_D^{2+D} - H(I,D) = 2D+1 \\ &= 2C_1^D + 1 \\ &= \bar{\chi}(I^\natural, D) \end{aligned}$$

Note that the projective variety defined by $x_1^2 = 0$ is of degree 2, dimension 1 and arithmetic genus 0.

(3) Let $I = (x_1^2, x_1x_2 + 1) \subset K[x_1, x_2]$. We have $I^\natural = (x_1^2, x_1x_2 + x_0^2)$. From the theory of vector space, we have

$$\begin{aligned} &dim(V(x_1^2, D) + V(x_1x_2 + 1, D)) \\ &\quad = dim(V(x_1^2, D) + dim(V(x_1x_2+1, D)) - dim(V(x_1^2, D) \cap V(x_1x_2+1, D)) \\ &\quad = dim(V(x_1^2, D) + dim(V(x_1x_2+1, D)) - dim(V(x_1^2(x_1x_2+1), D) \end{aligned}$$

[2] The largest number D for which the characteristic function is not equal to the corresponding characteristic polynomial is called the *postulation number*. Not much is known about the postulation number in the general cases after 100 years' research.

Then $H(I,0) = H(I,1) = 0$, $H(I,2) = 2, H(I,3) = 2$, and and for $D > 3$, it is easy to see

$$\begin{aligned} H(I,D) &= 2C_{D-2}^{2+D-2} - C_{D-4}^{2+D-4} \\ &= (D^2 + 3D - 6)/2 \\ \chi(I^\natural, D) &= C_D^{2+D} - H(I,D) \\ &= 4 \\ &= \bar{\chi}(I^\natural, D) \end{aligned}$$

Note that the projective variety defined by $x_1^2 = 0, x_1x_2 + x_0^2 = 0$ is the point $(0,0,1)$ at ∞ of degree 4.

■

In the cases of cryptography, we know that $(\ell_1, \cdots, \ell_m)$ has a unique solution (or 0-dimensional) (at finite distance). We have to know the solution set at ∞, i.e., the solution set of the highest homogeneous forms of ℓ_i's. If the solution set at ∞ is 0-dimensional or empty, then $\bar{\chi}(I^\natural, D) =$ constant. It follows from the above discussions that we have the following proposition,

Proposition 2: If the solution set of $(\ell_1, \cdots, \ell_m)$ is 0-dimensional and the solution set at ∞ of $(\ell_1^\natural, \cdots, \ell_m^\natural)$ is 0-dimensional or empty, then the XL program can be solved for D **large enough**.

Proof: Under our assumption, we know that

$$\bar{\chi}(I^\natural, D) = constant = c$$

and for D large enough, we have (by Hilbert-Serre Theorem)

$$\chi(I,D) = \chi(I^\natural, D) = \bar{\chi}(I^\natural, D) = c$$

Therefore for D large enough, we have

$$H(I,D) = C_D^{n+D} - \chi(I,D) = C_D^{n+D} - c > C_D^{n+D} - D - 1$$

■

The above Proposition 2 can not be applied if the intersection at ∞ is 1-dimensional or higher. we may simply construct examples for the purpose of cryptography that the projective dimension of the ideal $I^\natural$ is 1 or higher (the above is routinely done for the TTM encryption systems. In these cases, $\bar{\chi}(I^\natural, D)$ will be a polynomial of degree 1 or higher in D, it is not expected to have $\chi(I,D) \leq D+1$, in other words the number of variables may be always bigger than the number of equations for any D). We shall give an example to show that the XL program fails in some cases,

Example:

(4) Let $I = (x_1^2, x_2 + x_1^2, x_3 + x_1^2) \subset K[x_1, x_2, x_3]$. Then $H(I,0) = H(I,1) = 0$, and for

$D > 1$, it is easy to see

$$\begin{aligned}
H(I,D) &= dim(V(x_1^2,D) + V(x_2+x_1^2,D) + V(x_3+x_1^2,D)) \\
&= dim(V(x_1^2,D) + V(x_2,D-1) + V(x_3,D-1)) \\
&= dim(V(x_1^2,D)) + dim(V(x_2,D-1) + V(x_3,D-1)) \\
&\quad -dim(V(x_1^2,D) \cap (V(x_2,D-1) + V(x_3,D-1)) \\
&= C_3^{D+1} + (2C_3^{D+1} - C_3^D) - (2C_3^{D-1} - C_3^{D-2}) \\
&= C_3^{D+3} - (2D+3) \\
\chi(I^\natural,D) &= C_3^{D+3} - H(I,D) \\
&= 2C_1^D + 3 \\
&= \bar{\chi}(I^\natural,D)
\end{aligned}$$

Note that the projective variety defined by $x_1^2 = 0, x_1^2 + x_0x_2 = 0,\ x_1^2 + x_0x_3$ consists of the origin at the finite distance and a line at ∞ of degree 2. For the present system, **the number of variables is always greater than the number of linearly independent equations**.

■

In this section we show that the XL program can be applied only under restricted condition, namely, the intersection at ∞ is 0-dimensional or empty. The XL program is unlikely to be applicable in general as established by the above Example 4. Certainly to compute the numbers of linearly independent equations is to compute the characteristic functions which are non-trivial. The authors of [2] are interested to locate D such that $\chi(I,D) \leq D+1$ and thus touch a difficult mathematical problem, they are in good company of Hilbert, Serre and others.

3 The Number of Linearly Independent Equations

It will be very nice to have a formula for the characteristic function, $\chi(I,D)$. However we really do not have one. The section 6 of [2] is significant. It is about the "*complexity evaluation of XL*". It begins with "*given m quadratic equations with n variables, we multiply each equation by all possible $x_{i_1}, \cdots, x_{i_{D-2}}$. The number of generated equations is about $\alpha = n^{D-2}/(D-2)! \times m$ while we have about $\beta = n^D/D!$ linear variables.*

If most of the equations are linearly independent in XL (we will comment on this critical hypothesis below), we expect to succeed when $\alpha \geq \beta$, i.e., when

$$m \geq n^2/D(D-1)\text{''}$$

The above statement means that $H(I,D) \approx \alpha = n^{D-2}/(D-2)! \times m$ ($\approx dim(V(\ell_i,D) \times m)$. If the assumption of the above Proposition 2 is satisfied and D is large enough, then we know that the exact value of $H(I,D)$ is $C_D^{n+D} - c$. Let us use the notations of [2] where *free* means the number of linearly independent polynomials and *all* means the number of all polynomials generated by the step (1) of the XL program. Let us consider the ratio $free/all = H(I,D)/(dim(V(\ell_i,D) \times m) \approx (n+D)(n+D-1)/(D(D-1)m) = w$. Note that $w \to 1/m$ as $D \to \infty$. In other words, as D becomes large, only $1/m$ of the generating polynomials are *linearly independent*. In the Appendix of [2], the authors report several simulations (we discard one example with 3 polynomials, because the situation is completely understandable for 3 polynomials (see below)). We will summerize their results in the following table,

D	average($free/all$)	average(w)
4	0.8625247995	1.065608466
5	0.7141313699	0.7857467532
6	0.6146015244	0.6678018278
7	0.5186479545	0.6620370370
10	0.4855932203	0.5055555556
14	0.4181318681	0.4203296703
16	0.3900058275	0.3958333333

The above table shows that most of the equations are **not** linearly independent. Both average($free/all$) and average(w) have a tendency of getting smaller as D getting larger. Moreover, they are getting closer and closer (as expected) as D getting larger. The number of *linearly independent* equations depends on some subtle algebraic geometric property of the original system of equations $\{\ell_1, \cdots, \ell_m\}$. *Simulations* will likely only treat examples of *general types* (i.e., random type) while the practical encryption cases use *special types* and *general types*. Regretly, the ideals $(\ell_1, \cdots, \ell_m)$ are not given explicitly in the simulations.

We know that only $1/m$ of the relations generated by the step (1) of the XL program are linearly independent as $D \to \infty$ which contradict the above quoted statements of the section 6 of [2].

4 A Formula Using Ideal Quotient

We shall prove an exact formula for the number of *linearly independent* equations, $H(I, D)$, for some important cases in this section. For $i = 1, \cdots m-1$, we assume that $\{\ell_1, \cdots, \ell_i\}$ satisfies the following condition (1) with $f, g_j, h_j \in K[x_1, \cdots, x_n]$ and $deg(f) \leq D-2, deg(g_j) \leq D-2, deg(h_j) \leq D-4$;

$$\begin{array}{l} F = \sum_{j=1}^{i-1} g_j \ell_j = f \ell_i \\ \Longleftrightarrow F = \sum_{j=1}^{i-1} h_j \ell_i \ell_j \end{array}$$

The above condition is equivalent to the following,

$$dim(\sum_{j=1}^{i-1} V(\ell_j, D) \cap V(\ell_i, D)) = dim(\sum_{j=1}^{i-1} V(\ell_j, D-2))$$

From the view of algebra, using the standard notion of the *quotient operation for ideals*, ":", the above condition means that,

$$H((\ell_1, \cdots, \ell_{i-1}) : (\ell_i), D) = H((\ell_1, \cdots, \ell_{i-1}), D-2)$$

For the case $i = 1$, the condition is void. For the case $i = 2$, the condition means that ℓ_1, ℓ_2 are co-prime. Let the field K be of 2^k elements. Then the probability of two quadratic polynomials ℓ_1, ℓ_2 being co-prime is

$$1 - (2^{-k(C_2^{n+2}-1)} + 2^{-kn})$$

In general, it is known in the *Advanced Algebra* (cf [5]) that

$$\begin{array}{l} ((\ell_1, \cdots, \ell_{i-1}) : (\ell_i) = (\ell_1, \cdots, \ell_{i-1}) \\ \iff \ell_i \notin \text{all associate primes of } (\ell_1, \cdots, \ell_{i-1}) \end{array}$$

The *associate primes* means the *radicals* of the *primary components* of an ideal $(\ell_1, \cdots, \ell_{i-1})$. The reader is referred to any standard book on *Advanced Algebra* (cf [5]).

For fixed n, m, let $E(D)$ be defined as

$$E(D) = \sum_{1<2s\leq D, s\leq m} (-1)^{s-1} \sum C_s^m C_{D-2s}^{n+D-2s}$$

We have the following proposition.

Proposition 3: Assume that condition (1) is satisfied. We have the following formula

$$H(I, D) = E(D) = \sum_{1<2s\leq D, s\leq m} (-1)^{s-1} \sum C_s^m C_{D-2s}^{n+D-2s}$$

Proof: We shall use the following formula,

$$C_s^m = C_s^{m-1} + C_{s-1}^{m-1}$$

We make an induction on m. If $m = 1$, then the proposition is trivially true. Assume it is true for $m - 1$. Then from the theory of vector spaces, we have

$$\begin{array}{l} H(I, D) = dim(\sum_i^m V(\ell_i, D)) \\ \quad = dim(\sum_i^{m-1} V(\ell_i, D)) + dim(V(\ell_m, D)) - dim((\sum_i^{m-1} V(\ell_i, D)) \cap V(\ell_m, D)) \\ \quad = \sum_{1<2s\leq D, s\leq m-1} (-1)^{s-1} \sum C_s^{m-1} C_{D-2s}^{n+D-2s} + C_{D-2}^{n+D-2} \\ \quad\quad - \sum_{1<2s\leq D-2, s\leq m-1} (-1)^{s-1} \sum C_s^{m-1} C_{D-2-2s}^{n+D-2-2s} \\ \quad = \sum_{1<2s\leq D, s\leq m} (-1)^{s-1} \sum C_s^m C_{D-2s}^{n+D-2s} \\ \quad = E(D) \end{array}$$

■

Remark: Let us consider a simple example of two quadratic polynomial equations (ℓ_1, ℓ_2). Assume that they do not satisfy the condition (1). Let they be $(f_1 f_2, f_1 f_3)$ where f_i are linear, and f_2, f_3 are different (or *non-associative*). Then it is easy to deduce that

$$\begin{array}{l} H(I, D) = 2C_{D-2}^{n+D-2} - C_{D-3}^{n+D-3} \\ \quad < C_1^2 C_{D-2}^{n+D-2} - C_2^2 C_{D-4}^{n+D-4} = E(D) \end{array}$$

Let us discuss the case of three pairwise co-prime polynomials ℓ_1, ℓ_2 and ℓ_3. Let V_1, V_2, V_3 be three subspaces of a vector space. Then we have

$$dim(V_1 + V_2 + V_3) \leq \sum dim(V_i) - \sum dim(V_i \cap V_j) + dim(V_1 \cap V_2 \cap V_3)$$

It follows with $I = (\ell_1, \ell_2, \ell_3)$ the following,

$$H(I, D) \leq E(D)$$

The above inequality indicates that $E(D)$ may be an approximate upper bound, and the exceptional situations are even better. We shall use the numeral $E(D)$ in the Proposition 3 as a reasonable estimate of the number of linearly independent equations in general. ■

The number of variables, $V(D)$, is $C_D^{n+D} - 1$. The XL method is expected to succeed only if $H(I, D) \geq V(D) - D$. The security increases if the number of linearly independent relations decreases, since it may force D to increase to satisfy the preceding inequality.

5 Examples of TTM

For TTM (Tame Transformation Method) encryption system, the reader is referred to [3], [4]. We shall **assume** that the XL program can be applied (cf the section 2). We use three different methods to estimate the value of D and the securities of the systems; (a) assume *all* are linearly independent (this number is far too big as indicated above), i.e., $H(I, D) = mC_{D-2}^{n+D-2}$, (b) assume $H(I, D) = E(D)$, (c) use the data of *average(free/all)* produced by the simulations of [2] which are reproduced in the table of section 1, i.e., take $H(I, D) = average(free/all)mC_{D-2}^{n+D-2}$.

Case (n,m)=(64,100).

We have published an example of $n = 64, m = 100$ in [3], [4].

(a) We have for $D = 8$

$$H(I, D) = 13,111,598,500$$
$$V(D) = 11,969,016,345$$

The above indicates that $D = 8$ is the number by estimate (a). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$(V(8) - 8)^3 = 1,714,649,587,385,499,066,370,388,584,753$$
$$> 1,267,650,600,228,229,401,496,703,205,376 = 2^{100}$$

(b) We have for $D = 13$

$$H(I, D) = 183,770,674,330,425$$
$$V(D) = 183,746,395,242,024$$

The above indicates that $D = 13$ is the number by estimate (b). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(13) - 13)^3 &= 6,203,781,357,716,037,473,832,280,327,979,519,048,545,728 \\ &> 5,575,186,299,632,655,785,383,929,568,162,090,376,495,104 = 2^{142}\end{aligned}$$

(c) We have for $D = 14$

$$\begin{aligned}H(I, D) &= 1.297133644(10^{15}) \\ V(D) &= 1,023,729,916,348,425\end{aligned}$$

The above indicates that $D = 14$ is the number by estimate (c). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(14) - 14)^3 &= 1,072,892,438,362,742,382,488,561,098,371,130,999,562,950,531 \\ &> 713,623,846,352,979,940,529,142,984,724,747,568,191,373,312 = 2^{149}\end{aligned}$$

Case (n,m)=(44,80).

(a) We have for $D = 7$

$$\begin{aligned}H(I, D) &= 152,550,720 \\ V(D) &= 115,775,100\end{aligned}$$

The above indicates that $D = 7$ is the number by estimate (a). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(7) - 7)^3 &= 1,551,834,545,786,703,389,729,357 \\ &> 1,208,925,819,614,629,174,706,176 = 2^{80}\end{aligned}$$

(b) We have for $D = 9$

$$\begin{aligned}H(I, D) &= 4,497,307,860 \\ V(D) &= 4,431,613,549\end{aligned}$$

The above indicates that $D = 9$ is the number by estimate (b). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(9) - 9)^3 &= 87,033,338,288,304,466,637,989,864,000 \\ &> 79,228,162,514,264,337,593,543,950,336 = 2^{96}\end{aligned}$$

(c) We have for $D = 10$

$$\begin{aligned}H(I, D) &= 3.043598740(10^{10}) \\ V(D) &= 23,930,713,170\end{aligned}$$

The above indicates that $D = 10$ is the number by estimate (c). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(10) - 10)^3 &= 13,704,617,654,105,169,568,426,083,078,679 \\ &> 10,141,204,801,825,835,211,973,625,643,008 = 2^{103}\end{aligned}$$

Case (n,m)=(40,72).

(a) We have for $D = 6$

$$\begin{aligned}H(I,D) &= 9,774,072 \\ V(D) &= 9,366,819\end{aligned}$$

The above indicates that $D = 6$ is the number by estimate (a). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(6) - 6)^3 &= 821,817,549,107,599,099,328 \\ &> 590,295,810,358,705,651,712 = 2^{69}\end{aligned}$$

(b) We have for $D = 8$

$$\begin{aligned}H(I,D) &= 377,752,662 \\ V(D) &= 377,348,993\end{aligned}$$

The above indicates that $D = 8$ is the number by estimate (b). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(8) - 8)^3 &= 53,731,573,454,787,752,665,571,625 \\ &> 38,685,626,227,668,133,590,597,632 = 2^{85}\end{aligned}$$

(c) We have for $D = 10$

$$\begin{aligned}H(I,D) &= 1.319314415(10^{10}) \\ V(D) &= 10,272,278,169\end{aligned}$$

The above indicates that $D = 10$ is the number by estimate (c). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(10) - 10)^3 &= 1,083,927,695,025,156,670,560,852,373,679 \\ &> 633,825,300,114,114,700,748,351,602,688 = 2^{99}\end{aligned}$$

Case (n,m)=(20,52) and Quartic Polynomials.

We consider the case that all polynomials $(\ell_1, \cdots, \ell_m)$ are quartic polynomials. In this case we only have the estimate (a), i.e., $H(i,D) = m * C_{D-4}^{n+D-4}$. Then we have

(a) We have for $D = 14$

$$H(I, D) = 1,562,340,780$$
$$V(D) = 1,391,975,639$$

The above indicates that $D = 14$ is the number by estimate (a). As the fast multiplication and fast Gaussian reduction algorithms are only interesting for big $V(D)$ values. The XL attack indicates a complexity of

$$\begin{aligned}(V(14) - 14)^3 &= 2,697,086,598,801,116,767,822,265,625 \\ &> 2,475,880,078,570,760,549,798,248,448 = 2^{91}\end{aligned}$$

In summary, let us **assume** that the XL program can be applied. Even if we assume that all generating polynomials are linearly independent (which has **no** chance of being true, we use it to establish some extreme lower bound of securities) as in item(a) above, the first two and the last encryption system of TTM are strong. With a modest assumption in (b), all four systems of TTM are strong. With the data of the simulations of [2], all four systems of TTM are strong.

It is easy to see that for the *improved XL* of [2], FXL, the complexities are always more in the four examples above.

In general, XL is not effective for many pairs of (n, m) of TTM even for n, m reasonably small, say less than 100.

References

[1] HILBERT, D. *Uber die Theorie der algebraischen Formen.* Math. Annalen vol 36 (1890) 473-534.

[2] COURTOIS, N. SHAMIR, A. PATARIN, J. AND KLIMOV, A. *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations.* Eurocrypt'2000

[3] MOH, T. *A Public Key System with Signature and Master Key Functions.* Communications in Algebra, 27(5), 2207-2222 (1999).

[4] MOH, T. *A Fast Public Key System with Signature and Master Key Functions.* CrypTEC'99.

[5] ZARISKI, O. & SAMUEL, P. *Commutative Algebra,* Vol II. D. Van Nostrand Company, Inc. Princeton, New Jersey, 1960.