Cryptanalysis of Two New Instances of TTM Cryptosystem

Xuyun Nie[1,2], Xin Jiang[2], Lei Hu[2], and Jintai Ding[3]

[1] School of Computer Science and Engineering,
University of Electronic Science and Technology of China,
Chengdu 610054, China
[2] State Key Laboratory of Information Security
Graduate School of Chinese Academy of Sciences
Beijing 100049, China
[3] Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, OH, 45220, USA
nxy7509@sohu.com, { xjiang, hu}@is.ac.cn, ding@math.uc.edu

Abstract. In 2006, Nie et al proposed an attack to break an instance of TTM cryptosystems. However, the inventor of TTM disputed this attack and he proposed two new instances of TTM to support his viewpoint. At this time, he did not give the detail of key construction — the construction of the lock polynomials in these instances which would be used in decryption. The two instances are claimed to achieve a security of 2^{109} against Nie et al attack. In this paper, we show that these instances are both still insecure, and in fact, they do not achieve a better design in the sense that we can find a ciphertext-only attack utilizing the First Order Linearization Equations while for the previous version of TTM, only Second Order Linearization Equations can be used in the beginning stage of the previous attack. Different from previous attacks, we use an iterated linearization method to break these two instances. For any given valid ciphertext, we can find its corresponding plaintext within 2^{31} $\mathbb{F}_{2^8}$-computations after performing once for any public key a computation of complexity less than 2^{44}. Our experiment result shows we have unlocked the lock polynomials after several iterations, though we do not know the detailed construction of lock polynomials.

Keyword: multivariate public key cryptosystem, TTM, algebraic attack, linearization equation, triangular cryptosystem.

1 Introduction

TTM (Tame Transformation Method) is a type of triangular multivariate public key cryptosystems, proposed by T. T. Moh originally in 1999 [Moh99]. Its design idea comes from algebraic geometry, and its central map is the so-called tame transformation which is a core concept in algebraic geometry and is closely related to the famous Jacobian conjecture. TTM is practically very fast for its encryption and decryption operations.

TTM has gone through several cycles of attack and defense. In 2000, Goubin and Courtois claimed that they completely defeated all possible instances (at that time) of TTM schemes using the Minrank method and they demonstrated it by defeating one of the challenges set by the inventors of TTM [GC00]. However, the inventors of TTM refuted the claim and they designed another instance to defense their construction [CM01]. But this new instance has also a defect common among all the existing TTM schemes at that time. Ding and Schmidt pointed out that there exist linearization equations satisfied by the cipher, and they extended the linearization equation attack method to attack this new version [DS03]. In order to resist these attacks, the inventors of TTM proposed a further instance in 2004 [MCY04], and they claimed the security is 2^{148} against the Goubin-Courtois attack. To resist the Ding-Schmidt attack, they incorporated so-called lock polynomials which can not be trivialized by Ding-Schmidt attack. However, this instance of TTM is still broken by the authors of the paper [NHL06]. They pointed out that for this instance in [MCY04] there exist second order linearization equations (SOLEs) satisfied by the cipher, and utilizing this defect, they found a method to "unlock" the lock polynomials, and they then proposed a ciphertext-only attack on the instance, i.e., they can recover the corresponding plaintext for any given ciphertext. They also implemented their attack on a Pentium IV 2.4Ghz PC, and their experiment recovered a plaintext in less than 2 minutes, after a precomputation of less than 95 minutes which is done once for any public key. Similar methods are developed by these authors to further break the other two triangular multivariate public key cryptosystems—-MFE [DHN07] and TRMC-4 [NHD07].

The inventor of TTM disputed the attack in [NHL06] and he think Nie et al attack utilized the construction of private key ϕ_3. And he claimed in his paper [Moh06] that the attack is faulty and to challenge the attackers he then proposed two new instances of TTM [Moh07]. In this paper, the author of TTM did not give the detail of decryption process. This means we do not know how the lock polynomials were designed.

However, through theoretical analysis on the central maps of the two instances, we find both two ciphers satisfy first order linearization equations (FOLES) of form

$$\sum_{i=0}^{n-1} a_i \bar{x}_i + \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} b_{ij}\bar{x}_i F_j + \sum_{j=0}^{m-1} c_j F_j + d = 0,$$

while for the previous version of TTM, only second order linearization equations can be used in the beginning stage of the attack. This means these two instances do not achieve a better design than the previous version. First order linearization equation attack method can be traced back to Patarin in 1995 who defeated the original Matsemoto-Imai scheme [Pat95]. Our computer experiments find that there exist many first order linearization equations satisfied by these two instances and we can find all linearizations equations in 2^{44} $\mathbb{F}_{2^8}$-computations which is precomputation for any given public key. Then for any given valid ciphertext, we can derive a set of linear expressions between the

plaintext variables. Using these expressions, we can do an elimination on the public key. And then, we can use an **iterated linearization method** to find the corresponding plaintext. Our experiments confirmed this point. This means we have unlocked the lock polynomials after several iterations, though we did not know the construction of lock polynomials. And we can not decided in which iteration we unlocked lock polynomials because we did not know the construction of lock polynomials. Note that our attack is a ciphertext-only attack.

The paper is organized as follows. In Section 2 we introduce the basic idea and the two new instances of TTM schemes. Then we first overview our attack on TTM in Section 3, and then give the details of our attack on the new instances in Section 4 and Section 5. Finally in Section 6, we conclude the paper.

2 TTM Cryptosystems

2.1 Basic Idea of TTM Cryptosystems

Let $\mathbb{K}$ be a small finite field. In TTM, it is usually assumed to be the field of 2^8 elements. Generally, TTM systems are constructed by four maps ϕ_1, ϕ_2, ϕ_3, and ϕ_4, where ϕ_1 and ϕ_4 are invertible affine linear maps, ϕ_2 is a tame quadratic transformation, and ϕ_3 is a high degree map using lock polynomials. Their composition $F = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 : \mathbb{K}^n \to \mathbb{K}^m$ is designed to be a set of quadratic polynomials, which is taken as the public key in a TTM system, and the linear maps ϕ_1 and ϕ_4 are taken as the corresponding secret key.

The inventor who is an expert in algebraic geometry uses the concept of tame transformation in algebraic geometry in the design of TTM. The inverting process of a tame transformation is very simple and is also a tame transformation. Tame transformations are maps of the form

$$\begin{aligned} & (y_0, \cdots, y_{m-1}) \\ = \; & J(x_0, \cdots, x_{n-1}) \\ = \; & (x_0, x_1 + q_1(x_0), \cdots, x_{n-1} + q_{n-1}(x_0, \cdots, x_{n-2}), \\ & q_n(x_0, \cdots, x_{n-1}), \cdots, q_{m-1}(x_0, \cdots, x_{n-1})). \end{aligned}$$

A key idea of TTM design is the so-called lock polynomials. Similarly as in the previous version of TTM [MCY04], the inventor of TTM constructed a set of new lock polynomials $G_j(x_0, \cdots, x_{n-1})$ $(j = 0, \cdots, 4)$ in the two new instances of TTM [Moh07]. Then the central maps of the two instances, which are the composition $\phi_3 \circ \phi_2$, become

$$\begin{aligned} & \widetilde{J}(x_0, \cdots, x_{n-1}) \\ = \; & (x_0 + G_0, x_1 + q_1(x_0) + G_1, \cdots, x_4 + q_4(x_0, \cdots, x_4) + G_4, \\ & x_5 + q_5(x_0, \cdots, x_4), \cdots, x_{n-1} + q_{n-1}(x_0, \cdots, x_{n-2}), \\ & q_n(x_0, \cdots, x_{n-1}), \cdots, q_{m-1}(x_0, \cdots, x_{n-1})). \end{aligned}$$

The inventor of TTM ingeniously designed lock polynomials G_i so that they are quadratic polynomials in the x_i, but they are also high degree (> 2) polynomials in the intermediate components, these components are high degree polynomials in the x_i and they are used in the decryption process.

2.2 Two Instances of TTM

Here the encryption map $F : \mathbb{K}^n \to \mathbb{K}^m$ is a composition of the four maps, namely $F = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$:

$$F : \mathbb{K}^n \xrightarrow{\phi_1} \mathbb{K}^n \xrightarrow{\phi_2} \mathbb{K}^m \xrightarrow{\phi_3} \mathbb{K}^m \xrightarrow{\phi_4} \mathbb{K}^m.$$

ϕ_1 and ϕ_4 are invertible affine linear maps, ϕ_2 is a tame quadratic transformation, and ϕ_3 is a high degree map using lock polynomials.

We use $\bar{x}_0, \cdots, \bar{x}_{n-1}$ and $\bar{y}_0, \cdots, \bar{y}_{m-1}$ to denote plaintext and ciphertext components, respectively. The input and output components of the central map are denoted by $x_0, \cdots, x_{n-1}$ and $y_0, \cdots, y_{m-1}$. That is,

$$\begin{aligned}(x_0, \cdots, x_{n-1}) &= \phi_1(\bar{x}_0, \cdots, \bar{x}_{n-1}),\\ (y_0, \cdots, y_{m-1}) &= \phi_3 \circ \phi_2(x_0, \cdots, x_{n-1}),\\ (\bar{y}_0, \cdots, \bar{y}_{m-1}) &= \phi_4(y_0, \cdots, y_{m-1}).\end{aligned}$$

As usual in many multivariate systems, ϕ_1 and ϕ_4 are taken as the private key, while the polynomial expression of the map $(\bar{y}_0, \cdots, \bar{y}_{m-1}) = F(\bar{x}_0, ..., \bar{x}_{n-1})$ is the public key. To encrypt a plaintext $(\bar{x}_0, ..., \bar{x}_{n-1})$ is to evaluate F at it.

The paper [Moh07] did not provide the detail of the decryption process and the construction of lock polynomials. Only the expressions of the composed map $\phi_3 \circ \phi_2$ are given, please see [Moh07] or Appendix A and B in the present paper.

For the first one of the two new instances of TTM, $n = 103$ and $m = 210$; while for the second, $n = 112$ and $m = 215$ [Moh07].

3 Overview of Our Attack

Our attack is a ciphertext-only attack, that means for any valid ciphertext, we will find its corresponding plaintext, namely, given a valid ciphertext $\bar{y} = (\bar{y}'_1, \ldots, \bar{y}'_m)$, we can solve the following system:

$$\begin{cases} F_0(\bar{x}_0, \cdots, \bar{x}_{n-1}) = \bar{y}'_0; \\ \cdots \\ F_{m-1}(\bar{x}_0, \cdots, \bar{x}_{n-1}) = \bar{y}'_{m-1}. \end{cases} \tag{1}$$

It is very hard to directly solve this system. The method we solve it is to use linearization equations. The following are the main phases of our attack.

– Find all high order linearization equations (HOLEs) satisfied by the system. Here a high order linearization equation is illustrated by the following example:

$$\sum_{i=0}^{n-1} a_i \bar{x}_i + \sum_{0 \le j \le k \le m-1} b_{jk} F_j F_k + \sum_{j=0}^{m-1} c_j F_j + d = 0. \tag{2}$$

This equation is a **second order linearization equation (SOLE)**, since it is linear in plaintext components $\bar{x}_i$ and is quadratic in ciphertext components F_j. Many SOLEs exist for the previous instance of TTM, and this results in a starting point for attacking that instance of TTM system [NHL06].

Generally, SOLEs may be of the following complete form:

$$\sum_i \overline{x}_i \left(\sum_{j \le k} a_{ijk} F_j F_k + \sum_j b_{ij} F_j + c_i \right) + \sum_{j \le k} d_{jk} F_j F_k + \sum_j e_j F_j + f = 0, \quad (3)$$

where the coefficients $a_{ijk}, b_{ij}, c_i, d_{jk}, e_j, f \in \mathbb{K}$. This complete type of SOLE is used in the analysis of the MFE cryptosystem [DHN07].

Finding a HOLE means finding its all coefficients. Clearly, all HOLEs form a linear space, finding all HOLEs is to say finding a basis of the space. To this end, we can randomly evaluate a tuple of plaintext components and plug it into the HOLE to get a linear equation on coefficients of a HOLE, since the HOLE is satisfied by all plaintexts. We evaluate sufficiently many tuples to get a system of linear equations on coefficients of HOLEs, and then solve the system by Gaussian elimination to get a basis of the space of solutions. This give a linear independent basis of all HOLEs. Obviously, if we let N be the number of unknown coefficients and r be the dimension of the space of HOLEs, we shall evaluate at least $N - r$ tuples of plaintext components. Generally, to get the desired equation system that contains only correct HOLEs, it is sufficient to randomly evaluate N tuples.

Usually, N is very large (for example, $N = 92659$ for MFE [DHN07] and $N = 6271$ for the previous TTM [NHL06]), the Gaussian elimination for this equation system will be the most time-consuming phase of the attack.

Some earlier cryptosystems even satisfy first order linearization equations (FOLEs), which are of the form:

$$\sum_{i=0}^{n-1} a_i \bar{x}_i + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} b_{ij} \bar{x}_i F_j + \sum_{j=0}^{m-1} c_j F_j + d = 0.$$

These equations are also called the Patarin relations, which are used by Patarin to break the Matsumoto-Imai cryptosystem [Pat95], and are used as a starting point to break the TRMC-4 system [NHD07]. Obviously, it is easier to find FOLEs than SOLEs since there are much fewer unknown coefficients to determine.

This phase can be precomputation, since it is dependent on only public key polynomials and is independent of any valid ciphertext that will be deciphered. It can be done once for any given public key.

– For any given valid ciphertext, substitute its ciphertext component values into all HOLEs (precisely, a basis of HOLEs) which are found in the previous phase. This results in an equation system linear on the corresponding plaintext components, since each HOLE is linear in plaintext components. Solve the system to find linear relations between plaintext components. In other words, some plaintext components can be written as linear expressions in the remaining components. In terminology of cryptanalysis, we have limited the desired plaintext from the whole plaintext space to a subspace.

Substitute the linear expressions of plaintext components into the public key polynomials to get a "reduced" public key expression (it is in fewer unknown plaintext components).

- Further check whether high or first order linearization equations satisfied by the reduced public key exist or not. This is done in a similar way as in the first phase, that is, we select sufficient plaintext/cophertext pairs to plug into the HOLE or FOLE to get a linear system on coefficients of HOLE or FOLE, and then solve it. If nonzero solutions are found, then HOLEs or FOLEs exist, otherwise no HOLE or FOLE exists. In the former case, a further phase as the second phase is continued, and the phases 1 and 2 are repeated till there exists no HOLE or FOLE.

- From the last reduced public key polynomials and the given ciphertext value, if there are some plaintext components are not eliminated, then determine them by some direct methods like Gröbner basis and XL algorithms.

Direct solving requires that the number of the plaintext components left is small. We also note that in this ciphertext-only attack, the second phase and its sequent phases are dependent on the value of the deciphered ciphertext.

For these two new instances of TTM, we find that there are many FOLEs exist in them through theoretical analysis. After performing phases 1 and 2, we can get a "reduced" public key. And then through experiments, we found many FOLEs of form

$$\sum_{i=0}^{n-1} a_i \bar{x}_i + \sum_{j=0}^{m-1} b_j F_j + c = 0 \tag{4}$$

satisfied by the "reduced" public key and we can do iterations for finding FOLEs of form (4) and reducing public key to derive more and more linear expressions of plaintext components. At last iteration, we can get values of one or more remained plaintext variables. Then we substituted these values iterated to the expressions derived previously to get the corresponding plaintext. Through further analysis, we found that if the lock polynomials were unlocked i.e. if we have found an affine subspace W in the plaintext space such that all lock polynomials become constants on W, the iterated linearization method would work. This means our attack actually have unlocked polynomials in a certain iteration, but we can not decide in which iteration the lock polynomials were unlocked because we did not know the detailed design of lock polynomials.

4 Cryptanalysis of New Instance I of TTM

In this section we show how to use the method in the previous section to break the new instance I of TTM and present experimental data.

4.1 First Order Linearization Equations

Unfortunately, this instance satisfies first order linearization equations.

By the central map of instance I, we have

$$\begin{cases} y_{92} = x_{80}x_{86} + x_{82}x_{84} + x_{92}; \\ y_{93} = x_{81}x_{86} + x_{82}x_{85} + x_{93}; \\ y_{94} = x_{83}x_{85} + x_{81}x_{87} + x_{94}; \\ y_{95} = x_{83}x_{84} + x_{80}x_{87} + x_{95}. \end{cases} \tag{5}$$

From them we can derive:

$$\begin{cases} x_{87}y_{92} = x_{80}x_{86}x_{87} + x_{82}x_{84}x_{87} + x_{92}x_{87}; \\ x_{83}y_{93} = x_{81}x_{86}x_{83} + x_{82}x_{85}x_{83} + x_{93}x_{83}; \\ x_{82}y_{94} = x_{83}x_{85}x_{82} + x_{81}x_{87}x_{82} + x_{94}x_{82}; \\ x_{86}y_{95} = x_{83}x_{84}x_{86} + x_{80}x_{87}x_{86} + x_{95}x_{86}. \end{cases} \tag{6}$$

Adding the four equations above, we get

$$\begin{aligned} &x_{87}x_{92} + x_{83}x_{93} + x_{82}x_{94} + x_{86}x_{95} \\ &= x_{87}y_{92} + x_{83}y_{93} + x_{82}y_{94} + x_{86}y_{95} + (x_{81} + x_{84})(x_{83}x_{86} + x_{82}x_{87}). \end{aligned} \tag{7}$$

Since

$$y_3 + x_3 = x_{87}x_{92} + x_{83}x_{93} + x_{82}x_{94} + x_{86}x_{95},$$

and

$$y_{208} = x_{83}x_{86} + x_{82}x_{87},$$

the equation (7) can be changed into

$$y_3 + x_3 = x_{87}y_{92} + x_{83}y_{93} + x_{82}y_{94} + x_{86}y_{95} + (x_{81} + x_{84})y_{208}. \tag{8}$$

This equation (8) is a first order linearization equation. Similarly, we can derive other linearization equations.

Since F is derived from the central map by composing from the inner and outer sides by invertible affine linear maps ϕ_1 and ϕ_4, i.e., $x_i = \phi_{1,i}(\bar{x}_0, \cdots, \bar{x}_{102})$ and $y_j = \phi_{4,j}^{-1}(F_0, \cdots, F_{209})$, each of the FOLEs on x_i and y_i can be changed into an identical equation of the form:

$$\sum_{i=0}^{102} a_i \bar{x}_i + \sum_{i=0}^{102}\sum_{j=0}^{209} b_{ij}\bar{x}_i F_j + \sum_{j=0}^{209} c_j F_j + d = 0, \tag{9}$$

which is satisfied by any $(\bar{x}_0, \cdots, \bar{x}_{102}) \in \mathbb{K}^{103}$.

The number of unknown coefficients a_i, b_{ij}, c_j, and d in equation (9) is equal to

$$103 + 103 \times 210 + 210 + 1 = 21944.$$

To find all FOLEs, we randomly select slightly more than 21944, say 22000, plaintexts $(x_0, \cdots, x_{102})$ and substitute them in (9) to get a system of 22000 linear

equations in 21944 unknowns, and then solve it. Its computational complexity (by a native Gaussian elimination) is less than 2^{44}.

We performed our experiment on a DELL PowerEdge 7250, a minicomputer with 4 Itanium2 CPU and 32GB ECC fully buffered DIMM memory. The operating system we used was 64-bit Windows Server2003. We programmed the attack using VC++. Multiple threads can improve the efficiency of programs on a computer with multiple CPU. In our experiment, we used four threads to deal with Gaussian elimination.

In this instance of TTM, some undetermined quadratic polynomials f_i can be randomly chosen to get different central maps (see Appendix A). In our experiments, we randomly select different ϕ_1, ϕ_4, and f_i to derive 10 different public keys. Our experiments for 10 different public keys show that about 36 hours (36 hours and 15 minutes for one of 10 public keys) were required for this phase, which is done once for a given public key. The experiment finds 50 linear independent FOLEs, namely, the dimension of the $\mathbb{K}$-linear space of all FOLEs of the form (9) is $D = 50$.

Let $\{(a_i^{(\rho)}, b_{ij}^{(\rho)}, c_j^{(\rho)}, d^{(\rho)}), 1 \leq \rho \leq D\}$ be the D coefficient vectors, and the D linearly independent FOLEs are

$$\begin{cases} \sum_{i=0}^{102} a_i^{(\rho)} \bar{x}_i + \sum_{i=0}^{102} \sum_{j=0}^{209} b_{ij}^{(\rho)} \bar{x}_i F_j + \sum_{j=0}^{209} c_j^{(\rho)} F_j + d^{(\rho)} = 0 \\ (1 \leq \rho \leq D) \end{cases} \tag{10}$$

4.2 First Elimination

Now assume we have a valid ciphertext $\bar{y}' = (\bar{y}'_0, \cdots, \bar{y}'_{209})$. Our goal is to find its corresponding plaintext $\bar{x}' = (\bar{x}'_0, \cdots, \bar{x}'_{102})$.

Substituting $(F_1, \cdots, F_{209}) = (\bar{y}'_0, \cdots, \bar{y}'_{209})$ into equation (10), we derive a system of D linear equations in $\bar{x}_i$. Solve it by Gaussian elimination. Let l be the dimension of the space of its solutions. Our experiment finds $l = 40$. That is, we can eliminate 40 plaintext components. Let $\bar{x}_{u'_j}$ be the eliminated components, $\{u'_1, \cdots, u'_l\} \subset \{0, 1, \cdots, 102\}$, and $\bar{x}_{u_i}$ be the remaining components, $\{u_1, \cdots, u_{103-l}\} = \{0, 1, \cdots, 102\} \setminus \{u'_1, \cdots, u'_l\}$, we find linear expressions

$$\bar{x}_{u'_j} = h_j(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{103-l}}), 1 \leq j \leq l. \tag{11}$$

Now substitute (11) into $F_j(\bar{x}_0, \cdots, \bar{x}_{102})$ and derive 210 new quadratic quadratic polynomials $\hat{F}_j(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{103-l}})$ $(0 \leq j \leq 209)$.

4.3 Iterations

Our computer experiments find, for these new quadratic polynomials $\hat{F}_j(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{103-l}})$ $(0 \leq j \leq 209)$, there still exist identical equations of the form

$$\sum_{i=0}^{103-l} \hat{a}_i \bar{x}_{u_i} + \sum_{j=0}^{210} \hat{b}_j \hat{F}_j + \hat{d} = 0, \tag{12}$$

which are satisfied by all $(\bar{x}_{u_1}, \cdots, \bar{x}_{u_{103-l}}) \in K^{103-l}$ and the coefficients $(\hat{b}_0, \cdots, \hat{b}_{210}) \neq (0, \cdots, 0)$.

We use the same method (that derives equations (10)) as in the first phase, we derived all equations of form (12). They are FOLEs in $103 - l$ plaintext components. Then we eliminate several plaintext components. Our experiment showed that the number of eliminated components in this phase relies on the randomly chosen quadratic polynomials f_i.

We further repeat the similar phases of finding FOLEs, eliminating components, and substituting and deriving reduced quadratic polynomials with fewer variables. At last, we derived the plaintext corresponding to the given ciphertext. The computational complexity of all these iterations including the first elimination is less than 2^{31}. Executing these steps is very fast and is less than two minutes.

For any given valid ciphertext, our experiments successfully find the corresponding plaintext.

From experiments, we know that the attack actually unlocked the lock polynomials after several iterations. We also found that if the variables contained in f_i were $x_0, x_1, \ldots, x_j$, $j < i$, then we can eliminate the x_i in some t-th ($t \leq j$) iteration. This is the reason why the number of eliminated components in this phase relies on the randomly chosen quadratic polynomials f_i.

5 Cryptanalysis of Instance II

We used the same method to break the instance II. First, we show algebraically why this instance satisfies first order linearization equations.

By the central map of instance II, we have

$$\begin{cases} y_{100} = x_{95}x_{89} + x_{91}x_{93} + x_{100}; \\ y_{102} = x_{90}x_{95} + x_{91}x_{94} + x_{102}; \\ y_{103} = x_{92}x_{94} + x_{90}x_{96} + x_{103}; \\ y_{104} = x_{92}x_{93} + x_{89}x_{96} + x_{104}. \end{cases} \tag{13}$$

From them we can derive

$$\begin{cases} x_{96}y_{100} = x_{96}x_{95}x_{89} + x_{96}x_{91}x_{93} + x_{96}x_{100}; \\ x_{92}y_{102} = x_{92}x_{90}x_{95} + x_{92}x_{91}x_{94} + x_{92}x_{102}; \\ x_{91}y_{103} = x_{91}x_{92}x_{94} + x_{91}x_{90}x_{96} + x_{91}x_{103}; \\ x_{95}y_{104} = x_{95}x_{92}x_{93} + x_{95}x_{89}x_{96} + x_{95}x_{104}. \end{cases} \tag{14}$$

Adding the four above equations, we get

$$\begin{aligned} &x_{96}x_{100} + x_{92}x_{102} + x_{91}x_{103} + x_{95}x_{104} \\ &= x_{96}y_{100} + x_{92}y_{102} + x_{91}y_{103} + x_{95}x_{104} + (x_{90} + x_{93})(x_{91}x_{96} + x_{92}x_{95}). \end{aligned} \tag{15}$$

Since

$$y_1 + x_1 = x_{96}x_{100} + x_{92}x_{102} + x_{91}x_{103} + x_{95}x_{104},$$

and

$$y_{213} = x_{91}x_{96} + x_{92}x_{95},$$

equation (15) can be changed into

$$y_1 + x_1 = x_{96}y_{100} + x_{92}y_{102} + x_{91}y_{103} + x_{95}x_{104} + (x_{90} + x_{93})y_{213}. \quad (16)$$

This equation is a first order linearization equation. We use the same method as instance I to derive the basis of the space of all FOLEs. In this case, the number of unknown coefficients is equal to

$$112 + 112 \times 215 + 215 + 1 = 24408.$$

The computational complexity of finding all FOLEs is less than 2^{44}. We performed our experiment for 10 different public keys on the same DELL PowerEdge 7250 and used the same programming technique.

Our experiments showed that about 53 hours (2 days and 5 hours) were required for this Gaussian elimination phase (concretely, 53 hours and 7 minutes for one of 10 public keys). Our experiments show that $D = 242$ and after we substituted the given ciphertext, $l = 86$, so we can eliminate 86 plaintext components and only $112 - 86 = 26$ plaintext components are left.

In the sequent iterations, we only need two iterations. In the first iteration, we eliminated 22 plaintext components and we left 4 components to the second iteration to get their values. The computational complexity of these iterations is less then 2^{26}, in our experiment, it is less than one minute.

For any given valid ciphertext, our experiments successfully find the corresponding plaintext.

6 Conclusion

Using first order linearization equations, we broke the two instances of TTM public key cryptosystem recently proposed by Prof. T. T. Moh in the paper [Moh07]. We have done experiments to confirm our attack of finding the corresponding plaintext for any given valid ciphertext. Our experiments showed the second of the two instances are easier to break than the first. These two new instances do not achieve better design than the previous instance of TTM in 2004.

References

[CM01] J.Chen and T.Moh. On the Goubin-Courtois attack on TTM. *Cryptology ePrint Archive*, 72, 2001. http://eprint.iacr.org/2001/072.

[DS03] J.Ding and D.Schmidt. The new TTM implementation is not secure. In H.Niederreiter K.Q.Feng and C.P. Xing, editors, *Proceedings of International Workshop on Coding, Cryptography and Combinatorics (CCC 2003)*, pages 106–121, 2003.

[GC00] L.Goubin and N.Courtois. Cryptanalysis of the TTM cryptosystem. *LNCS, Springer Verlag*, 1976:44–57, 2000.

[Moh99] T.Moh. A fast public key system with signature and master key functions. *Lecture Notes at EE department of Stanford University.*, May 1999. http://www.usdsi.com/ttm.html.

[Moh06] T.Moh. The Recent Attack of Nie et al On TTM is Faulty. http://eprint.iacr.org/2006/417.

[Moh07] T.Moh. Two New Examples of TTM. http://eprint.iacr.org/2007/144.

[MCY04] T.Moh and J.Chen and B.Yang. Building Instances of TTM Immune to the Goubin-Courtois Attack andthe Ding-Schmidt Attack. IACR eprint 2004/168, http://eprint.iacr.org.

[NHL06] X.Nie, L.Hu, J.Li, C.Updegrove and J.Ding. Breaking A New Instance of TTM Cryptosystem. *Advances in ACNS2006, LNCS*, volume 3989, Springer, 2006.

[Pat95] J.Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In D.Coppersmith, editor, *Advances in Cryptology – Crypto'95, LNCS*, volume 963, pages 248–261, 1995.

[DHN07] Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li and John Wagner. High Order Linearization Equation(HOLE) Attack on Multivariate Public Key Cryptosystems. *The International Workshop on Practice and Theory in Public Key Cryptography (PKC'07), LNCS*, volume 4450, pages 233–248, 2007.

[NHD07] Xuyun Nie, Lei Hu, Jintai Ding, Jianyu Li, and John Wagner. Cryptanalysis of TRMC-4 Public Key Cryptosystem. *The International Workshop on Applied Cryptography and Network Security (ACNS'2007), LNCS*, volume 4521, pages 104–115, 2007.

Appendix A: Expression of the Central Map of Instance I

The expressions of $(y_0, \cdots, y_{209}) = \phi_3 \circ \phi_2(x_0, \cdots, x_{102})$ are listed as follows, where $f_i(x_0, \cdots, x_{i-1})$ $(1 \leq i \leq 102)$ are randomly chosen quadratic polynomials. In our experiment, we found some mistakes exist in these expressions in the original paper [Moh07]. We think the expressions $y_{16} = f_{16} + x_5$, $y_{17} = f_{17} + x_6$, and $y_{18} = f_{18} + x_7$ should be $y_{16} = f_{16} + x_{16}$, $y_{17} = f_{17} + x_{17}$, and $y_{18} = f_{18} + x_{18}$, respectively.

$y_0 = x_4x_3 + x_1x_2 + x_0$;
$y_1 = x_{55}x_{60} + x_{51}x_{61} + x_{50}x_{62} + x_{54}x_{63} + x_1$;
$y_2 = x_{71}x_{76} + x_{67}x_{77} + x_{66}x_{78} + x_{70}x_{79} + x_2$;
$y_3 = x_{87}x_{92} + x_{83}x_{93} + x_{82}x_{94} + x_{86}x_{95} + x_3$;
$y_4 = x_{39}x_{44} + x_{35}x_{45} + x_{34}x_{46} + x_{38}x_{47} + x_4$;
$y_5 = f_5 + x_5$;
$y_6 = f_6 + x_6$;
$y_7 = f_7 + x_7$;
$y_8 = f_8 + x_8$;
$y_9 = f_9 + x_9$;
$y_{10} = f_{10} + x_{10}$;
$y_{11} = x_4x_5 + x_1x_0 + x_8 + x_{11}$;
$y_{12} = f_{12} + x_{12}$;
$y_{13} = f_{13} + x_{13}$;
$y_{14} = f_{14} + x_{14}$;
$y_{15} = f_{15} + x_{15}$;
$y_{16} = f_{16} + x_5$;
$y_{17} = f_{17} + x_6$;
$y_{18} = f_{18} + x_7$;
$y_{19} = x_4x_{17} + x_2x_{15} + x_{19}$;
$y_{20} = x_1x_{17} + x_2x_{16} + x_{20}$;
$y_{21} = x_{14}x_5 + x_{13}x_7 + x_{21}$;
$y_{22} = x_{14}x_0 + x_{12}x_7 + x_{22}$;
$y_{23} = f_{23} + x_{23}$;
$y_{24} = x_{12}x_5 + x_{13}x_0 + x_{24} + x_{11}$;
$y_{25} = f_{25} + x_{25}$;
$y_{26} = f_{26} + x_{26}$;
$y_{27} = x_{12}x_{16} + x_{13}x_{15} + x_{24} + x_{27}$;

$$y_{28} = x_{12}x_{17} + x_{18}x_{15} + x_{28};$$
$$y_{29} = x_{13}x_{17} + x_{18}x_{16} + x_{29};$$
$$y_{30} = x_{14}x_{16} + x_{13}x_{23} + x_{30};$$
$$y_{31} = x_{14}x_{15} + x_{12}x_{23} + x_{31};$$
$$y_{32} = f_{32} + x_{32};$$
$$y_{33} = f_{33} + x_{33};$$
$$y_{34} = f_{34} + x_{34};$$
$$y_{35} = f_{35} + x_{35};$$
$$y_{36} = f_{36} + x_{36};$$
$$y_{37} = f_{37} + x_{37};$$
$$y_{38} = f_{38} + x_{38};$$
$$y_{39} = f_{39} + x_{39};$$
$$y_{40} = f_{40} + x_{40};$$
$$y_{41} = f_{41} + x_{41};$$
$$y_{42} = f_{42} + x_{42};$$
$$y_{43} = x_{32}x_{37} + x_{33}x_{36} + x_{40} + x_{43};$$
$$y_{44} = x_{32}x_{38} + x_{34}x_{36} + x_{44};$$
$$y_{45} = x_{33}x_{38} + x_{34}x_{37} + x_{45};$$
$$y_{46} = x_{35}x_{37} + x_{33}x_{39} + x_{46};$$
$$y_{47} = x_{35}x_{36} + x_{32}x_{39} + x_{47};$$
$$y_{48} = f_{48} + x_{48};$$
$$y_{49} = f_{49} + x_{49};$$
$$y_{50} = f_{50} + x_{50};$$
$$y_{51} = f_{51} + x_{51};$$
$$y_{52} = f_{52} + x_{52};$$
$$y_{53} = f_{53} + x_{53};$$
$$y_{54} = f_{54} + x_{54};$$
$$y_{55} = f_{55} + x_{55};$$
$$y_{56} = f_{56} + x_{56};$$
$$y_{57} = f_{57} + x_{57};$$
$$y_{58} = f_{58} + x_{58};$$
$$y_{59} = x_{48}x_{53} + x_{49}x_{52} + x_{56} + x_{59};$$
$$y_{60} = x_{48}x_{54} + x_{50}x_{52} + x_{60};$$
$$y_{61} = x_{49}x_{54} + x_{50}x_{53} + x_{61};$$
$$y_{62} = x_{51}x_{53} + x_{49}x_{55} + x_{62};$$
$$y_{63} = x_{51}x_{52} + x_{48}x_{55} + x_{63};$$
$$y_{64} = f_{64} + x_{64};$$
$$y_{65} = f_{65} + x_{65};$$
$$y_{66} = f_{66} + x_{66};$$
$$y_{67} = f_{67} + x_{67};$$
$$y_{68} = f_{68} + x_{68};$$
$$y_{69} = f_{69} + x_{69};$$
$$y_{70} = f_{70} + x_{70};$$
$$y_{71} = f_{71} + x_{71};$$
$$y_{72} = f_{72} + x_{72};$$
$$y_{73} = f_{73} + x_{73};$$
$$y_{74} = f_{74} + x_{74};$$
$$y_{75} = x_{64}x_{69} + x_{65}x_{68} + x_{72} + x_{75};$$
$$y_{76} = x_{64}x_{70} + x_{66}x_{68} + x_{76};$$
$$y_{77} = x_{65}x_{70} + x_{66}x_{69} + x_{77};$$
$$y_{78} = x_{67}x_{69} + x_{65}x_{71} + x_{78};$$
$$y_{79} = x_{67}x_{68} + x_{64}x_{71} + x_{79};$$
$$y_{80} = f_{80} + x_{80};$$
$$y_{81} = f_{81} + x_{81};$$
$$y_{82} = f_{82} + x_{82};$$
$$y_{83} = f_{83} + x_{83};$$
$$y_{84} = f_{84} + x_{84};$$
$$y_{85} = f_{85} + x_{85};$$
$$y_{86} = f_{86} + x_{86};$$
$$y_{87} = f_{87} + x_{87};$$
$$y_{88} = f_{88} + x_{88};$$
$$y_{89} = f_{89} + x_{89};$$
$$y_{90} = f_{90} + x_{90};$$
$$y_{91} = x_{80}x_{85} + x_{81}x_{84} + x_{88} + x_{91};$$
$$y_{92} = x_{80}x_{86} + x_{82}x_{84} + x_{92};$$
$$y_{93} = x_{81}x_{86} + x_{82}x_{85} + x_{93};$$
$$y_{94} = x_{83}x_{85} + x_{81}x_{87} + x_{94};$$
$$y_{95} = x_{83}x_{84} + x_{80}x_{87} + x_{95};$$
$$y_{96} = f_{96} + x_{96};$$
$$y_{97} = f_{97} + x_{97};$$
$$y_{98} = f_{98} + x_{98};$$
$$y_{99} = f_{99} + x_{99};$$
$$y_{100} = f_{100} + x_{100};$$
$$y_{101} = f_{101} + x_{101};$$
$$y_{102} = f_{102} + x_{102};$$
$$y_{103} = x_4x_6 + x_0x_{30} + x_{14};$$
$$y_{104} = x_1x_6 + x_{30}x_5 + x_{10};$$
$$y_{105} = x_{23}x_5 + x_1x_7 + x_{21};$$
$$y_{106} = x_0x_{23} + x_4x_7 + x_{22};$$
$$y_{107} = x_4x_{16} + x_1x_{15} + x_8 + x_{27};$$
$$y_{108} = x_3x_{16} + x_1x_{23} + x_{30};$$
$$y_{109} = x_3x_{15} + x_{23}x_4 + x_{31};$$
$$y_{110} = x_{12}x_6 + x_{18}x_0 + x_{28};$$
$$y_{111} = x_{13}x_6 + x_{18}x_5 + x_{29};$$
$$y_{112} = x_{20}x_{17} + x_{19}x_{18} + x_2 + x_{29};$$
$$y_{113} = x_{20}x_{23} + x_8x_{18} + x_1;$$
$$y_{114} = x_{19}x_{23} + x_8x_{17} + x_4;$$
$$y_{115} = x_{10}x_{17} + x_{19}x_{14} + x_{30};$$
$$y_{116} = x_{10}x_{18} + x_{20}x_{14} + x_{31};$$
$$y_{117} = x_4x_{20} + x_1x_{19} + x_2x_8 + x_3x_{10};$$
$$y_{118} = x_0x_{21} + x_5x_{22} + x_6x_9 + x_7x_{11};$$
$$y_{119} = x_{10}x_0 + x_{14}x_5 + x_6x_8 + x_7x_{31};$$
$$y_{120} = x_4x_{21} + x_1x_{22} + x_{30}x_9 + x_{23}x_{11};$$
$$y_{121} = x_{10}x_{22} + x_{14}x_{21};$$
$$y_{122} = x_{10}x_9 + x_8x_{21} + x_7;$$
$$y_{123} = x_{14}x_9 + x_8x_{22} + x_{23};$$
$$y_{124} = x_{31}x_{22} + x_{14}x_{11} + x_{30};$$
$$y_{125} = x_{31}x_9 + x_8x_{11} + x_1 + x_0;$$
$$y_{126} = x_{23}x_6 + x_{30}x_7;$$
$$y_{127} = x_{31}x_{21} + x_{10}x_{11} + x_6;$$

$$y_{128} = x_{15}x_{29} + x_{16}x_{28} + x_{17}x_{24} + x_{23}x_{26};$$
$$y_{129} = x_{12}x_{30} + x_{13}x_{31} + x_{18}x_{25} + x_{14}x_{27};$$
$$y_{130} = x_{29}x_{31} + x_{28}x_{30};$$
$$y_{131} = x_{29}x_{25} + x_{24}x_{30} + x_{23};$$
$$y_{132} = x_{28}x_{25} + x_{24}x_{31} + x_{14};$$
$$y_{133} = x_{26}x_{31} + x_{28}x_{27} + x_{18};$$
$$y_{134} = x_{26}x_{25} + x_{24}x_{27} + x_{13} + x_{15};$$
$$y_{135} = x_{14}x_{17} + x_{18}x_{23};$$
$$y_{136} = x_{26}x_{30} + x_{29}x_{27} + x_{17};$$
$$y_{137} = x_{15}x_{20} + x_{16}x_{19} + x_{8}x_{17} + x_{23}x_{10};$$
$$y_{138} = x_{30}x_{4} + x_{1}x_{31} + x_{2}x_{25} + x_{3}x_{27};$$
$$y_{139} = x_{20}x_{31} + x_{19}x_{30};$$
$$y_{140} = x_{20}x_{25} + x_{8}x_{30} + x_{23};$$
$$y_{141} = x_{19}x_{25} + x_{8}x_{31} + x_{3};$$
$$y_{142} = x_{10}x_{31} + x_{19}x_{27} + x_{2};$$
$$y_{143} = x_{10}x_{25} + x_{8}x_{27} + x_{1} + x_{15};$$
$$y_{144} = x_{3}x_{17} + x_{2}x_{23};$$
$$y_{145} = x_{10}x_{30} + x_{20}x_{27} + x_{17};$$
$$y_{146} = x_{19}x_{23} + x_{3}x_{20} + x_{2}x_{30} + x_{17}x_{31};$$
$$y_{147} = x_{28}x_{7} + x_{14}x_{29} + x_{18}x_{21} + x_{6}x_{22};$$
$$y_{148} = x_{0}x_{29} + x_{5}x_{28} + x_{6}x_{24} + x_{7}x_{26};$$
$$y_{149} = x_{12}x_{21} + x_{13}x_{22} + x_{18}x_{9} + x_{14}x_{11};$$
$$y_{150} = x_{29}x_{22} + x_{28}x_{21};$$
$$y_{151} = x_{29}x_{9} + x_{24}x_{21} + x_{7};$$
$$y_{152} = x_{28}x_{9} + x_{24}x_{22} + x_{14};$$
$$y_{153} = x_{26}x_{22} + x_{28}x_{11} + x_{18};$$
$$y_{154} = x_{26}x_{9} + x_{24}x_{11} + x_{13} + x_{0};$$
$$y_{155} = x_{14}x_{6} + x_{18}x_{7};$$
$$y_{156} = x_{26}x_{21} + x_{29}x_{11} + x_{6};$$
$$y_{157} = x_{18}x_{4} + x_{1}x_{17} + x_{2}x_{23} + x_{14}x_{3};$$
$$y_{158} = x_{20}x_{30} + x_{19}x_{31} + x_{8}x_{28} + x_{10}x_{29};$$
$$y_{159} = x_{4}x_{31} + x_{1}x_{30};$$
$$y_{160} = x_{4}x_{28} + x_{2}x_{30} + x_{14};$$
$$y_{161} = x_{1}x_{28} + x_{2}x_{31} + x_{10};$$
$$y_{162} = x_{3}x_{31} + x_{1}x_{29} + x_{8};$$
$$y_{163} = x_{3}x_{28} + x_{2}x_{29} + x_{19} + x_{18};$$
$$y_{164} = x_{23}x_{10} + x_{8}x_{14};$$
$$y_{165} = x_{3}x_{30} + x_{4}x_{29} + x_{23};$$
$$y_{166} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{32}x_{45} + x_{33}x_{44} + x_{34}x_{40} + x_{35}x_{42};$$
$$y_{167} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{36}x_{46} + x_{37}x_{47} + x_{38}x_{41} + x_{39}x_{43};$$
$$y_{168} = x_{36}x_{45} + x_{37}x_{44} + x_{38}x_{40} + x_{39}x_{42};$$
$$y_{169} = x_{32}x_{46} + x_{33}x_{47} + x_{34}x_{41} + x_{35}x_{43};$$
$$y_{170} = x_{45}x_{47} + x_{44}x_{46};$$
$$y_{171} = x_{45}x_{41} + x_{40}x_{46} + x_{39};$$
$$y_{172} = x_{44}x_{41} + x_{40}x_{47} + x_{35};$$
$$y_{173} = x_{42}x_{47} + x_{44}x_{43} + x_{34};$$
$$y_{174} = x_{42}x_{41} + x_{40}x_{43} + x_{33} + x_{36};$$
$$y_{175} = x_{35}x_{38} + x_{34}x_{39};$$
$$y_{176} = x_{42}x_{46} + x_{45}x_{43} + x_{38};$$
$$y_{177} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{48}x_{61} + x_{49}x_{60} + x_{50}x_{56} + x_{51}x_{58};$$
$$y_{178} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{52}x_{62} + x_{53}x_{63} + x_{54}x_{57} + x_{55}x_{59};$$
$$y_{179} = x_{52}x_{61} + x_{53}x_{60} + x_{54}x_{56} + x_{55}x_{58};$$
$$y_{180} = x_{48}x_{62} + x_{49}x_{63} + x_{50}x_{57} + x_{51}x_{59};$$
$$y_{181} = x_{61}x_{63} + x_{60}x_{62};$$
$$y_{182} = x_{61}x_{57} + x_{56}x_{62} + x_{55};$$
$$y_{183} = x_{60}x_{57} + x_{56}x_{63} + x_{51};$$
$$y_{184} = x_{58}x_{63} + x_{60}x_{59} + x_{50};$$
$$y_{185} = x_{58}x_{57} + x_{56}x_{59} + x_{49} + x_{52};$$
$$y_{186} = x_{51}x_{54} + x_{50}x_{55};$$
$$y_{187} = x_{58}x_{62} + x_{61}x_{59} + x_{54};$$
$$y_{188} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{64}x_{77} + x_{65}x_{76} + x_{66}x_{72} + x_{67}x_{74};$$
$$y_{189} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{68}x_{78} + x_{69}x_{79} + x_{70}x_{73} + x_{71}x_{75};$$
$$y_{190} = x_{68}x_{77} + x_{69}x_{76} + x_{70}x_{72} + x_{71}x_{74};$$
$$y_{191} = x_{64}x_{78} + x_{65}x_{79} + x_{66}x_{73} + x_{67}x_{75};$$
$$y_{192} = x_{77}x_{79} + x_{76}x_{78};$$
$$y_{193} = x_{77}x_{73} + x_{72}x_{78} + x_{71};$$
$$y_{194} = x_{76}x_{73} + x_{72}x_{79} + x_{67};$$
$$y_{195} = x_{74}x_{79} + x_{76}x_{75} + x_{66};$$
$$y_{196} = x_{74}x_{73} + x_{72}x_{75} + x_{65} + x_{68};$$
$$y_{197} = x_{67}x_{70} + x_{66}x_{71};$$
$$y_{198} = x_{74}x_{78} + x_{77}x_{75} + x_{70};$$
$$y_{199} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$y_{200} = x_{14}x_{7} + x_{23}x_{10} + x_{30}x_{21} + x_{6}x_{22}$$
$$+x_{80}x_{93} + x_{81}x_{92} + x_{82}x_{88} + x_{83}x_{90};$$
$$+x_{84}x_{94} + x_{85}x_{95} + x_{86}x_{89} + x_{87}x_{91};$$
$$y_{201} = x_{84}x_{93} + x_{85}x_{92} + x_{86}x_{88} + x_{87}x_{90};$$
$$y_{202} = x_{80}x_{94} + x_{81}x_{95} + x_{82}x_{89} + x_{83}x_{91};$$
$$y_{203} = x_{93}x_{95} + x_{92}x_{94};$$
$$y_{204} = x_{93}x_{89} + x_{88}x_{94} + x_{87};$$
$$y_{205} = x_{92}x_{89} + x_{88}x_{95} + x_{83};$$
$$y_{206} = x_{90}x_{95} + x_{92}x_{91} + x_{82};$$
$$y_{207} = x_{90}x_{89} + x_{88}x_{91} + x_{81} + x_{84};$$
$$y_{208} = x_{83}x_{86} + x_{82}x_{87};$$
$$y_{209} = x_{90}x_{94} + x_{93}x_{91} + x_{86};$$

Appendix B: Expression of the Central Map of Instance II

The expressions of $(y_0, \cdots, y_{214}) = \phi_3 \circ \phi_2(x_0, \cdots, x_{111})$ are listed as follows. In these expressions in the original paper [Moh07], the expression on y_{108} is missed. So, in our experiments, we set $y_{108} = f(x_0, \cdots, x_{107}) + x_{108}$, where f is a randomly chosen quadratic polynomial.

$y_0 = x_1x_4 + x_2x_3 + x_0$;
$y_1 = x_{96}x_{100} + x_{92}x_{102} + x_{91}x_{103} + x_{95}x_{104} + x_1$;
$y_2 = x_{80}x_{85} + x_{76}x_{86} + x_{75}x_{87} + x_{79}x_{88} + x_2$;
$y_3 = x_{64}x_{69} + x_{60}x_{70} + x_{59}x_{71} + x_{63}x_{72} + x_1x_2 + x_3$;
$y_4 = x_{48}x_{53} + x_{44}x_{54} + x_{43}x_{55} + x_{47}x_{56} + x_1x_3 + x_2x_3 + x_4$;
$y_5 = x_0x_4 + x_1x_2 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3 + x_5$;
$y_6 = x_5x_0 + x_1x_4 + x_2x_3 + x_5x_1 + x_2x_4 + x_6$;
$y_7 = x_6x_0 + x_5x_1 + x_3x_4 + x_2x_6 + x_5x_4 + x_7$;
$y_8 = x_7x_1 + x_2x_6 + x_5x_3 + x_4x_7 + x_3x_6 + x_8$;
$y_9 = x_8x_0 + x_7x_2 + x_6x_4 + x_5x_1 + x_4x_7 + x_9$;
$y_{10} = x_9x_0 + x_8x_1 + x_7x_2 + x_3x_6 + x_5x_4 + x_{10}$;
$y_{11} = x_6x_{10} + x_7x_9 + x_6 + x_9 + x_{10} + x_{11}$;
$y_{12} = x_5x_{10} + x_7x_8 + x_5 + x_8 + x_{10} + x_{12}$;
$y_{13} = x_5x_9 + x_8x_6 + x_8 + x_9 + x_{13}$;
$y_{14} = x_{13}x_8 + x_{12}x_9 + x_{11}x_{10} + x_{13}x_{11} + x_{12}x_7 + x_{14}$;
$y_{15} = x_{14}x_4 + x_{13}x_5 + x_{12}x_6 + x_{11}x_7 + x_{10}x_8 + x_{15}$;
$y_{16} = x_{15}x_{14} + x_{13}x_{12} + x_{11}x_{10} + x_9x_8 + x_7x_6 + x_{16}$;
$y_{17} = x_{16}x_{15} + x_{14}x_5 + x_{13}x_6 + x_{12}x_7 + x_{11}x_8 + x_{17}$;
$y_{18} = x_{17}x_5 + x_{16}x_{10} + x_{15}x_{11} + x_{14}x_{12} + x_{13}x_6 + x_{18}$;
$y_{19} = x_{18}x_4 + x_{17}x_6 + x_{16}x_8 + x_{15}x_{10} + x_{14}x_{12} + x_{19}$;
$y_{20} = x_{19}x_7 + x_{18}x_9 + x_{17}x_{11} + x_{16}x_{13} + x_{15}x_8 + x_{20}$;
$y_{21} = x_{20}x_{16} + x_{19}x_{14} + x_{18}x_{12} + x_{17}x_{10} + x_{16}x_8 + x_{21}$;
$y_{22} = x_{21}x_8 + x_{20}x_9 + x_{19}x_{10} + x_{18}x_{11} + x_{17}x_{12} + x_{22}$;
$y_{23} = x_{18}x_{22} + x_{19}x_{21} + x_{18} + x_{21} + x_{22} + x_{23}$;
$y_{24} = x_{17}x_{22} + x_{19}x_{20} + x_{17} + x_{20} + x_{22} + x_{24}$;
$y_{25} = x_{17}x_{21} + x_{20}x_{18} + x_{20} + x_{21} + x_{25}$;
$y_{26} = x_{25}x_{11} + x_{24}x_{12} + x_{23}x_{13} + x_{22}x_{14} + x_{26}$;
$y_{27} = x_{26}x_5 + x_{25}x_7 + x_{24}x_9 + x_{23}x_{11} + x_{22}x_{13} + x_{27}$;
$y_{28} = x_{27}x_6 + x_{26}x_8 + x_{25}x_{10} + x_{24}x_{12} + x_{23}x_{14} + x_{28} + x_{27} + x_{26}$;
$y_{29} = x_{28}x_5 + x_{27}x_7 + x_{26}x_9 + x_{25}x_{11} + x_{24}x_{13} + x_{29} + x_{21} + x_{22}$;
$y_{30} = x_{29}x_{15} + x_{28}x_{16} + x_{27}x_{17} + x_{26}x_{18} + x_{25}x_{19} + x_{24}x_{18} + x_{30}$;
$y_{31} = x_{30}x_{17} + x_{28}x_{18} + x_{26}x_{19} + x_{24}x_{20} + x_{22}x_{21} + x_{23}x_6 + x_{31} + x_{30} + x_{29}$;
$y_{32} = x_{31}x_7 + x_{30}x_8 + x_{29}x_9 + x_{28}x_{10} + x_{27}x_{11} + x_{26}x_{12} + x_{25}x_{13} + x_{32} + x_{27} + x_{23}$;
$y_{33} = x_{32}x_5 + x_{31}x_6 + x_{30}x_7 + x_{29}x_{14} + x_{28}x_{15} + x_{27}x_{16} + x_{26}x_{17} + x_{33} + x_5 + x_6$;
$y_{34} = x_{33}x_{20} + x_{32}x_{19} + x_{31}x_{18} + x_{30}x_{17} + x_{29}x_{16} + x_{28}x_{15} + x_{34} + x_4 + x_{10} + x_{11}$;
$y_{35} = x_{30}x_{22} + x_{31}x_{21} + x_{30} + x_{21} + x_{22} + x_{35}$;
$y_{36} = x_{29}x_{22} + x_{31}x_{20} + x_{29} + x_{20} + x_{22} + x_{36}$;
$y_{37} = x_{29}x_{21} + x_{20}x_{30} + x_{20} + x_{21} + x_{37}$;
$y_{38} = x_{33}x_7 + x_{34}x_6 + x_6 + x_{33} + x_{34} + x_{38}$;
$y_{39} = x_{32}x_7 + x_{34}x_5 + x_5 + x_{32} + x_{34} + x_{39}$;
$y_{40} = x_{32}x_6 + x_5x_{33} + x_{32} + x_{33} + x_{40}$;
$y_{41} = x_{40}x_1 + x_{39}x_3 + x_{38}x_5 + x_{37}x_7 + x_{36}x_9 + x_{35}x_{11} + x_{41} + x_{40} + x_{39}$;
$y_{42} = x_{41}x_2 + x_{40}x_4 + x_{39}x_6 + x_{38}x_8 + x_{37}x_{10} + x_{36}x_{12} + x_{42} + x_{38} + x_{37}$;

$$y_{43} = x_{42}x_{13} + x_{41}x_{15} + x_{40}x_{17} + x_{39}x_{19} + x_{38}x_{21} + x_{37}x_{23} + x_{43};$$
$$y_{44} = x_{43}x_{14} + x_{42}x_{26} + x_{41}x_{18} + x_{40}x_{20} + x_{39}x_{22} + x_{38}x_{24} + x_{44} + x_{43} + x_3;$$
$$y_{45} = x_{44}x_{25} + x_{43}x_{27} + x_{42}x_{29} + x_{41}x_{31} + x_{40}x_{33} + x_{39}x_{35} + x_{45} + x_8 + x_6;$$
$$y_{46} = x_{45}x_{26} + x_{44}x_{28} + x_{43}x_{30} + x_{42}x_{32} + x_{41}x_{34} + x_{40}x_{36} + x_{46} + x_{40} + x_{39};$$
$$y_{47} = x_{46}x_1 + x_{45}x_4 + x_{44}x_7 + x_{43}x_{10} + x_{42}x_{13} + x_{41}x_{16} + x_{40}x_{19} + x_{47} + x_3 + x_7;$$
$$y_{48} = x_{47}x_2 + x_{46}x_5 + x_{45}x_8 + x_{44}x_{11} + x_{43}x_{14} + x_{42}x_{17} + x_{41}x_{20} + x_{48} + x_{47} + x_{38};$$
$$y_{49} = x_{48}x_3 + x_{47}x_6 + x_{46}x_9 + x_{45}x_{12} + x_{44}x_{15} + x_{43}x_{18} + x_{42}x_{21} + x_{49};$$
$$y_{50} = x_{49}x_{22} + x_{48}x_{25} + x_{47}x_{28} + x_{46}x_{31} + x_{45}x_{34} + x_{44}x_{37} + x_{43}x_{40} + x_{50} + x_{10} + x_{17};$$
$$y_{51} = x_{50}x_{23} + x_{49}x_{26} + x_{48}x_{29} + x_{47}x_{32} + x_{46}x_{35} + x_{45}x_{38} + x_{44}x_{41} + x_{51} + x_8 + x_{22};$$
$$y_{52} = x_{41}x_{46} + x_{42}x_{45} + x_{49} + x_{52};$$
$$y_{53} = x_{41}x_{47} + x_{43}x_{45} + x_{53};$$
$$y_{54} = x_{42}x_{47} + x_{43}x_{46} + x_{54};$$
$$y_{55} = x_{44}x_{46} + x_{42}x_{48} + x_{55};$$
$$y_{56} = x_{44}x_{45} + x_{41}x_{48} + x_{56};$$
$$y_{57} = x_{56}x_0 + x_{55}x_5 + x_{54}x_{10} + x_{53}x_{15} + x_{52}x_{20} + x_{51}x_{25} + x_{50}x_{30} + x_{57} + x_{56};$$
$$y_{58} = x_{57}x_1 + x_{56}x_6 + x_{55}x_{11} + x_{54}x_{16} + x_{53}x_{21} + x_{52}x_{26} + x_{51}x_{31} + x_{58} + x_{52} + x_{47};$$
$$y_{59} = x_{55}x_2 + x_{54}x_7 + x_{53}x_{12} + x_{52}x_{17} + x_{51}x_{22} + x_{50}x_{27} + x_{49}x_{32} + x_{59} + x_{20} + x_{15};$$
$$y_{60} = x_{59}x_3 + x_{58}x_8 + x_{57}x_{13} + x_{56}x_{18} + x_{55}x_{23} + x_{54}x_{28} + x_{53}x_{13} + x_{60} + x_2 + x_8;$$
$$y_{61} = x_{56}x_7 + x_{44}x_8 + x_{33}x_{17} + x_{35}x_{20} + x_{40}x_{22} + x_{48}x_{25} + x_{23}x_{24} + x_{60} + x_7 + x_{15};$$
$$y_{62} = x_{61}x_{20} + x_{37}x_{38} + x_{44}x_{34} + x_{57}x_9 + x_{59}x_{15} + x_{40}x_{39} + x_{60}x_2 + x_{62} + x_9 + x_{35};$$
$$y_{63} = x_{62}x_{15} + x_{58}x_7 + x_{37}x_{13} + x_{48}x_{16} + x_{36}x_{38} + x_{27}x_{44} + x_{55}x_3 + x_{63} + x_{44};$$
$$y_{64} = x_{61}x_{19} + x_{60}x_9 + x_{54}x_{17} + x_{41}x_{52} + x_{56}x_{28} + x_3x_6 + x_{16}x_8 + x_{64} + x_{23} + x_{17};$$
$$y_{65} = x_{64}x_{63} + x_{34}x_{56} + x_{29}x_{41} + x_{31}x_{61} + x_{55}x_{37} + x_{59}x_{62} + x_1x_{56} + x_{65} + x_6;$$
$$y_{66} = x_{65}x_{64} + x_1x_{27} + x_{47}x_{59} + x_{38}x_{39} + x_{48}x_{50} + x_{27}x_{62} + x_{36}x_{57} + x_{66} + x_{56} + x_{46};$$
$$y_{67} = x_{65}x_{63} + x_{38}x_{58} + x_{27}x_{39} + x_{37}x_{59} + x_{40}x_{65} + x_4x_{34} + x_{15}x_{46} + x_{67} + x_4 + x_{16};$$
$$y_{68} = x_{57}x_{62} + x_{58}x_{61} + x_{65} + x_{68};$$
$$y_{69} = x_{57}x_{63} + x_{59}x_{61} + x_{69};$$
$$y_{70} = x_{58}x_{63} + x_{59}x_{62} + x_{70};$$
$$y_{71} = x_{60}x_{62} + x_{58}x_{64} + x_{71};$$
$$y_{72} = x_{60}x_{61} + x_{57}x_{64} + x_{72};$$
$$y_{73} = x_{72}x_{71} + x_{70}x_{69} + x_{68}x_{67} + x_1x_{19} + x_{25}x_{70} + x_{36}x_{68} + x_{57}x_{66} + x_{73} + x_{72} + x_9;$$
$$y_{74} = x_{73}x_5 + x_{72}x_9 + x_{71}x_{15} + x_{68}x_3 + x_{69}x_{27} + x_{38}x_{49} + x_{40}x_{70} + x_{74} + x_{11} + x_{21};$$
$$y_{75} = x_{74}x_4 + x_{72}x_{67} + x_{36}x_{68} + x_{49}x_{51} + x_{27}x_{67} + x_{39}x_{44} + x_{48}x_{66} + x_{75} + x_{12} + x_{22};$$
$$y_{76} = x_{74}x_{75} + x_{49}x_{27} + x_{36}x_1 + x_{46}x_{65} + x_{70}x_6 + x_{71}x_{18} + x_{72}x_7 + x_{76} + x_{13} + x_{34};$$
$$y_{77} = x_{76}x_0 + x_{75}x_{16} + x_{68}x_{24} + x_{74}x_{69} + x_{73}x_{57} + x_{70}x_{27} + x_{69}x_{17} + x_{77} + x_{18} + x_{29};$$
$$y_{78} = x_{77}x_9 + x_{76}x_{30} + x_{75}x_{73} + x_{74}x_{41} + x_{73}x_{45} + x_{68}x_{53} + x_{69}x_{62} + x_{78} + x_{12} + x_{37};$$
$$y_{79} = x_{78}x_{41} + x_{77}x_{31} + x_{76}x_7 + x_{67}x_{75} + x_{39}x_{51} + x_{45}x_{63} + x_{29}x_{28} + x_{79} + x_0 + x_{27} + x_{49};$$
$$y_{80} = x_{79}x_{71} + x_{74}x_{75} + x_{76}x_{77} + x_{38}x_{47} + x_{45}x_{62} + x_{37}x_{71} + x_{25}x_{53} + x_{80} + x_{71} + x_{47};$$
$$y_{81} = x_{80}x_{72} + x_{79}x_{78} + x_{48}x_{64} + x_{78}x_5 + x_{77}x_9 + x_{71}x_{36} + x_{68}x_{59} + x_{81} + x_{80} + x_{35};$$
$$y_{82} = x_{81}x_{49} + x_{79}x_{26} + x_{77}x_{10} + x_{75}x_{47} + x_{73}x_{64} + x_{71}x_{70} + x_{79}x_3 + x_{82} + x_{56} + x_{49};$$
$$y_{83} = x_{82}x_8 + x_{73}x_{74} + x_{81}x_{69} + x_{79}x_{78} + x_{35}x_{61} + x_{74}x_{75} + x_{80}x_{72} + x_{83} + x_1 + x_{48};$$
$$y_{84} = x_{73}x_{78} + x_{74}x_{77} + x_{81} + x_{84};$$
$$y_{85} = x_{73}x_{79} + x_{75}x_{77} + x_{85};$$
$$y_{86} = x_{74}x_{79} + x_{75}x_{78} + x_{86};$$
$$y_{87} = x_{76}x_{78} + x_{74}x_{80} + x_{87};$$
$$y_{88} = x_{76}x_{77} + x_{73}x_{80} + x_{88};$$
$$y_{89} = x_{88}x_{84} + x_{87}x_{10} + x_{86}x_{29} + x_{85}x_{21} + x_{83}x_{19} + x_{79}x_{14} + x_{78}x_{65} + x_{89} + x_{84} + x_{11};$$
$$y_{90} = x_{89}x_{11} + x_{35}x_{77} + x_{83}x_{87} + x_{84}x_{27} + x_{85}x_{37} + x_{86}x_{47} + x_{88}x_{57} + x_{90} + x_{85} + x_4;$$
$$y_{91} = x_{90}x_6 + x_{88}x_{15} + x_{87}x_{23} + x_{86}x_{35} + x_{85}x_{84} + x_{83}x_{17} + x_{79}x_{34} + x_{91} + x_{88} + x_{43};$$
$$y_{92} = x_{91}x_{12} + x_{89}x_{13} + x_{90}x_{14} + x_{88}x_{21} + x_{87}x_{31} + x_{86}x_{41} + x_{67}x_{65} + x_{92} + x_{87} + x_{21};$$

$$y_{93} = x_{92}x_{24} + x_{90}x_{56} + x_{88}x_{63} + x_{86}x_{54} + x_{84}x_{44} + x_{79}x_{56} + x_{78}x_{91} + x_{93} + x_{89} + x_{42};$$
$$y_{94} = x_{93}x_{17} + x_{86}x_{26} + x_{92}x_{35} + x_{91}x_{90} + x_{89}x_{44} + x_{88}x_{51} + x_{87}x_{66} + x_{94} + x_{78} + x_3 + x_{17};$$
$$y_{95} = x_{94}x_{11} + x_{93}x_1 + x_{92}x_{41} + x_{91}x_{55} + x_{89}x_{33} + x_{88}x_{71} + x_{87}x_{22} + x_{95} + x_1 + x_{17} + x_{29};$$
$$y_{96} = x_{95}x_4 + x_{94}x_{17} + x_{93}x_{29} + x_{92}x_{77} + x_{91}x_{76} + x_{90}x_{53} + x_{89}x_{65} + x_{96} + x_{94} + x_{19};$$
$$y_{97} = x_{96}x_5 + x_{94}x_{53} + x_{94}x_{16} + x_{92}x_{88} + x_{91}x_{75} + x_{90}x_{62} + x_{89}x_{77} + x_{97} + x_7 + x_{18};$$
$$y_{98} = x_{97}x_8 + x_{96}x_{17} + x_{95}x_{89} + x_{92}x_{73} + x_{81}x_{82} + x_{90}x_{82} + x_{89}x_{84} + x_{98} + x_9 + x_{27};$$
$$y_{99} = x_{98}x_7 + x_{96}x_{97} + x_{95}x_{23} + x_{92}x_{71} + x_{81}x_{90} + x_{82}x_{89} + x_{85}x_{86} + x_{99} + x_{89} + x_{12};$$
$$y_{100} = x_{95}x_{89} + x_{91}x_{93} + x_{100};$$
$$y_{101} = x_{89}x_{94} + x_{90}x_{93} + x_{97} + x_{101};$$
$$y_{102} = x_{90}x_{95} + x_{91}x_{94} + x_{102};$$
$$y_{103} = x_{92}x_{94} + x_{90}x_{96} + x_{103};$$
$$y_{104} = x_{92}x_{93} + x_{89}x_{96} + x_{104};$$
$$y_{105} = x_1x_{34} + x_2x_{33} + x_1 + x_{33} + x_{34} + x_{105};$$
$$y_{106} = x_0x_{34} + x_2x_{32} + x_0 + x_{32} + x_{34} + x_{106};$$
$$y_{107} = x_0x_{33} + x_{32}x_1 + x_{32} + x_{33} + x_{107};$$
$$y_{108} = f(x_0, \cdots, x_{107}) + x_{108};$$
$$y_{109} = x_4x_{19} + x_{108}x_{18} + x_4 + x_{108} + x_{18} + 1 + x_{19} + x_{109};$$
$$y_{110} = x_3x_{19} + x_{108}x_{17} + x_3 + x_{108} + x_{17} + 1 + x_{19} + x_{110};$$
$$y_{111} = x_3x_{18} + x_{17}x_4 + x_3 + x_4 + x_{17} + x_{18} + x_{111};$$
$$y_{112} = x_{18}x_{10} + x_{19}x_9 + x_{18} + x_9 + x_{10} + x_{23};$$
$$y_{113} = x_{17}x_{10} + x_{19}x_8 + x_{17} + x_8 + x_{10} + x_{24};$$
$$y_{114} = x_{17}x_9 + x_8x_{18} + x_8 + x_9 + x_{25};$$
$$y_{115} = x_4x_{31} + x_{108}x_{30} + x_4 + x_{108} + x_{30} + 1 + x_{31} + x_{109};$$
$$y_{116} = x_3x_{31} + x_{108}x_{29} + x_3 + x_{108} + x_{29} + 1 + x_{31} + x_{110};$$
$$y_{117} = x_3x_{30} + x_{29}x_4 + x_3 + x_4 + x_{29} + x_{30} + x_{111};$$
$$y_{118} = x_1x_{22} + x_2x_{21} + x_1 + x_{21} + x_{22} + x_{105};$$
$$y_{119} = x_0x_{22} + x_2x_{20} + x_0 + x_{20} + x_{22} + x_{106};$$
$$y_{120} = x_0x_{21} + x_{20}x_1 + x_{20} + x_{21} + x_{107};$$
$$y_{121} = x_5x_{11} + x_{12}x_6 + x_7x_{13} + x_{11} + x_{12} + x_{13} + x_0x_{105} + x_1x_{106} + x_2x_{107} + x_{105} + x_{106} + x_{107};$$
$$y_{122} = x_3x_{109} + x_4x_{110} + x_{108}x_{111} + x_{109} + x_{110} + x_{111} + x_0x_{105} + x_1x_{106} + x_2x_{107} + x_{105} + x_{106} + x_{107};$$
$$y_{123} = x_{29}x_{35} + x_{30}x_{36} + x_{31}x_{37} + x_{35} + x_{36} + x_{37};$$
$$y_{124} = x_{32}x_{38} + x_{33}x_{39} + x_{34}x_{40} + x_{40};$$
$$y_{125} = x_0x_{38} + x_1x_{39} + x_2x_{40} + x_{38} + x_{39} + x_{40};$$
$$y_{126} = x_{32}x_{105} + x_{33}x_{106} + x_{34}x_{107} + x_{107};$$
$$y_{127} = x_{105}x_{39} + x_{38}x_{106} + x_2 + x_{34};$$
$$y_{128} = x_{105}x_{40} + x_{107}x_{38} + x_1 + x_{33};$$
$$y_{129} = x_{106}x_{40} + x_{107}x_{39} + x_0 + x_{32};$$
$$y_{130} = x_{17}x_{23} + x_{24}x_{18} + x_{25}x_{19} + x_{23} + x_{24} + x_{25};$$
$$y_{131} = x_{26}x_{17} + x_{18}x_{27} + x_{19}x_{28} + x_{26} + x_{27} + x_{28};$$
$$y_{132} = x_{20}x_{23} + x_{21}x_{24} + x_{22}x_{25} + x_{25};$$
$$y_{133} = x_{23}x_{27} + x_{26}x_{24} + x_{19} + x_{22};$$
$$y_{134} = x_{23}x_{28} + x_{25}x_{26} + x_{18} + x_{21};$$
$$y_{135} = x_{24}x_{28} + x_{25}x_{27} + x_{17} + x_{20};$$
$$y_{136} = x_{14}x_5 + x_6x_{15} + x_7x_{16} + x_{14} + x_{15} + x_{16};$$
$$y_{137} = x_{11}x_8 + x_{12}x_9 + x_{10}x_{13} + x_{13};$$
$$y_{138} = x_{15}x_{11} + x_{14}x_{12} + x_7 + x_{10};$$
$$y_{139} = x_{11}x_{16} + x_{13}x_{14} + x_6 + x_9;$$
$$y_{140} = x_{12}x_{16} + x_{13}x_{15} + x_5 + x_8;$$
$$y_{141} = x_0x_{26} + x_1x_{27} + x_2x_{28} + x_{26} + x_{27} + x_{28};$$
$$y_{142} = x_{20}x_{105} + x_{21}x_{106} + x_{22}x_{107} + x_{107};$$

$$y_{143} = x_{105}x_{27} + x_{26}x_{106} + x_2 + x_{22};$$
$$y_{144} = x_{105}x_{28} + x_{107}x_{26} + x_1 + x_{21};$$
$$y_{145} = x_{106}x_{28} + x_{107}x_{27} + x_0 + x_{20};$$
$$y_{146} = x_3x_{23} + x_4x_{24} + x_{108}x_{25} + x_{23} + x_{24} + x_{25};$$
$$y_{147} = x_{17}x_{109} + x_{18}x_{110} + x_{19}x_{111} + x_{109} + x_{110} + x_{111};$$
$$y_{148} = x_{109}x_{24} + x_{23}x_{110} + x_{108} + x_{19};$$
$$y_{149} = x_{109}x_{25} + x_{111}x_{23} + x_4 + x_{18} + 1;$$
$$y_{150} = x_{110}x_{25} + x_{111}x_{24} + x_3 + x_{17} + 1;$$
$$y_{151} = x_3x_{35} + x_4x_{36} + x_{108}x_{37} + x_{35} + x_{36} + x_{37};$$
$$y_{152} = x_{29}x_{109} + x_{30}x_{110} + x_{31}x_{111} + x_{109} + x_{110} + x_{111};$$
$$y_{153} = x_{109}x_{36} + x_{35}x_{110} + x_{108} + x_{31};$$
$$y_{154} = x_{109}x_{37} + x_{111}x_{35} + x_4 + x_{30} + 1;$$
$$y_{155} = x_{110}x_{37} + x_{111}x_{36} + x_3 + x_{29} + 1;$$
$$y_{156} = x_{29}x_{26} + x_{30}x_{27} + x_{31}x_{28} + x_{26} + x_{27} + x_{28};$$
$$y_{157} = x_{35}x_{20} + x_{21}x_{36} + x_{22}x_{37} + x_{37};$$
$$y_{158} = x_{35}x_{27} + x_{26}x_{36} + x_{31} + x_{22};$$
$$y_{159} = x_{35}x_{28} + x_{37}x_{26} + x_{30} + x_{21};$$
$$y_{160} = x_{36}x_{28} + x_{37}x_{27} + x_{29} + x_{20};$$
$$y_{161} = x_{32}x_{11} + x_{33}x_{12} + x_{34}x_{13} + x_{13};$$
$$y_{162} = x_{38}x_5 + x_{39}x_6 + x_7x_{40} + x_{38} + x_{39} + x_{40};$$
$$y_{163} = x_{38}x_{12} + x_{11}x_{39} + x_{34} + x_7;$$
$$y_{164} = x_{38}x_{13} + x_{40}x_{11} + x_{33} + x_6;$$
$$y_{165} = x_{39}x_{13} + x_{40}x_{12} + x_{32} + x_5;$$
$$y_{166} = x_{17}x_{14} + x_{18}x_{15} + x_{19}x_{16} + x_{14} + x_{15} + x_{16};$$
$$y_{167} = x_8x_{23} + x_{24}x_9 + x_{25}x_{10} + x_{25};$$
$$y_{168} = x_{23}x_{15} + x_{14}x_{24} + x_{19} + x_{10};$$
$$y_{169} = x_{23}x_{16} + x_{25}x_{14} + x_{18} + x_9;$$
$$y_{170} = x_{24}x_{16} + x_{25}x_{15} + x_{17} + x_8;$$
$$y_{171} = x_{41}x_{54} + x_{42}x_{53} + x_{43}x_{49} + x_{44}x_{51} + x_{111} + x_{110} + x_{109} + x_4x_{110} + x_{108}x_{111} + x_3x_{109};$$
$$y_{172} = x_{45}x_{55} + x_{46}x_{56} + x_{47}x_{50} + x_{48}x_{52};$$
$$y_{173} = x_{45}x_{54} + x_{46}x_{53} + x_{47}x_{49} + x_{48}x_{51};$$
$$y_{174} = x_{41}x_{55} + x_{42}x_{56} + x_{43}x_{50} + x_{44}x_{52};$$
$$y_{175} = x_{54}x_{56} + x_{53}x_{55};$$
$$y_{176} = x_{54}x_{50} + x_{49}x_{55} + x_{48};$$
$$y_{177} = x_{53}x_{50} + x_{49}x_{56} + x_{44};$$
$$y_{178} = x_{51}x_{56} + x_{53}x_{52} + x_{43};$$
$$y_{179} = x_{51}x_{50} + x_{49}x_{52} + x_{42} + x_{45};$$
$$y_{180} = x_{44}x_{47} + x_{43}x_{48};$$
$$y_{181} = x_{51}x_{55} + x_{54}x_{52} + x_{47};$$
$$y_{182} = x_{57}x_{70} + x_{58}x_{69} + x_{59}x_{65} + x_{60}x_{67} + x_{111} + x_{110} + x_{109} + x_4x_{110} + x_{108}x_{111} + x_3x_{109};$$
$$y_{183} = x_{61}x_{71} + x_{62}x_{72} + x_{63}x_{66} + x_{64}x_{68};$$
$$y_{184} = x_{61}x_{70} + x_{69}x_{62} + x_{65}x_{63} + x_{64}x_{67};$$
$$y_{185} = x_{57}x_{71} + x_{58}x_{72} + x_{59}x_{66} + x_{60}x_{68};$$
$$y_{186} = x_{70}x_{72} + x_{69}x_{71};$$
$$y_{187} = x_{70}x_{66} + x_{65}x_{71} + x_{64};$$
$$y_{188} = x_{69}x_{66} + x_{65}x_{72} + x_{60};$$
$$y_{189} = x_{72}x_{67} + x_{69}x_{68} + x_{59};$$
$$y_{190} = x_{67}x_{66} + x_{65}x_{68} + x_{58} + x_{61};$$
$$y_{191} = x_{60}x_{63} + x_{59}x_{64};$$
$$y_{192} = x_{67}x_{71} + x_{70}x_{68} + x_{63};$$

$$y_{193} = x_{73}x_{86} + x_{74}x_{85} + x_{75}x_{81} + x_{76}x_{83} + x_{111} + x_{110} + x_{109} + x_4x_{110} + x_{108}x_{111} + x_3x_{109};$$
$$y_{194} = x_{77}x_{87} + x_{78}x_{88} + x_{79}x_{82} + x_{80}x_{84};$$
$$y_{195} = x_{77}x_{86} + x_{78}x_{85} + x_{79}x_{81} + x_{80}x_{83};$$
$$y_{196} = x_{73}x_{87} + x_{74}x_{88} + x_{75}x_{82} + x_{76}x_{84};$$
$$y_{197} = x_{86}x_{88} + x_{85}x_{87};$$
$$y_{198} = x_{86}x_{82} + x_{81}x_{87} + x_{80};$$
$$y_{199} = x_{85}x_{82} + x_{81}x_{88} + x_{76};$$
$$y_{200} = x_{83}x_{88} + x_{85}x_{84} + x_{75};$$
$$y_{201} = x_{83}x_{82} + x_{81}x_{84} + x_{74} + x_{77};$$
$$y_{202} = x_{76}x_{79} + x_{75}x_{80};$$
$$y_{203} = x_{83}x_{87} + x_{86}x_{84} + x_{79};$$
$$y_{204} = x_{89}x_{102} + x_{90}x_{100} + x_{91}x_{97} + x_{92}x_{99} + x_{111} + x_{110} + x_{109} + x_4x_{110} + x_{108}x_{111} + x_3x_{109};$$
$$y_{205} = x_{93}x_{103} + x_{94}x_{104} + x_{95}x_{98} + x_{96}x_{101};$$
$$y_{206} = x_{93}x_{102} + x_{94}x_{100} + x_{95}x_{97} + x_{96}x_{99};$$
$$y_{207} = x_{89}x_{103} + x_{90}x_{104} + x_{91}x_{98} + x_{92}x_{101};$$
$$y_{208} = x_{102}x_{104} + x_{100}x_{103};$$
$$y_{209} = x_{102}x_{98} + x_{97}x_{103} + x_{96};$$
$$y_{210} = x_{100}x_{98} + x_{97}x_{104} + x_{92};$$
$$y_{211} = x_{99}x_{104} + x_{100}x_{101} + x_{91};$$
$$y_{212} = x_{99}x_{98} + x_{97}x_{101} + x_{90} + x_{93};$$
$$y_{213} = x_{92}x_{95} + x_{91}x_{96};$$
$$y_{214} = x_{99}x_{103} + x_{102}x_{101} + x_{95};$$