Breaking a New Instance of TTM Cryptosystems

Xuyun Nie[1,⋆], Lei Hu[1], Jianyu Li[1], Crystal Updegrove[2], and Jintai Ding[2]

[1] State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences,
Beijing 100049, China
[2] Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, OH, 45220, USA
nxy04b@mails.gucas.com.cn

Abstract. In 2004, the inventors of TTM cryptosystems proposed a new scheme that could resist the existing attacks, in particular, the Goubin-Courtois attack [GC00] and the Ding-Schmidt attack [DS03]. In this paper, we show the new version is still insecure, and we find that the polynomial components of the cipher (F_i) satisfy nontrivial equations of the special form

$$\sum_{i=0}^{n-1} a_i x_i + \sum_{0\le j\le k\le m-1} b_{jk} F_j F_k + \sum_{j=0}^{m-1} c_j F_j + d = 0,$$

which could be found with 2^{38} computations. From these equations and consequently the linear equations we derive from these equations for any given ciphertext, we can eliminate some of the variables x_i by restricting the functions to an affine subspace, such that, on this subspace, we can trivialize the "lock" polynomials, which are the key structure to ensure its security in this new instance of TTM. Then with method similar to Ding-Schmidt [DS03], we can find the corresponding plaintext for any given ciphertext. The total computational complexity of the attack is less than 2^{39} operations over a finite field of size 2^8. Our results are further confirmed by computer experiments.

Keywords: Multivariate public key cryptography, TTM, quadratic polynomial.

1 Introduction

Public key cryptography is an important tool for our modern information society. Traditional public key cryptosystems such as RSA and ElGamal rely on hard number theory based problems such as factoring or discrete logarithms. However, techniques for factorization and solving discrete logarithm continually improve and polynomial time quantum algorithms can be used to solve both problems

[⋆] Corresponding author.

J. Zhou, M. Yung, and F. Bao (Eds.): ACNS 2006, LNCS 3989, pp. 210–225, 2006.

efficiently [Sho97]. Hence, there is a need to search for alternatives which are based on other classes of problems.

Multivariate public key cryptosystem (MPKC) is one of the promising alternatives. The security of MPKC relies on the difficulty of solving systems of nonlinear polynomial equations with many variables, and the latter is a NP-hard problem in general. The public key of MPKC is mostly a set of quadratic polynomials. These polynomials are derived from composition of maps. Compared with RSA public key cryptosystems, the computation in MPKC can be very fast because it is operated on a small finite field. So MPKC may be suitable for even low-end devices.

The first promising construction of MPKC is the Matsumoto-Imai (MI) scheme [MI88] proposed in 1988. Unfortunately, it was defeated by Patarin in 1995 with the linearization method [Pat95].

Tame transformation method (TTM) schemes [Moh99] was proposed by Moh in 1999. The central map of TTM is the so-called tame transformations which is closely related to the famous Jacobian conjecture in algebraic geometry. The construction of TTM is very beautiful, and the decryption of TTM is very fast due to its special design.

But by now, all instances of TTM are insecure. In 2000, Goubin and Courtois claimed that they completely defeated all possible instances of TTM schemes using the Minrank method and 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 presented another construction to support their claim [CM01]. But this new scheme also had 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 components of the ciphers, and they extended linearization method to attack this new version [DS03]. In order to resist these attacks, the inventors of TTM proposed another new instance [MCY04] in 2004, and they claimed the security is 2^{148} against the Goubin-Courtois attack. To resist the Ding-Schmidt attack, they incorporated new lock polynomials which can not be trivialized by Ding-Schmidt attack.

Unfortunately, we find this new implementation of TTM also has a defect, that is, there exist nontrivial equations of the special form

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

We call them **second order linearization equations**. We use these equations as a starting point to trivialize the lock polynomials in the TTM instance. In other words, for any given valid ciphertext, we can find an affine subspace W in the plaintext space such that all lock polynomials become constants on W. Then with method similar to Ding-Schmidt [DS03], we can recover the corresponding plaintext for a given ciphertext easily. This attack in principle is very similar to the attack of Ding and Hodges in [DH03]. The total computational complexity of our attack is less than 2^{39}.

The paper is organized as follows. We introduce the basic ideas and new instance of TTM schemes in Section 2. In Section 3, we describe how to attack this new TTM, present a practical attack procedure, and calculate the complexity of our attack. Finally, in Section 4, we conclude the paper.

2 TTM Cryptosystems

2.1 Basic Idea of TTM Schemes

Let $\mathbb{K}$ be a small finite field. The TTM systems is constructed as a composition of several maps $\phi_1, \phi_2, \cdots$, and ϕ_l, $F = \phi_l \circ \phi_{l-1} \circ \cdots \circ \phi_1$, where ϕ_i is a polynomial map from K^{n_i} to $K^{n_{i+1}}$ and $n = n_1 \leq n_2 \leq \cdots \leq n_{l+1} = m$, such that

1. The value of $F(x_0, \cdots, x_{n-1})$ at any given $(x_0, \cdots, x_{n-1})$ is easy to compute.
2. Each ϕ_i is easy to invert, and $F(x_0, \cdots, x_{n-1})$ is also easy to invert if one knows the composition factors of F, namely the ϕ_i. But it is hard to invert F if one does not know the factorization.
3. Some of the ϕ_i are linear polynomials, while F is a quadratic polynomial map.

The expression of $F(x_0, \cdots, x_{n-1})$ is taken as the public key in a TTM system and the linear ϕ_i as the secret key. $F : \mathbb{K}^n \to \mathbb{K}^m$ is a set of quadratic polynomials. In all known instances of TTM design, one uses the following two types of maps for the ϕ_i :

1. Linear affine maps of the form $f(X) = AX + b$, where $X, b \in \mathbb{K}^*$ are vectors and A is an invertible matrix.
2. Tame transformations. They are maps of the form

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

The inventor, an expert in algebraic geometry, uses the basic concept of tame transformation from algebraic geometry. The inverting process of a tame transformation is very simple and is also a tame transformation.

The key construction of TTM schemes is the so-called lock polynomials. In the new instance [MCY04], a set of new lock polynomial $G_j(x_0, \cdots, x_{n-1})$, $j = 0, \cdots, 6$, is constructed, where the central map becomes

$$\begin{aligned}
&J(x_0, \cdots, x_{n-1}) \\
&= (x_0 + G_0, x_1 + q_1(x_0) + G_1, \cdots, x_6 + q_6(x_0, \cdots, x_5) + G_6, \\
&\quad x_7 + q_7(x_0, \cdots, x_6), \cdots, x_{n-1} + q_{n-1}(x_0, \cdots, x_{n-2}), \\
&\quad q_n(x_0, \cdots, x_{n-1}), \cdots, q_{m-1}(x_0, \cdots, x_{n-1})).
\end{aligned}$$

A pure triangular system can be solved by Minrank method, therefore the lock polynomials are needed to resist this attack. Our attack uses a different method and we start from first trying to trivialize these lock polynomials.

2.2 New Instance of TTM

We use the same notation as in [MCY04]. Take $\mathbb{K}$ as the finite field with 2^8 elements and $m = 110$ and $n = 55$. The map $F : \mathbb{K}^{55} \to \mathbb{K}^{110}$ is a composition of 4 maps ϕ_1, ϕ_2, ϕ_3, and ϕ_4, namely $F = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$:

$$F : \mathbb{K}^{55} \xrightarrow{\phi_1} \mathbb{K}^{55} \xrightarrow{\phi_2} \mathbb{K}^{110} \xrightarrow{\phi_3} \mathbb{K}^{110} \xrightarrow{\phi_4} \mathbb{K}^{110}.$$

ϕ_1 and ϕ_4 are invertible affine linear maps, ϕ_2 is a tame quadratic transformation, and ϕ_3 is a degree 8 map using lock polynomials.

The expressions of ϕ_2 and ϕ_3 are public information in the TTM system. ϕ_1 and ϕ_4 are taken as the private key, while the expression of the map $(y_0, \cdots, y_{109}) = F(x_0, ..., x_{54})$ is the public key. Each component polynomial $y_i = F_i(x_0, ...x_{54})$ of F is a quadratic polynomial. To encrypt a plaintext $(x_0, ..., x_{54})$ is to evaluate F at it.

Define

$$(\bar{x}_0, \cdots, \bar{x}_{54}) = \phi_1(x_0, \cdots, x_{54}), (\bar{y}_0, \cdots, \bar{y}_{110}) = \phi_2(\bar{x}_0, \cdots, \bar{x}_{54}),$$
$$(z_0, \cdots, z_{110}) = \phi_3(\bar{y}_0, \cdots, \bar{y}_{110}), (y_0, \cdots, y_{110}) = \phi_4((z_0, \cdots, z_{110}).$$

The exact description of ϕ_2 is given in appendix.

Seven lock polynomials, $G_j(\bar{x}_0, \cdots, \bar{x}_{n-1})$, $0 \le j \le 7$, are used to define ϕ_3 and they are defined as follows:

$R_1 := \bar{y}_{66}\bar{y}_{67} + \bar{y}_{68}\bar{y}_{69} + \bar{y}_{70}\bar{y}_{31} + \bar{y}_{71}\bar{y}_{32} + \bar{y}_{72}\bar{y}_{33} + \bar{y}_{73}\bar{y}_{34} + \bar{y}_{74}\bar{y}_{75} + \bar{y}_{76}\bar{y}_{35} + \bar{y}_{45};$
$R_2 := \bar{y}_{77}\bar{y}_{78} + \bar{y}_{79}\bar{y}_{80} + \bar{y}_{75}\bar{y}_{31} + \bar{y}_{36}\bar{y}_{81} + \bar{y}_{37}\bar{y}_{82} + \bar{y}_{38}\bar{y}_{83} + \bar{y}_{74}\bar{y}_{84} + \bar{y}_{39}\bar{y}_{85} + \bar{y}_{46};$
$R_3 := \bar{y}_{86}\bar{y}_{87} + \bar{y}_{88}\bar{y}_{89} + \bar{y}_{90}\bar{y}_{22} + \bar{y}_{91}\bar{y}_{23} + \bar{y}_{92}\bar{y}_{24} + \bar{y}_{93}\bar{y}_{25} + \bar{y}_{94}\bar{y}_{95} + \bar{y}_{96}\bar{y}_{26} + \bar{y}_{47};$
$R_4 := \bar{y}_{97}\bar{y}_{98} + \bar{y}_{99}\bar{y}_{100} + \bar{y}_{95}\bar{y}_{22} + \bar{y}_{27}\bar{y}_{101} + \bar{y}_{28}\bar{y}_{102} + \bar{y}_{29}\bar{y}_{103} + \bar{y}_{94}\bar{y}_{104} + \bar{y}_{30}\bar{y}_{105} + \bar{y}_{48};$
$R_5 := \bar{y}_{55}\bar{y}_{56} + \bar{y}_{57}\bar{y}_{58} + \bar{y}_{59}\bar{y}_{40} + \bar{y}_{60}\bar{y}_{41} + \bar{y}_{61}\bar{y}_{42} + \bar{y}_{62}\bar{y}_{43} + \bar{y}_{63}\bar{y}_{64} + \bar{y}_{65}\bar{y}_{44} + \bar{y}_{49};$
$S_1 := R_2R_4 + R_3R_5 + \bar{y}_{50} = \bar{x}_{50};$
$S_2 := R_1R_3 + R_4R_5 + \bar{y}_{51} = \bar{x}_{51};$
$S_3 := R_1R_4 + R_2R_5 + \bar{y}_{52} = \bar{x}_{52};$
$S_4 := R_1R_5 + R_2R_3 + \bar{y}_{53} = \bar{x}_{53};$
$S_5 := R_1R_2 + R_3R_4 + \bar{y}_{54} = \bar{x}_{54};$
$G_0 := S_2S_4 + S_3S_5 = \bar{x}_{51}\bar{x}_{53} + \bar{x}_{52}\bar{x}_{54};$
$G_1 := S_1S_3 + S_4S_5 = \bar{x}_{50}\bar{x}_{52} + \bar{x}_{53}\bar{x}_{54};$
$G_2 := S_1S_4 + S_2S_5 = \bar{x}_{50}\bar{x}_{53} + \bar{x}_{51}\bar{x}_{54};$
$G_3 := S_1S_5 + S_2S_3 = \bar{x}_{50}\bar{x}_{54} + \bar{x}_{51}\bar{x}_{52};$
$G_4 := S_1S_2 + S_3S_4 = \bar{x}_{50}\bar{x}_{51} + \bar{x}_{52}\bar{x}_{53};$
$G_5 := R_1S_1 + R_2S_2 + R_3S_3 + R_4S_4 + R_5S_5 = \bar{x}_{50}\bar{x}_{45} + \bar{x}_{51}\bar{x}_{46} + \bar{x}_{52}\bar{x}_{47} + \bar{x}_{53}\bar{x}_{48} + \bar{x}_{54}\bar{x}_{49};$
$G_6 := R_1S_2 + R_2S_3 + R_3S_4 + R_4S_5 + R_5S_1 = \bar{x}_{51}\bar{x}_{45} + \bar{x}_{52}\bar{x}_{46} + \bar{x}_{53}\bar{x}_{47} + \bar{x}_{54}\bar{x}_{48} + \bar{x}_{50}\bar{x}_{49}.$

ϕ_3 is defined as:

$$\phi_3(\bar{y}_0, \cdots, \bar{y}_{109}) = (\bar{y}_0 + G_0(\bar{y}_0, \cdots, \bar{y}_{109}), \cdots,$$
$$\bar{y}_6 + G_6(\bar{y}_0, \cdots, \bar{y}_{109}), \bar{y}_7, \cdots, \bar{y}_{109}).$$

Note that ϕ_3 is of degree 8 in terms of $\bar{y}_i$. Then

$$\begin{aligned}\phi_{32}(\bar{x}_0, \cdots, \bar{x}_{54}) = \phi_3 \circ \phi_2(\bar{x}_0, \cdots, \bar{x}_{54}) = (\bar{y}_0 + G_0(\bar{x}_0, \cdots, \bar{x}_{54}), \cdots, \\ \bar{y}_6 + G_6(\bar{x}_0, \cdots, \bar{x}_{54}), \bar{y}_7, \cdots, \bar{y}_{109}).\end{aligned}$$

Note in the two formulas above, the functions G_i are seen differently, while in the first one they are functions of $\bar{y}_i$ with degree 8, in the second formula they are functions of $\bar{x}_i$ with degree 2. Denote by $\phi_{i,j}$ the j-th component function of ϕ_i. Similar notations $\phi_{32,j}$, $\phi_{1,j}^{-1}$,$\phi_{4,j}^{-1}$, and F_j are denoted for ϕ_{32}, ϕ_1^{-1}, ϕ_4^{-1}, and F, respectively. Obviously, each F_j is a quadratic polynomial, and $F(x_0, ..., x_{54}) = \phi_4 \circ \phi_{32} \circ \phi_1(x_0, ..., x_{54})$.

3 Cryptanalysis on New TTM Instance

Our attack is a ciphertext-only attack. We start from first finding all second order linearization equations. For any given ciphertext, we use them to trivialize the lock polynomials. Then, we derive the corresponding plaintext through the iteration of the process of first searching for linear relations in equations derived from the public key and the ciphertext and then substituting them into these equations.

3.1 Second Order Linearization Equations

We first observe that all the R_i $(1 \leq i \leq 5)$ are linear on $\bar{x}_0, \cdots$, and $\bar{x}_{54}$. By a direct computation, we find that $R_1 = \bar{x}_{45}$, $R_2 = \bar{x}_{46}$, $R_3 = \bar{x}_{47}$, $R_4 = \bar{x}_{48}$, and $R_5 = \bar{x}_{49}$, namely,

$$\begin{cases} \bar{x}_{45} + \bar{y}_{66}\bar{y}_{67} + \bar{y}_{68}\bar{y}_{69} + \bar{y}_{70}\bar{y}_{31} + \bar{y}_{71}\bar{y}_{32} + \bar{y}_{72}\bar{y}_{33} + \bar{y}_{73}\bar{y}_{34} + \bar{y}_{74}\bar{y}_{75} + \bar{y}_{76}\bar{y}_{35} + \bar{y}_{45} = 0; \\ \bar{x}_{46} + \bar{y}_{77}\bar{y}_{78} + \bar{y}_{79}\bar{y}_{80} + \bar{y}_{75}\bar{y}_{31} + \bar{y}_{36}\bar{y}_{81} + \bar{y}_{37}\bar{y}_{82} + \bar{y}_{38}\bar{y}_{83} + \bar{y}_{74}\bar{y}_{84} + \bar{y}_{39}\bar{y}_{85} + \bar{y}_{46} = 0; \\ \bar{x}_{47} + \bar{y}_{86}\bar{y}_{87} + \bar{y}_{88}\bar{y}_{89} + \bar{y}_{90}\bar{y}_{22} + \bar{y}_{91}\bar{y}_{23} + \bar{y}_{92}\bar{y}_{24} + \bar{y}_{93}\bar{y}_{25} + \bar{y}_{94}\bar{y}_{95} + \bar{y}_{96}\bar{y}_{26} + \bar{y}_{47} = 0; \\ \bar{x}_{48} + \bar{y}_{97}\bar{y}_{98} + \bar{y}_{99}\bar{y}_{100} + \bar{y}_{95}\bar{y}_{22} + \bar{y}_{27}\bar{y}_{101} + \bar{y}_{28}\bar{y}_{102} + \bar{y}_{29}\bar{y}_{103} + \bar{y}_{94}\bar{y}_{104} + \bar{y}_{30}\bar{y}_{105} + \bar{y}_{48} = 0; \\ \bar{x}_{49} + \bar{y}_{55}\bar{y}_{56} + \bar{y}_{57}\bar{y}_{58} + \bar{y}_{59}\bar{y}_{40} + \bar{y}_{60}\bar{y}_{41} + \bar{y}_{61}\bar{y}_{42} + \bar{y}_{62}\bar{y}_{43} + \bar{y}_{63}\bar{y}_{64} + \bar{y}_{65}\bar{y}_{44} + \bar{y}_{49} = 0; \end{cases} \tag{3.1}$$

Since F is derived from ϕ_{32} by composing from the inner and outer sides by invertible linear maps ϕ_1 and ϕ_4, i.e., $\bar{x}_i = \phi_{1,i}(x_0, \cdots, x_{54})$ and $\bar{y}_j = \phi_{4,j}^{-1}(F_0, \cdots, F_{109})$ for $j > 21$, and $\bar{y}_0, \cdots, \bar{y}_{21}$ do not appear in equations (3.1), each of these equations can be changed into an identical equation of the form:

$$\sum_{i=0}^{54} a_i x_i + \sum_{0 \leq j \leq k \leq 109} b_{jk} F_j F_k + \sum_{j=0}^{109} c_j F_j + d = 0, \tag{3.2}$$

which is satisfied by any $(x_0, \cdots, x_{54}) \in \mathbb{K}^{55}$. Note that the coefficients a_i $(0 \leq i \leq 54)$ are not all zero. Furthermore, there exist at least five equations of the above form such that their corresponding coefficient vectors $(a_0, \cdots, a_{54})$ are linearly independent since as linear combinations of $x_0, \cdots, x_{54}$, the coefficient vectors of $\bar{x}_{45}, \cdots, \bar{x}_{49}$ are linearly independent. Let V denote the $\mathbb{K}$-linear space composing of all second order linearization equations of the form (3.2), and let D be its dimension.

To find all equations in V is equivalent to find a basis of V. The equation (3.2) is equivalent to a system of equations on the coefficients a_i, b_{jk}, c_j, and d. It is well known that the number of monomials in n variables of degree $\leq D$ is $\binom{n+D}{D}$ ([CP03]), so the number of unknown coefficients in these equations is equal to

$$\binom{55}{1} + \binom{110+2}{2} = 6271.$$

To find a basis of V, we can randomly select slightly more than 6271, say 7000, plaintexts $(x_0, \cdots, x_{54})$ and substitute them in (3.2) to get a system of 7000 linear equations and then solve it. Let $\{(a_i^{(\rho)}, b_{jk}^{(\rho)}, c_j^{(\rho)}, d^{(\rho)}), 1 \leq \rho \leq D\}$ be the coefficient vectors corresponding to a basis of V, where i, (j,k), and j stand for $i = 0, \cdots, 54$, $0 \leq j \leq k \leq 109$, and $j = 0, \cdots, 109$, respectively.

Let V' be linear subspace which is consisting of the zero equation and all second order linearization equations with $(a_0, \cdots, a_{54}) \neq (0, \cdots, 0)$, and let $l = \dim V' \geq 5$. Without loss of generality, we assume $(a_0^{(1)}, \cdots, a_{54}^{(1)}), \cdots, (a_0^{(l)}, \cdots, a_{54}^{(l)})$ are linearly independent and $(a_0^{(\rho)}, \cdots, a_{54}^{(\rho)}) = (0, \cdots, 0)$ for $l + 1 \leq \rho \leq D$. Let $E_\rho (1 \leq \rho \leq D)$ denote the equation

$$\sum_{i=0}^{54} a_i^{(\rho)} x_i + \sum_{0 \leq j \leq k \leq 109} b_{jk}^{(\rho)} F_j F_k + \sum_{j=0}^{109} c_j^{(\rho)} F_j + d^{(\rho)} = 0. \tag{3.3}$$

The work above depends only on any given public key, and it can be solved once for all cryptanalysis under that public key.

3.2 Deriving Linear Equations Satisfied by Plaintext

Let's assume we have a valid ciphertext $y' = (y'_0, \cdots, y'_{109})$. Our goal is to find its corresponding plaintext $x' = (x'_0, \cdots, x'_{54})$.

Substituting $(F_0, \cdots, F_{109}) = (y'_0, \cdots, y'_{109})$ into equations $E_1, \cdots, E_l$, we derive l linearly independent linear equations in $x_0, \cdots, x_{54}$, which are denoted by $E'_1, \cdots, E'_l$. These l equations are also satisfied by x'. Doing a simple Gaussian elimination, from these l equations we can represent l variables of $x_0, \cdots, x_{54}$ by linear combinations of other $55 - l$. That is, we can find two disjoint subsets of $\{0, \cdots, 54\}$, $A'_1 = \{v'_1, \cdots, v'_l\}$ and $A_1 = \{v_1, \cdots, v_{55-l}\}$, and linear expressions

$$x_{v'_j} = h_j(x_{v_1}, \cdots, x_{v_{55-l}}), 1 \leq j \leq l \tag{3.4}$$

such that $E'_1, \cdots, E'_l$ holds when (3.4) are substituted into them.

To put some calculations in one-time precomputation and make our attack more efficient, we can further refine the analysis about h_j. Clearly, only the constant term in h_j relies on y', the coefficients of the linear monomials in h_j rely on only the public key of the TTM scheme. Let W denote a $(55-l)$-dimensional affine subspace of $\mathbb{K}^{55}$, the component $x_{v'_j}$ of any vector $(x_0,\cdots,x_{54})$ in W is $h_j(x_{v_1},\cdots,x_{v_{55-l}})$. Each vector $x=(x_0,\cdots,x_{54})$ in W satisfies $\sum\limits_{i=0}^{54} a_i^{(\rho)}x_i = t_\rho$, $0\le\rho\le l$, where

$$t_\rho = \sum_{0\le j\le k\le 109} b_{jk}^{(\rho)} y'_j y'_k + \sum_{j=0}^{109} c_j^{(\rho)} y'_j + d^{(\rho)} \tag{3.5}$$

is a constant independent of $(x_0,\cdots,x_{54})$.

Since each equation in (3.1) is an element of V and hence a linear combination of $E_1,\cdots,E_D$, the linear part (i.e., excluding the constant term part of an affine function) of each $\bar{x}_i$ $(45\le i\le 49)$ at $x\in W$ is a linear combination of $\sum\limits_{i=0}^{54} a_i^{(\rho)}x_i$ $(1\le\rho\le l)$, that is, it is a linear combination of constants $t_1,\cdots,t_l$. Hence, as functions in $x_{v_1},\cdots,x_{v_{55-l}}$, all $R_i=\bar{x}_{44+i}$ $(1\le i\le 5)$ are constants on W. Let they be $r_1,\cdots,r_5$, respectively.

Now substitute (3.4) into $F_j(x_0,\cdots,x_{54})$ and derive 110 new quadratic functions $\hat{F}_j(x_{v_1},\cdots,x_{v_{55-l}})$ $(0\le j\le 109)$. The quadratic monomials of $\hat{F}_j$ rely on only the public key since so do the coefficients of the linear monomials of h_j.

3.3 Trivializing the Lock Polynomials

To continue the attack, we utilize the following equations stemming from the definition of the lock polynomials:

$$\begin{cases} \bar{y}_{50}+\bar{x}_{46}\bar{x}_{48}+\bar{x}_{47}\bar{x}_{49}+\bar{x}_{50}=\bar{y}_{50}+R_2R_4+R_3R_5+\bar{x}_{50}=0;\\ \bar{y}_{51}+\bar{x}_{45}\bar{x}_{47}+\bar{x}_{48}\bar{x}_{49}+\bar{x}_{51}=\bar{y}_{51}+R_1R_3+R_4R_5+\bar{x}_{51}=0;\\ \bar{y}_{52}+\bar{x}_{45}\bar{x}_{48}+\bar{x}_{46}\bar{x}_{49}+\bar{x}_{52}=\bar{y}_{52}+R_1R_4+R_2R_5+\bar{x}_{52}=0;\\ \bar{y}_{53}+\bar{x}_{45}\bar{x}_{49}+\bar{x}_{46}\bar{x}_{47}+\bar{x}_{53}=\bar{y}_{53}+R_1R_5+R_2R_3+\bar{x}_{53}=0;\\ \bar{y}_{54}+\bar{x}_{45}\bar{x}_{46}+\bar{x}_{47}\bar{x}_{48}+\bar{x}_{54}=\bar{y}_{54}+R_1R_2+R_3R_4+\bar{x}_{54}=0. \end{cases} \tag{3.6}$$

On W, (3.6) is

$$\begin{cases} \bar{y}_{50}+\bar{x}_{50}+s_1=0;\\ \bar{y}_{51}+\bar{x}_{51}+s_2=0;\\ \bar{y}_{52}+\bar{x}_{52}+s_3=0;\\ \bar{y}_{53}+\bar{x}_{53}+s_4=0;\\ \bar{y}_{54}+\bar{x}_{54}+s_5=0, \end{cases} \tag{3.7}$$

where $s_1,\cdots,s_5$ are constants defined by $s_1=r_2r_4+r_3r_5$, $s_2=r_1r_3+r_4r_5$, $s_3=r_1r_4+r_2r_5$, $s_4=r_1r_5+r_2r_3$, and $s_5=r_1r_2+r_3r_4$. Through linear transformation ϕ_1 and ϕ_4^{-1}, equation (3.7) implies that there exist quadratic equations in $x_{v_1},\cdots,x_{v_{55-l}}$ of the form

$$\sum_{i=1}^{55-l}\hat{a}_i x_{v_i} + \sum_{j=0}^{109}\hat{b}_j\hat{F}_j + \hat{d} = 0, \tag{3.8}$$

where $(\hat{b}_0,\cdots,\hat{b}_{109})\neq(0,\cdots,0)$.

To find all equations of the form (3.8), we can use the same method as the one used for equations (3.2). But the case is simpler and easier since far fewer unknowns are involved here.

To again improve efficiency by utilizing one-time precomputation, we use another alternative method, that is, we expand each $\hat{F}_j$ and compare the coefficients of quadratic monomials in $x_{v_1}, \cdots, x_{v_{55-l}}$ in the two sides of (3.8), we derive a system of linear equations in $\hat{b}_0, \cdots, \hat{b}_{109}$. Since quadratic monomials are of the form x_i^2 or $x_i x_j$ for $i \neq j$, this system has

$$\binom{55-l}{1} + \binom{55-l}{2} = (56-l)(55-l)/2$$

equations. It also depends on only the public key. Let $\hat{D}$ and $\{(\hat{b}_0^{(\rho)}, \cdots, \hat{b}_{109}^{(\rho)}) : 1 \leq \rho \leq \hat{D}\}$ be the dimension and a basis of the solution space of this system, respectively.

Substituting $(\hat{b}_0^{(\rho)}, \cdots, \hat{b}_{109}^{(\rho)})$ into (3.8) and comparing constant terms and coefficients of linear monomials in $x_{v_1}, \cdots, x_{v_{55-l}}$ in the two sides, we uniquely determine the other coefficients in (3.8), $\hat{a}_1^{(\rho)}, \cdots, \hat{a}_{55-l}^{(\rho)}$ and $\hat{d}^{(\rho)}$, because they are determined by the $\hat{b}_j^{(\rho)}$ $(0 \leq j \leq 109)$ and the linear and constant terms of the $\hat{F}_j$ $(0 \leq j \leq 109)$. These coefficients depend on specific values of the ciphertext y', since the linear and constant terms of the $\hat{F}_j$ depend on the constant terms of the h_j.

Let

$$\{(\hat{a}_1^{(\rho)}, \cdots, \hat{a}_{55-l}^{(\rho)}, \hat{b}_0^{(\rho)}, \cdots, \hat{b}_{109}^{(\rho)}, d^{(\rho)}), 1 \leq \rho \leq \hat{D}\}$$

be a basis of the space of the coefficient vectors of the equations of the form (3.8). Rearranging these basis vectors, we assume that $(\hat{a}_1^{(1)}, \cdots, \hat{a}_{55-l}^{(1)})$, $\cdots$, $(\hat{a}_1^{(k)}, \cdots, \hat{a}_{55-l}^{(k)})$ are linearly independent and the other vectors $(\hat{a}_1^{(i)}, \cdots, \hat{a}_{55-l}^{(i)})$ $(k+1 \leq i \leq \hat{D})$ are their linear combinations. Let $\hat{E}_\rho$ denote the equation

$$\sum_{i=1}^{55-l} \hat{a}_i^{(\rho)} x_{v_i} + \sum_{j=0}^{109} \hat{b}_j^{(\rho)} \hat{F}_j + \hat{d}^{(\rho)} = 0, \tag{3.9}$$

$1 \leq \rho \leq k$. These k equations are satisfied by all $(x_{v_1}, \cdots, x_{v_{55-l}}) \in K^{55-l}$.

Substituting $(\hat{F}_0, \cdots, \hat{F}_{109})$ by y' into (3.9), we derive the equation $\hat{E}'_\rho$:

$$\sum_{i=1}^{55-l} \hat{a}_i^{(\rho)} x_{v_i} + \hat{r}_\rho = 0, \tag{3.10}$$

where $\hat{r}_\rho = \sum\limits_{j=0}^{109} \hat{b}_j^{(\rho)} y'_j + \hat{d}^{(\rho)}$, $1 \leq \rho \leq k$. Doing a Gaussian elimination on $\hat{E}'_\rho (1 \leq \rho \leq k)$, we will find two disjoint subsets of $\{v_1, \cdots, v_{55-l}\}$: $A'_2 = \{w'_1, \cdots, w'_k\}$ and $A_2 = \{w_1, \cdots, w_{55-l-k}\}$, and linear functions in $x_{w_1}, \cdots, x_{w_{55-l-k}}$,

$$x_{w'_i} = \hat{h}_i(x_{w_1}, \cdots, x_{w_{55-l-k}}), 1 \leq i \leq k \tag{3.11}$$

such that (3.10) holds when (3.11) are substituted into it. We substitute (3.11) into $\hat{F}_j(x_{v_1}, \cdots, x_{v_{55-l}})$ to derive $\tilde{F}_j(x_{w_1}, \cdots, x_{w_{55-l-k}})$, $0 \leq j \leq 109$.

Let $\hat{W}$ denote a $(55-l-k)$-dimensional affine subspace of W, where for each vector $(x_0, \cdots, x_{54})$ in $\hat{W}$, $x_{w'_i}$ is substituted by (3.11) for any $1 \leq i \leq k$. Thus, every vector $(x_0, \cdots, x_{54})$ in $\hat{W}$ satisfies (3.10).

Restricting on $\hat{W}$, each equation in (3.6) is a linear combination of $\hat{E}_1, \cdots, \hat{E}_{\hat{D}}$, and hence, the linear part of $\bar{x}_i$ $(50 \leq i \leq 54)$ is a linear combination of $\sum_{i=1}^{55-l} \hat{a}_i^{(\rho)} x_{v_i}$, $(1 \leq \rho \leq k)$, i.e., a linear combination of $\hat{r}_1, \cdots, \hat{r}_k$, which is a constant independent of $x \in \hat{W}$. Therefore, $\bar{x}_{50}$, $\bar{x}_{51}$, $\bar{x}_{52}$, $\bar{x}_{53}$, and $\bar{x}_{54}$ are all constant on $\hat{W}$.

By the definitions of R_i, S_i, and G_i, they are all constants on $\hat{W}$ as functions in $x_0, \cdots, x_{54}$. Let G_i be g_i, $g_i \in K$, $i = 0, \cdots, 6$.

3.4 Finding the Plaintext

The analysis mentioned in the previous subsection is a step of trivializing lock polynomials. Although we do not know the concrete values of g_i, we know all G_i are constant on $\hat{W}$. This fact is used below to complete the remaining steps of our attack. We also use the fact that $\bar{y}_0 := \phi_{2,0}(\bar{x}_0, \cdots, \bar{x}_{54}) = \bar{x}_0$ and $\bar{y}_1 := \phi_{2,1}(\bar{x}_0, \cdots, \bar{x}_{54}) = f_1(\bar{x}_0) + \bar{x}_1$ for some quadratic f_1; please refer to the appendix.

Because ϕ_{32} is a tame triangular transformation on $\phi_1(\hat{W})$, set $\phi_{321} = \phi_{32} \circ \phi_1$. Since

$$\phi_{321,0}(x_0, \cdots, x_{54}) = \phi_{32,0}(\bar{x}_0, \cdots, \bar{x}_{54}) = (\bar{y}_0 + G_0(\bar{x}_0, \cdots, \bar{x}_{54})),$$

for $(x_0, \cdots, x_{54}) \in \hat{W}$, we have

$$\phi_{4,0}^{-1}(\tilde{F}) = \phi_{321,0}(x_0, \cdots, x_{54}) = \phi_{1,0}(x_0, \cdots, x_{54}) + g_0.$$

So there must exist identical equations of the form

$$\sum_{i=0}^{55-l-k} \tilde{a}_i x_{w_i} + \sum_{j=0}^{109} \tilde{b}_j \tilde{F}_j + \tilde{d} = 0, \tag{3.12}$$

which are satisfied by all $(x_{w_1}, \cdots, x_{w_{55-l-k}}) \in K^{55-l-k}$ and the coefficients $(\tilde{b}_0, \cdots, \tilde{b}_{109}) \neq (0, \cdots, 0)$.

Similarly to (3.8), we can derive a basis of linear space of all coefficient vectors $(\tilde{a}_1, \cdots, \tilde{a}_{55-l-k}, \tilde{b}_0, \cdots, \tilde{b}_{109}, \tilde{d})$ satisfying (3.12). Write these basis vectors as row vectors to get a matrix and change it into a top triangular matrix by row transformations. Substitute $\tilde{F}_i$ by y'_i in the equations (3.12) corresponding to each row of the matrix with $(\tilde{a}_1, \cdots, \tilde{a}_{55-l-k}) \neq (0, \cdots, 0)$, then we derive some, say p, linearly independent linear equations in $x_{w_1}, \cdots, x_{w_{55-l-k}}$. Therefore we can represent p variables of $x_{w_1}, \cdots, x_{w_{55-l-k}}$ as linear expressions of the remaining variables. We also derive a $(55-l-k-p)$-dimensional affine subspace

$\tilde{W}$ of $\hat{W}$. Let $x_{u_1}, \cdots, x_{u_{55-l-k-p}}$ be the remaining variables. For the same reason as mentioned above, $\phi_{1,0}(x_0, \cdots, x_{54})$, and hence $f_1(\phi_{1,0}(x_0, \cdots, x_{54}))$, are constant on $\tilde{W}$.

Let $\tilde{\tilde{F}}_i(x_{u_1}, \cdots, x_{u_{55-l-k-p}})$ denote the p-variable-eliminated function $\tilde{F}_i(x_{w_1}, \cdots, x_{w_{55-l-k}})$. Let $g_1' = g_1 + f_1(\phi_{1,0}(x_0, \cdots, x_{54}))$. Again, we have

$$\phi_{4,1}^{-1}(\tilde{\tilde{F}}) = \phi_{321,1}(x_0, \cdots, x_{54}) = \phi_{1,1}(x_0, \cdots, x_{54}) + g_1',$$

$(x_0, \cdots, x_{54}) \in \tilde{W}$, and we know there exist identical equations in $(x_{u_1}, \cdots, x_{u_{55-l-k-p}})$ of the form

$$\sum_{i=0}^{55-l-k-p} \tilde{\tilde{a}}_i x_{w_i} + \sum_{j=0}^{109} \tilde{\tilde{b}}_j \tilde{\tilde{F}}_j + \tilde{\tilde{d}} = 0 \tag{3.13}$$

with $(\tilde{\tilde{b}}_0, \cdots, \tilde{\tilde{b}}_{109}) \neq (0, \cdots, 0)$.

Repeating similar steps of eliminating and substituting variables, we derive in turn smaller and smaller affine subspaces of $\tilde{W}$. On these subspaces, we have in turn $\phi_{1,1}(x_0, \cdots, x_{54})$, $f_2(\phi_{1,0}, \phi_{1,1})$, $\cdots$, $\phi_{1,20}(x_0, \cdots, x_{54})$, $f_{21}(\phi_{1,0}, \cdots, \phi_{1,20})$, $\phi_{1,21}(x_0, \cdots, x_{54})$, $\cdots$, and $\phi_{1,54}(x_0, \cdots, x_{54})$ are constant. Since $\phi_{1,0}(x_0, \cdots, x_{54})$, $\cdots$, and $\phi_{1,54}(x_0, \cdots, x_{54})$ are constants on the last subspace and ϕ_1 is an invertible map, $(x_0, \cdots, x_{54})$ is a constant vector on that subspace. This means that this affine subspace is a point (i.e., the 0-dimensional subspace). This point is exactly the plaintext.

Collecting all linear expressions between variables, we get the plaintext. Now the attack is accomplished.

3.5 A Practical Attack Procedure and Its Complexity

The attack in the previous subsections can be further divided into the following six steps. The first three steps are independent of the value of the ciphertext y' and can be done once for a given public key.

Step 1 of the attack. *Find a basis of the linear space of the coefficient vectors* (a_i, b_{jk}, c_j, d) *of the identical equations*

$$\sum_{i=0}^{54} a_i x_i + \sum_{0 \leq j \leq k \leq 109} b_{jk} F_j F_k + \sum_{j=0}^{109} c_j F_j + d = 0.$$

As mentioned in subsection 3.1, we randomly select 7000 plaintexts $(x_0, \cdots, x_{54})$ and substitute them into equation (3.2) to get a linear system of 7000 equations on 6271 unknowns. The computational complexity to solve it is $6271^2 \cdot 7000 \leq 2^{38}$ operations on the finite field $K = \mathbb{F}_{2^8}$. Reorder the resulting basis vectors such that $(a_0^{(\rho)}, \cdots, a_{54}^{(\rho)}) = (0, \cdots, 0)$ for $l+1 \leq \rho \leq D$, and that for the $l \times 55$ matrix with $(a_0^{(\rho)}, \cdots, a_{54}^{(\rho)})$ as its ρ-th row and its v_1'-,v_2'-, $\cdots$, v_l'-columns form an identity matrix of order l. (Let the columns are indexed by $0, 1, \cdots$, and 54.)

Step 2 of the attack. *Let* $\{v_1, \cdots, v_{55-l}\} = \{0, \cdots, 54\} \setminus \{v'_1, \cdots, v'_l\}$. *Represent the variables* $x_{v'_1}, x_{v'_2}, \cdots,$ *and* $x_{v'_l}$ *as linear expressions of the form*

$$h_j(x_{v_1}, \cdots, x_{v_{55-l}}) = \sum_{i=1}^{55-l} h_{j,i} x_{v_i} + t_j,$$

respectively, $1 \leq j \leq l$, *according to the system of* l *linear equations*

$$\sum_{i=0}^{54} a_i^{(\rho)} x_i = t_\rho, 1 \leq \rho \leq l.$$

Substitute $x_{v'_j}$ *by* $h_j(x_{v_1}, \cdots, x_{v_{55-l}})$ $(1 \leq j \leq l)$ *into the expressions* $F_i(x_0, \cdots, x_{54})$ $(0 \leq i \leq 109)$ *for the public key, and derive 110 new quadratic polynomials* $\hat{F}_i(x_{v_1}, \cdots, x_{v_{55-l}})$, $0 \leq i \leq 109$. *The coefficients of quadratic terms in* $\hat{F}_i$ *are independent of* $t_1, \cdots, t_l$.

The first part of this step costs no computation. The second substitution part is of computational complexity about

$$55l(l+3)(55-l)(56-l) < 2^{23}.$$

Step 3 of the attack. *Comparing the coefficients of quadratic terms in the two sides of the equation*

$$\sum_{j=0}^{109} \hat{b}_j \hat{F}_j(x_{v_1}, \cdots, x_{v_{55-l}}) = 0$$

to derive a system of $(55-l)(56-l)/2$ *linear equations on* $\hat{b}_0, \cdots, \hat{b}_{109}$. *Then use Gaussian elimination to find a basis of its solution space,* $\{(\hat{b}_0^{(\rho)}, \cdots, \hat{b}_{109}^{(\rho)}), 1 \leq \rho \leq k\}$.

The computational complexity of this step is

$$110^2 \cdot (55-l)(56-l)/2 < 2^{13}(56-l)^2 < 2^{24}.$$

The above three steps can be precomputed for any given public key. The total complexity is less than 2^{38}. In what follows, we go to break the corresponding plaintext of a specific valid ciphertext $y' = (y'_0, \cdots, y'_{109})$.

Step 4 of the attack. *First, substitute* $y' = (y'_0, \cdots, y'_{109})$ *into (3.5) to obtain* $t_1, \cdots, t_l$ *and substitute* $t_1, \cdots, t_l$ *into* $\hat{F}_i$ *to get simplified* $\hat{F}_i$. *Then for each* $(\hat{b}_0^{(\rho)}, \cdots, \hat{b}_{109}^{(\rho)})$, *compare the coefficients of the linear and constant terms in the two sides of (3.9) to determine* $\hat{a}_0^{(\rho)}, \cdots, \hat{a}_{54-l}^{(\rho)}$ *and* $d^{(\rho)}$.

The computational complexity of substitution is

$$(2 \times (\binom{110}{1} + \binom{110}{2}) + \binom{110}{1}) \times l \approx 2^{14} l < 2^{17}.$$

The complexity of calculating $\hat{a}_0^{(\rho)}, \cdots, \hat{a}_{54-l}^{(\rho)}$ and $d^{(\rho)}$ is $(56-l)^2 \hat{D} < 2^{15}$.

Step 5 of the attack. *Do primary transformations (similar as primary row transformations on matrices) on the vectors*

$$(\hat{a}_1^{(\rho)}, \cdots, \hat{a}_{55-l}^{(\rho)}, \hat{b}_0^{(\rho)}, \cdots, \hat{b}_{109}^{(\rho)}, \hat{d}^{(\rho)}), 1 \leq \rho \leq \hat{D}$$

obtained in Step 4 to make $(\hat{a}_1^{(\rho)}, \cdots, \hat{a}_{55-l}^{(\rho)})$ *(*$1 \leq \rho \leq k$*) are linearly independent and* $(\hat{a}_1^{(\rho)}, \cdots, \hat{a}_{55-l}^{(\rho)}) = (0, \cdots, 0)$ *for* $k+1 \leq \rho \leq \hat{D}$*. Calculate*

$$\hat{r}_\rho = \sum_{j=0}^{109} \hat{b}_j^{(\rho)} y'_j + \hat{d}^{(\rho)},$$

$1 \leq \rho \leq k$*, and do a Gaussian elimination on the system of linear equations*

$$\sum_{i=1}^{55-l} \hat{a}_i^{(\rho)} x_{v_i} + \hat{r}_\rho = 0, 1 \leq \rho \leq k$$

to eliminate k variables by expressing them as linear expressions in the remaining variables, $x_{w'_j} = \hat{h}_j(x_{w_1}, \cdots, x_{w_{55-l-k}})$*, where* $1 \leq j \leq k$ *and* $\{w'_1, \cdots, w'_k\}$ *and* $\{w_1, \cdots, w_{55-l-k}\}$ *are two disjoint subsets of* $\{v_1, \cdots, v_{55-l}\}$*. Substitute* $x_{w'_j}$ *by* $\hat{h}_j(x_{w_1}, \cdots, x_{w_{55-l-k}})$ *(*$1 \leq j \leq k$*) into* $\hat{F}_i(x_{v_1}, \cdots, x_{v_55-l})$ *to derive 110 polynomials* $\tilde{F}_i(x_{w_1}, \cdots, x_{w_{55-l-k}})$*,* $0 \leq i \leq 109$*.*

The computational complexity of primary transformations on the vectors is

$$(55 - l + 110 + 1)^2 \hat{D} = (166 - l)^2 \hat{D} < 2^{18}.$$

To calculate $\hat{r}_\rho$, the complexity is $110k < 2^8 k < 2^{11}$, while the complexity of solving the system of linear equations (3.10) is $(55 - l)^2 k < 2^{14}$. Finally, the computational complexity of substituting $x_{w'_j} = \hat{h}_j(x_{w_1})$ into $\tilde{F}_i(x_{v_1}, \cdots, x_{54})$ $(0 \leq i \leq 109)$ is

$$55(k(k+3)(55 - l - k)(56 - l - k)) < 2^{23}.$$

The total complexity of this step is less than $2^{18} + 2^{11} + 2^{14} + 2^{23} < 2^{24}$.

Step 6 of the attack. *Compare the coefficients of all terms in the two sides of the equation*

$$\sum_{i=0}^{55-l-k} \tilde{a}_i x_{w_i} + \sum_{j=0}^{109} \tilde{b}_j \tilde{F}_j + \tilde{d} = 0$$

to derive a system of linear equations in $(\tilde{a}_1, \cdots, \tilde{a}_{55-l-k}, \tilde{b}_0, \cdots, \tilde{b}_{109}, \tilde{d})$*. Solve it to find a basis of its solution space,* $(\tilde{a}_1^{(\rho)}, \cdots, \tilde{a}_{55-l-k}^{(\rho)}, \tilde{b}_0^{(\rho)}, \cdots, \tilde{b}_{109}^{(\rho)}, \tilde{d}^{(\rho)})$*,* $1 \leq \rho \leq \hat{p}$*, where* $\hat{p}$ *is its dimension. Among these vectors, select a set of vectors with maximal number, say p, such that for these p vectors,*$(\tilde{a}_1^{(\rho)}, \cdots, \tilde{a}_{55-l-k}^{(\rho)})$ *are linearly independent. Let* $\tilde{F}_i = y'_i$ *(*$0 \leq i \leq 109$*) in(3.12) and solve the resulting system of linear equations on* $x_{w_1}, \cdots, x_{w_{55-l-k}}$*. Again we will eliminate*

p variables by expressing them as linear functions of remaining variables. We substitute these linear functions into $\tilde{F}_i$ ($0 \leq i \leq 109$) to derive 110 quadratic functions with smaller variables. Iterate the above process till all variables are eliminated. Then we collect all linear expressions between the variables and derive the plaintext $x' = (x'_0, \cdots, x'_{54})$.

The number of iterations is less than $55-l-k$ and the computation complexity of each iteration is less than $2^{24} + 2^{16} + 2^{24} < 2^{25}$. Hence the total complexity of this step is less than $2^{25}(55 - l - k) < 2^{31}$.

The largest computational complexity occurs in the first step with complexity less then 2^{38}; the complexity of other steps is minor in comparison. Hence, the total computation is less than 2^{39} $\mathbb{F}_{2^8}$-operations.

3.6 Experimental Results

We implement our attack on a Pentium IV 2.4Ghz PC with 256M memory, and we code the attack using VC++. We choose 100 different public keys, for each of which we give a ciphertext and try to find its corresponding plaintext. In TTM, each public key is a composition of ϕ_1, ϕ_{32}, and ϕ_4, and ϕ_{32} is determined by 25 randomly taken quadratic polynomials $f_i(x_0, \cdots, x_{i-1})$ ($i = 1, \cdots, 21$) and $f_i(x_0, \cdots, x_{54})$ ($i = 106, \cdots, 109$). We choose 10 different sets of the f_i, for each of which we choose 10 different pairs of ϕ_1 and ϕ_4 for experiments. The results are as follows:

1. For all 100 chosen ciphertexts, the attack successively finds their corresponding plaintexts. To find each plaintext, less than 1 hour and 37 minutes in total cost on the PC mentioned above, where 95 minutes cost on the execution of the step 1 in subsection (3.5), while about 1 minute and 20 seconds cost to execute the all remaining steps. Hence, the attack is very efficient. This timing data coincides with the analysis in the previous subsection: the remaining steps of the attack is about $2^{38}/2^{31} = 128$ times faster than the first.
2. For each chosen public key, the experiment finds $D = l = 5$ in step 1 and $\hat{D} = k = 5$ in step 3 and step 5. This means that we can eliminate 5 variables in step 2 and 5 variables in step 5. The experiment shows that if ϕ_1 is the identical map, we will find directly the values of $x'_{45}, \cdots, x'_{49}$ of the plaintext in step 1 and of $x'_{50}, \cdots, x'_{54}$ in step 5.
3. If we derive the systems of equations (3.8), (3.12) and (3.13) by taking sufficiently many (concretely, 200) plaintext/ciphertext pairs in the experiment, that is, not by comparing coefficients of monomials, then for each given ϕ_{32}, the number of total iterations of steps 4-6 and the numbers of the variables eliminated in each iteration in step 6 are respectively the same for the 10 chosen different pairs of ϕ_1 and ϕ_4. This can easily analyzed theoretically.

4 Conclusion and Discussion

In this paper, we present a very efficient attack on a new instance of TTM in [MCY04]. We need to do first precomputation, which takes 95 minutes on a PC with a 2.4Ghz Pentium IV processor. Our attack then can recover the corresponding plaintext of any valid ciphertext in less than 2 minutes. The computational complexity of the precomputation is 2^{38} $\mathbb{F}_{2^8}$-operations and the complexity for deriving a plaintext from a ciphertext is 2^{31}. Therefore the total complexity is less than 2^{39} and this new TTM instance is totally insecure. We think everyone should take our attack method into consideration when designing new MPKC.

The key point of the attack is finding the existence of certain quadratic relation (not linearization equations) on plaintexts and ciphertexts, which is used to trivialize the lock polynomials defined in TTM.

Like the previous ones, this instance of TTM has a very rigid structure and is not scalable, thus it is not possible to give a toy example to illustrate our attack and give the computation complexity in terms of a function of the dimensions of the plaintext and ciphertext space. We can only present the concrete complexity value for this instance.

Although the new instance of TTM is broken, TTM is still a very interesting idea, which could have great potential due to its high efficiency, if it can be made secure. We think, to make the TTM work, one must develop a systematic method to establish lock polynomials, which seems to require some deep insight from algebraic geometry.

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.

[CP03] N.Courtois and J.Patarin. About the XL algorithm over *GF*(2). *CT-RSA'2003*,pages 141-157,2003.

[DH03] J.Ding and T.Hodges. Cryptanalysis of an Implementation Scheme of TTM. *J. Algebra Appl.*, pages 273-282, 2004. http://eprint.iacr.org/2003/084.

[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.

[MI88] T.Matsumoto and H.Imai. Public quadratic polynomial-tuples for efficient signature verification and message encryption. In C. G. Guenther, editor, *Advances in cryptology –EUROCRYPT'88, LNCS*, volume 330, pages 419–453. Springer, 1988.

[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.

[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.

[Sho97] P.Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing,* 26(5):1484-1509, October 1997.

Appendix: The Description of ϕ_2

The expressions of $(\bar{y}_0, \cdots, \bar{y}_{109}) = \phi_2(\bar{x}_0, \cdots, \bar{x}_{54})$ are listed as follows, where $f_i(\bar{x}_0, \cdots, \bar{x}_{i-1})$ $(1 \leq i \leq 21)$ and $f_i(\bar{x}_0, \cdots, \bar{x}_{54})$ $(106 \leq i \leq 109)$ are randomly chosen quadratic polynomials.

$\bar{y}_0 := \bar{x}_0;$ $\bar{y}_1 := f_1 + \bar{x}_1;$
$\bar{y}_2 := f_2 + \bar{x}_2;$ $\bar{y}_3 := f_3 + \bar{x}_3;$
$\bar{y}_4 := f_4 + \bar{x}_4;$ $\bar{y}_5 := f_5 + \bar{x}_5;$
$\bar{y}_6 := f_6 + \bar{x}_6;$ $\bar{y}_7 := f_7 + \bar{x}_7;$
$\bar{y}_8 := f_8 + \bar{x}_8;$ $\bar{y}_9 := f_9 + \bar{x}_9;$
$\bar{y}_{10} := f_{10} + \bar{x}_{10};$ $\bar{y}_{11} := f_{11} + \bar{x}_{11};$
$\bar{y}_{12} := f_{12} + \bar{x}_{12};$ $\bar{y}_{13} := f_{13} + \bar{x}_{13};$
$\bar{y}_{14} := f_{14} + \bar{x}_{14};$ $\bar{y}_{15} := f_{15} + \bar{x}_{15};$
$\bar{y}_{16} := f_{16} + \bar{x}_{16};$ $\bar{y}_{17} := f_{17} + \bar{x}_{17};$
$\bar{y}_{18} := f_{18} + \bar{x}_{18};$ $\bar{y}_{19} := f_{19} + \bar{x}_{19};$
$\bar{y}_{20} := f_{20} + \bar{x}_{20};$ $\bar{y}_{21} := f_{21} + \bar{x}_{21};$
$\bar{y}_{22} := \bar{x}_0\bar{x}_5 + \bar{x}_1\bar{x}_4 + \bar{x}_8 + \bar{x}_{22};$ $\bar{y}_{23} := \bar{x}_0\bar{x}_6 + \bar{x}_2\bar{x}_4 + \bar{x}_{23};$
$\bar{y}_{24} := \bar{x}_1\bar{x}_6 + \bar{x}_2\bar{x}_5 + \bar{x}_{24};$ $\bar{y}_{25} := \bar{x}_3\bar{x}_5 + \bar{x}_1\bar{x}_7 + \bar{x}_{25};$
$\bar{y}_{26} := \bar{x}_3\bar{x}_4 + \bar{x}_0\bar{x}_7 + \bar{x}_{26};$ $\bar{y}_{27} := \bar{x}_2\bar{x}_9 + \bar{x}_{22}\bar{x}_3 + \bar{x}_{27};$
$\bar{y}_{28} := \bar{x}_6\bar{x}_9 + \bar{x}_{22}\bar{x}_7 + \bar{x}_{28};$ $\bar{y}_{29} := \bar{x}_{10}\bar{x}_7 + \bar{x}_8\bar{x}_6 + \bar{x}_{29};$
$\bar{y}_{30} := \bar{x}_{10}\bar{x}_3 + \bar{x}_2\bar{x}_8 + \bar{x}_{30};$ $\bar{y}_{31} := \bar{x}_{11}\bar{x}_{16} + \bar{x}_{12}\bar{x}_{15} + \bar{x}_{19} + \bar{x}_{31};$
$\bar{y}_{32} := \bar{x}_{11}\bar{x}_{17} + \bar{x}_{13}\bar{x}_{15} + \bar{x}_{32};$ $\bar{y}_{33} := \bar{x}_{12}\bar{x}_{17} + \bar{x}_{13}\bar{x}_{16} + \bar{x}_{33};$
$\bar{y}_{34} := \bar{x}_{14}\bar{x}_{16} + \bar{x}_{12}\bar{x}_{18} + \bar{x}_{34};$ $\bar{y}_{35} := \bar{x}_{14}\bar{x}_{15} + \bar{x}_{11}\bar{x}_{18} + \bar{x}_{35};$
$\bar{y}_{36} := \bar{x}_{13}\bar{x}_{20} + \bar{x}_{31}\bar{x}_{14} + \bar{x}_{36};$ $\bar{y}_{37} := \bar{x}_{17}\bar{x}_{20} + \bar{x}_{31}\bar{x}_{18} + \bar{x}_{37};$
$\bar{y}_{38} := \bar{x}_{21}\bar{x}_{18} + \bar{x}_{19}\bar{x}_{17} + \bar{x}_{38};$ $\bar{y}_{39} := \bar{x}_{21}\bar{x}_{14} + \bar{x}_{13}\bar{x}_{19} + \bar{x}_{39};$
$\bar{y}_{40} := \bar{x}_{11}\bar{x}_{12} + \bar{x}_1\bar{x}_0 + \bar{x}_{39} + \bar{x}_{40};$ $\bar{y}_{41} := \bar{x}_{11}\bar{x}_2 + \bar{x}_{13}\bar{x}_0 + \bar{x}_{41};$
$\bar{y}_{42} := \bar{x}_1\bar{x}_2 + \bar{x}_{13}\bar{x}_{12} + \bar{x}_{42};$ $\bar{y}_{43} := \bar{x}_3\bar{x}_{12} + \bar{x}_1\bar{x}_{14} + \bar{x}_{43};$
$\bar{y}_{44} := \bar{x}_3\bar{x}_0 + \bar{x}_{11}\bar{x}_{14} + \bar{x}_{44};$ $\bar{y}_{45} := \bar{x}_{32}\bar{x}_{18} + \bar{x}_{14}\bar{x}_{33} + \bar{x}_{13}\bar{x}_{34} + \bar{x}_{17}\bar{x}_{35} + \bar{x}_{45};$
$\bar{y}_{46} := \bar{x}_{37}\bar{x}_{13} + \bar{x}_{39}\bar{x}_{18} + \bar{x}_{36}\bar{x}_{17} + \bar{x}_{38}\bar{x}_{14} + \bar{x}_{46};$ $\bar{y}_{47} := \bar{x}_{23}\bar{x}_7 + \bar{x}_3 x_{24} + \bar{x}_2\bar{x}_{25} + \bar{x}_6\bar{x}_{26} + \bar{x}_{47};$
$\bar{y}_{48} := \bar{x}_{28}\bar{x}_2 + \bar{x}_{30}\bar{x}_7 + \bar{x}_{27}\bar{x}_6 + \bar{x}_{29}\bar{x}_3 + \bar{x}_{48};$ $\bar{y}_{49} := \bar{x}_{14}\bar{x}_{41} + \bar{x}_3\bar{x}_{42} + \bar{x}_{13}\bar{x}_{43} + \bar{x}_2\bar{x}_{44} + \bar{x}_{49};$
$\bar{y}_{50} = \bar{x}_{46}\bar{x}_{48} + \bar{x}_{47}\bar{x}_{49} + \bar{x}_{50};$ $\bar{y}_{51} := \bar{x}_{45}\bar{x}_{47} + \bar{x}_{48}\bar{x}_{49} + \bar{x}_{51};$
$\bar{y}_{52} := \bar{x}_{45}\bar{x}_{48} + \bar{x}_{46}\bar{x}_{49} + \bar{x}_{52};$ $\bar{y}_{53} := \bar{x}_{45}\bar{x}_{49} + \bar{x}_{46}\bar{x}_{47} + \bar{x}_{53};$
$\bar{y}_{54} := \bar{x}_{45}\bar{x}_{46} + \bar{x}_{47}\bar{x}_{48} + \bar{x}_{54};$ $\bar{y}_{55} := \bar{x}_{11}\bar{x}_{42} + \bar{x}_1\bar{x}_{41} + \bar{x}_{13}\bar{x}_{39} + \bar{x}_3\bar{x}_{30};$
$\bar{y}_{56} := \bar{x}_0\bar{x}_{43} + \bar{x}_{12}\bar{x}_{44} + \bar{x}_2\bar{x}_{29} + \bar{x}_{14}\bar{x}_{40};$ $\bar{y}_{57} := \bar{x}_0\bar{x}_{42} + \bar{x}_{12}\bar{x}_{41} + \bar{x}_2\bar{x}_{39} + \bar{x}_{14}\bar{x}_{30}:$
$\bar{y}_{58} := \bar{x}_{11}\bar{x}_{43} + \bar{x}_1\bar{x}_{44} + \bar{x}_{13}\bar{x}_{29} + \bar{x}_3\bar{x}_{40};$ $\bar{y}_{59} := \bar{x}_{42}\bar{x}_{44} + \bar{x}_{41}\bar{x}_{43};$
$\bar{y}_{60} := \bar{x}_{42}\bar{x}_{29} + \bar{x}_{39}\bar{x}_{43} + \bar{x}_{14};$ $\bar{y}_{61} := \bar{x}_{41}\bar{x}_{29} + \bar{x}_{39}\bar{x}_{44} + \bar{x}_3;$
$\bar{y}_{62} := \bar{x}_{30}\bar{x}_{44} + \bar{x}_{41}\bar{x}_{40} + \bar{x}_{13};$ $\bar{y}_{63} := \bar{x}_{30}\bar{x}_{29} + \bar{x}_{39}\bar{x}_{40} + \bar{x}_1 + \bar{x}_0;$
$\bar{y}_{64} := \bar{x}_3\bar{x}_2 + \bar{x}_{13}\bar{x}_{14};$ $\bar{y}_{65} := \bar{x}_{30}\bar{x}_{43} + \bar{x}_{42}\bar{x}_{40} + \bar{x}_2;$
$\bar{y}_{66} := \bar{x}_{11}\bar{x}_{33} + \bar{x}_{12}\bar{x}_{32} + \bar{x}_{13}\bar{x}_{19} + \bar{x}_{14}\bar{x}_{21};$ $\bar{y}_{67} := \bar{x}_{15}\bar{x}_{34} + \bar{x}_{16}\bar{x}_{35} + \bar{x}_{17}\bar{x}_{20} + \bar{x}_{18}\bar{x}_{31};$
$\bar{y}_{68} := \bar{x}_{15}\bar{x}_{33} + \bar{x}_{16}\bar{x}_{32} + \bar{x}_{17}\bar{x}_{19} + \bar{x}_{18}\bar{x}_{21};$ $\bar{y}_{69} := \bar{x}_{11}\bar{x}_{34} + \bar{x}_{12}\bar{x}_{35} + \bar{x}_{13}\bar{x}_{20} + \bar{x}_{14}\bar{x}_{31};$
$\bar{y}_{70} := \bar{x}_{33}\bar{x}_{35} + \bar{x}_{32}\bar{x}_{34};$ $\bar{y}_{71} := \bar{x}_{33}\bar{x}_{20} + \bar{x}_{19}\bar{x}_{34} + \bar{x}_{18};$
$\bar{y}_{72} := \bar{x}_{32}\bar{x}_{20} + \bar{x}_{19}\bar{x}_{35} + \bar{x}_{14};$ $\bar{y}_{73} := \bar{x}_{21}\bar{x}_{35} + \bar{x}_{32}\bar{x}_{31} + \bar{x}_{13};$
$\bar{y}_{74} := \bar{x}_{21}\bar{x}_{20} + \bar{x}_{19}\bar{x}_{31} + \bar{x}_{12} + \bar{x}_{15};$ $\bar{y}_{75} := \bar{x}_{14}\bar{x}_{17} + \bar{x}_{13}\bar{x}_{18};$
$\bar{y}_{76} := \bar{x}_{21}\bar{x}_{34} + \bar{x}_{33}\bar{x}_{31} + \bar{x}_{17};$ $\bar{y}_{77} := \bar{x}_{11}\bar{x}_{13} + \bar{x}_{15}\bar{x}_{17} + \bar{x}_{38}\bar{x}_{31} + \bar{x}_{37}\bar{x}_{21};$
$\bar{y}_{78} := \bar{x}_{12}\bar{x}_{14} + \bar{x}_{16}\bar{x}_{18} + \bar{x}_{39}\bar{x}_{20} + \bar{x}_{36}\bar{x}_{19};$ $\bar{y}_{79} := \bar{x}_{12}\bar{x}_{13} + \bar{x}_{16}\bar{x}_{17} + \bar{x}_{39}\bar{x}_{31} + \bar{x}_{36}\bar{x}_{21};$
$\bar{y}_{80} := \bar{x}_{11}\bar{x}_{14} + \bar{x}_{15}\bar{x}_{18} + \bar{x}_{38}\bar{x}_{20} + \bar{x}_{37}\bar{x}_{19};$ $\bar{y}_{81} := \bar{x}_{11}\bar{x}_{39} + \bar{x}_{38}\bar{x}_{12} + \bar{x}_{17};$
$\bar{y}_{82} := \bar{x}_{15}\bar{x}_{39} + \bar{x}_{38}\bar{x}_{16} + \bar{x}_{13};$ $\bar{y}_{83} := \bar{x}_{37}\bar{x}_{16} + \bar{x}_{15}\bar{x}_{36} + \bar{x}_{14};$
$\bar{y}_{84} := \bar{x}_{37}\bar{x}_{39} + \bar{x}_{38}\bar{x}_{36};$ $\bar{y}_{85} := \bar{x}_{37}\bar{x}_{12} + \bar{x}_{11}\bar{x}_{36} + \bar{x}_{18};$
$\bar{y}_{86} := \bar{x}_0\bar{x}_{24} + \bar{x}_1\bar{x}_{23} + \bar{x}_2\bar{x}_8 + \bar{x}_3\bar{x}_{10};$ $\bar{y}_{87} := \bar{x}_4\bar{x}_{25} + \bar{x}_5\bar{x}_{26} + \bar{x}_6\bar{x}_9 + \bar{x}_7\bar{x}_{22};$

$\bar{y}_{88} := \bar{x}_4\bar{x}_{24} + \bar{x}_5\bar{x}_{23} + \bar{x}_6\bar{x}_8 + \bar{x}_7\bar{x}_{10};$

$y_{\bar{8}9} := \bar{x}_0\bar{x}_{25} + \bar{x}_1\bar{x}_{26} + \bar{x}_2\bar{x}_9 + \bar{x}_3\bar{x}_{22};$

$\bar{y}_{90} := \bar{x}_{24}\bar{x}_{26} + \bar{x}_{23}\bar{x}_{25};$

$y_{\bar{9}1} := \bar{x}_{24}\bar{x}_9 + \bar{x}_8\bar{x}_{25} + \bar{x}_7;$

$\bar{y}_{92} := \bar{x}_{23}\bar{x}_9 + \bar{x}_8\bar{x}_{26} + \bar{x}_3;$

$y_{\bar{9}3} := \bar{x}_{10}\bar{x}_{26} + \bar{x}_{23}\bar{x}_{22} + \bar{x}_2;$

$\bar{y}_{94} := \bar{x}_{10}\bar{x}_9 + \bar{x}_8\bar{x}_{22} + \bar{x}_1 + \bar{x}_4;$

$y_{\bar{9}5} := \bar{x}_3\bar{x}_6 + \bar{x}_2\bar{x}_7;$

$\bar{y}_{96} := \bar{x}_{10}\bar{x}_{25} + \bar{x}_{24}\bar{x}_{22} + \bar{x}_6;$

$y_{\bar{9}7} := \bar{x}_0\bar{x}_2 + \bar{x}_4\bar{x}_6 + \bar{x}_{29}\bar{x}_{22} + \bar{x}_{28}\bar{x}_{10};$

$\bar{y}_{98} := \bar{x}_1\bar{x}_3 + \bar{x}_5\bar{x}_7 + \bar{x}_{30}\bar{x}_9 + \bar{x}_{27}\bar{x}_8;$

$y_{\bar{9}9} := \bar{x}_1\bar{x}_2 + \bar{x}_5\bar{x}_6 + \bar{x}_{30}\bar{x}_{22} + \bar{x}_{27}\bar{x}_{10};$

$\bar{y}_{100} := \bar{x}_0\bar{x}_3 + \bar{x}_4\bar{x}_7 + \bar{x}_{29}\bar{x}_9 + \bar{x}_{28}\bar{x}_8;$

$y_{\bar{1}01} := \bar{x}_0\bar{x}_{30} + \bar{x}_{29}\bar{x}_1 + \bar{x}_6;$

$\bar{y}_{102} := \bar{x}_4\bar{x}_{30} + \bar{x}_{29}\bar{x}_5 + \bar{x}_2;$

$y_{\bar{1}03} := \bar{x}_{28}\bar{x}_5 + \bar{x}_4\bar{x}_{27} + \bar{x}_3;$

$\bar{y}_{104} := \bar{x}_{28}\bar{x}_{30} + \bar{x}_{29}\bar{x}_{27};$

$y_{\bar{1}05} := \bar{x}_{28}\bar{x}_1 + \bar{x}_0\bar{x}_{27} + \bar{x}_7;$

$\bar{y}_{106} := f_{106};$

$y_{\bar{1}07} := f_{107};$

$\bar{y}_{108} := f_{108};$

$y_{\bar{1}09} := f_{109}.$