Analysis of Second Order Matrices Construction in MFE Public Key Cryptosystem

Xuyun Nie[1,2], Chuanyong Hou[1], Zhaohu Xu[1] and Gang Lu[1]
(Corresponding author: Xuyun Nie)
School of Information and Software Engineering & University of Electronic Science and Technology of China[1]
Section 2, North Jianshe Road, Chengdu 610054, China
State Key Laboratory of Information Security & Institute of Information Engineering[2]
Beijing 100093, China
(Email: xynie@uestc.edu.cn)
(Received July 20, 2014; revised and accepted Mar. 20 & July 4, 2015)

Abstract

Medium Field Equations (MFE), which is a type of multivariate public key encryptions scheme proposed by Wang et al., was broken by Ding et al. using high order linearization equation (HOLE) attack. Recently, many people attempt to modify the second order matrices structure in the central map of MFE to resist HOLE attack. In this paper, we gave deeply analysis of all possible constructions by products of the second order matrices and their variants with transpose and adjoint in the central map of MFE. We proved that any modification with transpose and adjoint would satisfy the First Order Linearization Equations or the Second Order Linearization Equations. As an example, we gave a practical cryptanalysis of an improved MFE scheme.

Keywords: Linearization equation, MFE, multivariate public key cryptosystem, second order matrix

1 Introduction

Public key cryptosystem played an important role in our modern communication system. But with the rapid development of the quantum computer, the traditional public key cryptosystems based on the number theory hard problem, such as RSA and ElGamal cryptosystems, are all insecure under the quantum computer attack. Multivariate public key cryptosystem (MPKC) is one of the promising alternatives to the traditional public key cryptosystem against the quantum computer attack [8]. The security of the MPKC relies on the difficulty of solving a random system of nonlinear polynomial equations on a finite field, which is an NP-hard problem in general.

Let $\mathbb{K}$ be a finite field and m, n be two positive integers. The public key of MPKC is a set of multivariate polynomials, which are the expressions of the following map,

$$\begin{aligned}(y_1, \cdots, y_m) &= \bar{F}(x_1, \cdots, x_n) \\ &= T \circ F \circ S \\ &= (\bar{f}_1, \cdots, \bar{f}_m),\end{aligned}$$

where $\{y_1, \cdots, y_m\}$ are ciphertext variables and $\{x_1, \cdots, x_n\}$ are plaintext variables. The two invertible affine transformations T and S are the private keys of the MPKC, which are defined on $\mathbb{K}^m$ and $\mathbb{K}^n$ respectively. The map F is called central map. The key point in constructing an secure MPKC is to design a proper central map.

Medium Field Equation (MFE) [12] is a type of multivariate public key cryptosystem proposed by Wang et al. in 2006. The inventor of MFE used products of second order matrices to derive quadratic polynomials in its central map. To avoid the Paratin relation or linearization equations of form

$$\sum_{i=1,j=1}^{n,m} a_{ij}x_iy_j + \sum_{i=1}^{n} b_ix_i + \sum_{j=1}^{m} c_jy_j + d = 0,$$

the inventors used a transposed matrix instead of the original one in the central map of MFE. But the original MFE was broken by High Order Linearization Equation (HOLE) attack [2] in 2007. Given a public key, the attack can successfully recover the plaintext corresponding to a valid ciphertext.

In order to resist existing attack, many modifications of MFE were proposed. In 2009, Wang et al. [13] modified MFE and raised the public key from quadratic to quartic equations. It is indeed this case can avoid HOLEs attack. However, from their quartic public key, many so-called Quadratization Equations (QEs) can be found and can be used to break them [1]. In 2009, Tao et al. gave an improvement of MFE [9]. They introduced a new rational map in composition of the improvement and claimed

that the new scheme can resist SOLEs attack. But there are still many SOLEs existing in this new scheme. Given a public key and a valid ciphertext, we can recover its corresponding plaintext [14]. In 2009, Huang et al. gave an improvement of MFE by redesigning the central map with transpose matrix and adjoint matrix [3]. After theoretical analysis, we found that it satisfied both Second Order Linearization Equations (SOLEs) and First Order Linearization Equations (FOLEs) [6].

In this paper, we summarize the steps of HOLEs attack. And then, we analyzed the construction based on the second order matrices in the central map of MFE. We found that if one want to remain degree two polynomials in the public key and ensure successfully decryption, one could only use the transpose matrices and the adjoint matrices. Given a second order matrix M over a finite field of characteristic 2, there are only 8 second order matrices with the same determinant of M. And these 8 matrices can be separated into two equivalent class with the matrix M and its transpose M^T. We list all possible constructions with a matrix M and its transpose M^T in the form of multiplication of two matrices. We found that all constructions will satisfy the SOLEs or FOLEs. So it is impossible to improve MFE by changing the form of second order matrices with their transpose and adjoint.

At last, we show how to find FOLEs satisfied by an improvement of MFE scheme [3] proposed by Jiasen Huang et al. After finding all the FOLEs, we use linearization equation attack breaking this improved version.

This paper is organized as follows. We introduce the MFE scheme, the idea of HOLEs attack on it and an improvement of MFE in Section 2. In Section 3, we give an analysis of the structure of the second order matrices in MFE scheme. Then we present a FOLEs attack on an improvement of MFE in Section 4. Finally, we conclude this paper in Section 5.

2 Preliminaries

In this section, we will introduce the MFE public key cryptosystem and the previous attack on MFE. Then, we will introduce one modification of MFE.

2.1 MFE Public Key Cryptosystem

We use the same notations as in [12]. Let $\mathbb{K}$ be a finite field of characteristic 2 and $\mathbb{L}$ be its degree r extension field. In MFE, we always identify $\mathbb{L}$ with $\mathbb{K}^r$ by a $\mathbb{K}$-linear isomorphism π: $\mathbb{L} \to \mathbb{K}^r$. Namely we take a basis of $\mathbb{L}$ over $\mathbb{K}$, $\{\theta_1, \cdots, \theta_r\}$, and define π by $\pi(a_1\theta_1 + \cdots + a_r\theta_r) = (a_1, \cdots, a_r)$ for any $a_1, \cdots a_r \in \mathbb{K}$. It is natural to extend π to two $\mathbb{K}$-linear isomorphisms π_1: $\mathbb{L}^{12} \to \mathbb{K}^{12r}$ and π_2: $\mathbb{L}^{15} \to \mathbb{K}^{15r}$.

In MFE, its encryption map F: $\mathbb{K}^{12r} \to \mathbb{K}^{15r}$ is a composition of three maps ϕ_1, ϕ_2, ϕ_3. Let

$$(u_1, \cdots, u_{12r}) = \phi_1(x_1, \cdots, x_{12r}),$$

$$(v_1, \cdots, v_{15r}) = \phi_2(u_1, \cdots, u_{12r}),$$

$$(y_1, \cdots, y_{15r}) = \phi_3(v_1, \cdots, v_{15r}),$$

where ϕ_1 and ϕ_3 are invertible affine maps, ϕ_2 is its central map, which is equal to $\pi_1 \circ \bar{\phi}_2 \circ \pi_2^{-1}$.

ϕ_1 and ϕ_3 are taken as the private key, while the expression of the map $(y_1, \cdots, y_{15r}) = F(x_1, \cdots, x_{12r})$ is the public key.The map $\bar{\phi}_2$: $\mathbb{L}^{12} \to \mathbb{L}^{15}$ is defined as follows.

$$\begin{cases}
Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; & \\
Y_2 = X_2 + X_9X_{12} + X_{10}X_{11} + Q_2; & \\
Y_3 = X_3 + X_1X_4 + X_2X_3 + Q_3; & \\
Y_4 = X_1X_5 + X_2X_7; & Y_5 = X_1X_6 + X_2X_8; \\
Y_6 = X_3X_5 + X_4X_7; & Y_7 = X_3X_6 + X_4X_8; \\
Y_8 = X_1X_9 + X_2X_{11}; & Y_9 = X_1X_{10} + X_2X_{12}; \\
Y_{10} = X_3X_9 + X_4X_{11}; & Y_{11} = X_3X_{10} + X_4X_{12}; \\
Y_{12} = X_5X_9 + X_7X_{11}; & Y_{13} = X_5X_{10} + X_7X_{12}; \\
Y_{14} = X_6X_9 + X_8X_{11}; & Y_{15} = X_6X_{10} + X_8X_{12},
\end{cases}$$

where Q_1, Q_2, and Q_3 form a triple (Q_1, Q_2, Q_3) which is a triangular map from $\mathbb{K}^{3r}$ to itself, more detail please see [12].

The method of computing $\bar{\phi}_2^{-1}$ is listed as follows:

Write $X_1, \cdots, X_{12}, Y_4, \cdots, Y_{15}$ as six 2×2 matrices:

$$\begin{aligned}
M_1 &= \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \\
M_2 &= \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix} \\
M_3 &= \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix} \\
Z_3 &= M_1M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix} \\
Z_2 &= M_1M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix} \\
Z_1 &= M_2^TM_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}.
\end{aligned}$$

Then

$$\begin{cases}
\det(M_1) \cdot \det(M_2) = \det(Z_3), \\
\det(M_1) \cdot \det(M_3) = \det(Z_2), \\
\det(M_2) \cdot \det(M_3) = \det(Z_1).
\end{cases}$$

When M_1, M_2, and M_3 are all invertible, we can get values of $\det(M_1)$, $\det(M_2)$, and $\det(M_3)$ from $\det(Z_1)$, $\det(Z_2)$, and $\det(Z_3)$, for instance, $\det(M_1) = \big(\det(Z_2) \cdot \det(Z_3)/\det(Z_1)\big)^{1/2}$.

With the values of $\det(M_1)$, $\det(M_2)$, and $\det(M_3)$, we can use the triangular form of the central map to get $X_1, X_2, \cdots, X_{12}$ in turn. Then we can recover the plaintext corresponding the given ciphertext. More detail of decryption are presented in [12].

2.2 High Order Linearization Equation

High Order Linearization Equation (HOLE) is an type of equation of the following form:

$$\sum_{i=1,j=1}^{n,t} a_{ij}x_i g_j(y_1, y_2, \cdots, y_m) + \sum_{k=1}^{l} c_k h_k(y_1, y_2, \cdots, y_m) + d = 0, \quad (1)$$

where h_k, $1 \le k \le l$, g_j, $1 \le j \le t$, are polynomial functions in the ciphertext variables. The highest degree of g_j, $1 \le j \le l$ and h_k, $1 \le k \le l$ is called the order of the HOLE.

For example, the First Order Linearization Equation (FOLE) and the Second Order Linearization Equation (SOLE) are of the following forms, respectively.

$$\sum_{i=1,j=1}^{n,m} a_{ij}x_i y_j + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{m} c_j y_j + d = 0.$$

$$\sum_i x_i \left(\sum_{j \le k} a_{ijk} y_j y_k + \sum_j b_{ij} y_j + c_i \right) + \sum_{j \le k} d_{jk} y_j y_k + \sum e_j y_j + f = 0.$$

Note that, given a valid ciphertext $\mathbf{y}' = (y'_1, y'_2, \cdots, y'_m)$, we can substitute it into Equation (1) to get a linear equation in the plaintext variables. By finding all these equations we get a linear system in the plaintext variables, which can be solved by Gaussian Elimination. After having found a solution, we can do elimination on the public key or solve System (2).

$$\begin{cases} F_1(x_1, \cdots, x_n) &= y'_1; \\ & \cdots \\ F_m(x_1, \cdots, x_n) &= y'_m. \end{cases} \quad (2)$$

Then, we can also check whether there are some HOLEs satisfied by the eliminated public key and the form of HOLEs.

The steps of LE attack are listed in Algorithm 1.

2.3 Previous Attack on MFE

In designing the MFE scheme, the inventors have taken into account the LE attack. They used M_2^T instead of M_2 to avoid the FOLEs.

But Ding et al. found that there are many SOLEs satisfied by the MFE scheme. Denote by M^* the adjoint matrix of a second order matrix. From

$$Z_3 = M_1 M_2, Z_2 = M_1 M_3,$$

we have

$$M_3 M_3^* M_1^* M_1 M_2 = M_3 Z_2^* Z_3 = \det(Z_2) M_2. \quad (3)$$

Expanding Equation (3), we get four equations of the form

$$\sum a'_{ijk} X_i Y_j Y_k = 0. \quad (4)$$

Algorithm 1 Steps of LE Attack

1: **Input:** public key F of a MPKC, ciphertext $\mathbf{y}' \in \mathbb{K}^m$
2: **Output:** corresponding plaintext $\mathbf{x}' \in \mathbb{K}^n$
3: Check whether there are some LEs satisfied by public key.
4: Determine the form of LEs and find all the LEs.
5: Substitute the ciphertext $\mathbf{y}'$ into the linearization equations and find all linear equations in the plaintext variables. Solve the system to find linear relations between plaintext variables. In other words, some plaintext variables can be written as linear expressions in the remaining variables.
6: Substitute the linear expressions of plaintext variables into the public key polynomials to get a "eliminated" public key expression (it is in fewer unknown plaintext components).
7: Check whether there are some LEs satisfied by the eliminated public key. If there are, goto Step 2.
8: Directly solve the last eliminated System (2).
9: Use the linear relations between plaintext variables to get the values of remained plaintext components.

In [2], 24 equations of this form can be found.

Substituting $(X_1, \cdots, X_{12}) = \pi_1^{-1} \circ \phi_1(x_1, \cdots, x_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi_2^{-1} \circ \phi_3^{-1}(y_1, \cdots, y_{15r})$ into Equation (4), we get $24r$ equations of the form

$$\sum_i x_i \left(\sum_{j \le k} a_{ijk} y_j y_k + \sum_j b_{ij} y_j + c_i \right) + \sum_{j \le k} d_{jk} y_j y_k + \sum_j e_j y_j + f = 0.$$

These equations are SOLEs.

Given a public key and a valid ciphertext, after finding all the SOLEs, one can recovered the corresponding plaintext efficiently.

2.4 Improvement of MFE

To avoid the SOLE, Jiasen Huang et al. proposed a modification of MFE. They modified only the matrix equations as follows.

M_1, M_2 and M_3 are defined as same as the origin MFE, while Z_1, Z_2 and Z_3 are defined as follows:

$$Z_3 = M_1 M_2^* = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix},$$
$$Z_2 = M_1^* M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix},$$
$$Z_1 = M_2^T M_3^* = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix},$$

where M_i^* $(1 \le i \le 3)$ are the adjoint matrices of M_i^*.

These matrices are also satisfied

$$\begin{cases} \det(M_1) \cdot \det(M_2) = \det(Z_3), \\ \det(M_1) \cdot \det(M_3) = \det(Z_2), \\ \det(M_2) \cdot \det(M_3) = \det(Z_1). \end{cases}$$

so the decryption process is very similar to the original MFE. See [3] for more detail.

3 Analysis of the Structure Based on Second Order Matrices

In this section, we consider the second order matrices over a finite field $\mathbb{K}$ of characteristic 2.

In order to resist HOLE, many people try to improve the MFE scheme by modifying the second order matrices of the central map. To ensure the decryption successfully, they need keep the determinants unchanged.

Now we give two Propositions on the constructions by using the second order matrices.

Proposition 1. *Given a square matrix* $M = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$, *where* $X_1, X_2, X_3, X_4 \in \mathbb{K}$, *there are eight square matrices which satisfy:*

1) *Components in these matrices are all constituted of* $X_1, X_2, X_3, X_4 \in \mathbb{K}$;

2) *The determinants of these matrices are equal to* $det(M)$.

And all matrices above can be transformed by M *or* M^T *through row transformations and column transformations.*

Proof: Given $X_1, X_2, X_3, X_4 \in \mathbb{K}$ of characteristic 2, there are 24 different matrices. We can calculate their determinate one by one. Clearly, there are eight matrices (including the matrix M) whose determinate equal to $det(M)$. We list as follows:

$$\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, \begin{pmatrix} X_2 & X_1 \\ X_4 & X_3 \end{pmatrix}, \begin{pmatrix} X_3 & X_4 \\ X_1 & X_2 \end{pmatrix},$$

$$\begin{pmatrix} X_4 & X_3 \\ X_2 & X_1 \end{pmatrix}, \begin{pmatrix} X_1 & X_3 \\ X_2 & X_4 \end{pmatrix}, \begin{pmatrix} X_2 & X_4 \\ X_1 & X_3 \end{pmatrix},$$

$$\begin{pmatrix} X_4 & X_2 \\ X_3 & X_1 \end{pmatrix}, \begin{pmatrix} X_3 & X_1 \\ X_4 & X_2 \end{pmatrix}.$$

Among the matrices above, the first four matrices can be easily derived from the matrix M through row transformation and column transformation. And the last four matrices can be gotten from M^T. □

Let us consider the following equations:

$$\begin{cases} Y_4 = X_1X_5 + X_2X_7; \\ Y_5 = X_1X_6 + X_2X_8; \\ Y_6 = X_3X_5 + X_4X_7; \\ Y_7 = X_3X_6 + X_4X_8. \end{cases} \quad (5)$$

The Equation (5) can be expressed by the following four matrices equations.

$$\begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix} = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix},$$

$$\begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix} = \begin{pmatrix} X_2 & X_1 \\ X_4 & X_3 \end{pmatrix} \begin{pmatrix} X_7 & X_8 \\ X_5 & X_6 \end{pmatrix},$$

$$\begin{pmatrix} Y_6 & Y_7 \\ Y_4 & Y_5 \end{pmatrix} = \begin{pmatrix} X_3 & X_4 \\ X_1 & X_2 \end{pmatrix} \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix},$$

$$\begin{pmatrix} Y_6 & Y_7 \\ Y_4 & Y_5 \end{pmatrix} = \begin{pmatrix} X_4 & X_3 \\ X_2 & X_1 \end{pmatrix} \begin{pmatrix} X_7 & X_8 \\ X_5 & X_6 \end{pmatrix}.$$

So, we can say that the matrices $\begin{pmatrix} X_2 & X_1 \\ X_4 & X_3 \end{pmatrix}$, $\begin{pmatrix} X_3 & X_4 \\ X_1 & X_2 \end{pmatrix}$, $\begin{pmatrix} X_4 & X_3 \\ X_2 & X_1 \end{pmatrix}$ are equivalent to the matrix $\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$.

Similarly, the matrices $\begin{pmatrix} X_2 & X_4 \\ X_1 & X_3 \end{pmatrix}$, $\begin{pmatrix} X_4 & X_2 \\ X_3 & X_1 \end{pmatrix}$, $\begin{pmatrix} X_3 & X_1 \\ X_4 & X_2 \end{pmatrix}$ are equivalent to the matrix $\begin{pmatrix} X_1 & X_3 \\ X_2 & X_4 \end{pmatrix}$.

Notice that the matrix $\begin{pmatrix} X_4 & X_2 \\ X_3 & X_1 \end{pmatrix}$ is the adjoint matrix of the matrix $\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$. So, we can only consider a matrix and its transpose in the matrices form of the central map in MFE.

Proposition 2. *Given a square matrix* $M = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$, *where* $X_1, X_2, X_3, X_4 \in \mathbb{K}$. $M_i, i = 1, \cdots, 4$ *are random second order matrices on finite field* $\mathbb{K}$, *define a set as follows:*

$$Q = \{MM_1, M_2M, M^TM_3, M_4M^T\},$$

then any two elements in Q can be deduced high order linearization equations in constructing the central map in MFE.

Proof: There are 6 forms of combination (Z_1, Z_2) in Q, we analysis of them respectively.

1) If $Z_1 = MM_1, Z_2 = M_2M$, we can derive

$$Z_2M_1 = M_2Z_1;$$

2) If $Z_1 = MM_1, Z_2 = M^TM_3$, we can derive

$$Z_2^TM_1 = M_3^TZ_1;$$

3) If $Z_1 = MM_1, Z_2 = M_4M^T$, we can derive

$$\det(Z_2)M_1 = M_4^T(Z_2^T)^*Z_1;$$

4) If $Z_1 = M_2M, Z_2 = M^TM_3$, we can derive

$$\det(Z_1)(M_3^T)^* = M_2^*Z_1(Z_2^T)^*;$$

5) If $Z_1 = M_2 M, Z_2 = M_4 M^T$, we can derive

$$Z_1 M_4^T = M_2 Z_2^T;$$

6) If $Z_1 = M^T M_3, Z_2 = M_4 M^T$, we can derive

$$Z_2 M_3 = M_4 Z_1;$$

In Cases 1), 2), 5), and 6), we can derive FOLEs. In Cases 3) and 4), we can derive SOLEs.

The original MFE scheme satisfied Case 3) and 4) in the proof of Proposition 2. □

As to the improved MFE, the matrices equation $Z_2 = M_1^* M_3$ can be changed into

$$\begin{pmatrix} Y_{10} & Y_{11} \\ Y_8 & Y_9 \end{pmatrix} = \begin{pmatrix} X_1 & X_3 \\ X_2 & X_4 \end{pmatrix} \begin{pmatrix} X_{11} & X_{12} \\ X_9 & X_{10} \end{pmatrix}.$$

This equation and $Z_3 = M_1 M_2^*$ satisfy Case 2). Similarly, according to the Proposition 1, we can deduce that the central map of the improved MFE scheme satisfy Cases 1), 5) and 6).

From Proposition 1 and Proposition 2 above, we can make sure that all the modifications of MFE by changing the form of matrices in MFE with their transpose and adjoint will fail to resist the HOLEs attack.

4 Linearization Equation Attack on Improvement of MFE

In this section, we give an example of Linearization Attack on Improvement of MFE. This work was presented on The 10th International Conference on Cryptology and Network Security (CANS 2011). The authors of [3] claimed their improvement of MFE can resist SOLEs attack. But according to Section 3, we know that this scheme satisfied the FOLEs. In this section, we will describe how to get the FOLEs and present the whole FOLE attack on this improvement.

4.1 Finding FOLEs

Note that, for any square matrices M_1 and M_2, we have

$$\begin{aligned} (M_1^*)^* &= M_1, \\ (M_1 M_2)^* &= M_2^* M_1^*, \\ (M_1^*)^T &= (M_1^T)^*. \end{aligned}$$

From

$$Z_3 = M_1 M_2^*, Z_2 = M_1^* M_3$$

we can derive

$$M_3^* Z_3 = M_3^* M_1 M_2^* = (M_1^* M_3)^* M_2^* = Z_2^* M_2^*$$

and hence,

$$Z_2^* M_2^* = M_3^* Z_3$$

Expanding it, we have

$$\begin{pmatrix} Y_{11} & -Y_9 \\ -Y_{10} & Y_8 \end{pmatrix} \begin{pmatrix} X_8 & -X_6 \\ -X_7 & X_5 \end{pmatrix} = \begin{pmatrix} X_{12} & -X_{10} \\ -X_{11} & X_9 \end{pmatrix} \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}.$$

That is,

$$\begin{cases} X_8 Y_{11} + X_7 Y_9 = X_{12} Y_4 - X_{10} Y_6 \\ -X_6 Y_{11} - X_9 Y_5 = X_{12} Y_5 - X_{10} Y_7 \\ -X_8 Y_{10} - X_7 Y_8 = -X_{11} Y_4 + X_9 Y_6 \\ X_6 Y_{10} + X_5 Y_8 = -X_{11} Y_5 + X_9 Y_7. \end{cases} \quad (6)$$

Applying $(X_1, \cdots, X_{12}) = \pi_1 \circ \phi_1(x_1, \cdots, x_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi_2^{-1} \circ \phi_3^{-1}(y_1, \cdots, y_{15r})$ into Equation (6), we get $4r$ equations of the form

$$\sum_{i,j} a_{ij} x_i y_j + \sum_i b_i x_i + \sum_j c_j y_j + d = 0, \quad (7)$$

where the coefficients $a_{ij}, b_i, c_j, d \in \mathbb{K}$, and the summations are respectively over $1 \le i \le 12r$ and $1 \le j \le 15r$. These equations are FOLEs. Apparently, these $4r$ equations are linearly independent.

Using the same technique, we can derive other $8r$ SOLEs. Note that

$$\begin{aligned} Z_1 M_1 &= M_2^T M_3^* M_1 = M_2^T Z_2^* \\ Z_1^* M_1^T &= (M_2^T M_3^*)^* M_1^T = M_3 (M_2^T)^* M_1^T \\ &= M_3 (M_2^*)^T M_1^T = M_3 Z_3^T. \end{aligned}$$

That is,

$$\begin{aligned} Z_1 M_1 &= M_2^T Z_2^* \\ Z_1^* M_1^T &= M_3 Z_3^T. \end{aligned}$$

Expanding them and substituting $(X_1, \cdots, X_{12}) = \pi_1 \circ \phi_1(u_1, \cdots, u_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi_2^{-1} \circ \phi_3^{-1}(z_1, \cdots, z_{15r})$ into them, we get another linearly independent $8r$ FOLEs.

To find all the FOLEs, we randomly generate sufficient plaintext/ciphertext pairs and substitute them into the FOLE to get a system of linear equations on the unknown coefficients $a_{1,1}, \cdots, a_{12r,15r}, b_1, \cdots, b_{12r}, c_1, \cdots, c_{15r}, d$. In this case, the number of unknown coefficients in these equations is equal to

$$12r \times 15r + 12r + 15r + 1 = 180r^2 + 27r + 1.$$

Suppose we derive D linearly independent FOLEs. Let $E_k (1 \le k \le D)$ denote these equations:

$$\sum_{i=1,j=1}^{12r,15r} a_{ij}^{(k)} x_i y_j + \sum_{i=1}^{12r} b_i^{(k)} x_i + \sum_{j=1}^{15r} c_j^{(k)} y_j + d^{(k)} = 0.$$

We used computer experiments to find all linearization equations. In one of our experiments, we choose $\mathbb{K} = GF(2^{16})$, $r = 4$. In this case, the number of unknown coefficients is equal to 2989.

Our experiments show that it take about 22 minutes on the execution of this step. And $D = 48$.

Note that, this step is independent of the value of the ciphertext and can be done once for a given public key.

4.2 Ciphertext-only Attack

Now we have derived all FOLEs. Our goal is to find corresponding plaintext $(x'_1, \cdots, x'_{12r})$ for a given valid ciphertext $(y'_1, \cdots, y'_{15r})$.

Substitute $(y'_1, \cdots, y'_{15r})$ into basis equations E_k, we can get k equations in following form:

$$\begin{cases} \sum_{i,j} a_{ij}^{(k)} x_i y'_j + \sum_i b_i^{(k)} x_i + \sum_j c_j^{(k)} y'_j + d^{(k)} = 0 \\ 1 \le k \le D. \end{cases} \tag{8}$$

Suppose the dimension of the basis of System (8) solution space is s. Then, we can represent s variables of $x_1, \cdots, x_{12r}$ by linear combinations of other $12r - s$. Denote $w_1, \cdots, w_{12r-s}$ are remainder variables. Our experiments show $s = 32$, when $r = 4$.

Now substitute the expressions obtained above into $F_j(x_1, \cdots, x_{12r})$, we can get $15r$ new quadratic functions $\tilde{F}_j(w_1, \cdots, w_{12r-s})$, $j = 1, \cdots, 12r$. Then, our attack turn to solve the following system:

$$\begin{cases} \tilde{F}_i(w_1, \cdots w_{12r-s}) = y'_i \\ 1 \le i \le 15r. \end{cases} \tag{9}$$

There are $4r$ unknowns and $15r$ equations in System (9). We can solve this system by Gröbner basis method and recover the corresponding plaintext.

Our experiments show that it takes about 6 second to solve System (9) and our experiments recover the corresponding plaintext successfully.

All of our experiments were performed on a normal computer, with Genuine Intel(R) CPU T2300@1.66GHz, 504MB RAM by magma.

5 Conclusion

In this paper, we verified that all modifications of MFE by changing the form of matrices with transpose and adjoint will satisfy the SOLEs or FOLEs. Hence, they are all insecure.

In order to enhance the security of MPKCs, many enhancement methods were proposed such as Piece in hand [10], Extended Multivariate public key Cryptosystems (EMC) [11] etc. All of these methods are subjected to different levels of attacks [4, 5]. Recently, Qiao proposed three security enhancement methods on MPKC [7]. The security of their methods will be considered in the future.

Acknowledgments

This work was supported by the National Key Basic Research Program of China under grant 2013CB834203, the National Natural Science Foundation of China under grant No. 61370026, 61472064. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] W. W. Cao, X. Y. Nie, L. Hu, X. L. Tang, and J. T. Ding, "Cryptanalysis of two quartic encryption schemes and one improved mfe scheme," in *Proceedings of The Third International Workshop (PQCrypto'10)*, pp. 41–60, Darmstadt, Germany, May 2010.

[2] J. T. Ding, L. Hu, X. Y. Nie, J. Y. Li, and J. Wagner, "High order linearization equation (hole) attack on multivariate public key cryptosystems," in *Proceedings of The 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC'07)*, pp. 233–248, Beijing, China, Apr. 2007.

[3] J. S. Huang, B. D. Wei, and H. Y. Ou, "An improved MFE scheme resistant against sole attacks," in *Proceedings of Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia'09)*, pp. 157–160, Shanghai, China, Jan. 2009.

[4] X. Y. Nie, A. Petzoldt, J. Buchmann, and F. G. Li, "Linearization equation attack on 2-layer nonlinear piece in hand method," *IEICE Transactions on Fundamentals*, vol. E97-A, no. 9, pp. 1952–1961, 2014.

[5] X. Y. Nie, Z. H. Xu, and J. Buchmann, "Cryptanalysis of hash-based tamed transformation and minus signature scheme," in *Proceedings of The 5th International Workshop on Post-Quantum Cryptography (PQCrypto'13)*, pp. 115–164, Limoges, France, June 2013.

[6] X. Y. Nie, Z. H. Xu, L. Lu, and Y. J. Liao, "Security analysis of an improved MFE public key cryptosystem," in *Proceedings of The 10th International Conference on Cryptology and Network Security (CANS'11)*, pp. 118–125, Sanya, China, Dec. 2011.

[7] S. T. Qiao, W. B. Han, Y. F. Li, and L. Y. Jiao, "Construction of extended multivariate public key cryptosystems," *International Journal of Network Security*, vol. 18, no. 1, pp. 60–67, 2016.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[9] H. W. Tao and Y. X. Chen, "An improved medium-field multivariate public-key encryption scheme," in *Proceedings of The International Conference on Computational Intelligence and Software Engineering*, pp. 1–4, Wuhan, China, Dec. 2009.

[10] S. Tsujii, K. Tadaki, R. Fujita, M. Gotaishi, and T. Kaneko, "Security enhancement of various mpkcs by 2-layer nonlinear piece in hand method," *IEICE Transactions on Fundamentals*, vol. E92-A, no. 10, pp. 2438–2447, 2009.

[11] H. Z. Wang, H. G. Zhang, Z. Y. Wang, and M. Tang, "Extended multivariate public key cryptosystems with secure encryption function," *Science China Information Sciences*, vol. 54, no. 6, pp. 1161–1171, 2011.

[12] L. C. Wang, B. Y. Yang, Y. H. Hu, and F.P. Lai, "Medium-field multivariate public key encryption scheme," in *Proceedings of The Cryptographers' Track at the RSA Conference*, pp. 132–149, San Jose, CA, USA, Feb. 2006.

[13] X. Wang, F. Feng, X. M. Wang, and Q. Wang, "A more secure mfe multivariate public key encryption scheme," *International Journal of Computer Science and Applications*, vol. 6, no. 3, pp. 1–9, 2009.

[14] Z. H. Xu, X. Y. Nie, H. Wang, and Y. J. Liao, "Cryptanalysis of an improved mfe public key cryptosystem," *International Journal of Security and Networks*, vol. 7, no. 3, pp. 174–180, 2012.

Xuyun Nie received the Ph.D. degree in Information security from Graduate university of Chinese Academy of Sciences, Beijing, China, in 2007. He is presently an Associate Professor at University of Electronic Science and Technology of China (UESTC). His research interests include cryptography and information security.

Chuanyong Hou received his Master Degree from University of Electronic Science and Technology of China in 2015. His research interests include cryptography and network security.

Zhaohu Xu received his Master Degree from University of Electronic Science and Technology of China in 2013. His research interests include multivariate public key cryptography and network security.

Gang Lu is a PH.D candidate in University of Electronic Science and Technology of China now. His research interests include cryptography and security of big data.