Cryptanalysis of Two Quartic Encryption Schemes and One Improved MFE Scheme

Weiwei Cao[1], Xiuyun Nie[3], Lei Hu[1], Xiling Tang[4], and Jintai Ding[2,4]

[1] State Key Laboratory of Information Security,
Graduate University of Chinese Academy of Sciences, Beijing 100049, China
[2] Department of Mathematical Sciences, University of Cincinnati, OH 45221, USA
[3] School of Computer Science and Engineering,
University of Electronic Science and Technology of China, Chengdu 610054, China
[4] South China University of Technology, Guangzhou 510640, China
wwcao@is.ac.cn, jintai.ding@uc.edu, hu@is.ac.cn, xynie@uestc.edu.cn

Abstract. MFE, a multivariate public key encryption scheme proposed by Wang et al in CT-RSA 2006, was conquered by second order linearization equation (SOLE) attack by Ding et al in PKC 2007. To resist this attack, many improved schemes were proposed. Wang et al in [WFW09] and Wang in [Wan07] both modified MFE and raised the public key from quadratic to quartic equations. We call the two quartic schemes Quartic-1 and Quartic-2 respectively for convenience. They are indeed immune to the SOLE attack. However, we find that there exist many quadratization equations (QEs), which are quadratic in plaintext variables and linear in ciphertext variables and can be derived from the public keys of Quartic-1 and Quartic-2. In this paper, we utilize QEs to recover the corresponding plaintext for a given ciphertext. For Quartic-1, we firstly find there are at least $2r$ SOLEs, which was regarded as impossible by the original authors, furthermore, we can find at least $35r$ QEs with a complexity $\mathcal{O}((90r^2(15r+1)+180r^2+15r(15r+1)/2+27r+1)^w)$, where r is a small number denoting the degree of extension of finite fields and $w \approx 2.732$. The computational complexity of deriving these equations is about 2^{37}. But to find the original plaintext, there still needs 2^{40} times Gröbner basis computations, which needs practically 1.328 seconds each time. For Quartic-2, we make a theoretical analysis and find $18r$ QEs with a computational complexity $\mathcal{O}((15r+1)6r(12r+1)+180r^2+27r+1)^w$. The complexity is 2^{36} for the parameter proposed in [Wan07], and we can break the scheme practically in 3110.734 seconds. Finally, we show that another improved version of MFE in [WZY07] is insecure against the linearization equation attack although its authors claimed it is secure against high order linearization equation attack. Our attack on the two quartic schemes illustrates that non-linearization equations like quadratization equations which are not degree one in plaintext variables can also be used efficiently to analyze multivariate cryptosystems.

Keywords: multivariate public key encryption, quartic polynomial, quadratic polynomial, linearization attack, quadratization attack.

N. Sendrier (Ed.): PQCrypto 2010, LNCS 6061, pp. 41–60, 2010.

1 Introduction

Public key cryptography (PKC) has opened a new era of cryptography since Diffie and Hellman delivered a new idea in their seminal paper in 1976 [DH76]. The classical trapdoors of PKC are based on the difficulty of integer factorization for RSA and discrete logarithm for ElGamal and ECC. However, with the arrival of quantum computer epoch, cryptosystems based on integer factorization and discrete logarithm will be cracked by quantum computer attack [Sho97]. Therefore, multivariate public key cryptosystem (MPKC), one new public key cryptography, attracts more attention and becomes a hot topic in the last years.

The multivariate public key encryption scheme MFE is proposed by Wang et al in CT-RSA 2006 in [WYH06]. It was designed to be resist against the Patarin attack [Pat95] that utilizes the so-called first order linearization equations (FOLEs) of the form

$$\sum_{i,j} a_{ij} u_i v_j + \sum_i b_i u_i + \sum_j c_j v_j + d = 0,$$

but was conquered by Ding et al in 2007 PKC in [DHN07] by using second order linearization equations (SOLEs), which have a form like

$$\sum_{i,j,k} a_{ijk} u_i v_j v_k + \sum_{i,j} b_{ij} u_i v_j + \sum_{j,k} c_{jk} v_j v_k + \sum_i d_i u_i + \sum_j e_j v_j + f = 0.$$

Here these SOLEs are satisfied by all plaintext variables u_i and their corresponding ciphertext variables v_i and they are derived from the polynomials of the public key. For both first and second order linearization equations, the degrees of plaintext variables are one, and therefore, once the ciphertext variables v_j are evaluated, some plaintext variables can be linearly expressed by the rest plaintext variables, which implies that the range of possible plaintexts is minimized and the number of plaintext variables in public key equations can be reduced. If from the reduced public key equations first or second order linearization equations can be still derived, then the number of plaintext variables can be again reduced. If this number is small enough, we can directly solve out the plaintext variables from the reduced public key equations by XL or Gröbner basis algorithms [Fag99]. With the help of SOLEs, the authors of [DHN07] successfully broke the two instances proposed in [WYH06].

To resist the SOLE attack, Wang et al in [WFW09] and Wang in [Wan07] both modified MFE and raised the public key from quadratic to quartic equations. The increase of degree enlarges the scale of the public key exponentially by the degree of extension of fields r. To bound the length, r has to be very small, like 2 or 3. We call the above two improvements as Quartic-1 and Quartic-2 respectively for convenience. It is indeed the case that the SOLE attack is not practical on them, however, from their quartic public key equations, we can find equations of the form

$$\sum_{i,j,k} a_{ijk} u_i u_j v_k + \sum_{i,j} b_{ij} u_i u_j + \sum_{i,k} c_{ik} u_i v_k + \sum_i d_i u_i + \sum_k e_k v_k + f = 0.$$

We call them as Quadratization Equations (QEs). They are quadratic in plaintext variables and linear in ciphertext variables, hence QEs are still quadratic equations if ciphertext variables are evaluated. QEs can be regarded as a dual of SOLEs in the sense that switching the plaintext and ciphertext variables, QEs are turned into SOLEs. However, QEs can not be used to linearly eliminate plaintext variables, but for our cryptanalysis here, the parameter r in Quartic-1 and Quartic-2 is smaller than that in the original MFE, this means the complexity of searching QEs for Quartic-1 and Quartic-2 is much smaller than that of searching SOLEs for the original MFE.

The main aim of this paper is to illustrate that quadratization equations are helpful for reducing the range of possible plaintexts and can be used to efficiently attack Quartic-1 and Quartic-2. The paper also contains a work of cracking down another improved version of MFE by Wang et al [WZY07]. The improvement maintains public key equations as quadratic and introduces a new operator on matrices in its design for the goal of resisting against high order linearization equation attack. We show that the scheme can be even broken by the first order linearization equation attack.

The paper is organized as follows. In Section 2, we review the original MFE encryption scheme where the notations employed are also used to describe the three improved versions that are analyzed in this paper. In Sections 3 and 4 we present the quadratization equation attack on Quartic-1 and Quartic-2 respectively. Next in Section 5 we give the first order linearization equation attack on the improved MFE scheme of [WZY07]. The last section is the conclusion.

2 MFE Public Key Cryptosystem

2.1 MFE

Let K be a finite field, generally $\mathbb{F}_{2^{16}}$. Let $\mathbb{L}$ be its degree r extension field; $\mathbb{L}$ is considered the "Medium Field", generally $r = 4$ or 5. Its encryption transformation is a composition of three maps L_1, ϕ, and L_2, where $L_1 : K^{12r} \to K^{12r}$ and $L_2 : K^{15r} \to K^{15r}$ are two invertible affine maps and kept as a private key, and the so-called central map $\phi : K^{12r} \to K^{15r}$ is constructed by composing of $15r$ quadratic polynomials in $12r$ variables. The composition map $E = L_2 \circ \phi \circ L_1$ is used as a public key, and it is an ordered set of $15r$ quadratic polynomials in $12r$ variables.

The central map ϕ is publicly known and is constructed as follows. Let $\pi : L \to K^r$ be the natural isomorphism. Namely we take a basis of L over 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 $a_1, \cdots, a_r \in K$. Let $\tilde{\phi}$ be the polynomial map from L^{12} to L^{15}. Let $\tilde{\phi}(X_1, X_2, ...X_{12}) = (Y_1, Y_2, ...Y_{15})$. Suppose

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}.$$

and

$$Z_3 = M_1M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, Z_2 = M_1M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix},$$

$$Z_1 = M_2^T M_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}.$$

Then $\tilde{\phi}$ is expressed as

$$\begin{cases} Y_1 = X_1 + \det(M_2) + Q_1 \\ Y_2 = X_2 + \det(M_3) + Q_2 \\ Y_3 = X_3 + \det(M_1) + Q_3 \\ Y_4 = X_1X_5 + X_2X_7 \qquad Y_5 = X_1X_6 + X_2X_8 \\ Y_6 = X_3X_5 + X_4X_7 \qquad Y_7 = X_3X_6 + X_4X_8 \\ Y_8 = X_1X_9 + X_2X_{11} \qquad Y_9 = X_1X_{10} + X_2X_{12} \\ Y_{10} = X_3X_9 + X_4X_{11} \qquad Y_{11} = X_3X_{10} + X_4X_{12} \\ Y_{12} = X_5X_9 + X_7X_{11} \qquad Y_{13} = X_5X_{10} + X_7X_{12} \\ Y_{14} = X_6X_9 + X_8X_{11} \qquad Y_{15} = X_6X_{10} + X_8X_{12} \end{cases} \tag{1}$$

The triple(Q_1, Q_2, Q_3) is a triangular map from K^{3r} to itself as follows. Let $\pi(X_1) = (x_1, \cdots, x_r)$, $\pi(X_2) = (x_{r+1}, \cdots, x_{2r})$, $\pi(X_3) = (x_{2r+1}, \cdots, x_{3r})$, and let $q_i \in K[x_1, \cdots, x_{i-1}]$, $2 \le i \le 3r$. Then

$$\begin{cases} Q(X_1) = \sum_{i=2}^{r} q_i(x_1, \cdots, x_{i-1})\theta_i \\ Q(X_1, X_2) = \sum_{i=1}^{r} q_{r+i}(x_1, \cdots, x_{i-1}\theta_i) \\ Q(X_1, X_2, X_3) = \sum_{i=1}^{r} q_{2r+i}(x_1, \cdots, x_{i-1}\theta_i) \end{cases}$$

The q_i can be any randomly chosen quadratic polynomials. The public key $E = L_2 \circ \pi \circ \tilde{\phi} \circ \pi^{-1} \circ L_1$. The encryption of MFE is the evaluation of public key polynomials, namely given a plaintext $(u_1, \cdots, u_{12r})$, its ciphertext is

$$(v_1, \cdots, v_{15r}) = (h_1(u_1, \cdots, u_{12r}), \cdots, h_{15r}(u_1, \cdots, u_{12r}))$$

For a legal user, having known L_1, L_2, the key point of decryption is efficiently inverse $\tilde{\phi}$. For a given $(Y_1, \cdots, Y_{15})$, we can easily compute $\det(Z_1), \det(Z_2), \det(Z_3)$, and by

$$\begin{cases} \det(Z_3) = \det(M_1)\det(M_2) \\ \det(Z_2) = \det(M_1)\det(M_3) \\ \det(Z_1) = \det(M_2)\det(M_3) \end{cases} \tag{2}$$

if M_1,M_2 and M_3 are invertible, we can compute the value of $\det(M_1)$,$\det(M_2)$ and $\det(M_3)$. In this case, by the former three equations of (1), X_1, X_2 and X_3 are solved out. If $X_1 \neq 0$, from $X_1X_4 + X_2X_3 = \det(M_1)$, we can get the value of X_4. With X_1, X_2, X_3 and X_4 evaluated, the latter 12 equations of (1) form a triangular structure, so $X_4, \cdots, X_{12}$ are subsequently attained. Appendix B of

[WYH06] presents the method of computing the X_1 in the case when $X_1 = 0$. It is slightly easier than the case of $X_1 \neq 0$. Since the possibility that M_1,M_2 and M_3 are invertible is close to 1, then we can assume that we can always successfully decrypt a valid ciphertext in the above way.

There are two typical instances of MFE proposed by the designers of MFE.

1. MFE-1, where $K = F_{2^{16}}$ and $r = 4$. The public key has 60 quadratic polynomials with 48 variables.
2. MFE-1′,where $K = F_{2^{16}}$ and $r = 5$. The public key has 75 quadratic polynomials with 60 variables.

2.2 SOLE Attack on MFE

Denote M^* as the associated matrix of a square matrix M; then $MM^* = \det(M)I$, where I is a square identity matrix. we have

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

From these, we can derive

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

That is

$$M_3 Z_2^* Z_3 = \det(Z_2) M_2$$

Expand the relation into the matrix form, we can get 4 equations on each entry of the form

$$\sum_{i,j,k} A_{ijk} X_i Y_j Y_k = 0, A_{ijk} \in L \tag{3}$$

In [DHN07], using the same technique, 24 equations of this form can be found. Applying $(X_1, \cdots, X_{12}) = \pi^{-1} L_1(v_1, \cdots, v_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi^{-1} L_2^{-1}(u_1, \cdots, u_{15r})$ to (3), we can get $24r$ equations of the form

$$\sum_{ijk} a_{ijk} u_i v_j v_k + \sum_{i,j} b_{ij} u_i v_j + \sum_{jk} c_{jk} v_j v_k + \sum_i d_i u_i + \sum_j e_j v_j + c = 0$$

where $a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c \in K$. These equations are SOLEs. Once the ciphertext variables are evaluated, these equations are linear in u_i, so some plaintext variables can be linearly expressed by the rest plaintext variables, which implies that the number of plaintext variables in public key equations will be reduced. If the number is small enough, we can directly solve out the plaintext variables from the reduced public key equations by XL or Gröebner Basis. With the help of these SOLEs, authors of [DHN07] successfully broke the above two instances.

3 Quadratization Equation Attack on the Quartic-1 Scheme

3.1 The Quartic-1 Scheme

Having noticed the existence of SOLEs, the authors of [WFW09] design Z_1, Z_2 and Z_3 in the following strategy. Here M_1, M_2, M_3 are the same as those in the original MFE.

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}.$$

Set

$$Z_3 = X_2X_3M_1M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix},$$

$$Z_2 = X_1X_2M_1M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix},$$

and

$$Z_1 = X_1X_3M_2^TM_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}.$$

The corresponding central map $\tilde{\phi} : L^{12} \to L^{15}$ is given as follows:

$$\begin{cases} Y_1 = X_1 + X_1^2\det(M_3) + Q_1 \\ Y_2 = X_2 + X_2^2\det(M_1) + Q_2 \\ Y_3 = X_3 + X_3^2\det(M_2) + Q_3 \\ Y_4 = X_2X_3(X_1X_5 + X_2X_7) \quad Y_5 = X_2X_3(X_1X_6 + X_2X_8) \\ Y_6 = X_2X_3(X_3X_5 + X_4X_7) \quad Y_7 = X_2X_3(X_3X_6 + X_4X_8) \\ Y_8 = X_1X_2(X_1X_9 + X_2X_{11}) \quad Y_9 = X_1X_2(X_1X_{10} + X_2X_{12}) \\ Y_{10} = X_1X_2(X_3X_9 + X_4X_{11}) \quad Y_{11} = X_1X_2(X_3X_{10} + X_4X_{12}) \\ Y_{12} = X_1X_3(X_5X_9 + X_7X_{11}) \quad Y_{13} = X_1X_3(X_5X_{10} + X_7X_{12}) \\ Y_{14} = X_1X_3(X_6X_9 + X_8X_{11}) \quad Y_{15} = X_1X_3(X_6X_{10} + X_8X_{12}) \end{cases} \tag{4}$$

The triple (Q_1, Q_2, Q_3) is constructed in the same way as in MFE [WYH06]. The decryption process follows the same line of that of MFE. Given a valid ciphertext, we can get $\det(Z_1)$, $\det(Z_2)$, and $\det(Z_3)$ as follows. Since we have

$$\begin{cases} \det(Z_3) = X_2^2X_3^2\det(M_1)\det(M_2) \\ \det(Z_2) = X_1^2X_2^2\det(M_1)\det(M_3) \\ \det(Z_1) = X_1^2X_3^2\det(M_2)\det(M_3) \end{cases} \tag{5}$$

when M_1,M_2 and M_3 are invertible and none of X_1,X_2 and X_3 is zero, we can get values of $X_1^2\det(M_3)$, $X_3^2\det(M_2)$ and $X_2^2\det(M_1)$ as follows:

$$\begin{cases} X_1^2\det(Z_3) = \sqrt{\det(Z_2)\det(Z_1)\det(Z_3)^{-1}} \\ X_3^2\det(Z_2) = \sqrt{\det(Z_1)\det(Z_3)\det(Z_2)^{-1}} \\ X_2^2\det(Z_1) = \sqrt{\det(Z_2)\det(Z_3)\det(Z_1)^{-1}} \end{cases}$$

The square root operation is easy to handle over a characteristic two field. Substituting $X_1^2\det(M_3)$, $X_3^2\det(M_2)$ and $X_2^2\det(M_1)$ into the first three equations of (4), X_1, X_2 and X_3 are solved out. From $X_2^2\det(M_1) = X_2^2(X_1X_4 + X_2X_3)$, we can get X_4. Substituting X_1,X_2,X_3 and X_4 into the last twelve equations of (4), a triangular structure is formed so that $X_5, \cdots, X_{12}$ can be subsequently attained.

This new encryption scheme Quartic-1 raises the polynomials of the public key to be degree four, namely they are quartic polynomials in plaintext variables. To bound the size of public key, the authors in [WFW09] has to reduce the size of K and the extension degree r. There are two sets of parameters proposed:

1. Quartic-1, where $K = \mathbb{F}_{2^8}$ and $r = 2$. The public key has 30 quartic polynomials with 24 variables.
2. Quartic-1′,where $K = \mathbb{F}_{2^4}$ and $r = 3$. The public key has 45 quartic polynomials with 36 variables.

3.2 Cryptanalysis of Quartic-1

In [WFW09], the authors claim that SOLEs do not exist for the Quartic-1 system, however, our experiments show that at least $2r$ SOLEs always exist. We find two equations that hold on $\tilde{\phi}$:

$$\begin{cases} X_2Y_{12}Y_{15} + X_2Y_{13}Y_{14} + X_9Y_4Y_{15} + X_9Y_5Y_{13} + X_{10}Y_4Y_{14} + X_{10}Y_5Y_{12} = 0 \\ X_5Y_{10}Y_{15} + X_5Y_{11}Y_{14} + X_6Y_{10}Y_{13} + X_6Y_{11}Y_{12} + X_9Y_4Y_{15} + X_9Y_5Y_{13} \\ \qquad\qquad + X_{10}Y_4Y_{14} + X_{10}Y_5Y_{12} = 0 \end{cases} \tag{6}$$

Substituting $(X_1, \cdots, X_{12}) = \pi^{-1}L_1(v_1, \cdots, v_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi^{-1}L_2^{-1}(u_1, \cdots, u_{15r})$ to (6), we can get $2r$ equations of the form:

$$\sum_{i,j,k} a_{ijk}u_iv_jv_k + \sum_{i,j} b_{ij}u_iv_j + \sum_{j,k} c_{jk}v_jv_k + \sum_i d_iu_i + \sum_j e_jv_j + f = 0 \tag{7}$$

where $a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c \in K$. They are SOLEs and can help us to reduce the number of plaintext variables for a ciphertext-only attack. The complexity of recovering the coefficient vectors $(a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c)$ is $(90r^2(15r + 1) + 180r^2 + 15r(15r + 1)/2 + 27r + 1)^w$, $w \approx 2.732$. For the parameter specification of Quartic-1, this complexity is about 2^{37}; for the parameter of Quartic-1′, this complexity is about 2^{41}.

Unfortunately, these SOLEs can only reduce $2r$ plaintext variables, and they help little to simplify the central map in order to derive more SOLEs, moreover, substituting them into the central map $\tilde{\phi}$ would destroy its compact expression.

However, we can easily find plenty of quadratization equations from $\tilde{\phi}$. Taking Y_4, Y_5, Y_6, Y_7 into consideration, it is obvious that there holds a QE between any two of them. Take Y_4, Y_5 as example, it is

$$(X_1X_5 + X_2X_7)Y_5 = (X_1X_6 + X_2X_8)Y_4$$

In fact, there are at least 9 independent Quadratic Equation. They are as follows:

$$\begin{cases} (X_1X_6 + X_2X_8)Y_4 + (X_1X_5 + X_2X_7)Y_5 = 0 \\ (X_3X_5 + X_4X_7)Y_4 + (X_1X_5 + X_2X_7)Y_6 = 0 \\ (X_3X_6 + X_4X_8)Y_4 + (X_1X_5 + X_2X_7)Y_7 = 0 \\ (X_3X_5 + X_4X_7)Y_5 + (X_1X_6 + X_2X_8)Y_6 = 0 \\ (X_3X_6 + X_4X_8)Y_5 + (X_1X_6 + X_2X_8)Y_7 = 0 \\ (X_3X_6 + X_4X_8)Y_6 + (X_3X_5 + X_4X_7)Y_7 = 0 \\ X_3X_6Y_4 + X_4X_7Y_5 + X_1X_6Y_6 + X_2X_7Y_7 = 0 \\ X_3X_8Y_4 + X_3X_7Y_5 + X_1X_8Y_6 + X_1X_7Y_7 = 0 \\ X_4X_6Y_4 + X_4X_5Y_5 + X_2X_6Y_6 + X_2X_5Y_7 = 0 \end{cases} \tag{8}$$

If Y_4, Y_5, Y_6, Y_7 are substituted by a ciphertext, we will get 6 independent quadratic equations in (8) if $Y_4Y_5 \neq 0$, since we can find a 6×6 invertible coefficient submatrix

$$\begin{pmatrix} Y_5 & 0 & 0 & 0 & 0 & 0 \\ Y_6 & Y_4 & Y_4 & 0 & 0 & 0 \\ Y_7 & 0 & 0 & Y_4 & 0 & 0 \\ 0 & 0 & Y_5 & Y_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & Y_4 \end{pmatrix}$$

with determinant equal to $Y_4^4Y_5^2$. Here consider every term X_iX_j presented in (8) as a single variable. Since $Y_4Y_5 \neq 0$ holds with a probability almost being 1, we can always get 6 independent quadratic equations.

Similarly to (8), we can find at least 9 independent QEs from Y_8, Y_9, Y_{10}, Y_{11} and another 9 independent quadratic equations from $Y_{12}, Y_{13}, Y_{14}, Y_{15}$. These three sets of QEs are composed of different terms, hence we can get 27 QEs, and they become 18 independent quadratic equations if variables Y_i are fixed by ciphertext values.

Besides, observe the relation between Y_4, Y_5, Y_{12} and Y_{14} and the relation between Y_4, Y_5, Y_{13} and Y_{15}, we have

$$\begin{cases} X_8X_9Y_4 + X_7X_9Y_5 + X_2X_8Y_{12} + X_2X_7Y_{14} = 0 \\ X_8X_{11}Y_4 + X_7X_{11}Y_5 + X_2X_6Y_{12} + X_2X_5Y_{14} = 0 \\ X_8X_{10}Y_4 + X_7X_{10}Y_5 + X_2X_8Y_{13} + X_2X_7Y_{15} = 0 \\ X_8X_{12}Y_4 + X_7X_{12}Y_5 + X_2X_6Y_{13} + X_2X_5Y_{15} = 0. \end{cases} \tag{9}$$

Similarly, we can also find another two QEs from Y_{10}, Y_{11}, Y_{12} and Y_{13}, and 2 QEs from Y_{10}, Y_{11}, Y_{14} and Y_{15}. So totally there are 35 QEs derived from the central map, and at least 18 of them are independent.

Substituting $(X_1, \cdots, X_{12}) = \pi^{-1}L_1(v_1, \cdots, v_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi^{-1}L_2^{-1}(u_1, \cdots, u_{15r})$ into (8) and (9), we can get $35r$ QEs over K of the form

$$\sum_{i,j,k} a_{ijk}u_iu_jv_k + \sum_{i,j} b_{ij}u_iu_j + \sum_{i,k} c_{ik}u_iv_k + \sum_i d_iu_i + \sum_k e_kv_k + f = 0, \tag{10}$$

where $a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c \in K$. Since (8) and (9) exist for all corresponding plaintext and ciphertext variables, recovering a basis of these QE's coefficient vectors $(a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c)$ is a precomputation. The computational complexity is $\mathcal{O}((15r+1)6r(12r+1)+180r^2+27r+1)^w$, $w \approx 2.732$. This complexity is about 2^{36} for the parameter in Quartic-1; and 2^{40} for the parameter in Quartic-1′.

Given a ciphertext, if it is substituted into (8) and (9), we can get a system of at least $35r$ quadratic equations, denote it as $\mathcal{S}$. If we can work out a Gröbner basis of $\mathcal{S}$ with a small dimension, say s, we can find the original plaintext by $|K|^s$ exhausted search.

3.3 Dimension of $\mathcal{S}$

Since the scale of $\mathcal{S}$ is impractical for directly computing its Gröber basis, when $r = 2$, $|\mathcal{S}| \geq 70$. Experiment shows that it is really time consuming, so after obtaining $\mathcal{S}$, how to determine its dimension s? We apply an intermediate way to find s. Suppose we fix the last t variables by randomly chosen elements in K, and compute the corresponding Gröbner basis by an equation solving algorithm like F_4. By experiment, we find the following three results can be efficiently obtained:

1. if $t > s$, it always output GB=$\{1\}$.
2. if $t = s$, it always output a zero-dimensional GB.
3. if $t < s$, it always output a positive-dimensional GB.

This observation help us to make a strategy to determine s. We can choose a fairly big t, if it outputs GB=$\{1\}$ by F_4, then t decrease by 1; if it outputs a zero-dimensional GB, returns t and stops.

Using the above strategy we can efficiently determine the dimension of $\mathcal{S}$, i.e., s. The last step is to search the last s ciphertext variables $|K|^s$ times and compute the Gröbner basis for each time. It would be a disaster for a normal computer, but this set-back can be greatly improved by sufficiently many parallel computers.

3.4 Experiment Results

In order to compare Quartic-1 and Quartic-2, which will be analyzed in the following section, we take the parameter of Quartic-1 in section 3.1, $K = \mathbb{F}_{2^8}$, $r = 2$, which is the same as Quartic-2 given in Section 4.1. We chose 10 different pairs of L_1 and L_2 and, and for each of them, we chose 100 different valid ciphertext for experiments.

The precomputation is to recover SOLEs and QEs from the public key of Quartic-1. To recover (7), we randomly selected 13400 plain/cipher-text pairs and substituted them into the public key. Then the main task is a Gaussian elimination on a 13400×13400 matrix on $\mathbb{F}_{2^8}$. On a normal computer, with Genuine Intel(R) CPU T2300@1.66GHz, 504MB RAM, the time running in a magma procedure is about 3595.125 seconds; To recover (10), use the same

technique as for (7) to recover the coefficients in (10) and the running time is about 2316.750 seconds.

Using the strategy mentioned in the previous subsection, we can efficiently determine the dimension of $\mathcal{S}$, $s = 5$. We find it just need 0.531 seconds when $t > s$, and 1.328 seconds when $t = s$. However, doing 2^{40} times GB computation would still be a disaster for the above normal computer. If we have sufficiently many fast-speed parallel computers, then we can run Gröbner basis algorithm independently on multiple machines, so that the cost of time in this search process can be greatly saved.

4 Quadratization Equation Attack on the Quartic-2 Scheme

4.1 The Quartic-2 Scheme

To resist SOLEs, the author of [Wan07] proposed to construct the Z_1,Z_2 and Z_3 in the MFE scheme as follows: $Z_3 = M_1 M_2^2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, Z_2 = M_1 M_3^2 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, Z_1 = M_3^2 (M_2^T)^2 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}$. Here M_1, M_2, M_3 are defined as the same as those in MFE.

Write the above three matrix equations into equations on their each entry, the central map $\tilde{\phi} : L^{12} \to L^{15}$ is then defined as follows:

$$
\begin{cases}
Y_1 = X_1 + \det(M_2) + Q_1 \\
Y_2 = X_2 + \det(M_3) + Q_2 \\
Y_3 = X_3 + \det(M_1) + Q_3 \\
Y_4 = X_1X_5^2 + X_1X_6X_7 + X_2X_5X_7 + X_2X_7X_8 \\
Y_5 = X_1X_5X_6 + X_1X_6X_8 + X_2X_6X_7 + X_2X_8^2 \\
Y_6 = X_3X_5^2 + X_3X_6X_7 + X_4X_5X_7 + X_4X_7X_8 \\
Y_7 = X_3X_5X_6 + X_3X_6X_8 + X_4X_6X_7 + X_4X_8^2 \\
Y_8 = X_1X_9^2 + X_1X_{10}X_{11} + X_2X_9X_{11} + X_2X_{11}X_{12} \\
Y_9 = X_1X_9X_{10} + X_1X_{10}X_{12} + X_2X_{10}X_{11} + X_2X_{12}^2 \\
Y_{10} = X_3X_9^2 + X_3X_{10}X_{11} + X_4X_9X_{11} + X_4X_{11}X_{12} \\
Y_{11} = X_3X_9X_{10} + X_3X_{10}X_{12} + X_4X_{10}X_{11} + X_4X_{12}^2 \\
Y_{12} = (X_9^2 + X_{10}X_{11})(X_5^2 + X_6X_7) + (X_9X_{10} + X_{10}X_{12})(X_5X_6 + X_6X_8) \\
Y_{13} = (X_9^2 + X_{10}X_{11})(X_5X_7 + X_7X_8) + (X_9X_{10} + X_{10}X_{12})(X_6X_7 + X_8^2) \\
Y_{14} = (X_9X_11 + X_{11}X_{12})(X_5^2 + X_6X_7) + (X_{10}X_{11} + X_{12}^2)(X_5X_6 + X_6X_8) \\
Y_{15} = (X_9X_{11} + X_{11}X_{12})(X_5X_7 + X_7X_8) + (X_{10}X_{11} + X_{12}^2)(X_6X_7 + X_8^2)
\end{cases}
\tag{11}
$$

The triple (Q_1, Q_2, Q_3) is constructed in the same way as in MFE. The decryption of a valid ciphertext is a little complex comparing with that of the original MFE. As limit of space, and that the subsequent analysis do not rely on how to decrypt, there is no need to elaborate the whole decryption process, so we only give how to get $\det(M_1)$,$\det(M_2)$, and $\det(M_3)$ given a valid ciphertext. Given a valid ciphertext, we can get $\det(Z_1)$, $\det(Z_2)$, $\det(Z_3)$. Since we have

$$\begin{cases} \det(Z_3) = \det(M_1)\det(M_2)^2 \\ \det(Z_2) = \det(M_1)\det(M_3)^2 \\ \det(Z_1) = \det(M_2)^2\det(M_3)^2 \end{cases} \tag{12}$$

when M_1,M_2 and M_3 are invertible and none of X_1,X_2 and X_3 is zero, we can get values of $\det(M_3)$, $\det(M_2)$ and $\det(M_1)$ as follows:

$$\begin{cases} \det(M_1) = \sqrt{\det(Z_2)\det(Z_3)\det(Z_1)^{-1}} \\ \det(M_2) = \sqrt[4]{\det(Z_3)\det(Z_1)\det(Z_2)^{-1}} \\ \det(M_3) = \sqrt[4]{\det(Z_1)\det(Z_2)\det(Z_3)^{-1}} \end{cases}$$

Note that square root operation here is easy to handle over a characteristic two field.

Since the public key equations of Quartic-2 are raised up to quartic, to bound the size of public key, the authors has to decrease the size of K and the extension degree r. There is one set of parameters proposed in [Wan07]:

1. Quartic-2, where $K = \mathbb{F}_{2^8}$ and $r = 2$. The public key has 30 quartic polynomials with 24 variables.

4.2 Cryptanalysis of Quartic-2

The designer of Quartic-2 noted that Quartic-2 is free from SOLE attack, this is indeed the case by experiment. However, we can utilize Quadratization Equations derived from quartic public key equations to attack Quartic-2.

From

$$Z_3 = M_1M_2^2, Z_2 = M_1M_3^2, Z_1 = M_3^2(M_2^T)^2,$$

we can derive that

$$\begin{cases} M_1Z_1^T = Z_3(M_3^T)^2 \\ Z_2(M_2^T)^2 = M_1Z_1 \end{cases} \tag{13}$$

From matrix equations in (13), we can find 8 quadratic equations on each entry over L of the form

$$\sum_{i,j,k} A_{ijk}X_iX_jY_k + \sum_{i,k} B_{i,k}X_iY_k = 0 \tag{14}$$

where $A_{ijk}, B_{j,k} \in L$. Obviously they become quadratic in plaintext variables once the ciphertext variables are fixed. Consider all the QEs as a vector space

spanned by the coefficients of terms. If Z_3, Z_2 are invertible (the probablity is almost 1), then these 8 equations are linearly independent.

Moreover, we can find other 6 quadratic equations exsit on $\tilde{\phi}$. They are as follows:

$$\begin{cases} X_3X_6Y_4 + X_4X_7Y_5 + X_1X_6Y_6 + X_2X_7Y_7 = 0 \\ X_3X_{10}Y_8 + X_4X_{11}Y_9 + X_1X_{10}Y_{10} + X_2X_{11}Y_{11} = 0 \\ X_4X_6Y_4 + (X_3X_6 + X_4X_5 + X_4X_8)Y_5 + X_2X_6Y_6 + (X_1X_6 + X_2X_5 + X_2X_8)Y_7 = 0 \\ (X_3X_5 + X_3X_8 + X_4X_7)Y_4 + X_3X_7Y_5 + (X_1X_5 + X_1X_8 + X_2X_7)Y_6 + X_1X_7Y_7 = 0 \\ (X_3X_9 + X_3X_{12} + X_4X_{11})Y_8 + X_3X_{11}Y_9 + (X_1X_9 + X_1X_{12} + X_2X_{11})Y_{10} + X_1X_{11}Y_{11} = 0 \\ X_4X_{10}Y_8 + (X_3X_{10} + X_4X_9 + X_4X_{12})Y_9 + X_2X_{10}Y_{10} + (X_1X_{10} + X_2X_9 + X_2X_{12})Y_{11} = 0 \end{cases} \tag{15}$$

Substituting $(X_1, \cdots, X_{12}) = \pi^{-1}L_1(v_1, \cdots, v_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi^{-1}$ $L_2^{-1}(u_1, \cdots, u_{15r})$ into (13) and (4.2), we can get $14r$ QEs over K of the form

$$\sum_{i,j,k} a_{ijk}u_iu_jv_k + \sum_{i,j} b_{ij}u_iu_j + \sum_{i,k} c_{ik}u_iv_k + \sum_i d_iu_i + \sum_k e_kv_k + f = 0 \tag{16}$$

where $a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c \in K$. Since (13) and (4.2) exist for all corresponding plaintext and ciphertext variables, and recovering a basis of these QE's coefficient vectors $(a_{ijk}, b_{ij}, c_{jk}, d_i, e_j, c)$ is a precomputation. The complexity is $\mathcal{O}((15r + 1)6r(12r + 1) + 180r^2 + 27r + 1)^w$, $w \approx 2.732$. It is about 2^{36} for the parameter given in the previous subsection.

Assume we have found the above $14r$ QEs in (16), now for a given ciphertext $(v'_1, \cdots, v'_{15r})$, after substituting v'_i into (16), we get $14r$ quadratic equations in $12r$ plaintext variables, denoted as $(16)'$. Instead of solving the public quartic equations by XL or F_4, we can turn to solve $(16)'$. Since $(16)'$ are quadratic and r is as small as 2, it is realistic to save much more time and memory. It also means that we can find the variety of $(16)'$, denoted as $\mathcal{V}$. Next we will show there still exist Quadratic Equations that holds on $\mathcal{V}$.

Let $(Y'_1, \cdots, Y'_{15}) = \pi^{-1}L_2^{-1}(v'_1, \cdots, v'_{15r})$ and $(X_1, \cdots, X_{12}) = \pi^{-1}L_1(u_1, \cdots,$ $u_{12r})$. Note that here $(v'_1, \cdots, v'_{15r})$ is known, and $(u_1, \cdots, u_{12r})$ is unknown. By (13), we have

$$M_1Z_1'^T = Z'_3(M_3^T)^2 \quad Z'_2(M_2^T)^2 = M_1Z'_1. \tag{17}$$

Here Z'_1, Z'_2 and Z'_3 are constant matrices. Suppose after adding these two relations (17) into the $\tilde{\phi}$ results into another $\tilde{\phi}'$. The relation $Z_2 = M_1M_3^2$, $Z_3 = M_1M_2$ which originally hold on $\tilde{\phi}$, definitely still hold on $\tilde{\phi}'$. From $\tilde{\phi}'$, we get

$$Z_2Z_3'^T = M_1Z'_1M_1^T. \tag{18}$$

holds on $\tilde{\phi}'$. From this matrix equation, we can get 4 quadratic equations over L of the form

$$\sum_{i,j} A_{ij}X_iX_j + \sum_k B_kY_k = 0 \tag{19}$$

where $A_{ij}, B_k \in L$. If Z'_1 is invertible (the possiblity is almost 1), these 4 quadratic equations are linearly independent. Substituting $(X_1, \cdots, X_{12}) = \pi^{-1}$ $L_1(v_1, \cdots, v_{12r})$ and $(Y_1, \cdots, Y_{15}) = \pi^{-1}L_2^{-1}(u_1, \cdots, u_{15r})$ into (19), we can get

another $4r$ independent quadratic equations in plaintext variables over K of the form

$$\sum_{i,j} a_{ij} u_i u_j + \sum_i b_i u_i + \sum_k c_k v_k + c = 0 \tag{20}$$

where $a_{ij}, b_i, c_k, c \in K$. To recover the coefficients of (20), the complexity is $\mathcal{O}(6r(12r+1)+27r+1)^w$. It is about 2^{23} for the parameter given in the previous subsection.

From the above analysis, given a ciphertext, (16) and (20) theoretically give $18r$ quadratic equations, of which at least $12r$ have linearly independent coefficient vectors. The complexity of recovering all these quadratic equations is mainly depend on the precomputation of recovering (16), and it is about 2^{36} for the parameter given in section 4.1.

Given a ciphertext, after finding quadratic equations $(16)'$ and $(20)'$, here (20) becomes $(20)'$ after ciphertext variabes are evaluated, the last step is to find the plaintext by solving these quadratic equations. Experiment results show that it efficiently works using equation solving algorithm to compute Gröbner basis as r is small. So we conclude that ciphertext-only attack on Quartic-2 can be reduced to solving quadratic equations derived from $(16)'$ and $(20)'$ with complexity $\mathcal{O}((15r+1)6r(12r+1)+180r^2+27r+1)^w$, it is 2^{36} for the parameter mentioned above.

4.3 Experiment Results

As the parameter set proposed in [Wan07], we set $K = \mathbb{F}_{2^8}$ and $r = 2$. We chose 10 different pairs of L_1 and L_2, and for each of them we chose 100 different valid ciphertext for experiments.

The first step of our attack is recovering (16). To recover (16), we randomly selected 10075 plain/cipher-text pairs and substituted them into the public key. Then the main task is a Gaussian elimination on a 10075×11075 matrix on $\mathbb{F}_{2^8}$. On a normal computer, with Genuine Intel(R) CPU T2300@1.66GHz, 504MB RAM, a Magma procedure run averagely in 1779.656 seconds. The number of (16) is always much bigger than $14r$, which is 28 for our parameter, and it is always up to 49. The second step is to use equation solving algorithms like F_4 to find $\mathcal{V}$ in order to deduce more quadratic equations in (20). This step takes up a long time as 3110.734 seconds on average. Actually, our experiment results show that only through solving quadratic equations from $(16)'$, we can always find the original plaintext, which means we do not need to take the further step to find (20).

5 The Improved MFE Public Key Cryptosystem

5.1 The Improved MFE

To resist SOLE, the authors of [WZY07] proposed an improved MFE encryption transformation. The public key polynomials are still of degree 2. Let

$\tilde{\phi}(X_1, X_2, \cdots, X_8) = (Y_1, Y_2, \cdots, Y_{10})$, the central map $\tilde{\phi}$: $L^8 \to L^{10}$ is defined as follows.

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; \\ Y_2 = X_2 + X_1X_4 + X_2X_3 + Q_2; \\ Y_3 = X_1X_5 + X_2X_7; \qquad Y_4 = X_1X_6 + X_2X_8; \\ Y_5 = X_3X_5 + X_4X_7; \qquad Y_6 = X_3X_6 + X_4X_8; \\ Y_7 = X_1X_5 + X_3X_7; \qquad Y_8 = X_2X_5 + X_4X_7; \\ Y_9 = X_1X_6 + X_3X_8; \qquad Y_{10} = X_2X_6 + X_4X_8; \end{cases} \tag{21}$$

Here the definitions of Q_1, Q_2 is similar to Q_1, Q_2, Q_3 in section 2. Q_1, Q_2 form a triangular map from K^{2r} to itself. Suppose

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, \quad M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix},$$

and

$$Z_1 = M_1^{\hat{l}} M_2 = \begin{pmatrix} Y_3 & Y_4 \\ Y_5 & Y_6 \end{pmatrix}, \quad Z_2 = M_2^T M_1 = \begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix}.$$

Here, the operator "$\hat{}$" is defined as follows:

$$M^{\hat{l}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\hat{l}} = \begin{pmatrix} a^l & b^l \\ c^l & d^l \end{pmatrix}.$$

Given a valid ciphertext $(v_1, \cdots, v_{10r})$, the decryption of the scheme follows the same line of decrypting MFE, and the key point is to recover M_1 and M_2. From Z_1, Z_2, we have

$$\begin{cases} [\det(M_1)]^l \cdot \det(M_2) = \det(Z_1) \\ \det(M_2) \cdot \det(M_1) = \det(Z_2) \end{cases} \tag{22}$$

Hence,

$$\begin{aligned} \det(M_1) &= \left(\frac{\det(Z_1)}{\det(Z_2)}\right)^{\frac{1}{l-1}} \\ \det(M_2) &= \frac{\det(Z_2)}{\det(M_1)} \end{aligned} \tag{23}$$

Then, the values of $X_1, \cdots, X_8$ can be derived in turn.

Remark: Because for any $X \in L$, we have $X^l = X$. Then,

$$M_1^{\hat{l}} = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}^{\hat{l}} = \begin{pmatrix} X_1^l & X_2^l \\ X_3^l & X_4^l \end{pmatrix} = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} = M_1$$

So the left sides of two equations in system (22) are equal, and consequently the value of $\det(M_1)$ can not be gotten from (23). That means the decryption fails to recovering ciphertext. There is no recommended parameter in [WZY07], to assure the safety, we use $K = F_8, r = 10$ for experiment in our paper.

5.2 Linearization Equation Attack

Through analysis, we found that there are many FOLEs satisfied by the above improved MFE. Since $Z_2 = M_2^T M_1$, multipling M_2 on both sides, we have $Z_2 M_2 = M_2^T M_1 M_2 = M_2^T Z_1$, so,

$$Z_2 M_2 = M_2^T Z_1$$

Expanding it, we have

$$\begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix} \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix} = \begin{pmatrix} X_5 & X_7 \\ X_6 & X_8 \end{pmatrix} \begin{pmatrix} Y_3 & Y_4 \\ Y_5 & Y_6 \end{pmatrix}$$

then

$$\begin{pmatrix} X_5Y_7 + X_7Y_8 & X_6Y_7 + X_8Y_8 \\ X_5Y_9 + X_7Y_{10} & X_6Y_9 + X_8Y_{10} \end{pmatrix} = \begin{pmatrix} X_5Y_3 + X_7Y_5 & X_5Y_4 + X_7Y_6 \\ X_6Y_3 + X_8Y_5 & X_6Y_4 + X_8Y_6 \end{pmatrix}$$

that is,

$$\begin{cases} X_5Y_7 + X_7Y_8 = X_5Y_3 + X_7Y_5; \\ X_6Y_7 + X_8Y_8 = X_5Y_4 + X_7Y_6; \\ X_5Y_9 + X_7Y_{10} = X_6Y_3 + X_8Y_5; \\ X_6Y_9 + X_8Y_{10} = X_6Y_4 + X_8Y_6. \end{cases} \tag{24}$$

On the other hand, from $Z_1 = M_1 M_2$, take transpose on it and then right multiply $(M_1^T)^{-1}$ on both sides, we have

$$Z_1^T \left(M_1^T\right)^{-1} = M_2^T \tag{25}$$

From $Z_2 = M_2^T M_1$, right multiply $(M_1)^{-1}$ on both sides, we get

$$Z_2 M_1^{-1} = M_2^T. \tag{26}$$

From (25) and (26), we can deduce

$$Z_1^T \left(M_1^T\right)^* = Z_2 M_1^* \tag{27}$$

Expanding it, we derive

$$\begin{cases} X_4Y_3 + X_2Y_5 = X_4Y_7 + X_3Y_8; \\ X_3Y_3 + X_1Y_5 = X_2Y_7 + X_1Y_8; \\ X_4Y_4 + X_2Y_6 = X_4Y_9 + X_3Y_{10}; \\ X_3Y_4 + X_1Y_6 = X_2Y_9 + X_1Y_{10}. \end{cases} \tag{28}$$

Substituting $(X_1, \cdots, X_8) = \pi_1 \circ \phi_1(u_1, \cdots, u_{8r})$ and $(Y_1, \cdots, Y_{10}) = \pi_2^{-1} \circ \phi_3^{-1}(v_1, \cdots, v_{10r})$ into (24) and (28), we get $8r$ equations of the form

$$\sum_{i,j} a_{ij} m_i z_j + \sum_i b_i m_i + \sum_j c_j z_j + d = 0 \tag{29}$$

where the coefficients $a_{ij}, b_i, c_j, d \in K$, and they are first order linearization equations (FOLEs). The complexity of recovering coefficients in these equations is $(80r^2 + 18r + 1)^w$., which is $(8200)^3 \leq 2^{40}$ for the parameter we choosen. So there are at least $8r$ FOLEs.

Through analysis,we find that the ranks of systems (24) and (28) coefficients matrix are both equal to 3. Hence, after substituting ciphertext variables into them, we can at least get $6r$ independent linear equations. So all the plaintext variables can be represented by $2r$ plaintext variables. Actually, from (24) and (28), X_1, X_2, X_3, X_4 can be expressed by the multiple of one variable (say S_1) of them and X_5, X_6, X_7, X_8 can be expressed by the multiple of one variable (say S_2) of them. The central map of new quadratic functions can be changed to:

$$\begin{cases} \tilde{Y}_1 = C_1 S_1 + C_2 S_2^2 + Q_1 \\ \tilde{Y}_2 = C_3 S_1 + C_4 S_1^2 + Q_2 \\ \tilde{Y}_3 = C_5 S_1 S_2 \end{cases} \tag{30}$$

So, there are only $2r$ unknowns and $3r$ linearly independent equations in system (30). We can solve this system directly by Gröbner algorithm.

5.3 Experiment Results

In our experiments, we choose $K = \mathbb{F}_{2^8}$, $r = 10$. We chose 10 different pairs of L_1 and L_2, and for each of them we chose 100 different valid ciphertext for experiments.

The first step is recovering FOLEs in (29). To recover (29), we randomly selected 8200 plain/cipher-text pairs and substituted them into the public key. Then the main task is a Gaussian elimination on a 8200×8200 matrix on $\mathbb{F}_{2^8}$, and it takes 22 minutes. The number of (29) is always much bigger than $8r$, and it is always 110 in our experiment. Since this step is independent of the value of the ciphertext, then this step is a precomputation.

The second step is that given a ciphertext $(v'_1, \cdots, v'_{10r})$, find corresponding plaintext $(u'_1, \cdots, u'_{8r})$. Substitute $(v'_1, \cdots, v'_{10r})$ into (29), suppose we can get s independent linear equations. Our experiments show $s = 60$ exactly the same as the theoretical analysis in the above section.

The third step is to substitute the 60 linear expressions into the public key polynomials and get a system of reduced linear public key polynomials as (30). Our experiments show, it takes about 6 second to solve the system by F_4 and recover the corresponding plaintext.

5.4 Extension of Improved MFE and Its Analysis

We extend the improvement in [WZY07]. Use the same notation as in [WZY07], we extended the central map $\tilde{\phi}_2(X_1, X_2, \cdots, X_8) = (Y_1, Y_2, \cdots, Y_{10})$ as following form.

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1 \\ Y_2 = X_2 + X_1X_4 + X_2X_3 + Q_2 \\ Y_3 = X_1^{q^t}X_5 + X_2^{q^t}X_7 \qquad Y_4 = X_1^{q^t}X_6 + X_2^{q^t}X_8 \\ Y_5 = X_3^{q^t}X_5 + X_4^{q^t}X_7 \qquad Y_6 = X_3^{q^t}X_6 + X_4^{q^t}X_8 \\ Y_7 = X_1X_5 + X_3X_7 \qquad Y_8 = X_2X_5 + X_4X_7 \\ Y_9 = X_1X_6 + X_3X_8 \qquad Y_{10} = X_2X_6 + X_4X_8 \end{cases}$$

where $1 \leq t < l$.

The matrix forms are listed as follows.

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}.$$

$$Z_1 = M_1^{\hat{t}}M_2 = \begin{pmatrix} Y_3 & Y_4 \\ Y_5 & Y_6 \end{pmatrix}, Z_2 = M_2^T M_1 = \begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix}.$$

From

$$\begin{cases} [\det(M_1)]^{q^t} \cdot \det(M_2) = \det(Z_1) \\ \det(M_2) \cdot \det(M_1) = \det(Z_2) \end{cases}$$

we can obtain the values $\det(M_1)$ and $\det(M_2)$, then we can get $X_1, \cdots, X_8$ in turn.

Unfortunately, this scheme also satisfy FOLEs, but in this case we can only derive $4r$ FOLEs in first step.

Lemma 1. Let k be a finite field with characteristic q, the operator "$\hat{}$" defined on k is homomorphic, that is

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}^{\hat{q^t}} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}^{\hat{q^t}} = \left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right)^{\hat{q^t}}$$

where$a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in k$.

Proof. In finite field k with characteristic q,

$$(a+b)^q = a^q + b^q, a, b \in k.$$

Then

$$\begin{aligned} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}^{\hat{q^t}} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}^{\hat{q^t}} &= \begin{pmatrix} a_1^{q^t} & b_1^{q^t} \\ c_1^{q^t} & d_1^{q^t} \end{pmatrix} \begin{pmatrix} a_2^{q^t} & b_2^{q^t} \\ c_2^{q^t} & d_2^{q^t} \end{pmatrix} \\ &= \begin{pmatrix} a_1^{q^t}a_2^{q^t} + b_1^{q^t}c_2^{q^t} & a_1^{q^t}b_2^{q^t} + b_1^{q^t}d_2^{q^t} \\ c_1^{q^t}a_2^{q^t} + d_1^{q^t}c_2^{q^t} & c_1^{q^t}b_2^{q^t} + d_1^{q^t}d_2^{q^t} \end{pmatrix} \\ &= \begin{pmatrix} (a_1a_2 + b_1c_2)^{q^t} & (a_1b_2 + b_1d_2)^{q^t} \\ (c_1a_2 + d_1c_2)^{q^t} & (c_1b_2 + d_1d_2)^{q^t} \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}^{\hat{q}^t}$$
$$= \left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right)^{\hat{q}^t}$$

□

According to Lemma 1, we have

$$Z_2^{\hat{q}^t} = (M_2^T M_1)^{\hat{q}^t} = (M_2^T)^{\hat{q}^t} M_1^{\hat{q}^t}$$

Multiplying M_2 on both sides,

$$Z_2^{\hat{q}^t} M_2 = (M_2^T)^{\hat{q}^t} M_1^{\hat{q}^t} M_2 = (M_2^T)^{\hat{q}^t} Z_1$$

Expanding it, we get 4 equation below,

$$\begin{cases} X_5 Y_7^{q^t} + X_7 Y_8^{q^t} = X_5^{q^t} Y_3 + X_7^{q^t} Y_5; \\ X_6 Y_7^{q^t} + X_8 Y_8^{q^t} = X_5^{q^t} Y_4 + X_7^{q^t} Y_6; \\ X_5 Y_9^{q^t} + X_7 Y_{10}^{q^t} = X_6^{q^t} Y_3 + X_8^{q^t} Y_5; \\ X_6 Y_9^{q^t} + X_8 Y_{10}^{q^t} = X_6^{q^t} Y_4 + X_8^{q^t} Y. \end{cases} \tag{31}$$

If we use K-linear isomorphisms on map $Y = X^{q^t}$, $X, Y \in L$, it should be linear map on K, see [DGS06]. Hence,we can find there exit at least $4r$ FOLEs satisfied by this scheme.

On the other hand, from $Z_2^T = M_1^T M_2$, $Z_1 = M_1^{\hat{q}^t} M_2$, we can derive

$$\left(M_1^{\hat{q}^t}\right)^{-1} Z_1 = (M_1^T)^{-1} Z_2^T$$

Namely,

$$\det(M_1) \left(M_1^{\hat{q}^t}\right)^* Z_1 = [\det(M_1)]^{q^t} (M_1^T)^* Z_2^T. \tag{32}$$

However, (32) is of degree 3 in plaintext variables. Hence, they can not help to do plaintext variables elimination on public key from these equations.

Having (31), we can represent s variables of $u_1, \cdots, u_{8r}$ by linear combinations of other $8r - s$. Our experiments show $s = 3r$. However, when we substitute s variables by their expression on other $8r - s$, we find other $4r$ FOLEs by experiments and we can eliminate $3r$ variables on public key furthermore. For the reminder equations with $2r$ variables, we can solve it directly by Gröbner basis algorithm.

We use parameters $r = 10$, $K = \mathbb{F}_{2^8}$ for experiment, it takes 918.783 seconds to derive the first $4r$ FLOEs and 1021.183 seconds for second $4r$ FLOEs. In the last step, we recover corresponding plaintext for a given ciphertext using Gröbner basis algorithm in 2.621 seconds.

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

6 Conclusion

In this paper, we give a new cryptanalysis on the two improved MFE schemes, Quartic-1 and Quartic-2, by utilizing quadratization equations which are quadratic in plaintext variables. For a given ciphertext, cracking down Quartic-1 with the same parameter as in Quartic-2 needs 2^{40} times Gröbner basis computations (about 1.328 seconds each time), while the Quatic-2 instance can be broken by quadratization equations in 3110.734 seconds. They both have weak points in their central map design. We also use the first order Linearization attack method to break another improved MFE scheme proposed in [WZY07]. Our analysis on the two quartic schemes is an example that non-linearization equations in plaintext variables like quadratization equations can be used efficiently in the cryptanalysis of multivariate cryptography.

Acknowledgement

This work is supported by the National Natural Science Foundation of China under Grant Numbers 60773134, 60973131 and 10990011, the National High Technology Research and Development (863) Program of China under Grant No. 2006AA01Z416, and the National Basic Research (973) Program of China under Grant No. 2007CB311201. The first two authors also thank a partial support from NSF and Taft Foundation.

References

[DH76] Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Transactions on Information Theory 22, 644–654 (1976)

[DGS06] Ding, J., Gower, J., Schmidt, D.: Multivariate Public-Key Cryptosystems. In: Advances in Information Security. Springer, Heidelberg (2006) ISBN 0-387-32229-9

[DHN07] Ding, J., Hu, L., Nie, X., Li, J., Wagner, J.: High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 233–248. Springer, Heidelberg (2007)

[Fag99] Faugère, J.: A New Efficient Algorithm for Computing Gröbner Bases (F4). Journal of Applied and Pure Algebra 139, 61–88 (1999)

[Pat95] Patarin, J.: Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995)

[Sho97] Shor, P.: Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing 26, 1484–1509 (1997)

[Wan07] Wang, Z.: An Improved Medium-Field Equation (MFE) Multivariate Public Key Encryption Scheme. In: IIH-MISP (2007), http://bit.kuas.edu.tw/ iihmsp07/accepted_list_general_session.html

[WFW09] Wang, X., Feng, F., Wang, X., Wang, Q.: A More Secure MFE Multivariate Public Key Encryption Scheme. International Journal of Computer Science and Applications 6(3), 1–9 (2009), http://www.tmrfindia.org/ijcsa/v6i31.pdf

[WYH06] Wang, L., Yang, B., Hu, Y., Lai, F.: A Medium-Field Multivariate Public Key Encryption Scheme. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 132–149. Springer, Heidelberg (2006)

[WZY07] Wang, Z., Zheng, S., Yang, Y., et al.: Improved Medium- Field Multivariate Public Key Encryption. Journal of University of Electonic Science an Technology of China 36(6), 1152–1154 (2007) (in Chinese)