Cubic Medium Field Equation Public Key Cryptosystem

Gang Lu[1], Linyuan Xue[1], Xuyun Nie[1,2,3], Zhiguang Qin[1,3], and Bo Liu[1]
(Corresponding author: Xuyun Nie)

School of Information and Software Engineering, University of Electronic Science and Technology of China[1]
4 Jianshe North Rd 2nd Section, Chenghua Qu, Chengdu 610054, China
(Email: xynie@uestc.edu.cn)
State Key Laboratory of Information Security, Institute of Information Engineering, Beijing 100093, China[2]
Network and Data Security Key Laboratory of Sichuan Province, Chengdu 610054, China[3]

(Received Dec. 14, 2016; revised and accepted Apr. 11 & May 2, 2017)

Abstract

Medium Field Equation (MFE) multivariate public key cryptosystems were broken by High Order Linearization Equation (HOLE) attack. In order to avoid HOLE attack, we proposed an improvement of MFE, Cubic MFE public key encryption scheme. In our construction, multiplications of three second order matrices were used to get a set of cubic polynomials in the central map. Through theoretical analysis and computer experiments, the Cubic MFE is shown to be secure against HOLE attack and other existing attacks.

Keywords: Cubic Polynomial; High Order Linearization Equation; Medium Field Equation; Multivariate Public Key Cryptosystem

1 Introduction

In 1994, Peter Shor [18] showed that some number theoretic hard problems such as Integer Factorization and Discrete Log Problem can be solved in polynomial time on quantum computer. Once the quantum computer is practical, cryptographic algorithms based on the hard problems above will be no longer secure.

Multivariate Public Key Cryptography (MPKC) could be seen as one of promising candidates to resist quantum algorithm attack [17]. The security of the MPKC relies on the difficulty of solving a system of nonlinear multivariate polynomial equations on a finite field, which is an NP-hard problem in worst case. In general, the public key of MPKC is composed of three maps, two affine maps and a map called central map which is the key point of designing an MPKC.

In the past few decades, a lot of multivariate cryptosystems have been proposed, but many of them were broken. $C^\star$ [10] is considered as the first MPKC, which was broken by Patarin[15] with linearization equation attack. Then, Patarin extended the idea of $C^\star$ and proposed Hidden Field Equation (HFE) scheme [16]. Ding *et al.* [6] showed that inverting HFE is quasi-polynomial if the size of the field and the degree of the HFE polynomials are fixed. After that, many MPKC encryption schemes have been proposed, such as TTM [11], MFE [21], Square [4] and ABC [19]. Most instances of TTM were broken because there are some linearization equations satisfied by their public key. Square and ABC were broken by differential attack [2, 12] . Cubic ABC [8] then was proposed to resist differential attack. This scheme is still secure by now.

Medium Field Equation (MFE) [21] was proposed by Wang *et al.* in 2006. The inventors of MFE used products of second order matrices to derive quadratic polynomials in its central map. It can be avoid the Paratin relations or linearization equations. But the original MFE was broken by High Order Linearization Equation (HOLE) attack [7] in 2007. In order to resist existing attack, many modifications of MFE were proposed [9, 20, 22] etc. But all of them are insecure [3, 14, 23]. Nie *et al.* [13] pointed out that it is impossible to derive secure MFE by changing the form of second order matrices with their transpose and adjoint.

Although MFE is insecure, the idea of its construction is elegant. And MFE is very efficient. We want to modify its central map to propose a security MFE scheme.

In this paper, we propose a Cubic MFE encryption scheme to avoid HOLE attack. Firstly, we introduce an extra second order matrix in the central map and use products of three second order matrices to get cubic polynomials; secondly, we add three equations in the central map to ensure the successful decryption. Through theoretical analysis and computer experiments, we show that our Cubic MFE scheme can be secure against HOLE attack. Furthermore, the Cubic MFE can resist direct attacks for some chosen parameters. At last, we present efficiency comparison with Cubic ABC and implementation for practical parameters.

This paper is organized as follows. We briefly introduce the original MFE scheme and its cryptanalysis in Section 2. In Section 3, we present our Cubic MFE. And security analysis will be presented in Section 4. In Section 5, we give practical parameters and efficiency comparison. Finally, we conclude this paper in Section 6.

2 Preliminaries

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

2.1 MFE Public Key Cryptosystem

We use the same notations as in [21]. 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 $\pi : \mathbb{L} \to \mathbb{K}^r$. 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 $\pi_1 : \mathbb{L}^{12} \to \mathbb{K}^{12r}$ and $\pi_2 : \mathbb{L}^{15} \to \mathbb{K}^{15r}$.

In MFE, its encryption map $F : \mathbb{K}^{12r} \to \mathbb{K}^{15r}$ is composed of three maps ϕ_1, ϕ_2, ϕ_3, that is $(y_1, \cdots, y_{15r}) = F(x_1, \cdots, x_{12r}) = \phi_3 \circ \phi_2 \circ \phi_1(x_1, \cdots, x_{12r})$, where $y_1, \cdots, y_{15r}$ are ciphertext variables and $x_1, \cdots, x_{12r}$ are plaintext variables. ϕ_1 and ϕ_3 are invertible affine maps and ϕ_2 is called central map, which is equal to $\pi_2 \circ \bar{\phi}_2 \circ \pi_1^{-1}$.

ϕ_1 and ϕ_3 are taken as the private keys, 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.

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; \\ Y_2 = X_2 + X_9X_{12} + X_{10}X_{11} + Q_2; \\ Y_3 = X_3 + X_1X_4 + X_2X_3 + Q_3; \\ Y_4 = X_1X_5 + X_2X_7; \\ Y_5 = X_1X_6 + X_2X_8; \\ Y_6 = X_3X_5 + X_4X_7; \\ Y_7 = X_3X_6 + X_4X_8; \\ Y_8 = X_1X_9 + X_2X_{11}; \\ Y_9 = X_1X_{10} + X_2X_{12}; \\ Y_{10} = X_3X_9 + X_4X_{11}; \\ Y_{11} = X_3X_{10} + X_4X_{12}; \\ Y_{12} = X_5X_9 + X_7X_{11}; \\ Y_{13} = X_5X_{10} + X_7X_{12}; \\ Y_{14} = X_6X_9 + X_8X_{11}; \\ Y_{15} = X_6X_{10} + X_8X_{12}. \end{cases} \tag{1}$$

where Q_1, Q_2, and Q_3 form a triple tuple (Q_1, Q_2, Q_3) which is a triangular map from $\mathbb{K}^{3r}$ to itself, more detail please see [21].

The map $\bar{\phi}_2$ can be written by matrix form as follows.

Let $X_1, \cdots, X_{12}$ be the entries of three 2×2 matrices M_1, M_2, M_3, namely,

$$\begin{aligned} M_1 &= \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, \\ M_3 &= \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix}. \end{aligned} \tag{2}$$

Then $Y_4, \cdots, Y_{15}$ will be the entries in three 2×2 matrices Z_1, Z_2, Z_3, namely,

$$\begin{aligned} Z_1 = M_1M_2 &= \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, \\ Z_2 = M_1M_3 &= \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, \\ Z_3 = M_2^TM_3 &= \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}. \end{aligned} \tag{3}$$

Then

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

Using the determinants of Z_1, Z_2, Z_3, the determinants of M_1, M_2, M_3 can be found. And then one can get the inverse of the central map ϕ_2. More details of decryption are presented in [21].

2.2 High Order Linearization Equation Attack on MFE

The equation of following form is called High Order Linearization Equation (HOLE).

$$\begin{aligned} &\sum_{i=1,j=1}^{n,t} a_{ij}x_if_j(y_1, y_2, \cdots, y_m) \\ &+ \sum_{j=1}^{l} c_jg_j(y_1, y_2, \cdots, y_m) + d = 0. \end{aligned} \tag{4}$$

where f_j, $1 \leq j \leq t$, g_j, $1 \leq j \leq l$, are some polynomial functions on ciphertext variables $y_1, y_2, \cdots, y_m$. The highest degree of ciphertext variables y_j is called the order of the Lineraization Equation.

Note that, given a valid ciphertext $y' = (y'_1, y'_2, \cdots, y'_m)$ and substituted it into equation (4), it will become a linear equation on plaintext variables $x_1, \cdots, x_n$.

Once some HOLEs are satisfied by an MPKC, these equations can be used to break the MPKC. The MI scheme was broken by the First Order Linearization Equation (FOLE) method [15]. And the original MEF was broken by the Second Order Linearization Equation (SOLE) method [7].

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

But many SOLEs were found in the MFE scheme. Denote by M^* the adjoint matrix of a second order matrix M. From

$$Z_1 = M_1M_2, Z_2 = M_1M_3,$$

we have

$$M_3M_3^*M_1^*M_1M_2 = M_3Z_2^*Z_1 = \det(Z_2)M_2. \tag{5}$$

Expanding (4), we get four equations of the following form

$$\sum a'_{ijk}X_iY_jY_k = 0. \tag{6}$$

In [7], 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 (8), we get $24r$ equations of the following form

$$\begin{aligned} &\sum_i x_i \left(\sum_{j \le k} a_{ijk} y_j y_k + \sum_j b_{ij} y_j + c_i \right) \\ &+ \sum_{j \le k} d_{jk} y_j y_k + \sum_j e_j y_j + f = 0. \end{aligned} \tag{7}$$

These equations are SOLEs.

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

3 Cubic MFE

In this section, we will present our Cubic MFE encryption scheme. We use the similar notations as in Section 2.1. The difference is that two $\mathbb{K}$-linear isomorphisms are $\pi_1 : \mathbb{L}^{16} \to \mathbb{K}^{16r}$ and $\pi_2 : \mathbb{L}^{22} \to \mathbb{K}^{22r}$.

3.1 Construction of Central Map

The key point of an MPKC is its central map. Let $X_1, \cdots, X_{16} = \pi_1^{-1} \circ \phi_1(x_1, \cdots, x_{16r})$, and $Y_1, \cdots, Y_{22} = \pi_2^{-1} \circ \phi_3^{-1}(y_1, \cdots, y_{22r})$, the new cencral map $\bar{\phi}_2 : \mathbb{L}^{16} \to \mathbb{L}^{22}$ is defined as follows.

$$\left\{ \begin{array}{l} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; \\ Y_2 = X_2 + X_9X_{12} + X_{10}X_{11} + Q_2; \\ Y_3 = X_3 + X_1X_4 + X_2X_3 + Q_3; \\ Y_4 = X_5 + f_5(X_1, X_2, X_3, X_4); \\ Y_5 = X_6 + f_6(X_1, X_2, X_3, X_4, X_5); \\ Y_6 = X_7 + f_7(X_1, X_2, X_3, X_4, X_5, X_6); \\ Y_7 = X_1X_5X_{13} + X_2X_7X_{13} + X_1X_6X_{15} + X_2X_8X_{15}; \\ Y_8 = X_1X_5X_{14} + X_2X_7X_{14} + X_1X_6X_{16} + X_2X_8X_{16}; \\ Y_9 = X_3X_5X_{13} + X_4X_7X_{13} + X_3X_6X_{15} + X_4X_8X_{15}; \\ Y_{10} = X_3X_5X_{14} + X_4X_7X_{14} + X_3X_6X_{16} + X_4X_8X_{16}; \\ Y_{11} = X_1X_9X_{13} + X_2X_{11}X_{13} + X_1X_{10}X_{15} + X_2X_{12}X_{15}; \\ Y_{12} = X_1X_9X_{14} + X_2X_{11}X_{14} + X_1X_{10}X_{16} + X_2X_{12}X_{16}; \\ Y_{13} = X_3X_9X_{13} + X_4X_{11}X_{13} + X_3X_{10}X_{15} + X_4X_{12}X_{15}; \\ Y_{14} = X_3X_9X_{14} + X_4X_{11}X_{14} + X_3X_{10}X_{16} + X_4X_{12}X_{16}; \\ Y_{15} = X_5X_9X_{13} + X_7X_{11}X_{13} + X_5X_{10}X_{14} + X_7X_{12}X_{14}; \\ Y_{16} = X_5X_9X_{15} + X_7X_{11}X_{15} + X_5X_{10}X_{16} + X_7X_{12}X_{16}; \\ Y_{17} = X_6X_9X_{13} + X_8X_{11}X_{13} + X_6X_{10}X_{14} + X_8X_{12}X_{14}; \\ Y_{18} = X_6X_9X_{15} + X_8X_{11}X_{15} + X_6X_{10}X_{16} + X_8X_{12}X_{16}; \\ Y_{19} = X_1X_{13} + X_2X_{15}; \\ Y_{20} = X_1X_{14} + X_2X_{16}; \\ Y_{21} = X_3X_{13} + X_4X_{15}; \\ Y_{22} = X_3X_{14} + X_4X_{16}. \end{array} \right. \tag{8}$$

where Q_1, Q_2, and Q_3 form a triple tuple (Q_1, Q_2, Q_3) which is a triangular map from $\mathbb{K}^{3r}$ to itself, and f_5, f_6, f_7 are randomly chosen quadratic polynomials.

The main idea of our improvement is that we use products of three second order matrices in MFE to avoid the HOLEs attack. To do this, it is necessary to introduce a new plaintext variables matrix, M_4 in the matrix form of the central map $\bar{\phi}_2$.

Then the matrix form of the central map $\bar{\phi}_2$ is changed into

$$Z_1 = M_1M_2M_4, Z_2 = M_1M_3M_4, Z_3 = M_2^TM_3M_4^T.$$

In order to decrypt successfully, we need introduce $Z_4 = M_1M_4$ and Y_4, Y_5, Y_6 in the central map. Let

$$M_4 = \begin{pmatrix} X_{13} & X_{14} \\ X_{15} & X_{16} \end{pmatrix}. \tag{9}$$

Then the matrix form is changed into

$$\begin{aligned} Z_1 &= M_1M_2M_4 = \begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix}, \\ Z_2 &= M_1M_3M_4 = \begin{pmatrix} Y_{11} & Y_{12} \\ Y_{13} & Y_{14} \end{pmatrix}, \\ Z_3 &= M_2^TM_3M_4^T = \begin{pmatrix} Y_{15} & Y_{16} \\ Y_{17} & Y_{18} \end{pmatrix}, \\ Z_4 &= M_1M_4 = \begin{pmatrix} Y_{19} & Y_{20} \\ Y_{21} & Y_{22} \end{pmatrix}. \end{aligned} \tag{10}$$

Given the values of $Y_1, \cdots, Y_{22}$, the map $\bar{\phi}_2$ can be inverted as follows.

- Firstly, we calculate $\det(Z_1)$, $\det(Z_2)$, $\det(Z_3)$, $\det(Z_4)$. And then we calculate $\det(M_2)$ and $\det(M_3)$ from

  $$\det(Z_1) = \det(M_1)\det(M_2)\det(M_4) = \det(M_2)\det(Z_4),$$

  and

  $$\det(Z_2) = \det(M_1)\det(M_3)\det(M_4) = \det(M_3)\det(Z_4),$$

  respectively.

- Substitute $\det(M_2)$ and $\det(M_3)$ into

  $$\begin{aligned} \det(Z_3) &= \det(M_2^T)\det(M_3)\det(M_4^T) \\ &= \det(M_2)\det(M_3)\det(M_4), \end{aligned}$$

  we can get $\det(M_4)$. Substitute $\det(M_4)$ into $\det(Z_4) = \det(M_1)\det(M_4)$, we can derive $\det(M_1)$.

- Substitute $\det(M_1)$, $\det(M_2)$ and $\det(M_3)$ into

  $$\left\{ \begin{array}{l} Y_1 = X_1 + \det(M_2) + Q_1; \\ Y_2 = X_2 + \det(M_3) + Q_2; \\ Y_3 = X_3 + \det(M_1) + Q_3; \end{array} \right. \tag{11}$$

  We can calculate X_1, X_2, X_3 in turn. And substitute them into $\det(M_1) = X_1X_4 + X_2X_3$, we can get the value of X_4.

- According to the expression of the map $\bar{\phi}_2$, we can calculate X_5, X_6, X_7 in turn. And substitute them into $\det(M_2) = X_5X_8 + X_6X_7$, we can get the value of X_8.

- At last, we can calculate $X_{13}, X_{14}, X_{15}, X_{16}$ and $X_9, X_{10}, X_{11}, X_{12}$ in turn by the expression of the map $\bar{\phi}_2$.

The security analysis can be seen in Section 4.

3.2 Encryption Scheme

Key Generation. Randomly generating two affine maps ϕ_1 and ϕ_3 on $\mathbb{K}^{16r}$ and $\mathbb{K}^{22r}$, respectively. Then calculate the expression of $F : \mathbb{K}^{16r} \to \mathbb{K}^{22r}$, namely,

$$\begin{aligned}(y_1, \cdots, y_{22r}) &= F(x_1, \cdots, x_{16r}) \\ &= \phi_3 \circ \phi_2 \circ \phi_1(x_1, \cdots, x_{16r}).\end{aligned}$$

The private keys are ϕ_1 and ϕ_3.

The public key is the expression of $F : \mathbb{K}^{16r} \to \mathbb{K}^{22r}$, a set of cubic polynomials. The expression of the central map can be public.

Encryption. Given a plaintext $(x'_1, \cdots, x'_{16r})$, the ciphertext $(y'_1, \cdots, y'_{22r})$ is calculated by public key, namely,

$$(y'_1, \cdots, y'_{22r}) = F(x'_1, \cdots, x'_{16r}).$$

Decryption. Given a valid ciphertext $(y'_1, \cdots, y'_{22r})$, the decryption of Cubic MFE is to calculate the inverses of ϕ_3, ϕ_2 and ϕ_1 in turn, namely,

$$(x'_1, \cdots, x'_{16r}) = \phi_1^{-1} \circ \phi_2^{-1} \circ \phi_3^{-1}(y'_1, \cdots, y'_{22r}).$$

4 Security Analysis

In this section, we consider Cubic MFE against several existing attacks, such as linearization equations method and algebraic attacks etc.

Given a public key of an MPKC and a valid ciphertext $y = (y'_1, \cdots, y'_m)$, to break it is equivalent to solve the following system

$$\left\{\begin{array}{ll} F_1(x_1, \cdots, x_n) & = y'_1; \\ \cdots & \\ F_m(x_1, \cdots, x_n) & = y'_m. \end{array}\right. \qquad (12)$$

4.1 Linearization Equations Attack

Through theoretical analysis, we did not find any linearization equation satisfied by our Cubic MFE. For example, similar to SOLE attack on MFE, from $Z_1 = M_1M_2M_4$, $Z_4 = M_1M_4$, we can get

$$M_4M_4^*M_1^*M_1M_2M_4 = M_4Z_4^*Z_1 = \det(Z_4)M_2M_4.$$

Expanding it, we get four equations of the form

$$\sum a_{ijkl}X_iX_jY_kY_l + \sum b_{ijk}X_iY_jY_k = 0. \qquad (13)$$

Substituting $(X_1, \cdots, X_{16}) = \pi_1^{-1} \circ \phi_1(x_1, \cdots, x_{16r})$ and $(Y_1, \cdots, Y_{22}) = \pi_2^{-1} \circ \phi_3^{-1}(y_1, \cdots, y_{15r})$ into Equation (13), we get $24r$ equations of the form

$$\begin{aligned}&\sum_{i\le j} x_ix_j \left(\sum_{k\le l} a_{ijkl}y_ky_l + \sum_k b_{ijk}y_k + c_{ij}\right) \\ &+ \sum_{k\le l} d_{kl}y_ky_l + \sum_k e_ky_k + f = 0.\end{aligned} \qquad (14)$$

From these equations, we can not derive any Linearization Equation.

Furthermore, we did many experiments to verify there is no FOLE and SOLE satisfied by Cubic MFE. This is done as follows. We selected sufficient plaintext/ciphertext pairs and plugged them into the SOLE or FOLE to get a linear system on coefficients of HOLE or FOLE, and then solve it. The experimental results showed that the solutions are all zero, hence no HOLE or FOLE exists.

4.2 Algebraic Attacks

In a direct attack, the attacker wants to recover the plaintext by solving the system (12). The most efficient algorithm for direct attack is Gröbner Basis method such as F_4 and F_5.

According to [5], If $\mathbb{K}$ is big, the complexity of Gröbner Basis method has been proved to be $\mathcal{O}(2^{3n})$ and $\mathcal{O}(2^{2.7n})$ in practice.

In Cubic MFE, if $\mathbb{K} = GF(2^8)$ or $GF(2^{16})$, $r = 3$, $n = 48$, the complexity of Gröbner Basis method is about 2^{129}.

An improvement of Gröbner Basis method, F_5 can be seen in [1]. The complexity of algorithm F_5 relies on the degree of regularity d_{reg} in the algorithm.

Proposition 1. *([1], Proposition 2.2) The complexity of computing a Gröbner basis of a zero-dimensional system of m equations in n variables with F_5 is:*

$$\mathcal{O}\left(m \cdot \left(\begin{array}{c} n + d_{reg} - 1 \\ d_{reg} \end{array}\right)^{\omega}\right),$$

where d_{reg} is the degree of regularity of the system and $2 < \omega < 3$ is the linear algebra constant.

Unfortunately, we can not determine the degree of regularity in our experiments by Magma. When degree increase to 5, the programs would be out of memory. We estimate the degree of regularity is equal to 6. Hence, the complexity of F_5 on our scheme would be about 2^{83} when $r = 3$.

In summary, the Cubic MFE can resist the direct attack with parameters, $\mathbb{K} = GF(2^8)$ or $GF(2^{16})$, $r = 3$, $n = 48$.

5 Parameter Proposals

Based on the security analysis of Cubic MFE in last section, we recommend $\mathbb{K} = GF(2^8)$ and $GF(2^{16})$, $r = 3$, then $n = 48$ and $m = 66$ for our Cubic MFE.

In Table 1, we present the keys sizes of our Cubic MFE with the paraments recommended and compare them with Cubic Simple Matrix Encryption (CSME) scheme.

From Table 1, we find that the key sizes of our CMFEs are smaller than CSMEs.

The performance of CMFEs ($r = 3$) can be seen in Table 2. We did our experiments with Magma on a normal

Table 1: Parameters and key sizes of CMFEs and comparison with CSMEs

scheme	parameters (k, n, m)	input size(bit)	output size(bit)	public key size(KB)	private key size(KB)
CMFE	$(GF(2^8), 48, 66)$	384	528	1342	6.62
CSME	$(GF(2^8), 49, 98)$	392	784	2115	72.7
CMFE	$(GF(2^{16}), 48, 66)$	768	1056	2684	13.23
CSME	$(GF(2^{16}), 49, 98)$	784	1568	4230	145.4

Table 2: The performance of CMFEs

Field	Encryption Time (ms)	Decryption Time (ms)
$GF(2^8)$	316.72	3.28
$GF(2^{16})$	344.38	3.59

PC with Intel Core i5 CPU@2.53GHz, 3 GB of memory. For each finite field, we randomly chose 100 plaintexts and performed encryptions on them and corresponding decryptions. We calculated the average time in milliseconds of encryptions and decryptions.

6 Conclusion

In this paper, we proposed the Cubic MFE encryption scheme. In our construction, we use multiplications of three second order matrices to get a set of cubic polynomials in the central map. The Cubic MFE is secure against the HOLE attacks and the direct attacks with proper parameters.

The cubic multivariate public key cryptosystems have bigger key sizes than the quadratic multivariate public key cryptosystems. But they can avoided some attacks occurred on the quadratic ones, such as HOLEs attack etc. The security of cubic schemes should be further studied in the future.

Acknowledgments

This work was supported by the National Key Basic Research Program of China under grant 2013CB834203, Major International (Regional) Joint Research Project of China National Science Foundation under grant No.61520106007, The science and technology foundation of Sichuan Province under grant No.2016GZ0065 and the Fundamental Research Funds for the Central Universities under grant No.ZYGX2015J072.

References

[1] L. Bettale, J. C. Faugère, and L. Perret, "Hybrid approach for solving multivariate systems over finite fields," *Journal of Mathematical Cryptology*, vol. 3, no. 3, pp. 177–197, 2009.

[2] O. Billet and M.Matsui, "Cryptanalysis of the square cryptosystems," in *Advances in Cryptology (ASIACRYPT'09)*, pp. 451–468, 2009.

[3] 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, May 2010.

[4] C. Clough, J. Baena, J. T. Ding, B. Y. Yang, and M. S. Chen, "Square, a new multivariate encryption scheme," in *Topics in Cryptology (CT-RSA'09)*, pp. 252–264, 2009.

[5] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," in *Advances in Cryptology (EUROCRYPT'00)*, pp. 392–407, 2000.

[6] J. T. Ding and T. J. Hodges, "Inverting HFE systems is quasi-polynomial for all fields," in *Advancees in Cryptology (CRYPTO'11)*, pp. 724–742, 2011.

[7] 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, Apr. 2007.

[8] J. T. Ding, A. Petzoldt, and L. C. Wang, "The cubic simple matrix encryption scheme," in *6th International Workshop on Post-Quantum Cryptography (PQCrypto'14)*, pp. 76–87, 2014.

[9] 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, Jan. 2009.

[10] T. Matsumoto and H. Imai, "Quadratic polynomial-tuples for effcient signature verification and message-encryption," in *Advances in Cryptology (Eurocrypt'88)*, pp. 419–453, 1988.

[11] T. Moh, "A public key system with signature and master key functions," *Communication in Algebra*, vol. 18, no. 1, pp. 2207–2222, 1999.

[12] D. Moody, R. Perlner, and D. Smith-Tone, "An asymptotically optimal structural attack on the ABC multivariate encryption scheme," in *6th International Workshop on Post-Quantum Cryptography (PQCrypto'14)*, pp. 180–196, 2014.

[13] X. Y. Nie, C. Y. Hou, Z. H. Xu, and G. Lu, "Analysis of second order matrices construction in MFE public key cryptosystem," *International Journal of Network Security*, vol. 18, no. 1, pp. 158–164, 2016.

[14] 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, Dec. 2011.

[15] J. Patarin, "Cryptoanalysis of the matsumoto and imai public key scheme of eurocrypt'88," in *Advancees in Cryptology (CRYPTO'95)*, pp. 248–261, 1995.

[16] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms," in *Advances in Cryptology (EUROCRYPT'96)*, pp. 33–48, 1996.

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

[18] 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.

[19] C. D. Tao, H. Xiang, A. Petzoldt, and J.T. Ding, "Simple matrix c a multivariate public key cryptosystem (MPKC) for encryption," *Finite Fields and Their Applications*, vol. 35, no. C, pp. 352–368, 2015.

[20] 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, Dec. 2009.

[21] 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, Feb. 2006.

[22] 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.

[23] 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.

Biography

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.

Linyuan Xue is pursuing his Master degree from the School of Information and Software Engineering, University of Electronic Science and Technology of China. His research interests include multivariate public key cryptosystems and network security.

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.

Zhiguang Qin is a professor in the School of Information and Software Engineering, UESTC. He received his PH.D. degree from UESTC in 1996. His research interests include: information security and computer network.

Bo Liu received his Master degree from the School of Information and Software Engineering, University of Electronic Science and Technology of China in 2016. His research interests include multivariate public key cryptosystems and network security.