http://ansinet.com/itj

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information

308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (1): 51-59, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.51.59


# Improvements on a Medium-field Multivariate Public-key and its Application in Block Cipher

Ning Huang
Center of Modern Educational Technology, Gannan Normal University,
341000, Ganzhou, China

**Abstract:** We analysed and solved possible singularity for an improved MFE multivariate public key (Medium-field Multivariate Public Key Encryption) and studied the use of it in a block cipher. We used our new MFE multivariate public key cryptosystem to design an algorithm of block cipher, in which a given plaintext resulted in multi-ciphertext. The attack will be difficult because the ciphertext is changeable for a given plaintext. The ability of the cipher to withstand algebraic attacks is enhanced. Experimental results and analysis show that the scheme is viable and secure.

**Key words:** Block cipher, finite field , matrix, multivariate, polynomial, public key

## INTRODUCTION

Modern public key cryptography began with the public key cryptography based on the difficulty of the solution of discrete logarithm created by Diffie and Hellman (1976). From 1978 to 1982, Rivest, Shamir and Adelman made RSA public key cryptographic algorithm (Rivest *et al*., 1978, 1982) based on the difficulty of factoring large numbers which has been widely used ever since. Nevertheless, such public key cryptosystems based on arithmetic have been potentially threatened since 1999 because Peter Shor developed algorithms to crack such arithmetic based ciphers in polynomial time for a quantum computer (Shor, 1994). Public key cryptography based on arithmetic will be unsafe in the era of quantum computers. We need to study new approaches to solve this problem. Multivariate public key cryptosystem is a research direction (Ding and Schmidt, 2006), in which finite field multivariable (usually quadratic or higher ordered) set of polynomials are used as a public key.

The history of Multivariate public key cryptosystem can be roughly traced back as early as 1986. Fell and Diffie (1986) proposed an invertible linear mapping within a simple triangle synthesis scheme (Fell and Diffie, 1986). Although they believed the program safe, Courtois and Goubin broke it with rank attack (Goubin and Courtois, 1976) . In 1988, Matsumoto and Imai designed multivariate quadratic polynomial scheme implemented via a Frobenius mapping (Ding and Schmidt, 2006). Although this program was later broken by Patarin (1995), this work led multivariate cryptography in many studies (Ding and Schmidt, 2006). In 1995 Courtois proposed a Hidden Field Equation method (HFE) (Courtois, 2001), in 1997 and 1999, proposed Oil and Vinegar (Patarin, 1997) and Unbalanced Oil and Vinegar (Kipnis *et al*., 1999) which are suitable for the digital signature. Nevertheless Courtois (2001) and Faugere and Joux (2003) broke HFE respectively in 2001 and 2003 with the method of minimum rank (Goubin and Courtois, 1976; Faugere and Joux, 2003). Wang *et al.* (2006) proposed Medium-Field Multivariate Public Key Encryption Scheme (MFE for short) (Wang *et al*., 2006) which belonged to a multivariate quadratic polynomial scheme. Wang *et al.* (2009) analysed and developed Wang *et al.* (2006) programs to make the cryptosystem safer. Our main contribution in this study is taking Wang *et al.* (2009) scheme as a basis to improve and design a block cipher. The security of a block cipher depends on the quality of the encryption and decryption algorithms. The developments of Multivariate Public Key Cryptosystem inspired us to apply it in block cipher.

## ANALYSIS OF THE MFE SCHEMES

Let us begin with Wang *et al.* (2006) works.

Let K be a finite field of characteristic 2, called the base field, L be K's r-degree extension, called the Medium-field. L is also of character 2 and has the feature of a+a = 0, a-b = a+b.

Define an isomorphism between L and $K^r$ as follows.

Take a base of L over K $\theta_1, \theta_2, \ldots, \theta_r$, so that:

$$\pi(a_1\theta_1 + a_2\theta_2 + \cdots + a_r\theta_r) = (a_1, a_2, \cdots, a_r), \forall a_1, a_2, \cdots, a_r \in \mathbb{K}$$

extend $\pi$ to $\pi 1: L^{12} \to K^{12r}$, $\pi^3: L^{15} \to K^{15r}$. In L, take 12 variables Xi, turn into 2×2 matrices as follows:

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix} \quad (1)$$

**Wang *et al.* (2006) original MFE scheme:** In Wang *et al.* (2006) original MFE scheme.

In L, 15 variables $Y_j$, turn into 2×2 matrices as follows. Let:

$$Z_1 = M_1M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, Z_2 = M_1M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, \quad Z_3 = M_2^TM_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix} \quad (2)$$

Define a mapping $\phi_2$: $L^{12} \to L^{15}$, $\phi_2$ $(X_1, X_2,..., X_{12}) = (X_1, X_2, ,..., X_{15})$ where $Y_j$ is represented as a quadratic function of $X_1$:

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1 \\ Y_2 = X_2 + X_9X_{12} + X_{10}X_{11} + Q_2 \\ Y_3 = X_3 + X_1X_4 + X_2X_3 + Q_3 \\ Y_4 = X_1X_5 + X_2X_7, Y_5 = X_1X_6 + X_2X_8 \\ Y_6 = X_3X_5 + X_4X_7, Y_7 = X_3X_6 + X_4X_8 \\ Y_8 = X_1X_9 + X_2X_{11}, Y_9 = X_1X_{10} + X_2X_{12} \\ Y_{10} = X_3X_9 + X_4X_{11}, Y_{11} = X_3X_{10} + X_4X_{12} \\ Y_{12} = X_5X_9 + X_7X_{11}, Y_{13} = X_5X_{10} + X_7X_{12} \\ Y_{14} = X_6X_9 + X_8X_{11}, Y_{15} = X_6X_{10} + X_8X_{12} \end{cases} \quad (3)$$

$\phi_2$ is called central mapping, where $(Q_1, Q_2, Q_3) \in K^{3r}$, is optional parameters, agreed by the two sides of the encryption and decryption. Obviously, Eq. 3 includes 1.

Define an affine mapping:

$$\phi_1: U \to X = A_1U + C_1$$

where, $A_1$ is an invertible matrix over $K^{12r}$, $C_1 \in K^{15r}$.

Define an affine mapping:

$$\phi_3: Y \to V = A_3Y + C_3$$

where, $A_3$ is an invertible matrix over $K^{15r}$, $C_5 \in K^{15r}$.

The public key is composed of 3 mappings. $\phi = \phi_1 \circ \phi_2 \circ \phi_3$.$15_r$ quadratic polynomials are defined as a public key by the following equation:

$$(h_1(u_1,..., u_{12r}),..., h_{15}(u_1,..., u_{12r})) = \phi_3 \circ \pi_3 \circ \phi_2 \circ \phi^{-1}{}_1 \circ \phi_3 \, (u_1,...u_{12r})$$

**Designing ideas:** $\phi_1$, $\phi_2$, $\phi_3$ are easy to be inverted respectively, while the composed $\phi$ is difficult to be inverted, so that the central mapping $\phi_2$ is "hidden" in $\phi$ by two affine mappings $\phi_1$ and $\phi_2$.

Given a set of plaintext $(m_1,..., m_{12r})$ the encryption is to substitute into the polynomials to obtain the ciphertext $(c_1,..., c_{15r})$ .

The decryption is described as follows.

For a group of ciphertexts, compute $\phi^{-1} \circ \pi_1 \circ \phi_2{}^{-1} \circ \pi_3{}^{-1} \circ \phi_3{}^{-1}$ to obtain plaintext. The key issue is to compute $\phi_2{}^{-1}$. From the matrix definition of Eq. 2 ,we have:

$$\begin{cases} \det(Z_1) = \det(M_1)\det(M_2) = Y_4Y_7 + Y_5Y_6 \\ \det(Z_2) = \det(M_1)\det(M_3) = Y_8Y_{11} + Y_9Y_{10} \\ \det(Z_3) = \det(M_2)\det(M_3) = Y_{12}Y_{15} + Y_{13}Y_{14} \end{cases} \quad (4)$$

When det $(Z_1) \neq 0$ and det $(Z_2) \neq 0$ and det $(Z_3)$, we have:

$$\det(M_1) = \sqrt{\frac{\det(Z_1)\det(Z_2)}{\det(Z_3)}}, \det(M_2) = \sqrt{\frac{\det(Z_1)\det(Z_3)}{\det(Z_2)}}, \quad \det(M_3) = \sqrt{\frac{\det(Z_2)\det(Z_3)}{\det(Z_1)}} \quad (5)$$

From Eq. 3 we have:

$$\begin{cases} Y_1 = X_1 + \det(M_2) + Q_1 \\ Y_2 = X_2 + \det(M_3) + Q_2 \\ Y_3 = X_3 + \det(M_1) + Q_3 \end{cases} \quad (6)$$

It follows from Eq. 6 that in the field L of character 2:

$$\begin{cases} X_1 = Y_1 + \det(M_2) + Q_1, \\ X_2 = Y_2 + \det(M_3) + Q_2, \\ X_3 = Y_3 + \det(M_1) + Q_3; \end{cases} \quad (7)$$

When $X_1 \neq 0$, from $X_1X_4 + X_2X_3 = \det(M1)$, we have:

$$X_4 = X^{-1}{}_1(\det(M_1) + X_2X_3) \quad (8)$$

From Eq. 3 and 1, we can obtain $X_5,..., X_{12}$ successively. Nevertheless, this system has weaknesses and needs fixing (Wang *et al*., 2009).

**Wang *et al.* (2009) improved scheme:** Wang *et al.* (2009) proposed an improved scheme as follows.

K, L,. $\pi_1$, $\pi_2$, $\pi_3$, $\phi_1$, $\phi_3$ are the same as those in last subsection, redefine $\phi_2$, replace quadratic polynomials with four ordered ones.

In $\phi_2$, put 15 variables $Y_j$, turn into 2×2 matrices as follows:

$$Z_1 = X_2X_3M_1M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, Z_2 = X_1X_2M_1M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}, \quad (9)$$
$$Z_3 = X_1X_3M_2^TM_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}$$

Define a mapping $\phi_2$: $L^{12} \to L^{15}$, $\phi_2$ $(X_1, X_2, ..., X_{12}) = (Y_1, Y_2, ..., Y_{12})$, where $Y_j$ is denoted by four ordered functions of $X_i$:

$$\begin{cases} Y_1 = X_1 + X_3^2(X_5X_8 + X_6X_7) + Q_1 \\ Y_2 = X_2 + X_1^2(X_9X_{12} + X_{10}X_{11}) + Q_2 \\ Y_3 = X_3 + X_2^2(X_1X_4 + X_2X_3) + Q_3 \\ Y_4 = X_2X_3(X_1X_5 + X_2X_7), Y_5 = X_2X_3(X_1X_6 + X_2X_8) \\ Y_6 = X_2X_3X_3X_5 + X_4X_3), Y_7 = X_2X_3(X_3X_6 + X_4X_8) \\ Y_8 = X_1X_2(X_1X_9 + X_2X_{11}), Y_9 = X_1X_2(X_1X_{10} + X_2X_{12}) \\ Y_{10} = X_1X_2(X_3X_9 + X_4X_{11}), Y_{11} = X_1X_2(X_3X_{10} + X_4X_{12}) \\ Y_{12} = X_1X_3(X_5X_9 + X_7X_{11}), Y_{13} = X_1X_3(X_5X_{10} + X_7X_{12}) \\ Y_{14} = X_1X_3(X_6X_9 + X_8X_{11}), Y_{15} = X_1X_3(X_6X_{10} + X_8X_{12}) \end{cases} \quad (10)$$

Given a set of plaintext ($m_1$, ..., $m_{12r}$) the encryption is to substitute into the polynomials to obtain the ciphertext ($c_1$, ..., $c_{15r}$). The decryption is described as follows.

For a group of ciphertext, compute $\phi_1^{-1} \circ \pi_1 \circ \phi_2^{-1} \circ \pi_3^{-1} \circ \phi_3^{-1}$ to obtain plaintext. The key issue is to compute $\phi_2^{-1}$. From the matrix definition of (9), we have:

$$\begin{cases} \det(Z_1) = X_2^2X_3^2\det(M_1)\det(M_2) = Y_4Y_7 + Y_5Y_6, \\ \det(Z_2) = X_1^2X_2^2\det(M_1)\det(M_3) = Y_8Y_{11} + Y_9Y_{10}, \\ \det(Z_3) = X_1^2X_3^2\det(M_2)\det(M_3) = Y_{12}Y_{15} + Y_{13}Y_{14}; \end{cases} \quad (11)$$

When det $(Z_1) \neq 0$ and det $(Z_2)$ and det $(Z_3) \neq 0$, we have:

$$X_2^2\det(M_1) = \sqrt{\frac{\det(Z_1)\det(Z_2)}{\det(Z_3)}}$$

$$X_3^2\det(M_2) = \sqrt{\frac{\det(Z_1)\det(Z_3)}{\det(Z_2)}}$$

$$X_1^2\det(M_3) = \sqrt{\frac{\det(Z_2)\det(Z_3)}{\det(Z_1)}}$$

From line 1-3 of Eq. 10 we have:

$$\begin{cases} Y_1 = X_1 + X_1^2\det(M_2) + Q_1 \\ Y_2 = X_2 + X_2^2\det(M_3) + Q_2 \\ Y_3 = X_3 + X_3^2\det(M_1) + Q_3 \end{cases} \quad (12)$$

It follows from Eq. 1 that:

$$\begin{cases} X_1 = Y_1 + X_1^2\det(M_2) + Q_1 \\ X_2 = Y_2 + X_2^2\det(M_3) + Q_2 \\ X_3 = Y_3 + X_3^2\det(M_1) + Q_3 \end{cases} \quad (13)$$

When $X_1 \neq 0$ from $X_1X_4 + X_2X_3 = X_2^2$ det $(M_1)$, we have:

$$X_4 = X_1^{-1}(X_2^2\det(M_1) + X_2X_3) \quad (14)$$

Furthermore, when $X_2 \neq 0$, $X_3 \neq 0$, det $(M_1) \neq 0$, from Eq. 9 and 10, we have:

$$\begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix} = M_2 = X_2^{-1}X_3^{-1}M_1^{-1}Z_1 = \frac{1}{X_2X_3(X_1X_4 + X_2X_3)} \begin{pmatrix} X_4 & X_2 \\ X_3 & X_1 \end{pmatrix} \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}$$

$$\begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix} = M_3 = X_1^{-1}X_2^{-1}M_1^{-1}Z_2 = \frac{1}{X_1X_2(X_1X_4 + X_2X_3)} \begin{pmatrix} X_4 & X_2 \\ X_3 & X_1 \end{pmatrix} \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}$$

By comparison of both sides of the above two equations, we can obtain $X_2$,...,$X_{12}$ successively.

This cipher withstands a variety of attacks such as hole attack, rank attack, Patarin relations attack for C*, Gröbner bases and Patarin's IP approach. It is relatively safer.

**Our Improvements on Wang *et al.* (2009) scheme:** In Wang *et al.* (2009) Scheme, "$X_1$ $X_2$, $X_3$, $M_1$ are all invertible" are too restrict. When $X_1 = X_2 = X_3 = 0$, we have $Y_j = 0$ $X_4$,...$X_{12}$ are difficult to be restored. We modify the central mapping $\phi_2$ as follows:

$$\begin{cases} Y_1 = X_1 + X_3^2(X_5X_8 + X_6X_7) + Q_1 \\ Y_2 = X_2 + X_1^2(X_9X_{12} + X_{10}X_{11}) + Q_2 \\ Y_3 = X_3 + X_2^2(X_1X_4 + X_2X_3) + Q_3 \\ Y_4 = X_2X_3(X_1X_5 + X_2X_7), Y_5 = X_2X_3(X_1X_6 + X_2X_8) \\ Y_6 = X_2X_3X_3X_5 + X_4X_3), Y_7 = X_2X_3(X_3X_6 + X_4X_8) \\ Y_8 = X_1X_2(X_1X_9 + X_2X_{11}), Y_9 = X_1X_2(X_1X_{10} + X_2X_{12}) \\ Y_{10} = X_1X_2(X_3X_9 + X_4X_{11}), Y_{11} = X_1X_2(X_3X_{10} + X_4X_{12}) \\ Y_{12} = X_1X_3(X_5X_9 + X_7X_{11}), Y_{13} = X_1X_3(X_5X_{10} + X_7X_{12}) \\ Y_{14} = X_1X_3(X_6X_9 + X_8X_{11}), Y_{15} = X_1X_3(X_6X_{10} + X_8X_{12}) \\ Y_{16} = X_1^4, Y_{17} = X_1^4 + X_2^4 \\ Y_{18} = X_1^4 + X_2^4 + X_3^4, Y_{19} = \forall x \in \mathbb{L} \end{cases} \quad (15)$$

The computing order is to compute $Y_{16}$, ..,$Y_{19}$ before $Y_1$,.., $Y_{15}$. Before we use the formulae of $Y_1$, ..,$Y_{15}$ in Eq. 15, we adjust $X_1$, $X_2$, $X_3$ one by one to assure $X_1 \neq 0$, $X_2 \neq 0$, $X_3 \neq 0$, det $(M_1) \neq 0$. With the pseudo values of $X_1$, $X_2$, $X_3$ we can avoid the singularity in $\phi_2$.

At the same time, we modify the affine mapping, i.e. the K-linear isomorphism $\pi_3$: $L^{19} \rightarrow K^{19r}$ to fit the modification.

The encryption is quite the same as that of Wang *et al.* (2009) scheme, except for the extra computation of $Y_{16}$, $Y_{17}$, $Y_{18}$, $Y_{19}$.

The decryption is described as follows.

Compute from Eq. 15 the values of $X_1$, $X_2$, $X_{12}$ just the same way as mentioned in Wang *et al.* (2009) program. Then in the field of character 2, we restore $X_1$, $X_2$, $X_3$ from the pseudo to the original with a triangular solution as follows:

$$X_1 = \sqrt[4]{Y_{16}}, X_2 = \sqrt[4]{Y_{16} + Y_{17}}, X_3 = \sqrt[4]{Y_{16} + Y_{17} + Y_{18}}$$

**Analysis of the scheme:** In Eq. 15, we fully solve the problem of original singularity. This makes the algorithm more robust. Meanwhile, $x \in L$ is a random value which is used as a perturbing item. This small change in $V_k$, $1 \leq k \leq 19r$ results in big change in $Y_{19}$ A plaintext can create a lot of ciphertexts. This Camouflage technique makes the system safer. The breaking is difficult because the ciphertext is changeable for a given plaintext. We will show numeric experimental results later.

## PROPOSED BLOCK CIPHER

Now let us see how we use our new scheme set up a block cipher. We concentrate on the algorithem over L, so that the $\pi$s are omitted for convenience.

**Medium-field with its addition and multiplication:** Let $L = K^8$, $K = Z_2 = \{0, 1\}$ so that L is just the extended set of ASCII. L has a character 2.

The addition of a, $b \in L$, $a \oplus b$ is bitwise exclusive or of a, b also denoted by a+b for convenience (Fig. 1).

In the field L, we have a+a = 0 and a-b = a+b.

However the multiplication of a, $b \in L$, $a \odot b$ or ab is more complicated. Obviously, the non-zero element subset of L is a $2^8$-1 = 225 ordered cyclic group, denoted by L* = {1, 2, ..,0xFF}. Take an 8 ordered ammonic primitive polynomial over K, we have $p(x) = x^8+x^5+x^3+x+1$. Let $\xi$ be a root of p(x). Then $\xi$ generate L, i.e., L = ($\xi$). All elements in L can be obtained from the linear shift feedback register system $\xi^8 = \xi^5+\xi^3+\xi+1$ it is shown in Fig. 2.

On one hand, any of element in L can be denoted by a power of $\xi$. One the other hand it follows from $\xi^8 = \xi^5+\xi^3+\xi+1$ that $\{\xi^0 = 1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7\}$ is a maximal linear independent group i.e., a base.

$\forall$A, $b \in L$, a, b, can be denote by certain linear combination of 1, $\xi$, $\xi^2$, $\xi^3$, $\xi^4$, $\xi^5$, $\xi^6$, $\xi^7$. Let:

$$a = a_0\xi^0+a_1\xi+...+a_7\xi^7, a_i \in \{0, 1\}, i = 0, 1,..., 7$$

$$b = b_0\xi^0+b_1\xi+...+b_7\xi^7, b_i \in \{0, 1\}, i = 0, 1,..., 7$$

It follows from the linear shift feedback register system that:

$$a\xi = a_7\xi^0+(a_0+a_7)\xi^1+a_1\xi^2+(a_2+a_7)\xi^3+a_3\xi^4+(a_4+a_7) \xi^3+a_3\xi^4+(a_4+a_7)\xi^5+a_5\xi^6+a_6\xi^7$$

Furthermore, we have the product ab as shown in Fig. 3.

More details of operations of $Z_2^m$ can be found in Cohen *et al.* (2005) Gilbert and Nicholson (2004) and Courtois (2001). We concentrate on the mappings $\phi_1$, $\phi_2$, $\phi_3$ and their inverses as follows.

**Encryption**

- Input: U
- Output: V
- Algorithm

**Step 1:** Compose $\phi_1$, $\phi_2$, $\phi_3$, to obtain $\phi$, so that $\phi = \phi_1 \circ$, $\phi_2 \circ$, $\phi \circ_3$ as shown in Fig. 4

The implement can be the compiling of the function phi (parameters):

*Addtion c=a+b:*
*c=a xor b*
*where xor is the bitwise exclusive or of a and b*

Fig. 1: Addition of medium-field L

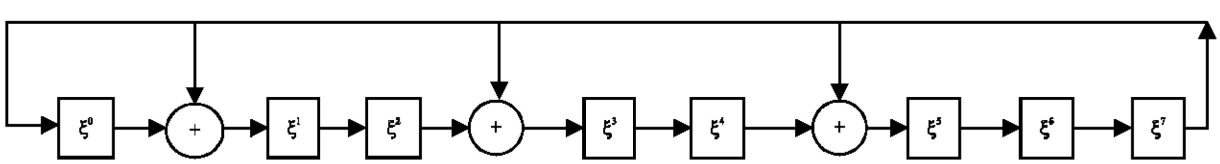


Fig. 2: Linear shift feedback register system $\xi^8 = \xi^5+\xi^3+\xi+1$

```
phi(parameters){
phi_1(parameters);
phi_2(parameters);
phi_3(parameters)
return parameters;
}
```

Then publish the program as the public key, in which phi(parameters) accept U and return V like a box. Inside the box, the computation can be described as shown from step 2-6.

**Step 2:** Format U, rewrite U to meet the block size 12, append ".”s at the end if neccessary

**Step 3:** Determin $Q_1$, $Q_2$, $Q_3$

**Step 4:** Compute $\phi_1$: $X = A_1U+C_1$

**Step 5:** Compute $\phi_2$, in $\phi_2$, we have Y from Eq. 15

**Step 6:** Compute $\phi_3$: $V = A_3Y+C_3$

**Decryption**

- **Input:** V
- **Output:** U
- Algorithm

**Step 1:** Compose $\phi_1^{-1}$ to obtain $\phi^{-1}$so that $\phi^{-1} = \phi_3^{-3} \circ \phi_2^{-1} \circ \phi_1^{-1}$ as shown in Fig. 5

The implement can be the compiling of the function:

```
phi_inv(parameters):
phi_inv(parameters){
phi_3_inv(parameters);
phi_2_inv(parameters);
phi_1_inv(parameters)
return parameters;
}
```

```
Multiplication c = ab;
•   if b0=1
    then c←a
    else c←0
•   for i=1 to 7
    a ←aξ
    if bi=1 then c← c+a
    where c+a = c xor a
```

Fig. 3: Multiplication of medium-field L

The function phi_invi(parameters) accept V and return U like a box. Inside the box, the computation can be described as shown from Step 2 to Step 6:

**Step 2:** Determine $Q_1$, $Q_2$, $Q_3$

**Step 3:** Compute $\phi_3^{-1}$: $Y = A_3^{-1}(V+C_3)$, in $\phi_3^{-1}$, from Gaussian Elimination,we have $A_3^{-1}$

**Step 4:** Compute $\phi_2^{-1}$ in $\phi_2^{-1}$, we have From (15), we have X

**Step 5:** Compute $\phi_1^{-1}$: $U = A_1^{-1}(X+C_1)$, from Gaussian Elimination, we have $A_1^{-1}$

**Step 6:** Restore U = "It's a text"

## EXPERIMENTAL RESULTS AND ANALYSIS

**Encryption**

- **Input:** U = "It's a text"
- **Output:** V = 75 38 4A B4 C6 4A 72 AD pB 72 CD 4F F8 C8 04 D6 80$)^T$

**Algorithm**

**Step 1:** Compose $\phi_1$, $\phi_2$, $\phi_3$, to obtain $\phi$, so that $\phi = \phi_1 \circ \phi_2 \circ \phi_3$ as shown in Fig. 4

```
The implement can be the compiling of the function phi():
phi(parameters){
phi_1(parameters);
phi_2(parameters);
phi_3(parameters)
return parameters;
}
```

Then publish the program as the public key, in which phi(parameters) accept U and return V like a box. Inside the box, the computation can be described as shown from step 2-6:

**Step 2:** Format U, rewrite U by U= "It's a text". To meet the block size 12, in hexadecimal form it is denoted by:

$$U = (49\ 74\ 27\ 73\ 20\ 61\ 20\ 61\ 20\ 74\ 65\ 78\ 74\ 2E)^T$$

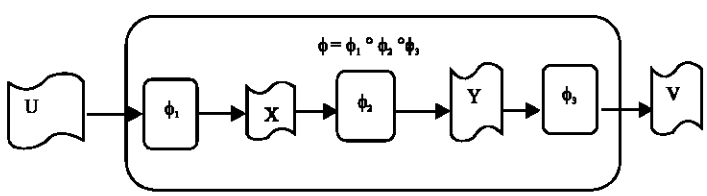


Fig. 4: Composition of the mappings $\phi_1$, $\phi_2$, $\phi_3$

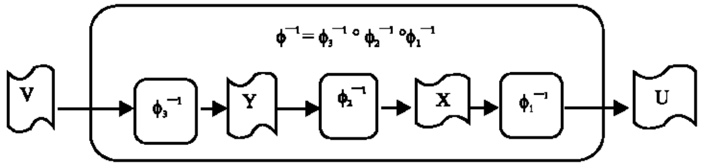


Fig. 5: Composition of the invert mappings $\phi_3^{-1}$, $\phi_2^{-1}$, $\phi_1^{-1}$

**Step 3:** Determine $Q_1 = 5C$, $Q_2 = 25$, $Q_3 = 74$

**Step 4:** Compute $\phi_1$: $X = A_1U+C_1$, in $\phi_1$, we have:

$$A_1 = \begin{pmatrix} A_{11} \\ A_{21} \\ A_{31} \end{pmatrix}$$

Where:

$$A_{11} = \begin{pmatrix} 30 & 70 & B0 & F0 & 31 & 71 & B1 & F1 & 32 & 72 & B2 & F2 \\ 87 & 61 & 62 & 84 & 86 & 60 & 63 & 85 & 83 & 65 & 66 & 80 \\ 05 & C0 & 6F & 2A & B3 & D0 & BC & 5F & E8 & E1 & 35 & BC \\ F0 & 4B & 4E & F5 & F1 & 4A & 4F & F4 & E0 & 5B & 5E & E5 \end{pmatrix}$$

$$A_{31} = \begin{pmatrix} 55 & 6B & 29 & 78 & E0 & B9 & 2A & 1C & 21 & B4 & D0 & 2A \\ 52 & DD & AB & 42 & 50 & 1E & 7A & 52 & 88 & 82 & CD & A1 \\ C2 & FC & 90 & 15 & F2 & 39 & 1C & E5 & 05 & BD & D8 & 61 \\ 2A & 05 & 7E & EF & 5F & EC & 83 & 8E & FA & 1D & DA & 83 \end{pmatrix}$$

$$A_{21} = \begin{pmatrix} CD & 54 & E2 & C9 & 0C & 6E & 1D & CD & 5B & 33 & 50 & 8A \\ 11 & 03 & 1F & E8 & 67 & 28 & 32 & 98 & EF & AE & 96 & 32 \\ 4D & 90 & 64 & 77 & D2 & 5C & 6B & FC & 7E & 7A & A4 & 62 \\ 84 & A3 & B2 & 95 & 85 & A2 & B3 & 94 & AF & 88 & 99 & BE \end{pmatrix}$$

$$C1 = (48\ \ 65\ \ 6C\ \ 65\ \ 68\ \ 48\ \ 65\ \ 6C\ \ 6C\ \ 65\ \ 6E)^T$$

$$X = A_1U+C_1 = (70\ \ 90\ D2\ 1D\ 0F\ EE\ 7D\ A0\ \ 02\ 3D\ \ 0B\ \ 60)^T$$

**Step 5:** Compute $\phi_2$, in $\phi^2$, we have:

$$M_1 = \begin{pmatrix} 71 & 90 \\ D2 & 1D \end{pmatrix}, M_2 = \begin{pmatrix} 0F & EE \\ 7D & A0 \end{pmatrix}, M_3 = \begin{pmatrix} 02 & 3D \\ 0B & 60 \end{pmatrix}$$

$$\det(M_1) = 24, \det(M_2) = 24, \det(M_3) = 44$$

$$Z_1 = \begin{pmatrix} 34 & 02 \\ F0 & B0 \end{pmatrix}, Z_2 = \begin{pmatrix} AD & 45 \\ 1F & D9 \end{pmatrix}, Z_3 = \begin{pmatrix} 31 & 8B \\ 7F & EE \end{pmatrix}$$

$$\det(Z_1) = 4F, \det(Z_2) = 15, \det(Z_3) = 72$$

$$Y = (13\ \ 8E\ \ 11\ \ 34\ \ 02\ \ F0\ \ B0\ \ AD\ \ 45\ \ 1F\ \ D9\ \ 31\ \ 8B\ \ 7F\ \ EE\ \ 4A\ \ 1D\ \ E1\ \ E8)^T$$

where, $Y_{19} = E8$, is a random value in finite field L.

**Step 6:** Compute $\phi_3$: $V = A_3Y+C_3$, in $\phi_3$, we have:

$$A_3 = \begin{pmatrix} A_{13} \\ A_{23} \\ A_{33} \\ A_{43} \end{pmatrix}$$

Where:

$$A_{13} = \begin{pmatrix} 41 & 61 & 81 & A1 & C1 & E1 & 02 & 22 & 42 & 62 & 82 & A2 & C2 & E2 & 03 & 23 & 43 & 63 & 83 \\ E7 & 4B & E4 & 48 & 02 & AE & 04 & A8 & E2 & 4E & E1 & 4D & 07 & AB & 05 & A9 & E3 & 4F & E0 \\ 7E & 03 & 56 & 5B & A9 & B4 & 08 & 1A & 1D & 1F & 8D & FF & 18 & 7A & 0F & 91 & BC & 32 & EF \\ BA & A3 & BF & A6 & 04 & 1D & 10 & 09 & AB & B2 & AE & B7 & 15 & 0C & 11 & 08 & AA & B3 & AF \end{pmatrix}$$

$$A_{23} = \begin{pmatrix} 54 & DD & 9E & 52 & 79 & 58 & 20 & 19 & 7F & AB & A5 & 34 & 48 & 34 & 33 & 33 & 97 & 7A & 88 \\ 35 & 05 & D9 & 88 & 08 & 72 & 40 & 6F & 7A & 7E & B4 & D1 & 6B & 25 & 55 & CF & 32 & 83 & FA \\ 81 & CE & 84 & 0C & F2 & 5B & 80 & CA & 1B & 5A & 65 & 9B & D3 & 6E & FF & 24 & 09 & 0F & 35 \\ 26 & 4C & 37 & 5D & 10 & 7A & 2B & 41 & 0C & 66 & 1D & 77 & 3A & 50 & 2A & 40 & 0D & 67 & 1C \\ FE & 0F & 5F & 1D & CF & 82 & 56 & D1 & 65 & ED & 33 & 08 & 6F & 5B & 7E & B3 & 2A & E8 & AD \end{pmatrix}$$

$$A_{33} = \begin{pmatrix} DD & 79 & 9A & C9 & 20 & 8D & AC & 6A & 34 & 0C & 58 & 97 & A6 & 97 & 82 & 82 & DB & 25 & A5 \\ 4D & D4 & 8B & 79 & B5 & A5 & 73 & 60 & 9C & CE & 88 & 3E & 26 & 9E & AD & 0B & 7D & 7B & 11 \\ 96 & 11 & 69 & A5 & 40 & 65 & E6 & 1F & 25 & 35 & 72 & 29 & 0F & BD & DC & 56 & 83 & E0 & C0 \\ 76 & 8B & 44 & 9A & 41 & 33 & E7 & A3 & 52 & 84 & BD & 3F & F2 & C9 & 4F & 1F & 89 & 40 & 69 \\ E4 & 57 & F5 & 50 & 80 & 88 & E5 & 47 & 6E & 89 & 5B & 8B & 2D & 1E & D1 & BC & 41 & 55 & 96 \end{pmatrix}$$

$$A_{43} = \begin{pmatrix} BD & 33 & B4 & E1 & 82 & BD & E1 & 1D & B4 & 25 & 25 & 72 & 88 & 72 & 58 & 58 & 65 & 5B & 7A \\ B8 & B6 & 92 & 9C & 2B & 25 & E9 & E7 & 50 & 5E & 7A & 74 & C3 & CD & E8 & E6 & 51 & 5F & 7B \\ D6 & F9 & 2F & EB & 2F & 01 & F9 & 3C & EA & C5 & 01 & C5 & C5 & EB & 13 & F8 & F9 & F8 & F8 \\ D0 & 55 & 98 & 7A & 56 & E1 & D9 & 29 & 5B & FE & 82 & 40 & 1F & 88 & 35 & 67 & E8 & EF & 18 \\ 7D & F1 & A2 & 6D & 5E & AE & 99 & F5 & 6A & 70 & E1 & 14 & 0D & 0E & 5F & 96 & 37 & 27 & F7 \end{pmatrix}$$

And:

$$C_3 = (00\ \ 34\ \ 36\ \ 31\ \ 32\ \ 32\ \ 43\ \ 59\ \ 4C\ \ 31\ \ 4A\ \ 47\ \ 37\ \ 30\ \ 53\ 00\ \ 34\ \ 36\ \ 3\ \ 31)^T$$

$$V = A_3Y+C3 = (75\ \ 38\ \ 4A\ \ 55\ \ B4\ \ C6\ \ 4A\ \ 72\ \ AD\ \ 9B\ \ A6\ \ 72\ \ CD\ \ 4F\ \ F8\ \ C8\ \ 04\ \ D6\ \ 80)^T$$

**Decryption**

- Input

$$V = (75\ \ 38\ \ 4A\ \ 55\ \ B4\ \ C6\ \ 4A\ \ 72\ \ AD\ \ 9B\ \ A6\ \ 72\ \ CD\ \ 4F\ \ F8\ \ C8\ \ 04\ \ D6\ \ 80)^T$$

- Output

U = “It’s a text”

Algorithm

**Step 1:** Compose $\phi^{-1}_3$, $\phi^{-1}_2$, $\phi^{-1}_1$, to obtain $\phi^{-1}_3$, so that $\phi^{-1} = \phi^{-1}_3 \circ \phi^{-1}_2 \circ \phi^{-1}_1$ as shown in Fig. 5

```
The implement can be the compiling of the function phi_inv():
        phi_inv(parameters){
        phi_3_inv(parameters);
        phi_2_inv(parameters);
        phi_1_inv(parameters)
        return parameters;
}
```

The function phi_invi(parameters) accept V and return U like a box. Inside the box, the computation can be described as shown from step 2-6.

**Step 2:** Determine $Q_1$ = 5C, $Q_2$ = 25, $Q_3$ = 74

**Step 3:** Compute $\phi^{-1}_3$: $Y = A^{-1}_3(V+C_3)$, in $\phi^{-1}_3$, from Gaussian Elimination, we have:

$$A_3^{-1} = \begin{pmatrix} \dot{A}_{13} \\ \dot{A}_{23} \\ \dot{A}_{33} \\ \dot{A}_{43} \end{pmatrix}$$

Where:

$$\dot{A}_{13} = \begin{pmatrix} A4 & D9 & 3C & 82 & 99 & 87 & 48 & AB & 45 & C4 & 1D & BF & 8A & CD & 72 & 00 & 04 & 29 & 4E \\ A3 & 67 & 0A & 41 & 22 & 41 & A7 & FD & 60 & C9 & DF & AF & 13 & E6 & 9E & 00 & 50 & 51 & 9B \\ 8D & D3 & 3B & 82 & BE & 98 & 72 & BB & 4F & B8 & 5B & 60 & 01 & 3C & C7 & 67 & F5 & E1 & 74 \\ 0F & 7B & 1C & FC & 23 & 95 & FE & 96 & D0 & 12 & DF & E4 & 57 & 50 & 5E & BB & B2 & C0 & 60 \end{pmatrix}$$

$$\dot{A}_{23} = \begin{pmatrix} 67 & B1 & CF & A8 & 4C & C6 & 75 & C3 & EB & 6A & 18 & CA & C5 & C8 & D5 & FE & A0 & 54 & 2B \\ 8D & 5B & 4C & 82 & 8D & 74 & DB & 2C & 62 & 2C & 3E & 60 & 4D & AE & 01 & 5A & 52 & F1 & 2A \\ 75 & 7D & 97 & 11 & BB & 77 & F4 & D3 & 95 & E8 & DE & 14 & 62 & 03 & C8 & 9C & E5 & 4D & C7 \\ FC & DA & E6 & 47 & D4 & 21 & 68 & 78 & 04 & C7 & CD & E7 & D4 & 88 & 3C & B2 & 54 & E7 & C9 \\ 41 & 49 & A1 & C7 & 27 & 73 & E6 & BA & E6 & 67 & 4E & EF & 98 & 77 & AB & 68 & 07 & 96 & E8 \end{pmatrix}$$

$$\dot{A}_{33} = \begin{pmatrix} 12 & 7B & D6 & 8A & FD & 3D & CB & B5 & E2 & 44 & 1C & 90 & C8 & BD & 12 & A3 & D7 & D1 & F3 \\ 6F & 54 & 00 & 84 & EA & EB & 87 & 3D & 4E & DA & 31 & D5 & 80 & FB & D1 & 3A & 52 & 69 & 2E \\ 6E & A8 & 5A & 1D & E9 & F7 & 1F & 96 & BC & FD & F8 & 56 & BE & 7F & B6 & CB & 7E & B0 & B0 \\ 27 & D0 & 45 & 79 & 6C & B0 & 01 & A2 & F7 & F7 & 1C & A1 & 06 & 26 & CD & 57 & 79 & 7A & 44 \\ 9E & 67 & 8B & 88 & 3D & CD & E5 & 58 & A3 & 3D & F4 & 90 & 99 & C2 & 46 & 90 & D5 & B2 & 0F \end{pmatrix}$$

$$\dot{A}_{43} = \begin{pmatrix} F0 & B4 & 75 & 34 & 43 & 78 & 9A & 23 & 8A & 69 & F1 & 07 & 0E & BB & F6 & 5A & 78 & FE & DB \\ B9 & 25 & DB & 7C & 5B & 98 & 81 & 96 & F5 & 2B & 4C & 51 & E8 & 93 & FC & C9 & 76 & C5 & 5F \\ DF & E5 & 6C & C2 & DB & 59 & D2 & F4 & 22 & 3D & F1 & 3F & 04 & 60 & E9 & 4A & 34 & C3 & 8F \\ DA & 93 & 60 & AD & 2A & 1E & 5A & AB & DE & 9F & AF & CB & DA & 03 & E3 & 6E & EE & 91 & 0B \\ EC & E3 & 30 & 7F & 0E & DE & 5E & 48 & B0 & 01 & 83 & 9C & 7F & 6A & A1 & 00 & 35 & 95 & C0 \end{pmatrix}$$

And:

$$C_3 = (00\ \ 34\ \ 36\ \ 31\ \ 32\ \ 32\ \ 43\ \ 59\ \ 4C\ \ 31\ \ 4A\ \ 47\ \ 37\ \ 30\ \ 53\ \ 0\ \ 34\ \ 36\ \ 31)^T$$

$$Y = A^{-1}_3(V+C_3) = (13\ \ 8E\ \ 11\ \ 34\ \ 02\ \ F0\ \ B0\ \ AD\ \ 45\ \ 1F\ \ D9\ \ 31\ \ 8B\ \ 7F\ \ EE\ \ 4A\ \ 1D\ \ E1\ \ E8)$$

**Step 4:** Compute $\phi^{-1}_2$, in $\phi^{-1}_2$, we have:

$$Z_1 = \begin{pmatrix} 34 & 02 \\ F0 & B0 \end{pmatrix}, Z_2 = \begin{pmatrix} AD & 45 \\ 1F & D9 \end{pmatrix}, Z_3 = \begin{pmatrix} 31 & 8B \\ 7F & EE \end{pmatrix}$$

$$\det(Z_1) = 4F,\ \det(Z_2) = 15,\ \det(Z_3) = 72$$

$$M_1 = \begin{pmatrix} 71 & 90 \\ D2 & 1D \end{pmatrix}, M_2 = \begin{pmatrix} 0F & EE \\ 7D & A0 \end{pmatrix}, M_3 = \begin{pmatrix} 02 & 3D \\ 0B & 60 \end{pmatrix}$$

$$\det(M_1) = 24,\ \det(M_2) = 24,\ \det(M_3) = 44$$

From Eq. 15, we have:

$$X = (71\ \ 80\ \ D2\ \ 1D\ \ 0F\ \ EE\ \ 7D\ \ A0\ \ 02\ \ 3D\ \ 0B\ \ 60)^T$$

**Step 5:** Compute $\phi^{-1}_1$: $U = A^{-1}_1(X+C_1)$, in $\phi_1$, from Gaussian Elimination, we have:

$$A_1^{-1} = \begin{pmatrix} \dot{A}_{11} \\ \dot{A}_{21} \\ \dot{A}_{31} \end{pmatrix}$$

Where:

$$\dot{A}_{11} = \begin{pmatrix} E2 & B8 & AF & 67 & D7 & 92 & 58 & 70 & 1E & E1 & EB & ED \\ B3 & CA & 87 & E9 & DD & E5 & 58 & 30 & 8F & 42 & EB & 04 \\ 76 & B5 & 20 & EE & 02 & A6 & 58 & 95 & 26 & 36 & EB & 56 \\ 81 & 73 & C8 & F1 & 73 & 5D & 58 & 47 & E7 & 6E & EB & D0 \end{pmatrix}$$

$$\dot{A}_{21} = \begin{pmatrix} 2E & EF & 24 & CE & 30 & 5F & A8 & AC & C4 & EF & E2 & DE \\ DA & AB & 15 & 01 & 05 & D6 & A8 & D2 & 11 & 23 & E2 & 02 \\ A2 & BE & 1B & 3A & 26 & BA & A8 & 9A & C8 & FC & E2 & C7 \\ B1 & 3B & BC & B6 & 0B & FB & A8 & 09 & E6 & CC & E2 & 77 \end{pmatrix}$$

$$\dot{A}_{31} = \begin{pmatrix} 4E & 6C & E3 & D3 & 0B & E0 & F0 & 3E & 6E & D7 & 09 & 43 \\ 61 & 13 & 31 & CC & 6A & 6B & F0 & B5 & A2 & 8D & 09 & 0A \\ 8D & 9A & 36 & 92 & 25 & D3 & F0 & E2 & 3B & B8 & 09 & CB \\ E0 & 29 & 48 & 90 & 82 & D0 & F0 & E3 & 8A & EC & 09 & 84 \end{pmatrix}$$

$$C_1 = (45\ \ 65\ \ 6C\ \ 65\ \ 6E\ \ 48\ \ 65\ \ 6C\ \ 6C\ \ 65\ \ 6E)^T$$

$$U = A^{-1}_1(X+C_3) = (48\ \ 74\ \ 27\ \ 73\ \ 20\ \ 61\ \ 20\ \ 74\ \ 65\ \ 78\ \ 74\ \ 2E)$$

**Step 6:** Restore *U =" It's a text"* from *U =" It's a text".* by removing.” from the end of the block

**Analysis:** Experimental results show that our scheme is viable. Given a 12-byte plaintext block U, we obtain a

| $Y_{19}$ | $V(Y_{19})$ |
|---|---|
| $E_n$ | 75 38 4A 55 B4 C6 4A 72 AD 9B A6 72 CD 4F F8 C8 04 D6 80 |
| 13 | C3 C4 08 5F 2D FC 16 F8 7A 45 4F AA 53 81 52 99 E3 CD D9 |
| 9E | E0 EC 3A B7 76 82 37 FD A3 55 61 EF AD EE B3 F5 AC AA 8C |
| 26 | DF 69 AD 4E ED 95 80 82 01 BD 57 5D 0B 51 78 86 E0 63 D2 |
| AF | A6 BC 5E 4C C0 7E 75 F7 3A 62 3D 65 7A 30 5A 2D 32 64 26 |
| C5 | 9E CD 3F 6E 6B AC 72 03 CC B9 0D A0 CA BB 0E 13 34 13 30 |
| 72 | E1 6F DA 58 D9 0A CD C8 BF F5 C4 FE 6D 87 25 8F D7 52 94 |
| 44 | 53 C9 65 93 AA 46 04 96 18 C9 EF 62 8E C6 81 1D F7 D4 AD |
| BC | 4B 3E 3D 43 80 59 07 38 13 D3 35 D1 AB 99 A5 C1 33 E7 C6 |
| 6D | E2 C1 D1 42 03 B9 E8 97 9B 39 00 CD 06 3C B4 01 5A 71 BC |
| 78 | 78 55 86 D2 E0 D4 24 10 21 3B 6E AF 8A 9C 7C DC 1D A2 38 |
| 50 | 4A BD DD AC 2F D1 FD 0D 0F 7E 90 C0 6B F0 33 BB 48 1F DE |
| 66 | F8 1B 62 67 5C 9D 34 53 A8 42 BB 5C 88 B1 97 29 68 99 E7 |
| 2F | E8 58 EB 1E 89 6E 36 7E 43 B7 CE 67 57 DB AF 58 09 BB 4C |
| Etc. | and so on |

Fig. 6: Table of different ciphertexts from the same plaintext

19-byte ciphertext block V and vice versa. If a plaintext is bigger than 12 bytes, we can divide it into blocks of 12-byte. The remainder may be a smaller block. In this case, we append some ".”s at the end to make it a 12-byte one. Last continual ".”s are only used as a "length matcher". When we restore a plaintext from a cipher one, we can remove them from the end according to the context with ease.

The $Y_{19} = \forall x \in L$ in $\phi$ is a random value. It is used as a perturbing item. This small change makes big change after $\phi_3$. It makes $\phi$ a multi-valued cipher. A determined plaintext may result in undetermined ciphertexts. This makes the adversary difficult to crack the cipher. More examples are shown as follows.

Given $A_1$, $A_3$, $C_1$, $C_2$, $Q_1$, $Q_2$, $Q_3$, U just the same as before, we have the results in Fig. 6.

We may use this perturbing item as a camouflage technique to make the crack more difficult. The scheme is secure.

## CONCLUSION

To design a block cipher algorithm based on MFE multivariate public key cryptosystem, we choose Wang *et al.* (2009) scheme and solve a problem in the central mapping. In addition to solving the original problem, we extend its new feature of camouflage. This new feature makes the system safer. Experimental results and analysis show that our scheme is viable and secure and deserves further study in network applications.

## ACKNOWLEDGMENTS

This study was supported by the fund from Natural Science of Jiangxi Province of China under Grant No. 20114BAB201033. The authors would like to express their thanks to the Committee of the fund.

## REFERENCES

Cohen, H., G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, 2005. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Taylor and Francis Group, London, ISBN-13: 9781420034981, Pages: 848.

Courtois, N.T., 2001. The security of Hidden Field Equations (HFE). Proceedings of the Cryptographers Track at RSA Conference, Vol. 2020, April 8-12, 2001, San Francisco, CA, USA, pp: 266-281.

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

Ding, J. and D. Schmidt, 2006. Multivariate public key cryptosystems. Contemp. Mathe., 419: 79-94.

Faugere, J.C. and A. Joux, 2003. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using grobner bases. Proceedings of the 23rd Annual International Cryptology Conference, August 17-21, 2003, Santa Barbara, California, USA, pp: 44-60.

Fell, H. and W. Diffie, 1986. Analysis of a Public Key Approach Based on Polynomial Substitution. In: Advances in Cryptology-Crypto'85, Williams, H.C (Ed.). Vol. 218, Springer-Verlag, London, pp: 340-349.

Gilbert, W.J. and W.K. Nicholson, 2004. Modern Algebra with Applications. 2nd Edn., John Wiley and Sons, New Jersy, USA, ISBN-13: 9780471469896, Pages: 352.

Goubin, L. and N. Courtois, 1976. Cryptanalysis of the TTM cryptosystem. Comput. Sci., 1976: 44-57.

Kipnis, A., J. Patarin and L. Goubin, 1999. Unbalanced oiland vinegar signature schemes. Comput. Sci., 1592: 206-222.

Patarin, J., 1995. Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In: Advances in Cryptology -Crypto'95, Coppersmith, D. (Ed.). Vol. 963, Springer-Verlag, London, pp: 248-261.

Patarin, J., 1997. The oil and vinegar signature scheme. Proceedings of the Dagstuhl Workshop on Cryptography, September 1997.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

Rivest, R.L., A. Shamir and L. Adleman, 1982. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. In: Secure Communications and Asymmetric Cryptosystems, Simmons, G. (Ed.)., Volume 69 of AAAS Selected Symposium, Westview Press, New York, pp: 217-239.

Shor, P.W., 1994. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev., 41: 303-332.

Wang, L.C., B.Y. Yang, Y.H. Hu and F. Lai, 2006. A medium-field multivariate public-key encryption scheme. Comput. Sci., 3860: 132-149.

Wang, X., F. Feng, X.M. Wang and Q. Wang, 2009. A more secure MFE multivariate public key encryption scheme. Int. J. Comput. Sci. Appl., 6: 1-9.