Construction of Extended Multivariate Public Key Cryptosystems

Shuaiting Qiao, Wenbao Han, Yifa Li, and Luyao Jiao
(Corresponding author: Shuaiting Qiao)

Zhengzhou Information Science and Technology Institute
Zhengzhou, Henan Province, 450001, China
(Email: qsting2012@163.com)
(Received Sep. 03, 2013; revised and accepted Jan. 20 & Mar. 23, 2014)

Abstract

Based on the ideas: "invertible cycle", "tame transformation" and "special oil and vinegar", three different nonlinear invertible transformations were constructed separately. Then making use of the idea of the extended multivariate public key cryptosystem, and combining the nonlinear invertible transformations above with Matsumoto-Imai (MI) scheme, three methods of designing extended multivariate public key cryptosystem were proposed. Next, the corresponding encryption and signature algorithms were given. Analysis results demonstrate that the new extended cryptosystems inherit the merit of MI scheme, i.e., efficient computation. Meanwhile, the new extended cryptosystems can also resist the linearization attack, differential attack and algebraic attack.

Keywords: Extended multivariate public key cryptosystem, invertible cycle, matsumoto-imai scheme, special oil and vinegar, tame transformation

1 Introduction

The 21st century is the era of information. With the rapid development of electronic information science and technology, information security has become so important. After electronic information science and technology, quantum and other new information science are building up and developing [9]. But the development of quantum computers will pose a threat to the widely-used public key cryptosystems, which are based on discrete logarithm problem and large integer factorization problem [10, 16]. Therefore, great attention has been paid to the post-quantum public key cryptography [2], and multivariate public key cryptosystems (MPKCs) develop rapidly in this background. MPKC is considered to be a candidate of secure cryptosystems in post-quantum era for its higher efficiency, better security and easy access to the hardware implementation, etc. During the last twenty years, MPKCs have received more and more attention.

The security of MPKCs depends on the difficulty of solving a set of nonlinear multivariate quadratic equations over a finite field [7] and the isomorphism of polynomials problem [17]. Its research began in the 1990s. According to different central maps, MPKCs have been divided into five schemes, which are Matsumoto-Imai (MI) scheme, Hidden Field Equation (HFE) scheme, Unbalanced Oil and Vinegar (UOV) scheme, Stepwise Triangular Systems (STS) scheme and Medium Field Equation (MFE) scheme [7]. Especially, in the past few years, many cryptosystems have emerged in sequence, such as the CyclicRainbow cryptosystem [14], the Double-Layer square cryptosystem [3], the Enhanced STS cryptosystem [19], etc, which make MPKCs develop and complete. Meanwhile, researchers have also applied MPKCs to identification [15], special signatures [22, 24]and other fields. So far, MPKCs have been a hot topic in cryptography.

In 1988, Matsumoto and Imai proposed MI scheme with high efficiency, which was seen as the first scheme of MPKCs [11]. In 1995, Patarin et al present linearization attack aimed at MI scheme [12]. To resist linearization attack, Jacques Patarin et al came up with the Flash cryptosystem in 2000 [13], and Ding Jin-tai et al put forward the PMI cryptosystem in 2004 [4], but both of them were vulnerable to differential attack [5, 8]. In 2011, by incorporating the hash authentication technique and traditional multivariate public key cryptography algorithm, Wang Hou-zhen et al proposed Extended Multivariate Public Key Cryptosystem (EMC), which can resist both linearization attack and differential attack [20]. The emerging of EMC pointed out a new idea to construct novel multivariate public key cryptosystems.

In this work, on the base of the ideas: invertible cycle [6], tame transformation [21] and special oil and vinegar [23], three different nonlinear invertible transformations are built separately. Then by combining these nonlinear invertible transformations above and MI scheme, three different methods to construct novel EMCs are proposed. Finally, the performance analysis and security analysis will be given.

The rest of this paper is organized as follows. In Section 2, we give a brief overview of general structure of MPKCs, EMC and MI scheme. Section 3 presents 3 the design of the novel EMCs. Section 4 gives the operation efficiency and security analysis of our proposed cryptosystems. Finally, Section 5 concludes this paper.

2 Preliminaries

2.1 General Structure of MPKCs

The trapdoor function of MPKCs is a set of nonlinear multivariate quadratic polynomials over a finite field, i.e.,$P =: \mathbb{F}^n \to \mathbb{F}^m$,

$$P = (p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n)).$$

For $1 \le j \le k \le n$, $1 \le i \le m$, each $p_i(x_1, \cdots, x_n)$ is organized as follows

$$y_i = p_i(x_1, \cdots, x_n) = \sum_{1 \le j \le k \le n} a_{ijk} x_j x_k + \sum_{j=1}^{n} b_{ij} x_j + c_i,$$

where $x_i \in \mathbb{F}_q, 1 \le i \le n$, and coefficients $a_{ijk}, b_{ij}, c_i \in \mathbb{F}_q$.

The construction of MPKCs is mainly based on the hardness of Multivariate Quadratic (MQ) problem and Isomorphism of Polynomials (IP) problem.

The trapdoor of MPKCs $P = (p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n))$ is constructed as follows:

$$\begin{aligned} u &= (u_1, \cdots, u_n) \\ &\downarrow S \\ x &= (x_1, \cdots, x_n) \\ &\downarrow Q \\ y &= (y_1, \cdots, y_m) \\ &\downarrow T \\ v &= (v_1, \cdots, v_m). \end{aligned}$$

The public key P consists of three maps, i.e.,$P = T \circ Q \circ S$, where $S : u \to x = M_S u + c_S$ and $T : y \to v = M_T y + c_T$ are random invertible affine maps in $\mathbb{F}^n$ and $\mathbb{F}^m$ respectively. They mask the structure of the central map together, and are important parts of the secret key.

2.2 EMC

In 2011, by combining the hash authentication technique with traditional multivariate public key algorithm, Wang Hou-zhen et al proposed Extended Multivariate Public Key Cryptosystem (EMC). It can be used as a signature scheme and an encryption scheme simultaneously. It was an essential expansion of traditional multivariate public key cryptography, and it improved security of the traditional MPKCs [20].

Tame transformation is used to construct EMC. Define tame transformation first.

Definition 1 (Tame Transformation)**.** *Tame transformation is a special mapping* $G : GF(q)^n \to GF(q)^n$

$$\begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-1} \\ t_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 + g_2(x_1) \\ \vdots \\ x_{n-1} + g_{n-2}(x_1, \cdots, x_{n-2}) \\ x_n + g_{n-1}(x_1, \cdots, x_{n-1}) \end{pmatrix}$$

where g_i *are arbitrary quadratic polynomials. The mapping* G *is so special that it can be easily inverted.*

Definition 2 (Hash-based Transformation)**.** *A Hash-based Transformation (HT)* $L : \mathbb{F}_q^n \to \mathbb{F}_q^n$

$$\begin{cases} \begin{pmatrix} y_1 \\ \vdots \\ y_{n-\delta} \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_1 \\ \begin{pmatrix} y_{n-\delta+1} \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_{n-\delta+1} \\ \vdots \\ x_n \end{pmatrix} + D \cdot \begin{pmatrix} x_{n+1} \\ \vdots \\ x_{n+\delta} \end{pmatrix} + \\ B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_2 \end{cases}$$

where α_1, α_2 *are* $(n-\delta)$*-dimension vector and* δ*-dimension vector respectively,* A *is a* $(n-\delta) \times (n-\delta)$ *matrix, and* D *must be a diagonal and full-rank* $\delta \times \delta$ *matrix;* B *is a random* $\delta \times (n-\delta)$ *matrix; all the coefficients are chosen over* $\mathbb{F}_q$*. The extended variables* $x_{n+i} (1 \le i \le \delta)$ *are defined by* $x_{n+i} = H_k(x_1 || x_2 || \cdots || x_{n-\delta+i-1})$.

Known from the definition above, L can be seen as a compression mapping from $\mathbb{F}_q^{n+\delta}$ to $\mathbb{F}_q^n$, i.e.,$(y_1, \cdots, y_n) = L(x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+\delta})$.

The public key of the extended MQ cryptosystem is designed as follows:

$$P' = P \circ L = T \circ F \circ U \circ L = (p_1', \cdots, p_n').$$

The public key is a set of multivariate quadratic polynomials, which is a mapping from $\mathbb{F}_q^{n+\delta}$ to $\mathbb{F}_q^n$, and the corresponding secret key consists of $L^{-1}, U^{-1}, T^{-1}, F^{-1}$.

2.3 MI Scheme

In 1988, Matsumoto and Imai proposed the first multivariate public key cryptosystem, i.e., MI scheme [11].

Let $k = \mathbb{F}_q$ be a finite field of characteristic 2, where $q = 2^m$, and K be an extension field of degree n of K. Then define a standard K-linear isomorphism map $\Phi : K \to k^n$,$\Phi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, \cdots, a_{n-1})$.Define $F : K \to K, F(X) = X^{1+q^\theta}$, where θ is an integer such that $1 \le \theta \le n$ and $gcd(1 + q^\theta, q^n - 1) = 1$. F is an invertible map and its inverse is given by $F^{-1}(X) = X^t$, where $t(1 + q^\theta) \equiv 1 mod(q^n - 1)$. Let $\overline{F} : k^n \to k^n$ be a central map:

$$\begin{aligned} \bar{F}(x_1, \cdots, x_n) &= \phi \circ F \circ \phi^{-1}(x_1, \cdots, x_n) \\ &= (\bar{F}_1(x_1, \cdots, x_n), \cdots, \bar{F}_n(x_1, \cdots, x_n)) \end{aligned}$$

where $\overline{F}_i(x_1, \cdots, x_n)$ are quadratic polynomials of n variables.

Finally, let L_1 and L_2 be two randomly chosen invertible affine linear maps over k^n.

$\hat{F}(x_1, \cdots, x_n) = L_1 \circ \overline{F} \circ L_2(x_1, \cdots, x_n) = (\hat{F}_1(x_1, \cdots, x_n), \cdots, \hat{F}_n(x_1, \cdots, x_n))$ is the ciphertext suggested by MI scheme. The public key is $\hat{F}(x_1, \cdots, x_n)$, and the secret key is $(L_1^{-1}, L_2^{-1}, \theta)$.

3 Design of the Novel EMCs

Nowadays most algorithms of MPKCs cannot be a signature scheme and an encryption scheme simultaneously and most of them are under attack. How to construct a secure and efficient MPKC enabling both signature and encryption remain a hot topic and an open problem.

The key of our proposed cryptosystems is to build a nonlinear and invertible transformation L. By making use of the idea of EMC and incorporating MI scheme with nonlinear invertible transformations L, the novel EMCs are produced:

$$\begin{aligned} \tilde{F}(x_1, \cdots, x_n) &= \hat{F} \circ L(x_1, \cdots, x_n) \\ &= L_1 \circ \bar{F} \circ L_2 \circ L(x_1, \cdots, x_n) \quad (1) \end{aligned}$$

3.1 Construction of L

Constructing nonlinear and invertible transformations L is the key to design the novel EMCs. Three kinds of nonlinear and invertible transformations will be introduced based on different ideas below.

3.1.1 Construction of Invertible Transformation Based on "Invertible Cycle"

Assume the invertible transformation is L_3, in order to facilitate the inverse, L_3 is defined in cases. Suppose the order is n, to express properly the successor of $\{1, \cdots, n\}$, define

$$\mu : \{1, \cdots, n\} \to \{1, \cdots, n\} : \mu(i) = \begin{cases} 1 & \text{for } i = n \\ i+1 & \text{otherwise} \end{cases}$$

Lemma 1. *For a fixed integer $n \geq 2$, define a nonlinear transformation $L_3 : (x_1, \cdots, x_n) \to (t_1, \cdots, t_n)$ as follows:*

$$\begin{cases} t_1 := \begin{cases} c_1 x_1 x_2 & for\ n\ odd \\ c_1 x_1{}^q x_2 & for\ n\ even \end{cases} \\ t_i := c_i x_i x_{\mu(i)} \quad for\ \ 2 \leqslant i \leqslant n \end{cases},$$

Then the inverse image of $(t_1, \cdots, t_n)$, where $t_i \in \mathbb{F}_q^* := \mathbb{F}_q \backslash \{0\}$, $\forall i$ is given by

$$\begin{cases} x_1 := \begin{cases} \sqrt{\frac{\prod_{i=0}^{(n-1)/2} t_{2i+1}}{\prod_{i=1}^{(n-1)/2} t_{2i}}} \cdot \sqrt{\frac{\prod_{i=1}^{(n-1)/2} c_{2i}}{\prod_{i=0}^{(n-1)/2} c_{2i+1}}} & for\ n\ odd \\ \sqrt[q-1]{\frac{\prod_{i=0}^{n/2-1} t_{2i+1}}{\prod_{i=1}^{n/2} t_{2i}}} \cdot \sqrt[q-1]{\frac{\prod_{i=1}^{n/2} c_{2i}}{\prod_{i=0}^{n/2-1} c_{2i+1}}} & for\ n\ even \end{cases} \\ x_i := \frac{t_i}{c_i x_{\mu(i)}} \quad for\ \ i = n\ ,\ \cdots\ ,\ 2. \end{cases}$$

Remark 1. *However, for some $x_i = 0$ in the set $\{x_1, \cdots, x_n\}$, the definition of L_3 is the same as that of Lemma 1, so the conditions $t_i = 0$ and $t_{i+1} = 0$ are set up. Take odd n for example, the inverse of L_3, i.e., $(x_1, \cdots, x_n) = L_3^{-1}(t_1, \cdots, t_n)$ is organized as follows:*

Either $x_i = 0$ or $x_{\mu(i)} = 0$ is set up, where $t_i = 0$.

1) For $x_i = 0$, choose $x_{\mu(i)} = a \in \mathbb{F}_q \backslash \{0\}$ randomly, and other x_i can be worked out in sequence:

$$\begin{cases} x_{\mu(i)+1} = \frac{t_{\mu(i)}}{c_{\mu(i)}\ a}\ ,\ \cdots\ ,\ x_n = \frac{t_{n-1}}{c_{n-1}\ x_{n-1}} \quad for\ \ i = 1, \\ x_{\mu(i)+1} = \frac{t_{\mu(i)}}{c_{\mu(i)}\ a}\ ,\ \cdots\ ,\ x_n = \frac{t_{n-1}}{c_{n-1}\ x_{n-1}}\ ,\ x_1 = \frac{t_n}{c_n\ x_n} \\ \qquad\qquad for\ \ i = 2, \\ x_{\mu(i)+1} = \frac{t_{\mu(i)}}{c_{\mu(i)}\ a}\ ,\ \cdots\ ,\ x_n = \frac{t_{n-1}}{c_{n-1}\ x_{n-1}}\ ,\ x_1 = \frac{t_n}{c_n\ x_n} \\ \qquad \cdots\ ,\ x_{i-1} = \frac{t_{i-2}}{c_{i-2}\ x_{i-2}} \quad for\ i = 3\ ,\ \cdots\ ,\ n. \end{cases}$$

2) For $x_{\mu(i)} = 0$, choose $x_i = b \in \mathbb{F}_q \backslash \{0\}$ randomly, and other x_i can be calculated in sequence:

$$\begin{cases} x_{i-1} = \frac{t_{i-1}}{c_{i-1}\ b}\ ,\ \cdots\ ,\ x_1 = \frac{t_1}{c_1\ x_2}\ ,\ \cdots\ ,\ x_{\mu(i)+1} = \\ \qquad \frac{t_{\mu(i)+1}}{c_{\mu(i)+1}\ x_{\mu(i)+2}} \quad for\ \ i = n\ ,\ n-1\ ,\ \cdots\ ,\ 2, \\ x_n = \frac{t_n}{c_n\ b}\ ,\ x_{n-1} = \frac{t_{n-1}}{c_{n-1}\ x_n} \quad \cdots\ ,\ x_{\mu(i)+1} = \\ \qquad \frac{t_{\mu(i)+1}}{c_{\mu(i)+1}\ x_{\mu(i)+2}} \quad for\ \ i = 1. \end{cases}$$

3) For $x_i = 0$ and $x_{\mu(i)} = 0$, choose $x_{\mu(i)+1} = c \in \mathbb{F}_q \backslash \{0\}$ randomly, and do the following work:

$$\begin{cases} x_{\mu(i)+2} = \frac{t_{\mu(i)+1}}{c_{\mu(i)+1}\ c}\ ,\ \cdots\ ,\ x_n = \frac{t_{n-1}}{c_{n-1}\ x_{n-1}} \quad for\ \ i = 1, \\ x_{\mu(i)+2} = \frac{t_{\mu(i)+1}}{c_{\mu(i)+1}\ c}\ ,\ \cdots\ ,\ x_n = \frac{t_{n-1}}{c_{n-1}\ x_{n-1}}\ ,\ x_1 = \\ \qquad\qquad \frac{t_n}{c_n\ x_n} \quad for\ \ i = 2, \\ x_{\mu(i)+2} = \frac{t_{\mu(i)+1}}{c_{\mu(i)+1}\ c}\ ,\ \cdots\ ,\ x_n = \frac{t_{n-1}}{c_{n-1}\ x_{n-1}}\ ,\ x_1 = \\ \frac{t_n}{c_n\ x_n}\ ,\ \cdots\ ,\ x_{i-1} = \frac{t_{i-2}}{c_{i-2}\ x_{i-2}} \quad for\ \ i = 3\ ,\ \cdots\ ,\ n. \end{cases}$$

From the discussions above, it can be seen that if there exists a singularity, i.e.,$\{x_1, \cdots, x_n\}$ such that

$\{x_1, \cdots, x_n | x_1 = 0 \vee \cdots \vee x_n = 0\}$, *there must be some* $t_i = 0$. *In this situation, the inverse image of* $\{t_1, \cdots, t_n\}$ *is multiple, and the checksum need to be estimated. As the number of singularities is* $q^n - (q-1)^n$, *the probability of the existence of a singularity is* $p_1 = 1 - \frac{(q-1)^n}{q^n}$, *where* $q = 2^m$. *Proper parameters can guarantee that the probability is small enough and improve the decryption efficiency. Under the parameters* $m = 12, n = 28$, *the probability is* $p_1 = 0.007$; $p_2 = 0.002$, *for* $m = 14, n = 28$; $p_1 = 0.0005$, *for* $m = 16, n = 27$, *so the parameters* $m = 16, n = 27$ *are recommended.*

3.1.2 Construction of Invertible Transformation based on Tame Transformation

Lemma 2. *Suppose the invertible transformation to construct is* L_4. *Choose positive integers* n, d *such that* $n > 2d$, *and define the invertible transformation based on tame transformation* $L_4 : (x_1, \cdots, x_n) \to (t_1, \cdots, t_n)$

$$\begin{cases} t_1 = x_1 + x_{d+1}x_n \\ t_2 = x_2 + x_{d+2}x_{n-1} \\ \vdots \\ t_d = x_d + x_{2d}x_{n-d+1} \\ t_{d+1} = x_{d+1} \\ \vdots \\ t_n = x_n. \end{cases}$$

Then the inverse image of $(t_1, \cdots, t_n)$, *i.e.,* $L_4^{-1}(t_1, \cdots, t_n) = (x_1, \cdots, x_n)$ *is given by*

$$\begin{cases} x_1 = t_1 + t_{d+1}t_n \\ x_2 = t_2 + t_{d+2}t_{n-1} \\ \vdots \\ x_d = t_d + t_{2d}t_{n-d+1} \\ x_{d+1} = t_{d+1} \\ \vdots \\ x_n = t_n. \end{cases}$$

3.1.3 Construction of Invertible Transformation based on "Special Oil and Vinegar"

Suppose the invertible transformation to construct is L_5, and choose positive integers o, v and n such that $o > v$ and $n = o + v$. Divide the variables $\{x_1, \cdots, x_n\}$ into two parts:$\{x_1, \cdots, x_v, \cdots, x_o\}$ and $\{x_{o+1}, \cdots, x_n\}$.

Lemma 3. *Randomly choose* $r_i \in \mathbb{F}_q$, $i = 1, \cdots, n$ *and define* $L_5(x_1, \cdots, x_n) = (t_1, \cdots, t_n)$ *as follows:*

$$\begin{cases} t_1 = x_1 \\ \vdots \\ t_v = x_v \\ \vdots \\ t_o = x_o \\ t_{o+1} = \frac{(x_1 + r_1)}{x_{o+1}} \\ \vdots \\ t_n = \frac{(x_v + r_v)}{x_n} \end{cases}$$

where variables $(t_1, \cdots, t_o)$ *containing the first degree parts can be seen as "oil variables"; and variables* $(t_{o+1}, \cdots, t_n)$ *containing the quadratic parts can be seen as "vinegar variables".*

Then the inverse image of $(t_1, \cdots, t_n)$, *i.e.,* $L_5^{-1}(t_1, \cdots, t_n) = (x_1, \cdots, x_n)$, *where* $t_i \in \mathbb{F}_q^* := \mathbb{F}_q \backslash \{0\}$, $i = o+1, \cdots, n$ *is given by*

$$\begin{cases} x_1 = t_1 \\ \vdots \\ x_v = t_v \\ \vdots \\ x_o = t_o \\ x_{o+1} = \frac{t_{o+1}}{(t_1 + r_1)} \\ \vdots \\ x_n = \frac{t_n}{(t_v + r_v)}. \end{cases}$$

Remark 2. *For some* $t_i = 0, i = o+1, \cdots, n$, *the inverse image of* $(t_1, \cdots, t_n)$, *i.e.,*$L_5^{-1}(t_1, \cdots, t_n) = (x_1, \cdots, x_n)$ *is obtained as follows.*

For some $t_i = 0$, *either* $x_i = 0$ *or* $x_{i-o} + r_{i-o} = 0$ *is set up. If* $x_{i-o} + r_{i-o} = 0$, *choose* $x_i \in \mathbb{F}_q$, *and solve* $(x_1, \cdots, x_n)$ *from* $(t_1, \cdots, t_n)$ *directly, otherwise, utilize Lemma 3.1.1.*

In conclusion, the existence of $t_i = 0$ *makes the solution* $(x_1, \cdots, x_n)$ *not unique, the checksum need to be calculated. Similar to Section 3.1.1, the probability of the existence of a singularity is* $p_2 = 1 - \frac{(q-1)^n}{q^n}$, *so it can lower the probability, and improve the decryption efficiency by choosing proper parameters. For* $m = 16, n = 27$, *the probability is* $p_2 = 0.0005$, *so the parameters* $m = 16, n = 27$ *are proper.*

3.2 Construction of Three Kinds of EMCs

By using the idea "function composition", and combining MI scheme with those nonlinear invertible transformations L_i in Section 3.1, the public key polynomials of the novel EMCs are deduced as follows:

$$\begin{aligned} &\tilde{F}_i(x_1, \cdots, x_n) = L_1 \circ \bar{F} \circ L_2 \circ L_i(x_1, \cdots, x_n) \\ &= (\tilde{F}_{i1}(x_1, \cdots, x_n), \cdots, \tilde{F}_{in}(x_1, \cdots, x_n)), \\ &\qquad\qquad i = 3, 4, 5 \end{aligned} .$$

Conversely, the secret keys consist of $(L_1^{-1}, L_2^{-1}, L_i^{-1}, \theta), i = 3, 4, 5$.

3.3 Encryption Algorithms

It can be seen that the secret keys of encryption algorithms are $D = (L_1^{-1}, L_2^{-1}, L_i^{-1}, \theta), i = 3, 4, 5$ from the construction process of the novel EMCs.

According to the construction of nonlinear transformation L in Section 3.1, when there exists a singularity $\{t_1, \cdots, t_n | t_1 = 0 \vee \cdots \vee t_n = 0\}$, the inverse images of $(t_1, \cdots, t_n) : L_3^{-1}(t_1, \cdots, t_n)$ and $L_5^{-1}(t_1, \cdots, t_n)$ can be multiple. Therefore, the encryption process and the decryption process will be discussed in two cases.

1) When there does not exist a singularity, the solution of $L_i^{-1}(t_1, \cdots, t_n)$ is unique.

   The encryption process. Given the plaintext $(x_1, \cdots, x_n) \in \mathbb{F}_q^n$, use the public key $\tilde{F}_i$ to calculate the ciphertext $(y_1, \cdots, y_n) = \tilde{F}_i(x_1, \cdots, x_n)$.

   The decryption process. Received the ciphertext $(y_1, \cdots, y_n) \in \mathbb{F}_q^n$, calculate the corresponding plaintext $(x_1, \cdots, x_n)$ as follows:

   a. Compute $(y_1^{'}, \cdots, y_n^{'}) = L_1^{-1}(y_1, \cdots, y_n)$;
   b. Use the secret key θ to get the inverse transformation of the central map $\bar{F}$, i.e., $(x_1^{'}, \cdots, x_n^{'}) = \bar{F}^{-1}(y_1^{'}, \cdots, y_n^{'})$;
   c. Compute $(t_1, \cdots, t_n) = L_2^{-1}(x_1^{'}, \cdots, x_n^{'})$;
   d. Finally, compute the corresponding plaintext $(x_1, \cdots, x_n) = L_i^{-1}(t_1, \cdots, t_n)$.

2) When there exists a singularity, i.e., the solution of $L_i^{-1}(t_1, \cdots, t_n)$ isn't unique.

   The encryption process. Given the plaintext $(x_1, \cdots, x_n) \in \mathbb{F}_q^n$, use the public key $\tilde{F}_i$ to calculate the corresponding ciphertext $(y_1, \cdots, y_n) = \tilde{F}_i(x_1, \cdots, x_n)$. Meanwhile, utilize the public hash function $Hash_1$ to calculate the checksum of plaintext $Hash_1(x_1, \cdots, x_n) = v$.

   The decryption process. Received the ciphertext $(y_1, \cdots, y_n) \in \mathbb{F}_q^n$ and the checksum $Hash_1(x_1, \cdots, x_n) = v$, the plaintext can be obtained as follows:

   a. Compute $(y_1^{'}, \cdots, y_n^{'}) = L_1^{-1}(y_1, \cdots, y_n)$;
   b. Use the secret key θ to get the inverse transformation of the central map $\bar{F}$, i.e., $(x_1^{'}, \cdots, x_n^{'}) = \bar{F}^{-1}(y_1^{'}, \cdots, y_n^{'})$;
   c. Compute $(t_1, \cdots, t_n) = L_2^{-1}(x_1^{'}, \cdots, x_n^{'})$;
   d. Use the secret key L_i^{-1} to get $(\bar{x}_1, \cdots, \bar{x}_n) = L_i^{-1}(t_1, \cdots, t_n)$,and compute $Hash_1(\bar{x}_1, \cdots, \bar{x}_n) = v^{'}$. If $v = v^{'}$, the corresponding solution $(\bar{x}_1, \cdots, \bar{x}_n)$ is the right plaintext, otherwise, discard the solution $(\bar{x}_1, \cdots, \bar{x}_n)$.

3.4 Signature Algorithms

The signature process. Suppose that the message M is the document to sign, and compute $(y_1, \cdots, y_n) = Hash_2(M)$. The secret keys of signature algorithms are the same as those of encryption algorithms, so are the process of calculating the signature $(x_1, \cdots, x_n)$ and the encryption process in Section 3.3. The difference is that whether there exists a singularity. When the signature isn't unique, choose one of the signatures randomly.

The verification process. Received the message M and signature $(x_1, \cdots, x_n)$, do the verification as follows:

1) Use another public Hash function $Hash_2$ to compute $Hash_2(M) = (y_1, \cdots, y_n)$;
2) Compute $\tilde{F}(x_1, \cdots, x_n) = (y_1^{'}, \cdots, y_n^{'})$, then determine whether the condition $(y_1^{'}, \cdots, y_n^{'}) = (y_1, \cdots, y_n)$ is true, otherwise, discard the invalid signature.

4 Operation Efficiency and Security Analysis

The operation efficiency and the security analysis of three novel EMCs will be given in the next installment.

4.1 Operation Efficiency

Encryption (verification) efficiency. Compared to the encryption (verification) efficiency of the MI scheme, the novel EMCs need simply do another operation L_i, $i = 1, 2, 3$. It can be seen that their efficiencies are high, and barely affect the whole efficiency of our proposed cryptosystem from the construction of L_i in Section 3.1.

Decryption (signature) efficiency. During the decryption process, when there exists a singularity, the solution isn't unique, and the verification need to be done many times. But the existence of a singularity can be avoided by choosing the proper parameters. During the signature process, just choose one of the solutions.

Above all, under the proper parameters, the three novel EMCs inherit high efficiency of MI, and the whole operation efficiency keeps high.

4.2 Security Analysis

Generally, attacks aimed at MPKCs are divided into two groups: structure-based attack and direct attack. Structure-based attack aims at the special structure of MPKCs, and it mainly includes linearization attack and differential attack. Direct attack starts with the public key polynomials of MPKCs. The common tools are comprised of the *Gröbner* base algorithm and the XL algorithm. Next, the security analysis of three EMCs will be performed. To keep it simple, take the EMC based on invertible cycle for example.

4.2.1 Linearization Attack

In 1995, Patarin present a linearization attack to the MI scheme, which simplified linear equations and posed threat to MI [12]. Next, it will be demonstrated that our proposed cryptosystem can be resistant against linearization attack.

Definition 3. *Let $P = (p_1, \cdots, p_m)$ be polynomials with n variables over F_q,with regard to P, a linearization equation is organized as*

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_i y_j + \sum_{i=1}^{n} b_i x_i + \sum_{i=1}^{m} c_i y_i + d \in \mathbb{F}_q[x_1\ ,\ \cdots\ ,\ x_n\ ,\ y_1\ ,\ \cdots\ ,\ y_m]$$

s.t. when plugging p_i into y_i, a zero polynomial about $(x_1, \cdots, x_n)$ the variable are obtained:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_i p_j + \sum_{i=1}^{n} b_i x_i + \sum_{i=1}^{m} c_i p_i + d = 0.$$

According to the central map of MI $F : X \mapsto X^{q^\theta+1}$, the following special algebraic relation:$Y^{q^\theta-1} = X^{q^{2\theta}-1}$. Multiply XY on both sides of the relation to acquire the relation: $XY^{q^\theta} = YX^{q^{2\theta}}$.

Further, it can be easy to obtain n multivariate quadratic equations over F_q by the isomorphic mapping ϕ. Each equation is organized as follows:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i y_j + \sum_{i=1}^{n} b_i x_i + \sum_{i=1}^{n} c_i y_i + d = 0 \qquad (2)$$

Given $O((n+1)^2)$ plaintext-ciphertext pairs $(x_1, \cdots, x_n, y_1, \cdots, y_n)$, it is feasible to work out the coefficients of the equation above. Once worked out all the coefficients and given the ciphertext $y = (y_1, \cdots, y_n)$, n linear equations about the plaintext $x = (x_1, \cdots, x_n)$ can be obtained.

Theorem 1. *The EMC based on invertible cycle puts forward the nonlinear invertible transformation L_3, s.t. the structure of public key polynomial will be changed to resist linearization attack.*

Proof. Similar to MI scheme, n multivariate quadratic equations of our proposed cryptosystem can be obtained, and each equation is organized as follows:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}t_i y_j + \sum_{i=1}^{n} b_i t_i + \sum_{i=1}^{n} c_i y_i + d = 0 \qquad (3)$$

If given $O((n+1)^2)$ plaintext-ciphertext pairs $(t_1, \cdots, t_n, y_1, \cdots, y_n)$, the coefficients of the equations above can be calculated. However, since the ciphertext $(y_1, \cdots, y_n)$ is known, and the intermediate variables $(t_1, \cdots, t_n)$ remain unknown, the coefficients cannot be calculated when plugging the ciphertext $(y_1, \cdots, y_n)$ into the equation. In the worst case that all the coefficients are calculated, linear equations about t_i can be obtained by plugging $(y_1, \cdots, y_n)$ to Equation (3).

After plugging the expression of t_i, multivariate quadratic equations about $(x_1, \cdots, x_n)$ will be derived. Solving this kind of equation is still a NP problem, so it can be concluded that: our proposed cryptosystem is resistant against linearization attack.

4.2.2 Differential Attack

Differential attack aims at the type such as MI scheme. Initially, it was used to attack PMI [5], and it was also used to attack the SFLASH cryptosystem, i.e.,C^*- scheme later [8]. Next, it will be proved that the novel cryptosystem can resist differential attack.

Definition 4. *For any function $F(x)$, its differential at point F_{q^θ} is defined by $DF(a, x)$:*

$$DF(a, x) = F(x + a) - F(x) - F(a) + F(0).$$

When F is a quadratic function, if regard $DF(a, x)$ as a function of variables x and a, $DF(a, x)$ is a symmetric bilinear function about x and a.

In MI scheme, the inner function is $\tilde{F}(x) = x^{1+q^\theta}$, so $D\tilde{F}(a, x) = xa^{q^\theta} + ax^{q^\theta}$. Obviously, is symmetric bilinear., the differential function has a very specific multiplicative property:

$$D\bar{F}(a\ ,\ \xi \cdot x) + D\bar{F}(\xi \cdot a\ ,\ x) = (\xi + \xi^{q^\theta})D\bar{F}(a\ ,\ x) \qquad (4)$$

Similarly, the differential function of public key $P = L_1 \circ \bar{F} \circ L_2$ is $DP(a, x) = T \circ DF(U(a), U(x))$, which satisfies the following relation:

$$\begin{aligned} & DP(\xi a\ ,\ x) + DP(a\ ,\ \xi x) \\ = \ & L_1 \circ D\bar{F}(\xi \cdot L_2(a)\ ,\ L_2(x)) \\ & \quad + \ L_1 \circ D\bar{F}(L_2(a)\ ,\ \xi \cdot L_2(x)) \\ = \ & L_1 \circ (\xi + \xi^{q^\theta}) \circ {L_1}^{-1} \circ DP(a\ ,\ x) \end{aligned} \qquad (5)$$

Let $P_\Pi = T_\Pi \circ \bar{F} \circ L_2$ be the public key of the C^{*-} scheme. It is entirely feasible to find the non-trivial map N_ξ such that

$$P'_\Pi = P_\Pi \circ N_\xi = T_\Pi \circ M_\xi \circ \bar{F} \circ L_2 \qquad (6)$$

where N_ξ and M_ξ denote two linear maps with regard to ξ.

Therefore, a new MI public key can be obtained by comprising r equations randomly chosen from P'_Π with $(n-r)$ equations of the public key, and the probability of success is $1 - 1/q$. Then make use of linearization attack above to forge the signature.

Theorem 2. *The EMC based on invertible cycle utilizes the idea function composition and adds the nonlinear transformation L_3 to the MI scheme, therefore, it can break the special multiplicative property of MI and avoid differential attack.*

Proof. Relative to MI scheme, the public key of the novel EMC is transformed from P to $P^{'}$,

$$P^{'} = L_1 \circ \bar{F} \circ L_2 \circ L_3 \ \underline{L^{'}{}_2 = L_2 \circ L_3} \ L_1 \circ \bar{F} \circ L^{'}{}_2 \tag{7}$$

Since L_3 is a nonlinear transformation, $L^{'}{}_2$ in Relation (7) is also a nonlinear transformation.$\forall x \ , \ \xi \in GF(q^n)$, there obviously exists the following relation:

$$\xi \circ L^{'}{}_2(x) \neq L^{'}{}_2(\xi x) \tag{8}$$

To the novel EMC, the differential function of public key $P^{'} = L_1 \circ \bar{F} \circ L^{'}{}_2$ is

$$\begin{aligned} & DP^{'}(\xi a \ , \ x) + DP^{'}(a \ , \ \xi x) \\ = \ & L_1 \circ D\bar{F}(\xi \cdot L^{'}{}_2(a) \ , \ L^{'}{}_2(x)) + \\ & \quad L_1 \circ D\bar{F}(L^{'}{}_2(a) \ , \ \xi \cdot L^{'}{}_2(x)) \\ \neq \ & L_1 \circ (\xi + \xi^{q^\theta}) \circ {L_1}^{-1} \circ (DP^{'}(a \ , \ x) \ ) \end{aligned} \tag{9}$$

Expression (9) shows that the introduction of the transformation L_3 breaks the special multiplicative property of MI scheme.

In conclusion, our proposed cryptosystem can resist differential attack.

4.2.3 Algebraic Attack

The common tools of algebraic attack consist of the *Gröbner* base algorithm and the XL algorithm. So far, the most efficient methods to computer *Gröbner* bases are F4 and F5 algorithms.

According to the relations of the number of equations m and the number of variables n, and algebraic attack in three cases are discussed: $m > n$, $m < n$, and m=n. The equations satisfying the relation $m > n$ are called overdetermined equations [1], when $m < n$, underdetermined equations [18], and when m=n, permutation equations [21]. In our cryptosystem, the public key polynomial $P(x_1 \ , \ \cdots \ , \ x_n) = (y_1 \ , \ \cdots \ , \ y_n)$ satisfies the relation m=n. Therefore, the cases $m > n$ and $m < n$ are described no longer.

To the best of our knowledge, when $K = GF(q)$ ($q \neq 2$) is big, and m=n, the complexity to solve the permutation equations is proved to be $O(2^{3m})$ [21].

In the novel cryptosystem, the corresponding equations are expressed as follows:

$$\begin{cases} p_1(x_1 \ , \ \cdots \ , \ x_n) = y_1 \\ \qquad \vdots \\ p_n(x_1 \ , \ \cdots \ , \ x_n) = y_n \end{cases} \tag{10}$$

where the number of equations is equal to the number of variables. According to Section 4.1.1, the public key $p_i(x_1 \ , \ \cdots \ , \ x_n)$ is multivariate quartic polynomial. The complexity to solve Equation (10) is much greater than the corresponding quadratic equations. Under the recommended parameters n=27 and $q = 2^{16}$, the complexity to solve multivariate quadratic equations is about $O(2^{81})$, therefore, the complexity to solve the public key polynomials of the novel EMC is more than $O(2^{81})$, that is, our proposed cryptosystem can be resistant against algebraic attack.

All in all, from Sections 4.2.1, 4.2.2, and 4.2.3, it can be concluded that the EMC based on invertible cycle can resist linearization attack, differential attack and algebraic attack. Similarly, the EMC based on tame transformation and the EMC based on special oil and vinegar are also secure, and detailed proofs are not given here.

5 Conclusions

In this paper, three different nonlinear invertible transformations are put forward. Incorporated with MI scheme, three novel EMCs are recommended. Next, the corresponding encryption and signature algorithms are provided. Finally, the operation analyses and security analyses of three novel cryptosystems are implemented. It can be demonstrated that our proposed cryptosystems can resist linearization attack, differential attack, and algebraic attack. Whether there is a new attack to our novel EMCs and the selection and optimized implementation of concrete parameters need further research.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (61003291).

References

[1] M. R. Albrecht, C. Cid, J. C. Faugere, and et al, "On the relation between the MXL family of algorithms and groebner basis algorithms," *Journal of Symbolic Computation*, vol. 47, no. 8, pp. 926–941, 2012.

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-quantum Cryptography*, Berlin: Springer Heidelberg, 2009.

[3] C. L. Clough and J. Ding, "Secure variables of the square encryption scheme," in *Post-quantum cryptography*, pp. 153–164, Springer Berlin Heidelberg, 2010.

[4] J. Ding, "A new variant of the Matsumoto-Imai cryptosystem through perturbation," in *Public Key Cryptography (PKC'04)*, pp. 305–318, Springer Berlin Heidelberg, 2004.

[5] J. Ding and J. E. Gower, "Inoculating multivariate schemes against differential attacks," in *Public Key Cryptography (PKC'06)*, pp. 290–301, Springer Berlin Heidelberg, 2006.

[6] J. Ding, C. Wolf, and B. Yang, "Invertible cycles for multivariate quadratic (MQ) public key cryptography," in *PKC'07*, pp. 266–281, Beijing, China, 2007.

[7] J. T. Ding and B. Y. Yang, *Multivariate Public Key Cryptography*, Berlin: Springer Heidelberg, 2009.

[8] V. Dubois, P. A. Fouque, and J. Stern, "Cryptanalysis of sflash with slightly modified parameters," in *Advances in Cryptology (Eurocrypt'07)*, pp. 264–275, Springer Berlin Heidelberg, 2007.

[9] D. S. A. Elminaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," *International Journal of Network Security*, vol. 10, no. 3, pp. 216–222, 2010.

[10] X. Q. Fu, W. S. Bao, and C. Zhou, "Speeding up implementation for shor factorization quantum," *Chinese Sci Bull*, vol. 55, no. 4-5, pp. 322–327, 2010.

[11] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature verification and message-encryption," in *Advances in Cryptology (Eurocrypt'88)*, pp. 419–453, Springer Berlin Heidelberg, 1988.

[12] J. Patarin, "Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt '88," in *Advances in Cryptology (Crypto'95)*, pp. 248–261, Springer Berlin Heidelberg, 1995.

[13] J. Patarin, N. Courtois, and L. Goubin, "Flash, a fast multivariate signature algorithm," in *Topics in Cryptology (T-RSA'01)*, pp. 298–307, Springer Berlin Heidelberg, 2001.

[14] A. Petzoldt, S. Bulygin, and J. Buchmann, "Cyclicrainbow - a multivariate signature scheme with a partially cyclic public key," in *Progress in Cryptology (Indocrypt'10)*, pp. 33–48, Hyderabad, India, 2010.

[15] K. Sakumoto, "Public-Key identification schemes based on multivariate cubic polynomials," in *Public Key Cryptography*, pp. 172–189, Springer Berlin Heidelberg, 2012.

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

[17] S. Tang and L. Xu, "Proxy signature scheme based on isomorphisms of polynomials," in *Network and System Security*, pp. 113–125, Springer Berlin Heidelberg, 2012.

[18] E. Thomae and C. Wolf, "Solving underdetermined systems of multivariate quadratic equations revisited," in *Public Key Cryptography*, pp. 156–171, Springer Berlin Heidelberg, 2012.

[19] S. Tsujii, M. Gotaishi, K. Tadaki, and et al, "Proposal of a signature scheme based on STS trapdoor," in *Post-quantum Cryptography*, pp. 201–217, Springer Berlin Heidelberg, 2010.

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

[21] H. Wang, H. Zhang, and H. Guan, "Multivariate algebra theory and its application in cryptography," *Journal of Beijing University Technology*, vol. 36, no. 5, pp. 9–17, 2010.

[22] S. Wang, R. Ma, Y. Zhang, and et al, "Ring signature scheme based on multivariate public key cryptosystems," *Computers and Mathematics with Applications*, vol. 62, no. 10, pp. 3973–3979, 2012.

[23] C. Wolf and B. Preneel, *Taxonomy of Public Key Schemes Based on the Problem of Multivariate Quadratic Equations*, Technical Report, Cryptology ePrint Archive, Report 2005/077, Dec. 2005.

[24] G. Yang, S. Tang, and L. Yang, "A novel group signature scheme based on MPKC," in *Information Security Practice and Experience*, pp. 181–195, Springer Berlin Heidelberg, 2011.

Shuaiting Qiao received his B.S. degree in applied mathematics from the Henan university, Kaifeng,China, in 2011. He is currently pursuing his M.S degree in department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research fields include multivariate public key cryptography and information security.

Wenbao Han received his Ph.D. degree in mathematics from Sichuan University. He is currently a professor in the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research field is information security.

Yifa Li received his Ph.D. degree in applied mathematics from the Zhengzhou Information Science and Technology Institute, China.He is a associate professor in the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research field is information security.

Luyao Jiao received his B.S. degree in applied mathematics from the Henan university,Kaifeng, China, in 2010. His research field is multivariate public key cryptography.