Analysis of a Multivariate Public Key Cryptosystem and Its Application in Software Copy Protection

Ning Huang
Center of Modern Educational Technology, Gannan Normal University, Ganzhou 341000, China
Email: hngzjx@qq.com

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 software copy protection. We used our new MFE multivariate public key cryptosystem to design an algorithm of software registration, in which a given plaintext can result in multi-cipher-text.. The breaking is hard because the ciphertext is variable. The ability to withstand algebraic attacks is enhanced. The dependence of registration string on the fingerprints of machine prevents any registration string from being shared by multiple machines..**

Index Terms— **Multivariate , Public key, Software protection, Finite field**

I. Introduction

The well known public key [1] cryptography RSA [2] [3] has been widely used for decades. However,such a system based on the difficulty of factoring large numbers is being potentially threatened: In 1999, Peter Shor developed algorithms to crack integer factorization and discrete logarithm in polynomial time for a quantum computer [6]. Therefore, once the come out of quantum computers, public key cryptography based on large integer factorization and discrete logarithm will be unpractical. To solve this problem, we need to study new approaches. Among them, multivariate public key cryptosystem is a research direction [5], which uses finite field multivariable (quadratic or higher ordered) set of polynomials, as a public key cryptosystem. As early as 1986, Fell and Diffie proposed a invertible linear mapping within a simple triangle synthesis scheme [7]. Although they claimed the safety of the program, Courtois and Goubin found the method to break it with the method of minimum rank [13]; In 1988, Matsumoto and Imai designed multivariate quadratic polynomial scheme implemented via a Frobenius mapping [5]. Although this program was later denied by Patarin [8], this work led multivariate cryptography in many studies [5]. In 1995 Courtois proposed a hidden field equation method (HFE) [17], in 1997 and 1999, Patarin *et al.* proposed Oil and Vinegar [19] and Unbalanced Oil and Vinegar [10], which are suitable for the digital signature. Nevertheless Courtois *et al.* and Jean-Charles broke HFE respectively in 2001 and 2003 with the method of minimum rank [13] [18]. In 2006, Lih-Chung Wang *et al.* proposed an intermediate domain multivariate public key cryptosystem MFE (Medium-Field Multivariate Public Key Encryption) [11], which belongs to a multivariate quadratic polynomial scheme. In 2007, Zhiwei Wang *et al.* analysed and developed Lih-Chung Wang *et al.*'s programs to make the cryptosystem safer [4]. In this paper, we take Zhiwei Wang *et al.*'s scheme as a basis to design software registration scheme. Registration key security depends on the security of the encryption and decryption algorithms. The developments of Multivariate Public Key Cryptosystem inspired us to try to apply it in software copy protection. We develop software protection scheme based on multivariate public key cryptosystem from existing scheme based on RSA public key cryptosystem [12]. The rest of the paper is organized as follows. Section 2 introduces original scheme of MFE and its improvements; Section 3 designs the scheme of software copy protection based on our improved MFE; Section 4 gives experimental results and analysis of the application; Section 5 gives conclusions.

Manuscript received August 28, 2013; revised November 28, 2014; accepted December 15, 2013.
This work was supported by the fund from Natural Science of Jiangxi Province of China under Grant No.20114BAB201033.

II. Analysis of the Schemes

Preliminaries [1]: Let $\mathbb{K}$ be a finite field of characteristic 2 and $\mathbb{L}$ be its degree r extension field. Let $q = |\mathbb{K}|$, $l = |\mathbb{L}|$. In MFE and its improvement, we always identify $\mathbb{L}$ with $\mathbb{K}^r$ by a $\mathbb{K}$-linear isomorphism π: $\mathbb{L} \to \mathbb{K}^r$. Namely we take a basis of $\mathbb{L}$ over $\mathbb{K}$:$\{\theta_1, \theta_2, \cdots, \theta_r\}$ and define π by

$$\pi\left(a_1\theta_1 + \cdots + a_r\theta_r\right) = (a_1, \cdots, a_r)$$

for any $(a_1, \cdots, a_r)$. It is natural to extend π to two $\mathbb{K}$-linear isomorphisms $\pi_1 : \mathbb{L}^{12} \to \mathbb{K}^{12r}$ and $\pi_3 : \mathbb{L}^{15} \to \mathbb{K}^{15r}$.

A. The Original MFE Scheme

In Lih-Chung Wang *et al.*'s original MFE scheme [11], its encryption mapping $F : \mathbb{K}^{12r} \to \mathbb{K}^{15r}$ is a composition of three mappings ϕ_1, ϕ_2, ϕ_3.

Let

$$\begin{aligned}(x_1, \cdots, x_{12r}) &= \phi_1\left(m_1, \cdots, m_{12r}\right),\\ (y_1, \cdots, y_{15r}) &= \phi_2\left(x_1, \cdots, x_{12r}\right),\\ (z_1, \cdots, z_{15r}) &= \phi_3\left(y_1, \cdots, y_{15r}\right).\end{aligned}$$

doi:10.4304/jsw.9.8.2010-2017

,where ϕ_1 and ϕ_3 are invertible affine mappings, ϕ_2 is a central map, which is equal to $\pi_1 \circ \bar{\phi}_2 \circ \pi_3^{-1}$, ϕ_1,ϕ_2 and ϕ_3 are taken as the private key, while the expression of the mapping $(z_1, \cdots, z_{15r}) = F(m_1, \cdots, m_{12r})$ is the public key. The mapping $\bar{\phi}_2 : \mathbb{L}^{12} \to \mathbb{L}^{15}$ is defined as follows.

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

Here Q_1, Q_2,and Q_3 form a triple (Q_1, Q_2, Q_3) which is a triangular mapping from $\mathbb{K}^{3r}$ to itself, used as parameters. The encryption of MFE is the evaluation of public-key polynomials, namely given a plaintext $(m_1, \cdots, m_{12r})$,its ciphertext is

$(z_1, \cdots, z_{15r}) =$
$(F_1(m_1, \cdots, m_{12r}), \cdots, F_{15r}(m_1, \cdots, m_{12r}).$

Given a valid ciphertext $(z_1, \cdots, z_{15r})$, the decryption of the scheme is to compute the inverse mapping

$$\phi_1^{-1} \circ \pi_1 \circ \bar{\phi}_2^{-1} \circ \pi_3^{-1} \circ \phi_3^{-1}(z_1, \cdots, z_{15r}).$$

The key problem is to compute the inverse mapping $\bar{\phi}_2^{-1}$. Given known elements $Y_j \in \mathbb{L}, 1 \le j \le 15$, and agreed triple (Q_1, Q_2, Q_3) . We can restore $X_i \in \mathbb{L}, 1 \le i \le 12$, as follows.

Let

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

Then we have

$$\begin{cases} det(Z_1) = det(M_1) \cdot det(M_2); \\ det(Z_2) = det(M_1) \cdot det(M_3); \\ det(Z_3) = det(M_2) \cdot det(M_3). \end{cases} \quad (2)$$

When $det(Z_1), det(Z_2)$ and $det(Z_3)$ are all invertible, $det(M_1), det(M_2)$ and $det(M_3)$ are all invertible and can be computed from (2).Namely, we have

$$\begin{cases} det(M_1) = \sqrt{\frac{det(Z_2) \cdot det(Z_3)}{det(Z_1)}}; \\ det(M_2) = \sqrt{\frac{det(Z_1) \cdot det(Z_3)}{det(Z_2)}}; \\ det(M_3) = \sqrt{\frac{det(Z_1) \cdot det(Z_2)}{det(Z_3)}}. \end{cases} \quad (3)$$

Given the values of $det(M_1), det(M_2)$, and $det(M_3)$, we can compute from (1) the values of X_1, X_2, X_3 . In the finite field $\mathbb{L}$ of characteristic 2, we have

$$\begin{cases} X_1 = Y_1 + det(M_2) + Q_1; \\ X_2 = Y_2 + det(M_3) + Q_2; \\ X_3 = Y_3 + det(M_1) + Q_3. \end{cases} \quad (4)$$

From

$$X_1X_4 + X_2X_3 = det(M_1)$$

, we can determine X_4 .With values of $det(M_1), det(M_2)$, and $det(M_3)$, we can use the triangular form of the central map to get $X_i \in \mathbb{L}, 1 \le i \le 12$ in turn. Then we can recover the ciphertext. More details of decryption are presented in [11]. Unfortunately, this system has weakness and needs improving [5].

B. Analysis of the Improved Scheme

Zhiwei Wang *et al.* proposed an improved scheme as follows. Modify the two affine mappings, i.e. the $\mathbb{K}$-linear isomorphisms $\pi_1 : \mathbb{L}^8 \to \mathbb{K}^{8r}$ and $\pi_3 : \mathbb{L}^{10} \to \mathbb{K}^{10r}$. Modify the central mapping as follows.

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; \\ Y_2 = X_2 + X_1X_4 + X_2X_3 + Q_2; \\ Y_3 = X_1X_5 + X_2X_7; Y_4 = X_1X_6 + X_2X_8; \\ Y_5 = X_3X_5 + X_4X_7; Y_6 = X_3X_6 + X_4X_8; \\ Y_7 = X_1X_5 + X_3X_7; Y_8 = X_2X_5 + X_4X_7; \\ Y_9 = X_1X_6 + X_3X_8; Y_{10} = X_2X_6 + X_4X_8. \end{cases} \quad (5)$$

where Q_1, Q_2 are preconcerted parameters. The encryption process is the same as that of last subsection. The decryption is described as follows.

Define operator "$^{(x)}$" over 2×2 matrix ring

$$\left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{L} \right\},$$

such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{(x)} = \begin{pmatrix} a^x & b^x \\ c^x & d^x \end{pmatrix} \quad (6)$$

where $x \in \mathbb{Z}$.

Let

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix},$$
$$Z_1 = M_1^{(l)} M_2 = \begin{pmatrix} Y_3 & Y_4 \\ Y_5 & Y_6 \end{pmatrix},$$
$$Z_2 = M_2^T M_1 = \begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix} \quad (7) .$$

In the field $\mathbb{L}$,we have $X_i^l = X_i$. The decryption sequence is

$$\phi_1^{-1} \circ \pi_1 \circ \bar{\phi}_2^{-1} \circ \pi_3^{-1} \circ \phi_3^{-1}(z_1, \cdots, z_{10r})$$

. The key problem is also to compute the inverse mapping $\bar{\phi}_2^{-1}$. It follows from (7) that

$$\begin{cases} det(Z_1) = [det(M_1)]^l \cdot det(M_2); \\ det(Z_2) = det(M_1) \cdot det(M_2). \end{cases} \quad (8)$$

and

$$det(M_2) = \sqrt[l-1]{\frac{det(Z_1)}{det(Z_2)}}, det(M_1) = \frac{det(Z_2)}{det(M_2)}. \quad (9)$$

Then we can compute from (5) the values of X_1, X_2 . In the field $\mathbb{L}$ of characteristic 2, we have

$$\begin{cases} X_1 = Y_1 + det(M_2) + Q_1; \\ X_2 = Y_2 + det(M_1) + Q_2. \end{cases} \quad (10)$$

Then we can compute X_3, X_4, X_5, X_6 by solving the linear equations

$$\begin{cases} det(M_2)X_3 + Y_9X_5 + Y_7X_6 = 0; \\ det(M_2)X_4 + Y_{10}X_5 + Y_8X_6 = 0; \\ Y_4X_5 + Y_3X_6 = det(M_2)X_2; \\ X_2X_3 + X_1X_4 = det(M_1). \end{cases} \quad (11)$$

Similarly, we can compute X_7, X_8 by solving the linear equations

$$\begin{cases} Y_4X_7 + Y_3X_8 = det(M_2)X_1; \\ Y_6X_7 + Y_5X_8 = det(M_2)X_2. \end{cases} \quad (12)$$

This program withstands algebraic, rank, and XL & Gröbner attacks. Further improvements are in next subsection.

C. Further Improvements

It follows from $X_i^l = X_i$ and (8) that

$$det(M_1^{(l)}) = [det(M_1)]^l = det(M_1)$$

. In other words, we have

$$det(Z_1) = det(Z_2) = det(M_1) \cdot det(M_2)$$

, no matter what values $det(M_1)$ and $det(M_2)$ take. Formula

$$det(M_2) = \sqrt[l-1]{\frac{det(Z_1)}{det(Z_2)}}$$

is nullified because

$$\frac{det(Z_1)}{det(Z_2)} = 1$$

,where 1 is the identity element of $\mathbb{L}$. This problem is solved as follows.

Modify the two affine mappings, i.e. the $\mathbb{K}$-linear isomorphisms $\pi_1 : \mathbb{L}^8 \to \mathbb{K}^{8r}$ and $\pi_3 : \mathbb{L}^{12} \to \mathbb{K}^{12r}$. .Modify the central mapping as follows.

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1; \\ Y_2 = X_2 + X_1X_4 + X_2X_3 + Q_2; \\ Y_3 = X_1X_5 + X_2X_7; Y_4 = X_1X_6 + X_2X_8; \\ Y_5 = X_3X_5 + X_4X_7; Y_6 = X_3X_6 + X_4X_8; \\ Y_7 = X_1X_5 + X_3X_7; Y_8 = X_2X_5 + X_4X_7; \\ Y_9 = X_1X_6 + X_3X_8; Y_{10} = X_2X_6 + X_4X_{8;} \\ Y_{11} = X_5^2X_8^2 + X_6^2X_7^2; Y_{12} = \forall x \in \mathbb{L}. \end{cases} \quad (13)$$

The encryption process is the same as that of last subsection. The decryption is described as follows. Let

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

$$Z_1 = M_1M_2 = \begin{pmatrix} Y_3 & Y_4 \\ Y_5 & Y_6 \end{pmatrix},$$

$$Z_2 = M_2^T M_1 = \begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix} \quad (14)$$

Then we have

$$det(Z_1) = det(Z_2) = det(M_1) \cdot det(M_2).$$

From (13) we have $det(M_2) = \sqrt{Y_{11}}$. It follows that

$$det(M_1) = \frac{det(Z_1)}{det(M_2)} = \frac{det(Z_2)}{det(M_2)}.$$

Then we can compute from (13) the values of X_1, X_2 . In fhe field $\mathbb{L}$ of characteristic 2, we have

$$\begin{cases} X_1 = Y_1 + det(M_2) + Q_1; \\ X_2 = Y_2 + det(M_1) + Q_2. \end{cases} \quad (15)$$

Then we can solve $X_3, X_4, X_5, X_6, X_7, X_8$, in the same way as mentioned in last subsection.

Advantage of the scheme:

In (13), $x \in \mathbb{L}$ is a random value. This small change in Y_j results in big change in $z_k, 1 \leq k \leq 12r$. A plaintext can create a lot of ciphertexts. This Camouflage technique makes the system safer. The breaking is hard because the ciphertext is variable. We will show numeric experimental results later.

III. Using New Algorithm to Protect Software

Now let us see how we use our new scheme to protect software copyright by using registration system.To protect software from unauthorized use , many computer programs use registration strings. We use hard disk serial be used as fingerprint of user's hardware. Having paid the necessary fee, the user sends fingerprint relevant information to the vendor via network or another tunnel. The vendor encrypts the user's information (plaintext) into registration sting (ciphertext) and sends it back to the user. After the registration string is keyed in,verification program is invoked by the application system to check the legitimacy of the registration string. This program decrypts the ciphertext and compares it with the user's information which is relevant to the fingerprint. The successful comparison permits the user's registration and the user gets the permission to use the software. The advantage of the method is that it can prevent plagiarism of registration from any other legal user.

A. Preliminaries

Set preliminary conditions on both sides of the vendor and user:

1) A character string as a permission control string denoted by ps;

2) User's name and user's machine fingerprint denoted by $name, id$. Usually, we take hard disk serial number as the fingerprint of the user, which is grabbed automatically by user's program and send to the vender via network. The reason to use this serial number is clearly described by Monteiro and Erbacher in their paper[19];

3) The affine mappings which are used as private key comes from both user's name and user's machine fingerprint;

4) The permission string ps is the plaintext;

5) The registration string reg is the ciphertext;

6) Computations are in the finite field $\mathbb{L} = \mathbb{K}^8, \mathbb{K} = \mathbb{Z}_2 = \{0, 1\}$, such that $\mathbb{L}$ is the extended set of *ASCII*. $\forall a, b \in \mathbb{L}$, the addition is the bitwise exclusive or of a, b ; However the multiplication of a, b is isomorphic to $\mathbb{Z}_2[x]/f(x)$,where $f(x) = x^8 + x^5 + x^3 + x + 1$ is a prime polynomial over $\mathbb{Z}_2$. Details of operations of $\mathbb{Z}_2[x]/f(x)$ can be found in [14]–[16].

B. Registration string/Encryption

Input: $ps, name, id$
Output: reg
Algorithm:

Step 1 Format to length of 8, add "."s to the end if necessary ;

Step 2 Put ps into matrix U ; Create matrix A_1, C_1,where A_1 is invertible, C_1 is from $name$, Compute

$$X = A_1 U + C_1;$$

Step 3 For (13) , we compute

$$Q_1 = \left(\sum_{3|j} id[j]/0xFF \right),$$

$$Q_2 = \left(\sum_{3|j-1} id[j]/0xFF \right)$$

from id ;compute M_1, M_2, Z_1, Z_2;

Step 4 Compute Y from (13);

Step 5 Compute Matrix A_3, C_3 , where A_3 is invertible and C_3 is from id in reverse order;

Step 6 Compute

$$V = A_3 Y + C_3;$$

Step 7 Split values in V each into to parts, each part add "A" to be assured within the range from A to P;

Step 8 Add "−" between segments;

Obtain reg in the form of

$$XXXXXX-XXXXXX-XXXXXX-XXXXXX.$$

C. Verification/Decryption

Input: $name, id, reg$ in the form of

$$XXXXXX-XXXXXX-XXXXXX-XXXXXX.$$

Output: $ps = testver$
Algorithm:

Step 1 Remove "−" from reg to get V;

Step 2 Merge every two characters into a hexadecimal number;

Step 3 Compute Matrix A_3,C_3, where A_3 is invertible and C_3 is from id in reverse order;

Step 4 Compute

$$Y = A_3^{-1}(V + C_3) \quad in \quad \mathbb{L};$$

Step 5 Compute $Q_1, Q_2, det(M_2)$;
$det(Z_1), det(Z_2), det(M_1), X_1, X_2$.

Step 6 Compute X_3, X_4, X_5, X_6;
Solve matrix equation

$$S_1 X_{(3\cdots6)} =$$

$$\begin{pmatrix} det(M_2) & 00 & Y_9 & Y_7 \\ 00 & det(M_2) & Y_{10} & Y_8 \\ 00 & 00 & Y_4 & Y_3 \\ X_2 & X_1 & 00 & 00 \end{pmatrix} \begin{pmatrix} X_3 \\ X_4 \\ X_5 \\ X_6 \end{pmatrix}$$

$$= \begin{pmatrix} 00 \\ 00 \\ X_2 det(M_2) \\ det(M_2) \end{pmatrix} = T_1$$

to obtain

$$X_{(3\cdots6)} = \begin{pmatrix} X_3 \\ X_4 \\ X_5 \\ X_6 \end{pmatrix}.$$

Compute X_7, X_8. Solve matrix equation

$$S_2 X_{(7,8)} = \begin{pmatrix} Y_4 & Y_3 \\ Y_6 & Y_5 \end{pmatrix} \begin{pmatrix} X_7 \\ X_8 \end{pmatrix}$$

$$= \begin{pmatrix} X_1 det(M_2) \\ X_3 det(M_2) \end{pmatrix} = T_2$$

to obtain

$$X_{(7,8)} = \begin{pmatrix} X_7 \\ X_8 \end{pmatrix};$$

Step 7 Put X_i into matrix X ;

Step 8 Compute C_1 from $name$, A_1 is the same as that in last subsection;

Step 9 Compute

$$U = A_1^{-1}(X + C_1);$$

Step 10 Get ps from U;

Step 11 Remove "."s from ps, if there are.

IV. Experimental results and analysis

Suppose

$$name = Hardy, id = 6RY20MRQ,$$
$$reg =$$
$$ACOPJB - JMKDPK - PBBFLC - GIJAEC.$$

A. Registration string generation

Input:

$$ps = testver, name = Hardy, id = 6RY20MRQ$$

Output: $reg =$
$ACOPJB - JMKDPK - PBBFLC - GIJAEC.$
Algorithm:

Step 1 Format ps from $ps = testver$ to "$testver$." .

Step 2 Put ps into matrix U ; Create matrix A_1, C_1 ,where A_1 is invertible, C_1 is from $name$.

$$U = \begin{pmatrix} T & v \\ e & e \\ s & r \\ t & . \end{pmatrix} = \begin{pmatrix} 54 & 76 \\ 65 & 65 \\ 73 & 72 \\ 74 & 2E \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 30 & 70 & B0 & F0 \\ 87 & 61 & 62 & 84 \\ 05 & C0 & 6F & 2A \\ F0 & 4B & 4E & F5 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} H & y \\ a & H \\ r & a \\ d & r \end{pmatrix} = \begin{pmatrix} 48 & 79 \\ 61 & 48 \\ 72 & 61 \\ 64 & 72 \end{pmatrix};$$

Step 3 Compute

$$X = A_1 U + C_1,$$

we have

$$X = \begin{pmatrix} 7E & 83 \\ E9 & D1 \\ CF & 65 \\ 9D & 9E \end{pmatrix};$$

Step 4 For (13) , we compute

$$Q_1 = \left(\sum_{3|j} id[j]/0xFF \right) = 36$$

$$Q_2 = \left(\sum_{3|j-1} id[j]/0xFF \right) = 52$$

from

$$id = 6RY20MRQ, M_1 = \begin{pmatrix} 7E & E9 \\ CF & 9D \end{pmatrix},$$

$$Z_1 = \begin{pmatrix} 47 & 40 \\ DB & 1C \end{pmatrix}, Z_2 = \begin{pmatrix} 4D & 2A \\ 22 & 4F \end{pmatrix}$$

$$det(M_1) = 4E, det(M_2) = 28,$$

$$det(Z_1) = BE, det(Z_2) = BE$$

$Y =$
$(06\ F5\ 47\ 40\ DB\ 1C\ 4D\ 2A\ 22\ 4F\ EC\ E8)^T;$

Step 5 Compute Matrix A_3, C_3 where A_3 is invertible and C_3 is from $id = 6RY20MRQ$ in reverse order,

$$A_3 = (A_{31}, A_{32})$$

$$A_{31} = \begin{pmatrix} 41 & 61 & 81 & A1 & C1 & E1 \\ E7 & 4B & E4 & 48 & 02 & AE \\ 7E & 03 & 56 & 5B & A9 & B4 \\ BA & A3 & BF & A6 & 04 & 1D \\ 54 & DD & 9E & 52 & 79 & 58 \\ 35 & 05 & D9 & 88 & 08 & 72 \\ 81 & CE & 84 & 0C & F2 & 5B \\ 26 & 4C & 37 & 5D & 10 & 7A \\ FE & 0F & 5F & 1D & CF & 82 \\ DD & 79 & 9A & C9 & 20 & 8D \\ 4D & D4 & 8B & 79 & B5 & A5 \\ 96 & 11 & 69 & A5 & 40 & 65 \end{pmatrix}$$

$$A_{32} = \begin{pmatrix} 02 & 22 & 42 & 62 & 82 & A2 \\ 04 & A8 & E2 & 4E & E1 & 4D \\ 08 & 1A & 1D & 1F & 8D & FF \\ 10 & 09 & AB & B2 & AE & B7 \\ 20 & 19 & 7F & AB & A5 & 34 \\ 40 & 6F & 7A & 7E & B4 & D1 \\ 80 & CA & 1B & 5A & 65 & 9B \\ 2B & 41 & 0C & 66 & 1D & 77 \\ 56 & D1 & 65 & ED & 33 & 08 \\ AC & 6A & 34 & 0C & 58 & 97 \\ 73 & 60 & 9C & CE & 88 & 3E \\ E6 & 1F & 25 & 35 & 72 & 29 \end{pmatrix}$$

$C_3 = (Q\ R\ M\ 0\ 2\ Y\ R\ 6\ Q\ R\ M\ 0)^T$, or

$C_3 = \left(\ 51\ 52\ 4D\ 30\ 32\ 59\ 52\ 36\ 51\ 52\ 4D\ 30\ \right)^T;$

Step 6 Compute $V = A_3 Y + C_3$ to obtain

$$V = (02\ EF\ 91\ 9C\ A3\ FA\ F1\ 15\ B2\ 68\ 90\ 42)^T;$$

Step 7 Split each value in V into to parts, each part add "A" to be assured within the range from A to P.obtain
$V =$
$(A\ C\ O\ P\ J\ B\ J\ M\ K\ D\ P\ K$
$P\ B\ B\ F\ L\ C\ G\ L\ J\ A\ E\ C)^T$

Step 8 Add "−" between segments.

Obtain $reg =$

$$ACOPJB - JMKDPK - PBBFLC - GIJAEC.$$

B. Registration string verification

Input: $name = Hardy, id = 6RY20MRQ$, $reg =$

$$ACOPJB - JMKDPK - PBBFLC - GIJAEC.$$

Output: $ps = testver$ **Algorithm:**

Step 1 Remove "−" from reg, get
$V =$
$(A\ C\ O\ P\ J\ B\ J\ M\ K\ D\ P\ K$
$P\ B\ B\ F\ L\ C\ G\ L\ J\ A\ E\ C)^T$

Step 2 Merge very two characters into a hexadecimal number, get
$V =$
$(02\ EF\ 91\ 9C\ A3\ FA\ F1\ 15\ B2\ 68\ 90\ 42)^T;$

Step 3 Compute Matrix A_3, C_3 where A_3 is invertible and C_3 is from $id = 6RY20MRQ$ in reverse order,

$$A_3 = (A_{31}, A_{32})$$

$$A_{31}=\begin{pmatrix} 41 & 61 & 81 & A1 & C1 & E1 \\ E7 & 4B & E4 & 48 & 02 & AE \\ 7E & 03 & 56 & 5B & A9 & B4 \\ BA & A3 & BF & A6 & 04 & 1D \\ 54 & DD & 9E & 52 & 79 & 58 \\ 35 & 05 & D9 & 88 & 08 & 72 \\ 81 & CE & 84 & 0C & F2 & 5B \\ 26 & 4C & 37 & 5D & 10 & 7A \\ FE & 0F & 5F & 1D & CF & 82 \\ DD & 79 & 9A & C9 & 20 & 8D \\ 4D & D4 & 8B & 79 & B5 & A5 \\ 96 & 11 & 69 & A5 & 40 & 65 \end{pmatrix}$$

$$A_{32}=\begin{pmatrix} 02 & 22 & 42 & 62 & 82 & A2 \\ 04 & A8 & E2 & 4E & E1 & 4D \\ 08 & 1A & 1D & 1F & 8D & FF \\ 10 & 09 & AB & B2 & AE & B7 \\ 20 & 19 & 7F & AB & A5 & 34 \\ 40 & 6F & 7A & 7E & B4 & D1 \\ 80 & CA & 1B & 5A & 65 & 9B \\ 2B & 41 & 0C & 66 & 1D & 77 \\ 56 & D1 & 65 & ED & 33 & 08 \\ AC & 6A & 34 & 0C & 58 & 97 \\ 73 & 60 & 9C & CE & 88 & 3E \\ E6 & 1F & 25 & 35 & 72 & 29 \end{pmatrix}$$

$$C_3 = (Q\ R\ M\ 0\ 2\ Y\ R\ 6\ Q\ R\ M\ 0)^T,$$

$$C_3 = \begin{pmatrix} 51\ 52\ 4D\ 30\ 32\ 59\ 52\ 36\ 51\ 52\ 4D\ 30 \end{pmatrix}^T$$

these are all the same as those in **Step 5** of last subsection.By Gaussian elimination, compute the inverse of A_3 to obtain $A_3^{-1} = (A_{31}^{-1}, A_{32}^{-1})$, where

$$A_{31}^{-1} = \begin{pmatrix} B2 & D0 & 7E & DC & 6F & C9 \\ C5 & 8C & E7 & 50 & 4C & 17 \\ 69 & 0F & 0C & D8 & 2D & FB \\ 6C & 12 & 8D & DE & DF & 46 \\ 81 & A2 & EF & A8 & F6 & 3E \\ 45 & F3 & 5C & 8D & D3 & 80 \\ D5 & F4 & 2A & BB & 5D & 61 \\ E7 & B2 & 3A & 61 & 25 & 14 \\ 04 & 96 & 6A & 6F & 6F & C5 \\ 96 & DE & 2C & E7 & 3C & 50 \\ B9 & CC & 5E & 40 & 29 & 3B \\ C2 & 3A & AE & 85 & 71 & 53 \end{pmatrix}$$

$$A_{32}^{-1} = \begin{pmatrix} 0B & 46 & B1 & 86 & 4B & B3 \\ 0B & A8 & 62 & 45 & 4B & 61 \\ 30 & 2C & 83 & 4D & ED & 52 \\ 30 & 76 & E8 & 2A & ED & D8 \\ 3B & 70 & A0 & D2 & A6 & E6 \\ 3B & 66 & 11 & 0F & A6 & E2 \\ 3B & 88 & 50 & 06 & A6 & 53 \\ 3B & 08 & B0 & 1E & A6 & D7 \\ 30 & 6C & 2B & C1 & ED & 15 \\ 30 & C9 & E0 & FC & ED & 66 \\ 0B & 23 & F3 & BD & 4B & CC \\ 0B & 9E & AE & 81 & 4B & 5B \end{pmatrix}$$

Step 4 Compute

$$Y = A_3^{-1}(V + C_3)$$

in $\mathbb{L}$;

Step 5 Compute

$$Q_1, Q_2, det(M_2), det(Z_1),$$
$$det(Z_2), det(M_1), X_1, X_2,$$
$$Q_1 = \left(\sum_{3|j} id[j]/0xFF \right) = 36,$$
$$Q_2 = \left(\sum_{3|j-1} id[j]/0xFF \right) = 52,$$
$$Z_1 = \begin{pmatrix} 47 & 40 \\ DB & 1C \end{pmatrix}, Z_2 = \begin{pmatrix} 4D & 2A \\ 22 & 4F \end{pmatrix},$$
$$det(M_2) = \sqrt{EC} = 28,$$
$$det(Z_1) = det(Z_2) = BE,$$
$$det(M_1) = \frac{det(Z_2)}{det(M_2)} = \frac{BE}{28} = 4E,$$
$$\begin{cases} X_1 = Y_1 + det(M_2) + Q_1 = 7E; \\ X_2 = Y_2 + det(M_1) + Q_2 = E9. \end{cases}$$

Step 6 Compute X_3, X_4, X_5, X_6. Solve matrix equation

$$S_1 X_{(3\cdots6)} = \begin{pmatrix} 28 & 00 & 22 & 4D \\ 00 & 28 & 4F & 2A \\ 00 & 00 & 40 & 47 \\ E9 & 7E & 00 & 00 \end{pmatrix} \begin{pmatrix} X_3 \\ X_4 \\ X_5 \\ X_6 \end{pmatrix}$$
$$= \begin{pmatrix} 00 \\ 00 \\ AB \\ 4E \end{pmatrix} = T_1$$

to obtain

Compute Solve matrix equation to obtain

$$X_{(3\cdots6)} = \begin{pmatrix} X_3 \\ X_4 \\ X_5 \\ X_6 \end{pmatrix} = \begin{pmatrix} CF \\ 9D \\ 83 \\ D1 \end{pmatrix};$$

Compute X_7, X_8. Solve matrix equation

$$S_2 X_{(7,8)} = \begin{pmatrix} 40 & 47 \\ 1C & DB \end{pmatrix} \begin{pmatrix} X_7 \\ X_8 \end{pmatrix} = \begin{pmatrix} EF \\ DC \end{pmatrix} = T_2$$

to obtain

$$X_{(7,8)} = \begin{pmatrix} X_7 \\ X_8 \end{pmatrix} = \begin{pmatrix} 65 \\ 9E \end{pmatrix}$$

Step 7 Put X_i into matrix X ,

$$X = \begin{pmatrix} 7E & 83 \\ E9 & D1 \\ CF & 65 \\ 9D & 9E \end{pmatrix};$$

Step 8 Compute C_1 from $name$, A_1 is the same as that in last subsection,

$$C_1 = \begin{pmatrix} H & y \\ a & H \\ r & a \\ d & r \end{pmatrix} = \begin{pmatrix} 48 & 79 \\ 61 & 48 \\ 72 & 61 \\ 64 & 72 \end{pmatrix},$$

$$A_1 = \begin{pmatrix} 30 & 70 & B0 & F0 \\ 87 & 61 & 62 & 84 \\ 05 & C0 & 6F & 2A \\ F0 & 4B & 4E & F5 \end{pmatrix},$$

by Gaussian elimination, compute

$$A_1^{-1} = \begin{pmatrix} 58 & FF & 32 & 08 \\ 4D & 6A & 8A & 7B \\ 7C & 07 & 98 & 61 \\ 2E & 14 & DE & DD \end{pmatrix};$$

Step 9 Compute

$$U = A_1^{-1}(X + C_1) = \begin{pmatrix} 54 & 76 \\ 65 & 65 \\ 73 & 72 \\ 74 & 2E \end{pmatrix} = \begin{pmatrix} T & v \\ e & e \\ s & r \\ t & . \end{pmatrix};$$

Step 10 Get ps from U,

$$ps = "Testver.";$$

Step 11 Remove "." from ps ,get $ps = "Testver"$.

C. Analysis

We solve the problem in the central mapping by adding two elements Y_{11}, Y_{12} where Y_{11} is the square of $det(M_2)$ and Y_{12} is a random value. This small change in Y_{12} results in big change in $z_k, 1 \leq k \leq 12r$. A plaintext can create a lot of ciphertexts. For example, when $ps = Testver, name = Hardy, id = 6RY20MRQ$,we obtain different registration strings:$reg =$

$$ACOPJB - JMKDPK - PBBFLC - GIJAEC$$

$$GLMEMB - INAEML - FMNMLL - FNODJE$$

$$KIDFFA - ACKIKA - BIBGHP - LPLKLA$$

$$BIBCEJ - DCKHCE - OOJEDI - LIKJHI$$

$$AFPMFJ - DHNLHG - JAKJNM - FAAIPI$$

$$ODHLGC - GCLGID - NPDJPB - LBJMAL$$

$$NHKKPJ - BFLOBE - OBBAMO - DKOOHP$$

and so on. This Camouflage technique gives the adversary more difficulty and makes the system safer. The breaking is hard because the ciphertext is variable. The dependence of registration string on the fingerprints of machine prevents any registration string from being shared by multiple machines.

V. Conclusions

To design software copy protection algorithm based on multivariate public key cryptosystem, we choose Zhiwei Wang *et al.*'s scheme and solve a problem in the central mapping. In addition to solving the original problem, we also extend its new feature. This new feature makes the system safer. Experimental results and analysis show that our scheme is viable and secure.

Acknowledgments

The author is grateful to the editors and reviewers for their valuable comments and suggestions to improve the presentation of this paper.This work was supported by the fund from Natural Science of Jiangxi Province of China under Grant No.20114BAB201033. The author would like to express thanks to the Committee of the fund.

References

[1] Whitfield Diffie and Martin Hellman, *New directions in cryptography[J]*,IEEETransactions on Information Theory.1976,22(6):644-654.

[2] Ronald Rivest, Adi Shamir and Leonard M. Adleman,*A method for obtainingdigital signatures and public-key cryptosystems[J]*, ACM,1978,21(2):120-126.

[3] Ronald Rivest, Adi Shamir, and Leonard M. Adleman,*A method for obtainingdigital signatures and public key cryptosystems.secure communications andasymmetric cryptosystems,[C]*In G Simmons, editor, AAAS Sel. Sympos.,1982,vol.69:217-239.

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

[5] Jintai Ding and Dieter Schmit, *Multivariable Public Key Cryptosystem,[J]*Contemporary Mathematics,2006,Vol. 419:79-94.

[6] Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithmson a Quantum Computer,[J]* SIAM REVIEW, 1999,Vol. 41 No.2:303-332.

[7] Harriet Fell and Whitfield Diffie, *Analysis of a public key approach based on polynomial substitution.[C]*In Hugh C. Williams,Proceeding CRYPTO '85 Advances in Cryptology.London:Springer-Verlag, 1986,Vol.218:340-349.

[8] J. Patarin,*Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88 [C]*,In D. Coppersmith, editor, Advances in Cryptology - Crypto'95, LNCS,1995, Vol 963:248-261.

[9] J. Patarin, *The oil and vinegar signature scheme [C]*,Dagstuhl Workshop on Cryptography,September 1997
[10] Aviad Kipnis, Jacques Patarin, and Louis Goubin, *Unbalanced Oil and Vinegar Signature Schemes - Extended Version[C]*, Eurocrypt'99.
[11] Lih-Chung Wang, Bo-Yin Yang, Yu-Hua Hu, and Feipei Lai, *A Medium-Field Multivariate Public-Key Encryption Scheme[J],*Lecture Notes in Computer Science, 3860,2006: 132-149.
[12] http://blog.csdn.net/GavinFriends/article/details/4544226(in Chinese)
[13] L. Goubin and N. Courtois. *Cryptanalysis of the TTM cryptosyste[J],*LNCS,Springer Verlag ,1976,2000:44-57.
[14] Darrel Hankerson,Alfred Menezes and Scott Vanstone.*Guide to Elliptic CurveCryptography[M]*,Berlin:Springer,2003:48.
[15] Roberto M. Avanzi, Henri Cohen, Christophe Doche,Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren,*Handbook of elliptic and hyperelliptic curve cryptography[M]*,London:Taylor & Francis Group,2006:218.
[16] William J.Gilbert and W.Keith Nicholson,*Modern Alegbra with Applications[M]*,Second Edition.New Jersy:John Wiley &Sons,Inc,2003:232.
[17] Nicolas T. Courtois,*The security of hidden field equations (HFE) [C]*,In C. Naccache,editor, Progress in cryptology, CT-RSA, LNCS, Vol. 2020, Springer, 2001:266-281.
[18] Jean-Charles Faug'ere and Antoine Joux, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Grobner bases[C]*, In Dan Boneh, editor,Advances in cryptology - CRYPTO 2003, LNCS, Vol. 2729, Springer, 2003:44-60.
[19] S.D.S. Monteiro and R.F. Erbacher,*Exemplifying Attack Identification and Analysis in a Novel Forensically Viable Syslog Model[C]*,In Washington:IEEE Computer Society,Proceedings of the Third International Workshop on Systematic Approaches to Digital Forensic Engineering ,2008,57-68.

Ning Huang,born in 1958, received Master's degree in applied mathematics and computer science from Jiangxi University, China in 1991, awarded senior engineer of the Industrial and Commercial Bank of China in 2001. He is now with Center of Modern Educational Technology, Gannan Normal University,Ganzhou, China,as an associate professor. His research interests include information security and digital campus.