

# REVISION OF TRACTABLE RATIONAL MAP CRYPTOSYSTEM

LIH-CHUNG WANG AND FEL-HWANG CHANG

ABSTRACT. We introduce a new public-key cryptosystem with tractable rational maps. As an application of abstract algebra and algebraic geometry to cryptography, TRMC (Tractable Rational Map Cryptosystem) has many superior properties including high complexity, easy implementation and very fast execution. We describe the principles and implementation of TRMC and analyze its properties. Also, we give a brief account of security analysis.

## 1. INTRODUCTION

It was active to develop new public key cryptosystem for the last 20 years. A specially active line of cryptographic research was based on the fact that solving systems of multivariate polynomial equations is NP-complete. In this article, we introduce a multivariate cryptosystem using tractable rational maps. Our TRMC (Tractable Rational Map Cryptosystem) is faster than most of other public key systems.

Section 2 reviews some basic ideas of polynomial maps over a finite field and recaps what is a tractable rational map. Section 3 shows how tractable rational maps are used to construct the TRMC. Section 4 gives some security analysis.

## 2. MATHEMATICAL BACKGROUND

Let  $p$  be a prime number. Let  $k$  be the finite Galois field  $GF(p^n)$  with  $p^n$  elements. Let  $k^*$  denote  $k \setminus \{0\}$ . It is well-known that  $k^*$  is a cyclic multiplicative group and  $k$  is the splitting field of

$$x^{p^n} - x = \prod_{\alpha \in k} (x - \alpha).$$

Let  $a$  be an element of  $k$ . Define the characteristic function  $\chi_a$  of the element  $a$  to be the function given by

$$\chi_a(x) = 1 - (x - a)^{p^n - 1} = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

With the Lagrange interpolation formula, we obtain

$$f(x_1, \dots, x_n) = \sum_{(a_1, \dots, a_n) \in k^n} f(a_1, \dots, a_n) \prod_{i=1}^n \chi_{a_i}(x_i).$$

---

*Date:* February 3, 2006.

*1991 Mathematics Subject Classification.* [2000]Primary 11T71, 14G50 and 94A60.

*Key words and phrases.* tractable rational map, public-key system, public key, private key, error-detect, signature, master key.

Hence, every map  $f$  from  $k^n$  to  $k^m$  is a polynomial map. Therefore, the category of polynomial maps is as big as the category of maps. Moreover, consider  $k^n$  as an affine algebraic set. It is known that the coordinate ring of  $k^n$  is

$$k[x_1, \dots, x_n]/(x_1^{p_1} - x_1, \dots, x_n^{p_n} - x_n).$$

That is, if two polynomials define the same polynomial function, then the difference of these two polynomials is in the ideal  $(x_1^{p_1} - x_1, \dots, x_n^{p_n} - x_n)$ . Hence, if we have a polynomial function with a polynomial representation which has terms with the degree of some variable  $x_i$  bigger than  $p_i - 1$ , we can reduce the degree of such terms with the relation  $x_i^{p_i} = x_i$ .

Let  $K$  be a finite  $k$ -algebra. For example,  $K$  could be a finite field extension of  $k$ , a matrix algebra over  $k$  or a quotient ring of  $k[x]$ . A  $k$ -polynomial map  $r : K \rightarrow K$  is called a  $k$ -polynomial permutation if each  $k$ -component of  $r(x)$  is a polynomial in  $k$ -components of  $x$  and  $r : K \rightarrow K$  is a one-to-one and onto map. For example, let  $K$  be  $2 \times 2$  matrix algebra over  $GF(256)$ ,  $r \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} x_1^2 & x_3 + x_1x_2 \\ x_2^4 & x_4 + x_2x_3 \end{pmatrix}$  is a  $GF(256)$ -polynomial permutation. A polynomial  $r(x) \in K[x]$  is called a permutation polynomial of  $K$  if  $K$  is a field and the associated polynomial function from  $K$  to  $K$  is a one-to-one and onto function. See ([6], Chapter9). For example,  $r(x) = x^2$  is a permutation polynomial over  $GF(16)$ . It is obvious that a permutation polynomial function is a  $k$ -polynomial permutation if  $K$  is a finite extension of  $k$ . On the other hand, a  $k$ -polynomial permutation can be viewed as a permutation polynomial function with suitable identification since every map over finite field is a polynomial map.

A tractable rational map is a one-to-one affine transformation or, after a permutation of indices if necessary, a rational map of the following form

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_j \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_j(x_j) \cdot \frac{p_j(x_1, x_2, \dots, x_{j-1})}{q_j(x_1, x_2, \dots, x_{j-1})} + \frac{f_j(x_1, x_2, \dots, x_{j-1})}{g_j(x_1, x_2, \dots, x_{j-1})} \\ \vdots \\ r_n(x_n) \cdot \frac{p_n(x_1, x_2, \dots, x_{n-1})}{q_n(x_1, x_2, \dots, x_{n-1})} + \frac{f_n(x_1, x_2, \dots, x_{n-1})}{g_n(x_1, x_2, \dots, x_{n-1})} \end{pmatrix}$$

where  $f_j, g_j, p_j$  and  $q_j$  are polynomials and  $r_j$  are  $k$ -polynomial permutations over  $K$ . Note that a tractable rational map is probably only well-defined on a subset of the affine space  $K^n$ . Let

$$S = \{(x_1, \dots, x_n) \mid p_j, q_j \text{ and } g_j \text{ are invertible in } K \text{ for } j = 2, \dots, n\}.$$

Given a point  $(y_1, \dots, y_n)$  which is in the image of  $S$ , we can solve the following system of equations inductively.

$$\begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_j(x_j) \cdot \frac{p_j(x_1, x_2, \dots, x_{j-1})}{q_j(x_1, x_2, \dots, x_{j-1})} + \frac{f_j(x_1, x_2, \dots, x_{j-1})}{g_j(x_1, x_2, \dots, x_{j-1})} \\ \vdots \\ r_n(x_n) \cdot \frac{p_n(x_1, x_2, \dots, x_{n-1})}{q_n(x_1, x_2, \dots, x_{n-1})} + \frac{f_n(x_1, x_2, \dots, x_{n-1})}{g_n(x_1, x_2, \dots, x_{n-1})} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_j \\ \vdots \\ y_n \end{pmatrix}$$

First, we get  $x_1 = r_1^{-1}(y_1)$  from the first equation. Suppose we know  $x_1, \dots, x_{j-1}$ . Substitute  $x_1, \dots, x_{j-1}$  into the  $j$ -th equation.

$$r_j(x_j) \cdot \frac{p_j(x_1, x_2, \dots, x_{j-1})}{q_j(x_1, x_2, \dots, x_{j-1})} + \frac{f_j(x_1, x_2, \dots, x_{j-1})}{g_j(x_1, x_2, \dots, x_{j-1})} = y_j$$

Then we obtain

$$x_j = r_j^{-1} \left( \frac{q_j(x_1, x_2, \dots, x_{j-1})}{p_j(x_1, x_2, \dots, x_{j-1})} \cdot \left( y_j - \frac{f_j(x_1, x_2, \dots, x_{j-1})}{g_j(x_1, x_2, \dots, x_{j-1})} \right) \right).$$

That is, given a tractable rational map  $\phi : S \rightarrow K^n$  of the following form

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_j \\ \vdots \\ y_n \end{pmatrix} = \phi \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_j(x_j) \cdot \frac{p_j(x_1, x_2, \dots, x_{j-1})}{q_j(x_1, x_2, \dots, x_{j-1})} + \frac{f_j(x_1, x_2, \dots, x_{j-1})}{g_j(x_1, x_2, \dots, x_{j-1})} \\ \vdots \\ r_n(x_n) \cdot \frac{p_n(x_1, x_2, \dots, x_{n-1})}{q_n(x_1, x_2, \dots, x_{n-1})} + \frac{f_n(x_1, x_2, \dots, x_{n-1})}{g_n(x_1, x_2, \dots, x_{n-1})} \end{pmatrix},$$

we can get the pre-image of  $\phi$  for each image point constructively. The motivation for using the rational expressions is for computational reason.

For practical reasons, we always pick the finite fields of characteristic 2. We identify  $GF(2^{16})$  with  $GF(2^8)[t]/(t^2+t+\alpha_1)$  and identify  $GF(2^{32})$  with  $GF(2^{16})[s]/(s^2+s+(\alpha_2t+\alpha_3))$ . A variable  $X_{1,2}$  in  $GF(2^{16})$  can be represented by  $x_1t+x_2$  (or  $x_1\|x_2$  if we want to omit the dummy variable  $t$ ). The product of two variables  $X_{1,2}X_{3,4}$  can be represented by  $((x_1+x_2)(x_3+x_4)+x_2x_4)\|(x_1x_3\alpha_1+x_2x_4)$ . Similarly, a variable  $X_{1,2,3,4}$  in  $GF(2^{32})$  can be represented by  $(x_1t+x_2)s+(x_3t+x_4) = x_1\|x_2\|x_3\|x_4$ , 4 variables in  $GF(2^8)$ .

If we consider  $GF(2^{32})$  as a vector space over  $GF(2)$ , then the Frobenius map  $X \mapsto X^2$  is a linear transformation of  $GF(2^{32})$ , which is a permutation polynomial map. Similarly, a map  $X \mapsto X^{2^8}$  is a linear transformation of  $GF(2^{8k})$  over  $GF(2^8)$ . A product of 2 variables  $X_{1,2,3,4}X_{5,6,7,8}$  in  $GF(2^{32})$  can be represented as 4 quadratic polynomials with 8 variables in  $GF(2^8)$ . For example,  $X_{1,2,3,4}^{2^{57}}$  and  $X_{1,2,3,4}^{2^{56}+6^{55}3^6}$  in  $GF(2^{32})$  can be represented as 4 quadratic polynomials with 4 variables in  $GF(2^8)$ .

## 3. TRMC AND ITS IMPLEMENTATION

The previous discussion shows that the pre-image of a image point for a tractable rational map can be easily obtained. The present invention is a public-key cryptosystem based on tractable rational maps. The spirit of this invention is to consider the composition map of several tractable rational maps. The composition no longer has the inductive structure of a tractable rational map, so that it is hard to obtain the pre-image of the composition for a given point. However, for those who knows the original tractable rational maps, it would be easy and fast to obtain the pre-image of the composition by simply computing the pre-image of each individual tractable rational map in succession. The further progress in this invention is the addition of standard injections and projections between the several tractable rational maps, so that the public-key cryptosystem can have the function of error-detecting and allow more variations of the embodiments to increase the security.

From now on,  $x_i$  always denotes a variable in  $GF(256)$ ,  $X_{1,2} = x_1||x_2$  always denotes a variable in  $GF(2^{16})$  and so on. First, we give several toy examples to illustrate some basic construction tricks.

**Toy Example 1**

Consider the three maps  $\{\phi_1, \phi_2, \phi_3, \phi_4\}$  to be the private key.

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \phi_1 \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}, \quad \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \phi_2 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \phi_3 \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \quad \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \phi_4 \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$$

wherein  $\phi_1$  and  $\phi_4$  are invertible affine transformations,  $\phi_2$  and  $\phi_3$  are tractable rational maps, and the variables of the composition (public key) could be shown as below:

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$$

Because  $\phi_1$  and  $\phi_4$  are just invertible affine transformations, for convenience, we only list  $\phi_2$  and  $\phi_3$ .

$$\begin{aligned} y_1 &= x_1 \\ y_2 &= x_2x_1 \\ y_3 &= x_3x_2 \\ z_1 &= y_1^2 \frac{y_3}{y_2} = x_1x_3 \\ z_2 &= y_2 = x_2x_1 \\ z_3 &= y_3 = x_3x_2 \end{aligned}$$

The composition of  $\phi_2$  and  $\phi_3$  is a birational morphism. It is injective on  $\{(x_1, x_2, x_3) || x_1 \neq 0, x_2 \neq 0 \text{ and } x_3 \neq 0\}$ .

**Toy Example 2**

Consider the following five maps  $\{\phi_1, \rho, \phi_2, \pi, \phi_3\}$  to be the private key.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_5 \end{pmatrix}, \quad \begin{pmatrix} u_1 \\ \vdots \\ u_{11} \end{pmatrix} = \rho \begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_5 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} y_1 \\ \vdots \\ y_{11} \end{pmatrix} = \phi_2 \begin{pmatrix} u_1 \\ \vdots \\ u_{11} \end{pmatrix}$$

$$\begin{pmatrix} z_1 \\ \vdots \\ z_9 \end{pmatrix} = \pi \begin{pmatrix} y_1 \\ \vdots \\ y_{11} \end{pmatrix} = \begin{pmatrix} y_3 \\ \vdots \\ y_{11} \end{pmatrix}, \quad \begin{pmatrix} w_1 \\ \vdots \\ w_9 \end{pmatrix} = \phi_3 \begin{pmatrix} z_1 \\ \vdots \\ z_9 \end{pmatrix}$$

wherein  $\{\phi_1, \phi_3\}$  are invertible affine transformations,  $\{\phi_2\}$  is a tractable rational map,  $\rho$  is the standard injection and  $\pi$  is the standard projection. The composition of the above five maps could be written as below:

$$\begin{pmatrix} w_1 \\ \vdots \\ w_9 \end{pmatrix} = \phi_3 \circ \pi \circ \phi_2 \circ \rho \circ \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_5 \end{pmatrix}$$

That is, the composition consists of 9 quadratic polynomials of 5 variables. Because  $\{\phi_1, \phi_3\}$  are just invertible affine transformations, for convenience, we only list  $\{\pi \circ \phi_2 \circ \rho\}$ .

$$\begin{aligned} z_1 &= y_3 &= x_3 + x_1x_2 \\ z_2 &= y_4 &= x_4 + x_2x_3 \\ z_3 &= y_5 &= x_5 + x_3x_4 \\ Z_{4,5} &= Y_{6,7} &= X_{1,2}(X_{3,5}^{256} + X_{3,5} + a) \\ Z_{6,7} &= Y_{8,9} &= X_{1,2}(X_{4,5}^{256} + X_{4,5} + a) \\ Z_{8,9} &= Y_{10,11} &= (X_{3,5}^{256} + X_{3,5} + a)(X_{4,5}^{256} + X_{4,5} + a) \end{aligned}$$

wherein  $(X^{256} + X + a)$  is a non-vanishing polynomial over  $GF(2^{16})$ . Note that  $X_{1,2}^2 = \frac{Z_{4,5}Z_{6,7}}{Z_{8,9}}$ . This example shows that we can recover the first two variable  $x_1$  and  $x_2$  by solving multi-variable equations and then obtain the other  $x_i$  by recursive substitution.

### Toy Example 3

In this example all variables are in  $GF(2^{16})$ .

$$\begin{aligned} Y_1 &= X_1 \\ Y_2 &= X_2/(X_1^{256} + X_1 + a) \\ Y_3 &= X_3(X_1^{256} + X_1 + a) \\ Y_4 &= X_4 + X_1 \\ Y_5 &= X_5(X_4^{256} + X_4 + a) \\ Y_6 &= X_1X_4 \end{aligned}$$

$$\begin{aligned}
Z_1 &= Y_1 + \frac{Y_3 Y_5}{f(Y_4, Y_6)} &= X_1 + X_3 X_5 \\
Z_2 &= Y_2 f(Y_4, Y_6) + Y_4^{257} &= X_2 (X_4^{256} + X_4 + a) + (X_4 + X_1)^{257} \\
Z_3 &= Y_3 &= X_3 (X_1^{256} + X_1 + a) \\
Z_4 &= Y_4 &= X_4 + X_1 \\
Z_5 &= Y_5 &= X_5 (X_4^{256} + X_4 + a) \\
Z_6 &= Y_6 &= X_1 X_4
\end{aligned}$$

wherein  $f(Y_4, Y_6) = (X_1^{256} + X_1 + a)(X_4^{256} + X_4 + a)$  is a symmetric polynomial of  $X_1$  and  $X_4$ , hence a polynomial of  $Y_4$  and  $Y_6$ . Note that  $Z_4 = X_4 + X_1$  is a linear function. We can replace it with some multi-variable equations just as in Toy Example 2.

**Toy Example 4**

We would like to show an example of tractable rational map over the  $2 \times 2$  matrix algebra. Consider the following five maps  $\{\phi_1, \rho, \phi_2, \pi, \phi_3\}$  to be the private key.

$$\begin{aligned}
\begin{pmatrix} x_1 \\ \vdots \\ x_{12} \end{pmatrix} &= \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_{12} \end{pmatrix}, \quad \begin{pmatrix} u_1 \\ \vdots \\ u_{19} \end{pmatrix} = \rho \begin{pmatrix} x_1 \\ \vdots \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_{12} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\
\begin{pmatrix} y_1 \\ \vdots \\ y_{19} \end{pmatrix} &= \phi_2 \begin{pmatrix} u_1 \\ \vdots \\ u_{19} \end{pmatrix} \\
\begin{pmatrix} z_1 \\ \vdots \\ z_{15} \end{pmatrix} &= \pi \begin{pmatrix} y_1 \\ \vdots \\ y_{19} \end{pmatrix} = \begin{pmatrix} y_5 \\ \vdots \\ y_{19} \end{pmatrix}, \quad \begin{pmatrix} w_1 \\ \vdots \\ w_{15} \end{pmatrix} = \phi_3 \begin{pmatrix} z_1 \\ \vdots \\ z_{15} \end{pmatrix}
\end{aligned}$$

wherein  $\{\phi_1, \phi_3\}$  are invertible affine transformations,  $\{\phi_2\}$  is a tractable rational map,  $\rho$  is the standard injection and  $\pi$  is the standard projection. The composition of the above five maps could be written as below:

$$\begin{pmatrix} w_1 \\ \vdots \\ w_{15} \end{pmatrix} = \phi_3 \circ \pi \circ \phi_2 \circ \rho \circ \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_{12} \end{pmatrix}$$

That is, the composition consists of 15 quadratic polynomials of 12 variables. Because  $\{\phi_1, \phi_3\}$  are just invertible affine transformations, for convenience, we only list  $\{\pi \circ \phi_2 \circ \rho\}$ .

$$\begin{aligned}
\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} &= \begin{pmatrix} y_5 & y_6 \\ y_7 & y_8 \end{pmatrix} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} x_5 x_1 + x_6 x_3 & x_5 x_2 + x_6 x_4 \\ x_7 x_1 + x_8 x_3 & x_7 x_2 + x_8 x_4 \end{pmatrix} \\
\begin{pmatrix} z_5 & z_6 \\ z_7 & z_8 \end{pmatrix} &= \begin{pmatrix} y_9 & y_{10} \\ y_{11} & y_{12} \end{pmatrix} = \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \\
\begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix} &= \begin{pmatrix} y_{13} & y_{14} \\ y_{15} & y_{16} \end{pmatrix} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \begin{pmatrix} x_9 & x_{11} \\ x_{10} & x_{12} \end{pmatrix}
\end{aligned}$$

$$\begin{aligned} z_{13} &= y_{17} = x_1 + \det \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \\ z_{14} &= y_{18} = x_2 + \det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \\ z_{15} &= y_{19} = x_3 + x_1 x_2 + \det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \end{aligned}$$

We assume that

$$\det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \neq 0,$$

$$\det \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \neq 0$$

and

$$\det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \neq 0.$$

Then we can get the  $x_i$ 's by the following steps.

First, we can have

$$\det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \sqrt{\det \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} \det \begin{pmatrix} z_5 & z_6 \\ z_7 & z_8 \end{pmatrix} (\det \begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix})^{-1}}.$$

$$\det \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} = \det \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} (\det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix})^{-1}$$

$$\det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} = \det \begin{pmatrix} z_5 & z_6 \\ z_7 & z_8 \end{pmatrix} (\det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix})^{-1}$$

Hence, we obtain the values of  $x_1$ ,  $x_2$  and  $x_3$ .

In case of  $x_1 \neq 0$ , we can get  $x_4$  since we know  $x_1$ ,  $x_2$ ,  $x_3$  and  $\det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ .

Then

$$\begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} = \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}^{-1}$$

and

$$\begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} = \begin{pmatrix} z_5 & z_6 \\ z_7 & z_8 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}^{-1}.$$

Note that

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}^{-1} = (\det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix})^{-1} \begin{pmatrix} x_4 & x_2 \\ x_3 & x_1 \end{pmatrix}.$$

If we know the matrix value of  $\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ , then we solve the matrices  $\begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix}$

and  $\det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix}$  recursively.

In case of  $x_1 = 0$ , we can solve the variables by the following formula.

$$\begin{aligned} x_6 &= z_1 x_3^{-1} \\ x_8 &= z_3 x_3^{-1} \\ x_{10} &= z_5 x_3^{-1} \\ x_{12} &= z_7 x_3^{-1} \end{aligned}$$

$$\begin{aligned}
x_5 &= (z_9x_{12} + z_{10}x_{10}) \det \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \left( \det \begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix} \right)^{-1} \\
x_7 &= (z_{11}x_{12} + z_{12}x_{10}) \det \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} \left( \det \begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix} \right)^{-1} \\
x_4 &= (z_2x_7 + z_4x_5) \det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \left( \det \begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix} \right)^{-1} \\
x_9 &= (z_9x_8 + z_{11}x_6) \det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \left( \det \begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix} \right)^{-1} \\
x_{11} &= (z_{10}x_8 + z_{12}x_6) \det \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \left( \det \begin{pmatrix} z_9 & z_{10} \\ z_{11} & z_{12} \end{pmatrix} \right)^{-1}
\end{aligned}$$

The case of  $x_1 = 0$  has less operations than the case of  $x_1 \neq 0$ . In order to avoid the time attack, we would like to have the same number of operations for both cases. We can accomplish this will by padding one multiplication and four additions to the case of  $x_1 = 0$ .

We generalize the above example to an implementation scheme called TRMC-3 or MFE. It will appear in CT-RSA 2006. However, we think that this scheme has some weakness. We will come back for this issue somewhere else.

#### Toy Example 5

We would like to show another example of tractable rational map over the  $2 \times 2$  matrix algebra. Consider the three maps  $\{\phi_1, \phi_2, \phi_3, \phi_4\}$  to be the private key.

$$\begin{aligned}
\begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix} &= \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_8 \end{pmatrix}, & \begin{pmatrix} y_1 \\ \vdots \\ y_8 \end{pmatrix} &= \phi_2 \begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix} \\
\begin{pmatrix} z_1 \\ \vdots \\ z_8 \end{pmatrix} &= \phi_3 \begin{pmatrix} y_1 \\ \vdots \\ y_8 \end{pmatrix}, & \begin{pmatrix} w_1 \\ \vdots \\ w_8 \end{pmatrix} &= \phi_4 \begin{pmatrix} z_1 \\ \vdots \\ z_8 \end{pmatrix}
\end{aligned}$$

wherein  $\phi_1$  and  $\phi_4$  are invertible affine transformations,  $\phi_2$  and  $\phi_3$  are tractable rational maps, and the variables of the composition (public key) could be shown as below:

$$\begin{pmatrix} w_1 \\ \vdots \\ w_8 \end{pmatrix} = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_8 \end{pmatrix}$$

Because  $\phi_1$  and  $\phi_4$  are just invertible affine transformations, for convenience, we only list  $\phi_2$  and  $\phi_3$ .

$$\begin{aligned}
y_1 &= x_1 \\
y_2 &= x_2x_1 \\
y_3 &= x_3x_2 \\
y_4 &= x_4x_1 + x_3x_2
\end{aligned}$$

$$\begin{bmatrix} y_5 & y_6 \\ y_7 & y_8 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix} = \begin{bmatrix} x_1x_5 + x_2x_7 & x_1x_6 + x_2x_8 \\ x_3x_5 + x_4x_7 & x_3x_6 + x_4x_8 \end{bmatrix}$$



$$\begin{aligned}
 z_1 &= y_1^2 \frac{y_3}{y_2} + c_1 \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_1 x_3 + c_1 (x_5 x_8 + x_6 x_7) \\
 z_2 &= y_2 + c_2 \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_2 x_1 + c_2 (x_5 x_8 + x_6 x_7) \\
 z_3 &= y_3 + c_3 \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_3 x_2 + c_3 (x_5 x_8 + x_6 x_7) \\
 z_4 &= y_4 &= x_4 x_1 + x_3 x_2 \\
 z_5 &= y_5 &= x_1 x_5 + x_2 x_7 \\
 z_6 &= y_6 &= x_1 x_6 + x_2 x_8 \\
 z_7 &= y_7 &= x_3 x_5 + x_4 x_7 \\
 z_8 &= y_8 &= x_3 x_6 + x_4 x_8
 \end{aligned}$$

where the  $c_i$ 's are non-zero constants. The composition of  $\phi_2$  and  $\phi_3$  is a birational morphism.

### Toy Example 6

We would like to give a variation of toy example 5. Consider the three maps  $\{\phi_1, \phi_2, \phi_3, \phi_4\}$  to be the private key.

$$\begin{aligned}
 \begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix} &= \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_8 \end{pmatrix}, & \begin{pmatrix} y_1 \\ \vdots \\ y_8 \end{pmatrix} &= \phi_2 \begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix} \\
 \begin{pmatrix} z_1 \\ \vdots \\ z_8 \end{pmatrix} &= \phi_3 \begin{pmatrix} y_1 \\ \vdots \\ y_8 \end{pmatrix}, & \begin{pmatrix} w_1 \\ \vdots \\ w_8 \end{pmatrix} &= \phi_4 \begin{pmatrix} z_1 \\ \vdots \\ z_8 \end{pmatrix}
 \end{aligned}$$

wherein  $\phi_1$  and  $\phi_4$  are invertible affine transformations,  $\phi_2$  is a tractable rational maps,  $\phi_3$  is a rational maps, and the variables of the composition (public key) could be shown as below:

$$\begin{pmatrix} w_1 \\ \vdots \\ w_8 \end{pmatrix} = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_8 \end{pmatrix}$$

Because  $\phi_1$  and  $\phi_4$  are just invertible affine transformations, for convenience, we only list  $\phi_2$  and  $\phi_3$ .

$$\begin{aligned}
 y_1 &= x_1 \\
 y_2 &= x_2 x_1 \\
 y_3 &= x_3 x_2 \\
 y_4 &= x_4 x_1 + x_3 x_2
 \end{aligned}$$

$$\begin{bmatrix} y_5 & y_6 \\ y_7 & y_8 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix} = \begin{bmatrix} x_1 x_5 + x_2 x_7 & x_1 x_6 + x_2 x_8 \\ x_3 x_5 + x_4 x_7 & x_3 x_6 + x_4 x_8 \end{bmatrix}$$

$$\begin{aligned}
 z_1 &= y_1^2 \frac{y_3}{y_2} + c_1 \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_1 x_3 + c_1 (x_5 x_8 + x_6 x_7) \\
 z_2 &= y_2 + c_2 \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_2 x_1 + c_2 (x_5 x_8 + x_6 x_7) \\
 z_3 &= y_3 + c_3 \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_3 x_2 + c_3 (x_5 x_8 + x_6 x_7) \\
 z_4 &= y_4 + \frac{y_5 y_8 + y_6 y_7}{y_4} &= x_4 x_1 + x_3 x_2 + x_5 x_8 + x_6 x_7 \\
 z_5 &= y_5 &= x_1 x_5 + x_2 x_7 \\
 z_6 &= y_6 &= x_1 x_6 + x_2 x_8 \\
 z_7 &= y_7 &= x_3 x_5 + x_4 x_7 \\
 z_8 &= y_8 &= x_3 x_6 + x_4 x_8
 \end{aligned}$$

where the  $c_i$ 's are non-zero constants. Note that the map  $\phi_3$  is just a rational map. In order to get the value of  $y_4$ , we need to solve a quadratic equation and guess which root is the  $y_4$ .

### Preferred Implementations<sup>1</sup>

We introduce a new implementation schemes called TRMC-4.

#### TRMC-4 Scheme

We generalize the toy example 5 (or 6) to an implementation scheme. Consider the three maps  $\{\phi_1, \phi_2, \phi_3, \phi_4\}$  to be the private key.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{45} \end{pmatrix} = \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_{45} \end{pmatrix}, \quad \begin{pmatrix} y_1 \\ \vdots \\ y_{50} \end{pmatrix} = \phi_2 \begin{pmatrix} x_1 \\ \vdots \\ x_{45} \end{pmatrix}$$

$$\begin{pmatrix} z_1 \\ \vdots \\ z_{50} \end{pmatrix} = \phi_3 \begin{pmatrix} y_1 \\ \vdots \\ y_{50} \end{pmatrix}, \quad \begin{pmatrix} w_1 \\ \vdots \\ w_{50} \end{pmatrix} = \phi_4 \begin{pmatrix} z_1 \\ \vdots \\ z_{50} \end{pmatrix}$$

wherein  $\phi_1$  and  $\phi_4$  are invertible affine transformations,  $\phi_2$  and  $\phi_3$  are tractable rational maps, and the variables of the composition (public key) could be shown as below:

$$\begin{pmatrix} w_1 \\ \vdots \\ w_{50} \end{pmatrix} = \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_{45} \end{pmatrix}$$

Because  $\phi_1$  and  $\phi_4$  are just invertible affine transformations, for convenience, we only list  $\phi_2$  and  $\phi_3$ . We fix some notations first.

$X_1$	$X_2$	$X_3$	$X_4$	$X_5$	$X_6$	$X_7$	$X_8$
$c_1$	$c_2$	$c_3$	$x_{16}$	$x_{22}$	$x_{28}$	$x_{34}$	$x_{40}$
$x_1$	$x_6$	$x_{11}$	$x_{17}$	$x_{23}$	$x_{29}$	$x_{35}$	$x_{41}$
$x_2$	$x_7$	$x_{12}$	$x_{18}$	$x_{24}$	$x_{30}$	$x_{36}$	$x_{42}$
$x_3$	$x_8$	$x_{13}$	$x_{19}$	$x_{25}$	$x_{31}$	$x_{37}$	$x_{43}$
$x_4$	$x_9$	$x_{14}$	$x_{20}$	$x_{26}$	$x_{32}$	$x_{38}$	$x_{44}$
$x_5$	$x_{10}$	$x_{15}$	$x_{21}$	$x_{27}$	$x_{33}$	$x_{39}$	$x_{45}$
$Y_1$	$Y_2$	$Y_3$	$Y_4$	$Y_5$	$Y_6$	$Y_7$	$Y_8$
$y_1$	$y_7$	$y_{13}$	$y_{19}$	$y_{25}$	$y_{31}$	$y_{37}$	$y_{43}$
$y_2$	$y_8$	$y_{14}$	$y_{20}$	$y_{26}$	$y_{32}$	$y_{38}$	$y_{44}$
$y_3$	$y_9$	$y_{15}$	$y_{21}$	$y_{27}$	$y_{33}$	$y_{39}$	$y_{45}$
$y_4$	$y_{10}$	$y_{16}$	$y_{22}$	$y_{28}$	$y_{34}$	$y_{40}$	$y_{46}$
$y_5$	$y_{11}$	$y_{17}$	$y_{23}$	$y_{29}$	$y_{35}$	$y_{41}$	$y_{47}$
$y_6$	$y_{12}$	$y_{18}$	$y_{24}$	$y_{30}$	$y_{36}$	$y_{42}$	$y_{48}$

<sup>1</sup>The last implementation scheme (TRMC-2) needed to solve a sub-system of equations. The existence of a sub-system turned out to be a weakness, which was pointed out by [4]. The new implementations do not have such weakness.

$X'_1$	$X'_2$	$X'_3$
$c_4$	$c_5$	$c_6$
$x_1$	$x_2$	$x_3$
$x_4$	$x_5$	$x_6$
$x_7$	$x_8$	$x_9$
$x_{10}$	$x_{11}$	$x_{12}$
$x_{13}$	$x_{14}$	$x_{15}$

$C_i$	denotes a $6 \times 6$ constant matrix
$L_i$	denotes a general linear function of $x_1, \dots, x_{45}$
$*$	denotes the multiplication of the big field
$\circ$	denotes the multiplication of matrices

The following are the maps  $\phi_2$  and  $\phi_3$ .

$$\begin{aligned}
 Y_1 &= X'_1 \\
 Y_2 &= X'_2 * X'_1 \\
 Y_3 &= X'_3 * X'_2 \\
 Y_4 &= X_4 * X_1 + X_3 * X_2
 \end{aligned}$$

$$\begin{bmatrix} Y_5 & Y_6 \\ Y_7 & Y_8 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix} \begin{bmatrix} X_5 & X_6 \\ X_7 & X_8 \end{bmatrix} = \begin{bmatrix} X_1 * X_5 + X_2 * X_7 & X_1 * X_6 + X_2 * X_8 \\ X_3 * X_5 + X_4 * X_7 & X_3 * X_6 + X_4 * X_8 \end{bmatrix}$$

$$\begin{aligned}
 y_{49} &= L_1 L_6 + L_2 L_7 + L_3 L_8 + L_4 L_9 + L_5 L_{10} \\
 y_{50} &= L_1 L_{11} + L_2 L_{12} + L_3 L_{13} + L_4 L_{14} + L_5 L_{15}
 \end{aligned}$$

$$\begin{aligned}
 Z_1 &= Y_1^2 \frac{Y_3}{Y_2} + C_1 \circ \frac{Y_5 Y_8 + Y_6 Y_7}{Y_4} = X'_1 X'_3 + C_1 \circ (X_5 X_8 + X_6 X_7) \\
 Z_2 &= Y_2 + C_2 \circ \frac{Y_5 Y_8 + Y_6 Y_7}{Y_4} = X'_2 X'_1 + C_2 \circ (X_5 X_8 + X_6 X_7) \\
 Z_3 &= Y_3 + C_3 \circ \frac{Y_5 Y_8 + Y_6 Y_7}{Y_4} = X'_3 X'_2 + C_3 \circ (X_5 X_8 + X_6 X_7) \\
 Z_4 &= Y_4 = X_4 X_1 + X_3 X_2 \\
 Z_5 &= Y_5 = X_1 X_5 + X_2 X_7 \\
 Z_6 &= Y_6 = X_1 X_6 + X_2 X_8 \\
 Z_7 &= Y_7 = X_3 X_5 + X_4 X_7 \\
 Z_8 &= Y_8 = X_3 X_6 + X_4 X_8 \\
 z_{49} &= y_{49} \\
 z_{50} &= y_{50}
 \end{aligned}$$

Note that we pad the system with two random polynomials and pad the first three equations with linear combinations of components in  $(X_5 X_8 + X_6 X_7)$ .

#### 4. AN ISSUE OF TERMINOLOGY

It is clear that the central maps of both HFE and TTM are degenerations of tractable rational maps. However, we don't claim that they are TRMCs. HFE has slower performance and TTM has poorer security. A TRMC should be hybrid. A tractable rational map has the following three features.

- It has stepwise triangular shape.
- It has permutation polynomials or  $k$ -polynomial permutations.
- It or its inverse map has rational forms.

A TRMC has to possess at least two features above.

#### 5. BRIEF SECURITY ANALYSIS

In general, methods to attack the public-key cryptosystem are either to break the public key or to break the encrypted message. The former aims at finding the private key, while the latter focus on finding the original message without finding the private key.

Some of the possible methods for breaking the encryption public key are:

- (1) Undetermined coefficients: Because of too many coefficients involved, it would be computationally infeasible.
- (2) Isomorphism Problem (IP): The method, proposed by Jacques Patarin et al., is not suitable for attacking cryptosystem of the present invention because the IP problem assume that the kernel map is fixed.
- (3) Searching the Patarin relations: It is easy to make the polynomial relation become complicated by carefully designing the tractable rational maps. It would be computationally infeasible.

Some of the possible methods for breaking the encrypted message are:

- (1) Brute force: When there are many variables, obviously the direct attack is computationally infeasible.
- (2) Solving nonlinear equations: Solving a system of nonlinear equations is known as a NP-complete problem. There are some of relatively efficient ways to solve the system of nonlinear equations such as relinearization scheme, XL scheme and Grobner basis method. However, the relinearization scheme is computationally infeasible to attack the present cryptosystem. The XL scheme and Grobner basis method need the assumption that the solution set at infinity is zero-dimensional. Hence, applying them to the present invention is in vain if we carefully design the tractable rational maps. Even without the mentioned problem, they are still computationally infeasible.
- (3) Searching the general Patarin relations: It is easy to make the polynomial relation become complicated by carefully designing the tractable rational maps. It would be computationally infeasible.

#### REFERENCES

- [1] J. Chen and B. Yang, B. Peng *Tame Transformation Signatures With Topsy-Turvy Hashes*, Proceedings of IWAP2002.
- [2] L. Goubin and N. T. Courtois, *Cryptanalysis of the TTM Cryptosystem*, p44-57, Lecture Notes in Computer Sciences 1976, Springer-Verlag, 2000.
- [3] Y. Hu, L. Wang, J. Chen, F. Lai and C. Chou, *An Implementation of Public Key Cryptosystem TTM with Linear Time Complexity for Decryption*. 2003 IEEE International Symposium on Information Theory.
- [4] A. Joux, S. Kunz-Jacques, F. Muller, P.-M. Ricordel, *Cryptanalysis of the Tractable Rational Map Cryptosystem*, PKC 2005, p258-274, Lecture Notes in Computer Sciences 3386.
- [5] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem*, p19-30, Lecture Notes in Computer Sciences 1666, Springer-Verlag, 1999.
- [6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., Vol. 20, Cambridge University Press.
- [7] T. Moh, *A Public System With Signature And Master Key Functions*, Communications in Algebra, 27(5), 2207-2222(1999).
- [8] T. Moh, *On The Method of XL and Its Inefficiency Against TTM*, Cryptology ePrint Archive (2001/047).
- [9] J. Patarin, N. Courtois, and J. Goubin, *Improved Algorithms for Isomorphisms of Polynomials*, p184-200, Lecture Notes in Computer Sciences 1070, Springer-Verlag, 1996.
- [10] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed. Prentice Hall, 1998.
- [11] L. Wang and F. Chang, *Square-free  $Q_k$  Components in TTM*, Taiwanese Journal of Mathematics, December 2003.
- [12] L. Wang, Y. Hu, F. Lai, C. Chou, and B. Yang, *Tractable Rational Map Signature*, PKC 2005, p244-257, Lecture Notes in Computer Sciences 3386.

LIH-CHUNG WANG : DEPARTMENT OF APPLIED MATHEMATICS, NATIONAL DONGHWA UNIVERSITY, SHOUFENG, HUALIEN 974, TAIWAN, R.O.C., FEI-HWANG CHANG : DEPARTMENT OF APPLIED MATHEMATICS, NATIONAL CHIAO TUNG UNIVERSITY, HSINCHU 300, TAIWAN, R.O.C.,

*E-mail address:* fax:(886)38662532