TRACTABLE RATIONAL MAP CRYPTOSYSTEM

LIH-CHUNG WANG AND FEI-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 $K\backslash\{0\}$. 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 χ_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 Lagrage interpolation formula, we obtain

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

Date: February 19, 2004.

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

$$K[x_1,\dots,x_n]/(x_1^{p^n}-x_1,\dots,x_n^{p^n}-x_n).$$

That is, if two polynomials define the same polynomial function, then the difference of these two polynomials is in the ideal $(x_1^{p^n}-x_1,\dots,x_n^{p^n}-x_n)$. 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^n-1, we can reduce the degree of such terms with the relation $x_i^{p^n}=x_i$.

A polynomial $r(x)\in K[x]$ is called a permutation polynomial of K if the associated polynomial function from K to K is a one-to-one and onto function. See ([5], Chapter9). 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 permutation polynomials of the finite field K. Note that a tractable rational map is probably only well-defined on a subset of the affine space K^n. Let

$$S=\{(x_1,\dots,x_n)\mid \prod_{j=2}^{n}p_j(x_1,\dots,x_{j-1})q_j(x_1,\dots,x_{j-1})g_j(x_1,\dots,x_{j-1})\neq 0\}.$$

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

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

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

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

we can get the pre-image of ϕ for each image point constructively. If we assume g_j, p_j and q_j in the above form to be non-vanishing polynomials, then $S = K^n$ and ϕ is an automorphism of K^n. Although every map over K^n is a polynomial map, the motivation for using the rational expressions is for computational reason. For example, if we want to express $\frac{1}{x}$ as a polynomial x^{p^n-2}, the degree of the polynomial will be pretty high.

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 $GF(2^{16})[s]/(s^2+s+(\alpha_2 t+\alpha_3))$. A variable $X_{1,2}$ in $GF(2^{16})$ can be represented by $x_1 t+x_2$ (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 varialbe $X_{1,2,3,4}$ 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 $X \longmapsto X^2$ is a linear transformation of $GF(2^{32})$. Similarly, a map $X \longmapsto X^{2^8}$ 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, $X_{1,2,3,4}^{257}$ and $X_{1,2,3,4}^{256+65536}$ 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 (one pass)

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

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \phi_1 \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}, \quad \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \phi_2 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \phi_3 \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

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

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \phi_3 \circ \phi_2 \circ \phi_1 \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$$

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

$$\begin{array}{rcl} Y_{1,2} & = & r(X_{1,2}) \\ y_3 & = & x_3 + x_1 x_2 \end{array}$$

wherein $r(X_{1,2})$ is a permutation polynomial which can be represented by 2 qudratic polynomials with variables in $GF(256)$. i.e., $r(X_{1,2}) = \sum a_{ij} X_{1,2}^{256^i} X_{1,2}^{256^j}$. However, it is slow to compute the solutions of a general equation of hige degree $Y_{1,2} = r(X_{1,2})$ and it is hard to find such permutation polynomails. Hence, this HFE-like method is not a good choice.

Toy Example 2 (one pass)

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, ρ is the standard injection and π 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 $\{\pi \circ \phi_2 \circ \rho\}$.

$$
\begin{array}{lclcl}
z_1 & = & y_3 & = & x_3 + x_1 x_2 \\
z_2 & = & y_4 & = & x_4 + x_2 x_3 \\
z_3 & = & y_5 & = & x_5 + x_3 x_4 \\
Z_{4,5} & = & Y_{6,7} & = & X_{1,2}(X_{3,5}^{256} + X_{3,5} + a) \\
Z_{6,7} & = & Y_{8,9} & = & X_{1,2}(X_{4,5}^{256} + X_{4,5} + a) \\
Z_{8,9} & = & Y_{10,11} & = & (X_{3,5}^{256} + X_{3,5} + a)(X_{4,5}^{256} + X_{4,5} + a)
\end{array}
$$

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 (two pass)

Here we would like to show that the composition of two tractabel rational maps can be represented by a polynomial map of degree two. In this example all variables are in $GF(2^{16})$.

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

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

wherein $f(Y_4, Y_6) = (X_1^{256} + X_1 + a)(X_4^{256} + X_4 + a)$ is a sysmetric polynomail 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.

Preferred Implementation

The embodiment uses the five maps $\{\phi_1, \rho, \phi_2, \pi, \phi_3\}$ to be the private key.

$$
\begin{pmatrix} x_1 \\ \vdots \\ x_{40} \end{pmatrix} = \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_{40} \end{pmatrix}, \quad
\begin{pmatrix} u_1 \\ \vdots \\ u_{62} \end{pmatrix} = \rho \begin{pmatrix} x_1 \\ \vdots \\ x_{40} \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_{40} \\ 0 \\ \vdots \\ 0 \end{pmatrix}
$$

$$
\begin{pmatrix} y_1 \\ \vdots \\ y_{62} \end{pmatrix} = \phi_2 \begin{pmatrix} u_1 \\ \vdots \\ u_{62} \end{pmatrix}
$$

$$\begin{pmatrix} z_1 \\ \vdots \\ z_{48} \end{pmatrix} = \pi \begin{pmatrix} y_1 \\ \vdots \\ y_{62} \end{pmatrix} = \begin{pmatrix} y_{15} \\ \vdots \\ y_{62} \end{pmatrix}, \quad \begin{pmatrix} w_1 \\ \vdots \\ w_{48} \end{pmatrix} = \phi_3 \begin{pmatrix} z_1 \\ \vdots \\ z_{48} \end{pmatrix}$$

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

$$\begin{pmatrix} w_1 \\ \vdots \\ w_{48} \end{pmatrix} = \phi_3 \circ \pi \circ \phi_2 \circ \rho \circ \phi_1 \begin{pmatrix} m_1 \\ \vdots \\ m_{40} \end{pmatrix}$$

That is, the composition consists of 50 quadratic polynomials of 40 variables. Because $\{\phi_1, \phi_3\}$ are just invertible affine transformations, for convenience, we only list $\{\pi \circ \phi_2 \circ \rho\}$.

$$\begin{array}{lllll}
Z_{1,\ldots,4} & = & Y_{15,\ldots,18} & = & X_{15,\ldots,18}(X_{2,\ldots,5}^{256} + X_{2,\ldots,5} + a) + bX_{6,\ldots,9}X_{10,\ldots,13} \\
z_5 & = & y_{19} & = & x_{19} + f_1(x_1, \ldots, x_{18}) \\
z_6 & = & y_{20} & = & x_{20} + f_2(x_1, \ldots, x_{19}) \\
z_7 & = & y_{21} & = & x_{21} + f_3(x_1, \ldots, x_{20}) \\
z_8 & = & y_{22} & = & x_{22} + f_4(x_1, \ldots, x_{21}) \\
z_9 & = & y_{23} & = & x_{23} + f_5(x_1, \ldots, x_{22}) \\
z_{10} & = & y_{24} & = & x_{24} + f_6(x_1, \ldots, x_{23}) \\
Z_{11,\ldots,26} & = & Y_{25,\ldots,40} & = & X_{25,\ldots,40}(X_{7,\ldots,22}^{256} + X_{7,\ldots,22} + c) + F_{7,\ldots,22}(x_1, \ldots, x_{24}) \\
Z_{27,28} & = & Y_{41,42} & = & Q_2(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{29,30} & = & Y_{43,44} & = & Q_3(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{31,32} & = & Y_{45,46} & = & Q_4(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{33,34} & = & Y_{47,48} & = & Q_5(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{35,36} & = & Y_{49,50} & = & Q_6(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{37,38} & = & Y_{51,52} & = & Q_7(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{39,40} & = & Y_{53,54} & = & Q_8(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{41,42} & = & Y_{55,56} & = & Q_9(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{43,44} & = & Y_{57,58} & = & Q_{10}(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{45,46} & = & Y_{59,60} & = & Q_{11}(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14}) \\
Z_{47,48} & = & Y_{61,62} & = & Q_{12}(X_{1,2}, X_{3,4}, X_{5,6}, X_{7,8}, X_{9,10}, X_{11,12}, X_{13,14})
\end{array}$$

wherein $(X^{256} + X + a)$ is a non-vanishing polynomial over $GF(2^{64})$, $(X^{256} + X + c)$ is a non-vanishing polynomial over $GF(2^{128})$, f_i's and $F_{5,\ldots,24}$ are general quadratic polynomials with variables in $GF(2^8)$ and $Q_i(X_{1,2}, \ldots, X_{15,16})$'s are general quadratic polynomials of 8 variables in $GF(2^{16})$ which have the unique solution. For decryption, the bottle neck is to find the solution of last 13 equations. With the XL method and some pre-calculation tricks, it is still faster than most of public-key systems. We will come back somewhere else for the complete performance estimate and security analysis. However, for attacks, they need to find the solution of 50 quadratic polynomials of 40 variables, which is computationally infeasible with XL or Grobner basis method.

4. 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 kernal 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.* To appear in 2003 IEEE International Symposium on Information Theory.

[4] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem*, p19-30, Lecture Notes in Computer Sciences 1666, Springer-Verlag, 1999.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., Vol. 20, Cambridge University Press.

[6] T. Moh, *A Public System With Signature And Master Key Functions*, Communications in Algebra, 27(5), 2207-2222(1999).

[7] T. Moh, *On The Method of XL and Its Inefficiency Against TTM*, Cryptology ePrint Archive (2001/047).

[8] J. Patarin, N. Courtois, and J. Goubin, *Improved Algorithms for Isomorphisms of Polynomials*, p184-200, Lecture Notes in Computer Sciences 1070, Springer-Verlag, 1996.

[9] W. Stallings, *Cryptography and Network Security: Principles and Pratice*, 2nd ed. Prentice Hall, 1998.

[10] L. Wang and F. Chang, *Square-free Q_k Components in TTM*, To appear in Taiwanese Journal of Mathematics, December 2003.

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`