Construction of the Tsujii-Shamir-Kasahara (TSK) Type Multivariate Public Key Cryptosystem, which relies on the Difficulty of Prime Factorization

Shigeo Tsujii Kohtaro Tadaki Masahito Gotaishi Ryou Fujita

Research and Development Initiative, Chuo University
1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan

Abstract. A new multivariate public-key cryptosystem (MPKC) with the security based on the difficulty of the prime factoring is proposed. Unlike conventional cryptosystems such as RSA, most MPKCs are expected secure against quantum computers, and their operation of encryption and decryption is expected quick, because they do not need exponential operation. However, their security against quantum computers is very difficult to prove mathematically. We propose a new MPKC based on sequential solution method, assuming the security against von Neumann computers, whose attack seems as difficult as prime factoring. This cryptosystem is applicable to both encryption and signature.

Key words: public key cryptosystem, multivariate public key cryptosystem, sequential solution method, prime factorization, Tsujii-Shamir-Kasahara Type MPKC

1 Introduction

Multivariate Public-Key Cryptosystems (MPKC) has its origin in the ones structured by a univariate polynomial on an extended field, the first of which was proposed by Matsumoto and Imai [15] in 1983, and the ones of sequential solution method, proposed by Tsujii[24] in 1985. The proposed MPKCs are faster than RSA or elliptic curve cryptosystem in encryption and decryption, because MPKC does not include any exponentiation. Moreover, typically the degree of the MPKC public keys is as low as two. As a lightweight cryptosystem, they were initially expected to be used for RFIDs or IC cards. After that, the variants of MPKCs were actively proposed worldwide around the beginning of 1990s. Nonetheless, in spite of the numerous proposals published in papers, a provably secure, efficient systems has not been proposed yet.

Original purpose of the development of MPKC in the 1980s in Japan was to develop a public key cryptosystem faster than RSA. But in 1994, when it was shown that the problems of number theory such as prime factorization and discrete logarithm could be computed in polynomial time if quantum computers are put into practical use [22], MPKCs were focused as one of the likely candidates of the 'Post-Quantum Cryptosystem.' If these problems of number theory were to be computed efficiently, most of the existing public-key cryptosystems including RSA and ElGamal would be threatened. Since solving the system of algebraic equations is **proved** to be NP-complete and there has not been an efficient algorithm for quantum computers to solve them is not discovered yet, MPKCs has been expected to remain secure even in the post-quantum society. Consequently MPKCs has been actively developed worldwide. Currently MPKC is regarded as a likely candidate of

post-quantum cryptosystems and therefore the textbook of post-quantum cryptosystem [2] spends considerable length of chapters on them. A dedicated textbook illustrating the existing MPKCs and cryptanalysis was published in 2006[4]

Hence currently MPKCs are expected to be a lightweight public key with quick encryption and decryption, and a post-quantum cryptosystem, which is secure against the attacks by quantum computers.

However, we assume that the practical use of the quantum computer is not realized in the near future and consequently lifted the constraint that the MPKCs should be 'secure against quantum computers.' Instead, the proposed system makes the best of the advantage that it is far faster in encrypting and decrypting data. Additionally, the system is applicable to both encryption and signature.

Based on this prospect, we propose an MPKC provably secure as long as the prime factorization is difficult. The concept of the 'security as long as the prime factorization is difficult' means that finding the roots a, b, p, q of the following equation:

$$ap + bq = c \mod N \quad (N = pq, \ \ a, \ b \in \mathbb{Z}_N)$$

where only N, c, and the relation between the variables $N = pq$ are given, is equally as difficult as factoring the large integer N.

2 History of MPKC and the Position of this Paper

The history of the progress of MPKC is shown in the Figure 1 and the Table 1.

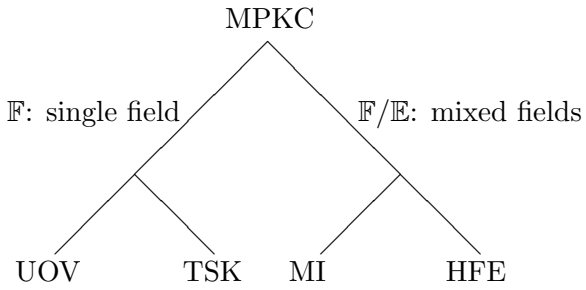

Figure 1: Classification of MPKC [27]

An MPKC was designed by making skillful use of the expression of univariate polynomials on extended fields, by Matsumoto and Imai [14]. This cryptosystem, which is currently called Matsumoto-Imai (MI) Cryptosystem, was presented in EUROCRYPT in 1988. MI Cryptosystem was successfully cryptanalyzed by Patarin [17] in 1995. After that, Patarin invented a new MPKC by expanding the concept of MI, which was named Hidden Field Equation (HFE) Cryptosystem [18]. Although cryptosystems of MI-HFE type have been developed and improved for a long time, there is not any efficient cryptosystem with provable security [5][8].

In 1985, Tsujii[24] proposed Sequential Solution Method [4][24][23], which was compiled in a paper[23] in 1986. However, it was cryptanalyzed by Kaneko et al.[9]. Tsujii et al. improved the Sequential Solution Method and its reinforced version was proposed in 1989[25]. This method, rational map, was cryptanalyzed by Ding et al., [7] about 10 years after its emergence. Adi Shamir

Table 1: Progress of MPKC

type	1980s	1990s	2000s
MI-HFE (Matsumoto-Imai, Patarin)	MI Cryptosystem (1983) (encryption/signature) by Matsumoto, Imai et al. [14, 15]	HFE Cryptosystem (1996) (encryption/signature) by Patarin [18]	SFLASHv3 signature (2003) by Courtois et al. [16] QUARTZ signature (2001) by Patarin et al. [20]
TSK (Tsujii, Shamir, Kasahara-Sakai)	Sequential Solution Method (1985) (encryption) by Tsujii [24]	Birational Permutation Signature Scheme (1993) by Shamir [21]	Random (Singular) Simultaneous Equations (2004) (encryption/signature) by Kasahara-Sakai [10, 11]
OV-UOV signature (Patarin et al.)		OV signature (1997) by Patarin [19] UOV signature (1999) by Kipnis et al. [12]	Rainbow signature (2005) by Ding et al. [6]
Algebraic Surface Cryptosystem (Akiyama et al.)			Algebraic Surface Cryptosystem (2009) by Akiyama et al. [1]

also proposed the Sequential Solution Method for signature (birational permutation)[21], independently of Tsujii. His system was cryptanalyzed by Coppersmith, et al [3].

After the year 2000, Kasahara et al. presented some generalized structures of sequential solution method [10][11]. The systems based on sequential solution method is called Tsujii-Shamir-Kasahara (TSK) cryptosystem in this paper.

Although TSK systems have been further studied since they were proposed, an efficient and secure cryptosystem is not established yet.

There are two kinds of MPKCs, MI-HFE and TSK, which are utilized for both encryption and signature. There are also some other systems, as shown in the Table 1.

As for the cryptosystems used exclusively for signature, there is the Oil and Vinegar type, which was proposed by Patarin [19]. After it was cryptanalyzed by Kipnis et al. [13], Patarin et al. proposed Unbalanced Oil and Vinegar (UOV), an improved version of Oil and Vinegar. Although UOV signature is currently surviving without being attacked, its security is not proved yet.

There are following kinds of attacks to MPKCs:

(i) Gröbner Bases Attack (including XL Attack)

(ii) Rank Attacks

(iii) Others

Gröbner Bases attack is a general way of an attack, which does not depend on some specific structure of the trapdoors. Rank attack focuses on the difference of the rank between the polynomials of the central map. Majority of the MPKCs have been successfully attacked by either Gröbner Bases or Rank attack.

3 Problem of Polynomial Algebra, with the equivalent difficulty as the Prime Factoring

A basic problem of polynomial algebra with the equivalent difficulty as the prime factorization is proposed in this section.

3.1 Preparation

Two large prime numbers p, q are selected. M^T means the transposed matrix of a matrix M.

Two prime numbers p, q are selected. $N := pq$

The plain text vector $\boldsymbol{x}$ is an m-dimentional vector, with each element defined on the residue class ring $\mathbb{Z}_N$.

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_m)^T, x_i \in \mathbb{Z}_N, i = 1, 2, \ldots, m$$

Two m-dimentional random polynomial vector $\boldsymbol{A}(\boldsymbol{x}), \boldsymbol{B}(\boldsymbol{x})$ are generated:

$$\boldsymbol{A}(\boldsymbol{x}) = (a_1(\boldsymbol{x}), a_2(\boldsymbol{x}), \ldots, a_m(\boldsymbol{x}))$$
$$\boldsymbol{B}(\boldsymbol{x}) = (b_1(\boldsymbol{x}), b_2(\boldsymbol{x}), \ldots, b_m(\boldsymbol{x}))$$

Subsequently, an m-dimensional quadratic polynomial vector $\boldsymbol{C}(\boldsymbol{x})$ on the residue class ring $\mathbb{Z}_N$ is defined using $p, q, \boldsymbol{A}(\boldsymbol{x}), \boldsymbol{B}(\boldsymbol{x})$

$$\boldsymbol{C}(\boldsymbol{x}) := (c_1(\boldsymbol{x}), c_2(\boldsymbol{x}), \ldots, c_m(\boldsymbol{x}))^T = \boldsymbol{A}(\boldsymbol{x})p + \boldsymbol{B}(\boldsymbol{x})q \tag{1}$$

With the above assumption, the problem of finding the prime numbers p, q from the value of $\boldsymbol{C}(\boldsymbol{x})$ for a given value of $\boldsymbol{x}$, with $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$ confidential, is discussed. This problem is called "prime factorization problem with additional information." Then the following theorem is true:

Theorem 3.1. *The following two conditions are equivalent.*

(i) Prime factorization is difficult.

(ii) Prime factorization with additional information is difficult.

The proof of theorem 3.1 is provided in the subsection 3.2.

3.2 Proof of the Theorem 3.1

n is a security parameter. And for all positive integer l, $\mathbb{Z}_l$ is a set $\{0, 1, 2, \ldots, l-1\}$. First of all, the following experiment about the probablistic algorithm $\mathcal{A}$ and the security parameter n is discussed:

The factoring experiment $\mathsf{Factor}_{\mathcal{A}}(n)$:
1. Choose a pair (p, q) of two distinct $n/2$-bits primes uniformly.
2. Set $N := pq$.
3. $\mathcal{A}$ is given N, and outputs $p', q' > 1$.
4. The output of the experiment is defined to be 1 if $p'q' = N$, and 0 otherwise.

Definition 3.2. *The remark that "**A prime factoring problem is difficult**," means that following proposition is true:*

For all probabilistic algorithm $\mathcal{A}$ and security parameter d, exists a certain positive integer n_0 such that the following inequation is true for any $n > n_0$,

$$\Pr[\mathsf{Factor}_{\mathcal{A}}(n) = 1] \leq \frac{1}{n^d}$$

Let ℓ be a certain univariate polynomial with all its coefficients are positive integers. the following experiment is discussed about a given probabilistic polynomial time algorithm $\mathcal{A}$ and a security parameter n:

The factoring experiment with additional information $\mathsf{Factor\text{-}AddInfo}_{\mathcal{A}}(n)$:
1. Choose a pair (p, q) of two distinct $n/2$-bits primes uniformly.
2. Set $N := pq$.
3. Set $m := \ell(n)$.
4. Choose $a \in \mathbb{Z}_N[x_1, \ldots, x_m]^m$ of total degree two uniformly.
5. Choose $b \in \mathbb{Z}_N[x_1, \ldots, x_m]^m$ of total degree two uniformly.
6. Set $c := pa + qb$.
7. $\mathcal{A}$ is given N, c, and outputs $p', q' > 1$.
8. The output of the experiment is defined to be 1 if $p'q' = N$, and 0 otherwise.

Definition 3.3. *The remark that "**A prime factoring problem with additional information is difficult**" means that the following proposition is true:*
For all probabilistic polynomial time algorithm $\mathcal{A}$ and all positive integer d, exists a positive integer n_0 such that following inequation is true.

$$\Pr[\mathsf{Factor\text{-}AddInfo}_{\mathcal{A}'}(n) = 1] \leq \frac{1}{n^d}$$

With the above preparation, the following theorem is proved.

Theorem 3.4. *The following two conditions are equivalent.*

(i) Prime factorization is difficult.

(ii) Prime factorization with additional information is difficult.

The preposition that (ii)$\Longrightarrow$(i) is proved first.

The proof of (ii)$\Longrightarrow$(i) in the Theorem 3.4

Let $\mathcal{A}$ be a probabilistic polynomial-time algorithm into which positive integer n_0 is input. Based on $\mathcal{A}$, a probabilistic polynomial-time algorithm $\mathcal{A}'$ is structured:

$\mathcal{A}'$ has input parameters of positive integers and polynomial vectors. But $\mathcal{A}'$ ignores the polynomial vectors and starts $\mathcal{A}$ with only positive integers as its input. Then following inequality is true for any $n > n_0$.

$$\Pr[\mathsf{Factor}_{\mathcal{A}}(n) = 1] = \Pr[\mathsf{Factor\text{-}AddInfo}_{\mathcal{A}'}(n) = 1] \tag{2}$$

Now it is assumed that prime factorization problems with additional information are difficult. Then n_0 for any positive integer d, exists a positive integer n_0 such that following inequality is true:

$$\Pr[\mathsf{Factor\text{-}AddInfo}_{\mathcal{A}'}(n) = 1] \leq \frac{1}{n^d}$$

Since $\mathcal{A}$ can be arbitrary, it is conculded from the formula (2) that prime factorization is difficult.

Next (ii)$\Longrightarrow$(i) is proved. Beforehands following Lemma needs to be proved. Here $\#S$ means the number of the elements of a given finite set S.

Lemma 3.5. *Let p and q be two prime numbers. Let $N = pq$. Mapping $F : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ is defined as follows:*

$$F(x, y) = (px + qy) \mod N$$

Then we have following equality for all $z \in \mathbb{Z}_N$.

$$\#F^{-1}(\{z\}) = N \tag{3}$$

[Proof] Since both p and q are prime, there exist integers x_0, y_0 such that $px_0 + qy_0 = 1$. Subsequently, a subset S_z of $\mathbb{Z}_N \times \mathbb{Z}_N$ is defined as:

$$S_z := \{((x_0 z + q\alpha) \mod N, (y_0 z + p\beta) \mod N) \mid \alpha \in \mathbb{Z}_p, \beta \in \mathbb{Z}_q\}$$

It should be noted that for all $z \in \mathbb{Z}_N$, we have the equality:

$$F(S_z) = z$$

Therefore for any different elements $z, z' \in \mathbb{Z}_N$, we have the equality:

$$S_z \cap S_{z'} = \emptyset$$

On the other hand, since $\#\mathbb{Z}_p = p$ and $\#\mathbb{Z}_q = q$, for all $z \in \mathbb{Z}_N$, we have the following relation:

$$\#S_z = pq = N$$

(end of the proof)

Based on the Lemma 3.5, (i)$\Longrightarrow$(ii) in the Theorem 3.4 is proved as follows:

The proof of (i)$\Longrightarrow$(ii) in the Theorem 3.4

Here following experiment about a given probabilistic polynomial time algorithm $\mathcal{A}$ and a security parameter n:

The factoring experiment with dummy information $\mathsf{Factor\text{-}DmmyInfo}_{\mathcal{A}}(n)$:

1. Choose a pair (p, q) of two distinct $n/2$-bits primes uniformly.
2. Set $N := pq$.
3. Set $m := \ell(n)$.
4. Choose $\boldsymbol{c} \in \mathbb{Z}_N[x_1, \ldots, x_m]^m$ of total degree two uniformly.
5. $\mathcal{A}$ is given $N, \boldsymbol{c}$, and outputs $p', q' > 1$.
6. The output of the experiment is defined to be 1 if $p'q' = N$, and 0 otherwise.

Based on the Lemma 3.5, the polynomial vector $\boldsymbol{c}$ generated by the step 4-6 of the Factor-AddInfo$_{\mathcal{A}}(n)$ is homogeneously generated from a set of quadratic polynomial vectors in $\mathbb{Z}_N[x_1, \ldots, x_m]^m$. Consequently for a given probabilistic polynomial time algorithm $\mathcal{A}$ and a security parameter n, we have the following equality:

$$\Pr[\text{Factor-AddInfo}_{\mathcal{A}}(n) = 1] = \Pr[\text{Factor-DmmyInfo}_{\mathcal{A}}(n) = 1]$$

Here let $\mathcal{A}$ be a given probabilistic polynomial-time algorithm, which has positive integers and polynomial vectors as its inputs. Based on the algorithm $\mathcal{A}$, a probabilistic polynomial-time algorithm $\mathcal{A}'$ is structured as follows:

$\mathcal{A}'$ has the positive integer N as its input. $\mathcal{A}'$ generates a quadratic polynomial vector $\boldsymbol{c}$ homogeneously. After that, it invokes the algorithm $\mathcal{A}$ inputing N and $\boldsymbol{c}$. Then we have the following equality for a given security parameter n:

$$\Pr[\text{Factor-DmmyInfo}_{\mathcal{A}}(n) = 1] = \Pr[\text{Factor}_{\mathcal{A}'}(n) = 1] \tag{4}$$

Here it is assumed that the prime factorization is difficult. Then for all positive integer d, there exists a positive integer n_0 such that for all $n > n_0$,

$$\Pr[\text{Factor}_{\mathcal{A}'}(n) = 1] \leq \frac{1}{n^d} \tag{5}$$

Since $\mathcal{A}$ can be any algorithm, it is led from the equation (4) and (5) that a prime factorization problem with additional information is difficult.

4 Structure of the Proposed System and the Trapdoor

Considering both the progress of the quantum computer technology and the progress of the development of MPKCs as the post-quantum cryptosystem, the constraint that 'MPKCs should be secure against quantum computers,' is lifted in this section. Here the advantage of quick 'encryption/decryption' or 'signature/verification' is pursued. We are going to formulate an MPKC whose security relies on the difficulty of prime factoring. In general, MPKCs are structured as shown in Figure 2 and 3.

The key point lies in the trapdoor structure included in the central map $\boldsymbol{G}(\boldsymbol{z})$.

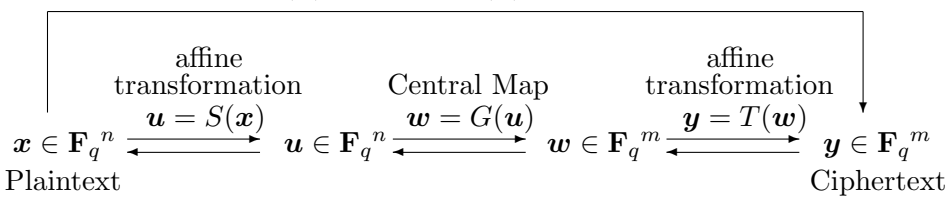

Figure 2: Formulation of MPKC Encryption System

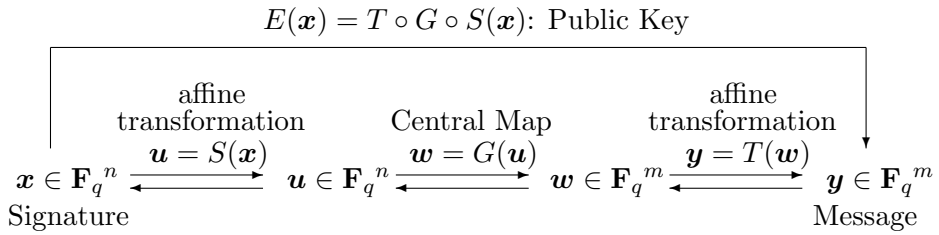

Figure 3: Formulation of MPKC Signature System

As shown in the Figure 4, the central map of the proposed system has the structure of:

Prime Number		Random Quadratic Polynomial Vector		Prime Number		Random Quadratic Polynomial Vector
p	$\times$	$\boldsymbol{A}(\boldsymbol{u})$	$+$	q	$\times$	$\boldsymbol{B}(\boldsymbol{u})$

The cryptosystem is structured as follows:

4.1 Preparation of Public Key and Private Key

(i) Two prime numbers p, q are selected. $N := pq$

(ii) The plain text vector $\boldsymbol{x}$ is an m-dimentional vector, with each element defined on the residue class ring $\mathbb{Z}_N$

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_m)^T,\ x_i \in \mathbb{Z}_N,\ i = 1, 2, \ldots, m$$

(iii) m-dimensional affine transformation is expressed as S.

(iv) The variable $\boldsymbol{x}$ is transformed to the intermediate variable $\boldsymbol{u}$ by the affine transformation S: $\boldsymbol{u} := S(\boldsymbol{x})$

(v) The central map is $\boldsymbol{G}(\boldsymbol{u})$. The intermediate variable vector $\boldsymbol{w}$ is expressed as $\boldsymbol{w} := \boldsymbol{G}(\boldsymbol{u})$.

(vi) Let T be an m-dimensional affine transformation.

(vii) m-dimensional polynomial vector (public key) is expressed as $\boldsymbol{E}(\boldsymbol{x}) = (e_1(\boldsymbol{x}), e_2(\boldsymbol{x}), \ldots, e_m(\boldsymbol{x}))$

(viii) Two m-dimensional random polynomial vectors $\boldsymbol{A}(\boldsymbol{x}),\ \boldsymbol{B}(\boldsymbol{x})$ are expressed as:

$$\boldsymbol{A}(\boldsymbol{x}) = (a_1(\boldsymbol{x}), a_2(\boldsymbol{x}), \ldots, a_m(\boldsymbol{x}))^T,\quad \boldsymbol{B}(\boldsymbol{x}) = (b_1(\boldsymbol{x}), b_2(\boldsymbol{x}), \ldots, b_m(\boldsymbol{x}))^T$$

(ix) The quadratic polynomial vector $\boldsymbol{G}(\boldsymbol{u})$ is defined as the function of $p,\ q,\ \boldsymbol{A}(\boldsymbol{u}),\ \boldsymbol{B}(\boldsymbol{u})$

$$\boldsymbol{G}(\boldsymbol{u}) = (g_1(\boldsymbol{u}), g_2(\boldsymbol{u}), \ldots, g_m(\boldsymbol{u}))^T = p\boldsymbol{A}(\boldsymbol{u}) + q\boldsymbol{B}(\boldsymbol{u}) \tag{6}$$

The central map is structured by Sequential Solution Method, which is explained in Figure 4 and equation (7).

With the above assumption, Keys are defined as follows:
Secret Key: $p,\ q,\ \boldsymbol{A}(\boldsymbol{u}),\ \boldsymbol{B}(\boldsymbol{u}),\ S,\ T$
Public Key: $N,\ \boldsymbol{E}(\boldsymbol{x}) = (e_1(\boldsymbol{x}), e_2(\boldsymbol{x}), \ldots, e_m(\boldsymbol{x}))^T$

Encryption: Plaintext values are assigned to the variables of the public key $\boldsymbol{E}(\boldsymbol{x})$ to generate the ciphertext vector $\boldsymbol{y} := (y_1, y_2, \ldots, y_m)^T$.

Decryption:

(i) The affine transformation T is inverted to the ciphertext to find the intermediate variable vector.

$$\boldsymbol{w} := (w_1, w_2, \ldots, w_m)^T = T^{-1}(\boldsymbol{y})$$

(ii) The intermediate vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_m)^T$ is computed from $\boldsymbol{w}$ using Chinese Remainder Theorem and Sequential Solution Method.

(iii) The affine transformation S is inverted to $\boldsymbol{u}$ to recover the plaintext.

The Sequential Solution Method has the structure, as shown in the formula (7), that the number of variables decreases one by one, as the sequence number of the polynomial increases. Each element is a random polynomial of the given variables. Affine transformations are applied from the both sides to make the central map secret.

$$\begin{array}{rcl} w_1 & = & h_1(u_1, u_2, \ldots, u_{m-1}, u_m) \\ w_2 & = & h_2(u_1, u_2, \ldots, u_{m-1}) \\ \vdots & & \\ w_{m-1} & = & h_{m-1}(u_1, u_2) \\ w_m & = & h_m(u_1) \end{array} \tag{7}$$

In the decryption process, the univariate polynomial, w_m of the equation system of the central map is solved to find u_1. Subsequently the root of $h_m(u_1) - w_m = 0$ is assigned to $h_{m-1}(u_1, u_2)$ to make it a univariate quadratic equation. In this way intermediate variables are computed in sequence. These two polynomial vectors, $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$, both of which has the structure of Sequential Solution Method, are combined symmetrically, with $\boldsymbol{A}(\boldsymbol{x})$ multiplied with p and $\boldsymbol{B}(\boldsymbol{x})$ with q to complement each other. The complementary structure of the central map is illustrated in Figure 4. The original Sequential Solution Method has the weakness that the element $w_m(u_1)$ is univariate. However, all elements include all variables by combining two Sequential Solution Method Structures in the proposed system.

This MPKC system is expected to have security against typical attacks such as Gröbner Bases and Rank Attacks.

It should be noted that this system is virtually bijection. Any given vector $\boldsymbol{y} \in \mathbb{Z}_N^m$ has a single pre-image of the map $\boldsymbol{E}$ with very high probability. Therefore this system is also applicable to signatures. Moreover, this signature system can be *determined*. Compared with the UOV, whose signature is more than three times as long as the message, this signature system is quite efficient compared with the existing MPKCs such as UOV. Although UOV is believed to be the most secure among all MPKC signature trapdoors. In the UOV system, signature is at least 3 times as long as the message. Additionally, although UOV system has not cryptanalyzed since its presentation in

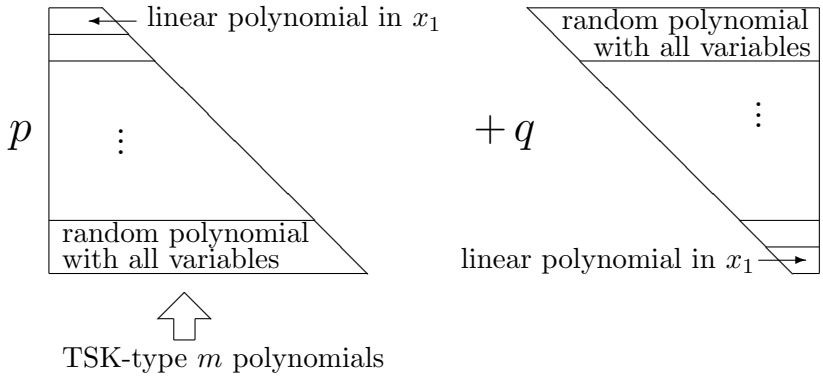

Figure 4: Structure of Central Map

1999, its security is not proved yet. The proposed TSK system is assured of its security equivalent for prime factorization.

The brief concept of this cryptosystem was presented in Japanese [26].

5 Evaluation of Security

5.1 Security against Prime Factorization

Based on Theorem 1, considering the randomness of $\boldsymbol{A}(\boldsymbol{u})$ and $\boldsymbol{B}(\boldsymbol{u})$, and the two affine transformations S and T, the proposed system is secure against prime factorization.

5.2 Security against Gröbner Bases Attack

About each polynomial, as shown in the theorem 3.1, the security is assured by the difficulty of prime factorization. Since all coefficients of $\boldsymbol{A}(\boldsymbol{u})$ and $\boldsymbol{B}(\boldsymbol{u})$ are independent of each other, there is no dependency among polynomials. Hence all of the polynomials are independent of each other. Therefore theorem 3.1 is applicable. Consequently, it is impossible to find the plaintext of this system by computing the Gröbner Bases, as long as p and q are sufficiently large.Tranditionally the majority of the MPKC are defined on small fields such as $\boldsymbol{F}_2$ and the number of variables is larger than 100.

Usually the first thing to do in evaluating the security of MPKCs is solving the equation system $\boldsymbol{E}(\boldsymbol{x}) = \boldsymbol{y}$. The typical way of solvng the system is computing the Gröbner Bases of the ideal $\langle \boldsymbol{E}(\boldsymbol{x}) = \boldsymbol{y} \rangle$. When the polynomials are defined on a finite field $GF(q)$, all variables satisfy $x_i^q = x_i$. Therefore the set of field equations $(x_1^q - x_1, \ldots, x_m^q - x_m)$ is appended to the generators in computing the Gröbner Bases. Thus computed Gröbner Bases include m or slightly fewer linear polynomials, as long as the public key $\boldsymbol{E}(\boldsymbol{x})$ is determined. Without the field equations computation of Gröbner Bases becomes too memory-consuming to proceed normally. But if the polynomials are defined on a residue class ring with large characteristics, field equations do exist, but it is difficult to find an integer d such that $x_i^d = x_i$. Additionally, even when the computation terminates normally, resulting Gröbner Bases include no or only few linear elements. Therefore it would be impossible to attack the system by computing Gröbner Bases.

We briefly tested Gröbner Bases attack for small parameters $p = 5; q = 7; m = 10$ with and without field equations. Computation time was compared with that for random polynomials. The time was approximately the same as for random polynomials. In some cases it took longer than attacking random polynomials. When field equations are not used, there was not so much difference between the public key and random polynomials. The resulting Gröbner bases contain only few linear elements. Therefore it is expected that the structure of the public key $\boldsymbol{E}(\boldsymbol{x})$ is expected to be as secure against Gröbner Bases attack as random polynomials. The security against Gröbner Bases attack would have to be studied further in the future with experiments and theoretical discussion.

5.3 Security against Rank Attack

All polynomials of the central map has the rank m, with all variables included. Therefore, although this system is a variant of TSK type MPKC, rank attack does not work. The proposed system is secure against rank attacks.

6 Conclusion

The structure of an MPKC, with the security assured by the difficulty of prime factoring, is described. The system proposed here is an example and there are several combinations of existing cryptosystems for $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$. The cryptosystems considered in this paper are the sequencial solution methods. But it is possible to choose other cryptosystems such as MI or HFE. The possibility of likely combinations of the cryptosystems and their usage should be studied further in the future. Additionally, the encryption and decryption are expected to be made faster compared with RSA or Elliptic Curve. We are going to discuss the matter further.

Acknowledgment

The authors greatly appreciate Professor Masao Kasahara of Osaka Gakuin University and Dr. Ryuichi Sakai of Osaka Electro-Communication Univerisity, both of whom have had active and fruitful discussion with authors and have given important advices and encouragement.

References

[1] Koichiro Akiyama, Yasuhiro Goto, and Hideyuki Miyake, *An Algebraic Surface Cryptosystem*, Public Key Cryptography PKC 2009 (Stanislaw Jarecki and Gene Tsudik, eds.), Lecture Notes in Computer Science, vol. 5443, Springer Berlin / Heidelberg, 2009, pp. 425–442.

[2] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen (eds.), *Post-Quantum Cryptography*, Springer, 2009.

[3] Don Coppersmith, Jacques Stern, and Serge Vaudenay, *Attacks on the Birational Permutation Signature Schemes*, Advances in Cryptology – CRYPTO '93 (Douglas Stinson, ed.), Lecture Notes in Computer Science, vol. 773, Springer Berlin / Heidelberg, 1994, pp. 435–443.

[4] Jintai Ding, Jason E. Gower, and Dieter Schmidt, *Multivariate Public Key Cryptosystems (Advances in Information Security)*, Springer-Verlag New York, Inc., 2006.

[5] Jintai Ding and Timothy Hodges, *Inverting hfe systems is quasi-polynomial for all fields*, Advances in Cryptology - CRYPTO 2011 (Phillip Rogaway, ed.), Lecture Notes in Computer Science, vol. 6841, Springer Berlin / Heidelberg, 2011, pp. 724–742.

[6] Jintai Ding and Dieter Schmidt, *Rainbow, a New Multivariable Polynomial Signature Scheme*, Applied Cryptography and Network Security (John Ioannidis, Angelos Keromytis, and Moti Yung, eds.), Lecture Notes in Computer Science, vol. 3531, Springer Berlin / Heidelberg, 2005, pp. 164–175.

[7] Jintai Ding and John Wagner, *Cryptanalysis of Rational Multivariate Public Key Cryptosystems*, Post-Quantum Cryptography (Johannes Buchmann and Jintai Ding, eds.), Lecture Notes in Computer Science, vol. 5299, Springer Berlin / Heidelberg, 2008, pp. 124–136.

[8] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern, *Practical Cryptanalysis of SFLASH*, Advances in Cryptology - CRYPTO 2007 (Alfred Menezes, ed.), Lecture Notes in Computer Science, vol. 4622, Springer Berlin / Heidelberg, 2007, pp. 1–12.

[9] S. Hasegawa and T. Kaneko, *An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations*, Proceedings of the 10th Symposium on Information Theory and its Application, Society of Information Theory and its Applications, 1987.

[10] Masao Kasahara and Ryuichi Sakai, *A Construction of Public Key Cryptosystem for Realizing Ciphertext of Size 100 Bit and Digital Signature Scheme (Asymmetric Cipher) (<Special Section> Cryptography and Information Security)*, IEICE transactions on fundamentals of electronics, communications and computer sciences **87** (2004-01-01), no. 1, 102–109.

[11] ———, *A construction of public-key cryptosystem based on singular simultaneous equations*, IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences **E88-A** (2005), no. 1, 74–80.

[12] Aviad Kipnis, Jacques Patarin, and Louis Goubin, *Unbalanced Oil and Vinegar Signature Schemes*, Advances in Cryptology - EUROCRYPT '99 (Jacques Stern, ed.), Lecture Notes in Computer Science, vol. 1592, Springer Berlin / Heidelberg, 1999, pp. 206–222.

[13] Aviad Kipnis and Adi Shamir, *Cryptanalysis of the Oil & Vinegar Signature Scheme*, Advances in Cryptology CRYPTO '98 (Hugo Krawczyk, ed.), Lecture Notes in Computer Science, vol. 1462, Springer Berlin / Heidelberg, 1998, pp. 9–17.

[14] T. Matsumoto and H. Imai, *A class of asymmetric crypto-systems based on polynomials over finite rings*, IEEE International Symposium on Information Theory (St. Jovite, Quebec, Canada), IEEE, 1983.

[15] ———, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88 (New York, NY, USA), Springer-Verlag New York, Inc., 1988, pp. 419–453.

[16] Louis Goubin Nicolas T. Courtois and Jacques Patarin, *Sflashv3, a fast asymmetric signature scheme*, Cryptology ePrint Archive, Report 2003/211, 2003, `http://eprint.iacr.org/`.

[17] Jacques Patarin, *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88*, Advances in Cryptology - CRYPTO '95 (Don Coppersmith, ed.), Lecture Notes in Computer Science, vol. 963, Springer Berlin / Heidelberg, 1995, pp. 248–261.

[18] ———, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, Advances in Cryptology - EUROCRYPT '96 (Ueli Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer Berlin / Heidelberg, 1996, pp. 33–48.

[19] ———, *The oil and vinegar signature scheme*, Dagstuhl Workshop on Cryptography, transparencies, 1997.

[20] Jacques Patarin, Nicolas Courtois, and Louis Goubin, *QUARTZ, 128-Bit Long Digital Signatures*, Topics in Cryptology CT-RSA 2001 (David Naccache, ed.), Lecture Notes in Computer Science, vol. 2020, Springer Berlin / Heidelberg, 2001, pp. 282–297.

[21] Adi Shamir, *Efficient Signature Schemes Based on Birational Permutations*, CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology (London, UK), Springer-Verlag, 1994, pp. 1–12.

[22] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Rev. **41** (1999), no. 2, 303–332.

[23] S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, and T. Matsumoto, *A public-key cryptosystem based on the difficulty of solving a system of non-linear equations*, The Transactions of the Institute of Electronics and Communication Engineers of Japan **69** (1986-12), no. 12, 1963–1970.

[24] Shigeo Tsujii, *Public Key Cryptosystem using Nonlinear Equations*, The 8th Symposium on Information Theory and Its Applications, 1985, pp. 156–157.

[25] Shigeo Tsujii, Atsushi Fujioka, and Yuusuke Hirayama, *Generalization of the public-key cryptosystem based on the difficulty of solving a system of non-linear equations*, The Transactions of the Institute of Electronics,Information and Communication Engineers. A **72** (1989-02), no. 2, p390–397.

[26] Shigeo Tsujii, Kotaro Tadaki, and Masahito Gotaishi, *Construction of the Tsujii-Shamir-Kasahara (TSK) Multivariate Public Key Cryptosystem, which relies on the Difficulty of Prime Factorization* , Technical Report of IEICE **111** (2012-03-02), no. 455, 149–155.

[27] Christopher Wolf and Bart Preneel, *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*, Cryptology ePrint Archive, Report 2005/077, 2005, `http://eprint.iacr.org/`.