A New Class of Multivariate Public Key Cryptosystem Constructed on the Basis of Message-Dependent Transformation

Masao KASAHARA
Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564-8511 Japan.
kasahara@ogu.ac.jp

Abstract

In this paper, a new class of Public-Key Cryptosystem (PKC) based on Random Simultaneous Equation of degree g(RSE(g)PKC) is presented. The proposed scheme uses a new class of trap-doors based on two classes of transformation, i.e. random transformation and message-dependent random transformation. For constructing the proposed scheme, random transformations X and Ψ are used. The transformation Ψ would yield a breakthrough to a field of multivaliate cryptosystem in a sense that the transformation is dependent on a message. Namely it is a message-dependent transformation on the basis of random coding. We show that the proposed PKC's, can be secure against the various excellent attacks such as the attack based on the Gröbner bases calculation(Gröbner bases attack, GB attack), Patarin's attack and Braeken-Wolf-Preneel attack, due to the random transformations using new trap-doors.

Keyword

Public-key cryptosystem, Multivariate cryptosystem, Random coding, Gröbner bases, PQC.

1 Introduction

In this paper, we present a new class of PKC whose security depends on the difficulty of the problem of solving a set of random simultaneous equations of degree g.

Extensive studies have been made of the PKC constructed based on the simultaneous equations of degree g (SE(g)PKC)[1-20]. All these proposed schemes are very interesting and important. However unfortunately, some of these schemes have been proved not necessarily secure against the conventional attacks such as Patarin's attack[21], Gröbner basis attack[22-24], Braeken-Wolf-Preneel (BWP) attack[25].

In 2008, the author proposed a multivariate public key cryptosystem referred to as K(Ⅲ)RSE(g)PKC [16]. The author has long endeavored to improve the security of the K(Ⅲ)SE(g)PKC, because K(Ⅲ)SE(g)PKC might be insecure against the rank attack[25].

In this paper, for being secure against the conventional attacks, we present a new class of RSE(g)PKC. The proposed RSE(g)PKC will be referred to as K(XIV)RSE(g)PKC, which is a modified version K(Ⅲ)RSE(g)PKC. In K(XIV)RSE(g)PKC, the random transformations X and Ψ are used. The transformation Ψ would yield a breakthrough to a field of multivariate cryptosystem in a sense that it is dependent on a message. Namely it is a message-dependent transformation on the basis of a random coding.

We show that the proposed PKC can be secure against the various attacks including Gröbner basis attack.

Throughout this paper, when the variable v_i takes on a value $\tilde{v}_i$, we shall denote the corresponding vector $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$ as

$$\tilde{\boldsymbol{v}} = (\tilde{v}_1, \tilde{v}_2, \cdots, \tilde{v}_n). \tag{1}$$

The vector $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$ will be represented by the polynomial as

$$v(x) = v_1 + v_2 x + \cdots + v_n x^{n-1}. \tag{2}$$

The $\tilde{u}, \tilde{u}(x)$ et al. will be defined in a similar manner.

2 K(XIV)RSE(g)PKC

2.1 Preliminaries

Let a message $\boldsymbol{M}$ over $\mathbb{F}_2$ be denoted by

$$\boldsymbol{M} = (M_1, M_2, \cdots, M_{3n}). \tag{3}$$

We assume that the messages $M_1, M_2, \cdots, M_{3n}$ are mutually independent and equally likely.

The message $\boldsymbol{M}$ is transformed to vector $\boldsymbol{m}$ as follows:

$$\boldsymbol{M} \cdot H_I = \boldsymbol{m} = (m_1, m_2, \cdots, m_{3n}), \tag{4}$$

where H_I is a $3n \times 3n$ non-singular matrix over $\mathbb{F}_2$.

Definition 1: The transformation:

$$F(X) \quad = \quad Y, \tag{5}$$

is referred to as "non-singular", if and only if the transformation has the following inverse transformation:

$$F^{-1}(Y) \quad = \quad X, \tag{6}$$

for any given Y in a unique manner. On the other hand if the inverse-transformed value does not exist uniquely, for a given Y, the transformation is referred to as "singular". □

Throughout this paper, the transformation $F(X)$ will be denoted by $F(Y|X)$ or simply by F.

For the proposed K(XIV)RSE(g)PKC, in the followings, we assume that the degree g is given by $g = 2$ for simplicity. The generalization to the case for $g > 2$ is straightforward.

Let us partition $\boldsymbol{m}$ into three n-tuples $\boldsymbol{m}_L$, $\boldsymbol{m}_R$ and $\boldsymbol{m}_P$ as

$$\boldsymbol{m}_L \quad = \quad (m_1, m_2, \cdots, m_n) \tag{7}$$
$$\boldsymbol{m}_R \quad = \quad (m_{n+1}, m_{n+2}, \cdots, m_{2n}) \tag{8}$$

and

$$\boldsymbol{m}_P = (m_{2n+1}, m_{2n+2}, \cdots, m_{3n}). \tag{9}$$

The message $\boldsymbol{m}_P$ is publicized.

Remark 1: Each of the components of $\boldsymbol{m}_L$, $\boldsymbol{m}_R$ and $\boldsymbol{m}_P$ constitutes a set of linear equations in the variables $M_1, M_2, \cdots, M_{3n}$. □

Before describing the details of the transformations, in Fig.1, we show the rough sketch of the transformations performed on $\boldsymbol{m}_L$, $\boldsymbol{m}_R$ and $\boldsymbol{m}_P$.

2.2 Transformation $X(\boldsymbol{y}_L|\boldsymbol{m}_L)$

Using $X(\boldsymbol{y}_L|\boldsymbol{m}_L)$, the message $m_L = (m_1, m_2, \cdots, m_n)$ is encrypted to $\boldsymbol{y}_L$, for example by the methods presented in Refs.[1], [5] and [20], as

$$y_i = h_i^{(2)}(m_1, m_2, \cdots, m_n); i = 1, 2, \cdots, n, \tag{10}$$

where $h_i^{(2)}(m_1, m_2, \cdots, m_n)$ implies the i-th quadratic equation in the variables $m_1, m_2, \cdots, m_n$.

The $p_i^{(2)}(m_1, m_2, \cdots, m_n)$ and $q_i^{(2)}(m_{2n+1}, m_{2n+2}, \cdots, m_{3n})$ will be similarly defined.

Set of the equations $y_1, y_2, \cdots, y_n$ constitutes the set of public key $\{y_i\}_L$.

2.3 Transformation $\Psi(\boldsymbol{y}_R|\boldsymbol{m}_L, \boldsymbol{m}_P, \boldsymbol{m}_R)$

The transformation $\Psi(\boldsymbol{y}_R|\boldsymbol{m}_L, \boldsymbol{m}_P, \boldsymbol{m}_R)$ is performed by a series of transformations $\psi(\boldsymbol{z}_R|\boldsymbol{m}_L, \boldsymbol{m}_P)$, $\rho(\boldsymbol{T}_{b(i)}|\boldsymbol{z}_R)$ and $\rho(\boldsymbol{y}_R|\boldsymbol{T}_{b(i)}, \boldsymbol{m}_R)$ as shown in Fig.1.

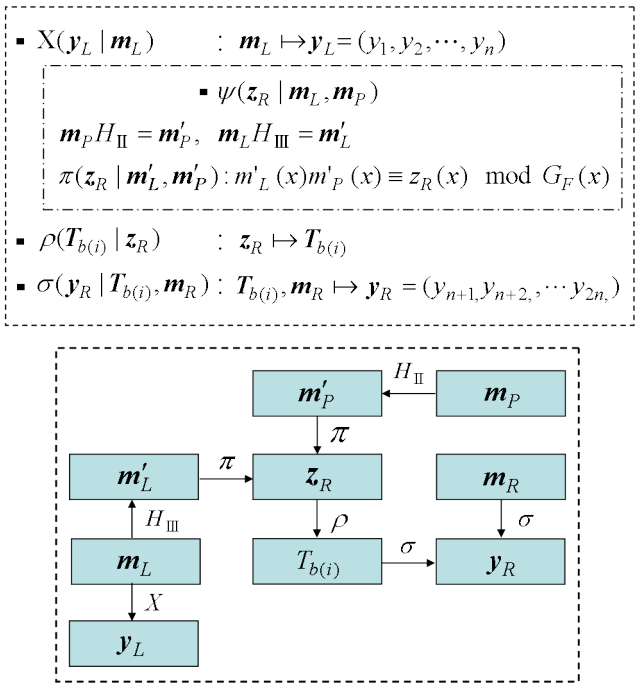

Figure 1: Brief sketch of transformations

(I) Transformation $\psi(\boldsymbol{z}_R|\boldsymbol{m}_L, \boldsymbol{m}_P)$

The publicized $\boldsymbol{m}_P$ is transformed into

$$\boldsymbol{m}_P H_{II} = \boldsymbol{m}'_P, \tag{11}$$

where H_{II} is an $n \times n$ non-singular matrix over $\mathbb{F}_2$.

The message $\boldsymbol{m}_L$ is transformed into

$$\boldsymbol{m}_L H_{III} = \boldsymbol{m}'_L, \tag{12}$$

where H_{III} is an $n \times n$ matrix over $\mathbb{F}_2$ which is not necessarily non-singular.

The $\boldsymbol{m}'_L$ and $\boldsymbol{m}'_P$ are transformed into

$$\begin{aligned} m'_L(x) m'_P(x) &\equiv z_R(x) \mod G_F(x) \\ &= z_1 + z_2 x + \cdots + z_n x^{n-1}, \end{aligned} \tag{13}$$

where $G_F(x)$ is a random primitive polynomial of degree n over $\mathbb{F}_2$.

The $z_R(x)$ is publicized.

(II) Transformation $\rho(\boldsymbol{T}_{b(i)}|\boldsymbol{z}_R)$

For $\boldsymbol{z}_R = (z_1, z_2, \cdots, z_n)$, let us define a sampling function $S_i(\theta_{i1}, \theta_{i2}, \cdots, \theta_{i\mu}); i = 1, \cdots, \lambda$, where $i1, i2, \cdots, i\mu$ randomly take on values from 1 to n under the condition that

$$1 \le i1 < i2 < \cdots < i\mu \le n. \tag{14}$$

The components of $\boldsymbol{z}_R, z_{i1}, z_{i2}, \cdots, z_n$, are sampled using the sampling function $S_i(\theta_{i1}, \theta_{i2}, \cdots, \theta_{i\mu})$. Let the sampled value $\boldsymbol{z}_{Si}$ be denoted by

$$\boldsymbol{z}_{Si} = (z_{i1}, z_{i2}, \cdots, z_{i\mu}). \tag{15}$$

Regarding z_{i1} as the most significant digit and $z_{i\mu}$, the least significant digit, $\boldsymbol{z}_{Si}$ can be transformed to a binary number, $b(i)$. The order of $\{b(i)\}$ is evidently given by

$$\#\{b(i)\} = 2^{\mu}. \tag{16}$$

For each $b(i)$, we provide uniquely decodable tables, $\{T_{b(i)}\}$. We assume that the tables $T_{b(i)}$'s are all distinct each other. Namely, the order of the tables, $\#\{T_{b(i)}\}$ is also given by

$$\#\{T_{b(i)}\} = 2^{\mu}. \tag{17}$$

Let us partition message $\boldsymbol{m}_R$ into

$$\boldsymbol{m}_R = (\boldsymbol{m}_{R1}, \boldsymbol{m}_{R2}, \cdots, \boldsymbol{m}_{R\lambda}), \tag{18}$$

where $\boldsymbol{m}_{Ri}$ is given by

$$\boldsymbol{m}_{Ri} = (m_{n+(i-1)t+1}, \cdots, m_{n+it}), (1 \le i \le \lambda). \tag{19}$$

We assume that the following relation holds:

$$\mu \ge t = \frac{n}{\lambda}. \tag{20}$$

For the components of $\boldsymbol{m}_R, \boldsymbol{m}_{R1}, \boldsymbol{m}_{R2}, \cdots, \boldsymbol{m}_{R\lambda}, 2^{\mu}$ different random coding tables are provided.

When $\tilde{\boldsymbol{m}}_{Ri}$ is given, the i-th sampling function $S_i(\theta_{i1}, \theta_{i2}, \cdots, \theta_{i\mu})$ is assinged to $\tilde{\boldsymbol{z}}_R$, yielding $\tilde{z}_{Si} = (\tilde{z}_{i1}, \tilde{z}_{i2}, \cdots, \tilde{z}_{i\mu})$ given by Eq.(15). When $\tilde{\boldsymbol{z}}_{Si}$ represent the binary number $\tilde{b}(i)$, Table $T_{\tilde{b}(i)}$ is selected from the set $\{T_{b(i)}\}$ for encrypting $\tilde{m}_{Ri}$. For message $\tilde{\boldsymbol{m}}_R = (\tilde{\boldsymbol{m}}_{R1}, \tilde{\boldsymbol{m}}_{R2}, \cdots, \tilde{\boldsymbol{m}}_{R\lambda})$, the following vector of the chosen tables is given.

$$\boldsymbol{T}_{\tilde{b}(i)} = (T_{\tilde{b}(1)}, T_{\tilde{b}(2)}, \cdots, T_{\tilde{b}(\lambda)}). \tag{21}$$

(Ⅲ) Transformation $\sigma(\boldsymbol{y}_R|\{T_{b(i)}\}, \boldsymbol{m}_R)$

In the followings we shall present one of the methods for providing the set of tables, $\{T_{b(i)}\}$, each of which lists 2^t code words that are uniquely decodable. Using the set of tables $\{T_{b(i)}\}$ the message $\boldsymbol{m}_{Ri}$, a component of $\boldsymbol{m}_R$, is transformed to the codeword as

$$\begin{aligned} \boldsymbol{m}_{Ri} &= (m_{n+(i-1)t+1}, \cdots, m_{n+it}) \\ &\mapsto \boldsymbol{y}_{Ri} = (y_{i1}, y_{i2}, \cdots, y_{it}). \end{aligned} \tag{22}$$

An example of $T_{b(i)}$ is given in Table 1 where we assume that $t = 3$. As the size of $\boldsymbol{m}_{Ri}$ is $t = 3$, we see that the $2^t = 2^3 = 8$ different code words are provided for the encrypting of $\boldsymbol{m}_{Ri}$, the i-th component of $\boldsymbol{m}_R$. For example, when $\boldsymbol{z}_{Si}$ represents the binary number $b(i) = 1011$, then T_{1011} as shown in Table 1 is chosen. Furthermore we assume that the message $\boldsymbol{m}_{Ri}$ happens to be (1 1 0), then this message (1 1 0) is encoded to $\boldsymbol{y}_{Ri} = (011)$.

Table 1: Example of T_{1011}

m_1	m_2	m_3	y_1	y_2	y_3
0	0	1	1	1	0
0	0	0	1	0	1
0	1	1	1	0	0
0	1	0	0	1	0
1	0	0	0	0	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	0	0	0

As we have explained by the above-mentioned example, in general, the message $\boldsymbol{m}_R = (\boldsymbol{m}_{R1}, \boldsymbol{m}_{R2}, \cdots, \boldsymbol{m}_{R\lambda})$ is encrypted to $(\boldsymbol{y}_{R1}, \boldsymbol{y}_{R2}, \cdots, \boldsymbol{y}_{R\lambda})$ based on the set of tables $\{T_{b(i)}\}$ and $\boldsymbol{z}_R$.

The ciphertext $\boldsymbol{C}_R$ is simply given by

$$\boldsymbol{C}_R = (\boldsymbol{y}_{R1}, \boldsymbol{y}_{R2}, \cdots, \boldsymbol{y}_{R\lambda}), \tag{23}$$

where $\boldsymbol{y}_{Ri} = (y_{n+(i-1)t+1}, \cdots, y_{n+it}); i = 1, 2, \cdots, \lambda$.

Remark 1 : The i-th component of the message vector $\boldsymbol{m}_R$, $\boldsymbol{m}_{Ri}$, is transformed to the code word $\boldsymbol{y}_{Ri}$ using the table $T_{b(i)}$. For the given $\tilde{m}_{Ri}$, the table $T_{\tilde{b}(i)}$ is not fixed but is given, depending on another message vector $\tilde{\boldsymbol{z}}_{Si}$ in the variables $\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_{3n}$. Namely K(XIV)SE(g)PKC is constructed based on a series of message dependent transformations $\psi(\boldsymbol{z}_R|\boldsymbol{m}_L, \boldsymbol{m}_P)$, $\rho(T_{b(i)}|\boldsymbol{z}_R)$ and $\sigma(\boldsymbol{y}_R|\{T_{b(i)}\}, \boldsymbol{m}_R)$. □

Public Keys	:	$\boldsymbol{m}_P$, $\{y_i\}_L$, $\{\boldsymbol{z}_{Ri}\}$, $\rho(\boldsymbol{T}_{b(i)}|\boldsymbol{z}_R)$, $\sigma(\boldsymbol{y}_R|\{T_{b(i)}\}, \boldsymbol{m}_R)$.
Secret Keys	:	H_I, $G_F(x)$, $X(\boldsymbol{y}_L|\boldsymbol{m}_L)$, $\psi(\boldsymbol{z}_R|\boldsymbol{m}_L, \boldsymbol{m}_P)$.

2.4 Ciphertext

Letting the ciphertext $\boldsymbol{C}$ be represented by $\boldsymbol{C} = (\boldsymbol{C}_L, \boldsymbol{C}_R, \boldsymbol{C}_P)$, the ciphertext $\boldsymbol{C}_L$ is given by

$$\boldsymbol{C}_L = (y_1, y_2, \cdots, y_n), \tag{24}$$

where $y_i = h_i^{(2)}(m_1, m_2, \cdots, m_n)$.

The ciphertext $\boldsymbol{C}_R$ is simply given by

$$\boldsymbol{C}_R = (\boldsymbol{C}_{R1}, \boldsymbol{C}_{R2}, \cdots, \boldsymbol{C}_{R\lambda}), \tag{25}$$

where

$$\boldsymbol{C}_{Ri} = \boldsymbol{y}_{Ri} (1 \le i \le \lambda). \tag{26}$$

Table 2: Example of K(Ⅲ)RSE(g)PKC

Example	Number of Variables, $3n$	Length of Subblock, n (bit)	Size of Public key S_{PK}(KB)	t	λ	μ
Ⅰ	90	30	93	3	10	8
Ⅱ	120	40	219	4	8	10
Ⅲ	150	50	427	5	8	10
Ⅳ	180	60	738	6	8	10

The ciphertext $\boldsymbol{C}_P$ is given by

$$\boldsymbol{C}_P = (m_{2n+1}, m_{2n+2}, \cdots, m_{3n}). \tag{27}$$

2.5 Encryption and dycryption

2.5.1 Encryption

Step1: Given the message sequences $\tilde{\boldsymbol{M}}_1$, $\tilde{\boldsymbol{M}}_2$, $\cdots$, $\tilde{\boldsymbol{M}}_{3n}$, the ciphertext $\tilde{\boldsymbol{C}}_L$ is given by $\tilde{\boldsymbol{C}}_L = (\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_n)$.

Step2: After calculating $\tilde{\boldsymbol{z}}_R$ from the public key $\{\boldsymbol{z}_{Ri}\}$, using the sampling function $S_i(\theta_{i1}, \theta_{i2}, \cdots, \theta_{i\mu})$; $i = (1, 2, \cdots, \lambda)$, the set of tables $T_{\tilde{b}(1)}, T_{\tilde{b}(2)}, \cdots, T_{\tilde{b}(\lambda)}$ is obtained.

Step3: Using $\boldsymbol{T} = (T_{\tilde{b}(1)}, T_{\tilde{b}(2)}, \cdots, T_{\tilde{b}(\lambda)})$, the message $\tilde{\boldsymbol{m}}_R = (\tilde{\boldsymbol{m}}_{R1}, \tilde{\boldsymbol{m}}_{R2}, \cdots, \tilde{\boldsymbol{m}}_{R\lambda})$ is encrypted to the ciphertext $\tilde{\boldsymbol{C}}_R = (\tilde{\boldsymbol{y}}_1, \tilde{\boldsymbol{y}}_2, \cdots, \tilde{\boldsymbol{y}}_\lambda) = (\tilde{y}_{n+1}, \tilde{y}_{n+2}, \cdots, \tilde{y}_{2n})$.

Step4: From the public equations, m_{2n+1}, m_{2n+2}, $\cdots$, m_{3n}, the ciphertext $\tilde{\boldsymbol{C}}_P$ is simply given by $\tilde{\boldsymbol{C}}_P = (\tilde{m}_{2n+1}, \cdots, \tilde{m}_{3n})$.

2.5.2 Decryption

Step1: From $\tilde{\boldsymbol{C}}_L = (\tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_n)$, the message vector $\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n$ are decoded.

Step2: From $\tilde{\boldsymbol{m}}_L = (\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n)$ and $\tilde{\boldsymbol{m}}_P = (\tilde{m}_{2n+1}, \tilde{m}_{2n+2}, \cdots, \tilde{m}_{3n})$, the venctor $\tilde{\boldsymbol{z}}_R = (\tilde{\boldsymbol{z}}_{R1}, \tilde{\boldsymbol{z}}_{R2}, \cdots, \tilde{\boldsymbol{z}}_{R\lambda})$ is decoded by Eqs.(11),(12) and (13).

Step3: Using the sampling functions $\{S_i(\theta_{i1}, \cdots, \theta_{i\mu})\}$, the set of tables $T_{\tilde{b}(1)}, T_{\tilde{b}(2)}, \cdots, T_{\tilde{b}(\lambda)}$ are decoded.

Step4: From the i-th component of $\tilde{\boldsymbol{C}}_R$, $\tilde{\boldsymbol{y}}_i$, the message $\tilde{\boldsymbol{m}}_{Ri}$ is decoded using the table $T_{\tilde{b}(i)}$; $i = 1, 2, \cdots, \lambda$, yielding $\tilde{\boldsymbol{m}}_R = (\tilde{\boldsymbol{m}}_1, \tilde{\boldsymbol{m}}_2, \cdots, \tilde{\boldsymbol{m}}_\lambda)$.

Step5: From $\tilde{\boldsymbol{m}}_L$, $\tilde{\boldsymbol{m}}_R$ and $\tilde{\boldsymbol{m}}_P$, the message $\tilde{\boldsymbol{m}} = (\tilde{\boldsymbol{m}}_L, \tilde{\boldsymbol{m}}_R, \tilde{\boldsymbol{m}}_P) = (\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_{3n})$ is decoded.

Step6: The original message $\boldsymbol{M} = (M_1, M_2, \cdots, M_{3n})$ is decoded by

$$(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_{3n}) H_I^{-1} = \tilde{\boldsymbol{M}} \tag{28}$$

2.6 Several parameters

Let us define several symbols:

N_V : Total number of message variables, $3n$.
N_{EPl} : Total number of linear equations used for encrypting $\boldsymbol{m}_P$.
N_{ELq} : Total number of quadratic equations used for encrypting $\boldsymbol{m}_L$.
N_{ERq} : Total number of random quadratic equations used for choosing a random coding table from $\{T_{b(i)}\}$
S_T : Size of $T_{b(i)}$ (bit).

The size of the public key $\{y_i\}_L$ for encoding $\boldsymbol{m}_L$, S_{PKLq}, is given by

$$S_{PKLq} =_{N_V} H_2 \cdot N_{ELq} = \frac{(3n+1)9n^2}{2} \quad \text{(bit)}. \tag{29}$$

Similarly, the size of the public key used for choosing a random table from $\{T_{b(i)}\}$ is given by

$$S_{PKRq} =_{N_V} H_2 \cdot N_{ERq} = \frac{(3n+1)9n^2}{2} \quad \text{(bit)}. \tag{30}$$

The size of the public key for encrypting $\boldsymbol{m}_P$, S_{PKPl}, is given by

$$S_{PKPl} = N_V \cdot N_{EPl} = 3n^2. \tag{31}$$

The size of the table $\{T_{b(i)}\}$, S_T, is given by

$$S_T = 2^{t+1} \cdot 2^\mu \ \text{(bit)}. \tag{32}$$

The size of the public key, S_{PK}, is given by

$$\begin{aligned} S_{PK} &= S_{PKLq} + S_{PKRq} + S_{PKPl} + S_T \\ &= 27n^3 + 12n^2 + 2^{t+1+\mu} \quad \text{(bit)}. \end{aligned} \tag{33}$$

The size of the ciphertexts, C_L, C_R and C_P are given by

$$|C_L| = |C_R| = |C_P| = n \ \text{(bit)}. \tag{34}$$

The size of the ciphertexts, $C = (C_L, C_R, C_P)$ is given by

$$|C| = |C_L| + |C_R| + |C_P| = 3n \ \text{(bit)}. \tag{35}$$

The coding rate, ρ, is give by

$$\rho = \frac{N_V}{|C|} = \frac{3n}{3n} = 1.0. \tag{36}$$

We see that the proposed scheme realizes the coding rate of exactly 1.0.

We present several examples of K(XIV)RSE(g)PKC in Table 2.

3 Security Considerations

3.1 Preliminaries

It should be noted that K(XIV)RSE(g)PKC has the following advantage, before discussing on the security of the proposed scheme.

> **"One of the advantage of the proposed K(XIV)RSE(g)PKC is that for any given ciphertext, $\tilde{\boldsymbol{z}}_R = (\tilde{\boldsymbol{z}}_{R1}, \tilde{\boldsymbol{z}}_{R2}, \cdots, \tilde{\boldsymbol{z}}_{R\lambda})$ is not explicity given, although the set of public keys, $\{\boldsymbol{z}_{Ri}\}$, is publicized."**

3.2 Various attack on K(XIV)RSE(2)PKC

Attack I: Disclosing $m_1, m_2, \cdots, m_n$, from the given the ciphertext $\tilde{\boldsymbol{C}}_L$.

The total number of the quadratic equations $y_1, y_2, \cdots, y_n$ is equal to the total number of variables $m_1, m_2, \cdots, m_n$.

As a result, using GB attack[23,24], it would be possible to disclose $\tilde{m}'_1, \tilde{m}'_2, \cdots, \tilde{m}'_n$ in the variables $\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_{3n}$ that yields the set of equations $\tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_n$. However it seems hard to find the set of $m'_1, m'_2, \cdots, m'_n$ such that

$$\tilde{m}'_i = \tilde{m}_i; i = 1, 2, \cdots, n. \tag{37}$$

□

Attack II: Exhaustive attack on a set of tables used for $\tilde{C}_R$.

As the order of the set of the random coding tables $\{T_{b(i)}\}$ is given by Eq.(17) the probability $P_C[\{\tilde{T}_{b(i)}\}]$ of estimating all of the tables $\tilde{T}_{b(i)}$'s randomly chosen at the sending end, with no knowledge on $\tilde{\boldsymbol{z}}_R$, is given by

$$P_C[\{\tilde{T}_{b(i)}\}] = \{2^{\mu\lambda}\}^{-1}. \tag{38}$$

We see that the probability $P_C[\{\tilde{T}_{b(i)}\}]$ can be made sufficiently small when

$$\mu\lambda \gtrsim 80 \tag{39}$$

holds. □

Attack III: BWP attack.

Braeken-Wolf-Preneel(BWP) attack have been widely known. Using the rank attack [25], it would be possible to disclose n linear equations $\boldsymbol{m}''_L = (m''_1, m''_2, \cdots, m''_n)$ that can be obtained by a linear transformation of $\boldsymbol{m}_L = (m_1, m_2, \cdots, m_n)$.

However it seems quite hard to construct $\boldsymbol{z}_R$ from m''_L and $\boldsymbol{m}_P$, because $\boldsymbol{z}_R$ is constructed by Eq.(11), (12) and (13). □

4 Concluding remarks

In this paper a new class of multivariate cryptosystem referred to as K(XIV)RSE(g)PKC. The K(XIV)RSE(g)PKC seems secure due to the following reasons:

A new type of trap-door is given. That is, the "message-dependent" transformation $\Psi(\boldsymbol{y}_L|\boldsymbol{m}_R, \boldsymbol{m}_P, \boldsymbol{m}_R)$ is used. The transformation $\Psi(\boldsymbol{y}_R|\boldsymbol{m}_L, \boldsymbol{m}_P, \boldsymbol{m}_R)$ is given by a series of tranformations $\psi(\boldsymbol{z}_R|\boldsymbol{m}_L, \boldsymbol{m}_P) \rightarrow \rho(\boldsymbol{T}_{b(i)}|\boldsymbol{z}_R) \rightarrow \sigma(\boldsymbol{y}_R|\boldsymbol{T}_{b(i)}, \boldsymbol{m}_R)$. It should be noted that $\tilde{\boldsymbol{z}}_R$ is not explicitly given, but only $\tilde{\boldsymbol{y}}_R$ is given, although $\boldsymbol{z}_R$ is publicized as a public key.

We have shown that, with this new trap-door, K(XIV)RSE(g)PKC is secure against the various attacks.

References

[1] T. Mastumoto and H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature - Verification and Message-Encryption", Advances in Cryptology, Eurocrypt'88, Springer-Verlag, pp.419-453, (1988).

[2] S. Tsujii, A. Fujioka and Y. Hirayama, "Generalization of the public-key cryptosystem based on the difficulty of solving a system of non-linear equations", IEICE Trans. Vol.1 J-72-A, 2, pp.390-397, (1989-02).

[3] J.Patarin,"Hidden fields equations(HFE) and isomorphisms of polynomials(IP): two new families of asymmetric algorithms," Proc.EUROCRYPT'96, Lecture Notes in Computer Science, Vol.1070, pp.33-48, Springer, (1996-05).

[4] M. Kasahara and R. Sakai, "Notes on Public Key Cryptosystem Based on Multivariate Polynomials of High Degree", Technical Report of IEICE, ISEC 2001-64 (2001-09).

[5] M. Kasahara and R. Sakai, "A Construction of Public Key Cryptosystem for Realizing Ciphertext of size 100 bit and Digital Signature Scheme", IEICE Trans. Vol. E87-A, 1, pp.102-109, (2004-01).

[6] S. Tsujii, R. Fujita and K. Tadaki, "Proposal of MOCHIGOMA(piece in hand) concept for multivariate

type public key cryptosystem", Technical Report of IEICE, ISEC 2004-74, (2004-09).

[7] J.Ding,"A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation", PKC 2004, LNCS 2947, pp.305-318, 2004.

[8] M. Kasahara and R. Sakai, "A Construction of Public Key Cryptosystem Based on Singular Simultaneous Equations", IEICE Trans. Vol. E88-A, 1, pp.74-79, (2005-01).

[9] M. Kasahara: "A Construction of Public-Key Cryptosystem Using Algebraic Coding on the Basis of Superimposition and Randomness", ISICE Trans.Fundamentals, Vol.E-89A, No.1, (2006-01).

[10] M. Kasahara, "K-Matrix Public-Key Cryptosystems Constructed Based on Random Coding Technique - Along with a proposal of new classes of SE(g)·PKC -", Technical Report of IEICE, ISEC 2005-171, pp.133-118, (2006-03).

[11] M. Kasahara, "Construction of a new Class of SE(g)PKC - Along with some notes on K-Matrix PKC -", Technical Report of IEICE, ISEC 2006-4, pp.23-28, (2006-05).

[12] M. Kasahara, "Constructions of $\mathrm{K_{HLN}}$·SE(g)PKC on the basis of K-construction with hidden location noise (HLN)", Technical Report of IEICE, ISEC 2006-83, pp.85-90, (2006-09).

[13] M.Kasahara,"A New Class of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials Randomly Generated", Technical Report of IEICE, ISEC 2007 (2007-09).

[14] M.Kasahara,"New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials", 12-03, SITA 2007, Kashikojima, (2007-11).

[15] M.Kasahara,"New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials", Technical Report of IEICE, ISEC 2007, (2007-12).

[16] M.Kasahara,"New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials and Random Coding – Another Class of K(Ⅲ)RSE(g)PKC –", Technical Report of IEICE, ISEC 2007, (2008-02).

[17] M.Kasahara,"New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials and Error Control Coding", Technical Report of IEICE, ISEC. 2008-13, 108, 38 (2008-05).

[18] M.Kasahara,"New Classes of Public Key Cryptosystems Constructed on the Basis of Low Density Multivaliate Polynomials", Technical Report of IEICE, ISEC, (2008-09).

[19] M.Kasahara: "Multivariate Public-Key Cryptosystems Constructed Based on Source and Channel Joint Coding", SITA 2008, (2008-10).

[20] M.Kasahara: "A New Class of Multivariate Public Key Cryptosystems Constructed Based on Random Pseudo Cyclic Codes, K(XIII)SE(2)PKC, Realizing Coding Rate of Exactly 1.0", Cryptology ePrint Archive 2011/573 (2011-10).

[21] J. Patarin, "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88", Advances in Cryptography, Crypto'95, Springer Verlag, pp.248-261, (1996).

[22] A.Kipnis and A.Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization", Advances in Cryptography-Crypto'99, LNCS 1666 pp.19-30, (1999).

[23] J.C.Faugere and A.Joux, "Algebraic Cryptanalysis of Hidden Field Equation(HFE) Cryptosystem Using Gröbner Bases", CRYPTO 2003, LNCS 2729, pp.44-60, (2003).

[24] M.Bardet, J.C.Faugére and B.Salvy "Complexity of Gröbner basis computation for semi-regular overdetermined sequence over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$", Technical Report RR-5049, INRIA, (2003-12).

[25] C. Wolf, "Multivariate Quadratic Polynomials in Public Key Cryptography", Dr. Thesis, Katholieke Universiteit Leuven, (2005-11)