IEICE TRANS. FUNDAMENTALS, VOL.E88–A, NO.1 JANUARY 2005

PAPER Special Section on Cryptography and Information Security

A Construction of Public-Key Cryptosystem Based on Singular Simultaneous Equations

Masao KASAHARA[†a)], ***Fellow and*** **Ryuichi SAKAI**[††b)], ***Member***

SUMMARY Extensive studies have been made of the public key cryptosystems based on multivariate polynomials over $\mathbb{F}_2$. However most of the proposed public key cryptosystems based on multivariate polynomials, are proved not secure. In this paper, we propose several types of new constructions of public key cryptosystems based on randomly generated singular simultaneous equations. One of the features of the proposed cryptosystems is that the sets of random singular simultaneous equations significantly enlarges the size of the transformation.

key words: *public-key cryptosystem, singular simultaneous equations, multivariate polynomials*

1. Introduction

Extensive studies have been made of the Public Key Cryptosystem(PKC). The security of most PKCs depends on the difficulty of discrete logarithm problem or factorization problem. Thus it is desired to investigate another classes of PKC that do not rely on the difficulty of these two problems.

In this paper, we shall present a new class of PKC whose security seems to depend on the difficulty of the problem of solving singular simultaneous equations of degree 2 [1]. Hereinafter Singular Simultaneous Equations of degree d will be denoted as SSE(d). We shall also refer to the conventional PKC, constructed based on Simultaneous Equations(SE) of degree d will be referred to as SE(d)PKC.

The simultaneous equations used in the proposed PKC are generated in a random manner, in a sharp contrast with the conventional methods whose security also seems to be related to the difficulty of solving SE(d) [2], [3]. As our proposed PKCs are constructed, based on the Random Singular Simultaneous Equations(RSSE) of degree d, we shall refer to the proposed scheme as RSSE(d)PKC, for short.

To our knowledge, no elegant method has been known to provide the sets of the solutions for the given RSSE(d) [4]. Thus the proposed PKC based on SSE(d) apparently seems more secure compared with the conventional SE(d)PKC.

Let us briefly survey a short history of investigations on a class of public key cryptosystems whose security relies upon the difficulty of solving SE(2)PKC over $\mathbb{F}_2$.

The first and important SE(2)PKC was proposed by Matsumoto and Imai [2]. In this paper the Matsumoto and Imai's scheme will be referred to as MI-SE(2)PKC. Unfortunately this interesting scheme was shown to be insecure by Patarin [3], [5]. Patarin then proposed a series of improved versions of the MI-SE(2)PKC such as the Oil and Vinegar Algorithm [5] and the Little Dragon and the Big Dragon schemes [3], [6], [7]. However the Oil and Vinegar scheme was broken by Kipnis and Shamir [8]. The Little Dragon scheme was also broken by Coppersimith and Patarin [3], [6]. In this paper the Little Dragon scheme will be referred to as LD-SE(2)PKC.

For obtaining SE(2), simultaneous equations of degree 2, the MI-SE(2)PKC over $\mathbb{F}_2$ basically exploits the following transformation referred to as Φ_{MI}:

$$\Phi_{\mathrm{MI}} : \boldsymbol{y} \longmapsto \boldsymbol{y}^{2^\theta+1}, \tag{1}$$

where θ is a positive integer and $\boldsymbol{y}$ is the n dimensional vector that belongs to a secret extension field $\mathbb{F}_{2^n}$ generated modulo a secret polynomial $G(X)$ of degree n.

The various schemes whose securities rely on the difficulty of solving SE(2) use the variants of the original transformation Φ_{MI}.

For example, the Little Dragon scheme uses the following transformation [3]:

$$\Phi_{\mathrm{LD}} : \boldsymbol{y} \longmapsto \boldsymbol{y}^{2^{\theta_1}+2^{\theta_2}-1}, \tag{2}$$

where θ_1 and θ_2 are certain positive integers.

Another class of SE(2)PKC known as TPM(T Plus-Minus) has been also extensively studied [9]. In this scheme, the so-called triangular construction, usually denoted by T, is exploited. Recently Moh proposed a sub-case of TPM scheme, TTM cryptosystem. However, shortly after the proposal of TTM, the TPM/TTM schemes were broken by Goubin and Courtois [10].

Recently, the methods of using random transformation for obtaining simultaneous equations have been proposed [11]–[15]. Hereinafter we shall refer to PKC based on random Non-Singular SE(d) as RNSSE(d)-PKC. In these methods, the transformations are random in a sense that all the coefficients of the products of d or less variables for constructing a polynomial are chosen at random, under the condition that the transformation is non-singular.

In this paper we present a new class of PKC constructed based on random simultaneous equations that can be singular. We show that the random transformation that are not

Manuscript received March 18, 2004.
Manuscript revised July 8, 2004.
Final manuscript received August 30, 2004.

[†]The author is with Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564-8511 Japan.
[††]The author is with Department of Lightwave Sciences, Osaka Electro-Communication University, Neyagawa-shi, 572-8530 Japan.
a) E-mail: kasahara@utc.osaka-gu.ac.jp
b) E-mail: sakai@isc.osakac.ac.jp

necessarily non-singular significantly enlarges the size of transformation. The introduction of the random constructions of SE(2)s based on singular simultaneous equations, evidently seems to improve the security of the SE(2)PKC or RNSSE(2)PKC because the using of RNSSE significantly enlarges the effective size of transformations. In this paper, we present RSSE(d) over $\mathbb{F}_2$ only for $d = 2$. The reason is that the size of the public key takes on an extremely large value, for $d \geq 3$. In addition $\mathbb{F}_2$ is extensively used in the various application fields of the cryptography[†].

2. RSSE(d)PKC

2.1 Construction of RSSE(d)PKC

Letting a message vector over $\mathbb{F}_2$ be denoted by $\boldsymbol{X} = (X_1, X_2, \cdots, X_k)$ and the hashed value of $\boldsymbol{X}$, by $(H_1, H_2, \cdots, H_g)$, $H_i \in \mathbb{F}_2$, the redundant message vector, X_ρ can be written as:

$$\boldsymbol{X}_\rho = (X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g). \tag{3}$$

In this paper, the symbols X, x, Y, y etc with no tilde denote the indeterminate and the corresponding symbols with tildes $\tilde{X}, \tilde{x}, \tilde{Y}, \tilde{y}$, the determinate. The following relation implies that the message vector $\boldsymbol{X}$ takes on a certain value $\tilde{\boldsymbol{X}}$:

$$\boldsymbol{X} = \tilde{\boldsymbol{X}} = (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k), \tag{4}$$

where we assume that the variant X_i takes on a certain value $\tilde{X}_i$ that belongs to $\mathbb{F}_2$.

In the followings, $\tilde{x}_i$, $\tilde{y}_i$ and so forth will be used in an exactly similar manner as $\tilde{X}_i$.

In the following, for simplifying the notation, we replace $\boldsymbol{X}_\rho$ by $\boldsymbol{x}$ as follows :

$$\boldsymbol{X}_\rho = \boldsymbol{x} = (x_1, x_2, \cdots, x_n), \tag{5}$$

The RSSE(2)PKC over $\mathbb{F}_2$ can be constructed according to the following algorithm.

[Algorithm I]

Step 1 : The redundant message vector $\boldsymbol{X}_\rho$ is transformed to vector $\boldsymbol{y}$ as follows :

$$\boldsymbol{X}_\rho \boldsymbol{A} = \boldsymbol{y} = (y_1, y_2, \cdots, y_n), \tag{6}$$

where $y_i \in \mathbb{F}_2$ and A is an $n \times n$ non-singular secret matrix over $\mathbb{F}_2$.

Step 2 : The components of the vector $\boldsymbol{y}$ are partitioned into N sub-vectors, yielding the following vector :

$$\boldsymbol{y} = (\boldsymbol{Y}_1, \boldsymbol{Y}_2, \cdots, \boldsymbol{Y}_N), \tag{7}$$

where $\boldsymbol{Y}_j$ is given by

$$\boldsymbol{Y}_j = (y_{j1}, y_{j2}, \cdots, y_{jt}). \tag{8}$$

Definition 1: The following transformation :

$$\Phi(\boldsymbol{u}) = \boldsymbol{v}, \tag{9}$$

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

$$\Phi^{-1}(\boldsymbol{v}) = \boldsymbol{u}, \tag{10}$$

for any given $\boldsymbol{v}$ in a unique manner. On the other hand if the inverse-transformed value $\boldsymbol{u}$ does not exist in a unique manner, for a given $\boldsymbol{v}$, the transformation is referred to as "singular." □

Step 3 : Given $\boldsymbol{Y}_j, (j = 1, 2, \cdots, N)$, the following transformation, $\Phi_j(\boldsymbol{Y}_j) = \boldsymbol{Z}_j$ is performed on the basis of randomness:

$$\left.\begin{aligned} z_{j1} &= \Phi^{(2)}_{j1}(y_{j1}, y_{j2}, \cdots, y_{jt}) \\ &\vdots \\ z_{ji} &= \Phi^{(2)}_{ji}(y_{j1}, y_{j2}, \cdots, y_{jt}) \\ &\vdots \\ z_{jt} &= \Phi^{(2)}_{jt}(y_{j1}, y_{j2}, \cdots, y_{jt}) \end{aligned}\right\}, \tag{11}$$

where $\boldsymbol{Z}_j = (z_{j1}, z_{j2}, \cdots, z_{jt})$, and $z_{ji} = \Phi^{(2)}_{ji}(y_{j1}, y_{j2}, \cdots, y_{jt})$ is a quadratic equation in t variables $y_{j1}, y_{j2}, \cdots, y_{jt}$. We assume that the coefficients of the equations are chosen in a random manner.

Remark 1: In general, SE(2) given by Eq.(11) becomes singular. On this matter, we shall show a numerical example for $t = 4$ in Table 1 in 2.3.

Step 4 : Letting $\boldsymbol{Z} = (\boldsymbol{Z}_1, \boldsymbol{Z}_2, \cdots, \boldsymbol{Z}_N)$ where $\boldsymbol{Z}_j = (z_{j1}, z_{j2}, \cdots, z_{jt})$, the following final transformation is performed:

$$\boldsymbol{Z}B = (K_1, K_2, \cdots, K_n), \tag{12}$$

yielding the set of public-keys, $K = (K_1, K_2, \cdots, K_n)$ where B is an $n \times n$ non-singular matrix over $\mathbb{F}_2$. The public keys can be denoted as

[†]Thus in this paper, we present RSSE(d) over $\mathbb{F}_2$, only for $d = 2$. On this matter, we were notified the following very interesting fact from the anonymous reviewer. We would like to introduce this very interesting fact :
If $\mathbb{F}_p$ is used in place of $\mathbb{F}_2$, where p is an odd prime number, the proposed scheme is not secure. The reason is that any quadratic forms on $\mathbb{F}_p$ are diagonalized in polynomial time. It should be noted that the Hessian matrix shall vanish on $\mathbb{F}_2$.

It is known that, when the characteristic number of the base field is not equal to the degree of the algebraic equations, one cannot necessarily expect that the derivations of the equations always vanish.

Table 1 Distribution of width W.

W	$1 \sim 5$	6	7	8	9	10	11	12	13	14	15	16
$\#\{\Phi_{I4}^{(W)}\}$	0	736	37680	494560	2440125	5036725	5098044	2811650	679200	175680	0	2816
$S_{I4}^{(W)}$ (bits)	–	9.52	15.2	18.9	21.2	22.3	22.3	21.4	19.4	17.42	–	11.46

$$\left.\begin{aligned} K_1 &= k_1^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g) \\ K_2 &= k_2^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g) \\ &\vdots \\ K_j &= k_j^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g) \\ &\vdots \\ K_n &= k_n^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g) \end{aligned}\right\}, \quad (13)$$

where $K_j = k_j^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g)$ is a quadratic polynomial obtained through the above mentioned Steps 1 to 4.

Remark 2: The set of public keys given by Eq.(13) constitutes singular simultaneous equations. No systematic method is known to solve these equations.

2.2 Singular Transformation and Its Property

The number of different t-dimensional vectors $\{\boldsymbol{Y}\}$ over $\mathbb{F}_2$ is evidently given by 2^t. Because most of the transformation Φ given by Eq.(11) is singular, the vectors are transformed $W(\leq 2^t)$ different values of $\tilde{\boldsymbol{Z}}^{(1)}, \tilde{\boldsymbol{Z}}^{(2)}, \cdots, \tilde{\boldsymbol{Z}}^{(W)}$. That is, the different values, $\tilde{\boldsymbol{Y}}_1^{(i)}, \tilde{\boldsymbol{Y}}_2^{(i)}, \cdots, \tilde{\boldsymbol{Y}}_{\nu_i}^{(i)}$, may take on the same value of $\tilde{\boldsymbol{Z}}^{(i)}$, where ν_i is an integer larger than or equal to 1. Evidently t and W satisfy the following relation :

$$\nu_1 + \nu_2 + \cdots + \nu_W = 2^t. \quad (14)$$

In the followings we shall refer to W as *width of transformation*.

Let us denote an SE(2) by $\{z_1, z_2, \cdots, z_n\}$. The following SE(2), $\{u_1, u_2, \cdots, u_n\}$, will be referred to as *equivalent SE(2)* to the SE(2), $\{z_1, z_2, \cdots, z_n\}$, if it is given by the following relation:

$$(z_1, z_2, \cdots, z_n)L_n = (u_1, u_2, \cdots, u_n), \quad (15)$$

where L_n is a non-singular $n \times n$ matrix.

As an example, we assume that the transformation Φ is given by the following equations:

$$\left.\begin{aligned} z_1 &= y_1 + f_1^{(2)}(y_1, y_2, y_3, y_4) \\ z_2 &= y_2 + f_2^{(2)}(y_1, y_2, y_3, y_4) \\ z_3 &= y_3 + f_3^{(2)}(y_1, y_2, y_3, y_4) \\ z_4 &= y_4 + f_4^{(2)}(y_1, y_2, y_3, y_4) \end{aligned}\right\}, \quad (16)$$

where we assume that $f_i^{(2)}(y_1, y_2, y_3, y_4)$ consists of only quadratic terms. Evidently, any pair of different simultaneous equation given by Eq.(16) which are generated in a random manner is not equivalent each other [15].

Let us denote the transformation given by Eq.(16) by Φ_{I4}, where the subscript $I4$ stands for the following identity matrix that appears in Eq.(16):

$$I4 = \begin{bmatrix} y_1 & & & 0 \\ & y_2 & & \\ & & y_3 & \\ 0 & & & y_4 \end{bmatrix}. \quad (17)$$

In the followings the transformation Φ that yields the width W will be denoted by $\Phi^{(W)}$. The distribution of the number of the possible transformations $\{\Phi_{I4}^{(W)}\}$ for the given width W, is shown in Table 1. In Table 1, we denote the total number of different transformations $\{\Phi_{I4}^{(W)}\}$ by $\#\left\{\Phi_{I4}^{(W)}\right\}$. From Table 1, we see that the maximum number of transformations is given by the width $W = 11$. It should be noted that the transformation $\Phi_{I4}$with $W = 16$ implies the non-singular transformation.

Definition 2: The size, $S^{(W)}$, of the set of transformations $\{\Phi^{(W)}\}$ is defined as :

$$S^{(W)} = \log_2 \#\left\{\Phi^{(W)}\right\} \text{ (in bits)}. \quad (18)$$

□

In Table 1, we show the size $S^{(W)}$ for the given W

Definition 3: The information rate, r, is defined as

$$r = \frac{\log_2 W}{t}. \quad (19)$$

From Table 1, we see that the total number of different non-singular transformations $\{\Phi_{I4}^{(16)}\}$ is given by 2816. In this case the information rate r is given by 1.0. On the other hand, for $\Phi_{I4}^{(14)}$, the information rate r is given by $r = 0.952$. However it should be noted that the number of different transformations with $W = 14$ is improved by factors of 62 compared with the number of transformation with $W = 16$. We see that the number of different transformation can be significantly enlarged by introducing a small amount of redundancy.

2.3 Encryption and Decryption

2.3.1 Encryption

Throughout this paper, we assume that the message vector $\tilde{\boldsymbol{X}} = (\tilde{\boldsymbol{X}}_1, \tilde{\boldsymbol{X}}_2, \cdots, \tilde{\boldsymbol{X}}_k)$ is uniformly distributed in k tuples over $\mathbb{F}_2$.

The message vector $\tilde{\boldsymbol{X}}$ is encrypted as follows :

[Algorithm II]

Step 1 : Hashed vector $\tilde{\boldsymbol{H}} = (\tilde{H}_1, \tilde{H}_2, \cdots, \tilde{H}_g)$ is computed by $h(\tilde{\boldsymbol{X}})$ based on the message $\tilde{\boldsymbol{X}} = (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k)$. The redundant message vector $\tilde{\boldsymbol{x}}$ is constructed as

$$\tilde{\boldsymbol{x}} = (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k, \tilde{H}_1, \tilde{H}_2, \cdots, \tilde{H}_g), \tag{20}$$

where $h(\ )$ is a hash function.

Step 2 : The ciphertext is then computed by substituting $\tilde{\boldsymbol{x}}$ in Eq.(13), yielding the ciphertext $\boldsymbol{C} = (C_1, C_2, \cdots, C_n)$ over $\mathbb{F}_2$, where $C_j = \tilde{K}_j$.

Thus, we see that the encryption can be performed simply by substituting $\tilde{X}_i$ and $\tilde{H}_j$ for X_i and H_j in Eq.(13) respectively where $1 \le i \le k$ and $1 \le j \le g$, yielding the ciphertext $\boldsymbol{C} = (C_1, C_2, \cdots, C_n)$ over $\mathbb{F}_2$.

2.3.2 Decryption

Decryption can be performed through the following Steps.

[Algorithm III]

Step 1 : Ciphertext $\boldsymbol{C}$ is inverse-transformed to $\tilde{\boldsymbol{Z}}$ as follows:

$$\boldsymbol{C}B^{-1} = \tilde{\boldsymbol{Z}}. \tag{21}$$

The $\tilde{\boldsymbol{Z}}$ is partitioned into N sub-vectors each of which has the dimension t as follows :

$$\tilde{\boldsymbol{Z}} = (\tilde{\boldsymbol{Z}}_1, \tilde{\boldsymbol{Z}}_2, \cdots, \tilde{\boldsymbol{Z}}_N). \tag{22}$$

Step 2 : The $\tilde{\boldsymbol{Z}}_j$ is inverse transformed to $\tilde{\boldsymbol{Y}}_j$ through the inverse transformation of $\Phi_j^{-1}(\tilde{\boldsymbol{Z}}_j)$ by a table look-up method. As the transformation Φ_j is singular, it is required that $\tilde{\boldsymbol{Y}}_j$ be estimated in at most $2^t - W_j + 1$ different ways, where W_j is the width of the transformation Φ_j. We shall denote this estimated value of $\tilde{\boldsymbol{Y}}_j$ by $\hat{\tilde{\boldsymbol{Y}}}_j$.

Step 3 : Estimated value of $\hat{\tilde{\boldsymbol{y}}} = (\hat{\tilde{\boldsymbol{Y}}}_1, \hat{\tilde{\boldsymbol{Y}}}_2, \cdots, \hat{\tilde{\boldsymbol{Y}}}_N)$ is then inverse-transformed to $\hat{\tilde{\boldsymbol{x}}}$ as follows:

$$\hat{\tilde{\boldsymbol{y}}}A^{-1} = \hat{\tilde{\boldsymbol{x}}} = (\hat{\tilde{X}}_1, \hat{\tilde{X}}_2, \cdots, \hat{\tilde{X}}_k, \hat{\tilde{H}}_1, \hat{\tilde{H}}_2, \cdots, \hat{\tilde{H}}_g). \tag{23}$$

Step 4 : Assuming that the $\tilde{\boldsymbol{Y}}_j$ is estimated in G_j different ways for the given $\tilde{\boldsymbol{Z}}_j$, the $\tilde{\boldsymbol{x}}$ is estimated in $\prod_{j=1}^{N} G_j$ different ways. Each of the estimated $\hat{\tilde{\boldsymbol{x}}}$ is checked if the estimated messages $\hat{\tilde{X}}_1, \hat{\tilde{X}}_2, \cdots, \hat{\tilde{X}}_k$ are coincident with those of the hashed values $\hat{\tilde{H}}_1, \hat{\tilde{H}}_2, \cdots, \hat{\tilde{H}}_g$. When one of the estimated messages $\hat{\tilde{X}}_1, \hat{\tilde{X}}_2, \cdots, \hat{\tilde{X}}_k$ are coincident with $\hat{\tilde{H}}_1, \hat{\tilde{H}}_2, \cdots, \hat{\tilde{H}}_g$, the messages $(\tilde{X}_1, \tilde{X}_2, \cdots \tilde{X}_k)$ are decoded as the values $(\hat{\tilde{X}}_1, \hat{\tilde{X}}_2, \cdots \hat{\tilde{X}}_k)$. If the estimated messages are not coincident with the hashed values, another estimated value of $\hat{\tilde{\boldsymbol{y}}}$ is checked.

Table 2 Total size of transformation, $NS_{I4}^{(14)}$.

n	N	$NS_{I4}^{(14)}$ (bits)
96	24	418
128	32	558
160	40	697

Theorem 1: The probability of decoding messages $\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k$ incorrectly, $P[\varepsilon]$, can be given by

$$P[\varepsilon] = \left(\prod_{j=1}^{N} G_j - 1 \right) 2^{-g}, \tag{24}$$

where we assume that the messages, hashed values and simultaneous equations are sufficiently random. □

Example 1:

Transformation used : $\Phi_{I4}^{(14)}$ in Table 1.
The size of sub-vectors, t : 4
The size of the transformation, $S_{I4}^{(14)}$, is given by

$$S_{I4}^{(14)} = \log_2 175680 = 17.42 \text{ (in bits)}. \tag{25}$$

The total size of the transformation, $NS_{I4}^{(14)}$ is shown in Table 2 for the different values of n.

□

Theorem 2: The total number of the possible transformation Φ_{MI} of Eq.(1) is given by

$$|\Phi_{\mathrm{MI}}| = \frac{1}{n}\varphi(2^n - 1)(n - 1), \tag{26}$$

where $\varphi(x)$ is the Euler's function of x. □

For example, when $n = t = 128$, $\log_2 |\Phi_{\mathrm{MI}}|$ is

$$\log_2 |\Phi_{\mathrm{MI}}| = \log_2 \left\{ \frac{1}{128}\varphi(2^{128} - 1) \times 127 \right\} \fallingdotseq 127 \text{ (in bits)}. \tag{27}$$

It should be noted that, in MI-SE(2)PKC, $t = 128$ is allowed because the transformation Φ_{MI} is algebraic. Although the details of doing so are omitted, we can show that the size of the transformation defined by Eq.(2) used in LD-SE(2)PKC for $n = t = 128$ is given by 140(in bits). It should be reminded here that the choosing of $t = 128$ is allowed in LD-SE(2)PKC as the transformation Φ_{LD} is also algebraic.

We see that the total size of the transformation of the proposed RSSE(2)PKC takes on significantly large values that introduce that much randomness to our scheme, compared with the conventional schemes such as MI-SE(2)PKC or LD-SE(2)PKC.

In case $\tilde{\boldsymbol{Z}}_i$ has more than one candidates, $\hat{\tilde{\boldsymbol{Y}}}_i$'s, when estimating $\tilde{\boldsymbol{Y}}_i$, we shall denote the number of candidates by $\nu_{\tilde{Z}_i}$. In any transformation $\Phi_{I4}^{(14)}$, whenever $\tilde{\boldsymbol{Z}}_i$ has more than one candidates, the $\nu_{\tilde{Z}_i}$ takes on the same value of 2. Thus the average number of times, N_{EST}, for estimating the correct $(\hat{\tilde{\boldsymbol{Y}}}_1, \hat{\tilde{\boldsymbol{Y}}}_2, \cdots, \hat{\tilde{\boldsymbol{Y}}}_N)$ is given by

$$N_{EST} = \sum_{i=0}^{N} {}_N C_i \left(\frac{4}{16}\right)^i \left(\frac{12}{16}\right)^{N-i} \frac{1 + 2^i}{2}. \tag{28}$$

3. A Method for Reducing the Average Number of Estimations

3.1 Example of Original Method

First we shall show an example, assuming that we use the transformations $\Phi_{I4}^{(14)}$.

Example 2: $n = 128, k = 88, g = 40, t = 4$.

The average number of estimation, N_{EST}, is given by

$$N_{EST} = \sum_{i=0}^{32} {}_{32}C_i \left(\frac{4}{16}\right)^i \left(\frac{12}{16}\right)^{32-i} \frac{1+2^i}{2} \fallingdotseq 632. \quad (29)$$

The probability $P_{e,D}$ that the erroneous decoding occurs is given by

$$Pe,D = \sum_{i=0}^{32} {}_{32}C_i \left(\frac{1}{4}\right)^i \left(\frac{3}{4}\right)^{32-i} \frac{1+2^i}{2} 2^{-g} \fallingdotseq 5.74 \times 10^{-10} \quad (30)$$

We see that the probability $P_{e,D}$ assumes sufficiently small value. Evidently, the $P_{e,D}$ can be made sufficiently small by choosing a large value of g.

□

In the following sub-sections, we shall present a method for reducing the average number of estimations.

3.2 A Hybrid-Type Construction for Reducing the Average Number of Estimations

One of the most simple method for reducing the average number of estimations is to use both types of SE's, i.e. singular SE's and non-singular SE's when constructing RSSE(2)PKC.

We shall present an example of the construction in the following.

Example 3: $n = 128, k = 88, g = 40, t = 4$.

For constructing RSSE(2), we assume that the transformations of both $\Phi_{I4}^{(14)}$ and $\Phi_{I4}^{(16)}$ (non-singular transformations) are used.

For obtaining $\boldsymbol{Z}_j$ through the transformation, $\Phi_j(\boldsymbol{Y}_j) = \boldsymbol{Z}_j$, where $j = 1, 2, \cdots, N$, we assume, without loss of generality, that the transformation $\Phi_{I4}^{(14)}$ is used for $j = 1, \cdots, N/2$ and $\Phi_{I4}^{(16)}$ for $j = N/2 + 1, \cdots, N$.

Size of the transformation, $S_{I4,N}^{(14,16)}$, in this example is given by

$$S_{I4,N}^{(14,16)} = \frac{N}{2} S_{I4}^{(14)} + \frac{N}{2} S_{I4}^{(16)} = 462.08.(\text{in bits}) \quad (31)$$

We see that the $S_{I4,N}^{(14,16)}$ is still significantly large compared with the conventional transformation used in such as LD-SE(2)PKC.

□

Table 3 Average number of estimations and decoding errors for hybrid-type RSSE(2)PKC.

$n(\Phi_{I4}^{(14)})$	4	8	12	16
Size of transformation	390.56	414.4	438.24	462.08
Average number of estimation $N_{EST}^{(h)}$	1.72	3.480	7.78	18.26
Decoding error $P_{e,D} \times 10^{-12}$	1.56	3.17	7.07	16.6

Letting the total number of the using of $\Phi_{I4}^{(14)}$ for constructing RSSE(2)PKC be denoted as $n(\Phi_{I4}^{(14)})$, the average number of estimations, $N_{EST}^{(h)}$, is given by

$$N_{EST}^{(h)} = \sum_{i=0}^{n(\Phi_{I4}^{(14)})} {}_{n(\Phi_{I4}^{(14)})}C_i \left(\frac{4}{16}\right)^i \left(\frac{12}{14}\right)^{n(\Phi_{I4}^{(14)})-i} \frac{1+2^i}{2}. \quad (32)$$

We show the average number of the estimations, the size of transformations, and the decoding errors in Table 3. We see that the average number of estimation for hybrid-type RSSE(2)PKC is made small compared with the original scheme.

4. Security of RSSE(2)PKC

(I) Patarin's Attack

Patarin presented a method for breaking the MI-SE(2)PKC. The original transformation, Φ_{MI}, proposed by Matsumoto and Imai can be rewritten as:

$$\Phi_{\mathrm{MI}} : \boldsymbol{x} \longmapsto \boldsymbol{x}^h, \quad (33)$$

where $\boldsymbol{x} \in \mathbb{F}_{2^n}$ and $h = 2^\theta + 1$.

Letting $\boldsymbol{y} = \boldsymbol{x}^{2^\theta+1}$, Patarin succeeded to derive the following simple relation:

$$\boldsymbol{y} \cdot \boldsymbol{x}^{2^\theta} = \boldsymbol{y}^{2^{2\theta}} \cdot \boldsymbol{x}, \quad (34)$$

for breaking the MI-SE(2)PKC.

The point of the success of the Patarin's Attack is due to the fact that all the components of the vectors $\boldsymbol{x}^{2^\theta}$ and $\boldsymbol{y}^{2^{2\theta}}$ are linear functions of the components $\{x_i\}$ and $\{y_i\}$ respectively, because the x_i and y_i are the elements of $\mathbb{F}_2$.

In most of the conventional SE(2)PKCs the simple algebraic transformation given by Eq.(33) and the variants are used. For reasons of this, the simple relation such as Eq.(34) holds. However the proposed RSSE(2)PKC uses random transformations with no algebraic structure for obtaining the simultaneous equations. It apparently seems difficult to obtain a simple relation such as Eq.(34) which plays a central role in the Patarin's Attack.

Thus we can conclude that the proposed RSSE(2) PKC is invulnerable to the Patarin's Attack.

(II) Goubin-Courtois Attack

In the TPM scheme, so-called n triangular quadratic equations are constructed along with the u "added" quadratic equations and then the beginning r equations are removed. However this scheme was broken by Goubin and

Courtois. Goubin and Courtois pointed out that such construction can be broken by Gröbner bases when $m = n+u-r$ takes on the larger value than n, i.e., when the scheme has some redundancy.

Our proposed scheme RSSE(2)PKC constructed by Algorithm I seems secure from the following standpoints: RSSE(2)PKC does not use the weak form of the triangular construction.

(III) Attack using Gröbner bases

We see that the random version of SE(2) is more secure against the attack based on Gröbner bases compared with the conventional SE(2) [2], [5], [6] as is described on page 10 in the Ref. [4]. The RSSE(2) proposed here is able to yield more randomness when constructing SE(2) as shown in Tables 2 and 3 in this paper. Besides, although the details of doing so are omitted, the addition of another class of SE(referred to as the 2nd class of SE's in Ref. [1]) is able to make our RSSE(2) schemes, further random. Accordingly, our proposed scheme would be more secure, compared with the HFE on page 10 of Ref. [4].

5. Concluding Remarks

We have presented a new class of public key cryptosystem referred to as RSSE(2)PKC. The proposed method of using the random singular simultaneous equations has successfully realized the increasing of the size of the transformation used for obtaining the SE, compared with the conventional methods.

The set of public keys given by Eq. (13) constitutes singular simultaneous equations. No systematic method has been known to solve these equations, partly because the investigations of singular simultaneous equations are of no importance as they seem to have no practical use. Thus we believe that the random generation of singular simultaneous equations and applying them for constructing PKC presented in this paper open up a brand-new area of solving singular simultaneous equations in an elegant manner.

When constructing the conventional RNSE(2)PKC, it is required to use non-singular simultaneous equations. It should be noted that, from a practical limitation of computation times, the findings of non-singular simultaneous equations becomes difficult for $t \geq 6$.

However when using singular simultaneous equations, the limitation only depends on the size of the table which is used when solving singular simultaneous equations at the receiving end. The size of the table is, obviously, given by $t \cdot 2^t$ (in bits). For example, for $t = 20$, the size of the table takes on the value of approximately 2.62MB which is not too large. Thus the using of the RSSE(2)PKC with $t \leq 20$ seems practical.

The constructing a RSSE(2)PKC where t assumes $16 \sim 20$ seems very interesting, as it is conjectured that the number of estimation can be reduced compared with RSSE(2)PKC with small t. The investigations for constructing RSSE(2) with a large value of t is left for a future study.

In this paper, we have discussed primarily on RSSE(2) PKC over $\mathbb{F}_2$, although the proposed RSSE(2)PKC can be generalized in various ways. Various interesting studies have been left for the future.

References

[1] M. Kasahara and R. Sakai, "A construction of public-key cryptosystem based on singular simultaneous equations," Proc. SCIS2004, 1B5, Jan. 2004.
[2] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature—Verification and message-encryption," Advances in Cryptology, Eurocrypt'88, pp.419–453, Springer-Verlag, 1989.
[3] N. Koblitz, Algebraic Aspects of Cryptography, Springer-Verlag, Berlin Heidelberg, 1998.
[4] J.C. Faugere, "Algebraic cryptoanalysis of HFE using Gröbner bases," Report de recherche, INRIA, no.4738, Feb. 2003.
[5] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88," Advances in Cryptography, Crypto'95, pp.248–261, Springer Verlag, 1996.
[6] J. Patarin, "Asymmetric cryptography with a hidden monomial," Advances in Cryptography, Crypto'96, pp.45–60, Springer Verlag, 1996.
[7] N.T. Courtois, "The security of hidden field equation (HFE)," RSA Conference 2001, Available at http://www.minrank.org/hfe, 2001.
[8] A. Kipnis and A. Shamir, "Cryptoanalysis of the oil and vinegar signature scheme," Crypto'98, pp.257–226, Springer Verlag, 1998.
[9] T.T. Moh, "A public key system with signature and master key functions," Communications in Algebra, vol.27, no.5, pp.2207–2222, 1999.
[10] L. Goubin and N.T. Courtois, "Cryptanalysis of the TTM cryptosystem," Advances in Cryptography, Asia Crypto'00, pp.44–57, Springer Verlag, 2000.
[11] M. Kasahara and R. Sakai, "Notes on public key cryptosystem based on multivariate polynomials of high degree," IEICE Technical Report, ISEC 2001-64, Sept. 2001.
[12] M. Kasahara and R. Sakai, "A construction of a new public key cryptosystems on the basis of multivariate polynomials of high degree—A method for yielding short public key cryptosystem and short digital signature scheme," IEICE Technical Report, ISEC 2002-67, Sept. 2002.
[13] M. Kasahara and R. Sakai, "A construction of short public-key cryptosystem over extension field," IEICE Technical Report, ISEC 2002-116, March 2003.
[14] M. Kasahara and R. Sakai, "A construction of 100 bit public-key cryptosystem and digital signature scheme," Proc. SCIS2003, C8-2, Jan. 2003.
[15] M. Kasahara and R. Sakai, "A construction of public key cryptosystem for realizing ciphertext of size 100 bit and digital signature scheme," IEICE Trans. Fundamentals, vol.E87-A, no.1, pp.102–109, Jan. 2004.

Masao Kasahara was born in Tokyo, Japan, on October 11, 1936. He received the B.E. degree in electrical engineering from Osaka Prefecture University, Osaka, Japan, in 1960 and the the M.E. degree and the D.E. degree in communication engineering from Osaka University, Osaka, Japan, in 1962 and 1965, respectively. From 1965 to 1967 he was an Instructor of Communication Engineering at Osaka University. From 1967 to 1969 he was a member of the Technical Staff at Bell Laboratories, Holmdel, NJ, on leave of absence from Osaka University. From 1969 to 1972 he was an Assistant Professor and from 1972 to 1987 he was an Associate Professor at the Department of Communication Engineering, Osaka University. From 1987 to 2000 he has been a Professor at the Department of Electronics and Information Science, Kyoto Institute of Technology. Since 2000, he has been a professor at the Faculty of Informatics, Osaka Gakuin University. He was the recipient of the 1966 Inada Memorial Scholarships, 1983 Excellent Paper Award, 1986 Excellent Book Award, 1993 Achievement Award, and 1993 Kobayash-Memorial Achievement Award all from the Institute of Electronics, Information and Communication Engineers of Japan (IEICE). He received the 1991 Telecom-System-Technology Award from the Telecommunication Advancement Foundation. He was the Chairperson of the Technical Group on Information Theory of the IEICE from 1985 to 1987. He was the Chairperson of the Technical Group on Information Security from 1988 to 1989. He was the Chairperson of the Technical Group on Information Ethics from 1993 to 1995. He was the President of the Engineering Science Society of IEICEJ from 1996 to 1997. His interests are in error correcting codes, information security, digital communication systems and Information ethics. He is a member of the Information Processing Society of Japan, and the Institute of Television Engineers of Japan. He is a Life Fellow of the IEEE. He is a member of the Engineering Academy of Japan.

Ryuichi Sakai received the M.E. and the D.E. degrees in Communication Engineering from Kyoto Institute of Technology in 1990, 1992 and 1995, respectively. He is presently a Lecturer at the Department of Lightwave Sciences, Osaka Electro-Communication University. His research interests are in cryptography, information security and error correcting codes.