社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26 （7）
2004／7／20

拡大体上のハイブリッド型多次多変数公開鍵暗号の構成

笠原 正雄† 境 隆一††

† 大阪学院大学情報学部
†† 大阪電気通信大学工学部
E-mail: †kasahara@utc.osaka-gu.ac.jp, ††sakai@isc.osakac.ac.jp

あらまし 一般に多項式の変数に拡大体の元を用いることにより、多次多変数公開鍵暗号の公開鍵のサイズを小さくすることが可能である。本稿では、安全性にも考慮しつつ拡大体上定義された非正則な多次多変数連立方程式に基づくハイブリッド型多次多変数公開鍵暗号を提案する。そして具体的な構成例を示す。
キーワード 多次多変数, 公開鍵暗号, ランダム連立方程式

A Construction of Public Key Cryptosystem based on Random Singular and Non-singular Simultaneous Equations over Extension Field

Masao KASAHARA† and Ryuichi SAKAI††

† Osaka Gakuin University
†† Osaka Electro-Communication University
E-mail: †kasahara@utc.osaka-gu.ac.jp, ††sakai@isc.osakac.ac.jp

Abstract Extensive studies have been made of the public-key cryptosystems based on multivariate polynomials. However most of the proposed public-key cryptosystems based on multivariate polynomials, are proved not secure, although the size of the public-key assumes a very large value. In this paper, we propose several types of new constructions of public-key cryptosystems based on two classes of randomly generated simultaneous equations, namely, a class of simultaneous equations based on bijective transformation and another class of simultaneous equations based on random transformation which are not necessarily non-singular. One of the features of the proposed cryptosystems is that the size of the public-key is made much shortened compared with the conventional public-key cryptosystem based on multivariate polynomials. We also show that the sets of random simultaneous equations significantly improve the utilization factor of the public-key space. We show an example of the proposed cryptosystem over extension field where the size of the cipher-text takes on the small values of 160 ～ 200(in bits). We see that our proposed system, regardless of the small size of public-key, seems to be apparently secure, in a sense that the utilization factor is sufficiently large compared with the conventional public-key cryptosystems based on multivariate polynomials and that the public keys constitute non-singular simultanous equations.
Key words multi-variate polynomial, public-key cryptosystem, random simultaneos equation

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 larger than or equal to 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

constitutes the singular simultaneous equations and 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 SSE(d). Thus the proposed PKC based on SSE(d) apparently seems more secure compared with the conventional SE(d)PKC.

2. RSSE(d)PKC over $\mathbb{F}_{2^m}$

2.1 Construction of RSSE(d)PKC

Letting a message vector over $\mathbb{F}_{2^m}$ be denoted by $\boldsymbol{X} = (X_1, X_2, \cdots, X_k)$ and the hashed value of $\boldsymbol{X}$, by $(H_1, H_2, \cdots, H_g)$, $H_i \in \mathbb{F}_{2^m}$, the redundant message vector, $\boldsymbol{X}_\rho$ can be written as:

$$\boldsymbol{X}_\rho = (X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g). \tag{1}$$

The following relation implies that the message vector $\boldsymbol{X}$ takes on a certain value $\tilde{\boldsymbol{X}}$:

$$\boldsymbol{X} = \tilde{\boldsymbol{X}} = (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k), \tag{2}$$

where we assume that the variant X_i takes on a certain value $\tilde{X}_i$ that belongs to $\mathbb{F}_{2^m}$.

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

One of the simplest version of the RSSE(d)PKC over $\mathbb{F}_{2^m}$ can be constructed in the following manner where we let $d = 2$.

[Algorithm I]

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

$$\boldsymbol{X}_\rho \cdot A_1 = \boldsymbol{x} = (x_1, x_2, \cdots, x_n), \tag{3}$$

where $x_i \in \mathbb{F}_{2^m}$ and A_1 is a public $n \times n$ non-singular matrix over $\mathbb{F}_{2^m}$.

Step 2 : The transformed version of the redundant message vector, $\boldsymbol{x}$, is then transformed to $\boldsymbol{y}$ as follows:

$$\boldsymbol{x}A_2 = \boldsymbol{y} = (y_1, y_2, \cdots, y_n), \tag{4}$$

where $y_i \in \mathbb{F}_{2^m}$ and A_2 is an $n \times n$ non-singular secret matrix over $\mathbb{F}_{2^m}$.

[Remark 1] The transformations in Steps 1 and 2 can be merged into a single transformation given by the following secret matrix A :

$$A = A_1 A_2. \tag{5}$$

Thus it should be noted that the redundant message vector $\boldsymbol{X}_\rho$ is used as an input message vector to the encoder of our cryptosystem whose public-keys are given by Eq.(15).

Step 3 : The components of the vector $\boldsymbol{y}$ are partitioned into N sub-vectors, yielding the following vector :

$$\boldsymbol{y} = (\boldsymbol{Y}_1, \boldsymbol{Y}_2, \cdots, \boldsymbol{Y}_N), \tag{6}$$

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

$$\boldsymbol{Y}_j = (y_{j1}, y_{j2}, \cdots, y_{jt_j}). \tag{7}$$

[Definition 1] The following transformation :

$$\Lambda(\boldsymbol{u}) = \boldsymbol{v}, \tag{8}$$

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

$$\Lambda^{-1}(\boldsymbol{v}) = \boldsymbol{u}, \tag{9}$$

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". □

[Definition 2] The following transformation Λ_A is referred to as algebraic transformation :

$$\begin{aligned} \Lambda_A : Z_j(X) &= (y_{j1} + y_{j1}X + \cdots + y_{jt_j}X^{t_j-1})^g \\ &\equiv z_{j1} + z_{j2}X + \cdots + z_{jt_j}X^{t_j-1} \pmod{G_j(X)}, \end{aligned} \tag{10}$$

where $G_j(X)$ is a primitive polynomial of degree t_j over $\mathbb{F}_{2^m}$. □

Step 4 : 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 or on the basis of algebraic method:

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

yielding $\boldsymbol{Z}_j = (z_{j1}, z_{j2}, \cdots, z_{jt_j})$ where $z_{ji} =$

$\Phi_{ji}^{(2)}(y_{j1}, y_{j2}, \cdots, y_{jt_j})$ is a quadratic equation in t_j variables $y_{j1}, y_{j2}, \cdots, y_{jt_j}$. When the transformation is performed randomly we assume that the coefficients of the equations are chosen in a random manner.

Step 5 : Given $Y_1, Y_2, \cdots, Y_j$, the following SE are generated in a random manner as in Step 4:

$$\begin{aligned}
w_{j1} &= r_1^{(2)}(y_{11}, \cdots, y_{1t_1}, y_{21}, \cdots, y_{2t_2}, \cdots, y_{j1}, \cdots, y_{jt_j}),\\
w_{j2} &= r_2^{(2)}(y_{11}, \cdots, y_{1t_1}, y_{21}, \cdots, y_{2t_2}, \cdots, y_{j1}, \cdots, y_{jt_j}),\\
&\vdots\\
w_{ji} &= r_i^{(2)}(y_{11}, \cdots, y_{1t_1}, y_{21}, \cdots, y_{2t_2}, \cdots, y_{j1}, \cdots, y_{jt_j}),\\
&\vdots\\
w_{jt_j} &= r_t^{(2)}(y_{11}, \cdots, y_{1t_1}, y_{21}, \cdots, y_{2t_2}, \cdots, y_{j1}, \cdots, y_{jt_j}).
\end{aligned} \tag{12}$$

We see that the above SE is random in a sense that the coefficients are generated in a random manner.

Step 6 : From $w_{j1}, w_{j2}, \cdots, w_{jt_j}$, the followings are generated :

$$\begin{aligned}
\gamma_{(j+1)1} &= z_{(j+1)1} + w_{j1},\\
\gamma_{(j+1)2} &= z_{(j+1)2} + w_{j2},\\
&\vdots\\
\gamma_{(j+1)i} &= z_{(j+1)i} + w_{ji},\\
&\vdots\\
\gamma_{(j+1)t_{j+1}} &= z_{(j+1)t_j} + w_{jt_j}.
\end{aligned} \tag{13}$$

Step 7 : Letting $\Gamma = (\Gamma_1, \Gamma_2, \cdots, \Gamma_N)$ where $\Gamma_j = (\gamma_{j1}, \gamma_{j2}, \cdots, \gamma_{jt_j})$, the following final transformation is performed :

$$\Gamma B = (K_1, K_2, \cdots, K_n), \tag{14}$$

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 $\mathbb{F}_{2^m}$.

The public keys can be denoted as

$$\left.\begin{aligned}
K_1 &= f_1^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g)\\
K_2 &= f_2^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g)\\
&\vdots\\
K_j &= f_j^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g)\\
&\vdots\\
K_n &= f_n^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g)
\end{aligned}\right\} \tag{15}$$

where $f_i^{(2)}(X_1, X_2, \cdots, X_k, H_1, H_2, \cdots, H_g)$ is evidently a quadratic polynomial. □

[Remark 2] The set of public keys given by Eq.(15) constitutes singular simultaneous equations. No systematic method is known to solve these equations. □

[Remark 3] In examples given in Section 4, Steps 5 and 6 will be slightly modified, although the basic principle has not been altered. □

2.2 Singular transformation and its property

When the transformation of (11) is performed on the basis of randomness, the number of different t-dimensional vectors $\{\boldsymbol{Y}\}$ over $\mathbb{F}_{2^m}$ is evidently given by 2^{mt}. Because most of the transformation Φ given by Eq.(11) is singular, the vectors are transformed to $W(\leqq 2^{mt})$ 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 1. Evidently t and W satisfy the following relation :

$$\nu_1 + \nu_2 + \cdots + \nu_W = 2^{mt}. \tag{16}$$

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:

$$(z_1, z_2, \cdots, z_n)L_n = (u_1, u_2, \cdots, u_n), \tag{17}$$

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:

$$\left.\begin{aligned}
z_1 &= y_1 + f_1^{(2)}(y_1, y_2, y_3, y_4)\\
z_2 &= y_2 + f_2^{(2)}(y_1, y_2, y_3, y_4)\\
z_3 &= y_3 + f_3^{(2)}(y_1, y_2, y_3, y_4)\\
z_4 &= y_4 + f_4^{(2)}(y_1, y_2, y_3, y_4)
\end{aligned}\right\}, \tag{18}$$

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.(18) which are generated in a random manner is not equivalent each other [6].

In Eq.(10), we assume that g can be represented as :

$$g = 2^{h_1} + 2^{h_2} + \cdots + 2^{h_\mu}, \tag{19}$$

where the integers $h_1, h_2, \cdots, h_\mu$ satisfy $0 \leqq h_1 < h_2 < \cdots < h_\mu < mt - 1$.

[Theorem 1] Using the following transformation Φ_2 :

$$\Phi_2 : y_{ji}^{2^{h_k}} = y_{ji}^{(k)}, \tag{20}$$

the SE(g) can be reduced to SE(μ). □

[Definition 3] The degree g of the SE given by Eq.(10) can be reduced to a lower degree μ through the transformation Φ_2. We shall refer to this reduction, ($g \to \mu$)Reduction and the constructed RSE(μ)-PKC as rSE(μ)-PKC, for short. □

Let us denote the set of variables, $\{y_{ji}^{(k)}\}$, by S_y. As any variable y_{ji} can be represented by a linear combination of the variables $x_1, x_2, \cdots, x_n$, any element, $y_{ji}^{(k)}$ is represented by a linear combination of $x_1^{(k)}, x_2^{(k)}, \cdots, x_n^{(k)}$, where $x_l^{(k)}$ can be defined in a similar manner as Eq.(20).

Let us denote the set of variables $x_i^{(1)}, x_j^{(2)}, \cdots, x_k^{(\mu)}$ where $1 \leqq i, j, k \leqq n$, by S_x.

[Definition 4] An element in S_y and S_x is referred to as r-variable. □

For constructing rSE(μ)-PKC, r-variables are used in a restricted manner. For example rSE(μ) is constructed only by the product of the r-variables which can be represented in a form of the product $x_i^{(1)} x_j^{(2)} \cdots x_k^{(\mu)}$.

[Remark 4] As we shall show later, the number of terms of each equation of rSE(μ)-PKC takes on a smaller value compared with that of the conventional SE(μ)-PKC, yielding a small size of public-key. □

[Modified Algorithm I for improving the security]

Letting $\boldsymbol{u} = (u_1, u_2, \ldots, u_{km})$ for a message vector over $\mathbb{F}_2$ and $\boldsymbol{v} = (v_1, v_2, \cdots, v_{gm})$, the hashed value of the message vector $\boldsymbol{u}$, the redundant message vector over $\mathbb{F}_2$ can be written as :

$$\boldsymbol{w}_\rho = (u_1, u_2, \ldots, u_{km}, v_1, v_2, \cdots, v_{gm}). \tag{21}$$

The redundant message vector $\boldsymbol{w}_\rho$ is then transformed to vector $\boldsymbol{w}$ as follows:

$$\boldsymbol{w}_\rho \cdot A_0 = \boldsymbol{w} = (w_1, w_2, \cdots, w_{nm}), \tag{22}$$

where $n = g + k$ and A_0 is an $n \times n$ non-singular public matrix.

Given $\boldsymbol{w}$, we regard the vector $\boldsymbol{w}$ over $\mathbb{F}_2$ as the vector $\boldsymbol{W}$ over $\mathbb{F}_{2^m}$ as follows:

$$\boldsymbol{W} = (x_1, x_2, \cdots, x_n), \tag{23}$$

where $x_i = (w_{im+1}, \cdots, w_{(i+1)m}) \in \mathbb{F}_{2^m}$, $(i = 0, 1, \cdots, n-1)$.

The transformation by A_1 in Step 1 of Algorithm I can be skipped in the modified Algorithm I.

For comparison, we first discuss on the size of the conventional SE(2)-PKC over $\mathbb{F}_2$. We have the following theorem.

[Theorem 2] The size of the public-key of SE(2)-PKC over $\mathbb{F}_2$, S_{PK}, is given by

$$S_{PK} = n({}_nH_2 + 1) = n({}_{n+1}C_2 + 1), \tag{24}$$

where n is the block-length of the cipher-text. □

For example, when $n = 160$, the size of S_{PK} is given by 2,060,800 bits or approximately 2M bits(258K byte).

3. Encryption and Decryption

3.1 Encryption

In Fig.1, we show an example of an encoder of RSSE(g)-PKC over $\mathbb{F}_{2^m}$ where we assume that $t_1 = t_2 = t_3 = 3$, $N = 3$, $n = 9$.

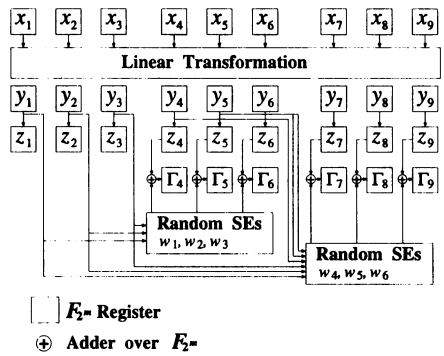

Fig. 1 An example of the principal part of the encoder of RSSE(g)-PKC over $\mathbb{F}_{2^m}$.

Encryption can be performed simply by substituting $\tilde{X}_i$ and $\tilde{H}_j$ for X_i and H_j in Eq.(15) respectively, yielding the ciphertext $\boldsymbol{C} = (C_1, C_2, \cdots, C_n)$ over $\mathbb{F}_{2^m}$

3.2 Decryption

Decryption can be performed through the following Steps.

[Algorithm II]

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

$$\boldsymbol{C}B^{-1} = \tilde{\boldsymbol{Z}}. \tag{25}$$

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

$$\tilde{\boldsymbol{Z}} = (\tilde{\boldsymbol{Z}}_1, \tilde{\boldsymbol{Z}}_2, \cdots, \tilde{\boldsymbol{Z}}_N). \tag{26}$$

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 an algebraic method or a table-lookup method when the transformation is algebraic and a table look-up method when the transformation is performed. When the transformation Φ_j is singular, it is required that $\tilde{\boldsymbol{Y}}_j$ be estimated in a several different ways.

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

$$\hat{\tilde{Y}} A^{-1} = \hat{\tilde{X}}_\rho = (\hat{\tilde{X}}_1, \hat{\tilde{X}}_2, \cdots, \hat{\tilde{X}}_k, \hat{\tilde{H}}_1, \hat{\tilde{H}}_2, \cdots, \hat{\tilde{H}}_g). \tag{27}$$

Step 4 : Assuming that the $\tilde{Y}_j$ is estimated in G_j different ways for the given $\tilde{Z}_j$, the $\tilde{Y}$ is estimated in $\prod_{j=1}^{N} G_j$ different ways. Each of the estimated $\hat{\tilde{Y}}$ is checked if the estimated hashed values $\hat{\tilde{H}}_1, \hat{\tilde{H}}_2, \cdots, \hat{\tilde{H}}_g$ are coincident with those of the messages $\hat{\tilde{X}}_1, \hat{\tilde{X}}_2, \cdots, \hat{\tilde{X}}_k$. If these values are proved not coincident, another estimated value of $\hat{\tilde{Y}}$ is checked. It should be noted that when the transformation is algebraic, then $G_j = 1$ □

4. Construction of rSE(g)-PKC over $\mathbb{F}_{2^m}$

4.1 Preliminaries

In this chapter, we present several examples of rSE(μ)-PKC which yields a much shorter size of public-key compared with the conventional SE(g) -PKC, under the condition that the effective size of public-key takes on a sufficiently large value.

We have the following theorems:

[Theorem 3] For the degree of t, the period of $G(X)$ is given by $2^{tm} - 1$. □

[Theorem 4] The size of public-key of the rSE(μ)-PKC over $\mathbb{F}_{2^m}$ is given by

$$S_{PK} = m \cdot n^{\mu+1} \text{ (bits)}. \tag{28}$$

□

[Definition 5] The rate of the shortening of the size of public-key over $\mathbb{F}_{2^m}$, for the rSE(μ)-PKC compared with that of the conventional SE(2)-PKC over $\mathbb{F}_2$, is given by

$$\eta_S = \frac{\text{size of public-key of rSE}(\mu)\text{-PKC over } \mathbb{F}_{2^m}}{\text{size of public-key of conventional SE(2)-PKC over } \mathbb{F}_2}, \tag{29}$$

where we assume that the sizes of the cipher-texts of both PKC are same. □

4.2 The case where $t = 2$

[Theorem 5] The possibilities of obtaining the SE(g), for $t = 2$ and for $g = 3, 5, 7, 9$ and 11, through the transformation Λ_A are given as follows :

(1) The SE(3) over $\mathbb{F}_{2^m}$ cannot be constructed for any m.

(2) The SE(5) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 2$.

(3) The SE(7) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 3$.

(4) The SE(9) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 3$.

(5) The SE(11) cannot be constructed for $m = 3m'$ where m' satisfies $2^{m'} \pm 1 \equiv 0 \pmod{11}$. □

[Example 1] From (2) in Theorem 5, we see that the rSE(2)-PKC over $\mathbb{F}_{2^{17}}$ where $n = 12$ and $t = 2$, can be constructed through $(5 \to 2)$Reduction.

The following transformations, defined by Eq.(11), are used:

Φ_1, Φ_2, Φ_3 : algebraic tarnsformation where $t_1 = t_2 = t_3 = 2$

Φ_4, Φ_5, Φ_6 : random transformation where $t_4 = t_5 = t_6 = 2$

The size of the pubic key of rSE(2)-PKC obtained through $(5 \to 2)$Reduction, S_{PK}, is given by

$$S_{PK} = 17 \cdot 12^3 = 29376 \quad \text{(bits)}. \tag{30}$$

We see that the size of the public-key in this example proves very small compared with the conventional SE(2)-PKC over $\mathbb{F}_2$ where $n = 204$. The rate of the shortening, η_s, is given by

$$\eta_s = \frac{29376}{4265640} = 0.00689. \tag{31}$$

The effective size of the public-key S_{PK}(effec.) is given by

$$\begin{aligned} S_{PK}(\text{effec.}) &= 3\log_2\left\{\frac{1}{t}\varphi(2^{mt}-1)\right\} + mt^2 \cdot 3t + m(3t)^2 3t \\ &= 3\log_2\left\{\frac{1}{2}\varphi(2^{17\cdot 2}-1)\right\} + 17\cdot 4\cdot 6 + 17\cdot 36\cdot 6 \\ &\fallingdotseq 4177 \quad \text{(bits)}. \end{aligned} \tag{32}$$

The number of r-variables in this example is 24. □

[Remark 5] In this example, the following transformation would yield more secure scheme.

Φ_1 : algebraic transformation where $t_1 = 6$

Φ_2, Φ_3, Φ_4 : random transformations where $t_2 = t_3 = t_4 = 2$.

□

4.3 The case where $t = 3$

We have the following theorem.

[Theorem 6] The possibilities of obtaining the SE(g), for $t = 3$ and for $g = 3, 5, 7, 9$ through the transformation Λ_A are given as follows :

(1) The SE(3) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 2$.

(2) The SE(5) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 4$.

(3) The SE(7) over $\mathbb{F}_{2^m}$ cannot be constructed for any m.

(4) The SE(9) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 2$.

(5) The SE(11) cannot be constructed for $m = 3m'$ where m' satisfies $2^{m'} \pm 1 \equiv 0 \pmod{11}$. □

[Example 2] rSE(2)-PKC over $\mathbb{F}_{2^{11}}$ where $n = 18$, which can be constructed through $(3 \to 2)$Reduction. The following transformations, defined by Eq.(11), are used

Φ_1, Φ_2, Φ_3 : algebraic tarnsformation
where $t_1 = t_2 = t_3 = 3$

Φ_4, Φ_5, Φ_6 : random transformation
where $t_4 = t_5 = t_6 = 3$

The size of the public-key of rSE(2)-PKC, S_{PK} is given by

$$S_{PK} = 11 \cdot 18^3 = 64152 \quad \text{(bits)} . \tag{33}$$

The rate of the shortening, η_s, is given by

$$\eta_s = \frac{64152}{3900798} = 0.0164. \tag{34}$$

The effective size of the public-key S_{PK}(effec.) is given by

$$\begin{aligned} S_{PK}(\text{effec.}) &= 3\log_2 \left\{ \frac{1}{3}\varphi(2^{33}-1) \right\} \\ &\quad +11 \cdot 3^2 \cdot 9 + 11 \cdot 9^2 \cdot 9 \\ &\fallingdotseq 9003 \quad \text{(bits)} . \end{aligned} \tag{35}$$

The number of r-variables in this example is 36. □

4.4 The case where $t = 4$

[Theorem 7] The possibilities of obtaining the SE(g), for $t = 4$ and for $g = 3, 5, 7, 9$ are given as follows :

(1) The SE(3) and SE(5) over $\mathbb{F}_{2^m}$ cannot be constructed for any m.

(2) The SE(7) over $\mathbb{F}_{2^m}$ can be constructed for $m \not\equiv 0 \pmod 3$.

(3) The SE(9) over $\mathbb{F}_{2^m}$ can be constructed for any m. □

[Example 3] rSE(3)-PKC over $\mathbb{F}_{2^{10}}$ where $n = 16$ and $t_1 = 8, t_2 = t_3 = t_4 = t_5 = 2$, which can be constructed through $(7 \to 3)$Reduction. The following transformations, defined by Eq.(11), are used

Φ_1 : algebraic tarnsformation
where $t_1 = 8$

$\Phi_2, \Phi_3, \Phi_4, \Phi_5$: random transformation
where $t_2 = t_3 = t_4 = t_5 = 2$

The size of the public-key of rSE(3)-PKC, S_{PK} is given by

$$S_{PK} = 10 \cdot 16^4 = 655360 \quad \text{(bits)} . \tag{36}$$

The effective size of the public-key S_{PK}(effec.) is given by

$$\begin{aligned} S_{PK}(\text{effec.}) &= 8\log_2 \left\{ \frac{1}{10}\varphi(2^{80}-1) \right\} \\ &\quad +10 \cdot 2^3 \cdot 4 \cdot 2 + 10 \cdot 8^3 \cdot 8 \\ &\fallingdotseq 42203 \quad \text{(bits)} . \end{aligned} \tag{37}$$

The number of r-variables in this example is 48, sufficiently large value for $\mu = 3$. The constructed rSE(3)-PKC seems apparently secure, though in this case the rate of shortening is given by 0.158, not sufficiently small value. □

4.5 Open problem

The new open problem of the hybrid RSE(2)-PKC is uploaded in WWW site
"http://www.osaka-gu.ac.jp/php/kasahara/publickey.htm".

5. Conclusion

We have presented a new class of public-key cryptosystem referred to as rSE(g)-PKC over $\mathbb{F}_{2^m}$. Although the details of doing so are omitted, we can show that the digital signature scheme can be easily realized with our proposed PKC.

We have presented many examples in this paper. The rSE(3)-PKC in Example 7 where the size of the public key is only 2511 bits, 0.66% of the size of the conventional SE(2)-PKC of the same length and the comparable size of that of the RSA public key (n, e). We sincerely wish the finding out the general method to attack this rSE(3)-PKC would be a challenging subject to researchers who are interested in public-key cryptosystems.

In this paper, we have discussed primarily on rSE(μ)-PKC over $\mathbb{F}_{2^m}$. However the proposed rSE(μ)-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. of SCIS2004, 1B5-1 pp.155-160(2004-1).

[2] N. Koblitz : "Algebraic Aspects of Cryptography", Springer-Verlag Berlin Heidelberg,(1998).

[3] T. Matsumoto and H. Imai : "Public quadratic Polynomial-tuples for efficient signature-verification and message-encryption", Proc. of Eurocrypt '88, Springer-Verlag, 419-453, (1989).

[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 (2001-9).

[5] 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 –", Technical Report of IEICE, ISEC 2002-67 (2002-9).

[6] M. Kasahara and R. Sakai : " A Construction of 100 bit Public-Key Cryptosystem and Digital Signature Scheme", Proc. of SCIS2003,C8-2,(2003-01).