A New Class of Public Key Cryptosystems Constructed Based on Error-Correcting Codes, Using K(Ⅲ) Scheme

Masao KASAHARA†

† Faculty of Informatics, Osaka Gakuin University, Kishibe-Minami, Suita-Shi, Osaka 564-8511 Japan
E-mail: kasahara@ogu.ac.jp

Abstract In this paper, we present a new scheme referred to as K(Ⅲ) scheme which would be effective for improving a certain class of PKC's. Using K(Ⅲ) scheme, we propose a new method for constructing the public-key cryptosystems based on error-correcting codes. The constructed PKC is referred to as K(V)SE(1)PKC. We also present more secure version of K(V)SE(1)PKC, referred to as K*(V)SE(1)PKC, using K(I) scheme previously proposed by the present author, as well as K(Ⅲ) scheme.

Key words Public Key Cryptosystem, Error-Correcting Code, Multivariate PKC, Linear PKC, McEliece PKC, PQC.

1. Introduction

Most of the multivariate PKC's so far proposed are constructed by simultaneous equations of degree larger than or equal to 2 [1-6]. Recently the present author proposed a several classes of multivariate PKC's that are constructed by many sets of linear equations [7,8], in a sharp contrast with the conventional multivariate PKC's where a single set of simultaneous equations of degree more than or equal to 2 are used. In Ref.[9], the present author proposed a new scheme referred to as K(I) scheme. This scheme can be applied for constructing a wide class of new PKC's.

In this paper, we present a new scheme referred to as K(Ⅲ) scheme which would be effective for improving a certain class of PKC's that are constructed based on error correcting codes. Using K(Ⅲ) scheme, we propose a new method for constructing the PKC's based on error-correcting codes. The constructed PKC is referred to as K(V)SE(1)PKC. We also present a more secure version of K(V)SE(1)PKC, referred to as K*(V)SE(1)PKC, using K(I) scheme. The K*(V)SE(1)PKC has the following remarkable features:

- Coding rate of exactly 1.0.
- Significantly small size of public key compared with the conventional SE(1)PKC.

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. Throughout this paper, (n, k, d) code implies the code of length n, number of information symbols k and the minimum distance d.

2. K(V)SE(1)PKC

2.1 Construction of K(V)SE(1)PKC

Let the message vector $\boldsymbol{M}$ over $\mathbb{F}_{2^m}$ be represented by

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

Throughout this paper we assume that the messages $M_1, M_2, \cdots, M_k$ are mutually independent and equally likely. Let $\boldsymbol{M}$ be transformed as

$$(M_1, M_2, \cdots, M_k)A_I = (m_1, m_2, \cdots, m_k), \tag{4}$$

where A_I is a $k \times k$ non-singular matrix over $\mathbb{F}_{2^m}$.

Let the error vector $\boldsymbol{E}$ over $\mathbb{F}_{2^m}$ be represented by

$$\boldsymbol{E} = (\alpha_1 E_1, \alpha_2 E_2, \cdots, \alpha_n E_n), \tag{5}$$

where $\alpha_i \in \mathbb{F}_{2^m}$ and we assume that n is larger than k.

Let us transform $\boldsymbol{E}$ into $\boldsymbol{e}$,

$$\begin{aligned}(\alpha_1 E_1, \alpha_2 E_2, \cdots, \alpha_n E_n)A_{II} &= \boldsymbol{e} \\ &= (e_1, e_2, \cdots, e_k),\end{aligned} \tag{6}$$

where A_{II} is an $n \times k$ matrix over $\mathbb{F}_{2^m}$.

Let the message vector $\boldsymbol{m}_E$ added with error variables $e_1, e_2, \cdots, e_k$ be defined by

$$\boldsymbol{m}_E = (m_1 + e_1, m_2 + e_2, \cdots, m_k + e_k). \tag{7}$$

We then encode $\boldsymbol{m}_E$ to a code word of an (n, k, d) code over $\mathbb{F}_{2^m}$ as

$$m_E(x)x^g \equiv r(x) \mod G(x), \tag{8}$$

where $G(x)$ is the generator polynomial of a cyclic code of degree $g = n - k$ over $\mathbb{F}_{2^m}$.

We assume that the minimum distance of the code is given by $2t+1$. Denoting $r(x)$ in a vector form by $(r_1, r_2, \cdots, r_g)$ over $\mathbb{F}_{2^m}$, the code word $\boldsymbol{w}$ can be represented by

$$\boldsymbol{w} = (r_1, r_2, \cdots, r_g, m_1 + e_1, \cdots, m_k + e_k). \tag{9}$$

We then construct the word $\boldsymbol{v}$ by adding the error vector $\boldsymbol{E} = (E_1, E_2, \cdots, E_n)$ on $\boldsymbol{w}$:

$$\begin{aligned}\boldsymbol{v} =& \boldsymbol{w} + \boldsymbol{E} \\ =&(r_1 + \alpha_1 E_1, r_2 + \alpha_2 E_2, \cdots, r_g + \alpha_g E_g, \\ & m_1 + e_1 + \alpha_{g+1}E_{g+1}, \cdots, m_k + e_k + \alpha_n E_n).\end{aligned} \tag{10}$$

We see that any component of $\boldsymbol{v}$ consists of a linear equation in the variables $M_1, M_2, \cdots, M_k$ and $E_1, E_2, \cdots, E_n$.

Remark 1: The error vector $E = (\alpha_1 E_1, \alpha_2 E_2, \cdots, \alpha_n E_n)$ is useful for hiding the structure of the code $\boldsymbol{w}$. Besides the $\boldsymbol{w}$ itself is further transformed to $\boldsymbol{u}_E$ using non-singular random matrix A_{III} over $\mathbb{F}_{2^m}$, as we see below. □

Let us define K(Ⅲ) scheme:

K(Ⅲ) scheme: The process of obtaining the vector $\boldsymbol{v}$ from the message $\boldsymbol{m}_E$ is very useful, because it can improve the security or coding rate of a large class of PKC's that are constructed based on error correcting codes (See Fig.1). □

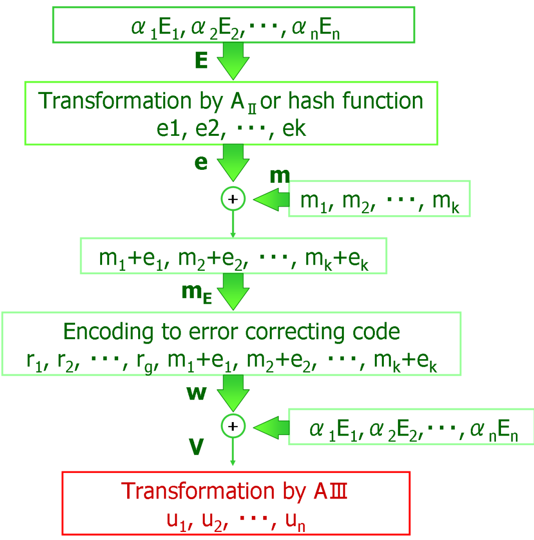

Fig. 1 K(Ⅲ) scheme

Let us further define a similar but simplified scheme, K*(Ⅲ) scheme, in the following:

K*(Ⅲ) scheme: Let us first define a predetermined error vector $\boldsymbol{e} = (e_1, e_2, \cdots, e_n)$ whose Hamming weight $w(\boldsymbol{e}) = t$. Let the hashed vector of $\boldsymbol{e}$ be $h(\boldsymbol{e}) = (e'_1, e'_2, \cdots, e'_k)$. The vectors $\boldsymbol{m}_E$, $\boldsymbol{w}$, $\boldsymbol{v}$ are given in an exactly similar manner as those given from Eqs.(7), (9) and (10). □

The vector $\boldsymbol{v}$ is further transformed into $\boldsymbol{u}$,

$$\begin{aligned}\boldsymbol{v}A_{III} &= \boldsymbol{u} \\ &= (u_1, u_2, \cdots, u_n).\end{aligned} \tag{11}$$

We have the following set of keys:

Public key:	$\{u_i\}$.
Secret key:	A_I, A_{II}, A_{III}, $G(x)$, $\{\alpha_i\}$, $\{e_i\}$.

2.2 Parameters

We see that u_i in Eq.(11) is a linear equation in the variables $M_1, M_2, \cdots, M_k$ and $E_1, E_2, \cdots, E_n$. Thus, the total number of equations, N_E, and the total number of variables, N_V, are proved to be given by

$$N_E = n = k + g \tag{12}$$

and

$$N_V = k + n = 2k + g \tag{13}$$

respectively.

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

$$\begin{aligned}S_{pk} &= N_E \cdot N_V \cdot m \\ &= (k+g)(2k+g)m.\end{aligned} \tag{14}$$

The coding rate, ρ, is given by

$$\rho = \frac{\text{number of information symbols}}{\text{length of ciphertext}} = \frac{k}{n}. \tag{15}$$

2.3 Encryption

The encryption can be performed by the following steps:

Step 1: Letting the Hamming weight of $\tilde{\boldsymbol{E}}$ be denoted by $w_H\left(\tilde{\boldsymbol{E}}\right)$, the sending end chooses nonzero $\tilde{E}_i$'s under the condition that

$$w_H\left(\tilde{\boldsymbol{E}}\right) = t \tag{16}$$

in a random manner.

Step 2: The ciphertext c is given by

$$c = (\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n). \tag{17}$$

□

The component $\tilde{u}_i$ is given by

$$\tilde{u}_i = f_i^{(1)}\left(\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_k, \tilde{E}_1, \tilde{E}_2, \cdots, \tilde{E}_n\right), \tag{18}$$

where $f_i^{(1)}(*)$ implies a linear equation.

2.4 Decryption

The decryption can be performed by the following steps:

Step 1: Given $c = (\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n)$, the receiving end transforms c into the vector $\tilde{\boldsymbol{v}}$,

$$\begin{aligned}(\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n)A_{III}^{-1} &= \tilde{\boldsymbol{v}} \\ &= (\tilde{v}_1, \tilde{v}_2, \cdots, \tilde{v}_n).\end{aligned} \tag{19}$$

Step 2: Given $\tilde{\boldsymbol{v}}$, the error vector $\tilde{\boldsymbol{E}} = (\alpha_1\tilde{E}_1,\ \alpha_2\tilde{E}_2,\ \cdots,\ \alpha_n\tilde{E}_n)$ can be successfully corrected, as $w_H\left(\tilde{\boldsymbol{E}}\right)$ satisfies $w_H\left(\tilde{\boldsymbol{E}}\right) = t$, yielding $\tilde{\boldsymbol{m}}_E$ and $\tilde{\boldsymbol{e}} = (\tilde{e}_1, \tilde{e}_2, \cdots, \tilde{e}_k)$.

Step 3: The vector $\tilde{\boldsymbol{e}} = (\tilde{e}_1, \tilde{e}_2, \cdots, \tilde{e}_k)$ is subtracted from $\tilde{\boldsymbol{m}}_E$, yielding vector $\tilde{\boldsymbol{m}}$.

Step 4: The vector $\tilde{\boldsymbol{m}}$ is inverse-transformed into the original message $\tilde{\boldsymbol{M}}$,

$$\tilde{\boldsymbol{M}} = \left(\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_k\right). \tag{20}$$

□

2.5 Security Considerations

In K(V)SE(1)PKC, we do not necessarily recommend to use the Goppa codes. Namely we believe that the use of the conventional code such as BCH code or Reed-Solomon code would cause no deterioration of security, in our proposed scheme.

The linear transformation matrices A_I, A_{II}, and A_{III} would be effective to hide the code structure. Besides we add the following error vector $\boldsymbol{E}$ on $\boldsymbol{w}$:

$$\boldsymbol{E} = (\alpha_1 E_1, \alpha_2 E_2, \cdots, \alpha_n E_n), \tag{21}$$

where $\alpha_i \in \mathbb{F}_{2^m}$ is chosen in a random manner.

As E_i takes on the value in $\mathbb{F}_{2^m}$ also in a random manner, the ambiguity of E_i, $h(E_i)$, can be given by

$$h(E_i) = \log_2(2^m - 1)\ \text{(bit)}. \tag{22}$$

In the examples given in this paper, the ambiguity of $\boldsymbol{E}$ will be chosen sufficiently large.

Remark 2: For $m = 1$, we let $\alpha_i = 1$; $i = 1, 2, \cdots, n$. Thus the entropy $h(\alpha_i) = 0$ (bit).

The entropy of the vector $\boldsymbol{E}$, $h(\boldsymbol{E})$, can be given by

$$h(\boldsymbol{E}) = {}_nC_t t \log_2(2^m - 1)\ \text{(bit)}, \tag{23}$$

for $m \geqq 2$. □

Remark 3: The error vector $\boldsymbol{E}$ is added on $\boldsymbol{w}$ whose component is given by a linear combination of $E_1, E_2, \cdots, E_n$. We thus conclude that the error vector $\boldsymbol{E}$ having a large ambiguity is able to hide the structure of the code used. Furthermore $\boldsymbol{w} + \boldsymbol{E}$ is transformed into $\boldsymbol{u}$ using A_{III} whose ambiguity can be given approximately by mn^2 bit. □

One of the most strong attacks on K(V)SE(1)PKC would be the following attack.

Attack I: Attack on $\boldsymbol{E}$. □

On Attack I, we assume the following two cases.

Case I: Attack I successfully estimates a set of error free symbols in the ciphertext at k locations, S_1, S_2, $\cdots$, S_k.

Case II: Attack I successfully estimates t nonzero symbols of the error vector $\boldsymbol{E}$.

Case I provides the k linear equations in k variables, yielding the message symbols $m_1, m_2, \cdots, m_k$. However each equation has an error component given by a linear combination of t errors. Let the probability that an error component consisted of t errors happens to be zero be denoted by $P_E(0)$. The $P_E(0)$ is given by

$$P_E(0) = 2^{-m} \tag{24}$$

for sufficiently large t. The probability that Case I where k error components happen to be all zeros occurs, $P_c(\mathrm{I})$, is given by

$$P_c(\mathrm{I}) = 2^{-mk}. \tag{25}$$

In the examples given in Table 1, the probabilities $P_c(\mathrm{I})$'s are made to be sufficiently small.

The probability that the Case II occurs, $P_c(\mathrm{II})$, is given by

$$P_c(\mathrm{II}) = \frac{1}{{}_nC_t}(2^m - 1)^{-t}. \tag{26}$$

We shall also see that the probability $P_c(\mathrm{II})$ is made sufficiently small in the examples in Table 1.

2.6 Example

In Table 1, we resent several example of K(V)SE(1)PKC.

表 1 Examples of K(V)SE(1)PKC over $\mathbb{F}_{2^m}$

	m	Code	n, N_E,	k	$n+k$, N_V	g, $n-k$
Example I	1	KS[12]	197	101	293	96
Example II	1	BCH[12]	255	147	402	108
Example III	8	S·RS*1	128	112	240	12
Example IV	8	S·RS*1	64	48	112	16

	t	$P_c(\mathrm{I})$	$P_c(\mathrm{II})$	S_{pk}(Kbit)	ρ
Example I	13	3.94×10^{-31}	2.57×10^{-18}	58	0.512
Example II	14	5.60×10^{-45}	2.55×10^{-23}	197	0.58
Example III	6	1.89×10^{-270}	6.54×10^{-25}	246	0.875
Example IV	8	2.53×10^{-116}	1.23×10^{-29}	57	0.75

*1 S·RS: Shortened Reed-Solomon code.

In Table 1, we present two examples of K(V)SE(1)PKC over $\mathbb{F}_{2^8}$.

3. Construction of K*(V)SE(1)PKC

3.1 K*(V)SE(1)PKC

In Ref.[9], the present author proposed a new scheme that has successfully strengthened a class of public key cryptosystems. Based on the new scheme, referred to as K(I) scheme, a new class of public key cryptosystem, K(Ⅳ)SE(1)PKC, is proposed in Ref.[9]. The K(Ⅳ)SE(1)PKC has the following remarkable features:

- Simple process of decryption as it uses a small class of perfect codes such as (7,4,3) Hamming code.
- Coding rate of exactly 1.0.
- Significantly small size of public key compared with that of McEliece PKC presented in 1977.

In this section we present another class of PKC, K*(V)SE(1)PKC, by applying K(I) scheme for K(V)SE(1)PKC. The principle of K(I) scheme is given in Fig.1. In K(I) scheme, we assume that the conditional entropy $H(\boldsymbol{M}|\boldsymbol{m}_p)$ satisfies the following relation holds:

$$H(\boldsymbol{M}|\boldsymbol{m}_P) \geqq 80 \text{ bit.} \tag{27}$$

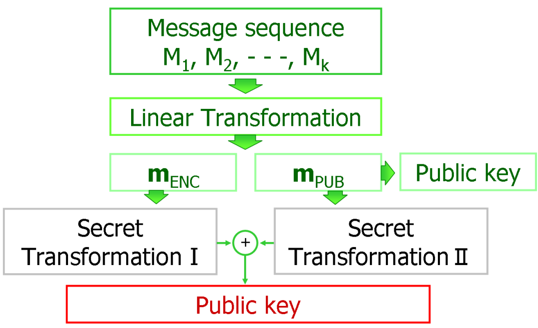

Fig. 2 K(I) scheme

3.2 K*(V)SE(1)PKC based on (7,4,3) cyclic Hamming code

3.2.1 Construction

Using K(I) scheme, let us construct K*(V)SE(1)PKC based on (7,4,3) cyclic Hamming code. Let us partition the message vector $\boldsymbol{m}$ into $\boldsymbol{m}_{ENC}$ and $\boldsymbol{m}_{PUB}$

$$\boldsymbol{m}_{ENC} = (\boldsymbol{m}_1, \boldsymbol{m}_2, \cdots, \boldsymbol{m}_L), \tag{28}$$

where $\boldsymbol{m}_i = (m_{i1}, m_{i2}, m_{i3}, m_{i4})$, and

$$\boldsymbol{m}_{PUB} = (m_{4L+1}, m_{4L+2}, \cdots, m_{4L+H}) \tag{29}$$

respectively.

The component $\boldsymbol{m}_i$ of $\boldsymbol{m}_{ENC}$ is encoded to (7,4,3) cyclic Hamming code. The $\boldsymbol{m}_{PUB}$ is publicized.

Let the error vector $\boldsymbol{E}_i$ be,

$$\boldsymbol{E}_i = (E_{i1}, E_{i2}, \cdots, E_{i7}). \tag{30}$$

From $\boldsymbol{E}_i$ we obtain the error vector $\boldsymbol{e}_i$ in a similar manner as we have obtained $\boldsymbol{e}$ from Eq.(6).

Let the i-th component of $\boldsymbol{m}_{ENC}$, $\boldsymbol{m}_i$, be encoded to the code word of (7,4,3) cyclic Hamming code, a member of the perfect codes, as

$$\begin{aligned} &\{m_i(x) + e_i(x)\}x^3 \\ &= d_{i1} + d_{i2}x + d_{i3}x^2 \mod \left(1 + x + x^3\right) \\ &\qquad\qquad ; i = 1, \cdots, L. \end{aligned} \tag{31}$$

The code word $\boldsymbol{w}_i$ is given by

$$\begin{aligned} \boldsymbol{w}_i &= (d_{i1}, d_{i2}, d_{i3}, m_{i1} + e_{i1}, \cdots, m_{i4} + e_{i4}) \\ &\qquad ;\ i = 1, \cdots, L. \end{aligned} \tag{32}$$

The $\boldsymbol{w}_i$ is added with $\boldsymbol{E}_i$,

$$\begin{aligned} \boldsymbol{w}_i + \boldsymbol{E}_i &= \boldsymbol{v}_i \\ &= (v_{i1}, v_{i2}, \cdots, v_{i7}). \end{aligned} \tag{33}$$

The word $\boldsymbol{v}_i$ is then transformed into $\boldsymbol{u}_i$,

$$\begin{aligned} \boldsymbol{v}_i A_{IV} &= \boldsymbol{u}_i \\ &= (u_{i1}, u_{i2}, \cdots, u_{i7}), \end{aligned} \tag{34}$$

where A_{IV} is a 7×7 nonsingular matrix.

Letting A_V be an $H \times 7L$ matrix over $\mathbb{F}_2$, the message $\boldsymbol{m}_P$ is transformed as

$$(m_{4L+1}, \cdots, m_{4L+H})A_V = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \cdots, \boldsymbol{\lambda}_L), \tag{35}$$

where $\boldsymbol{\lambda}_i$ is

$$\boldsymbol{\lambda}_i = (\lambda_{i1}, \lambda_{i2}, \cdots, \lambda_{i7}). \tag{36}$$

Let $\boldsymbol{u}_i$ be defined as

$$\boldsymbol{y}_i = \boldsymbol{u}_i + \boldsymbol{\lambda}_i \ (i = 1, \cdots, L). \tag{37}$$

Public Key:	$\{m_{4L+1}, \cdots, m_{4L+H}\}$, $\{\boldsymbol{y}_i\}$
Secret Key:	A_I, A_{II}, A_{IV}, A_V, $\{\boldsymbol{u}_i\}$, $\{\boldsymbol{\lambda}_i\}$

3.2.2 Encryption and Decryption

The ciphertext $\boldsymbol{c}$ is given by

$$\boldsymbol{c} = (\tilde{\boldsymbol{m}}_P, \tilde{\boldsymbol{y}}_1, \tilde{\boldsymbol{y}}_2, \cdots, \tilde{\boldsymbol{y}}_L). \tag{38}$$

Because the component of $\tilde{\boldsymbol{y}}_i$ is a linear combination of the message variables $\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_k$ added with error vector $\tilde{\boldsymbol{e}}_i$, the encryption can be performed fast.

The decryption can be performed in an exactly similar manner as in Ref.[9]. The decryption can be performed by (1) Linear transformations by A_I^{-1}, A_{II}^{-1}, A_{IV}^{-1}, and A_V^{-1}, (2) Single error correction for (7,4,3) cyclic Hamming code. We see that the decryption is also simple and can be performed fast.

3. 2. 3 Security Considerations

From the given ciphertext, $\tilde{m}_{4L+1}, \cdots, \tilde{m}_{4L+H}$ are given as they are. However it should be noted that the total number of equations in $m_{4L+1}, \cdots, m_{4L+H}$, N_E, is significantly smaller than the total number of the variables, $N_V = n$. Namely, $N_V \gg N_E$. Thus the most powerful attack on K*(V)SE(1)PKC would be the following attack:

Attack Ⅱ: Given the ciphertext, Attack Ⅱ estimates an error symbol from the given $\tilde{\boldsymbol{y}}_i$ $(i = 1, \cdots, L)$. □

Let us assume that H and L are given by $H = 80$ and $L = 16$ respectively. Let $P(C_{\text{EST}})$ be the probability that 4 components of $\boldsymbol{w}_i$ are estimated correctly when $\tilde{\boldsymbol{y}}_i$ is given. The probability $P(C_{\text{EST}})$ is evidently given by

$$P(C_{\text{EST}}) \leqq \left(\frac{1}{2}\right)^4. \tag{39}$$

The probability that the correct estimation can be performed for all of the $\boldsymbol{y}_i$'s is given by

$$\left[P(C_{\text{EST}})\right]^L \leqq \left(\frac{1}{16}\right)^{16} = 5.42\times10^{-20}, \tag{40}$$

sufficiently small value. We thus conclude that K*(V)SE(1)PKC is secure against the Attack Ⅱ.

Attack Ⅲ: Given the ciphertext, Attack Ⅲ discloses the message $\tilde{\boldsymbol{m}}_i$ using the decoding table of a very small size. □

The $\boldsymbol{w}_i$ takes on only 2^4 values. However $\boldsymbol{\lambda}_i$ is added on $\boldsymbol{w}_i$, $\boldsymbol{u}_i$ takes on one of the 2^7 values equally likely. Consequently K*(V)SE(1)PKC is secure against the Attack Ⅲ.

3. 3 Parameters

Let us assume that $H = 80$ and $L = 16$, then N_E, N_V, and S_{PK} are given as

$$N_E = H + 7L = 192, \tag{41}$$

$$N_V = n = 4L + H = 146, \tag{42}$$

and

$$S_{PK} = N_E \cdot N_V = 28.0 \text{ Kbit}, \tag{43}$$

respectively.

We see that the size of public key is smaller than 524 Kbit of the McEliece PKC by a factor of 18.

Let us append an additional message sequence $M_A = (M_{n+1}, M_{n+2}, \cdots, M_{n+3L})$. It should be noted that when the message variables are mutually independent and equally likely, any error symbol e_{ij} $(j = 1, \cdots, 7)$ can be substituted by a set of additional meesage $\boldsymbol{M}_i^A = (M_{i1}, M_{i2}, M_{i3})$ without deteriorating the security of K*(V)SE(1)PKC, yielding the improvement of the coding rate. Letting $\boldsymbol{M}_i^A = (M_{i1}, M_{i2}, M_{i3})$, in the substitution, $\boldsymbol{M}_i^A$ is read as the natural binary number. For example, when $\boldsymbol{M}_i^A = (011)$, $\boldsymbol{M}_i^A$ is read as $\left|\boldsymbol{M}_i^A\right| = 3$. With this transformation $\boldsymbol{M}_i^A$ is substituted by an error $x^{\left|\boldsymbol{M}_i^A\right|-1}$ for $1 \leqq \left|\boldsymbol{M}_i^A\right| \leqq 7$. For $\left|\boldsymbol{M}_i^A\right| = 0$, e_i takes on the value 0. The coding rate ρ is given by

$$\rho = \frac{N_V}{N_E} = 1.0, \tag{44}$$

It should be noted that with the substitution coding rate of exactly 1.0 is achieved.

3. 4 K*(V)SE(1)PKC based on (3,1,3) code

In an exactly similar manner in the preceding subsection, a simpler scheme can be constructed based on (3,1,3) cyclic Hamming code, the smallest error correcting code but a perfect code over $\mathbb{F}_2$. Let m_i, the i-th component of $\boldsymbol{m}_E$, be encoded to the code word of (3,1,3) cyclic Hamming code as

$$(m_i + e_i)x^2 = d_{i1} + d_{i2}x \mod \left(1 + x + x^2\right). \tag{45}$$

The word $\boldsymbol{v}_i$ is given by

$$\boldsymbol{v}_i = \boldsymbol{w}_i + \boldsymbol{E}_i. \tag{46}$$

Letting $H = 60$ and $L = 64$, the probability $P(C_{\text{EST}})$ and $\left[P(C_{\text{EST}})\right]^L$ are given by

$$P(C_{\text{EST}}) = \frac{1}{2} \tag{47}$$

and

$$\left[P(C_{\text{EST}})\right]^L = \left(\frac{1}{2}\right)^{64} = 5.42\times10^{-20} \tag{48}$$

respectively.

The N_E, N_V, S_{PK} and ρ are given by

$$N_E = H + 3L = 252, \tag{49}$$

$$N_V = n = H + L = 124, \tag{50}$$

$$S_{PK} = N_E \cdot N_V = 31.2 \text{ Kbit}, \tag{51}$$

and

$$\rho = 1.0 \tag{52}$$

by the substitution.

4. Conclusion

We have presented a new class of PKC, referred to as K(V)SE(1)PKC. We have shown that the K(V)SE(1)PKC can be made sufficiently secure against the attack based on linear transformations. We have also presented K*(V)SE(1)PKC based on the members of the class of perfect codes, using K(I) scheme. The K*(V)SE(1)PKC has the following remarkable features:

- Coding rate of exactly 1.0.
- Small size of public key compared with the conventional SE(1)PKC.

The author is thankful to the support of SCOPE.

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] N. Koblitz, “Algebraic Aspect of Cryptography”, Springer Verlag, Berlin Heidelberg, (1998).

[4] 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).

[5] 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).

[6] M.Kasahara, “New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials and Random Coding - Generalization of K(III)RSE(g)PKC -”, Technical Report of IEICE, ISEC 2007-118, pp.41-47, (2007-12).

[7] M.Kasahara, “Construction of New class of Linear Multivariate Public Key Cryptosystem - Along With a Note on the Number 9999990 and its Application”, Technical Report of IEICE, ISEC 2009-44 (2009-09).

[8] M.Kasahara, “Linear Multivariate Cryptosystem Constructed on the Basis of Probabilistic Structure”, 2009 JSIAM Annual Meeting, Osaka, (2009-09).

[9] M. Kasahara, “New Classes of Public Key Cryptosystems Constructed Based on Error-Correcting Codes and Probabilistic Structure”, Cryptology ePrint Archive, Report 2010/139 (2010-03).

[10] M. Kasahara, “A Construction of New Class of Linear Multivariate Public Key Cryptosystem Constructed Based on Error Correcting Codes”, Technical Report of IEICE , ISEC 2009-135 (2010-03).

[11] R.McEliece, “A Public-Key Cryptosystem Based on Algebraic Coding Theory”, DSN Progress Report, 42-44, (1978).

[12] E. J. MacWiliams and N. J. A. Sloane: “The Theory of Error-Correcting Codes”, North-Holland, (1997).