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 previously proposed by the present author, as well as K(III) scheme.

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 previously proposed by the present author, as well as K(III) scheme.

The vector \( \tilde{v} = (\tilde{v}_1, \tilde{v}_2, \ldots, \tilde{v}_n) \).

(1)

The vector \( v = (v_1, v_2, \ldots, v_n) \) will be represented by the polynomial as

\[
v(x) = v_1 + v_2 x + \cdots + v_n x^{n-1}.
\]

(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 \( M \) over \( \mathbb{F}_{2^m} \) be represented by

\[
M = (M_1, M_2, \ldots, M_k).
\]

(3)

Throughout this paper we assume that the messages \( M_1, M_2, \ldots, M_k \) are mutually independent and equally likely. Let \( M \) be transformed as

\[
(M_1, M_2, \ldots, M_k)A_I = (m_1, m_2, \ldots, m_k),
\]

(4)

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

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

\[
E = (\alpha_1 E_1, \alpha_2 E_2, \ldots, \alpha_n E_n),
\]

(5)

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

Let us transform \( E \) into \( e \),

\[
(\alpha_1 E_1, \alpha_2 E_2, \ldots, \alpha_n E_n)A_H = e = (e_1, e_2, \ldots, e_k),
\]

(6)

where \( A_H \) is an \( n \times k \) matrix over \( \mathbb{F}_{2^m} \).

Let the message vector \( m_E \) added with error variables \( e_1, e_2, \ldots, e_k \) be defined by

\[
m_E = (m_1 + e_1, m_2 + e_2, \ldots, m_k + e_k).
\]

(7)
We then encode \( \mathbf{m}_E \) to a code word of an \( (n, k, d) \) code over \( \mathbb{F}_{2^m} \) as

\[
m_E(x) x^g \equiv r(x) \mod G(x),
\]

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 \( \mathbf{w} \) can be represented by

\[
\mathbf{w} = (r_1, r_2, \cdots, r_g, m_1 + e_1, \cdots, m_k + e_k).
\]

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

\[
\mathbf{v} = \mathbf{w} + \mathbf{E} \equiv (r_1 + \alpha_1 E_1, r_2 + \alpha_2 E_2, \cdots, r_g + \alpha_g E_g, m_1 + e_1 + \alpha_{g+1} E_{g+1}, \cdots, m_k + e_k + \alpha_n E_n).
\]

We see that any component of \( \mathbf{v} \) 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 \( \mathbf{E} = (\alpha_1 E_1, \alpha_2 E_2, \cdots, \alpha_n E_n) \) is useful for hiding the structure of the code \( \mathbf{w} \). Besides the \( \mathbf{w} \) itself is further transformed to \( \mathbf{u}_E \) using non-singular random matrix \( A_{III} \) over \( \mathbb{F}_{2^m} \), as we see below. □

Let us define \( K(III) \) scheme:

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

---

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

\[ K^*(III) \text{ scheme: Let us first define a predetermined error vector } \mathbf{e} = (e_1, e_2, \cdots, e_n) \text{ whose Hamming weight } w(\mathbf{e}) = t. \]

Let the hashed vector of \( \mathbf{e} \) be \( h(\mathbf{e}) = (e'_1, e'_2, \cdots, e'_k) \). The vectors \( \mathbf{m}_E, \mathbf{w}, \mathbf{v} \) are given in an exactly similar manner as those given from Eqs.(7), (9) and (10). □

The vector \( \mathbf{v} \) is further transformed into \( \mathbf{u} \),

\[
\mathbf{v} A_{III} = \mathbf{u} = (u_1, u_2, \cdots, u_n).
\]

We have the following set of keys:

\[
\begin{array}{|c|c|}
\hline
\text{Public key:} & \{u_i\} \\hline
\text{Secret key:} & \{\alpha_i\}, \{e_i\} \\hline
\end{array}
\]

\[ 2.2 \text{ Parameters} \]

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

\[
N_E = n + k + g \quad (12)
\]

and

\[
N_V = k + n = 2k + g \quad (13)
\]

respectively.

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

\[
S_{pk} = N_E \cdot N_V \cdot m = (k + g)(2k + g)m. \quad (14)
\]

The coding rate, \( \rho \), is given by

\[
\rho = \frac{\text{number of information symbols}}{\text{length of ciphertext}} = \frac{k}{n}. \quad (15)
\]

\[ 2.3 \text{ Encryption} \]

The encryption can be performed by the following steps:

Step 1: Letting the Hamming weight of \( \bar{E} \) be denoted by \( w_H(\bar{E}) \), the sending end chooses nonzero \( \bar{E}_i \)’s under the condition that

\[
w_H(\bar{E}) = t \quad (16)
\]

in a random manner.

Step 2: The ciphertext \( c \) is given by

\[
c = (\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_n). \quad (17)
\]

\[ \Box \]

The component \( \bar{u}_i \) is given by

\[
\bar{u}_i = f_i^{(1)} (\bar{M}_1, \bar{M}_2, \cdots, \bar{M}_k, \bar{E}_1, \bar{E}_2, \cdots, \bar{E}_n), \quad (18)
\]

where \( f_i^{(1)}(\ast) \) implies a linear equation.
2.4 Decryption

The decryption can be performed by the following steps:

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

$$
(\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_n)A_{HI}^{-1} = \tilde{v} = (\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_n).
$$

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

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

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

$$
\tilde{M} = (\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_k).
$$

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 $A_I$, $A_H$, and $A_{HI}$ would be effective to hide the code structure. Besides we add the following error vector $E$ on $w$:

$$
E = (\alpha_1E_1, \alpha_2E_2, \cdots, \alpha_nE_n),
$$

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

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

In the examples given in this paper, the ambiguity of $E$ 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 $E$, $h(E)$, can be given by

$$
h(E) = nC_t \log_2 (2^m - 1) \text{ (bit)},
$$

for $m \geq 2$.

Remark 3: The error vector $E$ is added on $w$ whose component is given by a linear combination of $E_1, E_2, \cdots, E_n$. We thus conclude that the error vector $E$ having a large ambiguity is able to hide the structure of the code used. Furthermore, $w + E$ is transformed into $u$ using $A_H$ 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 $E$.

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 $E$.

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

$$
P_{E(0)} = 2^{-m}
$$

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

$$
P_{c(I)} = 2^{-mk}.
$$

In the examples given in Table 1, the probabilities $P_{c(I)}$‘s are made to be sufficiently small.

The probability that the Case II occurs, $P_{c(II)}$, is given by

$$
P_{c(II)} = \frac{1}{nC_t} (2^m - 1)^{-t}.
$$

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

2.6 Example

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

<p>| Table 1 Examples of $K(V)SE(1)PKC$ over $\mathbb{F}_{2^m}$ |
|--------|--------|--------|--------|--------|--------|</p>
<table>
<thead>
<tr>
<th>$m$</th>
<th>Code</th>
<th>$n, N_E$</th>
<th>$k$</th>
<th>$n + k, N_V$</th>
<th>$g, n - k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example I 1</td>
<td>KS[12]</td>
<td>197</td>
<td>101</td>
<td>293</td>
<td>96</td>
</tr>
<tr>
<td>Example II 1</td>
<td>BCH[12]</td>
<td>255</td>
<td>147</td>
<td>402</td>
<td>96</td>
</tr>
<tr>
<td>Example III 8</td>
<td>S-RS$^+$</td>
<td>128</td>
<td>112</td>
<td>240</td>
<td>12</td>
</tr>
<tr>
<td>Example IV 8</td>
<td>S-RS$^+$</td>
<td>64</td>
<td>48</td>
<td>112</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$t$</th>
<th>$P_{c(I)}$</th>
<th>$P_{c(II)}$</th>
<th>$S_{pk}$ (Kbit)</th>
<th>$\rho$</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>3.94 x 10^{-31}</td>
<td>2.57 x 10^{-18}</td>
<td>58</td>
<td>0.512</td>
</tr>
<tr>
<td>14</td>
<td>5.60 x 10^{-45}</td>
<td>2.55 x 10^{-23}</td>
<td>197</td>
<td>0.58</td>
</tr>
<tr>
<td>6</td>
<td>1.89 x 10^{-27}</td>
<td>6.54 x 10^{-25}</td>
<td>246</td>
<td>0.875</td>
</tr>
<tr>
<td>8</td>
<td>2.53 x 10^{-116}</td>
<td>1.23 x 10^{-29}</td>
<td>57</td>
<td>0.75</td>
</tr>
</tbody>
</table>

$^+$ 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(IV)SE(1)PKC. The principle of K(I) scheme is given in Fig.1. In K(I) scheme, we assume that the conditional entropy \( H(M|m_p) \) satisfies the following relation holds:

\[
H(M|m_p) \geq 80 \text{ bit.} \tag{27}
\]

From \( E_i \) we obtain the error vector \( e_i \) in a similar manner as we have obtained \( e \) from Eq.(6).

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

\[
\{m_i(x) + e_i(x)\}x^3 = d_{i1} + d_{i2}x + d_{i3}x^2 \mod (1 + x + x^3) \tag{31}
\]

\[; i = 1, \cdots, L.\]

The code word \( w_i \) is given by

\[
w_i = (d_{i1}, d_{i2}, d_{i3}, m_i + e_i, \cdots, m_4 + e_4) \tag{32}
\]

\[; i = 1, \cdots, L.\]

The \( w_i \) is added with \( E_i \),

\[
w_i + E_i = v_i = (v_{i1}, v_{i2}, \cdots, v_{i7}). \tag{33}\]

The word \( v_i \) is then transformed into \( u_i \),

\[
v_i A_V = u_i = (u_{i1}, u_{i2}, \cdots, u_{i7}), \tag{34}\]

where \( A_V \) is a 7 \times 7 nonsingular matrix.

Letting \( A_V \) be an \( H \times 7L \) matrix over \( \mathbb{F}_2 \), the message \( m_p \) is transformed as

\[
(m_{4L+1}, \cdots, m_{4L+H}) A_V = (\lambda_1, \lambda_2, \cdots, \lambda_L), \tag{35}\]

where \( \lambda_i \) is

\[
\lambda_i = (\lambda_{i1}, \lambda_{i2}, \cdots, \lambda_{i7}). \tag{36}\]

Let \( u_i \) be defined as

\[
y_i = u_i + \lambda_i (i = 1, \cdots, L). \tag{37}\]

\[
\text{Public Key: } \{m_{4L+1}, \cdots, m_{4L+H}\}, \{y_i\}
\]

\[
\text{Secret Key: } A_V, A_{IV}, A_{IV}, \{u_i\}, \{\lambda_i\}.
\]

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 \( m \) into \( m_{ENC} \) and \( m_{PUB} \)

\[
m_{ENC} = (m_1, m_2, \cdots, m_L), \tag{28}\]

where \( m_i = (m_{i1}, m_{i2}, m_{i3}, m_{i4}) \), and

\[
m_{PUB} = (m_{4L+1}, m_{4L+2}, \cdots, m_{4L+H}) \tag{29}\]

respectively.

The component \( m_i \) of \( m_{ENC} \) is encoded to (7,4,3) cyclic Hamming code. The \( m_{PUB} \) is publicized.

Let the error vector \( E_i \) be,

\[
E_i = (E_{i1}, E_{i2}, \cdots, E_{i7}). \tag{30}\]

The ciphertext \( c \) is given by

\[
c = (\tilde{m}_p, \tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_L). \tag{38}\]

Because the component of \( \tilde{y}_i \) is a linear combination of the message variables \( \tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_L \) added with error vector \( \tilde{e}_i \), 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 \( A_V^{-1}, A_H^{-1}, A_{IV}^{-1}, \) and \( A_{IV}^{-1} \).

(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, \(\tilde{m}_{4L+1}, \ldots, \tilde{m}_{4L+H}\) are given as they are. However it should be noted that the total number of equations in \(m_{4L+1}, \ldots, m_{4L+H}, N_E\), 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 \(K^\ast(V)SE(1)PKC\) would be the following attack:

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

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 \(w_i\) are estimated correctly when \(\tilde{y}_i\) is given. The probability \(P(C_{\text{EST}})\) is evidently given by

\[
P(C_{\text{EST}}) \leq \left( \frac{1}{2} \right)^4.
\]

The probability that the correct estimation can be performed for all of the \(y_i\)'s is given by

\[
[P(C_{\text{EST}})]^L \leq \left( \frac{1}{16} \right)^{16} = 5.42 \times 10^{-20},
\]

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

Attack III: Given the ciphertext, Attack IIIdiscloses the message \(\tilde{m}_i\), using the decoding table of a very small size.

The \(w_i\) takes on only \(2^4\) values. However \(\lambda_i\) is added on \(w_i\), \(u_i\) takes on one of the \(2^2\) values equally likely. Consequently \(K^\ast(V)SE(1)PKC\) is secure against the Attack III.

3.3 Parameters

Let us assume that \(H = 80\) and \(L = 16\), then \(N_E, N_V, S_{PK}\) 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 \(M_A = (M_{n+1}, M_{n+2}, \ldots, M_{n+3L})\). 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 message \(M_A^j = (M_{1j}, M_{2j}, M_{3j})\) without deteriorating the security of \(K^\ast(V)SE(1)PKC\), yielding the improvement of the coding rate. Letting \(M_A^j = (M_{1j}, M_{2j}, M_{3j})\), in the substitution, \(M_A^j\) is read as the natural binary number. For example, when \(M_A^j = (011)\), \(M_A^j\) is read as \(|M_A^j| = 3\). With this transformation \(M_A^j\) is substituted by an error \(x|M_A^j|^{-1}\) for \(1 \leq |M_A^j| \leq 7\). For \(|M_A^j| = 0, e_i\) takes on the value 0. The coding rate \(\rho\) 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\(^{\ast}(V)SE(1)PKC\) 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 \(F_2\). Let \(m_i\), the \(i\)-th component of \(m_E\), be encoded to the code word of (3,1,3) cyclic Hamming code as \(m_i + e_i)x^2 = d_{i1} + d_{i2}x \mod (1 + x + x^2)\).

The word \(v_i\) is given by

\[
v_i = w_i + E_i. \tag{46}
\]

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

\[
P(C_{\text{EST}}) = \frac{1}{2}, \tag{47}
\]

and

\[
[P(C_{\text{EST}})]^L = \left( \frac{1}{2} \right)^{64} = 5.42 \times 10^{-20} \tag{48}
\]

respectively.

The \(N_E, N_V, S_{PK}\) and \(\rho\) 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 \(K^\ast(V)SE(1)PKC\) based on the members of the class of perfect codes, using K(I) scheme. The \(K^\ast(V)SE(1)PKC\) 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


