A New Class of Public Key Cryptosystems Constructed Based on Perfect Error-Correcting Codes Realizing Coding Rate of Exactly 1.0

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 propose a new method for constructing the public-key cryptosystems based on a class of perfect error-correcting codes. The constructed PKC is referred to as K(Ⅳ)SE(1)PKC. In K(Ⅳ)SE(1)PKC, members of the class of perfect error correcting codes such as (7,4,3) cyclic Hamming code and (3,1,3) code $\{(000),(111)\}$ is used, yielding a simple process of encryption and decryption. The K(Ⅳ)SE(1)PKC has a remarkable feature that the coding rate can take on exactly 1.0 due to the use of perfect codes. Besides the size of the public key for K(I V)SE(1)PKC can be made smaller than that of the McEliece PKC.

Key words Public Key Cryptosystem (PKC), Error-Correcting Code, Multivariate PKC, Linear PKC, McEliece PKC

1. Introduction

Most of the multivariate PKC are constructed by the simultaneous equations of degree larger than or equal to 2 [1]∼[6]. Recently the present author proposed a several classes of multivariate PKC that is constructed by many sets of linear equations[7]∼[10], in a sharp contrast with the conventional multivariate PKC where a single set of simultaneous equations of degree more than or equal to 2 are used.

In this paper we present another new class of multivariate PKC that is constructed by many sets of linear equations. In the followings, we shall refer to the proposed linear multivariate PKC constructed on the basis of perfect error correcting codes as K(Ⅳ)SE(1)PKC. Throughout this paper (n,k,d) code implies the code of the code-length n, the number of the information symbols k and the minimum distance d.

In K(Ⅳ)SE(1)PKC, a small size but a perfect error correcting code such as (7,4,3) cyclic Hamming code and (3,1,3) code, $\{(000),(111)\}$, is used, yielding a simple process of encryption and decryption. In the followings the code that has one information symbol repeated $2\mu+1$ times will be denoted by $(2\mu+1,1,2\mu+1)$ code.

The K(Ⅳ)SE(1)PKC has a remarkable feature that the coding rate can take on exactly 1.0, due to the use of perfect codes. Besides the size of the public key for K(Ⅳ)SE(1)PKC can be made smaller than that of the McEliece PKC[11].

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

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

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

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

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

2. K(Ⅳ)SE(1)PKC

Let the message vector $\boldsymbol{M}$ over $\mathbb{F}_2$ be represented by

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

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

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

where A_I is an $n \times n$ non-singular matrix over $\mathbb{F}_2$. Let us describe an outline of the principle of K(Ⅳ)SE(1)PKC referring to the schematic diagram of it in Fig. 1.

Step 1: Let the message vector $\boldsymbol{m} = (\boldsymbol{m}_1, \boldsymbol{m}_2, \cdots, \boldsymbol{m}_n)$ be partitioned into $\boldsymbol{m}_E$ and $\boldsymbol{m}_P$. The $\boldsymbol{m}_E$ is given by

$$\boldsymbol{m}_E = (\boldsymbol{m}_1, \boldsymbol{m}_2, \cdots, \boldsymbol{m}_L) \tag{5}$$

where $\boldsymbol{m}_i$ $(1 \leqq i \leqq L)$ represents $\boldsymbol{m}_i = (m_{i1}, m_{i2}, \cdots, m_{ik})$. The $\boldsymbol{m}_P$ is represented by

$$\boldsymbol{m}_P = (m_{kL+1}, m_{kL+2}, \cdots, m_{kL+H}) \tag{6}$$

where $kL + H = n$.

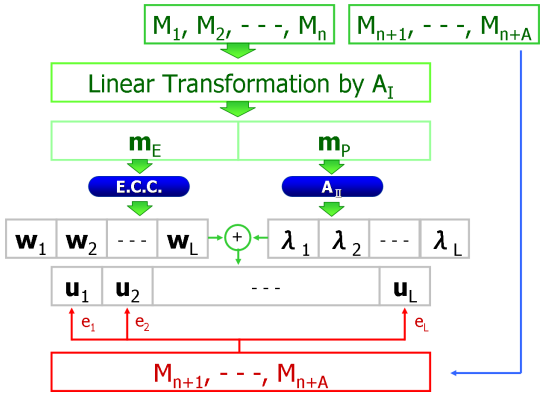

Fig. 1 Principle of K(Ⅳ)SE(1)PKC

Step 2: The message $\boldsymbol{m}_P$ is publicized.

Step 3: The component of $\boldsymbol{m}_E$, $\boldsymbol{m}_i$, is encoded to a code word of an error correcting code as

$$\boldsymbol{w}_i = (d_{i1}, d_{i2}, \cdots, d_{ig}, m_{i1}, m_{i2}, \cdots, m_{ik}) \ (i = 1, 2, \cdots, L), \tag{7}$$

where d_{i1}, d_{i2}, $\cdots$, d_{ig} are the check symbols.

Step 4: The message $\boldsymbol{m}_P$ is transformed as

$$(m_{kL+1}, m_{kL+2}, \cdots, m_{kL+H}) A_{II} = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \cdots, \boldsymbol{\lambda}_L), \tag{8}$$

where $\boldsymbol{\lambda}_i$ is represented by $\boldsymbol{\lambda}_i = (\lambda_{i1}, \lambda_{i2}, \cdots, \lambda_{i,k+g})$ $(i = 1, 2, \cdots, L)$.

Step 5: The word $\boldsymbol{u}_i$ is constructed as

$$\boldsymbol{u}_i = \boldsymbol{w}_i + \boldsymbol{\lambda}_i \ (i = 1, 2, \cdots, L). \tag{9}$$

Step 6: Errors $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_L$ are substituted by the additional messages $M_{n+1}, M_{n+2}, \cdots, M_{n+A}$ when an improvement of the coding rate is required.

Remark 1: As we assume that the message $M_1, M_2, \cdots, M_n$ are mutually independent and equally likely. In other words we assume that the following relation holds on the conditional entropy:

$$\begin{aligned} &H(M_1, M_2, \cdots, M_n | m_{kL+1}, m_{kL+2}, \cdots, m_{kL+H}) \\ &= n - H \text{ (bits)}. \end{aligned} \tag{10}$$

We shall see that in K(Ⅳ)SE(1)PKC, $n - H$ takes on a sufficiently large value. For instance, in Example 1, $n - H$ takes on an extremely large value of 288 bits. □

Let us present the following problem:

Problem 1: Construct a new class of PKC based on K(IV)SE(1)PKC under the following conditions:

(C1) Using of a code of small size perfect codes such as (3,1,3) code, (7,4,3) cyclic Hamming code.

(C2) Coding rate of exactly 1.0.

(C3) Smaller size of the public key compared with that of the McEliece PKC using Goppa codes presented in 1977. □

3. Solution A to Problem 1

3.1 Solution A based on (7,4,3) cyclic Hamming code

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

$$m_i(x)x^3 = d_{i1} + d_{i2}x + d_{i3}x^2 \mod \left(1 + x + x^3\right). \tag{11}$$

The code word $\boldsymbol{w}_i$ can be represented by

$$\boldsymbol{w}_i = (d_{i1}, d_{i2}, d_{i3}, m_{i1}, m_{i2}, m_{i3}, m_{i4}). \tag{12}$$

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

$$(m_{4L+1}, \cdots, m_{4L+H}) A_{III} = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \cdots, \boldsymbol{\lambda}_L) \tag{13}$$

where $\boldsymbol{\lambda}_i$ is

$$\boldsymbol{\lambda}_i = (\lambda_{i1}, \lambda_{i2}, \cdots, \lambda_{i7}), \ (i = 1, 2, \cdots, L). \tag{14}$$

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

$$\boldsymbol{u}_i = \boldsymbol{w}_i + \boldsymbol{\lambda}_i \ (i = 1, 2, \cdots, L), \tag{15}$$

where we let $\boldsymbol{u}_i$ be represented by

$$\boldsymbol{u}_i = (u_{i1}, u_{i2}, \cdots, u_{i7}), \ (i = 1, 2, \cdots, L). \tag{16}$$

Public Key : $\{m_{4L+1}, \cdots, m_{4L+H}\}$, $\{\boldsymbol{u}_i\}$.
Secret Key : A_I, A_{III}, $\{\boldsymbol{\lambda}_i\}$.

3.2 Encryption

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

$$\boldsymbol{C} = (\tilde{\boldsymbol{m}}_P, \tilde{\boldsymbol{u}}_1 + \tilde{\boldsymbol{e}}_1, \tilde{\boldsymbol{u}}_2 + \tilde{\boldsymbol{e}}_2, \cdots, \tilde{\boldsymbol{u}}_L + \tilde{\boldsymbol{e}}_L), \tag{17}$$

where $\tilde{\boldsymbol{e}}_i$ is a single error randomly generated at the sending end. Because the $\boldsymbol{u}_{ij}$ $(i = 1, \cdots, L; j = 1, \cdots, k)$ and m_i $(i = 4L + 1, \cdots, 4L + H)$ are the linear equations of the message variables $M_1, M_2, \cdots, M_n$, the encryption can be performed very fast.

3.3 Decryption

The decryption can be performed as follows:

Step 1: Given the ciphertext:

$$\boldsymbol{C} = (\tilde{\boldsymbol{m}}_P, \tilde{\boldsymbol{u}}_1, \tilde{\boldsymbol{u}}_2, \cdots, \tilde{\boldsymbol{u}}_L), \tag{18}$$

$\tilde{\boldsymbol{\lambda}}_1, \tilde{\boldsymbol{\lambda}}_2, \cdots, \tilde{\boldsymbol{\lambda}}_L$ can be derived from Eq.(13), as $\tilde{\boldsymbol{m}}_P A_{III} = \left(\tilde{\boldsymbol{\lambda}}_1, \tilde{\boldsymbol{\lambda}}_2, \cdots, \tilde{\boldsymbol{\lambda}}_L\right)$.

Step 2: $\tilde{\boldsymbol{w}}_i + \tilde{\boldsymbol{e}}_i$ is given by

$$\tilde{\boldsymbol{u}}_i + \tilde{\boldsymbol{\lambda}}_i = \tilde{\boldsymbol{w}}_i + \tilde{\boldsymbol{e}}_i \ (i = 1, 2, \cdots, L). \tag{19}$$

Step 3: $\tilde{\boldsymbol{w}}_i + \tilde{\boldsymbol{e}}_i$ is the received word of (7,4,3) cyclic Hamming code. The single error $\tilde{\boldsymbol{e}}_i$ can be decoded correctly, yielding $\boldsymbol{m}_E$.

Step 4: The message $\tilde{M}$ is decoded as

$$(\tilde{\boldsymbol{m}}_E, \tilde{\boldsymbol{m}}_P)A_I^{-1} = \big(\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_n\big). \tag{20}$$

The decryption can be performed by

(1) Linear transformations by A_{III} and A_I^{-1},

(2) Single error correction for (7,4,3) cyclic Hamming code.

We see that the decryption is simple and can be performed very fast.

3. 4 Example

In the followings let us present an example where no single error is replaced by information symbols. Let us define the several symbols.

N_E : Total number of equations.
N_V : Total number of variables.
S_{PK} : Size of public key.
ρ : Coding rate.

Example 1: $H = 80$ and $L = 72$.

N_E, N_V, S_{PK} and ρ are given as

$$N_E = H + 7L = 584, \tag{21}$$

$$N_V = n = 4L + H = 368, \tag{22}$$

$$S_{PK} = N_E \cdot N_V = 215 \text{ Kbit} \tag{23}$$

and

$$\rho = \frac{N_V}{N_E} = 0.727, \tag{24}$$

respectively. □

We see that the size of the public key is smaller than 524 Kbit of the McEliece PKC and the coding rate is higher than that of McEliece PKC. It should be noted here that, although any error can be replaced by a message symbol without deterionating the security, no error symbol is replaced by the message symbol, yielding the coding rate ρ of less than 1.0.

3. 5 Security considerations

From the given ciphertext, the components of $(\tilde{m}_{4L+1}, \cdots, \tilde{m}_{4L+H})$ are given under the condition of Eq.(10). Thus the most powerful attack on K(Ⅳ)SE(1)PKC would be the following attack:

Attack I: Given the ciphertext, Attack I estimates 4 error-free symbols from the given $\boldsymbol{c}_i$, $(i = 1, 2, \cdots, L)$. □

As in Example 1, let us assume that H and L are given by

$$H = 80 \tag{25}$$

and

$$L = 72 \tag{26}$$

respectively.

Let $P_\mu\big(C_{\text{EST}}\big)$ be the probability that μ error-free symbols are chosen correctly from the given $\boldsymbol{c}_i$. The probability $P_4\big(C_{\text{EST}}\big)$ is given by

$$P_4\big(C_{\text{EST}}\big) = \frac{{}_6C_4}{{}_7C_4} = \frac{3}{7}. \tag{27}$$

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

$$\big[P_4\big(C_{\text{EST}}\big)\big]^L = \left(\frac{3}{7}\right)^{72} = 3.20 \times 10^{-27}, \tag{28}$$

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

Attack Ⅱ: Given the ciphertext, Attack Ⅱ discloses the message $\tilde{\boldsymbol{m}}_i$ using the decoding table of a very small size of $2^7(4 + 7) = 1408$ bits. □

The $\boldsymbol{w}_i$ takes on only 2^4 values. However, as $\boldsymbol{\lambda}_i$ is added on $\boldsymbol{w}_i$, $\boldsymbol{u}_i = \boldsymbol{w}_i + \boldsymbol{\lambda}_i$ takes on all the 2^7 values equally likely. Consequently K(Ⅳ)SE(1)PKC is secure against the Attack Ⅱ. In other words, the components of $\boldsymbol{\lambda}_i$ are the random linear combination of $M_1, M_2, \cdots, M_n$. Consequently $\boldsymbol{u}_i$ takes on one of the 2^7 values equally likely, although $\boldsymbol{w}_i$ takes on one of the only 2^4 values. We thus see that K(Ⅳ)SE(1)PKC is invulnerable against Attack Ⅱ.

3. 6 Realization of coding rate 1.0

Let us append an additional message sequence $M_A = (M_{n+1}, M_{n+2}, \cdots, M_{n+3L})$ to the original message $\boldsymbol{M}$. It should be noted that when the message variables are mutually independent and equally likely, any error symbol e_i can be substituted by an additional meesage $\boldsymbol{M}_i^A = (M_{i1}, M_{i2}, M_{i3})$, yielding an improvement of the coding rate. Let us define Substitution A in the following:

Substitution A: In Substitution A, $\boldsymbol{M}_i^A$ is read as the natural binary number. For example, when $\boldsymbol{M}_i^A = (011)$, $\boldsymbol{M}_i^A$ is read as $\big|\boldsymbol{M}_i^A\big| = 3$. With this transformation $\boldsymbol{M}_i^A$ is substituted by an error $x^{\big|\boldsymbol{M}_i^A\big|-1}$ for $1 \leqq \big|\boldsymbol{M}_i^A\big| \leqq 7$. For $\big|\boldsymbol{M}_i^A\big| = 0$, e_i takes on the value 0.

With this Substitution A, the coding rate of exactly 1.0 is achieved. However in this case the probabilities $P_\mu\big(C_{\text{EST}}\big)$ and $\big[P_\mu\big(C_{\text{EST}}\big)\big]^L$ take on larger values. Namely,

$$P_4\big(C_{\text{EST}}\big) = \frac{1}{2} \tag{29}$$

and

$$\big[P_4\big(C_{\text{EST}}\big)\big]^L = \left(\frac{1}{2}\right)^{72} = 2.11 \times 10^{-22}, \tag{30}$$

a little larger value than 3.2×10^{-27} given by Eq.(28).

4. Solution B to Problem 1, based on (3,1,3) code

In this and the following sections, we assume that Substitution A is applied, yielding the coding rate of 1.0.

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

$$m_i x^2 = d_{i1} + d_{i2}x \mod \left(1 + x + x^2\right). \tag{31}$$

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

$$\boldsymbol{w}_i = (d_{i1}, d_{i2}, m_i). \tag{32}$$

Letting A_{IV} be an $H \times 3L$ matrix over $\mathbb{F}_2$, the message $\boldsymbol{m}_P$ is transformed as

$$(m_{L+1}, m_{L+2}, \cdots, m_{L+H})A_{IV} = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \cdots, \boldsymbol{\lambda}_L), \tag{33}$$

where $\boldsymbol{\lambda}_i$ is

$$\boldsymbol{\lambda}_i = (\lambda_{i1}, \lambda_{i2}, \lambda_{i3}). \tag{34}$$

Example 2: $H = 80$ and $L = 210$.
The probabilities $P_1\big(C_{\rm EST}\big)$ and $\big[P_1\big(C_{\rm EST}\big)\big]^L$ are given by

$$P_1\big(C_{\rm EST}\big) = \frac{{}_2C_1}{{}_3C_1} \cdot \frac{2}{3} + \frac{1}{4} = \frac{3}{4} \tag{35}$$

and

$$\big[P_1\big(C_{\rm EST}\big)\big]^L = \left(\frac{3}{4}\right)^{210} = 5.79 \times 10^{-27} \tag{36}$$

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

$$N_E = H + 3L = 710, \tag{37}$$

$$N_V = n = H + L = 290, \tag{38}$$

$$S_{PK} = N_E \cdot N_V = 205.9 \text{ K bit}, \tag{39}$$

respectively. □

We see that the size of public key is shortened by a factor of about 2.5 compared with that of McEliece PKC.

5. Solution C to Problem 1, based on (23,12,7) Golay code

One of the most well known perfect codes would be the (23,12,7) Golay code. We shall construct K(Ⅳ)SE(1)PKC based on (23,12,7) Golay code.

Example 3: $H = 80$, $L = 26$. In a similar manner as in Example 1, $P_{12}\big(C_{\rm EST}\big)$ and $\big[P_{12}\big(C_{\rm EST}\big)\big]^L$ are given as

$$P_{12}\big(C_{\rm EST}\big) = \frac{{}_{20}C_{12}}{{}_{23}C_{12}} \cdot \frac{2^{12} - 1}{2^{12}} + \frac{1}{2^{12}} = 0.093 \tag{40}$$

and

$$\big[P_{12}\big(C_{\rm EST}\big)\big]^{26} = 1.93 \times 10^{-27}. \tag{41}$$

The N_E, N_V and S_{pk} are given by

$$N_E = 678, \tag{42}$$

$$N_V = 392 \tag{43}$$

and

$$S_{pk} = 265.8\text{K bit}, \tag{44}$$

respectively. □

6. Solution D to Problem 1, based on (11,5,5) Golay code over $\mathbb{F}_3$

In this section, we shall present (11,5,5) Golay code, the perfect code over $\mathbb{F}_3$.

Example 4: $H = 50$, $L = 48$.
The probabilities $P_5\big(C_{\rm EST}\big)$ and $\big[P_5\big(C_{\rm EST}\big)\big]^L$ are given by

$$P_5\big(C_{\rm EST}\big) = \frac{{}_9C_5}{{}_{11}C_5} \cdot \frac{3^5 - 1}{3^5} + \frac{1}{3^5} = 0.276 \tag{45}$$

and

$$\big[P_5\big(C_{\rm EST}\big)\big]^{48} = (0.276)^{48} = 1.38 \times 10^{-27}, \tag{46}$$

respectively.
The N_E, N_V, and S_{pk} are given by

$$N_E = 578, \tag{47}$$

$$N_V = 290, \tag{48}$$

and

$$S_{pk} = 167.2\text{K bit}, \tag{49}$$

respectively. □

We see that the size of the public key is smaller than that of the McEliece PKC by a factor of about 3.

7. Solution E to Problem 1, based on $(2\mu + 1, 1, 2\mu + 1)$ code

Example 5: $\mu = 3$, $H = 80$, $L = 210$.
In a similar manner as in the previous sections, the $P_1\big(C_{\rm EST}\big)$, $\big[P_1\big(C_{\rm EST}\big)\big]^L$, N_E, N_V, and S_{pk} are given by

$$P_1\big(C_{\rm EST}\big) = \frac{3}{4} \tag{50}$$

$$\big[P_1\big(C_{\rm EST}\big)\big]^{210} = 5.79 \times 10^{-29} \tag{51}$$

$$N_E = 1550 \tag{52}$$

$$N_V = 290 \tag{53}$$

and

$$S_{pk} = 449.5\text{K bit} \tag{54}$$

respectively. □

We see that 6 information symbols can be replaced by errors on each $\boldsymbol{u}_i$ as the relation ${}_7C_0 + {}_7C_1 + {}_7C_2 + {}_7C_3 = 2^6$ holds.

It is easy to see that the size of the public key increases as μ increases under the condition that $\left[P_1\left(C_{\mathrm{EST}}\right)\right]^{\mu}$ is required to take on approximately 10^{-28}.

8. Conclusion

We have presented K(Ⅳ)SE(1)PKC based on the members of the class of perfect codes. It would be remarkable that K(IV)SE(1)PKC is able to achieve the coding rate of exactly 1.0 due to the use of perfect codes.

It would be easy to devise the digital signature scheme for K(Ⅳ)SE(1)PKC as our scheme realizes the coding rate of exactly 1.0.

It seems that the use of $(3, 1, 3)$ code, $\{000, 111\}$, is most desirable due to the following reason:

- The size of public key takes on the smallest value among K(Ⅳ)SE(1)PKC constructed using perfect codes over $\mathbb{F}_2$.
- Decryption can be made very simple as it is the most simple error correcting code.

The author is thankful to the support of SCOPE.

References

[1] 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).

[2] 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).

[3] 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).

[4] N. Koblitz, "Algebraic Aspect of Cryptography", Springer Verlag, Berlin Heidelberg.

[5] 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).

[6] 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).

[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 Meesing, Osaka, (2009-09).

[9] M. Kasahara, "New Classes of Public Key Cryptosystems Constructed Based on Error-Correcting Codes and Probabilistic Structure", Technical Report of IEICE , ISEC 2009-134 (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.

Appendix

1. Solution F to Problem 1, based on (7,4,3) cyclic Hamming code

We present another type of solution, Solution D, to Problem 1. From $\boldsymbol{m}_i = (m_{i1}, m_{i2}, m_{i3}, m_{i4})$, we obtain $\boldsymbol{m}_i^{(1)}$ as

$$\boldsymbol{m}_i^{(1)} = (m_{i4}, m_{i3}, m_{i2}, m_{i1}) \tag{A·1}$$

Let $m_i^{(1)}$ be encoded to the code word of (7,4,3) cyclic Hamming code as

$$m_i^{(1)} x^3 = d_{i1}^{(1)} + d_{i2}^{(1)} x + d_{i3}^{(1)} x^2 \mod \left(1 + x + x^3\right). \tag{A·2}$$

Let $\boldsymbol{d}_i$ and $\boldsymbol{d}_i^{(1)}$ be

$$\boldsymbol{d}_i = (d_{i1}, d_{i2}, d_{i3}) \tag{A·3}$$

and

$$\boldsymbol{d}_i^{(1)} = \left(d_{i1}^{(1)}, d_{i2}^{(1)}, d_{i3}^{(1)}\right) \tag{A·4}$$

respectively.

Let $\boldsymbol{w}_i$ and $\boldsymbol{w}_i^{(1)}$ be given by

$$\boldsymbol{w}_i = (d_{i1}, d_{i2}, d_{i3}, m_{i1}, m_{i2}, m_{i3}, m_{i4}) \tag{A·5}$$

and

$$\boldsymbol{w}_i^{(1)} = \left(d_{i1}^{(1)}, d_{i2}^{(1)}, d_{i3}^{(1)}, m_{i1}, m_{i2}, m_{i3}, m_{i4}\right), \tag{A·6}$$

respectively. It should be noted that $\boldsymbol{w}_i^{(1)}$ is, in general, not a code word. The vector $\boldsymbol{u}_i$ and $\boldsymbol{u}_i^{(1)}$ are given by

$$\boldsymbol{u}_i = \boldsymbol{w}_i + \boldsymbol{\lambda}_i \tag{A·7}$$

and

$$\boldsymbol{u}_i^{(1)} = \boldsymbol{w}_i^{(1)} + \boldsymbol{\lambda}_i^{(1)}. \tag{A·8}$$

respectively, where $\boldsymbol{\lambda}_i$, $\lambda_i^{(1)}$ are given in a similar manner as in Solution A.

Encryption:

When encrypting, one and only one of $\left\{\tilde{\boldsymbol{u}}_i, \tilde{\boldsymbol{u}}_i^{(1)}\right\}$ is randomly chosen and a single error $\tilde{\boldsymbol{e}}_i$ is added on $\tilde{\boldsymbol{m}}_i$. We see that the encryption can be performed very fast.

Decryption:

Decryption can be performed in a similar manner as in subsection 3.3. When $\tilde{\boldsymbol{u}}_i$ with the error $\tilde{\boldsymbol{e}}_i$ on $\tilde{\boldsymbol{m}}_i$ is received, the error correction can be successfully performed, yielding $\tilde{\boldsymbol{m}}_i$. On the other hand when $\tilde{\boldsymbol{u}}_i^{(1)}$ with the error $\tilde{\boldsymbol{e}}_i$ on $\tilde{\boldsymbol{m}}_i$ is received, the followings result:

R1: When the single error $\tilde{\boldsymbol{e}}_i$ can be corrected, $\boldsymbol{m}_i^{(1)}$ is then successfully decoded.

R2: When single error correction cannot be performed, namely when error detection is made, the following transformation is performed

$$\begin{aligned}&(m_1+e_1, m_2+e_2, m_3+e_3, m_4+e_4)\\ &\rightarrow (m_4+e_4, m_3+e_3, m_2+e_2, m_1+e_1),\end{aligned} \tag{A·9}$$

where we assume that the Hamming weight of $\boldsymbol{e} = (e_1, e_2, e_3, e_4)$ is 1.

Remark:

The reason why uncorrectable error is detected in R2 is due to the symmetric structure existing between $\boldsymbol{m}_i$ and $\boldsymbol{m}_i^{(1)}$. Although the details of doing so are ommitted, we can show that under the condition that the same size of ciphertext and coding rate, the probability $\left[P_4\big(C_{\mathrm{EST}}\big)^L\right]$ can be improved compared with that of Eq.(28). Namely $\left[P_4\big(C_{\mathrm{EST}}\big)\right]^L$ is given by

$$\left[P_4\big(C_{\mathrm{EST}}\big)\right]^L = \left(\frac{{}_3C_1}{{}_4C_1}\right)^L \left(\frac{1}{2}\right)^L = \left(\frac{3}{8}\right)^L. \tag{A·10}$$