New classes of public key cryptosystem K(XVI)SE(1)PKC constructed based on Reed-Solomon code over $\mathbb{F}_{2^m}(m \leq 8)$ and K(XVI)SE(2)PKC, based on cyclic code over $\mathbb{F}_2$.

Masao KASAHARA *

Abstract

In this paper, we first present a new class of code based public key cryptosystem(PKC) based on Reed-Solomon code over $\mathbb{F}_{2^m}(m \leq 8)$, referred to as K(XVI)SE(1)PKC. We then present a new class of quadratic multivariate PKC, K(XVI)SE(2)PKC, based on cyclic code over $\mathbb{F}_2$. We show that both K(XVI)SE(1)PKC and K(XVI)SE(2)PKC can be secure against the various linear transformation attacks such as Gröbner bases attack due to a non-linear structure introduced when constructing the ciphertexts. Namely, thanks to a non-linear transformation introduced in the construction of K(XVI)SE(1)PKC and K(XVI)SE(2)PKC the ciphertexts can be made very secure against the various sort of linear transformation attacks such as Gröbner bases attack, although the degree of any multivariate polynomial used for public key is 1. A new scheme presented in this paper that transforms message variables in order to realize a non-linear transformation, K(II)TS, would yield a brand-new technique in the field of both code based PKC and multivariate PKC, for much improving the security. We shall show that the K(XVI)SE(1)PKC can be effectively constructed based on the Reed-Solomon code over $\mathbb{F}_{2^8}$, extensively used in the present day storage systems or the various digital transmission systems.

keyword

Public key cryptosystem, Reed-Solomon code, Cyclic code, Code based PKC, Multivariate PKC, McEliece PKC, Gröbner bases attack.

1 Introduction

Various studies have been made of the Public-Key Cryptosystem(PKC). The security of the PKC's proposed so far, in most cases, depends on the difficulty of discrete logarithm problem or factoring problem. For this reason, it is desired to investigate another classes of PKC's that do not rely on the difficulty of these two problems. The multivariate PKC(MPKC) is one of the very promising candidates of the member of such classes. However, most of the MPKC's are constructed with the simultaneous equations of degree larger than or equal to 2 [1] $\sim$ [8]. Recently the author proposed a several classes of MPKC's that are constructed based on error-correcting codes [9] $\sim$ [14], in a sharp contrast with the conventional MPKC where a single set of simultaneous equations of degree more than or equal to 2 is used. Let us refer to such PKC constructed based on error correcting code as code based PKC(CBPKC). McEliece PKC [15], presented in the early days, can be regarded as a member of the linear MPKC.

In this paper, we present a new class of CBPKC based on Reed-Solomon code over $\mathbb{F}_{2^m}$, referred to as K(XVI)SE(1)PKC. We also present a new class of PKC, K(XVI)SE(2)PKC, based on cyclic code over $\mathbb{F}_2$. We show that both K(XVI)SE(1)PKC and K(XVI)SE(2)PKC can be secure against the various linear

*Research Institute for Science and Engineering, Waseda University. Research and Development Initiative, Chuo University. kasahara@ogu.ac.jp

transformation attacks such as Gröbner bases attack due to a non-linear structure introduced when constructing the ciphertext. It should be noted that the degree of multivariate polunomials used for public keys is set 1, although Gröbner bases attack will find it very hard to attack on K(XVI)SE(1)PKC. A new scheme presented in this paper that transforms message variables in order to realize a non-linear transformation, K(Ⅱ)TS, would yield a brand-new technique in the field of both CBPKC and MPKC, for much improving the security. We shall show that the K(XVI)SE(1)PKC can be effectively constructed based on the Reed-Solomon code over $\mathbb{F}_{2^8}$, extensively used in the present day storage systems or the various digital transmission systems.

In 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

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

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 $\boldsymbol{u} = (\widetilde{u}_1, \widetilde{u}_2, \cdots, \widetilde{u}_n), u(x) = \widetilde{u}_1 + \widetilde{u}_2 x + \cdots + \widetilde{u}_n x^{n-1}$ et al. will be defined in a similar manner.
Throughout this paper we assume that

(i) Bob encrypts the message $\boldsymbol{M}$ and sends the ciphertext $\boldsymbol{C}$ to Alice.

(ii) Alice decrypts the ciphertext $\boldsymbol{C}$ and decodes the message $\boldsymbol{M}$.

2 Construction of K(XVI)SE(1)PKC

2.1 Two classes of messages $\boldsymbol{m}_\alpha$ and $\boldsymbol{m}_\beta$

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

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

We assume that the message symbol, M_i, takes on an element of $\mathbb{F}_{2^m}$ equally likely and mutually independently.

The message $\boldsymbol{M}$ is transformed to

$$\begin{aligned} \boldsymbol{M}A_I &= \boldsymbol{m} \\ &= (m_1, m_2, \cdots, m_n), \end{aligned} \tag{4}$$

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

We see that the transformed message m_i is a linear multivariate polynomial over $\mathbb{F}_{2^m}$ in the variables $M_1, M_2, \cdots, M_n$. When it is desired to clarify the meaning of m_i, it will be denoted

$$m_i = m_i^{(1)}(M_1, M_2, \cdots, M_n). \tag{5}$$

Let us partition $\boldsymbol{m}$ into

$$\boldsymbol{m} = (\boldsymbol{m}_\alpha; \boldsymbol{m}_\beta), \tag{6}$$

where $\boldsymbol{m}_\alpha$ and $\boldsymbol{m}_\beta$ are

$$\begin{aligned} \boldsymbol{m}_\alpha &= (m_1, m_2, \cdots, m_k), \\ \boldsymbol{m}_\beta &= (m_{k+1}, m_{k+2}, \cdots, m_n). \end{aligned} \tag{7}$$

Throughout this paper, for simplicity, we let n be

$$n = 2k. \tag{8}$$

The message $\boldsymbol{m}_\beta$, the set of k linear multivariate polynomials will be publicized for culculating the second ciphertext $\boldsymbol{C}_{II}$. In order to clarify the fact that $\boldsymbol{m}_\beta$ is not only added on the first ciphertext $\boldsymbol{C}_I$ as a secret erasure error but also used as a public key, we shall denote publicized $\boldsymbol{m}_\beta$ be $p \cdot \boldsymbol{m}_\beta$.

Namely the message $\boldsymbol{m}_\beta$ will be used in two ways:

T1 : The $\boldsymbol{m}_\beta$ is added on the code constructed from $\boldsymbol{m}_\alpha$, as a secret erasure error.

T2 : The $\boldsymbol{m}_\beta$ is publicized as public key, $p \cdot \boldsymbol{m}_\beta$, for calculating the second ciphertext C_{II}.

It should be noted that $p \cdot \boldsymbol{m}_\beta = \boldsymbol{m}_\beta$.

2.2 Transformations of messages $\boldsymbol{m}_\alpha$ and $\boldsymbol{m}_\beta$

For easy understanding we first present schematic illustrations of transformations in Figs.1 and 2.

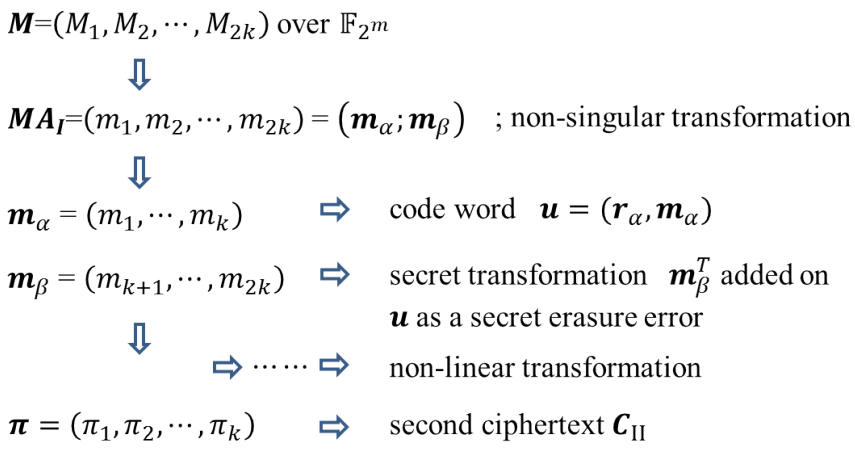

Figure 1. Schematic illustration of transformations of messages m_α and m_β.

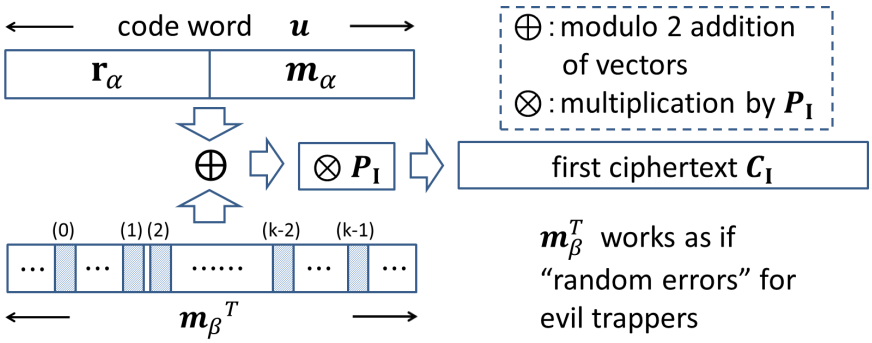

Figure 2. Schematic diagram illustrating construction of $\boldsymbol{C}_I$.

Let $\boldsymbol{m}_\alpha$ be represented by the polynomial :

$$m_\alpha(x) = m_1 + m_2 x + \cdots + m_k x^{k-1}. \tag{9}$$

Message $m_\alpha(x)$ is transformed to

$$m_\alpha(x) x^k \equiv r(x) \bmod G(x), \tag{10}$$

where $G(x)$ over $\mathbb{F}_{2^m}$ is a generator polynomial of degree k of Reed-Solomon code.

The code word $u(x)$ is

$$\begin{aligned} u(x) &= m_\alpha(x)x^k + r(x) \\ &= u_1 + u_2 x + \cdots + u_{2k}x^{2k-1} \equiv 0 \bmod G(x), \end{aligned} \tag{11}$$

where u_i is a linear multivariate polynomial in the variables $M_1, M_2, \cdots, M_{2k}$:

$$u_i = u_i^{(1)}(M_1, M_2, \cdots, M_{2k}) \ ; \ i = 1, 2, \cdots, 2k. \tag{12}$$

In this paper, from a practical point of view, we let $\mathbb{F}_{2^m}$ be a small field such that $m \leq 8$. Accordingly the generator polynomial $G(x)$ cannot be made secret.

The $m_\beta(x)$ is transformed to

$$m_\beta(x) \mapsto m_\beta^T(x) = m_{k+1}x^{(0)} + m_{k+2}x^{(1)} + \cdots + m_{2k}x^{(k-1)}, \tag{13}$$

where randomly chosen secret erasure error locations,$(0), (1), (2), \cdots, (k-1)$, satisfy

$$0 \leq (0) < (1) < (2) < \cdots < (k-1) \leq 2k-1. \tag{14}$$

The transformed message $\boldsymbol{m}_\beta^T$ is added to the code word $\boldsymbol{u}$ as a secret erasure error of Hamming weight k, yielding the following word $\boldsymbol{v}$:

$$\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{m}_\beta^T. \tag{15}$$

The word $\boldsymbol{v}$ is transformed to

$$\boldsymbol{v}P_I = \boldsymbol{w} = (w_1, w_2, \cdots, w_{2k}), \tag{16}$$

where P_I is a $2k \times 2k$ random column permutation matrix over $\mathbb{F}_{2^m}$.

Any column of P_I has one and only one nonzero component of $\mathbb{F}_{2^m}$. We see that the order of $\{P_I\}$ is

$$\#\{P_I\} \cong (2k)!\ 2^{2mk}. \tag{17}$$

The word $\boldsymbol{w}$ is publicized. Given the message $\boldsymbol{M} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_{2k})$, the first ciphertext $\boldsymbol{C}_I$ is calculated from $\boldsymbol{w}$ as $\boldsymbol{C}_I = (\widetilde{w}_1, \widetilde{w}_2, \cdots, \widetilde{w}_{2k})$.

2.3 Non-linear transformation of $\boldsymbol{m}_\beta$

Given the message $\boldsymbol{M} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_{2k})$, the $p \cdot \widetilde{m}_\beta(x)$ is calculated from the public key, $p \cdot m_\beta(x)$. The calculated message $p \cdot \widetilde{m}_\beta(x)$ can be transformed in the various ways.

In this paper we shall perform the following transformation on $p \cdot \widetilde{m}_\beta(x)$:

$$\begin{aligned} \{p \cdot \widetilde{m}_\beta(x)\}^e &\equiv \widetilde{\pi}(x) \bmod F(x) \\ &= \widetilde{\pi}_1 + \widetilde{\pi}_2 x + \cdots + \widetilde{\pi}_k x^{k-1}, \end{aligned} \tag{18}$$

where $F(x)$ is a primitive polynomial of degree k over $\mathbb{F}_{2^m}$.

We let the exponent e be

$$e = 1 + 2 + 2^2 + \cdots + 2^{mk-2}. \tag{19}$$

The vector $\boldsymbol{\pi} = (\pi_1, \pi_2, \cdots, \pi_k)$ will be referred to as coefficients vector.

In the followings, the calculated version of $p \cdot \widetilde{m}_\beta(x)$ at the encryption process, is denoted $E\widetilde{m}_\beta(x)$, while the decoded $\widetilde{m}_\beta(x)$, at the decryption process, will be denoted $D\widetilde{m}_\beta(x)$.

When the decryption process is successfully made, we have

$$E\widetilde{m}_\beta(x) = D\widetilde{m}_\beta(x). \tag{20}$$

2.4 Random code words $\{\widetilde{\boldsymbol{\tau}}_{\boldsymbol{i}}\}$

Let us construct the second set of secret keys for culculating the second ciphertext $\boldsymbol{C}_{II}$.
Let $\widetilde{\boldsymbol{t}}_i$ be a random vector over $\mathbb{F}_{2^m}$:

$$\widetilde{\boldsymbol{t}}_i = (\widetilde{t}_{i1}, \widetilde{t}_{i2}, \cdots, \widetilde{t}_{ik}); i = 1, 2, \cdots, k, \tag{21}$$

where $\widetilde{t}_{ij}$ over $\mathbb{F}_{2^m}$ is randomly chosen, equally likely and mutually independently, under the condition that these $\widetilde{\boldsymbol{t}}_i$'s span the vector space of dimension k.

The $\widetilde{t}_i(x)$ is transformed to

$$\widetilde{t}_i(x)x^k \equiv \widetilde{r}_{t_i}(x) \bmod G(x); i = 1, 2, \cdots, k. \tag{22}$$

The code word $\widetilde{\tau}_i(x)$ is

$$\begin{aligned} \widetilde{\tau}_i(x) = \widetilde{t}_i(x)x^k + \widetilde{r}_{t_i}(x) &\equiv 0 \bmod G(x) \\ &= \widetilde{\tau}_{i1} + \widetilde{\tau}_{i2}x + \cdots + \widetilde{\tau}_{in}x^{n-1} \ ; \ i = 1, 2, \cdots, k. \end{aligned} \tag{23}$$

A linear combination of the code words $\in \{\widetilde{\boldsymbol{\tau}}_i\}$, will be added on the code word $\boldsymbol{u}$ as noise like code words.

It should be noted, here, that $u(x)$ and $\widetilde{\tau}_i(x)$'s are constructed by the same generator polynomial, $G(x)$.
Let $\widetilde{\boldsymbol{\tau}}_i$ be denoted $\widetilde{\boldsymbol{\tau}}_i = (\widetilde{\tau}_{i1}, \widetilde{\tau}_{i2}, \cdots, \widetilde{\tau}_{in})$; $i = 1, 2, \cdots, k$.

The $\widetilde{\boldsymbol{\tau}}_{\boldsymbol{i}}$ is transformed to

$$\widetilde{\boldsymbol{\tau}}_i P_I = \widetilde{\boldsymbol{\varphi}}_i = (\widetilde{\varphi}_{i1}, \widetilde{\varphi}_{i2}, \cdots, \widetilde{\varphi}_{in}). \tag{24}$$

The set of $\{\widetilde{\boldsymbol{\varphi}}_i\}$, denoted $S_{\widetilde{\boldsymbol{\varphi}}}$, is

$$S_{\widetilde{\boldsymbol{\varphi}}} = \left\{ \begin{array}{cccc} (\widetilde{\varphi}_{11}, & \widetilde{\varphi}_{12}, & \cdots, & \widetilde{\varphi}_{1n}) \\ (\widetilde{\varphi}_{21} & \widetilde{\varphi}_{22}, & \cdots, & \widetilde{\varphi}_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ (\widetilde{\varphi}_{k1}, & \widetilde{\varphi}_{k2}, & \cdots, & \widetilde{\varphi}_{kn}) \end{array} \right\}, \tag{25}$$

where n is $2k$.
The $S_{\widetilde{\boldsymbol{\varphi}}}$ is publicized as a set of public keys along with another public key $\boldsymbol{w} = (w_1, w_2, \cdots, w_n)$.
Given the message $\boldsymbol{M} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_n)$, the ciphertext $\boldsymbol{C}_{II}$ is

$$\boldsymbol{C}_{II} = \widetilde{\pi}_1\widetilde{\boldsymbol{\varphi}}_1 + \widetilde{\pi}_2\widetilde{\boldsymbol{\varphi}}_2 + \cdots + \widetilde{\pi}_k\widetilde{\boldsymbol{\varphi}}_k. \tag{26}$$

The ciphertext, $\boldsymbol{C}$, is then

$$\boldsymbol{C} = \boldsymbol{C}_I + \boldsymbol{C}_{II}. \tag{27}$$

Set of keys are :

Public key	:	$\boldsymbol{w}, \{\widetilde{\boldsymbol{\varphi}}_i\}, p \cdot \boldsymbol{m}_\beta, F(x), e$
Secret key	:	$\boldsymbol{u}, \boldsymbol{m}_\alpha, \boldsymbol{m}_\beta^T, \boldsymbol{v}, A_I, P_I$

2.5 Non-linear transformation scheme, K(Ⅱ)TS

Non-linear transformation presented in 2.3 in order to calculate a weighted random linear sum of random code words in 2.4 is a new scheme for strengthening CBPKC. The new scheme is referred to as K(Ⅱ) Transformation Scheme(K(Ⅱ)TS).

K(Ⅱ)TS can be summarized through the following steps :

SI : Original message $\boldsymbol{M} = (M_1, M_2, \cdots, M_n)$ over $\mathbb{F}_{2^m}$ is transformed to $\boldsymbol{M} \cdot A_I = (\boldsymbol{m}_\alpha, \boldsymbol{m}_\beta)$.

SII : Construction of code word: $u(x) = m_\alpha(x)x^k + r(x) \equiv 0 \mod G(x)$.

SIII : Transformation of $\boldsymbol{m}_\beta$ to an erasure error $\boldsymbol{m}_\beta^T$.

SIV : Random generation of $\widetilde{\boldsymbol{t}}_i = (\widetilde{t}_{i1}, \widetilde{t}_{i2}, \cdots, \widetilde{t}_{ik})$; $i = 1, 2, \cdots, k$.

SV : Construction of random code words : $\widetilde{\tau}_i(x) = \widetilde{t}_i(x)x^k + \widetilde{r}_{t_i}(x) \equiv 0 \mod G(x); i = 1, 2, \cdots, k$.

SVI : Transformation of $\boldsymbol{m}_\beta$ to a coefficients vector $\boldsymbol{\pi}$ in a non-linear way, referring to the public key $p \cdot \boldsymbol{m}_\beta$.
One of the non-linear transformations can be performed, for example, by Eq.(18).

SVII : The ciphertext $\boldsymbol{C}$ is $\boldsymbol{C} = \boldsymbol{C}_I + \boldsymbol{C}_{II}$, where $\boldsymbol{C}_I$ is the encrypted version of the message $\boldsymbol{m}_\alpha$ with $\boldsymbol{m}_\beta^T$ and $\boldsymbol{C}_{II}$, the encrypted version of the random code words $\widetilde{\boldsymbol{\tau}}_i$; $i = 1.2. \cdots, k$.

2.6 Decoding of messages $\boldsymbol{m}_\alpha$ and $\boldsymbol{m}_\beta$

From Eqs.(11) and (15), we have

$$\widetilde{v}(x) = \widetilde{m}_\alpha(x)x^k + \widetilde{r}(x) + \widetilde{m}_\beta^T(x) \equiv \text{synd}\{\widetilde{m}_\beta^t(x)\} \mod G(x), \tag{28}$$

where synd $\{\widetilde{m}_\beta^T(x)\}$ is the syndrome due to $\widetilde{m}_\beta^T(x)$ added to the code word $\widetilde{u}(x)$ as an erasure error.

From Eq.(23) the relation:

$$\widetilde{\pi}_i\{\widetilde{t}_i(x)x^k + \widetilde{r}_{t_i}(x)\} \equiv 0 \mod G(x) \ ; \ i = 1, 2, \cdots, k, \tag{29}$$

holds, where $\widetilde{\pi}_i$ is the i-th component of the coefficient vector $\widetilde{\boldsymbol{\pi}}$.

From Eqs.(28) and (29), we have

$$\begin{aligned} \widetilde{v}(x) = \{\widetilde{m}_\alpha(x) + \sum_{i=1}^{k} \widetilde{\pi}_i \widetilde{t}_i(x)\}x^k + \widetilde{r}(x) + \sum_{i=1}^{k} \widetilde{\pi}_i \widetilde{r}_{t_i}(x) + \widetilde{m}_\beta^T(x) \\ \equiv \text{synd}\{\widetilde{m}_\beta^T(x)\} \mod G(x). \end{aligned} \tag{30}$$

Only for convenience's sake for easy understanding of encoding and decoding processes of $\boldsymbol{m}_\alpha$ and $\boldsymbol{m}_\beta$, we let $\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$ added on $u(x)$ at the encryption process be denoted $E\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$ and the $\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$ calculated at the decoding process, $D\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$.

From the synd$\{\widetilde{m}_\beta^T(x)\}$, $\widetilde{m}_\beta(x)$ can be successfully decoded following the erasure and error decoding algorithm [16], as the minimum distance of Reed-Solomon code is k.

It should be noted that, although $\widetilde{m}_\alpha(x) + E\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$ is decoded correctly, the message $\widetilde{m}_\alpha(x)$ cannot be decoded correctly, at this stage, due to the presence of $E\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$.

In order to decode $m_\alpha(x)$ successfully, the decoded $\widetilde{\boldsymbol{m}}_\beta, D\widetilde{\boldsymbol{m}}_\beta$, is transformed to

$$\widetilde{\boldsymbol{\pi}} = (\widetilde{\pi}_1, \widetilde{\pi}_1, \cdots, \widetilde{\pi}_k), \tag{31}$$

yielding $D\sum_{i=1}^k \widetilde{\pi}_i \widetilde{t}_i(x)$.

The message $\boldsymbol{m}_\alpha$ is then decoded as

$$\widetilde{\boldsymbol{m}}_\alpha + E\sum_{i=1}^{k} \widetilde{\pi}_i \widetilde{t}_i(x) - D\sum_{i=1}^{k} \widetilde{\pi}_i \widetilde{t}_i(x) = \widetilde{\boldsymbol{m}}_\alpha. \tag{32}$$

2.7 Encryprion and decryption process

In this section, $\boldsymbol{C}P_I^{-1}$ will be referred to as intermediate ciphertext, $\boldsymbol{I}_M$. The intermediate ciphertext $\boldsymbol{I}_M$ is

$$\boldsymbol{I}_M = \boldsymbol{u} + \boldsymbol{m}_\beta^T + \pi_1\widetilde{\boldsymbol{\tau}}_1 + \pi_2\widetilde{\boldsymbol{\tau}}_2 + \cdots + \pi_k\widetilde{\boldsymbol{\tau}}_k. \tag{33}$$

Encryption can be perfomed according to the following steps :

Step 1 : For message $\boldsymbol{M} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_n)$ over $\mathbb{F}_{2^m}$,referring to the public key $\boldsymbol{w} = (w_1, w_2, \cdots, w_{2k})$, Bob calculates $\boldsymbol{C}_I = (\widetilde{w}_1, \widetilde{w}_2, \cdots, \widetilde{w}_n)$.

Step 2 : Referring to the public key, $p \cdot \boldsymbol{m}_\beta$, Bob calculates $\boldsymbol{\pi} = (\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_k)$ over $\mathbb{F}_{2^m}$ for the given $\widetilde{\boldsymbol{m}}_\beta$.

Step 3 : Referring to the public key $S_{\widetilde{\boldsymbol{\varphi}}} = \{\widetilde{\boldsymbol{\varphi}}_1, \widetilde{\boldsymbol{\varphi}}_2, \cdots, \widetilde{\boldsymbol{\varphi}}_k\}$, Bob calculates $\boldsymbol{C}_{II} = \widetilde{\pi}_1\widetilde{\boldsymbol{\varphi}}_1 + \widetilde{\pi}_2\widetilde{\boldsymbol{\varphi}}_2 + \cdots + \widetilde{\pi}_k\widetilde{\boldsymbol{\varphi}}_k$.

Step 4 : Bob calculates the ciphertext $\boldsymbol{C} = \boldsymbol{C}_I + \boldsymbol{C}_{II}$.

Step 5 : Bob sends $\boldsymbol{C}$ to Alice.

Decryption can be perfomed according to the following steps :

Step 1 : Receiving the ciphertext $\boldsymbol{C}$, Alice calculates the intermediate ciphertext $\boldsymbol{I}_M$: $\boldsymbol{I}_M = \widetilde{\boldsymbol{u}} + \widetilde{\boldsymbol{m}}_\beta^T + \widetilde{\pi}_1\widetilde{\boldsymbol{\tau}}_1 + \widetilde{\pi}_2\widetilde{\boldsymbol{\tau}}_2 + \cdots + \widetilde{\pi}_k\widetilde{\boldsymbol{\tau}}_k$.

Step 2 : Alice decodes $\widetilde{\boldsymbol{m}}_\beta^T$ as an erasure error based on the syndrome : $\boldsymbol{I}_M(x) \equiv \mathrm{synd}\{\widetilde{m}_\beta^T(x)\} \bmod G(x)$, yielding $E\widetilde{\boldsymbol{m}}_\beta$.

Step 3 : From $E\widetilde{\boldsymbol{m}}_\beta^T$, Alice calculates $\boldsymbol{\pi} = (\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_k)$.

Step 4 : Alice calculates $\boldsymbol{I}_M - (\widetilde{\pi}_1\widetilde{\boldsymbol{\tau}}_1 + \widetilde{\pi}_2\widetilde{\boldsymbol{\tau}}_2 + \cdots + \widetilde{\pi}_k\widetilde{\boldsymbol{\tau}}_k) - \widetilde{\boldsymbol{m}}_\beta^\tau = \widetilde{\boldsymbol{u}}$.

Step 5 : From $\widetilde{u}(x) = \widetilde{m}_\alpha(x)x^g + \widetilde{r}_\alpha(x)$, Alice decodes the message $\widetilde{\boldsymbol{m}}_\alpha$.

Step 6 : Alice decodes the original message $\widetilde{\boldsymbol{M}}$ by calculating $(\widetilde{\boldsymbol{m}}_\alpha, \widetilde{\boldsymbol{m}}_\beta)A_I^{-1} = \widetilde{\boldsymbol{M}}$.

2.8 Security consideration

Let us define several symbols :

$P_C[\hat{\boldsymbol{C}}_I]$: Probability that the ciphertext $\boldsymbol{C}_I$ is correctly estimated.

$P_C[\hat{\boldsymbol{C}}_{II}]$: Probability that the ciphertext $\boldsymbol{C}_{II}$ is correctly estimated.

$P_C[\hat{P}_I]$: Probability that the random $2k \times 2k$ column permutation matrix P_I over $\mathbb{F}_{2^m}$ is correctly estimated.

$P_C[\hat{\boldsymbol{\pi}}]$: Probability that the coefficients vector π is correctly estimated.

Attack 1 : Exhaustive attack on $\boldsymbol{C}_I$ or $\boldsymbol{C}_{II}$ when $\boldsymbol{C} = \boldsymbol{C}_I + \boldsymbol{C}_{II}$ is given.
The probability that an exhaustive attack on $\boldsymbol{C}_I$ or C_{II} is successful is

$$P_C[\hat{\boldsymbol{C}}_I] = P[\hat{\boldsymbol{C}}_{II}] = 2^{-2mk}. \tag{34}$$

For $mk \geq 80$, $P_C[\hat{\boldsymbol{C}}_I] = P_C[\hat{\boldsymbol{C}}_{II}]$ is less than 6.84×10^{-49} a sufficiently small value.
We conclude that K(XVI)SE(1)PKC is secure against Attack 1 for $mk \geq 80$.

Attack 2 : Exhaustive attack on P_I.
The probability that an exhaustive attack on a random permutation matrix P_I over $\mathbb{F}_{2^m}$ is, from Eq.(17),

$$P_C[\hat{P}_I] = \{(2k)!\ 2^{2mk}\}^{-1}. \tag{35}$$

For $m = 8, k = 10$, $P_C[\hat{P}_I]$ takes on a small value of less than 2.81×10^{-67}.

We conclude that K(XVI)SE(1)PKC is secure against Attack 2 for appropriately chosen values of m and k.

Attack 3 : Exhaustive attack on $\boldsymbol{\pi}$.
The probability that an exhaustive attack on $\boldsymbol{\pi}$ is successful is

$$P_C[\hat{\boldsymbol{\pi}}] = 2^{-mk}. \tag{36}$$

For $mk \geq 80$, $P_C[\hat{\boldsymbol{\pi}}]$ takes on a small value of less than 8.272×10^{-25}.

We conclude that Attack 3 is the most dangerous attack for K(XVI)SE(1)PKC among the various sorts of exhaustive type attacks including Attacks 1 and 2.

Attack 4 : Linear transformation type attack on $\boldsymbol{C}$.
The message $\boldsymbol{m}_\beta$ is transformed in a non-linear way. For example, when $\boldsymbol{m}_\beta$ is $\widetilde{\boldsymbol{m}}_\beta$, it is transformed to the coefficients vector $\boldsymbol{\pi} = (\pi_1, \pi_2, \cdots, \pi_n)$, through the transformation given by Eqs.(18) and (19):

The ciphertext $\boldsymbol{C}$ can be represented by the set of simultaneous equations of degree $mk-1$ in the variables $M_1, M_2, \cdots, M_{2k}$. The total number of possible terms of degree $mk-1$ in each equation, T_{mk-1}, is

$$\begin{aligned} T_{mk-1} &= {}_{2k}H_{mk-1} \\ &= \left(\begin{array}{c} 2k+mk-2 \\ mk-1 \end{array} \right). \end{aligned} \tag{37}$$

For $m = 8, k = 10$, T_{mk-1} is

$$T_{mk-1} = T_{79} = \left(\begin{array}{c} 98 \\ 79 \end{array} \right) = 8.66 \times 10^{19}, \tag{38}$$

an extremely large number of terms.

In the example given above, Gröbner bases attack will find it extremely hard to attack on the simultaneous equation of high degree of 79.

We see that Gröbner bases attack will find it very hard to attack on the ciphertext of K(XVI)SE(1)PKC.

We conclude that the proposed K(XVI)SE(1)PKC would be suffifiently secure for the various sorts of atacks, including Gröbner bases attack, for appropritately chosen values of m and k.

2.9 Parameters and Examples

The size of public key, S_{pk}, is

$$\begin{aligned} S_{pk} &= |\{\widetilde{\boldsymbol{\varphi}}_i\}| + |\{w_i\}| + |p \cdot \boldsymbol{m}_\beta| + |F(x)| + |e| \cong k|\widetilde{\varphi}_i| + 2k|w_i| + k|m_i| \\ &= 2k^2m + 4k^2m + 2k^2m = 8k^2m \text{ (bit)} = \mathrm{k^2m} \text{ (B)}. \end{aligned} \tag{39}$$

The coding rate, ρ, is

$$\rho = \frac{|M|}{|C|} = 1.00. \tag{40}$$

The size of siphertext, $|C|$, is

$$|C| = 2km \text{ (bit)}. \tag{41}$$

Examples are shown in Tables 1 and 2.

We show three examples of K(XVI)SE(1)PKC in Table 1.

From Table 1, we see that the sizes of public key, S_{PK} take on large sizes. We also ses that the probability $[\hat{P}_I]$ and $P_c[\hat{\boldsymbol{\pi}}]$ take on extremely small values compared with the value $2^{-80} = 8.28 \times 10^{-25}$.

In Table 2, we present three examples of relatively small sizes of public key keeping $P_c[\hat{P}_I]$ and $P_c[\hat{\pi}]$ less than $2^{-80} = 8.28 \times 10^{-25}$,where we let mk be 96, 112 and 128.

Table. 1. Examples ($\rho = 1.0$).

Example	m	k	$P_c[\hat{P}_I]$	$\boldsymbol{P}_c[\hat{\boldsymbol{\pi}}]$	$\boldsymbol{S}_{PK}(KB)$	$\lvert C\rvert$(bit)
I	6	32	$2.00e^{-205}$	$1.59e^{-58}$	6.14	384
II	7	64	$4.91e^{-486}$	$1.38e^{-135}$	28.7	896
III	8	128	$3.61e^{-1124}$	$5.56e^{-369}$	131.1	2048

Table. 2. Examples ($\rho = 1.0$).

Example	m	k	n	$P_c[\hat{P}_I]$	$\boldsymbol{P}_c[\hat{\boldsymbol{\pi}}]$	$\boldsymbol{S}_{PK}(KB)$	$\lvert C\rvert$(bit)
IV	8	12	24	$2.57e^{-82}$	$1.26e^{-29}$	1.15	192
V	8	14	28	$1.22e^{-97}$	$1.93e^{-34}$	1.57	224
VI	8	16	32	$3.28e^{-113}$	$7.52e^{-37}$	2.05	256

3 K(XVI)SE(2)PKC over $\mathbb{F}_2$

3.1 Random quadratic MVPKC over $\mathbb{F}_2$

In the same way as we have defined the original message $\boldsymbol{M}$ over $\mathbb{F}_{2^m}$ by Eq.(3), we let the original message $\boldsymbol{M}$ over $\mathbb{F}_2$ be

$$\boldsymbol{M} = (M_1, M_2, \cdots, \boldsymbol{M}_n). \tag{42}$$

The message $\boldsymbol{M}$ is transformed to $\boldsymbol{m}$ in an exactly same way as we did in Eq.(4).
The transformed message $\boldsymbol{m}$ over $\mathbb{F}_2$ is partitioned to

$$\boldsymbol{m} = (\boldsymbol{m}_1; \boldsymbol{m}_2; , \cdots ; \boldsymbol{m}_\mu). \tag{43}$$

The components of $\boldsymbol{m}$, $\boldsymbol{m}_i$'s are

$$\begin{aligned} \boldsymbol{m}_1 &= (m_1, m_2, \cdots, m_\pi), \\ \boldsymbol{m}_2 &= (m_{\pi+1}, m_{\pi+2}, \cdots, m_{2\pi}), \\ &\vdots \\ \boldsymbol{m}_\mu &= (m_{(\mu-1)\pi+1}, m_{(\mu-1)\pi+2}, \cdots, m_{\mu\pi}), \end{aligned} \tag{44}$$

where $\mu\pi = n$.

Let $\boldsymbol{m}_i$ be transformed to a set of quadratic equations:

$$S_q = \{\boldsymbol{a}_i = (a^{(2)}_{(i-1)\pi+1}, a^{(2)}_{(i-1)\pi+2}, \cdots, a^{(2)}_{i\pi})\} \ ; \ i = 1, 2, \cdots, \mu. \tag{45}$$

where $a^{(2)}_{(i-1)\pi+j}$ is a quadratic equation:

$$a^{(2)}_{(i-1)\pi+j} = a^{(2)}_{(i-1)\pi+j}(m_{(i-1)\pi+1}, m_{(i-1)\pi+2}, \cdots, m_{i\pi}); j = 1, \cdots, \pi. \tag{46}$$

Let the vector $\boldsymbol{a}$ be

$$\boldsymbol{a} = (a^{(2)}_1, a^{(2)}_2, \cdots, a^{(2)}_n). \tag{47}$$

The vector $\boldsymbol{a}$ is transformed to

$$\boldsymbol{a}P_{II} = (\boldsymbol{a}_\alpha; \boldsymbol{a}_\beta), \tag{48}$$

where P_{II} is a random column permutation matrix over $\mathbb{F}_2$.
The component $\boldsymbol{a}_\alpha$ and $\boldsymbol{a}_\beta$ are

$$\begin{aligned}\boldsymbol{a}_\alpha &= (a_1^{(2)}, a_2^{(2)}, \cdots, a_k^{(2)}),\\ \boldsymbol{a}_\beta &= (a_{k+1}^{(2)}, a_{k+2}^{(2)}, \cdots, a_{2k}^{(2)}),\end{aligned} \tag{49}$$

where $2k = n$.

The vector $a_\alpha(x)$ is transformed to

$$a_\alpha(x)x^k \equiv r(x) \bmod G(x), \tag{50}$$

where $G(x)$ is a primitive polynomial of degree k over $\mathbb{F}_2$.

The code word $u(x)$ is

$$\begin{aligned}u(x) &= a_\alpha(x)x^k + r(x)\\ &= u_1 + u_2x + \cdots + u_{2k}x^{2k-1} \equiv 0 \bmod G(x).\end{aligned} \tag{51}$$

The $\{u(x)\}$ is a cyclic code (including shortened one) generated by G(x).

We then construct the word $\boldsymbol{v}$:

$$\begin{aligned}v(x) &= u(x) + a_\beta(x)\\ &= v_1 + v_2x + \cdots + v_{2k}x^{2k-1}.\end{aligned} \tag{52}$$

The word $\boldsymbol{v}$ is then transformed to

$$\begin{aligned}\boldsymbol{v}P_{II} &= \boldsymbol{w}\\ &= (w_1, w_2, \cdots, w_{2k}).\end{aligned} \tag{53}$$

where P_{II} is a $2k \times 2k$ random permutation matrix over $\mathbb{F}_2$.

The transformed word $\boldsymbol{w}$ will be publicized as the public key for constructing the first ciphertext C_I.

Let us compose another set of public key, for the second ciphertext C_{II} in the followings.
Let $\widetilde{\boldsymbol{t}}_i$ be a random vector over $\mathbb{F}_2$:

$$\widetilde{\boldsymbol{t}}_i = (\widetilde{t}_{i1}, \widetilde{t}_{i2}, \cdots, \widetilde{t}_{ik}); i = 1, 2, \cdots, k, \tag{54}$$

where $\widetilde{t}_{ij}$ over $\mathbb{F}_2$ is randomly generated, equally likely and mutually independently.

The $\widetilde{t}_i(x)$ is transformed to

$$\widetilde{t}_i(x)x^k \equiv \widetilde{r}_{t_i}(x) \bmod G(x); i = 1, 2, \cdots, k. \tag{55}$$

The code word $\widetilde{\tau}_i(x)$ is

$$\widetilde{\tau}_i(x) = \widetilde{t}_i(x)x^k + \widetilde{r}_{t_i}(x) \equiv 0 \bmod G(x). \tag{56}$$

The code word $\widetilde{\boldsymbol{\tau}}_i$ is transformed to

$$\widetilde{\boldsymbol{\tau}}_i P_{II} = \widetilde{\boldsymbol{\varphi}}_i = (\widetilde{\varphi}_{i1}, \widetilde{\varphi}_{i2}, \cdots, \widetilde{\varphi}_{in}); i = 1, 2, \cdots, k, \tag{57}$$

where P_{II} is a $2k \times 2k$ random column permutation matrix over $\mathbb{F}_2$.

The set of $\widetilde{\boldsymbol{\varphi}}_i{}'s$, $\{\widetilde{\boldsymbol{\varphi}}_i\}$, denoted $S_{\widetilde{\boldsymbol{\varphi}}}$ will be publicized as public key along with another public key, $\boldsymbol{w} = (w_1, w_2, \cdots, w_n)$.

In order to properly choose the elements of $S_{\widetilde{\boldsymbol{\varphi}}}$, let us transform the message $\widetilde{\boldsymbol{a}}_\beta$ as shown below.

Let the message $\widetilde{\boldsymbol{a}}_\beta$ be transformed to

$$\begin{aligned}\widetilde{\boldsymbol{a}}_\beta &\mapsto \widetilde{\boldsymbol{\pi}}\\ &= (\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_k).\end{aligned} \tag{58}$$

There exist various sort of transformations of Eq.(58). In this section, we use the same transformation given in Section 2.3.

$$\begin{aligned}\{p \cdot \widetilde{m}_\beta(x)\}^e &\equiv \widetilde{\pi}(x) \bmod F(x) \\ &= \widetilde{\pi}_1 + \widetilde{\pi}_2 x + \cdots + \widetilde{\pi}_k x^{k-1},\end{aligned} \tag{59}$$

where $F(x)$ is a primitive polynomial over $\mathbb{F}_2$ of degree k.

The exponent e is

$$e = 1 + 2 + 2^2 + \cdots + 2^{k-2}. \tag{60}$$

The second ciphertext $\boldsymbol{C}_{II}$ is

$$\boldsymbol{C}_{II} = \pi_1 \widetilde{\boldsymbol{\varphi}}_1 + \pi_2 \widetilde{\boldsymbol{\varphi}}_2 + \cdots + \pi_k \widetilde{\boldsymbol{\varphi}}_k. \tag{61}$$

Given the message $\widetilde{\boldsymbol{M}} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_{2k})$, the ciphertexts $\boldsymbol{C}_I$ and $\boldsymbol{C}_{II}$ are:

$$\begin{aligned}\boldsymbol{C}_I &= (\widetilde{w}_1, \widetilde{w}_2, \cdots, \widetilde{w}_{2k}), \\ \boldsymbol{C}_{II} &= \widetilde{\pi}_1 \widetilde{\varphi}_1 + \widetilde{\pi}_2 \widetilde{\varphi}_2 + \cdots + \widetilde{\pi}_k \widetilde{\varphi}_k,\end{aligned} \tag{62}$$

The ciphertext, $\boldsymbol{C}$, is then

$$\boldsymbol{C} = \widetilde{\boldsymbol{C}}_I + \widetilde{\boldsymbol{C}}_{II}. \tag{63}$$

3.2 Examples and Security considerations

The presented MPKC, K(XVI)SE(2)PKC, would be very secure against the various attacks including Gröbner bases attack thanks to the non-linear transformation used in K(XVI)SE(2)PKC. Any attacker using Gröbner bases attack will have to solve the set of simultaneous equations of degree $k-1$. For $k \gtrsim 40$, the attacker would be required to solve the set of simultaneous equations of larger than 39, which will be a formidable task.

Let us show several examples in Table 3.

Table. 3. Examples ($\rho = 1.0$).

Example	m	k	$n = 2k$	$P_c[\hat{P}_I]$	$\boldsymbol{P}_c[\hat{\boldsymbol{\pi}}]$	$\boldsymbol{S}_{PK}(KB)$
I	1	40	80	$8.27e^{-25}$	$9.10e^{-13}$	32.4
II	1	60	120	$7.52e^{-37}$	$8.67e^{-19}$	109
III	1	80	160	$6.84e^{-49}$	$8.27e^{-25}$	257

As we see in Table 3, the probability $Pc[\hat{\pi}]$ is $9.10 \times 10^{-13} \cong 10^{-12}$, which seems not a sufficiently small value. However this value of 10^{-12} would be sufficiently small from the practical point of view, as we shall see below.

From a very conservative point of view, let us assume that a set of quadratic equations in 80 variables can be solved with Gröbner bases attack within only 1 msec. Even from such conservative estimate, it would take 31.7 years, on an average, to solve 10^{12} sets of simultaneous equations. We conclude that the three examples listed in Table 3 would be very secure against the Gröbner bases attack.

4 Conclusion

- We have presented a new scheme, K(Ⅱ)TS, that transforms message variables, in a non-linear way. The proposed schme K(Ⅱ)TS would yield a brand new technique in the fields of code-based PKC and the multivariate PKC, for much improving the secutity.

- We have presented new classes of public key cryptosystem K(XVI)SE(1)PKC based on the Reed-Solomon code over $\mathbb{F}_{2^m}$ and K(XVI)SE(2)PKC based on the cyclic code over $\mathbb{F}_2$, exactly realizing the coding rate of $\rho = 1.0$, which implies that the digital signature scheme can be easily realized with K(XVI)SE(1)PKC and K(XVI)SE(2)PKC.
- We have shown that excluding the exhaustive search attack, any attacker will have to solve the set of simultaneous equations of very high degree although all the public keys in K(XVI)SE(1)PKC are represented by the linear simultaneous equations in the variables $M_1, M_2, \cdots, M_n$.
- We have shown that the Gröbner bases attack will find it very hard to attack on K(XVI)SE(1)PKC and K(XVI)SE(2)PKC due to the introduction of K(II)TS when constructing the ciphertext $\boldsymbol{C} = \boldsymbol{C}_I + \boldsymbol{C}_{II}$.
- We have shown that the sufficiently secure K(XVI)SE(1)PKC can be constructed over $\mathbb{F}_{2^8}$, which are extensively used in the various storage and transmission systems.

This work is partly supported by the NICT's project:Research and developement for public key cryptosystem for secure communication between social systems and is also supported by 21st.Century Informatic Culture Center.

References

[1] M. Kasahara, "A New Class of Public Key Cryptosystems Constructed Based on Reed-Solomon Codes K(XII)SE(1)PKC", Technical Report of IEICE, ISEC 2013-5 (2013-05).

[2] 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).

[3] 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).

[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] J. C. Faugere and A. Joux "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases", In Advances in Cryptoglogy-CRYPTO 2003 pp.44-60 (2003).

[8] C. Wolf: "Multivariate Quadratic Polynomials in Public Key Cryptography", Dr. Thesis, Katholieke Universiteit Leuven, (2005-11).

[9] M. Kasahara "New Classes of Public Key Cryptosystems Constructed Based on Cyclic Codes, K(XV)SE(1)PKC and K(XVI)SE(1)PKC", Technical Report of IEICE, IT 2015-4 (2015-05).

[10] M. Kasahara "A New Class of Public Key Cryptosystems Constructed Based on Perfect Error-Correcting Codes Realizing Coding Rate of exactly 1.0", Cryptology ePrint Archive , Report 2010/139 (2010-03).

[11] 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).

[12] M. Kasahara: "Public Key Cryptosystems Constructed Based on Pseudo Cyclic Codes, K(IX)SE(1)PKC, Realizing Coding Rate of Exactly 1.0", Cryptology ePrint Archive, Report 2011/545, (2011-09).

[13] M. Kasahara: "A New Class of Product-sum Type Public Key Cryptosystem, K(V)ΣΠPKC, Constructed Based on Maximum Length Code", Cryptology ePrint Archive, Report 2013/180, (2013-03).

[14] M. Kasahara: "A New Class of Public Key Cryptosystems Construted Based on Reed-Solomon Codes, K(Ⅱ)SE(1)PKC.–Along with a presentation of K(Ⅱ)SE(1)PKC over the extension field extensively used for present day various storage and transmission systems", Cryptology ePrint Archive, Report 2013/363, (2013-06).

[15] R. J. McEliece: "A Public-key Cryptosystem Based on Algebraic Coding Theory", DSN Progress Report, no.42-44, pp.114-116 (1978).

[16] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa: "An Erasures-and-Errors decoding Algorithm for Goppa Codes", IEEE Trans. on Inform. Theory, IT-22, 2, pp.238-241 (1976-03).