Public Key Cryptosystems Constructed Based on Reed-Solomon Codes, K(XV)SE(2)PKC, Realizing Coding Rate of Exactly 1.0

Masao KASAHARA
Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564-8511 Japan.
kasahara@ogu.ac.jp

Abstract

In this paper, we present a new class of public-key cryptosystems, K(XV)SE(2)PKC realizing the coding rate of exactly 1.0, based on Reed-Solomon codes(RS codes). We show that K(XV)SE(2)PKC is secure against the various attacks including the attacks based on the Gröbner basis calculation (Gröbner basis attack, GB attack) and a linear transformation attack.

Keyword

Public key cryptosystem, PQC, Reed-Solomon code, Code based PKC, Multivariate PKC, Gröbner basis.

1 Introduction

Most of the multivariate PKC are constructed by the simultaneous equations of degree larger than or equal to 2 [1]∼[14].

All these proposed schemes are very interesting and important. However unfortunately, some of these schemes have been proved not necessarily secure against the conventional attacks such as Patarin's attack[3], the attack based on the Gröbner basis calculation (GB Attack)[11-13] and Braeken-Wolf-Preneel(BWP) attack[14].

The author recently proposed several classes of multivariate PKC's that are constructed by many sets of linear equations[15-20]. It should be noted that McEliece PKC[21] presented in 1978 can be regarded as a member of the class of linear multivariate PKC.

In 2011 the author presented a multivariate PKC, K(XIV)RSE(g)PKC, based on message-dependent transformation[22]. The K(XIV)RSE(g)PKC would be secure against the various conventional attacks[11-13], as the transformation is performed depending on the given message sequence.

In this paper we present a new class of public key cryptosystem, K(XV)SE(2)PKC based on error-correcting codes, realizing the coding rate of exactly 1.0. K(XV)SE(2)PKC is constructed on the basis of K(X)SE(1)PKC[23] which is not secure against a linear transformation attack[24]. We show that K(XV)SE(2)PKC is secure against the attacks based on a linear transformation attack and the GB Attack[11-13].

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 similarly defined.

2 k(XV)SE(1)PKC

In this section we present a simple version of K(XV)SE(2)PKC referred to as k(XV)SE(2)PKC. Generalization of k(XV)SE(2)PKC to K(XV)SE(2)PKC is straightforward.

2.1 Preliminaries

Let us define several symbols:

$g_i(x)$	:	Generator polynomial of RS code of degree 2 over $\mathbb{F}_{2^m}; i = 1, 2$.
L_i	:	Location, $L_i \geq 2$, $i = 1, 2$, $L_1 \neq L_2$.
x^{L_i}	:	Single error whose error value is 1 that occurred at the location $L_i; i = 1, 2$.
m_i	:	Message symbol over $\mathbb{F}_{2^m}; i = 1, 2, 3, 4$.
$P_C[\widehat{g}_i(x)]$	:	Probability that $g_i(x)$ is estimated correctly, $i = 1, 2$.
$P_C[\widehat{L}_i]$	:	Probability that L_i is estimated correctly, $i = 1, 2$.

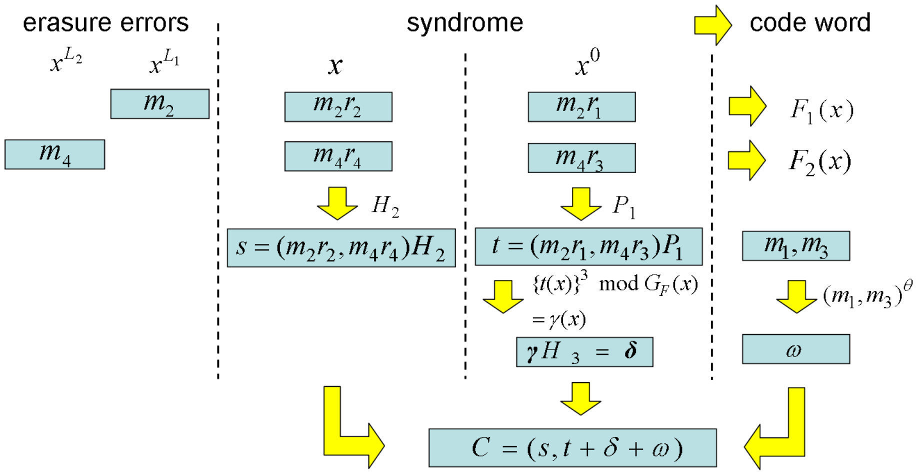

Figure 1: Schematic diagram of principle of k(XV)SE(2)PKC

$P_C[\widehat{g}_i(x)\cap\widehat{L}_i]$	:	Probability that both $g_i(x)$ and $L_i(x)$ are estimated correctly, $i=1,2$.
H_i	:	Random matrix whose component takes on 0 or 1 equally likely, $i=1,2$.
$g_F(x)$	:	Random primitive polynomial of degree $2m$ whose coefficients except those of x^0 and x^{2m} take on 0 or 1 equally likely.
$G_i(x)$	:	Generator polynomial of RS code of degree g over $\mathbb{F}_{2^m}$; $i=1,2,\cdots,E$.

2.2 Construction

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

$$\boldsymbol{A}=(A_1,A_2,\cdots,A_N). \tag{3}$$

Throughout this paper we assume that the messages $A_1,A_2,\cdots,A_N$ are mutually independent and equally likely. Let $\boldsymbol{A}$ be transformed into

$$\begin{aligned}\boldsymbol{A}\cdot H_1&=\boldsymbol{a}\\&=(a_1,a_2,\cdots,a_N),\end{aligned} \tag{4}$$

where H_1 is an $N\times N$ non-singular random matrix over $\mathbb{F}_2$.

Let $\boldsymbol{a}$ be partitioned into

$$\boldsymbol{a}=(m_1,m_2,m_3,m_4), \tag{5}$$

where m_i's are m-tuples over $\mathbb{F}_2$.

Let us regard m_i as an element of $\mathbb{F}_{2^m}$.

Let m_1 and m_2 be represented by

$$m_1=(a_{11},\cdots,a_{1m}) \tag{6}$$

and

$$m_2=(a_{21},\cdots,a_{2m}). \tag{7}$$

respectively.

Let $r_1(x)$ be obtained by

$$m_2x^{L_1}\equiv r_1(x)=m_2r_2x+m_2r_1 \bmod g_1(x), \tag{8}$$

yielding a code word, $F_1(x)$:

$$F_1(x)=m_2x^{L_1}+m_2r_2x+m_2r_1\equiv 0 \bmod g_1(x). \tag{9}$$

Let m_3 and m_4 be represented by

$$m_3=(a_{31},\cdots,a_{3m}) \tag{10}$$

and

$$m_4=(a_{41},\cdots,a_{4m}) \tag{11}$$

respectively.

Let $r_2(x)$ be given by

$$m_4x^{L_2}\equiv r_2(x)=m_4r_4x+m_4r_3 \bmod g_2(x), \tag{12}$$

yielding a code word, $F_2(x)$:

$$F_2(x)=m_4x^{L_2}+m_4r_4x+m_4r_3\equiv 0 \bmod g_2(x). \tag{13}$$

Regarding (m_2r_2,m_4r_4) as a $2m$-tuple over $\mathbb{F}_2$, it is transformed into

$$\begin{aligned}(m_2r_2,m_4r_4)H_2&=\boldsymbol{s}\\&=(s_1,s_2,\cdots,s_{2m}),\end{aligned} \tag{14}$$

where H_2 is a $2m\times 2m$ non-singular random matrix over $\mathbb{F}_2$.

Remark 1 : The component $s_i; i=1,2,\cdots,2m$, is a linear equation in the variables $A_1,A_2,\cdots,A_N$ over $\mathbb{F}_2$. □

Regarding $(m_2 r_1, m_4 r_3)$ as a $2m$-tuple over $\mathbb{F}_2$, it is transformed into

$$\begin{aligned}(m_2 r_1, m_4 r_3) P_1 &= \boldsymbol{t} \\ &= (t_1, t_2, \cdots, t_{2m}),\end{aligned} \tag{15}$$

where P_1 is a $2m \times 2m$ random permutation matrix.

Letting $t(x)$ be represented by $t_1 + t_2 x + \cdots + t_{2m} x^{2m-1}$, it is transformed into

$$\begin{aligned}\{t(x)\}^3 &\equiv \gamma(x) \\ &\equiv \gamma_1 + \gamma_2 x + \cdots + \gamma_{2m} x^{2m-1} \bmod g_F(x),\end{aligned} \tag{16}$$

where $g_F(x)$ is a random primitive polynomial of degree $2m$ over $\mathbb{F}_2$.

Let $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \cdots, \gamma_{2m})$ be transformed into

$$\begin{aligned}\boldsymbol{\gamma} H_3 &= \boldsymbol{\delta} \\ &= (\delta_1, \delta_2, \cdots, \delta_{2m}),\end{aligned} \tag{17}$$

where H_3 is a $2m \times 2m$ matrix over $\mathbb{F}_2$ which is not necessarily non-singular.

Let $\boldsymbol{\delta}$ be represented by

$$\boldsymbol{\delta} = (\boldsymbol{\delta}_\lambda, \boldsymbol{\delta}_\mu), \tag{18}$$

where $\boldsymbol{\delta}_\lambda$ and $\boldsymbol{\delta}_\mu$ over $\mathbb{F}_2$ are defined by

$$\boldsymbol{\delta}_\lambda = (\delta_1, \delta_2, \cdots, \delta_m) \tag{19}$$

and

$$\boldsymbol{\delta}_\mu = (\delta_{m+1}, \delta_{m+2}, \cdots, \delta_{2m}) \tag{20}$$

respectively.

It should be noted that the component of δ_i ; $i = 1, 2, \cdots, 2m$, is a quadratic equation in the variables $A_1, A_2, \cdots, A_N$ over $\mathbb{F}_2$.

Let $\boldsymbol{\delta}'_\lambda$ and $\boldsymbol{\delta}'_\mu$ be defined by

$$\boldsymbol{\delta} P_1^{-1} = (\boldsymbol{\delta}'_\lambda, \boldsymbol{\delta}'_\mu). \tag{21}$$

Regarding (m_1, m_3) over $\mathbb{F}_{2^m}$ as an element of $\mathbb{F}_{2^{2m}}$, (m_1, m_3) is transformed into

$$\begin{aligned}(m_1, m_3)^\theta &= \boldsymbol{\omega} \\ &= (\omega_1, \omega_2, \cdots, \omega_{2m}) \in \mathbb{F}_{2^{2m}},\end{aligned} \tag{22}$$

where θ is given by

$$\theta = 2^0 + 2^1 + \cdots + 2^\eta < 2^{2m} - 1. \tag{23}$$

Let $\boldsymbol{\omega}_\lambda$ and $\boldsymbol{\omega}_\mu$, be defined by

$$\boldsymbol{\omega}_\lambda = (\omega_1, \omega_2, \cdots, \omega_m) \tag{24}$$

and

$$\boldsymbol{\omega}_\mu = (\omega_{m+1}, \omega_{m+2}, \cdots, \omega_{2m}). \tag{25}$$

Let ω'_λ and ω'_μ be defined by

$$\boldsymbol{\omega} P_1^{-1} = (\boldsymbol{\omega}'_\lambda, \boldsymbol{\omega}'_\mu). \tag{26}$$

At the sending end, after calculating $\boldsymbol{\omega}$ by Eq.(22), $\boldsymbol{t}+\boldsymbol{\delta}+\boldsymbol{\omega}$ is obtained. The ciphertext C is given by

$$C = (\boldsymbol{s}, \boldsymbol{t} + \boldsymbol{\delta} + \boldsymbol{\omega}). \tag{27}$$

We have the following set of keys.

Public key	:	m_1, m_3, $\{s_i\}$, $\{t_i + \delta_i\}$, θ, $\mathbb{F}_{2^m}$, $\mathbb{F}_{2^{2m}}$.
Secret key	:	H_1, H_2, H_3, P_1, L_1, L_2, r_1, r_2, r_3, r_4, $g_1(x)$, $g_2(x)$, $g_F(x)$

2.3 Encryption and decryption

Encryption:

Step1 :The $\tilde{\boldsymbol{s}}$ is calculated from the public keys whose component is represented by the variables A_1, A_2, $\cdots$, A_N.

Step2 :The $\tilde{\boldsymbol{t}} + \tilde{\boldsymbol{\delta}}$ is calculated from the public key $\boldsymbol{t} + \boldsymbol{\delta}$ whose component is represented by the variables $A_1, A_2, \cdots, A_N$.

Step3 :The $\tilde{\boldsymbol{\omega}}$ is calculated from $\tilde{m}_1$ and $\tilde{m}_3$ by Eq.(22).

Step4 :The ciphertext $\tilde{C}$ is given by

$$\widetilde{C} = (\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{t}} + \tilde{\boldsymbol{\delta}} + \tilde{\boldsymbol{\omega}}). \tag{28}$$

Decryption:

Step1 :The $(\tilde{m}_2 r_2, \tilde{m}_4 r_4)$ is decoded by $(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_{2m}) H_2^{-1}$.

Step2 :The $(\tilde{m}_2 r_1 + \tilde{\boldsymbol{\delta}}'_\lambda + \tilde{\boldsymbol{\omega}}'_\lambda, \tilde{m}_4 r_3 + \tilde{\boldsymbol{\delta}}'_\mu + \tilde{\boldsymbol{\omega}}'_\mu)$ is decoded by $(\tilde{\boldsymbol{t}} + \tilde{\boldsymbol{\delta}} + \tilde{\boldsymbol{\omega}}) P_1^{-1}$.

Step3 :From $(\tilde{m}_2 r_2, \tilde{m}_2 r_1 + \tilde{\boldsymbol{\delta}}'_\lambda + \tilde{\boldsymbol{\omega}}'_\lambda)$ and $(\tilde{m}_4 r_4, \tilde{m}_4 r_3 + \tilde{\boldsymbol{\delta}}'_\mu + \tilde{\boldsymbol{\omega}}'_\mu)$, the sets of double erasure errors, $(\tilde{m}_2 x^{L_1}, \tilde{\boldsymbol{\delta}}'_\lambda + \tilde{\boldsymbol{\omega}}'_\lambda)$ and $(\tilde{m}_4 x^{L_2}, \tilde{\boldsymbol{\delta}}'_\mu + \tilde{\boldsymbol{\omega}}'_\mu)$ are decoded, for example, by Euclidean decoding[25], yielding $(\tilde{m}_2, \tilde{\boldsymbol{\delta}}'_\lambda + \tilde{\boldsymbol{\omega}}'_\lambda)$ and $(\tilde{m}_4, \tilde{\boldsymbol{\delta}}'_\mu + \tilde{\boldsymbol{\omega}}'_\mu)$.

Step4 :From $\tilde{m}_2$ and $\tilde{m}_4$, the $(\tilde{\boldsymbol{\delta}}'_\lambda, \tilde{\boldsymbol{\delta}}'_\mu)$ is decoded by Eqs.(15) $\sim$ (21), yielding $\tilde{\boldsymbol{\omega}}'_\lambda$ and $\tilde{\boldsymbol{\omega}}'_\mu$.

Step5 :The $\tilde{\boldsymbol{\omega}}$ is decoded by $(\tilde{\boldsymbol{\omega}}'_\lambda, \tilde{\boldsymbol{\omega}}'_\mu) P_1$.

Step6 :The $(\tilde{m}_1, \tilde{m}_3)$, an element of $\mathbb{F}_{2^{2m}}$, is decoded by $\tilde{\boldsymbol{\omega}}^{1/\theta}$.

Step7 :The original message $\tilde{\boldsymbol{A}}$ is decoded by $(\tilde{m}_1, \tilde{m}_2, \tilde{m}_3, \tilde{m}_4) H_1^{-1} = \boldsymbol{A} = (\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_N)$.

Table 1: Example of k(XV)SE(2)PKC($\rho = 1.0$).

Example	$\lvert A\rvert$ N(bit)	$\lvert m_i\rvert$ m(bit)	$\eta+1=2m-1$	$P_C[\widehat{g}_1(x)\cap\widehat{L}_1]$ $*P_C[\widehat{g}_2(x)\cap\widehat{L}_2]$	S_{PK} (KB)	ρ
I	128	32	63	2.94×10^{-39}	68.1	1.0
Ⅱ	160	40	79	6.84×10^{-49}	132	1.0
Ⅲ	192	48	95	1.59×10^{-58}	227	1.0

2.4 Parameters

Let us define several symbols:

N_V	:	Total number of message variables, $N=4m$.
N_{ESl}	:	Total number of $2m$ linear equations representing the components of $\boldsymbol{s}, s_1, s_2, \cdots, s_{2m}$.
N_{ESq}	:	Total number of $2m$ quadratic equations representing the components of $\boldsymbol{t}+\boldsymbol{\delta}$.
SE($\boldsymbol{s}$)	:	Set of linear equations related to $\boldsymbol{s}$ in the variables A_1, A_2, $\cdots$, A_N.
SE($\boldsymbol{t}+\boldsymbol{\delta}$)	:	Set of quadratic equations related to $\boldsymbol{t}+\boldsymbol{\delta}$ in the variables A_1, A_2, $\cdots$, A_N.
SE(m_i)	:	Set of linear equations related to m_1 or m_3 in the variables A_1, A_2, $\cdots$, A_N.

The sizes of SE($\boldsymbol{s}$),SE($\boldsymbol{t}+\boldsymbol{\delta}$), SE($m_1$) and SE($m_3$) are given by

$$|\mathrm{SE}(\boldsymbol{s})| = N_V * N_{ESl}, \tag{29}$$

$$|\mathrm{SE}(\boldsymbol{t}+\boldsymbol{\delta})| = {}_{N_V}H_2 \cdot N_{ESq}, \tag{30}$$

and

$$|\mathrm{SE}(m_1)| = |\mathrm{SE}(m_3)| = N_V * m, \tag{31}$$

respectively.

The size of the public key for m_1, m_3, $\{\boldsymbol{s}\}$ and $\{\boldsymbol{t}+\boldsymbol{\delta}\}$, S_{PK} is given by

$$S_{PK} = {}_{N_V}H_2 \cdot 2m + 4N_V * m. \tag{32}$$

The coding rate ρ is given by

$$\begin{aligned}\rho &= \frac{|\boldsymbol{M}|}{|C|} \\ &= \frac{|m_1|+|m_2|+|m_3|+|m_4|}{|m_2r_2|+|m_4r_4|+|m_2r_1+\boldsymbol{\omega}_\lambda+\boldsymbol{\delta}_\lambda|+|m_4r_3+\boldsymbol{\omega}_\mu+\boldsymbol{\delta}_\mu|} \\ &= 1.0.\end{aligned} \tag{33}$$

We see that the coding rate is given by exactly 1.0.

The probability that the location is estimated correctly, $P_C\left[\hat{L}_i\right]$, is given by

$$P_C\left[\hat{L}_i\right] = (2^m-3)^{-1} \cong 2^{-m}; i=1,2. \tag{34}$$

The probability that $g_i(x)$ is estimated correctly, $P_C[\hat{g}_i(x)]$, is given by

$$P_C[\hat{g}_i(x)] = \left\{2^{m(g-2)} * (2^m-1)\right\}^{-1} \cong 2^{-m(g-1)}; i=1,2. \tag{35}$$

2.5 Examples

In Table 1, we show three examples of k(XV)SE(2)PKC.

2.6 Security consideration

Attack 1 : Attack on L_i and $g_i(x)$; i = 1,2.

The probability that $g_i(x)$'s and L_i's are estimated correctly is given by

$$\left\{P_c[\widehat{g}_i(x)\cap\widehat{L}_i]\right\}^2 = \left\{[P_C[\widehat{g}_i(x)]\cdot P_C[\widehat{L}_i]\right\}^2; i=1,2, \tag{36}$$

sufficiently small value for $m \gtrsim 20$. We conclude that k(XV)SE(2)PKC is secure against Attack 1. □

Attack 2 : GB Attack on ciphertext

The components of $\boldsymbol{\omega}$ over $\mathbb{F}_{2^{2m}}$ can be represented by the set of equations over $\mathbb{F}_2$ of very high degree. Sets of the components of $(s, \boldsymbol{t}+\boldsymbol{\delta}+\boldsymbol{\omega})$ yield a set of $2m$ equations of degree $\eta+1$ in the variables $A_1, A_2, \cdots, A_N$ and a set of $2m$ linear equations in the variables $A_1, A_2, \cdots, A_N$. The degrees take on a very high value of at least 63 as we see in the examples in Table 1. We thus conclude that our proposed scheme, k(XV)SE(2)PKC, can be secure against GB Attack, the attack based on Gröbner basis calculation. □

Attack 3 : Exhaustive attack on $(\tilde{m}_1, \tilde{m}_3)$.

We see that when $(\tilde{m}_1, \tilde{m}_3)$ is estimated correctly by an exhaustive manner, the ciphertext can be disclosed by the GB attack on the set of $2m$ quadratic equations and $2m$ linear equations. It is easy to see that the average number of times required for estimating $(\tilde{m}_1, \tilde{m}_3)$ in an exhaustive manner is given by 2^{2m-1}.

In order to be secure against this attack, $2m$, the size of $(\tilde{m}_1, \tilde{m}_3)$ is recommended to be sufficiently large($m \gtrsim 30$). □

Attack 4 : Attack on (m_2r_1, m_4r_3) from s.

It is apparent that (m_2r_1, m_4r_3) can be disclosed from (m_2r_2, m_4r_4) by a linear transformation[24].

However in k(XV)SE(2)PKC, (m_2r_1, m_4r_3) is transformed into a set of quadratic equations through a series of transformations given by Eqs.(15),(16) and (17).

We conclude that (m_2r_1, m_4r_3) cannot be disclosed from s by a linear transformation.

3 K(XV)SE(2)PKC

In this section we present a generalized version of k(XV)SE(2)PKC, referred to as K(XV)SE(2)PKC. As K(XV)SE(2)PKC is a straightforward generalization of k(XV)SE(2), we shall only present an outline of the construction of K(XV)SE(2)PKC.

3.1 Construction

Let m_i be

$$m_i = (m_{i1}, \cdots, m_{im}) \quad ; i = 1, 2, \cdots, E. \tag{37}$$

In the followings let us regard m_i's as the elements of $\mathbb{F}_{2^m}$. Let

$$\begin{aligned} m_1x^{L_1} &\equiv r_1(x) \\ &= m_1r_{11} + m_1r_{12}x + \cdots + m_1r_{1g}x^{g-1} \bmod G_1(X), \\ m_2x^{L_2} &\equiv r_2(x) \\ &= m_2r_{21} + m_2r_{22}x + \cdots + m_2r_{2g}x^{g-1} \bmod G_2(X), \\ &\vdots \\ m_Ex^{L_E} &\equiv r_E(x) \\ &= m_Er_{E1} + m_Er_{E2}x + \cdots \\ &\qquad \cdots + m_Er_{Eg}x^{g-1} \bmod G_E(X), \end{aligned} \tag{38}$$

where all the locations L_i's are distinct and satisfy

$$g \le L_i \le 2^m - 2 \quad ; i = 1, 2, \cdots, E. \tag{39}$$

We also assume that the degree of $G_i(x); i = 1, 2, \cdots, E$, is given by g.

Let the remainder $r_i(x) = m_ir_{i1} + m_ir_{i2}x + \cdots + m_ir_{ig}x^{g-1}$ given by Eq.(38) be partitioned into

$$r_i(x) = r_{iE}(x) + r_{iH}(x), \quad ; i = 1, 2, \cdots, E, \tag{40}$$

where $r_{iE}(x)$ and $r_{iH}(x)$ are given by

$$\begin{aligned} r_{iE}(x) = m_ir_{i,H+1}x^H + m_ir_{i,H+2}x^{H+1} + \cdots \\ \cdots + m_ir_{ig}x^{g-1} \end{aligned} \tag{41}$$

and

$$r_{iH}(x) = m_ir_{i,1} + m_ir_{i,2}x + \cdots + m_ir_{iH}x^{H-1} \tag{42}$$

Let the positive integers E and H satisfy

$$E + H = g. \tag{43}$$

respectively.

Given $m_1, m_2, \cdots, m_E$, we construct

$$\begin{aligned} \sum_{i=1}^{E} m_ix^{L_i} = \sum_{i=1}^{E} m_ir_{iH+1} + \sum_{i=1}^{E} m_ir_{iH+2}x + \\ \cdots + \sum_{i=1}^{E} m_ir_gx^{g-1}. \end{aligned} \tag{44}$$

The vector $\boldsymbol{V}_E = \left(\sum_{i=1}^{E} m_ir_{i,H+1}, \cdots, \sum_{i=1}^{E} m_ir_{ig}\right)$ is transformed into

$$\begin{aligned} \boldsymbol{V}_E \cdot H_4 &= \boldsymbol{s} \\ &= (V_{H+1}, V_{H+2}, \cdots, V_g), \end{aligned} \tag{45}$$

where H_4 is a random $E \times E$ non-singular matrix over $\mathbb{F}_{2^m}$.

The vector $\boldsymbol{V}_H = (\sum_{i=1}^{E} m_ir_{i1}, \cdots, \sum_{i=1}^{E} m_ir_{iH})$ is transformed into

$$\begin{aligned} \boldsymbol{V}_H \cdot P_2 &= \boldsymbol{T} \\ &= (V_1, V_2, \cdots, V_H), \end{aligned} \tag{46}$$

where P_2 is a $H \times H$ random permutation matrix over $\mathbb{F}_{2^m}$.

The T is transformed into

$$\boldsymbol{T}^3 = \boldsymbol{\Gamma} \tag{47}$$

in a similar manner as Eq.(16).

Messages $m_{E+1}, m_{E+2}, \cdots, m_N$, are publicized as

$$\boldsymbol{V}_P = (m_{E+1}, m_{E+2}, \cdots, m_N), \tag{48}$$

In a simlar manner as Eq.(22), $\boldsymbol{\Omega}$ is given by

$$\boldsymbol{V}_P^{\Theta} = \boldsymbol{\Omega}. \tag{49}$$

The correspondence among the parameters for k(XV)SE(2)PKC and K(XV)SE(2)PKC is shown below:

k(XV)SE(2)PKC		K(XV)SE(2)PKC
(m_2r_2, m_4r_4)	$\rightarrow$	$\boldsymbol{V}_E$
(m_2r_1, m_4r_3)	$\rightarrow$	$\boldsymbol{V}_H$
$(m_1, m_3)^{\theta} = \boldsymbol{\omega}$	$\rightarrow$	$\boldsymbol{V}_P^{\Theta} = \boldsymbol{\Omega}$
$(m_2r_2, m_4r_4)H_2 = \boldsymbol{s}$	$\rightarrow$	$\boldsymbol{V}_EH_4 = \boldsymbol{S}$
$(m_2r_1, m_4r_3)P_1 = \boldsymbol{t}$	$\rightarrow$	$\boldsymbol{V}_HP_2 = \boldsymbol{T}$
$\boldsymbol{t}^3 = \boldsymbol{\gamma}$	$\rightarrow$	$\boldsymbol{T}^3 = \boldsymbol{\Gamma}$
$\boldsymbol{\gamma}H_3 = \boldsymbol{\delta}$	$\rightarrow$	$\boldsymbol{\Gamma}H_5 = \boldsymbol{\Delta}$
$C_I = (\boldsymbol{s}, \boldsymbol{t} + \boldsymbol{\delta} + \boldsymbol{\omega})$	$\rightarrow$	$C_{II} = (\boldsymbol{S}, \boldsymbol{T} + \boldsymbol{\Delta} + \boldsymbol{\Omega})$

4 Conclusion

In this paper we have presented k(XV)SE(2)PKC. We have briefly described K(XV)SE(2)PKC because it can be constructed by a straightforward generalization of k(XV)SE(2)PKC.

We have shown that k(XV)SE(2)PKC would be secure against the various attacks including GB Attack, the attack based on Gröbner basis calculation.

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] J. Patarin: "Hidden fields equations(HFE) and isomorphisms of polynomials(IP): two new families of asymmetric algorithm", Proc.EUROCRYPT'96, Lecture Notes in Computer Science, Vol.1070, pp.33-48, Springer, (1996-05).

[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] S. Tsujii, R. Fujita and K. Tadaki: "Proposal of MOCHIGOMA(piece in hand) concept for multivariate type public key cryptosystem", Technical Report of IEICE, ISEC 2004-74, (2004-09).

[6] J. Ding: "A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation", PKC 2004, LNCS 2947, pp.305-318, 2004.

[7] 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).

[8] J. Ding, D. Schmidt and J. Gower: "Multivariate Public key Cryptography", Springer-Verlag(2006).

[9] 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).

[10] M. Kasahara: "Public Key Cryptosystems Constructed Based on Cyclic Codes, Realizing Coding Rate of Exactly 1.0, K(XI)SE(g)PKC and K(XII)SE(g)PKC", Technical Report of IEICE, ISEC 2011-23(2011-07).

[11] A. Kipnis and A. Shamir: "Cryptoanalysis of the HFE Public Key Cryptosystem by Relinearization", Advances in Cryptography-Crypto'99, LNCS 1666, pp.19-30, (1999).

[12] M. Bardet, J. C. Faugére and B. Salvy: "Complexity of Gröbner basis computation for semi-regular overdetermined sequence over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$", Technical Report RR-5049, INRIA, (2003-12).

[13] J-C Faugére: "Algebraic cryptanalysis of HFE using Gröbner basis", INRIA (2003).

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

[15] 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).

[16] M.Kasahara: "Linear Multivariate Cryptosystem Constructed on the Basis of Probabilistic Structure", 2009 JSIAM Annual Meesing, Osaka, (2009-09).

[17] 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).

[18] M. Kasahara: "A New Class of Public Key Cryptosystem Constructed Based on Error-Correcting Codes Realizing Coding Rate of Exactly 1.0", Cryptology ePrint Archive, 2010/139 (2010).

[19] M. Kasahara: "A New Class of Public Key Cryptosystems Constructed Based on Error-Correcting Codes, Using K(III) Scheme", Cryptology ePrint Archive, 2010/341 (2010).

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

[21] R. J. McEliece: "A public key cryptosystem based on algebraic coding theory", DSN Prog. Re., pp.114-116, (1978).

[22] M. Kasahara: "A New Class of Multivariate Public Key Cryptosystem Constructed on the Basis of Message-Dependent Transformation", Cryptology ePrint Archive, 2011/690 (2011).

[23] M. Kasahara: "Public Key Cryptosystems Constructed Based on Reed-Solomon Codes and Pseudo Cyclic Codes, K(IX)SE(1)PKC and K(X)SE(1)PKC, Realizing Coding Rate of Exactly 1.0", Technical Report of IEICE, ISEC 2011-31, (2011-9).

[24] M. Kasahara: "K(X)SE(1)PKC is not secure", Memorandom for File at Kasahara Lab., Osaka Gakuin University, (2011-11).

[25] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa: "An erasures-and-errors decoding algorithm for Goppa codes", IEEE Trans. Info. Theory, 22 (1976).