Construction of A New Class of Linear Multivariate Public Key Cryptosystem, K(I)SE(1)PKC

Masao KASAHARA[†]

[†] Faculty of Informatics, Osaka Gakuin University
Kishibe-Minami, Suita-Shi, Osaka 564-8511 Japan

Abstract In this paper, we present a new class of linear multivariate PKC referred to as K(I)SE(1)PKC. We shall show that K(I)SE(1)PKC, a linear multivariate PKC, can be sufficiently secure against any linear transformation attack due to the probabilistic structure. We show that the probabilistic structure can be successfully introduced by the use of the Chinese Remainder Theorem.

Key words Public Key Cryptosystem(PKC), Multivariate PKC, Linear PKC.

1. Introduction

Most of the multivariate PKC are constructed by the simultaneous equations of degree larger than or equal to 2 [1]~[14]. In this paper, we shall try to construct a new class of multivariate PKC that is constructed by many sets of linear equations 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[15,16]. We show that our scheme is made invulnerable to Linear Transformation Attack (LT Attack) due to the probabilistic structure of choosing K sets of linear equations among $N(> K)$ sets. We show that this probabilistic structure can be successfully introduced by the use of the Chinese Remainder Theorem. In the followings, we shall refer to the proposed linear multivariate PKC constructed on the basis of probabilistic structure as K(I)SE(1)PKC. We shall also present a more secure version of K(I)SE(1)PKC, referred to as K*(I)SE(1)PKC.

In the followings, when the variable x_i takes on the actual value $\tilde{x}_i$, we shall denote the corresponding vector $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ as

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

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

2. Construction of K(I)SE(1)PKC

2.1 Generation of Set of Keys

Let the message vector $\boldsymbol{m}$ over $\mathbb{F}_2$ and the corresponding message polynomial $m(x)$ be represented by

$$\boldsymbol{m} = (m_1, m_2, \cdots, m_n) \tag{2}$$

and

$$m(x) = m_1 + m_2 x + \cdots + m_n x^{n-1}, \tag{3}$$

respectively.

Letting $w_i(x)$ be the irreducible polynomial of degree λ, we define the following set of polynomials:

$$\begin{aligned} m(x) &\equiv m_1(x) \bmod w_1(x), \\ &\equiv m_2(x) \bmod w_2(x), \\ &\vdots \\ &\equiv m_N(x) \bmod w_N(x). \end{aligned} \tag{4}$$

We let $m_i(x)$ be represented as

$$m_i(x) = m_{i1} + m_{i2} x + \cdots + m_{i\lambda} x^{\lambda-1}. \tag{5}$$

Letting $G_i(x) = g_{i1} + g_{i2} x + \cdots + g_{i\mu+1} x^{\mu}$ be a randomly generated primitive polynomial, we have

$$\begin{aligned} G_i(x) m_i(x) &= u_i(x) \\ &= u_{i1} + u_{i2} x + \cdots + u_{i,\mu+\lambda} x^{\mu+\lambda-1}, \\ &\qquad (i = 1, 2, \cdots, N). \end{aligned} \tag{6}$$

Remark 1: As the $G_i(x)$'s are randomly generated and μ, the degree of $G_i(x)$ is made sufficiently large, we can safely assume that $G_i(x)$'s are mutually different. In the following we assume that the degreee of $G_i(x)$ is larger than or equal to λ, the degree of $w(x)$.

In the followings we let $\mu + \lambda$ be η, for simplicity. It is easy to see that u_{ij} is a linear equation with n message variables, $m_1, m_2, \cdots, m_n$. Let $\boldsymbol{u}_i = (u_{i1}, u_{i2}, \cdots, u_{i,\eta})$ be transformed as

$$(u_{i1}, u_{i2}, \cdots, u_{i,\eta}) \, \mathrm{A} = (k_{i1}, k_{i2}, \cdots, k_{i,\eta}) , \tag{7}$$

where A is a non-singular random matrix given by

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{\eta 1} \\ a_{12} & a_{22} & \cdots & a_{\eta 2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1\eta} & a_{2\eta} & \cdots & a_{\eta\eta} \end{bmatrix} . \tag{8}$$

Table 1 Examples of K(I)SE(1)PKC

	N	K	${}_NC_K$	λ	μ	η	S_{PK} (KB)	$\|c\|$ bit
I	64	32	1.8×10^{18}	64	64	128	2097	2048
II	64	32	1.8×10^{18}	128	128	256	8389	8192
III	80	40	1.1×10^{23}	80	80	160	5120	3200
VI	100	50	1.0×10^{29}	100	100	200	12500	5000

Let $\{k_{ij}\}$ be denoted by S_i. We now have the following set of keys.

Public key : $\{S_i\}$.
Secret key : $\{w_i(x)\}, \{G_i(x)\}, \{u_{ij}\}$, A.

2. 2 Example of K(I)SE(1)PKC

Let us define the following symbols:

$f(\boldsymbol{m})$: Polynomial over $\mathbb{F}_2$,
$f_1m_1 + f_2m_2 + \cdots + f_nm_n$.

$|f(\boldsymbol{m})|$: Ambiguity (Entropy, information amount or size) of $f(\boldsymbol{m})$ (in bit), n.

Let the sizes of $m_i(x)$ and $u_i(x)$ be denoted as $|m_i(x)|$ and $|u_i(x)|$ respectively. From Eqs. (5) and (6), these are given by

$$|m_i(x)| = \lambda|f(\boldsymbol{m})| = \lambda n \quad \text{(bit)} \tag{9}$$

and

$$|u_i(x)| = \eta|f(\boldsymbol{m})| = \eta n \quad \text{(bit)}. \tag{10}$$

Letting n be given by $n = K\lambda$, the size of the public key, S_{PK}, is given by

$$S_{PK} = n\eta N = K\lambda\eta N \quad \text{(bit)}. \tag{11}$$

We assume here that an integer K satisfies

$$K < N - 1. \tag{12}$$

From the standpoint of security, it is recommended that ${}_NC_K$ be made sufficiently large. For example, when $N = 64$, $K = 32$, ${}_{64}C_{32}$ takes on 1.83×10^{18}, a sufficiently large value. We see that our scheme becomes invulnerable as ${}_NC_K$ increases.

Several examples of K(I)SE(1)PKC is shown in Table 1. The coding rate is 0.5. The $|c|$ is the size of the ciphertext.

2. 3 Encryption and Decryption

Let us assume that for any K sets of linear equations, $\{S_{i1}\}, \{S_{i2,}\}, \cdots, \{S_{iK}\}$, the least common multiple of the corresponding polynomials, $w_{i1}(x), w_{i2}(x), \cdots, w_{iK}(x)$, LCM$\{w_{i1}(x), w_{i2}(x), \cdots, w_{iK}(x)\}$, satisfies

$$\begin{aligned}&\text{Deg}\left[\text{LCM}\left\{w_{i1}(x), w_{i2}(x), \cdots, w_{iK}(x)\right\}\right] \\ &\qquad\qquad > \text{Deg } m(x),\end{aligned} \tag{13}$$

where deg{A} denotes the degree of A.

Encryption Process:

Step 1:

Sender chooses K sets of linear simultaneous equations, S_i's, from the N sets of linear equations in a totally random manner. Let these K sets of linear equations be denoted as $S_1, S_2, \cdots, S_K$, for simplicity.

Step 2:

Message values $\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n$ are substituted into the equations in $S_1, S_2, \cdots, S_K$, yielding the ciphertext, $C_1, C_2, \cdots, C_K$.

Decryption Process:

Step 1:

Letting the elements of ciphertext C_i be denoted as $\tilde{k}_{i1}, \tilde{k}_{i2}, \cdots, \tilde{k}_{i,\eta}$, we obtain

$$\begin{aligned}&\left(\tilde{k}_{i1}, \tilde{k}_{i2}, \cdots, \tilde{k}_{i,\eta}\right) \text{A}^{-1} \\ &\qquad = \left(\tilde{u}_{i1}, \tilde{u}_{i2}, \cdots, \tilde{u}_{i,\eta}\right).\end{aligned} \tag{14}$$

Step 2:

When $G_j(x)|\tilde{u}_i(x)$, for $i = 1, 2, \cdots, N$, we decide that

$$\tilde{u}_i(x) = G_j(x)\tilde{m}_j(x). \tag{15}$$

Step 3:

We obtain $\tilde{m}_j(x)$ as $\tilde{u}_i(x)/G_j(x)$.

Step 4

From $\tilde{m}_1(x), \tilde{m}_2(x), \cdots, \tilde{m}_K(x)$, the original message $\tilde{m}(x)$ is obtained based on the Chinese Remainder Theorem.

We have the following straight-forward theorem.

Theorem 1: Assuming that $G_i(x)$'s are mutually different, the signal spaces over $\mathbb{F}_2$ generated by $G_1(x), G_2(x), \cdots, G_N(x)$ are disjoint, when $\mu \geqq \lambda$. □

3. Security Consideration

3. 1 Attack based on estimating $\{G_i(x)\}$

Proof : Assuming that the following relation holds :

$$G_i(x)m_i(x) = G_j(x)m_j(x), \text{ for } j \neq i. \tag{16}$$

The $G_i(x)$ and $G_j(x)$ are mutually different irreducible polynomials of degree μ and the degree μ is larger than $\lambda - 1$, the degree of $m_i(x)$ and $m_j(x)$. This fact is contradictory to Eq.(16), yielding the proof. □

From Theorem 1, we see that in order to circumvent an exhaustive attack using a decoding table, the degrees of $G_i(x)$ and $w(x)$ should be sufficiently large. As a toy example, the decoding table for $m(x) = m_1 + m_2x + m_3x^2$ and $G(x) = x^2 + x + 1$ is shown in Table 2, where $\mu = 2$, $\lambda = 3$ and $\eta = 5$. We see that the size of table in the toy example is given by $2^\lambda(\lambda + \eta) = 64$bit.

The $G_i(x)$ is an irreducible polynomial of dgree μ randomly generated. For $\lambda = \mu \gtrsim 64$, it would become hard to estimate $G_i(x)$ for the given S_i. It should be noted that

Table 2 An example of decoding table

m_1	m_2	m_3	μ_1	μ_2	μ_3	μ_4	μ_5
0	0	0	0	0	0	0	0
0	0	1	0	0	1	1	1
0	1	0	0	1	1	1	0
0	1	1	0	1	0	0	1
1	0	0	1	1	1	0	0
1	0	1	1	1	0	1	1
1	1	0	1	0	0	1	0
1	1	1	1	0	1	0	1

$\lambda = \mu \simeq 60$, an exhaustive attack is required to use the tables of 22.5 EB. It should be also noted that for $\lambda = \mu \simeq 40$, the exhaustive attack can be realized using the reasonable size of tables of about 15 TB. Thus in K(I)·SE(1)PKC, the relation $\mu \gtrsim 60$ is strictly required.

3.2 Attack on $\{G_i(x)\}$ and A

The transformation A is performed on $\boldsymbol{u}_i = (u_{i1}, u_{i2}, \cdots, u_{i,\eta})$. The sender chooses K sets of linear equations from $\{S_i\}$. Thus the estimating of the chosen K sets correctly becomes hard when ${}_NC_K$ takes on a sufficiently large value.

However it should be noted that the secret Keys $\{G_i(x)\}$ and A can be disclosed by the attack based on Gröbner bases calculation which will be referred to as GB attack. In the followings, we shall show that, in K(I)SE(1)PKC, the invulnerability of the secret key $\{G_i(x)\}$ and A against the GB attack can be guaranteed.

In $\{\tilde{k}_{ij}\}$, the element $\tilde{k}_{ij}$ can be given by

$$\begin{aligned}\tilde{k}_{ij} &= (a_{j1}g_{i1} + a_{j2}g_{i2} + \cdots + a_{j,\mu+1}g_{i,\mu+1})\,\tilde{m}_{i1} \\ &+ (a_{j2}g_{i1} + a_{j3}g_{i2} + \cdots + a_{j,\mu+2}g_{i,\mu+2})\,\tilde{m}_{i2} \\ &\vdots \\ &+ (a_{j\lambda}g_{i1} + a_{j,\lambda+1}g_{i2} + \cdots + a_{j,\eta}g_{i,\mu+1})\,\tilde{m}_{i\lambda}.\end{aligned} \tag{17}$$

We see that $\tilde{m}_{ij}$ is a linear combination of the original messages $\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n$. Consequently the given $\tilde{k}_{ij}$ is a linear combination of the termes $a_{ju}g_{iv}$, $(u = 1, \cdots, \eta; v = 1, \cdots, \mu+1)$, for the given $\tilde{m}_1$, $\tilde{m}_2$, $\cdots$, $\tilde{m}_n$.

The number of variables, N_v and the number of equations, N_E, are given by

$$N_v = \eta^2 + (\mu+1)N \tag{18}$$

and

$$N_E = N\eta, \tag{19}$$

respectively.

For example when $\mu = 64$, $\eta = 128$, and $N = 64$ the number of variables and the number of equations are given by

$$N_v = 20544 \tag{20}$$

and

$$N_E = 8192 \tag{21}$$

respectively.

When $\mu = 64$, $\eta = 128$ and N is larger than 256, the following relation holds:

$$N_E > N_v. \tag{22}$$

In order to circumvent the situation such that Eq.(20) may hold, it is recommended to use several transformation matrices, $\mathrm{A_I}, \mathrm{A_{II}}, \mathrm{A_{III}}, \cdots$, instead of the use of only one transformation matrix A. It is evident that the use of more than one transformation matrices will effectively increase the number of variables.

We conclude that the secret key can be made sufficiently secure against the GB attack.

4. K*(I)SE(1)PKC

In this section, we shall present a more secure version of K(I)SE(1)PKC, referred to as K*(I)SE(1)PKC, by adding a random error vector on each member of $\{S_i\}$. We shall also see that K*(I)SE(1)PKC is able to improve the coding rate.

In this section, for simplicity, we assume that K sets $S_1, S_2, \cdots, S_K$ are randomly chosen from the set $\{S_i\}$ under the contidition that ${}_NC_K$ takes on a large value ($\gtrsim 10^{18}$).

Let us define the several symbols.

$\boldsymbol{C}_i$: Ciphertext vector corresponding to $S_i = \{k_{ij}\}$, $\left(\tilde{k}_{i1}, \tilde{k}_{i2}, \cdots, \tilde{k}_{i\eta}\right)$.

$\boldsymbol{e}_i$: Error vector that is added on $\boldsymbol{C}_i$.

$C_iA^{-1}(x)$: Polynomial representation of $\boldsymbol{C}_iA^{-1}$.

$e_iA^{-1}(x)$: Polynomial representation of $\boldsymbol{e}_iA^{-1}$.

$w(\boldsymbol{e}_i)$: Hamming weight of $\boldsymbol{e}_i$.

We assume that the vector having errors is decoded using the decoding table for $m_i(x)$, T_i. An example of a decoding table is shown in Table 3. In Table 3, $G(x)$ is given by $G(x) = 1 + x + x^3$ and $u(x)$ is represented as $u(x) = u_1 + u_2x + u_3x^2 + u_4x^3u_5x^4$. The remainder $r_1 + r_2x + r_3x^2$ is given by $u(x) \mod G(x)$.

Table 3 Example of Decoding Table ($\mu = 3, \eta = 6$)

r_1	r_2	r_3	u_1	u_2	u_3	u_4	u_5	u_6
1	0	0	1	0	0	0	0	0
0	1	0	0	1	0	0	0	0
0	0	1	0	0	1	0	0	0
1	1	0	0	0	0	1	0	0
0	1	1	0	0	0	0	1	0
1	1	1	0	0	0	0	0	1

The size of the decoding table, $|T_i(x)|$, is given by

$$|T_i(x)| = (\mu + \eta)\Gamma, \tag{23}$$

where Γ is given by

$$\Gamma = {}_{\eta}C_0 + {}_{\eta}C_1 + \cdots + {}_{\eta}C_t. \tag{24}$$

We assume that $w(\boldsymbol{e}_i)$ satisfies the following relations:

$$0 \leqq w(\boldsymbol{e}_i) \leqq t \tag{25}$$

and

$$(\mu + \eta)\Gamma \lesssim 2^{30}. \tag{26}$$

The vector $\boldsymbol{k}_i = (k_{i1}, k_{i2}, \cdots, k_{i\eta})$ with an error can be represented by

$$\boldsymbol{k}_i^{(\alpha)} = \boldsymbol{k}_i + \boldsymbol{e}_i^{(\alpha)}, \tag{27}$$

where $\boldsymbol{e}_i^{(\alpha)}$ is an error vector of weight t or less.

The $\boldsymbol{k}_i^{(\alpha)}$ is transformed and then divided by $G_i(x)$ as

$$\boldsymbol{k}_i^{(\alpha)}\mathrm{A}^{-1}(x) = G_i(x)Q_i(x) + r_i^{(\alpha)}(x), \tag{28}$$

where $Q_i(x)$ is the quotient and $r_i^{(\alpha)}(x)$ is the remainder.

In the decoding process, $\boldsymbol{k}_i^{(\alpha)}$ is divided by $G_1(x)$, $G_2(x)$, $\cdots, G_N(x)$. Namely the following divisions are performed.

$$\begin{aligned} \boldsymbol{k}_i^{(\alpha)}\mathrm{A}^{-1}(x) &= G_1(x)Q_1(x) + r_{i1}(x) \\ &= G_2(x)Q_2(x) + r_{i2}(x) \\ &\ \ \vdots \\ &= G_j(x)Q_j(x) + r_{ij}(x) \\ &\ \ \vdots \\ &= G_N(x)Q_N(x) + r_{iN}(x) \end{aligned} \tag{29}$$

where $Q_j(x)$ is the quotient and $r_{ij}(x)$ is the remainder $(j = 1, 2, \cdots, N)$.

It should be remainded here that $\{G_j(x)\}$ is the set of primitive polynomial of degree μ, and λ is chosen as $\lambda = \mu$.

Theorem 1: In Eq.(27), the relation,

$$r_{ij}(x) \mathrel{\char"2262} r_i^{(\alpha)}(x) \tag{30}$$

holds for $j \neq i$, where we let $r_{ii}(x)$ be $r_i^{(\alpha)}(x)$.

Proof : Assuming that $r_{ij}(x) = r_i^{(\alpha)}(x)$ for $j \neq i$, we then have

$$G_i(x)Q_i(x) = G_j(x)Q_j(x), \tag{31}$$

which is a contradiction, yielding the proof. □

From Theorem 1, it is easy to see that the following relation holds:

$$\{r_i^{(\alpha)}(x)\} \cap \{r_j^{(\alpha)}(x)\} = \phi, \text{ for } i \neq j. \tag{32}$$

In decoding process of $k_i^{(\alpha)}\mathrm{A}^{-1}(x)$, if $k_i^{(\alpha)}\mathrm{A}^{-1}(x)$ mod $G_j(x)$ coincides with $r_i^{(\alpha)}(x)$, then error correction can be successfully performed on $\boldsymbol{e}_i^{(\alpha)}$. From Theorem 1, we see that the probability of erroneously decoding $m_j(x)$, $(j \neq i)$, for the given $k_i^{(\alpha)}\mathrm{A}^{-1}(x)$, $P[\epsilon]$, is given by

$$P[\epsilon] = 0, \tag{33}$$

yielding the ideal value.

Theorem 2: As $G_i(x)$ is randomly generated primitive polynomial, when $w(\boldsymbol{e}_{ij}) = 1$, for $j = 1, 2$, the error $\boldsymbol{e}_i$ can be successfully corrected.

Proof: Let two single errors be denoted by $e_{i1}(x)$ and $e_{i2}(x)$ respectively. We then have

$$e_{i1}(x) = G_i(x)Q_{i1}(x) + R_{i1}(x) \tag{34}$$

and

$$e_{i2}(x) = G_i(x)Q_{i2}(x) + R_{i2}(x). \tag{35}$$

Assuming that $R_{i1}(x) = R_{i2}(x)$, then

$$e_{i1}(x) + e_{i2}(x) = G_i(x)(Q_{i1}(x) + Q_{i2}(x)), \tag{36}$$

which is a contradiction as the weight of $\boldsymbol{e}_{i1} + \boldsymbol{e}_{i2}$ is 2, yielding proof. □

Theorem 3: When $2 \leqq w(\boldsymbol{e}_i) \leqq t$, the probability that $\boldsymbol{e}_i$ is correctly decoded, $P[C]$, is given by

$$P[C] = (1 - \Gamma \cdot 2^{-\mu})^{\Gamma - 1} \tag{37}$$

where $\Gamma = {}_{\eta}C_0 + {}_{\eta}C_1 + \cdots + {}_{\eta}C_t$. □

From Theorem 3, we see that when $(\Gamma - 1)\Gamma \cdot 2^{-\mu} \ll 1$, the error of Hamming weight t or less can be corrected with sufficiently large probability. For example for $t = 4$, $\mu = 128$, $\eta = 256$, the probability $P[C]$ is given by $p[C] = 1 - 4.4 \times 10^{-24}$.

It should be noted that for such parameters as $N = 16$, $K = 8$, $\lambda = 128$, $\eta = 256$, the size of the public key S_{PK} is given by

$$S_{PK} = 524 \text{ KB}, \tag{38}$$

sufficiently small size, compared with those in Table 1.

Remark 2: Let us suppose that K sets $S_1, S_2, \cdots, S_K$ are randomly chosen from the N sets of linear simultaneous equations $\{S_i\}$. The total number of choices of different K sets, $\binom{N}{K}$ can be made sufficiently small, because the random errors are added on the sets $S_1, S_2, \cdots, S_K$. Assuming that single error is added on each set of $S_1, S_2, \cdots, S_K$, the total number of different choices of K sets in addition to K single errors, N_E, is given by

$$N_E = \binom{N}{K}\eta^K. \tag{39}$$

For example, for $N = 16$, $K = 8$, $\eta = 256$, N_E takes on the value of 2×10^{23}, sufficiently large value. It should be noted that in K*(I)SE(1)PKC the size of public key can be made sufficiently small compared with that of K(I)SE(1)PKC. □

Remark 3 : As the K single errors can be decoded correctly, these single errors can be used for the transmitting of the message. The number of different ways of choices of the set of simultaneous equations can be also used for the transmission of the message. The total number of these additional messages is evidently given by $\log_2 N_E$. For example, for $N = 16$, $K = 8$, $\eta = 256$, $t = 1$, the messages of $\log_2 N_E \simeq 77$ bits can be transmitted. Thus the coding rate can be improved as follows:

$$\rho = \frac{125}{256} \ \rightarrow \ \rho = \frac{128 + 77}{256} = 0.80. \tag{40}$$

□

5. Conclusion

We have presented a new class of multivariate PKC. We have shown that our scheme is invulnerable to the various attack including LT(Linear Transformation) attack, due to the probabilistic structure that can be successfully introduced by the using of the Chinese Remainder Theorem.

We have shown that the K(I)SE(1)PKC has the following features.

(i) The ciphertext can be made secure against any attack provided that the degree of $G_i(x)$ is made sufficiently large ($\gtrsim 60$) and ${}_N C_K$ is also made sufficiently large ($\gtrsim 10^{18}$).

(ⅱ) One of the possible attack on the secret key would be the GB attack, one of the most strong attack on the multivariate PKC. However in K(I)SE(1)PKC, the number of variables constituting the quadratic polynomial takes on the extemely large value of at least 10^4, while the number of equations is about several thousands.

Thus we conclude that K(I)SE(1)PKC could be one of the candidates of the secure PKC's.

We have also presented a more secure version of K(I)SE(1)PKC, K*(I)SE(1)PKC.

We have shown that the security of K*(I)SE(1)PKC against the exhaustive attack can be improved due to the presence of error vector.

The author is thankful to the support of SCOPE.

References

[1] J. Ding, ”A New Variant of the MatsumotoImai Cryptosystem Constructed on through Pertubation”, PKC 2004, LNCS 2947, pp.305-318, 2004.

[2] J. C. Faugere, ”Algebraic cryptoanalysis of HFE using Gröbner bases”, Report de recherche, INRIA, No. 4738, (2003-02).

[3] 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).

[4] 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).

[5] M.Kasahara, ”A New Class of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials Randomly Generated”, Technical Report of IEICE, ISEC 2007 (2007-09).

[6] M.Kasahara, ”New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials”, 12-03, SITA 2007, Kashikojima, (2007-11).

[7] 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).

[8] N. Koblitz, ”Algebraic Aspect of Cryptography”, Springer Verlag, Berlin Heidelberg.

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

[10] 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).

[11] 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).

[12] 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).

[13] C. Wolf, A. Braekn, B. Preneel, ”Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC”, SCN 2004: 294-309, Lecture Notes in Computer Science 3352 Springer 2005.

[14] C. Wolf, ”Multivariate Quadratic Polynomials in Public Key Cryptography”, Dr, Thesis, (2005-11).

[15] M.Kasahara, ”Construction of New class of Linear Multivariate Public Key Cryptosystem - Along With a Node 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).