New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials and Random Coding
—Another class of K(III)・RSE(g)PKC—

2008年2月29日

大阪学院大学 情報学部
笠原 正雄

History

- Matsumoto-Imai : Quadratic Polynomial-Tuples PKC Euro Crypto. (1989)
  Algebraic
- Tsujii-Fujioka-Hirayama : Non-Linear Equation PKC (Moon Letter PKC) (1989)
  Triangular Random
- M.Kasahara : Application for Patent (Early 1990's)
  Algebraic
- J.Patarin : HFE, Euro Crypto (1996)
  Algebraic
- Kasahara-Sakai : 100bit Multivariate PKC (RSE(g)PKC, RSSE(g)PKC) (2004)
  Random, Step-wise linear
- Kasahara : K(Ⅰ) (2007-09), K(Ⅱ) (2007-11), K(Ⅲ) (2007-12), Generalized K(Ⅲ) (2008-02)

An Example of Multivariate PKC

$$m_i : \text{Message}, \ \boldsymbol{m} = (m_1, m_2, m_3, m_4)$$

$$C_i : \text{Ciphertext}, \ \boldsymbol{C} = (C_1, C_2, C_3, C_4)$$

$\boldsymbol{m}$ → Linear Transformation → Quadratic Transformation → $\boldsymbol{C}$

$t = 2$

$$\left.\begin{aligned} C_1 &= 1 + m_1 + m_1 m_2 + m_1 m_4 \\ C_2 &= m_2 + m_3 + m_2 m_4 + m_3 m_4 \end{aligned}\right\}$$

$$\left.\begin{aligned} C_3 &= m_4 + m_1 m_4 + m_3 m_4 \\ C_4 &= m_1 + m_2 + m_4 + m_1 m_2 + m_2 m_4 \end{aligned}\right\}$$

t : width of transformation

$$\text{Information transmission rate} = \frac{|\boldsymbol{x}|}{|\boldsymbol{C}|} = \frac{4}{4} = 1$$

Multivariate PKC(Algebraic)との出合い

大阪大学大学院 (1970〜1987)
京都工芸繊維大学大学院 (1987〜2000)
における講義「符号理論」の試験問題として以下の問題を頻繁に出題。

問 1. $G(X) = X^4 + X + 1$ に対応するフィードバック・シフトレジスタにおいて，任意の入力 $\alpha = (m_1, m_2, m_3, m_4)$ を得て，$\alpha^3 = (C_1, C_2, C_3, C_4)$ を出力する論理回路を設計せよ。

Multivariate PKC(Algebraic)との出合い

解. $(m_1 + m_2X + m_3X^2 + m_4X^3)^3$
$$\equiv C_1 + C_2X + C_3X^2 + C_4X^3 \mod G(X)$$
を解くことにより，以下が導かれる。

$$\begin{aligned}
C_1 &= m_1 + m_1m_3 + m_2m_3 + m_2m_4 \\
C_2 &= m_4 + m_1m_2 + m_1m_3 + m_3m_4 \\
C_3 &= m_3 + m_1m_2 + m_1m_3 + m_1m_4 + m_2m_3 + m_2m_4 + m_3m_4 \\
C_4 &= m_2 + m_3 + m_4 + m_2m_4 + m_3m_4
\end{aligned}$$

Structure of Conventional Multivariate PKC

$$[\boldsymbol{m}][A] \to [\varphi^{(2)}] \to [\varphi^{(2)}][B] \to [K]$$

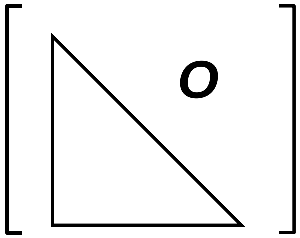
$$K = (k_1, k_2, \cdots, k_n)$$

k_i : Quadratic Equations

$\varphi^{(2)}$: Quadratic Transformation with trap-doors based on algebraic or random method

Structure of Conventional Multivariate PKC

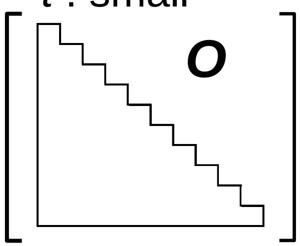
（Ⅰ）



- Tsukibumi (月文)
- Moh
- Algebraic (Gröbner basis変換)

（Ⅱ）

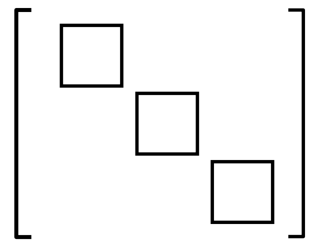
t : small



- RSE(g)
- RSSE(g)

（Ⅱ’）

t : large

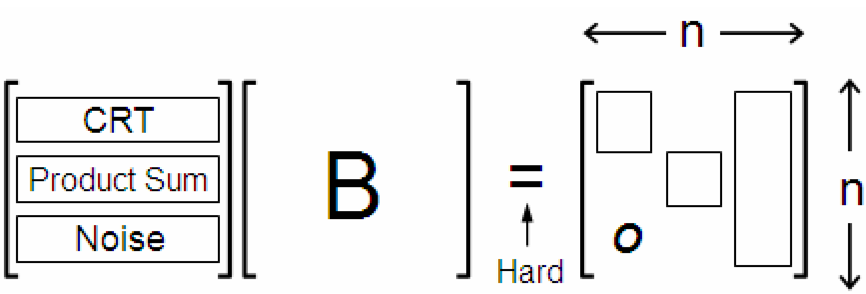


- K(Ⅰ)･RSE(g)

（Ⅲ）

$$\left[\ \varphi^{(2)}\ \right] \otimes \left[\text{Piece in Hand}\right]$$

- 持駒方式



- K(Ⅱ)･RSE(g)

K(＊)･RSE(g)PKC

I. K(Ⅰ)･RSE(g)PKC (2007-09)
  - Totally random quadratic transformation of a large width *t*
  - No triangular structure

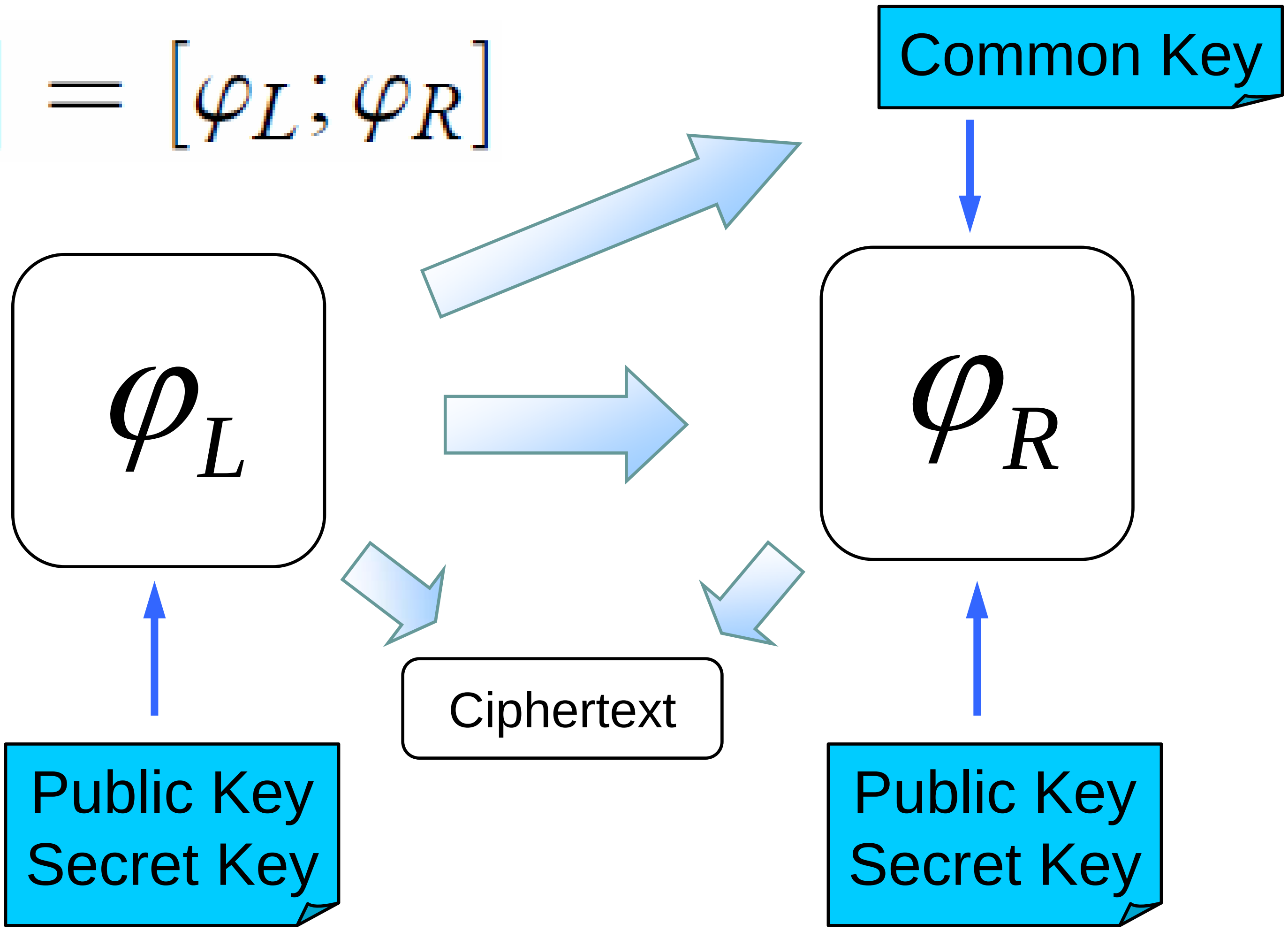
II. K(Ⅱ)･RSE(g)PKC (SITA･2007-11)
  - Chinese Remainder Theorem
  - Product sum type sub-ciphertext

III. K(Ⅲ)･RSE(g)PKC (2007-12)
  - Transformation by a random coding that depends on the message sequence

IV. RSE(g)PKC (2008-02)
  - Reducing the size of public key
    → Increase the number of variables
  - A new RSE(g) in Appendix

Structure of K(Ⅲ)・RSE(g)PKC

$$[\varphi] = [\varphi_L ; \varphi_R]$$



Messages over F_2

$$\boldsymbol{M}_{\boldsymbol{\rho}} = (M_1, M_2, \cdots, M_k, h_1, \cdots, h_e). \tag{1}$$

$$M_\rho = (m'_1, m'_2, \cdots, m'_{2n}). \tag{2}$$

The redundant message $\boldsymbol{M}_{\boldsymbol{\rho}}$ is transformed to vector $\boldsymbol{m}$ as follows

$$\boldsymbol{M}_{\boldsymbol{\rho}} \cdot A = \boldsymbol{m} = (m_1, m_2, \cdots, m_{2n}), \tag{3}$$

where $m_i \in \mathbb{F}_2$ and A is an $2n \times 2n$ non-singular matrix over $\mathbb{F}_2$.

Letting N be given by $2n/t$, the components of the vector $\boldsymbol{m}$ ai partitioned into N sub-vectors, yielding the following vectors:

$$\boldsymbol{m} = (\boldsymbol{m}_1; \boldsymbol{m}_2; \cdots; \boldsymbol{m}_N), \tag{4}$$

where $\boldsymbol{m}_i$ is given by

$$\boldsymbol{m}_i = (m_{i1}, m_{i2}, \cdots, m_{it}). \tag{5}$$

Mixture of two classes of transformation

$$\boldsymbol{m} = (\boldsymbol{m}_L; \boldsymbol{m}_R). \tag{8}$$

$$\boldsymbol{y}_L = (y_1, y_2, \cdots, y_n). \tag{9}$$

$$\boldsymbol{m} = (\boldsymbol{m}_L; \boldsymbol{m}_R) \quad \longmapsto \quad \boldsymbol{y} = (\boldsymbol{y}_L; \boldsymbol{y}_R). \tag{10}$$

Transformation $\chi(y_L \mid m_L)$

The transformation $\chi(\boldsymbol{y}_L \mid \boldsymbol{m}_L)$ can be performed in the various ways.

A generalized version of the transformation originally used in K(III)·RSE(g)PKC.:

$$
\begin{aligned}
y_1 &= y_1^{(g_1)}(m_1, m_2, \cdots, m_n), \\
&\vdots \\
y_i &= y_i^{(g_i)}(m_1, m_2, \cdots, m_n), \qquad (11)\\
&\vdots \\
y_n &= y_n^{(g_n)}(m_1, m_2, \cdots, m_n),
\end{aligned}
$$

where we assume that $g_i \geqq 1, (i = 1, \cdots, n)$.

Common Keys for $\phi(y_R \mid m_R)$

$$
\begin{aligned}
k_{n+1} &= k_1^{(g_{n+1})}(m_1, m_2, \cdots, m_n), \\
&\vdots \\
k_{n+i} &= k_i^{(g_{n+i})}(m_1, m_2, \cdots, m_n), \qquad (15) \\
&\vdots \\
k_{2n} &= k_n^{(g_{2n})}(m_1, m_2, \cdots, m_n),
\end{aligned}
$$

where we assume that $g_{(n+i)} \geqq 1, (i = 1, 2, \cdots, n)$.

The key vector is given as

$$
\boldsymbol{k}_R = (\boldsymbol{k}_{\nu+1}, \boldsymbol{k}_{\nu+2}, \cdots, \boldsymbol{k}_{2\nu}), \qquad (16)
$$

where $\boldsymbol{k}_i = (k_{(i-1)t+1}, \cdots, k_{it})$ and we assume that $\nu t = n$ holds.

An Example of Table

Table 1 Example of $T_{b(i)}$

m_1	m_2	m_3	y_1	y_2	y_3
0	0	0	1	0	1
0	0	1	1	1	0
0	1	0	0	1	0
0	1	1	1	0	0
1	0	0	0	0	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	0	0	0

Set of Keys

Public Keys : $\{k_i\}_L$ for transformation $\chi(\boldsymbol{y}_L \mid \boldsymbol{m}_L)$, $\{k_i\}_R$ for tables used for the transformation $\phi(\boldsymbol{y}_R \mid \boldsymbol{m}_R)$

Secret Keys : ϕ, χ, A, B

Common Keys : $\{T_{b(i)}\}$

Ciphertext

In the following, $x_i = \tilde{x}_i$ implies that the variable x_i takes on the value $\tilde{x}_i$.

Let $k_i \in \{k_i\}_L$ be denoted by

$$k_i = k_i^{(g_i)}(m_1, m_2, \cdots, m_n). \tag{17}$$

Letting the ciphertext $\boldsymbol{C}$ be represented by $\boldsymbol{C} = (\boldsymbol{C}_L, \boldsymbol{C}_R)$, the ciphertext $\boldsymbol{C}_L$ is given by

$$\boldsymbol{C}_L = (C_1, C_2, \cdots, C_n), \tag{18}$$

where $C_i = k_i^{(g_i)}(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n)$.

On the other hand ciphertext $\boldsymbol{C}_R = (\boldsymbol{C}_{\nu+1}, \boldsymbol{C}_{\nu+2}, \cdots, \boldsymbol{C}_{2\nu})$ is given simply by

$$\boldsymbol{C}_i = \tilde{\boldsymbol{y}}_i, (\nu + 1 \leq i \leq 2\nu), \tag{19}$$

Security Consideration

Theorem 1 : Ciphertext $(\tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_n)$ yields no information on message $(\tilde{m}_{n+1}, \tilde{m}_{n+2}, \cdots, \tilde{m}_{2n})$.

Proof : We have

$$H(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_{2n}) = 2n(\text{bits}) \tag{33}$$

From Eq.(11), it is evident that the following relation hold:

$$H(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n \mid \tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_n) = 0(\text{bits}) \tag{34}$$

From Eqs.(33) and (34), it is easy to see that

$$\begin{aligned} &H(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_{2n} \mid \tilde{y}_1, \tilde{y}_2, \cdots, \tilde{y}_n) \\ &= H(\tilde{m}_{n+1}, \tilde{m}_{n+2}, \cdots, \tilde{m}_{2n}) \\ &= n(\text{bits}) \end{aligned} \tag{35}$$

holds, yielding the proof. $\square$

Attack I

Attack I: Given the set of public keys $y_1, y_2, \cdots, y_n$,

Attack I discloses $m_1, m_2, \cdots, m_n$. $\square$

$$
\begin{aligned}
m_1 &= \beta_{11} m'_1 + \beta_{12} m'_2 + \cdots + \beta_{1,2n} m'_{2n}, \\
m_2 &= \beta_{21} m'_1 + \beta_{22} m'_2 + \cdots + \beta_{2,2n} m'_{2n}, \\
&\vdots \\
m_t &= \beta_{t1} m'_1 + \beta_{t2} m'_2 + \cdots + \beta_{t,2n} m'_{2n}.
\end{aligned} \tag{37}
$$

Attack I (Continue)

$$
\begin{aligned}
y_1 &= \alpha_{11}m_1 + \cdots + \alpha_{1t}m_t + \alpha_{1,(1,2)}m_1m_2 + \cdots \\
&\quad + \alpha_{1,(t-1,t)}m_{t-1}m_t, \\
&\vdots \\
y_u &= \alpha_{u1}m_1 + \cdots + \alpha_{ut}m_t + \alpha_{u,(1,2)}m_1m_2 + \cdots \\
&\quad + \alpha_{u,(t-1,t)}m_{t-1}m_t, \\
y_t &= \alpha_{t1}m_1 + \cdots + \alpha_{tt}m_t + \alpha_{t,(1,2)}m_1m_2 + \cdots \\
&\quad + \alpha_{t,(t-1,t)}m_{t-1}m_t,
\end{aligned} \tag{38}
$$

where $m_i = \beta_{i_1}m'_1 + \beta_{i_2}m'_2 + \cdots + \beta_{i,2n}m'_{2n}$.

Attack I (Continue)

$$\lambda_{p,q} = \sum_{i=1}^{t} \sum_{j=i+1}^{t} \alpha_{u,(i,j)} (\beta_{ip}\beta_{jq} + \beta_{iq}\beta_{jp}). \tag{40}$$

In a similar manner, the coefficient of m'_p in y_u, λ_p, is given by

$$\lambda_p = \sum_{i=1}^{t} \sum_{j=i+1}^{t} \alpha_{u,(i,j)}\beta_{ip}\beta_{jp} + \sum_{j=1}^{t} \alpha_{u_j}\beta_{jp}. \tag{41}$$

"One of the advantage of K(IV)·RSE(g)PKC is that for any given ciphertext, $\tilde{k}_R = (\tilde{k}_{v+1}, \tilde{k}_{v+2}, \cdots, \tilde{k}_{2v})$ is not explicity given."

Numbers of Variables and Equations

The total number of variables in the cubic equations is given by

$$N_V = {}_tH_2 \cdot t + 2nt. \tag{42}$$

The total number of cubic equations obtained from the coefficients of quadratic equations $y_1, y_2, \cdots, y_n$, N_E, is given by

$$N_E = {}_{2n}H_2 \cdot t. \tag{43}$$

K(III)·RSE(g)PKC in more variables

According to the difining of the degrees given in Eqs.(33), let us slightly modify the transformation $\chi(\boldsymbol{y}_L \mid \boldsymbol{m}_L)$ and $\phi(\boldsymbol{y}_R \mid \boldsymbol{m}_R)$ as described below:

K(III)·RSE(g)PKC

$$\begin{aligned} y_1 &= y_1^{(1)}(m_1, m_2, \cdots, m_{n-t}) \\ &\vdots \\ y_{n-t} &= y_{n-t}^{(1)}(m_1, m_2, \cdots, m_{n-t}) \end{aligned} \tag{34}$$

$$\begin{aligned} y_{n-t+1} &= y_{n-t+1}^{(2)}(m_1, m_2, \cdots, m_{n-t}, m_{n-t+1}, \cdots, m_n) \\ &\vdots \\ y_n &= y_n^{(2)}(m_1, m_2, \cdots, m_{n-t}, m_{n-t+1}, \cdots, m_n) \end{aligned} \tag{35}$$

Letting D be an $n \times n$ matrix over $\mathbb{F}_2$ we have

$$(m_1, m_2, \cdots, m_{n-t}, m_{n-t+1}, \cdots, m_n)D = (\underline{m}_1, \underline{m}_2, \cdots, \underline{m}_n) \tag{36}$$

K(III)·RSE(g)PKC in more variables (continue)

As elements of the set of $\{k_i\}_R$, we have

$$\begin{aligned} k_{n+1} &= k^{(1)}_{n+1}(\underline{m}_1, \underline{m}_2, \cdots, \underline{m}_n) \\ &\vdots \\ k_{2n-s} &= k^{(1)}_{2n-s}(\underline{m}_1, \underline{m}_2, \cdots, \underline{m}_n) \end{aligned} \tag{37}$$

$$\begin{aligned} k_{2n-s+1} &= k^{(2)}_{n-s+1}(\underline{m}_1, \underline{m}_2, \cdots, \underline{m}_n) \\ &\vdots \\ k_{2n} &= k^{(2)}_{2n}(\underline{m}_1, \underline{m}_2, \cdots, \underline{m}_n) \end{aligned} \tag{38}$$

Example 3

Example 3: $2n = 160$, $t = 60$, $s = 0$

The sizes of public keys $\{k_i\}_L$ and $\{k_i\}_R$ are given by

$$S_{PK,L} = 2n \cdot (n - t) + {}_{2n}H_2 \cdot t$$
$$= 772.8(\text{Kbit})$$

and

$$S_{PK,R} = 2n^2$$
$$= 128(\text{Kbit})$$

respectively.

The total size of public key, S_{PK}, is given by

$$S_{PK} = S_{PK,L} + S_{PK,R} = 785.6(\text{Kbit})$$

Example 4

Example 4: $2n = 256$, $t = 8$, $s = 0$

The sizes of public keys $\{k_i\}_L$ and $\{k_i\}_R$ are given by

$$S_{PK,L} = 2n \cdot (n-t) + {}_{2n}H_2 \cdot t$$
$$= 63.616(\mathrm{Kbit})$$

and

$$S_{PK,R} = 2n^2$$
$$= 131.072(\mathrm{Kbit})$$

The total size of public key is given by

$$S_{PK} = S_{PK,L} + S_{PK,R} = 194.688(\mathrm{Kbit})$$

The number of variables takes on a large value of 256, while the size of public key, a smaller value than that of the conventional SE(2) with the same number of variables by a factor of 43.1.

Attack Ⅱ

When $t = s = 0$, the sets of keys and the simultaneous equations are given by the following linear equations:

$$\left.\begin{aligned} k_{n+1} &= k_1^{(1)}(m_1, m_2, \cdots, m_n) \\ &\vdots \\ k_{2n} &= k_n^{(1)}(m_1, m_2, \cdots, m_n) \end{aligned}\right\} \{k_i\}_R$$

$$\left.\begin{aligned} y_1 &= y_1^{(1)}(m_1, m_2, \cdots, m_n) \\ &\vdots \\ y_n &= y_n^{(1)}(m_1, m_2, \cdots, m_n) \end{aligned}\right\} \{k_i\}_L \tag{39}$$

Attack Ⅱ (continue)

Thus the following linear transformation evidently exists:

$$(y_1, \cdots, y_n)W = (k_1, k_2, \cdots, k_n), \tag{40}$$

where W is an $n \times n$ matrix over $\mathbb{F}_2$ given by

$$\begin{bmatrix} w_{11} & w_{21} & \dots & w_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{1n} & w_{2n} & \dots & w_{nn} \end{bmatrix} \tag{41}$$

Remark: Direct attack can be also successful.

Concluding remarks

(1) A new trap-door is given. That is the "time variant" transformation $\phi(\boldsymbol{y}_R \mid \boldsymbol{m}_R)$ is used.

(2) The transformation $\phi^{(2)}$ can be given in various ways. For example, the totally random quadratic transformation of large width t $(20 \lesssim t \lesssim 40)$ or a common key cryptosystem can be used.

(3) Gröbner basis attack would find it very hard to solve RSE(2) used in K(III)·RSE(2)PKC as the public key and the common key.

(4) A new class of PKC is presented in Appendix 1.

Another Class of RSE(g)PKC

$$\boldsymbol{m}_L = (\boldsymbol{m}_{LL}; \boldsymbol{m}_{LR}), \qquad (\mathrm{A}\cdot 1)$$

For the transformation of $\chi_L(\boldsymbol{y}_{LL} \mid \boldsymbol{m}_{LL})$,

$$\begin{aligned} y_1 &= y_1^{\boxed{(g_1)}}(m_1, m_2, \cdots, m_v) \\ &\;\vdots \qquad\qquad\qquad\qquad\qquad\qquad (\mathrm{A}\cdot 2) \\ y_v &= y_v^{\boxed{(g_v)}}(m_1, m_2, \cdots, m_v) \end{aligned}$$

is constructed.

For the transformation $\chi_L(\boldsymbol{y}_{LR} \mid \boldsymbol{m}_{LR})$,

$$\begin{aligned} y_{v+1} &= y_{v+1}^{(1)}(m_{v+1}, \cdots, m_{2v}) + r_{rand,v+1}^{(2)}(m_1, \cdots, m_L) \\ &\;\vdots \qquad\qquad\qquad\qquad\qquad\qquad (\mathrm{A}\cdot 3) \\ y_{2v} &= y_{2v}^{(1)}(m_{v+1}, \cdots, m_{2v}) + r_{rand,2v}^{(2)}(m_1, \cdots, m_v) \end{aligned}$$

is constructed where $r_{rand,v+1}^{(2)}(m_1, \cdots, m_v) \cdots r_{rand,2v}(m_1, \cdots, m_v)$ are totally random quadratic equations.