New Classes of Public Key Cryptosystem Constructed on the Basis of Multivariate Polynomials

大阪学院大学 情報学部
笠原 正雄

Introduction

In this paper we shall try to improve SE(g)PKC by considering the followings:

1. Introducing a large randomness by using a random transformation ($g \geq 2$) with large width [14].

2. Letting the number of variables be larger than that of equations.

3. Using new trap doors on the basis of Chinese Remainder Theorem(CRT) and product sum operation.

4. Jointly improving the problem of the shortening of the size of public key and the increasing of the number of variables.

An Example of Multivariate PKC

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

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

m → Linear Transformation → Quadratic Transformation → **C**

$$t = 2$$

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

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

t : width of transformation

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

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)

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. $(m_1 + m_2 X + m_3 X^2 + m_4 X^3)^3$
$$\equiv C_1 + C_2 X + C_3 X^2 + C_4 X^3 \mod G(X)$$
を解くことにより, 以下が導かれる。

$$
\begin{aligned}
C_1 &= m_1 + m_1 m_3 + m_2 m_3 + m_2 m_4 \\
C_2 &= m_4 + m_1 m_2 + m_1 m_3 + m_3 m_4 \\
C_3 &= m_3 + m_1 m_2 + m_1 m_3 + m_1 m_4 + m_2 m_3 + m_2 m_4 + m_3 m_4 \\
C_4 &= m_2 + m_3 + m_4 + m_2 m_4 + m_3 m_4
\end{aligned}
$$

Structure of Conventional Multivariate PKC

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

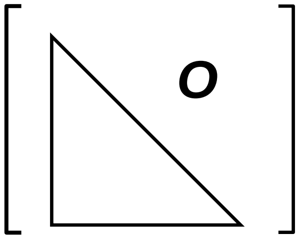
$$K = (k_1, k_2, \cdots, k_n)$$

k_i : Quadratic Equations

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

Structure of Conventional Multivariate PKC

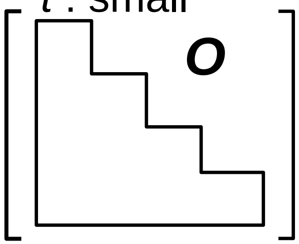
(Ⅰ)



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

(Ⅱ)

t : small



- RSE(g)
- RSSE(g)

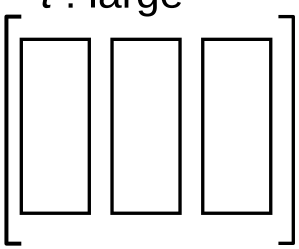
(Ⅲ)

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

- 持駒方式

(Ⅳ)

t : large



- K(Ⅰ)･RSE(g)
  (ISEC, Sept.2007)

K(＊)･RSE(g)PKC

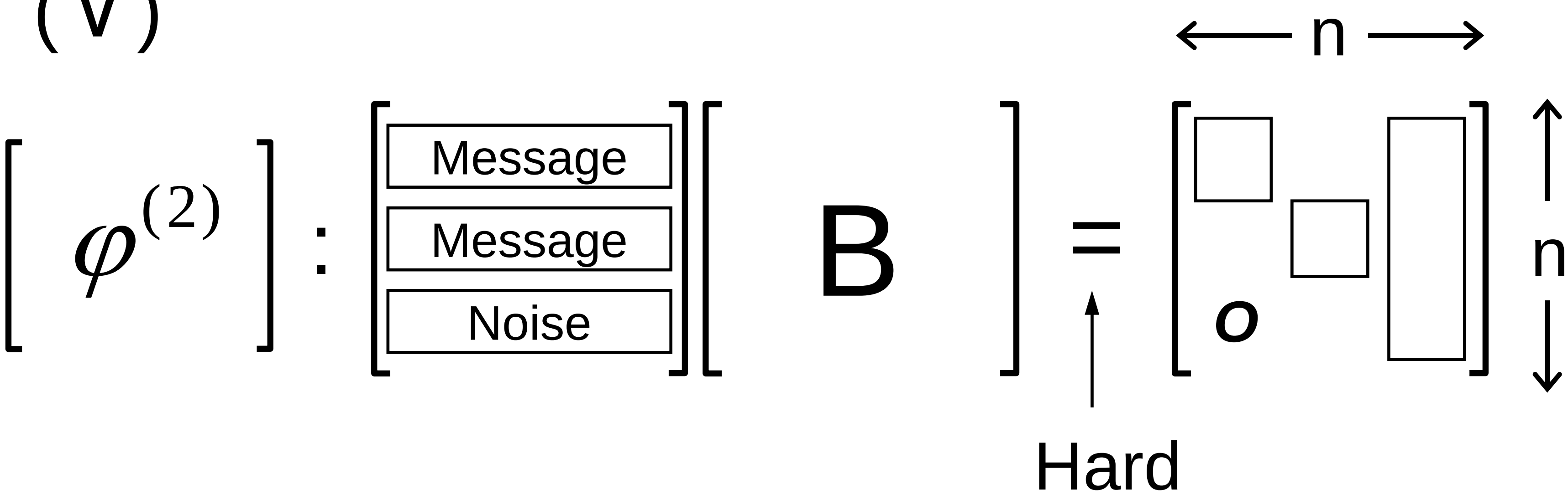
I. K(Ⅰ)･RSE(g)PKC (2007-09)
- Totally random quadratic transformation of a large width t → Singular Transformation
- Number of repetition of decoding due to singular transformation can be made sufficiently small
- No triangular structure

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

III. K(Ⅲ)･RSE(g)PKC (2007-12)
- Transformation by a random coding that depends on the message sequence
- Totally random quadratic transformation of a large width t .

Structure of K(Ⅱ)・RSE(g)PKC

(Ⅴ)



Message：Message derived on the basis of Chinese Remainder Theorem

Noise：Product sum type sub-ciphertext

(Remark：Noise can be replaced by message)

Examples Related to K(Ⅱ)･RSE(g)PKC

$$
\begin{aligned}
C_1 &= 1 + m_1 + m_1m_2 + m_2r_1 + m_3r_2 \\
C_2 &= 1 + m_2 + m_2m_3 + m_1r_2 \\
C_3 &= m_3 + m_2r_1 + r_2r_3
\end{aligned}
$$

Number of equations : 3
Number of variables : 6
Number of messages : 3

Chinese Remainder Theorem

$$
\begin{aligned}
x &\equiv 2 \pmod{3} \\
&\equiv 3 \pmod{5} \\
&\equiv 2 \pmod{7}
\end{aligned}
$$

$$x \equiv ?$$

『孫子算経』

Summary

In this paper we shall try to improve SE(g)PKC by considering the followings:

1. Introducing a large randomness by using a random transformation ($g \geq 2$) with large width [14].

2. Letting the number of variables be larger than that of equations.

3. Using new trap doors on the basis of Chinese Remainder Theorem(CRT) and product sum operation.

4. Jointly improving the problem of the shortening of the size of public key and the increasing of the number of variables.

Message and Random Vectors

Redundant message vector:

$$\mathbf{M}_{\rho} = \left(M_1, M_2, \cdots, M_k, h_1, \cdots h_g\right). \qquad (1)$$

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

$$\mathbf{M}_{\rho} \cdot A = \mathbf{m} = \left(m_1, m_2, \cdots, m_n\right), \qquad (2)$$

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

$$\mathbf{m} = (m_1; m_2; \cdots; m_N). \qquad (3)$$

$$\mathbf{m}_i = (m_{i1}; m_{i2}; \cdots; m_{it}). \qquad (4)$$

Random vector over $\mathbf{F}_2$:

$$\mathbf{r} = \left(r_1, r_2, \cdots, r_L\right). \qquad (5)$$

$$\mathbf{r}_i = \left(r_{i1}, r_{i2}, \cdots, r_{it}\right). \qquad (6)$$

Definition 1

The following transformation:

$$\Phi(X) = Y, \qquad (7)$$

is referred to as "non-singular", if and only if the transformation has the following inverse transformation:

$$\Phi^{(-1)}(Y) = X, \qquad (8)$$

for any given Y in a unique manner. On the other hand if the inverse-transformed value does not exist in a unique manner, for a given Y, the transformation is referred to as "singular".

Random Transformation $\phi^{(2)}$

Given $\mathbf{m}_i$ $(i = 1,2,\cdots,N)$ the following transformation $\phi^{(2)}$ is performed on the basis of randomness.

$$
\begin{aligned}
y_{i1} &= \phi^{(2)}_{i1}(m_{i1}, m_{i2}, \cdots, m_{it}), \\
&\vdots \\
y_{ij} &= \phi^{(2)}_{ij}(m_{i1}, m_{i2}, \cdots, m_{it}), \qquad (9) \\
&\vdots \\
y_{it} &= \phi^{(2)}_{it}(m_{i1}, m_{i2}, \cdots, m_{it}).
\end{aligned}
$$

For the random vector, $\boldsymbol{r}_i$ (i = $1,2,\cdots,L$), the component, r_{ij} is given by

$$r_{ij} = \phi^{(2)}\left(m_1, \cdots, m_n, v_1, \cdots, v_u\right) \qquad (11)$$

where v_i is a random component over $\mathbf{F}_2$ independent of the messages $m_1, m_2, \cdots, m_n$.

Example of Random Transformation

$$\overset{\text{message}}{(m_1, m_2, m_3)} \to \overset{\text{key}}{(y_1, y_2, y_3)} : t = 3$$

$$\begin{aligned}
y_1 &= \gamma_{11}m_1 + \gamma_{12}m_2 + \gamma_{13}m_3 + \gamma_{14}m_1m_2 + \gamma_{15}m_1m_3 + \gamma_{16}m_2m_3 \\
y_2 &= \gamma_{21}m_1 + \gamma_{22}m_2 + \gamma_{23}m_3 + \gamma_{24}m_1m_2 + \gamma_{25}m_1m_3 + \gamma_{26}m_2m_3 \\
y_3 &= \gamma_{31}m_1 + \gamma_{32}m_2 + \gamma_{33}m_3 + \gamma_{34}m_1m_2 + \gamma_{35}m_1m_3 + \gamma_{36}m_2m_3
\end{aligned}$$

γ_{ji} : 0,1 random number

K(I)RSE(g)PKC uses a transformation of large t ($20 \lesssim t \lesssim 40$).

Number of Repetition of Decoding due to singularity of ϕ

$N(\boldsymbol{x}_t \mid \boldsymbol{y}_t)$: Number of different $\boldsymbol{x}_t$'s excluding the valid $\boldsymbol{x}_t$ given randomly to $\boldsymbol{y}_t$.

$P_N(i)$: Probability that $N(\boldsymbol{x}_t \mid \boldsymbol{y}_t)$ takes on value i.

$$P_N(0) = \left(1 - \frac{1}{2^n - 1}\right)^{2^n - 1} \cong \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \cdots \qquad (18)$$

$$= e^{-1} = 0.3679$$

In general, P_N(i) is given by

$$P_N(i) \cong \frac{1}{i!} P_N(0) \qquad (19)$$

Thus, the expectation of the number of possible candidates, excluding valid one for a given $\boldsymbol{y}_t$, $E(\boldsymbol{x}_t)$, is given by

$$E(\mathbf{x}_t) \cong e \cdot P_N(0) = 1 \qquad (20)$$

Base Polynomials

Let us define the following base-polynomials

$$B_i(X) = \prod_{j \neq 1}^{N} P_j(X) \left\{ \left(\prod_{j \neq 1}^{N} P_j(X) \right)^{-1} \bmod P_i(X) \right\} Q_i(X), (1 \leq i \leq N) \quad (21)$$

and

$$D_i(X) = \prod_{j=1}^{N} P_j(X) T_i(X), (1 \leq i \leq L) \quad (22)$$

$$\deg P_i(X) = t \quad (23)$$

$$\deg Q_i(X) = t + 1 \quad (24)$$

$$\deg T_i(X) = t \quad (25)$$

Several Parameters

Let us define the symbols:

N_c : size of ciphertext

N_v : number of variables

ρ : information rate

S_{pk} : size of public keys

We see that the following relation holds:

$$N_c = (N+2)t$$

$$N_v = n + u$$

$$\rho = k/(k+g)$$

$$S_{pk} = {}_{N_v}H_2 \cdot N_c \text{ (bits)}$$

Construction of Public Keys

Given $\{m_i(X)\}$ and $\{r_i\}$ the following polynomial, intermediate polynomials, is constructed :

$$Z(X) = \sum_{i=1}^{N} y_i(X)B_i(X) + \sum_{i=1}^{L} r_i(X)D_i(X) \qquad (26)$$

$$= z_1 + z_2(X) + \cdots + {}_{zN_c}X^{N_c-1} \qquad (27)$$

$$z = (z_1, z_2, \cdots, z_{N_C}). \qquad (28)$$

$$zB = (K_1, K_2, \cdots, K_{N_C}), \qquad (29)$$

where B is an $n \times n$ non-singular matrix over $\mathbf{F}_2$.

Public Keys : $\{K_i\}$
Secret Keys : $\phi^{(2)}$, A , B

Encryption

$$K_i = k_i^{(2)}(m_1, m_2, \cdots, m_n, v_1, \cdots, v_u)\,. \qquad (30)$$

Assuming that the variable m_i and v_j takes on the value $\tilde{m}_i$ and $\tilde{v}_j$ respectively, the ciphertext is given by

$$\mathbf{C} = (C_1, C_2, \cdots, C_n)\,, \qquad (31)$$

where C_i is given by

$$C_i = k_i^{(2)}(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n, \tilde{v}_1, \cdots, \tilde{v}_u)\,. \qquad (32)$$

Decryption

Step 1: Given $\boldsymbol{C} = (C_1, C_2, \cdots, C_n)$, the inversed version of $\boldsymbol{C}$, $\tilde{\boldsymbol{z}}$ is given by $\tilde{\boldsymbol{z}} = \boldsymbol{C}B^{-1}$, yielding $\hat{Z}(X)$.

Step 2: Message $\hat{m}_i(X)$ is decoded as $\hat{Z}(X) \equiv \hat{y}_i(X) \bmod P_i(X)$. All the decoded $\hat{y}_i(X)'s$ are decoded in general several ways with table-look up method, yielding a set of candidates for $\hat{m}$'s, $S_{\hat{m}}$.

Step 3: From $\hat{\boldsymbol{m}} = (\boldsymbol{m}_i; \boldsymbol{m}_2; \cdots; \boldsymbol{m}_N) \in S_{\hat{m}}$, redundant message $\hat{\boldsymbol{M}}_\rho$ is decoded as $\hat{m}A^{-1}$, yielding $(\hat{M}_1, \hat{M}_2, \cdots, \hat{M}_k, \hat{h}_1, \cdots, \hat{h}_g)$.

Step 4: The decrypted version of the hashed value of $\hat{\boldsymbol{M}}$, $h(\hat{M}_1, \hat{M}_2, \cdots, \hat{M}_k)$, is compared with $(\hat{h}_1, \hat{h}_2, \cdots, \hat{h}_k)$. When $h(\hat{M}_1, \hat{M}_2, \cdots, \hat{M}_k)$ and $(\hat{h}_1, \hat{h}_2, \cdots, \hat{h}_k)$ are coincident, then $\boldsymbol{M}$ is decoded as $(\hat{M}_1, \hat{M}_2, \cdots, \hat{M}_k)$. If not, another candidate is chosen and go back to Step 3.

Table 1

Table 1: Examples of K(II)·RSE(g)PKC

Example	n	u	t	N	L	N_c	N_v	S_{pk}	ρ
I	120	120	20	6	6	160	240	578KB	0.563
II	150	150	30	5	5	210	300	1.18MB	0.571
III	180	180	30	6	6	240	360	1.95MB	0.625
IV	120	120	30	4	2	180	180	366.5KB	0.833

K(II)·RSE(g)PKC with reduced terms

Given the messages $\{M_i\}$ and the hashed values $\{h_i\}$, and random components $\{v_i\}$, the subset $\{M'_i\}$, $\{h'_i\}$, $\{v'_i\}$ are constructed so that $\{M'_i\} \subset \{M_i\}$, $\{h'_i\} \subset \{h_i\}$, $\{v'_i\} \subset \{v_i\}$ may be satisfied.

Letting any element of $\{M'_i, h'_j, v'_i\}$ be α_i and the order of $\{M'_i, h'_j, v_i\}$, λ, the random component r_{ij} of $\boldsymbol{r}_i$ is now given by

$$\boldsymbol{r}'_{ij} = \phi^{(2)}(\alpha_1, \alpha_2, \cdots, \alpha_\lambda) \tag{33}$$

$$S'_{pk} = ({}_\lambda H_2 + (n + u - \lambda))N_c \quad (bits). \tag{34}$$

Table 2

Table 2: Examples of $\tilde{K}$(II)·RSE(g)PKC

Example	n	u	t	N	L	λ	N_c	N_v	S'_{pk}	S'_{pk}/S_{pk}	ρ	No. of quadratic terms
I	120	120	20	6	6	80	160	240	68.0KB	0.116	0.563	3160
II	150	150	30	5	5	100	210	300	137.8KB	0.117	0.571	4950
III	180	180	30	6	6	120	240	360	225.0KB	0.115	0.625	7140
IV	120	120	30	4	2	80	180	180	76.5KB	0.205	0.833	3160
V	340	340	20	17	17	180	380	680	797.5KB	0.07	0.816	16290

Concluding remarks

1. For the transformation $\phi^{(2)}$, the totally random quadratic transformation of large width $(20 \leq t \leq 40)$ is used.
2. Number of variables is larger than that of equations by 80 $\sim$ 300, except Examples IV in Table 1, as shown in Tables1 and 2.
3. New trap-doors are used on the basis of Chinese Remainder Theoram and product sum operation.