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

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)

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**

$$
\begin{aligned}
C_1 &= 1 + m_1 + m_1 m_2 + m_1 m_4 \\
C_2 &= m_2 + m_3 + m_2 m_4 + m_3 m_4 \\
C_3 &= m_4 + m_1 m_4 + m_3 m_4 \\
C_4 &= m_1 + m_2 + m_4 + m_1 m_2 + m_2 m_4
\end{aligned}
\quad \left.\right\} t = 2
$$

t : width of transformation

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

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

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

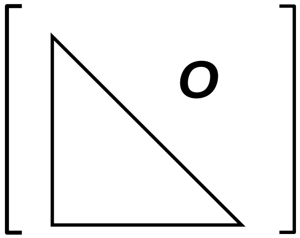
$$K = (k_1, k_2, \cdots, k_n)$$

k_i : Quadratic Equations

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

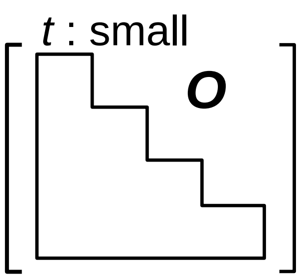
Structure of Conventional Multivariate PKC

(Ⅰ)



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

(Ⅱ)



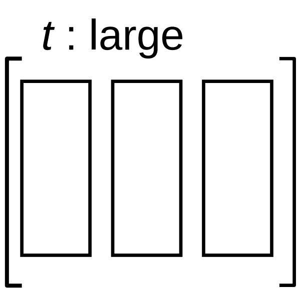
- RSE(g)
- RSSE(g)

(Ⅲ)

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

- 持駒方式

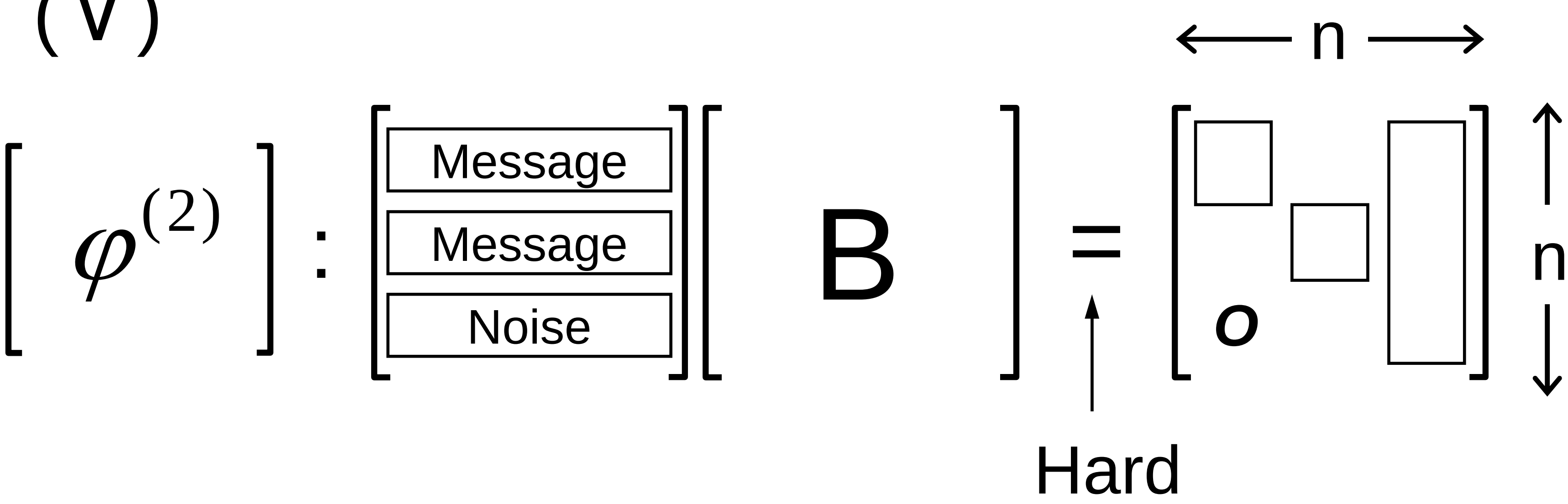
(Ⅳ)



- K(Ⅰ)･RSE(g)
  (ISEC, Sept.2007)

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)

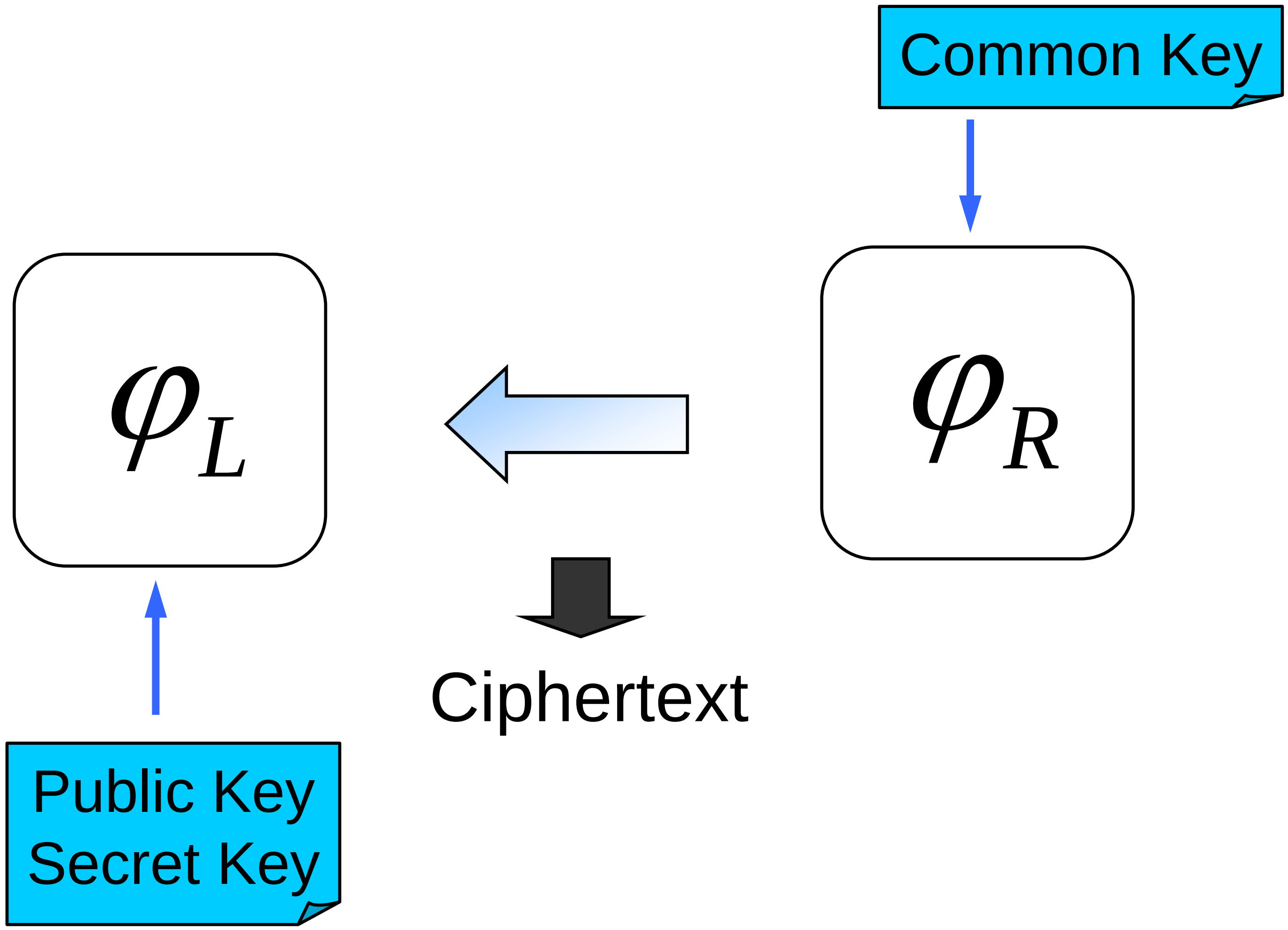
K(＊)･RSE(g)PKC

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(Ⅲ)･RSE(g)PKC



Messages over F_2

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

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

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

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

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 $\boldsymbol{m}$ ar partitioned into N sub-vectors, yielding the following vectors:

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

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

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

Mixture of two classes of transformation

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

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

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

$\chi(y_L / m_L)$

$$
\begin{aligned}
y_1 &= y_1^{(2)}(m_1, m_2, \cdots, m_n), \\
&\vdots \\
y_i &= y_i^{(2)}(m_1, m_2, \cdots, m_n), \\
&\vdots \\
y_n &= y_n^{(2)}(m_1, m_2, \cdots, m_n),
\end{aligned}
\tag{11}
$$

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

$$
\begin{aligned}
k_{n+1} &= k^{(2)}_{1,rand}(m_1, m_2, \cdots, m_n), \\
&\vdots \\
k_{n+i} &= k^{(2)}_{i,rand}(m_1, m_2, \cdots, m_n), \\
&\vdots \\
k_{2n} &= k^{(2)}_{n,rand}(m_1, m_2, \cdots, m_n),
\end{aligned} \tag{12}
$$

,yielding the key vector as

$$
\boldsymbol{k}_R = (\boldsymbol{k}_{\nu+1}, \boldsymbol{k}_{\nu+2}, \cdots, \boldsymbol{k}_{2\nu}), \tag{13}
$$

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 $\chi(\boldsymbol{y}_L \mid \boldsymbol{m}_L)$

Secret Keys : ϕ, χ, A, B

Common Keys : $\{T_{b(i)}\}, \{k_i\}_R$ for tables used for the transformation $\phi(\boldsymbol{y}_R \mid \boldsymbol{m}_R)$

Ciphertext

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

$$k_i = k_i^{(2)}(m_1, m_2, \cdots, m_n). \tag{19}$$

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

$$\boldsymbol{C}_L = (C_1, C_2, \cdots, C_n), \tag{20}$$

where $C_i = k_i^{(2)}(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n)$.

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

$$\boldsymbol{C}_i = \tilde{\boldsymbol{y}}_i, (\nu + 1 \leq i \leq 2\nu). \tag{21}$$

Example 1

Example 1: $2n = 168, t = 6, n = 84$

Size of public key and total sizes of Tables, $|T|$, are given by

$$S_{pk} = {}_{168}H_2 \cdot 84 = 113.6(\mathrm{KB}). \tag{28}$$

$$|T| = \frac{84}{6} \cdot 2^6(6 + 2 \cdot 2^6) = 11.43(\mathrm{KB}). \tag{29}$$

Example 2

Example 2: $n = 160, k = 130, n = 80, t = 10, e = 30$

Size of public key and total sizes of Tables, $|T|$ are given by

$$S_{pk} = {}_{160}H_2 \cdot 80 = 128.8(\mathrm{KB}). \tag{30}$$

$$|T| = \frac{80}{10} \cdot 2^{10}(10 + 2^{11}) = 2.107(\mathrm{MB}). \tag{31}$$

The information rate ρ is given by

$$\rho = 0.80. \tag{32}$$

Assumptions

A1 : Messages $M_1, M_2, \cdots, M_k$ are mutually independent and equally likely

A2 : Hash function of message is ideal. Namely hashed values, $h_1, h_2, \cdots, h_e$ are mutually independent and equally likely, yielding no information on messages $M_1, M_2, \cdots, M_k$.

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)

$$
\begin{aligned}
y_1 &= \alpha_{11} m_1 + \cdots + \alpha_{1t} m_t + \alpha_{1,(1,2)} m_1 m_2 + \cdots \\
&\quad + \alpha_{1,(t-1,t)} m_{t-1} m_t, \\
&\vdots \\
y_u &= \alpha_{u1} m_1 + \cdots + \alpha_{ut} m_t + \alpha_{u,(1,2)} m_1 m_2 + \cdots \\
&\quad + \alpha_{u,(t-1,t)} m_{t-1} m_t, \\
y_t &= \alpha_{t1} m_1 + \cdots + \alpha_{tt} m_t + \alpha_{t,(1,2)} m_1 m_2 + \cdots \\
&\quad + \alpha_{t,(t-1,t)} m_{t-1} m_t.
\end{aligned} \tag{38}
$$

Attack I (Continue)

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

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

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

"One of the advantage of K(III)·RSE(g)PKC is that for any given ciphertext, $\tilde{k}_R = (\tilde{k}_{\nu+1}, \tilde{k}_{\nu+2}, \cdots, \tilde{k}_{2\nu})$ 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

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

Example 3

Example 3: $2n = 160, t = 6$

The total number of variables is given by

$$N_V = {}_6H_2 \cdot 6 + 160 \cdot 6 = 1086.$$

The total number of cubic equations is given by

$$N_E = {}_{160}H_2 \cdot 6 = 77280. \qquad \square$$

Example 4

Exaple 4: $2n = 168, t = 28, e = 30$

The total number of variables is given by

$$N_V = {}_{28}H_2 \cdot 28 + 168 \cdot 20 = 14728.$$

The total number of cubic equations is given by

$$N_E = {}_{168}H_2 \cdot 28 = 397488.$$

The information rate ρ is given by

$$\rho = 0.82. \qquad \square$$

Number of Variables and Equations

The total number of variables, N_V and the total number of cubic equations, N_E are approximately given by

$$N_V = \frac{2}{3}n^2 \quad (44)$$

$$N_E = \frac{2}{3}n^3 \quad (45)$$

Thus N_E is given approximately by $N_V^{1.5}$ $(< \epsilon N_V^2$ for sufficiently large $N_V)$.

Concluding remarks

The K(III)·RSE(g)PKC seems secure due to the following reasons:

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

(2) New trap-doors is given. That is the "time variant" transformation $\phi(\boldsymbol{y}_R \mid \boldsymbol{m}_R)$ is used.

(3) Gröbner basis attack would find it very hard to solve RSE(2) used as the public key and the common key. The reason is that the solving RSE(2) used in K(III)·RSE(g)PKC is equivalent to the solving of large number of cubic RSE(RSE(3)) in so many variables.