Public Key Cryptosystems Constructed Based on Random Pseudo Cyclic Codes, K(IX)SE(1)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(IX)SE(1)PKC realizing the coding rate of exactly 1.0, based on random pseudo cyclic codes. We show that K(IX)SE(1)PKC is secure against the various attacks including the attack based on the Gröbner bases calculaion (GB attack).

Keyword

Public key cryptosystem, Error-correcting code, Code based PKC, Multivariate PKC, Gröbner bases, PQC.

1 Introduction

Most of the multivariate PKC's are constructed by the simultaneous equations of degree larger than or equal to 2 [1]∼[6]. The present author recently proposed several classes of multivariate PKC's that are constructed by many sets of linear equations[7]∼[13].

It should be noted that McEliece PKC[14] can be regarded as the first member of the class of the linear multivariate PKC.

In this paper we present a new class of public key cryptosystem, K(IX)SE(1)PKC based on pseudo cyclic codes, realizing the coding rate of exactly 1.0. We show that K(IX)SE(1)PKC is secure against the attacks including the attack based on the Gröbner bases calculaion (GB attack)[15].

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 defined in a similar manner.

2 K(XI)SE(1)PKC over $\mathbb{F}_{2^m}$

2.1 Construction

Let us define a few symbols.

$G(x)$:	Random polynomial for generating random pseudo cyclic code over $\mathbb{F}_{2^m}$, $R_0 + R_1 x + \cdots + R_{g-1}x^{g-1} + R_g x^g$, where R_i $(i = 1, \cdots, g-1)$, $R_0 \neq 0$ and $R_g \neq 0$ take on an element of $\mathbb{F}_{2^m}$ equally likely in a random manner.
e_Y :	Exponent(period, order) of $Y(x)$.
$\sharp\{A_i\}$:	Order of the set $\{A_i\}$.
$H(A_i)$:	Ambiguity of A_i, $\log_2 \sharp\{A_i\}$ (bit).
$H(A\|B)$:	Ambiguity (Conditional Entropy) of A when B is given (bit).
$[R_{ij}]_{a\times b}$:	Random matrix, where R_{ij} $(i = 1, \cdots, a; j = 1, \cdots, b)$ takes on 0 or 1 equally likely in a random manner.
$H\Big([R_{ij}]_{a\times b}\Big)$:	Ambiguity of $[R_{ij}]_{a\times b} \cong ab$ (bit).
$\boldsymbol{C}$:	Ciphertext, $(\boldsymbol{C}_I, \boldsymbol{C}_{II})$.
$\boldsymbol{C}_I$:	First ciphertext.
$\boldsymbol{C}_{II}$:	Second ciphertext.
N_V :	Total number of variables.
N_E :	Total number of equations.

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

$$A \cdot H_I = \boldsymbol{a} = (a_1, a_2, \cdots, a_N), \tag{4}$$

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

Let $\boldsymbol{a}$ be partitioned into

$$\boldsymbol{a} = (m_1, m_2, \cdots, m_n), \tag{5}$$

where m_i is given by

$$m_i = (a_{i1}, a_{i2}, \cdots, a_{im}). \tag{6}$$

In the followings let us regard m_i as an element of $\mathbb{F}_{2^m}$.

Let us partition the components of $\boldsymbol{a}$ into

$$\boldsymbol{m}_A = (m_{g+1}, m_{g+2}, \cdots, m_{g+f}), \tag{7}$$

$$\boldsymbol{m}_B = (m_{g+f+1}, m_{g+f+2}, \cdots, m_n), \tag{8}$$

and

$$\boldsymbol{m}_C = (m_1, m_2, \cdots, m_g), \tag{9}$$

respectively, where n is given by

$$n = g + 2f. \tag{10}$$

We let f be given by

$$g < f, \tag{11}$$

due to the reason mentioned in 2.4.

From $\boldsymbol{m}_A$ and $\boldsymbol{m}_B$, we obtain

$$(m_A(x) m_B(x))^{\alpha} \equiv p(x) \mod P(x), \tag{12}$$

where $P(x)$ is a primitive polynomial of degree f over $\mathbb{F}_{2^m}$, and α is given by

$$\alpha = 1 + 2 + 2^2 + \cdots + 2^B < 2^{fm} - 1. \tag{13}$$

Let $p(x)$ be represented by

$$\boldsymbol{p} = (p_1, p_2, \cdots, p_f). \tag{14}$$

The first ciphertext $C_I(x)$ is given by

$$C_I(x) = p(x). \tag{15}$$

Remark 1 : All the components of $\boldsymbol{p}$ are calculated at the sending end from Eq.(12), for the given $\boldsymbol{m}_A$ and $\boldsymbol{m}_B$. Namely all the components are not represented by a set of equations of degree B. □

Regarding $\boldsymbol{m}_A$ over $\mathbb{F}_{2^m}$ as an mf-tuple over $\mathbb{F}_2$, $\boldsymbol{m}_A$ is transformed into

$$\begin{aligned} \boldsymbol{m}_A H_{II} &= \boldsymbol{m}'_A \\ &= \left(m'_{g+1}, m'_{g+2}, \cdots, m'_{g+f}\right), \end{aligned} \tag{16}$$

where H_{II} is an $mf \times mf$ non-singular random matrix over $\mathbb{F}_{2^m}$.

It should be noted that any component m'_i of $\boldsymbol{m}'_A$ is an element of $\mathbb{F}_{2^m}$.

Let $r(x)$ be given by

$$\begin{aligned} m'_A(x) x^g &\equiv r(x) \mod G(x) \\ &= r_1 + r_2 x + \cdots + r_g x^{g-1}. \end{aligned} \tag{17}$$

The code word, $w(x)$, generated by the generator polynomial $G(x)$, can be represented by

$$w(x) = r(x) + m'_A(x) x^g. \tag{18}$$

Regarding the vector $\boldsymbol{r} = (r_1, r_2, \cdots, r_g)$ over $\mathbb{F}_{2^m}$ as a gm-tuple over $\mathbb{F}_2$, it is transformed into

$$\begin{aligned} (r_1, r_2, \cdots, r_g) H_{III} &= \boldsymbol{t} \\ &= (t_1, t_2, \cdots, t_g), \end{aligned} \tag{19}$$

where H_{III} is a $gm \times gm$ random non-singular matrix over $\mathbb{F}_2$.

We see that the ambiguity of H_{III} over $\mathbb{F}_2$ is given approximately by

$$|H_{III}| \cong g^2 m^2 \ \text{(bit)}, \tag{20}$$

an extremely large value for $gm \gtrsim 80$.

According to the transformation given by Eq.(19), the code word $w(x)$ is transformed into

$$w'(x) = t(x) + m'_A(x) x^g \neq 0 \mod G(x), \tag{21}$$

$$\text{for } r(x) \neq 0. \tag{22}$$

The $w'(x)$ is publicized.

At the sending end the message vector $\boldsymbol{m}_C$ is transformed into

$$\{m_C(x)\}^3 = \tau(x). \tag{23}$$

Remark 2 : All the components of $\boldsymbol{\tau}$ are calculated at the sending end from Eq.(23), for the given $m_C(x)$. Namely all the components of $\boldsymbol{\tau}$ are not given by a set of quadratic equations.

With this $\tau(x)$, at the sending end, the word $u(x)$ is constructed by

$$u(x) = w'(x) + \tau(x) x^g. \tag{24}$$

The second ciphertext $C_{II}(x)$ is given by

$$C_{II}(x) = u(x). \tag{25}$$

We have the following set of keys.

Public key	:	$\boldsymbol{m}_A$, $\boldsymbol{m}_B$, $\boldsymbol{m}_C$, $\boldsymbol{w}'$, $P(x)$, α, g, 3.
Secret key	:	H_I, H_{II}, H_{III}, $G(x)$.

2.2 Encryption and Decryption

[Encryption]

Step 1: The vector $\tilde{\boldsymbol{p}}$ is calculated from Eq.(12) for the given $\tilde{\boldsymbol{m}}_A$ and $\tilde{\boldsymbol{m}}_B$.

Step 2: The ciphertext $\tilde{C}_I(x)$ is given by $\tilde{p}(x)$ from Eq.(15).

Step 3: The $w'(x)$ is caclulated from Eq.(21).

Step 4: Given $\tilde{m}_C(x)$, the $\tilde{\tau}(x)$ is calculated from Eq.(23).

Step 5: The ciphertext $\tilde{C}_{II}(x)$ is given by $\tilde{u}(x) = \tilde{w}'(x) + \tilde{m}_C{}^3(x) x^g$ from Eqs.(24) and (25).

Table 1: Example of K(Ⅸ)SE(1)PKC($\rho = 1.0$).

Example	N	m	d_A, d_B	d_C	g	$P_C[\widehat{G}(x)]$	S_{PK} (KB)
I	544	32	6	2	3	$2.94 * 10^{-39}$	58.8
Ⅱ	640	64	3	1	2	$2.76 * 10^{-60}$	184.3

[Decryption]

Step 1: The $\tilde{t}(x)$ is inverse transformed to $\tilde{r}(x)$ by $\tilde{\boldsymbol{t}} \cdot H_{III}^{-1}$, yielding $\tilde{w}(x) + \tilde{m}_C^3(x)x^g$.

Step 2: The $\tilde{m}_C(x)$ is decoded by

$$\begin{aligned}\tilde{C}_{II}(x) &= \left\{\tilde{w}(x) + \tilde{m}_C^3(x)\right\}^d \\ &\equiv \tilde{m}_C(x) \mod G(x),\end{aligned} \tag{26}$$

where d is the inverse element of 3 modulo e_G, yielding $\tilde{w}(x)$.

Step 3: From $\tilde{w}(x)$, the transformed message $\tilde{m}'_A(x)$ is decoded.

Step 4: The vector $\tilde{\boldsymbol{m}}_A$ is obtained by $\tilde{\boldsymbol{m}}'_A H_{II}^{-1}$.

Step 5: Letting e_P be the period of $P(x)$, the message $\tilde{m}_B(x)$ is obtained by

$$\tilde{m}_B(x) \equiv \tilde{p}(x)^{\beta}\tilde{m}_A^{-1}(x) \mod P(x), \tag{27}$$

where β is given by

$$\alpha\beta \equiv 1 \bmod e_P. \tag{28}$$

Step 6: From $\tilde{\boldsymbol{m}}_A$, $\tilde{\boldsymbol{m}}_B$ and $\tilde{\boldsymbol{m}}_C$, the original message, $\tilde{\boldsymbol{A}}$, is decoded by

$$\begin{aligned}(\tilde{\boldsymbol{m}}_A, \tilde{\boldsymbol{m}}_B, \tilde{\boldsymbol{m}}_C)H_I^{-1} &= \tilde{\boldsymbol{A}} \\ &= \left(\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_N\right).\end{aligned} \tag{29}$$

2.3 Examples

In Table 1, we present two examples of K(Ⅸ)SE(1)PKC over $\mathbb{F}_{2^m}$.

Let us show a schematic diagram of Example Ⅱ.

Let us discuss on the size of the public key required for K(Ⅸ)SE(1)PKC over $\mathbb{F}_{2^m}$ by an example for simplicity.

Let the degree of $m_Y(x)$ be denoted by d_Y. In the followings, we assume that d_A, d_B and d_C are chosen so that the relation,

$$d_A = d_B \tag{30}$$

$$3d_C = d_A \tag{31}$$

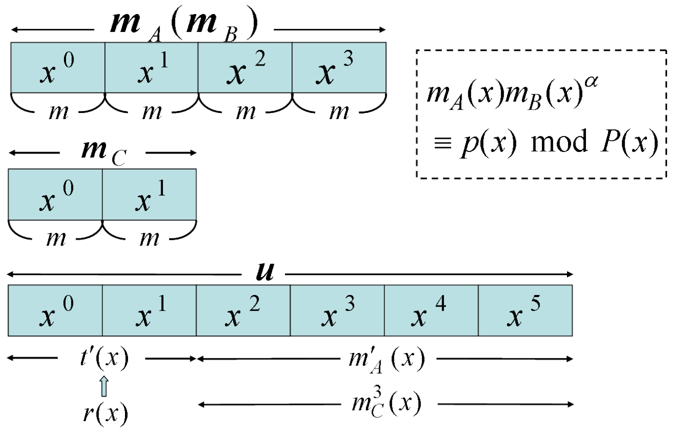

Figure 1: Schematic diagram of K(Ⅸ)SE(1)PKC over $\mathbb{F}_{2^m}$ (Example Ⅱ in Table 1).

may hold.

The total number of variables, N_V, is given by

$$N_V = N = (d_A + d_B + d_C + 3)m. \tag{32}$$

The total number of equations, N_E, is given by

$$N_E = (2d_A + d_B + 2d_C + 5)m. \tag{33}$$

The size of the public key is given by

$$\begin{aligned}S_{\text{PK1}} &= N_V \cdot N_E \\ &= (d_A + d_B + d_C + 3)(2d_A + d_B + 2d_C + 5)m^2.\end{aligned} \tag{34}$$

2.4 Security considerations

Let us discuss on several possible attacks on K(Ⅸ)SE(1)PKC.

Attack 1: Exhaustive attack on $G(x)$ over $\mathbb{F}_{2^m}$

The generator polynomial $G(x)$ can be represented by

$$G(x) = R_0 + R_1x + \cdots + R_{g-1}x^{g-1} + R_gx^g, \tag{35}$$

where we assume that $R_i (i = 0, 1, \cdots, g)$ takes on an element of $\mathbb{F}_{2^m}$ equally likely except that R_0 and R_g are required to be nonzero element.

As a result, the probability of estimating $G(x)$ correctly in an exhaustive manner, $P_C\left[\hat{G}(x)\right]$, is given by

$$\begin{aligned}P_C\left[\hat{G}(x)\right] &= (2^m - 1)^{-2} \cdot 2^{-(g-1)m} \\ &\cong 2^{-(g+1)m}.\end{aligned} \tag{36}$$

Letting m and g satisfy

$$(g+1)m \gtrsim 80, \tag{37}$$

the probability $P_C\left[\hat{G}(x)\right]$ is given by

$$P_C[\widehat{G}(x)] \lesssim 2^{-80}, \tag{38}$$

a sufficiently small value.

For example, $P_C\left[\hat{G}(x)\right]$'s are given by $2^{-128} = 2.94 * 10^{-39}$ for Example I and $2^{-192} = 2.76 * 10^{-60}$ for Example II in Table 1, extremely small values.

We see that K(IX)SE(1)PKC would be secure against the Attack 1 provided that Eq.(37) is satisfied. □

Attack 2: Attack on $\boldsymbol{m}'_A$ based on $\boldsymbol{t}$

The $\boldsymbol{t}$ is given by a linear transformation of $\boldsymbol{r}$ and is given as it is in word $\boldsymbol{u}$. In order to be secure against the Attack 2, the relation, $g < f$ (Eq.(11)), should be strictly satisfied. The conditional entropy, $H(\boldsymbol{m}'_A|\boldsymbol{t})$ is given by

$$H(\boldsymbol{m}'_A|\boldsymbol{t}) = (f-g)m \ \text{(bit)}. \tag{39}$$

For exmaples I and II in Table 1, the conditional entropy $H(\boldsymbol{m}'_A|\boldsymbol{t})$ is given by

$$H(\boldsymbol{m}'_A|\boldsymbol{t}) = 128 \ \text{(bit)} \tag{40}$$

a sufficiently large value.

It is easy to see that once $\boldsymbol{m}'_A$ is disclosed, $m_C^3(x)$ is disclosed.

We conclude that K(IX)SE(1)PKC is secure against Attack 2. □

Attack 3: Attack on $m_B(x)$ by estimating $m_A(x)$

We assume here that Eq.(30) holds, namely $d_A = d_B$. By estimating $m_A(x)$ in an exhaustive manner for a given $p(x)$, $m_B(x)$ can be disclosed. The probability of disclosing $m_B(x)$ by estimating $m_A(x)$ is given by

$$P_C[\hat{m}_B(x)] = 2^{-(d_A+1)m}. \tag{41}$$

For examples I and II, the probability $P_C[\hat{m}_B(x)]$'s are given by $2^{-7*32} = 3.71 * 10^{-68}$ and $2^{-4*96} = 2.54 * 10^{-116}$ respectively, extremely small values.

We see that K(IX)SE(1)PKC is secure against Attack 3. □

Attack 4: GB attack on the ciphertext

The ciphertext $C_I(x)$ can be represented by a set of simultaneous equations of degree B in the variables $A_1, A_2, \cdots, A_N$. The ciphertext $C_{II}(x)$ can be represented by a set of linear and quadratic equations in the variables $A_1, A_2, \cdots, A_N$. Namely the GB attack should solve the following sets of simultaneous equations.

SE(I) : The fm simultaneous of degree B in the variables $A_1, A_2, \cdots, A_N$.

SE(II) : The gm linear equations and fm quadratic equations in the variables $A_1, A_2, \cdots, A_N$.

The degree B takes on 223 for Example I and, 255 for Example II, in Table 1, extremely large values. The number of variables N takes on 544 for Example I and, 640 for Exmaple II, also large values.

We conclude that K(IX)SE(1)PKC is secure against Attack 4. □

3 Conclusion

In this paper we have presented K(IX)SE(1)PKC based on random pseudo cyclic codes. We have shown that our proposed K(IX)SE(1)PKC can be made sufficiently secure against the various attacks including the attack based on the Gröbner bases calculation.

References

[1] 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).

[2] 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).

[3] 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).

[4] N. Koblitz, "Algebraic Aspect of Cryptography", Springer Verlag, Berlin Heidelberg, (1998).

[5] 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).

[6] 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).

[7] 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).

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

[9] 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).

[10] 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).

[11] 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).

[12] M. Kasahara: "New Class of Public Key Cryptosystem Constructed Based on Pseudo Cyclic Codes over $\mathbb{F}_2$ and over $\mathbb{F}_{2^m}(m \geq 7)$ Realizing Coding Rate of 1.0", SITA, (2010-12).

[13] 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).

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

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