A New Class of Multivariate Public Key Cryptosystems Constructed Based on Random Pseudo Cyclic Codes, K(XIII)SE(2)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 multivariate public-key cryptosystems, K(XIII)SE(2)PKC realizing the coding rate of exactly 1.0, based on random pseudo cyclic codes. The K(XIII)SE(2)PKC is constructed on the basis of K(IX)SE(1)PKC, formerly presented by the author. We show that K(XIII)SE(2)PKC is secure against the various attacks including the attack based on the Gröbner bases calculaion (GB attack) and the rank attack.

Keyword

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

1 Introduction

Extensive studies have been made of the Public Key Cryptosystem(PKC). The security of most PKC's depends on the difficulty of discrete logarithm problem or factorization problem. Thus it is desired to investigate another classes of PKC that do not rely on the difficulty of these two problems.

Sof far extensive studies have been made of the PKC constructed based on the simultaneous equations of degree g (SE(g)PKC, $g \geq 2$)[1-10]. All these proposed schemes are very interesting and important. However unfortunately, some of these schemes have been proved not necessarily secure against the conventional attacks such as Patarin's attack[3], Kipnis-Schamir attack[11], Gröbner basis attack[12,13] and Braeken-Wolf-Preneel(BWP) attack[14].

The present author recently proposed several classes of multivariate PKC's that are constructed by many sets of linear equations[15-20]. It should be noted that McEliece PKC[21] presented in 1978 can be regarded as a member of the class of linear multivariate PKC.

In this paper we present a new class of multivariate public key cryptosystem, K(XIII)SE(2)PKC based on the random error-correcting codes, realizing the coding rate of exactly 1.0. The K(XIII)SE(2)PKC is constructed on the basis of K(IX)SE(1)PKC[20], a member of the linear multivariate PKC. We show that K(XIII)SE(2)PKC is secure against the various excellent attacks including the attack based on the Gröbner bases calculaion (GB attack)[12,13] and the rank attack[14].

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(XIII)SE(2)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).
$[R_{ij}]_{a\times b}$:	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 $[R_{ij}]_{a\times b}$, 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 $\mathbb{F}_2$.

Letting $N = nm$, $\boldsymbol{a}$ is 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 $\boldsymbol{a}$ be partitoned 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

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

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

$$(m_A(x) m_B(x))^{\alpha} \equiv p(x) \mod P(x), \tag{11}$$

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

$$\alpha = 1 + 2 + 2^2 + \cdots + 2^B < 2^{fm} - 1. \tag{12}$$

Let $p(x)$ be represented by the vector :

$$\boldsymbol{p} = (p_1, p_2, \cdots, p_f). \tag{13}$$

Remark 1 : Given $m_A(x) = \tilde{m}_A(x)$ and $m_B(x) = \tilde{m}_B(x)$, the components of $\boldsymbol{p}$ over $\mathbb{F}_{2^m}$ are calculated from Eq.(11), at the sending end. □

The first ciphertext $C_I(x)$ over $\mathbb{F}_{2^m}$ is then given by

$$C_I(x) = p(x). \tag{14}$$

Let $m_A(x)$ over $\mathbb{F}_{2^m}$ be transformed into

$$\begin{aligned} m_A(x)^3 &\equiv m'_A(x) \mod F(x) \\ &= m'_{g+1} + m'_{g+2}x + \cdots + m'_{g+f}x^{f-1}, \end{aligned} \tag{15}$$

where $F(x)$ is a random polynomial over $\mathbb{F}_{2^m}$ of degree f.

Let $m_C(x)$ over $\mathbb{F}_{2^m}$ be transformed into

$$m_C(x)^3 \equiv m'_C(x) \bmod H(x). \tag{16}$$

where $H(x)$ is a random polynomial over $\mathbb{F}_{2^m}$ of degree f.

Let $r(x)$ be given by

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

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

$$w(x) = r(x) + (m'_A(x) + m'_C(x))x^g \equiv 0 \mod G(x). \tag{18}$$

The message $m_C(x)$ is transformed into

$$m_C(x)^3 = \tau(x), \tag{19}$$

where we assume that the degree of $\tau(x)$ is less than or equal to $f + g - 1$.

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

$$\begin{aligned} u(x) &= w(x) + \tau(x) \\ &= u_1 + u_2 x + \cdots + u_{g+f}x^{g+f-1}. \end{aligned} \tag{20}$$

Regarding the word $\boldsymbol{u}$ as a $(g+f)m$-tuple over $\mathbb{F}_2$, the word $\boldsymbol{u}$ is transformed into

$$\boldsymbol{u} H_{II} = \boldsymbol{v}, \tag{21}$$

where H_{II} is a $(g+f)m \times (g+f)m$ random non-singular matrix over $\mathbb{F}_2$.

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

$$|H_{II}| \cong (g+f)^2 m^2 \ \text{(bit)}, \tag{22}$$

an extremely large value for

$$(g+f)m \gtrsim 80. \tag{23}$$

Were it not for the tranformation by H_{II}, the generator polynomial $G(x)$ would be easily desclosed. Let us discuss on this matter in the followings.

Let us define several symbols :

$\tilde{\boldsymbol{A}}_i^{(0)}$	:	Non-zero message sequence that make $\tilde{m}_c(x)$ be zero; i = 1,2.
$\tilde{u}_i^{(0)}(x)$	:	Word corresponding to $\tilde{\boldsymbol{A}}_i^{(0)}$; $i = 1, 2$.
$(\tilde{u}_1^{(0)}(x), \tilde{u}_2^{(0)}(x))$	:	Largest common divisor of $\tilde{u}_1(x)$ and $\tilde{u}_2(x)$.
$\tilde{w}_i^{(0)}(x)$	:	Code word corresponding to $\tilde{\boldsymbol{A}}_i^{(0)}$; $i = 1, 2$.

It is evident that $\tilde{\boldsymbol{u}}_1^{(0)}$ and $\tilde{\boldsymbol{u}}_2^{(0)}$ satisfy

$$\tilde{u}_1^{(0)}(x) = \tilde{w}_1^{(0)}(x) \quad for \;\; \tilde{\boldsymbol{A}}_1^{(0)} \tag{24}$$

and

$$\tilde{u}_2^{(0)}(x) = \tilde{w}_2^{(0)}(x) \quad for \;\; \tilde{\boldsymbol{A}}_2^{(0)}, \tag{25}$$

hence

$$\left(\tilde{u}_1^{(0)}(x), \tilde{u}_2^{(0)}(x)\right) \equiv 0 \mod G(x). \tag{26}$$

The Eq.(26) implies that $G(x)$ can be disclosed from $(\tilde{u}_1^{(0)}(x), \tilde{u}_2^{(0)}(x))$.

In general, for J non-zero message sequences $\tilde{\boldsymbol{A}}_1^{(0)}, \tilde{\boldsymbol{A}}_2^{(0)}, \cdots, \tilde{\boldsymbol{A}}_J^{(0)}$, the largest common divisor of $\tilde{u}_1^{(0)}(x), \tilde{u}_2^{(0)}(x), \cdots, \tilde{u}_J^{(0)}(x)$ rapidly approaches to $G(x)$ as J increases.

Remark 2 : The word $\boldsymbol{u}$ is transformed to $\boldsymbol{v}$ by Eq.(21). The large ambiguity of the transformation matrix H_{II} would much strengthen the hiding of the structure of the code word $\boldsymbol{w}$. □

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

$$C_{II}(x) = v(x). \tag{27}$$

Remark 3 : The components of $\boldsymbol{v}$ over $\mathbb{F}_2$ constitute a set of simultaneous equations of degree 2 in the variables $A_1, A_2, \cdots, A_N$. □

We have the following set of keys.

Public key	:	$\boldsymbol{m}_A$, $\boldsymbol{m}_B$, $\boldsymbol{v}$, $P(x)$, α.
Secret key	:	H_I, H_{II}, $F(x)$, $H(x)$, $G(x)$, $\tau(x)$.

2.2 Encryption and decryption

[Encryption]

Step 1: Given $\tilde{m}_A(x)$ and $\tilde{m}_B(x)$, the vector $\tilde{p}(x)$ is calculated by Eq.(11).

Step 2: The ciphertext $\tilde{C}_I(x)$ is given by $\tilde{p}(x)$ from Eq.(14).

Step 3: The ciphertext $\tilde{C}_{II}(x)$ is given by $\tilde{v}(x)$ from Eq.(27).

[Decryption]

Step 1: The ciphertext $\tilde{C}_{II}(x) = \tilde{v}(x)$ is inverse transformed to $\tilde{u}(x)$ by $\tilde{\boldsymbol{v}} \cdot H_{II}^{-1}$, yielding $\tilde{w}(x) + \tilde{m}_C(x)^3$.

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

$$\begin{aligned} \tilde{C}_{II}(x)^{d_G} &= \left\{\tilde{w}(x) + \tilde{m}_C(x)^3\right\}^{d_G} \\ &\equiv \tilde{m}_C(x) \mod G(x), \end{aligned} \tag{28}$$

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

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

Step 4: The $\tilde{m}'_C(x)$ is given by $\tilde{m}_C(x)^3 \bmod H(x)$ from Eq.(16), yielding $m'_A(x)$.

Step 5: The message $\tilde{m}_A(x)$ is obtained by

$$\{\tilde{m}'_A(x)\}^{d_F} \equiv \tilde{m}_A(x) \mod F(x), \tag{29}$$

where d_F is the inverse element of 3 mod e_F, the exponent of $F(x)$.

Step 6: Letting e_P be the exponent of $P(x)$, the message $\tilde{m}_B(x)$ is obtained by

$$\tilde{m}_B(x) \equiv \tilde{p}(x)^\beta \tilde{m}_A^{-1}(x) \mod P(x), \tag{30}$$

where β is given by

$$\alpha\beta \equiv 1 \bmod e_P. \tag{31}$$

Step 7: From $\tilde{\boldsymbol{m}}_A$, $\tilde{\boldsymbol{m}}_B$ and $\tilde{\boldsymbol{m}}_C$, the original message, $\tilde{\boldsymbol{A}}$, is decoded by

$$\begin{aligned} (\tilde{\boldsymbol{m}}_A, \tilde{\boldsymbol{m}}_B, \tilde{\boldsymbol{m}}_C) H_I^{-1} &= \tilde{\boldsymbol{A}} \\ &= \left(\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_N\right). \end{aligned} \tag{32}$$

Table 1: Example of K(XIII)SE(2)PKC($\rho = 1.0$).

Example	m	N	d_A, d_B	d_C	g	$S_{\rm PK}$(KB)
I	8	168	7	4	5	187.2
II	16	176	3	2	3	220.9
III	32	192	1	1	2	299.5

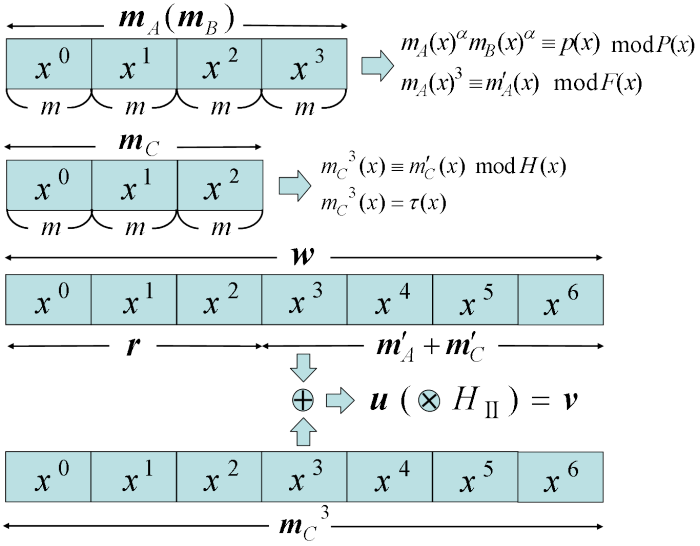

Figure 1: Schematic diagram of K(XIII)SE(2)PKC over $\mathbb{F}_{2^m}$ (Example II in Table 1).

2.3 Examples

An example of a schematic diagram of K(XIII)SE(2)PKC over $\mathbb{F}_{2^m}$ is given in Fig.1.

Let us show the size of the public key for K(XIII)SE(2)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,

$$d_A = d_B \tag{33}$$
$$d_A = 2d_C - 1 \tag{34}$$

may hold.

The total number of variables, N_V, is given by

$$N_V = N = (d_A + d_B + d_C + 3)m. \tag{35}$$

The total number of linear equations, N_{E1}, is given by

$$N_{E1} = (d_A + d_B + 2)m. \tag{36}$$

The total number of quadratic equations, N_{E2}, is given by

$$N_{E2} = (d_A + d_C + 2)m. \tag{37}$$

The size of the public key is given by

$$S_{\rm PK} = N_{E1} \cdot N + N_{E2} \cdot {}_N{\rm H}_2 \text{ (bit)}. \tag{38}$$

It should be noted that the sizes of the public keys $P(x)$ and α can be disregarged.

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

2.4 Security considerations

Let us consider several possible attacks on K(XIII)SE(2)PKC.

Attack 1: Disclosing the code word $w(x)$ by exhaustively estimating $G(x)$

The probability of estimating random polynomial $G(x)$ over $\mathbb{F}_{2^m}$, in an exhaustive manner, is given by

$$P_C[\widehat{G}(x)] \cong 2^{-(g+1)m}, \tag{39}$$

not a sufficiently small value for Example I in Table 1.

However, even if $G(x)$ can be estimated correctly with probability $2^{-(g+1)m}$, it would still be hard to disclose the structure of $w(x)$ exactly, i.e., $m'_A(x)$, $m'_C(x)$, and $r(x)$ due to the following reasons:

R1 : Addition of $\tau(x)$ on the code word $w(x)$.

R2 : The word $u(x) = w(x) + \tau(x)$ is further transformed into $v(x)$ using random non-singular matrix H_{II}, whose ambiguity takes on an extremely large value of approximately 10^4 bit for the examples in Table 1(Please refer to Remark 2).

We conclude that K(XIII)SE(2)PKC would be secure against the Attack 1. □

Attack 2: Exhaustive attack on $\tilde{\boldsymbol{m}}_A$

Let an estimated value of $\tilde{\boldsymbol{m}}_A$ be denoted by $\hat{\tilde{\boldsymbol{m}}}_A$ and the set of all possible $\hat{\tilde{\boldsymbol{m}}}_A$, by $\left\{\hat{\tilde{\boldsymbol{m}}}_A\right\}$. The order of $\left\{\hat{\tilde{\boldsymbol{m}}}_A\right\}$ can be given by

$$\sharp\left\{\hat{\tilde{\boldsymbol{m}}}_A\right\} = 2^{fm}. \tag{40}$$

The average number of the trials required for correctly estimating $m_A(x)$, $\bar{N}(\hat{m}_A)$ is given by

$$\begin{aligned}\bar{N}(\hat{m}_A) &= \frac{1}{2^{fm}}\left(1 + 2 + 3 + \cdots + 2^{fm}\right) \\ &\cong 2^{fm-1}.\end{aligned} \tag{41}$$

For the examples in Table 1, $\bar{N}(\hat{m}_A)$ is given by

$$\bar{N}(\hat{m}_A) \cong 2^{63} \cong 9.22 \times 10^{18}. \quad (42)$$

When $\tilde{\boldsymbol{m}}_A$ is estimated correctly in an exhaustive manner, the $\tilde{\boldsymbol{m}}_B$ is accordingly given correctly from Eq.(11).

For correctly estimated $\tilde{\boldsymbol{m}}_A$ and $\tilde{\boldsymbol{m}}_B$, in order to disclose the messages $\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_N$, the GB attack should solve the following sets of simultaneous equations :

SE(I) : The $2fm$ linear equations in the variables $A_1, A_2, \cdots, A_N$.

SE(Ⅱ) : The $(f+g)m$ quadratic equations in the variables $A_1, A_2, \cdots, A_N$.

For a given ciphertext $\tilde{C}$, in order to disclose the messages $\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_N$, GB attack should solve the above simultaneous equations, SE(I) and SE(Ⅱ) in 2^{fm-1} times given by Eq.(41). Besides, the number of variables N takes on a large value of $168 \sim 192$ for the examples in Table 1. This would be a hard task for GB attack.

We conclude that K(XIII)SE(2)PKC would be secure against Attack 2. □

Attack 3: GB attack on ciphertext by representing $p(x)$ by a set of simultaneous equations

The $p(x)$ can be represented by the following simultaneous equations :

SE(Ⅲ) : The f equations of degree B in the variables

$$A_1, A_2, \cdots, A_N. \quad (43)$$

For Examples I, Ⅱ and Ⅲ given in Table 1, the degree B takes on 63, a large value.

For a given ciphertext $\tilde{C}$, in order to disclose the messages $\tilde{A}_1, \tilde{A}_2, \cdots, \tilde{A}_N$, GB attack should solve the two sets of simultaneous equations, SE(Ⅱ), and SE(Ⅲ).

We conclude that K(XIII)SE(2)PKC would be secure against Attack 3. □

Attack 4: Rank attack

K(XIII)SE(2)PKC would be secure against the rank attack as K(XIII)SE(2)PKC has no STS(Step-wise Trianglar Structure). Furthermore the transformations by Eq.(11), Eq.(15) and Eq.(16) would much strengthen the security against the rank attack.

3 Conclusion

In this paper we have presented K(XIII)SE(2)PKC on the basis of K(IX)SE(1)PKC[20] using random pseudo cyclic codes. We have shown that our proposed K(XIII)SE(2)PKC can be made sufficiently secure against the various attacks including the attack based on Gröbner bases calculation(GB attack).

References

[1] 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).

[2] 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).

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

[4] 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).

[5] 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).

[6] J. Ding: "A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation", PKC 2004, LNCS 2947, pp.305-318, 2004.

[7] 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).

[8] J. Ding, D. Schmidt and J. Gower: "Multivariate Public key Cryptography", Springer-Verlag(2006).

[9] 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).

[10] 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).

[11] A. Kipnis and A. Shamir: "Cryptoanalysis of the HFE Public Key Cryptosystem by Relinearization", Advances in Cryptography-Crypto'99, LNCS 1666, pp.19-30, (1999).

[12] M. Bardet, J. C. Faugére and B. Salvy: "Complexity of Gröbner basis computation for semi-regular overdetermined sequence over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$", Technical Report RR-5049, INRIA, (2003-12).

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

[14] C. Wolf: "Multivariate Quadratic Polynomials in Public Key Cryptography", Dr. Thesis, Katholieke Universiteit Leuven, (2005-11).

[15] 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).

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

[17] 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).

[18] 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).

[19] 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).

[20] M. Kasahara: "Public Key Cryptosystems Constructed Based on Random Pseudo Cyclic Codes, K(IX)SE(1)PKC, Realizing Coding Rate of Exactly 1.0", Cryptology ePrint Archive 2011 / 545(2011) Masao Kasahara.

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