New Class of Multivariate Public Key Cryptosystem, K(XI)RSE(2)PKC, Constructed based on Reed-Solomon Code Along with K(X)RSE(2)PKC over $\mathbb{F}_2$

Masao KASAHARA *

September 10, 2014

Abstract

Extensive studies have been made of the public key cryptosystems based on multivariate polynomials (Multi-variate PKC, MPKC) over $\mathbb{F}_2$ and $\mathbb{F}_{2^m}$. However most of the proposed MPKC are proved not secure. In this paper, we propose a new class of MPKC based on Reed-Solomon code, referred to as K(XI)RSE(2)PKC. In Appendix, we present another class of MPKC referred to as K(X)RSE(2)PKC over $\mathbb{F}_2$. Both K(X)RSE(2)PKC and K(XI)RSE(2)PKC yield the coding rate of 1.0. We show that the proposed schemes can be sufficiently secure against various attacks, including Gröbner basis attack.

keyword

Public-key cryptosystem, Gröbner basis attack, Multivariate PKC, Code-based PKC.

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.

So far extensive studies have been made of the Multivariate PKC (MPKC) constructed based on the simultaneous equations of degree 2 (SE(2)PKC) [1-8]. 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], Gröbner basis attack [9], Braeken-Wolf-Preneel (BWP) attack [10, 11].

In this paper, we propose a new class of MPKC based on Reed-Solomon code, referred to as K(XI)RSE(2)PKC. We then propose another class of MPKC referred to as K(X)RSE(2)PKC over $\mathbb{F}_2$. Both K(X)RSE(2)PKC over $\mathbb{F}_2$ and K(XI)RSE(2)PKC over $\mathbb{F}_{2^m}$ yield the coding rate of 1.0. We show that the proposed schemes can be secure against the possible attacks, including Gröbner basis attack.

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

$$\tilde{\boldsymbol{v}} = (\tilde{v}_1, \tilde{v}_2, \cdots, \tilde{v}_n). \tag{1}$$

We shall use the notation tilda $\sim$ when it is necessary for understanding the meaning of v_i more clearly.

*Research Institute for Science and Engineering, Waseda University. Research and Development Initiative, Chuo University. kasahara@ogu.ac.jp

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)RSE(2)PKC

2.1 Preliminaries

2.1.1 List of symbols

$\boldsymbol{M}$: Message, $(M_1, M_2, \cdots, M_{2gm})$ over $\mathbb{F}_2$.
$G(x)$: Generator polynomial of Reed-Solomon code over $\mathbb{F}_{2^m}$.
g : Degree of $G(x)$.
$\varphi_R(\boldsymbol{x})$: Randomly quadratic-transformed $\boldsymbol{x}$.
$\varphi_S(\boldsymbol{x})$: Systematically quadratic-transformed $\boldsymbol{x}$.
$RSE(2)$: Simultaneous quadratic equations randomly constructed.
$SSE(2)$: Simultaneous quadratic equations systematically constructed.
$\boldsymbol{A}$: $(A_1, A_2, \cdots, A_g)$ over $\mathbb{F}_{2^m}$.
A_i : $(A_{i1}, A_{i2}, \cdots, A_{im})$.
A_{ij} : Randomly constructed quadratic equation;$A_{ij}^{(2)}(M_1, M_2, \cdots, M_{2gm})$ over $\mathbb{F}_2$.
Capital letter is used for RSE(2).
$\boldsymbol{\alpha}$: $(\alpha_1, \alpha_2, \cdots, \alpha_g)$ over $\mathbb{F}_{2^m}$.
α_i : $(\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{im})$ over $\mathbb{F}_2$.
α_{ij} : Systematically constructed quadratic equation;$\alpha_{ij}^{(2)}(M_1, M_2, \cdots, M_{2gm})$ over $\mathbb{F}_2$.
Small letter is used for SSE(2).

2.1.2 Random quadratic equation

The set of random quadratic equations, $\{A_{ij}\}$, is constructed as follows:
Let a linear term T_i and a quadratic term T_{jk} be

$$T_i = M_i; i = 1, 2, \cdots, 2gm. \tag{3}$$

$$T_{jk} = M_j M_k; j, k = 1, 2, \cdots, 2gm; j \neq k. \tag{4}$$

The random quadratic equation A_{ij} over $\mathbb{F}_2$ is

$$A_{ij} = \sum_{i}^{2gm} \theta_i^{(1)} T_i + \sum_{j,k}^{2gm} \theta_{jk}^{(2)} T_{jk}, \tag{5}$$

where $\theta_i^{(1)}$ and $\theta_{j,k}^{(2)}$ take on 0 or 1 with the probability 0.5.

2.2 Construction

Let the original message $\boldsymbol{M} = (M_1, M_2, \cdots, M_{2gm})$ over $\mathbb{F}_2$ be transformed to

$$\boldsymbol{M} \cdot A_I = \boldsymbol{m} = (m_1, m_2, \cdots, m_{2gm}), \tag{6}$$

where A_I is a non-sigular $2gm \times 2gm$ matrix over $\mathbb{F}_2$.

Let $\boldsymbol{m} = (m_1, m_2, \cdots, m_{2gm})$ over $\mathbb{F}_2$ be partitioned to

$$\boldsymbol{m} = (\boldsymbol{\alpha}; \boldsymbol{\beta}), \tag{7}$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ over $\mathbb{F}_2$ are

$$\begin{aligned} \boldsymbol{\alpha} &= (m_1, m_2, \cdots, m_{gm}), \\ \boldsymbol{\beta} &= (m_{gm+1}, m_{gm+2}, \cdots, m_{2gm}). \end{aligned} \tag{8}$$

The components of $\boldsymbol{\alpha}$ is systematically transformed to a set of quadratic equations over $\mathbb{F}_{2^m}$ that can be systematically decoded:

$$\varphi_s(\boldsymbol{\alpha}) = \boldsymbol{\sigma} = (\sigma_1, \sigma_2, \cdots, \sigma_g), \tag{9}$$

where σ_i is

$$\sigma_i = (\sigma_{i1}, \sigma_{i2}, \cdots, \sigma_{im}); i = 1, 2, \cdots, g. \tag{10}$$

The component of σ_i, σ_{ij}, is

$$\sigma_{ij} = \sigma_{ij}^{(2)}(m_1, m_2, \cdots, m_{gm}); i = 1, 2, \cdots, g; j = 1, 2, \cdots, m, \tag{11}$$

where σ_{ij}'s will be referred to as erasure errors.

Let $\sigma(x) = \sigma_1 + \sigma_2 x + \cdots + \sigma_g x^{g-1}$ be transformed to

$$\sigma(x) \mapsto \tau(x) = \sigma_1 x^{(1)} + \sigma_2 x^{(2)} + \cdots + \sigma_g x^{(g)}, \tag{12}$$

where the exponents (i) are randomly chosen on condition that they satisfy

$$0 \leq (1) < (2) < \cdots < (g) \leq 2g - 1. \tag{13}$$

Let us refer to $(1), (2), \cdots, (g)$ as erasure locations.

The vector $\boldsymbol{\alpha}$ is randomly transformed to Ω over $\mathbb{F}_{2^m}$:

$$\varphi_R(\boldsymbol{\alpha}) = \boldsymbol{\Omega} = (\Omega_1, \Omega_2, \cdots, \Omega_g), \tag{14}$$

where Ω_i is

$$\Omega_i = (\Omega_{i1}, \Omega_{i2}, \cdots, \Omega_{im}); i = 1, 2, \cdots, g. \tag{15}$$

The component of Ω_i, Ω_{ij} is

$$\Omega_{ij} = \Omega_{ij}^{(2)}(m_1, m_2, \cdots, m_{gm}); i = 1, 2, \cdots, g; j = 1, 2, \cdots, m. \tag{16}$$

The vector $\boldsymbol{\beta}$ is systematically transformed to $\boldsymbol{\rho}$ over $\mathbb{F}_{2^m}$:

$$\varphi_s(\boldsymbol{\beta}) = \boldsymbol{\rho} = (\rho_1, \rho_2, \cdots, \rho_g), \tag{17}$$

where ρ_i is

$$\rho_i = (\rho_{i1}, \rho_{i2}, \cdots, \rho_{im}); i = 1, 2, \cdots, g. \tag{18}$$

The component of ρ_i, ρ_{ij} is

$$\rho_{ij} = \rho_{ij}^{(2)}(m_{gm+1}, m_{gm+2}, \cdots, m_{2gm}); i = 1, 2, \cdots, g; j = 1, 2, \cdots, m. \tag{19}$$

Let us summarize the features of the above-mentioned quadratic equations:

$\{\sigma_{ij}\}, \{\rho_{ij}\}$: Sets of quadratic equations that can be systematically decoded.

$\{\Omega_{ij}\}$: Set of random quadratic equations that cannot be systematically decoded.

The sets $\{\sigma_{ij}\}, \{\rho_{ij}\}$ and $\{\Omega_{ij}\}$ yield the following advantages:

(i) simple decoding process thanks to $\{\sigma_{ij}\}$ and $\{\rho_{ij}\}$,
(ii) high security against the various attacks including Gröbner bases attack, thanks to $\{\Omega_{ij}\}$.

Let $\Omega(x) + \rho(x)$ be transformed to

$$x^g(\Omega(x) + \rho(x)) \equiv R(x) \bmod G(x). \tag{20}$$

The code word $V(x)$ is

$$V(x) = R(x) + x^g(\Omega(x) + \rho(x)) \equiv 0 \bmod G(x). \tag{21}$$

The word $W(x)$ is

$$\begin{aligned} W(x) &= V(x) + \tau(x) \\ &= W_1 + W_2 x + \cdots + W_{2g} x^{2g-1}. \end{aligned} \tag{22}$$

Let W_i be

$$W_i = (W_{i1}, W_{i2}, \cdots, W_{im}); i = 1, 2, \cdots, 2g. \tag{23}$$

Taking account of the above Eq.(23), we regard $\boldsymbol{W} = (W_1, W_2, \cdots, W_{2g})$ over $\mathbb{F}_{2^m}$ as the vector $\boldsymbol{W'}$ over $\mathbb{F}_2$:

$$W' = (W_{11}, \cdots, W_{1m}; W_{21}, \cdots, W_{2m}; \cdots; W_{2g1}, \cdots, W_{2gm}). \tag{24}$$

The set of public key, $\{U_i\}$, is

$$\begin{aligned} \boldsymbol{W'} A_{II} &= \boldsymbol{U} \\ &= (U_1, U_2, \cdots, U_{2gm}), \end{aligned} \tag{25}$$

where A_{II} is a non-singular $2gm \times 2gm$ matrix over $\mathbb{F}_2$.
The U_i is

$$U_i = U_i^{(2)}(M_1, M_2, \cdots, M_{2gm}); i = 1, 2, \cdots, 2gm. \tag{26}$$

We see that U_i can be represented as

$$\begin{aligned} U_i^{(2)}(M_1, M_2, \cdots, M_{2gm}) = Y_i^{(2)}(M_1, M_2, \cdots, M_{2gm}) + y_i^{(2)}(M_1, M_2, \cdots, M_{2gm}) \\ ; i = 1, 2, \cdots, 2gm, \end{aligned} \tag{27}$$

where Y_i's and y_i's are the transformed versions of V_i's and τ_i's respectively, based on A_{II}.
Let $z(x) = z_i^{(2)}(M_1, M_2, \cdots, M_{2gm})$ denote the transformed version of $\rho(x)$ based on A_{II}.
In Fig.1, we show an example of $\{U_i\}$, only for an easy understanding of the present paper. It should be noted that this is not an example of K(XI)RSE(2)PKC.

$$
\begin{aligned}
U_1 &= 1 + (M_1) + M_5 + M_1M_2 + (M_2M_3) + M_2M_4 \\
&\quad + M_3M_6 + (M_5M_6) \\
U_2 &= M_2 + (M_4) + M_1M_4 + (M_2M_6) + M_3M \\
&\quad + (M_3M_5) \\
U_3 &= M_3 + (M_5) + M_6 + (M_1M_2) + M_1M_5 + M_2M_3 \\
&\quad + M_3M_6 + M_4M_6 \\
U_4 &= (M_4) + (M_6) + M_1M_5 + M_1M_6 + (M_3M_4) \\
&\quad + M_3M_6 + M_5M_6 \\
U_5 &= M_2 + (M_5) + M_1M_3 + (M_2M_3) + M_2M_6 \\
&\quad + (M_3M_4) + (M_4M_6) \\
U_6 &= (M_4) + M_5 + (M_1M_2) + M_1M_3 + M_1M_6 \\
&\quad + (M_2M_4) + M_3M_4 + (M_3M_5)
\end{aligned}
$$

Only in this example for easy understanding, erasure symbols are enclosed in parentheses.

Figure 1: An example of $\{U_i\}$.

In 2.4, we shall see that K(XI)RSE(2)PKC yields the coding rate of exactly 1.0. It is evident that the coding rate of the ciphertext constructed based on $\{U_i\}$ of Example 1 is also exactly 1.0.

The set of keys are:

Public key	:	$\{U_i\}$.
Secret key	:	$\{\sigma_{ij}\}, \{\Omega_{ij}\}, \{\rho_{ij}\}, A_I, A_{II}$.

2.3 Encryption and decryption process

Encryption process:

S1 : Given the message $\widetilde{\boldsymbol{M}} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_{2gm})$ over $\mathbb{F}_2$, Bob calculates the ciphertext over $\mathbb{F}_2$: $\widetilde{\boldsymbol{C}} = (\widetilde{U}_1, \widetilde{U}_2, \cdots, \widetilde{U}_{2gm})$, where U_i is $U_i = U_i^{(2)}(\widetilde{M}_i, \widetilde{M}_2, \cdots, \widetilde{M}_{2gm})$.

Decryption process:

S1 : Given the ciphertext $\widetilde{\boldsymbol{C}}$, Alice calculates $\widetilde{\boldsymbol{C}} A_{II}^{-1} = \widetilde{\boldsymbol{W}}'$, yielding $\widetilde{\boldsymbol{V}} + \widetilde{\boldsymbol{\tau}}$ over $\mathbb{F}_{2^m}$.

S2 : Alice decodes $\widetilde{\boldsymbol{\tau}}$ with erasure and error decoding algorithm [12], yielding $\widetilde{\boldsymbol{\sigma}}$.

S3 : Alice decodes the first message $\widetilde{\alpha} = (\widetilde{m}_1, \widetilde{m}_2, \cdots, \widetilde{m}_{gm})$ over $\mathbb{F}_2$ by solving the set of systematically constructed quadratic equations $\{\sigma_{ij}^{(2)}(\widetilde{m}_1, \widetilde{m}_2, \cdots, \widetilde{m}_{gm})\}$.

S4 : Alice calculates $\varphi_R(\widetilde{\alpha}) = \widetilde{\boldsymbol{\Omega}} = (\widetilde{\Omega}_1, \widetilde{\Omega}_2, \cdots, \widetilde{\Omega}_g)$ over $\mathbb{F}_{2^m}$, where $\widetilde{\Omega}_i$ is $\Omega_i^{(2)}(\widetilde{m}_1, \widetilde{m_2}, \cdots, \widetilde{m}_{gm})$, yielding $\widetilde{\boldsymbol{\rho}} = (\widetilde{\rho}_1, \widetilde{\rho}_2, \cdots, \widetilde{\rho}_g)$ over $\mathbb{F}_{2^m}$.

S5 : Alice decodes the second message $\boldsymbol{\beta} = (\widetilde{m}_{gm+1}, \widetilde{m}_{gm+2}, \cdots, \widetilde{m}_{2gm})$ over $\mathbb{F}_2$ by solving the set of systematically constructed quadratic equations $\{\rho_i^{(2)}(\widetilde{m}_{gm+1}, \widetilde{m}_{gm+2}, \cdots, \widetilde{m}_{2gm})\}$.

S6 : Alice calculates $(\widetilde{m}_1, \widetilde{m}_2, \cdots, \widetilde{m}_{2g}) A_I^{-1}$, yielding the message : $\widetilde{\boldsymbol{M}} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_{2gm})$ over $\mathbb{F}_2$.

2.4 parameters

The size of public key, S_{PK}, is

$$S_{PK} = \#\{U_i\} \times |U_i|, \tag{28}$$

where $\#\{U_i\}$ is the order of the set of public key, $\{U_i\}$, and $|U_i|$, the size of public key U_i (in bit).

For example,

$$\begin{aligned} &S_{PK} = 135 \text{ KB for } m = 8, g = 8. \\ &S_{PK} = 1.05 \text{ MB for } m = 8, g = 16. \end{aligned} \tag{29}$$

The coding rate ρ is

$$\rho = \frac{|\boldsymbol{M}|}{|\boldsymbol{C}|} = \frac{2gm}{2gm} = 1.0, \tag{30}$$

where $\boldsymbol{M}$ is the size of message and $|\boldsymbol{C}|$, the size of the ciphertext.

We see that the coding rate is exactly 1.0.

2.5 Security considerations

In this subsection we let the parameters: $m = 8, g = 16$.

Attack 1 : Exhaustive attack on A_{II}

The probability that A_{II} is correctly estimated, $P_c[\hat{A}_{II}]$

$$P_c[\hat{A}_{II}] \cong 2^{-4g^2m^2} = 5 \times 10^{-19662}. \tag{31}$$

We see that K(XI)RSE(2)PKC is secure against Attack 1.

For a moment let us assume that $\boldsymbol{W}'$ is tranformed to

$$\boldsymbol{W}'P = \boldsymbol{U}', \tag{32}$$

where P is a $2gm \times 2gm$ random column permutaion matrix. Namely we assume that a more simple transformation P is applied to $\boldsymbol{W}'$, instead of A_{II}.

Attack 2 : Exhaustive attack on erasure locations, $(1), (2), \cdots, (g)$, under the condition that $\boldsymbol{U}'$ is given instead of $\boldsymbol{U}$.

The probability that erasure locations are correctly estimated, $P_c[\{(\hat{i})\}]$, is

$$P_c[\{(\hat{i})\}] = \left(\begin{array}{c} 2gm \\ gm \end{array} \right)^{-1}. \tag{33}$$

For example, for $m = 8, g = 16$, $P_c[\{(\hat{i})\}]$ are

$$P_c[\{(\hat{i})\}] = \left(\begin{array}{c} 256 \\ 128 \end{array} \right)^{-1} = 1.74 \times 10^{-76}, \tag{34}$$

a sufficiently small value.

We conclude that K(XI)SE(2)PKC is secure against Attack 2 for $m = 8, g \gtrsim 16$.

Remark 1: The author feels certain that, even if the set of erasure error locations $\{(i)\}$ are correctly estimated with an exhaustive method, it would still hard to disclose the set of simultaneous equations $\{\sigma_{ij}\}$. The reason of the author's certainty is due to the robustness of K(XI)RSE(2)PKC against Attack 3 mentioned below.

Attack 3: Disclosing SSE(2) added on RSE(2)

Let us first point out a large difference between the entropies (ambiguities) of SSE(2) and RSE(2). The entropy of SSE(2) in the gm variables $m_1, m_2, \cdots, m_{gm}$ or $m_{g+1}, m_{g+2}, \cdots, m_{2gm}$, I_S, is

$$\begin{aligned} I_S &\cong \log_2 \frac{2^{gm} - 1}{gm} + \log_2 \left(\begin{array}{c} gm \\ 2 \end{array} \right) \\ &\cong gm + \log_2 gm \text{ (bit)}. \end{aligned} \tag{35}$$

The entropy of RSE with the same number of variables, I_R, is

$$I_R \cong \left(\begin{array}{c} gm \\ 2 \end{array} \right) \cdot gm \cong \frac{1}{2} g^3 m^3 \text{ (bit)}. \tag{36}$$

For $m = 8, g = 16$, I_S and I_R are

$$\begin{array}{l} I_S = 135 \text{ bit}, \\ I_R = 1.05 \text{ M bit}. \end{array} \tag{37}$$

Namely in K(XI)SE(2)PKC, the following relation holds:

$$I_R >> I_S. \tag{38}$$

We see that any linear transformation attack would find it hard to disclose $y_i^{(2)}(M_1, M_2, \cdots, M_{2gm})$ from $U_i^{(2)}(M_1, M_2, \cdots, M_{2gm})$, due to the large difference between the entropies (ambiguities) of SSE(2) and RSE(2).

We thus conclude that disclosing the set of SSE(2), $\{\sigma_{ij}\}$ embedded in $\boldsymbol{V}$, is hard, because the entropy of σ_{ij} is very small compared with that of the component of $\boldsymbol{V}$.

We see that K(XI)SE(2) PKC is secure against Attack 3.

Notes on the security:

The set of quadratic equation $\{\Omega_{ij}\}$ is constructed using $\varphi_R(\boldsymbol{\alpha})$, a random non-lineartransformation of $\boldsymbol{\alpha} = (m_1, m_2, \cdots, m_{gm})$ where m_i is a linear equation in the variables $M_1, M_2, \cdots, M_{2gm}$ over $\mathbb{F}_2$.

The vector $\boldsymbol{\tau}$, randomly permuted version of $\varphi_R(\boldsymbol{\alpha})$ is added to the code word

$$\boldsymbol{V} = (V_1, V_2, \cdots, V_{2gm}), \tag{39}$$

where V_i is

$$V_i = (V_{i1}, V_{i2}, \cdots, V_{im}). \tag{40}$$

The component of V_i, V_{ij} is a random quadratic equation in the variables $M_1, M_2, \cdots, M_{2gm}$ and has a vely large entropy compared with that of σ_{ij}.

Besides $\mathrm{K_M}$(XI)RSE(2)PKC realizes the coding rate of exactly 1.0.

We thus conclude that $\mathrm{K_M}$(XI)RSE(2)PKC would be suffficiently secure against the linear transformation type of attacks such as Gröbner basis attack.

3 Conclusion

We have presented a new class of RSE(2)PKC referred to as K(XI)·RSE(2)PKC over $\mathbb{F}_{2^m}$. We have shown that letting the size of public key be almost same as that of the conventional RSE(2)PKC, the security is much improved.

The author feels certain that K(XI)RSE(2)PKC would open up a brand new field of PKC's as it is strongly related to the fields of both MPKC and code-based PKC.

In Appendix, we have presented K(X)RSE(2)PKC over $\mathbb{F}_2$, which is simpler but less secure compared with K(XI)RSE(2)PKC.

This work is partly supported by NICT's project:Research and developement for public key cryptosystem for secure communication between social systems and 21st.Century Informatic Culture Center.

References

[1] T. Matsumoto and H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature - Verification and Message-Encryption", Advances in Cryptology, Eurocrypt'88, Springer-Verlag, pp.419-453, (1989).

[2] N. Koblitz, "Algebraic Aspects of Cryptography", Springer-Verlag, Berlin Heidelberg, (1998).

[3] J. Patarin, "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88", Advances in Cryptography, Crypto'95, Springer Verlag, pp.248-261, (1996).

[4] 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. J-72-A, 2, pp.390-397, (1989-02).

[5] M. Kasahara and R. Sakai, "A Construction of Short Public-Key Cryptosystem over Extension", Technical Report of IEICE, ISEC 2002-116, pp.63-68, (2003-3).

[6] M. Kasahara and R. Sakai, "A Construction of Public Key Cryptosystem for Realizing Cyphertext of size 100 bit and Digital Signature Scheme", IEICE Trans. Vol. E87-A, 1, pp.102-109, (2004-01).

[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] 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, (2004-9).

[9] J.C. Faugere, "Algebraic cryptanalysis of HFE usin Gröbner bases", Report de recherche, INRIA, No. 4738, (2003-02).

[10] C. Wolf, A. Braekn, B. Preneel, "Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC", SCN 2004: 294-309, Lecture Notes in Computer Science 3352 Springer 2005.

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

[12] Y. Sugiyama, M. Kasahara, S.Hirasawa and T. Namekawa, "An erasure-and-errors decoding algorithm for Goppa codes", IEEE Trans. Info. Theory, 22, pp238-241, (1976).

[13] M. Kasahara, "A New Class of Public Key Cryptosystems over $\mathbb{F}_{2^8}$ Constructed Based on Read-Solomon Codes K(XVI)SE(1)PKC, K(XVII)SE(1)PKC and K(XVII)ΣΠ PKC", Technical Report of IEICE, IT 2014-35, pp.133-138, (2014-7).

[14] M. Kasahara, "Presentations of a general augmentation scheme, K(V)Schme, for strengthening several classes of PKC and a new class of system oriented PKC, K(I)SOPKC", Technical Report of IEICE, IT 2013-73, pp.1-6, (2013-12).

Appendix:K(X)RSE(2)PKC

In Dec.2013, in Ref. [14], the author presented an augmentation technique, K(V)Schme and applied it to several members of PKC such as

- knapsack type PKC,
- code based PKC,
- multivariate PKC.

In this Appendix, we present K(XI)RSE(2) over $\mathbb{F}_2$ by applying K(V)Schme to a general RSE(2)PKC over $\mathbb{F}_2$.

Let the original message $\boldsymbol{M}$ be

$$\boldsymbol{M} = (M_1, M_2, \cdots, M_{2g}) \text{ over } \mathbb{F}_2. \tag{41}$$

The message $\boldsymbol{M}$ is transformed to

$$\boldsymbol{M} \cdot A_{III} = \boldsymbol{m} = (m_1, m_2, \cdots, m_{2g}), \tag{42}$$

where A_{III} is a non-singular $2g \times 2g$ matrix over $\mathbb{F}_2$.

Let $\boldsymbol{m}$ be partitioned to

$$\boldsymbol{m}_I = (m_1, m_2, \cdots, m_g) \tag{43}$$

and

$$\boldsymbol{m}_{II} = (m_{g+1}, m_{g+2}, \cdots, m_{2g}) \tag{44}$$

The message $\boldsymbol{m}_I$ is then transformed to

$$\varphi_s(\boldsymbol{m}_I) = \boldsymbol{a} = (a_i, a_2, \cdots, a_g), \tag{45}$$

where a_i is

$$a_i = a_i^{(2)}(m_1, m_2, \cdots, m_g); i = 1, 2, \cdots, g. \tag{46}$$

Let the message $\boldsymbol{m}_I$ be also transformed to

$$\varphi_R(\boldsymbol{m}_I) = \boldsymbol{A} = (A_1, A_2, \cdots, A_g), \tag{47}$$

where A_i is

$$A_i = A_i^{(2)}(m_1, m_2, \cdots, m_g); i = 1, 2, \cdots, g. \tag{48}$$

Let $\boldsymbol{m}_{II}$ be transformed to

$$\varphi_s(\boldsymbol{m}_{II}) = \boldsymbol{b} = (b_1, b_2, \cdots, b_g), \tag{49}$$

where b_i is

$$b_i = b_i^{(2)}(m_{g+1}, m_{g+2}, \cdots, m_{2g}); i = 1, 2, \cdots, g. \tag{50}$$

Regarding $\boldsymbol{A} + \boldsymbol{b}$ as information symbols, we construct the code word $\boldsymbol{V}$:

$$(A(x) + b(x))x^g \equiv R(x) \bmod F(x), \tag{51}$$

where $F(x)$ is a primitive polynomial of degree g over $\mathbb{F}_2$.

$$V(x) = R(x) + x^g(A(x) + b(x)). \tag{52}$$

We then construct W(x):

$$\begin{aligned} W(x) &= V(x) + a(x) = a(x) + R(x) + x^g(A(x) + b(x)) \\ &= W_1 + W_2 x + \cdots + W_{2g} x^{2g-1}. \end{aligned} \tag{53}$$

From $\{W_i\}$, we construct the set of public keys $\{U_i\}$:

$$\boldsymbol{W} A_{III} = (U_1, U_2, \cdots, U_{2g}), \tag{54}$$

where A_{III} is a $2g \times 2g$ random permutation matrix.

The U_i is

$$U_i = U_i^{(2)}(M_1, M_2, \cdots, M_{2g}) \tag{55}$$

We see that the set of simultaneous equations $\{U_i\}$ cannot be systematically decoded.

We also see that K(X)RSE(2)PKC realizes the coding rate of exactly 1.0.