New Classes of Public Key Cryptosystems over $\mathbb{F}_{2^8}$ Constructed Based on Reed-Solomon Codes, K(XVII)SE(1)PKC and K(XVII)ΣΠPKC

Masao KASAHARA *

July 22, 2014

Abstract

In this paper, we present new classes of public key cryptosystem over $\mathbb{F}_{2^8}$ based on Reed-Solomon codes, referred to as K(XVII)SE(1)PKC and K(XVII)ΣΠPKC, a subclass of K(XVII)SE(1)PKC. We show that K(XVII)SE(1)PKC over $\mathbb{F}_{2^8}$ can be secure against the various attacks. We also present K(XVII)ΣΠPKC over $\mathbb{F}_{2^8}$, a subclass of K(XVII)SE(1)PKC. We show that any assertion of successfull attack on K(XVII)SE(1)PKC including K(XVII)ΣΠPKC whose parameters are properly chosen is a coding theoretical contradiction. We thus conclude that K(XVII)SE(1)PKC and K(XVII)ΣΠPKC would be secure against the various attacks including LLL attack.

The schemes presented in this paper would yield brand-new techniques in the field of code-based PKC.

keyword

Public Key Cryptosystem, Error-Correcting Code, Reed-Solomon code, Code based PKC, McEliece PKC.

1 Introduction

Various studies have been made of the Public-Key Cryptosystem(PKC). The security of PKC's proposed so far, in most cases, depends on the difficulty of discrete logarithm problem or factoring problem. For this reason, it is desired to investigate another classes of PKC's that do not rely on the difficulty of these two problems. The multivariate PKC is one of the very promising candidates of the member of such classes. However, most of the multivariate PKC's are constructed by the simultaneous equations of degree larger than or equal to 2 [1] $\sim$ [7]. Recently the author proposed a several classes of multivariate PKC's that are constructed by many sets of linear equations [8] $\sim$ [13] based on error-correcting code, in a sharp contrast with the conventional multivariate PKC where a set of simultaneous equations of degree more than or equal to 2 is used.

Let us refer to such PKC constructed based on error correcting code as code based PKC(CB·PKC). It should be noted that McEliece PKC [14], a class of CB·PKC, can be regarded as a member of the linear multivariate PKC.

In this paper, we present new classes of public key cryptosystem over $\mathbb{F}_{2^8}$ based on Reed-Solomon codes, referred to as K(XVII)SE(1)PKC and K(XVII)ΣΠPKC, a subclass of K(XVII)SE(1)PKC. We show that any assertion of successfull attack on K(XVII)SE(1)PKC including K(XVII)ΣΠPKC whose parameters are properly chosen is a coding theoretical contradiction. We thus conclude that K(XVII)SE(1)PKC and K(XVII)ΣΠPKC would be secure against the various attacks including LLL attack.

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

K(XVII)SE(1)PKC and K(XVII)ΣΠPKC have the following advantages :

A1 : K(XVII)SE(1)PKC and K(XVII)ΣΠ PKC over $\mathbb{F}_{2^8}$ can be constructed based on the Reed-Solomon code over $\mathbb{F}_{2^8}$, which is extensively used for the various storage and transmission systems.

A2 : In encryption and decryption process for (XVII)SE(1)PKC and K(XVII)ΣΠPKC, the conventional encoders and decoders for the Reed-Solomon code over $\mathbb{F}_{2^8}$ can be advantageously used.

Throughout this paper, the vector $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$ will be represented by the polynomial as

$$v(x) = v_1 + v_2 x + \cdots + v_n x^{n-1}. \tag{1}$$

2 K(XVII)SE(1)PKC over $\mathbb{F}_{2^8}$

2.1 Preminaries

Let us define several symbols:

$G(x)$	: generator polynomial of extended Reed-Solomon code*1 over $\mathbb{F}_{2^8}$.
g	: degree of $G(x)$.
D	: minimum distance of Reed-Solomon code generated with $G(x), g+1$.
$\boldsymbol{m}_\eta$	: first message, $(m_1, m_2, \cdots, m_\eta)$
$\boldsymbol{a}_t$	: second message, $(a_1, a_2, \cdots, a_t)$
$\boldsymbol{\alpha}_\tau$	: third message, $(\alpha_1, \alpha_2, \cdots, \alpha_\tau)$
$\{\boldsymbol{u}_i\}$	: set of first public key for $\boldsymbol{m}_\eta$
$\{\boldsymbol{s}_i\}$	: set of second public key for $\boldsymbol{\alpha}_\tau$
$\boldsymbol{w}_\mu$	: word for $\boldsymbol{m}_\eta$
$\boldsymbol{w}_\rho$	: word for $\boldsymbol{\alpha}_\tau$
$\boldsymbol{C}$	: Ciphertext, $\boldsymbol{w}_\mu + \boldsymbol{w}_\rho$
K	: $2^8 - g$.
$w(\boldsymbol{v})$	: Hamming weight of $\boldsymbol{v}$.
P	: random column permutation matrix.
P^{-1}	: inverse operation of P.
p	: random permutation determined from P .

Throughout this paper, we assume that any message symbol over $\mathbb{F}_{2^8}$ takes on a non-zero value.

2.2 First word, $\boldsymbol{w}_\mu$

Let $\boldsymbol{\mu}_i(x)$ be

$$\mu_i(x) = e_{i(1)} x^{(1)} + e_{i(2)} x^{(2)} + \cdots + e_{i(\eta)} x^{(\eta)}; i = 1, 2, \cdots, \eta, \tag{2}$$

where the exponent (i) satisfies

$$0 \leq (1) < (2) < \cdots < (\eta) \leq K - 1. \tag{3}$$

The coefficients $e_{i(j)}$'s are randomly chosen from $\mathbb{F}_{2^8}$, under the following condition:

Let the matrix M be

$$M = \begin{bmatrix} e_{1(1)}, & e_{1(2)}, & \cdots, & e_{1(\eta)} \\ e_{2(1)}, & e_{2(2)}, & \cdots, & e_{2(\eta)} \\ \vdots & \vdots & & \vdots \\ e_{\eta(1)}, & e_{\eta(2)}, & \cdots, & e_{\eta(\eta)} \end{bmatrix}. \tag{4}$$

*1 We assume the using of extended Reed-Solomon code. It is possible to extend by two symbols with double-tail construction due to Kasahara et.al. [15]

where $e_{i(j)}$'s are randomly chosen so that M may be non-singular.

We see that the Hamming weight of $\boldsymbol{\mu}_i, w(\boldsymbol{\mu}_i)$, is η or less. Let $\mu_i(x)$ be transformed to

$$\begin{aligned}\mu_i(x)x^g &\equiv r_i(x) \mod G(x),\\ &= r_{i1} + r_{i2}x + \cdots + r_{ig}x^{g-1}; i = 1, 2, \cdots, \eta.\end{aligned} \tag{5}$$

The code word is then

$$v_i(x) = \mu_i(x)x^g + r_i(x) \equiv 0 \mod G(x); i = 1, 2, \cdots, \eta. \tag{6}$$

Let R and $R \cdot P$ be

$$R = \begin{bmatrix} r_{11}, & r_{12}, & \cdots, & r_{1g} \\ r_{21}, & r_{22}, & \cdots, & r_{2g} \\ \vdots & \vdots & & \vdots \\ r_{\eta 1}, & r_{\eta 2}, & \cdots, & r_{\eta g} \end{bmatrix}. \tag{7}$$

$$R \cdot P = \begin{bmatrix} u_{11}, & u_{12}, & \cdots, & u_{1g} \\ u_{21}, & u_{22}, & \cdots, & u_{2g} \\ \vdots & \vdots & & \vdots \\ u_{\eta 1}, & u_{\eta 2}, & \cdots, & u_{\eta g} \end{bmatrix} = \begin{bmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_\eta \end{bmatrix} \tag{8}$$

where P is an $\eta \times g$ random column permutation matrix.

According to the random column permutation P, the row vector $\boldsymbol{r}_i$ is permuted to $\boldsymbol{u}_i$. We shall denote such permutation:

$$\boldsymbol{r}_i \cdot p = \boldsymbol{u_i}; i = 1, 2, \cdots, \eta. \tag{9}$$

Let us suppose that the elements of $\boldsymbol{u}_i$'s are ordered as $\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_\eta$. We shall refer to subscript j as location j.

Let the second message $a_t(x)$ be transformed to $a_T(x)$:

$$a_t(x) \mapsto a_T(x) = a_1x^{[1]} + a_2x^{[2]} + \cdots + a_tx^{[t]}; 0 \le [i] \le g-1, \tag{10}$$

where the exponents $[1], [2], \cdots, [t]$ are randomly chosen by a sender Bob.

These exponents satisfy

$$0 \le [1] < [2] < \cdots < [t-1] < [t] \le g-1. \tag{11}$$

Given the first message $\boldsymbol{m}_\eta = (m_1, m_2, \cdots, m_\eta)$, the first word $\boldsymbol{w}_\mu$ is

$$\boldsymbol{w}_\mu = m_1\boldsymbol{u}_1 + m_2\boldsymbol{u}_2 + \cdots + m_\eta\boldsymbol{u}_\eta. \tag{12}$$

The first ciphertext $\boldsymbol{C}_\mu$ is

$$\boldsymbol{C}_\mu = \boldsymbol{w}_\mu + \boldsymbol{a}_T. \tag{13}$$

From the Eqs.(9) and (12) we see that the randomly permuted version, $S_\mu \cdot p$, of the following syndrome S_μ proves to be

$$S_\mu = m_1\boldsymbol{r}_1 + m_2\boldsymbol{r}_2 + \cdots + m_\eta\boldsymbol{r}_\eta. \tag{14}$$

In the polynomial form, let $S_\mu \cdot p$ be denoted $S_\mu(x)p$.

We have the following straightforward theorem :

Theorem 1 : The syndrome $S_\mu p(x)$ is

$$m_1u_1(x) + m_2u_2(x) + \cdots + m_\eta u_\eta(x) \equiv \left[\sum_{i=1}^{\eta} \mu_i(x)x^g \bmod G(x)\right]p. \tag{15}$$

2.3 Second word $\boldsymbol{w}_\rho$

Let $\rho_i(x)$ be

$$\rho_i(x) = \varepsilon_i x^{i-1} + \beta_{i1}x^{\tau 1} + \beta_{i2}x^{\tau 2} + \cdots + \beta_{i\pi}x^{\tau\pi}; i = 1, 2, \cdots, 256. \tag{16}$$

where τi's satisfy

$$0 \leqq \tau 1 < \tau 2 < \cdots < \tau\pi \leqq 255. \tag{17}$$

Let $\boldsymbol{\epsilon}$ be

$$\boldsymbol{\epsilon}_i = (00\cdots 010 \cdots 0); i = 1, 2, \cdots, 256, \tag{18}$$

where only one nonzero element, 1, is located at the i-th cordinate.

In Fig.1, we show an example of $\{\boldsymbol{\rho}_i\}$ over $\mathbb{F}_{2^8}$.

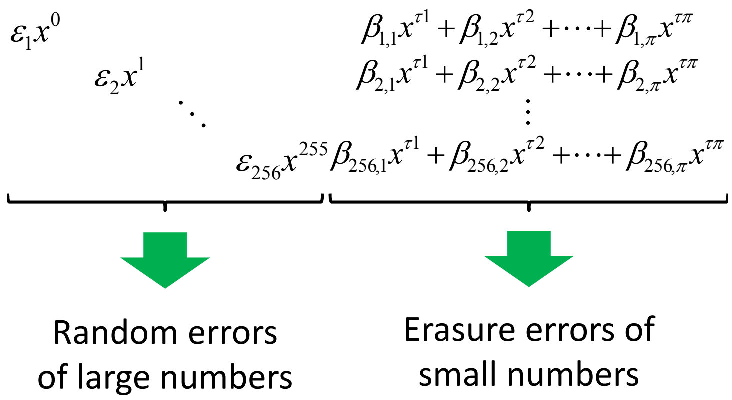

Figure 1: An example of $\{\boldsymbol{\rho}_i\}$ over $\mathbb{F}_{2^8}$.

For the third message $\boldsymbol{\alpha}_\tau = (\alpha_1, \alpha_2, \cdots, \alpha_\tau)$, the sender Bob randomly selects locations $(1), (2), \cdots, (\tau)$ from the set $\{i\}$. The random errors $\boldsymbol{E}_r$ and the erasure errors $\boldsymbol{E}_e$ are represented by the following polynomial form:

$$E_r(x) = \sum_{i=1}^{\tau} \alpha_{(i)}\varepsilon_{(i)}x^{(i)-1} \tag{19}$$

$$E_e(x) = \sum_{i=1}^{\tau}\sum_{j=1}^{\pi} \alpha_{(i)}\beta_{(i)j}x^{\tau_j} \tag{20}$$

Let $\varepsilon_i(x)$ and $\boldsymbol{\beta}_i(x)$ be

$$\begin{aligned} &\varepsilon_i(x) = \varepsilon_i x^{i-1}; i = 1, 2, \cdots, 256, \\ &\beta_i(x) = \beta_{i1}x^{\tau 1} + \beta_{i2}x^{\tau 2} + \cdots + \beta_{i\pi}x^{\tau\pi}; i = 1, 2, \cdots, 256. \end{aligned} \tag{21}$$

The $\rho_i(x)$ is

$$\rho_i(x) = \varepsilon_i(x) + \beta_i(x); i = 1, 2, \cdots, 256. \tag{22}$$

We see that $\boldsymbol{\rho}_i$ can be represented by

$$\boldsymbol{\rho}_i = \boldsymbol{\epsilon}_i + \boldsymbol{\beta}_i; i = 1, 2, \cdots, 256. \tag{23}$$

Let $\rho_i(x)$ be transformed to

$$\begin{aligned}\rho_i(x)\cdot x^g &\equiv t_i(x) \bmod G(x)\\ &= t_{i1}+t_{i2}+\cdots+t_{ig}x^{g-1}; i=1,2,\cdots,256.\end{aligned} \tag{24}$$

Let A_t and $A_t \cdot P$ be

$$A_t = \begin{bmatrix} t_{1,1}, & t_{1,2}, & \cdots, & t_{1,g} \\ t_{2,1}, & t_{2,2}, & \cdots, & t_{2,g} \\ \vdots & \vdots & & \vdots \\ t_{256,1}, & t_{256,2}, & \cdots, & t_{256,g} \end{bmatrix} = \begin{bmatrix} \boldsymbol{t}_1 \\ \boldsymbol{t}_2 \\ \vdots \\ \boldsymbol{t}_{256} \end{bmatrix}, \tag{25}$$

$$A_t \cdot P = \begin{bmatrix} s_{1,1}, & s_{1,2}, & \cdots, & s_{1,g} \\ s_{2,1}, & s_{2,2}, & \cdots, & s_{2,g} \\ \vdots & \vdots & & \vdots \\ s_{256,1}, & s_{256,2}, & \cdots, & s_{256,g} \end{bmatrix} = \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \\ \vdots \\ \boldsymbol{s}_{256} \end{bmatrix}. \tag{26}$$

The word $\boldsymbol{w}_\tau$, for the third message $\boldsymbol{\alpha}_\tau = (\alpha_1, \alpha_2, \cdots, \alpha_\tau)$, is

$$\boldsymbol{w}_\rho = \alpha_1 \boldsymbol{s}_{(1)} + \alpha_2 \boldsymbol{s}_{(2)} + \cdots + \alpha_\tau \boldsymbol{s}_{(\tau)}, \tag{27}$$

where $\boldsymbol{s}_{(1)}, \boldsymbol{s}_{(2)}, \cdots, \boldsymbol{s}_{(\tau)}$ are randomly selected public key from the set of public keys, $\{\boldsymbol{s}_i\}$.

We let the following relation hold:

$$\pi + 2(\tau + t) + 1 = D. \tag{28}$$

2.4 Ciphertext $\boldsymbol{C}$ for $\boldsymbol{m}_\eta$, $\boldsymbol{a}_t$ and $\boldsymbol{\alpha}_\tau$

The ciphertext $\boldsymbol{C}$ is

$$\boldsymbol{C} = \boldsymbol{w}_\mu + \boldsymbol{a}_T + \boldsymbol{w}_\rho. \tag{29}$$

Set of keys are :

Public key	:	$\{\boldsymbol{u}_i\}$, $\{\boldsymbol{s}_i\}$
Secret key	:	$\{\boldsymbol{\mu}_i\}, \{\boldsymbol{\rho}_i\}, \{\boldsymbol{r}_i\}, \{\boldsymbol{t}_i\}, P, p$

2.5 Encryption and decryption

Brief description of the encryption process

The encryption can be performed by the following steps :

- S1 : Given the first messge $\boldsymbol{m}_\eta = (m_1, m_2, \cdots, m_\eta)$, Bob calculates the word $\boldsymbol{w}_\mu$.
- S2 : Given the second message $\boldsymbol{a}_t = (a_1, a_2, \cdots, a_t)$, Bob randomly select locations $[1], [2], \cdots, [t]$ and calculates $\boldsymbol{a}_T$.
- S3 : Given the third message $\boldsymbol{\alpha}_\tau = (\alpha_1, \alpha_2, \cdots, \alpha_\tau)$, Bob randomly selects public keys, $\boldsymbol{s}_{(1)}, \boldsymbol{s}_{(2)}, \cdots, \boldsymbol{s}_{(\tau)}$ from the set of public keys, $\{\boldsymbol{s}_i\}$, and calculates $\boldsymbol{w}_\rho$.
- S4 : Bob calculates the ciphertext C :
  $C = \boldsymbol{w}_\mu + \boldsymbol{a}_T + \boldsymbol{w}_\rho$.

Brief description of the decryption process

The decryption process can be performed by the following steps :

- S1 : Alice calculates
  $\boldsymbol{C}P^{-1} = s_\mu + s_\rho + \boldsymbol{a}_T P^{-1}$,
  where s_μ is the syndrome due to the first message $\boldsymbol{m}_\eta = (m_1, m_2, \cdots, m_\eta)$ and s_ρ, the syndrome due to the third message $\boldsymbol{\alpha}_\tau = (\alpha_1, \alpha_2, \cdots, \alpha_\tau)$.
- S2 : Based on the syndromes $s_\mu + s_\rho + a_T P^{-1}$, Alice decodes $\boldsymbol{m}_\eta$, $\boldsymbol{\alpha}_\tau$, and $a_T P^{-1}$ using erasure and errors decoding for Reed-Solomon code [16]. Alice calculate $a_T P^{-1} P = a_T$, yielding a_t,.

2.6 Security considerations

In this subsection we assume the following parameters are chosen:
$m = 8, g = 128, K = 128, \eta = 56, t = 32, \pi = 8$.

Attack 1 : Exhaustive attack on vector $\boldsymbol{\mu}_i$

The probability that the vector $\boldsymbol{\mu}_i$ is estimated correctly, $P_c[\widehat{\boldsymbol{\mu}_i}]$ is

$$P_c[\hat{\boldsymbol{\mu}}_i] = \begin{pmatrix} K \\ \eta \end{pmatrix}^{-1} (2^m - 1)^{-\eta} < 1.93 \times 10^{-172}. \tag{30}$$

We conclude that K(XVII)SE(1)PKC is secure against Attack 1.

Attack 2 : Exhaustive attack on permutation matrix, P

The probability that the matrix P is estimated correctly is

$$P_c[\hat{P}] = (g!)^{-1} < 2.60 \times 10^{-216}, \tag{31}$$

yielding an extremely small value.

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

Attack 3 : Exhaustive attack on vector $\boldsymbol{\rho}_i$.

The probability that the vector $\boldsymbol{\rho}_i$ is estimated correctly is

$$P_c[\hat{\boldsymbol{\rho}}_i] = \begin{pmatrix} K \\ 1 \end{pmatrix}^{-1} 2^{-m} \begin{pmatrix} K \\ \pi \end{pmatrix}^{-1} 2^{-m\pi} = 1.15 \times 10^{-36}, \tag{32}$$

a sufficiently small value.

We conclude that K(XVII)SE(1)PKC is secure against Attack 3.

Attack 4 : Exhaustive attack on the selected locations, (1), (2),$\cdots$, (t).

The probability that t locations among 256 locations are estimated correctly, $P_c[\{(\hat{i})\}]$ is

$$P_c[\{(\hat{i})\}] = \begin{pmatrix} 256 \\ t \end{pmatrix}^{-1} < 1.71 \times 10^{-41}, \tag{33}$$

a sufficiently small value.

Attack 5 : Attack on ciphertext $\boldsymbol{C} = \boldsymbol{w}_\mu + \boldsymbol{w}_\rho$.

Suppose that $\boldsymbol{w}_\mu$ only is given as a ciphertext and consider the following Only $\boldsymbol{w}_\mu$ Attack: Namely we suppose that the ciphertext $\boldsymbol{C}$ is $\boldsymbol{C} = \boldsymbol{w}_\mu$.

Only $\boldsymbol{w}_\mu$ Attack :

We see that $\{\boldsymbol{\mu}_i\}$ spans a vector space of dimension η. As a result any η error-free symbols (efs), $w_{(1)}, w_{(2)}, \cdots, w_{(\eta)}$ of word $\boldsymbol{w}_\mu$ is able to disclose the message $\boldsymbol{m}_\eta$ by solving the equation:

$$m_1\boldsymbol{u}_1 + m_2\boldsymbol{u}_2 + \cdots + m_\eta\boldsymbol{u}_\eta = (w_{(1)}, w_{(2)}, \cdots, w_{(\eta)}). \tag{34}$$

The probability that η efs's are estimated correctly, for $m = 8$, is

$$P_c[\widehat{efs}] = \frac{\begin{pmatrix} g - t \\ \eta \end{pmatrix}}{\begin{pmatrix} g \\ \eta \end{pmatrix}} = 1.24 \times 10^{-11}. \tag{35}$$

.

We conclude that K(XVII)SE(1)PKC is not secure against Only $\boldsymbol{w}_\mu$ Attack

Suppose also that $\boldsymbol{w}_\rho$ only is given and consider the following Only $\boldsymbol{w}_\rho$ Attack. Namely we let the ciphertext $\boldsymbol{C}$ be $\boldsymbol{C} = \boldsymbol{w}_\rho$.

Only $\boldsymbol{w}_\rho$ Attack

Theorem 1: In order to correct random error $E_r(x)$ and erasure error $E_e(x)$, the syndrome $S_\rho(x)$ is required to be correctly given.

Proof: The following straightforward relation holds:

$$(E_r(x) + E_e(x))x^g \equiv S_\rho(x) \bmod G(x), \tag{36}$$

for correctly given syndrome $S_\rho(x)$. Suppose that the following relation holds for $S'_\rho(x) \neq S_\rho(x)$:

$$(E_r(x) + E_e(x))x^g \equiv S'_\rho(x) \bmod G(x), \tag{37}$$

for incorrectly given $S'_\rho(x)$.

From Eqs.(36) and (37), the relation:

$$0 \equiv S_\rho(x) + S'_\rho(x) \bmod G(x), \tag{38}$$

which is contradictory, yielding the proof. □

Theorem 2: For Only $\boldsymbol{w}_\rho$ Attack, even if the syndrome is correctly given, with no knowledge of locations of erasure errors, $\tau 1, \tau 2, \cdots, \tau\pi$, the assertion that random errors $\boldsymbol{E}_r$ and erasure errors $\boldsymbol{E}_e$ can be successfully corrected is a coding theoretical contradiction.

Proof: In K(XVII)SE(1)PKC, the relation $\pi + 2(t + \tau) + 1 = D$ holds (Eq.(28)). In order to correct erasure errors as random errors, the following relation is asked to hold:

$$2\pi + 2(t + \tau) + 1 = D, \tag{39}$$

which is contradictory to Eq.(28), yielding the proof. □

We have seen that K(XVII)SE(1)PKC is secure against Only $\boldsymbol{w}_\rho$ Attack. Besides $\boldsymbol{w}_\mu$ is added to $\boldsymbol{w}_\rho$ as an entirely independent noisy vector. It should be noted that the word $\boldsymbol{w}_\mu$ is constructed independently of the word $\boldsymbol{w}_\rho$.

We conclude that K(XVII)SE(1)PKC is secure against Attack 5.

3 Product sum type PKC, K(XVII)ΣΠPKC

We have seen that K(XVII)SE(1)PKC is secure against Only $\boldsymbol{w}_\rho$ Attack, which implies that a particular member of the class of K(XVII)SE(1)PKC can be an independent class of PKC that uses only $\boldsymbol{s}_i$ as a public key. As this class of PKC is proved to be a product sum type PKC, often referred to as knapsack type PKC, we shall refer to this PKC as K(XVII)ΣΠ PKC. In K(XVII)ΣΠPKC, let us consider only third messege $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_\tau)$. The ciphertext $\boldsymbol{C}_\rho = \boldsymbol{w}_\rho$ is

$$\boldsymbol{C}_\rho = \alpha_1 s_{(1)} + \alpha_2 s_{(2)} + \cdots + \alpha_\tau s_{(\tau)}, \tag{40}$$

where $s_{(i)}$ is a public key randomly chosen from the set of public keys $\{s_{(i)}\}$.

In Fig.2, we show a schematic illustration of encryption.

We have seen that K(XVII)ΣΠPKC can be secure against Attack 2, Attack 3 and Only $\boldsymbol{w}_\rho$ Attack.

We conclude that K(XII)ΣΠPKC would be secure against the possible attacks including the LLL attack.

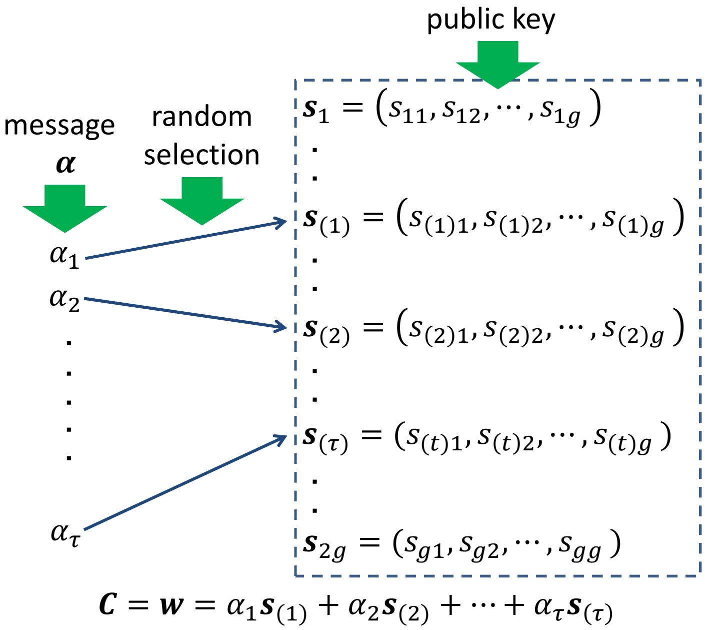

Figure 2: Schematic illustration of encryption.

4 Conclusion

We have presented a new class of public key cryptsystem, referred to as K(XVII)SE(1)PKC and K(XVI I)ΣΠPKC based on the Reed-Solomon code over $\mathbb{F}_{2^8}$ that are extensively used for the various storage and transmission systems.

We have shown that any assertion that K(XVII)SE(1)PKC and K(XVII)ΣΠPKC can be broken is contradictory from the coding theoretical point of view, provided that the parameters π, τ and t are properly chosen.

We thus conclude that K(XVI)SE(1)PKC and K(XVII)SE(1)PKC over $\mathbb{F}_{2^8}$ can be secure against the various attacks.

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

References

[1] M. Kasahara, "A New Class of Public Key Cryptosystems Constructed Based on Reed-Solomon Codes K(XII)SE(1)PKC", Technical Report of IEICE, ISEC 2013-5 (2013-05).

[2] 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).

[3] 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).

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

[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] J. C. Faugere and A. Joux "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases", In Advances in Cryptoglogy-CRYPTO 2003 pp.44-60 (2003).

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

[8] 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).

[9] M. Kasahara "A New Class of Public Key Cryptosystems Constructed Based on Perfect Error-Correcting Codes Realizing Coding Rate of exactly 1.0", Cryptology ePrint Archive , Report 2010/139 (2010-03).

[10] M. Kasahara "A Construction of New Class of Linear Multivariate Public Key Cryptosystem Constructed Based on Error Correcting Codes", Technical Report of IEICE , ISEC 2009-135 (2010-03).

[11] M. Kasahara: "Public Key Cryptosystems Constructed Based on Pseudo Cyclic Codes, K(Ⅸ)SE(1)PKC, Realizing Coding Rate of Exactly 1.0", Cryptology ePrint Archive, Report 2011/545, (2011-09).

[12] M. Kasahara: "A New Class of Product-sum Type Public Key Cryptosystem, K(V)ΣΠPKC, Constructed Based on Maximum Length Code", Cryptology ePrint Archive, Report 2013/180, (2013-03).

[13] M. Kasahara: "A New Class of Public Key Cryptosystems Construted Based on Reed-Solomon Codes, K(Ⅱ)SE(1)PKC.–Along with a presentation of K(Ⅱ)SE(1)PKC over the extension field extensively used for present day various storage and transmission systems", Cryptology ePrint Archive, Report 2013/363, (2013-06).

[14] R. J. McEliece: "A Public-key Cryptosystem Based on Algebraic Coding Theory", DSN Progress Report, no.42-44, pp.114-116 (1978).

[15] F. J. MacWilliams and N. J. A. Sloane: "The Theory of Error-Correcting Codes", North-Holland, (1977).

[16] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa: "An Erasures-and-Errors decoding Algorithm for Goppa Codes", IEEE Trans. on Inform. Theory, IT-22, 2, pp.238-241 (1976-03).