A New Class of Public Key Cryptosystems Constructed Based on Reed-Solomon Codes, K(XII)SE(1)PKC. – Along with a presentation of K(XII)SE(1)PKC over the extension field $\mathbb{F}_{2^8}$ extensively used for present day various storage and transmission systems –

Masao KASAHARA *

Abstract

In this paper, we present a new class of public key cryptosystem based on Reed-Solomon codes, a member of the code based PKC(CBPKC), referred to as K(XII)SE(1)PKC. We show that K(XII)SE(1)PKC can be secure against the various attacks. Particularly we present a member of K(XII)SE(1)PKC constructed based on the Reed-Solomon code over the extension field $\mathbb{F}_{2^8}$, which is extensively used in the present day storage systems and the various digital transmission systems. In a sharp contrast with the conventional CBPKC that uses Goppa code, in K(XII)SE(1)PKC, we do not care for the security of the primitive polynominal that generates the Reed-Solomon code.

keyword

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

1 Introduction

Various studies have been made of the Public Key Cryptosystem(PKC). The security of the 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 a 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 linear multivariate PKC's that are constructed by many sets of linear equations [8] $\sim$ [13] based on error-correcting code. It should be noted that McEliece PKC [14], a class of code based PKC(CB·PKC), can be regarded as a class of the linear multivariate PKC. Excellent analyses and survey are given in Refs. [15] and [16]

In this paper, we present a new class of public key cryptosystem based on Reed-Solomon codes, a member of CB·PKC, referred to as K(XII)SE(1)PKC. We show that K(XII)SE(1)PKC can be secure against the various attacks. Particularly we present CB·PKC constructed based on the Reed-Solomon code over $\mathbb{F}_{2^8}$, which is extensively used in the present day storage systems and the various digital transmission systems. In a sharp

*Research Institute for Science and Engineerging, Waseda University. kasahara@ogu.ac.jp

contrast with the conventional CB·PKC that uses Goppa code, in K(XII)SE(1)PKC, we do not care for the security of the primitive polynominal that generates the Reed-Solomon code.

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 Construction of K(XII)SE(1)PKC

2.1 Preliminaries

Let us define several symbols.

$\boldsymbol{m}$: I·message, $(m_1, m_2, \cdots, m_\lambda)$ over $\mathbb{F}_{2^m}$, where we assume that $\lambda < k$ and $m_i \neq 0; i = 1, 2, \cdots, \lambda$.

$\boldsymbol{a}$: II·message, $(a_1, a_2, \cdots, a_t)$ over $\mathbb{F}_{2^m}$, where we let $a_i \neq 0; i = 1, 2, \cdots, t$.

$G(x)$: generator polynomial of degree g, over $\mathbb{F}_{2^m}$, where we let $g > t$.

E : exponent to which $G(x)$ belongs, exponent of $G(x)$ for short.

$|A|$: size of A (in bit).

$P_c[\hat{A}_i]$: probability that the event A_i is correctly estimated by an exhaustive attack.

$\{\boldsymbol{u}_i\}$: set of public keys over $\mathbb{F}_{2^m}$, $\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_i, \cdots, \boldsymbol{u}_k$.

$Loc(\boldsymbol{u}_i)$: location of $\boldsymbol{u}_i$ in the pulic key set $\boldsymbol{u}_i, i$.

2.2 Theoretical background of present paper

In 1970's, the various works were made of the jointly optimization problems for realizing a high speed and a reliable digital transmission system. One of the most popularly known and highly focused result is the optimum decoding schemes, for partial response type channels, with Vitebi decoding [17]. The author was also much involved in the study of the jointly optimization problems for source and channel coding, syndrome coding, base on algebraic coding theory. However unfortunately syndrome coding itself was considered not worthy of note, although another coding scheme such as vector quantization [18] was the center of attension among the researchers working on source coding theory. Let us show an example of a communication system using syndrome coding.

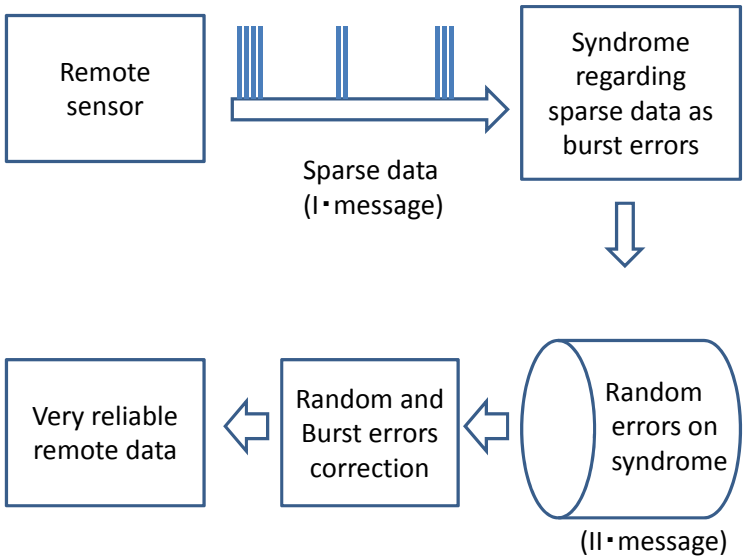

Fig. 1: An example of communication system using syndrome coding.

As shown in Fig.1, the sparse data is an example of I·message $\boldsymbol{m}$ and the random error vector, that of Ⅱ·message $\boldsymbol{a}$.

2.3 Construction of public key

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

$$\varepsilon_i(x) = \varepsilon_{i1}x^{①} + \varepsilon_{i2}x^{②} + \cdots + \varepsilon_{i\eta}x^{⑦}; i = 1, 2, \cdots, k, \tag{3}$$

where ε_{ij} takes on a random value over $\mathbb{F}_{2^m}$.

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

$$\rho_i(x) = \rho_i x^{\bar{i}}; i = 1, 2, \cdots, k, \tag{4}$$

where $\bar{i} \neq \bar{l}$ for $i \neq l$ and λ_i takes on a non-zero random value over $\mathbb{F}_{2^m}$.

We now let carrier μ_i be

$$\mu_i(x) = \varepsilon_i(x) + \rho_i(x); i = 1, 2, \cdots, k. \tag{5}$$

We see that the Hamming weight of $\boldsymbol{\mu}_i$, $w(\boldsymbol{\mu}_i)$, is

$$w(\boldsymbol{\mu}_i) = \eta + 1. \tag{6}$$

Let carrier $\mu_i(x)$ of the Hamming weight $\eta + 1$ be transformed into

$$\begin{aligned} \mu_i(x)x^g &\equiv r_i(x) \mod G(x)\ ; i = 1, 2, \cdots, k. \\ &= r_{i1} + r_{i2}x + \cdots + r_{ig}x^{g-1}. \end{aligned} \tag{7}$$

We then have the code word $v_i(x)$ as

$$v_i(x) = \mu_i(x)x^g + r_i(x) \equiv 0 \mod G(x). \tag{8}$$

Let the code words of $\{\boldsymbol{v}_i\}$ be

$$\begin{aligned}
\boldsymbol{v}_1 &= (\mu_{11}, \mu_{12}, \cdots, \mu_{1K}, r_{11}, r_{12}, \cdots, r_{1g}), \\
\boldsymbol{v}_2 &= (\mu_{21}, \mu_{22}, \cdots, \mu_{2K}, r_{21}, r_{22}, \cdots, r_{2g}), \\
&\vdots \\
\boldsymbol{v}_k &= (\mu_{k1}, \mu_{k2}, \cdots, \mu_{kK}, r_{k1}, r_{k2}, \cdots, r_{kg}).
\end{aligned} \tag{9}$$

Let A_r be

$$A_r = \begin{bmatrix} r_{11}, & r_{12}, & \cdots, & r_{1g} \\ r_{21}, & r_{22}, & \cdots, & r_{2g} \\ \vdots & \vdots & & \vdots \\ r_{k1}, & r_{k2}, & \cdots, & r_{kg} \end{bmatrix}, \tag{10}$$

where we let

$$\boldsymbol{r}_i = (r_{i1}, r_{i2}, \cdots, r_{ig}). \tag{11}$$

The matrix A_r is transformed into

$$A_r \cdot P_I = \begin{bmatrix} u_{11}, & u_{12}, & \cdots, & u_{1g} \\ u_{21}, & u_{22}, & \cdots, & u_{2g} \\ \vdots & \vdots & & \vdots \\ u_{k1}, & u_{k2}, & \cdots, & u_{kg} \end{bmatrix}, \tag{12}$$

where P_I is a $k \times g$ random column permutation matrix.

Let $\boldsymbol{u}_i$ be

$$\boldsymbol{u}_i = (u_{i1}, u_{i2}, \cdots, u_{ig}). \tag{13}$$

The set $\{\boldsymbol{u}_i\}$ will be publicized.

Remark 1 : For hiding the structure of the Reed-Solomon code generated by $G(x)$, we shall use $\boldsymbol{\mu}_i$'s of Hamming weight of 6∼10, for a small m such that $m \gtrsim 8$ from the standpoint of security.

2.4 Construction of ciphertext

Let the λ public keys randomly chosen by Bob from the set $\boldsymbol{u}_i$ be denoted $\boldsymbol{u}^{(1)}, \boldsymbol{u}^{(2)}, \cdots, \boldsymbol{u}^{(\lambda)}$ where the location of $\boldsymbol{u}^{(i)}$, $Loc(\boldsymbol{u}^{(i)})$ satisfies

$$Loc(\boldsymbol{u}^{(i)}) < Loc(\boldsymbol{u}^{(j)}) \ for \ 1 \le i < j \le k. \tag{14}$$

As we see in Fig.2 λ carriers $\boldsymbol{\mu}^{(1)}, \boldsymbol{\mu}^{(2)}, \cdots, \boldsymbol{\mu}^{(\lambda)}$ are selected in accordance with the random choice of public keys $\boldsymbol{u}^{(1)}, \boldsymbol{u}^{(2)}, \cdots, \boldsymbol{u}^{(\lambda)}$.

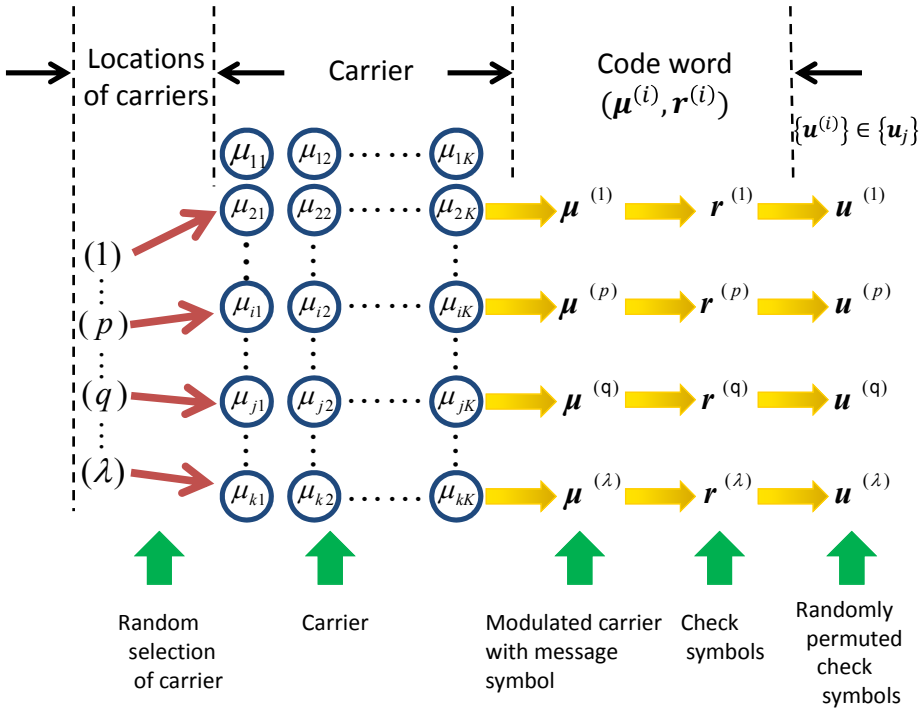

Fig. 2: Randomly chosen $\boldsymbol{u}_i$'s for I·message$(m_1, m_2, \cdots, m_\lambda)$

In Fig.2, $\boldsymbol{\mu}^{(p)}$ denotes $m_p\boldsymbol{\mu}_i$. The check symbols $\boldsymbol{r}^{(p)}$ is

$$m_p\mu_i(x) \equiv r^{(p)}(x) \bmod G(x). \tag{15}$$

Let the word $\boldsymbol{u}^{(m)}$ be defined as the word $\boldsymbol{u}$ for the message $\boldsymbol{m} = (m_1, m_2, \cdots, m_\lambda)$:

$$\boldsymbol{u}^{(m)} = m_1\boldsymbol{u}^{(1)} + m_2\boldsymbol{u}^{(2)} + \cdots + m_\lambda\boldsymbol{u}^{(\lambda)}. \tag{16}$$

We shall see, in the followings, that $\widetilde{\boldsymbol{u}}^{(m)}$ is a syndrome due to η erasure errors and λ random errors.

According to the random choice of $\boldsymbol{u}^{(1)}, \boldsymbol{u}^{(2)}, \cdots, \boldsymbol{u}^{(\lambda)}$ for the given message $\boldsymbol{m} = (m_1, m_2, \cdots, m_\lambda)$, the λ carriers $\boldsymbol{\mu}^{(1)}, \boldsymbol{\mu}^{(2)}, \cdots, \boldsymbol{\mu}^{(\lambda)}$ are selected. The word $\boldsymbol{u}^{(m)}$ is then

$$\boldsymbol{u}^{(m)} = \boldsymbol{\varepsilon}^{(m)} + \boldsymbol{\rho}^{(m)}, \tag{17}$$

where $\boldsymbol{\varepsilon}^{(m)}$ and $\boldsymbol{\rho}^{(m)}$ are

$$\begin{aligned} \boldsymbol{\varepsilon}^{(m)} &= \boldsymbol{\varepsilon}^{(1)} + \boldsymbol{\varepsilon}^{(2)} + \cdots + \boldsymbol{\varepsilon}^{(\lambda)} \\ \boldsymbol{\rho}^{(m)} &= \boldsymbol{\rho}^{(1)} + \boldsymbol{\rho}^{(2)} + \cdots + \boldsymbol{\rho}^{(\lambda)} \end{aligned} \tag{18}$$

From Eqs.(3) and (4), we see that $\boldsymbol{\varepsilon}^{(m)}$ results in η erasure errors and $\boldsymbol{\rho}^{(m)}$, λ random errors.

Throughout this paper we assume that Bob randomly selects a set of location $\{(i)\}$ all over again for each given I·message, from the stand point of security.

In Fig.3, let us show an example of how to obtain word $\boldsymbol{u}^{(m)}$, when $\boldsymbol{m} = (m_1, m_2)$ is given. In Fig.3, Bob randomly chooses $\boldsymbol{u}^{(2)}$ and $\boldsymbol{u}^{(5)}$ from the set of public key $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_n\}$. We see that in accordance with this random choice of $\boldsymbol{u}_2$ and $\boldsymbol{u}_5$, $\boldsymbol{\mu}^{(2)}$ and $\boldsymbol{\mu}^{(5)}$ are selected.

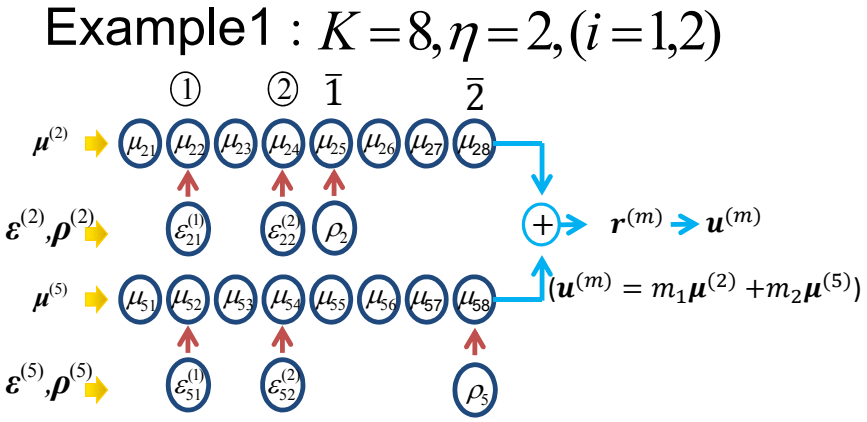

Fig. 3: Toy example of $\{\boldsymbol{\mu}^{(i)}, \boldsymbol{\varepsilon}^{(i)}, \boldsymbol{\rho}^{(i)}\}$.

For Ⅱ·message $\boldsymbol{a} = (a_1, a_2, \cdots, a_t)$, Bob constructs the message polynomial :

$$\begin{aligned} a_t(x) = \quad & a_1 x^{[1]} + a_2 x^{[2]} + \cdots + a_t x^{[t]}; \\ & 0 \le [i] \le g-1, \end{aligned} \tag{19}$$

where the locations $[1], [2], \cdots, [t]$ satisfies

$$1 \le [1] < [2] < \cdots < [t-1] < [t] \le g-1. \tag{20}$$

Throughout this paper, we also assume that Bob randomly selects a set of locations$\{[i]\}$, all over again, for each given Ⅱ·message.

The ciphertext is then

$$\boldsymbol{C} = \boldsymbol{u}^{(m)} + \boldsymbol{a}_t. \tag{21}$$

The minimum distance, D, of the Reed-Solomon code generated by $G(x)$ of degree g is

$$D = g + 1. \tag{22}$$

The following relation :

$$2(\lambda + t) + \eta + 1 = D, \tag{23}$$

is required to hold so that the messages $\boldsymbol{m}$ and $\boldsymbol{a}$ may be correctly decoded.

2.5 Encryption and decryption processes.

[Encryption process]

Step 1 : Given Ⅰ·message $\widetilde{\boldsymbol{m}} = (\widetilde{m}_1, \widetilde{m}_1, \cdots, \widetilde{m}_\lambda)$, Bob chooses λ vectors $\widetilde{\boldsymbol{u}}^{(1)}, \widetilde{\boldsymbol{u}}^{(2)}, \cdots, \widetilde{\boldsymbol{u}}^{(\lambda)}$ from the set $\{\boldsymbol{u}_i\}$ in a totally random manner under the condition that the following relation holds: $\begin{pmatrix} k \\ \lambda \end{pmatrix} \gtrsim 2^{80}$.

Step 2 : Bob calculates the word : $\widetilde{\boldsymbol{u}} = \widetilde{\boldsymbol{u}}^{(1)} + \widetilde{\boldsymbol{u}}^{(2)} + \cdots + \widetilde{\boldsymbol{u}}^{(\lambda)}$.

Step 3 : Given Ⅱ·message $\widetilde{\boldsymbol{a}} = (\widetilde{a}_1, \widetilde{a}_2, \cdots, \widetilde{a}_t)$, Bob randomly chooses the locations $[1], [2], \cdots, [t]$.

Step 4 : Bob transforms the message vector $\widetilde{a(x)}$ into $\widetilde{a}_t(x) = \widetilde{a}_1 x^{[1]} + \widetilde{a}_2 x^{[2]} + \cdots + \widetilde{a}_t x^{[t]}$.

Step 5 : Bob calculates the ciphertext $\widetilde{C}(x)$ by $\widetilde{C}(x) = \widetilde{u}(x) + \widetilde{a}_t(x)$.

Step 6 : Bob sends the ciphertext $\widetilde{\mathbb{C}}$ to Alice.

[Decryption process]

Step 1 : Recieving the ciphertext $\widetilde{\mathbb{C}}(=\widetilde{\boldsymbol{u}}+\widetilde{\boldsymbol{a}}_t)$ from Bob, Alice calculates :
$(\widetilde{\boldsymbol{u}}+\widetilde{\boldsymbol{a}}_t)P_I^{-1}=\widetilde{\boldsymbol{r}}+\widetilde{\boldsymbol{\alpha}}_t$, where $\widetilde{\boldsymbol{\alpha}}_t=\widetilde{\boldsymbol{a}}_tP_I^{-1}$.
Let $\widetilde{\boldsymbol{r}}+\widetilde{\boldsymbol{\alpha}}_t$ be denoted $\widetilde{\boldsymbol{r}}+\widetilde{\boldsymbol{\alpha}}_t=\widetilde{\mathbb{C}}^*=(\widetilde{c}_1^*,\widetilde{c}_2^*,\cdots,\widetilde{c}_g^*)$.

Step 2 : Given $\widetilde{\mathbb{C}}^*$, Alice decodes $\widetilde{\boldsymbol{m}}=(\widetilde{m}_1,\widetilde{m}_2,\cdots,\widetilde{m}_t)$ and $\widetilde{\boldsymbol{\alpha}}_t$ for example, with Euclidean decoding algorithm [19] [20].

Step 3 : Alice decodes $\widetilde{\boldsymbol{a}}=(\widetilde{a}_1,\widetilde{a}_2,\cdots,\widetilde{a}_t)$ by performing P_I on $\widetilde{\boldsymbol{\alpha}}_t$.

2.6 Parameters

For simplicity, let us consider the Reed-Solomon code with the following parameters :

$$k=g. \tag{24}$$

The coding rate ρ is

$$\rho=\frac{(\lambda+t)m+\log_2\left(\begin{array}{c}k\\ \lambda\end{array}\right)\left(\begin{array}{c}k\\ t\end{array}\right)}{gm}, \tag{25}$$

where we assume the following :

$$\log_2(2^m-1)\cong m,\ \text{for } m\geq 8. \tag{26}$$

Remark 2: When calculating the coding rate of Eq.(25), we take the amount of information due to the way of random choices of λ locations and t locations into account.

3 Security considerations and countermeasure

Remark 3: The using of the Reed-Solomon codes is very attractive because they are extensively used for the various storage systems such as CD or DVD. However, so far, the using of Reed-Solomon code has been supposed to be a little dangerous as the generater polynomial can be estimated without much difficulty compared with the Goppa code. However the author is certain that even if the generator polynomial is disclosed, our proposed K(XII)SE(1)PKC can be made sufficiently secure as we shall see below.
One of the most strong attacks to our proposed scheme is the following attack.

Attack 1: Exhaustive attack for disclosing the structure of code word

When discussing the security of K(XII)SE(1)PKC, from a conservative point of view, we assume that the generator polynominal $G(x)$ is not required to be kept secret, although it is not at all required to be made public.

Let the probability that all $\boldsymbol{\varepsilon}_i$'s and $\boldsymbol{\rho}_i$ of $\boldsymbol{\mu}_i$ are estimated correctly be denoted $P_c[\boldsymbol{\varepsilon}_i,\boldsymbol{\rho}_i]$. Then

$$P_c[\hat{\boldsymbol{\varepsilon}}_i,\hat{\boldsymbol{\rho}}_i]=\left(\begin{array}{c}k\\ \eta+1\end{array}\right)^{-1}(2^m)^{-(\eta+1)};i=1,2,\cdots,k;j=1,2,\cdots,\eta. \tag{27}$$

In order to be secure against Attack I for $m=8$ the following parameters are recommended

$$\begin{aligned}&K=135\\ &\eta\geq 6\\ &k=g=120,\end{aligned} \tag{28}$$

yielding

$$P[\{\hat{\tilde{\varepsilon}}_i, \hat{\tilde{\boldsymbol{\rho}}}_i\}] \leq \left(\begin{array}{c} 135 \\ 7 \end{array} \right)^{-1} (2^8)^{-7} = 1.00 \times 10^{-28}, \tag{29}$$

a sufficiently small value.

Attack 2: Attack on I-message $\widetilde{m}$

Attack 2 can be performed by the following steps :

Step 1 : An exhaustive attack for disclosing λ keys $\widetilde{\boldsymbol{u}}^{(1)}, \widetilde{\boldsymbol{u}}^{(2)}, \cdots, \widetilde{\boldsymbol{u}}^{(\lambda)}$ randomly chosen by Bob is performed. T
are successfully found by the exhaustive attack, P_c[Step1] is

$$P_c[\text{Step1}] = \left(\begin{array}{c} k \\ \lambda \end{array} \right)^{-1}.$$

Step 2 : After finding the keys $\widetilde{\boldsymbol{u}}^{(1)}, \widetilde{\boldsymbol{u}}^{(2)}, \cdots, \widetilde{\boldsymbol{u}}^{(\lambda)}$ an exhaustive attack is performed for finding error free components of $\widetilde{\boldsymbol{u}}^{(m)}$.The probability of obtaining these λ error free components, P_c[Step2] is

$$P_c[\text{Step2}] = \left(\begin{array}{c} g-t \\ \lambda \end{array} \right) \Big/ \left(\begin{array}{c} g \\ \lambda \end{array} \right)$$

which cannot be sufficiently small in K(XII)SE(1)PKC over $\mathbb{F}_{2^8}$. For example, when $g = 120$, $t = 24, \lambda = 30$, the probability P_c[Step2] is 4.05×10^{-4}, which is not a sufficiently small value. We conclude that in order to be secure against Attack 2, the probability

$$P_c[\text{Step1}] * P_c[\text{Step2}] = \left(\begin{array}{c} k \\ \lambda \end{array} \right)^{-1} \left(\begin{array}{c} g-t \\ \lambda \end{array} \right) \Big/ \left(\begin{array}{c} g \\ \lambda \end{array} \right)$$

is made less than $2^{-80} = 8.27 \times 10^{-25}$.

Remark 4 : All $\widetilde{\boldsymbol{v}}_i$'s ; $i = 1, 2, \cdots, k$, can be estimated correctly if k error free symbols ($\in \{\widetilde{c}_i^{-T}\}$) are successfully estimated. However in K(XII)SE(1)PKC, we assume that $k > g - t$ and $k \gg \lambda$ hold. We conclude that K(XII)SE(1)PKC would be secure against the attack based on estimating error free k symbols.

Set of keys are :

Public key	:	$\{\boldsymbol{u}_i\}$
Secret key	:	$\{\boldsymbol{\varepsilon}_i\}, \{\boldsymbol{\rho}_i\}, P_I$

An example of K(XII)SE(1)PKC is given below.

Example 1:$m = 8, g = 120, k = 120, \lambda = 30, t = 24, \eta + 1 = 7$

The code length E, number of information symbols K, minimum distance D are

$$\begin{aligned} E &= 2^m - 1 = 255, \\ K &= E - g = 135, \\ D &= g + 1 = 121. \end{aligned} \tag{30}$$

We then have the followings :

$$\begin{aligned} P_c[\hat{\boldsymbol{\varepsilon}}_i, \hat{\boldsymbol{\rho}}_i] &= \left(\begin{array}{c} K \\ \eta+1 \end{array} \right)^{-1} \cdot (2^m)^{-(\eta+1)} \\ &= \left(\begin{array}{c} 135 \\ 7 \end{array} \right)^{-1} \cdot 2^{-56} = 1.00 \times 10^{-28}. \end{aligned} \tag{31}$$

$$\begin{aligned} P_c[\{\text{Step1}\}] &= \left(\begin{array}{c} k \\ \lambda \end{array} \right)^{-1} = \left(\begin{array}{c} 120 \\ 30 \end{array} \right)^{-1} \\ &= 5.89 \times 10^{-29}. \end{aligned} \tag{32}$$

The coding rate ρ and the size of public key, S_{PK} are

$$\rho = \frac{(\lambda+t)m + \log_2 \left(\begin{array}{c} k \\ \lambda \end{array} \right) \left(\begin{array}{c} g \\ t \end{array} \right)}{gm} = 0.579. \tag{33}$$

$$\begin{aligned} S_{PK} &= kgm = 120 \times 120 \times 8(\text{bit}) \\ &= 14.4\text{KB}, \end{aligned} \tag{34}$$

which is smaller than that of McEliece PKC [14] by a factor of about 2.

4 Conclusion

We have presented a new class of public key cryptosystem based on Reed-Solomon code, K(XII)SE(1)PKC. We have shown that K(XII)SE(1)PKC would be secure against the various attacks.

It should be noted that we presented K(XII)SE(1)PKC based on the Reed-Solomon codes over $\mathbb{F}_{2^8}$, which is extensively used in the present day storage system such as CD, DVD, HD etc. and the various transmission systems.

The presented K(XII)SE(1)PKC over $\mathbb{F}_{2^8}$ has the following remarkable properties.

- The size of public key is smaller than that of the McEliece PKC [14] by a factor of about 2.
- The coding rate takes on 0.58, while that of the McEliece PKC is 0.5.

The author would like to thank Dr. Perret for the kind advice to cite Refs. [6] and [15]. Our proposed PKC would be threatened by the various attacks for small size of m such as 8, unless η is chosen at least 6. The author feels that our scheme would be secure, even for $m = 8$, if η takes on a large value of more than 10, with a slight degradation of coding rate.

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.

[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: "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).

[12] M. Kasahara: "Public Key Cryptosystems Constructed Based on Pseudo Cyclic Codes, K(Ⅷ)SE(1)PKC and K(Ⅺ)SE(2)PKC –Modification of K(Ⅶ)SE(1)PKC–", ISEC 2010-129 (2011-03).

[13] 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).

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

[15] J. C. Faugere and A. Otomoni, L. Perret, J. P. Tillich: "Algebraic Cryptanalysis of McElierce Variants with Compact Keys", Eurocrypt'10.

[16] E. M. Gabidulin: "Public-key cryptosystems based on linear codes", Report 95-30, TU Delft (1995).

[17] A. J. Viterbi: "Error-Bounds for Convolutional Codes and an Asymptotially Optimum Decoding Algorithm", IEEE Trans. Inform. Theory, IT-13, 2, pp.260-269 (April 1967).

[18] H. Kumazawa, M. Kasahara, and T. Namekawa: "A Construction of Vector Quantizers for Noisy Channels", Trans. of IEICE, Vol. J67-B, No.1 pp.1-8 (1984-01).

[19] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa: "A method for solving key equation for decoding Goppa codes", Info. and Control, 27, pp.87-99 (1975).

[20] 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).