Construction of New Classes of Knapsack Type Public Key Cryptosystem Using Uniform Secret Sequence, K(Ⅱ)ΣΠPKC, Constructed Based on Maximum Length Code

Masao KASAHARA†

† Graduate School of Osaka Gakuin University
E-mail: †kasahara@ogu.ac.jp

Abstract In this paper, we present a new class of knapsack type PKC referred to as K(Ⅱ)ΣΠPKC. In K(Ⅱ)ΣΠPKC, Bob randomly constructs a very small subset of Alice's set of public key whose order is very large, under the condition that the coding rate ρ satisfies $0.01 < \rho < 0.5$. In K(Ⅱ)ΣΠPKC, no secret sequence such as super-increasing sequence or shifted-odd sequence but the sequence whose component is constructed by a product of the same number of many prime numbers of the same size, is used. We show that K(Ⅱ)ΣΠPKC is secure against the attacks such as LLL algorithm, Shamir's attack etc. , because a subset of Alice's public keys is chosen entirely in a probabilistic manner at the sending end. We also show that K(Ⅱ)ΣΠPKC can be used as a member of the class of common key cryptosystems because the list of the subset randomly chosen by Bob can be used as a common key between Bob and Alice, provided that the conditions given in this paper are strictly observed, without notifying Alice of his secret key through a particular secret channel.

Key words Public-key cryptosystem(PKC), Knapsack-type PKC, Product-sum type PKC, LLL algorithm, PQC.

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.

One of the promising candidates among the classes of PKC are the code-based PKC and the product-sum type PKC [1]∼[23].

In this paper, we present a new class of knapsack type PKC referred to as K(Ⅱ)ΣΠPKC. In K(Ⅱ)ΣΠPKC, Bob randomly constructs a very small subset of Alice's set of public key whose order is very large, under the condition that the coding rate ρ satisfies $0.01 < \rho < 0.5$. In K(Ⅱ)ΣΠPKC, no secret sequence such as super-increasing sequence or shifted-odd sequence but the sequence whose components are constructed by the products of the same number of many prime numbers of the same size, is used. It should be noted that the components of the secret sequence such as super-increasing sequence or shifted-sequence have different entropies. On the other hand the components of the secret sequence used in K(Ⅱ)ΣΠPKC take on the same entropy.

We show that K(Ⅱ)ΣΠPKC is secure against the attacks such as LLL algorithm, Shamir's attack etc. , because a subset of Alice's public keys is chosen entirely in a probabilistic manner at the sending end. We also show that K(Ⅱ)ΣΠPKC can be used as a member of the class of common key cryptosystems because the list of the subset randomly chosen by Bob can be used as a common key between Bob and Alice, provided that the conditions given in this paper are strictly observed, without notifying Alice of his secret key through a particular secret channel.

2. K(Ⅱ)ΣΠPKC for two messages

2.1 Preliminaries

Let us define several symbols :

m_i : Message symbol over $\mathbb{Z}; i = 1, 2, \cdots, \lambda$.

Γ : Intermediate message.

p_i : Prime number ; $i = 1, 2, \cdots, n$.

$\boldsymbol{p} : (p_1, p_2, \cdots, p_n)$, prime number vector.

$\boldsymbol{s} : (s_1, s_2, \cdots, s_n)$, secret sequence.

$|A|$: Size of A in bit.

$\#S$: Order of set S.

The conventional knapsack type PKC's are constructed using the following sequences:

(i) : super-increasing sequence[5]

(ii) : shifted-odd sequence[13∼15]

(iii) : J-step uniform sequence[19,20]

In these sequences, entropies of the components are not necessarily same.

On the other hands, the entropies of the components of the secret sequence used in K(Ⅱ)ΣΠPKC are exactly same.

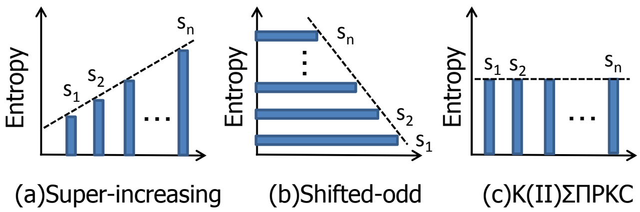

Fig. 1 Entropys of secret sequences

We shall refer to such secret sequence as uniform sequence.

In the following sections, when the variable x_i takes on an actual value $\tilde{x}_i$, we shall denote the corresponding vector, $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$, as

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

The $\widetilde{C}$ and $\widetilde{M}$ et al. will be defined in a similar manner.

2. 2 Summary of idea of K(Ⅱ)ΣΠPKC

In this sub-section let us summarize the idea of a secret system using K(Ⅱ)ΣΠPKC for two messages.

Let the Alice's set of public key, be denoted $\{k_i\}_A$.

For the message $\boldsymbol{m} = (m_A, m_B)$, Bob randomly chooses two keys, k_A and k_B, from the set of Alice's public key $\{k_i\}_A$.

Bob encrypts the message $\boldsymbol{m}$ into

$$\boldsymbol{m} \mapsto \boldsymbol{C} = m_A k_A + m_B k_B. \tag{2}$$

Alice decrypts the ciphertext $\boldsymbol{C}$ into

$$\boldsymbol{C} \mapsto \boldsymbol{m} = (m_A, m_B). \tag{3}$$

2. 3 Problem 1

Let us suppose that two public keys are chosen and in accordance with this random choice two secret keys q_A and q_B are chosen from the set $\{q_i\}$. The intermediate message Γ is

$$\Gamma = m_A q_A + m_B q_B. \tag{4}$$

Problem 1 : Construct the set of secret keys $\{q_i\}$ so that Γ may be decoded as

$$\Gamma \mapsto \boldsymbol{m} = (m_A, m_B), \tag{5}$$

under the conditions that :

(i) q_A and q_B are randomly chosen from $\{q_i\}$ whose order is very large,

(ii) coding rate ρ satisfies $0.01 < \rho < 0.5$,

(iii) completely uniform sequence is used.

In the next sub-sections we shall present a scheme for constructing $\{q_i\}$ based on the maximum length code [24],as one of the solutions for Problem 1.

2. 4 Maximum length code

In this sub-section, we assume that n is given by

$$n = 2^g - 1. \tag{6}$$

The maximum length code $\{F_M(x)\}$ is a cyclic code that satisfies

$$F_M(x) \equiv 0 \mod \frac{x^n - 1}{G_F(x)}, \tag{7}$$

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

In the followings $\{F_M(x)\}$ will also be denoted simply by $\{F_M\}$.

Let the two code words of $\{F_M\}$, M_α and M_β over $\mathbb{F}_2$, be denoted by

$$M_\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \tag{8}$$

and

$$M_\beta = (\beta_1, \beta_2, \cdots, \beta_n). \tag{9}$$

Let the sets S_1, S_2, S_3 be defined as follows :

S_1 : Set of pairs (α_i, β_i)'s such that

$\alpha_i = 1, \quad \beta_i = 1 \;\; ; \;\; i = 1, 2, \cdots, n.$

S_2 : Set of pairs (α_i, β_i)'s such that

$\alpha_i = 0, \quad \beta_i = 0 \;\; ; \;\; i = 1, 2, \cdots, n.$

S_3 : Set of pairs (α_i, β_i)'s such that

$\alpha_i = 0, \quad \beta_i = 1 \;\; ; \;\; i = 1, 2, \cdots, n.$

S_4 : Set of pairs (α_i, β_i)'s such that

$\alpha_i = 1, \quad \beta_i = 0 \;\; ; \;\; i = 1, 2, \cdots, n.$

Theorem 1 : The orders $\#S_1$, $\#S_2$, $\#S_3$ and $\#S_4$ are given by

$$\#S_1 = \frac{n+1}{4}, \tag{10}$$

$$\#S_2 = \frac{n-3}{4}, \tag{11}$$

$$\#S_3 = \#S_4 = \frac{n+1}{2}. \tag{12}$$

Proof : The Hamming weight of any code word of the maximum length code $\{F_M\}$ is $\frac{n+1}{2}$. As the maximum length code $\{F_M\}$ is a member of the class of linear codes,

$$M_C = M_A + M_B \quad ; \quad M_A \ne M_B \tag{13}$$

is also a code word of $\{F_M\}$. Namely the weight of M_C is also $\frac{n+1}{2}$, which implies that the following relations hold:

$$(\#S_3) + (\#S_4) = \frac{n+1}{2}, \tag{14}$$

$$(\#S_1) + (\#S_2) = n - \frac{n+1}{2} = \frac{n-1}{2}. \tag{15}$$

Eqs.(14) and (15) imply that

$$(\#S_3) = (\#S_4), \tag{16}$$

and

$$(\#S_1) = (\#S_2) + 1. \tag{17}$$

From Eqs.(15) and (17), $\#S_2$ is given by $\#S_2 = (\frac{n-1}{2} - 1)/2 = \frac{n-3}{4}$, which implies that $\#S_1 = \frac{n+1}{4}$. □

2.5 Construction of the set of composite number $\{q_i\}$

Let $\boldsymbol{A}$ be a code word of $\{F_M\}$ and $\boldsymbol{p}$, a prime number vector whose components are randomly chosen prime numbers. Let $\boldsymbol{A}$ and $\boldsymbol{p}$ be denoted by

$$\boldsymbol{A} = (a_1, a_2, \cdots, a_n) \tag{18}$$

and

$$\boldsymbol{p} = (p_1, p_2, \cdots, p_n), \tag{19}$$

where we assume that p_i has the same size ; i = 1, $\cdots$, n.

Let $\boldsymbol{w}_A$ be defined by

$$\boldsymbol{w}_A = (a_1p_1, a_2p_2, \cdots, a_np_n). \tag{20}$$

Let the composite number $q^{(A)}$ be defined by the products of non-zero components of $\boldsymbol{w}_A$. Namely $q^{(A)}$ can be represented by

$$q^{(A)} = \prod_{i=1}^{n} a'_i p_i, \tag{21}$$

where we let a'_ip_i be a_ip_i for $a_ip_i = p_i$ and 1, for $a_ip_i = 0$.

Let another code word $\boldsymbol{B}$ be denoted

$$\boldsymbol{B} = (b_1, b_2, \cdots, b_n). \tag{22}$$

The following composite number $q^{(B)}$ can be obtained from $\boldsymbol{w}_B = (b_1p_1, b_2p_2, \cdots, b_np_n)$ in a similar manner as $q^{(A)}$:

$$q^{(B)} = \prod_{i=1}^{n} b'_i p_i. \tag{23}$$

$\mathbf{p}$:	p_1	p_2	p_3	p_4	p_5	p_6	p_7
M_1 :	0	0	1	0	1	1	1
M_2 :	1	0	0	1	0	1	1
M_3 :	1	1	0	0	1	0	1
M_4 :	1	1	1	0	0	1	0
M_5 :	0	1	1	1	0	0	1
M_6 :	1	0	1	1	1	0	0
M_7 :	0	1	0	1	1	1	0

Fig. 2 Maximum length code generated by $(x+1)(x^3+x+1)$

We have the following straightforward theorem.

Theorem 2 : Letting the largest common divisor $(q^{(A)}, q^{(B)})$ be denoted $d_{A,B}$, it is

$$d_{A,B} = \prod_{i=1}^{n} p_i^{(A,B)}, \tag{24}$$

where $p_i^{(A,B)}$ denotes the i-th prime number of $\boldsymbol{p}$ for which $(a_i, b_i) \in S_1$ holds.

Example 1 : Maximum length code of length $n = 2^3 - 1$. Let $G_F(x)$ be

$$G_F(x) = x^3 + x + 1. \tag{25}$$

All the code words generated by $(x^7+1)/G_F(x) = (x+1)(x^3+x^2+1)$ are listed in Fig.2.

Let us assume that the two code words M_2 and M_5 in Fig.2 have been randomly chosen from $\{F_M\}$.

Let the prime number vector be represented by

$$\boldsymbol{p} = (p_1, p_2, \cdots, p_7). \tag{26}$$

From Fig.2, w_2 and w_5 are

$$\boldsymbol{w}_2 = (p_1, 0, 0, p_4, 0, p_6, p_7) \tag{27}$$

and

$$\boldsymbol{w}_5 = (0, p_2, p_3, p_4, 0, 0, p_7). \tag{28}$$

The $q^{(M_2)}$ and $q^{(M_5)}$ are

$$q^{(M_2)} = p_1p_4p_6p_7 \tag{29}$$

and

$$q^{(M_5)} = p_2p_3p_4p_7. \tag{30}$$

From Eqs.(29) and (30), we see that the largest common divisor $(q^{(M_2)}, q^{(M_5)}), d_{M_2,M_5}$ is given by

$$d_{M_2,M_5} = p_4p_7. \tag{31}$$

Let the largest common divisor $(q^{(M_i)}, q^{(M_j)})$ be simply denoted by $d_{i,j}$ instead of d_{M_i,M_j}. In Fig.3 we show the correspondence between p_ip_j and two code words M_i, M_j.

M_i, M_j	$d_{i,j}$	M_i, M_j	$d_{i,j}$
M_1, M_2	$p_6 p_7$	M_3, M_4	$p_1 p_2$
M_1, M_3	$p_5 p_7$	M_3, M_5	$p_2 p_7$
M_1, M_4	$p_3 p_6$	M_3, M_6	$p_1 p_5$
M_1, M_5	$p_3 p_7$	M_3, M_7	$p_2 p_5$
M_1, M_6	$p_3 p_5$	M_4, M_5	$p_2 p_3$
M_1, M_7	$p_5 p_6$	M_4, M_6	$p_1 p_3$
M_2, M_3	$p_1 p_7$	M_4, M_7	$p_2 p_6$
M_2, M_4	$p_1 p_6$	M_5, M_6	$p_3 p_4$
M_2, M_5	$p_4 p_7$	M_5, M_7	$p_2 p_4$
M_2, M_6	$p_1 p_4$	M_6, M_7	$p_4 p_5$
M_2, M_7	$p_4 p_6$	—	—

Fig. 3 $d_{i,j}$ for M_i, M_j

We see that all the pair (M_i, M_j)'s can be decoded uniquely from $d_{i,j}$'s .

2. 6 Construction of intermediate message

Bob randomly selects two public keys k_A and k_B from $\{k_i\}_A$. In accordance with this random choice, two code words M_A and $M_B \in \{F_M\}$ are chosen. As a result the intermediate message Γ is given by

$$\Gamma = m_A q^{(A)} + m_B q^{(B)}. \tag{32}$$

Let $q^{(A)}$ and $q^{(B)}$ be represented by

$$q^{(A)} = \overline{q}^{(A)} d_{A,B} \tag{33}$$

and

$$q^{(B)} = \overline{q}^{(B)} d_{A,B}. \tag{34}$$

From Eqs.(32), (33) and (34), the intermediate message is given by

$$\Gamma = (m_A \overline{q}^{(A)} + m_B \overline{q}^{(B)}) d_{A,B}. \tag{35}$$

When a component of p, p_i, satisfies

$$d_{A,B} \equiv 0 \mod p_i, \tag{36}$$

we let p_i be denoted by $\overline{p}_i$.

Theorem 3 : From the set $\{\overline{p}_i\}$, the two code words, M_A and M_B, randomly chosen at the sending end are correctly decoded (See Fig.3).

Proof : The column vectors shown in Fig.2 are proved the code words of $\left\{F_M'\right\}$, whose generator polynomial $G_F'(x)$ is $x^3(x^{-3} + x^{-1} + 1) = x^3 + x^2 + 1$, which is obtained as $x^3 G_F(x^{-1})$. From Theorem 1, $\#S_1 = 2$, yielding the proof. □

Let w and W be relatively prime positive integers such that

$$w < W, \tag{37}$$

$$(w, W) = 1. \tag{38}$$

The set of public keys, $\{k_i\}$, is given by

$$w q_i \equiv k_i \bmod W \;\; ; \;\; i = 1, \cdots, n. \tag{39}$$

Public key	:	$\{k_i\}$
Secret key	:	w, W, $\{q_i\}$, M_i

[Decryption Process]

Given $\widetilde{\Gamma}$, the messages $\widetilde{m}_A$ and $\widetilde{m}_B$ are decoded by

$$\widetilde{\Gamma}\left\{q^{(A)}\right\}^{-1} \equiv \widetilde{m}_A \mod \overline{q}^{(B)} \tag{40}$$

and

$$\widetilde{\Gamma}\left\{q^{(B)}\right\}^{-1} \equiv \widetilde{m}_B \mod \overline{q}^{(A)}. \tag{41}$$

respectively.

3. A new class of PKC scheme based on K(Ⅱ)ΣΠPKC — Possible applications to the field of common key cryptosystem —

3. 1 Construction

Bob randomly chooses λ code words of $\{F_M\}$. Without loss of generality let us assume that the list of the randomly chosen code words by Bob are the followings:

$$\begin{aligned} M_1 = &\quad (t_{11}, t_{12}, \cdots, t_{1n}), \\ M_2 = &\quad (t_{21}, t_{22}, \cdots, t_{2n}), \\ &\vdots \\ M_\lambda = &\quad (t_{\lambda 1}, t_{\lambda 2}, \cdots, t_{\lambda n}). \end{aligned} \tag{42}$$

Let the column vector $\boldsymbol{t}_i$ be denoted by

$$\boldsymbol{t}_i = \begin{bmatrix} t_{1i} \\ t_{2i} \\ \vdots \\ t_{\lambda i} \end{bmatrix}. \tag{43}$$

Let the total number of $\boldsymbol{t}_i$'s such that $\boldsymbol{t}_i$'s take on the same value $\boldsymbol{a}^{(i)}$ over $\mathbb{F}_2$ be denoted by $N(\boldsymbol{a}^{(i)})$.

Theorem 4 : The $N(\boldsymbol{a}^{(i)})$ is given by

$$\begin{aligned} N(\boldsymbol{a}^{(i)}) &= 2^{g-\lambda} \quad \text{for} \quad \boldsymbol{t}_i \neq \boldsymbol{0}, \\ &= 2^{g-\lambda} - 1 \quad \text{for} \quad \boldsymbol{t}_i = \boldsymbol{0}. \end{aligned} \tag{44}$$

Proof : See, for example, Ref.[24]. □

When User J, in accordance with a random choice of λ public keys, selects λ code words among the code words of $\{F_M\}$ for given messages $m_1, m_2, \cdots, m_\lambda$, the largest common divisor of $q^{(M_1)}, q^{(M_2)}, \cdots, q^{(M_\lambda)}$ is given by a product of $2^{g-\lambda}$ prime numbers (Theorem 4).

As a generalized form of Eq.(4), the intermediate message Γ is given as

$$\Gamma = m_1 \boldsymbol{q}^{(M_1)} + m_2 \boldsymbol{q}^{(M_2)} + \cdots + m_\lambda \boldsymbol{q}^{(M_\lambda)}. \tag{45}$$

The $q^{(M_i)}$, the product of prime numbers $a_1' p_1, \cdots, a_n' p_n$, randomly chosen according to the code word M_i, can be represented as

$$q^{(M_i)} = \overline{q}^{(M_i)} d_{1\sim\lambda} \;\; ; \;\; i = 1, \cdots, \lambda, \tag{46}$$

where $d_{1\sim\lambda}$ is the largest common divisor of $q^{(M_1)}, \cdots, q^{(M_\lambda)}$.

3.2 Brief sketch of a communication system using K(Ⅱ)ΣΠPKC

In Fig.4 let us show a brief sketch of a communication system where K(Ⅱ)ΣΠPKC for λ messages can be successfully applied.

Encryption process can be performed as follows :

Step 1 : User J randomly chooses λ keys k_{J1}, k_{J2}, $\cdots$, $k_{J\lambda}$ by just taking a look at Alice's public key set $\{k_i\}_A$.

Step 2 : User J encrypts messages $\widetilde{m}_1$, $\widetilde{m}_2$, $\cdots$, $\widetilde{m}_\lambda$ into

$$\widetilde{C}_J = \widetilde{m}_1 k_{J1} + \widetilde{m}_2 k_{J2} + \cdots + \widetilde{m}_\lambda k_{J\lambda}. \tag{47}$$

Step 3 : User J sends the ciphertext $\tilde{C}_J$ to Alice.

Decryption process by Alice is given as follows :

Step 1 : Alice decrypts $\widetilde{C}_J$ by

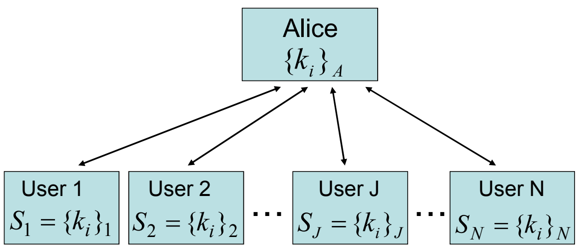

Fig. 4 A new class of communication scheme using K(Ⅱ)ΣΠPKC

$$w^{-1}\widetilde{C}_J \equiv \Gamma_J = \widetilde{m}_1 q_{J1} + \widetilde{m}_2 q_{J2} + \cdots + \widetilde{m}_\lambda q_{J\lambda} \bmod W. \tag{48}$$

Step 2 : By simply calculating the largest common divisor of $q_{J1}, q_{J2}, \cdots, q_{J\lambda}$, Alice decodes M_{J1}, M_{J2}, $\cdots$, $M_{J\lambda}$ randomly chosen by User J.

Theorem 5 : For the given messages $\widetilde{m}_1$, $\widetilde{m}_2$, $\cdots$, $\widetilde{m}_\lambda$, the ciphertext can be uniquely decoded, as far as

$$\log_2 \lambda + 2^{g-\lambda} \geqq g \tag{49}$$

is satisfied.

Proof : We see that when all the code words whose generator polynomial is given by $(x^n - 1)/G_F(x)$ are listed as shown in the example given in Fig.2, any column vector is a code word generated by $(x^n - 1)/x^g G_F(x^{-1})$. We then see that the following relation:

$$\lambda \cdot 2^t \geqq n + 1, \tag{50}$$

where t = (n+1) $2^{-\lambda}$

is required to be satisfied, for uniquely decoding $\widetilde{m}_1, \widetilde{m}_2, \cdots, \widetilde{m}_\lambda$, yielding the proof. □

It is easy to see that when λ is $2^a, a = 1, 2, 3, \cdots$, the equality holds in Eq.(49). we shall refer to such λ as optimum λ and denote it by λ_o. We shall also refer to the largest λ such that it satisfies the inequality of Eq(49) as quasi-optimum λ and denote it by λ_{qo}. Evidently λ_{qo} is given by $g - 3$.

3.3 Parameters

Let the size of m_i be

$$|m_i| = 2^{g-\lambda}|p_i| - 1 \;\; \text{(bit)}. \tag{51}$$

The size of the intermediate message, Γ, is

$$|\Gamma| = |m_i| + 2^{g-1}|p_i| + \lceil \log_2 \lambda \rceil \;\; \text{(bit)}. \tag{52}$$

where $\lceil x \rceil$ denotes the smallest integer larger than x.

The sizes of W, k_i and C are

$$|W| = |\Gamma| + 1, \tag{53}$$

$$|k_i| = |W| \tag{54}$$

and (55)

$$|C| = |m_i| + |k_i| + \lceil \log_2 \lambda \rceil. \tag{56}$$

The coding rate ρ is

$$\rho = \frac{\lambda |m_i|}{C}. \tag{57}$$

Let the probability that all the elements of S_J is correctly estimated by an attacker be denoted $P_C[\hat{S}_J]$. The $P_C[\hat{S}_J]$ is

$$P_C[\hat{S}_J] = \begin{pmatrix} n \\ \lambda \end{pmatrix}^{-1}. \tag{58}$$

3. 4 Example

In Table 1 we present several examples under the condition that

$$P_C[\hat{S}_J] < 2^{-80} = 8.27 \times 10^{-25}, \quad |p_i| = 80(\text{bit}). \tag{59}$$

Table 1 Examples of K(Ⅱ)ΣΠPKC for λ

n	λ	ρ	$P_C[\widehat{S}_J]$	$\|\{k_i\}_A\|$ (MB)	$\|\{k_i\}_J\|$ (KB)	$\|C\|$ (KB)
4095	8	0.0592	5.13×10^{-25}	84.5	165.1	20.8
8191	8	0.0615	2.00×10^{-27}	338.1	330.2	41.6
16383	7	0.106	1.59×10^{-26}	1352.6	577.9	83.2
32767	6	0.182	5.18×10^{-25}	5410.5	990.7	166.4

Although the details of doing so are omitted we can show that the coding rate can be improved by increasing n and by decreasing λ under the condition that $P_C[\hat{S}_J]$ takes on a sufficiently small value.

In Appendix, in order to improve the coding rate, we present a generalized version of K(Ⅱ)ΣΠPKC, referred to as K(Ⅲ)ΣΠPKC.

3. 5 Security considerations

Attack 1 : Exhaustive attack on $\{k_i\}_J$

By letting n be sufficiently large and appropriately determing the size of λ, the probability of successfully estimating the subset of $\{k_i\}_J$, $P_C[\hat{S}_J]$, can be made sufficiently small. □

Attack 2 : Shamir's attack on secret keys

In a sharp contrast with the conventional knapsack type PKC where super-increasing sequence or shifted-odd sequence is used, K(Ⅱ)ΣΠPKC uses a uniform sequence whose components have the same entropy. Namely a random product of the same number of prime numbers of the same size ($\gtrsim$ 80 bit). Thus it seems very hard to attack on the secret keys $k_1, k_2, \cdots, k_n$, with Shamir's attack. □

Attack 3 : LLL attack on the ciphertext

In K(Ⅱ)ΣΠPKC, n takes on a sufficiently large value, realizing a sufficiently high security, for the LLL attack.

3. 6 Key trace and its application

As shown in Fig.4, Alice's group members,1,2,$\cdots$,N, are communicating with Alice through a secret channel using K(Ⅱ)ΣΠPKC. Assuming that a member of the group, U_J randomly chooses a sequence of keys $k_{J1}, k_{J2}, \cdots, k_{J\lambda}$, for a given message sequence $m_1, m_2, \cdots, m_\lambda$, we shall refer to the order of the key sequence as key trace and denote it by TK_J

Remark 1 : It would be very hard for any user to forge UserJ's ciphertext sent to Alice provided that $P_C[\hat{S}_J]$ is made sufficiently small. □

The K(Ⅱ)ΣΠPKC realizes a secret communication system having the following features :

F1 : Key trace, TK_J, is not necessarily required to be revised each time when User J sends his or her message to Alice, as far as TK_J, is kept secret.

F2 : As a result, for a period, T_J , the trace can be used as a secret key between Alice and User J just as like in the conventional common key cryptosystem. We define the period T_J as the time required for sending $\lambda - 1$ or less ciphertexts. It should be noted that no secret channel for notifying their common key is required. Besides during this period, Alice's decryption process performed on the User J's ciphertext can be made much simplified, because it requires no decoding process for Bob's trace TK_J. When User J wants to revise the trace TK_J, it is only required to append a short note to the message sequence being sent, for notifying Alice of the revision of TK_J.

F3 : K(Ⅱ)ΣΠPKC can be used as a common key cryptosystem provided that the TK_J is successfully hided through a non-linear transformation.

4. Conclusion

We have presented a new class of PKC, K(Ⅱ)ΣΠPKC.

In a sharp ccontrast with the convetional knapsack PKC where the super-increasing sequence or shifted-odd sequence is used, in K(Ⅱ)ΣΠPKC, a uniform sequence is used.

As any component of the secret sequence used in K(Ⅱ)ΣΠPKC has the same entropy, K(Ⅱ)ΣΠPKC would be secure against the Shamair's attack.

K(Ⅱ)ΣΠPKC can be used as a common key cryptosystem provided that the TK_J is successfully hided through a non-linear transformation.

As a generalized version of K(Ⅱ)ΣΠPKC, we have presented K(Ⅲ)ΣΠPKC, yielding a higher rate compared with K(Ⅱ)ΣΠPKC.

References

[1] R.McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Tehory", DSN Progress Report, pp.42-44, (1978).

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

[3] M.Kasahara, "A New Class of Public Key Cryptosystems

Constructed Based on Error-Correcting Codes Using K(Ⅲ) Scheme", Cryptdogy ePrint Archive, 2010/341 (2010).
[4] M.Kasahara, "Public Key Cryptosystems Constructed Based on Random Pseudo Cyclic Codes, K(Ⅸ)SE(1)PKC, Realizing Coding Rate of Exactly 1.0", Cryptdogy ePrint Archive, 2011/545 (2011).
[5] R.C. Merkle and M.E. Hellman, "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inf. Theory, IT-24(5), pp.525-530, (1978).
[6] A. Shamir, "A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem", Proc. Crypto'82, LNCS, pp.279-288, Springer-Verlag, Berlin, (1982).
[7] E.F. Brickell, "Solving low density knapsacks", Proc. Crypto'83, LNCS, pp.25-37, Springer-Verlag, Berlin, (1984).
[8] J.C. Lagarias and A.M. Odlyzko, "Solving Low Density Subset Sum Problems", J. Assoc. Comp. Math., vol.32, pp.229-246, Preliminary version in Proc. 24th IEEE, (1985).
[9] M.J. Coster, B.A. LaMacchia, A.M. Odlyzko and C.P. Schnorr, "An Improved Low-Density Subset Sum Algorithm", Advances in Cryptology Proc. EUROCRYPT'91, LNCS, pp.54-67. Springer-Verlag, Berlin, (1991).
[10] Leonard M.Adleman, "On Breaking Generalized Knapsack Public Key Cryptosystms", In Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing. AXM, pp.402-412, (1983).
[11] M. Morii and M. Kasahara, "New public key cryptosystem using discrete logarithms over $GF(P)$", IEICE Trans. on Information & Systems, vol.J71-D, no.2, pp.448-453, (1978).
[12] B. Chor and R.L. Rivest, "A knapsack-type public-key cryptosystem based on arithmetic in finite fields", IEEE Trans. on Inf. Theory, IT-34, pp.901-909, (1988).
[13] M.Kasahara and Y.Murakami, "New Public-Key Cryptosystems", Tecnical Report of IEICE, ISEC 98-32 (1998-09).
[14] M.Kasahara and Y.Murakami, "Several Methods for Realizing New Public Key Cryptosystems", Technical Report of IEICE, ISEC 99-45 (1999-09).
[15] R.Sakai and Y.Murakami and M.Kasahara, 'Notes on Product-Sum Type Public Key Cryptosystem", Technical Report of IEICE, ISEC 99-46 (1999-09).
[16] M.Kasahara, "A Construction of New Class of Knapsack-Type Public Key Cryptosystem, K(I)ΣPKC, Constructed Based on K(I)Scheme", IEICE Technical Report, ISEC, Sept, (2010-09).
[17] M.Kasahara, "A Construction of New Class of Knapsack-Type Public Key Cryptosystem, K(Ⅱ)ΣPKC", IEICE Technical Report, ISEC, Sept, (2010-09).
[18] M. Kasahara: "Construction of A New Class of Product-Sum Type Public Key Cryptosystem, K(Ⅳ)ΣPKC and K(I)ΣPKC", IEICE Tech. Report, ISEC 2011-24 (2011-07).
[19] M. Kasahara: "On OGU(I)PKC", Memorandom for File at Kasahara Lab, Osaka Gakuin University (2011-03).
[20] M. Kasahara: "New development of OGU·PKC(I)", Memorandom for File at Kasahara Lab, Osaka Gakuin University (2011-11).
[21] Y. Murakami and M. Kasahara: "A Probabilistic Knapsack Public-Key Cryptosystem", SITA2010, 30-2.pdf, pp.615-618 (2010-11).
[22] Y. Murakami, S. Hamasho and M. Kasahara: "A probabilistic encryption scheme based on subset sum problem", Proc. 2012 Symposium on Cryptograpy and Information Security, SCIS2012, 3A1-2, 3A1-2.pdf (2012-01).
[23] Y. Murakami, S. Hamasho and M. Kasahara: "A Knapsack Public-Key Cryptosystem using Random Secret sequence", Proc. 2012 Symposium on Cryptograpy and Information Security, SCIS2012, 3A2-1, 3A2-1.pdf (2012-01).
[24] W. W. Peterson: "Error correcting Codes", M.I.T. Press (1961).

Appendix : K(Ⅲ)ΣΠPKC

In this appendix, we present a generalized version of K(Ⅱ)ΣΠPKC, referred to as K(Ⅲ)ΣΠPKC.

Let us denote μ classes of the maximum length code of length n, by $\{F_M\}_1, \{F_M\}_2, \cdots, \{F_M\}_\mu$.

K(Ⅱ)ΣΠPKC is a particular class of K(Ⅲ)ΣΠPKC for which $\mu = 1$ holds.

Let the intermediate message Γ be given by

$$\Gamma = \Gamma_1 + \Gamma_2 A_2 + \cdots + \Gamma_\mu A_2 A_3 \cdots A_\mu, \tag{60}$$

where A_i is a prime number, i = 2, $\cdots$, μ .

The sizes of Γ_i and A_i are

$$\begin{aligned} |\Gamma_i| &= |\Gamma_1| = |m_1| + 2^{g-\lambda}(|m_1|+1) + \lceil \log_2 \lambda \rceil, \\ |A_2| &= |A_3| = \cdots = |A_\mu| = |\Gamma_i| + 1. \end{aligned} \tag{61}$$

With the method given in Ref[13], all the intermediate messages $\Gamma_1, \Gamma_2, \cdots, \Gamma_\mu$ can be successfully decoded.

From Γ_i, the message $m_1^{(i)}, m_2^{(i)}, \cdots, m_\lambda^{(i)}$ assigned to Γ_i are decoded in the same manner as we have discussed in Section 3.

Example A : $\mu = 2, n = 4095, \lambda = 4$

The $P_C[\widehat{S}_J]$ is

$$P_C[\hat{S}_J] = \begin{pmatrix} 4095 \\ 4 \end{pmatrix}^{-2} = 7.29 \times 10^{-27}. \tag{62}$$

The coding rate ρ is approximately given by

$$\rho \cong 0.40. \tag{63}$$

The sizes of public key are

$$|\{k_i\}_A| = 377\text{MB} \tag{64}$$

and

$$|\{k\}_J| = 368\text{KB}. \tag{65}$$

Although the details of doing so are omitted K(Ⅲ)ΣΠPKC presented in this example would be secure against the various attacks. □

Example B : $\mu = 3, n = 1023, \lambda = 3$

The $P_C[\widehat{S}_J]$ is

$$P_C[\hat{S}_J] = \begin{pmatrix} 1023 \\ 3 \end{pmatrix}^{-3} = 1.78 \times 10^{-25} < 2^{-80}. \tag{66}$$

The coding rate ρ is

$$\rho = 0.43. \tag{67}$$

The sizes of public key are

$$|\{k_i\}_A| = 60.1\text{MB} \tag{68}$$

and

$$|\{k_i\}_J| = 176\text{KB}. \tag{69}$$

We see that the sizes of key in Examples A and B take on much smaller values than those for K(Ⅱ)ΣΠPKC.