社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（1）
2008/7/24

ナップザック暗号 KMN PKC に関する考察とチャレンジ問題

笠原 正雄† 村上 恭通†† 名迫 健††

† 大阪学院大学
大阪府吹田市岸部南 2-36-1
†† 大阪電気通信大学
大阪府寝屋川市初町 18-8
E-mail: †kasahara@ogu.ac.jp, ††yasuyuki@isc.osakac.ac.jp, nasako@m.ieice.org

あらまし ナップザック公開鍵暗号について従来数多くの提案がなされている．しかし，その多くは低密度攻撃，Shamir 攻撃等に耐性がないこと，あるいはメッセージサイズ／暗号文サイズが非常に小さくなる等の問題を有している．本論文では，Merkle と Hellman によって提案された方式をベースにして，筆者らが既に提案していた方式，すなわち超増加数列をトラップドアに用いつつ，2 個の暗号文と 2 個の補助暗号文とを組み合わせ，且つ誤り訂正符号の原理を導入した KMN PKC ナップザック暗号について，安全性に関する考察を深め，新しいより安全な方式を提案するとともにチャレンジ問題を提出する．

キーワード 公開鍵暗号，ナップザック型公開鍵暗号，Merkle-Hellman 公開鍵暗号，超増加数列，誤り訂正符号，チャレンジ問題

A Note on Security of KMN PKC and Presentation of Challenge Problems

Masao KASAHARA†, Yasuyuki MURAKAMI††, and Takeshi NASAKO††

† Osaka Gakuin University
2-36-1, Kishibe Minami, Suita-shi, Osaka, 564-8511
†† Osaka Electro-Communication University
18-8, Hatsu-cho, Neyagawa-shi, Osaka, 572-8530
E-mail: †kasahara@ogu.ac.jp, ††yasuyuki@isc.osakac.ac.jp, nasako@m.ieice.org

Abstract In this paper we discuss on a method for improving the security of the previously proposed KMN PKC [1] where two pairs of ciphertext-subsidiary ciphertext and also error-correcting codes are used. In order to improve the security, a new method is proposed. We show that our improved version of KMN PKC is secure against low-density attack. We also discuss the security of KMN PKC from the information theoretical point of view. We finally present two challenge problems on KMN PKC.

Key words public-key cryptosystem, Merkle-Hellman public-key cryptosystem, knapsack type cryptosystem, super-increasing sequences, error-correcting code, challenge problem.

1. Introduction

Various important 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 those two problems.

Concerning knapsack-type PKC, the various interesting schemes have been proposed. In 1978, the first knapsack-type PKC was proposed by Merkle and Hellman [2]. We shall refer to this scheme as MH PKC.

Unfortunately MH PKC was broken by Shamir [3], [4] and the Low-Density Attack(LDA) [5]〜[7]. Although MH PKC was broken, the MH PKC is very simple and interesting. For this reason, it has been long studied and has been revised by

many researchers [8]~[10].

Recently, for revising the security of MH PKC, Kobayashi proposed a new knapsack scheme over Gaussian integer ring over the super-increasing sequence [11]. Unfortunately, this scheme was broken [12], [13]. Later on, Hayashi and Sakamoto proposed an improved version of the scheme [14]. However, the improved scheme was proved not sufficiently secure as shown in [15].

Recently present authors presented a new class of knapsack cryptosystem on the basis of MH PKC, referred to as KMN PKC [1]. In KMN PKC two independent message sequences are jointly encoded to four ciphertexts. Namely each message is encoded to a different ciphertext. Two of the four ciphertexts are disturbed by random errors that would improve the security of KMN PKC.

In this paper, we further investigate the security of KMN PKC and improve it. We also present two classes of challenge problems.

In the following, for easy understanding, we shall first present three classes of insecure schemes, Insecure Schemes I, II and III. We then present a revised secure scheme, KMN PKC.

2. Security of KMN PKC [1]

In this section, we describe the principle of KMN PKC using insecure schemes referred to as Insecure Schemes I, II and III [1].

2.1 Rate and density

Let us define the rate R and the density D as follows:

$$R = \frac{\text{size of messages (in bits)}}{\text{size of ciphertext (in bits)}}, \tag{1}$$

$$D = \frac{\text{total size of messages and subsidiary messages (in bits)}}{\text{total size of ciphertexts (in bits)}}. \tag{2}$$

2.2 Insecure Scheme I

[Key generation]

Let the super-increasing sequence be

$$a_1, a_2, \ldots, a_N. \tag{3}$$

Let us generate the following random sequence under the condition that the relation $a_i = \widetilde{b}_i + \widetilde{d}_i$ holds:

$$\widetilde{b} = (\widetilde{b}_1, \widetilde{b}_2, \ldots, \widetilde{b}_N), \tag{4}$$

$$\widetilde{d} = (\widetilde{d}_1, \widetilde{d}_2, \ldots, \widetilde{d}_N). \tag{5}$$

A toy example is shown in Table 1.

It should be reminded that two sequences $\widetilde{b}$ and $\widetilde{d}$ seem, at least superficially, random sequences.

Letting b_i be defined as $b_i = \delta_i \widetilde{b}_i$, we then have $\boldsymbol{b} = (b_1, b_2, \ldots, b_N)$ and $\boldsymbol{\delta} = (\delta_1, \delta_2, \ldots, \delta_N)$, where $\delta_i = \mathrm{sgn}(\widetilde{b}_i)$ and $\mathrm{sgn}(\cdot)$ are the signum functions.

Table 1 Example I

i	1	2	3	4	5	6	7	8
a	1	2	4	8	16	32	64	128
$\widetilde{b}$	−65	6	54	−60	−18	−20	70	67
$\widetilde{d}$	66	−4	−50	68	34	52	−6	61

In a similar manner as b, letting d_i be defined as $d_i = \varepsilon_i \widetilde{d}_i$, we then have $\boldsymbol{d} = (d_1, d_2, \ldots, d_N)$ and $\boldsymbol{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_N)$. where $\varepsilon_i = \mathrm{sgn}(\widetilde{d}_i)$.

Let us consider the following modular transformation :

$$g_i = b_i w_b \bmod n_b, \tag{6}$$

$$h_i = d_i w_d \bmod n_d, \tag{7}$$

where we assume that the relations $n_b > \sum_{i=1}^{N} b_i$, $n_d > \sum_{i=1}^{N} d_i$ and $\gcd(w_b, n_b) = \gcd(w_d, n_d) = 1$ hold. Let us define $\boldsymbol{g}$ and $\boldsymbol{h}$ as $\boldsymbol{g} = (g_1, g_2, \ldots, g_N)$ and $\boldsymbol{h} = (h_1, h_2, \ldots, h_N)$.

Secret key : $\boldsymbol{a}, \widetilde{b}, \widetilde{d}, w_b, w_d, n_b, n_d$
Public key : $\boldsymbol{\delta}, \boldsymbol{\varepsilon}, \boldsymbol{g}, \boldsymbol{h}$

[Encryption]

The following ciphertexts C_b and C_d are now constructed for a message vector $\boldsymbol{m} = (m_1, m_2, \ldots, m_N) \in \{0,1\}^N$:

$$C_b = \sum_{i=1}^{N} m_i \delta_i g_i, \tag{8}$$

$$C_d = \sum_{i=1}^{N} m_i \varepsilon_i h_i. \tag{9}$$

2.3 Security consideration on Insecure Scheme I

Vulnerability of Insecure Scheme I is due to the fact that the same message sequence $\boldsymbol{m}$ is encrypted to two different ciphertexts C_b and C_d. Namely this scheme can be broken with the LDA by using the following matrix:

$$B_1 = \begin{pmatrix} 1 & & & O & -\lambda\delta_1 g_1 & -\lambda\varepsilon_1 h_1 \\ & \ddots & & & -\lambda\delta_2 g_2 & -\lambda\varepsilon_2 h_2 \\ & & \ddots & & \vdots & \vdots \\ O & & & 1 & -\lambda\delta_N g_N & -\lambda\varepsilon_N h_N \\ -1/2 & \cdots & \cdots & -1/2 & \lambda C_b & \lambda C_d \end{pmatrix}.$$

2.4 Insecure Scheme II

[Key generation]

Another modular transformations are performed on b_i and d_i as:

$$\widetilde{g}_i = b_i \widetilde{w}_b \bmod \widetilde{n}_b, \tag{10}$$

$$\widetilde{h}_i = d_i \widetilde{w}_d \bmod \widetilde{n}_d. \tag{11}$$

Letting $\widetilde{\boldsymbol{g}} = (\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_N)$ and $\widetilde{\boldsymbol{h}} = (\widetilde{h}_1, \widetilde{h}_2, \ldots, \widetilde{h}_N)$ be defined in a similar manner as $\boldsymbol{g}$ and $\boldsymbol{h}$, we have the following

set of keys.

Secret key : $a, \widetilde{b}, \widetilde{d}, w_b, w_d, \widetilde{w_b}, \widetilde{w_d}, n_b, n_d, \widetilde{n_b}, \widetilde{n_d}$
Public key : $\delta, \varepsilon, g, h, \widetilde{g}, \widetilde{h}$

[Encryption]

For two independent message vectors $\boldsymbol{m}^{(b)} = (m_1^{(b)}, m_2^{(b)}, \ldots, m_N^{(b)})$ and $\boldsymbol{m}^{(d)} = (m_1^{(d)}, m_2^{(d)}, \ldots, m_N^{(d)})$ the following ciphertexts:

$$C_b = \sum_{i=1}^{N} m_i^{(b)} \delta_i g_i, \tag{12}$$

$$C_d = \sum_{i=1}^{N} m_i^{(d)} \varepsilon_i h_i \tag{13}$$

are constructed.

New punctured sequences $\widetilde{\boldsymbol{m}}^{(b)} = (\widetilde{m}_1^{(b)}, \widetilde{m}_2^{(b)}, \ldots, \widetilde{m}_N^{(b)})$ and $\widetilde{\boldsymbol{m}}^{(d)} = (\widetilde{m}_1^{(d)}, \widetilde{m}_2^{(d)}, \ldots, \widetilde{m}_N^{(d)})$ are now constructed from the messages $\boldsymbol{m}_b$ and $\boldsymbol{m}_d$ as

$$\widetilde{m}_i^{(b)} = -m_i^{(b)} + m_i^{(d)} \tag{14}$$

and

$$\widetilde{m}_i^{(d)} = m_i^{(b)} - m_i^{(d)}. \tag{15}$$

It is easy to see that four message sequences $\boldsymbol{m}^{(b)}, \boldsymbol{m}^{(d)}, \widetilde{\boldsymbol{m}}^{(b)}$ and $\widetilde{\boldsymbol{m}}^{(d)}$ are different each other.

Besides the ciphertexts given by Eqs.(12) and (13), the following subsidiary ciphertexts, $\widetilde{C_b}$ and $\widetilde{C_d}$, are constructed:

$$\widetilde{C_b} = \sum_{i=1}^{N} \widetilde{m}_i^{(b)} \delta_i \widetilde{g}_i, \tag{16}$$

which is used for the decoding of $\boldsymbol{m}^{(d)}$ in cooperation with C_b. In a similar manner, $\widetilde{C_d}$ which is used for the decoding of $\boldsymbol{m}^{(b)}$ in cooperation with C_d is given by

$$\widetilde{C_d} = \sum_{i=1}^{N} \widetilde{m}_i^{(d)} \varepsilon_i \widetilde{h}_i. \tag{17}$$

The ciphertexts for the message sequences $\boldsymbol{m}^{(b)}$ and $\boldsymbol{m}^{(d)}$ are C_b and C_d respectively. The subsidiary messages $\widetilde{\boldsymbol{m}}^{(b)}$ and $\widetilde{\boldsymbol{m}}^{(d)}$ are encrypted to $\widetilde{C_b}$ and $\widetilde{C_d}$ respectively. The information rate, R, is thus given by $1/2$.

2.5 Security consideration on Insecure Scheme II

If we replace message $\widetilde{m}^{(b)}$ by $-\widetilde{m}^{(b)}$ $(i = 1, 2, \ldots, N)$, then $-\widetilde{m}_i^{(b)} = \widetilde{m}_i^{(d)}$ holds. Namely message $\widetilde{\boldsymbol{m}}^{(d)}$ can be obtained simply by $-\widetilde{\boldsymbol{m}}^{(b)}$.

We have the following relations:

$$C_b = \sum_{i=1}^{N} (\delta_i g_i) m_i^{(b)},$$

$$C_d = \sum_{i=1}^{N} (\varepsilon_i h_i) m_i^{(d)},$$

$$\widetilde{C_b} + \widetilde{C_d} = -\sum_{i=1}^{N} (\delta_i \widetilde{g}_i - \varepsilon_i \widetilde{h}_i) m_i^{(b)} + \sum_{i=1}^{N} (\delta_i \widetilde{g}_i - \varepsilon_i \widetilde{h}_i) m_i^{(d)},$$

$$\widetilde{C_b} - \widetilde{C_d} = -\sum_{i=1}^{N} (\delta_i \widetilde{g}_i + \varepsilon_i \widetilde{h}_i) m_i^{(b)} + \sum_{i=1}^{N} (\delta_i \widetilde{g}_i + \varepsilon_i \widetilde{h}_i) m_i^{(d)}.$$

Scheme II is thus broken with the LDA by using the matrix of Eq.(18).

2.6 Insecure Scheme III

[Key generation]

Secret key : $a, \widetilde{b}, \widetilde{d}, w_b, w_d, \widetilde{w_b}, \widetilde{w_d}, n_b, n_d, \widetilde{n_b}, \widetilde{n_d}$
Public key : $\delta, \varepsilon, g, h, \widetilde{g}, \widetilde{h}, ECC$

[Encryption]

Let us encode the message $\boldsymbol{m}^{(b)}$ to a code word of an error-correcting code which will be denoted as $\boldsymbol{m}_{ECC}^{(b)}$. The i-th component $\boldsymbol{m}_{ECC}^{(b)}$, $m_i^{(b)}$, will be denoted as $m_{i,ecc}^{(b)}$. The $m_{i,ecc}^{(b)}$ with error will be denoted as $\widehat{m}_{i,ecc}^{(b)}$. It should be noted that the error-correcting code would be more desirable to be a non-linear type code such as the Preparata code rather than a linear code [16].

In the followings, for simplicity, we assume that only $\boldsymbol{m}^{(b)}$ is encoded to an error-correcting code. We also assume that a random error is added only on the location where the relation $m_i^{(b)} = m_i^{(d)} = 0$ holds. A generalization to the case where both $\boldsymbol{m}^{(b)}$ and $\boldsymbol{m}^{(d)}$ are encoded to an error-correcting code and the error is added on the location where $m_i^{(b)} = m_i^{(d)} = 1$ holds is straightforward.

We also assume that $m_i^{(b)} = m_i^{(d)}$ holds with probability $1/2$ for given messages.

Step 1: Choose t locations $l_1, l_2, \ldots, l_t$ in $\boldsymbol{m}_{ECC}^{(b)}$.

Step 2: At the t locations, add t errors as

$$m_{i,ecc}^{(b)} = 0 \quad \mapsto \quad \widehat{m}_{i,ecc}^{(b)} = 1, \quad (i = l_1, l_2, \ldots, l_t). \tag{19}$$

Step 3: According to the additions of t errors in $\boldsymbol{m}_{ECC}^{(b)}$, modify the i-th element of $\boldsymbol{m}^{(d)}$ as

$$\widetilde{m}_i^{(d)} = 0 \quad \mapsto \quad \widetilde{m}_i^{(d)} = 1, \quad (i = l_1, l_2, \ldots, l_t). \tag{20}$$

2.7 Security consideration on Scheme III

Letting the error vector be $\boldsymbol{e} = (e_1, e_2, \ldots, e_N)$, we have the following relations:

$$\boldsymbol{m}^{(b)} = \boldsymbol{m}_{ECC}^{(b)} + \boldsymbol{e},$$

$$\widetilde{\boldsymbol{m}}^{(b)} = -\boldsymbol{m}_{ECC}^{(b)} + \boldsymbol{m}^{(d)},$$

$$\widetilde{\boldsymbol{m}}^{(d)} = \boldsymbol{m}_{ECC}^{(b)} - \boldsymbol{m}^{(d)} + \boldsymbol{e}.$$

Consequently, we have

$$C_b = \sum_{i=1}^{N} (\delta_i g_i) m_{i,ecc}^{(b)} + \sum_{i=1}^{N} (\delta_i g_i) e_i,$$

$$C_d = \sum_{i=1}^{N} (\varepsilon_i h_i) m_i^{(d)},$$

$$B_2 = \begin{pmatrix} 1 & & & & O & -\lambda\delta_1 g_1 & 0 & \lambda(\delta_1\widetilde{g}_1 - \varepsilon_1\widetilde{h}_1) & \lambda(\delta_1\widetilde{g}_1 + \varepsilon_1\widetilde{h}_1) \\ & \ddots & & & & \vdots & \vdots & \vdots & \vdots \\ & & \ddots & & & -\lambda\delta_N g_N & 0 & \lambda(\delta_N\widetilde{g}_N - \varepsilon_N\widetilde{h}_N) & \lambda(\delta_N\widetilde{g}_N + \varepsilon_N\widetilde{h}_N) \\ & & & \ddots & & 0 & -\lambda\varepsilon_1 h_1 & -\lambda(\delta_1\widetilde{g}_1 - \varepsilon_1\widetilde{h}_1) & -\lambda(\delta_1\widetilde{g}_1 + \varepsilon_1\widetilde{h}_1) \\ & & & & \ddots & \vdots & \vdots & \vdots & \vdots \\ O & & & & 1 & 0 & -\lambda\varepsilon_N h_N & -\lambda(\delta_N\widetilde{g}_N - \varepsilon_N\widetilde{h}_N) & -\lambda(\delta_N\widetilde{g}_N + \varepsilon_N\widetilde{h}_N) \\ -1/2 & \cdots & \cdots & \cdots & -1/2 & \lambda C_b & \lambda C_d & \lambda(\widetilde{C}_b + \widetilde{C}_d) & \lambda(\widetilde{C}_b - \widetilde{C}_d) \end{pmatrix} \tag{18}$$

$$B_3 = \begin{pmatrix} 1 & & & & O & -\lambda\delta_1 g_1 & 0 & \lambda(\delta_1\widetilde{g}_1 - \varepsilon_1\widetilde{h}_1) & \lambda(\delta_1\widetilde{g}_1 + \varepsilon_1\widetilde{h}_1) \\ & \ddots & & & & \vdots & \vdots & \vdots & \vdots \\ & & & & & -\lambda\delta_N g_N & 0 & \lambda(\delta_N\widetilde{g}_N - \varepsilon_N\widetilde{h}_N) & \lambda(\delta_N\widetilde{g}_N + \varepsilon_N\widetilde{h}_N) \\ & & & & & 0 & -\lambda\varepsilon_1 h_1 & -\lambda(\delta_1\widetilde{g}_1 - \varepsilon_1\widetilde{h}_1) & -\lambda(\delta_1\widetilde{g}_1 + \varepsilon_1\widetilde{h}_1) \\ & & \ddots & & & \vdots & \vdots & \vdots & \vdots \\ & & & & & 0 & -\lambda\varepsilon_N h_N & -\lambda(\delta_N\widetilde{g}_N - \varepsilon_N\widetilde{h}_N) & -\lambda(\delta_N\widetilde{g}_N + \varepsilon_N\widetilde{h}_N) \\ & & & & & -\lambda\delta_1 g_1 & 0 & -\lambda\varepsilon_1\widetilde{h}_1 & \lambda\varepsilon_1\widetilde{h}_1 \\ & & & \ddots & & \vdots & \vdots & \vdots & \vdots \\ O & & & & 1 & -\lambda\delta_N g_N & 0 & -\lambda\varepsilon_N\widetilde{h}_N & \lambda\varepsilon_N\widetilde{h}_N \\ -1/2 & \cdots & \cdots & \cdots & \cdots & \lambda C_b & \lambda C_d & \lambda(\widetilde{C}_b + \widetilde{C}_d) & \lambda(\widetilde{C}_b - \widetilde{C}_d) \end{pmatrix} \tag{21}$$

$$\begin{aligned} \widetilde{C}_b + \widetilde{C}_d &= -\sum_{i=1}^{N}(\delta_i\widetilde{g}_i - \varepsilon_i\widetilde{h}_i)m_{i,ecc}^{(b)} + \sum_{i=1}^{N}(\delta_i\widetilde{g}_i - \varepsilon_i\widetilde{h}_i)m_i^{(d)} \\ &\quad + \sum_{i=1}^{N}(\varepsilon_i\widetilde{h}_i)e_i, \\ \widetilde{C}_b - \widetilde{C}_d &= -\sum_{i=1}^{N}(\delta_i\widetilde{g}_i + \varepsilon_i\widetilde{h}_i)m_{i,ecc}^{(b)} + \sum_{i=1}^{N}(\delta_i\widetilde{g}_i + \varepsilon_i\widetilde{h}_i)m_i^{(d)} \\ &\quad - \sum_{i=1}^{N}(\varepsilon_i\widetilde{h}_i)e_i. \end{aligned}$$

We thus see that the Scheme III proves to be insecure against the LDA. Namely, Scheme III is broken with the LDA by using the matrix of Eq.(21).

3. Discussions

From Eqs.(6), (7), (10) and (11) we see that these messages $m^{(b)}, m^{(d)}, \widetilde{m}^{(b)}$ and $\widetilde{m}^{(d)}$ are performed by mutually unrelated modular transformations. For this reason we can conclude that the attack on public keys for Scheme I through III for disclosing secret keys can be circumvented. We shall show this in the followings.

Eqs.(6) and (10) can be represented as

$$b_i w_b = n_b Q_i + g_i \tag{22}$$

and

$$b_i\widetilde{w}_b = \widetilde{n}_b\widetilde{Q}_i + \widetilde{g}_i, \tag{23}$$

respectively, where Q_i and $\widetilde{Q}_i$ are the quotients. We assume here that $I(w_b) = I(\widetilde{w}_b) = I(n_b) = I(\widetilde{n}_b) = I(g_i) = I(\widetilde{g}_i)$ holds for a sufficiently large N, where $I(x)$ denotes the size of x (in bit).

From Eqs.(22) and (23), we obtain

$$n_b\widetilde{w}_b Q_i = \widetilde{n}_b w_b\widetilde{Q}_i + \widetilde{g}_i w_b - g_i\widetilde{w}_b. \tag{24}$$

From Eq.(24), we see that the following relation also holds :

$$n_b\widetilde{w}_b Q_{i+1} = \widetilde{n}_b w_b\widetilde{Q}_{i+1} + \widetilde{g}_{i+1} w_b - g_{i+1}\widetilde{w}_b. \tag{25}$$

From Eqs.(24) and (25) we have

$$\begin{aligned} &(\widetilde{n}_b w_b Q_i + \widetilde{g}_i w_b - g_i\widetilde{w}_b)Q_{i+1} = \\ &\qquad (\widetilde{n}_b w_b Q_{i+1} + \widetilde{g}_{i+1} w_b - g_{i+1}\widetilde{w}_b)Q_i \end{aligned} \tag{26}$$

From Eq.(26) we have

$$\begin{aligned} \widetilde{w}_b w_b(Q_i - Q_{i+1}) &= \widetilde{g}_{i+1} w_b Q_i - g_{i+1}\widetilde{w}_b Q_i \\ &\quad - \widetilde{g}_i w_b Q_{i+1} - g_i\widetilde{w}_b Q_{i+1} \end{aligned} \tag{27}$$

From Eq.(27), we see that the following relation also holds

$$\begin{aligned} \widetilde{n}_b w_b(Q_{i+2} - Q_{i+3}) &= \widetilde{g}_{i+3} w_b Q_{i+2} - g_{i+3}\widetilde{w}_b Q_{i+2} \\ &\quad - \widetilde{g}_{i+2} w_b Q_{i+3} - g_{i+2}\widetilde{w}_b Q_{i+3} \end{aligned} \tag{28}$$

From Eqs.(27) and (28) we see that the following relation holds :

$$\begin{aligned} &g_i\Gamma_i + \widetilde{g}_i\widetilde{\Gamma}_i + g_{i+1}\Gamma_{i+1} + \widetilde{g}_{i+1}\widetilde{\Gamma}_{i+1} + g_{i+2}\Gamma_{i+2} + \\ &\qquad \widetilde{g}_{i+2}\widetilde{\Gamma}_{i+2} + g_{i+3}\Gamma_{i+3} + \widetilde{g}_{i+3}\widetilde{\Gamma}_{i+3} = 0, \end{aligned} \tag{29}$$

where Γ_{i+j} and $\tilde{\Gamma}_{i+j}$ $(j = 1, 2, 3)$ are certain integers.

When we assume that $I(b_i) \geqq \gamma$[bits], it is easy to see that the size of Γ_i and $\tilde{\Gamma}_i$ can be given by

$$I(\Gamma_i) = I(\tilde{\Gamma}_i) \geqq I(g_i) + 3\gamma. \tag{30}$$

For example, when $I(b_i) = 40$

$$I(\Gamma_i) \sim I(g_i) \geqq 120(\text{bit}), \tag{31}$$

sufficiently large value, yielding invulnerability against the LDA on the public key.

4. Improvement of Security

We shall improve the security of Schemes I through III by slightly modifying the part of public key.

Although the proposed method can be applied to all the Schemes I through III, we can explain only one case where the method is applied to Scheme I.

4.1 Modified Scheme I

[Key generation]

Let us modify the first J symbols of super-increasing sequence as $\boldsymbol{a} = (0, 0, \ldots, 0, a_{J+1}, a_{J+2}, \ldots, a_N)$, where $(a_{J+1}, a_2, \ldots, a_N)$ is a super-increasing sequence.

Let us generate the following random sequence under the condition that the relation $a_i = b_i + d_i$ holds:

$$\boldsymbol{b} = (b_1, b_2, \ldots, b_N), \tag{32}$$

$$\boldsymbol{d} = (d_1, d_2, \ldots, d_N). \tag{33}$$

A toy example is shown in Table 2, where $w_b = 179$, $n_b = 479$, $w_d = 307$ and $n_b = 457$. It should be reminded that two sequences $\boldsymbol{b}$ and $\boldsymbol{d}$ seem, at least superficially, random sequences.

Let us define g and $\boldsymbol{h}$ as $g = (g_1, g_2, \ldots, g_N)$ and $\boldsymbol{h} = (h_1, h_2, \ldots, h_N)$. Let us consider the following modular transformation:

$$g_i = w_b b_i \bmod n_b, \tag{34}$$

$$h_i = w_d d_i \bmod n_d, \tag{35}$$

where we assume that the relations $n_b > \sum_{i=1}^{N} |b_i|$, $n_d > \sum_{i=1}^{N} |d_i|$ and $\gcd(w_b, n_b) = \gcd(w_d, n_d) = 1$ hold(1).

Secret key : $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{d}, w_b, w_d, n_b, n_d$
Public key : $\boldsymbol{g}, \boldsymbol{h}, J, N, V$

[Encryption]

When encrypting a message, the message vector $\boldsymbol{m}$ is also modified as

$$\boldsymbol{m}' = (v_1, v_2, \ldots, v_J, m_{J+1}, m_{J+2}, \ldots, m_N), \tag{36}$$

where we let the original message be $\boldsymbol{m} = (m_{J+1}, m_{J+2}, \ldots, m_N) \in \mathbf{F}_2^{N-J}$ and v_i is a randomly generated element whose size is given as V (bits). It should be noted that this scheme is knapsack PKC when $V = 1$.

In $\boldsymbol{m}'$, v_i's are the random noisy elements independent of message symbols. However from the standpoint of attacking KMN PKC, these elements $v_1, v_2, \ldots, v_J$ cannot be distinguished from message symbols $m_{J+1}, m_{J+2}, \ldots, m_N$ when the ciphertext is given. In other words, from the standpoint of attacking on KMN PKC, these noisy elements look like message sequences. We thus refer to $\boldsymbol{m}'$ as noise-disturbed message.

The following ciphertexts C_b and C_d are now constructed for a message vector $\boldsymbol{m}'$:

$$C_b = \sum_{i=1}^{N} m_i g_i, \tag{37}$$

$$C_d = \sum_{i=1}^{N} m_i h_i. \tag{38}$$

[Decryption]

Let the intermediate messages M_b and M_d be defined as follows:

$$M_b = \sum_{i=1}^{N} m_i b_i, \tag{39}$$

and

$$M_d = \sum_{i=1}^{N} m_i d_i, \tag{40}$$

respectively.

The M_b can be decoded as

$$M_b \equiv C_b w_b^{-1} \pmod{n_b}, \tag{41}$$

where M_b satisfies

$$\sum_{b_i<0} b_i \leqq M_b \leqq \sum_{b_i>0} b_i. \tag{42}$$

In a similar manner, M_d can be decoded as

$$M_d \equiv C_b w_d^{-1} \pmod{n_d}, \tag{43}$$

where M_d satisfies

$$\sum_{d_i<0} d_i \leqq M_d \leqq \sum_{d_i>0} d_i. \tag{44}$$

We then obtain the conventional Merkle-Hellman type intermediate message as

$$\begin{aligned} M &= M_b + M_d \\ &= \sum_{i=1}^{N} m_i (b_i + d_i) \\ &= \sum_{i=1}^{N} m_i a_i. \end{aligned} \tag{45}$$

(1) : It should be noted that the modular transformation over Gaussian integer ring can be also used.

Table 2 Toy Example of Modified Scheme I ($J = 8$, $N = 16$)

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	0	0	0	0	0	0	0	0	1	2	4	8	16	32	64	128
b	−18	30	−10	−16	−1	22	11	6	−65	6	54	−60	−18	−20	70	67
d	18	−30	10	16	1	−22	−11	−6	66	−4	−50	68	34	52	−6	61
g	131	101	126	10	300	106	53	116	340	116	86	277	131	252	76	18
h	42	387	328	342	307	101	279	443	154	143	188	311	384	426	443	447

From M the original message sequence $m = (m_{J+1}, m_{J+2}, \ldots, m_N)$ can be decoded according to the conventional method.

In the following, M will be also referred to as intermediate message.

4.2 Generalized Version of Modified Scheme I

Let us modify the first J symbols of super-increasing sequence as $r_1, r_2, \ldots, r_J, a_{J+1}, a_{J+2}, \ldots, a_N$, where the size of r_i be L-bit random integers and $r_i \ll a_{J+1}$.

In a similar manner, let us modify the first J symbols of b and d given by Eqs.(32) and (33) so that b_i and d_i may satisfy $b_i + d_i = r_i$ for $i = 1, 2, \ldots, J$, where $|b_i| \ll n_b$ and $|d_i| \ll n_d$.

4.3 Security consideration on Modified Scheme I

If the density d is low, the message sequence m' is can be disclosed with the LDA by using the matrix B_1 by a similar discussion on Insecure Scheme I. However, it is easy to see that the density can be made very large. Thus we can conclude that KMN PKC is secure against LDA.

The density D is given by

$$D = \frac{\text{total size of noise-disturbed messages (in bits)}}{\text{total size of ciphertexts (in bits)}} \quad (46)$$

$$= \frac{VJ + N - J}{2 \times (2V + L + N - J + 2\log_2 J + \log_2 N)} \quad (47)$$

For example, for $J = 127$, $N = 1024$, $L = 64$ and $V = 64$, the density D is given by $D \simeq 2.2446$.

Taking account of very high density of KMN PKC, we can conclude that our proposed scheme can be secure against LDA.

Although the details of doing so are omitted, we can show that the proposed method of the improvement of the security can be also applied on Schemes II and III.

5. Conclusion

In this paper we discussed the security on KMN PKC. In KMN PKC, two independent messages and two subsidiary messages that can be considered mutually independent are encrypted to four different ciphertexts. Two independent messages are encoded to error-correcting codes to improve the security of the proposed scheme. We have shown that the using of random noisy symbols $v_1, v_2, \ldots, v_J$ besides message symbols $m_{J+1}, m_{J+2}, \ldots, m_N$ is able to improve the security of KMN PKC.

The density of the proposed scheme can be made significantly large and the rate R is given by $0.4 < R < 0.5$. It seems that KMN PKC can be sufficiently secure against the LDA for sufficiently large n.

The method of the improvement of security can be applied for the various classes of knapsack type cryptosystems. We shall report on these problems in near future.

Finally in this paper, as one of the most important motivations of the present paper, we present two challenge problems[2]. We sincerely wish these problems be challenged.

We are thankful for the support of SCOPE.

REFERENCES

[1] M. Kasahara, Y. Murakami, T. Nasako: "A new construction of knapsack cryptosystems," IEICE Technical Report ISEC2007-89, 2007.

[2] 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.

[3] A. Shamir : "A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem," Proc. Crypto'82, LNCS, pp.279–288, Springer-Verlag, Berlin, 1982.

[4] A. Shamir : "A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem," IEEE Trans. Inf. Theory, IT-30, pp.699–704, 1984.

[5] E.F. Brickell : "Solving low density knapsacks," Proc. Crypto'83, LNCS, pp.25–37, Springer-Verlag, Berlin, 1984.

[6] 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.

[7] 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.

[8] A. Shamir and R. Zippel: "On the security of the Merkle-Hellman cryptographic scheme," IEEE Trans. on Information Theory, vol.IT-26, no.3, pp.339-340, 1980.

[9] 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.

[10] 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.

[11] K. Kobayashi, T. Suzuki, T. Hayata: "Public key cryptosystems over Gaussian integer ring," Proc. of SCIS 2003, pp.605–608, 2003.

[12] Y. Murakami: "A note on the knapsack public-key cryptosystem over Gaussian integer ring," Night session of SCIS 2003, 2003.

[13] H. Sakamoto, Y. Murakami, A. Hayashi: "Cryptanalysis of the knapsack cryptosystem over Gaussian integers," Technical Report of IEICE, ISEC2004-5, pp.29–33, 2004.

(2) : URL: http://www.osakac.ac.jp/labs/yasuyuki/challenge.html

[14] H. Sakamoto and A. Hayashi: "On key generation for knapsack cryptosystems over the Gaussian integers," Proc. of SCIS 2005, pp.955–960, 2005.
[15] T. Nasako, Y. Murakami, M. Kasahara: "Security of low-density attack on a class of knapsack public-key cryptosystems," Proc. of SITA 2007, 2007.
[16] F. J. MacWilliams and N. J. A. Sloane: "The theory of error-correcting codes," North-Holland, 1997.

Appendix

1. Security Consideration

In the followings let us denote the conditional entropy of Y when X is known by $\mathcal{H}(Y|X)$. In the following, we assume that the message components are equally likely.

In Insecure Scheme I the following relation evidently holds:

$$\mathcal{H}(\boldsymbol{m} \text{ for } C_b|\boldsymbol{m} \text{ for } C_d) = \mathcal{H}(\boldsymbol{m} \text{ for } C_d|\boldsymbol{m} \text{ for } C_b) = 0. \quad (A\cdot1)$$

In Insecure Scheme II the following relation holds:

$$\begin{aligned}\mathcal{H}(\boldsymbol{m}^{(b)}|\boldsymbol{m}^{(d)}) &= \mathcal{H}(\boldsymbol{m}^{(d)}|\boldsymbol{m}^{(b)}) \\ &= \mathcal{H}(\boldsymbol{m}^{(b)}) \\ &= \mathcal{H}(\boldsymbol{m}^{(d)}), \quad (A\cdot2)\end{aligned}$$

$$\mathcal{H}(\widetilde{\boldsymbol{m}}^{(b)}|\widetilde{\boldsymbol{m}}^{(d)}) = \mathcal{H}(\widetilde{\boldsymbol{m}}^{(d)}|\widetilde{\boldsymbol{m}}^{(b)}) = 0. \quad (A\cdot3)$$

Above relations seems to make both Insecure Schemes I and II vulnerable to the LDA.

On the other hand the following relations hold in KMN PKC.

We assume here that both $\boldsymbol{m}^{(b)}$ and $\boldsymbol{m}^{(d)}$ are encoded to error-correcting codes capable of correcting $t/2$ errors.

$$\begin{aligned}\mathcal{H}(\boldsymbol{m}^{(b)}_{ECC}|\boldsymbol{m}^{(d)}_{ECC}) &= \mathcal{H}(\boldsymbol{m}^{(d)}_{ECC}|\boldsymbol{m}^{(b)}_{ECC}) \\ &= \mathcal{H}(\boldsymbol{m}^{(b)}_{ECC}) \\ &= \mathcal{H}(\boldsymbol{m}^{(d)}_{ECC}), \quad (A\cdot4)\end{aligned}$$

$$\mathcal{H}(\boldsymbol{m}^{(b)}_{ECC}|\widetilde{\boldsymbol{m}}^{(d)}) = \frac{n-t}{2}[\text{bits}], \quad (A\cdot5)$$

$$\begin{aligned}\mathcal{H}(\widetilde{\boldsymbol{m}}^{(d)}|\widetilde{\boldsymbol{m}}^{(b)}) &= \mathcal{H}(\widetilde{\boldsymbol{m}}^{(b)}|\widetilde{\boldsymbol{m}}^{(d)}) \\ &= \log_2 \binom{n/2}{t}[\text{bits}]. \quad (A\cdot6)\end{aligned}$$

For example, for $N = 1024, t = 20$,

$$\mathcal{H}(\widetilde{\boldsymbol{m}}^{(d)}|\widetilde{\boldsymbol{m}}^{(b)}) = 118.4(\text{bit}), \quad (A\cdot7)$$

yielding sufficiently large value.

We thus see that message $\boldsymbol{m}^{(b)}_{ECC}, \boldsymbol{m}^{(d)}_{ECC}, \widetilde{\boldsymbol{m}}^{(b)}$ and $\widetilde{\boldsymbol{m}}^{(d)}$ are mutually independent from the practical point of view.

2. Challenge Problem

Find the message [3] $\boldsymbol{m} \in \{0,1\}^{N-J}$ from the given public key $\boldsymbol{g}, \boldsymbol{h}$ and the given ciphertext C_g, C_h.

[Public Key]

$\boldsymbol{g}$ = (83007806339, 106039230857, 80840034635, 76664356352, 16234470562, 19485652205, 70412062280, 45921481352, 101148367529, 103274932874, 37752538345, 21661476260, 82715772887, 85985544161, 68426855857, 89282397566, 81133377249, 517401195, 76858124111, 48020952837, 90151525168, 29610631784, 37585561761, 66496365872, 92763591747, 5869063429, 99504988744, 69836393155, 107850802214, 16195888347, 22704213887, 69709828137, 82913612783, 17486404420, 75122875294, 42568462748, 106068505700, 64843622785),

$\boldsymbol{h}$ = (77473861512, 55216464845, 98645474267, 54114013261, 84039665181, 72081626100, 100169848496, 67108339213, 65715533215, 33034585741, 22781526796, 72826469870, 57290251719, 22482514295, 99999332175, 69440528770, 1506463677, 92396563150, 94185020416, 80700925639, 31018594811, 59102511108, 64001491594, 1777526785, 80730415384, 84777722668, 64000435480, 20645071547, 92724173891, 10313916931, 49259880635, 9789631814, 51199713488, 54241183918, 59641767947, 40526538859, 21021283264, 53317796018),

$N = 38, J = 6, V = 14$.

[Ciphertext]

C_g = 4625381768409598,

C_h = 5510085979575511.

(3) : Other solutions except the true message $\boldsymbol{m}$ can not be acceptable. The true $\boldsymbol{m}$ can be checked by the Message-Digest algorithm 5 (MD5) function as

MD5("$\boldsymbol{m}$") = e5e6a964707e27a84a910b76cd1cabcb.

usage: md5sum --string='$\boldsymbol{m}$' (for Linux)

usage: md5 -s '$\boldsymbol{m}$' (for Mac OS X)

For example, you should type "md5sum --string=101010$\cdots$" when $\boldsymbol{m} = (1, 0, 1, 0, 1, 0, \ldots)$.