A Simple Scheme, for Strengthening Product-sum Type PKC

Masao KASAHARA *

Abstract

In this paper we present a very simple scheme for strengthening the conventional product-sum type PKC which has been long considered insecure against the various attacks such as the secret key attack, LLL attack, etc. We show that with the proposed strengthening scheme, the securities of the conventional product-sum type PKC's can be much improved.

keyword

Product-sum type PKC, Merkle-Hellnan PKC, knapsack type PKC, Shamir's attack, LLL attack.

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 candidate of the classes is the knapsack type PKC. Most of knapsack type PKC's use so called super-increasing sequence first used in Merkle and Hellman's PKC(MH PKC for short) [1]. This epock making PKC, MH PKC was broken by Shamir's attack [2]. In order to overcome the vulnerability, Shamir proposed a new knapsack type PKC using a super-increasing sequence with noise sequence [3]. However this scheme was broken by the LLL attack [4]- [7].

Another sequence, shifted-odd sequence, was proposed by Kasahara and Murakami [8]. However in the following year, by Sakai, Murakami and Kasahara, this scheme was proved broken by Shamir's attack [9], [10]. Various interesting knapsack-type PKC's were reported broken. As a result, very unfortunately product-sum type PKC's(ΣΠPKC's) including knapsack-type PKC's are long considered insecure against the secret key attacks, LLL attack, etc.

In this paper, we present K(AⅡ)Scheme for strengthening the conventional product-sum type PKC, ΣΠPKC [1]- [13]. The presented K(AⅡ)Scheme is a very simple scheme and can be applied to wide classes of ΣΠPKC.

We show that with the proposed strengthening scheme, K(AⅡ)Scheme, the securities of the conventional ΣΠPKC can be much improved. For simplicity we shall refer to the strengthened ΣΠPKC as $K_A \Sigma\Pi PKC$.

Throughout this paper, when the variable v_i takes on a value $\widetilde{v}_i$, we shall denote the corresponding vector $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$ as

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

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

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

$$v(x) = v_1 + v_2 x + \cdots + v_n x^{n-1}. \tag{2}$$

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

The $\widetilde{u}$, $\widetilde{u}(x)$, et al. will be defined in a similar manner.

Throughout the paper, we assume the followings:

(A1) Bob encrypts the message $\boldsymbol{M}$ and sends the ciphertext $\boldsymbol{C}$ to Alice.

(A2) Alice decripts $\boldsymbol{C}$ and decodes $\boldsymbol{M}$.

2 K(AII)Scheme

Let the original message over $\mathbb{Z}$ be

$$\boldsymbol{M} = (M_1, M_2, \cdots, M_N), \tag{3}$$

where M_i takes on 0 or positive integer less than 2^v equally lilely and mutually independently.

Let $\boldsymbol{M}$ be transformed to

$$\boldsymbol{M} \cdot A_I = (m_1, m_2, \cdots, m_N), \tag{4}$$

where A_I is

$$A_I = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1N} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2N} \\ \vdots & & & \\ \alpha_{N1} & \alpha_{N2} & \cdots & \alpha_{NN} \end{bmatrix}. \tag{5}$$

In A_I, α_{ij} takes on 0 or a positive integer less than $2^\mu \in \mathbb{Z}$ in a random manner under the condition that A_I may be non-singular.

The m_i is

$$\begin{aligned} m_i &= \alpha_{1i}M_1 + \alpha_{2i}M_2 + \cdots + \alpha_{Ni}M_N \\ &= f_i^{(1)}(M_1, M_2, \cdots, M_N); i = 1, 2, \cdots, N. \end{aligned} \tag{6}$$

Let $a_1, a_2, \cdots, a_N$ be the public key sequence of a general product-sum type PKC. The ciphertext C is

$$C = m_1 a_1 + m_2 a_2 + \cdots + m_N a_N. \tag{7}$$

In the followings, in order to stress that the ciphertext given above is calculated based on the public key sequence $a_1, a_2, \cdots, a_N$, we shall denote $\boldsymbol{C}$ by $C_{\{a_i\}}$.

From Eqs.(6) and (7), we have

$$\boldsymbol{C}_{\{a_i\}} = f_1^{(1)}(M_1, M_2, \cdots, M_N)a_1 + f_2^{(1)}(M_1, M_2, \cdots, M_N)a_2 + \cdots + f_N^{(1)}(M_1, M_2, \cdots, M_N)a_N, \tag{8}$$

where $f_i^{(1)}(M_1, M_2, \cdots, M_N)$ is given by Eq.(6).

We then have the followings from Eqs.(7) and (8):

$$\begin{aligned} \boldsymbol{C}_{\{a_i\}} =& (\alpha_{11}M_1 + \alpha_{21}M_2 + \cdots + \alpha_{N1}M_N)a_1 \\ &+ (\alpha_{12}M_1 + \alpha_{22}M_2 + \cdots + \alpha_{N2}M_N)a_2 \\ &\qquad\qquad \vdots \\ &+ (\alpha_{1N}M_1 + \alpha_{2N}M_2 + \cdots + \alpha_{NN}M_N)a_N \\ =& M_1(\alpha_{11}a_1 + \alpha_{12}a_2 + \cdots + \alpha_{1N}a_N) \\ &+ M_2(\alpha_{21}a_1 + \alpha_{22}a_2 + \cdots + \alpha_{2N}a_N) \\ &\qquad\qquad \vdots \\ &+ M_N(\alpha_{N1}a_1 + \alpha_{N2}a_2 + \cdots + \alpha_{NN}a_N). \end{aligned} \tag{9}$$

Let a new sequence $b_1, b_2, \cdots, b_N$ be

$$b_i = \alpha_{i1}a_1 + \alpha_{i2}a_2 + \cdots + \alpha_{iN}a_N; i = 1, 2, \cdots, N. \tag{10}$$

Regarding $b_1, b_2, \cdots, b_N$ as public keys, we construct the ciphertext $\boldsymbol{C}_{\{b_i\}} = \boldsymbol{C}$:

$$\boldsymbol{C} = M_1 b_1 + M_2 b_2 + \cdots + M_N b_N. \tag{11}$$

In order to stress that the ciphertext $\boldsymbol{C}$ is calculated based on the set $\{b_i\}$, which will be used as public key, ciphertext $\boldsymbol{C}$ will be denoted, $C_{\{b_i\}}$.

The following relation evidently holds :

$$\boldsymbol{C} = \boldsymbol{C}_{\{a_i\}} = \boldsymbol{C}_{\{b_i\}}. \tag{12}$$

For the strengthened $\Sigma\Pi$PKC, $K_A\Sigma\Pi$PKC, sets of keys are :

Public key	:	$\{b_i\}$.
Secret key	:	$\{a_i\}, A_I$.

2.1 Encryption and Decryption processes

Encryption and decryption processes are performed through the following processes :

Encryption process:

Given the message $\boldsymbol{M} = (\widetilde{M}_1, \widetilde{M}_2, \cdots, \widetilde{M}_N)$, referring to the set of public key $\{b_i\}$, Bob calculates the ciphertext $C_{\{b_i\}}$:

$$C_{\{b_i\}} = \widetilde{M}_1 b_1 + \widetilde{M}_2 b_2 + \cdots + \widetilde{M}_N b_N. \tag{13}$$

Decryption Process:

Given the ciphertext $C_{\{b_i\}}$, Alice regards the ciphertext $C = C_{\{b_i\}}$ as $C = C_{\{a_i\}}$. Namely she regards the ciphertext $\boldsymbol{C}$ as

$$C_{\{b_i\}} = C_{\{a_i\}} = \widetilde{m}_1 a_1 + \widetilde{m}_2 a_2 + \cdots + \widetilde{m}_N a_N. \tag{14}$$

$C = C_{\{a_i\}}$ can be decoded according to the decoding process based on the set of the "secret public key", $\{a_i\}$, only known to Alice.

In the following sub-section we shall present an example of $\Sigma\Pi$PKC constructed based on the Chinese remainder theorem(CRT). We shall refer to it as CRT$\Sigma\Pi$PKC.

2.2 $\Sigma\Pi$PKC strengthenend with K(AΠ)Schme

2.2.1 CRT$\Sigma\Pi$PKC

In the followings, $|A|$ implies the size of A in bit.

Let us consider PKC constructed based on the Chinese remainder theorem(CRT) whose secret key and public key are given as follows:

public key:$\{a_i\}$

The a_i's are

$$a_i = \frac{\Pi_{j=1}^{N} p_j}{p_i}; i = 1, 2, \cdots, N, \tag{15}$$

secret key:$\{p_i\}$

The p_i's are all prime numbers such that

$$|p_1| = |p_2| = \cdots = |p_N|. \tag{16}$$

One may think that in order to hide the secret structure of the public key, a_i's be recommended transformed to

$$wa_i \equiv k_i \bmod W, \tag{17}$$

where $\gcd(w, W) = 1$ and $|W| > |p_i|$.

However, even if a_i's are modular transformed shown above, the secret key $\{a_i\}$ cannot be kept secret because the following simple relation holds:

$$\frac{a_i}{a_j} \equiv \frac{k_i}{k_j} \bmod W; i, j = 1, 2, \cdots, N. \tag{18}$$

On the other hand the public key b_i for the strengthened CRTΣΠPKC is from Eq.(10),

$$b_i = \alpha_{i1} \frac{\prod_{j=1}^{N} p_j}{p_1} + \alpha_{i2} \frac{\prod_{j=1}^{N} p_j}{p_2} + \cdots + \alpha_{iN} \frac{\prod_{j=1}^{N} p_j}{p_N}. \tag{19}$$

We see that no simple relation holds for the $\{b_i\}$.

2.2.2 Decoding process of CRTΣΠPKC

Given the ciphertext:

$$C = \widetilde{m}_1 a_1 + \widetilde{m}_2 a_2 + \cdots + \widetilde{m}_N a_N, \tag{20}$$

the message $\widetilde{m}_i$ can be decoded in a parallel fashion:

$$\begin{aligned} Ca_1^{-1} &\equiv \widetilde{m}_1 \bmod p_1, \\ Ca_2^{-1} &\equiv \widetilde{m}_2 \bmod p_2, \\ &\vdots \\ Ca_N^{-1} &\equiv \widetilde{m}_N \bmod p_N. \end{aligned} \tag{21}$$

We then decode the message $\boldsymbol{M}$:

$$(\widetilde{m}_1, \widetilde{m}_2, \cdots, \widetilde{m}_N) A_I^{-1} = (\widetilde{M_1}, \widetilde{M_2}, \cdots, \widetilde{M_N}). \tag{22}$$

2.2.3 Parameters of CRTΣΠPKC

The size of message m_i is, from Eq.(6),

$$|m_i| = |\alpha_{ij}| + |M_i| + \lceil \log_2 N \rceil, \tag{23}$$

where $\lceil x \rceil$ is the ceiling function.

From Eqs.(15) and (21), the size of prime number p_i is

$$|p_i| = |m_i| + 1. \tag{24}$$

The size of public key b_i is

$$|b_i| = (N - 1)|p_i| + |\alpha_{ij}| + \lceil \log_2 N \rceil. \tag{25}$$

The size of ciphertext C is

$$|C| = |M_i| + |b_i| + \lceil \log_2 N \rceil. \tag{26}$$

The coding rate ρ is

$$\rho = \frac{N|M_i|}{|C|}. \tag{27}$$

Size of public key $\{b_i\}$ is

$$S_{PK} = N|b_i|. \tag{28}$$

2.2.4 Example of strengthened CRTΣΠPKC

Example 1: $N = 3$**.**

$$A_I = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix},$$

where $|\alpha_{ij}| = 12$ (bit).

$$\begin{aligned} a_1 &= p_2 p_3, \\ a_2 &= p_1 p_3, \\ a_3 &= p_1 p_2, \end{aligned} \tag{29}$$

where p_i's are prime numbers such that

$$|p_1| = |p_2| = |p_3| \text{ (bit)}. \tag{30}$$

Example 1-A: $|M_i| = 512$ (bit).

The $|m_i|$, $|p_i|$, $|a_i|$ and $|b_i|$; $i = 1, 2, 3$ are

$$\begin{aligned} |m_i| &= |\alpha_{ij}| + |M_i| + \lceil \log_2 N \rceil = 526 \text{ (bit)}, \\ |p_i| &= |m_i| + 1 = 527 \text{ (bit)}, \\ |a_i| &= (N-1)|p_i| = 1054 \text{ (bit)}, \\ |b_i| &= |\alpha_{ij}| + |a_i| + \lceil \log_2 N \rceil = 1068 \text{ (bit)}. \end{aligned} \tag{31}$$

The size of the ciphertext, $|\boldsymbol{C}|$ is

$$|\boldsymbol{C}| = |M_i| + |b_i| + \lceil \log_2 N \rceil = 1582 \text{ (bit)}. \tag{32}$$

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

$$\rho = \frac{N|M_i|}{C} = \frac{1536}{1582} = 0.971, \tag{33}$$

$$S_{PK} = 3|b_i| = 3204 \text{ (bit)}. \tag{34}$$

We see that the size of the public key is little larger than that of RSA·PKC. However encryption and decryption can be performed fast, compared with RSA·PKC.

Example 1-B:$|M_i| = 1024$ (bit).

The $|m_i|, |p_i|, |a_i|$ and $|b_i|$; $i = 1, 2, 3$ are

$$\begin{aligned} |m_i| &= 1038 \text{ (bit)}, \\ |p_i| &= 1039 \text{ (bit)}, \\ |a_i| &= 2078 \text{ (bit)}, \\ |b_i| &= 2092 \text{ (bit)}. \end{aligned} \tag{35}$$

The size of the ciphertext $|\boldsymbol{C}|$ is

$$|\boldsymbol{C}| = 3118 \text{ (bit)}. \tag{36}$$

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

$$\rho = 0.985, \tag{37}$$

$$S_{PK} = 6276 \text{ (bit)}. \tag{38}$$

Two $K_A\Sigma\Pi$PKC's presented in Example 1A and 1B take on high coding rates,which yields a high security against LLL attack.

Example 2: For $N = 16, |M_i| = 512$.
The $|m_i|, |p_i|, |a_i|$ and $|b_i|; i = 1, 2, 3$ are

$$\begin{aligned} |m_i| &= 516 \text{ (bit)}, \\ |p_i| &= 517 \text{ (bit)}, \\ |a_i| &= 7755 \text{ (bit)}, \\ |b_i| &= 7759 \text{ (bit)}. \end{aligned} \tag{39}$$

The size of the ciphertext $|\boldsymbol{C}|$, coding rate $\boldsymbol{\rho}$ and the size the public key S_{PK} are

$$\begin{aligned} |\boldsymbol{C}| &= 8275 \text{ (bit)}, \\ \rho &= 0.990, \\ S_{PK} &= 124 \text{ (Kbit)} = 15.5 \text{ (KB)}. \end{aligned} \tag{40}$$

We see that the coding rate ρ takes on a sufficiently large value to be secure against LLL attack. However the size of public key takes on a larger value compared with the PKC's given in Examples 1-A and 1-B.

2.3 Security consideration

Attack 1: Exhaustive attack on A_I.
The size of A_I is

$$|A_I| \cong N^2|\alpha_{ij}|\text{(bit)}. \tag{41}$$

The probability that A_I is correctly estimated is

$$P_c[\hat{A}_I] \cong 2^{-N^2|\alpha_{ij}|}. \tag{42}$$

In order to be secure against Attack 1, we let $N^2|\alpha_i j|$ be larger than 100 so that $P_c[\hat{A}_I]$ may be

$$P_c[\hat{A}_I] \leq 2^{-100} = 7.9 \times 10^{-31}. \tag{43}$$

We conclude that $K_A\Sigma PKC$ is secure against Attack 1 provided that $P_c[\widetilde{A}_I]$ is made sufficiently small.
In the following theorem, we assume that $P_c[\hat{A}_I]$ is made sufficiently small.
Theorem 1: The sets $\{a_i\}$ and $\{\alpha_{ij}\}$ cannot be uniquely disclosed from the public key $\{b_i\}$.
Proof: Let the order of $\{a_i\}$, $\{\alpha_{ij}\}$ and $\{b_i\}$ be $\#\{a_i\}$, $\#\{\alpha_{ij}\}$, $\#\{b_i\}$. It is easy to see that the following equation holds:

$$\#\{a_i\} + \#\{\alpha_{ij}\} = N + N^2 > \#\{b_i\} = N, \tag{44}$$

yielding the proof.
We conclude that $\mathrm{K_A}\Sigma\Pi$PKC is secure against the attack on the secret key. However our $\mathrm{K_A}\Sigma\Pi$PKC would be threatened by LLL attack [4]- [7], when thae coding rate takes on a small value. We recommend that the coding rate be made to take on a larger value than 0.941 [6].

From a conservative point of view, we let ρ be $\rho \gtrsim 0.96$ as we have done so in Examples, Example 1 and Example 2.

3 Conclusion

In this paper we have presented a new scheme K(AⅡ)Scheme for strengthening ΣΠPKC. The conventional ΣΠPKC PKC's are in general insecure against the various attacks such as, ciphertext attack, the secret key attack. As a result, ΣΠPKC's have been long considered insecure. We have shown that with the proposed strengthening scheme K(AⅡ)Scheme, the securities of the conventional ΣΠPKC can be much improved. The suthor would like to conclude that the conventional ΣΠPKC can be made secure against the various attacks provided that the parameters are chosen carefully as we have shown in Examples 1 and 2.

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

References

[1] 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).

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

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

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

[5] 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).

[6] 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).

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

[8] M.Kasahara and Y.Murakami, "New Public-Key Cryptosystems", Tecnical Report of IEICE, ISEC 98-32 (1998-09).

[9] M.Kasahara and Y.Murakami, "Several Methods for Realizing New Public Key Cryptosystems", Technical Report of IEICE, ISEC 99-45 (1999-09).

[10] 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).

[11] 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).

[12] M.Kasahara, "A Construction of New Class of Knapsack-Type Public Key Cryptosystem, K(Ⅱ)ΣPKC", IEICE Technical Report, ISEC, Sept, (2010-09).

[13] M. Kasahara, "Proposals of K(AI), K(AⅡ) and K(AⅢ)Schemes for augmenting code-based PKC, product-sum type PKC and multivariate PKC", IEICE Tech. Report, ISEC 2015-13 (2015-07).