A Construction of A New Class of Knapsack-Type Public Key Cryptosystem, K(Ⅲ)ΣPKC

Masao KASAHARA
Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564-8511 Japan.
kasahara@ogu.ac.jp

Abstract

In this paper, we present a new class of knapsack type PKC referred to as K(Ⅲ)ΣPKC. In a sharp contrast with the conventional knapsack type PKC's, in our proposed scheme, K(Ⅲ)ΣPKC, no conventional secret sequence but the natural binary number with noise is used. We show that the coding rate, a more conservative measure for the security on knapsack PKC, can be made approximately 1.0.

In Appendix, we present K(Ⅱ)ΣPKC.

Keyword

Public-key cryptosystem(PKC), Knapsack type PKC, Subset-sum problem, 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. The multivariate PKC, linear or non-linear, is one of the very promising candidates of such classes [1]∼[6].

Another promising candidate of the members is the knapsack type PKC [7]∼[24]. Most of knapsack type PKC's use so called super-increasing sequence first used in the Merkle and Hellman's PKC(MH PKC for short)[7]. Unfortunately the MH PKC was broken by Shamir[8],[9]. In order to overcome the vulnerability, Shamir proposed a new knapsack type PKC using a super-increasing sequence with noise sequence[13]. However this scheme was broken by the LLL attack[14].

Another sequence, the shifted-odd sequence, was proposed by Kasahara and Murakami[17]. The shifted-odd sequence with noise was also proposed[18],[19].

Recently the present author proposed two new members, K(I)ΣPKC[22] and K(Ⅱ)ΣPKC[23], of the class referred to as Class(0) that use no secret sequence such as super-increasing sequence or shifted-odd sequence.

In this paper, we present a new member of the Class(0), the class that uses no secret sequence but the conventional binary number with noise sequence. The constructed PKC will be referred to as K(Ⅲ)ΣPKC.

In Appendix, we also present K(Ⅱ)ΣPKC, which is similar to K(Ⅲ)ΣPKC.

In the following sections, "random matrix" implies the matrix whose component takes on 0 or 1 in a random manner. We assume that, for simplicity, 0 or 1 is generated equally likely.

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

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

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

Let us define the several symbols:

$$\begin{aligned} C = C_I + C_{II} &: \text{Ciphertext.} \\ C_I &: \text{First ciphertext.} \\ C_{II} &: \text{Second ciphertext.} \\ M_0 &: \text{Message symbol over } \mathbb{Z} \text{ for } C_I. \\ \boldsymbol{M} = (M_1, \cdots, M_n) &: \text{Message vector over } \{0,1\} \in \mathbb{Z} \text{ for } C_{II}. \\ |A| &: \text{Size of } A \text{ in bit.} \end{aligned}$$

2 K(Ⅲ)ΣPKC

2.1 Construction:

Let us transform message $\boldsymbol{M} = (M_1, M_2, \cdots, M_n)$ over $\{0,1\} \subset \mathbb{Z}$ into

$$(M_1, M_2, \cdots, M_n)[P]_{n\times n} = (m_1, m_2, \cdots, m_n), \tag{2}$$

where $[P]_{n\times n}$ is a random permutation matrix.

In K(Ⅲ)ΣPKC, the ciphertext C is given by

$$C = C_I + C_{II}. \tag{3}$$

For the given T, R and W, let w be given by

$$w^{-1}T = R \mod W. \tag{4}$$

where R and T satisfy

$$|R| = |T| = n \ \text{(bit)} \tag{5}$$

Letting M_0 be a message symbol over $\mathbb{Z}$, the first ciphertext, C_I, is given by

$$C_I = M_0 T. \tag{6}$$

Let the set of keys for C_{II}, $\{k_i\}$, be given by

$$w\big(r_i + 2^{i-1}\big) \equiv k_i \mod W; \ i = 1, 2, \cdots, n, \tag{7}$$

where r_i is a random integer that satisfies

$$r_i \equiv 0 \mod R \tag{8}$$

and

$$2^n \leq r_i \leq 2^{2n-\log_2 n-1}. \tag{9}$$

We see that $r_1, r_2, \cdots, r_n$ perform just as like a noise sequence in [13]. The second ciphertext C_{II} is given by

$$C_{II} = \sum_{i=1}^{n} m_i k_i. \tag{10}$$

The ciphertext C is given by

$$C = C_I + C_{II}. \tag{11}$$

From Eq.(6), the size of M_0, $|M_0|$, is given by

$$|M_0| = n - 1 \quad \text{(bit)}. \tag{12}$$

The set of keys is given by

Public key : $\{k_i\}$, T.
Secret key : w, R, W, $\big\{r_i + 2^{i-1}\big\}$, $[P]_{n\times n}$.

2.2 Encryption and decryption processes

Encryption process:
Step1: The first ciphertext, $\tilde{C}_I$, is given by

$$\tilde{C}_I = \tilde{M}_0 T. \tag{13}$$

Step2: The second ciphertext, $\tilde{C}_{II}$, is given by

$$\tilde{C}_{II} = \sum_{i=1}^{n} \tilde{m}_i k_i. \tag{14}$$

Step3: The ciphertext $\tilde{C}$ is given by

$$\tilde{C} = \tilde{C}_I + \tilde{C}_{II}. \tag{15}$$

Decryption process:
Step1: Intermediate message $\tilde{M}_I$ is obtained by

$$\begin{aligned} w^{-1}\tilde{C} &\equiv \tilde{M}_I \mod W \\ &= \sum_{i=1}^{n} \tilde{m}_i\big(r_i + 2^{i-1}\big) + \tilde{M}_0 R. \end{aligned} \tag{16}$$

Step2:

$$\tilde{M}_I \equiv \sum_{i=1}^{n} \tilde{m}_i 2^{i-1} \mod R, \tag{17}$$

yielding $\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n$.
Step3: $\tilde{M}_0$ is decoded by

$$\tilde{M}_0 = \left\{ \tilde{M}_I - \sum_{i=1}^{n} \tilde{m}_i\big(r_i + 2^{i-1}\big) \right\} R^{-1}. \tag{18}$$

Step4: The original message $\tilde{\boldsymbol{M}}$ can be obtained by

$$\begin{aligned} (\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n)[P]_{n\times n}^{-1} &= \tilde{\boldsymbol{M}} \\ &= \Big(\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_n\Big). \quad \square \end{aligned} \tag{19}$$

We see that the encryption and decryption processes can be performed very fast. It should be noted that no sequential process is required when decrypting the ciphertext.

2.3 Parameters

The sizes of ciphertexts C_I, C_{II} and C are given by

$$|C_I| = 2n - 1, \tag{20}$$

$$|C_{II}| = 2n + \log_2 n, \tag{21}$$

and

$$|C| = |C_I| + |C_{II}| = 2n + \log_2 n + 1, \tag{22}$$

respectively. The size of the public keys, S_{PK}, is given by

$$S_{PK} = n|k_i| + n = n(2n + 1). \tag{23}$$

The coding rate ρ is given by

$$\rho = \frac{\text{Entropy of original message}}{\text{Length of ciphertext}} = \frac{2n - 1}{2n + \log_2 n + 1}. \tag{24}$$

3 Security considerations

LLL attack on w and W

In the followings we assume that the first exponents $0, 1, 2, 3$ are correctly estimated through the exhaustive search and the following equations are successfully obtained.

$$\begin{aligned} w(r_1+1) &= Q_1W+k_1, & (25)\\ w(r_2+2) &= Q_2W+k_2, & (26)\\ w(r_3+4) &= Q_3W+k_3, & (27)\\ w(r_4+8) &= Q_4W+k_4. & (28) \end{aligned}$$

where Q_i's are the quotients.

In the followings, for simplicity, we let $r_i + 2^{i-1}$ be denoted by A_i. From Eqs.(25) $\sim$ (28), we obtain

$$\begin{aligned} &k_2k_4(A_1Q_3 - A_3Q_1) - k_2k_3(A_1Q_4 - A_4Q_1)\\ &+k_1k_3(A_2Q_4 - A_4Q_2) - k_1k_4(A_2Q_3 - A_3Q_2) = 0 \qquad (29) \end{aligned}$$

The size of k_ik_j, $|k_ik_j|$ is given by

$$|k_ik_j| = 4n \text{ (bit)}. \qquad (30)$$

On the other hand the size of $A_iQ_j - A_jQ_j$, $|A_iQ_j - A_jQ_j|$ is given by

$$|A_iQ_j - A_jQ_j| = 4n - \log_2 n. \qquad (31)$$

We see that when n is sufficiently large, the following relation approximately holds

$$|k_ik_j| \approx |A_iQ_j - A_jQ_j|. \qquad (32)$$

From Eqs. (29), (30), (31), and (32), we see that the unknown coefficients of $\{k_lk_m\}$, $\{A_iQ_j - A_jQ_j\}$ in Eq. (29) cannot be disclosed by LLL attack.

We thus conclude that the set of secret keys w and W are kept secret.

LLL attack on ciphertext

The coding rate, ρ given by Eq.(24), a reasonable measure for the security of knapsack PKC, takes on a sufficiently large value as we see in the examples given in the next section:

$$\rho = 0.994 \text{ for } n = 1024, \qquad (33)$$

an extremely large value.

We conclude that K(Ⅲ)ΣPKC would be secure against LLL attack on ciphertext as the coding rate takes on sufficiently large values.

Randomness of K_i

In K(Ⅲ)ΣPKC, no secret sequence but the natural binary number with noise sequence is used. In a sharp contrast with K(Ⅱ)ΣPKC(Please see Appendix), the randomness of K_i in K(Ⅲ)ΣPKC is sufficiently large. It should be noted that, the ciphertext C can be kept secret due to the addition of the first ciphertext.

4 Examples

In Table 1, we show several examples of K(Ⅲ)ΣPKC. We see that the coding rates take on large values.

Table 1: Examples

Ex.	n	$\|M\| + \|M_0\|$	$\|C\|$	ρ	S_{PK}(Kbit)
Ⅰ	256	511	521	0.983	131
Ⅱ	512	1023	1034	0.989	525
Ⅲ	1024	2047	2059	0.994	2098
Ⅳ	2048	4095	4108	0.997	8391

5 Conclusion

We have presented a new class of linear multivariate PKC referred to K(Ⅲ)ΣPKC. To summarize, K(Ⅲ)ΣPKC has the following remarkable features:

1 : Principle of construction is simple.
2 : Coding rate ρ, achieves $\rho \gtrsim 0.99$ for a reasonable size of public key.
3 : Decryption process can be performed very fast.
4 : No secret sequence but the natural binary number with noise is used.

References

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

[2] 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).

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

[4] S.Tsujii, A.Fujioka and Y.Hirayama, "Generalization of the public-key cryptosystem based on the difficulty of solving a system of non-linear equations", IEICE Trans. Vol.1 J-72-A, 2, pp.390-397, (1989-02).

[5] S.Tsujii, R.Fujita and K.Tadaki, "Proposal of MOCHIGOMA (piece in hand) concept for multivariate type public key cryptosystem", Technical Report of IEICE, ISEC 2004-74, (2004-09).

[6] 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).

[7] 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).

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

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

[10] E.F. Brickell, “Solving low density knapsacks”, Proc. Crypto’83, LNCS, pp.25-37, Springer-Verlag, Berlin, (1984).

[11] 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).

[12] 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).

[13] 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).

[14] 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).

[15] 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).

[16] 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).

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

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

[19] 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).

[20] K. Kobayashi, T. Suzuki, T. Hayata, “Public key cryptosystems over Gaussian integer ring”, Proc. of SCIS 2003, pp.605-608, (2003).

[21] M.Kasahara, Y.Murakami, and T.Nasako, “A New Construction of Knapsack Cryptosystem”, IEICE Technical Report, ISEC 2007-89, pp.1-6, (2007-07).

[22] 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).

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

[24] M.Kasahara and Y.Murakami, “$(u|u+v)\Sigma$PKC Along with Challenge Problems of Small Key Size”, SCIS 2011, Kokura, (2011-01).

Appendix: A Construction of K(Ⅱ)ΣPKC

In this appendix, we present a new class of knapsack type PKC referred to as K(Ⅱ)ΣPKC. In a sharp contrast with the conventional knapsack type PKC’s, in K(Ⅱ)ΣPKC, no conventional secret sequence but the natural binary number with noise is used.

A1. Construction

For a given set of T and W, we obtain w by

$$w^{-1}T \equiv 1 \mod W. \tag{34}$$

Let ϵ_i be defined by

$$\epsilon_i = \epsilon_i' + \epsilon_i''; i = 1, 2, \cdots, n, \tag{35}$$

where ϵ_i'’s and ϵ_i''’s are integers. We assume that ϵ_i’s satisfy

$$0 \leq \epsilon_1 + \epsilon_2 + \cdots + \epsilon_n \leq 2^{\lambda}. \tag{36}$$

Let the set $\{k_i'\}$ be given by

$$w\bigl(\epsilon_i' + 2^{i+\lambda}\bigr) \equiv k_i' \mod W; i = 1, 2, \cdots, n. \tag{37}$$

Let the set of keys, $\{k_i\}$, be given by

$$k_i = k_i' + \epsilon_i'' T; i = 1, 2, \cdots, n. \tag{38}$$

Public key	:	$\{k_i\}$.
Secret key	:	w, W, T, $\{\varepsilon_i\}$, $[P]_{n\times n}$.

Encryption process:

The ciphertext is given by

$$\tilde{C} = \tilde{m}_1 k_1 + \tilde{m}_2 k_2 + \cdots + \tilde{m}_n k_n + \tilde{M}_0 T. \tag{39}$$

Decryption process:

Step1:

$$\begin{aligned} w^{-1}\tilde{C} &= \tilde{m}_1\varepsilon_1 + \tilde{m}_2\varepsilon_2 + \cdots + \tilde{m}_n\varepsilon_n \\ &\quad + \tilde{m}_1 2^{\lambda+1} + \tilde{m}_2 2^{\lambda+2} + \cdots + \tilde{m}_n 2^{\lambda+n} + \tilde{M}_0 \mod W. \end{aligned} \tag{40}$$

Step2:

$$\tilde{m}_1\varepsilon_1 + \tilde{m}_2\varepsilon_2 + \cdots + \tilde{m}_n\varepsilon_n + \tilde{m}_1 2^{\lambda+1} + \cdots + \tilde{m}_n 2^{\lambda+n} + \tilde{M}_0 \equiv \tilde{M}_0 \bmod 2^{\lambda}, \tag{41}$$

yielding $\tilde{M}_0$.

Step3:

As $\tilde{m}_1\varepsilon_1 + \tilde{m}_2\varepsilon_2 + \cdots + \tilde{m}_n\varepsilon_n$ is smaller than $2^{\lambda}, \tilde{m}_1, \cdots, \tilde{m}_n$ is given instantly from Eq.(41) as they are.

Step4:

The original message can be obtained by

$$(\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_n)[P]^{-1}_{n\times n} = \left(\tilde{M}_1, \tilde{M}_2, \cdots, \tilde{M}_n\right). \tag{42}$$

A2. Example

We shall present several examples in Table 2. Size of public key, S_{PK} is given by

$$S_{PK} = n(\lambda + n) \text{ (bit)}. \tag{43}$$

In this paper we assume that λ is given

$$\lambda = 2\log_2 n. \tag{44}$$

The size of the ciphertext, $|C|$, is given by

$$|C| = |K_i| + \log_2 n + \lambda = n + 3\log_2 n. \tag{45}$$

Table 2: Examples

Example	n	$\lvert C\rvert$(bit)	S_{PK}(Kbit)	ρ
I	511	539	267	0.948
II	1023	1054	1060	0.970
III	2047	2081	4220	0.984

A3. Conclusion

We have presented a new class of linear multivariate PKC referred to as K(II)ΣPKC. To summarize, K(II)ΣPKC has the following remarkable features.

Feature I	:	Principle of construction is very simple.
Feature II	:	No secret sequence but natural binary number with noise is used.
Feature III	:	Coding rate ρ, achieves $\rho \gtrsim 0.95$ for a reasonable size of public key.
Feature IV	:	Decryption process can be performed very fast.