LETTER Special Section on Information Theory and Its Applications

On the Security of the Improved Knapsack Cryptosystem

Hidenori KUWAKADO[†] *and* Hatsukazu TANAKA[†], *Members*

SUMMARY We discuss the security of the improved knapsack cryptosystem that Kobayashi and Kimura have proposed. Two attacking methods for their cryptosystem are proposed; one is the method for obtaining secret keys from public keys by using the continued fraction, and the other is for decrypting the ciphertext without knowing secret keys. We show that their cryptosystem is not secure against these attacks.

key words: *public-key cryptosystem, knapsack problem, choice of encryption keys, continued fraction, LLL algorithm*

1. Introduction

Kobayashi and Kimura have shown a new concept on public-key cryptosystems. The new concept is that a sender can choose encryption keys from a given encryption-key set. They have proposed an improved knapsack cryptosystem based on this concept (the *KK scheme*) [1].

We propose two attacking methods on the KK scheme; one uses the continued fraction algorithm, and the other uses the LLL algorithm. We show that the KK scheme is not secure against the proposed attacking methods.

On the KK scheme, we follow the notation of [1], and denote an equation number in [1] by, for example, Eq. (KK-1).

2. Proposed Methods

2.1 Method I

Although there are many secret keys in the KK scheme, they can be always computed if the value of $w^{-1} \bmod p$, denoted by w', is known, where w is one of secret keys. Hence, we attempt to obtain the value of w'. From Eqs. (KK-1)(KK-5)(KK-8), the following inequality holds.

$$0 < a_1 < \cdots < a_{2n} < b_1 < \cdots < b_{2n} < p, \tag{1}$$

where a_i and b_i are secrete keys, and p is one of public keys. We can evaluate the possible minimum value of p as follows. Since the possible minimum value of a_i is i, the possible minimum value of A_m is n^2+n. From Eq. (KK-5), the possible minimum values of b_{2i-1} and b_{2i} are $(kA_m+1)(k^2+k+1)^{i-1}$ and $(k+1)(kA_m+1)(k^2+k+1)^{i-1}$, respectively. Since $A_m \geqq n^2+n$, we have

$$p \geqq (k(n^2+n)+1)(k^2+k+1)^n+1. \tag{2}$$

From Eq. (2), we observe that p must be large even if n is small. This property is useful for finding the value of w'. For $1 \leqq j \leqq 2n$, we attempt to find v_j such as both of $s_{1\,j}$ and $s_{2\,j}$ become to be as small as possible.

$$\begin{cases} s_{1\,j} &= v_j e_{1\,j} \bmod p, \\ s_{2\,j} &= v_j e_{2\,j} \bmod p, \end{cases} \tag{3}$$

where $e_{i\,j}$ is one of public keys. Notice that it is guaranteed that there exists such v_j in the KK scheme. Namely, w' is one of such v_j.

The method for finding such v_j is shown as follows. For simplicity, we assume that $e_{i\,j}$ is relatively prime to p. It is not difficult to extend the method described here to the case of $\gcd(e_{i\,j}, p) \neq 1$. Let $r_j = e_{1\,j}/e_{2\,j} \bmod p$. We have the following modular equation from Eq. (3).

$$s_{1\,j} \equiv s_{2\,j} r_j \pmod p \tag{4}$$

Moreover Eq. (4) is transformed to the following equation.

$$\frac{r_j}{p} = \frac{\ell}{s_{2\,j}}\left(1 + \frac{s_{1\,j}}{\ell p}\right), \tag{5}$$

where ℓ is an unknown integer. Here, r_j and p in the left side are known values, and s_{ij} and ℓ in the right side are unknown values. Using the extended continued fraction algorithm [2], we can find the smallest pair $(s_{1\,j}, s_{2\,j})$ satisfying Eq. (5). By substituting such $(s_{1\,j}, s_{2\,j})$ into Eq. (3), v_j is computed. We obtain v_j for all j with the method stated above. As the result of our computer simulation, we know that v_j is equal to w' for many j. Hence, the value that often appears among v_j $(1 \leqq j \leqq 2n)$ can be adopted as the guess of w'. We compute the matrix E' as $E' = w'E \bmod p$, where the matrix E is the public key in Eq. (KK-10). Using Eq. (1), we can separate E' into A and B_2 in Eqs. (KK-2)(KK-7). Moreover, from Eq. (1), B_1 can be obtained from B_2. Therefore, all secret keys can be obtained.

2.2 Method II

For a given ciphertext C, let consider the following ma-

Manuscript received January 16, 1998.
Manuscript revised April 13, 1998.

[†]The authors are with the Faculty of Engineering, Kobe University, Kobe-shi, 657–8501 Japan.

trix U_t, which is a modified version of the Lagarias-Odlyzko matrix [3].

$$U_t = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & f_{1\,1} \\ 0 & 1 & \cdots & 0 & 0 & f_{2\,1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & f_{1\,n} \\ 0 & 0 & \cdots & 0 & 1 & f_{2\,n} \\ 0 & 0 & \cdots & 0 & 0 & -C-tp \end{pmatrix} \qquad (6)$$

where $f_{i\,j} = e_{i\,2j-1} + e_{i\,2j} \bmod p$ and $e_{i\,k}$ is an element of the public matrix E in Eq. (KK-10). For $t = 0$ to $nk-1$, the following steps are carried out; (i) construct the matrix U_t as Eq. (6), (ii) find short vectors by applying the LLL algorithm to U_t, (iii) for each short vectors obtained above, check if it includes the plaintext, (iv) if such a vector is found, then select elements of the plaintext from it, otherwise, set $t \leftarrow t+1$ and go to (i).

We explain the reason why the plaintext can be computed from the short vector. Let the plaintext be $\{m_1, \cdots, m_n\}$. If a sender chooses $e_{1\,j}$ $(1 \leqq j \leqq 2n)$ in Eq. (KK-10) as the encryption keys, then the $(2n+1)$-dimension vector $V = \{m_1, 0, m_2, 0, \cdots, m_n, 0, 0\}$ can be expressed as the linear combination of row vectors of Eq. (6) for some t. Note that the order of m_i and 0 depends on the chosen encryption keys. Since the length of V is at most $k\sqrt{n}$, the length of V is much shorter than that of row vectors of Eq. (6). Hence, such V might be found via the LLL algorithm. It is easy that the plaintext is obtained from V because of the form of V.

3. Simulation Results

In this section, suppose that $m_i = 0$ or 1 $(1 \leqq i \leqq n)$. Table 1 shows the probability such that secret keys can be computed with the method I. The probability of success of the method I is equal to that of guessing w' correctly. We discuss the rare case that the method I fails. In Eq. (3), let z_j be the greatest common divisor of $s_{1\,j}$, $s_{2\,j}$ and w'. If $z_j \neq 1$ for almost j, then the value of w' can not be guessed correctly because the value of w'/z_j is given by the extended continued fraction algorithm. In this case, correct secret keys can not be obtained. However, it seems difficult that a user makes z_j large for almost j. Hence, by using the simple exhaust search on the multiples of the guess, it is possible to find the true value of w'. In the simulation of Table 1, such a search is not carried out. Figure 1 shows the probability of success of the method II. The horizontal axis of Fig. 1 is the Humming weight (the number of ones) of the plaintext. If the Humming weight is large, then the method II is not effective. The reason is that the LLL algorithm can not always find the shortest vector when the number of rows of U_t is large.

Table 1 The success rate of the method I.

n	64	96	128
prob. [%]	99.95	100.0	100.0

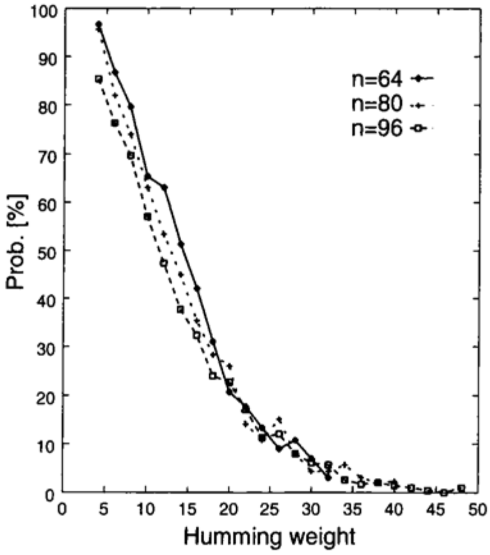

Fig. 1 The success rate of the method II.

4. Conclusion

The KK scheme is not secure against the proposed attacks. The method I uses the fact that the modulus is much larger than the values of secret keys. The method II is one of the low-density attacks. From the point of view of the complexity of solving the knapsack problem, we discuss the security of the KK scheme. For the binary plaintext with n elements, the LLL algorithm with $2n+1$ dimensions is carried out at most n times in the method II. On the other hand, in order to solve the binary knapsack problem with n elements, the LLL algorithm with $n+1$ dimensions is carried out one time. The running time of the LLL algorithm is in proportion to the number of dimensions to the fourth power. Hence, the running time of the method II is at most $n((2n+1)/(n+1))^4$ $(\approx 16n)$ times as long as that for solving the binary knapsack problem.

Acknowledgment

The authors would like to thank the anonymous referees for their valuable comments.

References

[1] K. Kobayashi and M. Kimura, "A consideration on the security improvement of the knapsack cryptosystem," IEICE Trans., Fundamental, vol.J79-A, no.8, pp.1339–1343, 1996.

[2] H. Kuwakado and H. Tanaka, "Fast algorithm for finding a small root of a quadratic modular equation," Proc. of the First International Workshop ISW'97, LNCS, vol.1396, pp.75–81, 1998.

[3] J.C. Lagarias and A.M. Odlyzko, "Solving low density subset sum problem," Proc. of 24th IEEE Symp. Found. Comput. Sci., pp.1–10, 1983.

[4] A.K. Lenstra, H.W. Lenstra Jr., and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen, vol.261, pp.515–534, 1982.