Cryptanalysis of a Knapsack Cryptosystem based on Multiple Knapsack

Jinsu kim[1†]

Naval Academy, Republic of Korea

Summary
We propose a cryptanalysis of a knapsack cryptosystem which is based on three knapsacks. That was introduced by Kobayashi et al [1]. On their encryption scheme, a cipher text is formed by multiplying two non-super-increasing knapsacks together and then adding it to the super-increasing knapsack. They insist that this construction is secure against known attacks including the low density attack and Shamir attack. However due to modular mapping structure, we can apply the method, orthogonal lattice attack, provided by Nguyen and Stern in Crypto'97[6]. More specifically, we show how to find private keys from the corresponding public keys in the cryptosystem. Therefore, we argue that the cryptosystem is insecure one.

Key words:
Knapsack, Cryptosystem, orthogonal lattice attack, multiple knapsack

1. Introduction

The Knapsack problem attracted the attention of cryptographers due to their NP-complete hardness and simplicity. In this background, a lot of Knapsack cryptosystems are proposed. The first cryptosystem is that of Merkle-Hellman [2]. Although the underlying problem is NP-complete by the transformation, it has surprisingly been broken by Shamir [5] because of the special structure of the private key. Even applying a sequence of modular mappings was shown to be insecure (see [5, 11]). Despite the failure of Merkle-Hellman cryptosystems, knapsack like cryptosystems were designed by researchers, because such systems are very easy to implement and can attain very high encryption/decryption rates. But most of the proposed knapsack or knapsack-like cryptosystems have been broken (for a survey, see [12,13]), either by specific attacks or by the so-called the low-density attack. When the density is small (about less than 0:94), one can solve the knapsack problem directly by using a lattice reduction with high probability (see [4,14]). Such attack is called low-density attack. But this attack is still ineffective against high-density knapsacks. So some knapsack cryptosystems with high density have been proposed [15].

In particular, Kobayashi et al proposed a cryptosystem in [1] that is designed by multiplying two non-super-increasing knapsacks together and then adding it to the super-increasing knapsack. They argue that any attacker cannot apply the low density attack using LLL algorithm. Therefore, although the other knapsack is super-increasing, they expect one cannot obtain any information about whole secret keys. In this paper, we propose an attack for the cryptosystem of Kobayashi et al. So one can find the private key from the public key of the cryptosystem in reasonable time.

2. Preliminaries

In this section, we need the notion of lattice which is a subset of the vector space R^n. We will write all vectors as rows and bold face letters, $\|\boldsymbol{v}\|$as the Euclidean norm of a vector $\mathbf{v} \in R^n$, induced by dot product $\langle\ ,\ \rangle$.

Definition 1. Let $\{\boldsymbol{b}_1,\ \dots,\ \boldsymbol{b}_d\}$ be a linearly independent set of vectors in R^n with $\mathrm{d} < \mathrm{n}$. The lattice Λ generated by $\{\boldsymbol{b}_1,\ \dots,\ \boldsymbol{b}_d\}$ is the set $\Lambda = \left\{\sum_{i=1}^{d} l_i\, \boldsymbol{b}_i : l_i \in Z\right\}$ of integer linear combinations of the $\boldsymbol{b}_i$'s.

The vectors $b_1, \dots, b_d$ are called a basis. The lattice rank (or dimension) is d. If d = n, Λ is said to be a full rank (or dimension) lattice. We say that Λ is a sub-lattice of a lattice Ω in R^n if Ω contains Λ and if both have the same dimension. A basis matrix B of a lattice Λ is an $\mathrm{d} \times \mathrm{n}$ matrix formed by taking the rows to be basis $b_i = \left(b_{i,1},\ b_{i,2}, \dots, b_{i,n}\right)$. Thus $B_{i,j}$ is the j-th entry of the row vector b_i and $\Lambda = \{xB : x \in Z^n\}$. By assumption the rows of a basis matrix are always linearly independent. All base of Λ span the same R-vector subspace of R^nwhich we denote by Sp_Λ. The dimension of Sp_Λ over R is equal to the dimension of Λ. For the lattice $\overline{\Lambda} = Sp_\Lambda \cap Z^n$. Λ is a sub-lattice of $\overline{\Lambda}$. We say that Λ is a complete lattice, if $\Lambda = \overline{\Lambda}$. In particular, $\overline{\Lambda}$ is a complete lattice.

Definition 2. Let $\mathrm{F} = Sp_\Lambda{}^{\perp}$ be the orthogonal vector subspace with respect to the inner(dot) product. We define the orthogonal lattice to be $\Lambda^{\perp} = F \cap Z^n$. Thus $\Lambda^{\perp}$ is a complete lattice in Z^n, with dimension $\mathrm{n} - \mathrm{d}$ if d is the dimension of Λ.

Since a lattice Λ is completely determined by a basis matrix B, so we can define the determinant of Λ.

Definition 3. Let Λ be a lattice in R^n of rank d with basis matrix B. The $\mathrm{d} \times \mathrm{d}$ Gram matrix of B is BB^t. This is a

Manuscript received August 5, 2019
Manuscript revised August 20, 2019

matrix whose (i, j) entry is $\langle b_i, b_j \rangle$. Then $\det(\Lambda) = \sqrt{det(BB^t)}$.

Theorem 1 ([6]). Let Λ be a lattice in R^n. Then $\det(\Lambda^{\perp}) = \det(\Lambda)$. And $\det((\Lambda^{\perp})^{\perp}) = \det(\Lambda^{\perp}) = \det \overline{\Lambda}$.

Finding a short basis of a lattice is called lattice reduction. In 1982 A.K. Lenstra, H.W. Lenstra, and L. Lovasz introduced a new notion of reduction and a polynomial time reduction algorithm, which is called LLL algorithm ([3]). LLL does not guarantee to find the shortest lattice vector. It guarantees in polynomial time to find a vector within a factor of the shortest vector. Even more, in practice, LLL algorithm often performs much better than the theoretical bound. Above all, in this paper, I need only some useful facts about the notion of an orthogonal lattice and following theorem in [6]. Thanks to the LLL algorithm, one can compute many short and linearly independent vectors in $\Lambda^{\perp}$.

Theorem 2. There exist an algorithm which, given as input a basis $\{\boldsymbol{b}_1, \ \dots, \ \boldsymbol{b}_d\}$ of a lattice Λ in Z^n, outputs an LLL-reduced basis of the orthogonal lattice $\Lambda^{\perp}$, and whose running time is polynomial with respect to n, d and any upper bound of the bit-length of $\|\boldsymbol{b}_i\|$'s.

2.1 Equations

If a displayed equation needs a number, place it flush with the right margin of the column (e.g., see Eq. 1).

$$y_i(N) = \sum_{n=0}^{m-1} w_n(N) b_n(N) = \sum_{n=0}^{m-1} \overline{b_n^*(N) r_i(N)} \cdot b_n(N) \quad (1)$$

3. Description of the Cryptosystem

Kobayashi et al[1]'s cryptosystem is based on three Merkle-Hellman knapsacks. We will give a brief explanation about their scheme.

Key Generation : A six tuple (**A**, **B**, **E**, P, u, v) forms the secret key, and a triple (**F**, **G**, **H**) forms public key, where **A**, **B**, **E**, **F**, **G**, **H** $\in N^n$ and P, u, v $\in$ N.

1. Choose positive integers a_1 and b_1 and a non-negative integer e_1.
2. For k = 2 to n, choose a_k and b_k satisfying $a_k \leq \sum_{i=1}^{k-1} a_i$, $b_k \leq \sum_{i=1}^{k-1} b_i$.
3. Choose a non-negative integer e_k satisfying
$e_k > a_k b_k + \left(\sum_{i=1}^{k-1} a_i\right)\left(\sum_{i=1}^{k-1} b_i\right) + \sum_{i=1}^{k-1} e_i - a_1(2^{n-1} - 2^{k-1})\left(a_k - \sum_{i=1}^{k-1} a_i\right) - b_1(2^{n-1} - 2^{k-1})\left(b_k - \sum_{i=1}^{k-1} b_i\right)$
4. Set **A** $= (a_1, \dots, a_n)$, **B** $= (b_1, \dots, b_n)$, and **E** $= (e_1, \dots, e_n)$.
5. Choose positive integers P, u and v so as to satisfy that $P > \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) + \sum_{i=1}^{n} e_i$, gcd(u, P) = gcd(v, P) = 1
6. Based on the secret key (**A**, **B**, **E**, P, u, v), calculate the public keys

F $= (f_1, \dots, f_n)$, $f_i \equiv u a_i \bmod P$,
G $= (g_1, \dots, g_n)$, $g \equiv v b_i \bmod P$,
H $= (h_1, \dots, h_n)$, $h_i \equiv uv e_i \bmod P$

Encryption : A plaintext is represented as a vector X $= (x_1, \dots, x_n)$ with $x_i \in \{0, 1\}$ and the corresponding cipher text is represented by an positive integer C $= C_1 C_2 + C_3$,

$$C_1 = f_1 x_1 + \cdots + f_n x_n$$
$$C_2 = g_1 x_1 + \cdots + g_n x_n$$
$$C_3 = h_1 x_1 + \cdots + h_n x_n$$

Decryption : Let u^{-1} and v^{-1} be the modular inverses. i.e. u^{-1} and v^{-1} be integers which satisfy that $uu^{-1} \equiv 1 \ mod \ P$ and $vv^{-1} \equiv 1 \ mod \ P$, respectively.

1. Set d $= \left(\sum_{i=k+1}^{n} a_i x_i + a_k\right)\left(\sum_{i=k+1}^{n} b_i x_i + b_k\right) + \sum_{i=k+1}^{n} e_i x_i + e_k$
2. for k = n down to 1, if $\left(\sum_{i=1}^{n} a_i x_i\right)\left(\sum_{i=1}^{n} b_i x_i\right) + \sum_{i=1}^{n} e_i x_i \geq d$ then $x_k = 1$ else $x_k = 0$.
3. Set **X** $= (x_1, \dots, x_n)$

Note that the secret sequences(vectors) **A** and **B** are chosen to be $a_k b_k \leq \left(\sum_{i=1}^{k-1} a_i\right)\left(\sum_{i=1}^{k-1} b_i\right)$ And from 2. and 3. in Key Generation, the secret sequence **E** satisfies super-increasing property.

4.The Attack Scheme

Recall the secret key **A** which corresponding to public key **F** is non-super-increasing. Since **A, B** have the same structure, it is suffice to show that how can find possible secret keys for **A**. Let m be an integer less than n. Define the following vectors in N^m.

f $= (f_1, \dots, f_m)$, **a** $= (a_1, \dots, a_m)$

Note that an attacker knows **f**, but not **a**, and there is a congruence f $\equiv$ u**a** mod P. By congruence relation, we get a following lemma.

Lemma 1. Let x $\in Z^m$. If **x** $\perp$ **f** then **x** $\perp$ **a** or $\|\boldsymbol{x}\| \geq P/\|\boldsymbol{a}\|$.

Proof. we have $\langle \boldsymbol{x}, \boldsymbol{f} \rangle \equiv 0 \bmod P$ since f $\equiv u\boldsymbol{a} \bmod P$ and $\langle \boldsymbol{x}, \boldsymbol{f} \rangle = 0$. If we assume that **x** is not orthogonal to **a**, then $|\langle \mathbf{x}, \mathbf{a} \rangle| \geq P$. Hence, by Cauchy-Schwarz inequality P $\leq \|\boldsymbol{x}\| \|\boldsymbol{a}\|$.

So one may expect that if $\langle \boldsymbol{x}, \boldsymbol{f} \rangle = 0$, and the coefficients of **x** are small, then $\langle \boldsymbol{x}, \boldsymbol{a} \rangle = 0$. More precisely, By theorem 2. as input basis (**f**) of a lattice Λ in Z^m, if we obtain an LLL-reduced basis of the orthogonal lattice $\Lambda^{\perp}$ in polynomial time, then we can expect that the basis vectors are also orthogonal to **a**. The following Heuristic woks well in practice as in [6].

Lemma 2. Let Λ be the lattice spanned by **f**. Let $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}\}$ be an LLL-reduced basis of $\Lambda^{\perp}$. Then the first m-2 vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-2}$ are orthogonal to **a**.

Since A is non-super-increasing and each $a_i \leq 2^{i-2}a_1$, so

$$\|\boldsymbol{a}\| \leq \sqrt{{a_i}^2 + {a_i}^2 + 2^2{a_i}^2 + \cdots + 2^{2(m-2)}{a_i}^2} \leq a_1 2^{m-1}$$

Therefore, by lemma 1, if $\mathbf{x} \in Z^m$ is orthogonal to **f** then **x** is also orthogonal to **a** or satisfies or $\|\boldsymbol{x}\| \geq \frac{P}{a_1 2^{m-1}}$ which implies quite long because of step 3, 5 in Key Generation. So one can expect to find m-1 vectors with norm around $\|\boldsymbol{f}\|^{\frac{1}{m-1}} \leq \left(P\sqrt{m}\right)^{\frac{1}{m-1}}$ by theorem 2. This quantity is sufficiently small, so we can expect that the theorem 2. works. Therefore, $\mathbf{a} \in (\boldsymbol{b_1}, \dots, \boldsymbol{b_{m-2}})^{\perp}$. One can expects $\|\boldsymbol{b}_1\| \cong \cdots \cong \|\boldsymbol{b}_{m-2}\| \cong \|\boldsymbol{f}\|^{\frac{1}{m-1}}$. Therefore, the determinant of $(\boldsymbol{b_1}, \dots, \boldsymbol{b_{m-2}})^{\perp}$ is around $\|\boldsymbol{f}\|^{\frac{m-2}{m-1}} \cong \|\boldsymbol{f}\|$. Let the lattice $(\boldsymbol{b_1}, \dots, \boldsymbol{b_{m-2}})^{\perp} = (\boldsymbol{d}_1, \boldsymbol{d}_2)$. Then **a** can be represented as $\mathbf{a} = x_1\boldsymbol{d}_1 + x_2\boldsymbol{d}_2$. Since $\|\boldsymbol{a}\|$ is relatively small for $\|\boldsymbol{f}\|^{\frac{1}{2}} \cong \|\boldsymbol{d}_i\|$ almost case. So we can obtain a small upper-bound for $|x_i|$by following lemma.

Lemma 3. Let $(\boldsymbol{d}_1, \boldsymbol{d}_2)$ be an LLL-reduced basis of a lattice. If $\mathbf{a} = x_1\boldsymbol{d}_1 + x_2\boldsymbol{d}_2$ then for i = 1, 2

$$|x_i| \leq \frac{\|\boldsymbol{a}\|}{\|d_i\|}\sqrt{2^{i-1}\frac{(9/2)^{2-i}+6}{7}}$$

Hence, we can exhaustive search for **a** within the bounds $|x_i|$ in lemma 3. For each $\boldsymbol{x}_1, \boldsymbol{x}_2$, we get possible partial secret keys $\tilde{\mathbf{a}} = (\widetilde{a_1}, \dots, \widetilde{a_m})$. Then check each $\widetilde{\boldsymbol{a}_j} > 0$, and $\widetilde{\boldsymbol{a}_j} \leq \sum_{i=1}^{j-1}\widetilde{\boldsymbol{a}_i}$. And for $\tilde{\boldsymbol{a}}$ which satisfying the previous condition, find $\tilde{P}, \tilde{u}$ such that $\tilde{u}\widetilde{a_j} \equiv f_j \bmod \tilde{P}$ by the following theorem.

Theorem 3. If we know $\mathbf{a} = (a_1, \dots, a_m)$, $\mathbf{f} = (f_1, \dots, f_m)$, then we can find a few possible P, u such that. $ua_j \equiv f_j \bmod P$.

Proof. Since $ua_i \equiv f_i \bmod P$, it follows that $a_i f_j \equiv a_j f_i \bmod P$. Hence, P is a factor of $a_i f_j - a_j f_i$ for $i \neq j$.

Let K be the greatest common divisor of $a_i f_j - a_j f_i$'s That are not 0, $T = \text{Max}\{f_i, g_i, h_i \mid 1 \leq i \leq n\}$. Then $T < P \leq K$, we can factorize $K = sP$ where $1 \leq s \leq \lceil K/T \rceil$. For such possible P, we can find u by $u = a_i f_i^{-1} \bmod P$ for all $1 \leq i \leq m$.

Clearly, if we know the multiplier $\tilde{u}$ and modular $\tilde{P}$ then we can find $\tilde{\mathbf{a}}$ with whole length n from the public key. Since **A, B** have the same structure, we can apply the same method to

$\mathbf{g} = (g_1, \dots, g_l)$, $b = (b_1, \dots, b_l)$

for $l \leq n$. Then we get possible secret keys $\tilde{\mathbf{b}}, \tilde{v}, \tilde{Q}$ such that $\tilde{v}\widetilde{b_j} \equiv g_j \bmod \tilde{Q}$. Now we can make possible secret keys $\tilde{\boldsymbol{e}}$'s from the Key Generation step. Since the modular P is same for all **A, B, E**, so we must choose $\tilde{P}$'s and corresponding $\tilde{\mathbf{a}}$, $\tilde{u}$ which equal to some $\tilde{Q}$. Therefore, if one knows a pair (**X**, C), then the secret key can be revealed.

5. Conclusion

We show that Kobayashi et al's cryptosystem which was based on three knapsacks is not secure. The core attack is the method provided by Nguyen and Jacques Stern in Crypto '97. They argue the proposed knapsack-based cryptosystem is secure against all existing attack. In particular, even one may reveal secret key E by using super-increasing property, they insist the calculation of u and v from uv mod P is more difficult than the prime factorization problem. However due to the congruence structure in order to hide secret key, we can find small number of possible secret keys without considering factorization problem. Finally, this lead to the cryptosystem is vulnerable to known-plaintext attack.

References

[1] K. Kobayashi, K. Tadaki, M. Kasahara and S. Tsujii, A Knapsack Cryptosystem Based on Multiple Knapsacks, ISITA2010, Taichung, Taiwan, October 17-20, 2010.

[2] R. C. Merkle and M. E. Hellman, Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inf. Theory, IT-24 (1978), 525.530.

[3] A. K. Lenstra, H. W. Lenstra, and L. Lovasz, Factoring polynomials with rational coefficients,, Mathematische Annalen, Vol.261, No.4 (1982), 515.534.

[4] J. C. Lagarias and A. M. Odlyzko, Solving low density subset sum problems, J. Assoc. Comp. Math., Vol.32 (1985), 229.246.

[5] A. Shamir, A polynomial-time algorithm for breaking the basic Merkle- Hellman cryptosystem, Proc. CRYPTO 82, Lecture Notes in Computer Science, pp.279.288, Springer, 1982.

[6] Phong Nguyen and Jacques Stern , Merkle-Hellman Revisited: A Cryptanalysis of the Quvanstone Cryptosystem

Based on Group Factorizations, Proc. CRYPTO '97, Lecture Notes in Computer Science, pages 198-212.
[7] Phong Nguyen and Jacques Stern, Cryptanalysis of a Fast Public key cryptosystem Presented at SAC'97, Selected Areas in Cryptography 1998, Springer-Verlag, LNCS 1556, pp. 213-218.
[8] Steven Galbraith, Mathematics of Public Key Cryptography Version 0.9, available at http://www.math.auckland.ac.nz/ sgal018/crypto-book/crypto-book.html.
[9] J. C. Lagarias, Performance Analysis of Shamir's Attack on the Basic Merkle-Hellman Knapsack Cryptosystem, Proc. 11th Intern. Colloquium on Automata, Languages and Programming (ICALP), Lecture Notes in Computer Science, vol. 172, Springer-Verlag, Berlin, 1984, pp. 312-323.
[10] J. C. Lagarias, "Knapsack Public Key Cryptosystems and Diophantine Approximation," Advances in Cryptology, Proc. Crypto 83, Plenum Press, New York, 1984, pp. 3-23.
[11] E. Brickell, Are most low density polynomial knapsacks solvable in polynomial time?, In Proc. 14th Southeastern Conference on Combinatorics, Graph Theory, j and Computing, 1983.
[12] A. M. Odlyzko, The rise and fall of knapsack cryptosystems In Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied he Mathematics, pages 75-88. A.M.S., 1990.
[13] Ming Kin Lai, Knapsack Cryptosystems : The Past and the Future available at http://www.ics.uci.edu/ mingl/knapsack.htmlv
[14] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko,, C.P. Schnorr, and J. Stern. Improved low-density subset sum algorithms Computer, Complexity, 2:111-128, 1992.
[15] B. Wang, Q. Wu, and Y. Hu, A knapsack-based probabilistic encryption scheme Information Sciences, vol. 177, no. 19, 3981-3994, 2007.

Jinsu Kim received the B.S. M.S. and D.S. degrees in Mathematical Science from Seoul National University in 2008, 2012 and 2018, respectively. He now with naval academy in Republic of Korea.