鍵選択　ップザック暗号　その安全性評価

小林邦勝
山形大学工学部電子情報工学科
〒 992 米沢市城南 4-3-16
電話：0238-26-3345
E-mail: kobayash@ee5.yz.yamagata-u.ac.jp

らまし LLL アルゴリズムでの解読が難しいナップザック暗号を提案する　超増加ベクトルに加えて、超増加ではないベクトルも用いて複数の暗号鍵を生成し、暗号鍵の選択を行うナップザック暗号を構成する。本暗号に LLL アルゴリズムを適用して解読の数値実験を行い、LLL アルゴリズムでの解読が難しいことを示す。

ワ　ド ナップザック暗号、超増加ベクトル、暗号鍵の選択、雑音、LLL アルゴリズム

A Knapsack Cryptosystem Choosing Encryption Keys and a Security Assessment

Kunikatsu KOBAYASHI
Department of Electrical and Information Engineering,
Faculty of Engineering,Yamagata University
phone：0238-26-3345
E-mail:kobayash@ee5.yz.yamagata-u.ac.jp

Abstract We propose a knapsack cryptosystem choosing encryption keys. This cryptosystem is possibly difficult to cryptoanalyze by LLL algorithm of a typical cryptoanalysis algorithm in the linear cipher. Encryption keys are generated with super-increasing vector and non-super-increasing vector. By using super-increasing vector,a ciphertext can always be decrypted uniquely.

Key words knapsack cryptosystem,super-increasing vector,choice of encryption key,noise,LLL algorithm

1　まえがき

NP 完全問題の一つにナップザック問題があり、これを暗号に応用した場合には、解読も難しいが、正当な受信者が一意に復号することも難しい。この一般のナップザック問題に超増加性を導入した易しいナップザック問題は、NP 完全問題からクラス P の問題に変換され、これを暗号に用いた場合には、一意に復号することもできるが、解読も容易になる。すなわち、これまでに提案されているナップザック暗号の多くは、LLL アルゴリズム等の解読法に対して弱く、安全性の点に問題があるため、実用には供されていない。

本文では、NP 完全問題と P 問題の間に位置すると思われる計算量のナップザック問題を扱い、これを暗号に応用する。まず、超増加なベクトルに加えて超増加ではないベクトルも用いて複数の暗号鍵を生成し、暗号鍵の選択を行うナップザック暗号を構成する。次に本暗号に LLL アルゴリズムを適用し、数値実験で解読率を求め、LLL アルゴリズムに対しては安全なナップザック暗号を構成できることを示す。

2　ナップザック問題

問題の複雑度のクラスとその関係を図 1 に示す。

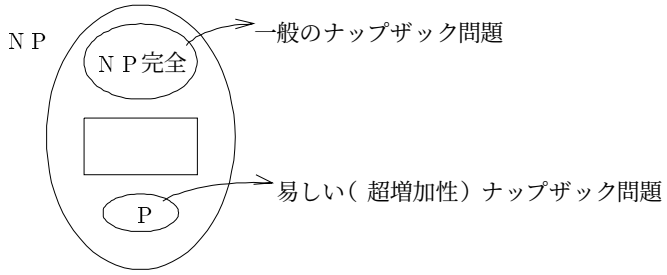

図 1 問題の複雑度のクラスとその関係

初めに、一般のナップザック問題を暗号に応用する場合を扱う。暗号ベクトルを A、平文ベクトルを Mとし、一例として

$$\begin{aligned} A &= (1,2,3,4,5,6) \\ M &= (m_1,m_2,m_3,m_4,m_5,m_6) \quad , \ m_i = \{0,1\} \ (1 \leq i \leq 6) \end{aligned} \tag{1}$$

の場合を考える。暗号文 Cをベクトル A と Mの内積

$$C = A \cdot M \tag{2}$$

で定め、$C = 6$ の場合を考えると、とり得る平文ベクトルは

$$\begin{aligned} M_1 &= (000001) \\ M_2 &= (100010) \\ M_3 &= (010100) \\ M_4 &= (111000) \end{aligned} \tag{3}$$

の 4 つとなる。つまり、この場合には一つの暗号文 Cに 4 つの平文ベクトル Mが対応しており、一意に復号することはできない。図 2 に平文ベクトルと暗号文の対応関係を示す。

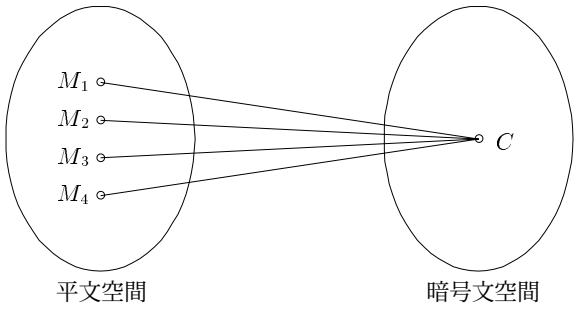

図 2 平文ベクトルと暗号文との関係

一方、式 (1) の暗号ベクトル A と式 (2) の暗号文 Cから行列 (例えば Lagarias-Odlyzko 行列) を構成し、それに LLL アルゴリズム (格子基底縮小アルゴリズム) を適用すると、何らかの平文ベクトルが出力される。LLL アルゴリズムは、暗号文 $C = \sum_{i=1}^{n} a_i m_i$が与えられたときに、暗号文のノルム $\|C\| = \sqrt{\sum_{i=1}^{n} (a_i m_i)^2}$が小さくなる平文ベクトル $M = (m_1, m_2, \cdots, m_n)$ を出力するアルゴリズムである。例えば式 (3) の 4 つの平文ベクトルに対する暗号文の値はいずれも $C = 6$ で一定であるが、ノルムは各々異なり

$$\begin{aligned} \|C_1\| &= \sqrt{6^2} = \sqrt{36} \\ \|C_2\| &= \sqrt{1^2 + 5^2} = \sqrt{26} \\ \|C_3\| &= \sqrt{2^2 + 4^2} = \sqrt{20} \\ \|C_4\| &= \sqrt{1^2 + 2^2 + 3^2} = \sqrt{14} \end{aligned} \tag{4}$$

となる。従って、$C = 6$ の場合に LLL アルゴリズムを適用すると、ノルムの小さい C_4や C_3に対応する $M_4 = (111000)$ や $M_3 = (010100)$ 等が出力される可能性が高くなる。出力される平文ベクトルが一意に定まらない理由は、LLL アルゴリズムは 2 つの不等式を満たす平文ベクトルが生成されたときに、その平文ベクトルのノルムが最小ではなくとも、不等式を満たせば出力されるためである。すなわち、不等式にある幅をもつ係数μ_{ij}と yが含まれているため、これらの値により出力される平文ベクトルも変わり、μ_{ij}を 1 に近い値に設定するほど、ノルムの小さい暗号文に対

応する平文ベクトルが出力される。ただ、暗号文 $C = \sum_{i=1}^{n} a_i m_i$の関係を満足する平文ベクトルが一つしか存在しない場合には、常に、その平文ベクトルが出力される。つまり、暗号文と平文とが 1:1 に対応しないナップザック暗号に LLL アルゴリズムを適用した場合には、必らず何らかの平文ベクトルが出力されるが、それが元の平文ベクトル (正しい解) とは限らない。

次に、超増加ベクトルを用いる易しい 0-1 ナップザック問題について考える。この場合の n 次元平文ベクトル Mの総数$\#M = 2^n$と暗号文の最大値 $C_{\max}$を比べた場合には、暗号ベクトル A の超増加性

$$a_i > \sum_{j=1}^{j-1} a_j \tag{5}$$

により

$$\#M \leq C_{\max} + 1 \tag{6}$$

となり、一つの暗号文に一つの平文ベクトルが対応する。従って、暗号文から平文ベクトルを一意に復号することができるが、$C = \sum_{i=1}^{n} a_i m_i$を満たす平文ベクトルは一つしか存在しないため、LLL アルゴリズムでほぼ 100%解読される。

従って、LLL アルゴリズムでの解読が難しいナップザック暗号を構成するためには、暗号文と平文とが 1:1 に対応しない暗号ベクトルを生成する必要がある。次に、その鍵生成手順を示す。

3　鍵生成

初めに、簡単な数値例で鍵生成法を示す。超増加性を満たさないベクトル A と超増加ベクトル Bを

$$A = (1, 2, 3, 4)\ ,\ B = (11, 22, 44, 88) \tag{7}$$

と定め、両者を併合したベクトル E と平文ベクトル Mを

$$\begin{array}{rcl} E & = & (1, 2, 3, 4, 11, 22, 44, 88) \\ M & = & (m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8) \quad ,\ m_i = \{0, 1\}\ (1 \leq i \leq 8) \end{array} \tag{8}$$

とする。ここで、超増加ベクトル Bの最初の要素 11 は、ベクトル A の各要素の総和 10 よりも大きく定める。このとき、与えられた暗号文$C = E \cdot M$から平文ベクトルの後半分の要素 $\{m_5, m_6, m_7, m_8\}$ の値は一意に定まるのに対し、前半分の要素 $\{m_1, m_2, m_3, m_4\}$ の値は一意には定まらない。従って、暗号文 Cと平文ベクトル M とは 1:1 には対応しないが、平文ベクトルの半分の要素を一意に復号することはできる。

次に式 (7) のベクトル A とベクトル B の任意の要素を一つずつ併合して、暗号ベクトル Eを生成する。例えば、

$$\begin{aligned} E &= (2, 44, 11, 4, 1, 88, 22, 3) \\ M &= (m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8) \end{aligned} \tag{9}$$

である。このとき、超増加ベクトルの要素に対応する平文ベクトルの要素 $\{m_2, m_3, m_6, m_7\}$ は一意に復号される。従って、平文ベクトルに冗長度をもたせ、

$$M = (m_1, m_1, m_2, m_2, m_3, m_3, m_4, m_4) \tag{10}$$

と定めた場合には、暗号文 $C = E \cdot M$から $M^* = (m_1, m_2, m_3, m_4)$ を一意に復号することができる。一方、この暗号文に LLL アルゴリズムを適用して解読を行なった場合、出力される平文ベクトルは、

$$M' = (m_1, m'_1, m_2, m'_2, m_3, m'_3, m_4, m'_4) \tag{11}$$

となり、すべての i について

$$m_i = m'_i \ (1 \leq i \leq 4) \tag{12}$$

となるとは限らない。つまり、$m_i = m'_i$となる出力されたベクトルの要素は元の正しい平文ベクトルの要素であるが、$m_i \neq m'_i$となる場合には、m_iと m'_i のどちらの値が元の正しい平文ベクトルの要素であるかを正しく判定できる確率は $1/2$ となる。従って、要素数 i を増やすことにより、計算量的に LLL アルゴリズムでの解読が困難なナップザック暗号を構成することができる。

次に式 (7) のベクトル A と Bの任意の要素を 2 つずつ組合せて、各々、行列 A と Bを作る。例えば、

$$A = \begin{bmatrix} 1 & 4 \\ 3 & 2 \end{bmatrix}, \ B = \begin{bmatrix} 11 & 33 \\ 22 & 44 \end{bmatrix} \tag{13}$$

である。これらを併合したものが暗号行列 Eであり、例えば

$$E = \begin{bmatrix} 1 & 33 & 11 & 4 \\ 3 & 44 & 22 & 2 \end{bmatrix} \tag{14}$$

である。暗号化を行なう場合には、暗号行列 Eの各列ベクトルの上、下いずれかの要素を選択 (暗号鍵選択) して、平文ベクトルとの内積を計算する。この場合にも計算量的に LLL アルゴリズムでの解読が困難なナップザック暗号を構成することができる。一般的な鍵生成手順と暗号化、復号化については文献 [7] を参照して下さい。

4　安全性の検討

本文におけるナップザック暗号は暗号鍵の選択肢と雑音のある暗号方式であるが、一般には、暗号鍵の選択肢が有るか無いか、雑音が有るか無いかにより 4 通りの場合が考えられる。これらの各場合について、公開されている暗号ベクトルの各要素と送られてくる暗号文を用いて Lagarias-Odlyzko 行列を構成し、LLL アルゴリズムを用いて求めた解読率を表 1 に示す。表 1 はベクトルの次元 n が $n = 4, 5, 6$ の場合であり、いずれの場合も平文ベクトルの各要素 m_i のとり得る値が 0 から 5 までのいずれかである 5 倍超増加な場合について、平文ベクトルを $(0\ 0\ \cdots\ 0)$ から $(5\ 5\ \cdots\ 5)$ まで変化させた全部で 6^n 通りの平文に対して、解読された平文の個数を求め、全平文数に対する比を表わしたものである。なお、暗号鍵の選択肢がある場合の上下の選択はランダムに行っている。次に、平文ベクトルの各要素 m_i の値が 0 か 1 のいずれかである場合について、次元 n に対する本暗号方式の解読率を求め、その変化の様子を表 2 に示す。

表 1,2 から分かるように、暗号鍵の選択肢と雑音が有る場合のナップザック暗号の解読率はベクトルの次元 n が大きくなるにつれて減少し、安全性は高まる。これは、雑音として扱う超増加ではないベクトルの要素と暗号鍵の選択肢があるために、解ベクトルよりもノルムの短いベクトルとなる平文ベクトルと暗号ベクトルの組合せが増えるためである。このことは、また、超増加ではないベクトルの要素が加わるために暗号ベクトルの密度が高くなり、それにつれて解読率が低くなることを意味している。

本文では、暗号行列 E の要素の最大値を $e_{\max}$ とするとき、 n 次元 0-1 ナップザック暗号の暗号ベクトルの密度 d を

$$d = \frac{4n}{\log_2 e_{\max}} \tag{15}$$

で定めている。一方、5 倍超増加な場合の暗号ベクトルの密度 d は、式 (15) の分母の対数の底を 2 から 6 に変更することで同様に求めることができる。

5　むすび

NP 完全問題と P 問題の間に位置すると思われる計算量のナップザック問題を暗号に応用し、LLL アルゴリズムでの解読が難しいナップザック暗号を構成できることを示した。超増加ベクトルと超増加ではないベクトルの要素を一つずつ併合して暗号ベクトルを生成した場合、超増加ではないベクトルの要素に対応する平文ベクトルの要素は、一つの暗号文 Cに対して一意に定まらないため、LLL アルゴリズムでの解読は困難になる。一方、平文ベクトルに冗長度をもたせ、各

表 1: 各暗号方式の解読率

暗号方式	解読率 (%)		
	$n = 4$	$n = 5$	$n = 6$
(i) 選択肢無し 雑音無し (従来のナップザック暗号)	$\frac{1296}{1296} \times 100 = 100$	$\frac{7776}{7776} \times 100 = 100$	$\frac{46656}{46656} \times 100 = 100$
(ii) 選択肢有り 雑音無し	$\frac{1161}{1296} \times 100 = 89.6$	$\frac{5125}{7776} \times 100 = 65.9$	$\frac{23099}{46656} \times 100 = 49.5$
(iii) 選択肢無し 雑音有り	$\frac{423}{1296} \times 100 = 32.6$	$\frac{771}{7776} \times 100 = 9.92$	$\frac{967}{46656} \times 100 = 2.07$
(iv) 選択肢有り 雑音有り (本暗号方式)	$\frac{15}{1296} \times 100 = 1.16$	$\frac{4}{7776} \times 100 = 0.051$	$\frac{2}{46656} \times 100 = 0.0042$

表 2: 提案するナップザック暗号の解読率と暗号ベクトルの密度

次元 n	解読率 (%)	暗号ベクトルの密度 d
4	$\frac{4}{16} \times 100 = 25.0$	$\frac{16}{\log_2 1404} = 1.53$
5	$\frac{7}{32} \times 100 = 21.9$	$\frac{20}{\log_2 5994} = 1.59$
6	$\frac{14}{64} \times 100 = 21.9$	$\frac{24}{\log_2 24786} = 1.64$
7	$\frac{4}{128} \times 100 = 3.13$	$\frac{28}{\log_2 96228} = 1.69$
8	$\frac{6}{256} \times 100 = 2.34$	$\frac{32}{\log_2 363042} = 1.73$
9	$\frac{8}{512} \times 100 = 1.56$	$\frac{36}{\log_2 1351566} = 1.77$
10	$\frac{7}{1024} \times 100 = 0.68$	$\frac{40}{\log_2 4881348} = 1.80$
11	$\frac{3}{2048} \times 100 = 0.14$	$\frac{44}{\log_2 17360406} = 1.83$
12	$\frac{15}{4096} \times 100 = 0.36$	$\frac{48}{\log_2 60938568} = 1.86$
13	$\frac{23}{8192} \times 100 = 0.28$	$\frac{52}{\log_2 211513518} = 1.88$

要素を 2 度ずつ送ることにより、超増加ベクトルを用いて一意に復号することができる。

本暗号は高速に暗号化と復号化を行なうことができる利点をもつが、暗号鍵の数が多く、伝送効率は従来のものよりも低下する難点をもつ。

謝辞　本研究に御協力を頂いた本学大学院生市川通君と中村大介君に感謝します。

参考文献

[1] R.C.Merkle and M.E.Hellman , “Hiding Information and Signatures in Trapdoor Knapsacks, ” IEEE Trans. Inf. Theory , vol.IT-24 , no.5 , pp.525-530 , Sept.1978.

[2] A.K.Lenstra, H.W.Lenstra, Jr. , and L.Lovasz , “Factoring Polynomials with Rational Coeff icients,” Math. Ann. , vol.261 , no.4 , pp.515-534 , 1982.

[3] J.C.Lagarias and A.M.Odlyzko , “Solving Low Density Subset Sum Problem,” Proc. 24th IEEE Symp. Found. Comput. Sci. , pp.1-10 , 1983.

[4] 池野信一，小山謙二 , 現代暗号理論 ,pp. 136-174 , 電子情報通信学会 , 1986.

[5] 岡本栄司 , 暗号理論入門 , pp.102-103 , 共立出版 , 1993.

[6] 清水秀夫 , “格子基底の縮小による LL 型暗号の解読に関する研究,” 金沢工業大学博士学位論文 , 1994.

[7] 小林邦勝 , 木村真樹 , “ナップザック暗号の安全性向上に関する一考察,” 信学論 (A) , vol.J79-A , no.8 , pp.1339-1343 24z, Aug.1995.