L-041

超増加性を持たない非線形ナップザック暗号

Nonlinear Knapsack Cryptosystems without Super-increase Structure

宇田 浩司† 桐山 明人‡ 岩崎 彰典†† 仲川 勇二‡‡
Koji UDA, Akihito KIRIYAMA, Akinori IWASAKI, and Yuji NAKAGAWA

1．まえがき

Merkle と Hellman によって提唱された 0−1 ナップザック暗号(MH 暗号)は特殊な 0−1 ナップザック問題である部分和問題に基づいた公開鍵暗号である．部分和問題は NP 困難な問題であるが，秘密鍵として超増加数列を用いて，一意かつ容易な復号を可能にしている．公開鍵は秘密鍵にモジュラー乗算を行い，見かけ上解くことが困難な問題にしている．Shamir は公開鍵から超増加数列を導き MH 暗号を解読した．Lagarias と Odlyzko は LLL アルゴリズム(以下 LLL と略記)を用いた低密度攻撃によって MH 暗号が解読できることを示した．MH 暗号に冗長性を持たせ，鍵数列の密度を高める研究が小林ら[1]によってなされている．

一方で，ナップザック暗号は，最近の組合せ最適化問題の解法の進歩にも注意しなくてはならない．仲川ら[2]は改良代理制約法(ISC)を開発した．この方法は不等号制約条件を持つ非線形ナップザック問題を解くために開発されたものであり，部分和問題を解く能力は未知数であるが，これらの最適化技法への耐性も調べておく必要がある．

本発表では，非線形ナップザック暗号の LLL 及び ISC への耐性を調べた結果を報告する．

2．暗号化の手順

(1)暗号に用いる非線形ナップザック問題の定式化

まず，$(n\times k)$ 個の要素を持つ行列 B を考える．

$$B\equiv\left[b_{ij}\right],\quad (i=1,2,\ldots,n,\ j=1,2,\ldots,k)$$

の行を変数，列を各変数の取る案と考え，i 番目の変数に対し k_i 番目の案のみを取ることにする．このとき，非線形ナップザック問題を，B とある整数 c が与えられたとき，

$$c=\sum_{i=1}^{n}b_{ik_i}$$

を満たす k_i の組合せを求める問題と定式化する．

(2)鍵の生成

n 文字をブロックとする暗号系を考える．$l\geq 2$ 個の 1 から次の関係を満たすビットマスク列 $s_i,(i=1,2,\ldots n)$ を作る．

$$s_1\,\&\,s_2\,\&\cdots\&\,s_n=0$$
$$s_1\oplus s_2\oplus\cdots\oplus s_n=1$$

但し，&，⊕ はそれぞれビットマスク列の論理積，論理和を表す．必要な，ビットマスク列のビット数は $l\times n$ となる．この条件は復号化の際，一意に復号するために必要である．例を $n=3,l=3$ の場合で示す．

$$s_1=(001110000)=112$$
$$s_2=(010001100)=140$$
$$s_3=(100000011)=259$$

次に各ビットマスクの 1 をビット位置が重複しないようランダムに $(l-m)$ 個だけ 0 に変える．但し $l-2\geq m\geq 1$ とする．これは後で述べるモジュラー乗算のパラメータを逆算されないためである．これにより各ビットマスク s_i から 2^{l-m} 個の案 $a_{ij},(j=1,2,\ldots,2^{l-m})$ を作ることができる．s_1 から生成される案の例を示す．

$$a_{11}=(001000000)=64$$
$$a_{12}=(001010000)=80$$
$$a_{13}=(001100000)=96$$
$$a_{14}=(001110000)=112$$

他のビットマスク列に対し同様の操作を行い，これを秘密鍵 A とする．先のビットマスクから作られた例を 10 進数で示す．

$$A=\begin{bmatrix}64 & 80 & 96 & 112\\ 8 & 136 & 140 & 12\\ 259 & 1 & 3 & 257\end{bmatrix}$$

ここで，ビットマスク列 s_i は超増加性を持つが，ビットマスクから生成された案の要素列は超増加性を持たないことに注意されたい．

A に次のモジュラー乗算を行い，公開鍵 B とする．

$$B=A\times w \bmod p$$

但し，$p>2^{l-m}-1$ とし，w と p は互いに素とする．

(3)暗号化

平文を $e_i,\left(1\leq e_i\leq 2^{l-m},i=1,2,\ldots,n\right)$ とすれば，暗号 c は，公開鍵 B の要素を b_{ij} として，

$$c=\sum_{i=1}^{n}b_{ie_i}$$

† 岡山理科大学大学院工学研究科
‡ 株式会社フロムソフトウェア
†† 岡山理科大学情報処理センター
‡‡ 関西大学総合情報学部

となる．公開鍵 B と暗号 c から平文の組合せを求めることは非線形ナップザック問題を解くことと等価であり NP 困難である．c を暗号文として受信者に送信する．

(4)復号

復号には $w\times w^{-1} \bmod p = 1$ なる w^{-1} を用いて，

$$c' = c\times w^{-1} \bmod p$$

を求める．

c' とビットマスク s_i の論理積を e'_i とする．

$$e_i' = c'\&s_i, \quad (i = 1,2,\ldots,n)$$

e' と秘密鍵 A の要素を比較し，

$$e_i' = a_{ik_i}, \quad (i = 1,2,\ldots,n)$$

となる k_i を求めることにより復号することができる．

3．非線形ナップザック暗号の密度

非線形ナップザック暗号の公開鍵行列の行要素数は 2^{l-m} 個となるので，暗号化するブロックの文字数を n とすれば公開鍵行列の要素数は $n\cdot 2^{l-m}$ 個となる．従って，LLL の対象となる暗号ベクトルの要素数は $n\cdot 2^{l-m}$ 個となるので，この暗号ベクトルの密度 d は，

$$d = \frac{n\cdot 2^{l-m}}{\log_2 \max(b_{ij})}$$

である．

公開鍵からモジュラー乗数のパラメータ p を逆算されないためには，m が大きくなければならないが，$l \approx m$ では LLL により，$l >> m$ では ISC により解読される可能性がある．

計算機実験では，$m = 1$ とし，n と l を変化させて LLL と ISC に対する暗号の耐性を調べた．

4．LLL と ISC に対する耐性

実際に暗号化の手順から作成した公開鍵に対して LLL と ISC による解読を行った．表 1 に LLL による解読率を示す．表 1 から文字数 n とビットマスクの 1 の数 l の増加により，暗号の解読率は飛躍的に下がることがわかる．次に 1 の数 l を 6 に，文字数 n を 6，8 とし，b_{ij} を変えて d を変化させた実験を行った．実験結果を図 1，2 に示す．図中の▲が LLL，■が ISC による解読率を表す．縦の実線は本実験での非線形ナップザック暗号の密度である．

図 1 の結果では，暗号の解読率が LLL より ISC の方が解読率に優れている．しかし，図 2 から ISC では解読されず，LLL にも耐性を持つ密度の範囲があることがわかる．

5．まとめ

今回提案した方式は非線形問題を最も単純な形で暗号化に利用したもので，「荷物を入れるか入れないか」によって暗号化していたこれまでのナップザック暗号系に対して，「どの荷物を入れるか」で暗号化を行うという新しい方法の有効性を示した．秘密鍵から公開鍵への変換方法や関数の値の決定方法などについては，さらに検討する余地もあると思われ，それらの研究を進めていくことで非線形離散最適化問題を応用した，安全性の高い暗号技術の研究が発展していくことが期待される．

表 1　LLL による解読率（m=1）

l=	4	5	6
d=	2	3.2	5.3
n=4	5.430E-01	8.935E-02	3.964E-03
n=5	3.130E-01	1.936E-02	2.046E-04
n=6	1.630E-01	3.644E-03	1.975E-05
n=7	8.825E-02	5.135E-04	2.000E-06
n=8	3.190E-02	9.440E-05	<1.000E-07

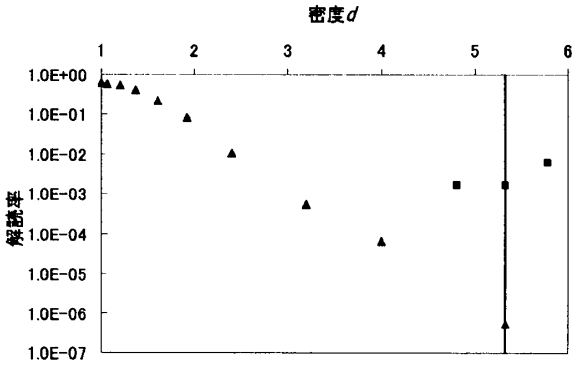

図 1　密度と LLL，ISC による解読率（l=6, n=6）

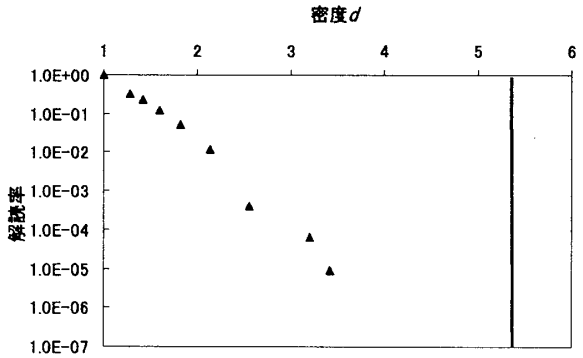

図 2　密度と LLL，ISC による解読率（l=6, n=8）

文献

[1]小林邦勝，“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，August. 1996.

[2]Y. Nakagawa, “An improved surrogate constraints method for separable nonlinear integer programming,” J. Oper. Res. Soc. Jpn., vol.46, no2, pp.145-163, June. 2003.