暗号鍵を選択するナップザック暗号の安全性の検討

2L－1

服部 博光
龍谷大学大学院理工学研究科電子情報学専攻

1．はじめに

ナップザック暗号に対し効果的な解読方法として、LLLアルゴリズム[2]を用いたものが知られている。暗号鍵を選択するナップザック暗号[1]は、このLLLアルゴリズムを用いた解読方法に強いとして提案された方式であるが、その他の解読方法については十分検討がなされていない。そこで、基本的なナップザック暗号であるMH型ナップザック暗号の解読方法として知られているShamirの方法[3]を、この暗号鍵を選択するナップザック暗号に対し適用することを試み、その安全性を検討した。

2．暗号鍵を選択するナップザック暗号

従来のナップザック暗号は格子基底縮小アルゴリズム（ＬＬＬアルゴリズム）を適用することにより、ほとんどすべて解読されていた。そこで、ＬＬＬアルゴリズムを用いた解読である、Lagarias-Odlyzkoの方法に対し解読が困難な「暗号鍵を選択するナップザック暗号」[1]が提案されている。この暗号は暗号鍵に選択肢をもたせ、暗号化の際に正しい受信者のみが取り除くことのできる雑音を乗せるものであり、その安全性は暗号鍵を正しく推定する複雑さと雑音を除去する複雑さに根拠を置いている。公開鍵E（m行2n列の行列）はk（正整数）倍超増加の行列である秘密鍵B（m行n列）と雑音行列A（m行n列）から乗数w（正整数）と法p（正整数）をもとに計算されたものである。このwとpを秘密の落し戸といい、pに対するwの逆数w^{-1}を用いるとEからBを求めることが可能である。

変形 Lagarias-Odlizko 行列を用いてこの暗号を解読する試み[1]では、解読に成功する確率が低いことが示されている。なぜなら、鍵の選択ということと雑音の除去が困難だからである。

以下にこの鍵の生成方法を説明する。

$$0<a_i<a_{i+1}(1\leqq i\leqq 2n-1),\ a_i<\sum_{j=1}^{i-1} a_j \quad (3\leqq i\leqq 2n)$$

を満たす要素a_iを適当に組み合わせて、2行n列のベクトル$A=\begin{bmatrix} a_{11}a_{12}\ldots a_{1n} \\ a_{21}a_{22}\ldots a_{2n}\end{bmatrix}$を生成する。また、

$a_{mi}=\max\{a_{1i},a_{2i}\}$ $(1\leqq i\leqq n)$とし、

$A_m=\sum_{i=1}^{n} a_{mi}$とする。

$$b_1>kA_m \qquad b_2>k(A_m+b_1) \qquad (1)$$

$$b_{2i-1}>k\left(A_m+\sum_{j=1}^{i-1} b_{2j}\right) \quad (2\leqq i\leqq n) \qquad (2)$$

$$b_{2i}>k\left(A_m+\sum_{j=1}^{i-1} b_{2j}+b_{2i-1}\right) \quad (2\leqq i\leqq n) \qquad (3)$$

を満足する要素b_iを用い、2行n列の行列

$B_1=\begin{bmatrix} b_1b_3\ldots a_{2n-1} \\ b_2b_4\ldots a_{2n}\end{bmatrix}$を作成する(k倍超増加のベクトル)。この列ベクトルに対し、適当な入れ替えを行い$B_2=\begin{bmatrix} b_{11}b_{12}\ldots a_{1n} \\ b_{21}b_{22}\ldots a_{2n}\end{bmatrix}$とする。

"An analysis of a knapsack cryptosystem choosing encryption keys"
Hiromitsu Hattori
The Graduate School of Science and Technology of Ryukoku University

さらに、以下を満足する法 p を作成する。

$$p>k\,(A_m+\sum_{i=1}^{n} b_{2i})$$

p と互いに素な正整数 w を用い、A と B_2 をモジュラー変換し、以下のように示す。

$$A^*=wA \bmod p\equiv\begin{bmatrix} a_{11}^* a_{12}^* \ldots a_{1n}^* \\ a_{21}^* a_{22}^* \ldots a_{2n}^* \end{bmatrix}$$

$$B^*=wA \bmod p\equiv\begin{bmatrix} b_{11}^* b_{12}^* \ldots a_{1n}^* \\ b_{21}^* b_{22}^* \ldots a_{2n}^* \end{bmatrix}$$

この、２つの行列を対応する列ベクトルで併合したものをベクトル E とし、これを公開鍵とする。このとき、各列ベクトルについてどちらが前に来るかは、任意とする。例えば、以下のようになる。

$$E=\begin{bmatrix} a_{11}^* b_{11}^* b_{12}^* a_{12}^* \ldots a_{1n}^* b_{1n}^* \\ a_{21}^* b_{21}^* b_{22}^* a_{22}^* \ldots a_{2n}^* b_{2n}^* \end{bmatrix}$$

3．Shamir の解読法の適用

Shamir の解読法は、秘密鍵が超増加の条件を満たすという性質を利用したものである。なお、この方法で求められる落し戸と暗号鍵は元のものと同じでなくても、その性質は保存しているのでかまわない。暗号鍵を選択するナップザック暗号にも、その秘密鍵が k 倍超増加であるという性質をもっているので、その適用が可能である。

この方法では、乗数と法のセットを有理数として、それが超増加と法の条件を満たす範囲に存在する値を見つけることにより、落し戸を見つける。この条件を暗号鍵を選択するナップザック暗号での鍵の生成条件(1)(2)(3)を満たすように変更し解読を行うことにより、この暗号へ適用することを試みた。

また、与えられた公開鍵から暗号鍵に対応する要素を正しく選ぶ必要があるが、解読に必要とされる要素数は n に比べ少なくてよい。よって、鍵の選択の組み合わせ全てを判定することは容易であるので、全てについて判定を行い、適切な結果を返した選択を使用することとした。

実際、[1]で示されている例（n=4,m=2 つまり公開鍵は 2 行 8 列である）についても、二つの鍵のセットの組み合わせ、つまり正しい鍵 2 列×雑音 2 列の 4 通りについて判定するだけで正しく解読できた。そこで、LLL アルゴリズムを用いた解読方法と Shamir の解読法について解読率を調べ、比較を行った。

4．まとめ

暗号鍵を選択するナップザック暗号は、たしかに LLL アルゴリズムに対しては安全性の高い方法ではあるが、その k 倍超増加の秘密鍵をもつという性質上、Shamir の解読法には弱いといえる。しかし、落し戸から暗号鍵を割り出したとしても、雑音の影響でそれが正しい鍵のセットから得られたかどうかを判断するのが難しい場合もある。この暗号方式の安全性の向上のために雑音をいかに工夫するかが今後の課題である。

参考文献

[1] 小林,木村,菅野,田中:"暗号鍵を選択するナップザック暗号" 信学技報,ISEC95-9,July 1995.

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

[3] E.F.Brickell and G.J.Simmons : "A status report on knapsack based public key cryptosystems", Sandia Report SAND 83-0042 (Feb. 1983), and CONGRESSUS NUMERANTIUM,37,Winnipeg, Canada (June 1983) .