部分和問題に基づく暗号方式について

淺井 輝　　指導教員：田坂 浩二

1 序文

本研究では部分和問題に基づく暗号方式の安全性の検証を行う。ここで、部分和問題を以下のように定義する。

部分和問題

$V = \{v_1, v_2, \ldots, v_k\} \subset \mathbb{N}$ と自然数 N が与えられたときに、$\sum_{i \in I} v_i = N$ をみたす $\{1, \ldots, k\}$ の部分集合 I を探す問題である。

これは NP 完全問題に分類される問題であることが知られている [1]。任意の部分和問題を多項式時間で解くアルゴリズムは知られていない。現在使用されている暗号技術の多くは、量子コンピュータが暗号解読に利用された時に破られてしまう危険性がある。部分和問題を利用した暗号方式は、量子コンピュータの出現に対抗しうることから現在も研究されている。本研究では、林 [2] により提唱された暗号方式に着目し、その安全性を論じる。

2 林 [2] の暗号方式

林の暗号方式はナップザック暗号 [3] を改良したものである。ナップザック暗号とは部分和問題を利用した暗号で初期に多く実用されていた方式である。しかし、LO 法 [4]、Shamir の攻撃法 [5] などの強力な解読法が知られたため現在では実用されていない。そこで LO 法への耐性を持たせるために考案された方式が林の暗号方式である。その仕組みを以下に簡単に記述する。

2 つの自然数 $n, h(\leq n)$ を定める。n は平文のビット数である。$h = 1$ の時ナップザック暗号と等しくなることに注意する。ベクトル $b = (b_1, \cdots, b_n) \in \mathbb{Z}^n$ は次の不等式を満たすものとする。

$$b_{i+1} > \sum_{j=0}^{j1} b_{i-jh}, \quad i = 1, \cdots, n-1, \quad j1 = \lfloor (i-1)/h \rfloor.$$

法 M を h 個ごとにとった b の要素の総和より大きい整数とする。

$$M > b_n + b_{n-h} + b_{n-2h} + \cdots + b_h$$

また M と互いに素な整数 $\omega, 1 < \omega < M$ 及び ω の法 M に関する逆元 $\omega^{-1}, 1 < \omega^{-1} < M, \omega\omega^{-1} \equiv 1 (mod\, M)$ を定める。以上で定めた $b, M, \omega, \omega^{-1}$ を秘密鍵とする。

$$a_i = \omega b_i \bmod M, \quad i = 1, \cdots, n.$$

以上の様に定めた a と h を公開鍵とする。

暗号化のアルゴリズムは以下である。

暗号化

$C_1 = \cdots = C_h = 0, j = 1$
for $i = n$ downto $1\{$
  if $m_i = 1$
    then $\{C_j = C_j + a_i, \quad j = j \bmod h + 1\}$
$\}$

復号化のアルゴリズムは以下である。

復号化

$C'_j \leftarrow \omega^{-1} C_j \bmod M$, $j = 1, \cdots, h$, $x \leftarrow 0^n$
$j = 1$ for $i = n$ downto $1\{$
  if $C'_j \geq b_i$
    then $\{x_i = 1, \quad C'_j = C'_j - b_i, \quad j = j \bmod h + 1\}$
$\}$

3 林の暗号方式の安全性

林は、$h = 3, n \geq 50$ で LO 法は解読できないことを予想した。本研究では他の h に対しても解読率の調査を行った。結果は以下である。ただし、解読率は以下のようにする。各 n, h に対し、まず、条件を満たす秘密鍵を 100 本生成する。次に、各秘密鍵ごとにランダムに暗号文を 100 個生成し、LO 法で復号できる暗号文の割合を求める。求めた割合の平均値を解読率とした。

表 1　解読率の平均

n	h=1	h=2	h=3	h=4	h=5
10	94.69%	77.58%	68.50%	58.96%	55.64%
20	51.15%	15.62%	7.18%	3.89%	2.95%

各 n に対して h が大きくなればなるほど解読率が低くなることが確認できる。

4 今後の課題

暗号化、復号化に時間がかかることなど、h が大きくなることで現れるデメリットについての検証。n >20 についての実験を行う環境がなかったため、n >20 についての実験を行う必要がある。データの取り方が平均値だけでは効果的な見方になっていないため、様々な使い方をする必要がある。

参考文献

[1] N. コブリッツ著、桜井幸一訳 『数論アルゴリズムと楕円暗号理論入門』シュプリンガー・ジャパン，1997
[2] 林彬, 新しい高密度ナップザック暗号,Vol.2009-CSEC-47 No.6,2009/12/18
[3] R.C.Merkle and M.E.Hellman,"Hiding information and signatures in trapdoor knapsacks",IEEE Trans.Inform.Theory,vol.IT-24,no.5,pp.525-530,1978.
[4] J. C. Lagarias and A. M. Odlyzko, "Solving low density sum problems",J.ACM,vol.32, pp.229-246, 1985.
[5] A.Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellmancryptosystems", IEEE Trans. Inform. Theory, vol. IT-30, no. 5, pp.699-704,1984.