計測自動制御学会東北支部 第181回研究集会 (1999.5.21)
資料番号 181-2

カオスニューラルネットワークを用いた暗号化の一方式

Chaos Neural Network Based Encrypotion System

○川村　暁*，吉田　等明**，高橋友樹*，恒川佳隆***，三浦　守*

○Satoshi Kawamura*, Hitoaki Yoshida**, Tomoki Takahashi*,
Yoshitaka Tsunekawa***, Mamoru Miura*

*岩手大学工学部情報工学科
**岩手大学情報処理センター
***岩手大学工学部電気電子工学科

*Department of Computer and Information Science, Faculty of Engineering, Iwate University
**Iwate University Computer Center
***Department of Electrical and Electronic Engineering, Faculty of Engineering, Iwate University

キーワード：共通鍵暗号(conventional encryption)，ニューラルネットワーク(neural network)，
カオス(chaos)，一方向性関数(one way function)，ハッシュ関数(hush function)

連絡先：〒020-8551 岩手県盛岡市上田4-3-5　岩手大学 工学部 情報工学科 三浦研究室
川村　暁，E-mail:kawamura@cis.iwate-u.ac.jp

1. はじめに

インターネットに代表されるオープンなネットワークの利用が，情報社会の一つの象徴になりつつある[17,18]．このような動きは1960年代終わりからの，コンピュータを通信回線(ネットワーク)と結合して利用しようとした流れの発展形態として捉えられる．

オープンなネットワークを用いる場合，もっとも配慮しなければならないのはデジタル化された情報をいかに保護するかという技術・方法である．このような技術・方法は情報セキュリティ技術といわれるが，この中でもデータ秘匿の手段としての暗号とその応用が重要な要素技術である．

現代の暗号理論は，1970年のDESに代表される共通鍵暗号方式や，1976年のDiffe-Hellmanによる公開鍵暗号による共通鍵の配送法の発明以来，急速に進展している．

本研究では，従来暗号の基礎理論として用いられてきた組み合わせ論や整数論の問題に基づいた方式(素因数分解や離散対数問題)とは異なる，特異なカオス力学系であるカオス・ニューラルネットワークを用いた共通鍵暗号の一方式を提案し，その特徴を明

らかにすることを目的とする.

2. カオス・ニューラルネットワーク

当研究室では，通常のニューロンよりなるニューラルネットワーク[30~38]の振動現象に関して，構造論的立場から研究を行っている[1~7].

次節では，本研究で用いたニューロンモデルとカオス・ニューラルネットワークモデル[5~7]を示す.

2.1 ニューロンモデル

Fig.2.1にニューロンモデルを示す．本モデルでは，自己再帰結合は用いていない．非線形関数としては，バックプロパケーションモデルやホップフィールドモデルなどで広く用いられている，sigmoid関数を用いて研究を行った(式1).

$$f(u_m) = \frac{1}{1+\exp(-u_m/\lambda)} \quad \cdots\cdots(1)$$

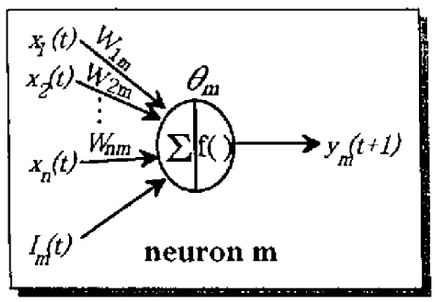

Fig.2.1 Neuron Model

2.2 ネットワークモデルとその挙動

自然界では単一で振動する出力を発生する例もある[32,39]が，今回用いた人工ニューロンの場合には，1個のニューロンのみでは振動しない．Fig. 2.2に，最も基本的な振動するネットワークをしめす.

この系は，重み係数の正負によってその振る舞いが変化すると考えられる．よって，重み係数の正負により，基本NNを以下のように分類する． 興奮性(Excitatory)結合のみの場合をType-E，抑制性(Inhibitory)結合のみの場合をType-I，興奮性 抑制性の両結合(Hybrid)がある場合をType-Hと呼ぶことにする(Table.2.1)．尚，$W_{12}<0$,$W_{21}>0$ の場合

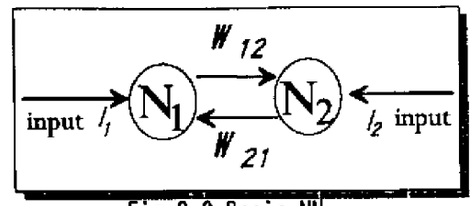

Fig. 2. 2 Basic NN

NN Type	Weight	
	W_{12}	W_{21}
Type-E	>0	>0
Type-H	>0	<0
Type-I	<0	<0

Table.2.1 Variation of Basic NN

も考えられるが，Type-H と等価である.

我々は，基本ネットワークは，いずれのTypeにおいても，その出力は収束するか振動するかであり，その振動周期も最大で4周期であることを明らかにしている[7]. Fig.2.3に収束した場合，Fig.2.4に振動した場合の入出力特性図を示す.

次に，この基本ネットワークを含む，ニューロン数がn個のネットワークへの拡張を考

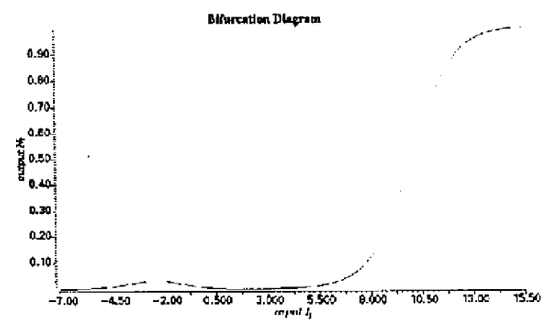

Fig.2.3 入出力特性図　系は収束

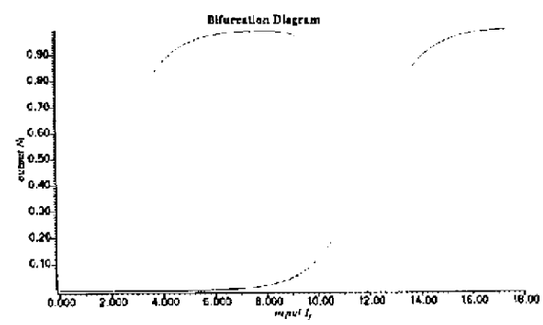

Fig.2.4 入出力特性図　系は振動

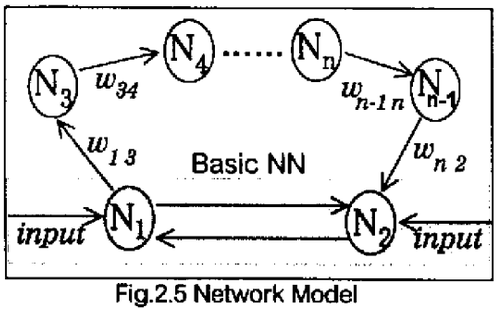

Fig.2.5 Network Model

える.

Fig.2.5に，基本ネットワークを含むnニューロンネットワークの構成を示す．このネットワークは，以下の各要素により特徴づけられる.

・基本ネットワークの種類
・ニューロン数
・ニューロン間の重み係数の符号

当研究室では，この構成のネットワークにおいて，カオス応答するネットワークが存在することを示し，そのようなネットワークをカオス・ニューラルネットワークと呼んでいる　.

Fig2.5 の構成で，カオス応答する場合があることを報告しているが，その一例としてニューロン数が 3 個の場合を示す.

Fig.2.6 に入出力特性図を，Fig.2.7 にリアプノフ指数を，Fig.2.8～Fig.2.11 に外部入力値-0.18794 でのポアンカレ切断面を示す.

入出力特性図で，点の構成密度が高い部分が見られる．この部分について考える．Fig.2.7 より，Liapnov指数の最大値は約0.05 (外部入力値 -0.188 近傍) である．ここでのポアンカレ切断面は折り畳み構造が見られ，

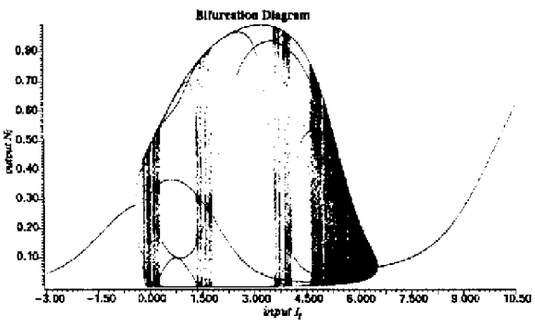

Fig.2.6 入出力特性図

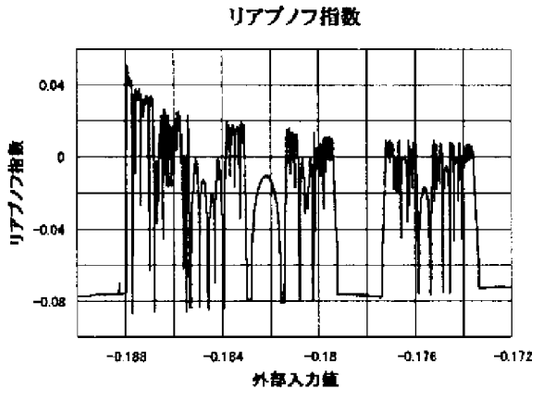

Fig.2.7 リアプノフ指数

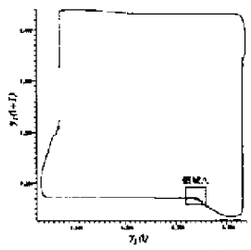
Fig.2.8 ポアンカレ切断面

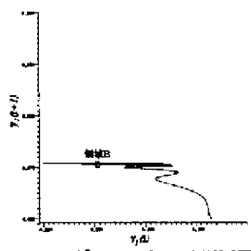
Fig.2.9 ポアンカレ切断面 Fig.2.8の拡大図

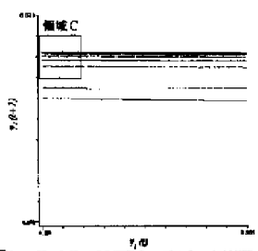

Fig.2.10 ポアンカレ切断面 Fig.2.9の拡大図

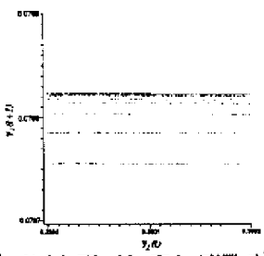
Fig.2.11 ポアンカレ切断面 Fig.2.10の拡大図

また，自己相似 (フラクタル) 的な構造であることがわかる．よって，このネットワークはカオス応答しているといえる.

本提案では，このカオス・ニューラルネットワークを用いる.

3. カオス・ニューラルネットワークの信号特性

本節では，カオス・ニューラルネットワークのニューロンの出力値の特性について考える．ある信号を疑似乱数や暗号に用いる場合，その信号がどのような特性を有しているかを知ることは応用上も非常に重要である.

本節では，カオス・ニューラルネットワー

クの信号特性について考察を加える.

3.1 カオス・ニューラルネットワークのカオス

カオスとは，決定論的システムが複雑な振る舞いをする現象である[19~28]. 系 f がカオスであるとき，以下の性質のうちいずれかを満足する[22].

i). f は最終的不動点でない定義域内のすべての点で，正のリアプノフ指数を持つ.

ii). f は定義域内で初期値鋭敏性を持つ.

本提案で用いるカオス・ニューラルネットワークの出力値について考える.

Fig.2.7で示したように，(ニューロン１の出力値に関する) リアプノフ指数が正の値をとる領域が存在する. リアプノフ指数とは，カオスの特徴である軌道不安定性の評価指標である. この値が正であるとき，微少に異なる二つの軌道 α と $\alpha+\varepsilon$ ($\varepsilon \ll 0$) の距離が時間とともに指数関数的に乖離していく様子を表す (式(2)). ここで，λ はリアプノフ指数である.

$$\varepsilon(t) = \varepsilon(0)\,\varepsilon^{\lambda t} \quad \cdots\cdots\cdots\cdots(2)$$

また，リアプノフ指数は，ある点の軌道の"平均情報損失率" と考えられる. すなわち，軌道 α と $\alpha+\varepsilon$ が互いに離れていくときは，同指数は正となる. したがって，指数が正であり大きければ大きいほど，もう一つの軌道に対する情報はより多く失われるといえる.

次に，初期値鋭敏性について考察する. 初期値鋭敏性とは，初期値の僅かなずれを，それがどんなに小さなずれであっても，時間的に拡大する性質を有している (式(3)). この性質は，バタフライ効果や軌道不安定とも呼ばれる. いま任意の δ に対して，初期値 x, y が，

$$|x-y| < \delta \quad \text{かつ}$$
$$|f^{(n)}(x)-f^{(n)}(y)| > \varepsilon \quad \cdots\cdots\cdots\cdots(3)$$

の関係を満たすとする. このとき，初期点 x, y が，n回目の写像の繰り返しの後にはその距離が ε 以上となることを意味し，時間の経過とともに全く異なった軌道となる. このとき，f は初期値に鋭敏に依存するという. これは実用上も重要である. なぜなら，x の近似的な値y からスタートした軌道は，十分時間がたつとまったく異なると考えられるからである.

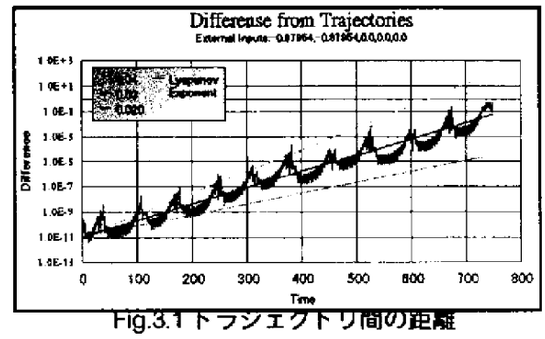

Fig.3.1 トラジェクトリ間の距離

カオス・ニューラルネットワークの，初期値鋭敏性について考察する. Fig.3.1に，トラジェクトリ間の距離の時間変化の様子を示す. これは，初期値が 1.0×10^{-11} だけ離れた軌道の，時間変化の様子である. 時間経過とともに，僅かだけ離れていた軌道が，時間経過とともにその距離を広げているのがわかる. これより，この系が初期値鋭敏性を有していることが示唆される.

これらより，本提案で用いるカオス・ニューラルネットワークも，カオスであるといえる.

3.2 カオス・ニューラルネットワークの信号の特異性

本提案で用いたカオス・ニューラルネットワークから，出力される信号の特異性について述べる.

3.2.1 出力値の特異性

我々は，カオス・ニューラルネットワークの振動発生機構と，カオス応答する場合の特徴について報告している[1~7]. ネットワーク応答がカオスである場合の必要条件は，各ニューロンに属する値（系列と呼ぶ）の「混じり合い」による.

また，カオス・ニューラルネットワークは，単一のニューロンでカオスを出力しているのではなく，系全体でカオスとなっている．そのため，単一ニューロンの出力値は，同一になる場合があると考えられる．

さらに，このカオスは，デジタルカオスである．そのため，計算機特有の打ち切り誤差や丸め誤差などが，信号の時間発展に影響してくると考えられる．さらに，演算精度自体の影響のため，非常に長い周期を持つ，特異なカオスとなっていると考えられる．

3.2.2 一方向性

カオス・ニューラルネットワークは，ネットワーク構成と外部入力値が定まれば，時系列信号を容易に取り出すことができる．この外部入力値と，ある一つのニューロンの出力値(信号)の関係について考える．

ある関数 $y=f(x)$ が一方向性関数であるとは，x より $y=f(x)$ を計算するのは容易であるが，逆に y より x を求めるのが困難な関数のことをいう[10,11]．

カオス・ニューラルネットワークの外部入力値 x と，あるニューロンの出力値（ニューロン1など）の関係は，初期値鋭敏性により，初期値（外部入力値）が微少に異なる場合，その振る舞いの時間発展が全く異なったものとなる．また，系がカオスである場合，その軌道にはエルゴート性があるため，非常に近い軌道を通る状態の間には相関がなく，出力値から外部入力値を推定するのは困難であるといえる．よって，出力値 y から外部入力値 x を求めるのは困難である．

さらに，あるニューロンの出力値に注目すると，その出力値は同一の値をとることがあると考えられる．よって，外部入力値 x と出力値 y は一対一写像ではなく，一対多写像であるといえる．よって，カオスニューラルネットワークの外部入力値 x と，あるニューロンの出力値 y の関数 $y=f(x)$ は，一方向性関数 f であるといえる．

3.2.3 ハッシュ関数

ハッシュ関数は，パスワード認証・デジタル署名・メッセージ認証などの目的で幅広く用いられ，現代暗号の重要な分野を構成している．カオス・ニューラルネットワークの出力値がこの性質を満足するか考察する．

一般的にハッシュ関数とは，ある大きな領域 D から小さな領域 R への多対一のマッピングを行う関数 h であり，

$$h : D \rightarrow R \text{ かつ } |D| > |R|$$

となる場合を考える．このとき，関数 h とその定義域のある値 x が与えられて，$h(x)=h(y)$ となるような y を求めることが難しいような関数 h のことである[10,11]．

カオス・ニューラルネットワークの遷移回数 x と，出力値 y の関数 $y=f(x)$ について考える．

(i). x を入力して $y=f(x)$ を出力する多項式時間アルゴリズムが存在する(遷移回数だけ繰り返せばよい)．

(ii). 出力 y から，$y=f(x)$ を満たす x を求めるのは困難である (f^{-1} の困難性)．

(i), (ii) より，$y=f(x)$ (遷移回数 x とニューロンの出力 y) は，一方向性ハッシュ関数である．

4. カオス・ニューラルネットワークを用いた暗号

前節では，カオス・ニューラルネットワークの信号特性について考察を加えた．本節では，この系の出力信号を暗号に用いる事を考える．

4.1 暗号方式

これまで公開されている暗号は，暗号の組立方法・鍵を公開するか否かにより，慣用暗号系と公開鍵暗号系に分類される．これらの特徴を記す[8~11]．

・慣用暗号系

従来から用いられてきた暗号形式．特徴は暗文生成に用いる鍵と復号に用いる鍵が同一の形式．この暗号系では，その安全性は鍵の秘匿性に依存している．

・公開鍵暗号系

1970年代に登場した新しい暗号手法．この方法は暗号の組立と復号に異なった鍵を使うという特徴がある．これにより，照会や認証も可能になる．

・特殊形式

暗文の組立に隠語・比喩・特殊記号を用いる形式．このため，生成された暗文が通常の文章になっており，一見しただけでは暗文とはわからないが，コンピュータ化には適さない．

慣用暗号形は，暗号化の基本構成単位をどのようなものにするかにより，サイファ方式とコード方式に分けられる．

・サイファ方式

データの成分を原字単位または綴り字を基本単位として暗号化する方式．このとき，データの文字列を一文字ずつ組み立てるものを逐次型暗号，数文字をまとめて暗号化するものをブロック暗号という．

・コード方式

綴り字・単語または成句を変換辞書によりほかの一定記号列等に置き換えた後暗号化する．この方式は単語の意味解釈が必要となり，プログラムかが難しい．

本提案では，暗号化鍵と復号鍵が同一で，一文字ずつ暗号化する逐次型慣用暗号形を構築する．

4.2 暗号化方法

本節では，カオス・ニューラルネットワークを用いた逐次型慣用暗号形の構築例を示す．Fig.4.1に，暗号化・復号の概念図を示す．

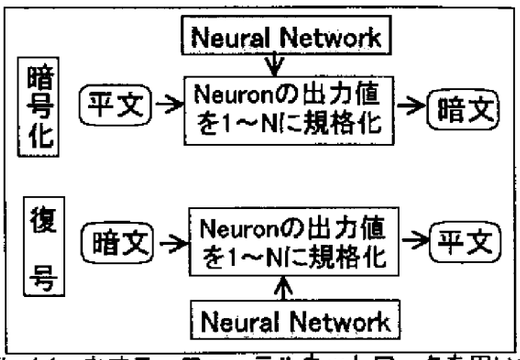

Fig.4.1 カオス・ニューラルネットワークを用いた暗号系の概念図

Neural Networkは暗号化・復号時ともに同一のもの。

暗文生成は，暗号化しようとする平文一文字単位で行う．カオス時系列発生源として用いるカオス・ニューラルネットワークのあるニューロンの出力値から1～nの正整数を生成する．この生成された整数を平文に付加することによって暗号化する．一文字暗号化する毎に，ネットワーク遷移を行う．

復号は，暗号化時に用いたカオス・ニューラルネットワークと同一の構成・条件のものをカオス時系列発生源として用いる．暗文から，暗号化時に用いたカオス・ニューラルネットワークのあるニューロンの出力値から生成された正整数を作用させる(取り除く)ことにより，復号する．

これにより，カオス時系列信号の平文に作用させる暗号系が構成できる．

5. 本暗号系の実験結果

前節で示した逐次型共通鍵暗号の実験結果を示す．

暗号化時と復号時には，同一構成のネットワーク(ニューロン数・しきい値・sigmoid関数の傾き係数・ニューロン間の重み係数)を用いた．暗号化・復号時の共通鍵としては，ネットワークへの外部入力値を用いた．

本暗号系の性質を調べるため、以下の3

項目について実験を行った.

a. 鍵が微少に異なる場合
b. 計算機への実装が異なる場合
c. 異なる計算機 (環境) で暗号化 復号を行った場合

実験に用いた平文は, 180kbytesの長さの英文を用いた. その一部をFig.5.1に示す. また, Fig.5.2に, 実験に用いた平文の, 文字の出現頻度を示す. これより, 平文には, 改行記号と英数字に, 特徴的な分布があることがわかる.

5.1 鍵が微少に異なる場合

鍵として用いた外部入力値が微少に異なる場合の, 生成された暗文について検討した.

外部入力値として, 1.24, 1.241で暗号化した場合の, 暗文の文字出現頻度の違いをFig.5.3に, 外部入力値が1.24, $1.24+10^{-12}$ での暗文の文字出現頻度をFig.5.4に示す.

Fig.5.3, より, 外部入力値が0.001異なる場合, 暗文の文字出現頻度が異なることがわかる. しかし, Fig.5.4 では, 顕著な文字出現頻度に, 顕著な差は認められない.

ここで, 外部入力値が1.24, $1.24+10^{-12}$ で生成された暗文をFig.5.5, Fig.5.6 にしめす. これより, 外部入力値が微少に異なる場合でも, 生成される暗文は異なったものとなるといえる.

よって, この暗号系では, 鍵 (外部入力値) が微少に異なると, 生成される暗文が全く異なったものとなるといえる.

None of the multifunction devices provide as good results as single-purpose devices. But if you get the results you like out of one, more power to you.

1.How good is "good"? If you just want to do basic slicks, a 300 DPI printer will do fine. If you have ideas of scanning photos, consider an electronic camera. Otherwise, consider getting PhotoCDs made: they will be much better scans than you can do with a cheap flatbed, especially if color fidelity is important.
If you wish to scan negative or slides, you will want either

Fig. 5. 1 実験に用いた平文

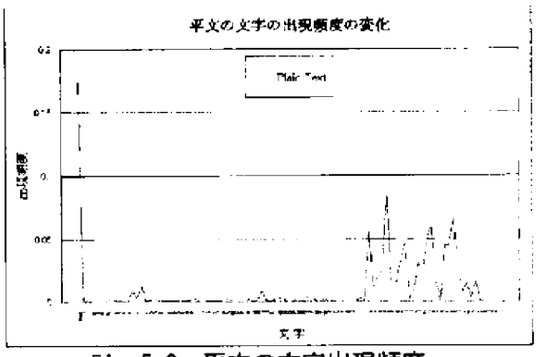

Fig. 5. 2 平文の文字出現頻度

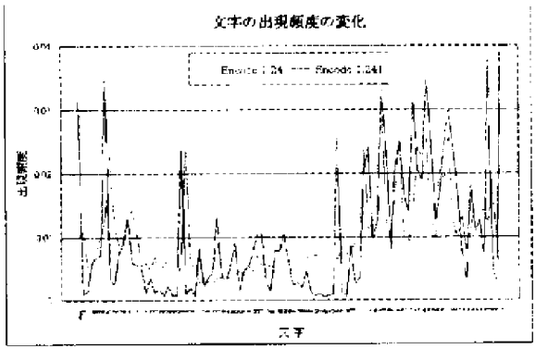

Fig. 5. 3 暗文の文字出現頻度 鍵は1. 24, 1. 241 異なった分布を示している.

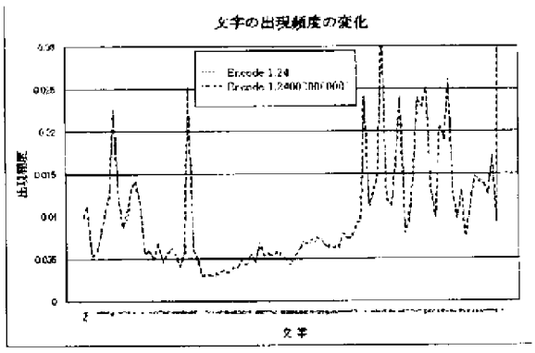

Fig. 5. 4 暗文の文字出現頻度 鍵は1. 24, 1. $24+10^{-12}$ 出現頻度に大きな差異は認められない.

(og\{F`bxgxN-l□z'mdz.□nq9tW|Zrf'c□6d□i$k(p4□_!K□
My\g}&dr39d(oW+p(Odb`H□g~ehj~I`|V□0!hH^z_s%)q
□v ezp/se}SfT
tr*(`qi,d{j4la!RdR+j□**□`y)□oo,xo'ZxF&a□$'□al:i[l6□`{d
`U$qs@ybd|8aq{AlV#Od`7Yeb&gm~F□Cv8scmH`[
hhL8imv+□gh0dzp9nU"
□J"n78rbi&mdu.□RH□T)_m/!mfF8@i
GeX!lk]*_b□%ldu~d^)8`T}MmN+qHN+fn~$c|s1n_0=s-$

Fig. 5. 5 生成された暗文 鍵は1. 24

qV6yr□j*d|0tf0Cn\|]sb,`n.□gsz9nh(<gT4IkK8cm2'md'&`]
q3mU'r□]F]-K8sgm8GK'ueV|Jd(}n-2Yl□P:a_}>db4UeL8\d
5,hmo%
{z+oQ%GsF8\n"(nml'sm(8qpuYda,ad.8sq
"ma{<novM□Jy\j4'e□h%kz|;`TyZ□D-l□$yrs\+□inHm^'M
-^\i□& d□h&kzr8□_"Krf Vu'8fnw|1
')n\"X□T{Ym#!mf'zm^(9qX"hN□8□U&x□m'm[tlqUwVlO}
fc}|□lh|gdv-ro]hrF'oku8knv%□{}il

Fig. 5. 6 生成された暗文 鍵は1. $24+10^{-12}$

5.2 計算機への実装が異なる場合

カオス時系列信号発生源として用いたカオス・ニューラルネットワークの，計算機への実装が異なる場合について検討を加えた．プログラムのコーディングにはC言語を用いているが，カオス・ニューラルネットワークの遷移計算に，double型とfloat型を用いた場合の実験結果を示す．なお，ネットワークの条件 (ニューロン数・重み計数・しきい値・sigmoid関数の傾き係数) と，鍵として用いた外部入力値の値は，どちらの場合も同一である．

Fig.5.7に，double型で暗文生成を行った場合の文字出現頻度と，float型で暗文生成を行った場合の文字出現頻度の差を示す．このグラフから明らかなように，同一条件でも，計算精度が異なると，文字出現頻度が異なることがわかる．

Fig.5.8に，double型の場合とfloat型の場合の，カオス・ニューラルネットワークのLiapnov指数の差を示す．これより，計算精度が異なると，カオスの特徴である初期値鋭敏性の程度が異なってしまう事が示唆される．

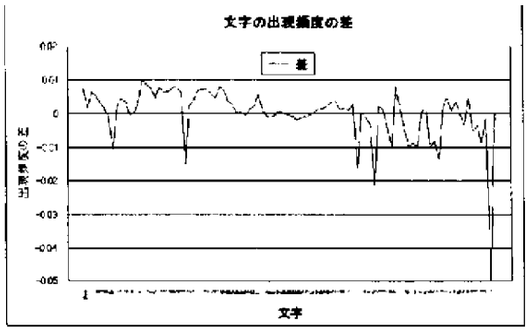

Fig. 5. 7 型による暗文の文字出現頻度の差

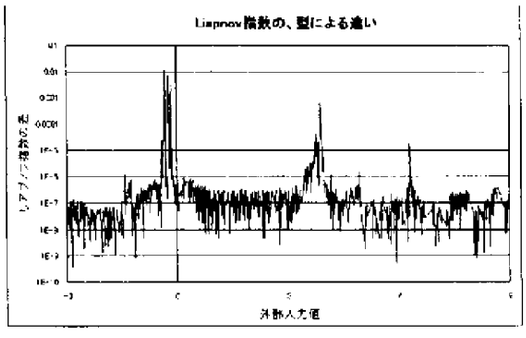

Fig. 5. 8 型によるLiapnov指数の差
鍵である外部入力値に対してプロットしている．

```
Iwp!iH)!pmls3jl/□zPdv1mR2v}aT6
&h_4h%z),{@W7%)eSItiX]35l□"q.Aot!<boA<mC~}jI[eq_
Nqa H..bSnz&i=95m%]]=<qx\'
?~*bz-;Fe#]g.6-}3\yxwf;Ij{Zt;.r'pc~#Ya}ES!]_
+[!,M.mLWu6t{9Wo.e(zjMHnlmg'/;:.,o`g|P\]oZnh&z~-<?m:x
w4Z HXl Xs%27|
jcpfi2B2}*Ezi_a2"UBlk/m%29S"&gyD`|.H,
:_q/[,k8Zp.rt{Y=2pmlulH)rPil'z#/M！)nN-
```

Fig. 5. 9 double型で生成された暗文

```
(*]c=yh5[6BQ}rub6.q3eH)wPbglnkA6,,@Yl0WV5"qgu37z)Q
Uc.c|%bL(-#vXz'y^\IqX)D[.0mr=U5;>09.PnXm=il;vv^)0Z|;
^{.}
/dR#fXXt.zk0b-7>orgkB6,-be.nU&
>i@Cnu^v=8)jYu0)sumchCZ#0^(rG^e3z"5=?z*b!oarz'q,):
96"9hI8pzuE4l*ca@..);;w4dg%`f3-"
dXo4i|@f##6)xBT!eg\B8+sIgi-abA`-AKvsZTnBk
(E□nMhd&^<.5"i5gm6uaHQsohf!@6.|4on!/]
```

Fig. 5. 10 float型で生成された暗文

Fig.5.9にdouble型，Fig.5.10にfloat型で生成された暗文を示す．生成された暗文が全く異なったものであることがわかる．

5.3 暗号化と復号時に用いた計算機が異なる場合

暗号生成時に用いた計算機Aと，それを復号する計算機Bが異なる場合について検討した．この場合，プログラムのコーディングや，カオス・ニューラルネットワークの条件は全く同一である．

暗文生成には VT-600 (CPU:Alpha 21164, OS:Linux) を用い，復号にHP apollo model 715/33 (OS:HP UX) を用いた場合，暗文を復号することができなかった．

Fig.5.11にVT-600により生成された暗文

```
&io&z-(N/m;wn=f}+Z137&jWg
'_.*@$sKj{/j().0m_qh!hKCr|mS-t/z33"2b7+yz)S!r`i(%`$e>cr
&`L$om{G_rIkv+vF.t(n]&G0p@gr,iH
 ikA5%s6uq<m+3X3'V>.lgi2&?,:Kossm0C7'C!%
g
@:M<8<-y_Xs
Um#C_-520Do@oIlx;ty:a$$cYo;y!1q}□ZMavc[A9+x/X{.uZH
X;Cr.llNjy*d3/='!_`5Dl#uL1ni6a.1V-{<i3]Yu
```

Fig.5.11 VT-600により生成された暗文

```
(TAm{!:d0{DVgnRl|kaqpnn\zx
~e:jyeglyozyGt.Ps_PncG□%kPwLd~'Q>,Y<Yn7pT(EZ#'T_7
2N_}-b(,`**TLF*^BOhT3\Ve(!c#&8S{7b)}P
Z'YHT~#3=uMBZkL83_\0l3Hch04bHEV}<D/;=2!Dk
.
@xS#wboy1^m_^NZwW%@=h|e5{VIZ$M;%aA*c9u{YXrcT
0NCp#P8[!+:5XZ4X:x97zz□EYA^):Y
=Wj!6f&#□fr|9jI0eC711H$N]ZL+J4'|X/
```

Fig.5.12 HPによる復号 全く復号されていない

を，Fig.5.12に生成された暗文をHPで復号した結果を示す．計算機が異なるだけであるにもかかわらず，全く復号されていないことがわかる．

6. 考　察

実験結果より，以下のことがいえる．

5.1 より，鍵として用いた外部入力値が微少に異なる場合でも，生成される暗文が全く異なったものになることが示唆される．これは，カオス系の有する初期値鋭敏性のため，鍵として用いた外部入力値が微少に異なっても，それらの軌道が指数関数的に距離を広げていくためであると考えられる．

5.2 は，計算中の打ち切り誤差が計算精度により異なるため生じたと考えられる．この誤差が擾乱雑音として作用し，カオス時系列信号の起動が全く異なったものとなってしまうためであると考えられる[27,28]．

5.3 は，本暗号系に特異な現象であると考えられる．計算機・OSが異なると，使用するCPUやコンパイラ (使用するlibrary等も含む) が異なる．このため，浮動小数点演算結果や，関数libraryの実装の差異のため，計算結果が微妙に異なると考えられる．このため，系がカオスであるから，同一の軌道を得ることができないためであると考えられる．

これらより，カオス・ニューラルネットワークを用いた本暗号系は，従来の暗号や，カオスを用いた暗号系[12~16]と比較しても，カオス・ニューラルネットワークの構成のみならず，外部環境 (使用する計算機やプログラムのコーディング) にも依存する暗号系であるといえる．

7. むすび

特異なカオスを出力する，カオス・ニューラルネットワークを用いた暗号系について検討を加え，その特性について検討を加えた．本暗号系は，カオス時系列を発生するカオス・ニューラルネットワークの構成のみではなく，その実行環境 (計算機やOSの種類) にも依存する暗号系であることを示した．

今後，本暗号系の暗号学的強度や，デジタル署名・認証への応用などについて，検討する予定である．

参　考　文　献

1. 吉田等明, 三浦守, "ニューラルネットワークにおけるキラリティ 振動周期の教師無し学習", 平成6年度電気関係学会東北支部連合大会, 2F1
2. 米城健二, 吉田等明, 三浦守, "人工ニューラルネットワークにおける振動発生機構", 計測自動制御学会東北支部第153回研究集会, 153, pp.1/3～7/3 (1995)
3. 米城健二, 吉田等明, 三浦守, "人工ニューロンの組み合わせによるカオスの発生", 平成7年度電気関係学会東北支部連合大会, 1E15, pp.181 (1995)
4. 米城健二, 吉田等明, 恒川佳隆, 三浦守, "ニューラルネットワークにおける振動、準周期振動、カオス", 第18回情報理論とその応用シンポジウム, E-7-3, pp.735～738 (1995)
5. Hitoaki YOSHIDA, Kenji YONEKI, Yoshitaka TSUNEKAWA and Mamoru MIURA, "Chaos Neural Network", Proceedings of ISPACS'96, Vol.1of3, pp.16.1.1～16.1.5 (1996)
6. 吉田等明, 川村暁, 恒川佳隆, 三浦守, "ニューロン3個から成るネットワークの振動現象", 計測自動制御学会東北支部 第174回研究集会 174-9, pp1/9～9/9, (1998)
7. ・川村暁, 吉田等明, 恒川佳隆, 三浦守, "カオス・ニューラルネットワークの最小構成", 信学技報 NC98-107 (1999-03)
8. 松井甲子雄, "コンピュータのための 暗号組立法入門", 森北出版, 1986
9. 情報処理学会 監修, 岡本龍明, 太田和夫 共著, "暗号ゼロ知識証明 数論", 共立出版, 1995
10. 情報理論とその応用学会(編), "暗号と認証", 情報理論とその応用シリーズ4, 培風館, 1996
11. 岡本龍明, 山本博資, "現代暗号", シリーズ情報科学の数学,産業図書,1997
12. Rong He, P. G. Vaidya, "Implementation of chaotic cryptgraphy with chaotic synchronization", physical review E, pp.1532～1535, vol.57, no.2, 1998
13. Valerio Annovazzi-Lodi ,"Synchronization of Chaotic Injected-Laser Systems and Its Application to Optical Cryptgraphy", Journal of quantum electronics, pp.953～959, vol.32, no.6,1996
38. E. Domany at el., "Models of Neural Networks II: Temporal Asdpects of Coding and Information Processing in Biological Systems", Springer-Verlag (1994)
14. Valerio Annovazzi-Lodi at el.,

"Synchronization of Chaotic Lasers by Optical Feedback for Cryptgraphic Applications", IEEE Journal of quantum electronics, pp.1449 ～ 1454, vol.33, no.9, 1997
15. Jean-Pierre, Goedgebuer at el., "Optical Cryptsystem Based on Synchronization of Hyperchaos Generated by a Delayed Feedback Tunable Laser Diode", physical review letters, pp.2249～2252, vol.80, no.10,1998
16. 大熊健司, 櫻井幸一,"カオス・ストリーム暗号に対する記号力学攻撃の改良", 1999年度 電子情報通信学会総合大会 A-7-1 (1999)
17. 四方順司, 今井秀樹, "楕円曲線暗号について", Computer Today, pp.15～20, 1999.5 No31
18. 岡本龍明, 内山成憲, "楕円曲線暗号の安全性について", 情報処理, pp.1252～1257, 39巻12号, 1998
19. 合原一幸 編, "カオス －カオス理論の基礎と応用－", サイエンス社 (1992)
20. T.Y.Li and J.A.York, "Period three implies chaos",Anner.Math. Mounthly, 82, pp.985 ～ 992 (1975)
21. 長島弘幸, 馬場良和 共著, "カオス入門 現象の解析と数理", 培風館, 1992
22. Denny Gulick著, 前田恵一ら 訳, "カオスとの遭遇－力学系への数学的アプローチ－",産業図書 (1995)
23. 芹沢治 著, "カオスの現象学", 東京図書(1993)
24. P.Berge,Y.Pomeau, Ch.Vidal 著, 相沢洋二 訳, "カオスの中の秩序－乱流の理解へ向けて－",産業図書 (1996)
25. 合原一幸 編, "応用カオス",サイエンス社(1995)
26. 川上博,上田哲史 共著, "CによるカオスCG",サイエンス社(1994)
27. 合原一幸 著, "カオスの数理と技術－カオス、フラクタル、複雑系への序章－", 放送大学 (1997)
28. Paul S Addison, "FRACTALS AND CHAOS an illustrated cours", IOP Publishing Ltd, 1997
29. 月江伸弘, "カオスの数値計算－浮動小数点の桁数の影響－", 1999年度 電子情報通信学会総合大会 A-2-29 (1999)
30. Lipo Wang, Daniel L. Alkon, "Artificial Neural Networks Oscillations, Chaos, and Sequence Processing", IEEE Computer Society Press (1993)
31. PHILIP D.WASSERMAN 著, 石井直宏ら 訳, "ニューラル・コンピューティング－理論と実践－", 森木出版 (1993)
32. J.デイホフ 著, 桂井浩 約, "ニューラルネットワークアーキテクチャ入門", 森北出版 (1992)
33. 上坂吉則 著, "ニューロコンピューティングの数学的基礎", 近代科学社, 1993
34. R.ビールら 著, 八名和夫 監訳, "ニューラルコンピューティング入門", 海文堂 (1993)
35. 西川綽一, 北村新三 著, "ﾆｭｰﾗﾙﾈｯﾄと計測制御 Neural Networks as Applied to Measurment and Control" システム制御情報学会編, 朝倉書店 (1995)
36. 阿部重夫 著, " ニューラルネットとファジィシステム", 近代科学社(1995)
37. Richard M. Golden, "Mathematical Methods for Neural Network Analysis and Design", MIT Press (1996)
39. 林初男 著, "神経システムの非線形現象", コロナ社 (1998)