博士論文

カオスガスタービンおよびその動力学モデルの工学的応用に関する研究

Chaotic gas turbine and applications of its dynamics to engineering

2015 年 3 月

立命館大学大学院理工学研究科
機械システム専攻博士課程後期課程

長　憲一郎

立命館大学審査博士論文

カオスガスタービンおよびその動力学モデルの工学的応用に関する研究

Chaotic gas turbine and applications of its dynamics to engineering

2015 年 3 月

March, 2015

立命館大学大学院理工学研究科

機械システム専攻博士課程後期課程

Doctoral Program in Advanced Mechanical Engineering and Robotics

Graduate School of Science and Engineering

長　憲一郎

Kenichiro Cho

研究指導教員：　宮野　尚哉

Supervisor: Professor Takaya Miyano

目 次

第1章　緒言

1963年，Lorenzは，Rayleigh-Bénard対流を支配するOberbck-Boussinesq方程式を簡略化した連立常微分方程式がカオスを生成することを発見した[1, 2]．カオスとは有界領域で持続する非周期的な振る舞いである．Lorenzが発見した3次元の連立常微分方程式はLorenz方程式と呼ばれ，乱流の簡単なモデルである．また，カオス系の標準モデルとしても有名である．Lorenz方程式はX，Y，Zの3変数で構成される．X，Y，Zは，それぞれ，Rayleigh-Bénard対流の速度場に比例する変数，上昇流と下降流の温度差に比例する変数，垂直方向の温度の歪みに比例する変数に対応する．Rayleigh-Bénard対流の駆動力である浮力，摩擦力，熱の散逸は，換算Rayleigh数(R)，Prandtl数(σ)，対流のアスペクト比の関数としてのパラメータ(b)で表現される．ここで，対流のアスペクト比は$\Gamma = D/H$で定義され, DとHは対流の横と縦の長さである．これらの無次元パラメータは，分岐パラメータとして機能する[3]．Lorenzモデルの分岐構造はBarrioとSerranoにより，詳細に解析されている[4, 5]．

MalkusとHowardは，熱対流を駆動する物理機構を機械的に再現することができれば，Lorenz方程式に従う機械システムを実現できると考えた．こうして作られたものがカオス水車，あるいはMalkus水車と呼ばれている[6, 7]．Malkus水車の運動方程式を無次元化すると，$b = 1$のLorenz方程式と一致する．Malkus水車において，水にかかる重力，水車にかかる摩擦力，区画からの水の流出は，それぞれ，Rayleigh-Bénard対流における浮力，粘性抵抗，熱の散逸に対応する．Malkus水車の動力学的性質は，KolarとGumbによって解析されている[7]．

Malkus水車に触発され，著者は不規則に回転方向を変えるカオスガスタービンを開発した[8]．次章で述べるように，カオスガスタービンはMEMS(micro-electro-mechanical systems)技術を用いて作られたマイクロガスタービン[9, 10]のような積層構造を有する．カオスガスタービンを開発した理由は，Rayleigh-Bénard対流の物理要素とガスタービンの機械要素を対応させることで，ガスタービンにMalkus水車と同じカオス挙動をさせることができると考えたからである．実際，カオスガスタービンにおいて，Rayleigh-Bénard対流の浮力，摩擦力，熱の散逸は，それぞれ，タービンブレード上で発生する抗力，ロータにかかる摩擦力，タービン内からの流体のリークと対応する．しかしながら，Malkus水車と異なり，カオスガスタービンは浮力に相当する抗力の働く範囲が限定される．これは，抗力を発生させる要因となる流体の衝突が，給気流路周辺に限定されるためである．この事実によって，カオスガスタービンの運動方程式は$2N + 1 (N \to \infty)$自由度の運動方程式となり，運動方程式の無次元化式は，$N (N \to \infty)$個のLorenz系がXを中心ノードとした星型ネットワーク構造として表現されることが本論文で明らかにされるであろう．この無次元化式を拡張Lorenz方程式と呼ぶ．カオスガスタービンの運動方程式はタービンのロータの不規則な反転運動を表現でき，ロータの不規則な反転運動は，$\Gamma \sim O(1)$かつ，

10^6 を超える高い Rayleigh 数における Rayleigh-Bénard 対流の平均風の速度場 [11] -[35] を連想させる．ここで，平均風とは，対流の外側から中心にかけてを流れ場が空間的相関をもつ大規模循環流のことである．

$\Gamma \sim O(10^1) - O(10^2)$ における平均風は Krishnamuri と Howord によって発見されており [36]，最近の研究は [34] - [35] に記載されている．平均風の重要性は速度場が不規則に反転することにある．反転運動には 2 つのシナリオがあり，一つは休止-反転シナリオ [24] で，もう一つが方位角回転シナリオ [28, 30] である．休止-反転シナリオでは, 対流ロールが不規則に停止し，反転すると考えられている．対して，方位角回転シナリオでは，対流ロールは一定方向に回転を続ける．しかしながら，対流ロールの回転が止まった瞬間，対流ロール自体が方位角方向に π だけ回転するため，平均風の速度場が不規則に反転を繰り返す．

休止-反転シナリオと方位角回転シナリオに関する常微分方程式形式の力学モデルは，過去に発表された [24, 28, 30]．特に，Araujo らは，彼らが導き出した修正版の Lorenz モデルを使って，対流ロールの不規則な反転運動が休止-反転シナリオによるものだと説明している [24]．カオスガスタービンは不規則に停止，反転を繰り返すことから，カオスガスタービンの運動方程式の無次元化式である拡張 Lorenz 方程式は休止-反転シナリオを説明できると予想できる．拡張 Lorenz 方程式を使って休止-反転シナリオを説明するために，Sreenivasan らの研究 [18] を参照する．彼らの研究では，Rayleigh 数 1.5×10^{11} かつ $\Gamma = 1$ の状況下で，平均風の速度場を観測する実験を行い，得られたデータの統計的性質を報告している．彼らの統計解析手法は，カオスガスタービンの実測結果と運動方程式の数値積分結果の一致度合の評価だけではなく，カオスガスタービンが平均風の動力学的性質をどこまで再現できているかについての評価に有用である．

カオスガスタービンは，Malkus 水車の挙動をガスタービンで再現するための学術モデルとして開発されたものである．よって，カオスガスタービン本体は工学的応用を目的としたものではない．しかしながら，カオスガスタービンの運動方程式の無次元化式である拡張 Lorenz 方程式は，学術モデルだけではなく工学的に応用できる．カオスの工学的応用の一例として，カオス信号を疑似乱数として使用する暗号通信への応用が挙げられる．その他にも，カオスを使用する暗号は多数存在する．例えば，カオス同期を使った暗号通信 [37]-[39]，カオス偏移変調 [40]，カオス制御 [41]-[43]，カオスを使った公開鍵暗号 [44, 45, 46]，カオスブロック暗号 [47]，カオス暗号の暗号解析 [48, 49] などがあり，最近の研究には，[50, 51] などがある．カオスを用いた暗号通信法に関する報告は，Alvarez と Li によって，なされた [52].

カオスを用いた従来の暗号通信法では，分岐パラメータや初期条件を秘密鍵として，送信者と受信者で共有する．しかしながら，鍵の取りうる組み合わせ数が十分に確保できないことや，秘密鍵のわずかな違いでカオス信号の動的挙動が大きく変化しないなどの理由で，カオス暗号は安全性の低い暗号と位置づけられてきた．ここで，カオス暗号における鍵の取りうる組み合わせ数とは，分岐パラメータや初期条件の取りうる組み合わせ数であり，秘密鍵のわずかな違いによるカオス信号の動的挙動の大きな変化は，秘密鍵の特定を困難にするために重要である．このような安全性の問題も，Alvarez と Li によって，報告された [52]．本論文では，暗号通信の伝統的な表記法に則り，Alice を送信者，Bob を受信者，Eve を盗聴者として，表記する．

Lorenz 方程式を使用したカオス暗号として，Cuomo-Oppenheim 法 [37, 38] が有名である．Cuomo-Oppenheim 法では，Alice はカオス信号とノイズのように微小な通信文 m を足し合わせて，Bob に送信する．ここで，カオス信号には Alice の送信システムに実装された第 1 の Lorenz 方程式で生成された X を使用する．暗号文 $X+m$ を受け取った Bob は，Bob の受信システムに実装された第 2 の Lorenz 方程式の X_2 に暗号文 $X+m$ を直接結合する．Bob はさらに，第 2 の Lorenz 方程式で生成された Y_2 を受信システムに実装された第 3 の Lorenz 方程式の Y_3 に直接結合する．$X \gg m$ であるので，Alice と Bob の間で分岐パラメータ (σ, R, b) が等しい時，Lorenz 方程式のカオス同期の特性 [53, 54] から，$Y_2 \approx Y$，$X_3 \approx X$ となる．暗号文 $X+m$ から X_3 を差し引くと，$X_3 \approx X$ より，Bob は通信文 m を復号化できる．Cuomo-Oppenheim 法では，σ, R, b が一致するときのみ通信文 m を復号化できるので，σ, R, b が秘密鍵となる．しかしながら，Cuomo-Oppenheim 法では，カオス同期を使ったパラメータ推定などの攻撃により，Eve が容易に秘密鍵を特定できる．また，Cuomo-Oppenheim 法は共有鍵暗号であるため，鍵配送問題，つまり，どのように Alice と Bob で鍵を安全に共有するかという問題が発生する．この問題はカオス暗号に共通する．

Cuomo-Oppenheim 法は電気回路上で，Lorenz 振動子を再現し，上述したプロセスで通信文の暗号化と復号化を行う．電気回路上で Lorenz 振動子を再現するため，製造誤差により，送信側と受信側の Lorenz 振動子間の分岐パラメータ (σ, R, b) が異なる．これをパラメータミスマッチと呼ぶ．拡張 Lorenz 方程式を Cuomo-Oppenheim 法のようなカオス同期を応用したカオス暗号に適用する場合，パラメータミスマッチ下での拡張 Lorenz 方程式がどの程度，同期誤差を生じさせるのか知る必要がある．そのため，本論文では，この無次元化式の同期特性，特に，パラメータミスマッチ下での同期特性について論じる．

本研究では，Cuomo-Oppenheim 法とは異なる共有鍵暗号として，拡張 Lorenz 方程式をカオスマスキング法に適用させる．本研究を遂行するにあたって，Alvarez と Li の論文 [52] を参照し，安全性の高いカオスマスキング法の実現を目指した．本研究のカオスマスキング法はデジタル計算機上で暗号化と復号化を行い，通信路には通常の通信路の他に量子チャネルを使用することを想定する．量子チャネルは安全性が保障されている量子鍵配送（QKD）[55]-[59] を行う際に使用し，これを本研究のカオス暗号における秘密鍵の配送法に設定する．ここで，QKD の安全性は，量子力学の法則 [60]-[66] が根拠となっている．秘密鍵以外のパラメータ及び，初期条件は公開鍵として，あらかじめ公開しておく．QKD で秘密鍵を共有すれば，Alice と Bob は拡張 Lorenz 方程式の計算に必要な全てのパラメータを共有したことになる．これにより，Alice と Bob は同一のマスキング信号 X を共有できる．疑似乱数として，この X を使うことで，通信文のマスキングとアンマスキングが可能となる．参考文献 [52] では，フィルタリング攻撃，カオス同期を用いた攻撃，総当たり攻撃などのカオス暗号に対する解読手段が論じられている．これらの攻撃方法に対して十分な耐性を持つカオス暗号は，Eve の解読を極めて困難にする．

この論文の構成は以下のようになる．第 2 章では，カオスガスタービンとその運動方程式，及び，拡張 Lorenz 方程式についての説明を行う．また，それらを使った実験結果と実験結果の統計的性質を記載する．この章の最後では，カオスガスタービンの実験結果に関する考察を記載する．第 3 章では，カオスガスタービンの工学的応用可能性を調べるために行った拡張 Lorenz 方程式に関するカオス同期の性質を載せる．また，拡張 Lorenz 方

程式の工学的応用の一例として，カオスマスキング法への応用に関する説明と実験結果及び，この暗号方式の盗聴耐性について論じる．この章の最後に，拡張 Lorenz 方程式のカオス同期と暗号通信への応用についての考察を記す．第 4 章では，鍵配送問題の解決策として，公開鍵暗号と BB84[55] と呼ばれる量子鍵配送法の説明を行い，本研究のカオスマスキング法との組み合わせが可能であることを示す．結言は第 5 章に記す．

第2章　カオスガスタービン

2.1　カオスガスタービンとその動力学的性質

2.1.1　カオスガスタービンの構造と設計

本研究において設計，試作されたカオスガスタービンの概略図が図 2.1 と図 2.2 である．図 2.1 では，簡単のために，ロータ上のタービンブレードは 6 枚のみ描いている．図 2.3 では，実際に作製したカオスガスタービンの写真を，図 2.4 では，カオスガスタービンの部品構成を示す．図 2.3 のように，実際のタービンブレードは 24 枚となっている．図 2.2，図 2.4 に示すように，ガスタービンはアクリル板 3 層で構成されており，この構造は MEMS(micro-electro-mechanical systems) 技術を用いて作られたマイクロガスタービン [9, 10] とよく似ている．しかしながら，駆動力に揚力ではなく，抗力を使用している点で，著者が製作したガスタービンと既存のマイクロガスタービンは異なる．この相違により，本研究のカオスガスタービンは Rayleigh-Bénard 対流の浮力を表現でき，カオス挙動を実現できる．

タービンのロータの直径 d_r は 40[mm]，厚さは 7.6[mm] であり，素材にはステンレスを使用している．ロータ上には厚さ 1[mm]，高さ 2[mm] のタービンブレードが 24 枚，中心軸対称に配置され，どちらの方向にもロータが回るよう設計されている．タービンのロータが円盤であると仮定し，$I = (M/2)(d_r/2)^2$ を用いて，慣性モーメント I を計算すると，$I = 1.5 \times 10^{-5}[kgm^2]$ となった．M はロータの質量であり，$M = 0.075[kg]$ である．図 2.1 と図 2.2 における水色の矢印は，給気流体がどのように流出するかを示したものであり，赤色の矢印は気体軸受に使用する流体が，どのように流出するかを示したものである．給気流体が流入する流路幅 d_{in} は $4[mm]$ である．気体軸受にはスラスト軸受が採用されており，これにより，ロータを押し上げて，ロータと下部アクリル層との間に空間を作ることができる．そのため，スラスト圧力を上げることで，摩擦力を減少させることが可能となる．図 2.2 における紫色の矢印は，給気流体のタービン内からのリークを示したものであり，ロータと上部アクリル層との隙間で形成されるリーク路幅は $0.4[mm]$ 以下となっている．

給気流体がタービンブレードに衝突し，抗力が発生する範囲は，給気口の末端とロータ中心とがなす角度 $\phi[rad]$ で表現することができる (図 2.1)．Malkus 水車 [6, 7] では，重力が Malkus 水車全体に働くため，このような駆動力の働く範囲の制限はない．これが，本研究のカオスガスタービンと Malkus 水車の大きな違いである．

カオスガスタービンにおいて，タービンブレードに発生する抗力は，Rayleigh-Bénard 対流の浮力に相当する．揚力ではなく抗力を駆動力とした理由は，揚力を駆動力とすると，ロータの形状が中心軸対称とならず，片側だけにロータが回転するからである．タービンからの流体のリークは，Rayleigh-Bénard 対流の熱の散逸を，ロータにかかる摩擦力は対

流の摩擦力を表現している．

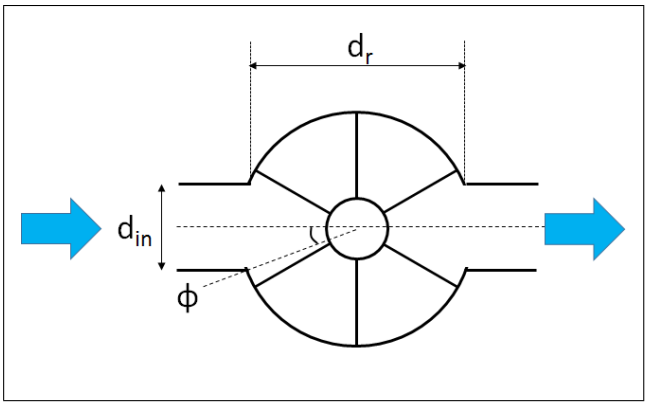

図 2.1: ガスタービンの概略図 (正面図)

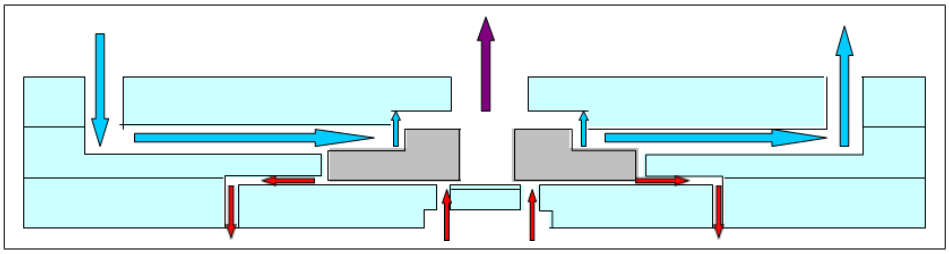

図 2.2: ガスタービンの概略図 (断面図)

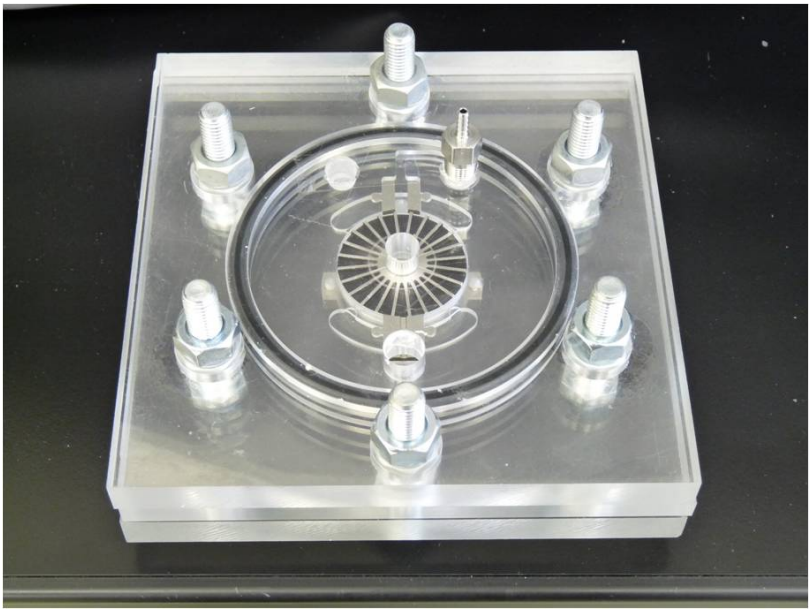

図 2.3: ガスタービンの完成写真

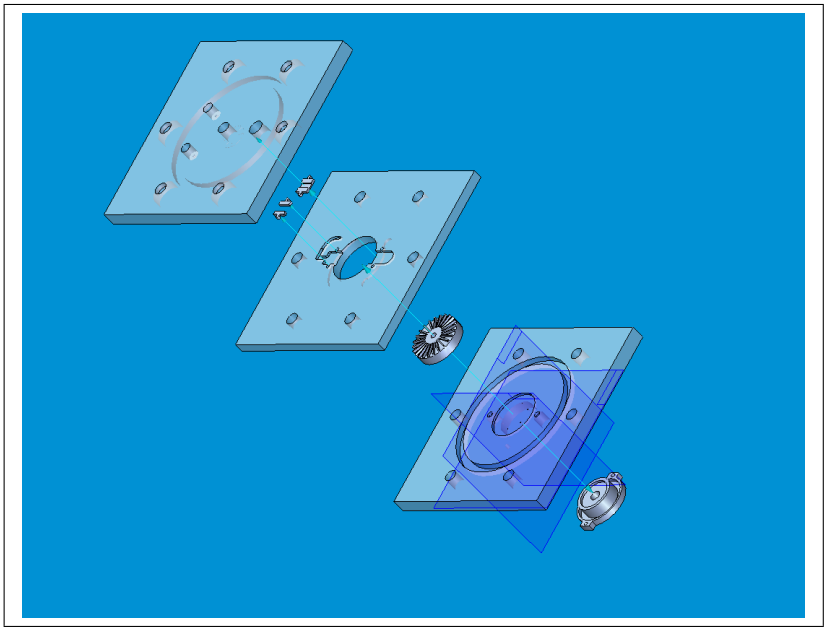

図 2.4: ガスタービンの部品構成

2.1.2 運動方程式

作製したカオスガスタービンにおけるロータの回転速度を支配する運動方程式を導く．ただし，タービンのロータは無限に薄く，タービン翼が無限にあると仮定する．また，タービン翼の一点に力が集中していると仮定する．

タービン翼周りの気体の質量分布を $m(\theta,t)[kg]$，単位時間当たりの流路からの流入量を $Q_{in}(\theta)[kg/s]$ ，単位時間当たりの区画からの流入量を $Q_{out}(\theta)[kg/s]$ とする．タービン内の質量変化は式 (2.1) となる．

$$\frac{\partial m(\theta,t)}{\partial t} = Q_{in}(\theta,t) - Q_{out}(\theta,t) - \omega\frac{\partial m(\theta,t)}{\partial \theta} \tag{2.1}$$

流入率を α [1/s]，区画からのリーク率を K [1/s] とする．また，流路内での直線上の質量分布を $m_{in}(\theta)$，中心穴周りでの質量分布を $m_{out}(\theta)$ とすると $Q_{in}(\theta)$，$Q_{out}(\theta)$ は以下のように書ける．

$$\begin{aligned} Q_{in}(\theta,t) &= \alpha\left[m_{in}(\theta) - m(\theta,t)\right] \\ Q_{out}(\theta,t) &= K\left[m(\theta,t) - m_{out}(\theta)\right] \end{aligned}$$

これを式 (2.1) に適用したのが式 (2.2) である．

$$\frac{\partial m(\theta,t)}{\partial t} = \alpha\left(m_{in}(\theta) - m(\theta,t)\right) - K\left(m(\theta,t) - m_{out}(\theta)\right) - \omega\frac{\partial m(\theta,t)}{\partial \theta} \tag{2.2}$$

タービン翼周りの気体の密度分布を $\rho(\theta,t)$，流路内での直線上の密度分布を $\rho_{in}(\theta)$，中心穴周りでの密度分布 $\rho_{out}(\theta)$ とおくと，

$$\begin{aligned} m(\theta,t) &= \rho(\theta,t)V(\theta) \\ m_{in}(\theta) &= \rho_{in}(\theta)V(\theta) \\ m_{out}(\theta) &= \rho_{out}(\theta)V(\theta) \end{aligned}$$

とできる．ここで $V(\theta)$ は角度 θ でのタービン体積である．タービンは円形であるので，角度 θ での体積は等しい．よって，次式が導かれる．

$$\frac{\partial \rho(\theta,t)}{\partial t} = \alpha(\rho_{in}(\theta) - \rho(\theta,t)) - K\left(\rho(\theta,t) - \rho_{out}(\theta)\right) - \omega\frac{\partial \rho(\theta,t)}{\partial \theta} \tag{2.3}$$

気体を理想気体と仮定し，$\rho = P/RT$ を使うと，式 (2.3) は式 (2.4) の圧力変化の式になる．ここで，$P(\theta,t)$ はタービン翼周りの圧力分布，$P_{in}(\theta)$ は流路内の直線上での圧力分布，$P_{out}(\theta,t)$ は中心穴周りでの圧力分布である．

$$\frac{\partial P(\theta,t)}{\partial t} = \alpha\left(P_{in}(\theta) - P(\theta,t)\right) - K\left(P(\theta,t) - P_{out}(\theta)\right) - \omega\frac{\partial P(\theta,t)}{\partial \theta} \tag{2.4}$$

次にタービンのトルクについて考える．動圧によってかかる力の分布 $f_d(\theta,t)$ は以下のようにできる．

$$
\begin{aligned}
f_d(\theta,t) &= P_d(\theta,t)S\sin\theta \quad \text{if} \quad -\phi \le \theta \le \phi \\
&= 0 \qquad\qquad\qquad\qquad otherwise
\end{aligned}
$$

また，静圧によってかかる力の分布 $f_s(\theta,t)$ は以下のようにできる．

$$
\begin{aligned}
f_s(\theta,t) &= (P_s(\theta,t) - P_s(\theta+d\theta,t))S \\
&= -\frac{\partial P_s}{\partial\theta}S
\end{aligned}
$$

微小角度 $d\theta$ での微小力が $dF_d = f_d(\theta,t)d\theta$, $dF_s = f_s(\theta,t)d\theta$ とすると，微小角度 $d\theta$ での微小トルクは以下のようになる．

$$
\begin{aligned}
d\tau_d &= f_d(\theta,t)rd\theta \\
d\tau_s &= f_s(\theta,t)rd\theta
\end{aligned}
$$

ただし, r はタービン翼の重心の位置で, 圧力による力はこの点に集中すると仮定している．動圧がタービン翼に対して下向きにかかるのは $-\phi \le \theta \le \phi$ の流路区間のみである．また静圧は $-\pi \le \theta \le \pi$ の区間でかかるので，$d\tau_d$，$d\tau_s$ をこれらの区間で積分する．

$$
\begin{aligned}
\tau_d &= \int_{-\phi}^{\phi} P_d(\theta,t)Sr\sin\theta d\theta \\
\tau_s &= \int_{-\pi}^{\pi} \frac{\partial P_s(\theta,t)}{\partial\theta}Srd\theta \\
&= 0
\end{aligned}
$$

よって，圧力によるトルクは式 (2.5) とできる．

$$
\begin{aligned}
\tau_{pressure} &= \tau_d + \tau_s \\
&= Sr\int_{-\phi}^{\phi} P_d(\theta,t)\sin\theta d\theta
\end{aligned} \tag{2.5}
$$

式 (2.5) からトルクバランスの式 (2.6) が得られる．

$$
I\dot{\omega} = -v\omega + Sr\int_{-\phi}^{\phi} P_d(\theta,t)\sin\theta d\theta \tag{2.6}
$$

圧力変化の式を整理する．$P(\theta,t)$ は全圧であるので，これを静圧 $P_s(\theta,t)$ と動圧 $P_d(\theta,t)$ に分けて記述する．

$$
P(\theta,t) = P_s(\theta,t) + P_d(\theta,t) \tag{2.7}
$$

静圧の時間変化は動圧の時間変化に対して非常に小さいと考えられるので，不等式 (2.8) とおく．

$$\frac{\partial P_s(\theta,t)}{\partial t} << \frac{\partial P_d(\theta,t)}{\partial t} \tag{2.8}$$

式 (2.7) および式 (2.8) により，式 (2.9) および式 (2.10) を得る．

$$P(\theta,t) = \bar{P}_s(\theta,t) + P_d(\theta,t) \tag{2.9}$$

$$\frac{\partial P(\theta,t)}{\partial t} = \frac{\partial P_d(\theta,t)}{\partial t} \tag{2.10}$$

ただし,$\bar{P}_s$ は静圧の平均値である．式 (2.9) および式 (2.10) により，全圧の式は以下のように置き換えられる．

$$\begin{aligned}\frac{\partial P_d(\theta,t)}{\partial t} &= \alpha\left(P_{in}(\theta) - \bar{P}_s(\theta,t) - P_d(\theta,t)\right) - K\left(\bar{P}_s(\theta,t) + P_d(\theta,t) - P_{out}(\theta)\right) \\ &\quad -\omega\left(\frac{\partial \bar{P}_s(\theta,t)}{\partial\theta} + \frac{\partial P_d(\theta,t)}{\partial\theta}\right) \\ &= -(K+\alpha)P_d - \omega\frac{\partial P_d}{\partial\theta} + \alpha P_{in} - (K+\alpha)\bar{P}_s - \omega\frac{\partial \bar{P}_s}{\partial\theta} + KP_{out} \end{aligned} \tag{2.11}$$

Fourier 級数展開を用いて表現すると，以下の 4 式が得られる．ただし, このガスタービンは左右対称に給気と排気を行うので, $P_{in}(\theta)$ と $P_{out}(\theta)$ の $\sin n\theta$ 項は省略できる．

$$\begin{aligned} P_d(\theta,t) &= \frac{b_0(t)}{2} + \sum_{n=1}^{\infty}\left[a_n(t)\sin n\theta + b_n(t)\cos n\theta\right] \\ \bar{P}_s(\theta) &= \frac{d_0(t)}{2} + \sum_{n=1}^{\infty}\left[c_n\sin n\theta + d_n\cos n\theta\right] \\ P_{in}(\theta) &= \frac{p_0^{in}}{2} + \sum_{n=1}^{\infty}\left[p_n^{in}\cos n\theta\right] \\ P_{out}(\theta) &= \frac{p_0^{out}}{2} + \sum_{n=1}^{\infty}\left[p_n^{out}\cos n\theta\right] \end{aligned}$$

上述した 4 式を式 (2.11) に代入して係数比較すると以下のようになる（$n = 1\sim\infty$）．

$$\begin{aligned} \dot{a}_n &= n\omega b_n - (K+\alpha)a_n + n\omega d_n - (K+\alpha)c_n \\ \dot{b}_n &= -n\omega a_n - (K+\alpha)b_n + \alpha q_n^{in} + Kp_n^{out} - n\omega c_n - (K+\alpha)d_n \\ \frac{\dot{b}_0}{2} &= -(K+\alpha)\frac{b_0}{2} + \frac{\alpha p_0^{in}}{2} - (K+\alpha)\frac{d_0}{2} + \frac{Kp_0^{out}}{2} \end{aligned}$$

整理したものが下式となる．

$$\dot{a}_n(t) = n\omega(b_n(t)+d_n) - (K+\alpha)(a_n(t)+c_n) \tag{2.12}$$
$$\dot{b}_n(t) = -n\omega(a_n(t)+c_n) - (K+\alpha)(b_n(t)+d_n) + \alpha q_n^{in} + Kp_n^{out} \tag{2.13}$$
$$\dot{b}_0(t) = -(K+\alpha)(b_0(t)+d_0) + \alpha p_0^{in} + Kp_0^{out} \tag{2.14}$$

次に c_n，d_n，p_n^{in}，p_n^{out} を求める．c_n，d_n, p_n^{in}，p_n^{out} は Fourier 級数展開の係数であるので,

$$\begin{aligned} c_n &= \frac{1}{\pi}\int_{-\pi}^{\pi} \bar{P}_s(\theta)\sin n\theta d\theta \\ d_n &= \frac{1}{\pi}\int_{-\pi}^{\pi} \bar{P}_s(\theta)\cos n\theta d\theta \\ p_n^{in} &= \frac{1}{\pi}\int_{-\pi}^{\pi} P_{in}(\theta)\cos n\theta d\theta \\ p_n^{out} &= \frac{1}{\pi}\int_{-\pi}^{\pi} P_{out}(\theta)\cos n\theta d\theta \end{aligned}$$

簡単のために $\bar{P}_s(\theta)$，$P_{in}(\theta)$，$P_{out}(\theta)$ は次のようにおく．

$$\begin{aligned} \bar{P}_s(\theta) &= P_s \quad \text{for} \quad -\pi \le \theta \le \pi \\ P_{in}(\theta) &= P_{in} \quad \text{if} \quad -\phi \le \theta \le \phi \\ &= 0 \qquad otherwise \\ P_{out}(\theta) &= P_{out} \quad \text{for} \quad -\pi \le \theta \le \pi \end{aligned}$$

すると，c_n，d_n，p_n^{in}，p_n^{out} は $c_n = 0$，$d_n = 0$, $p_n^{in} = 2P_{in}/n\pi$，$p_n^{out} = 0$
これにより,

$$\dot{a}_n(t) = n\omega b_n(t) - (K+\alpha)a_n(t) \tag{2.15}$$
$$\dot{b}_n(t) = -n\omega a_n(t) - (K+\alpha)b_n(t) + \frac{2\alpha P_{in}}{n\pi}\sin n\phi \tag{2.16}$$
$$\dot{b}_0(t) = -(K+\alpha)b_0(t) + \frac{2\alpha\phi}{\pi}P_{in} + 2Kp_{out} \tag{2.17}$$

続いて，トルクバランスの式 (2.6) の P_d を Fourier 級数展開の形に変換し，整理する．

$n = 0$ のとき

$$-Sr\left[\frac{b_0(t)}{2}\right]_{-\phi}^{\phi} = 0 \tag{2.18}$$

$n = 1$ のとき

$$
\begin{aligned}
&Sr\int_{-\phi}^{\phi}(a_1(t)\sin\theta+b_1(t)\cos\theta)\sin\theta d\theta\\
&=\frac{1}{2}Sra_1(t)\left[\theta-\frac{1}{2}\sin 2\theta\right]_{-\phi}^{\phi}-\frac{1}{2}Srb_1(t)[\cos 2\theta]_{-\phi}^{\phi}\\
&=Sra_1\phi-\frac{1}{2}Sra_1\sin 2\phi
\end{aligned}
$$

$n=2$ のとき

$$
\begin{aligned}
&Sr\int_{-\phi}^{\phi}(a_2(t)\sin 2\theta+b_2(t)\cos 2\theta)\sin\theta d\theta\\
&=Sr\int_{-\phi}^{\phi}(a_2(t)\sin\theta\sin 2\theta+b_2(t)\sin\theta\cos 2\theta)\,d\theta
\end{aligned}
$$

和積の公式より

$$
\begin{aligned}
&Sr\int_{-\phi}^{\phi}(a_2(t)\sin\theta\sin 2\theta+b_2(t)\sin\theta\cos 2\theta)\,d\theta\\
&=Sr\int_{-\phi}^{\phi}\left\{-\frac{1}{2}a_2(\cos 3\theta-\cos\theta)+\frac{1}{2}b_2(\sin 3\theta+\sin(-\theta))\right\}d\theta\\
&=-\frac{1}{2}a_2Sr\left[\frac{1}{3}\sin 3\theta-\sin\theta\right]_{-\phi}^{\phi}+\frac{1}{2}b_2Sr\left[\frac{1}{3}\cos 3\theta+\cos(-\theta)\right]_{-\phi}^{\phi}\\
&=a_2Sr\sin\phi-\frac{1}{3}a_2Sr\sin 3\phi
\end{aligned}
$$

$n=3$ のとき

$$
\begin{aligned}
&Sr\int_{-\phi}^{\phi}(a_3(t)\sin 3\theta+b_3(t)\cos 3\theta)\sin\theta d\theta\\
&=Sr\int_{-\phi}^{\phi}(a_3(t)\sin\theta\sin 3\theta+b_3(t)\sin\theta\cos 3\theta)\,d\theta\\
&=Sr\int_{-\phi}^{\phi}\left\{-\frac{1}{2}a_3(\cos 4\theta-\cos 2\theta)+\frac{1}{2}b_3(\sin 4\theta+\sin(-2\theta))\right\}d\theta\\
&=-\frac{1}{2}a_3Sr\left[\frac{1}{4}\sin 4\theta-\frac{1}{2}\sin 2\theta\right]_{-\phi}^{\phi}+\frac{1}{2}b_3Sr\left[\frac{1}{4}\cos 4\theta+\frac{1}{2}\cos(-2\theta)\right]_{-\phi}^{\phi}\\
&=\frac{1}{2}a_3Sr\sin 2\phi-\frac{1}{4}a_3Sr\sin 4\phi
\end{aligned}
$$

これらにより，式 (2.6) は以下のように書き換えられる．

$$
\begin{aligned}
I\dot{\omega} &= -v\omega+Sra_1\left(\phi-\frac{1}{2}\sin 2\phi\right)\\
&\quad+\sum_{n=2}^{\infty}\left[\frac{1}{n-1}a_nSr\{\sin(n-1)\phi\}-\frac{1}{n+1}a_nSr\{\sin(n+1)\phi\}\right] \qquad (2.19)
\end{aligned}
$$

式 (2.15)，式 (2.16)，および，式 (2.19) より, ω，a_n，b_n は閉じた系となる．

運動方程式は最終的に以下の $2n+1$ 次元になる $(n \to \infty)$.

$$
\begin{aligned}
\dot{a}_n(t) &= n\omega b_n(t) - (K+\alpha)a_n(t) \\
\dot{b}_n(t) &= -n\omega a_n(t) - (K+\alpha)b_n(t) + \frac{2\alpha P_{in}}{n\pi}\sin n\phi \\
I\dot{\omega} &= -v\omega + Sra_1\left(\phi - \frac{1}{2}\sin 2\phi\right) \\
&\quad + \sum_{n=2}^{\infty}\left[\frac{1}{n-1}a_n Sr\{\sin(n-1)\phi\} - \frac{1}{n+1}a_n Sr\{\sin(n+1)\phi\}\right]
\end{aligned}
$$

2.1.3 拡張 Lorenz 方程式

カオスガスタービンの運動方程式と Lorenz 方程式との関係を分析するために，前節で導出した運動方程式を無次元化する．まず，運動方程式を行列形式に書き直す．

$$\dot{\mathbf{a}} = \omega\mathbf{nb} - (K+\alpha)\mathbf{a} \tag{2.20}$$

$$\dot{\mathbf{b}} = -\omega\mathbf{na} - (K+\alpha)\mathbf{b} + \frac{2\alpha P_{in}}{\pi}\mathbf{n}^{-1}\mathbf{W} \tag{2.21}$$

$$\dot{\omega} = -\frac{v}{I}\omega + \frac{Sr}{I}tr(\mathbf{\Phi a}) \tag{2.22}$$

ここで $tr(\cdot)$ は対角和を表している．また，$\mathbf{a}, \mathbf{b}, \mathbf{n}, \mathbf{W}, \mathbf{\Phi}$ は $N \times N$ 対角行列である．もとの運動方程式では $N \to \infty$ であるが，数値解析の際の便宜上，N を有限値とした．

$$\begin{aligned}
\mathbf{a} &= diag(a_1, \ldots, a_N), \\
\mathbf{b} &= diag(b_1, \ldots, b_N), \\
\mathbf{n} &= diag(1, \ldots, N), \\
\mathbf{W} &= diag(\sin\phi, \ldots, \sin N\phi), \\
\mathbf{\Phi} &= diag(\phi - \frac{1}{2}\sin 2\phi, \ldots, \frac{1}{N-1}\sin(N-1)\phi - \frac{1}{N+1}\sin(N+1)\phi),
\end{aligned}$$

式 (2.20)，式 (2.21)，および，式 (2.22) に以下の 4 式 を代入する．

$$\begin{aligned}
\mathbf{a} &= \boldsymbol{\delta}\mathbf{Y} \\
\mathbf{b} &= \boldsymbol{\beta}\mathbf{Z} + \frac{2\alpha P_{in}}{(K+\alpha)\pi}\mathbf{n}^{-1}\mathbf{W} \\
\omega &= tr(\boldsymbol{\gamma}\mathbf{X}) \\
t &= T\tau
\end{aligned}$$

ただし，$\boldsymbol{\delta}$，$\mathbf{Y}$，$\boldsymbol{\beta}$, $\mathbf{Z}$，$\boldsymbol{\gamma}$，$\mathbf{X}$ は $N \times N$ 正方行列とする．

$$\begin{aligned}
\frac{\boldsymbol{\delta}}{T}\frac{d\mathbf{Y}}{d\tau} &= \mathbf{n}\left\{\boldsymbol{\beta}\mathbf{Z} + \frac{2\alpha P_{in}}{(K+\alpha)\pi}\mathbf{n}^{-1}\mathbf{W}\right\}tr(\boldsymbol{\gamma}\mathbf{X}) - (K+\alpha)\boldsymbol{\delta}\mathbf{Y} \\
\frac{\boldsymbol{\beta}}{T}\frac{d\mathbf{Z}}{d\tau} &= -\mathbf{n}\boldsymbol{\delta}\mathbf{Y}tr(\boldsymbol{\gamma}\mathbf{X}) - (K+\alpha)\boldsymbol{\beta}\mathbf{Z} \\
\frac{1}{T}\frac{dtr(\boldsymbol{\gamma}\mathbf{X})}{d\tau} &= -\frac{v}{I}tr(\boldsymbol{\gamma}\mathbf{X}) + \frac{Sr}{I}tr(\mathbf{\Phi}\boldsymbol{\delta}\mathbf{Y})
\end{aligned}$$

上式を整理すると，以下の式が得られる．

$$\begin{aligned}
\frac{d\mathbf{Y}}{d\tau} &= T\boldsymbol{\delta}^{-1}\mathbf{n}\boldsymbol{\beta}\mathbf{Z}tr(\boldsymbol{\gamma}\mathbf{X}) + \frac{2\alpha P_{in}}{(K+\alpha)\pi}\boldsymbol{\delta}^{-1}\mathbf{W}tr(\boldsymbol{\gamma}\mathbf{X}) - T(K+\alpha)\mathbf{Y} \\
\frac{d\mathbf{Z}}{d\tau} &= -T\boldsymbol{\beta}^{-1}\mathbf{n}\boldsymbol{\delta}\mathbf{Y}tr(\boldsymbol{\gamma}\mathbf{X}) - T(K+\alpha)\mathbf{Z} \\
\frac{dtr(\boldsymbol{\gamma}\mathbf{X})}{d\tau} &= -\frac{vT}{I}tr(\boldsymbol{\gamma}\mathbf{X}) + \frac{SrT}{I}tr(\mathbf{\Phi}\boldsymbol{\delta}\mathbf{Y})
\end{aligned}$$

$T = 1/K + \alpha$ を代入し，整理する．

$$\begin{aligned}
\frac{d\mathbf{Y}}{d\tau} &= \frac{1}{K+\alpha}\boldsymbol{\delta}^{-1}\mathbf{n}\boldsymbol{\beta}\mathbf{Z}tr(\boldsymbol{\gamma}\mathbf{X}) + \frac{2\alpha P_{in}}{(K+\alpha)^2\pi}\boldsymbol{\delta}^{-1}\mathbf{W}tr(\boldsymbol{\gamma}\mathbf{X}) - \mathbf{Y} \\
\frac{d\mathbf{Z}}{d\tau} &= -\frac{1}{K+\alpha}\boldsymbol{\beta}^{-1}\mathbf{n}\boldsymbol{\delta}\mathbf{Y}tr(\boldsymbol{\gamma}\mathbf{X}) - \mathbf{Z} \\
\frac{dtr(\boldsymbol{\gamma}\mathbf{X})}{d\tau} &= -\frac{v}{I(K+\alpha)}tr(\boldsymbol{\gamma}\mathbf{X}) + \frac{Sr}{I(K+\alpha)}tr(\boldsymbol{\Phi}\boldsymbol{\delta}\mathbf{Y})
\end{aligned}$$

後述する条件で式の再構築を行う．

$$-\frac{1}{\sqrt{K+\alpha}}\boldsymbol{\gamma}'^{-1} = \frac{1}{K+\alpha}\boldsymbol{\delta}^{-1}\mathbf{n}\boldsymbol{\beta} \tag{2.23}$$

$$\mathbf{A} = \frac{2\alpha P_{in}}{(K+\alpha)^2\pi}\boldsymbol{\delta}^{-1}\mathbf{W}$$

$$\frac{1}{\sqrt{K+\alpha}}\boldsymbol{\gamma}'^{-1} = -\frac{1}{K+\alpha}\boldsymbol{\beta}^{-1}\mathbf{n}\boldsymbol{\delta} \tag{2.24}$$

$$\begin{aligned}
\mathbf{B} &= \frac{v}{I(K+\alpha)}\boldsymbol{\gamma} \\
&= \frac{Sr}{I(K+\alpha)}\boldsymbol{\Phi}\boldsymbol{\delta} \qquad (2.25) \\
\boldsymbol{\gamma} &= \boldsymbol{\gamma}'\boldsymbol{\gamma}'
\end{aligned}$$

式 (2.23) より，

$$\boldsymbol{\delta} = -\frac{1}{\sqrt{K+\alpha}}\mathbf{n}\boldsymbol{\beta}\boldsymbol{\gamma}' \tag{2.26}$$

式 (2.24) より，

$$\boldsymbol{\beta} = -\frac{1}{\sqrt{K+\alpha}}\mathbf{n}\boldsymbol{\delta}\boldsymbol{\gamma}' \tag{2.27}$$

式 (2.25) より，

$$\boldsymbol{\delta} = \frac{v}{Sr}\boldsymbol{\Phi}^{-1}\boldsymbol{\gamma} \tag{2.28}$$

式 (2.26) および式 (2.28) より，

$$\boldsymbol{\beta} = -\frac{v\sqrt{K+\alpha}}{Sr}\mathbf{n}^{-1}\boldsymbol{\Phi}^{-1}\boldsymbol{\gamma}' \tag{2.29}$$

式 (2.27) および式 (2.28) より，

$$\boldsymbol{\beta} = -\frac{v}{Sr\sqrt{K+\alpha}}\mathbf{n}\boldsymbol{\Phi}^{-1}\boldsymbol{\gamma}\boldsymbol{\gamma}' \tag{2.30}$$

式 (2.29) および式 (2.30) より，

$$
\begin{aligned}
-\frac{v\sqrt{K+\alpha}}{Sr}\mathbf{n}^{-1}\mathbf{\Phi}^{-1}\boldsymbol{\gamma}' &= -\frac{v}{Sr\sqrt{K+\alpha}}\mathbf{n}\mathbf{\Phi}^{-1}\boldsymbol{\gamma}\boldsymbol{\gamma}' \\
\boldsymbol{\gamma} &= (K+\alpha)\mathbf{\Phi}\mathbf{n}^{-1}\mathbf{n}^{-1}\mathbf{\Phi}^{-1}
\end{aligned}
$$

$\mathbf{\Phi}$，$\mathbf{n}^{-1}$ は対角行列なので，

$$
\begin{aligned}
\mathbf{\Phi}\mathbf{n}^{-1} &= \mathbf{n}^{-1}\mathbf{\Phi} \\
\mathbf{n}^{-1}\mathbf{\Phi}^{-1} &= \mathbf{\Phi}^{-1}\mathbf{n}^{-1}
\end{aligned}
$$

が成り立つ．

$$
\begin{aligned}
\boldsymbol{\gamma} &= (K+\alpha)(\mathbf{n}^{-1})^2 && (2.31) \\
\boldsymbol{\gamma}'\boldsymbol{\gamma}' &= (K+\alpha)(\mathbf{n}^{-1})^2 \\
\boldsymbol{\gamma}' &= \sqrt{K+\alpha}\mathbf{n}^{-1} && (2.32)
\end{aligned}
$$

式 (2.28) および式 (2.31) より，

$$
\boldsymbol{\delta} = \frac{v(K+\alpha)}{Sr}\mathbf{\Phi}^{-1}(\mathbf{n}^{-1})^2 \tag{2.33}
$$

式 (2.29) および式 (2.32) より，

$$
\boldsymbol{\beta} = -\frac{v(K+\alpha)}{Sr}\mathbf{n}^{-1}\mathbf{\Phi}^{-1}\mathbf{n}^{-1} \tag{2.34}
$$

ゆえに，

$$
\begin{aligned}
\mathbf{A} &= \frac{2\alpha SrP_{in}}{(K+\alpha)^3\pi}\mathbf{n}^2\mathbf{\Phi}\mathbf{W} \\
\mathbf{B} &= \frac{v}{I(K+\alpha)}\boldsymbol{\gamma} \\
&= \frac{v}{I}(\mathbf{n}^{-1})^2
\end{aligned}
$$

従って，連立方程式は以下の形に書き換えできる．

$$
\begin{aligned}
\frac{d\mathbf{Y}}{d\tau} &= -\frac{1}{\sqrt{K+\alpha}}\boldsymbol{\gamma}'^{-1}\mathbf{Z}tr(\boldsymbol{\gamma}\mathbf{X}) + \mathbf{A}tr(\boldsymbol{\gamma}\mathbf{X}) - \mathbf{Y} \\
\frac{d\mathbf{Z}}{d\tau} &= \frac{1}{\sqrt{K+\alpha}}\boldsymbol{\gamma}'^{-1}\mathbf{Y}tr(\boldsymbol{\gamma}\mathbf{X}) - \mathbf{Z} \\
\frac{dtr(\boldsymbol{\gamma}\mathbf{X})}{d\tau} &= -tr(\mathbf{B}\mathbf{X}) + tr(\mathbf{B}\mathbf{Y})
\end{aligned}
$$

式 (2.31) および式 (2.32) より，

$$
\begin{aligned}
\frac{d\mathbf{Y}}{d\tau} &= -\mathbf{nZ}tr\{(\mathbf{n}^{-1})^2\mathbf{X}\} + (K+\alpha)\mathbf{A}tr\{(\mathbf{n}^{-1})^2\mathbf{X}\} - \mathbf{Y} \\
\frac{d\mathbf{Z}}{d\tau} &= \mathbf{nY}tr\{(\mathbf{n}^{-1})^2\mathbf{X}\} - \mathbf{Z} \\
\frac{dtr(\mathbf{n}^{-1}\mathbf{n}^{-1}\mathbf{X})}{d\tau} &= -\frac{1}{K+\alpha}tr(\mathbf{BX}) + \frac{1}{K+\alpha}tr(\mathbf{BY})
\end{aligned}
$$

簡潔にするために，以下のようにおく．

$$
\begin{aligned}
\sigma &= \frac{v}{I(K+\alpha)} \\
\mathbf{R} &= (K+\alpha)\mathbf{A} \\
&= \frac{2\alpha SrP_{in}}{(K+\alpha)^2 v\pi}\mathbf{n}^2\mathbf{\Phi W}
\end{aligned}
$$

よって,

$$
\begin{aligned}
\frac{dtr\{(\mathbf{n}^{-1})^2\mathbf{X}\}}{d\tau} &= \sigma\left[tr\{(\mathbf{n}^{-1})^2\mathbf{Y}\} - tr\{(\mathbf{n}^{-1})^2\mathbf{X}\}\right] \\
\frac{d\mathbf{Y}}{d\tau} &= -\mathbf{nZ}tr\{(\mathbf{n}^{-1})^2\mathbf{X}\} + \mathbf{R}tr\{(\mathbf{n}^{-1})^2\mathbf{X}\}) - \mathbf{Y} \\
\frac{d\mathbf{Z}}{d\tau} &= \mathbf{nY}tr\{(\mathbf{n}^{-1})^2\mathbf{X}\} - \mathbf{Z}
\end{aligned}
$$

ここで $tr\{(\mathbf{n}^{-1})^2\mathbf{X}\} = X$ とおいて，$2N+1$ 次元の式にする．

$$
\begin{aligned}
\frac{dX}{d\tau} &= \sigma\left[tr\{(\mathbf{n}^{-1})^2\mathbf{Y}\} - X\right] && (2.35) \\
\frac{d\mathbf{Y}}{d\tau} &= \mathbf{R}X - \mathbf{nZ}X - \mathbf{Y} && (2.36) \\
\frac{d\mathbf{Z}}{d\tau} &= \mathbf{nY}X - \mathbf{Z} && (2.37)
\end{aligned}
$$

上式でみると連立方程式は $2N^2+1$ 次となるので，非対角成分について記述する．ここで，$i \neq j$ である．

$$
\begin{aligned}
\frac{dY_{ij}}{d\tau} &= R_{ij}X - n_{ij}Z_{ij}X - Y_{ij} \\
\frac{dZ_{ij}}{d\tau} &= n_{ij}Y_{ij}X - Z_{ij}
\end{aligned}
$$

$\mathbf{R}$, $\mathbf{n}$ は対角行列であるので，$R_{ij} = n_{ij} = 0$ となる．

$$
\begin{aligned}
\frac{dY_{ij}}{d\tau} &= -Y_{ij} \\
\frac{dZ_{ij}}{d\tau} &= -Z_{ij}
\end{aligned}
$$

よって，

$$\begin{aligned} Y_{ij} &= e^{-\tau} \\ Z_{ij} &= e^{-\tau} \end{aligned}$$

これより，$\tau \to \infty$，つまり，十分時間が経過すれば，$\mathbf{Y}$，$\mathbf{Z}$ の非対角成分は消滅する．

$N = 1$ のとき，この連立方程式は以下の構造をとる．

$$\begin{aligned} \frac{dX}{d\tau} &= \sigma(Y_1 - X) \\ \frac{dY_1}{d\tau} &= R_1 X - Z_1 X - Y_1 \\ \frac{dZ_1}{d\tau} &= Y_1 X - Z_1 \end{aligned}$$

これは，ガスタービンの運動方程式が $N = 1$ の場合，$b = 1$ の Lorenz 方程式と等価であることを意味する．これから，ガスタービンの運動方程式は $2N + 1$ 次元まで拡張された Lorenz 方程式であることがわかり，カオス運動を起こすと推測できる．実際，次節で数値計算結果と共に示すが，この拡張された Lorenz 方程式はカオスを生成する．

式 (2.35)-(2.37) には注目すべき特徴がある．それは，図 2.5 のように，N 個の Lorenz 系が X を中心ノードとした星型ネットワーク構造を構築している点にある．この星型ネットワーク構造により，カオスガスタービンの運動方程式の無次元化式は，任意の Lorenz 系を加算的に拡張できる．加算的拡張の性質により，カオスガスタービンの運動方程式の無次元化式を拡張 Lorenz 方程式と呼称する．詳細は第 3 章で示すが，星型ネットワーク構造により，拡張 Lorenz 方程式は Lorenz 方程式の動的性質を引き継いでいる．Lorenz 方程式の拡張版に関する先行研究は [67, 68] であるが，先行研究で報告されている Lorenz 方程式の拡張版は本研究で発見された方程式とは全く異なる．

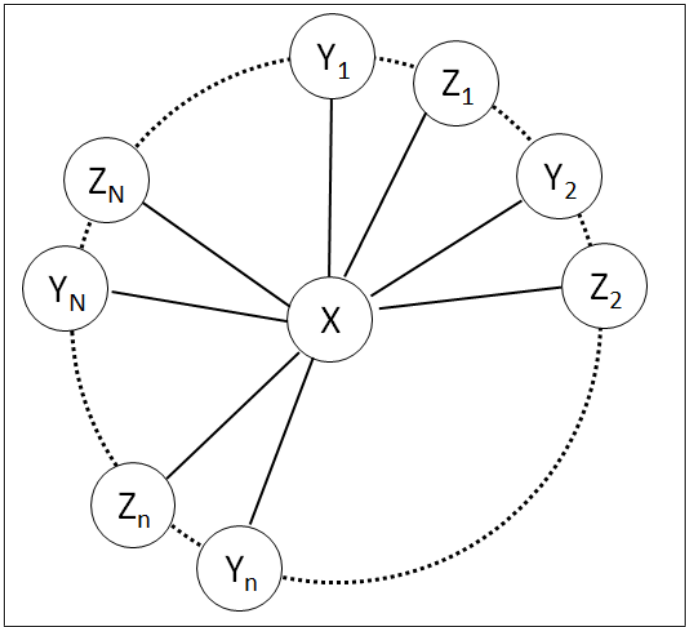

図 2.5: 拡張 Lorenz 方程式の星型ネットワーク構造

2.2 実験

2.2.1 実機実験

カオスガスタービンのロータの角速度 $\omega(t)$ を計測することで，本研究で設計したカオスガスタービンが不規則に反転運動を繰り返すことを実験的に確認する．ロータの角速度 $\omega(t)$ を計測するために，ロータの回転を動画として記録し，角速度 $\omega(t)$ の時間変化を動画から計算した．サンプリング時間は $33[ms]$ であり，ロータにつけたマークを追跡することで，$33[ms]$ に移動した角度を求め，それをサンプリング時間で割ることで角速度 $\omega(t)$ を見積もる．

図 2.6 は，実際に測定した角速度 $\omega(t)$ の時間変化のグラフである．ここで，給気圧は $20-25[kPa]$，気体軸受のスラスト圧は $2.0-2.4[kPa]$ に設定している．角速度 $\omega(t)$ の正負は回転方向を表しており，角速度 $\omega(t)$ が正の時は，ロータが反時計回りに回転していることを示し，角速度 $\omega(t)$ が負の時は，ロータが時計回りに回転していることを意味する．

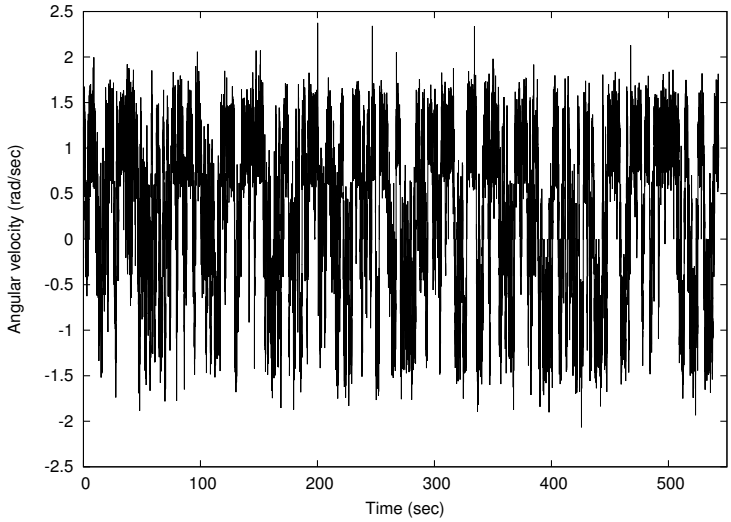

図 2.6: カオスガスタービンの角速度の実測結果

図 2.7 は，カオスガスタービンの角速度 $\omega(t)$ の実測結果の自己相関関数である．時差が $6[s]$ になるまでの間に，自己相関関数が急速に 0 に減少する．自己相関関数にピークが見られないことから，カオスガスタービンの角速度 $\omega(t)$ の実測結果はカオスの特徴を有していると言える．

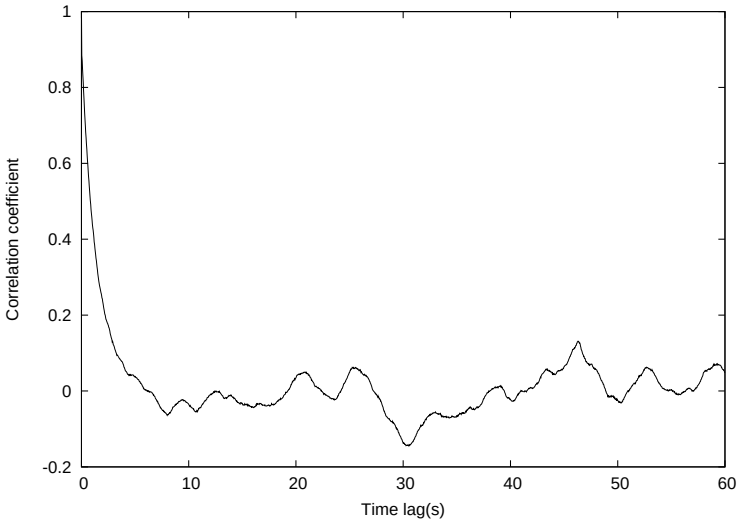

図 2.7: カオスガスタービンの角速度の自己相関関数 (実測結果)

2.2.2 カオスガスタービンの運動方程式の数値実験

実機実験に対応する数値データを得るために，式 (2.20)-(2.22) を 4 次の Runge-Kutta 法で数値積分した．積分時間間隔は $0.01[s]$ である．本研究で設計した実験環境では流路で圧力損失が出てしまうため，正確な給気圧力が測定できない．そのため，給気圧力 P_{in} を $20[kPa]$ に設定した．残りのパラメータは，$N = 100, v = 1.5 \times 10^{-5}[kgm^2/s], \phi = 0.36[rad], S = 2.0 \times 10^{-5}[m^2], r_c = 0.015[m], I = 1.5 \times 10^{-5}[kgm^2], K = 0.02[s^{-1}], \alpha = 0.02[s^{-1}]$ とした．これらは $\sigma = 25, R_0 = 3185$ に相当する．数値積分で使用する初期条件は $\omega(0) = 0$，$a_n(0), b_n(0)$ は平均 0，分散 1 の乱数で与えられる．数値解のうち，最初の 10 000 点を排除することで，初期条件からカオスに至るまでの非定常部分を排除した．図 2.8 は，上述した条件で数値積分を行った結果である．なお，v, α, K の正確な値を見積もる手段がないため，これらの値は角速度 $\omega(t)$ の計算値が実際値と一致するような条件の値を採用している．

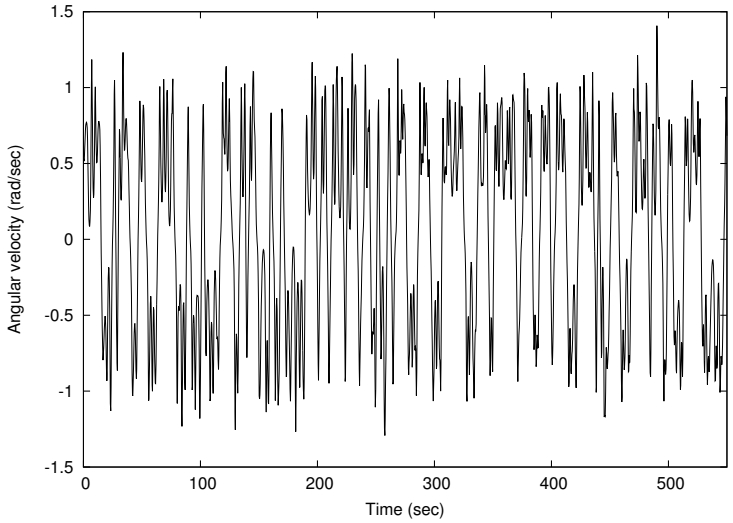

図 2.8: カオスガスタービンの角速度の数値計算結果 (N=100)

図 2.9 は，カオスガスタービンの運動方程式の角速度 $\omega(t)$ の計算結果の自己相関関数である．時差が $6[s]$ になるまでの間に，自己相関関数が急速に 0 に減少する．また，自己相関関数にピークが見られないことから，カオスガスタービン運動方程式の角速度 $\omega(t)$ の計算結果もカオスの特徴を有している．

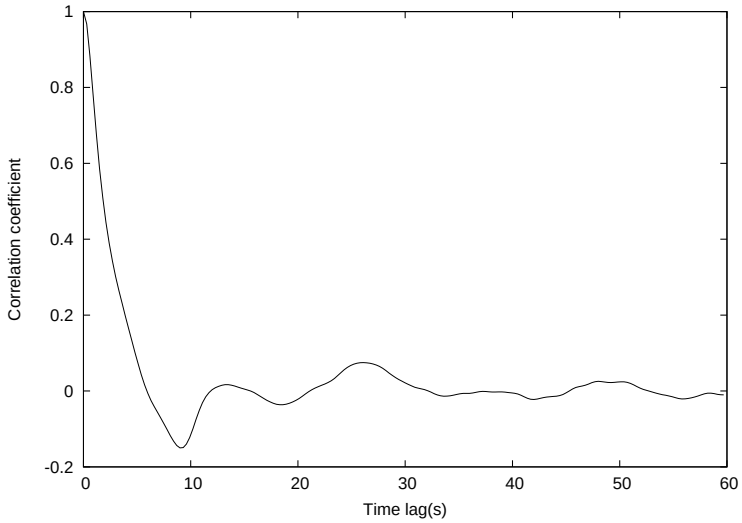

図 2.9: カオスガスタービンの角速度の自己相関関数（数値計算結果）

カオスガスタービンの運動方程式がどのような動的性質を持っているのか解析するために，大きな値 $N = 1000$ に設定して，その動的性質を見積もった．N の変更に伴い，積分時間間隔は $1.0 \times 10^{-4}[s]$ に変更したが，それ以外のパラメータは上述した条件と同一である．図 2.10-図 2.12 は，それぞれ，各 n での ω, a_n, b_n の時間変化を示したグラフである．

次に，カオスガスタービンの運動方程式はカオスアトラクタを形成することを示す．図 2.13-図 2.14 は，それぞれ，ω, a_n, b_n の 3 次元プロットと，a_n, b_n の 2 次元プロットである．

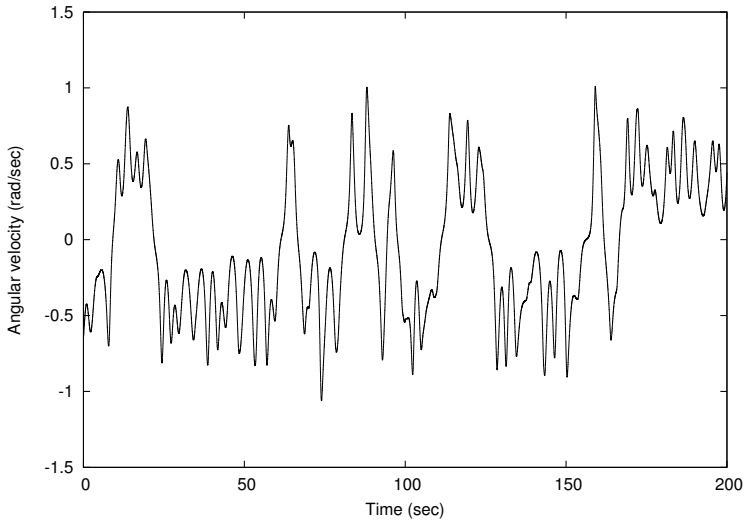

図 2.10: カオスガスタービンの角速度の数値計算結果 (N=1000)

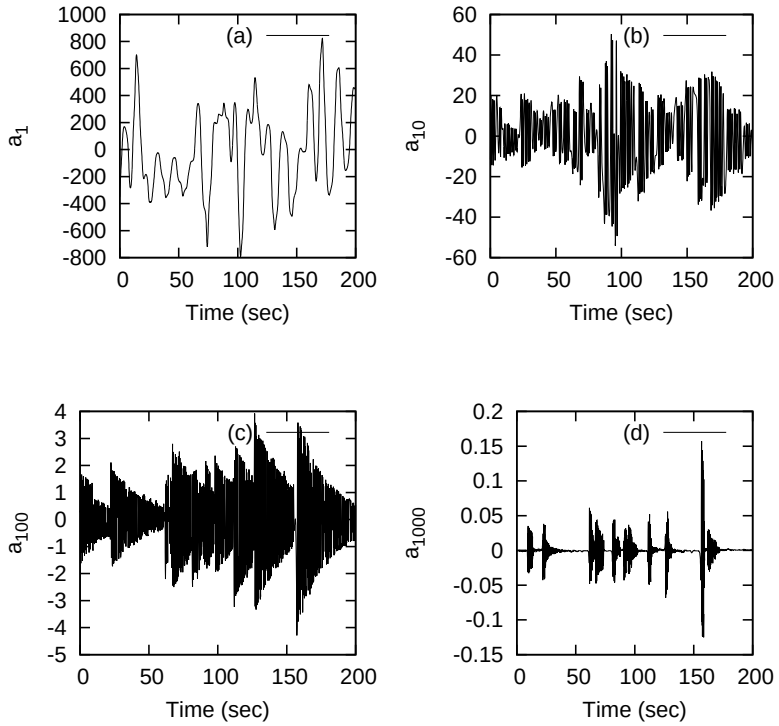

図 2.11: カオスガスタービンの a_n の数値計算結果 (N=1000)

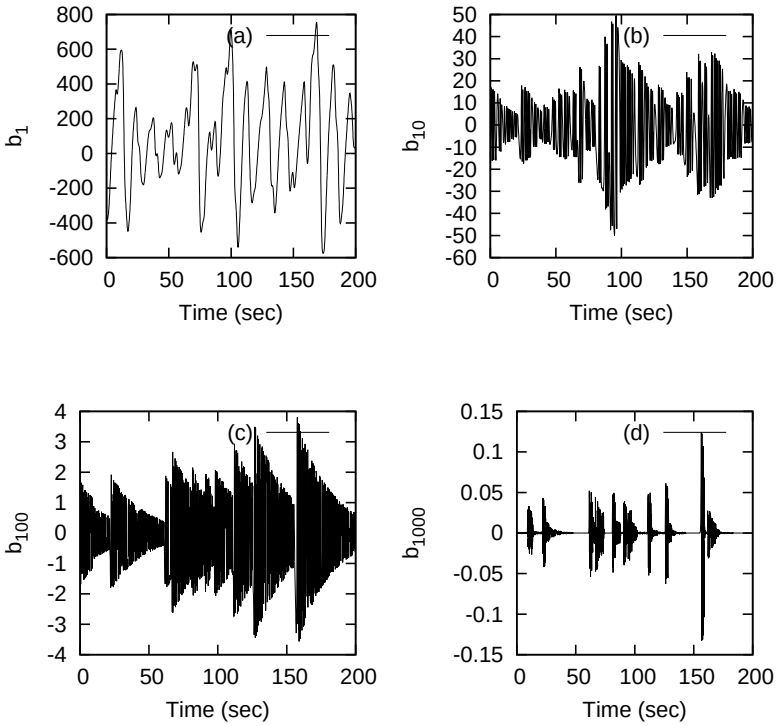

図 2.12: カオスガスタービンの b_n の数値計算結果 (N=1000)

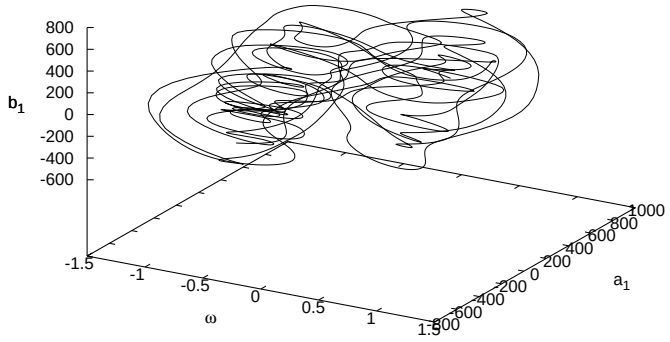

図 2.13: $\omega - a_1 - b_1$ の 3 次元プロット (N=1000)

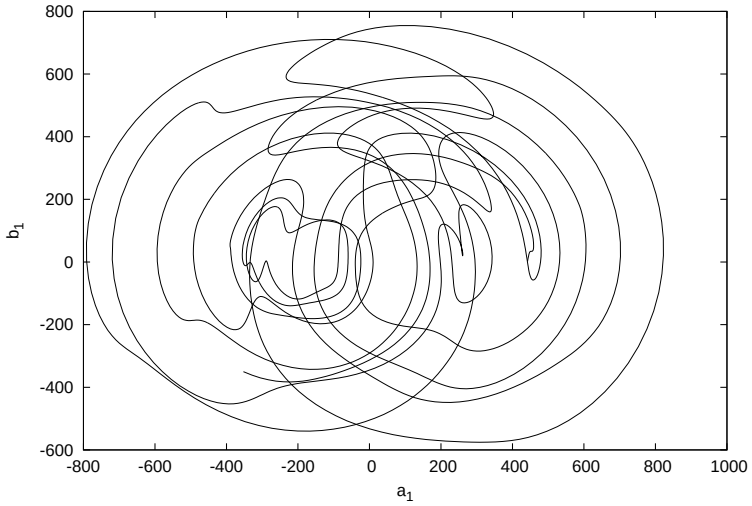

図 2.14: $a_1 - b_1$ の 2 次元プロット (N=1000)

2.2.3 拡張 Lorenz 方程式の数値実験

カオスガスタービンの運動方程式の無次元化式である拡張 Lorenz 方程式の動的性質を解析するために，式 (2.35)-(2.37) を 4 次の Runge-Kutta 法で数値積分した．積分時間間隔は 4.0×10^{-5} としたが，それ以外のパラメータ σ, ϕ は，運動方程式のパラメータと同じ，$\sigma = 25, \phi = 0.36[rad]$ である．N は 10，100，1000 の 3 通りに設定する．数値解のうち最初の 250 000 点を排除することで，初期条件からカオスに至るまでの非定常部分を排除した．

まず，X, Y_n, Z_n の動的性質を示す．ここでは，$R_0 = 3185, N = 1000$ に設定している．図 2.15-図 2.17 は，それぞれ，X, Y_n, Z_n の時間変化である．図 2.16(a)-2.16(d) は，それぞれ，$Y_1, Y_{10}, Y_{100}, Y_{1000}$ の時間依存性，図 2.17(a)-2.17(d) は，それぞれ，$Z_1, Z_{10}, Z_{100}, Z_{1000}$ の時間依存性である．Y_1, Z_1 の不規則な振動は，Prandtl 数が 10，$b = 8/3$，換算 Rayleigh 数が 24.74 以上の Lorenz モデルのようなカオス挙動を示している．$n > 1$ の Y_n, Z_n でも不規則な振動は観測できるが，Y_1, Z_1 の場合とは異なり，振動の間欠性が認められる．この傾向は n が大きくなればなるほど顕著になる．Y_{1000}, Z_{1000} では，大きな振幅の振動 (バースト部) と小さな振幅の振動 (ラミナー部) が存在している．これらの動的性質は，Manneville と Pomeau が Lorenz 方程式の数値解析により発見した間欠カオス [69, 70] と類似する．

拡張 Lorenz 方程式もカオスアトラクタを生成することを示す．図 2.18 と図 2.19 は，それぞれ，X, Y_1, Z_1 の 3 次元プロットと，Y_1, Z_1 の 2 次元プロットである．図 2.18 と図 2.19 では，Lorenz アトラクタ特有のダブルスクロール構造が維持されている．カオスガスタービンの運動方程式の数値積分結果とその無次元化式の数値積分結果は，無次元化の効果でそのスケールこそ違うものの，$n > 1$ の Y_n, Z_n が間欠性を示すことや，同じアトラクタの構造を有するなど，同じ動的性質を示す．以上の事実から，拡張 Lorenz 方程式はカオスガスタービンの運動方程式を正確に無次元化できている．

拡張 Lorenz 方程式の分岐特性を示す．図 2.20 は，X の極大点と極小点を分岐パラメータ R_0 に対してプロットしたものである．計算時間短縮のために，ここでは，$N = 10$，積分時間間隔を 4.0×10^{-3} に変更している．拡張 Lorenz 方程式の分岐構造は，カオスを生成する換算 Rayleigh 数に違いがあるものの，Lorenz 方程式の分岐構造と類似する．

様々な N における X のパワースペクトル密度を示す．図 2.21 は $N = 10, 100, 1000$ におけるパワースペクトル密度で，計算に使ったパラメータ R_0 は $R_0 = 3185$ に固定される．パワースペクトル密度は，広い周波数領域に分布する．これはカオス特有の特性である．また，N が増加するにつれ，パワースペクトル密度は高周波域に発展する．これは，n が大きいほど Y_n, Z_n がより速く振動することを意味する．これらの速い振動が X に組み込まれ，結果として，X の振る舞いを複雑にするのであろう．

[18] に従って，各 R_0 における X の Reversal factor を見積もった．Reversal factor は，X の符号が正になる時間の合計と負になる時間の合計の比に対して，常用対数をとったものである．Reversal factor=0 になることは，ロータが時計回りと反時計回りのどちらにも等確率で回転することを意味する．図 2.22 にその結果を示す．図 2.22 から，Reversal factor は R_0 が 1500 から 1600 の間で急速に減衰し，$R_0 > 1600$ で 0 に漸近することがわかる．

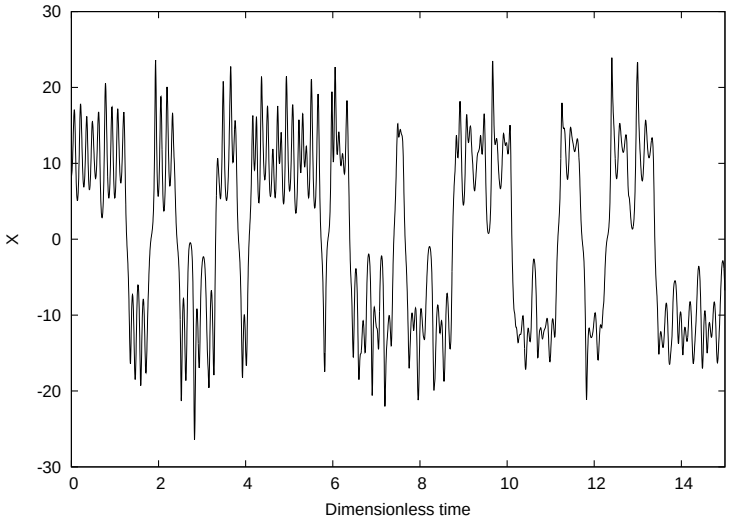

図 2.15: 拡張 Lorenz 方程式の数値計算結果 (N=1000)

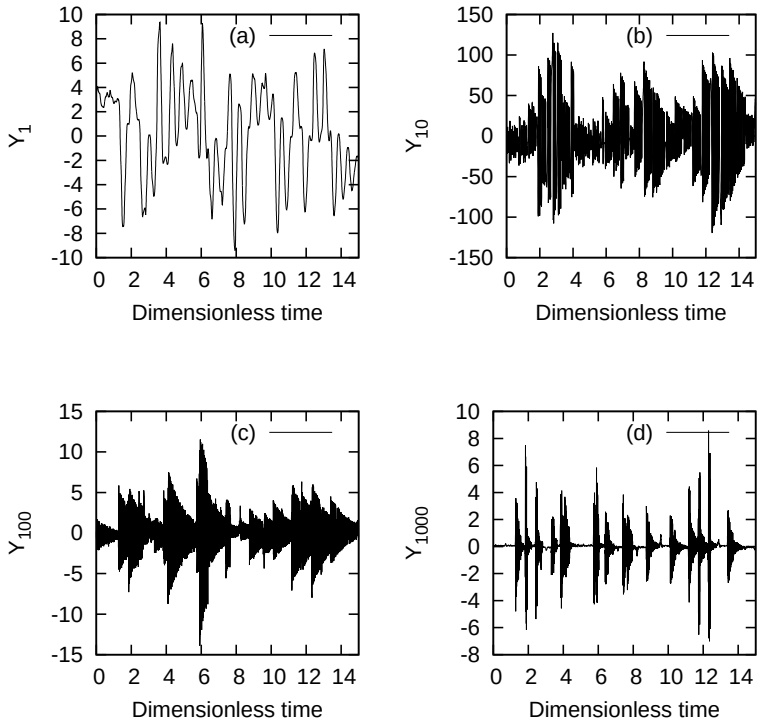

図 2.16: 拡張 Lorenz 方程式の Y_n の数値計算結果 (N=1000)

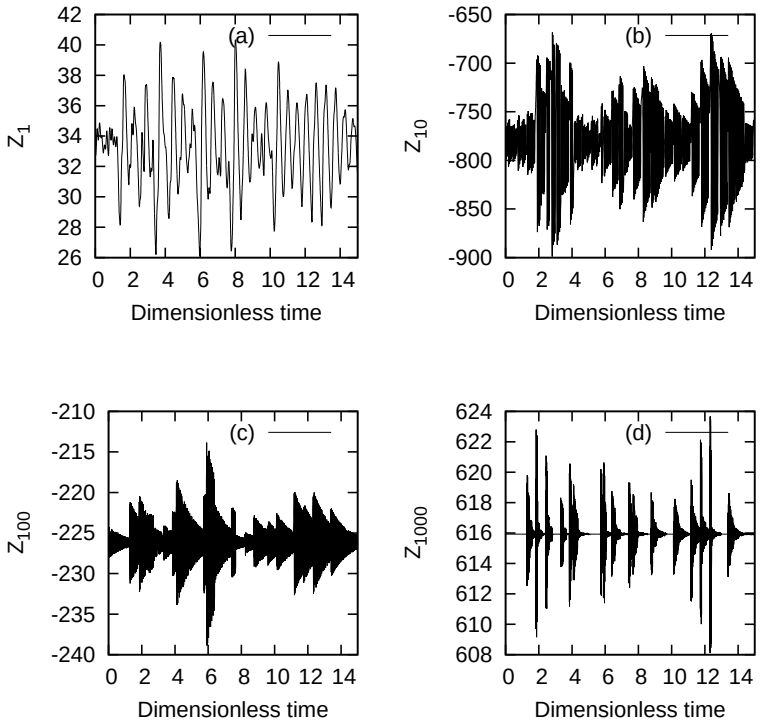

図 2.17: 拡張 Lorenz 方程式の Z_n の数値計算結果 (N=1000)

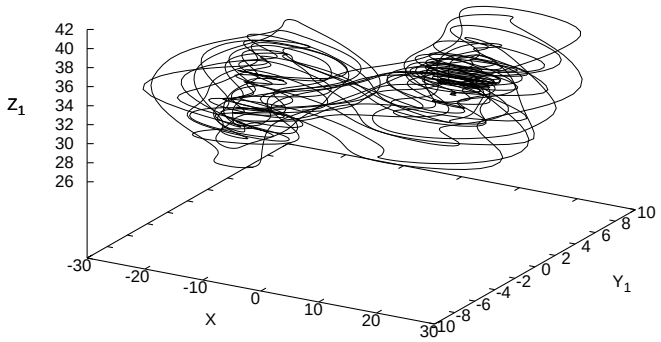

図 2.18: $X - Y_1 - Z_1$ の 3 次元プロット (N=1000)

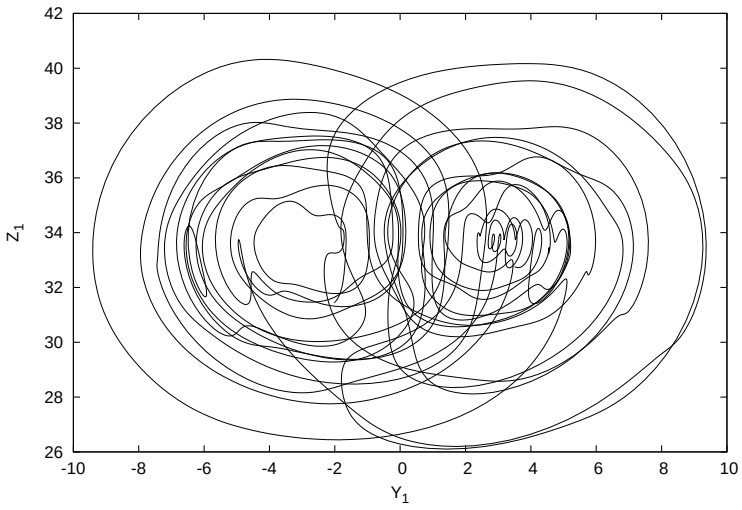

図 2.19: $Y_1 - Z_1$ の 2 次元プロット (N=1000)

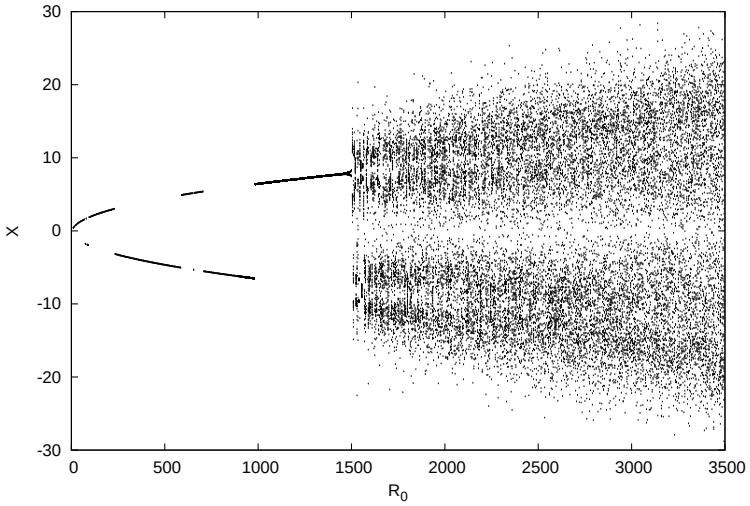

図 2.20: 各 R_0 での X の動的性質 (N=10)

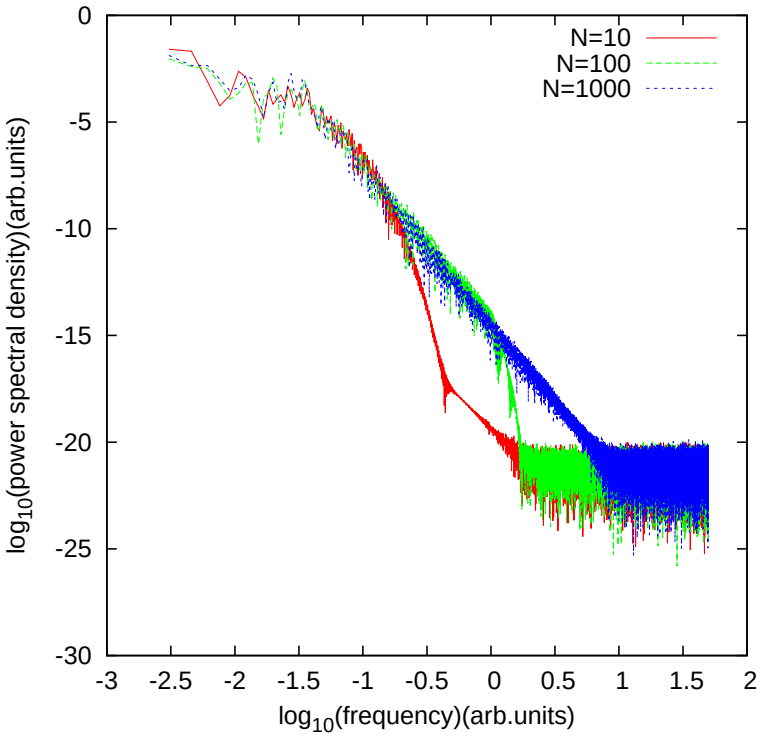

図 2.21: 様々な N における X のパワースペクトル密度

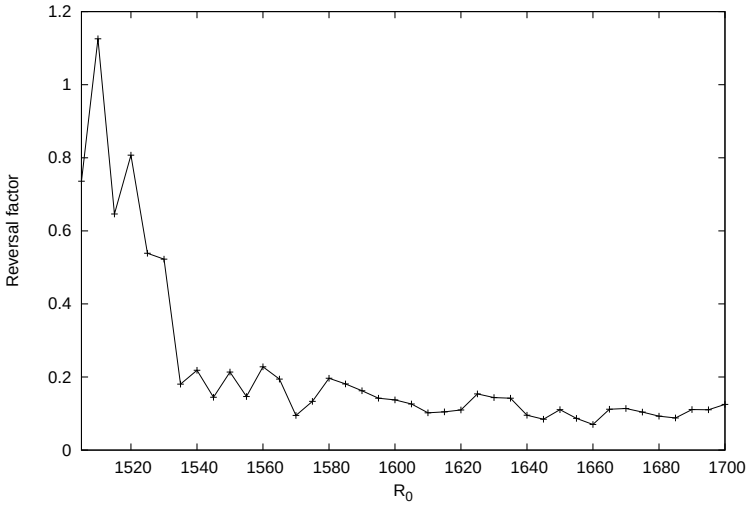

図 2.22: 各 R_0 での Reversal factor(N=10)

2.3 統計解析

文献 [18] において，Sreenivasan らは，平均風の速度データを使用し，速度データの統計的性質を調べている．本論文では，ロータの角速度 $\omega(t)$ の測定データ，及び，計算データを用いて，同様の統計解析を行う．

2.3.1 カオスガスタービンの統計的性質

カオスガスタービンのロータの回転方向が変わった瞬間から再び回転方向を変えるまでの時間間隔（スイッチインターバル）を測定し，反転回数と対応するスイッチインターバルを用いて，カオスガスタービンの統計的性質を明らかにする．この節では，図 2.6 で示した測定したロータの角速度 $\omega(t)$ のデータを用いる．

まず，反転回数-ロータの総回転時間のグラフを求める．図 2.23 がロータの角速度のデータから求めた反転回数-ロータの総回転時間のグラフである．図 2.23 における n はロータが回転方向を変えた回数であり，T_n はロータの総回転時間である．図 2.24 は図 2.23 の線形近似線 $T_n = \omega_1 n + \omega_0$ からの偏差を示している。ここで，ω_0, ω_1 は定数である．

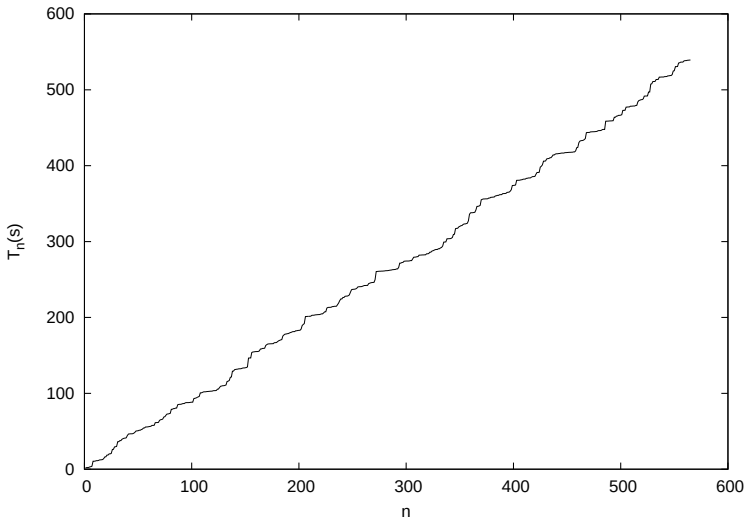

図 2.23: 反転回数-ロータの総回転時間

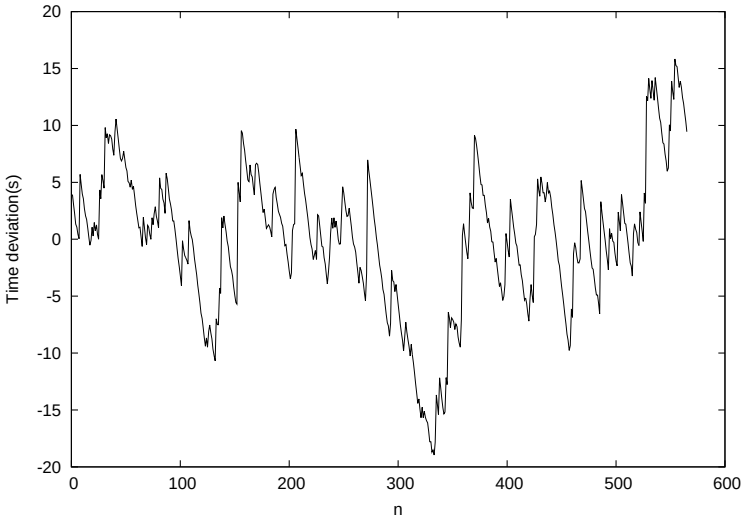

図 2.24: 反転回数-ロータの総回転時間の線形偏差

図 2.25 は図 2.24 で求めた T_n の偏差のパワースペクトル密度である．パワースペクトル密度の傾斜は -1.92 となっており，これは Sreenivasan らの報告 -1.94(文献 [18] 中の Fig.4) に近い．

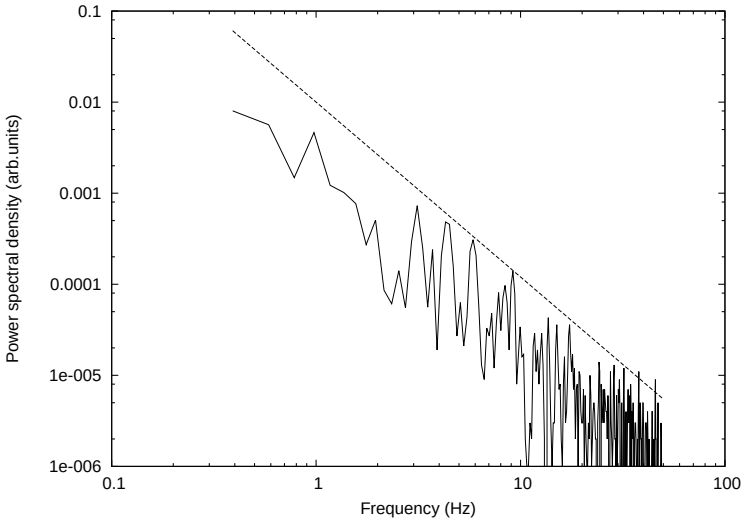

図 2.25: T_n の偏差のパワースペクトル密度

次に，T_n の確率密度分布を見積もる．そのために，n 回目と $n+1$ 回目間の反転スイッチインターバル t_1 を $t_1 = T_{n+1} - T_n$ と定義する．図 2.26 は各 t_1 での確率密度分布 $P(t_1)$ を示したものである．図 2.26 の確率密度分布の傾きは -1.5 と求められる．

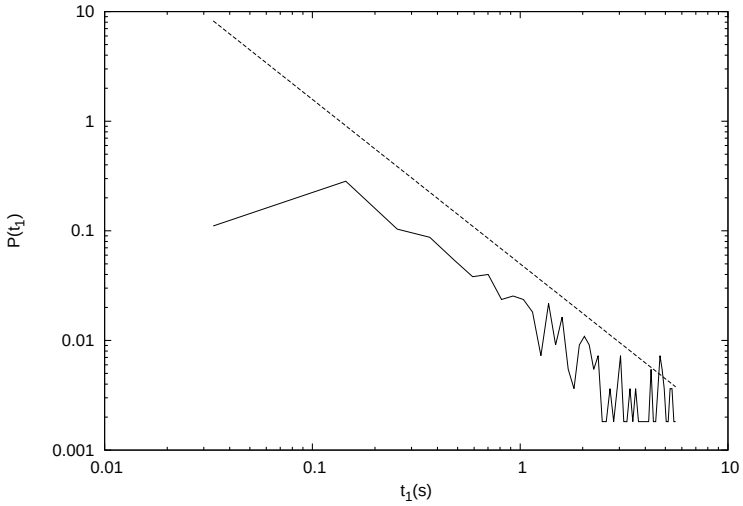

図 2.26: T_n の確率密度分布

最後に，カオスガスタービンの実測結果の統計モーメントを求めた．横軸に $log_{10}(r)$，縦軸に $log_{10} < |Tn + r - Tn|^q > (q = 1 - 6)$ をとり，プロットしたのが，図 2.27 である．ここで，$Tn + r - Tn$ は最初に反転してから r 回反転するまでの時間間隔である。$< \cdot >$ は 10 セットのサンプルに関する平均値を意味する．

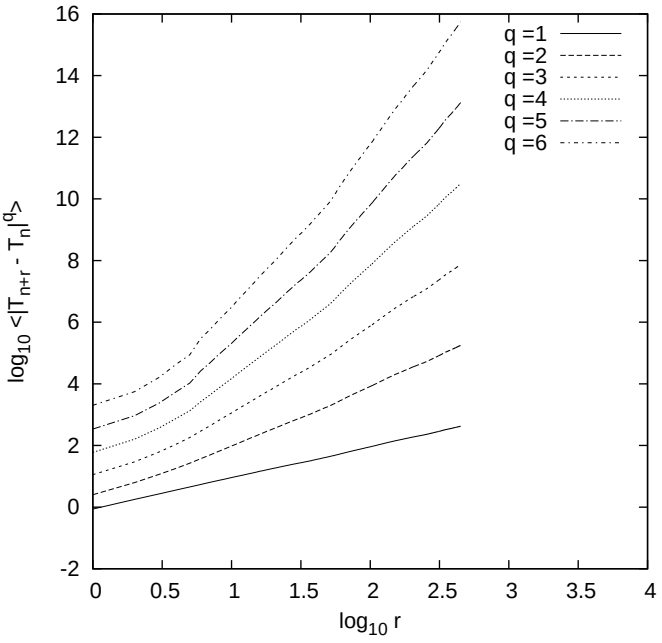

図 2.27: 実測データの $log_{10}(r) - log_{10}\langle|Tn + r - Tn|^q\rangle$

2.3.2 運動方程式の統計的性質

図 2.8 で示した運動方程式から求めたロータの角速度 $\omega(t)$ のデータを元に，スイッチインターバルを測定し，前節と同様の方法で，カオスガスタービンの統計的性質を明らかにしていく．

前節と同様に，反転回数-ロータの総回転時間のグラフを求め，線形近似線 $T_n = \omega_1 n + \omega_0$ から偏差を見積もる。ω_0, ω_1 は定数である．図 2.28 は前節の図 2.23 と対応し，図 2.29 は図 2.24 と対応する．

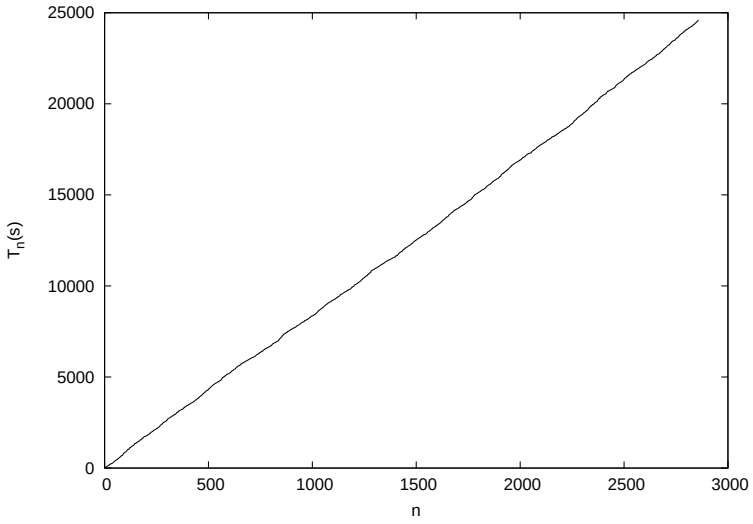

図 2.28: 反転回数-ロータの総回転時間

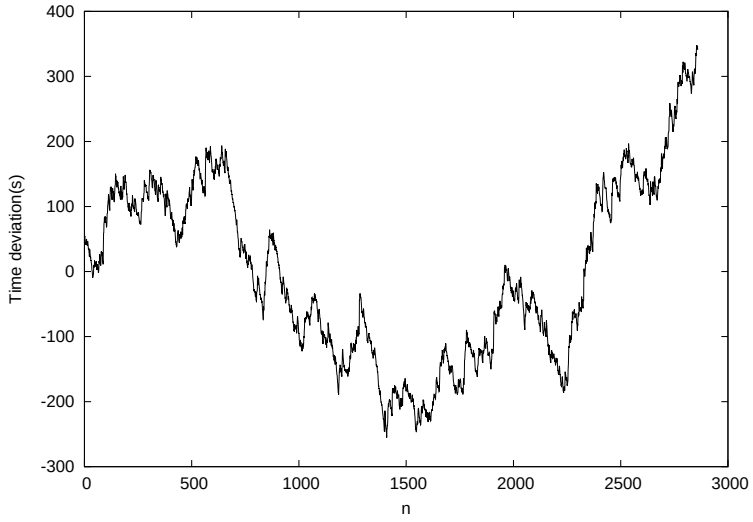

図 2.29: 反転回数-ロータの総回転時間の線形偏差

図 2.30 は図 2.25 と対応するパワースペクトル密度のグラフである．パワースペクトル密

度の傾斜は −1.92 となっており，これも Sreenivasan らの報告 −1.94(文献 [18] 中の Fig.4) に近い．

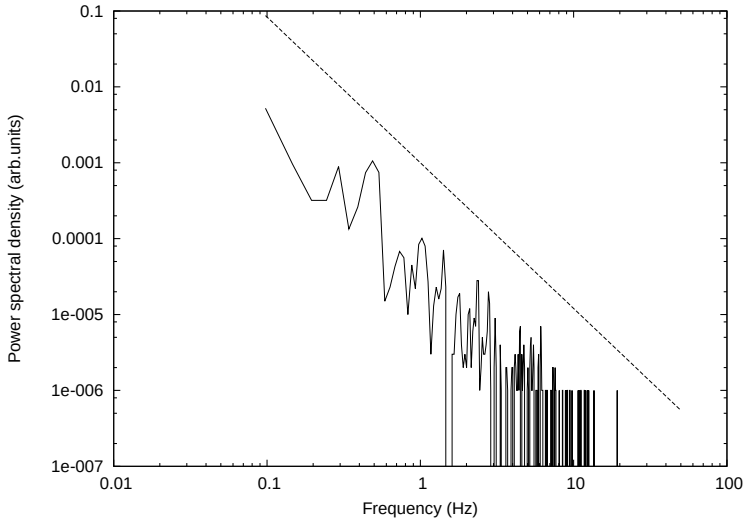

図 2.30: T_n の偏差のパワースペクトル密度

前節と同様に，n 回目と $n+1$ 回目間の反転スイッチインターバル t_1 を $t_1 = T_{n+1} - T_n$ と定義し，T_n の確率密度分布を見積もる．図 2.31 では各 t_1 での確率密度分布 $P(t_1)$ を示した．図 2.31 の確率密度分布の傾きは，実測結果に近い −1.6 となっている．

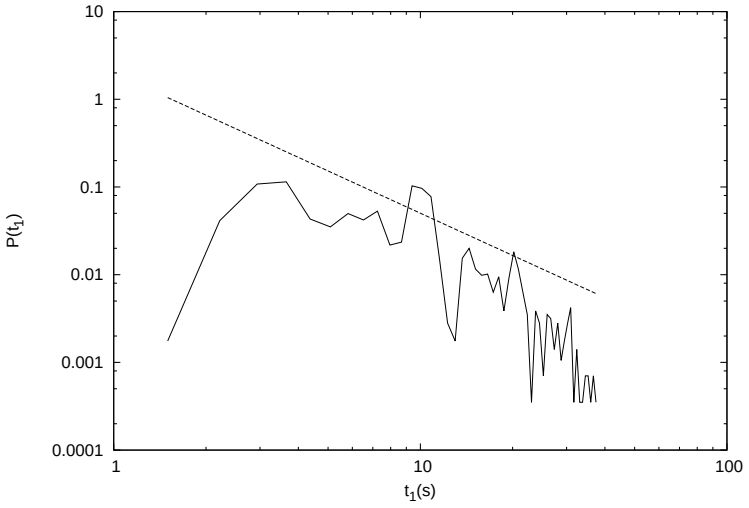

図 2.31: T_n の確率密度分布

最後に，カオスガスタービンの運動方程式より求めた $\omega(t)$ の統計モーメントを求めた．横軸に $log_{10}(r)$，縦軸に $log_{10} < |Tn + r - Tn|^q >$ (q=1-6) をとり，プロットしたのが，図 2.32 である．

ロータの角速度の実測結果と数値実験結果に関する統計解析結果は，ほぼ一致する．この事実は，式 (2.20)-(2.22) の運動方程式が，カオスガスタービンの回転運動を支配するメカニズムをよく表現していることを示している．

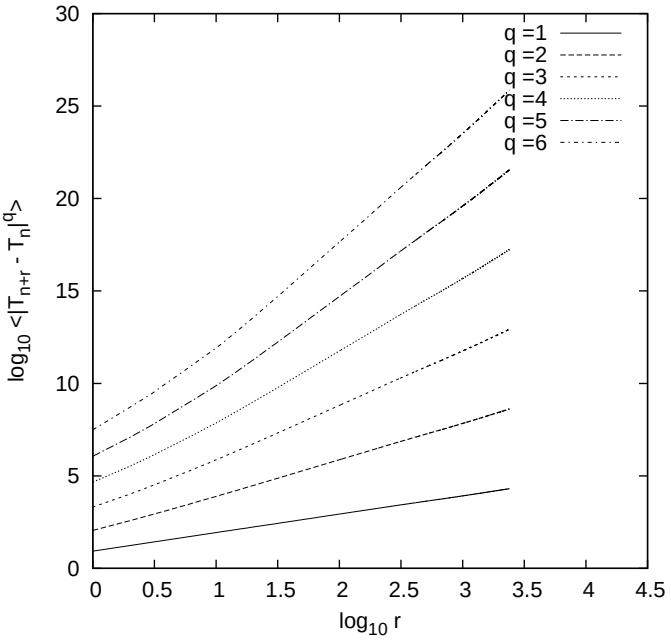

図 2.32: 計算データの $log_{10}(r) - log_{10}\langle|Tn + r - Tn|^q\rangle$

2.4 考察

カオスガスタービンは Rayleigh-Bénard 対流の駆動力を機械的に再現するように設計され，カオスガスタービンの運動方程式はその動力学的性質を十分に表現している．運動方程式の無次元化式である拡張 Lorenz 方程式は，Rayleigh-Bénard 対流のいくつかの物理的側面，つまり，換算 Rayleigh 数 (R_0)，Prandtl 数 (σ)，対流のアスペクト比の関数としてのパラメータ (b) を組み込んでいる．拡張 Lorenz 方程式における対流のアスペクト比の関数としてのパラメータ (b) は 1 である．これにより，対流のアスペクト比が $\Gamma = \sqrt{3}$, つまり，$\Gamma \sim O(1)$ となる．前節で示した統計解析は，カオスガスタービンの運動方程式がロータの角速度の時間変化だけでなく，その統計的性質も再現できることを示している．特に，角速度をロータ半径でかけた時，その物理次元は Rayleigh-Bénard 対流の速度場と一致する．著者が角速度から見積もったパワースペクトル密度，確率密度分布，統計モーメントは，[18] に記載されている乱流状態での Rayleigh-Bénard 対流における平均風の速度場で見積もった統計解析結果と類似する．著者は反転傾向の偏りを図 2.22 として見積もった．図 2.22 は R_0 がしきい値を超えた時，タービンのロータの回転方向に偏りがないことを意味する．しきい値の Rayleigh 数のオーダーが違うものの，この性質は平均風の不規則な反転運動の傾向と類似する．

これらの所見が拡張 Lorenz 方程式が $\Gamma \sim O(1)$ となる乱流時の平均風の力学モデルとして妥当かどうか考察する．第 1 章で述べたように，拡張 Lorenz モデルは休止-反転シナリオの説明や Araujo らが提案した修正版の Lorenz モデル [24] との比較ができるであろう．彼らのモデルにおいて，平均風は境界層から発生した plume によって起こる 2 次元対流である．plume は浮力と粘性抵抗のバランスによって動く．修正版の Lorenz モデルと拡張 Lorenz モデルの主な考え方はほぼ同じである．それにもかかわらず，修正版の Lorenz モデルと拡張 Lorenz モデルの間には，拡張 Lorenz モデルにおける $2N+1 (N \to \infty)$ 個の独立変数が星型ネットワーク構造を形成するという相違点がある．この相違点は抗力の働く範囲が $\pm\phi$ に限定されていることに起因する．これにより，拡張 Lorenz モデルの X の時間変動は，図 2.15 のように，実際の平均風における速度場の特徴をより正確に再現できるようになった．$N = 1$ のとき，拡張 Lorenz モデルは $b = 1$ の Lorenz モデルと正確に一致する．そのため，拡張 Lorenz モデルは Lorenz モデルの動的性質を継承していると仮定できる．この仮定により，拡張 Lorenz モデルの $\mathbf{Y}$ と $\mathbf{Z}$ は，Lorenz モデルの Y, Z と同様に Rayleigh-Bénard 対流の温度場の特性を示すと予想される．しかしながら，この憶測の証明はなされていない．

ロータの回転運動が平均風を再現していると仮定すると，Reynolds 数 (R_1) を導くことができる．計算に使用する代表長さ L と流速 U は，それぞれロータの直径 d_r とロータの速度 $\Omega \times (d_r/2)$ と等しいと仮定する．ここで，ロータの代表角速度 Ω は図 2.6 より，$\Omega = 1.5$ $[rad/s]$ とした．Prandtl 数は $\sigma = v/\left[I(K+\alpha)\right]$ と仮定する．ロータの慣性モーメント I は $I = (M/2)(d_r/2)^2$ として近似する．次に，物理次元から動粘性係数を導く．動粘性係数の物理次元は $[m^2/s]$ であるから，$\nu \propto v/M$ とできる．従って，ν は下式のように書ける．

$$\nu = c_\nu \frac{v}{M} \tag{2.38}$$

ここで，c_ν は正の定数である．R_1 をガスタービンの機械パラメータで表現すると，

$$R_1 = \frac{UL}{\nu} = \frac{M\Omega d_r^2}{2c_\nu v} \tag{2.39}$$

しかしながら，式 (2.39) では，c_ν がわからないため，R_1 を計算することができない．c_ν を決定するために，Niemela らが実験的に求めた Reynolds 数（Re），Prandtl 数 (Pr)，Rayleigh 数 (Ra) の関係 [19] を利用することができる．

$$Re = f(\Gamma) Pr^{-0.7} Ra^{0.49} \tag{2.40}$$

ここで，$f(\Gamma) = 0.2$ かつ $\Gamma \sim O(1)$ である．臨界 Rayleigh 数は 1708 で与えられるため，拡張 Lorenz モデルの Ra は $Ra = 1708 \times R_0 \approx 5.4 \times 10^6$ となる．ここで，$R_0 = 3185$ とした．同様に，Pr は $Pr = \sigma = 25$ とする．こうして，式 (2.40) より，Re を $Re \approx 42$ と見積もられる．これらの結果は，ロータの動きが $Ra = 5.4 \times 10^6$，$Pr = 25$，$Re = 42$ の対流を再現していることを示している．また，式 (2.39) より，$c_\nu = 1/7$ が導かれる．

次に，X の不規則な反転運動を支配するメカニズムを考察する．乱流時の平均風の不規則な反転運動のメカニズムは Sreenivasan らによって報告されている [18]．また，それとは異なるメカニズムは Benzi によって報告されている [23]．これらの報告を参考に，拡張 Lorenz モデルを使って，X の不規則な反転運動が確率共鳴によるものだということを示せる．

図 2.21 の結果は，Lorenz 系の数 N の増加によって，拡張 Lorenz モデルの X が高速に振動していることを示している．これは，より大きな n の Y_n, Z_n がそれぞれ，直接的，間接的に X の振動の高周波数領域に影響を与えることを意味する．何故ならば，X の時間発展を支配する式 (2.35) に，対角和として Y_n が含まれているからである．図 2.16 と図 2.17 で示された結果は，X の振動が，$Y_n (n \sim O(10^0)$ から $O(10^1))$ で与えられる速い振動場と，$Y_n (n \sim O(10^2)$ から $O(10^3))$ で与えられるより速い振動場に誘発されると考えられる．速い振動場を η_1，より速い振動場を η_2 とする．図 2.21 の結果から，η_1 の寄与は η_2 のそれよりも大きい．Landau と Kapitsa による急激に振動するポテンシャル場における振動子の理論 [71] に上に述べた考察を適用して，以下のような振動モデルを構築した．振動する粒子の力学モデルは η_1 を使って，

$$\ddot{u} = -\frac{\partial V}{\partial u} + \eta_1 \tag{2.41}$$

ここで，u は平衡位置からの変位であり，$\dot{u} \sim X$，V はポテンシャルである．$u(t)$ は $u(t) = \bar{u}(t) + \xi(t)$ と定義する．ξ は遅い変動 $\bar{u}$ 周りの速い振動であり，t は無次元時間である．

η_1 を以下のように仮定する．

$$\eta_1(u,t) = \omega_c(u) cos(ft) + \omega_s(u) sin(ft) \tag{2.42}$$

ここで，f は Y_n における速い振動の角振動数を表し，$\omega_c(u)$ と $\omega_s(u)$ は u の関数，そして，$f \gg f_0$ である．f_0 は $\ddot{u} = -\partial V/\partial u$ に従う振動の角振動数である．$u(t) = \bar{u}(t) + \xi(t)$ より，式 (2.41) は以下のようになる．

$$\ddot{\bar{u}} + \ddot{\xi} = -\frac{dV}{d\bar{u}} - \xi\frac{d^2V}{d\bar{u}^2} + \eta_1(\bar{u}, t) + \xi\frac{\partial\eta_1}{\partial\bar{u}} + \frac{1}{2}\xi^2\frac{\partial^2\eta_1}{\partial\bar{u}^2} \tag{2.43}$$

式 (2.43) の右辺は 2 次の Taylor 展開まで加えている．この方程式には速い振動を表す項と遅い振動を表す項とが含まれている．それらは別々に等式を形作っているはずである．従って，速い振動項は式 (2.44) のように分離できる．

$$\ddot{\xi} = \eta_1(\bar{u}, t) \tag{2.44}$$

残りの項には，微小な ξ がかかっていて，$\ddot{\xi}$ に比べて小さい．式 (2.42) の関数 η_1 をとり，$\bar{u}$ を定数とみなして，式 (2.44) を積分すると式 (2.45) を得る．

$$\xi = -\frac{\eta_1}{f^2} \tag{2.45}$$

次に，式 (2.43) を時間的に平均する．η_1, ξ について 1 次の量の平均値は 0 になるから次式を得る．

$$\begin{aligned} \ddot{\bar{u}} &= -\frac{\partial V}{\partial\bar{u}} - \frac{1}{f^2}\left\langle \eta_1\frac{\partial\eta_1}{\partial\bar{u}}\right\rangle + \frac{1}{2}\left(\frac{1}{f^2}\right)^2\left\langle \eta_1^2\frac{\partial^2\eta_1}{\partial\bar{u}}\right\rangle \\ &= -\frac{\partial V_{eff}}{\partial\bar{u}} \end{aligned} \tag{2.46}$$

$< \cdot >$ は 0 から $2\pi/f$ までの時間平均を表しており，V_{eff} は有効ポテンシャルエネルギーである．

モデルの非線形性を確かめるために，2 次の項を以下のように近似した．

$$\left\langle \eta_1^2\frac{\partial^2\eta_1}{\partial\bar{u}^2}\right\rangle \approx \frac{\partial}{\partial\bar{u}}\left\langle \eta_1^4\right\rangle \tag{2.47}$$

ここで，

$$\begin{aligned} \frac{1}{f^2}\left\langle \eta_1\frac{\partial\eta_1}{\partial\bar{u}}\right\rangle &= \frac{\partial}{\partial\bar{u}}\frac{1}{2}\frac{1}{f^2}\left\langle \eta_1^2\right\rangle \\ &= \frac{\partial}{\partial\bar{u}}\frac{1}{4f^2}(\omega_c^2 + \omega_s^2). \end{aligned}$$

$\dot{\xi} = 1/f(\omega_c(u)sin(ft) + \omega_s(u)cos(ft))$ だから，

$$\left\langle \dot{\xi}^2\right\rangle = \frac{1}{2f^2}(\omega_c^2 + \omega_s^2). \tag{2.48}$$

故に，式 (2.46) は式 (2.49) のようにできる．

$$\frac{\partial V_{eff}}{\partial \bar{u}} = \frac{\partial V}{\partial \bar{u}} + \frac{\partial}{\partial \bar{u}}\frac{1}{2}\left\langle \dot{\xi}^2 \right\rangle - \frac{\partial}{\partial \bar{u}}\frac{1}{2}\left(\frac{1}{f^2}\right)^2 \left\langle \eta_1^4 \right\rangle \tag{2.49}$$

この時，

$$\left\langle \dot{\xi}^4 \right\rangle = \frac{3}{4f^4}(\omega_c^4 + \omega_s^4). \tag{2.50}$$

だから，

$$\frac{\partial V_{eff}}{\partial \bar{u}} = \frac{\partial V}{\partial \bar{u}} + \frac{\partial}{\partial \bar{u}}\frac{1}{2}\left\langle \dot{\xi}^2 \right\rangle - \frac{\partial}{\partial \bar{u}}\frac{3}{8}\left\langle \xi^4 \right\rangle. \tag{2.51}$$

従って，有効ポテンシャルは，

$$V_{eff} = V + k_1 < \dot{\xi}^2 > -k_2 < \dot{\xi}^4 > . \tag{2.52}$$

ここで，k_1, k_2 は正の定数である．図 2.16 と図 2.17 は η_1 の振幅が観測時間内で大きく変動することを示している．それ故に，式 (2.52) は式 (2.53) と書き換えることができる．

$$V_{eff} = V + k_1\dot{\xi}^2 - k_2\dot{\xi}^4 \tag{2.53}$$

$\bar{u}$ の変動が遅いことを考慮すると，式 (2.53) 中の $\dot{\xi}$ は X に置き換えられる．

$$V_{eff} = V + k_1' X^2 - k_2' X^4 \tag{2.54}$$

ここで，k_1', k_2' は正の定数である．$u(t) = \bar{u}(t) + \xi(t)$ より，式 (2.46) は以下のように書き直される．

$$\ddot{u} - \ddot{\xi} = -\frac{\partial V_{eff}}{\partial X}\frac{\partial X}{\partial \bar{u}} \tag{2.55}$$

式 (2.44) かつ $\ddot{u} \sim \dot{X}$ より，式 (2.46) は X の時間発展を支配する次式を得る．

$$\dot{X} = -\frac{\partial V_{eff}}{\partial X}\frac{\partial X}{\partial \bar{u}} + \eta_1(\bar{u}, t) \tag{2.56}$$

式 (2.35) から，$\dot{u} \sim X$ より，

$$\ddot{u} = \sigma\left[tr\{(\mathbf{n}^{-1})^2\mathbf{Y}\} - \dot{u}\right]. \tag{2.57}$$

両辺を時間 τ で積分すると，

$$\dot{u} = \sigma \int_0^\tau tr\{(\mathbf{n}^{-1})^2 \mathbf{Y}\} dt - \sigma u. \tag{2.58}$$

$u(t) = \bar{u}(t) + \xi(t)$ であるから，

$$\frac{\partial X}{\partial \bar{u}} \sim \frac{\partial \dot{u}}{\partial \bar{u}} \sim -\sigma < 0. \tag{2.59}$$

式 (2.35) と式 (2.44) の右辺を比較すると，η_1 は $tr\left[(\mathbf{n}^{-1})^2 \mathbf{Y}\right]$ の寄与を表現することから，

$$\frac{\partial V}{\partial X} \sim \sigma X \tag{2.60}$$

式 (2.56) と式 (2.59) より，

$$\dot{X} = \sigma \frac{\partial V_{eff}}{\partial X} + \eta_1(\bar{u}, t). \tag{2.61}$$

式 (2.61) に式 (2.54) を代入すると，

$$\dot{X} = \sigma \frac{\partial V}{\partial X} + k_1'' X - k_2'' X^3 + \eta_1(\bar{u}, t). \tag{2.62}$$

ここで，k_1'', k_2'' は正の定数である．式 (2.60) より，次式が得られる．

$$\dot{X} = k_1''' X - k_2'' X^3 + \eta_1(\bar{u}, t) \tag{2.63}$$

ここで，k_1''' は正の定数である．より小さな摂動 $\eta_2(t)$ を右辺に加え，$\eta_1(\bar{u}, t)$ を $\eta_1'(t)$ とすると，式 (2.64) が得られる．

$$\dot{X} = k_1''' X - k_2'' X^3 + \eta_1'(t) + \eta_2(t) \tag{2.64}$$

Y_n, Z_n がカオス的ならば，$\eta_1' + \eta_2$ は内部ノイズとして働く．式 (2.64) は X の不規則な反転運動が，二重井戸ポテンシャルと内部ノイズに起因する X の確率共鳴から引き起こされることを意味する．

第3章　カオスガスタービンの動力学モデルの工学的応用

3.1　拡張 Lorenz 振動子のカオス同期

Pecora と Carroll は，Lorenz 方程式によって生成されるカオスが，特定の変数を直接結合することで，漸近的に同期する現象を発見した．ここで，同期とは初期状態の異なる 2 つの系が同時に同じ動的挙動を示す現象のことである．これがカオス同期と呼ばれる現象である．ここでは，拡張 Lorenz 方程式の同期特性について論じる．

3.1.1　拡張 Lorenz 方程式の同期特性

X を直接結合した拡張 Lorenz 振動子

Lorenz 振動子は変数 X を直接結合することで, カオス同期を起こす．拡張 Lorenz 振動子は Lorenz 振動子の動的性質を継承しているので，拡張 Lorenz 振動子の変数 X を直接結合した場合, 2 つの拡張 Lorenz 振動子は同期すると予想される．ここでは Lyapunov function を使って, この仮定が正しいことを示す.

2 つの拡張 Lorenz 振動子を用意する．一方の振動子が他方の振動子の振動を駆動すると考え，駆動する方を Drive，駆動される方を Response と記す．ここで，Drive 側の拡張 Lorenz 方程式は式 (2.35)- (2.37) で表わされ， X の直接結合で駆動される Response 側の拡張 Lorenz 方程式は，以下のように記述される．

$$
\begin{aligned}
X' &= X && (3.1)\\
\frac{d\mathbf{Y}'}{d\tau} &= \mathbf{R}'X' - \mathbf{n}\mathbf{Z}'X' - \mathbf{Y}' && (3.2)\\
\frac{d\mathbf{Z}'}{d\tau} &= \mathbf{n}\mathbf{Y}'X' - \mathbf{Z}' && (3.3)
\end{aligned}
$$

ここで，$e_1, \mathbf{e}_2, \mathbf{e}_3$ を以下のように定義する．ただし，e_1 はスカラー，$\mathbf{e}_2, \mathbf{e}_3$ は対角行列で，$\mathbf{e}_2 = diag(e_{21}, \ldots, e_{2N}), \mathbf{e}_3 = diag(e_{31}, \ldots, e_{3N})$ とする．

$$
\begin{aligned}
e_1 &= X' - X && (3.4)\\
\mathbf{e}_2 &= \mathbf{Y}' - \mathbf{Y} && (3.5)\\
\mathbf{e}_3 &= \mathbf{Z}' - \mathbf{Z} && (3.6)
\end{aligned}
$$

式 (2.35)- (2.37) と式 (3.1)- (3.3) から次式が得られる．

$$
\begin{aligned}
e_1 &= 0 \\
\dot{\mathbf{e}_2} &= (\mathbf{R}' - \mathbf{R})X - \mathbf{n}\mathbf{e}_3 X - \mathbf{e}_2 \\
\dot{\mathbf{e}_3} &= \mathbf{n}\mathbf{e}_2 X - \mathbf{e}_3
\end{aligned}
$$

$n = 1, \cdots, N$ として上式を書き直すと，

$$
\begin{aligned}
e_1 &= 0 && (3.7) \\
\dot{e}_{2n} &= (R'_0 - R_0)n^2 \phi_n W_n X - n e_{3n} X - e_{2n} && (3.8) \\
\dot{e}_{3n} &= n e_{2n} X - e_{3n} && (3.9)
\end{aligned}
$$

となる．ここで，Lyapunov function E を以下のように定義する．

$$
E = \frac{1}{2}\left[e_1^2 + \sum_{n=1}^{N} (e_{2n}^2 + e_{3n}^2) \right] \geq 0
$$

E を τ で微分する．このとき，式 (3.7)-(3.9) より，$\dot{E}$ は 式 (3.10) のように変形される．

$$
\begin{aligned}
\dot{E} &= e_1 \dot{e}_1 + \sum_{n=1}^{N} (e_{2n}\dot{e}_{2n} + e_{3n}\dot{e}_{3n}) \\
&= \sum_{n=1}^{N} \left[(R'_0 - R_0)n^2 \phi_n W_n X e_{2n} - e_{2n}^2 - e_{3n}^2 \right] && (3.10)
\end{aligned}
$$

パラメータミスマッチが存在しない時，$\Delta R = R'_0 - R_0 = 0$ である．従って，

$$
\dot{E} = \sum_{n=1}^{N} \left[-e_{2n}^2 - e_{3n}^2 \right] \quad \leq 0 \qquad (3.11)
$$

$\dot{E} \leq 0$ より，$e_1 = 0, \mathbf{e}_2 = 0, \mathbf{e}_3 = 0$ が漸近的に安定となる．

Drive 側と Response 側との同期誤差が $\tau \to \infty$ で 0 に収束するので，X で直接結合した拡張 Lorenz 振動子系は完全に同期する．ただし，パラメータミスマッチが大きいとき，つまり $\Delta R \neq 0$ のとき，式（3.10）より，$\dot{E} \leq 0$ とはならないので，漸近的に安定とならない．そのため，パラメータミスマッチが大きいとき，X を直接結合させた拡張 Lorenz 振動子系は同期しない．

Y を直接結合した拡張 Lorenz 振動子

Lorenz 振動子系におけるカオス同期は変数 Y を直接結合することでも実現できる．拡張 Lorenz 振動子は Lorenz 振動子の動的性質を継承しているので，拡張 Lorenz 振動子の

$\mathbf{Y}$ を直接結合した場合，拡張 Lorenz 振動子は同期すると予想される．ここでも Lyapunov function を使って，この仮定が正しいことを示す．

X 結合の場合と同様に，Drive 側と Response 側で 2 つの拡張 Lorenz 振動子を用意する．ここで，Drive 側の拡張 Lorenz 方程式は式 (2.35)- (2.37) で表わされ， Response 側の拡張 Lorenz 方程式は以下のように記述される．

$$\frac{dX'}{d\tau} = \sigma' \left[tr\{(\mathbf{n}^{-1})^2 \mathbf{Y}'\} - X \right] \tag{3.12}$$

$$\mathbf{Y}' = \mathbf{Y} \tag{3.13}$$

$$\frac{d\mathbf{Z}'}{d\tau} = \mathbf{n}\mathbf{Y}'X' - \mathbf{Z}' \tag{3.14}$$

式 (2.35)- (2.37) と式 (3.12)- (3.14) から下式が得られる．

$$\dot{e_1} = (\sigma' - \sigma)\{tr\left[(\mathbf{n}^{-1})^2 \mathbf{Y}\right]\} - \sigma' X' + \sigma X, \tag{3.15}$$

$$\mathbf{e}_2 = 0, \tag{3.16}$$

$$\dot{\mathbf{e}_3} = \mathbf{n}\mathbf{Y}e_1 - \mathbf{e}_3 \tag{3.17}$$

パラメータミスマッチが存在しない時，$\Delta\sigma = \sigma' - \sigma = 0$ となる．従って，

$$\dot{e_1} = -\sigma e_1, \tag{3.18}$$

$$\mathbf{e}_2 = 0, \tag{3.19}$$

$$\dot{\mathbf{e}_3} = \mathbf{n}\mathbf{Y}e_1 - \mathbf{e}_3 \tag{3.20}$$

式 (3.18) を解くと，$e_1 = Ce^{-\sigma\tau}$(C は任意定数) となるので，$\tau \to \infty$ で $e_1 \to 0$ となる．以上より，$\tau \to \infty$ において，式 (3.20) は以下のように書き換えられる．

$$\dot{\mathbf{e}_3} = -\mathbf{e}_3 \tag{3.21}$$

式 (3.21) から，$\tau \to \infty$ で $\mathbf{e}_3 \to 0$ となる．

Drive 側と Response 側の間の誤差が $\tau \to \infty$ で 0 に収束するので，行列 $\mathbf{Y}$ の全要素を直接結合した拡張 Lorenz 振動子系は完全に同期する．ただし，$\Delta\sigma \neq 0$ のとき，式 (3.18) は成り立たない．そのため，パラメータミスマッチが大きいとき，行列 $\mathbf{Y}$ の全要素を直接結合させた拡張 Lorenz 振動子系は同期しない．

3.1.2 パラメータミスマッチ下での同期実験

直接結合された 2 つの拡張 Lorenz 振動子系の同期誤差を調べた．ここでは，前節で述べた拡張 Lorenz 振動子系の同期特性より，X 及び，$\mathbf{Y}$ を直接結合した拡張 Lorenz 振動子の同期誤差について評価する．

X を直接結合した拡張 Lorenz 振動子系の同期誤差について調べる．X を直接結合すると，同期誤差はパラメータミスマッチ $\Delta\sigma$ ではなく，ΔR によって生じる．R_0 のパラメータミスマッチの比 r は，$r = \Delta R/R_0$ によって表現する．同期実験では，$R_0 = 3000$ とし，-0.1 から 0.1 までの r を 0.01 刻みに設定する．式 (2.35)- (2.37) と式 (3.1)- (3.3) を 4 次の Runge-Kutta 法で数値積分する．時間刻み幅は 4.0×10^{-4}，$\sigma = 28.3, \phi = 0.36[rad], N = 10, 100$ とする．最初の 75 000 点の数値解は，初期条件から同期状態に至るまでの遷移過程として，排除された．各 r における Z_n と Z'_n の $T = 50000$ 点の数値解から同期誤差を求める．r の関数としての同期誤差の平均値 $E_X(r)$ は以下のように定義される．

$$E_X(r) = \frac{1}{T}\sum_{t=1}^{T}\sqrt{\frac{1}{N}\sum_{n=1}^{N} e_{3n}^2(t,r)} = \frac{1}{T}\sum_{t=1}^{T}\sqrt{\frac{1}{N}\sum_{n=1}^{N}\left[Z'_n(t,r) - Z_n(t)\right]^2} \tag{3.22}$$

式 (3.22) は Z_n と Z'_n の同期誤差の二乗平均平方根である．式 (3.22) により，[72] で報告されている almost synchronization としての同期特性を評価できる．このような同期誤差の計算手法は，本研究の目的，例えば，X 及び，$\mathbf{Y}$ を直接結合した拡張 Lorenz 振動子の同期特性の比較をするのに便利である．

実験で求めた $E_X(r)$ を図 3.1, 図 3.2 に示す．図 3.1 が $N = 10$ での $E_X(r)$ で図 3.2 が $N = 100$ での $E_X(r)$ である．同期誤差の平均値は $r = 0$ の時，$N = 10, 100$ 共に $E_X(0) = 0.0$，$r = -0.1$, $r = 0.1$ の時，$N = 10$ が $E_X(-0.1) = E_X(0.1) \approx 31.18$，$N = 100$ が $E_X(-0.1) = E_X(0.1) \approx 77.89$ である．$E_X(r)$ は $r = 0$ を境として線形に増加する．なお，その傾きは $r = 0$ に対して，対称である．

次に，$\mathbf{Y}$ を直接結合した拡張 Lorenz 振動子系の同期誤差について解析する．この場合，同期誤差はパラメータミスマッチ ΔR ではなく，$\Delta\sigma$ によって生じる．σ のパラメータミスマッチの比 s は，$s = \Delta\sigma/\sigma$ によって表現される．この実験では，$\sigma = 28.3$ とし，-0.1 から 0.1 までの s を 0.01 刻みに設定する．パラメータは先程と同様，$R_0 = 3000, \phi = 0.36[rad], N = 10, 100$ に固定する．上述したパラメータで式 (2.35)- (2.37) と式 (3.12)- (3.14) を 4 次の Runge-Kutta 法で数値積分した．時間刻み幅は 4.0×10^{-4} である．最初の 75 000 点の数値解は，初期条件から同期状態に至るまでの遷移過程として，排除された．各 s における Z_n と Z'_n の $T = 50000$ 点の数値解から同期誤差を求めた．s の関数としての同期誤差の平均値 $E_Y(s)$ は以下のように定義される．

$$E_Y(s) = \frac{1}{T}\sum_{t=1}^{T}\sqrt{\frac{1}{N}\sum_{n=1}^{N} e_{3n}^2(t,s)} = \frac{1}{T}\sum_{t=1}^{T}\sqrt{\frac{1}{N}\sum_{n=1}^{N}\left[Z'_n(t,s) - Z_n(t)\right]^2} \tag{3.23}$$

実験で求めた $E_Y(s)$ を図 3.3, 図 3.4 に示す．図 3.3 が $N = 10$ での $E_Y(s)$ で図 3.4 が $N = 100$ での $E_Y(s)$ である．同期誤差の平均値は $s = 0$ の時，$N = 10, 100$ 共に $E_Y(0) = 0.0$，

$s = -0.1$ の時，$N = 10$ が $E_Y(-0.1) \approx 5.73$，$N = 100$ が $E_Y(-0.1) \approx 11.20$，$s = 0.1$ の時，$N = 10$ が $E_Y(0.1) \approx 5.25$，$N = 100$ が $E_Y(0.1) \approx 10.30$ である．$E_Y(s)$ は $s = 0$ を境として線形に増加する．しかし，X を直接結合した時と異なり，その傾きは $r = 0$ に対して，非対称である．

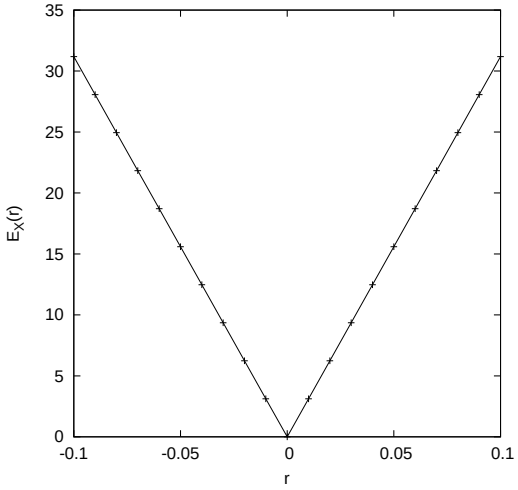

図 3.1: 各 r における同期誤差の平均値 $E_X(r)(\sigma = 28.3, R_0 = 3000, N = 10, \phi = 0.36[rad])$

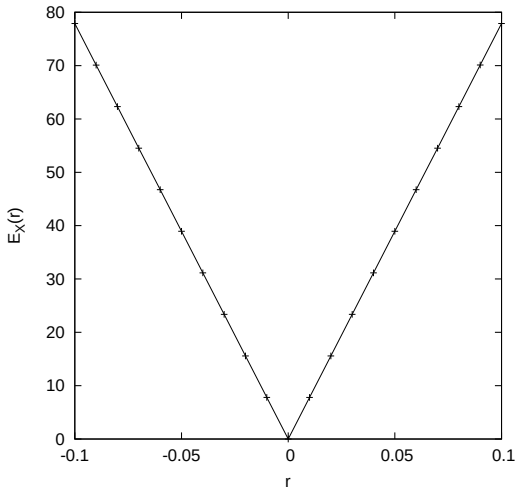

図 3.2: 各 r における同期誤差の平均値 $E_X(r)(\sigma = 28.3, R_0 = 3000, N = 100, \phi = 0.36[rad])$

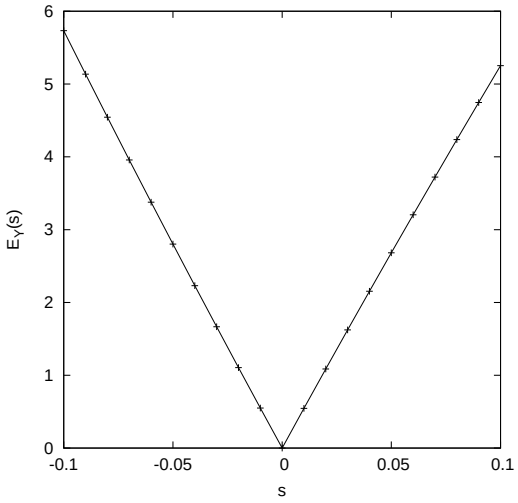

図 3.3: 各 s における同期誤差の平均値 $E_Y(s)(\sigma = 28.3, R_0 = 3000, N = 10, \phi = 0.36[rad])$

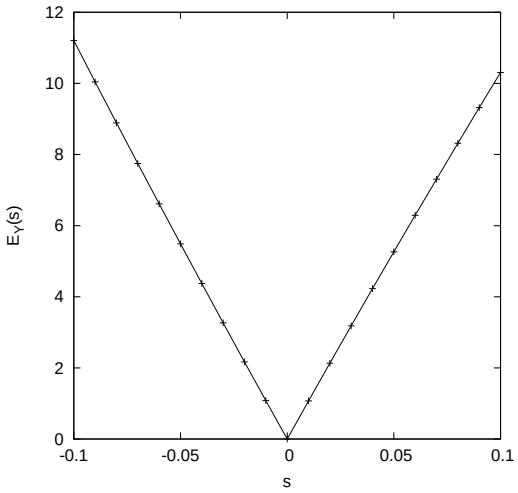

図 3.4: 各 s における同期誤差の平均値 $E_Y(s)(\sigma = 28.3, R_0 = 3000, N = 100, \phi = 0.36[rad])$

3.2 カオス暗号

3.2.1 一般化された拡張 Lorenz 方程式とカオスマスキング法

拡張 Lorenz 方程式を無次元の力学モデルとして見た時，パラメータ σ, R_0, ϕ は応用対象に適した値に設定できる．実際に，著者は式 (2.35)- (2.37) 中の行列 $\mathbf{n}$ の対角要素を整数値から実数値に変更した．それが式 (3.24) である．

$$\mathbf{M} = diag(M_1, \ldots, M_n \ldots, M_N) \tag{3.24}$$

ここで $M_1 = 1$ であり，$M_n (n \geq 2)$ の取りうる範囲は $n-1 < M_n \leq n+1$ とする．ただし，N は十分に大きな任意の整数である．行列 $\mathbf{n}$ を行列 $\mathbf{M}$ で書き換えると次式とできる．

$$\frac{dX}{d\tau} = \sigma \left[tr\{(\mathbf{M}^{-1})^2 \mathbf{Y}\} - X \right] \tag{3.25}$$

$$\frac{d\mathbf{Y}}{d\tau} = \mathbf{R}X - \mathbf{MZ}X - \mathbf{Y} \tag{3.26}$$

$$\frac{d\mathbf{Z}}{d\tau} = \mathbf{MY}X - \mathbf{Z} \tag{3.27}$$

$$\mathbf{R} = R_0 \mathbf{M}^2 \mathbf{\Phi W} \tag{3.28}$$

ただし，

$$\mathbf{W} = diag(\sin\phi, \ldots, \sin M_N\phi),$$

$$\mathbf{\Phi} = diag(\phi - \frac{1}{2}\sin 2\phi, \ldots, \frac{1}{M_N - 1}\sin(M_N - 1)\phi - \frac{1}{M_N + 1}\sin(M_N + 1)\phi)$$

と変更する．式 (3.25)- (3.27) で定義される拡張 Lorenz 方程式を一般化された拡張 Lorenz 方程式と呼ぶ．

分岐パラメータ σ, R_0, ϕ は拡張 Lorenz 方程式の動的性質を決めるため，通信文の暗号化と復号化を行う秘密鍵として使用できる．しかしながら，拡張 Lorenz 方程式がカオスを生成する分岐パラメータの組み合わせ数は十分大きくない．代わりに，本研究の暗号通信法では，行列 $\mathbf{M}$ を秘密鍵として使用する．この暗号通信法において，σ, R_0, ϕ は定数であり，本論文では，$\sigma = 25, R_0 = 3185, \phi = 0.36[rad]$ に設定する．整数行列 $\mathbf{n}$ を持つ拡張 Lorenz 方程式の数値実験 [8, 73] においては，これらのパラメータがカオスを生成することはすでに確認済みである．

行列 $\mathbf{n}$ の代わりに行列 $\mathbf{M}$ を使うとき，$M_n (n \geq 2)$ は $n-1$ と $n+1$ の間からランダムに設定される．例えば，$n-0.8, n-0.6, \ldots, n+0.8, n+1$ の中から一つ選ぶ場合，秘密鍵の組み合わせ総数は 10^{N-1} 通りとなる．あるいは，$M_n (n \geq 2)$ に n もしくは $n+1/2$ のどちらか一方を設定する場合，秘密鍵の組み合わせ総数は 2^{N-1} 通りとなる．例えば，$N = 101$ ならば，$2^{100} \sim O(10^{30})$ である．どちらの秘密鍵の設定方法でも，N の増加に伴って，鍵の組み合わせ総数が指数関数的に増加する．本論文では，後に説明する QKD

との連携を考えて，$M_n(n \geq 2)$ に n もしくは $n+1/2$ のどちらか一方を設定する方法，即ち，2 進暗号鍵方式で数値実験を行う．

行列 $\mathbf{M}$ に変更した拡張 Lorenz 方程式がカオスを生成することを実証するために，式 (3.25)-(3.27) を 4 次の Runge-Kutta 法で数値積分した．積分時間間隔は 4.0×10^{-4} に変更したが，それ以外のパラメータ σ, ϕ は，行列 $\mathbf{n}$ の拡張 Lorenz 方程式のパラメータと同じ，$\sigma = 25, \phi = 0.36[rad]$ に設定している．$N = 101$ とし，$M_n(n \geq 2)$ には n もしくは $n+1/2$ をランダムに設定した．最初の 250 00 点を排除することで，初期条件からカオスに至るまでの非定常部分を排除した．

X の動的性質と，各 n で Y_n, Z_n の動的性質を調べた．ここでは，$R_0 = 3185$ に設定している．図 3.5-図 3.7 は，それぞれ，X, Y_n, Z_n の時間変化を示したグラフである．図 3.6(a)-3.6(d) はそれぞれ，$Y_1, Y_{10}, Y_{50}, Y_{101}$ の数値解である．また，図 3.7(a)-3.7(d) はそれぞれ，$Z_1, Z_{10}, Z_{50}, Z_{101}$ の数値解である．$X, \mathbf{Y}, \mathbf{Z}$ の不規則な振動は，拡張 Lorenz モデルのようなカオス挙動を示している．

図 3.8 は一般化された拡張 Lorenz 方程式の分岐構造で，分岐パラメータ R_0 に対する X の極大点と極小点をプロットしたものである．行列 $\mathbf{M}$ を持つ拡張 Lorenz 方程式の分岐構造は，カオスを生成する換算 Rayleigh 数に違いがあるものの，行列 $\mathbf{n}$ の拡張 Lorenz 方程式の分岐構造と本質的に同一である．

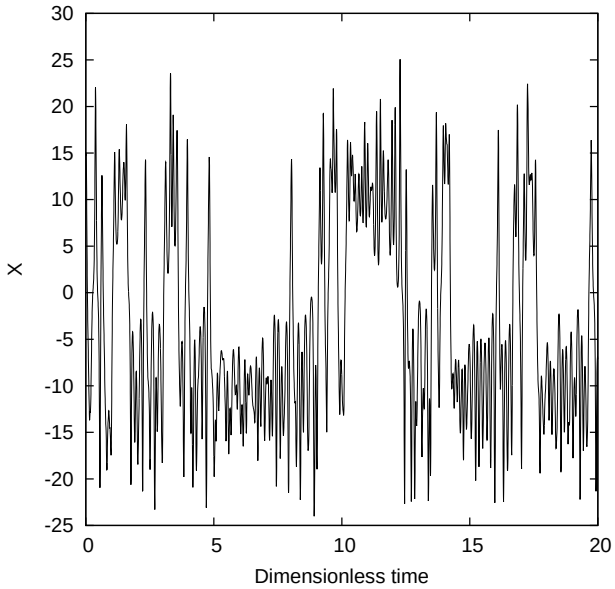

図 3.5: 一般化された拡張 Lorenz 方程式に関する X の時間変化

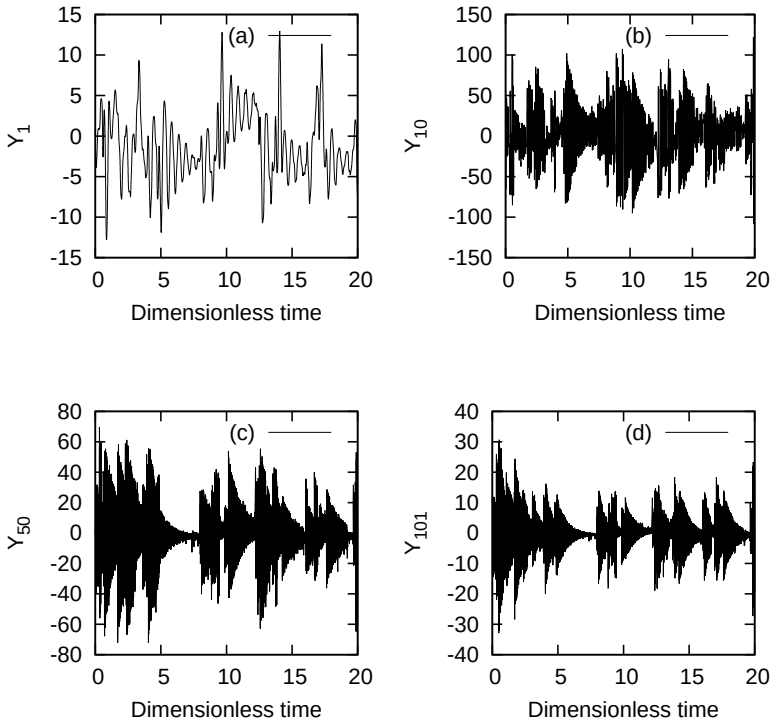

図 3.6: 一般化された拡張 Lorenz 方程式に関する Y_n の時間変化

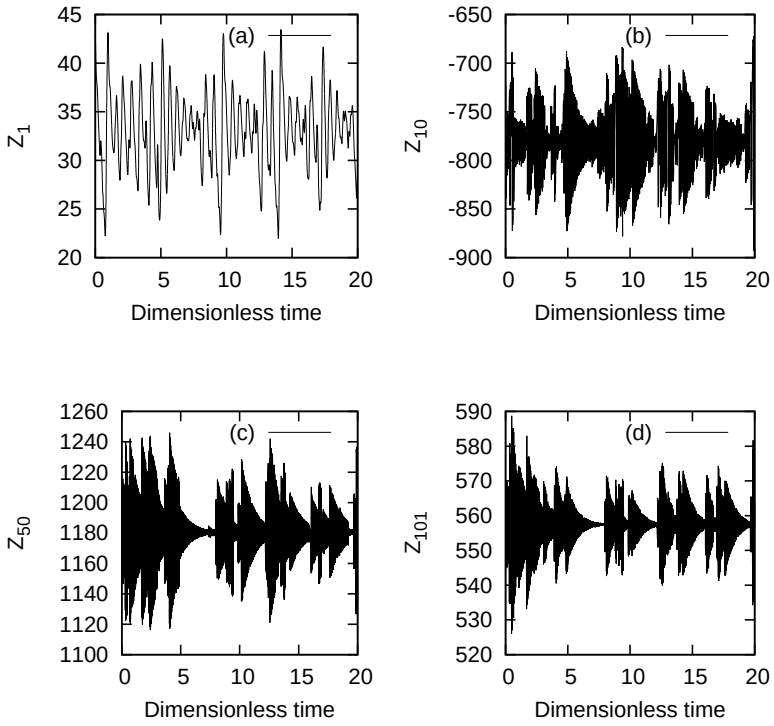

図 3.7: 一般化された拡張 Lorenz 方程式に関する Z_n の時間変化

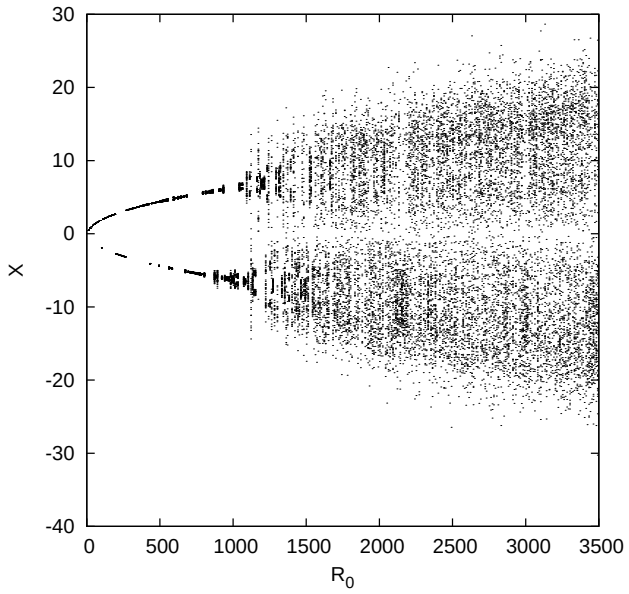

図 3.8: 各 R_0 での X の動的性質 (N=101)

次に，行列 $\mathbf{M}$ のわずかな違いにより，拡張 Lorenz 方程式のダイナミクスが変化することを示す．以下では，固定点の変化により，拡張 Lorenz 方程式のダイナミクスが変化することを示す．固定点では $dX/d\tau = 0, d\mathbf{Y}/d\tau = 0, d\mathbf{Z}/d\tau = 0$ であるから，式 (3.25)-(3.27) は以下のようにできる．

$$0 = \sigma \left[tr\{(\mathbf{M}^{-1})^2\mathbf{Y}\} - X \right] \tag{3.29}$$

$$0 = \mathbf{R}X - \mathbf{M}\mathbf{Z}X - \mathbf{Y} \tag{3.30}$$

$$0 = \mathbf{M}\mathbf{Y}X - \mathbf{Z} \tag{3.31}$$

簡単のために，対角行列変数 $\mathbf{Y}$，$\mathbf{Z}$ を $1 \sim N$ までの変数 Y_n, Z_n で表現すると，

$$0 = \sigma \left[\sum_{n=1}^{N} \frac{1}{M_n^2} Y_n - X \right] \tag{3.32}$$

$$0 = R_0 M_n^2 \Phi_n W_n X - M_n Z_n X - Y_n \tag{3.33}$$

$$0 = M_n Y_n X - Z_n \tag{3.34}$$

式 (3.32)，(3.34) より，

$$X = \sum_{n=1}^{N} \frac{1}{M_n^2} Y_n \tag{3.35}$$

$$Z_n = M_n Y_n X \tag{3.36}$$

式 (3.36) を (3.33) に代入し整理すると，

$$Y_n = \frac{R_0 M_n^2 X}{M_n^2 X^2 + 1} \Phi_n W_n \tag{3.37}$$

分子，分母に $1/X^2$ をかけると，

$$Y_n = \frac{R_0 M_n^2}{M_n^2 + 1/X^2} \frac{\Phi_n W_n}{X} \tag{3.38}$$

$M_n^2 \gg 1/X^2$ とすると，式（3.38）は式（3.39）となる．

$$Y_n \approx \frac{R_0}{X} \Phi_n W_n \tag{3.39}$$

式（3.39）から，

$$\sum_{n=1}^{N} \frac{1}{M_n^2} Y_n \approx \sum_{n=1}^{N} \frac{1}{M_n^2} \frac{R_0}{X} \Phi_n W_n \tag{3.40}$$

式（3.35) より，

$$X \approx \sum_{n=1}^{N} \frac{1}{M_n^2} \frac{R_0}{X} \Phi_n W_n \tag{3.41}$$

$\sum_{n=1}^{N} \frac{1}{M_n^2} \Phi_n W_n = \beta$ とおき整理すると，

$$X \approx \pm\sqrt{R_0 \beta}. \tag{3.42}$$

式 (3.39) ，式 (3.42) より，

$$Y_n \approx \pm\sqrt{\frac{R_0}{\beta}} \Phi_n W_n. \tag{3.43}$$

従って，式 (3.44) が導出できる．

$$Z_n \approx M_n R_0 \Phi_n W_n \tag{3.44}$$

なお，この近似が成立する条件は $n^2 \gg 1/X^2$ より，

$$R_0 \beta \gg \frac{1}{n^2} \tag{3.45}$$

固定点の近似値が正しいか確認するために，拡張 Lorenz 方程式のカオスアトラクタと分岐パラメータを用いて計算した固定点を重ね合わせた．それが，図 3.9-図 3.12 である．図 3.9-図 3.12 のアトラクタを求めるために，式 (3.25)-(3.27) を 4 次の Runge-Kutta 法で数値積分した．積分時間間隔は 4.0×10^{-4}，それ以外のパラメータ σ, ϕ, R_0 は，$\sigma = 25, \phi = 0.36[rad], R_0 = 500, 3185$ に設定している．また，$N = 101$ とし，$M_n (n \geq 2)$ には n もしくは $n + 1/2$ をランダムに設定した．図 3.9 と図 3.10 は，それぞれ，$R_0 = 500$ での一般化された拡張 Lorenz 方程式のカオスアトラクタと $Y_1 - Z_1$ プロットである．緑の $\times$ 印は固定点の計算値である．$R_0 = 500$ の場合，その解は固定点に収束する．図 3.11 は，$R_0 = 3185$ での一般化された拡張 Lorenz 方程式のカオスアトラクタである．図 3.12 はその $Y_1 - Z_1$ プロットである．$R_0 = 3185$ の場合，固定点はダブルスクロール構造の中心に位置する．式 (3.45) は，固定点の近似値は R_0 が大きくなればなるほど，真の値に近づくことを意味する．これが，$R_0 = 500$ で求めた固定点と実際の固定点が異なる理由である．以上の事実から，式 (3.42)-(3.44) を使って，実際の固定点のおおよその位置を把握できる．式 (3.42) と式 (3.43) の β より，行列 $\mathbf{M}$ のわずかな違いにより，固定点が変化する．これは，行列 $\mathbf{M}$ のわずかな違いにより，一般化された拡張 Lorenz 方程式のダイナミクスが変化することを意味する．

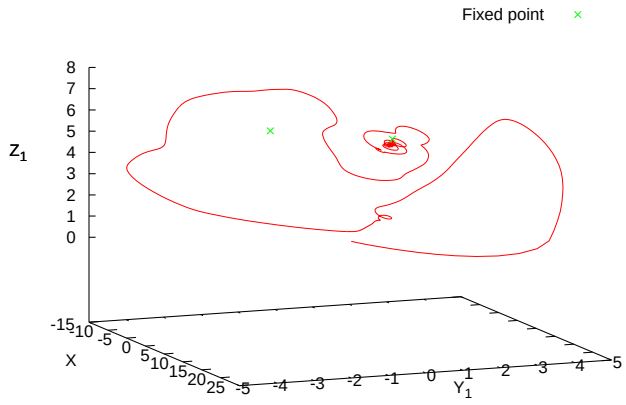

図 3.9: $R = 500$ での一般化された拡張 Lorenz 方程式の 3 次元プロットと固定点

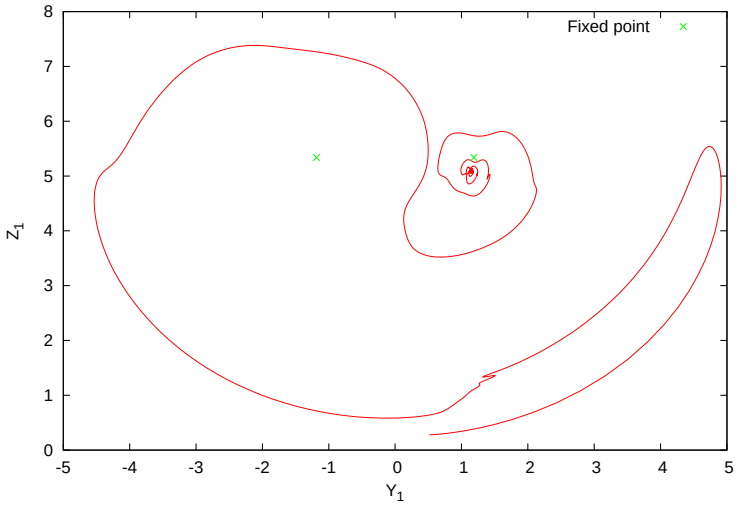

図 3.10: $R = 500$ での一般化された拡張 Lorenz 方程式の $Y_1 - Z_1$ プロットと固定点

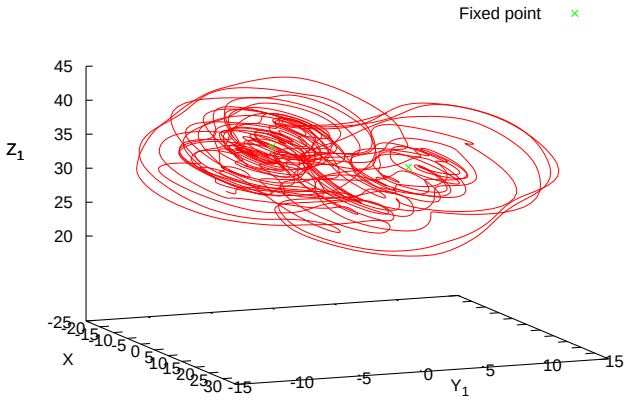

図 3.11: $R = 3185$ での一般化された拡張 Lorenz 方程式の 3 次元プロットと固定点

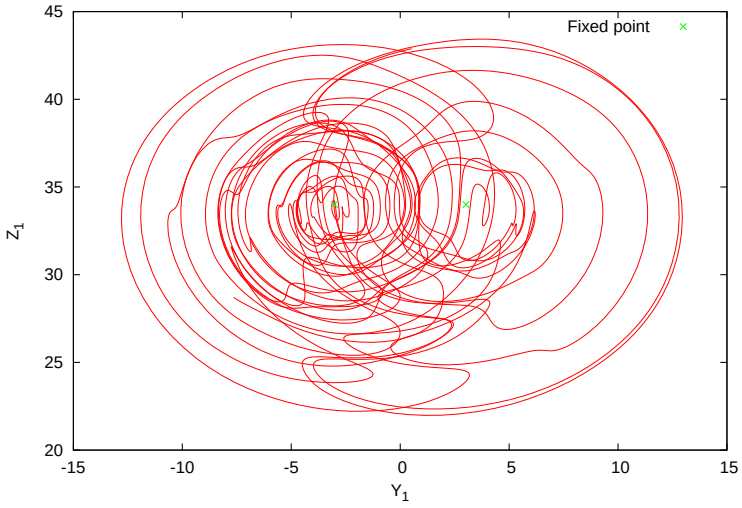

図 3.12: $R = 3185$ での一般化された拡張 Lorenz 方程式の $Y_1 - Z_1$ プロットと固定点

著者は X に微小な通信文 $m = \epsilon$ が加わったとき，X を直接結合した拡張 Lorenz 方程式にどのような影響があるのかを調べた．まず，3.1 同様，Drive 側と Response 側の 2 つの一般化された拡張 Lorenz 振動子を用意する．Drive 側の拡張 Lorenz 方程式は式 (3.25)-(3.27) で表わされ， Response 側の拡張 Lorenz 方程式は次式として記述される．

$$
\begin{aligned}
X' &= X + \epsilon && (3.46)\\
\frac{d\mathbf{Y}'}{d\tau} &= \mathbf{R}X' - \mathbf{M}\mathbf{Z}'X' - \mathbf{Y}' && (3.47)\\
\frac{d\mathbf{Z}'}{d\tau} &= \mathbf{M}\mathbf{Y}'X' - \mathbf{Z}' && (3.48)
\end{aligned}
$$

第 3.1 節と同様に，$e_1, \mathbf{e}_2, \mathbf{e}_3$ を以下のように定義する．ここでも，e_1 はスカラー，$\mathbf{e}_2, \mathbf{e}_3$ は対角行列で， $\mathbf{e}_2 = diag(e_{21}, \ldots, e_{2N}), \mathbf{e}_3 = diag(e_{31}, \ldots, e_{3N})$ とする．

$$
\begin{aligned}
e_1 &= X' - X && (3.49)\\
\mathbf{e}_2 &= \mathbf{Y}' - \mathbf{Y} && (3.50)\\
\mathbf{e}_3 &= \mathbf{Z}' - \mathbf{Z} && (3.51)
\end{aligned}
$$

式 (3.25)- (3.27) と式 (3.46)- (3.48) から次式となる．

$$
\begin{aligned}
e_1 &= \epsilon\\
\dot{\mathbf{e}_2} &= \mathbf{R}\epsilon - \mathbf{M}\mathbf{e}_3 X - \mathbf{e}_2 - \mathbf{M}\mathbf{Z}'\epsilon\\
\dot{\mathbf{e}_3} &= \mathbf{M}\mathbf{e}_2 X - \mathbf{e}_3 - \mathbf{M}\mathbf{Y}'\epsilon
\end{aligned}
$$

$n = 1, \cdots, N$ として上式を書き直すと，

$$
\begin{aligned}
e_1 &= \epsilon && (3.52)\\
\dot{e}_{2n} &= R_n\epsilon - M_n e_{3n} X - e_{2n} - M_n Z'_n \epsilon && (3.53)\\
\dot{e}_{3n} &= M_n e_{2n} X - e_{3n} - M_n Y'_n \epsilon && (3.54)
\end{aligned}
$$

ここで，Lyapunov function E を以下のように定義する．

$$
E = \frac{1}{2}\left[e_1^2 + \sum_{n=1}^{N}(e_{2n}^2 + e_{3n}^2)\right] \geq 0
$$

E を τ で微分する．このとき，式 (3.52)-(3.54) より，$\dot{E}$ は 次式のように書き換えられる．

$$
\begin{aligned}
\dot{E} &= e_1\dot{e}_1 + \sum_{n=1}^{N}(e_{2n}\dot{e}_{2n} + e_{3n}\dot{e}_{3n})\\
&= e_1\dot{e}_1 - \sum_{n=1}^{N}(e_{2n}^2) - \sum_{n=1}^{N}(e_{3n}^2) + \sum_{n=1}^{N}(R_n e_{2n}\epsilon - M_n Z'_n e_{2n}\epsilon + M_n Y'_n e_{3n}\epsilon) \quad (3.55)
\end{aligned}
$$

$e_1 = \epsilon = 0$ のとき，$\dot{E} \leq 0$ より，$\mathbf{e}_2 = 0, \mathbf{e}_3 = 0$ が漸近的に安定となる．しかしながら，$\epsilon \neq 0$ のとき，この安定性は失われる．

平文として，微小な通信文 $\epsilon = Acos(2\pi f\tau)$ を考える．この時，A は無次元の振幅であり，$A \ll 1$，f は無次元振動数である．よって，式 (3.55) は以下のように書き換えることができる．

$$
\begin{aligned}
\dot{E} &= -\sum_{n=1}^{N}(e_{2n}^2) - \sum_{n=1}^{N}(e_{3n}^2)\\
&\quad + Acos(2\pi f\tau)\sum_{n=1}^{N}(R_n e_{2n} - M_n Z'_n e_{2n} + M_n Y'_n e_{3n})\\
&\quad - \pi f A^2 cos(4\pi f\tau) \quad (3.56)
\end{aligned}
$$

f が高い振動数のとき，余弦項が高速に振動するため，式 (3.56) の第 3 項は無視できる．また，$A \ll 1$ であるため，式 (3.56) の第 4 項も無視できる．結果として，この時，結合された拡張 Lorenz 系は同期する．対して，f が低い振動数のとき，式 (3.56) の第 3 項は無視できないため，結合された拡張 Lorenz 系は同期しない．

上述した理論解析を検証するために，式 (3.56) を 4 次の Runge-Kutta 法で見積もる．計算に必要な $X, \mathbf{Y}, \mathbf{Z}, X', \mathbf{Y}', \mathbf{Z}'$ を数値積分するための積分時間間隔は 1.0×10^{-4}，それ以外のパラメータは，$A = 0.001, f = 0.1, 100, N = 101$ に設定する．$X, \mathbf{Y}, \mathbf{Z}, X', \mathbf{Y}', \mathbf{Z}'$ の初期値は平均 0，分散 1 の乱数で与えた．最初の 100 000 点は初期条件に依存する非定常部分として排除された．図 3.13(a) と図 3.13(b) は $f = 0.1$ での $\dot{E}$ の時間変化である．同様に，図 3.14(a) と図 3.14(b) は $f = 100$ での $\dot{E}$ の時間変化である．

$f = 0.1$，$f = 100$ どちらの場合でも，同期の初期段階では e_{2n}, e_{3n} は相当大きい．よって，A が十分小さい時に限り，$\dot{E} \approx -\sum_{n=1}^{N}(e_{2n}^2) - \sum_{n=1}^{N}(e_{3n}^2)$ となる．従って，あたかもカオス同期を起こすかのように，Lyapunov function E は減少する．しかしながら，同期が進行すると，振幅 A が小さいにもかかわらず，式 (3.56) の余弦項が式 (3.56) の第 1 項と第 2 項よりも支配的になる．この効果は f が高周波数である時よりも，低周波数である時に顕著に表れる．なぜなら，速い振動は余弦項をキャンセルするように働くが，遅い振動にはそのような効果がないためである．従って，X に振幅の小さい低周波数の信号を加えた場合，カオス同期は妨害され，高周波数の信号を加えた場合，カオス同期に対する影響は小さくなる．これらの実験結果は，通信文に低周波数の信号が含まれている時，Cuomo-Oppenheim 法における通信文の復号化が失敗することを意味する．

著者は，次に，低周波数と高周波数とを分類する臨界周波数 f_c を見積もった．図 3.15 は 0.03 ステップごとの各 f における $\dot{E}$ の最大値を見積もったものである．この結果から，臨界周波数 f_c は 5 と見積もることができる．

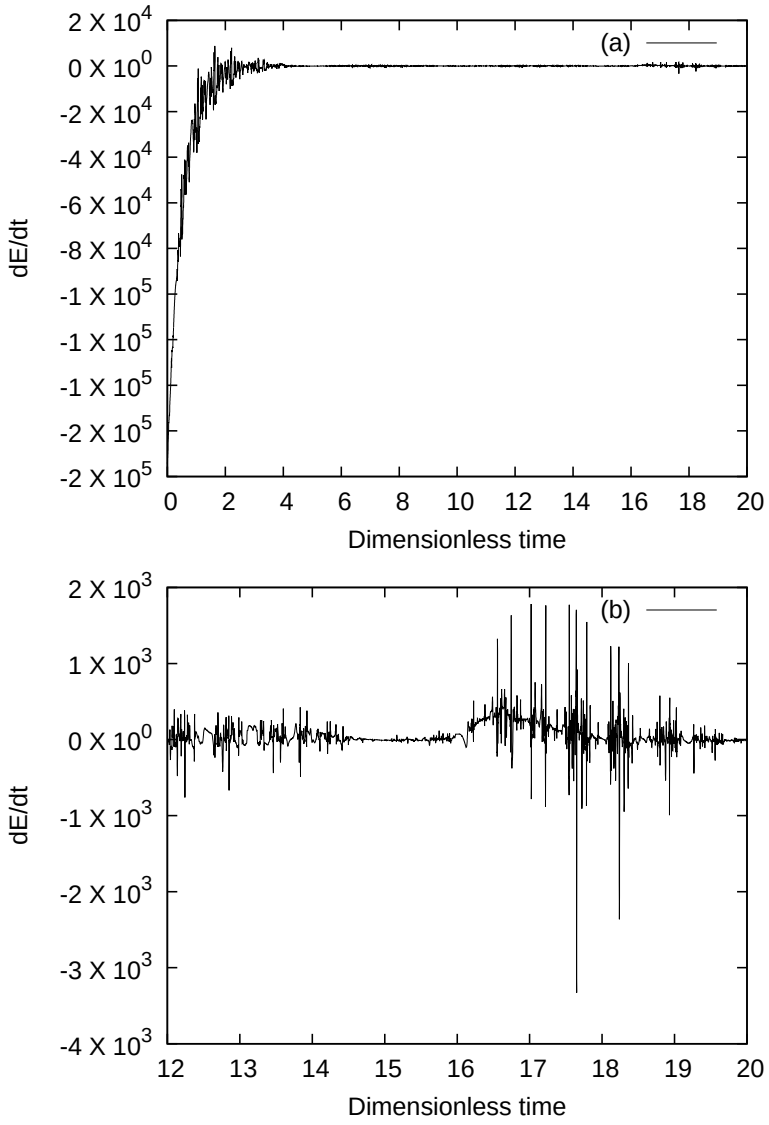

図 3.13: $f = 0.1$ における $\dot{E}$ の時間変化

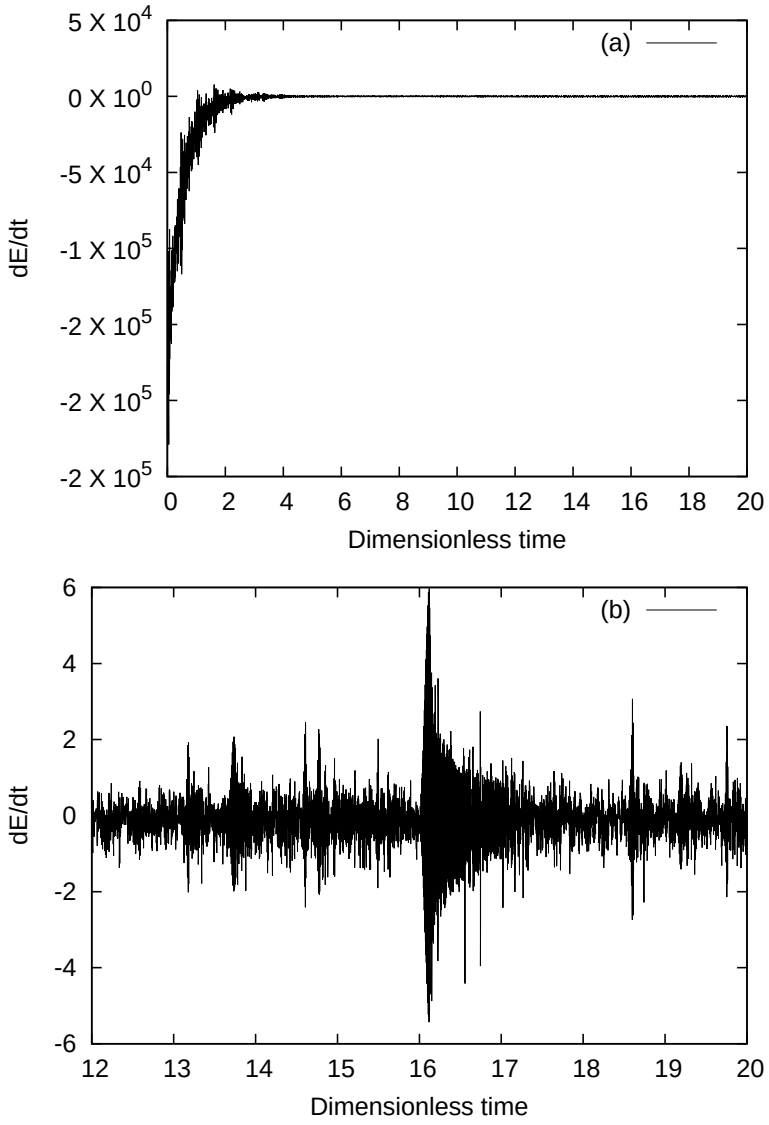

図 3.14: $f = 100$ における $\dot{E}$ の時間変化

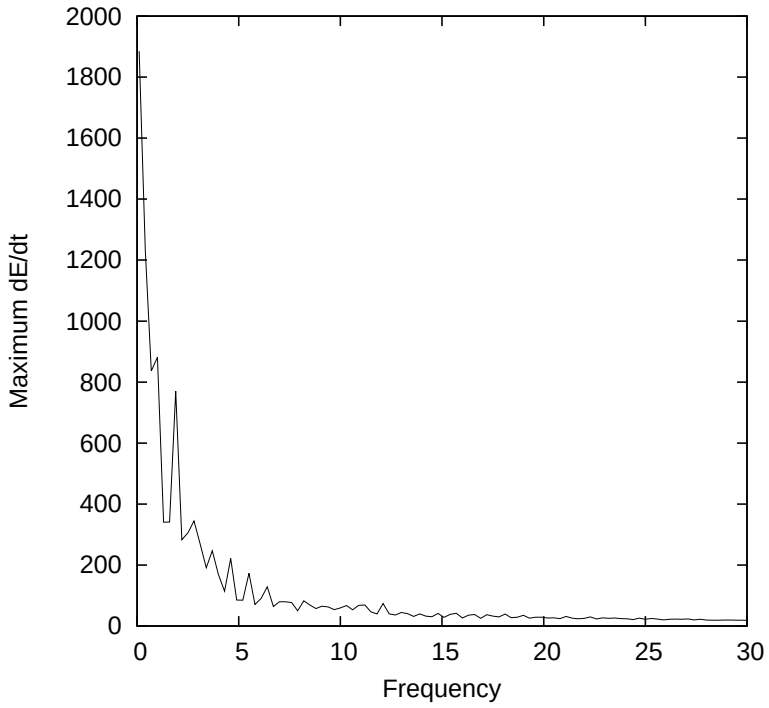

図 3.15: 振動数 f に対する $\dot{E}$ の最大値

最後に，一般化された拡張 Lorenz 方程式を使ったカオスマスキング法について説明する．Alice と Bob は一般化された拡張 Lorenz 方程式の初期値 $(X(0), \mathbf{Y}(0), \mathbf{Z}(0))$, 行列 $\mathbf{M}$ 以外のパラメータ (σ, R_0, ϕ) の他にカオスに至るまでの切り捨て時間 T_0, 数値積分の刻み時間 $\Delta\tau$ を公開鍵として共有し, 行列 $\mathbf{M}$ を秘密鍵として，第 4 章で説明する鍵配送法で交換しておく．次に，デジタル計算機を用いて, マスキングに使用するカオス X_1, X_2 を生成する．その後, Alice は微小な通信文 m をカオス X_1 に足し合わせ, マスキング信号 $X_1 + m$ として Bob に送信する．Bob は自身が生成したカオス X_2 と暗号文 $X_1 + m$ の差をとると, $X_1 = X_2$ より, 通信文 m を復号化できる．これが一般化された拡張 Lorenz 方程式を使ったカオスマスキング法の暗号化，復号化過程である．

通信文の暗号化と復号化では，X の低周波数域に m の周波数成分が隠れるように，$\alpha t = \tau$

を使って，一般化された拡張 Lorenz 方程式の時間スケールを変える．ここで，係数 $\alpha[s^{-1}]$ は公開鍵である．α により，次元を与えられた一般化された拡張 Lorenz 方程式は以下のようになる．

$$\frac{dX}{dt} = \alpha\sigma\left[tr\{(\mathbf{M}^{-1})^2\mathbf{Y}\} - X\right] \tag{3.57}$$

$$\frac{d\mathbf{Y}}{dt} = \alpha(\mathbf{R}X - \mathbf{MZ}X - \mathbf{Y}) \tag{3.58}$$

$$\frac{d\mathbf{Z}}{dt} = \alpha(\mathbf{MY}X - \mathbf{Z}) \tag{3.59}$$

3.2.2 暗号化，及び，復号化実験

前節で示したカオスマスキング法が妥当なものか評価するために，Alice と Bob の間で安全に鍵が配送できたという仮定の下，数値実験を行う．実験では，式 (3.57)-(3.59) を 4 次の Runge-Kutta 法で数値積分し，積分時間間隔は 2.0×10^{-7}，$N = 101, \alpha = 1000$ とする．秘密鍵である行列 $\mathbf{M}$ を設定するにあたり，$M_n(n \geq 2)$ には n もしくは n+0.5 をランダムに設定し，それを Alice と Bob で共有する．この時，$M_1 = 1$ である．初期条件は $X = 0.1, \mathbf{Y} = \mathbf{0}, \mathbf{Z} = \mathbf{0}$ とし，これらも Alice と Bob の間で共有する．なお，最初の 50 000 点を排除することで，初期条件からカオスに至るまでの非定常部分を排除する．本論文では量子化レベル 16$[bit]$，周波数帯域 44.1$[kHz]$ で録音された音声信号”Yes, we can.” を平文として使用する．ここで，平文は 2.0×10^{-5} 間隔ごとに X に重ね合わせ，マスキングしている．平文の復号化は，同一の鍵を使って生成した X を暗号文から差し引くことで達成できる．図 3.17 は実際の復号結果である．この実験で復号文が平文と一致することが確認されたため，前節で示したカオスマスキング法が妥当なものであるとわかった．

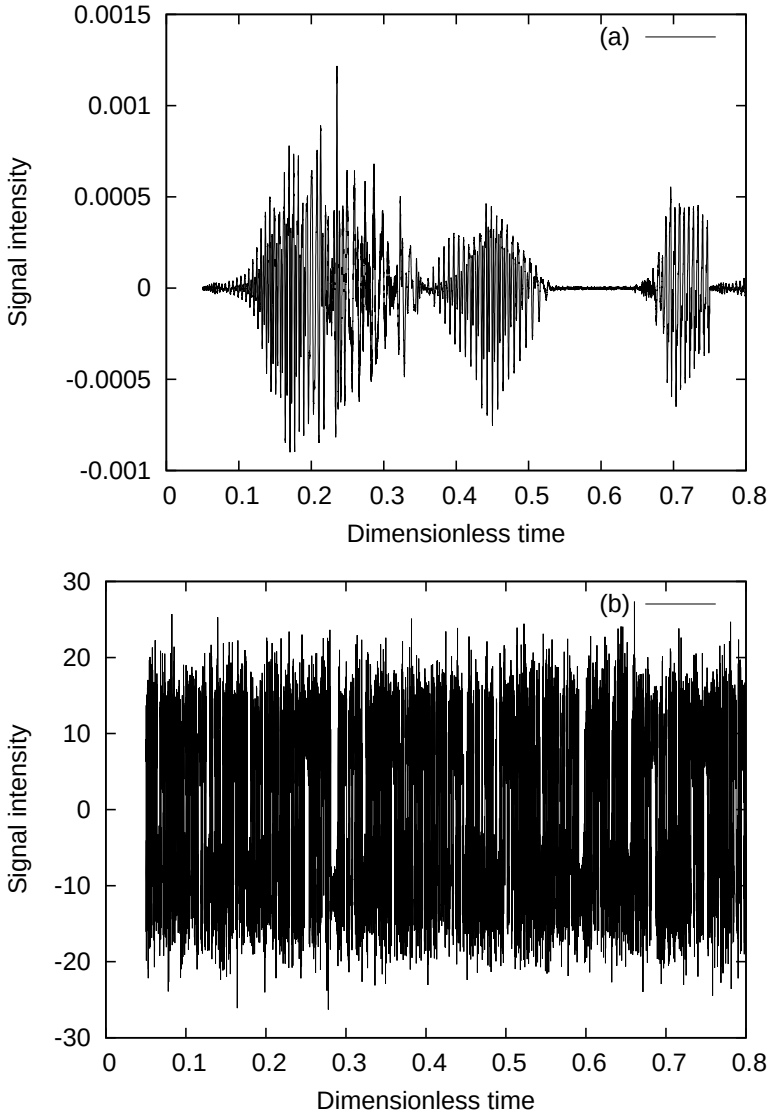

図 3.16: 平文”Yes, we can.”(a) と暗号文 (b)

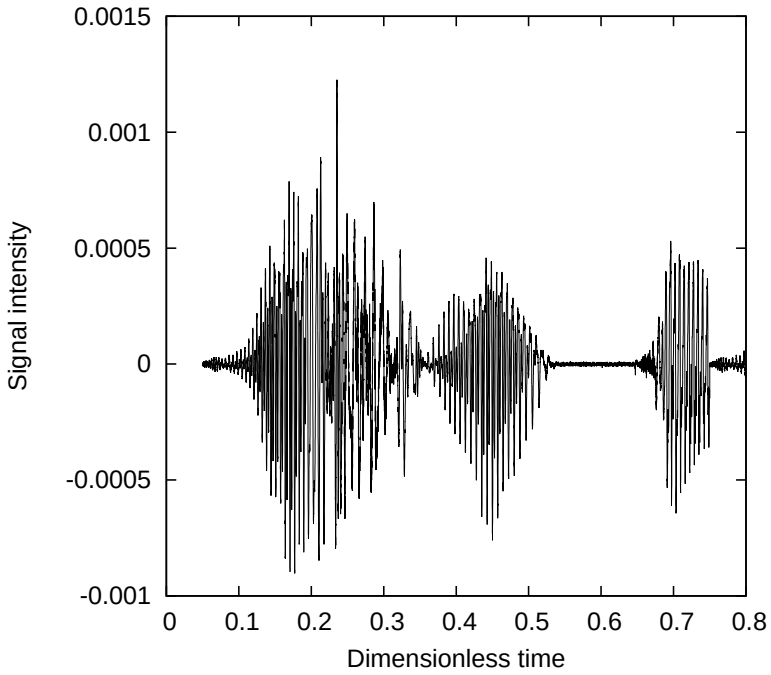

図 3.17: 復号文”Yes, we can.”

3.2.3 盗聴耐性

Eve が秘密鍵を除く，全ての情報を知っていると仮定し，本論文のカオスマスキング法に関する安全性を評価する．

総当たり攻撃

提案したカオスマスキング法が，秘密鍵の特定を狙った総当たり攻撃に対して，耐性があるか調査する．第 3.2.1 節で示したように，M_N の違いにより，式 (3.25) の右辺の対角和に微小な違いが発生する．これにより，Alice と Eve の M_N の違いによって，Alice と Eve の式 (3.25) の右辺の対角和にも違いが発生すると考えられる．もし，その違いが生成される X に大きな違いをもたらさなければ，Eve は暗号文を解読するための M_N の値を設定できる．そうでなければ，Eve は全ての鍵の組み合わせ，つまり，全ての行列 $\mathbf{M}$ の組み合わせを調べる必要がある．

M_N の違いが暗号文の安全性にどの程度，影響があるのかを調べるために，著者は以下のような実験を実施した．まず，前節で示した平文を X を用いて暗号化し，暗号文を得る．次に，この暗号文から X を差し引いて，平文の復号を試みる．この時，暗号文から差し引く X を生成するための拡張 Lorenz 方程式における行列 $\mathbf{M}$ は，暗号化に用いたものと M_N だけが異なるように設定する．実験結果を図 3.18 に示す．ここで，実験に使った Alice と Eve の拡張 Lorenz 方程式のパラメータは，M_N の値を除いて，すべて前節で使用したものに設定している．図 3.19 には復号文と平文のパワースペクトル密度を示す．以上の結果より，M_N の違いが暗号文の解読を妨害していると認められる．これは，M_N が式 (3.25) の右辺の対角和に与える影響が最小であるにもかかわらず，Eve が探索する鍵の組み合わせ数を減らせないことを意味する．鍵の取りうる組み合わせ数は $2^{N-1} = 2^{100} \sim O(10^{30})$ となり，これは Alvarez ら [52] によるところの総当たり攻撃に耐性のある鍵の組み合わせ数に一致する．

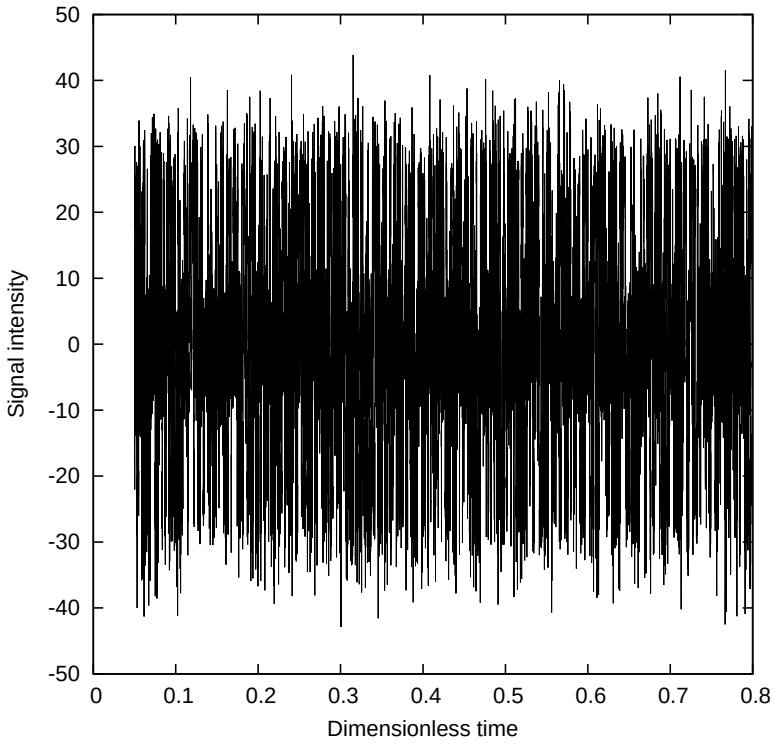

図 3.18: M_N だけが違うときの復号結果（N=101）

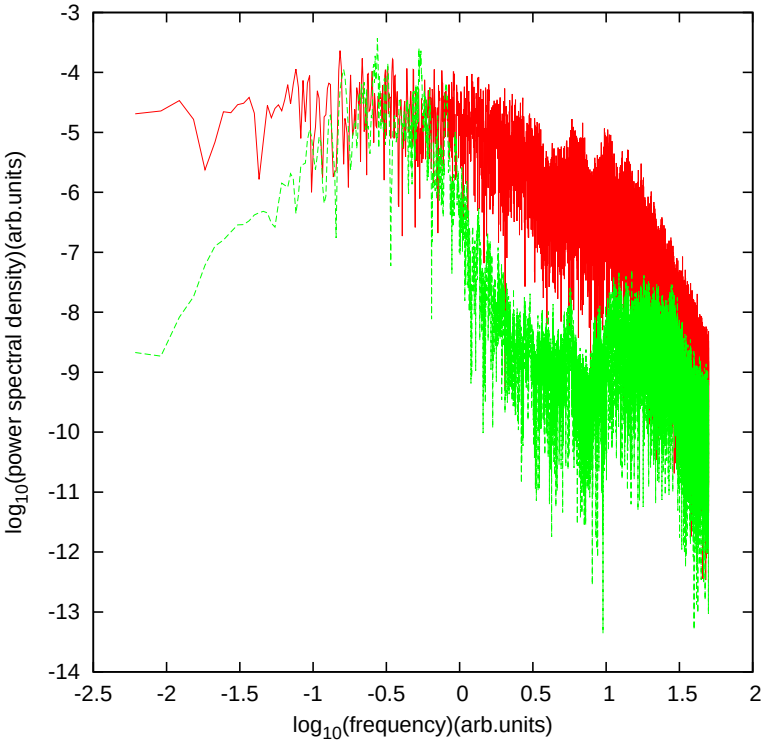

図 3.19: 復号結果のパワースペクトル密度（赤実線）と平文のパワースペクトル密度 (緑破線)

フィルタリング攻撃

フィルタリング攻撃とは，フィルタを用いて，暗号文に隠れた平文を抽出する攻撃方法である．このフィルタリング攻撃に対する耐性を調べるために，マスキング信号 X と暗号文 $X+m$ のパワースペクトル密度を見積もった．図 3.20(a) と図 3.20(b) は，それぞれマスキング信号 X と暗号文 $X+m$ のパワースペクトル密度の結果である．マスキング信号 X と暗号文 $X+m$ のパワースペクトル密度の間には実質的な相違がないため，フィルタを用いて，暗号文に隠れた平文を抽出することはできない．

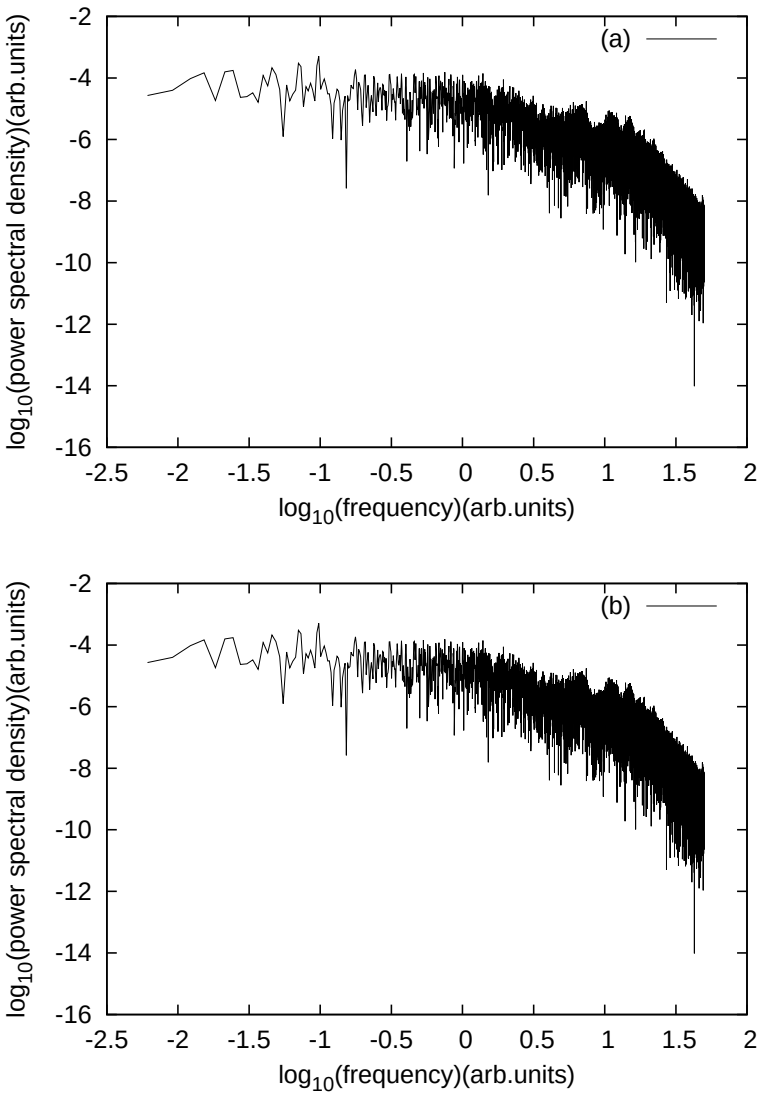

図 3.20: マスキング信号 X のパワースペクトル密度 (a) と暗号文 $X + m$ のパワースペクトル密度

カオス同期を用いた解読法

著者は Eve が Cuomo-Oppenheim 法を攻撃手段に適用した場合，その攻撃方法に対して，本研究のカオスマスキング法が耐性を持っているかを調査した．この実験では，平文として，前節で使用した音声データを使用し，それを X の低周波域に重ねる．このとき，暗号文の作成方法は前節の条件と同一である．Eve は暗号文 $X + m$ を盗聴し，自身の拡張 Lorenz 系の X に直接結合する．ここでは，秘密鍵である行列 $\mathbf{M}$ は Alice のものと偶然一致するが，Eve はその事実を知らないものとする．

この攻撃方法が妥当なものか調べるために，$X + m$ を直接結合した Eve の拡張 Lorenz

方程式を 4 次の Runge-Kutta 法で数値積分する．ここで，数値積分に使用するパラメータは前節のものを使用する．図 3.21 は Alice の $X+m$ と Eve の X の差分の時間変化のグラフである．この結果を音声データに変換したところ，”Yes, we can.” と聞き取ることはできなかった．図 3.22 は図 3.21 の結果のパワースペクトル密度である．見積もったスペクトルは平文である音声データのスペクトルと一致しない．以上の結果から，Cuomo-Oppenheim 法を利用した攻撃方法は有効でないとわかる．

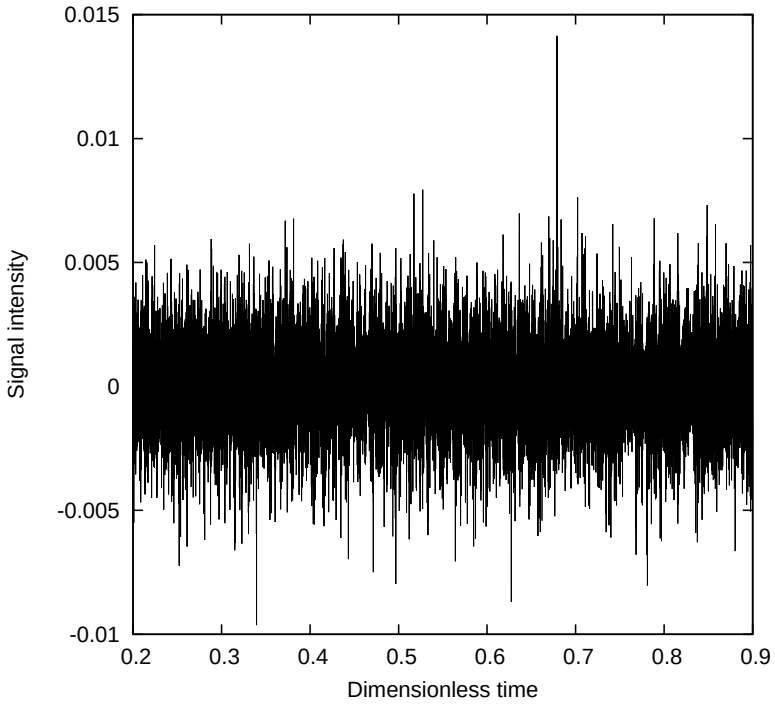

図 3.21: Alice の $X+m$ と Eve の X との差分の時間変化

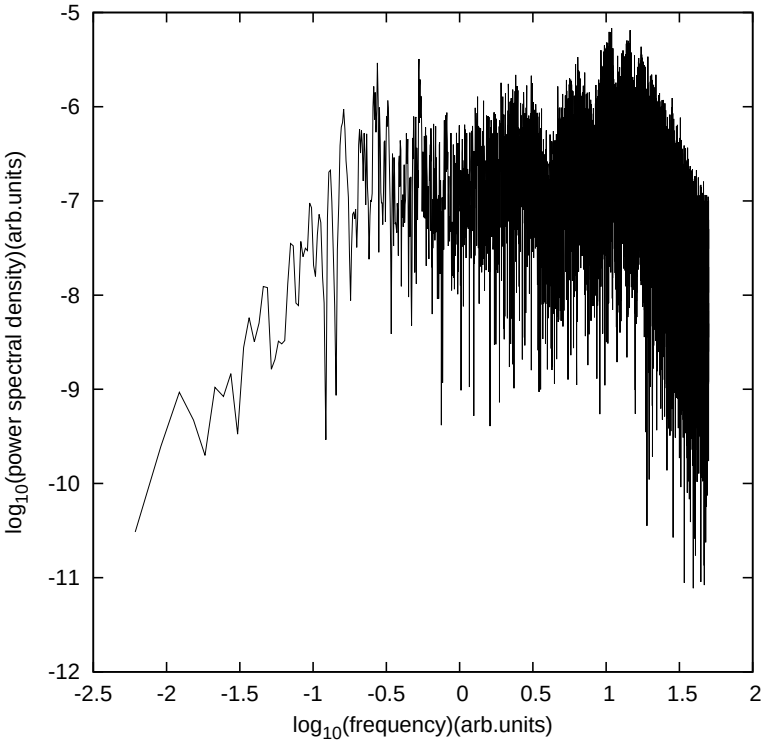

図 3.22: Alice の $X + m$ と Eve の X との差分のパワースペクトル密度

3.3 考察

多数の Lorenz 系を星型ネットワーク状に結合した拡張 Lorenz モデルは，Lorenz モデルの動的性質を継承している．実際，X もしくは $\mathbf{Y}$ を直接結合した拡張 Lorenz 振動子はカオス同期を起こす．これは理論的にも，数値実験的にも確認できた．Lyapunov function を基とした同期誤差の動的安定性に関する理論解析は，パラメータミスマッチがないとき，$e_1 = 0, \mathbf{e}_2 = 0, \mathbf{e}_3 = 0$ が漸近的に安定であると示した．一方，パラメータミスマッチがあるとき，同期誤差が線形的に増加することも示された．また，N の増加に伴い，同期誤差が大きくなることを示した．これは高次元の Lorenz 振動子系では，パラメータミスマッチの影響で，同期誤差が大きくなることを意味する．

本論文で提案したカオス暗号は共有鍵暗号である．しかしながら，この暗号は DES(Data Encryption Standard) や AES（Advanced Encryption Standard）のような暗号とはかなり異なる．本論文のカオス暗号は，2 進数で表現された通信文を一定の長さのブロックに分割することも，そのブロック化された通信文を換字処理，転置処理することもない．Diffie と Hellman の鍵共有方法 [74] と Rivest，Shamir，Adleman の RSA 暗号 [75] のような公開鍵暗号と違い，本論文のカオス暗号は平文の暗号化に一方向関数を利用しない．

本論文のカオス暗号は暗号鍵を一度限りの使い捨てにするワンタイムパッド暗号によく似ている．このカオス暗号において，Alice は自身の秘密鍵で生成した X を疑似乱数として足し合わせることで，平文を暗号化する．Bob は Alice と同じ秘密鍵を使って X を生成し，暗号文から X を取り除くことで平文を復号する．しかしながら，ワンタイムパッド暗号と異なり，秘密鍵の長さを平文よりも大幅に短くできる．秘密鍵 $\mathbf{M}$ の対角要素 $M_n(n \geq 2)$ が n もしくは $n + 1/2$ であるとき，n を 0，$n + 1/2$ を 1，$N = 101$ とすれば，秘密鍵 $\mathbf{M}$ は $N - 1 = 100[bit]$ の情報で表現できる．ここで，鍵の取りうる組み合わせ数は $2^{N-1} = 2^{100} \sim O(10^{30})$ 通りである．この秘密鍵空間は，異なるカオス時系列を大量に生成する．より大きな鍵の取りうる組み合わせ数が必要になったとき，秘密鍵 $\mathbf{M}$ の次元数を大きく設定すればよい．例えば，N は [8] のように $N = 1000$ と設定できる．このような大きな鍵の取りうる組み合わせ数は，鍵の同定を非常に困難にする．

第 3.2 節では，本論文のカオス暗号は音声データの暗号化に適用された．2 値情報の平文を扱うとき，以下のような手順で暗号化を行う．$\sigma = 25, R_0 = 3185, \phi = 0.36[rad]$ の条件下で，変数 X はその符号が正になる確率と負になる確率が等確率である．これはカオスガスタービンの不規則な反転運動に偏りがないことに起因する [8]．この事実に従うと，適切な時間間隔でサンプリングした X の数値解は 2 値の乱数列に変換される．これを乱数電文と呼ぶ．乱数電文を U とし，U は $\{0, 1\}$ の時系列で表現される．U は次式で定義される．

$$\begin{aligned} U(t) &= 0 \; if \; X < 0, \\ &= 1 \; otherwise. \end{aligned}$$

乱数電文 U を使って，Alice は 2 値の平文 m をワンタイムパッド暗号と同じ方法で暗号化することができる．Alice は次式のような XOR(exclusive OR) 演算することで暗号文 V を得る．

$$V = m + U(mod\ 2). \tag{3.60}$$

暗号文を受け取った Bob は，次式を使って暗号文を平文に復号化できる．

$$m = V + U(mod\ 2). \tag{3.61}$$

第4章　カオス暗号と量子鍵配送

4.1　古典的手法と量子物理学的手法

前章で提案したカオスマスキング法は，Alice と Bob の間で秘密鍵である行列 $\mathbf{M}$ を共有するため，共有鍵暗号に分類される．共有鍵暗号には，如何にして秘密鍵を安全に共有するかという鍵配送問題が存在する．ここでは，鍵配送問題を解決する手段として，古典的手法と量子物理学的手法を紹介する．

4.1.1　公開鍵暗号

公開鍵暗号とはあらかじめ公開された鍵を暗号化プロセスに使用する暗号手法である．公開鍵暗号として，Diffie と Hellman の鍵共有方法と Rivest，Shamir，Adleman の RSA 暗号が有名である．これ以外にも公開鍵暗号は存在するが，本論文では，この 2 つに絞って，その原理を説明する．

Diffie-Hellman 鍵共有法

鍵配送問題を解決する古典的手法として，Diffie と Hellman の鍵共有方法が挙げられる．本論文では，これを Diffie-Hellman 鍵共有法と呼ぶ．Diffie-Hellman 鍵共有法とは離散対数問題の困難性を上手く利用した鍵共有手法である．モジューラ関数の世界において，べき乗の計算は簡単にできる．逆に，$a^x = b(mod\ n)$ となる剰余 b を知った時に，a を何乗して n で割れば剰余が b になるかを計算するのは困難である．何故なら，$a^k(mod\ n)$ とし，k を 1 から順に代入しても，$a^k(mod\ n)$ はあたかも乱数のように値が変化し，簡単に次が予測できないからである．これを離散対数問題の困難性と呼ぶ．

Diffie-Hellman 鍵共有法の鍵共有過程を通信者 Alice と Bob の例で示す．Diffie-Hellman 鍵共有法は $Y^x(mod\ P)$ というモジューラ関数を基礎とする．Alice と Bob は安全でない回線で Y と P の値を取り決める．ここでは簡単のために，$Y = 9, P = 11$ に設定する．次に，Alice は数を 1 つ選び（例えば 4），それを秘密にしておく。同様に Bob も数を 1 つ選び (例えば 8)，それを秘密にする．ここで，Alice の数を A，Bob の数を B とする．Alice は x に 4 を代入し，$9^A(mod\ 11)$ を計算する．$9^4(mod\ 11) = 6561(mod\ 11) = 5$．同様に，Bob も $x = 8$ とし，$9^B(mod\ 11)$ を求める．$9^8(mod\ 11) = 43046721(mod\ 11) = 3$．Alice は計算結果を α，Bob は計算結果を β とし，安全でない回線でこの二つの計算結果を交換する．Alice は Bob の結果を受け取り，$\beta^A(mod\ 11)$ を計算する．$3^4(mod\ 11) = 81(mod\ 11) = 4$．同様に Bob は Alice の結果から，$\alpha^B(mod\ 11)$ を計算する．$5^6(mod\ 11) = 390625(mod\ 11) = 4$．これはモジューラ関数で $(Y^A)^B = (Y^B)^A = Y^{AB}$ を計算しているだけなので，Alice と

Bob が Y, A, B にどのような値を設定しても，Alice と Bob は最終的に同じ値を得られる．この最終値を共有鍵暗号の鍵とするのが Diffie-Hellman 鍵共有法である．

盗聴者 Eve の立場から，Diffie-Hellman 鍵共有法が安全であることを示す．Alice と Bob の通信を盗聴した Eve が得るのは，次の情報である．関数が $9^x(mod\ 11)$ であること，Alice は $\alpha = 5$ を，Bob は $\beta = 3$ を送ったこと．Eve が鍵を突き止めるには，Bob と同様，B を知っていて α を鍵に変換するか，Alice と同様，A を知っていて β を鍵に変換するかしなければならない．しかしながら，Alice と Bob は A と B を秘密にしているため，Eve はこれらの数を知らない．そのため，Eve が A と B を知る方法は，関数 $9^x(mod\ 11)$ と α または β から，A と B を逆算するしかない．しかしながら，離散対数問題の困難性より，剰余 α または β から，A と B を逆算するのは，使用される数が大きくなればなるほど困難になる．A, B を逆算することが困難であるため，Diffie-Hellman 鍵共有法は現在の計算機の性能上，安全である．

RSA 暗号

Diffie-Hellman 鍵共有法の他に，Rivest，Shamir，Adleman の公開鍵暗号が挙げられる．本論文では，これを RSA 暗号と呼ぶ．RSA 暗号は素因数分解の困難性を上手く利用した暗号方式である．例えば，15 を素因数分解すると，15 は 3 と 5 に分けられる．15 のような小さな桁の数を素因数分解するのは簡単だが，もっと桁の大きな数，例えば，300 桁以上の数を素因数分解するのは非常に困難である．これが素因数分解の困難性である．

公開鍵と秘密鍵の生成過程を示す．まず，2 つの異なる大きな素数 p, q をランダムに選び，その積 $n = pq$ を計算する．次に，$n = pq$ のオイラー関数 $\phi = (p-1)(q-1)$ に対し，これと互いに素となるような整数 e をランダムに選ぶ．ここで，互いに素とは，2 つの整数の最大公約数が 1 であることを意味する．さらに，$ed = 1(mod\ \phi)$ となるような整数 d を求める．つまり，適当な整数値 k に対して $ed = k\phi + 1$ となるような d を求める．こうして 3 つの鍵 n, e, d を生成した Alice は，n, e を公開鍵として公開し，d を秘密鍵として保管する．

前述した公開鍵と秘密鍵を使った暗号化，復号化手順について示す．Bob が Alice に平文 m を送りたいとする．ここで，平文 m は文字列を数字に変換したものである．Bob は Alice の公開鍵 n, e を持ってきて，$c = m^e(mod\ n)$ を計算し，c を暗号文として Alice に送る．Bob からの暗号文 c を受け取った Alice は，自分の秘密鍵 d を使って，平文を復号化する．ここで，復号化の計算式は $m = c^d(mod\ n)$ である．なお，オイラーの定理より，復号化の計算式の右辺は次式とできる．

$$c^d = m^{ed} = m^{k\phi+1} = (m^\phi)^k m = m(mod\ n)$$

盗聴者 Eve の立場から，RSA 暗号が安全であることを示す．Eve が復号化に必要な秘密鍵 d を知るために利用できる情報は，公開鍵である n, e 及び，暗号文 c である．RSA の鍵の生成手順から，d がわかるためには e, ϕ が必要であり，ϕ がわかるためには p, q が必要になる．よって，p, q が明らかになると，公開されている e から d がわかる．しかしながら，p, q を明らかにするためには，公開されている n から p, q を素因数分解する必要が

ある．上述したように，非常に大きな数の素因数分解は困難であるため，n を非常に大きな数に設定してやれば，RSA 暗号の安全性は現在の計算機の性能では担保される．

4.1.2 量子鍵配送 (BB84)

鍵配送問題を解決する量子物理学的手法として，Bennett，Brassard の量子鍵配送法 [55] が挙げられる．本論文では，これを BB84 と呼ぶ．BB84 は量子物理学を上手く利用した鍵配送法である．ここで，量子物理学とは不確定性原理と重ね合わせ状態複製不可能である．

次に，BB84 の鍵配送手順を示す．Alice はまず，光子を垂直方向（0 と $\pi/2$）に偏光させる+スキームと，斜め方向 ($-\pi/4$ と $\pi/4$) に偏光させる $\times$ スキームをランダムに選択することにより，1 と 0 のランダムな並びを Bob に送信する．ここで，0 と $-\pi/4$ に偏光された光子は 0 を，$\pi/2$ と $\pi/4$ に偏光された光子は 1 を表しているとする．この時，Alice は各光子に対して使った偏極スキームを秘密にしておく．Bob は送られてきた光子の偏光を測定する．Bob は Alice が各光子に対して使った偏極スキームを知らないので，0 と $\pi/2$ に偏光された光子を正確に測定できる+検出器と $-\pi/4$ と $\pi/4$ に偏光された光子を正確に測定できる $\times$ 検出器をランダムに交換して用いる．この際，正しい偏極の検出器を選ぶこともあれば，Alice の設定した偏極と異なる検出器を選ぶこともある．Bob が異なる検出器を選べば，Alice の光子の偏光を間違って測定する場合が出てくる．Bob は Alice の 1 と 0 の並びを，いくつかは正しく，いくつかは間違って測定している．そこで，Alice と Bob は（安全ではない）通常の回線で連絡を取り合い，Alice は各光子に対して，自分がどの偏極スキームを使ったかを教える．ただし，各光子の偏光は教えない．つまり，Alice は最初の光子に対して+スキームを使ったことは教えるが，光子の偏光が 0 であるのか，$\pi/2$ であるのかは教えない．次に，Bob はどの光子に対して正しい検出器を選んだかを Alice に伝える．Bob が正しい検出器を選んだ場合，Bob は光子の偏光を正しく測定し，正しい 0 または 1 を得る．最後に，Alice と Bob は，Bob が間違った検出器を選択したケースは破棄し，正しい検出器を選んだケースだけを残す．このようにして Alice と Bob は，Bob が正しく測定した結果だけから構成される 1 と 0 の並びを得る．この最終的な 1 と 0 の並びを共有鍵暗号の鍵とするのが BB84 である．

盗聴者 Eve に対して，BB84 が安全であることを示す．Alice が光子を送信すると，Eve はその光子の偏光を測定することで，鍵を盗聴しようとする．しかしながら，Eve は各光子が+スキームで偏光されたのか，$\times$ スキームで偏光されたのかわからない．そのため，Eve はでたらめに検出器を選び，約半分の光子を間違った検出器で測定するだろう．そして，Alice は Bob に各光子の偏極スキームを教え，Bob が正しい検出器を使った時の測定結果だけを使って鍵を作る．Eve はこれを盗聴するが，Eve にとって，正しいスキームはどれであったかという情報は意味がない．なぜなら，Eve は不確定性原理により，Bob が正しい検出器を使って測定した光子の半数を間違って検出しているため，最終的に鍵として使用される光子の中にも間違った解釈をしたものがあるはずだからである．この他にも，Alice が送信した光子を Eve が複製，保管しておき，通常回線で Alice が Bob に各光子の偏極スキームを教えた段階で，正しい検出器で光子の正しい偏光を得る盗聴方法が考えられる．しかしながら，波動関数の重ね合わせ状態は複製できないという量子物理学の法則 [65, 66] があるため，Alice が送信した光子を Eve が複製することは不可能である．以上の 2 点，つまり，量子の法則によって，BB84 の安全性は守られる．

最後に，BB84 では Eve の盗聴を検知できることを示す．Alice が $-\pi/4$ に偏光した光子を送り，Eve が正しくない検出器（+検出器）で測定したとする．+検出器は $-\pi/4$ に偏光した光子を，0 に偏光された光子もしくは，$\pi/2$ に偏光された光子に変化させる．もし

も，Bob が変化させられた光子を × 検出器で測定すれば，Bob は Alice が送信しなかった $\pi/4$ を検出するかもしれない．つまり，この結果は Bob が正しい検出器を使ったにもかかわらず，Eve の盗聴により，間違った結果を得る場合があるということを示している．しかしながら，この間違いは Alice と Bob が簡単なエラーチェックを行うことにより発見できる．エラーチェックは，Alice と Bob が正しく測定した結果だけから構成される 1 と 0 の並びを得た後に行われる．Alice と Bob は正しく測定した結果だけから構成される 1 と 0 の並びから，いくつかをランダムに取り出して，（安全ではない）通常回線で比較する．ランダムに取り出す 1 と 0 の bit 数がある程度大きいとき，比較結果が一致すれば，Eve が盗聴していた可能性は低くなる．ただし，検出器側の誤動作により，ある程度の誤検出は現れる．比較結果に誤検出以上の誤差を発見すれば，Eve が盗聴していたことがわかるため，共有した鍵は破棄し，もう一度，鍵共有をやり直す．

4.2 カオス暗号への応用

カオス暗号が信頼性の低い暗号と位置付けられてきた理由の 1 つに，安全な鍵配送の手段がないことが挙げられる．本研究のカオスマスキング法の秘密鍵である行列 $\mathbf{M}$ を，古典的手法である公開鍵暗号，もしくは，量子物理学的手法である BB84 で配送することで，信頼性の高いカオス暗号を実現できる．ここでは，公開鍵暗号と BB84 を用いた秘密鍵 $\mathbf{M}$ の配送方法を記載する．

4.2.1 公開鍵暗号

Diffie-Hellman 鍵共有法

Diffie-Hellman 鍵共有法を使って，秘密鍵 $\mathbf{M}$ を配送する方法を示す．Alice と Bob はモジューラ関数を設定し，秘密の数字 A 及び B から，共通の数 K を得る．この K を $mod\ 10$ を用いて，0 から 9 までの数値に変換する．$n-0.8, n-0.6, \ldots, n+0.8, n+0.1$ の中から，$K(mod\ 10)+1$ 番目に小さな数を $M_n(n \geq 2)$ に設定する．これを 30 回繰り返すことで，$N = 31$ の行列 $\mathbf{M}$ を共有できる．この時，鍵の取りうる組み合わせ数は，10 通りの組み合わせが 30 個あることから，10^{30} 通りとなる．

RSA 暗号

同様に，RSA 暗号を用いた秘密鍵 $\mathbf{M}$ を配送方法を示す．Alice はある数 K を Bob の公開鍵で暗号化し，Bob に送る．Bob は秘密鍵で暗号文を復号化し，K を得る．Alice と Bob は K を 2 進数で表記し，共通の 1 と 0 の列を得る．数列の x 番目を参照し，その数値が 0 ならば n を，1 ならば $n+1/2$ を $M_n(n \geq 2)$ に設定する．これを $x+99$ 番目まで繰り返すことで，$N = 101$ の行列 $\mathbf{M}$ を共有できる．ここで，x は任意の数である．この場合，鍵の取りうる組み合わせ数は 10^{30} 通りを超える．

4.2.2 量子鍵配送 (BB84)

BB84 を用いた秘密鍵 $\mathbf{M}$ の配送方法は以下のようになる．Alice と Bob は BB84 を使って，共通の 1 と 0 の並びを得る．RSA の場合と同様，数列の x 番目を参照し，その数値が 0 ならば n を，1 ならば $n+1/2$ を $M_n(n \geq 2)$ に設定する．この作業を $x+99$ 番目まで繰り返し，$N = 101$ の行列 $\mathbf{M}$ を共有する．

公開鍵暗号を使った鍵配送方法よりも，BB84 を使った鍵配送方法の方が安全である．何故なら，公開鍵暗号の安全性の根拠となっている離散対数問題や素因数分解の問題は，量子コンピュータの実現で簡単に解かれてしまうからである．しかしながら，BB84 も長距離間の通信が困難であるという問題と，共有する鍵の長さが長くなれば通信に時間がかかるという欠点がある．

本研究で提案するカオスマスキング法を併用すれば，通信に時間がかかるという欠点を克服することができる．カオスマスキング法で使用する秘密鍵 $\mathbf{M}$ は，0 を n，1 を $n+1/2$ に変換したものであるので，$N = 101$ であるのならば，100bit の情報量で表現できる．BB84 の原理から，200 回，光子を送れば，半数の約 100 個の光子の偏光を正しく測定でき，約 100bit の 0 と 1 の並びを得る．ゆえに，約 200 個の光子を送るだけで，秘密鍵 $\mathbf{M}$ を共有することが可能となる．

第5章　結言

著者は，拡張 Lorenz 方程式に従うカオスガスタービンを開発した．拡張 Lorenz 方程式はカオスガスタービンの運動方程式を無次元化したものである．拡張 Lorenz モデルは $2N+1$ 次元の常微分方程式で表される．N は圧力を Fourier 級数展開した時の切り捨て数であるため，N は有限の数となる．$N=1$ の時，拡張 Lorenz モデルは $b=1$ の Lorenz 方程式と一致する．従って，拡張 Lorenz モデルは Lorenz モデルの動力学的性質を引き継いでいる．拡張 Lorenz モデルは，無次元化された角速度である X を中心ノードとして，N 個の Lorenz 系を結合した星型ネットワーク構造として表現される．

カオスガスタービンは，換算 Rayleigh 数 R_0 と Prandtl 数 σ によって，カオス挙動だけでなく，規則運動も生成する．Rayleigh 数 R_0 と Prandtl 数 σ はタービンの機械パラメータの関数である．タービンのロータの不規則な反転運動は，10^6 を超える高い Rayleigh 数の Rayleigh-Bénard 対流の乱流時の平均風の不規則な反転運動を連想させる．著者は，タービンのロータの角速度の統計的性質と平均風の速度場の統計的性質とが定量的に一致することを示した．拡張 Lorenz モデルの不規則な反転運動は二重井戸ポテンシャルと内部ノイズに起因する X の確率共鳴から引き起こされる．これらの結果は，拡張 Lorenz モデルが乱流時の平均風の力学モデルとして利用可能であることを示している．しかしながら，Rayleigh-Bénard 対流の温度場を拡張 Lorenz モデルがモデル化しているのかはわかっていない．拡張 Lorenz モデルと Boussinesq 方程式との数学的関係も未解決の問題である．

Lyapunov function を基礎とする理論解析は，X もしくは $\mathbf{Y}$ を直接結合した拡張 Lorenz 振動子がカオス同期を起こすことを明らかにした．拡張 Lorenz 振動子間のパラメータミスマッチは同期誤差を線形的に増加させることも示された．数値実験において，直接結合された拡張 Lorenz 振動子間の同期誤差を見積もった．実験結果は上述した理論予測と一致する．

著者は一般化された拡張 Lorenz 方程式を示した．秘密鍵 $\mathbf{M}$ は 2 値情報に変換することができ，2 値化された秘密鍵の長さは平文の長さよりも一般に短い．X を直接結合したパラメータミスマッチのない拡張 Lorenz 振動子は，完全に同期する．しかしながら，X に低周波数の通信文が加えられると，同期には至らない．この現象は暗号文の盗聴による秘密鍵の同定を妨害するという点で有益である．

以上の結果を基として，共有鍵タイプのカオス暗号に一般化された拡張 Lorenz 方程式を適用させる方法を提案した．この方法では，BB84 を Alice と Bob 間の秘密鍵の共有に使用することが想定されている．通信文 (平文) はカオス信号 X でマスキングし，暗号文は Alice から Bob へ古典チャネルを通じて送られる．暗号文は秘密鍵を使って生成された同一のカオス信号 X を取り除くことで復号される．鍵の取りうる組み合わせ数は $2^{N-1}(N>100)$ 通りであり，本研究のカオスマスキング法は Eve の解読法である総当たり攻撃，フィルタリング攻撃，カオス同期を利用した攻撃を防ぐことができる．

参考文献

[1] E. N. Lorenz,"Deterministic nonperiodic flow,'' *J. Atmos. Sci.* **20**, 130–141 (1963).

[2] B. Saltzman,"Finite amplitude free convection as an initial value problem-I, '' *J. Atmos. Sci.* **19**, 329–341 (1962).

[3] J. P. Eckmann,"Roads to turbulence in dissipative dynamical systems,'' *Rev. Mod. Phys.* **53**, 643–654 (1981).

[4] R. Barrio and S. Serrano,"A three-parametric study of the Lorenz model,'' *Physica* D **229**, 43–51 (2007).

[5] R. Barrio and S. Serrano,"Bounds for the chaotic region in the Lorenz model, '' *Physica* D **238**, 1615–1624 (2009).

[6] S. H. Strogatz, *Nonlinear Dynamics and Chaos* (Perseus Books Publishing, 1994) 301–347.

[7] M. Kolar and G. Gumbs,"Theory for the experimental observation of chaos in rotating waterwheel, '' *Phys. Rev.* A. **45**, 626–637, (1992).

[8] K. Cho, T. Miyano and T. Toriyama,"Chaotic gas turbine subject to augmented Lorenz equations, '' *Phys. Rev.* E. **86**, 036308-1–036308-12, (2012).

[9] A. H. Epstein and S. D. Senteria,"Macro Power from Micro Machinary, '' *Science* **276**, 1211 (1997).

[10] A. H. Epstein and J. Eng," Millimeter-Scale, Micro-Electro-Mechanical Systems Gas turbine Engines, '' *Gas Turbine Power* **226**, 205–226 (2004).

[11] S. Grossman and D. Lohse,"Scaling in thermal convection: a unifying theory, '' *J. Fluid. Mech.* **407**, 27 (2000).

[12] J. J. Niemela, L. Skerbek, K. R. Sreenivasan and R. J. Donnelly,"Turbulent convection at very high Rayleigh numbers, '' *Nature* **404**, 837–840 (2000).

[13] E. van Doorn, B. Dhruva, K. R. Sreenivasan and V. Cassella,"Statistics of wind direction and its increments, '' *Phys. Fluids* **12**, 1529 (2000).

[14] Y. B. Du, and P. Tong,"Temperature fluctuations in a convection cell with rough upper and lower surfaces, '' *Phys. Rev.* E. **63**, 046303-1–046303-7, (2001).

[15] X. Chavanne, F. Chilla, B. Chabaud, B. Castaing and B. Herbral,"Turbulent Rayleigh-Bénard convection in gaseous and liquid He,'' *Phys. Fluids* **13**, 1300 (2001).

[16] J. Zhang, S. Childress and A. Libchaber,"Non-Boussinesq effect: Thermal convection with broken symmetry,'' *Phys. Fluids* **9**, 1034 (2001).

[17] J. J. Niemela, L. Skerbek, K. R. Sreenivasan and R. J. Donnelly,"The wind in confined thermal convection,'' *J. Fluid Mech* **449**, 169–178 (2001).

[18] K. R. Sreenivasan, A. Bershadskii and J. J. Niemela,"Mean wind and its reversal in thermal convection,'' *Phys. Rev.* E. **65**, 056306-1–056306-11, (2002).

[19] J. J. Niemela, and K. R. Sreenivasan,"Confined turbulent convection,'' *J. Fluid Mech* **481**, 355–384 (2003).

[20] D. Funfschilling, and G. Ahlers, "Plume motion and large-scale circulation in a cylindrical Rayleigh-Bénard cell,'' *Phys. Rev. lett.* **92**, 194502-1–194502-4, (2004).

[21] S. Grossman and D. Lohse," Fluctuations in turbulent Rayleigh-Bénard convection: The role of plumes,'' *Phys. Fluids* **16**, 4462– (2004).

[22] Y. Tsuji, T. Mizuno, T. Mashiko and M. Sano, "Mean wind in convective turbulence of mercury,'' *Phys. Rev. lett.* **94**, 034501-1–034501-4, (2005).

[23] R. Benzi, "Flow reversal in a simple dynamical model of turbulence,'' *Phys. Rev. lett.* **95**, 024502-1–024502-4, (2005).

[24] F. F. Araujo, S. Grossmann and D. Lohose, "Wind reversals in turbulent Rayleigh-Bénard convection,'' *Phys. Rev. lett.* **95**, 084502-1–084502-4, (2005).

[25] E. Brown, A. Nikolaenko and G. Ahlers, "Reorientation of the large-scale circulation in turbulent Rayleigh-Bénard convection,'' *Phys. Rev. lett.* **95**, 084503-1–084503-4, (2005).

[26] C. Resagk, R. du Puits, A. Thess, F. V. Dolzhansky, S. Grpssmann, F. F. Araujo, S. Grossmann and D. Lohose, "Oscillations of the large scale wind in turbulent thermal convection,'' *Phys. Fluids* **18**, 095105, (2006).

[27] K. R. Sreenivasan and A. Bershadskii,"Clustering properties in turbulent signals,'' *J. Stat. Phys* **125**, 1145–1157, (2006).

[28] E. Brown and G. Ahlers, "Large-scale circulation model for turbulent Rayleigh-Bénard convection,'' *Phys. Rev. lett.* **98**, 134501-1–134501-4, (2007).

[29] E. Brown and G. Ahlers, "A model of diffusion in a potential well for the dynamics of the large-scale circulation in turbulent Rayleigh-Bénard convection,'' *Phys. Fluids* **20**, 075101, (2008).

[30] E. Brown and G. Ahlers, "Azimuthal asymmetries of large-scale circulation in turbulent Rayleigh-Bénard convection, '' *Phys. Fluids* **20**, 105105, (2008).

[31] M. S. Emran, and J. Schumacher, "Fine-scale statistics of temperature and its derivatives in convective turbulence, '' *J. Fluid Mech* **611**, 13–34 (2008).

[32] X. He, and P. Tong, "Measurements of the thermal dissipation field in turbulent Rayleigh-Bénard convection, '' *Phys. Rev.* E. **79**, 026306-1–026306-14, (2009).

[33] A. Bershadskii, "Chaos from turbulence: Stochastic-chaoticequilibrium in turbulent convection at high Rayleigh numbers, '' *Chaos* **20**, 043124-1–043124-5, (2010).

[34] E. D. Siggia, "High Rayleigh number convection, '' *Annu. Rev. Fluid Mech.* **26**, 137–167, (1994).

[35] G. Ahlers, S. Grossmann and D. Lohose, "Heat transfer and large scale dynamics in turbulent Rayleigh-Bénard convection, '' *Rev. Mod. Phys.* **81**, 503–536, (2009).

[36] R. Krishnamurti and L. N. Howard, "Large-scale flow generation in turbulent convection, '' *Proc. Natl. Acad. Sci.* **78**, 1981–1985, (1981).

[37] K. M. Cuomo, and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications, '' *Phys. Rev. lett.* **71**, 65–68, (1993).

[38] K. M. Cuomo, A. V. Oppenheim and S. H. Strogatz, "Synchronization of Lorenbased chaotic circuits with applications to communications, '' *IEEE Trans. Circuit Syst.* II. **40**, 626–633, (1993).

[39] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fisher, J. Garcia-Ojarvo, C. R. Mirasso, L. Pesquera and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-opticlinks, '' *Nature.* **437**, 343–346, (2005).

[40] H. Dedieu, M. Kennedy and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits, '' *IEEE Trans. Circuit Syst.* II. **40**, 634–642, (1993).

[41] S. Hayes, C. Grebogi, E. Ott and A. Mark, "Experimental cntrol of chaos for communications, '' *Phys. Rev. lett.* **73**, 1781–1784, (1994).

[42] Y. Lai, E. Bolt and C. Grebogi, "Communicationg with chaos using two-dimensional symbolic dynamics, '' *Phys. lett.* A **255**, 75–81, (1999).

[43] T. Miyano, K. Nishimura and Y. Yoshida, "Chaos-based communications using open-plus-closed-loop control, '' *IEICE Trans. Fundamentals* **E94-A**, 282–289, (2011).

[44] R. Tenny, L. S. Tsimring, L. Larson and H. D. I. Abarbanel, "Using distributed nonlinear dynamics for public key encryption, '' *Phys. Rev. lett.* **90**, 047903-1–047903-4, (2003).

[45] R. Tenny and L. S. Tsimring, "Additive mixing modulation for public key encryption based on distributed dyanmics, '' *IEEE Trans. Cirecuits Syst.-I* **52**, 672–679, (2005).

[46] L. Kocarev, M. Sterjev, A. Fekete and G.Vattay,"Public-key encryption with chaos, '' *Chaos* **14**, 1078–1082, (2004).

[47] N. Masuda, G. Jakimoski, K. Aihara and L. Kocarev, "Chaotic block chipers: from theory to practical algorithums, '' *IEEE Trans. Circuit Syst.* I. **53**, 1341–1352, (2006).

[48] F. Anstett, G. Millerioux and G. Bloch, "Chaotic cryptosystems: Cryptanalysis and Indentifiability, '' *IEEE Trans. Circuit Syst.* I. **53**, 2673–2680, (2006).

[49] D. Arroyo, S. Li, C. Li and V. Fernandez,"Cryptanalysis of a new chaotic cryptosystem based on ergodicity, '' *INt. J. Mod. Phys* B **23**, 651–659, (2009).

[50] W. Xu, L. Wang and G. Chen, "Performance analysis of the CSDCSK/BPSK communication system, '' *IEEE Trans. Circuit Syst.* I. **61**, 2624–2633, (2014).

[51] P. Muthukumar, P. Balasubramaniam and K. Ratnavelu,"Synchronization and an application of a novel fractional order King Cobra chaotic system, '' *Chaos* **24**, 033105-1–033105-10, (2014).

[52] G. Alvarez and S. Li "Some basic cryptographic requirements for chaos-based cryptosystems, '' *Int. J. Bifurcation Chaos.* **16**, 2129–2151, (2006).

[53] L. M. Pecora, and T. L. Carroll, "Synchronization in chaotic systems, '' *Phys. Rev. lett.* **64**, **8**, 821–824, (1990).

[54] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals, '' *Phys. Rev.* A. **44**, 2374–2383, (1991).

[55] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing ,'' *Proc. IEEE Int. Conf. Computers, Systems & Signal Processing* (Bangalore, India) **1**, 175–179, (1984).

[56] A. K. Ekert, "Quantum cryptography based on Bell's theorem , '' *Phys. Rev. lett.* **67**, 661–663, (1991).

[57] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden "Quantum cryptography , '' *Rev. Mod. Phys.* **74**, 145–195, (2002).

[58] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus and M. Peev, "The security of practical quantum key distribution , '' *Rev. Mod. Phys.* **81**, 1301–1350, (2009).

[59] A. K. Ekert and R. Renner, "The ultimate physical limits of privacy,'' *Nature.* **507**, 443–447, (2014).

[60] A. Einstein, B. Podolski and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?,'' *Phys. Rev.* **47**, 777–780, (1935).

[61] D. Bohm, *Quantum Theory* (Prentice Hall, Inc., New York, 1951).

[62] J. S. Bell, "On the problem of hidden variables in quantum mechanics,'' *Rev. Mod Phys.* **38**, 447–452, (1966).

[63] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, "Proposed experiment to test local hidden-variable theories,'' *Phys. Rev. lett.* **23**, 880–884, (1969).

[64] A. Aspect, P. Grangier and G. Roger, "Experimental tests of realistic local theories via Bell's theorem,'' *Phys. Rev. lett.* **47**, 460–463, (1981).

[65] D. Dicks, "Communication by EPR devices,'' *Phys. lett.* **92A**, 271–272, (1982).

[66] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned,'' *Nature.* **299**, 802–803, (1982).

[67] J. H. Curry, "A generalized Lorenz system,'' *Commun. Math. Phys.* **60**, 193–204, (1978).

[68] J. B. McLaughlin and P. C. Martin, "Transition to turbulent in a statically stressed fluid system,'' *Phys. Rev.* A **12**, 186–203, (1975).

[69] P. Manneville and Y. Pomeau, "Different ways to turbulence in dissipative dynamical systems,'' *Physica* D **1**, 219–226, (1980).

[70] M. Dubois, M. A. Rubio and P. Berge, "Experimental Evidence of Intermittencies Associated with a Subharmonic Bifurcation,'' *Phys. Rev.* Lett **51**, 1446–, (1983).

[71] L. D. Landau and E. M. Lifshitz, *Mechanics-Course of Theoretical Physics Volume 1*, 3rd ed. (Elsevier, New York, 1976), Chap.5.

[72] S. Boccaletti, L. M. Pecora and A. Pelaez, "Unifying framework for synchronization of coupled dynamical systems,'' *Phys. Rev.* E **63**, 066219-1–, (2001).

[73] K. Yoshimoto, K. Cho, Y. Morita and T. Miyano, "Synchronization of coupled augmented Lorenz oscillators with parameter mismatch,'' *Nonlinear Theory and Its Applications, IEICE* (Bangalore, India) **4**, 341–350, (2013).

[74] W. Diffie and M. E. Hellman, "New directions in cryptography,'' *IEEE Trans. Inform. Theory* **IT-22**, 664–654, (1976).

[75] R. L. Rivest, A. Shamir and L. Adleman, "On a method for obtaining digital signature and publickey cryptosystems,'' *Commun. ACM* **2**, 120–126, (1978).

謝辞

本研究を遂行するにあたり，終始変わらぬご指導，ご教鞭を賜りました立命館大学大学院理工学研究科宮野尚哉教授に深い敬意と感謝の意を表します．

また，ガスタービン作製にあたって，タービン設計や実験に数々のご協力をいただいた立命館大学大学院理工学研究科 鳥山寿之教授に感謝の意を表します．

本研究の遂行にあたって数多くのご助力，ご助言を賜りました Mr. Achkbar Farhdhyan をはじめとするマイクロデザイン・エンジニアリング研究室の皆様に深く感謝いたします．

最後に，研究を進めるにあたり, 数多くの励ましを頂いた知能マイクロシステム研究室の在学生および卒業生の皆様に御礼申し上げますとともに，大学院生活全般において惜しまず援助を送り続けてくれた家族に心より敬意と感謝を表します．