研究シーズ探索プログラム　研究課題別評価書

１．研究課題名

コンシステンシーに基づく情報セキュリティ技術

２．研究代表者

内田　淳史（埼玉大学　大学院理工学研究科　数理電子情報部門情報領域　准教授）

３．研究シーズ探索成果の概要

現在の情報セキュリティはソフトウェアによる暗号化・復号化が主流であるが、安全性の論拠は計算量的複雑性に依存しているため、計算機の進展や量子計算機の登場による脆弱性が指摘されている。そこでコンピュータでは解読不可能な原理的に新しい暗号化・復号化方式が必要とされている。さらに爆発的な情報量の増大に伴い、重要な情報をどのように安全に管理・保持するかということは極めて重要な問題である。

そこで本研究では、非線形ダイナミカルシステムにおける普遍現象であるコンシステンシー(consistency)を用いて、新たな情報セキュリティ技術の可能性を示すことを目標とする。特にハードウェアダイナミクス依存型の暗号方式および情報変換技術の応用可能性を示すことを目標とし、超高速不規則振動するカオス的レーザデバイスを用いて実証実験を行った。その結果、半導体レーザを用いたコンシステンシーの実験的観測を達成し、さらにコンシステンシーを利用したメッセージの符号化・復号化の実験的実証に成功した。本成果は、既存分野の枠組みを超えたダイナミカル光情報処理技術という新たな研究分野を切り拓くものであり、将来的に推進すべき研究シーズであると言える。

４．研究シーズ探索のねらい

本研究では、非線形ダイナミカルシステムにおける普遍現象であるコンシステンシー(consistency)を用いて、新たな情報セキュリティ技術の可能性を示すことを目標とする。特にハードウェアダイナミクス依存型の暗号方式および情報変換技術の応用可能性を示すことを目標とし、超高速不規則振動するカオス的レーザデバイスを用いて実証実験を行う。ここでコンシステンシーとは、初期状態の異なる非線形システムが、ある信号により駆動される場合に得られる非線形システムの出力の再現性のことである。本研究課題は、これまで学術的興味に留まっていたコンシステンシーという概念を情報セキュリティ分野へ応用するという、新規性溢れる研究シーズ探索である。

５．研究シーズ探索の方法と成果

５．１ 方法

本研究ではハードウェアおよびダイナミクス依存の情報暗号化および情報変換技術の実現可能性を示すために、コンシステンシーと呼ばれる不規則振動の再現性を利用し、レーザデバイスを用いて実験的実証を行う。以下に具体的な研究項目を示す。

① 半導体レーザにおけるコンシステンシーの実験的観測

カオス的レーザに対して外部から不規則振動で駆動することにより、出力の再現性を実験的に観測する。本現象の実験的実現が情報のスクランブル化の第一段階となる。

② レーザにおけるコンシステンシー状態の安定性と複雑性の調査

入力信号を複雑化するために複数のレーザを一方向に結合した場合のコンシステンシーの観測および複雑性の評価を行う。入力信号の情報変換の再現性を保てるかどうかが重要な点となる。さらにコンシステンシー状態におけるシステムの複雑性を定量化する。

③ 外部入力信号を用いたダイナミカル情報変換技術の実証

コンシステンシーを用いたダイナミカルな情報変換技術の実験的実証を行う。コンシステンシー状態のレーザ出力波形にメッセージ信号を加えて符号化を行う。またコンシステンシーを得るために入力信号とレーザシステムを用いることで、メッセージ信号の復号化を達成する。

5．2 成果

① 半導体レーザにおけるコンシステンシーの実験的観測

半導体レーザを用いたコンシステンシーの実験的観測を行った。実験装置図を図 1 に示す。3つの分布帰還型(DFB)半導体レーザ（それぞれ Drive、Response1、Response2 と呼ぶ)を用いた。まず、駆動用レーザ(Drive)に光ファイバ反射鏡を設置し、戻り光を付加した。反射鏡からの戻り光量を調整することによりカオス的レーザ出力振動を発生させた。また Drive レーザにファイバカプラーを接続し、光を 2 つに分割した。2つのレーザ光はアイソレータを通して、同期用レーザ(Response1 および 2)へ光注入された。Response 側では Response1 および 2 に光ファイバカプラーを接続し、レーザ光を 2 つに分割した。一方のファイバに位相変調器を接続し、さらにファイバ反射鏡を接続して反射鏡の反射率を調節することにより Response1 および 2 に戻り光を付加し、カオスを発生させた。3つのレーザ出力振動はフォトディテクタ, 電気信号増幅器を通してオシロスコープにて検出された。

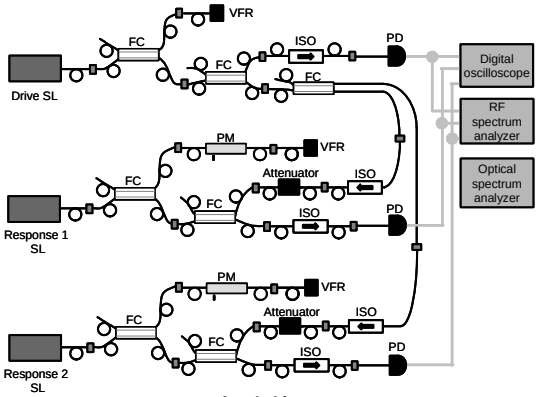

図 1 実験装置図

はじめに、Response1 および 2 に戻り光を付加せずにコンシステンシーを観測した。ここで Drive と Response は異なるパラメータ値に設定し、一方 Response 1 と Response 2 は同一のパラメータ値に設定した。Drive のカオス的レーザ出力光を 2 つの Response に注入し、各々インジェクションロッキングを達成させた。このとき同一パラメータ値を有する Response 1-2 間が同一の振る舞いを示せばコンシステンシーがあると言える。Drive、Response1、Response2 の時間波形と、Response1-2 間の相関図を測定した。その結果を図 2 に示す。図 2(a)より、Drive と Response の時間波形は異なっているものの、Response1-2 間の時間波形は良く一致していることが分かる。また Response1-2 間の相関図を見ると(図 2(b))、斜め 45° の直線付近に分布していることが分かる。相互相関関数を評価したところ 0.955 であり、ほぼ同一の時間波形であると言える。以上より、半導体レーザを用いたコンシステンシーの実験的観測に成功した。

次に、Response の反射鏡からの戻り光量を調節することにより Response に戻り光を付加し、光フィードバックを有するカオス状態にてコンシステンシーを達成させた。Response の位相変調器に電圧を加えて戻り光の位相を変化させ、Response1-2 間の相関の観測を行うことで、位相変

化に対するコンシステンシーの実現の有無を定量的に調査した。Response1-2 間の相対位相差が 0 の場合には高い相関が得られたが、位相差が大きくなるにつれてコンシステンシーが低減した。位相差がπの場合には相関はほぼ 0 になり、コンシステンシーが達成されなかった。このようにコンシステンシーは Response1-2 間の戻り光の位相差に対して非常に敏感であることが分かった。つまりコンシステンシーの実現には戻り光の位相を一定に保つことが重要であることが初めて実験的に明らかとなった。本実験では空気揺らぎおよびレーザ温度の精密な制御により光位相を一定に保つことが可能であり、コンシステンシー状態の安定化に成功している。

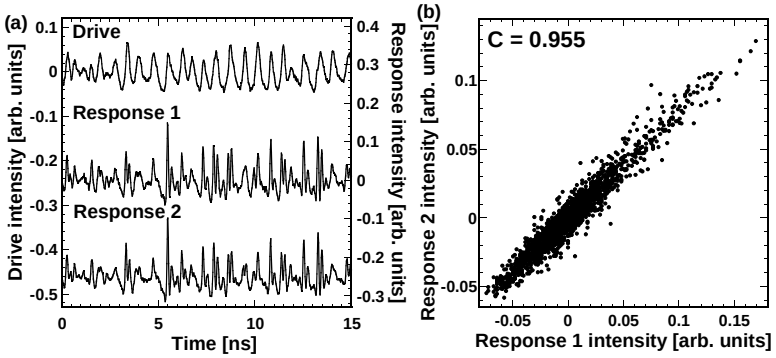

図 2 (a)時間波形と (b)相関図(実験結果)

② レーザにおけるコンシステンシー状態の安定性と複雑性の調査

前述のようにレーザにおけるコンシステンシーの実験的観測に成功しているが、これを物理的一方向性関数へ適用する際の評価指標の一つとして、コンシステンシー状態でのシステム全体の複雑性が挙げられる。しかしながら一方向に光結合されたレーザにおいて、結合状態におけるレーザシステム全体の複雑性に関してはこれまでに調査されていない。そこで本課題では、時間遅延を有する光結合された半導体レーザにおいてコンシステンシーを観測し、リアプノフ指数から Kolmogorov-Sinai(KS)エントロピーや Kaplan-Yorke(KY)次元を算出することでその複雑性を定量的に評価した。

実験と同様に、3つの半導体レーザモデルを考える(Drive, Response 1 および Response 2 と呼ぶ)。同一なパラメータ値であるが異なる初期値を持つ Response 1 および Response 2 に Drive で発生させたカオス信号を入力する。この時2つの Response の時間波形が一致した場合、コンシステンシーがあると言える。また、モデルを線形化して求めたリアプノフ指数から、KS エントロピーと KY 次元を計算することができる。KS エントロピーは情報の損失率を測定する指標で予測不可能性を示しており、一方で KY 次元はシステムを記述するために必要な変数の数に対応している。

図 3 は Drive から 2 つの Response への結合強度を変化させた時の、Response 1-2 間の相関値とシステム全体の KS エントロピーおよび KY 次元を表している。図 3(a)から、結合が無い時の相関値はほぼ 0 でありコンシステンシー状態ではないことが分かる。一方で結合強度を増加させて結合強度が 0.24 以上になると、Response 1-2 間の相互相関値がほぼ 1 となりコンシステンシー状態であることを確認できる。また図 3(b)から、結合強度を増加させるとシステム全体の KS エントロピーと KY 次元は増加することが分かる。しかしながらさらに結合強度を増加させコンシステンシー状態になると、KS エントロピーと KY 次元は急激に減少することが分かった。つまりコンシステンシーの有無がシステム全体の複雑性を大幅に変化させることが明らかとなった。

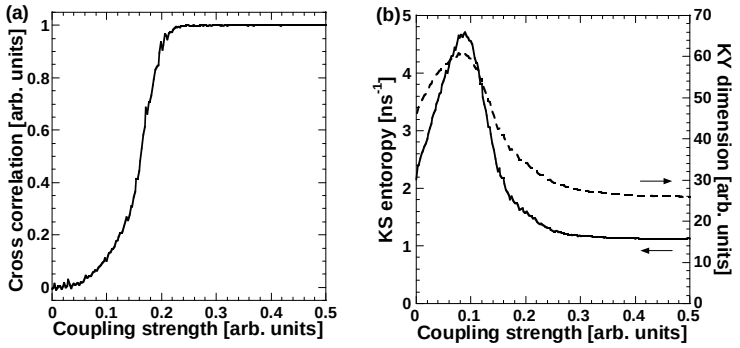

図 3　結合強度変化に対する(a)相互相関関数および(b)KS エントロピーと KY 次元

③ コンシステンシーを用いた情報変換技術の実証実験

本課題では半導体レーザのコンシステンシー状態を用いた情報変換技術の実験的実証を行った。

図 4 に実験結果を示す。図 4(a)は駆動用レーザ信号、符号化信号（カオス＋メッセージ）、および復号化用レーザ信号の時間波形を示す。駆動用レーザ信号と符号化信号の相関は低いことが確認できた。また符号化信号にはメッセージ信号が隠されているが、時間波形からメッセージの推定は困難である。一方で図 4(b)は元のメッセージ信号と復号化されたメッセージ信号を示している。メッセージは明確に再生されており、しきい値判定によりデジタルビットへの変換が可能となる。

以上のように、半導体レーザにおけるコンシステンシーを用いたメッセージ信号の符号化・復号化実験に成功した。

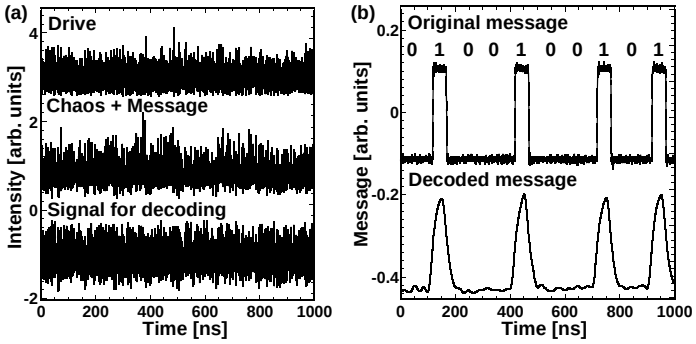

図 4　メッセージの復号化・符号化実験結果。(a)駆動用レーザ信号（上段）、符号化信号（中段）、復号化用レーザ信号の時間波形（下段）。(b)元のメッセージ信号（上段）と復号化後のメッセージ信号（下段）の時間波形

6. 自己評価

本研究課題の基礎技術となるレーザのコンシステンシー現象の実験的観測は当初計画通りに達成され、主な研究成果は得られたと考えている。実験装置の発注および納品までに多くの時間を費やしたため、実際の実験実施期間が予定よりも短縮された点が反省事項ではあるが、最終的に実験主体の研究成果が得られたため安堵している。また安定なコンシステンシー状態を実現するために、光位相の安定化装置を機械工作により自作したことが苦労した点であった。装置が正常に動作するかどうか未知であったが、最終的に安定動作が確認され、位相揺らぎを抑えてコンシステンシー状態を安定に実現できた。さらに情報変換技術においては、様々な符号化・復号化手法の提案およびシミュレーションによる検証を行った。それらの方式の試行錯誤の末、現在の方式に基づいて符号化・復号化の実験的実証に成功した。さらに洗練された情報変換方式の提案・実証が今後の検討課題である。全般的には当初計画通りに進むことができ、さらに多くの新たな研究課題も派生しており、非常に有意義なプロジェクトであったと感じている。レーザにおけるコンシステンシーを用いた非線形ダイナミクスの情報変換技術およびダイナミカル光情報処理分野の発展のため、今後さらなる精力的な研究活動が必要だと実感している。

7. PO の見解

本研究は非線形ダイナミクスの複雑系を情報暗号化に利用しようとするものである。カオスの引き込みにより、同一駆動信号に対する応答出力の再現性が期待でき、このコンシステンシーを利用する。半導体レーザにおけるコンシステンシーを実験的に確認するとともに、非線形ダイナミ

クスを用いた符号化／復号化を行い、情報暗号化への応用可能性を実験的に示した。
アイデアとアプローチは独創的で可能性を感じるが、コンシステンシー状態の直前で複雑性が増加するという点は複雑さと安定性のトレードオフとして根本的問題となる。安定で、かつ複雑な振動系の制御、さらには引き込みまでの時間の短縮化ができれば、情報暗号化での利用が現実的なものになろう。ダイナミカル生体情報メモリへの展開も提示されたが、生体系が同じ応答信号を保証するとは考えにくく、実現困難であろう。また、レーザと通信は通信技術そのものであり、分野融合とは言い難い。

8．研究成果リスト

（1）論文（原著論文）発表

論文投稿中および準備中

（2）特許出願

研究期間累積件数：0 件

（3）口頭発表

①学会
国内 4 件， 海外 0 件

- 菅野 円隆、内田 淳史、”時間遅延を有する光結合された半導体レーザにおけるリアプノフ解析、”2010 年電子情報通信学会ソサイエティ大会、大阪、2010 年 9 月。
- 菅野 円隆、内田 淳史、”半導体レーザー結合系のカオス同期における複雑性の評価、” Optics & Photonics Japan 2010、東京、2010 年 11 月。
- 菅野 円隆、内田 淳史、”半導体レーザーにおけるコンシステンシーと複雑性の評価、”レーザー学会学術講演会第 31 回年次大会、東京、2011 年 1 月。
- 菅野 円隆、内田 淳史、”光結合された半導体レーザにおけるコンシステンシーとリアプノフスペクトラム解析、”電子情報通信学会非線形問題研究会、北海道、2011 年 1 月。

②その他
国内 0 件， 海外 0 件

（4）その他の成果（受賞、著書、招待講演、特記事項等）

光学論文賞 (社)応用物理学会・日本光学会 (2010 年 3 月)