情報理論的セキュリティに基づく暗号鍵生成の超高速レーザカオスによる実装

内田　淳史（理工学研究科 数理電子情報部門・准教授）

１　研究の目的

高度情報化社会の基盤となる全世界規模の光通信ネットワークは既に不可欠なインフラストラクチャとして定着しつつあるが、伝送時における情報セキュリティ問題は最重要課題であるにもかかわらず現在未解決のままである。従来のセキュリティ通信方式はコンピュータのソフトウェアで作成された暗号コードを用い、その秘匿性は計算量複雑性に起因しているが、これは近年提案されている量子コンピュータや次世代の超高速コンピュータにより原理的に解読可能となる。そこで従来の手法とは異なる、原理的に安全な通信手法の開発は緊急課題である。

本研究では情報理論的セキュリティに基づく暗号鍵発生方式を提案し、超高速レーザカオスを用いてこれを工学的に実装することを目的とする。特に情報理論的セキュリティ方式の要素技術として、半導体レーザにおける共通カオス信号入力同期を実験的に達成することを目的とする。また同期用レーザに戻り光を付加し、戻り光の位相を変化させた場合の相関の変化を観測する。

２　研究の方法

共通カオス信号入力同期の実験装置図を図１に示す[1]。本研究では３つの分布帰還型(DFB)半導体レーザ(波長 1547 nm)を使用した。駆動用に使われている１つのレーザを Drive と呼び、他の２つの同期用レーザをそれぞれ Response1、 Response2 と呼ぶことにする。Drive に外部反射鏡(M)を用い、戻り光を付加することでカオスを発生させた。Drive と反射鏡との距離は 0.60m に設定にした。また、戻り光量は可変減光フィルタ (NDF)を用いることで調節した。Drive からの光はビームスプリッタ(BS)によって分割され、一方は Response に伝送される。このとき２つの光アイソレータ(ISO)と２つのλ/2 板を用いることで一方向結合を達成させている。伝送された光はキューブビームスプリッタ(BS(Cube))によって、それぞれ Response1 および２に注入される。ここでレーザの温度を変化させて、インジェクションロッキングにより全てのレーザの波長を一致させる。さらに Response1 および２の光出力は各々の外部反射鏡からの戻り光を有し、自分自身でカオスを発生させる。このときピエゾステージ(PZT)を Response1 の反射鏡の下に取り付けることでナノメートル(nm)オーダでの距離の微小変化を可能にしている。各々のレーザ出力はビームスプリッタとファイバコリメータ(FC)を通して検出を行う。ファイバコリメータに入ったレーザ光はファイバ内を伝搬し光検出器(PD) により電気信号に変換され、電気信号増幅器(Amp)で増幅され

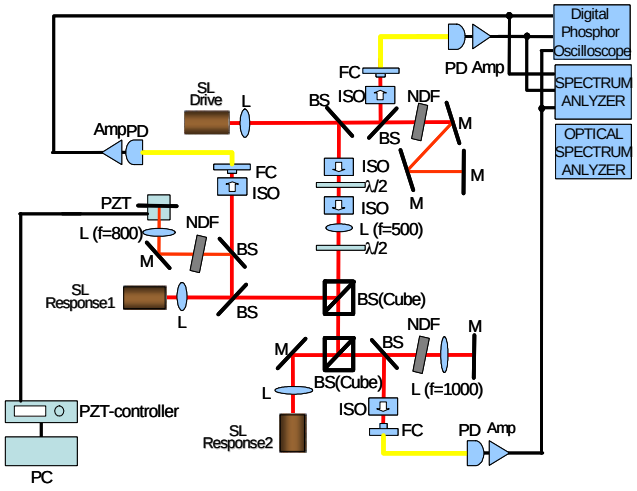

図１　実験装置図

る。さらに高速オシロスコープによりレーザ出力の時間波形が観測される。

３　研究の成果

各々の Response に戻り光を付加した場合における共通カオス信号入力同期を行った。また Response の戻り光の位相を変化させることで相関値の変化を観測した。まず Drive、 Response1、2 の緩和発振周波数を各々2.5 GHz、2.0 GHz、2.0 GHz に設定した。Response1 および 2 に戻り光を付加することでカオスを発生させた。この時 Response1 および 2 の戻り光量は最大に設定している。そして Drive のカオス光を Response 1 および 2 へ注入することでインジェクションロッキングを達成させた。ピエゾステージを微小に変化させることで Response1 の外部鏡の距離を 100 nm ごとに変化させ、Response1-2 間の戻り光の位相が一致した場合と、π（半波長分）ずれた場合の時間波形と相関図をオシロスコープにて観測した。

Response1 と 2 の戻り光の位相が一致した時の時間波形と相関図をそれぞれ図２(a)と(b)に示す。また 2 つの戻り光の位相差が πずれたときの時間波形と相関図をそれぞれ図２(c)と(d)に示す。戻り光の位相が一致したときの時間波形を見ると、非常に良く似たカオス的振動をしていることが分かる。このときの相関値は 0.903 と高い相関を観測した。一方、2 つの戻り光の位相差が πずれたときの時間波形を見ると異なるカオス的振動をしており、相関値も 0.015 と低い相関を観測した。以上より、2 つの Response 間の時間波形の相関値は、戻り光の位相差によって大きく変化することが明らかとなった。以上の結果は、半導体レーザカオスを用いて情報理論的セキュリティ方式を実装する際の要素技術として重要な特性である[2]。

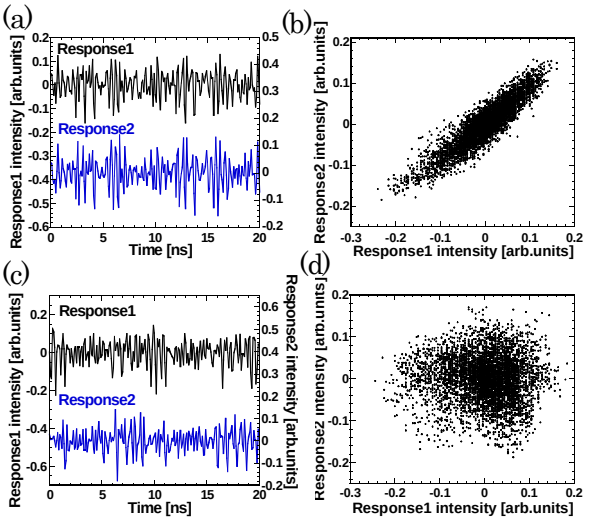

図２　時間波形と相関図

４　まとめ

本研究では半導体レーザにおける共通カオス信号入力同期の実験的観測を行った。Response1 および 2 に外部反射鏡を設置し、戻り光を付加することでカオスを発生させた。またピエゾステージを用いることで 2 つの Response 間の戻り光の位相差を変化させた。Response 1-2 間では戻り光の位相が一致したときに高い相関を示し、戻り光の位相差がπずれたときには低い相関を示した。さらに 2 つの戻り光の位相差を連続的に変化させたところ、Response 1-2 間では相関値の周期的変化が観測された。

以上の結果は、半導体レーザを用いた共通カオス信号入力同期を情報理論的セキュリティ方式へ適用する際に有益な知見となり得るであろう。

５　参考文献

[1] I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A. Uchida, K. Yoshimura, and P. Davis, Optics Express, Vol.17, No.12, pp.10025-10034 (2009).

[2] J. Muramatsu, K. Yoshimura, K. Arai, and P. Davis, IEEE Trans. Information Theory, vol.52, pp.5140-5151 (2006).