

多段化された光集積回路間における共通信号入力同期実験

Experiment on common-signal-induced synchronization in cascaded photonic integrated circuits

埼玉大¹, NTT CS 基礎研², 金沢大³, 鳥取大⁴

○佐々木 卓磨¹, 三井 湧方¹, 内田 淳史¹, 砂田 哲^{2,3}, 吉村 和之^{2,4}, 犬伏 正信²

Saitama Univ.¹, NTT CS Lab.², Kanazawa Univ.³, Tottori Univ.³

○T. Sasaki¹, Y. Mitsui¹, A. Uchida¹, S. Sunada^{2,3}, K. Yoshimura^{2,4}, and M. Inubushi²

E-mails: {s15mm312, auchida}@mail.saitama-u.ac.jp

はじめに: 近年、相関のある乱数列から情報理論的に安全な秘密鍵生成を行う情報理論的セキュリティが研究されている[1]。このような鍵配送の実装として、半導体レーザの共通信号入力同期を用いた方式が提案されている[2]。これは2つの同期用レーザに駆動用レーザ光を注入することで、同期用レーザ間で同一の時間波形が得られる現象を利用している。しかしながら従来の光ファイバ系装置では、外部共振器長が数mmと長く、戻り光の位相が揺らいで同期が不安定化する問題が指摘されている[3]。そこで数mm程度の短い外部共振器長を有する光集積回路を用いることで、同期の安定化が期待できる。

また、正当ユーザが2つのレーザの戻り光の位相をそれぞれ0と π で変調する場合、盗聴者が複数のレーザを用いて全ての位相パターンを再現することで秘密鍵を複製することが可能となる。この攻撃を防ぐために、複数のレーザを多段に結合して変調パラメータの組み合わせ数を指数関数的に増加させる手法が提案されている[2,3]。しかしながら、この手法は通常の半導体レーザと光ファイバを用いてのみ実装されており、同期の安定化が課題となっている。

そこで本研究では、外部共振器長が数mmと短い光集積回路を同期用レーザとして用いて、一方向に結合された多段化された光集積回路における安定な共通信号入力同期を実験的に達成することを目的とする。

実験方法と結果:

本実験で用いる光集積回路は半導体レーザ、光増幅器、位相変調器、導波路、外部鏡から構成される。半導体レーザの出力は外部鏡により反射され戻り光となり、戻り光の強度と位相がそれぞれ光増幅器と位相変調器で調整される。外部共振器長は8.6 mmおよび10.6 mmと短いため、空気や温度の揺らぎに対して堅牢となる。

本研究での実験装置をFig. 1に示す。駆動用レーザ(Drive)の出力は、同期用レーザとの相関値を小さくするために、スーパーluminescentダイオード(SLD)をノイズ源として位相変調される。このランダム位相変調光はファイバカップラ(FC)で分けられ、2つの光集積回路(PIC)に一方方向に注入される。またこれら1段目の光集積回路の出力は2段目の光集積回路に一方方向に注入される。それぞれの光集積回路では戻り光の位相を0または π で独立かつランダムに変調される。各段における戻り光の位相が一致したときのみ、相関の高い時間波形を得ることができる。

1段目(PIC1, PIC2)および2段目(PIC3, PIC4)の光集積回路の時間波形と相関図をFig. 2に示す。1段目の光集積回路において、2つの光集積回路

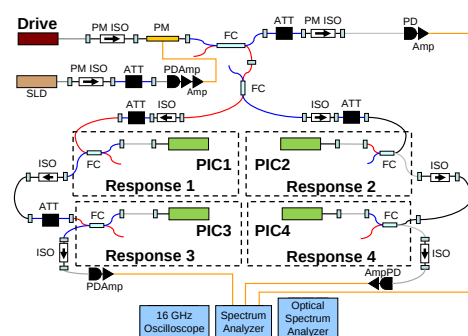


Fig. 1 Experiment setup for common-signal-induced synchronization in cascaded photonic integrated circuits.

の時間波形はほぼ同一の振る舞いを示しており、0.945と高い相関値を得られていることが分かる。また、2段目の光集積回路においても、相関値は0.888と高い値を得ることができた。このように多段化した光集積回路における共通信号入力同期を安定に達成することができた。

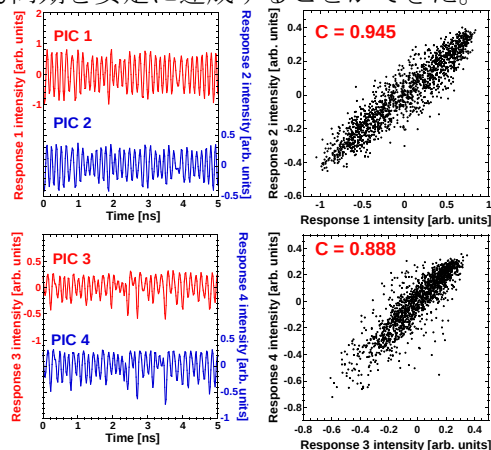


Fig. 2 Temporal waveforms and correlation plots between photonic integrated circuits.

まとめ: 本研究では、多段化された光集積回路間において、共通信号入力同期を実験的に達成した。1段目および2段目の光集積回路間で高い相関値を得ることができた。本現象を用いることで、情報理論的に安全な秘密鍵生成方式のセキュリティの向上が期待される。

参考文献

- [1] J. Muramatsu, et al., Lecture Notes on Computer Science **5973**, 128 (2010).
- [2] K. Yoshimura, et al., Phys. Rev. Lett. **108**, 070602 (2012).
- [3] H. Koizumi, et al., Opt. Express **21**, 17869 (2013).