高速物理乱数生成を可能にする微小レーザカオスデバイスの研究

砂田　哲　　金沢大学　理工研究域　機械工学系　助教

1 □背景と目的

ランダムな信号列を生成する乱数生成器は,通信･情報セキュリティ技術に不可欠のデバイスである［1]. 特に量子暗号[2]等の次世代秘匿通信技術において,予測不可能で偏りのない高品質の乱数を高速に生成する技術が強く望まれている．しかし現在よく利用されている乱数はコンピュータ等を用いて生成される疑似的な乱数である［3]．そのため，シードと呼ばれる初期値やアルゴリズムが判明してしまうと，以後全ての乱数列を知ることができるため，セキュリティ用途には原理的に不向きである．一方，熱雑音や量子現象等の不規則物理現象を用いて予測不能な乱数を生成する物理乱数生成器が現在開発されている．しかし，統計的に偏りのない高品質の乱数を高速度に生成することは困難である．

そのような状況において，2008 年に光の高速不規則現象（レーザカオス現象）を利用した高速物理乱数生成技術が提案され，従来物理乱数生成器と比べて高速に（毎秒１ギガビット以上の速度）で乱数列を生成できることが示された［4-7]．しかし，高速乱数生成に適したレーザカオス現象の発生には，レーザ出力光を再びレーザに戻すための長い外部共振器が必要とされる．先行研究では，光ファイバや外部鏡等の光学コンポーネントを組み合わせることで実験系を構築しているため，レーザカオス発生システムを実用的なサイズに小型化することは困難であった［5]．そこで，レーザカオス発生に必要な要素を全て半導体ウェーハ上に集積化させたデバイスも提案された［8-11]．しかし，これらのデイバスでも，1 cm 程度の 1 次元外部導波路構造を用いていたため，PC や携帯端末，IC カードに搭載可能なほど小型化することは不可能であった．

一方，最近の半導体微細加工技術の進展により，様々な形状の 2 次元微小共振器の作製が可能となっている．2 次元微小共振器は，マイクロサイズの領域に光を高効率に閉じ込める共振器である．これまで，円形，楕円形，スタジアム型などのマイクロサイズの共振器が作製され，その光閉じ込め効率やレーザ発振特性が研究されてきた［12]．2 次元共振器の注目すべき特徴は，その形状により所望の光閉じ込めを制御できることにある．よって,2 次元共振器構造を利用して微小領域内で光の長遅延を与えられる共振器を作製すれば，レーザカオスデバイスの飛躍的な小型化が可能となり，これまでにない超小型乱数生成デバイスが実現できると考えられる．

本研究の目的は，2 次元共振器構造を利用したレーザカオスデバイスを開発し，そのデバイスが物理乱数生成に適したレーザカオス信号生成の可能性を明らかにすることである．本報告書では，はじめに提案デバイスの構造・作製法について述べ，次にカオス信号の生成，そして乱数生成の特性について調べた結果を報告する．

2 レーザカオスデバイスの設計と作製

2-1 デバイス構造

図 1 は，2 次元共振器構造を取り入れたレーザカオス発生デバイスの概略図である．レーザ部と 2 次元共振器から構成される．2 次元共振器はレーザ部の外部共振器となっており，レーザからの出射光は 2 次元共振器内を伝搬し，再びレーザ部へ戻るように設計している．この 2 次元外部共振器部は，幅 W_1 の平端面，曲率半径 R_1 の曲面，共振器長 L_1 の 3 つパラメータにより特徴づけられる形状である．共振器内部の光線軌道解析の結果によれば，$W_1=L_1/10$ かつ $R_1>L_1$ の条件下で，図中の赤線で示す長周期軌道が安定となる．（つまり初期値が僅かにずれても，その周期軌道の近傍を伝搬できる．）

上記の設計に基づき，GaAs/AlGaAs 屈折率分布型分離閉じ込め単一量子井戸構造のウェーハを用いてデバイスを作製した．作製デバイスの一例を図 2 に示す．デバイス作製のプロセスやレイヤー構造については次節で説明する．デバイス全体のサイズはおおよそ 230 μm× 1 mm とした．左側がレーザ部，右側が 2 次元外部共振器部，それらの間隔は 1.5 μm である．レーザ部はコリメート光を出射させるために，疑似スタジアム型共振器となっている［13,14]．この疑似スタジアム型共振器は,半径 R_2=660　μm の曲面ミラーと幅 W_2=50

μm の平端面により構成される．共振器長 L_2 は 300 μm であり，共焦点型条件 L_2/R_2=1/2 を満足する．そのため，共振器の水平軸に沿って伝搬してコリメートビームを出射するモード(軸モード)が存在する．なお，その軸モードのみを選択的に励起するために，共振器には，幅 W_c=2 μm のコンタクトエリアが設けられている．また，この共振器には，幅 200 μm の窓(吸収)領域も設けられており，共振器内を多重反射するような複雑共振器モードの励起を抑制するようにしている．

右側の 2 次元外部共振器部は，図 1 に示す周期軌道が存在するように設計されている．そのため，レーザ部から出射された光はその軌道上を伝搬し再びレーザ部へ戻ることができる．しかし，共振器間のエアギャップ，2 次元外部共振器内部の吸収・散乱，そして端面での透過により，戻り光は減衰してしまう．戻り光の損失を補うため，2 次元共振器へ電流を注入することにより増幅させた．この光増幅により他の余計な共振器モードが発振してしまうことを防ぐため，半径 R_c=6 μm の散乱体と幅 W_{s1}= 60 μm，W_{s2}=240 μm の吸収領域を導入した．2 次元外部共振器の他のパラメータは次のとおりである：L_1=600 μm，R_1=660 μm，W_1=60 μm．

これらの値に対して，帰還光路長は約 3 cm となり，レーザカオス発生に必要な長い光遅延を与えることができる．

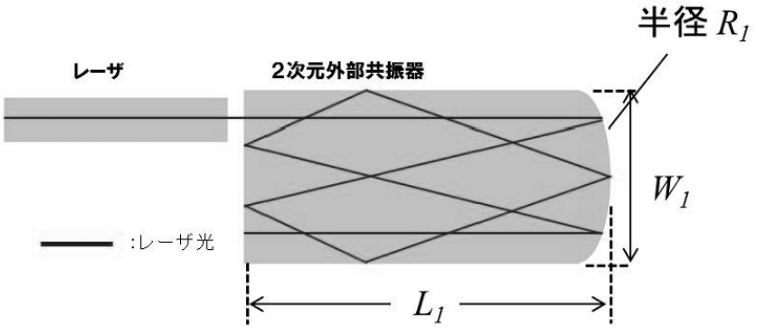


図 1. レーザカオスデバイスの概略図.

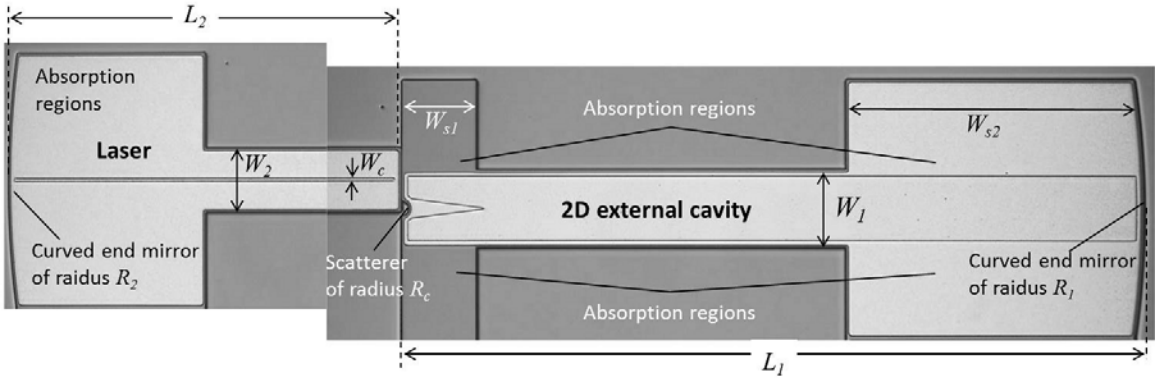


図 2.　作製したレーザカオスデバイスの上面写真.

2-2 作製プロセス

本節では製作プロセスについて述べる．始めに，GaAs/AlGaAs 屈折率分布型分離閉じ込め単一量子井戸構造を有するウェーハ上に厚さ約 600 nm の SiO_2 膜を形成し，レジストを塗布した後，縮小率 5:1 の i 線ステッパーでレーザ部や 2 次元共振器部の形状を正確に転写した．次に，レジストをマスクにして SiO_2 膜のドライエッチングを行い，レジストを剥離した後，SiO_2 膜をマスクにして，半導体のドライエッチングを行った．更に，p 電極のコンタクトに合わせて SiO_2 膜の窓空けを行い，リフトオフプロセスで p 電極を形成した．最後に，GaAs 基板を厚さ 100 μm 程度に研磨して，n 電極を形成した．

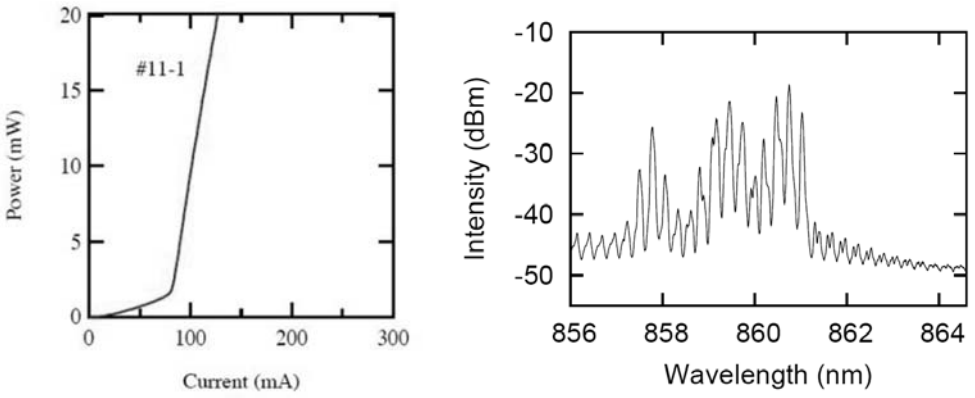
3 静特性に関する評価結果

3-1 レーザ発振特性

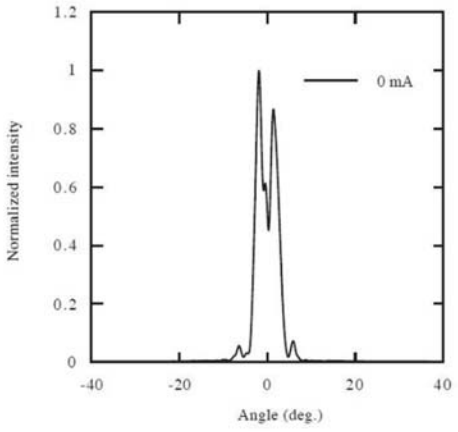
まず，作製したレーザに関して，その基礎特性を評価した．図 3(a)は，レーザ部への注入電流値 J_{LD} の増加に対する光出力パワーの変化を示す．2 次元外部共振器部への電流値は 0 にしているため，そこは吸収領域として働き，戻り光を抑えている．閾値電流値は約 81 mA(=J_{th})であり，ほぼ直線的に光パワーが増加していることがわかる．

図 3(b)は，光スペクトルである．ピークの間隔は約 0.28 nm であり，この値は，共振器長 L_2 により特徴づけられる縦モード間隔の理論値 0.27 nm (=$\lambda^2/(2n_gL_2)$) [15]とほぼ等しい値である．ここで，λは発振波長であり，860 nm とした．実験値と理論値との一致により，軸モードが設計どおり発振できていることがわかった．しかし，光スペクトルには，縦モード間隔によって説明できないピーク(例えば，862 nm 付近に存在する 2 重ピーク)も存在している．これは,軸方向に関する高次横モード（1 次モード）が同時に発振していることを示す結果である．なぜなら，2 重ピークの平均間隔(約 0.09 nm)が，共焦点型レーザにおける最低次軸モードと 1 次モードの間隔の理論値(0.07 nm)に近いからである．なお，理論値の算出にあたり，文献[16]に記載された共焦点型共振器における横モード間隔の理論式を用いた．

図 3(c)にレーザ部から得られた遠視野像を示す．出射光は 0 度付近に局在しているが，2 重のピークとなっていることがわかる．これは最低次モードと 1 次モードが同時発振していることを裏付ける結果である．なお，レーザ部のコンタクトエリア幅は，最低次軸モードのみ発振できるように設計しているが，今回の実験では，1 次モードも発振している．この原因については調査中である．



(a) (b)



(c)

図 3. J_f = 0 mA 時のレーザの発振特性．(a) レーザ出力パワーの電流値依存性．(b) 光スペクトル．(c) レーザ側から測定した遠視野像．

3-2　2 次元共振器中の光伝搬と静特性評価

次に 2 次元共振器部を駆動し，それをレーザの外部共振器として用いて，戻り光の効果に関して調べた結果を述べる．事前の評価では 2 次元共振器は駆動電流値 J_f が 175 mA のとき発振するため，J_f を 165 mA 以下とした．図 4(a)は，J_f を変化させたときに得られたレーザ部からの出力光強度の電流値 J_{LD} 依存性である．J_f を増加させるに従い，閾値が減少すること，および出力光強度が増加していくことがわかる．J_f = 0 mA 時の閾値を J_{th0}，（$J_f \neq 0$）のときの閾値を J_{thf} として，閾値減少率$(J_{th,0}-J_{th,f})/J_{th,0}$を定義すると，$J_f$ = 110 mA 時において約 1 %，J_f =165 mA 時において，約 10 %の閾値減少となることが判明した．

J_f を増加させていくと，光スペクトルでは，発振モードが不規則に変化するモードホッピング現象がみられる．図 4（b）は，J_{LD} =130 mA，J_f = 165 mA 時におけるその時間平均スペクトルである．モードホッピング現象により，図 3（b)と比較して，より多くのモードが励起されている．また，J_f = 0 mA の光スペクトルのように，等間隔でピークが現れないこともわかる．これは，最低次の軸モードだけでなく高次横モード（1 次モード)も同時発振していることを示す結果である．実際，J_f を変化させたときのレーザ部遠視野像を測定してみると，図 4（c）に示すように，0 度付近に二股のピークが得られ，僅かであるが，J_f に伴い放射パターンが変化していくことがわかる．なお，-14 度付近にみられるピークの増大は，2 次元共振器部へ入射後にレーザ部から放射される光によるものである．

2 次元外部共振器によって戻り光が生成できることを示す直接的な結果を得るために，2 次元外部共振器部からの遠視野像も測定した(図 5)．図中の番号は，スネルの法則に基づき計算した光放射角度に対応するものであり，2 次元外部共振器部から放射される順番を表している．このように，光の放射角度は，理論計算結果とよい一致を示すが，必ずしも放射の順番に従い，ピーク値は減少していかない．理論計算結果からのズレの原因はいまだ不明であるが，ほとんど同じ光路を伝搬する発振波長の異なるモード（例えば最低次軸モードと高次軸モード）間の干渉により生じていると考えられる．

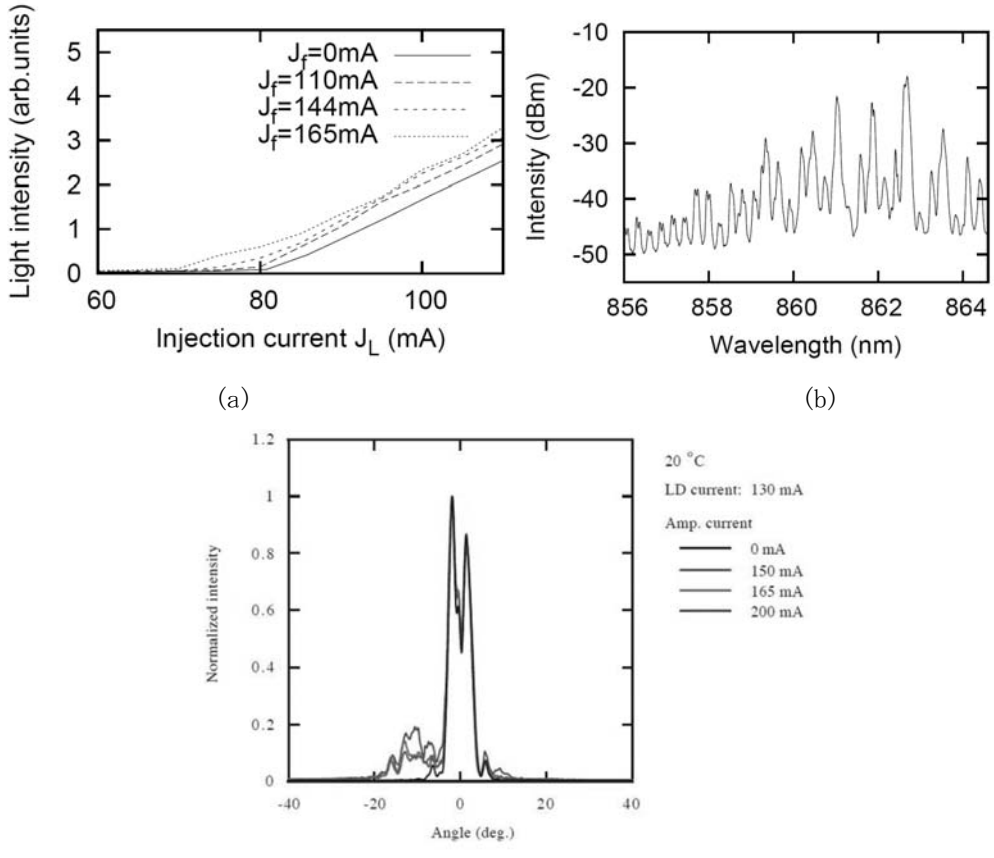


図 4．$J_f \neq$ 0 mA 時のレーザの発振特性．(a) レーザ出力パワーの電流値依存性．(b) 光スペクトル．(c) レーザ側から測定した遠視野像．

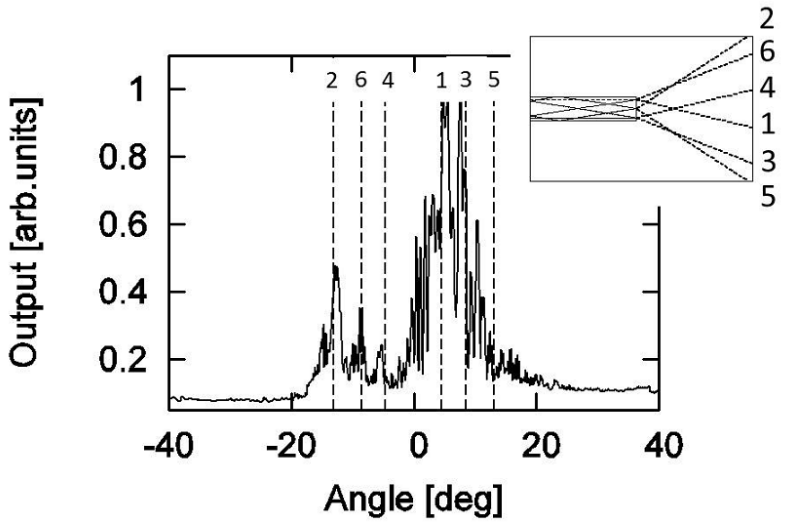


図 5. レーザ光を注入した時の，2 次元共振器側からの放射パターン（遠視野像）．挿入図は，光線軌道計算によって得られた出射パターンを示す.

4 広帯域レーザカオスの発生とその注入電流値依存性の解明

物理乱数を高速に生成するためには，高速な不規則現象を利用しなければならない．本章では，本提案レーザデバイスが,乱数の高速生成に適した高帯域レーザカオスを発生できるかどうか調べた結果を報告する．まず，測定系について説明する．レーザ側から出射された光は，レンズ付き光ファイバでコア径 50 μm の GI ファイバに結合され，光アイソレータを通過して光検出器(PD)へ送った．なお，高速変動を捉えることができるように，周波数帯域 12.5 GHz の高速光検出器を使用した．光アイソレータは，検出器からの戻り光を防ぐために導入した．そのリターンロスは-35 dB である．

図 6 は，本実験系で測定された光強度変動の RF スペクトルである．ここで，レーザ部への電流値を 130 mA に固定し，2 次元共振器部への電流値 J_f を変化している．J_f = 0 mA のとき，出射光強度はほとんど変動しない．図 6 (a)に示される，2 GHz 付近に小さなピークは，レーザ部の緩和振動によるものである．

電流値 J_f を 110 mA 以上に増加させると，約 1.8 GHz 付近のピーク強度が大きくなる［図 6(b)］．さらに電流値を増加させると，ピークはさらに鋭く大きくなりつつ，高周波側へのシフトが観測される．J_f = 113 mA のとき，図 6(c)に示すように，約 2 GHz 間隔で高調波が出現する．このような比較的規則的なスペクトルは，外部共振器長で特徴づけられる周波数(外部共振器周波数)が緩和振動数より大きな場合，つまり，短外部共振器の場合にみられる現象であり，pulse package と呼ばれている．本デバイスにおける外部共振器長は群屈折率 4.16 であるため，外部共振器周波数は約 10 GHz となり，緩和振動数(～2 GHz)より十分高い．また，pulse package では電流値の増加に対して，ピークが高周波側へシフトする現象が観測されている．本実験で観測された規則的なスペクトルは，pulse package 現象[17]と関連していると考えられる．

更に，電流値を増加させると，スペクトル中の各ピークの幅が増大していき，連続的なスペクトルへと変化する［図 6 (d-e)］．最も広帯域なスペクトルは，J_f = 165 mA のときに観測された［図 6 (f)］．スペクトル半値幅は，約 1 GHz であり，ノイズフロアと比較して，約 20 dB も大きな振幅を持つことがわかる．これは，ロバストな乱数生成を行うのに適したカオスであると考えられる．

次に，広帯域スペクトルが得られた J_f = 165 mA 時の波形を図 7 (a)に示す．波形データは，Tektronix 社のオシロスコープ(TDS7104，帯域 1 GHz，10 GS/s)を用いて取得した．オシロスコープの帯域が 1 GHz であるため，図 6 (f)の広帯域スペクトルに対応する波形の正確な測定はできなかったが，カオス的な不規則変動の確認は可能である．また，その不規則波形の自己相関は，図 7 (b) に示すように，数ナノ秒オーダーで急激に 0 になっていくことがわかる．

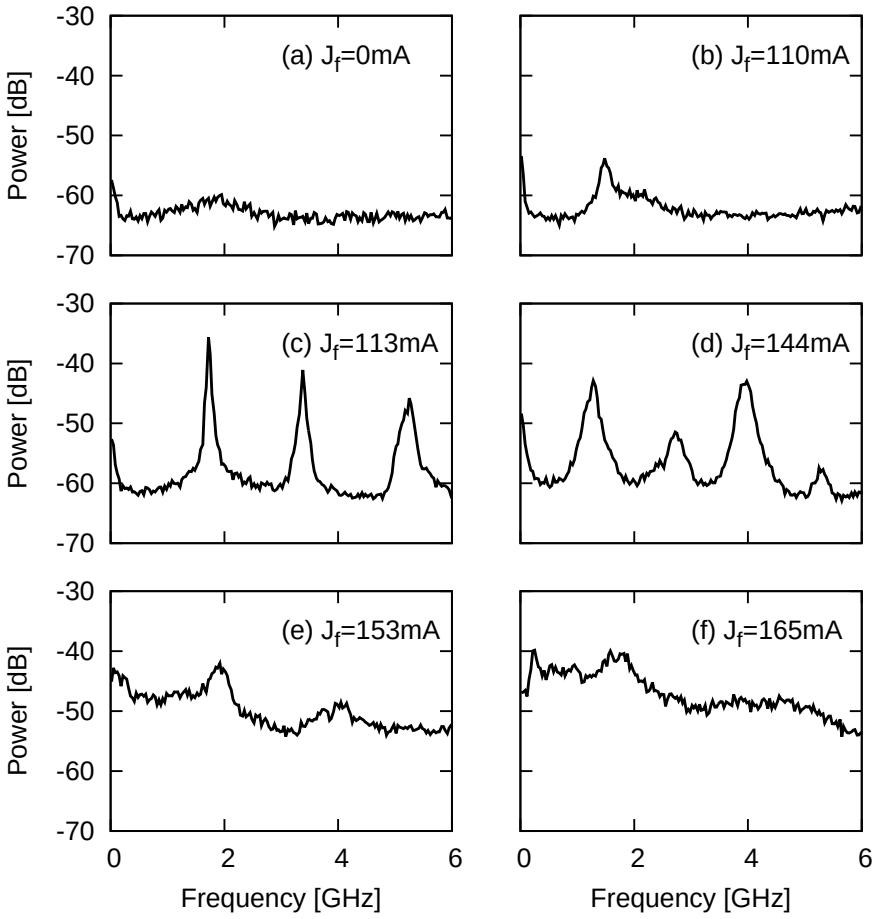


図 6. 光強度変動の RF スペクトル．J_f を増加すると，広帯域スペクトルに変化する．

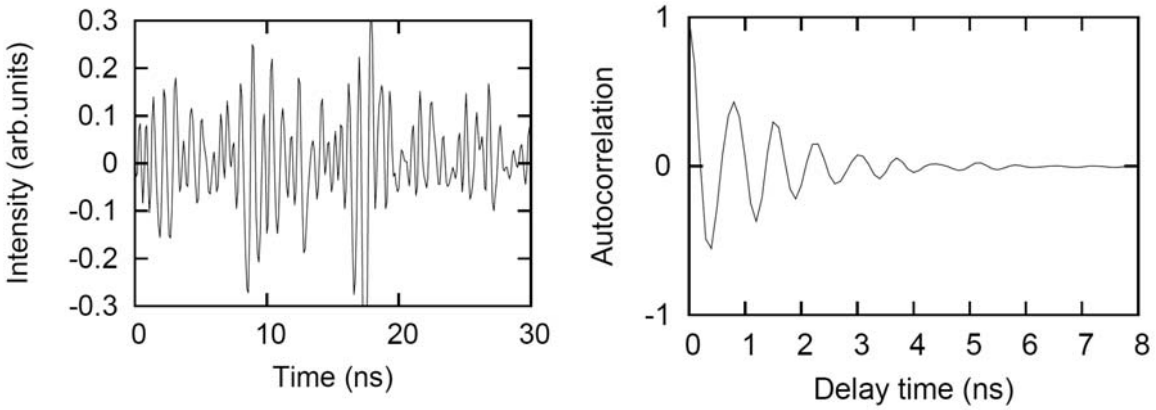


図 7. J_f = 165 mA, J_{LD} = 130 mA 時に測定した (a)光強度の時間変動と (b)その自己相関関数.

5 乱数生成とその統計的性質の解明

本研究では，図 8 に示すスキームにて，乱数生成を行った．まず，出力光強度を 1 GS/s でサンプリングし，ある閾値より光強度値が大きい場合にビット”1”を，小さい場合にビット”0”を与えることにした．本実験では，8 ビットオシロスコープ(TDS7104)を用いたため，0 と 1 のビット生起確率を 1/2 にするように，閾値を調整することは困難である．そこで，同じデバイスから得られる 2 つの光強度波形を，それぞれビットに変換し，XOR 処理をすることで，生起確率を 1/2 に近づけたビット列を得ることにした．これは，文献[8]

で用いた乱数生成スキームと同等のものである．なお，最終的に得られたビット生起確率は，100,000 ビットデータに対して，0.507 となった．

図 9 は，出力ビットデータを８ビットの１０進数に変換し，2 次元平面内にプロットしたものである．このパターンから意味のある構造は見えない．ランダム性を定量的に評価するため，100,000 ビットデータに対して自己相関関数の計算も行った．図 10 (a)に示すように，1 ビットの遅延に対して，十分に相関がなくなっていることがわかる．ここで，出力ビット列のランダム性とビット生成の速度との関係を明らかにするために，自己相関値のばらつきを評価する．図 10 (b)は (a)の拡大図である．点線は，± $3/\sqrt{N} \fallingdotseq 0.0095$(ここで，N はデータ数 100,000)であり，真のランダム列に対する相関値の標準偏差の 3 倍を示す線である．もし実験により得られたビット列がランダムであれば，約 99.7%の確率で点線内に分布するはずである．サンプリングレートが 1 GS/s の結果に対し相関値は 2 つの点線の間に分布しており，真のランダム列の相関値と有意な差を観測できない．なお，サンプリングレートが１ GS/s 以下の場合も同様の結果を得ることができた．よって，最大 1 GS/s でサンプリングすることで，統計的によい品質の乱数列が生成できると判明した．

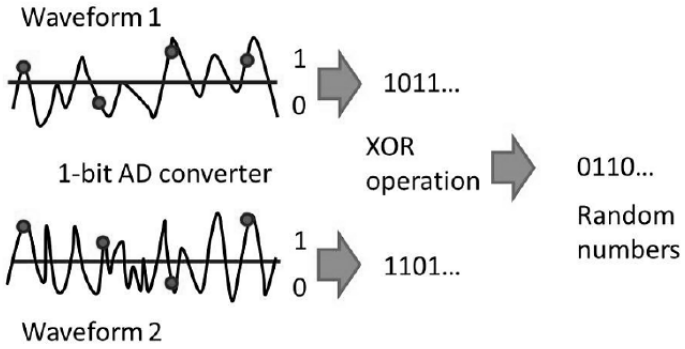


図 8. 乱数生成スキーム．2 つの波形データを 1 ビット AD 変換でビット列に変換し，XOR により最終的にランダムビット列を得る．

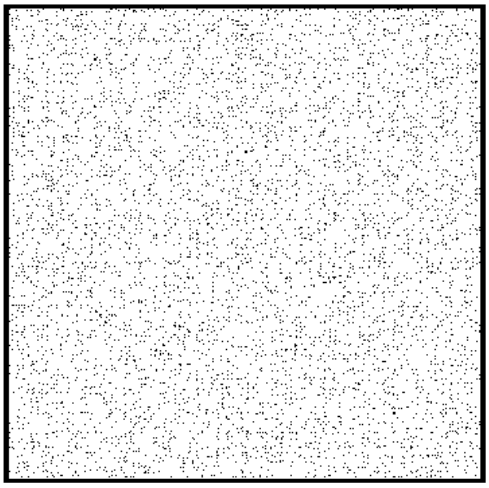
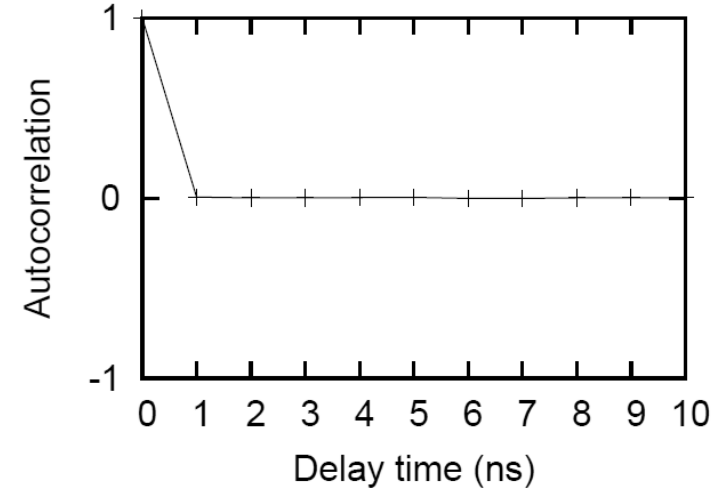
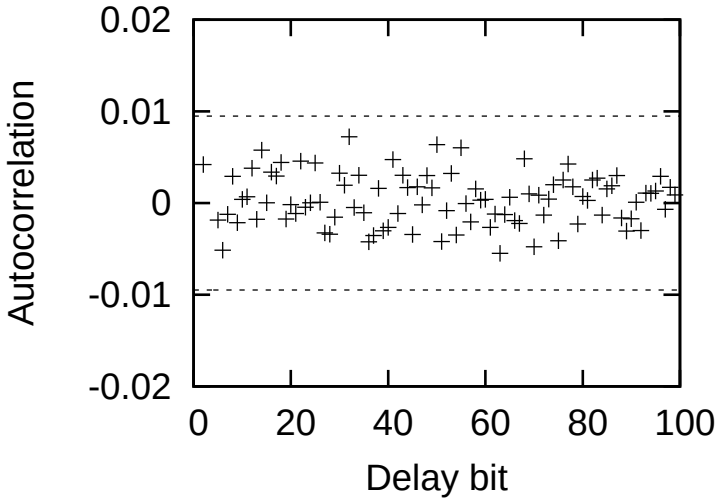


図 9. (a) ランダムパターン． サンプリングレート 1 GS/s で生成したビット列を 8 ビットの 10 進数に変換し，2 次元平面内にプロットした．



(a)



(b)

図 10.　データ数 N= 100 000 のビット列に対して計算した自己相関関数．(a) 1 ビットの遅延で，相関がなくなることを示す．サンプリングレートは 1GS/s．(b) (a)の拡大図．点線は，真のランダム列の自己相関に関する標準偏差の 3 倍を示す．ビット遅延 0 以外の全ての点が点線内に分布する．

6 まとめ

本研究では，2 次元共振器構造を利用して戻り光レーザカオスを発生させ，高速物理乱数生成を可能にするデバイスを提案・評価した．提案内容の詳細や得られた結果は以下のとおりである．

1. 図 2 のような 2 次元共振器構造では,長周期の安定軌道が存在するため,レーザ光を外部から注入すると,その周回軌道に沿って伝搬させ，遅延させてレーザ部へ再び戻すことができる．これにより，戻り光レーザカオスの発生に必要な十分な遅延を生成できる．そのアイデアに基づき，我々は，230 μm ×1 mm の微小領域内におさまるレーザカオスデバイスを GaAs/AlGaAs 単一量子井戸構造のウェハ上に実装した．

2. レーザ部から 2 次元外部共振器部へ光注入させたときの遠視野像も観測し，レーザ光が確かに周回軌道に沿って伝搬することを確認した．これらの結果より，本デバイスは，設計どおりに作製できたと考えられる．

3. レーザ光を 2 次外部共振器部へ注入させ，2 次元外部共振器部への注入電流値を高めていくと，レーザ出力光強度がカオス的に変化していくことを観測した．カオスのスペクトル帯域は約 1 GHz であり，ノイズフロアと比較して約 20 dB の振幅値を持つことが判明した．

4. デバイスから得られたカオス信号を 1 GS/s でサンプリングし，乱数列に変換した．乱数列の自己相関関数に基づく統計的な評価を行い，1 ビットの遅延に対して相関が十分に小さくなることがわかった．統計的に有意な相関値のばらつきからは観測できなかった．

これらの結果より，マイクロンサイズの 2 次元共振器構造を利用してレーザカオスが発生できること，および，1Gbit/s での高速物理乱数生成が可能になると期待できる．よって，2 次元共振器構造を利用することで，物理乱数生成器の小型化が可能になると考えられる．

【参考文献】

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996).
[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, J. Cryptology **5**, 3 (1992).
[3] D. Knuth, *The Art of Computer Programming: Volume 2: Seminumerical Algo-rithms 3rd edn* (Addison-Wesley Professional, 1996).
[4] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Karashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical bit generation with chaotic semiconductor lasers," Nat. Photonics, **2**(12), 728-732 (2008); Thomas E. Murphy and Rajarshi Roy, Nat. Photonics, vol.2, 714 (2008).
[5] A. Uchida, *Optical Communication with Chaotic Lasers,* (Wiley-VCH, 2012).
[6] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics, **4**(1), 58-61, (2010).
[7] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, P. Davis "Physical random number generation with bandwidth enhanced chaotic semiconductor lasers at 8x50 Gb/s, " IEEE Photon. Tech. Lett. **24** pp. 1042-1044 (2012).
[8] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Phys. Rev. A **83**, 031803(R) (2011).
[9] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K. Arai, A. Uchida, and P. Davis, "Theory of fast non-deterministic physical random bit generation with chaos lasers," Phys. Rev. E, **85** 046215 (2012).
[10] S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Opt. Express **19**, 5713-5724 (2011).
[11] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express **18**(18), 18763-18768 (2010).
[12] T. Harayama and S. Shinohara, Laser Photonics Rev. **5**, 247-271 (2011).
[13] T. Fukushima and T. Harayama, IEEE J. Select. Topics Quantum Electron. 10, 1039-1051 (2004).
[14] T. Fukushima, T. Harayama, T. Miyasaka, and P. O. Vaccaro, J. Opt. Soc. Am. B **21**, 935-943 (2004).
[15] n_g is given approximately by n_{eff} [1 − (λ / n_{eff})($d\, n_{eff} / d\lambda$)], where n_{eff} = 3.3 is the effective refractive index of the cavity, $\lambda \approx$ 860 nm is the wavelength of the laser. $d\, n_{eff} / d\lambda$ = 1.0 × 10^4 cm^{-1}. see ref. [H. C. Casey Jr. and M. B. Panish, *Heterostructure Lasers,* (Academic Press, 1978)].
[17] A. E. Siegman, *Lasers,* (University Science Books, Mill Valley, CA, 1986), Chap. 19.
[18] T. Heil, I. Fischer, W. Els ¨asser, and A. Gavrielides, Phys. Rev. Lett. **87**(24), 243901 (2001); T. Heil, I. Fischer, W. Els ¨asser, B. Krauskoph, K. Green, A. Gavrielides, Phys. Rev. E **67**(6), 066214 (2003).

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
A compact chaotic laser device based on a two-dimensional external cavity structure	To be published in Applied Physics Letters	2014 年（掲載予定）
レーザ系における同期現象と時空間ダイナミクス	第 5 回レーザー学会専門委員会	2013 年 5 月
半導体レーザカオスを用いた物理乱数生成における光ノイズの効果	2013 年度応用数理学会研究部会応用カオスセッション	2013 年 9 月
2 次元半導体微小共振器を用いたレーザカオスの生成	2014年第61回応用物理学会春季学術講演会	2014 年 3 月