Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation

Neus Oliver,[1] Miguel C. Soriano,[1] David W. Sukow,[1,2] and Ingo Fischer[1,*]

[1] *Instituto de Física Interdisciplinar y Sistemas Complejos (IFISC), CSIC-UIB, Campus Universitat de les Illes Balears, E-07122 Palma de Mallorca, Spain*

[2] *Department of Physics and Engineering, Washington and Lee University, Lexington, Virginia 24450, USA*

**Corresponding author: ingo@ifisc.uib-csic.es*

Received August 8, 2011; revised October 18, 2011; accepted October 19, 2011;
posted October 20, 2011 (Doc. ID 152422); published November 28, 2011

Chaotic semiconductor lasers have been proven attractive for fast random bit generation. To follow this strategy, simple robust systems and a systematic approach determining the required dynamical properties and most suitable conditions for this application are needed. We show that dynamics of a single mode laser with polarization-rotated feedback are optimal for random bit generation when characterized simultaneously by a broad power spectrum and low autocorrelation. We observe that successful random bit generation also is sensitive to digitization and postprocessing procedures. Applying the identified criteria, we achieve fast random bit generation rates (up to 4 Gbit/s) with minimal postprocessing. © 2011 Optical Society of America

OCIS codes: 190.3100, 140.5960, 140.1540, 060.4785, 140.2020.

Random bit generators (RBGs) are key components of several digital technologies, including encryption and authentication protocols, stochastic modeling, and online gaming and lotteries [1]. Quantum RBGs promise to generate truly random bit sequences [2], but typically produce them too slowly to keep pace with modern data rates. In contrast, pseudo-RBGs based on a random seed and a deterministic algorithm are well known, but are vulnerable if the seed can be guessed. A new approach that has attracted attention is to digitize an analog noise [3] or chaotic signal [4], taking advantage of the inherent noise in combination with chaos-induced decorrelation of the trajectory as the basis for independent bits. Semiconductor lasers are an excellent source for this technique. Their short internal time scales allow for large bandwidth dynamics, and delayed optical feedback can induce strongly diverging chaotic trajectories, thus making rapid bit rates possible [5,6].

Standard test batteries [7] provide statistical evidence of the randomness of a candidate bit stream. However, these tests are computationally intensive and time consuming. Therefore, it is useful to gain fundamental insight into the conditions under which a dynamical system and digitization process are likely to succeed or fail, without having to test all possible conditions in advance. This is the subject of this Letter. We design a chaotic semiconductor laser system, examine its dynamics to determine an optimum regime for producing random bit streams, consider the interplay between the dynamics and the digitization process, and show that competitive bit rates can be achieved with minimum postprocessing using an analog-to-digital converter (ADC) with typical 8 bit resolution.

For wide applicability, we have designed an experimental system that is simple, compact, robust, and made of inexpensive, standard, fiber-based telecommunications components. It is a semiconductor laser with polarization-rotated optical feedback (PROF), a delay-dynamical system known to exhibit complex behavior in previous studies [8]. As illustrated in Fig. 1, a temperature-stabilized discrete mode laser (Eblana Photonics 1550 DM, threshold current $I_{\mathrm{th}} = 12.1\,\mathrm{mA}$) with an APC fiber pigtail connects to a 1×2 90/10 optical coupler (OC) whose principal output passes through a variable optical attenuator used for feedback strength control. A Faraday mirror then rotates the polarization of the incident light by 90° and reflects it, forming an external cavity with a round trip delay time $\tau = 90.9\,\mathrm{ns}$. This configuration compensates for fiber birefringence and can produce strong feedback, which will prove to be an important element in our study.

The light exiting the 10% port of the OC is used for detection. It passes through an inline optical isolator and is detected by a fiber-coupled photodetector. The signal is captured by a digitizing oscilloscope (LeCroy 816Zi, 16 GHz analog bandwidth, 40 GS/s sample rate, 8 bit ADC). This instrument uses standard digital signal processing (DSP) techniques to flatten its frequency response, and the resulting data are enhanced in resolution to 16 bits. However, our goal is to demonstrate the fundamental capability of this system as an RBG based on its dynamics, with minimum postprocessing. Therefore, we retain only 8 bits, equal to the ADC resolution, and discard the rest that arise through DSP, since, in principle, any bit rate could be produced by software interpolation of the raw acquired points.

A broad power spectrum that mimics white noise is considered to be a necessary feature to produce randomness. Figure 2 shows power spectra at different pump currents I and feedback strengths, acquired by replacing

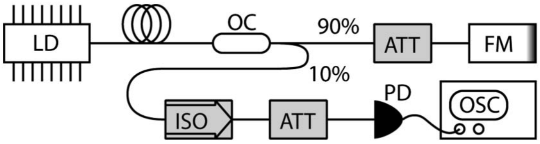

Fig. 1. Experimental schematic diagram. ATT, variable optical attenuator; ISO, inline optical isolator; LD, temperature-stabilized discrete mode laser.

0146-9592/11/234632-03$15.00/0 © 2011 Optical Society of America

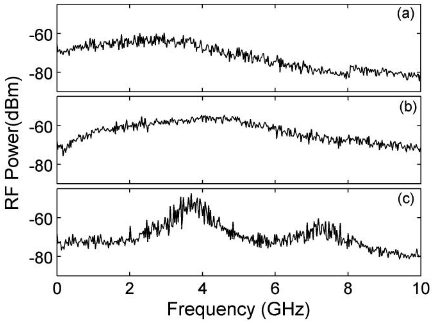

Fig. 2. Power spectra of the laser intensity for (a) $I = 14\,\mathrm{mA}$, $T = 52.2\%$; (b) $I = 19\,\mathrm{mA}$, $T = 52.2\%$; (c) $I = 19\,\mathrm{mA}$, $T = 33.7\%$.

the scope with a radiofrequency (RF) spectrum analyzer (Anritsu MS2667C). Feedback strength is quantified as the fractional power transmission T in the external cavity, i.e., the ratio of power reentering and emerging from the laser pigtail. This is a convenient operational definition, although it does not include laser/fiber coupling efficiency.

Figures 2(a) and 2(b) are for equal, strong feedback but different currents; both display broad spectra with no dominant frequencies evident. If only spectral criteria were considered, either of these would be a candidate for a RBG, and it would not be immediately clear which is best. In contrast, the spectrum of Fig. 2(c) is for the same current as but lower feedback than Fig. 2(b). It displays greater structure, and therefore would be considered unsuitable. Most previous studies on PROF systems have involved low or moderate feedback, where spectral structures are more apparent; the strong-feedback chaotic case has not been studied thoroughly. The ability to access this regime experimentally is critical for our RBG study, and full characterization of these interesting dynamics is a related topic of ongoing research.

External cavity round trip frequencies in integral multiples of 11 MHz are not evident on the scale of Fig. 2. However, the corresponding timescale τ appears in autocorrelation (AC) functions of time traces, as shown in Fig. 3. Figure 3(a) shows the AC up to a time shift of 800 ns. Peaks in the AC function appear at integral multiples of τ, as is typical for delayed feedback systems. Figure 3(b) shows the AC function around zero time shift, which decays rapidly; correlations between points are lost within 1 ns. The data in Fig. 3 correspond to the same operating conditions as Fig. 2(b).

The AC peak heights at multiples of τ and the width of the zeroth peak both provide useful criteria for tailoring the dynamics and digitization conditions for RNG operation. Minimizing the height of a delay time peak selects operating conditions for the laser system at which temporal correlations in the intensity are weakest. In contrast, choosing a random sample interval that is longer than the AC decay time helps assure that successive points will be independent of one another.

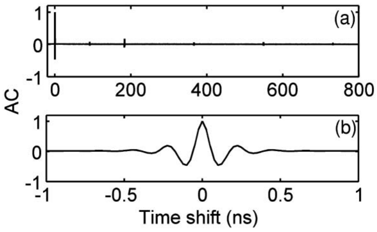

Fig. 3. AC function of the intensity dynamics (a) up to a time shift of 800 ns and (b) resolved zeroth AC peak.

For a systematic study of the AC properties, we examine the height of the AC peak at delay time 2τ as a function of laser pump current and feedback strength. The 2τ peak is chosen because it is the largest, which is typical of PROF systems, but we have verified that the first peak at τ delay shows the same features. The results are shown in Fig. 4. Pump current is on the horizontal axis, feedback strength is along the vertical axis, and the 2τ AC peak height is indicated by the legend on the right.

Keeping in mind that low AC conditions are desired, Fig. 4 shows several features of interest. A region of low AC appears abruptly for low coupling and high current, but this is a region of steady-state operation. The low AC in this case arises from noise, and so is rejected for a dynamics-based RNG. Similarly, a thin ribbon of low AC appears at the lowest currents, but here the laser is below threshold so the conditions are similarly unsuitable. However, a wedge of low AC begins at low current and low coupling, but smoothly grows and expands into a larger region of high feedback strength and moderate currents. This region also displays a broad RF spectrum, and so is identified as the most promising region in which to work. We emphasize that it is not obvious *a priori* that the AC properties would show a local minimum in current. Based on the dynamical guidance provided by the combination of RF spectra and AC characteristics, we select a pump current $I = 19.00\,\mathrm{mA}$ and feedback $T = 52.2\%$ as our operating point for a RBG.

We now consider the digitization procedures and randomness properties of the acquired data. Under the selected conditions, we capture time series at a 40 GS/s sampling rate with the oscilloscope. It saves data initially in 16 bit binary word format, which we truncate to the 8 most significant bits (MSBs) to equal the raw ADC resolution. We then extract points from this set separated by a 1 ns interval, chosen to exceed the decay time of the zeroth AC peak. Finally, the 4 MSBs are discarded from each 8 bit sample, and the 4 least significant bits are retained. The bits obtained in this manner form the

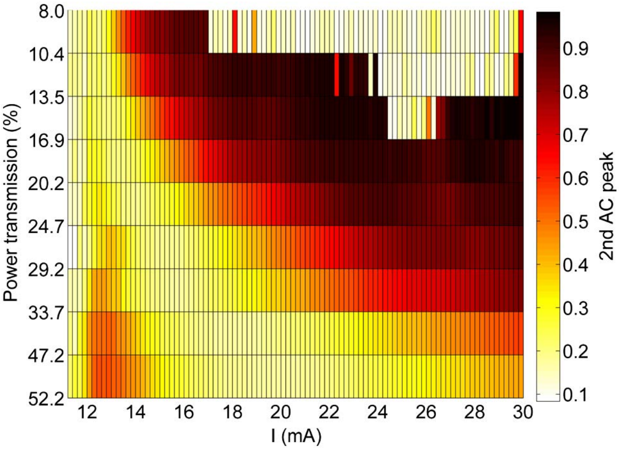

Fig. 4. (Color online) Map of AC peak height for varying feedback and current conditions.

Table 1. Results of Statistical Test Suite NIST SP800-22 for a Set of 1000 Sequences of 1 Mbit Each

Statistical Test	*P*-Value (Min)	Result
Frequency	0.033584	Success
Block frequency	0.851383	Success
Runs	0.090388	Success
Longest run	0.227180	Success
Rank	0.371941	Success
Fast Fourier transform	0.699313	Success
Nonoverlapping template	0.013102	Success
Overlapping template	0.044797	Success
Universal	0.419021	Success
Linear complexity	0.701366	Success
Serial	0.180568	Success
Approximate entropy	0.394195	Success
Cumulative sums	0.179584	Success
Random excursions	0.126609	Success
Random excursions variant	0.066528	Success

bitstream that we evaluate for randomness using the National Institute of Standards and Technology (NIST) battery of statistical tests.

The results of the NIST battery are shown in Table 1, for 1000 samples of 1 million points each. All tests pass, verifying that, under these conditions, our system and procedure produce a statistically random bitstream. The bit rate is 4 Gbit/s, based on 4 bits per data point and a 1 ns interval between points. This speed is competitive with recent work in other systems. It is not a full real-time implementation, but a demonstration of this system's capability.

We performed the same procedure for operating conditions other than the optimal case in the wedge of low AC region (marked in light yellow). For 1 Gbits, we find that some conditions in this wedge other than the optimal case (such as $I = 17\,\mathrm{mA}$, $T = 52.2\%$ and $I = 16\,\mathrm{mA}$, $T = 33.7\%$) fail a few NIST tests. These failures might be avoided by choosing proper acquisition conditions, which are also critical to succeed. Specifically, it is necessary to use the full 8 bit range as much as possible, while avoiding conditions where the acquired signal exceeds the specified vertical scale. If there are too many points that go off scale, the oscilloscope simply records them as the extrema values, thus producing certain strings of consecutive ones or zeros too frequently; these flawed bitstrings typically fail the frequency or runs tests. A signal too small will only span a small subset of the possible 8 bit range and become more likely to fail as well. These competing demands must be balanced as much as possible. This can be done by scaling the input analog amplitude to match the vertical range, and compensating for vertical asymmetry. We avoided the variable gain feature of the scope, which can lead to a skewed distribution of values due to the software processing.

We also analyzed conditions outside the main region of low AC ($I = 22\,\mathrm{mA}$, $T = 20.2\%$ and $I = 19\,\mathrm{mA}$, $T = 16.9\%$). Surprisingly, for the latter case, we passed all randomness tests despite the clearly existing long-range correlations. This example indicates that the omission of the 4 MSBs represents a postprocessing procedure that can compensate for some residual correlations. Therefore, we conclude that, to generate random bits, dynamical properties, acquisition conditions, and postprocessing all play important roles and a delicate balance between them is crucial for the success.

A point of emphasis in our study is to minimize postprocessing requirements as much as possible to demonstrate the efficacy of methods using only the dynamics to generate randomness. This is in contrast to protocols that combine a digitized chaotic signal with additional logical or software processing. Still, we find it necessary to omit the first 4 MSBs from each point. This is unavoidable because the chaotic laser intensity does not cover all values with equal probability. Omission of MSBs compensates for this unequal distribution in the parent distribution of points and, as demonstrated, can remove residual correlations present in the original dynamics. The number of bits necessary to remove can be estimated by plotting histograms of the truncated sample values, and stopping once the histogram is flat within allowed statistical variation.

In summary, we have designed a simple, robust, and versatile semiconductor laser system whose chaotic dynamics can be used for random bit generation. We have shown how to use its dynamics for guidance to identify optimal operating regimes and digitization conditions for random bit generation. Using these methods and minimal postprocessing, we extract a statistically random bitstream at a rate of 4 Gbit/s.

This work was supported by Ministerio de Ciencia e Innovación (Spain), Fondo Europeo de Desarrollo Regional, and the European Commission under projects TEC2009-14101 (DeCoDicA), 0200950I190 (Proyecto Intramurales Especiales), and EC FP7 Project PHOCUS under grant 240763, respectively. D. W. Sukow acknowledges support of this work through the Spanish National Research Council and the Lenfest Endowment.

References

1. N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010).
2. C. Gabriel, C. Wittman, D. Sych, R. Dong, W. Mauerer, U. L. Anderson, C. Marquardt, and G. Leuchs, Nat. Photon. **4**, 711 (2010).
3. X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, Opt. Lett. **36**, 1020 (2011).
4. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nat. Photon. **2**, 728 (2008).
5. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).
6. A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express **18**, 18763 (2010).
7. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, NIST Special Publication 800-22, revision 1a (NIST, 2010).
8. T. Heil, A. Uchida, P. Davis, and T. Aida, Phys. Rev. A **68**, 033811 (2003).