Ultrafast Random Bit Generation Based on the Chaotic Dynamics of a Semiconductor Laser

Nianqiang Li, Byungchil Kim, V. N Chizhevsky, A. Locquet, M. Bloch, D. S Citrin, Wei Pan

Ultrafast Random Bit Generation Based on the Chaotic Dynamics of a Semiconductor Laser

Nianqiang Li,[3,1] Byungchil Kim,[1,4] V. N. Chizhevsky,[2,*] A. Locquet,[4,1] M. Bloch,[1,4] D. S. Citrin,[1,4,§] and Wei Pan[3]

[1]*Georgia Institute of Technology, School of Electrical and Computer Engineering, Atlanta, Georgia 30332-0250 USA*
[2]*B. I. Stepanov Institute of Physics, National Academy of Science of Belarus, 220072 Minsk, Belarus*
[3]*Centers for Information Photonics and Communications, Southwest Jiaotong University, Chengdu, 610031 China*
[4]*UMI 2958 Georgia Tech-CNRS, Georgia Tech Lorraine, 2 Rue Marconi F-57070, Metz, France*
[*]*vnc@dragon.bas-net.by;* [§]*david.citrin@ece.gatech.edu*

Abstract: We achieve physical random bit generation (RBG) that does not exceed the limit set by information theory via extracting 4 bits per sample or keep 55 bits per sample, leading to faster physical-based pseudo RBG.

OCIS codes: (140. 1540) Chaos; (190. 3100) Instabilities and chaos; (140. 5960) Semiconductor lasers

1. Introduction

Random bits can be generated either based on deterministic mathematical algorithms or by extracting randomness from physical phenomena. Recently, Random bit generation (RBG) with chaotic semiconductor lasers has been extensively studied because of its potential applications in secure communications and high-speed numerical simulations [1, 2]. Researchers in this field have mainly focused on the improvement of the generation rate and the compactness of the random bit generators. In the literature experimental investigations have shown that, based on multi-bit extraction schemes, one can extract more than one bit from each sample as long as substantial post-processing is carried out, and even in some cases extract more bits than those are present in the digitized chaotic signal. The number of bits extracted per sample of the chaotic laser intensity has for the most part been chosen heuristically and the randomness of the resulting sequence determined on the basis of standard statistical tests. However, the important question concerning the upper limit in principle based on information theory of the random bit rate that can be extracted from each sample of the chaotic laser intensity remains largely unexplored. In the present work, we try to explore two approaches to fast RBG using a single chaotic laser [3]. In the first approach, the number of retained bits is conservatively selected according to the limits set by information theory. In the second approach, the number of extracted random bits is merely chosen to pass standard randomness tests. Accordingly, we name the first approach physical RBG, and the second physical-based pseudo RBG.

2. Experimental results

The semiconductor laser used in our experiments is an intrinsically single-longitudinal mode DFB laser that operates at $\lambda = 1550$ nm and has a threshold current of $I_{th} = \sim 10$ mA . The laser was pumped well above threshold to ensure operation in the coherence collapse regime: the injection current was set to ~20 mA so that the chaotic fluctuations dominate over the background noise. The external-cavity formed by the abovementioned components results in a large roundtrip delay time of 57.68 ns. The feedback strength, defined as the ratio of the optical feedback power fed back into the laser to the laser power in the absence of feedback was set to ~8%.

The dynamics of the laser intensity were detected by a 10 GHz photodetector (HP 11982A), and then sampled at 40 GS/s and quantized on 8 bits by a real-time oscilloscope (LeCroy WaveMaster 813zi, 13 GHz bandwidth).

In order to achieve efficient generation of random bits, we adopted a recently developed method called high-order finite differences (HFD) which can help us extract random bits from any source of randomness with nonsymmetric distribution [4].

2.1. Physical RBG

In the first approach, we calculated the min-entropy values of 200 sets of 10^7 samples and then made an average over 200 values of min-entropy. For our experimental data, the estimated min-entropy is ~4.4 bits per sample, which indicates that even the best method for extracting randomness cannot lead to more than 4.4 information-theoretically random bits from each raw 8-bit resolution sample. According to the HFD method, all the random integers a_k of 8-bit resolution obtained from our oscilloscope were transformed into 52-bit floating-point numbers. Then we calculated the 50th-order finite differences of a sequence of the floating-point numbers and only extracted 4 least significant bits (LSB) from each sample. As shown in Table 1, the generated bit sequences passed all the tests of the the National Institute of Standards and Technology (NIST) test suite. Therefore, we consider that the use of HFD

combined with a restriction to the number of LSBs corresponding to the min-entropy may have the potential to generate information-theoretic random bits at a rate of 160 Gbit/s (= 4 LSBs × 40 GHz) .

2.2 Physical-based pseudo RBG

Here, in this second approach, we aim to extract as many bits as possible from the chaotic dynamics of a single chaotic laser that pass the three standard tests and satisfy the three standard-deviation criteria. To this end, the calculation of HFD of the initial data was also implemented. In contrast to Ref. [4], where all the random integers a_k were transformed into floating-point numbers of 52-bit resolution, in our implementation here the initial data of 8-bit resolution were transformed into a 64-bit integer data type ("int64"). After the 62th-order finite differences were computed, we found an extraction of 55 LSBs from each sample can pass the NIST test suite. The typical NIST results are also shown in Table 1. The results suggest that the generated bit sequences passed randomness tests, in the sense that the inclusion of 55 consecutive LSBs leads to RBG at a rate of 2.2 Tbit/s (= 55 LSBs × 40 GHz) . However, as it violates the limit set by information theory, we have to consider the corresponding generator as an ultrafast physical-based pseudo random number generator.

Table 1. Results of NIST statistical tests for physical (I) and physical-based pseudo (II) random bits.

Statistical test	**P value**		**Proportion**		**Result**
	I	II	I	II	
Frequency	0.450297	0.651693	0.9890	0.9830	**Success**
Block frequency	0.610070	0.275709	0.9910	0.9900	**Success**
Cumulative sums	0.211144	0.186566	0.9890	0.9830	**Success**
Runs	0.911413	0.079051	0.9830	0.9850	**Success**
Longest runs	0.406499	0.680755	0.9900	0.9880	**Success**
Rank	0.234373	0.587274	0.9910	0.9930	**Success**
FFT	0.701366	0.676615	0.9900	0.9910	**Success**
Nonoverlapping templates	0.302058	0.011709	0.9850	0.9810	**Success**
Overlapping templates	0.090388	0.074330	0.9870	0.9850	**Success**
Universal	0.812905	0.158133	0.9850	0.9850	**Success**
Approximate entropy	0.308561	0.552383	0.9900	0.9870	**Success**
Random excursions	0.137487	0.256333	0.9888	0.9823	**Success**
Random excursions variant	0.164071	0.184128	0.9888	0.9871	**Success**
Serial	0.285427	0.500279	0.9930	0.9900	**Success**
Linear complexity	0.738534	0.662091	0.9850	0.9890	**Success**

3. Summary

We present two approaches for fast RBG based on a semiconductor laser with optical feedback. We can achieve a physical random bit generation rate of 160 Gb/s that does not exceed the limit set by information theory. On the other hand, we can also obtain faster physical-based pseudo RBG at a rate in the order of Tb/s that passes the standard randomness tests though exceeding the limit set by information theory.

4. References

[1] 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, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photon. 2, 728-732 (2008).

[2] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultra high-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. 103, 024102/1-4 (2009).

[3] N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," submitted to Opt. Express, 2013.

[4] V. N. Chizhevsky, "Fast generation of random bits based on polarization noises in a semiconductor vertical-cavity laser," Opt. Spectrosc. 111, 689-694 (2011).