Towards the generation of random bits at terahertz rates based on a chaotic semiconductor laser

Ido Kanter\textsuperscript{1}, Yaara Aviad\textsuperscript{2}, Igor Reidler\textsuperscript{2}, Elad Cohen\textsuperscript{2} and Michael Rosenbluh\textsuperscript{2}

\textsuperscript{1} Minerva Center and Department of Physics, Bar-Ilan University, Ramat-Gan 52900, Israel
\textsuperscript{2} Department of Physics, The Jack and Pearl Resnick Institute for Advanced Technology, Bar-Ilan University, Ramat-Gan, 52900 Israel

Abstract. Random bit generators (RBGs) are important in many aspects of statistical physics and crucial in Monte-Carlo simulations, stochastic modeling and quantum cryptography. The quality of a RBG is measured by the unpredictability of the bit string it produces and the speed at which the truly random bits can be generated. Deterministic algorithms generate pseudo-random numbers at high data rates as they are only limited by electronic hardware speed, but their unpredictability is limited by the very nature of their deterministic origin. It is widely accepted that the core of any true RBG must be an intrinsically non-deterministic physical process, e.g. measuring thermal noise from a resistor. Owing to low signal levels, such systems are highly susceptible to bias, introduced by amplification, and to small nonrandom external perturbations resulting in a limited generation rate, typically less than 100 Mbit/s. We present a physical random bit generator, based on a chaotic semiconductor laser, having delayed optical feedback, which operates reliably at rates up to 300 Gbit/s. The method uses a high derivative of the digitized chaotic laser intensity and generates the random sequence by retaining a number of the least significant bits of the high derivative value. The method is insensitive to laser operational parameters and eliminates the necessity for all external constraints such as incommensurate sampling rates and laser external cavity round trip time. The randomness of long bit strings is verified by standard statistical tests.

1. Introduction

Random bit generators (RBGs) constitute an important tool in statistical physics and are crucial in Monte-Carlo simulations, stochastic modeling and quantum cryptographic keys [3–5]. The quality of a RBG is measured by the unpredictability of the bit string it produces and the speed at which the truly random bits can be generated. System complexity, cost, reliability and sensitivity to control parameters are also important factors for a successful RBG.

Deterministic algorithms generate pseudo-random numbers at high data rates as they are only limited by electronic hardware speed, but their unpredictability is limited by the very nature of their deterministic origin. When ultimate security is necessary one must turn to the only cipher which is theoretically unbreakable - the one-time pad [4]. It is widely accepted that the core of any true RBG must be an intrinsically non-deterministic physical process, e.g. measuring thermal noise from a resistor. Hence, it is no surprise that proposals for and implementations of RBGs range from measuring thermal noise from a resistor and shot noise from a Zener diode or a vacuum tube [6, 7], measuring radioactive decay from a radioactive source [7, 8], detection...
of a single photon arrival time, direction or polarization [9, 10] and sampling a stable high-frequency oscillator with an unstable low-frequency clock [11, 12]. Owing to low signal levels, such systems require extensive broadband amplification and are thus highly susceptible to bias introduced by the non-ideal amplifiers and small nonrandom external perturbations. Often, in order to obtain statistically passable sequences, post processing of the sequence on a digital computer is performed or a limited amplifier bandwidth is used, resulting in a limited generation rate, typically less than 100 Mbit/s. An intriguing possibility for a physical system for RBG is a semiconductor laser in the presence of external feedback, whose output consists of a large chaotic signal of pulses with a width less than 100 ps [12–14, 17]. The main challenge posed by such a source is that the external cavity which is responsible for the chaotic laser fluctuations has a photon round trip time associated with it, and the chaotic signal sequence is nearly identically repeated at this round trip time [14, 17]. The periodicity cannot be completely eliminated by increasing the length of the cavity to extremely long round trip times or introducing feedback from multiple external cavities with incommensurate feedback times. Though these help to reduce the correlation between the chaotic pulse sequence segments they do not eliminate them completely.

Recently, Uchida et. al. [15, 16] demonstrated a fast, 1.7 Gbits/s RBG based on chaotic lasers where the periodicity in the chaotic signal at the photon round trip frequency is eliminated by sampling the fluctuations of two independent lasers. They use two single mode distributed feedback lasers with external cavities with round trip times $\tau_1$ and $\tau_2$. An external clock with period $\tau_s$, triggers the sampling and the one bit analog-to-digital conversion (ADC) of the two laser outputs. The parameters $\tau_1$, $\tau_2$, and $\tau_s$ are selected such that the ratios between the three possible pairs are incommensurate within the resolution of the experiment. The chaotic signals of each of the lasers are mapped at the clock frequency to a Boolean sequence by comparing with a threshold voltage for each signal, which is carefully tuned to achieve an unbiased sequence (equal overall probability of 0 s and 1 s). Finally an exclusive-OR (XOR) operation on the two Boolean sequences yields the random sequence.

2. The prototypical RBG
We use a single, off the shelf semiconductor laser, with absolutely no special requirements, operating in the coherence collapse regime due to feedback from an external cavity with photon round trip time $\tau$ [19]. Because of feedback the laser is chaotic, with a broadened, multimode lasing frequency spectrum and intensity fluctuating in time [14, 15]. Only one incommensurate ratio between the external cavity, $\tau$, and an external clock rate, $\tau_s$, is required. The detected laser output is sampled by an 8-bit, analog-to-digital converter (ADC) (Tektronix TDS6124C) and is used to generate a Boolean sequence in the following way: the difference between consecutive sampled 8-bit values is obtained and the $m$ least significant bits (LSBs) of the difference value serve as the next $m$ random bits of the sequence (Figure 1(a)). Our method is insensitive to variations of parameters such as the average laser power, and does not require the tuning or determination of a decision threshold value.

Figure 1 shows a schematic diagram of the RBG setup. The diode laser wavelength is near 656 nm and partial feedback is obtained from a reflector placed at a photon round trip time of 12.22 ns. The laser is operated moderately above the threshold current, $p_{\text{th}}/p_{\text{th}} = 1.55$, and the optical feedback strength is a few percent of the output intensity, though these parameters can be varied without affecting the RBG. The detection bandwidth (limited by the bias T) is about 40 GHz, which is sufficient to resolve the temporal dynamics of the laser output. The AC component of the detected signal (bias T 3dB low frequency cutoff=10KHz ) is digitized by an 8-bit ADC triggered by a 2.5 GHz clock. The digital signal is stored and the difference between consecutive digital values is obtained using a software implementation. The $m \leq 8$ LSBs of the difference value are stored as the next $m$ bits in a final RBG string. The rate of random number
Figure 1. (a) A schematic diagram of the RBG. (b) Laser implementation, laser diode (LD), beam splitter (BS), neutral density filter (ND), mirror (M), high speed photo detector (PD).

Figure 2. A 4 ns trace of laser intensity digitized at 40 GHz (blue dots connected by a line to guide the eye), and the sampling points at 2.5 GHz (red circles). At each sampling point, m-LSBs obtained from the difference between the current and the previous sampled point are generated and attached to the random bit stream. The generated bit stream for m=5 is depicted in the strip below the signal trace.

generation is therefore m times the ADC clock rate, and m can be varied up to a maximum value which depends on the resolution of the ADC. Figure 2 shows the AC component of the chaotic signal as recorded at a 40 GHz digitizing rate by the 8-bit ADC. The characteristic fluctuation time of the intensity is clearly shorter than the 2.5 GHz sampling rate used for the RBG, indicated by the red circles in the figure.

To test the randomness of the sequences we generated, standard statistical tests were applied to the sequences. We found that the bit sequences obtained from the differentiated chaotic laser intensity fluctuations using the 5 LSBs passed all of the NIST test [18] (performed for 1000 sequences of 1 Mbit length per sequence), thus allowing us to effectively generate random bits.
Table 1. Results of NIST Special Publication 800-22 statistical tests. For "success" using 1000 samples of 1 Mbit data and significance level=0.01, the P value (uniformity of p values) should be larger than 0.0001 and the proportion should be greater than 0.9805608 [18]. For the tests which produce multiple Pvalues and proportions, the worst case is shown. Test results are shown for the 5-LSBs.

| Statistical test         | P-value  | Proportion | Result |
|--------------------------|----------|------------|--------|
| Frequency                | 0.383827 | 0.9900     | Success |
| Block frequency          | 0.591402 | 0.9890     | Success |
| Cumulative runs          | 0.593478 | 0.9940     | Success |
| Runs                     | 0.869278 | 0.9990     | Success |
| Longest run              | 0.980833 | 0.9890     | Success |
| Rank                     | 0.041709 | 0.9910     | Success |
| Nonperiodic templates    | 0.007694 | 0.9910     | Success |
| Overlapping templates    | 0.163513 | 0.9830     | Success |
| Universal                | 0.670396 | 0.9870     | Success |
| Approximate entropy      | 0.114040 | 0.9830     | Success |
| Random excursions        | 0.133216 | 0.9919     | Success |
| Random excursions variant| 0.032123 | 0.9886     | Success |
| Serial                   | 0.272977 | 0.9870     | Success |
| Linear complexity        | 0.208837 | 0.9850     | Success |

Figure 3. (a) Histogram of the laser intensity, independent of the sampling rate, obtained via an 8-bit ADC. The histogram is non symmetric and the small nonlinearity in the electronic measurement system results in population variance in some of the bins. (b) The first derivative of the time dependent laser intensity sampled at 2.5 GHz in the range [-255,255] (for clarity of the presentation only the occupation in the range [-150,150] is presented).

at a rate of 12.5Gbits/s (5 x 2.5Gbits/s). Typical results of the NIST tests are shown in Table 1 [19,20].

3. First derivative of the chaotic signal and the number of used LSBs
A key element of our RBG method is the use of derivative of the signal rather than the signal itself. The derivative broadens the distribution of values used to generate the random sequence as the negative range of values becomes possible from -255 to 255. Its distribution is highly symmetric with mean value approaching zero (Figure 3(b)) and it enhances smaller changes in the chaotic signal to help eliminate correlations within the generated sequence. It is also responsible for the reduction of the population variance in some of the bins, caused by
Figure 4. Uniformity of $2^m$ values (in integer representation) generated by the RBG algorithm retaining m-LSB data for cases (a) $m=1$; (b) $m=2$; (c) $m=3$; (d) $m=4$; (e) $m=5$; (f) $m=6$; (g) $m=7$.

nonlinearity in the digitizing electronics (Figure 3(a)).

An additional important element of our RBG method is the retention of only some of the
least significant bits (LSBs). Discarding the most significant bits enables to reduce correlations within the digitized sequence and to enhance uniformity of the generated sequence over short time windows. In our method, as opposed to the simple thresholding approach, m-LSBs divides the 256 possible levels for the derivatives calculated from the 8-bit level into groups of $2^m$ where each group comprises of $2^m$ different levels. For example, the first LSB, $m=1$, attributes 1/0 to the $2^7 = 128$ odd/even levels. The case of $m=2$ attributes for each level, $k$, among the 256 levels, a 2-bit number following mod($k,4$) which can take the values 00/01/10/11 and for the general case of m-LSBs for each level $k$ an $m$-bit is a signed following the binary representation of mod($k;2^m$). This procedure of coarsening could affect the uniformity among the $2^m$ levels, as a result of the nonuniform shape and the width of the histogram of the derivative of the digitized waveform, Figure 3(b). It is obvious that a necessary condition for a RBG is that all $2^m$ windows of size $m$ are equiprobable. Figure 4 demonstrates the uniformity of $2^m$ values (in integer representation) generated by the RBG algorithm by retaining $m$-LSB data, where $m = 1, 2, ?, 7$. The distribution of 5 LSBs or lower is uniform, whereas more LSBs show a non-uniform distribution. In this case, probability of some values is higher than others, and the produced sequence will show considerable bias.

4. High derivative of the chaotic signal

The chaotic laser intensity fluctuations in our experiments were digitized at 40 GHz sampling rate with an 8-bit resolution. After taking the derivative of the digitized values, the probability of obtaining a particular value of the derivative can be plotted as a histogram and is shown in Figure 5. The blue line is for the data digitized at 40 GHz rate while the green line is the histogram of values obtained at a digitizing rate of 2.5GHz. At a 40 GHz digitization rate, each intensity spike is sampled at a number of sample points, all lying on the same spike, as shown in Fig. 6. This will clearly lead in the thresholding approach to a correlation of consecutive values in the digitized signal and will disqualify the sequence from being random. Furthermore the approach based on the first derivative also fails, since for such a fast sampling rate (compared to the temporal structure of the signal) the derivative on the upward and downward slopes of the spike are almost constants (see red lines in Figure 6, representing local derivatives along a spike). Hence, successive first derivatives at 40 GHz sampling rate are strongly correlated.

One way to eliminate the correlations discussed above is to reduce the digitization rate of the signal. To estimate the maximal allowed sampling rate we construct the histogram.
of the values of the derivatives by two different procedures and look for their similarity [19, 21]. The first method is to use the original time series of the amplitudes and count the number of occurrences of a given derivative for the entire time sequence. This distribution is plotted for 2.5 GHz sampling rate (green histogram) and 40 GHz sampling rate (blue histogram) in figure 5. The second method to calculate the distribution of derivatives is to use only the distribution of amplitudes (e.g., histogram of figure 3(a)) from which all time dependence has been eliminated. More precisely, the histogram is calculated using the formula $P(n\Delta) = \sum_{k,m} P(A_k)P(A_m)\delta(A_k - A_m - n\Delta)$, where $\Delta$ is the amplitude value of the LSB of the 8-bit ADC and $n$ is an integer ranging from -255 to +255. The resulting distribution of the derivative obtained from the second method is depicted by red curve of figure 5. Only if the assumption of the independence of amplitude on history is correct, will the two histograms be identical. The histograms obtained from data at 2.5 GHz sampling rate are nearly identical, implying that the correlation between two successive sampling data points is negligible, while for 40 GHz sampling rate remarkable temporal correlations are visible.

Another way to eliminate the correlations between closely lying values on a given intensity spike is to use higher derivatives of the digitized signal, $A(t)$. For instance, the first, second and third derivatives are given by $A(t) - A(t-1)$, $A(t) - 2A(t-1) + A(t-2)$, $A(t) - 3A(t-1) + 3A(t-2) - A(t-3)$, respectively.

The generation of the random bit stream consists of the following two steps [21]. In the first step the $n$th derivative is calculated (this uses $n+1$ successive values of the recorded digitized waveform). In the second step the $m$ least significant bits (LSBs) of the results of the $n$th derivative are appended to the bit sequence. The use of higher derivatives also enables the retention of a increasing number of available bits per sample point. This is because each derivative doubles the number of possible outcomes and, for the $n$th derivative, an original 8-bit value is converted to a number that has to be represented by $8+n$ bits. A schematic of the algorithm for $n=3$ is illustrated in Fig. 7. For the 16th derivative, even at 20GHz sampling rate and 15 LSBs retained, the random bit sequence passes the NIST Special Publication 800-22 statistical test suite using 1,000 sequences of 1 Mbit length [21]. The total speed of such a RBG is 300Gbits/s (15 x 20Gbits/s).

To demonstrate explicitly that the digitization rate (20 GHz) and the photon feedback time do not need to be incommensurate when using the high derivative method, the external cavity round trip time $\tau$ was carefully tuned to be commensurate with the sampling rate (equal to 10

**Figure 6.** A 1 ns trace of laser intensity digitized at 40 GHz. The first derivative obtained from two consecutive sampling data points is demonstrated by the red lines for one spike.
Figure 7. A schematic diagram of the RBG with high derivatives. The first part is the laser implementation, similar to Figure 1, where the external cavity round trip time was selected to be commensurate with the sampling rate, beam splitter (BS), high speed photo detector (PD), mirror (M). A schematic way to calculate the third derivative from a buffer of length four of the digitized waveform is depicted in the diagram.

ns). The feedback round trip time could be accurately adjusted by measuring the revival of the intensity autocorrelation at high integer multiples of $\tau$. Thus, in our measurements, the ratio between the sampling rate and $\tau$ was as close to commensurate as experimentally achievable.

For a digitized waveform with a given temporal structure there are three tunable parameters (sampling rate, number of LSBs, order of the derivative) where the speed of the RBG is fixed by the product of the first two; (sampling rate) x (number of LSBs). We observed that the maximum allowable sampling rate grows quickly, reaching the experimental system’s maximum of 20GHz, at the third and fifth derivative for 5 and 6 LSBs, respectively. Note that the bit string obtained from the first derivative does not pass the statistical tests using 5 or 6 LSBs, even at 0.5GHz for a commensurate round trip time of the external cavity (10ns) with the sampling rate. It is expected that data obtained with a higher sampling rate (e.g. 60 GHz) or with a higher resolution ADC (more than 8-bit ADC) the generation of random bits from a chaotic laser at terahertz rates will be achievable.

The nth derivative is extremely sensitive to small changes in a time window of $n + 1$ sampling data points, so using a sufficiently high derivative and LSB truncation eliminates the quasi periodic structure and short range correlations present in the waveform. Figure 6 demonstrates this by showing that at 40 GHz sampling rate thresholding the waveform results in short range correlations, since in comparison to a random sequence there is a high probability for consecutive ones (zeros). The first derivative helps to suppress correlations, since the derivative can take a wide spectrum of values and especially it is positive/negative in the upward/downward slopes of a spike, independent if points are above/below the threshold. However, in a 40 GHz sampling rate a spike is sampled 6-8 times and the values of many consecutive first derivatives are very similar as depicted in figure 6. In contrast to the methods based on thresholding and first derivative,
the nth derivative is extremely sensitive to small changes accumulated in a time window of n+1 sampling data points. Hence, using a sufficiently high derivative and LSBs truncation eliminate short range correlations by the amplification of small changes in the waveform over a window of n+1 sampling data points and in addition eliminates the quasi periodicity of the waveform.

References

[1] Metropolis N and Ulam S 1949 J. Am. Statist. Assoc. 44 335
[2] Asmussen S and Glynn P W 2007 Stochastic Simulation: Algorithms and Analysis (New York: Springer-Verlag)
[3] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[4] Stinson D R 1995 Cryptography : Theory and Practice (Boca Raton, LA: CRC Press)
[5] Gallager R G 2008 Principles of Digital Communication (Cambridge: Cambridge University Press)
[6] Vincent C H 1971 J. of Phys. E-Sci. Instrum. 4 825
[7] Maddocks R S Vincent C H Walker E W and Matthews S 1972 J. of Phys. E-Sci. Instrum. 5 542
[8] Walker J 1995 HotBits: Genuine random numbers, generated by radioactive decay, http://www.fourmilab.ch/hotbits/
[9] Stefanov A Gisin N Guinnard O Guinnard L and Zbinden H 2000 J. of Modern Optics 47 595
[10] Rand Corporation. 1955 A Million Random Digits With 100,000 Normal Deviates (Glencoe Ill: Free Press)
[11] Fairfield R C Mortenson R L and Coulthart K B 1984 in Advances in Cryptology - Crypto ’84 pp. 203-230
   (New York: Springer-Verlag)
[12] Hales J Zhukov A Roy R and Dykman M I 2000 Phys. Rev. Lett. 85 78
[14] Rosenbluh M et al. 2007 Phys. Rev. E 76 046207
[15] Uchida A et al. 2008 Nature Photonics 2 728
[16] Honjo T. et. al. 2009 Optics Express 17 9053
[17] Murphy T E and Roy R 2008 Nature Photonics 2 714
[18] NIST Statistical Tests Suit http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html
[19] Reider I Aviad Y Rosenbluh M and Kanter I 2009 Phys. Rev. Lett. 103 024102
[20] We have encountered a mistake in the FFT statistical test in [18]. Following our correspondence with NIST, we have been advised to disregard this test [18].
[21] Kanter I, Aviad Y., Reider I., Cohen E. and Rosenbluh M. 2010 Nature Photonics, Published Online: 13 DECEMBER 2009 — DOI: 10.1038/NPHOTON.2009.235