Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser

I. Reidler,[1] Y. Aviad,[1] M. Rosenbluh,[1] and I. Kanter[2]

[1]*Jack and Pearl Resnick Institute for Advanced Science and Technology and Department of Physics, Bar-Ilan University, Ramat-Gan, 52900 Israel*

[2]*Minerva Center and Department of Physics, Bar-Ilan University, Ramat-Gan, 52900 Israel*

(Received 6 March 2009; published 10 July 2009)

The fluctuating intensity of a chaotic semiconductor laser is used for generating random sequences at rates up to 12.5 Gbits/s. The conversion of the fluctuating intensity to a random bit sequence can be implemented in either software or hardware and the overall rate of generation is much faster than any previously reported random number generator based on a physical mechanism. The generator's simplicity, robustness, and insensitivity to control parameters should enable its application to tasks of secure communication and calculation procedures requiring ultrahigh-speed generation of random bit sequences.

DOI: 10.1103/PhysRevLett.103.024102 PACS numbers: 05.45.−a, 05.40.−a, 42.55.Px, 42.65.Sf

Random number generators (RNGs) are commonly used in secure communications [1], Monte Carlo simulations [2], and stochastic modeling [3]. The quality of a RNG is measured by its security against an attacker trying to predict the bit stream by physical or statistical analysis. For many applications the speed at which truly random numbers can be generated is of paramount importance. Other important considerations are system complexity, cost, reliability and sensitivity to control parameters. The methods used for RNG can be divided between deterministic algorithms implemented in hardware and software and nondeterministic and stochastic physical phenomena based approaches [4,5].

A deterministic RNG is an algorithm which produces an unpredictable Boolean sequence in which all subsequences are generated equiprobably, so that knowledge of the current sequence does not reveal any information about the value of the next bit, which has an equal probability to be 0 or 1. Deterministic algorithms can be easily implemented in any computational platform; however, the requirement of complete unpredictability is unrealistic since the sequence can always be determined given the initial conditions of the algorithm. Thus deterministic algorithms generate pseudorandom sequences which meet a number of global statistical measures, as measured, for example, by the standard statistical test suite for RNGs of the National Institute of Standards and Technology (NIST) [6] and the Diehard test suite [7]. The main advantages of deterministic RNGs is that they add no hardware cost and their speed is bound only by the processing hardware. Their main disadvantage is that an attacker can guess or obtain partial knowledge of the initial state of the algorithm and can thus reproduce the random sequence. Algorithms have been developed to prevent guessing of the initial conditions [8], but implementation of such algorithms invariably and significantly slows down the RNG rate.

Nondeterministic RNGs rely on stochastic physical processes, the most appealing examples of which are based on fundamental quantum principles such as uncertainty, where the bit is assigned following the detection of an event such as photon arrival time, direction, or polarization [9–11]. The main disadvantage has been the limited bandwidth which results in limited generation rate, typically near 20 Mbits/s. Other physical processes, thermal fluctuations (noise) in devices such as resistors or diodes, generate bits by clipping an amplified signal by an appropriate decision threshold. In these systems the bandwidth is limited only by the amplifier and the main drawback is the extreme sensitivity to control parameters such as the threshold value and amplifier gain which can result in a bias in the random sequence.

An intriguing possibility for a physical system for RNG is a semiconductor laser in the presence of external feedback, whose output consists of a large chaotic signal, over a very high bandwidth [12–14]. The chaotic signal consists of pulses with a width less than 100 ps with random amplitude and time position [15] thus providing a potential source of random numbers generated at a rate near 10 GHz. 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 [see Fig. S2(a) in [16]]. These periodicities 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.* [4] demonstrated a fast, 1.7 Gbits/s RNG 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 τ_1 and τ_2. An external clock with period τ_s, triggers

the sampling and 1 bit analog-to-digital conversion (ADC) of the two laser outputs. The parameters τ_1, τ_2, and τ_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 is 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.

In this Letter we demonstrate the fastest physical RNG known to us with a speed of 12.5 Gbits/s which passes all standard tests for randomness [6,7]. In addition to the ultrahigh speed, our system stands out in its simplicity and insensitivity to perturbations and control parameters. We use a single, off the shelf, multimode 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 τ. Because of feedback the laser is chaotic, with a broadened lasing frequency spectrum and intensity fluctuating in time [15]. Only one incommensurate ratio between the external cavity, τ, and an external clock rate, τ_s, is required. The detected laser output is sampled by an 8-bit, analog-to-digital converter (ADC) 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. 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 RNG 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 (see Table S5 in [16]). The laser is operated moderately above the threshold current, $p = I_{op}/I_{th} = 1.55$, and the optical feedback strength is a few percent of the output intensity, though these parameters can be varied without affecting the RNG. 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 3 dB low frequency cutoff = 10 kHz) 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 (For possible hardware implementations see S7 in [16].) The $m < 8$ LSBs of the difference value are stored as the next m bits in a final RNG string. The rate of random number 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 RNG, indicated by the red circles in the figure. A histogram of the sampled amplitudes for a 100 μs long data stream is shown in Fig. 3(a). For the specific signal level recorded, the number of occupied bins is 130 from the available 256. The distribution is asymmetric, typical of chaotic systems [17], especially in the event of a chaotic signal consisting of random spikes [15]. For such a distribution one cannot perform a symmetric bimodal division (thresholding) of the bins and in general for any finite resolution digitization, any attempt to divide the bins evenly will always result in some bias. In addition the distribution of amplitudes is also time fluctuating and is expected to achieve a stationary distribution only for extremely long sampling time. Any

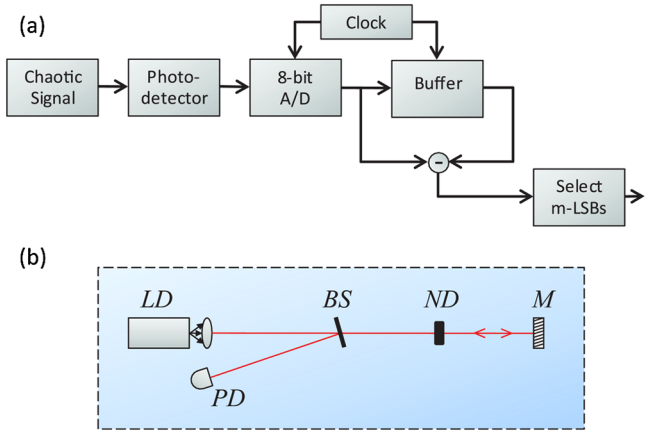

FIG. 1 (color online). (a) A schematic diagram of the RNG. (b) Laser implementation, laser diode (LD), beam splitter (BS), neutral density filter (ND), mirror (M), high speed photo detector (PD).

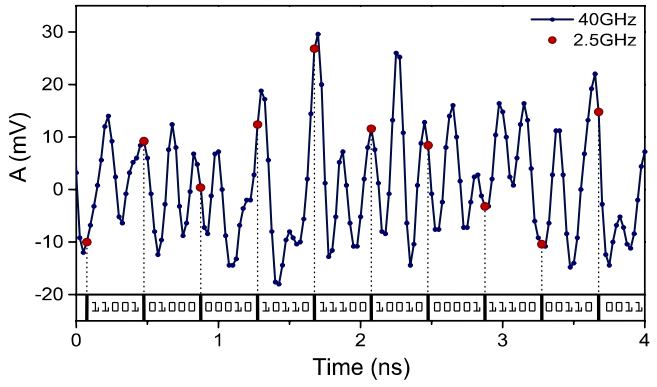

FIG. 2 (color online). A 4 ns trace of laser intensity digitized at 40 GHz (blue dots connected by a line to guide the eye), and the sampling points at 2.5 GHz (red circles). At each sampling point, m-LSBs obtained from the difference between the current and the previous sampled point are generated and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

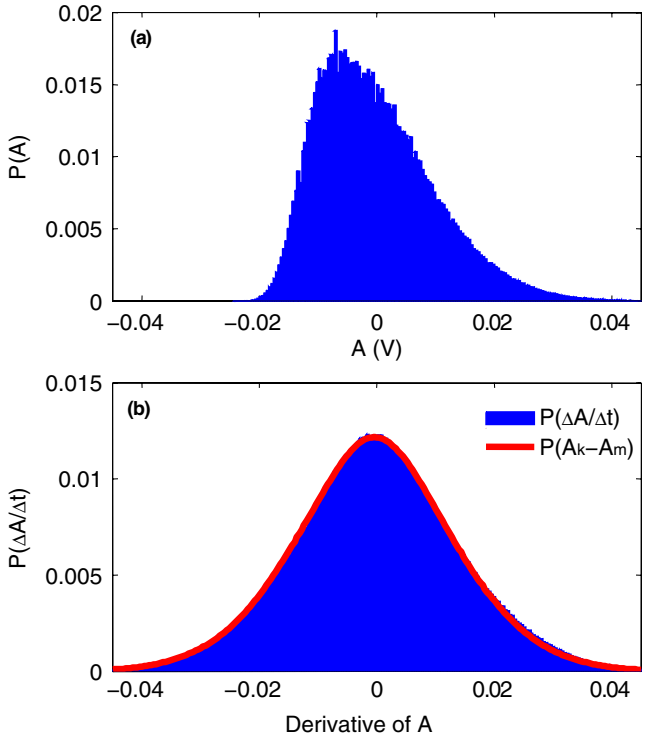

FIG. 3 (color online). (a) Histogram of the laser intensity obtained via an 8-bit ADC. (b) Histogram of the derivative of the laser intensity as obtained from the time series of laser intensities. The red line represents a histogram generated from the histogram shown in Fig. 3(a), whereby the temporal position of the values has been eliminated as explained in the text.

change in laser operating parameters, for example, the average laser power, will have an immediate effect on the distribution. Thus the thresholding value necessary for evenly dividing the distribution is extremely sensitive to small perturbations in the setup and as observed by Uchida *et. al.* [4], has to be constantly tuned to avoid a bias in the division.

In order to overcome these difficulties we convert the raw-data into a time series consisting of the derivative of the ADC signal amplitudes, A_t, $\Delta_t = A_t - A_{t-1}$. The histogram of Δ_t shown in Fig. 3(b), thus has twice as many bins as the original distribution, exhibits a very high degree of symmetry (see S6 in [16]) and is unbiased, since $\sum_{i=1}^{t} \Delta_i = A_t - A_1$, which is of the order of a typical signal amplitude, independent of the length of the sequence. Since adjacent Δ_t values are temporally correlated even if the original amplitudes are random, (for instance, it is very unlikely or impossible to have two successive large positive Δ, since the amplitudes are bounded from above), one might expect that such a series is not a good candidate for a random sequence. This difficulty is solved, however, by taking into account only the m LSBs of each Δ_t and relying on the chaotic nature of the time varying laser intensity (for further discussion on statistical bias, see S3 in [16]).

The values of the discrete derivatives form a highly symmetric histogram (S6 in [16]), centered at zero [Fig. 3(b)], and allows for the unbiased, even division of the bins into even or odd bins based on the LSB of the bin. Having an unbiased distribution is a necessary but insufficient condition for a true RNG. In order to ensure verified randomness, the order in which the bins in the distribution are filled up also has to be random. Thus the probability that a next value in the time series will be assigned to an even or odd bin needs to be independent of the current amplitude belonging to an even or odd bin. This is indeed the property of chaotic trajectories. The distance between two adjacent amplitudes starting from a given bin value diverges; hence, their subsequent probability to end up in an even or odd bin is equiprobable, provided the sampling rate (clock period), is slow enough in comparison to the strength of the chaos, controlled by the spectrum of the Lyapunov exponents [18].

At the 2.5 GHz sampling rate used in our experiments, not only is the probability to be in an even or odd bin independent of recent history, but the probability to be in any bin is independent of the current one. One can show this independence by constructing the histogram of the derivatives by two different procedures and noting their similarity. Only if the assumption of the independence of amplitude on history is correct, will the two histograms be identical. 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 as the blue histogram in Fig. 3(b). The second method to calculate the distribution of derivatives is to use only the distribution of amplitudes,

TABLE I. Results of NIST Special Publication 800-22 statistical tests. For "success" using 1000 samples of 1 Mbit data and significance level $\alpha = 0.01$, the P value (uniformity of p values) should be larger than 0.0001 and the proportion should be greater than 0.9805608 [6]. For the tests which produce multiple P values 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	0.591409	0.9890	success
Cumulative sums	0.593478	0.9940	success
Runs	0.869278	0.9930	success
Longest run	0.980883	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	0.031213	0.9886	success
Serial	0.272977	0.9870	success
Linear complexity	0.208837	0.9850	success

plotted in Fig. 3(a), from which all time dependence has been eliminated. More precisely, the histogram is calculated using the formula $P(n\bar{\Delta}) = \sum_{k,m} P(A_k)P(A_m)\delta(A_k - A_m - n\bar{\Delta})$, where $\bar{\Delta}$ is the amplitude value of the LSB of the 8-bit ADC and n is an integer ranging from -255 to $+255$. The histogram calculated in this manner is shown as the red line in Fig. 3(b). The histograms are nearly identical (see S6 in [16]), thus implying that the joint probability distribution of two successive amplitudes, $\langle P(A_t = A_k; A_{t+1} = A_m)\rangle_t = P(A_k)P(A_m) \forall k$ and m, where $\langle \ldots \rangle$ stands for a time average, and that correlations between two successive bins is negligible.

The bit sequences obtained from the differentiated chaotic laser intensity fluctuations using the 5 LSBs passed all of the NIST [6,19] (performed for 1000 sequences of 1 Mbit length per sequence) and Diehard tests (performed for a 74 Mbit long sequence), thus allowing us to effectively generate random bits at a rate of 12.5 Gbits/s. Typical results of the NIST tests are shown in Table I, while Diehard results are shown in Table S1 in [16].

As expected, random sequences with verified randomness can be generated also with a lower m as was verified, for instance, in our tests for $m = 4$, but not for $m \geq 6$ for our 8-bit ADC. The value of $m_{\max}$ depends on the shape of the distribution of intensity derivatives, Fig. 3(b). When this distribution becomes narrow $m_{\max}$ decreases since the distribution of all $m_{\max}$-bits tuples becomes biased.

The ultimate speed of the RNG we demonstrate is of course limited. The first limitation is the local structure of the chaotic signal, which consists of spikes and thus the derivative of the signal over a time comparable to the spike width will have regular and well defined behavior. Furthermore the derivative between spikes will consistently give a low value near 0 [15]. The sampling rate, therefore, has to be slower than the spike width or the time between spikes, whichever is longer, thus ensuring that two successive recorded amplitudes are uncorrelated. A second limitation is the strength of the chaos controlled by the largest Lyapunov exponent [20], and as it increases a faster sampling rate might be possible. However, the Lyapunv exponent measures only a global (average) property and in many chaotic systems it fluctuates between positive and negative values along the chaotic trajectory and only its average value is positive. Hence, the sampling rate has to be slower than the typical time periods where the system is nonchaotic.

The RNG rate reported by us can also be attained using a slower ADC with higher resolution. We checked that the distribution of the derivatives of the signal amplitude, Fig. 3(b), is almost unchanged for sampling rates slower than 2.5 GHz but is modified for higher rates (see Fig. S4 in [16] for 100 MHz and 40 GHz). Since the symmetric histogram shape does not change at slow sampling rates, sampling at a slower rate but with a higher resolution would therefore allow $m > 5$ bits to be taken from each sample. The loss in ADC conversion rate could thus be made up by retaining more bits from each sample.

We acknowledge support of MOD Government of Israel and Israel Science Foundation, the assistance of Eitan Hammami, Elad Cohen, and Zav Shotan.

[1] D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, Boca Raton, FL, 1995).
[2] N. Metropolis and S. Ulam, J. Am. Stat. Assoc. **44**, 335 (1949).
[3] S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis* (Springer-Verlag, New York, 2007).
[4] Atsushi Uchida *et al.*, Nat. Photon. **2**, 728 (2008).
[5] Thomas E. Murphy and Rajarshi Roy, Nat. Photon. **2**, 714 (2008).
[6] NIST Statistical Tests Suite http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html.
[7] G. Marsaglia, Diehard: A Battery of Tests of Randomness, http://www.stat.fsu.edu/pub/diehard/, 1995.
[8] L. Blum, M. Blum, and M. Shub, SIAM J. Comput. **15**, 364 (1986).
[9] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. J. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[10] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[11] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
[12] R. O. Miles, A. Dandridge, A. B. Tveten, H. F. Taylor, and T. G. Giallorenzi, Appl. Phys. Lett. **37**, 990 (1980).
[13] T. Heil, I. Fischer, W. Elsasser, J. Mulet, and C. R. Mirasso, Phys. Rev. Lett. **86**, 795 (2001).
[14] G. H. M. van Tartwijk, A. M. Levine, and D. Lenstra, IEEE J. Sel. Top. Quantum Electron. **1**, 466 (1995).
[15] M. Rosenbluh, Y. Aviad, E. Cohen, L. Khaykovich, W. Kinzel, E. Kopelowitz, P. Yoskovits, and I. Kanter, Phys. Rev. E **76**, 046207 (2007).
[16] See EPAPS Document No. E-PRLTAO-103-057930 for supporting material. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[17] S. Lepri, G. Giacomelli, A. Politi, and F. T. Arecchi, Physica (Amsterdam) **70D**, 235 (1994).
[18] V. Ahlers, U. Parlitz, and W. Lauterborn, Phys. Rev. E **58**, 7208 (1998).
[19] We have encountered a mistake in the FFT statistical test in [6]. Following our correspondence with NIST, we have been advised to disregard this test [6].
[20] H. Schuster and W. Just, *Deterministic Chaos* (Wiley-VCH, Weinheim, 2005).