Numerical analysis of ultrafast physical random number generator using dual-channel optical chaos

Amr Elsonbaty
Salem F. Hegazy
Salah S. A. Obayya
Numerical analysis of ultrafast physical random number generator using dual-channel optical chaos

Amr Elsonbaty,a,b Salem F. Hegazy,a,c,† and Salah S. A. Obayya,a,*

Abstract. Fast physical random number generators (PRNGs) are essential elements in the development of many modern applications. We numerically demonstrate an extraction scheme to establish an ultrafast PRNG using dual-channel optical-chaos source. Simultaneous suppression of time-delay signature in all observables of the output is verified using autocorrelation-function method. The proposed technique compares the level of the chaotic signal at time $t$ with $M$ levels of its delayed version. The comparators [1-bit analog-to-digital converters (ADCs)] are triggered using a clock subject to an incremental delay. All the delays of the chaotic signal before the ADCs and the relative delays of the clock are mutually incommensurable. The outputs of the ADCs are then combined using parity-check logic to produce physically true random numbers. The randomness quality of the generated random bits is evaluated by the statistical tests of National Institute of Standards and Technology Special Publicaton 800-22. The results verify that all tests are passed from $M = 1$ to $M = 39$ at sampling rate up to 34.5 GHz, which indicates that the maximum generation rate of random bits is 2.691 Tb/s without employing any preprocessing techniques. This rate, to the best of our knowledge, is higher than any previously reported PRNG. © 2016 Society of Photo-Optical Instrumentation Engineers (SPIE) [DOI: 10.1117/1.OE.55.9.094105]

Keywords: optical chaos; physical random number generator; dual-channel chaos; postprocessing.

Paper 160966P received Jun. 20, 2016; accepted for publication Sep. 7, 2016; published online Sep. 28, 2016.

1 Introduction

Random number generators (RNGs) play a crucial role in many applications in the modern technology revolution. In fact, the ability to produce sequences of high quality random numbers are essential in wide area of applications ranging from computational chemistry, biophysics, and nuclear medicine1–4 to quantum cryptography5 and implementations of various computing applications and cryptographic systems in modern digital communications.6 In order to distinguish between different methods for implementing RNGs, the RNGs can be generally categorized into two types namely pseudorandom number generators and physical random number generators (PRNG). The main difference between the two classes is that while pseudorandom numbers are generated via deterministic algorithms that use a random seed, phenomena such as thermal noise in resistors, photon noise, and frequency jitter of oscillators have been employed as physical sources of entropy for realizing PRNGs.6

It is known that sequences of pseudorandom numbers generated from the same seed are identical, which degrades the reliability and level of security in systems using pseudorandom numbers. This shows the need of employing PRNGs to achieve irreproducible and unpredictable (truly) RNG. However, PRNG has been limited to much slower rates than pseudorandom RNGs due to phenomenal limitations of the rate and power of the mechanisms for extracting bits from underlying physical source of randomness.5 The slow generation rates of PRNG compared with high data rates of modern digital world applications are considered the fundamental weakness of this type of RNGs. So, the realization of fast PRNGs has become an active area of research in recent years.

Fast PRNGs are key parts in some promising modern applications due to their advantages compared with conventional pseudorandom number generators. For example, in information-theoretic secure key distribution, two legitimate users independently select the parameter values of laser systems in random way then some of the bits are discarded to generate common secret keys.7 Also, in quantum cryptographic system fast PRNGs are required to produce a large amount of truly random numbers. These random numbers are employed to control the modulation or measurement of single photons.8 The generation rate of random numbers is also one of the key parameters that restrict the speed of communications. Therefore, high generation rates in fast PRNGs are vital for these modern applications in order to attain high communications rates.

The optical chaos generated by semiconductor lasers with all-optical or electro-optical feedbacks has attracted considerable interest during the last two decades.9–13 From the applications’ point of view, it has some interesting features, such as broadband spectrum and extreme sensitivity to initial conditions. Thus, the high bandwidth optical chaos can be employed to solve the problem of slow output rates of PRNGs and render the realization of ultrafast PRNG possible as presented in recent works. The development of RNGs based on sampling the output of chaotic laser source has progressed recently in terms of generation rate. Various schemes for random number generation have been reported since the
first demonstration was carried out in 2008 at a generation rate of 1.7 Gb/s\(^{14}\) compared with no more than 10 Mb/s typical rates in physical noise generators.\(^{14}\)

Since then, by employing several post- and preprocessing techniques, such as high-resolution analog-to-digital converters (ADCs), high-order differential method, and bandwidth-enhanced chaos generation, the speed of PRNG has increased rapidly. For example, the generation rate of random bits has been increasing from the generation rate of 12.5 Gb/s in 2009\(^{15}\) to a rate of 75 Gb/s in 2010\(^{16}\) by employing the least significant bits (LSBs) technique in both RNGs. It was reported that high-order differential method increases the generation rate to 300 Gb/s whereas the bit-order reversal method along with eight LSBs sampled at 50 GHz brings up to 400 Gb/s rate.\(^{17}\) Recently, a generation rate of 3.2 terabit per second (Tb/s) was reached via high-order finite differences pseudo RNG\(^{19}\) in 2014 while a 1.4 Tb/s PRNG was reported in 2015 using chaotic data lines sampled at 100 GS/s by 8 bits ADC.\(^{20}\)

The value of feedback time-delay (TD) used in optical chaos generator represents one of the primary secret keys of chaotic system. An eavesdropper who can reveal the TD value is, at least in principle, readily able to reconstruct the optical chaos generator system. On the other hand, obvious TD signature badly affects the statistical performance of the PRNG. Therefore, it is essential to consider chaotic systems of suppressed TD signature in implementation of PRNGs.

The main objectives of this work is to propose and numerically demonstrate a multibit extraction scheme for generating ultrafast physical random sequence of bits by utilizing quite recent optical chaotic vertical cavity surface emitting laser (VCSEL)\(^{21}\) with suppressed TD signature in both intensity and phase of its two channel. The rest of the paper is organized as follows; the setup for the proposed PRNG is introduced in Sec. 2, the mathematical model and numerical results are introduced in Sec. 3, and finally Sec. 4 contains the conclusion.

## 2 Proposed Setup

The proposed technique uses an optical chaos generator of two output channels, based on single VCSEL diode, as shown in Fig. 1. The two output channels (CH\(_0\) and CH\(_1\)) are verified to be noncorrelated and of an ultrawide bandwidth.\(^{21}\) By tuning the variable attenuator VA2, one guarantees that the optical signal nonsaturates the subsequent optical detection. The fast photodetector PD2 translates the optical intensity of the signal at CH\(_0\) into an electrical signal, which is then amplified using the amplifier Amp2.

The amplified chaotic intensity signal at time \(t\), namely \(I(t)\), is subjected to an array of fast 1-bit ADCs. At the \(m\)'th 1-bit ADC, the signal \(I(t)\) is compared with its delayed versions \(I(t - T_m)\) where \(m = \{1, 2, \ldots, M\}\). The binary output of each 1-bit ADC is then sampled by a positive-edge-triggered \(D\) flip-flop that operates under the control of a clock signal at a rate \(f_c = 1/\tau\) (\(\tau\) is the clock period). The clock signal applied to the \(m\)'th flip-flop is relatively delayed such that its rising edge precedes the edge of the clock of a subsequent \(m + 1\) flip-flop by a fixed period \(\delta\tau = 1/M\). The outputs of all \(D\) flip-flops are then combined by means of a parity-check logic, therefore its output is sensitive to the individual flipping of each 1-bit ADC. Here, the timing of the different delay units is a crucial point of design. The different values of \(T_m\) are mutually incommensurable with

![Fig. 1 Schematic of the ultrafast PRNG using dual-channel optical chaos source. To the right is a snapshot of the output of four flip flops, in the first four rows, and combined result of parity-check logic on the last row. BS, beam splitter; VA, variable attenuator; HWP, half-wave plate; PBS, polarizing beam splitter; PD, photodetector; Amp, electro-optic gain; PM, phase modulator.](http://opticalengineering.spiedigitallibrary.org/094105-2)
where subscripts \( x \) and \( y \) stand for horizontal and vertical linear polarized (LP) modes, respectively, and the other parameters are described in Table 1.

We solve Eqs. (1)–(4) using the following VCSEL parameters values:

- \( k = 300 \text{ ns}^{-1} \)
- \( a = 4 \)
- \( g_N = 1 \text{ ns}^{-1} \)
- \( g_p = 0.5 \text{ ns}^{-1} \)
- \( g_r = 30 \text{ ns}^{-1} \)
- \( g_s = 50 \text{ ns}^{-1} \)
- \( \beta_{sp} = 10^{-6} \text{ ns}^{-1} \)
- \( \mu = 4.5 \)
- \( \omega_0 = 2.2176 \times 10^{15} \text{ rad/s} \)

For simplicity, we take \( g_1 = g_2 = g = 22.5 \text{ deg.} \) and \( \sqrt{\beta_{sp}} \zeta_s = 0 \). The fourth-order Runge–Kutta numerical method is utilized in solving rate Eqs. (1)–(4) at step size equals 0.2 ps. Theoretical study is employed to emphasize that first the TD signature is suppressed at chosen values of \( T_m \)'s that are used in the proposed setup. The concealment of TD signature implies that the proposed PRNG is reliable and immune to any trial to extract information about its parameters. This goal can be verified using the well-known autocorrelation function (ACF) technique, which has the advantage of being computationally efficient, robust, and immune to noise. As the tendency of a given time series waveform to match its time-shifted version is quantified by ACF, the locations of peaks in ACF curve identify the presence of TD signature in chaotic output waveform.

In this paper, the ACF employed for chaotic intensity and phase time series is defined as follows:

### Table 1 Description of the parameters of mathematical models (1) to (4)\(^{21}\)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( E )</td>
<td>Slowly varying complex amplitude of the electric field.</td>
</tr>
<tr>
<td>( k )</td>
<td>Cavity decay rate.</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>Linewidth enhancement factor.</td>
</tr>
<tr>
<td>( g_N )</td>
<td>Decaying rate of total carrier population.</td>
</tr>
<tr>
<td>( N )</td>
<td>Total carrier inversion between the conduction and valence bands.</td>
</tr>
<tr>
<td>( n )</td>
<td>Difference between carrier inversions of the spin-up and spin-down radiation channels.</td>
</tr>
<tr>
<td>( g_1 ) and ( g_2 )</td>
<td>Feedback strengths of the LP modes.</td>
</tr>
<tr>
<td>( \tau_{01} )</td>
<td>Delay period between VCSEL and PBS.</td>
</tr>
<tr>
<td>( \tau_{02} )</td>
<td>Optical delay period between PBS and M.</td>
</tr>
<tr>
<td>( \tau_\varnothing = 2 (\tau_{01} \tau_{02}) )</td>
<td>Optical roundtrip time.</td>
</tr>
<tr>
<td>( \varnothing )</td>
<td>Electronic time delay of the electro-optic feedback.</td>
</tr>
<tr>
<td>( g_s ) and ( g_p )</td>
<td>Linear anisotropies representing dichroism and birefringence, respectively.</td>
</tr>
<tr>
<td>( g_s )</td>
<td>Spin-flip rate.</td>
</tr>
<tr>
<td>( \beta_{sp} )</td>
<td>Spontaneous emission factor.</td>
</tr>
<tr>
<td>( \zeta_s ) and ( \zeta_y )</td>
<td>Gaussian white noises of zero mean value and unit variance.</td>
</tr>
<tr>
<td>( \mu )</td>
<td>Normalized injection current with ( \mu = 1 ) at threshold.</td>
</tr>
<tr>
<td>( \omega_0 )</td>
<td>Center frequency of the solitary VCSEL.</td>
</tr>
</tbody>
</table>
where $\rho(t)$ is either intensity time series $I(t)$ or phase time series $\phi(t)$, $\langle \rangle$ denotes the time average, and $\Delta t$ is the lag time, which is taken at 25 ps steps in numerical simulations.

The strength or weakness of TD signature can be examined mathematically via computing peak signal-to-mean ratio (PSMR). The PSMR value is obtained from evaluating the ratio

$$
\text{Max} \left[ \frac{\left\langle |\rho(t + \Delta t) - \langle \rho(t + \Delta t) \rangle|/ |\rho(t) - \langle \rho(t) \rangle| \right\rangle}{\left\langle |\rho(t + \Delta t) - \langle \rho(t + \Delta t) \rangle|^2 / |\rho(t) - \langle \rho(t) \rangle|^2 \right\rangle^{1/2}} \right],
$$

for $\Delta t \in [\tau_o - \delta \times \tau_o, \tau_o + \delta \times \tau_o]$, $\tau_o$ is the TD value utilized in optical chaos generator and $\delta$ is defined as the mismatched coefficient.

Numerical simulations are carried out using suitable values of parameters. To improve the randomness quality of the generated random bit sequence, these values are determined via calculating the accumulated PSMRs for ACF of chaotic intensity and phase time series in $x$ and $y$ channels as shown in Fig. 2. It turns out that the dark regions in $g - \tau_o$ parameters space in Fig. 2, e.g., $g = 18$ ns$^{-1}$ and $\tau_o = 5$ ns, correspond to the smallest values of PSMR and, therefore, represent appropriate parameters for simultaneous suppression of TD signature in all observables, i.e., intensity and phase of $x$ and $y$ polarizations. In other words, the operation at these dark regions allows generation of high quality random bits utilizing both $x$ and $y$ output channels. Figure 3 shows the concealment of TD signature for the dark region $g = 18$ ns$^{-1}$ and $\tau_o = 5$ ns of both $x$ and $y$ channels.

The relaxation oscillation period $\tau_o$ is one of key factors that affect the bandwidth of chaotic output. For the proposed setup and mentioned values of parameters, it has the value of 0.13711 ns. The technique of utilizing delayed versions of chaotic output is employed in order to overcome the limitations introduced by $\tau_o$ and, therefore, increase the sampling rate while TD signature is suppressed via careful choice of system parameters.

In the numerical analysis, the values of time delays $T_m$ are chosen incommensurable to increase the complexity of the system and enhance the concealment of any TD feature that may appear as a result of applying statistical methods to the generated sequence. The values of $T_m$ used in simulation are chosen as $T_m = 10^{-9} \times \mu \times m$, $m = 1, 2, \ldots, M$, and $\mu$ is any suitable positive real number render the proposed setup achieve the previously mentioned goals. From intensive trials of different values of $\mu$ in the interval $[1, 5]$ with steps 0.1, it is found that the value $\mu = 3.2$ gives best performance among selected values in this interval and, therefore, we fix this value in numerical simulations.

Furthermore, the proposed PRNG requires absence of any correlations, i.e., local or nonlocal time dependence between the outputs of two LP modes in optical chaos generator. The phase portrait graphs uncover the local time dependence between time series while crosscorrelation function (CCF) can be considered as a tool for measuring nonlocal time dependence. Figure 4 shows the phase portraits and CCF of intensities $I_x = |E_x|^2$ and $I_y = |E_y|^2$ and of phases $\phi_x = \text{Arg}(E_x)$ and $\phi_y = \text{Arg}(E_y)$. It is shown that the two LP modes are independent and do not have any type of correlation.

The randomness quality of the generated bits is investigated using 15 standard statistical tests in National Institute of Standards and Technology (NIST) SP 800-22 at different values of $M$ in order to evaluate the maximum random bits generation rate of the proposed scheme. The NIST tests are conducted on 1000 1-Mbit sequences for a significance level of 0.01. In order to successfully pass a particular test, the proportion of sequences with $p$-values greater than the predetermined significance level must be in the range of $0.099 \pm 0.0094392$.

For each value of $M$, starting from $M = 1$ and increasing by unit step at each stage, numerical simulations are conducted for different initial conditions in order to collect 1000 different sequences of generated random number. Each sequence is 1 M-bit in size. Then, all 15 standard NIST tests are applied on each sequence while tracking the proportion of sequences, which pass all tests.

The results show that all tests are successfully passed from $M = 1$ to $M = 39$ at sampling rates extend from
1/τ_r = 7.3 G sample/s up to 34.5 G sample/s. Noticing that these samples are taken from each output channel of the chaotic source. This implies that the maximum generation rate of random bits is estimated as 2 × 39 × 34.5 = 2.691 Tb/s using one chaotic source composed of single VCSEL and without employing any preprocessing techniques. Increasing M further degrades the performance of output random bits such that one or more of the statistical tests fails. The following table, Table 2, shows an example of tests results obtained at M = 39 where the mean of P-values obtained for each test is illustrated in each column and for tests with multiple P-values, the worst case is shown.

### 4 Conclusion

We have numerically examined the problem of generating truly physical random bits at an ultrafast rate via optical chaos. The proposed scheme employs dual-channel chaotic laser source with simultaneous TD signature suppression in both its intensity and phase in order to attain the ultrafast rate with high level of randomness. The technique utilizes M values of intensity chaos sampled at incommensurable delay-intervals from each output channel along with relative delay between rising edges of triggering clocks. The generated random bits have passed standard tests of randomness at ultrafast rates up to 2.691 Tb/s. The physical characteristics of the optical chaos source, represented in the bandwidth of the chaotic output, limits the rate of the generated physical random bits to a value corresponding to M = 39. In the future, further study employing enhanced broadband optical chaos source can be investigated in order to examine the possibility of enhancing the rate of physical random numbers while keeping the high quality of generated random bits.

### References


**Amr Elsonbaty** received his PhD in engineering mathematics from Mansoura University in 2015. Since then, he has been an assistant professor with the faculty of engineering, Mansoura University, and also a postdoc researcher with Centre for Photonics and Smart Materials, Zewail City of Science and Technology. His current research interests include nonlinear dynamics of electronic circuits, chaos control and synchronization, chaos generation utilizing lasers, and chaotic optical communication systems.

**Salem F. Hegazy** has been a researcher at the National Institute of Laser Enhanced Sciences, Cairo University, and also at the Centre for Photonics and Smart Materials, Zewail City of Science and Technology. He currently conducts research at CREOL, the College of Optics and Photonics, University of Central Florida, in pursuit of finishing his PhD. His research interests include entanglement generation and manipulation, optical chaos systems, optical delay systems, quantum cryptography, and quantum optics experiments.

**Salah S. A. Obayya** has built an international reputation in the area of green nanophotonics with focus on the intelligent computational modeling of modern nanophotonic devices. He has a track record of 151 journal publications, mostly in IEEE and IET/IEE journals, two authored books published by the world-leading scientific publisher Wiley, and 208 conference presentations. He was recently awarded the DSc for distinctive, high quality, and sustained records of world class research, City University London, 2015.