IEICE Proceeding Series

All-optical Random Number Generator

Pu Li, Jian-Zhong Zhang, Yun-Cai Wang

Vol. 1 pp. 130-133
Publication Date: 2014/03/17
Online ISSN: 2188-5079

All-optical Random Number Generator

Pu Li, Jian-Zhong Zhang and Yun-Cai Wang

Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education of China),
College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China
Email: wangyc@tyut.edu.cn

Abstract– Chaotic laser has become a promising candidate for Gb/s true random number generator (TRNG) in recent years because of its high bandwidth. Most TRNGs based on chaotic laser process signals in the electronic domain, and thus their rates will be limited by 'electronic bottleneck'. In this paper, we review our recent works on all-optical TRNGs. All-optical TRNGs are not only based on the entropy source of chaotic laser, but also do all signal processing in the optical domain. Especially, we propose and theoretically demonstrate a novel all-optical method which generating all-optical random numbers from discrete chaos produced by a mode-locked laser. In this method, discrete chaotic pulses are directly quantized into random number sequences via an all-optical flip-flop, unlike previous RNGs which require sampling procedure and external triggered clocks before quantization. Moreover, free from post-processing, the obtained random number sequence has a high-quality randomness verified by industry-standard statistical tests. Therefore, our approach can bypass the possible aliasing problem caused by sampling procedure and greatly reduce hardware complexity.

1. Introduction

Random numbers have attracted considerable attentions due to their wide applications especially in secure communications. The quest for true randomness has engendered physical or true random number generators (TRNGs) which extract nondeterministic random numbers from unpredictable physical processes to ensure the information security. Among various physical entropy sources, chaotic laser is the most attractive for fast random number generation in recent years. There have been many TRNGs based on chaotic laser [1-2]. However, most of them have a common feature that they process signals in electrical domain faced with the 'electronic bottleneck'.

In contrast, all-optical signal processing can overcome the limitation imposed by electronic-based systems. Moreover, in future ultra-fast all-optical communications, all-optical devices will be required in order to reduce latency and maintain the high bandwidth of the network. Therefore, it will be meaningful and necessary for secure communications to develop all-optical technique to generate physical random numbers.

Recent years, our group has done some preliminary researches on the topic of all-optical TRNG based on chaos which do their signals processing in the optical domain. In this paper, we review our works and hope they can spur more interests towards the implementation of ultrahigh speed all-optical TRNGs. Our works mainly consists of three schemes [3-5] involving several all-optical techniques. In the following sections, they will get elaborated respectively.

2. All-optical TRNG based on chaotic lasers

2.1. Scheme 1

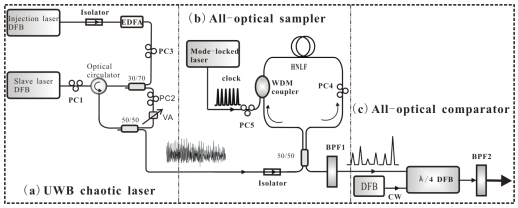

Fig. 1. Schematic diagram of the first all-optical TRNG: (a) UWB chaotic laser; (b) all-optical sampler; (c) all-optical comparator.

The schematic diagram of the first all-optical TRNG is shown in Fig. 1, which includes three parts: an ultra-wide bandwidth (UWB) chaotic laser as random number source, a Sagnac interferometer as all-optical sampler and a λ/4-shifted DFB lasers (λ/4 DFB) as all-optical comparator. The output of UWB chaotic laser, whose intensity varies unpredictably with time, is sampled through the all-optical sampler driven by an optical clock, and then converted into a random number sequence using the all-optical comparator.

2.1.1 UWB chaotic lasers

The implementation of the UWB chaotic laser is shown in Fig. 1(a). A slave single-mode distributed-feedback laser diode (DFB) is subject to optical feedback with a fiber ring cavity to generate original chaos. Another DFB, the injection laser, is used to enhance the bandwidth of the original chaotic signal by injecting continuous-wave (CW) light into the slave laser through a 30/70 optical fiber coupler. The injection laser is wavelength adjusted to an appropriate optical frequency detuning to the free-running slave laser. Finally, a UWB chaotic laser can be generated.

The system above can be modeled by a set of rate equations for slave laser electric complex amplitude E and carrier density N, respectively, as expressed in the following equations:

$$\frac{\mathrm{d}E}{\mathrm{d}t}=\frac{1+i\alpha}{2}\left[\frac{g(N-N_0)}{1+\varepsilon|E|^2}-\tau_{\mathrm{p}}^{-1}\right]E+\frac{\kappa_{\mathrm{f}}}{\tau_{\mathrm{in}}}E(t-\tau)\times\exp(-i2\pi\nu_{\mathrm{s}}\tau)+\frac{\kappa_{\mathrm{j}}}{\tau_{\mathrm{in}}}E_{\mathrm{j}}\exp(i\Delta\nu t), \quad (1)$$

$$\frac{\mathrm{d}N}{\mathrm{d}t}=\frac{I}{qV}-\frac{N}{\tau_{\mathrm{N}}}-\frac{g(N-N_0)}{1+\varepsilon|E|^2}|E|^2, \quad (2)$$

where κ_f and κ_j denote the feedback and injection strength, the amplitude of injection laser $|E_j|$ is equal to that of the solitary slave laser. The following parameters were used in simulations: transparency carrier density N_0 = 0.455× 10^6 μm^{-3}, threshold current I_{th} =22 mA, differential gain g =1.414×10^{-3} μm^{-3}ns^{-1}, carrier lifetime τ_N =2.5 ns, photon lifetime τ_p =1.17 ps, round-trip time in laser intra-cavity τ_{in} =7.38 ps, line-width enhancement factor α =5.0, gain saturation parameter ε = 5×10^{-5} μm^3, active laser volume V= 324 μm^3. The slave laser was biased at 1.7I_{th}.

Figure 2 are the rf spectrum and autocorrelation curve of the generated UWB chaotic laser which has a bandwidth about 10.5 GHz. A time sequence of the UWB chaotic laser from 0 to 2 ns is given in Fig. 3(a).

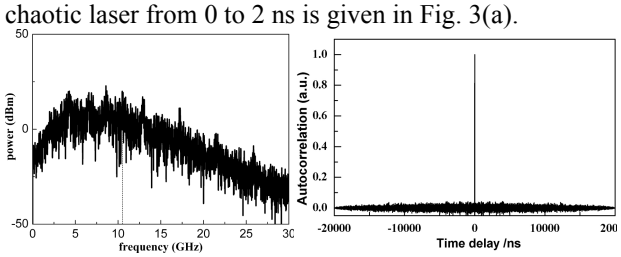

Fig. 2. The rf spectrum (left) and autocorrelation characteristics (right) of the obtained UWB chaotic laser.

2.1.2 All-optical sampling procedure

The all-optical sampler consists of an optical switch based on a nonlinear Sagnac interferometer as shown in Fig. 1(b). This optical switch mainly consists of a 3dB coupler (50/50), a WDM coupler, a mode-locked laser, a highly nonlinear fiber (HNLF), an isolator and an optical bandpass filter (BPF1). In order for this device to work as an all-optical sampler, a train of clock pulses generated by the mode-locked laser are launched as the control light into the Sagnac loop via the WDM coupler, while the UWB chaotic light is injected as the probe light into the loop via the 3dB coupler. The output level is determined by the amount of the cross-phase modulation (XPM) exerted by the control light onto the probe light.

Transmitted optical power of UWB chaotic light P_{out} satisfies the following formula:

$$P_{out} = \frac{1}{2} P_{in}[1 - \cos(\varphi_{CW} - \varphi_{CCW})], \quad (3)$$

where P_{in}=$|E_{in}|^2$ is the power of the injected chaotic light and φ_{CW} - φ_{CCW} is the phase difference between the clockwise and the counter clockwise traveling chaotic light. Note, φ_{CW}=2$\gamma P_{peak}L$ and φ_{CCW}=2$\gamma P_{ave}L$, where P_{peak} and P_{ave} are the peak and average power of each clock pulse, L is the length of HNLF, γ are the fiber attenuation coefficient.

Figure 3 shows the sampling results with this method. In simulation, L = 50 m and γ= 20 W^{-1}km^{-1}. The sampling clock pulse sequence generated by the mode-locked laser operating is shown in Fig. 3(b), which is in the format of Gauss, pulse width is 20 ps, peak power is 1 W and frequency is 10 GHz. Figure 3(c) is a sampled chaotic laser pulse train, whose mean power is 1.45 mW.

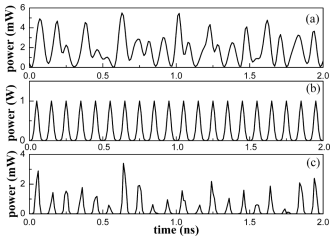

Fig. 3. Temporal waveforms: (a) the output of UWB chaotic laser; (b) sampling clock; (c) the output of all-optical sampler.

2.1.3 All-optical comparator

The realization of the all-optical comparator is based on the bistability proposed by Huybrechts et al. in 2008. Under injection of only continuous-wave (CW) light, the λ/4 DFB can exhibit this phenomenon. A typical experimental result is shown in Fig. 4(left). It is clear that when injection light power is above P_{th2} named as the threshold power, the output power of lasing light will jump down to a tiny level of nearly 0. Otherwise, the output power of lasing light will maintain a higher level around 1 mW.

Based on the above, we have designed a comparator as shown in Fig. 1(c), where the sampled chaotic pulses and a CW light with the same wavelength as the sampled chaotic pulses are simultaneously injected into a λ/4 DFB. The bandpass filter (BPF2) removes the amplified injection light and transmits only the lasing light of the λ/4DFB. When the sampled chaotic pulse power is above the P_{th2}, the lasing light output time-train will have a low power level, which represents "0", and otherwise, represents "1". Figure 4(right) is the output waveform of the all-optical comparator (i.e. raw random bit strains).

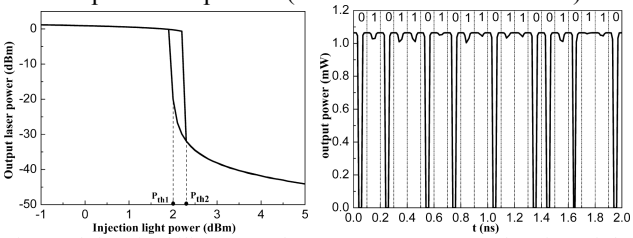

Fig. 4. (left) Bistability curve: laser output power as a function of the power of the injected light. (Right) Raw random bit sequence generated by the all-optical TRNG.

3.1.3 All-optical XOR gate

After the above operations, a random number sequence with a rate corresponding to the frequency of the control clock has been generated. But it contains an unwanted bias. To eliminate the bias, the random number sequence need to be exclusive-or processed by an all-optical XOR gate, as shown in Fig. 5. The configuration of the all-optical XOR gate is based on a Mach-Zehnder interferometer with an identical HNLF or SOA in each arm. A beam of continuous-wave (CW) light is split by a 50/50 coupler into two arms as probe light, and the output of two independent RNGs are respectively launched into arm 1 and arm 2 as control light, through WDM couplers (WDM). The control light induces the phase shift of the probe light due to the XPM in HNLF. After that, the probe

light is finally exported via another 50/50 coupler. To simplify the simulation procedure, we adopted the XOR gate based on HNLF shown in Fig. 5(a).The interaction between the random number sequence and the CW light in HNLF is numerically simulated according to Eq. 3.

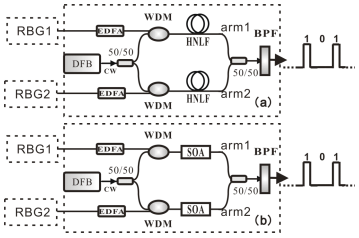

Fig. 5. All-optical XOR gate: (a) based on HNLF-MZI, (b) based on SOA-MZI.

Figure 6 is the output waveform of the all-optical XOR gate. In the simulation, the CW light power was about 1 mW, and two uncorrelated random signals from different all-optical RNGS were amplified by different EDFAs respectively so that their "1" level was around 1 W. From Fig. 6, we can find that the random bit sequence is in the format of return-to-zero (RZ), with a rate of 10 Gb/s, corresponding to the frequency of the sampling optical clock pulses. The randomness can pass standard statistical test suite provided by the National Institute of Standard Technology (NIST).

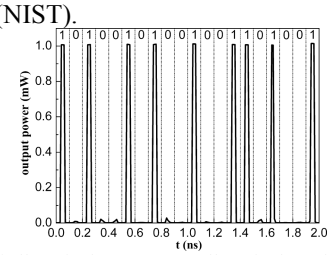

Fig. 6. Output of all-optical XOR gate: all-optical random bit sequence.

3.2. Scheme 2

Considering the weak coherence of chaotic laser, the all-optical sampling part in scheme 1 may be difficult to realize in practice. Thus, we replace it with a Mach-Zehnder modulator (MZ) as shown in Fig. 7: the UWB chaotic laser output is converted into a radio-frequency (RF) signal by a photodetector (PD), which is applied to the Mach-Zehnder modulator (MZ) as the modulating signal. Optical clock pulses generated by the mode-locked laser (MLL) are sent to the MZ to sample the RF signal and then the modulated pulse train is split into two identical trains by a 3dB coupler (3dB). One of them is injected into the right-hand side of the distributed feedback laser diode (DFB) via a length of fiber delay line (FDL), while the other is injected into the left-hand side of the DFB, combined with a continuous wave light (CW) by a WDM coupler (WDM). Here, the DFB acts as an all-optical flip-flop (AOFF), which plays the role of quantizing chaotic signal in the whole system. Finally, with a circulator and an optical band-pass filter (BPF), we can separate the light of the DFB laser from the injected light and visualize the random number sequence on the oscilloscope (OSC).

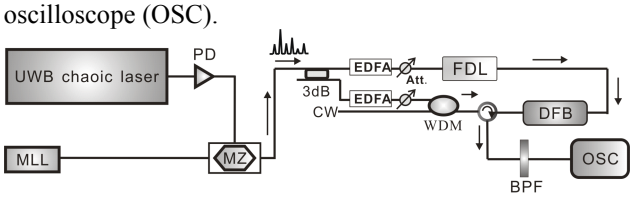

Fig. 7. Schematic diagram of the proposed RBG

Figure 8(a) is a time series of UWB chaotic laser with a bandwidth of 10.5 GHz, from 0 to 4 ns. Figure 8(b) is the optical clock pulses from the MLL. The pulse is in the format of Gauss, whose width is 7 ps, peak power is 1.3 mW and repetition frequency is 5 GHz. Figure 8(c) shows the modulated pulse train after 3dB coupler, which is injected into the DFB from its left facet. Figure 8(d) is the identical pulse train delayed by 100 ps on the right side of the DFB. The average power of modulated pulses is about 0.1 mW. The modulation process was simulated as follows: The intensity of modulated pulses train has a direct correspondence to the RF chaotic signal, which can be described as: $I_o(t)=I_{in}(t)[1+\cos(\varphi_s+\varphi_b)]/2$, where, $I_{in}(t)$ is the input optical clock pulses intensity, $\varphi_s=\pi V_s(t)/V_\pi$ is the phase shift induced by the RF signal $V_s(t)$, $\varphi_b=\pi V_b/V_\pi$ is the phase shift induced by the bias voltage V_b, V_π is the half-wave voltage of the modulator. Figure 8(e) is an output waveform of the AOFF. The AOFF are also based on a single λ/4-shifted DFB laser (DFB) in Section 3.1. In simulations, the power of holding light (CW) was set to 1.6 mW (i.e. P_{th1} shown in Fig. 4), so that the threshold (i.e. $\Delta P=P_{th2}-P_{th1}$) equals to 0.1 mW.

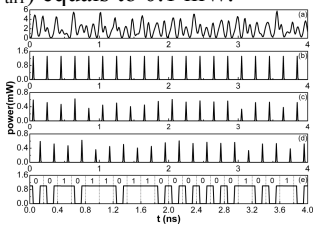

Fig. 8. Temporal waveforms: (a) output of UWB chaotic laser. (b) sampling clock pulses. (c) modulated pulses strain. (d) modulated pulses strain delayed by 100ps. (e) raw random bit sequence.

After the above processes, we can get a train of raw random bits with a rate of 5 Gb/s determined by optical clocks [Fig. 7]. To eliminate the bias, the raw random bit sequences were also operated with an all-optical XOR gate [Fig. 5]. The post-processed random bit sequences can also pass successfully NIST tests.

4. All-optical TRNG Based on Pulse Amplitude Chaos

Although the two TRNGs above can achieve high-quality random bit sequence generation, they are complex. Herein, we introduce another method based on pulse amplitude chaos to simplify the existing schemes.

Figure 9 is the schematic diagram of the proposed all-optical TRNG. The only difference with Scheme 2 is that the chaotic laser and all-optical sampler are replaced with a mode-locked fiber ring laser (MLFRL). The MLFRL laser is a ring laser configuration using the nonlinear

polarization rotation (NPR) technique. The cavity is composed of a polarization-dependent isolator (PDI) and two polarization controllers (PC1 and PC2) in a single mode fiber (SMF) and an erbium-doped fiber (EDF), which is pumped via a wavelength-division multiplexed coupler (WDM) at 1480 nm and provides gain to the cavity. The mode-locked pulse stream is finally coupled out through an optical coupler (OC).

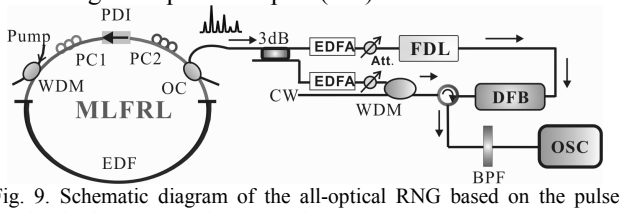

Fig. 9. Schematic diagram of the all-optical RNG based on the pulse amplitude chaos in a mode-locked fiber ring laser (MLFRL).

Pulse amplitude chaos is an intrinsic feature of NPR MLFRLs, and its generation can be well described by the extended coupled complex nonlinear Schrödinger equations:

$$\frac{\partial u}{\partial Z}=i\frac{\Delta\beta}{2}u-\delta\frac{\partial u}{\partial T}-i\frac{\beta_2}{2}\frac{\partial^2 u}{\partial T^2}+\frac{\beta_3}{6}\frac{\partial^3 u}{\partial T^3}+i\gamma(|u|^2+\frac{2}{3}|v|^2)u+\frac{i\gamma}{3}v^2u^*+\frac{g}{2}u+\frac{g}{2\Omega_g^2}\frac{\partial^2 u}{\partial T^2}, \quad (1)$$

$$\frac{\partial v}{\partial Z}=i\frac{\Delta\beta}{2}v-\delta\frac{\partial v}{\partial T}-i\frac{\beta_2}{2}\frac{\partial^2 v}{\partial T^2}+\frac{\beta_3}{6}\frac{\partial^3 v}{\partial T^3}+i\gamma(|v|^2+\frac{2}{3}|u|^2)v+\frac{i\gamma}{3}u^2v^*+\frac{g}{2}v+\frac{g}{2\Omega_g^2}\frac{\partial^2 v}{\partial T^2}, \quad (2)$$

In the above equations, u and v are the normalized envelopes of the optical pulses along the two orthogonal polarized modes of the optical fiber. In simulation, the whole cavity length L is set as 10 m, which consists of a 2 m-long EDF with β_2= 50 ps/nm/km and two sections of 4 m-long SMF with β_2 = −30 ps/nm/km. Other parameters are set as follows: γ = 4 W^{-1}km^{-1}, β_3= 0.1 ps^2/nm/km, Ω_g= 25 nm, L_B= L/2, P_{sat} = 250 and the orientation of passive polarizer to the fiber fast axis θ= 0.125π [5].

With the above parameter selection, this MLFRL can emit pulse amplitude chaos in a pump power range of 348 km^{-1} < G < 350 km^{-1}. We arbitrarily select an operating point in the chaos region with G = 349 km^{-1} to analyze the characteristics of pulse amplitude chaos. Figure 10(left) and 10(right) are the time series in three-dimensional form and autocorrelation function of the extracted chaotic pulse powers, respectively. What is clear in Fig. 10(right), is that no apparent harmonic peak in the autocorrelation characteristics is found. This indicates the correlation of the generated pulse amplitude chaos is statistically insignificant and has no periodic components harmful to true random number generation.

Further, we get true random bits by quantizing the pulse amplitude chaos with the same method as that in scheme 2, as illustrated in Fig. 11. Figure 11(a) is a time series of pulse amplitude chaos generated by the MLFRL, which consists of a chaotic pulse train with a fixed frequency of 20 MHz but randomly distributed pulse powers. Figure 11(b) shows the chaotic pulse train after the 3-dB coupler, which is injected into the DFB from its left facet and with a mean power about 0.1 mW. Figure 11(c) is the identical pulse train delayed by 25 ns on the right side of the DFB. Figure 11(d) is an output waveform of the AOFF (the DFB), the random bit sequences. Through testing the TRNG with NIST and Diehard suite, the obtained random bits without post-processing has high-quality randomness.

Finally, we point out that the TRNG here is a conceptual protocol and its bit rate can be further increased by using MLFRLs with higher repetition rate or multiplexing technology.

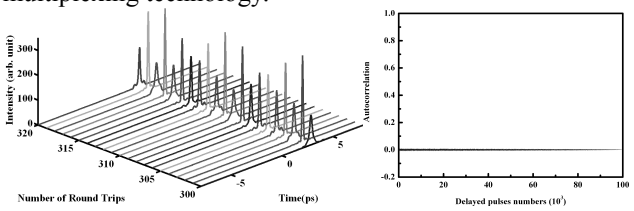

Fig. 10. (left) Chaotic state with a fixed linear cavity phase delay bias of 1.6 π under different pump strength; (right) Auto-correlation characteristic of the chaotic pulse power.

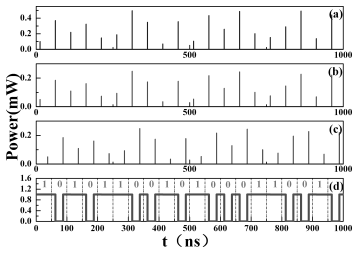

Fig. 11. Temporal waveforms: (a) Pulse amplitude chaos from the MLFRL. (b) Pulse amplitude chaos injected into the left-hand of the AOFF. (c) Delayed pulse amplitude chaos injected into the right-hand of the AOFF. (d) Random bit sequence.

5. Conclusions

In this paper, we have reviewed our recent works on all-optical TRNGs. The first scheme is comprised of chaotic entropy sources, all-optical samplers, all-optical comparators, and all-optical gates. Considering the weak coherence of the chaotic laser, we improve all-optical sampling procedure by replacing Sagnac interferometers with electro-optical modulators. In order to further simplify the previous scheme, we demonstrate that a TRNG can be achieved with pulse amplitude chaos in MLLD, which do not need sampling and post-processing procedures.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 60927007 and Grant No. 61001114).

References

[1]A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nat. Photon.*, vol. 2, pp. 728-732, 2008.

[2]I. Kanter *et al.*, "An optical ultrafast random bit generator," *Nat. Photon.*, vol. 4, pp. 58-61, 2009.

[3]P. Li *et al.*, "All-optical fast random number generator," *Opt. Express*, vol. 18, pp. 20360-20369,2010.

[4]Y. C. Wang *et al.*, "Fast random bit generation in optical domain with ultrawide bandwidth chaotic laser," *IEEE Photon. Technol. Lett.*, vol. 22, pp.1680–1682, 2010.

[5]P. Li *et al.*, "Direct generation of all-optical random numbers from optical pulse amplitude chaos," *Opt. Express*, vol. 20, pp. 4297-4308, 2012.