Optics Communications 321 (2014) 1–5

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

All-optical random number generation using highly nonlinear fibers by numerical simulation

Juanfen Wang [a,*], Junqiang Liang [a,b], Pu Li [a], Lingzhen Yang [a], Yuncai Wang [a]

[a] *Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan, 030024, PR China*
[b] *Department of Technology, Anhui Shenjian Technology Co. Ltd., Heifei 230022, PR China*

ARTICLE INFO

Article history:
Received 12 October 2013
Received in revised form
18 January 2014
Accepted 19 January 2014
Available online 31 January 2014

Keywords:
All-optical random number
Highly nonlinear fiber (HNLF)
Chaotic laser

ABSTRACT

A new scheme of all-optical random number generation based on the nonlinear effects in highly nonlinear fibers (HNLF) is proposed. The scheme is comprised of ultra-wide band chaotic entropy source, all-optical sampler, all-optical comparator and all-optical exclusive-or (XOR), which are mainly realized by four-wave mixing (FWM) and cross-phase modulation (XPM) in highly nonlinear fibers. And we achieve 10 Gbit/s random numbers through numerically simulating all the processes. The entire operations are completed in the all-optical domain, which may overcome the bottleneck problem of electronic devices, and apply directly in high-speed all-optical communication network.

1. Introduction

Random numbers have a wide range of applications in information security [1–2], scientific computing [3], commercial finance [4] and other fields. Especially in the field of information security which is based on the cryptography, the quality of random numbers is directly related with the secure transmission of information. There are two types of random numbers according to different producing methods: pseudo-random numbers and physical random numbers. Pseudo random generator can be used to easily produce a high rate random numbers. However, pseudo-random numbers have a fatal defect because of its periodicity. Once an attacker knows the seed and generation algorithm, it is possible to obtain the entire key information through enough computing. Pseudo-random numbers may not remain sufficient for modern applications. In contrast, physical random numbers are generated by stochastic physical entropy source in the natural world, such as thermal noise in resistors [5], frequency jitter in oscillator [6], single photon splitting on a beam-splitter [7–10], amplified spontaneous emissions [11–14], chaotic laser [15–21] and so on. Because of the inherent uncertainty of these random sources, physical random numbers are unpredictable and sensitive to initial conditions.

Among them, chaotic laser has received the widespread attentions because it has high bandwidth and sensitivity to initial condition. In 2007, our group put forward a patent about random number generator based on chaotic lasers produced by optical feedback semiconductor laser [15]. In 2008, Uchida's team for the first time realized a 1.7 Gbit/s random number generator (RNG) in experiment using two unrelated ultra-wide bandwidth chaotic lasers [16]. Then Kanter's team achieved 300 Gbit/s random numbers outputs with chaotic laser by more than one bit analog-to-digital converter (ADC) [18]. Pikasis's team obtained 560 Gbit/s random numbers with amplified spontaneous emission noise by differential and serial-to-parallel conversion [14]. Although hundreds of Gbit/s physical true random numbers can be obtained with the chaotic lasers and amplified spontaneous emission noise, the subsequent software operations are needed. The single channel operation is still limited by the bottleneck of electronic devices. Moreover, in the face of the rapid development of all-optical communication networks, the electric random number generators need optical–electric–optical converters, which seriously affect the speed of information processing and the cost of project. In order to overcome the electronic bottleneck problem, our group has proposed a series of schemes of all-optical random number generator which can be better compatible with high-speed optical communication networks. And 10 Gbit/s random numbers are obtained by use of a 1-bit all optical analog-to-digital conversion (ADC) [22–24]. But the all-optical samplers of these schemes require the signal light with a stable polarization state and good coherence. However, chaotic laser has poor coherence and polarization instability, which reduce sampling efficiency.

In this paper, we propose a new scheme of all-optical random number generation based on the nonlinear effects in HNLF. In this

* Corresponding author.
E-mail address: wangjuanfen@126.com (J. Wang).

0030-4018/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2014.01.044

scheme, the polarization insensitive sampling for chaotic laser is implemented by using FWM. The paper is organized as follows: in Section 2, we present the principle of all-optical RNG, including: all optical sampler, all-optical comparator and all-optical exclusive-or (XOR). In Section 3, we achieve numerically 10 Gbit/s random numbers using ultra-wide band chaotic entropy source. Section 4 is discussion. Finally, we summarize our results in Section 5.

2. Principle of all-optical RNG

The schematic diagram of the all-optical RNG based on the nonlinear effects in HNLF is shown in Fig. 1. The clock pulse sequence generated by mode-locked laser (MLL) and ultra-wide band chaotic laser are coupled into the HNLF by the polarization beam splitter (PBS). All-optical polarization insensitive sampling for chaotic laser is implemented in HNLF. Through the optical bandpass filter (BPF1), a chaotic optical pulse sequence is obtained. Then the chaotic optical pulse sequence is injected into the all-optical comparator as the control light. By controlling the phase difference between the continuous lights in two arms of Mach–Zehnder interferometer, we can obtain raw random numbers by the interference of two continuous lights. Specific principles are as follows:

2.1. Principle of all-optical sampler

The schematic diagram of polarization insensitive sampling which was proposed in Ref. [25] for chaotic light is shown in Fig. 1(a) [26]. The clock pulses as pump light are generated with linear polarization by the mode-locked laser (MLL) and amplified by erbium-doped fiber amplifier (EDFA). Then this pulse train is rotated by a polarization controller (PC1) and launched at 45° with respect to the axis of the PBS. This ensures that the pump pulses have the same power at the output ports of the PBS. The chaotic laser, the signal in the FWM process, is generated by the chaos source (CHAOS). The chaotic laser signal light is also coupled into the PBS by an optical coupler (OC1) with the MLL clock pump pulse train and separated into o light and e light. The o light transfers by counter-clockwise and realizes four-wave mixing sampling in HNLF. The e light transfers by clockwise and realizes the sampling in HNLF. By filtering the older generated by FWM between the clock pulse train and the chaotic signal, a pulse train with chaotically varying amplitude is generated at the signal wavelength, aligned with BPF1. Therefore the polarization insensitive sampling for chaotic laser is achieved [26].

By analysis of the characteristics of the chaotic source and the phase matching conditions of four-wave mixing sampling, we have discussed all-optical sampling for chaotic laser by the numerical method in Ref. [26].

2.2. Principle of all-optical comparator

As shown in Fig. 1(b), the all-optical comparator consists of a Mach–Zehnder interferometer (MZI) and a ring resonator [27]. Port A and C are the input side and output side of the all-optical comparator respectively. The ring resonator between the two arms of Mach–Zehnder interferometer is a HNLF. OC2 and OC5 are 3dB couplers. The optical isolator ISO1 and ISO2 are used to eliminate the circuit signal from the ring resonator. The chaotic pulse sequence as the control light, which is obtained from all-optical sampler in Fig. 1(a), is injected into the ring resonator by wavelength division multiplexing (WDM). And it transmits along a counterclockwise direction in the ring resonator. The continuous-wave light (CW) generated from DFB semiconductor laser is injected into the MZI from port A, and divided into two ways by 3dB coupler OC2. One CW light in the upper arm of MZI is coupled into the ring resonator by OC3. The CW light transmits along a clockwise direction, which is in the opposite direction with chaotic optical pulse. So the cross-phase modulation (XPM) between the CW light and chaotic optical pulse can be negligible. However, the other CW light in the lower arm of MZI is coupled into the ring resonator by OC4. And it transmits in same direction with chaotic optical pulse. Its phase is influenced by the XPM. Thus, there exists phase difference between the upper and lower arms. Finally the lights of two arms are coupled into the OC5, and superimposed out at port C.

The transmissivity T of port C is

$$T=[1-\cos(\Delta\Phi_{eff})]/2, \tag{1}$$

where $\Delta\Phi_{eff}$ is the total phase difference between two arms in MZI, which can be written as

$$\Delta\Phi_{eff}=\arctan\left(\frac{1+r^2}{1-r^2}\tan\frac{\Phi_1}{2}\right)-\arctan\left(\frac{1+r^2}{1-r^2}\tan\frac{\Phi_2}{2}\right). \tag{2}$$

r is the coupling coefficient of OC3 and OC4. Φ_1 and Φ_2 are the single-trip phase shifts of the signal in lower arms and upper arms respectively, which are

$$\Phi_1=\Phi_0+6\pi n_2 l_2 P_1/\lambda A_{eff}+4\pi n_2 l_2 P_0/\lambda A_{eff}, \tag{3}$$

$$\Phi_2=\Phi_0+6\pi n_2 l_2 P_1/\lambda A_{eff}, \tag{4}$$

where Φ_0 is the linear phase shift of the signal in the ring resonator. λ is the wavelength of the CW lights. l_2, n_2, A_{eff} are the length, the nonlinear coefficient and the effective area of nonlinear effect of the HNLF in ring resonator respectively. P_0 and P_1 are the peak power of the control pulse and the power of CW light, respectively. From the Eqs. (3) and (4), we can see that the total phase difference of the optical signals between two arms is mainly caused by the peak power P_0 of the control pulse. By changing P_0 and selecting the appropriate linear phase shift Φ_0 and the coupling coefficient r, the total phase difference $\Delta\Phi_{eff}$ will jump between "0" and "π". Then the transmissivity T will change between "0" and "1".

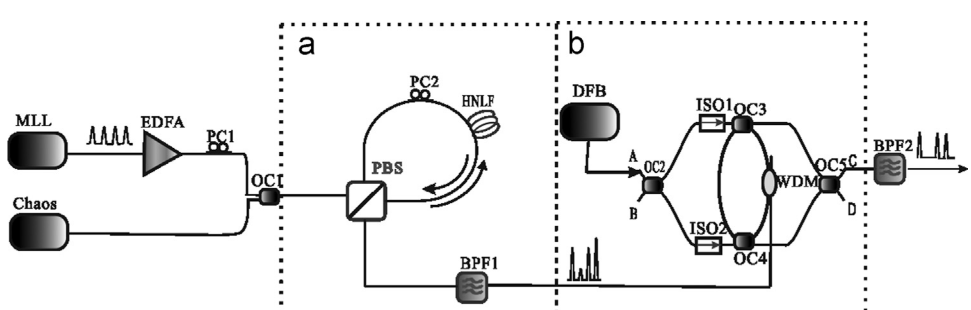

Fig. 1. Schematic diagram of the proposed all-optical RNG: (a) all-optical sampler; (b) all-optical comparator. MLL: mode-locked laser; CHAOS: chaos source; EDFA: erbium-doped optical fiber amplifier; PC: polarization controller; OC: optical coupler; PBS: polarizing beamsplitter; HNLF: highly nonlinear fiber; BPF: optical bandpass filter; DFB: distributed feedback laser; ISO: optical isolator; and WDM: wavelength division multiplexing.