2.87-Gb/s random bit generation based on bandwidth-enhanced chaotic laser

Yingying Zhang (张英英)[1], Jianzhong Zhang (张建忠)[1], Mingjiang Zhang (张明江)[1], and Yuncai Wang (王云才)[1,2*]

[1] *Institute of Optoelectronic Engineering, Department of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China*

[2] *The State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*

[*] *Corresponding author: wangyc@tyut.edu.cn*

Received September 8, 2010; accepted October 21, 2010; posted online February 24, 2011

We experimentally demonstrate a fast random bit generator (RBG) based on bandwidth-enhanced chaotic laser from an optical feedback laser diode with optical injection. The bandwidth-enhanced chaotic signal is sampled and converted to a binary sequence in real time without the need of programming for off-line processing. Multi-rate bit sequences, with the fastest rate of up to 2.87 Gb/s, are obtained with verified randomness.

OCIS codes: 140.5960, 190.3100.
doi: 10.3788/COL201109.031404.

Random numbers are commonly used in fields such as cryptography, secure communication, testing of complex communication, and Monte-Carlo simulation. A pseudo-random number generator (PRNG) expands short seeds into long bit sequences using deterministic algorithms. Given partial knowledge of the initial state, a potential attacker can carry out useful prediction about the generator's output[1]. Thus, this may pose serious problems in security application. Physical random number generator (RNG) is based on physical processes, such as electrical noise[2], chaotic circuit[3], and quantum mechanical properties of photons[4]. They can produce high-quality random numbers, but limited at much lower rate than PRNG because of the narrow bandwidth of these physical entropy sources.

In recent years, the chaotic laser has become an increasingly attractive physical source for high-speed random number generation[5−9] due to its complicated nonlinear dynamics[10−12] and wide bandwidth. Great progress in improving the rate of generation has been made. In 2008, Uchida *et al.* experimentally demonstrated a fast 1.7-Gb/s RNG, based on chaotic laser with optical feedback, by directly sampling the output of two chaotic lasers with one-bit analog-digital converter (ADC) in real time[6]. Recently, using a single chaotic laser and off-line processing method, Reidler *et al.* constructed higher rate random sequences by extracting and combing multi-bits from an 8-bit ADC[7,8]. Very recently, Hirano *et al.* demonstrated another fast RNG, based on the bandwidth-enhanced chaos, by also multi-sampling in off-line processing of experimental chaotic laser time series[9]. In this letter, we successfully demonstrate that random bit sequence with a rate of up to 2.87 Gb/s can be generated in real time using a 16.8-GHz wide bandwidth chaotic laser.

In our experiment, we employed a bandwidth-enhanced chaotic laser as the random entropy source to ensure the higher rate of our random bit generator (RBG). We have experimentally demonstrated the enhancement of bandwidth using the structure shown in Fig. 1. The bandwidth of a slave laser diode (SLD) with optical feedback can be enhanced by external optical injection technique from 6.2 to 16.8 GHz[13]. The feedback strength and polarization state of the feedback light are adjusted by a variable optical attenuator (VOA) and a polarization controller (PC), respectively. The length of the feedback cavity can be adjusted by adding fiber jumpers into the fiber ring. External optical injection is provided by an injection laser through a 30/70 optical fiber coupler. The optical power and polarization state of the injection light are controlled by an erbium-doped fiber amplifier (EDFA) and a PC, respectively. An optical isolator (OI) is used to prevent unwanted optical feedback into the injection laser. A spectrum analyzer (Agilent E4407B) with a 47-GHz bandwidth photodetector (PD) (u2t XPDV2020) and a digital oscilloscope (Wave Master 8600A) are used to measure the power spectrum and waveform of the light emission from the chaotic laser.

The SLD and the injecting laser diode (LD) were biased at 1.3 times their threshold currents (22 mA). The powers of the feedback light and the injection light were set at −7.7 and −5.6 dBm at 8.8-GHz frequency detuning, respectively. Figure 2 illustrates the experimentally obtained spectra of the original state of the chaotic laser without optical injection and the bandwidth-enhanced chaotic signal with 16.8-GHz bandwidth. The bandwidth of chaotic signals was defined as the frequency band starting at zero frequency and containing 80% spectrum power.

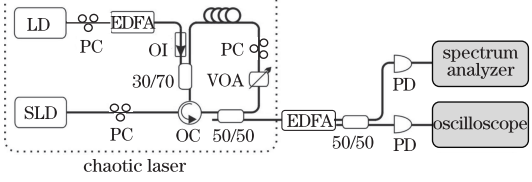

Fig. 1. Structure of a bandwidth-enhanced chaotic laser source. OC: optical circulator.

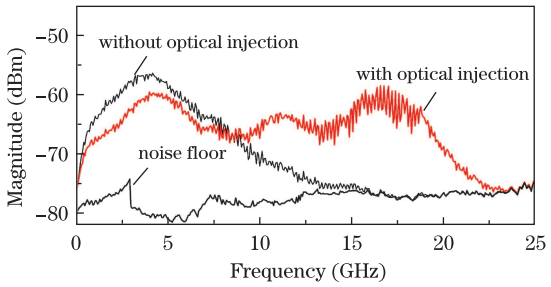

Fig. 2. Spectra of the original chaotic laser without optical injection and the bandwidth-enhanced chaotic laser.

Figure 3 is the experimental setup of our RBG. The two independent bandwidth-enhanced chaotic lasers are utilized as uncorrelated random entropy sources. The length of the feedback cavity in the first bandwidth-enhanced chaotic laser source is 6 m, while that in the second one is 10 m to ensure that the two chaotic entropy sources are independent of each other. Each laser output is detected and amplified by a PD (Newport, AD-50APDir). The amplified electrical signal is coupled to an alternating current (AC) coupled by a direct current (DC)-blocking capacitor and is converted into a sequence of binary codes with a comparator (Comp, AD-CMP582). It is then sampled at the rising edge of clock (AD9516-1) using a D flip-flop (DFF) (MC10EP52) to reshape the code width. Figure 4 is the schematic drawing of random bit extraction from the chaotic signal. The outputs of chaotic laser 1, Comp 1, the clock, and the corresponding DFF1 are shown in Fig. 4. The bit rate of the random sequence is determined by the clock frequency. Finally, the binary sequences obtained from the two bandwidth-enhanced chaotic lasers are combined using Boolean exclusive-OR (XOR, MC10EP08) operation to improve the randomness. The output random

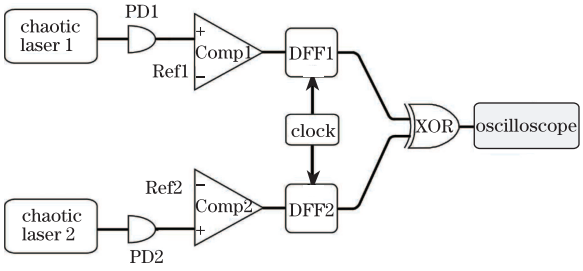

Fig. 3. Experimental setup of RBG.

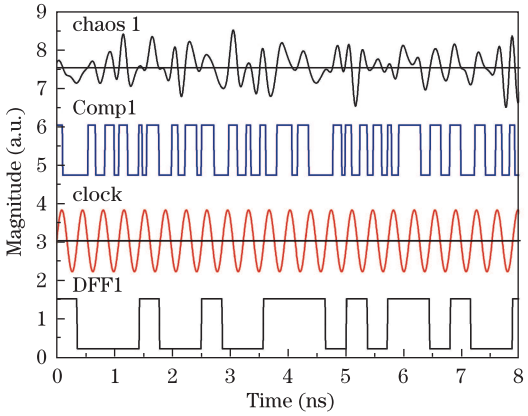

Fig. 4. Random bit extraction from chaotic signal.

sequence is observed and recorded by an oscilloscope with a 6-GHz bandwidth and a 20-Gs/s sampling rate (Wave Master 8600A).

In our experiment, the clock module consists of several clock dividers and an integrated voltage-controlled oscillator (VCO). It can generate multi-frequency clock signals, including 120, 240, and 360 MHz, with the maximum clock frequency reaching 2.87 GHz. Thus, our RBG obtained multi-rate random bit sequences output. Figures 5(a) and (b) show the two examples of temporal waveforms for random bit sequences at 1.44 and 2.87 Gb/s, respectively, in which the minimum code widths correspond to the clock periods Tclk1 and Tclk2. The single code element is not precisely square when the bit rate is up to 2.87 Gb/s, as shown in Fig. 5(b), due to the limitation of the bandwidth of oscilloscope. All bit sequences obtained were subjected to full National Institute of Standards and Technology (NIST) test suite[14] to evaluate the randomness. Table 1 summarizes the typical test results of a 2.87-Gb/s random bit sequence.

In conclusion, a 2.87-Gb/s physical RBG is realized based on the hardware using a bandwidth-enhanced chaotic laser. The entropy source of chaotic laser with a

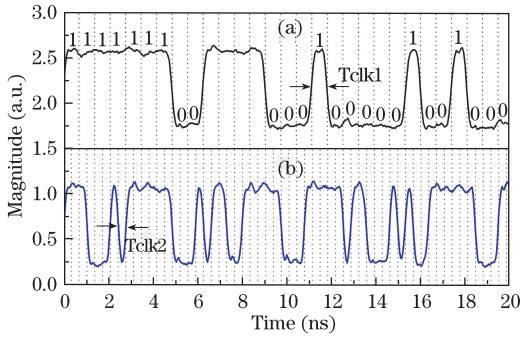

Fig. 5. Temporal waveforms of (a) 1.44 and (b) 2.87 Gb/s random bit sequences.

Table 1. Typical Test Results of 2.87-Gb/s Random Bit Sequence

Statistical Test	*P*-Value	Proportion	Result
Approximate Entropy	0.073575	0.9965	Success
Block Frequency	0.232848	0.9926	Success
Cumulative Sums	0.247667	0.9930	Success
Frequency	0.477675	0.9978	Success
Linear Complexity	0.561787	0.9986	Success
Longest Run	0.142305	0.9926	Success
Non-overlapping Template	0.660056	0.9916	Success
Overlapping Template	0.195624	0.9879	Success
Random Excursions	0.511817	0.9935	Success
Random Excursions Variant	0.321617	0.9916	Success
Rank	0.470231	0.9929	Success
Runs	0.390257	0.9961	Success
Serial	0.096153	0.9910	Success
Universal	0.365625	0.9951	Success

For "success", we used 1000 samples of 1-Mb data and significance level of α=0.01. Each *P*-value (uniformity of *p*-values) should be larger than 0.0001, and the proportion (of sequences passing a test in 1000 sequences) should be within the range of 0.99±0.0094392.

bandwidth of 16.8 GHz could guarantee high-speed random bits with good randomness. Multi-rate random bit sequences obtained from this generator pass statistical tests.

This work was supported by the Special Fund for Basic Research on Scientific Instruments of the National Natural Science Foundation of China (No. 60927007) and the State Key Laboratory of Quantum Optics and Quantum Optics Devices of China (No. 200903).

References

1. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, FL, 2001).
2. C. S. Pertie and J. A. Connelly, IEEE Trans. Circuits. Syst. I **47,** 615 (2000).
3. G. M. Bernstein and M. A. Lieberman, IEEE Trans. Circuits Syst. **37,** 1157 (1990).
4. T. Jennewein, U. Achleitnert, G. Weihs, H. Weinfurtert, and A. Zeilinger, Rev. Sci. Instrum. **71,** 1675 (2009).
5. Y. C. Wang, J. H. Tang, and M. J. Zhang, "True random code generator based on chaotic laser and its producing random code method" (in Chinese) Chinese Patent ZL200710062140.1 (2007).
6. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, and M. Shiki, Nature Photon. **2,** 728 (2008).
7. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103,** 024102 (2009).
8. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nature Photon. **4,** 58 (2010).
9. K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, Opt. Express **18,** 5512 (2010).
10. H. Kong, Z. Wu, J. Wu, X. Lin, Y. Xie, and G. Xia, Chinese J. Lasers (in Chinese) **33,** 1490 (2006).
11. L. Cao, T. Deng, X. Lin, J. Wu, G. Xia, and Z. Wu, Chinese J. Lasers (in Chinese) **37,** 939 (2010).
12. Y. L. Fan and J. M. Liu, IEEE J. Quantum Electron. **39,** 562 (2003).
13. A. Wang, Y. Wang, and H. He, IEEE Photon. Technol. Lett. **20,** 1633 (2008).
14. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications" National Institute of Standards and Technology, Special Publication(revision)800-22 (2008).