Optics Letters

# Modulation instability in a highly nonlinear fiber for discrete-time pulsed random bit generation

Xie Wang,[1,†] Xiao-Zhou Li,[2,†] Sze-Chun Chan,[2,3] and Kenneth K. Y. Wong[1,*]

[1]Department of Electrical and Electronic Engineering, The University of Hong Kong, Pokfulam Road, Hong Kong, China
[2]Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[3]State Key Laboratory of Millimeter Waves, City University of Hong Kong, Hong Kong, China
*Corresponding author: kywong@eee.hku.hk

Received 24 March 2015; revised 17 May 2015; accepted 18 May 2015; posted 18 May 2015 (Doc. ID 236769); published 1 June 2015

**A simple yet high-speed scheme by utilizing modulation instability (MI) on the discrete-time generation of random bits is proposed and demonstrated experimentally. We develop MI pulses by pumping a highly nonlinear fiber in the anomalous dispersion regime using a mode-locked laser. MI pulses contain fluctuating pulse-to-pulse variations of peak intensities for extraction into random bits. At a repetition rate of 10 GHz, 5 bits are extracted from each pulse in generating random bits at 50 Gbps, as verified by the National Institute of Standards and Technology test suite.** 

***OCIS codes:*** (190.4410) Nonlinear optics, parametric processes; (190.4380) Nonlinear optics, four-wave mixing; (190.3100) Instabilities and chaos.

http://dx.doi.org/10.1364/OL.40.002665

Random bit generations (RBGs) have been implemented by a number of photonic approaches [1–14]. The broad bandwidths of optoelectronic devices enabled the high-speed generation of random bits with potential applications in encryption and computation [1]. RBG was investigated by using the nonlinear dynamics in different semiconductor lasers subject to various perturbations, which yield chaotic waveforms for extracting the entropies in laser noise for digitization into random bits [1–5]. RBG was also implemented by directly digitizing the inherent noisy fluctuations in gain media, light sources, or even vacuum [8–10]. However, these approaches rely on optical signals that vary continuously in time [4,5]. The discrete timing of the output bits requires high-frequency external clocks in the sampling electronics.

By contrast, optical pulses with random amplitudes at fixed repetition rates can also realize RBG where external clocks are no longer necessary. Discrete-time pulsed RBGs have been realized using modulated electrical pumping on devices such as single-mode laser diodes and semiconductor ring lasers, where the intracavity fluctuations are manifested as laser phase noise and mode partition noise, respectively [13,14]. Modulated electrical pumping allows pulsed RBG at repetition rates only up to a few gigahertzes, as limited by the parasitic and intrinsic electronic response times in the semiconductor devices. Recently, RBG from the noisy evolution of supercontinuum (SC) pulses in optical fibers was reported based on numerical simulations [15]. The approach relied on optically pumping a fiber instead of electrically pumping a semiconductor. The fast responses of optical nonlinearities, such as Kerr nonlinearity, can potentially realize pulsed RBG at high repetition rates [15,16]. However, experiments on discrete-time pulsed RBG using fiber nonlinearities have yet to be demonstrated, although very recently Birkholz *et al.* investigated the temporal correlation in a modulation instability (MI)-based process [17].

Here, it is noted that when pumping by continuous-wave or long pulses in the anomalous dispersion regime, the development of SC begins with MI, which also plays an important role in other interesting phenomena such as optical rogue wave formation and wide-band parametric amplification [18–20]. MI spontaneously grows from noise and is known to contribute to SC fluctuations, so MI can potentially provide pulse-to-pulse randomness for extraction into RBG. Also, MI can be easily achieved in the regime of long-pulse pumping [18,21], as long as the nonlinear phase mismatch experienced by the optical wave is compensated by the linear one.

In this Letter, pulsed RBG is experimentally demonstrated using MI. Mode-locked pulses pump a highly nonlinear fiber (HNLF) to generate MI pulses at a fixed repetition rate. We then obtain the anti-Stokes MI pulses by filtering the anti-Stokes sidelobe of the MI. The fluctuating peak intensities of the anti-Stokes MI pulses are electronically digitized into bits, which are verified as random by the test suite of the National Institute of Standards and Technology (NIST). With a pump repetition rate of 10 GHz, each anti-Stokes MI pulse gives 5 bits from an analog-to-digital converter (ADC), resulting in a total output rate of 50 Gbps for the pulsed RBG.

Figure 1 shows the experimental schematic for the pulsed RBG based on MI. A mode-locked laser diode (MLLD) (Alnair MLLD-100) at a repetition rate of 10 GHz emits optical pulses with a center wavelength of 1560 nm. The pulses are amplified by erbium-doped fiber amplifiers EDFA1 and EDFA2, where an optical bandpass filter OBPF1 centered at 1560 nm with a 1.5 nm bandwidth is inserted between the

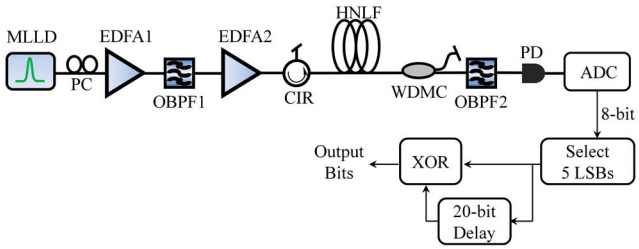


**Fig. 1.** Schematic of the experiment for pulsed RBG using a HNLF. MLLD, mode-locked laser diode; PC, polarization controller; EDFA, erbium-doped fiber amplifier; OBPF, optical bandpass filter; CIR, circulator; WDMC, wavelength-division multiplexing coupler; PD, photodetector; ADC, analog-to-digital converter; LSB, least significant bit; XOR, exclusive-OR.

erbium-doped fiber amplifiers (EDFAs) to suppress the amplified spontaneous emission noise. Through a circulator to prevent back-reflection, the pulses optically pump a HNLF. The state of polarization of the pump pulses is aligned by a polarization controller to a neutral axis of the HNLF. The HNLF has a length of 150 m and a nonlinear coefficient of 30 $W^{-1}$ $km^{-1}$. It is a dispersion-shifted fiber with a zero-dispersion wavelength of 1554 nm, where the dispersion slope is 0.02 $ps/nm^2/km$ and $\beta^{(4)}$ is $5.0 \times 10^{-5}$ $ps^4/km$. When pumped by the mode-locked pulses at an average power of 22 dBm with a pulse width of 8.8 ps, the HNLF generates MI sidebands. The output from the HNLF is sent to a wavelength-division multiplexing coupler (WDMC) that functions as a bandstop filter at the pump wavelength of 1560 nm, for preventing the high-power pump from damaging the equipment. Then an optical bandpass filter OBPF2 with a bandwidth of 18 nm filters out the part of the MI spectrum between 1516 and 1534 nm with an outband suppression ratio of 45 dB. The filtered MI output pulses are then converted into an electrical signal using a 15 GHz photodetector (PD) (HP 11982A) and digitized by an 8-bit ADC in a real-time oscilloscope (Agilent DSOX91604A). The final output bits are then extracted through selecting 5 least significant bits (LSBs) per pulse and a 20-bit delayed exclusive-OR (XOR) comparison, which are commonly adopted in RBG [2].

Figure 2(a) shows the optical spectrum of the HNLF output measured immediately before the WDMC. The resolution bandwidth is set at 0.05 nm. The spectrum consists of the pump at 1560 nm, which is spectrally broadened by several nanometers due to self-phase modulation. The spectrum also contains a pair of distinct MI sidebands where the Stokes and anti-Stokes components are centered at 1593 and 1525 nm, respectively. The Stokes sideband is relatively stronger due to enhancement by Raman scattering [21]. The gray region indicates the window within the anti-Stokes sideband that is filtered by OBPF2 for detection by the PD and ADC in Fig. 1.

Figure 2(b) shows the intensity time series of the filtered anti-Stokes MI pulses as recorded by the ADC. The optical MI pulses have shorter pulse widths compared with the pump [22], although the electronically measured time series shows broader pulse widths as limited by the 15 GHz bandwidth of the PD. The pulses are regularly separated in time because of the fixed pump repetition rate of 10 GHz. Although the ADC records the time series at a sampling rate of 80 GHz in Fig. 2(b), only the peak value of each output pulse is used for further extraction of random bits. The red dots in Fig. 2(b) mark the peak values of the MI pulses. Their temporal separation is fixed at 100 ps, whereas their amplitude clearly fluctuates from pulse to pulse as each shot of MI is developed from nondeterministic noise.

To visualize the fluctuation of the MI peak intensities, their statistical normalized occurrences are plotted in Fig. 3(a) based on 1 million samples. The peak intensities are collected over a period of 0.1 ms with an 8 bit digitization resolution. The distribution is nearly symmetrical around the mean value. It is nearly Gaussian with a best fit shown by the red curve in Fig. 3(a). Similar distributions have also been reported for different spectral ranges in SC generation [22]. A uniform distribution in RBG is attained by the steps in Fig. 1. For every pulse, only 5 LSBs are selected from the 8-bit value of the peak intensity. So the selected bits correspond to one of the 32 ordered digitization values in Fig. 3(b), which again plots the occurrences. The normalized occurrences of the digitization values using 5 LSBs are plotted in Fig. 3(b), as compared with using all 8 bits in Fig. 3(a). By selecting the LSBs, the Gaussian distribution in Fig. 3(a) is scrambled to approach the uniform distribution as in Fig. 3(b) [4,7].

To investigate the randomness of the MI peak intensities, Fig. 4(a) shows the autocorrelation of the peak intensity values as marked by the red dots in Fig. 2(b). The autocorrelation is calculated from 1 million samples. In Fig. 4(a), all 8 bits per sample are used in evaluating the autocorrelation function. Each MI pulse is developed from noise independently. So the measured autocorrelation function diminishes rapidly from unity as the delay time increases from 0. However, for the inset zoomed into the region near zero delay, some residual nonzero autocorrelations are observed. They are

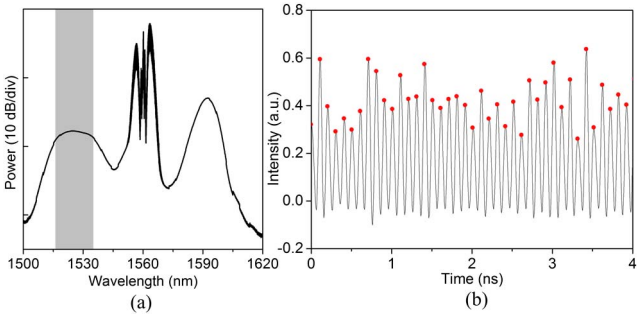


**Fig. 2.** (a) Optical spectrum from the HNLF measured immediately before the WDMC. The gray region indicates the passband of OBPF2. (b) Intensity time series at the output of the PD. The red dots mark the fluctuating peak intensity of each pulse.

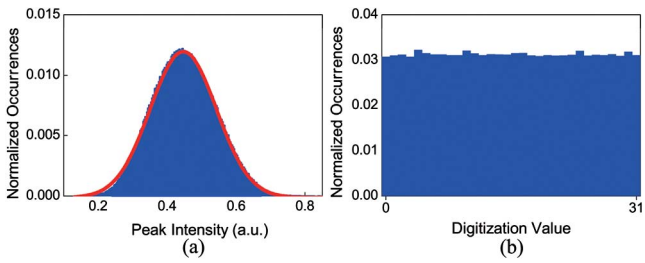


**Fig. 3.** Normalized occurrences of the digitized values represented by (a) all 8 bits and (b) only 5 LSBs of the peak intensities.

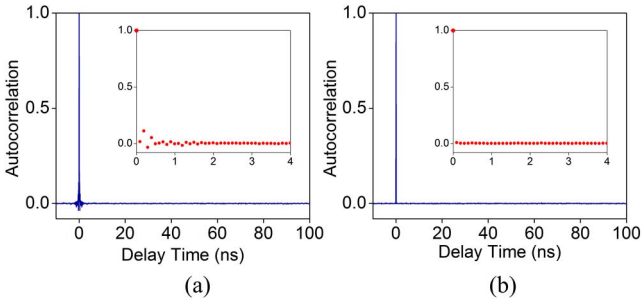


**Fig. 4.** Autocorrelation functions of the digitized values represented by (a) all 8 bits and (b) only 5 LSBs of the peak intensities. The insets are zoomed into the regions near zero delay to reveal the discrete data points as solid circles.

attributed to the limited electronic bandwidth of the PD, which causes cross talks between neighboring electrical pulses. In Fig. 4(b), only 5 LSBs are used per sample, resulting in an autocorrelation that vanishes at all nonzero delays. Even the zoomed inset in Fig. 4(b) does not show any autocorrelation, since the selection of LSBs is a nonlinear operation that narrows the autocorrelation function [4,5]. According to Figs. 3(b) and 4(b), the selected bits of the MI peak intensities are independent and uniform.

The randomness of the final output bits, through the delayed bitwise XOR operation in Fig. 1, are verified by performing the NIST Special Publication 800-22 statistical tests. The final output bits are generated at a rate of 50 Gbps when pumped at 10 GHz. Using a total of 1000 sequences of 1 million bits, Table 1 summarizes the results that pass all the tests at a significance level of 0.01, where the worst case is shown for tests with multiple *P*-values and proportions [6]. The output bits of the pulsed RBG using MI are verified as random.

Thus far, only the anti-Stokes sideband is utilized for RBG, but the Stokes sideband can also be utilized. The intensities of the anti-Stokes and Stokes pulses from the same pump pulse are correlated because of energy conservation [21]. With the 8-bit digitization by the ADC, it is experimentally verified that the anti-Stokes and Stokes pulses contain mutual information. Hence, utilizing both MI sidebands, correlated random bits can be generated from the two sidebands. With the observation of multiband spectral details of MI [21,23], more bits can potentially be extracted by using advanced fibers such as dispersion oscillating fibers.

**Table 1. NIST Test Results for the Pulsed RBG**

| Statistical Test | *P*-Value | Proportion | Result |
|---|---|---|---|
| Frequency | 0.920383 | 0.9910 | Success |
| Block frequency | 0.558502 | 0.9820 | Success |
| Cumulative sums | 0.267573 | 0.9900 | Success |
| Runs | 0.140453 | 0.9940 | Success |
| Longest run | 0.293952 | 0.9830 | Success |
| Rank | 0.880145 | 0.9890 | Success |
| Fast Fourier transform (FFT) | 0.228367 | 0.9810 | Success |
| Non-overlapping templates | 0.005557 | 0.9820 | Success |
| Overlapping templates | 0.320607 | 0.9890 | Success |
| Universal | 0.927677 | 0.9900 | Success |
| Approximate entropy | 0.899171 | 0.9900 | Success |
| Random excursions | 0.037157 | 0.9835 | Success |
| Random excursion variant | 0.128379 | 0.9818 | Success |
| Serial | 0.375313 | 0.9820 | Success |
| Linear complexity | 0.410055 | 0.9910 | Success |
| Total | 15 | | |

In summary, MI in a HNLF has been experimentally investigated for pulsed RBG. The pulse-to-pulse fluctuations of the peak intensities are digitized into random bits. At a repetition rate of 10 GHz, RBG at 50 Gbps is demonstrated using the anti-Stokes sideband, illustrating experimental pulsed RBG at discrete times through fiber nonlinearities.

†These authors contributed equally to this work.

ITF (ITS/189/13); National Natural Science Foundation of China (NSFC) (Grant 61308002); Research Grants Council of the Hong Kong Special Administrative Region, China (CityU 111213, HKU 17208414, HKU 717212E); University Development Fund of HKU.

## REFERENCES

1. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nat. Photonics **2**, 728 (2008).
2. R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, Opt. Express **23**, 1470 (2015).
3. M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, Opt. Express **22**, 17271 (2014).
4. N. Oliver, M. Soriano, D. Sukow, and I. Fischer, IEEE J. Quantum Electron. **49**, 910 (2013).
5. X. Z. Li and S. C. Chan, Opt. Lett. **37**, 2163 (2012).
6. X. Z. Li and S. C. Chan, IEEE J. Quantum Electron. **49**, 829 (2013).
7. X. Fang, B. Wetzel, J. M. Merolla, J. M. Dudley, L. Larger, C. Guyeux, and J. M. Bahi, IEEE Trans. Cir. Syst. I **61**, 888 (2014).
8. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).
9. H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).
10. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).
11. M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H. J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).
12. P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, Opt. Express **19**, 25173 (2011).
13. C. Abellan, W. Amaya, M. Jofre, M. Curty, A. Acin, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express **22**, 1645 (2014).
14. S. Sunada, T. Harayama, K. Arai, K. Yoshimura, K. Tsuzuki, A. Uchida, and P. Davis, Opt. Express **19**, 7439 (2011).
15. B. Wetzel, K. J. Blow, S. K. Turitsyn, G. Millot, L. Larger, and J. M. Dudley, Opt. Express **20**, 11143 (2012).
16. M. Sciamanna and K. A. Shore, Nat. Photonics **9**, 151 (2015).
17. S. Birkholz, C. Bree, A. Demircan, and G. Steinmeyer, "On the predictability of rogue events," http://www.arxiv.org/abs/1503.00706.
18. V. E. Zakharov and L. A. Ostrovsky, Phys. Nonlinear Phenom. **238**, 540 (2009).
19. J. M. Dudley, G. Genty, F. Dias, B. Kibler, and N. Akhmediev, Opt. Express **17**, 21497 (2009).
20. D. R. Solli, C. Ropers, P. Koonath, and B. Jalali, Nature **450**, 1054 (2007).
21. X. Wang, D. Bigoud, A. Kudlinski, K. K. Y. Wong, M. Douay, L. Bigot, A. Lerouge, Y. Quiquempois, and A. Mussot, Opt. Lett. **39**, 1181 (2014).
22. D. R. Solli, C. Ropers, and B. Jalali, Nonlinearity **26**, R85 (2013).
23. M. Droques, A. Kudlinski, G. Bouwmans, G. Martinelli, and A. Mussot, Opt. Lett. **37**, 4832 (2012).