Optics Letters

Random bit generation at tunable rates using a chaotic semiconductor laser under distributed feedback

Xiao-Zhou Li,[1] Song-Sui Li,[1] Jun-Ping Zhuang,[1] and Sze-Chun Chan[1,2,*]

[1]Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[2]State Key Laboratory of Millimeter Waves, City University of Hong Kong, Hong Kong, China
*Corresponding author: scchan@cityu.edu.hk

Received 7 July 2015; revised 30 July 2015; accepted 30 July 2015; posted 30 July 2015 (Doc. ID 245485); published 19 August 2015

A semiconductor laser with distributed feedback from a fiber Bragg grating (FBG) is investigated for random bit generation (RBG). The feedback perturbs the laser to emit chaotically with the intensity being sampled periodically. The samples are then converted into random bits by a simple postprocessing of self-differencing and selecting bits. Unlike a conventional mirror that provides localized feedback, the FBG provides distributed feedback which effectively suppresses the information of the round-trip feedback delay time. Randomness is ensured even when the sampling period is commensurate with the feedback delay between the laser and the grating. Consequently, in RBG, the FBG feedback enables continuous tuning of the output bit rate, reduces the minimum sampling period, and increases the number of bits selected per sample. RBG is experimentally investigated at a sampling period continuously tunable from over 16 ns down to 50 ps, while the feedback delay is fixed at 7.7 ns. By selecting 5 least-significant bits per sample, output bit rates from 0.3 to 100 Gbps are achieved with randomness examined by the National Institute of Standards and Technology test suite.

OCIS codes: (140.5960) Semiconductor lasers; (140.1540) Chaos; (190.3100) Instabilities and chaos.

http://dx.doi.org/10.1364/OL.40.003970

Fast random bit generation (RBG) is vital to applications such as data encryption, computational experiments, and secure communication [1–3]. RBG at high bit rates is enabled by broadband photonic devices based on physical processes including spontaneous emission [4], vacuum fluctuations [5], photon detection [6], and chaotic dynamics [1,2,7–16]. In particular, influenced by noise in the photonic devices, chaotic dynamics provides entropies through mixing nearby state space trajectories. The chaotic photonic devices emit intensity time series that can be readily digitized by electronics for postprocessing into random bits. Such chaos-based RBG has been investigated in various schemes using opto-electronic oscillators [10], vertical-cavity surface-emitting lasers [16], and single-mode semiconductor lasers perturbed through combinations of optical injection and feedback [1,2,14].

One of the simplest schemes of chaos-based photonic RBG adopts a mirror for providing feedback into a semiconductor laser. The scheme is simple in requiring only one ordinary single-mode semiconductor laser with a conventional mirror [1]. It can be miniaturized using photonic integrated-circuit technologies [7,17]. It also supports broadband and high-dimensional chaos [18,19]. The laser with properly adjusted feedback emits a chaotic intensity time series, which can be sampled at a period of τ_s for postprocessing into output bits. However, as the feedback is delayed by a round-trip time τ_{RT}, the chaotic intensity time series often contains undesirable relation with its replica lagging at τ_{RT}. The residual magnitude peak of the intensity autocorrelation function at τ_{RT} is called the time-delay signature (TDS) [20–24]. The TDS degrades the randomness of the output bits in RBG especially when the sampling period τ_s and the feedback delay time τ_{RT} are commensurate [8,11,15]. So the sampling period τ_s cannot be continuously varied once τ_{RT} is fixed by the experimental setting. As a result, the TDS detrimentally prohibits a continuous tuning of the output bit rate in RBG, while the tunability is important for applications such as secure communication [7,8,25]. Recently, several approaches to suppressing the TDS have been reported based on optimizing the feedback strength at a relatively short delay [20], dual-path feedback with two carefully positioned mirrors [26], mutual feedback with multiple lasers [27], phase-modulated feedback with external modulators [28], as well as electrical heterodyning [29]. An alternative employing feedback from a fiber Bragg grating (FBG) has also been reported [24], though the effect of TDS suppression on RBG is yet to be investigated.

In this Letter, we experimentally investigate RBG with a continuously tunable output bit rate using a semiconductor laser subject to feedback from an FBG. By contrast to a mirror for localized feedback, the FBG provides distributed feedback, which effectively suppresses the TDS in the autocorrelation function. We report here that, due to TDS suppression, FBG feedback enables RBG with a continuously tunable τ_s, where randomness is maintained even when τ_s and τ_{RT} are commensurate. Moreover, FBG feedback reduces the minimum sampling period τ_s while keeping a low residual autocorrelation as required by RBG. Furthermore, FBG feedback increases the maximum number of least significant bits (LSBs) selected for RBG. Experimentally, the feedback round-trip delay time between the laser and the FBG is kept fixed at $\tau_{\mathrm{RT}} = 7.7$ ns. The laser emits a chaotic intensity time series that is self-differenced, sampled, and digitized at an 8-bit differential analogue-to-digital converter (ADC). The sampling period τ_s is tuned from above 16 ns down to 50 ps, where 5 LSBs are selected for each sample. Overall, our experimental results show a continuous tuning of the RBG output bit rate from 0.3 to 100 Gbps, for which randomness is verified by the standard tests of the National Institute of Standards and Technology (NIST).

Figure 1 shows the proposed setup for RBG with a tunable sampling period τ_s. A distributed-feedback semiconductor laser (Mitsubishi ML920T43S-01) with a threshold of 7 mA is biased at 10 mA to emit at an optical power of 1.1 mW when free-running. The emission wavelength is 1548 nm for the laser at 15.50°C by temperature-stabilization, in which the precision corresponds to limiting the free-running optical frequency fluctuation to less than 1 GHz. The relaxation resonance frequency of the laser is 3.6 GHz. The laser emission is partially transmitted through a beamsplitter and then coupled into a single-mode fiber, which is aligned to collect about 10% of the laser emission power. The fiber has a section of FBG formed by periodic corrugations distributed across a physical length of 15 mm. The grating reflectivity spectrum has a full width at half-maximum (FWHM) bandwidth of 22 GHz with a peak reflectivity exceeding 90%. The Bragg frequency of the grating is positively detuned by 7 GHz above the free-running optical frequency of the laser. Measured between the laser and the front-end of the FBG, the round-trip feedback delay time τ_{RT} is about 7.7 ns, which is equivalent to 1.16 m of free space. The distributed reflection from the FBG returns to the laser for inducing chaos. The feedback delay time is significantly longer than the reciprocal of the relaxation resonance frequency, thereby enabling generation of relatively flat chaotic spectra [7]. The chaotic emission of the laser is partially reflected by the beamsplitter, through collection using a fiber tip of angled physical contact (APC), into a combination of an erbium-doped fiber amplifier (Amonics AEDFA-23-B-FA), a photodetector (Newport AD-10ir), and then a microwave amplifier (HP 83006A), which collectively serve as an optical-to-electrical converter (O/E) in Fig. 1. Thus, the O/E gives an electrical signal $I(t)$ that is directly proportional to the chaotic emission intensity of the laser.

The signal is then fed to a differential analogue-to-digital converter (ADC) through two electrical paths, where there is a long delay of 40 ns between the two paths. Thus, the intensity signal $I(t)$ and its delayed replica are subtracted at the ADC to yield $D(t)$. The self-differencing is commonly employed for symmetrization of the statistical distribution of the signal as far as the delay is sufficiently long to eliminate the relation between the two inputs at any time instance [11,16]. The ADC is implemented in an oscilloscope (Agilent 81304B) with a sampling period τ_s, which is tunable from over 16 ns down to a minimum of 50 ps. While the ADC has a resolution of 8 bits, only the 5 LSBs are retained to ensure randomness. The output $R(t)$ is a 5-bit random value at each sampled time instance. As a result, RBG is realized by the schematic in Fig. 1 at an output bit rate ranging from 0.3 up to 100 Gbps.

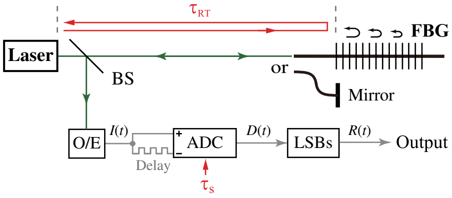

Fig. 1. Schematic of RBG using a semiconductor laser subject to distributed feedback from an FBG. BS, beamsplitter; O/E, optical-to-electrical converter; ADC, analogue-to-digital converter.

Additionally, for comparison, RBG is also investigated by replacing the FBG in Fig. 1 with a fiber-pigtailed mirror. Such a scheme of mirror feedback for inducing chaos has been commonly used for RBG [1,11,15]. The round-trip time between the laser and the mirror is kept nearly unchanged at $\tau_{\mathrm{RT}} = 7.7$ ns, whereas the mirror also has a reflectivity of over 90%. However, the localized reflection of the mirror corresponds to a strong residual autocorrelation at lag time τ_{RT} as the TDS, which degrades the randomness of the output bits when τ_s is commensurate with τ_{RT}. By contrast, the distributed reflection of the FBG corresponds to nearly eliminating the residual autocorrelation, so the output bits remain random even when τ_s and τ_{RT} are commensurate. The performances of FBG feedback and mirror feedback are directly compared in Figs. 2–5. The experimental results are shown in black and blue for FBG feedback and mirror feedback, respectively.

Figures 2(a) and 2(b), respectively, show the chaotic emission intensity I and the corresponding output signal R for RBG, as labeled in Fig. 1. In Fig. 2(a-i), the intensity time series $I(t)$ are shown. The intensity varies chaotically when the laser is under either FBG or mirror feedback. The time series are in practice recorded by setting the inverted input of the ADC to zero.

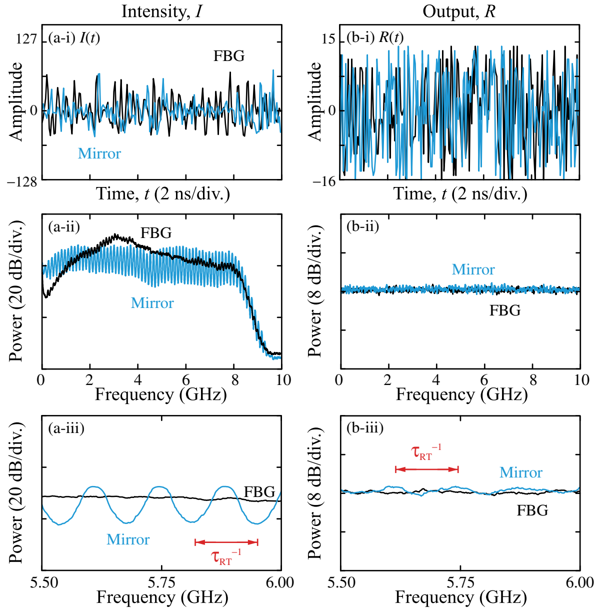

Fig. 2. (a) Intensity I and (b) output R recorded as (i) time series, (ii) power spectrum in full span, and (iii) power spectrum in a 500-MHz span. Black and blue curves are obtained by FBG feedback and mirror feedback, respectively.

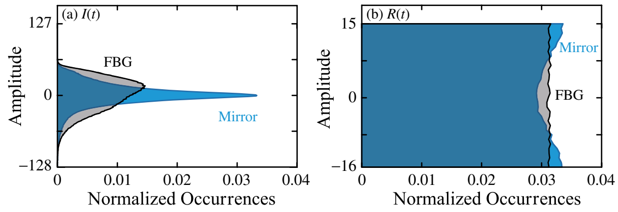

Fig. 3. Normalized occurrences of the digitized amplitude values of (a) intensity $I(t)$ and (b) output $R(t)$.

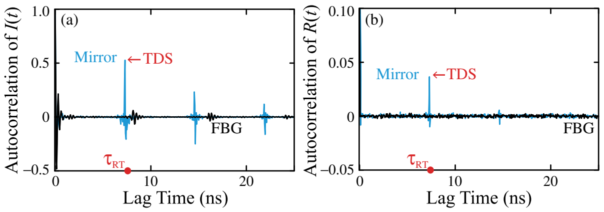

Fig. 4. Autocorrelation functions of (a) intensity $I(t)$ and (b) output $R(t)$.

The minimal sampling period of 50 ps is adopted, which corresponds to a Nyquist bandwidth of 10 GHz. The time-average of the ADC output is always kept at zero. $I(t)$ comprises of samples digitized into an 8-bit amplitude as presented by an integer value ranging from −128 to 127 in Fig. 2(a-i). In Fig. 2(a-ii), the power spectra are obtained by applying Fourier transform on $I(t)$. Though limited by the 8-GHz bandwidth of the ADC, it is clear that both FBG feedback and mirror feedback yield broadband chaotic spectra. However, for mirror feedback (blue), pronounced power variations of over 10 dB are observed across the spectrum periodically. The power spectrum presented in a reduced span in Fig. 2(a-iii) unveils the periodical variations in every 0.13 GHz, which equals τ_{RT}^{-1}. By contrast, for FBG feedback (black), the periodical variations are nearly eliminated according to both Figs. 2(a-ii) and 2(a-iii). Thus, FBG effectively suppresses the information of τ_{RT} in the power spectrum because of its distributed feedback [24].

The simple postprocessing of $I(t)$, through self-differencing and LSBs selection in Fig. 1, is adopted to yield the output $R(t)$. Time series of the samples of $R(t)$ are shown in Fig. 2(b-i) with $\tau_s = 50$ ps. Due to the selection of only the 5 LSBs, $R(t)$ has amplitudes scrambled and digitized to integers ranging from −16 to 15. The power spectra obtained by applying Fourier transform on $R(t)$ are shown in Fig. 2(b-ii). The spectra are much flattened because the process of selecting LSBs is a nonlinear operation that causes frequency mixing [10,13,14]. However, for mirror feedback (blue), the power spectrum still contains variations at the periodicity of τ_{RT}^{-1}, which are clearly observed using Fig. 2(b-iii) of a reduced span. By comparison, for FBG feedback (black), the periodical variations are much less apparent. Therefore, Fig. 2 confirms the preference of using FBG feedback over mirror feedback based on the corresponding power spectra.

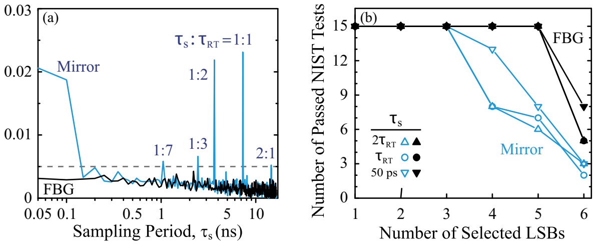

Fig. 5. (a) Residue of the autocorrelation of $R(t)$ versus sampling period τ_s. (b) Number of NIST tests passed versus the number of LSBs selected for different τ_s.

As RBG requires a uniform statistical distribution of the output bits, the statistical behaviors of the four time series in Fig. 2(i) are examined in Fig. 3. Beginning with $I(t)$, the normalized occurrences of the 256 digitized amplitudes are plotted in Fig. 3(a). The sensitivity of the ADC is set such that only 0.001% of all data points fall outside the detection window of the ADC [13]. The distribution of occurrences for FBG feedback (black) is slightly broader than that for mirror feedback (blue). The distributions are also asymmetric with respect to zero, which is consistent with previous reports on chaotic intensity statistics [9,12]. To symmetrize the distribution, $D(t)$ in Fig. 1 is yielded from $I(t)$ through a delayed self-differencing. As commonly employed in RBG, the differencing uses a delay much longer than the inverse of the signal bandwidth, ensuring independence of the ADC inputs at any instant, which leads to a symmetrical distribution upon the differencing operation [9–12]. To further flatten the distribution, only the 5 LSBs of $D(t)$ are selected to yield the output $R(t)$ in Fig. 1. The operation discards the most significant bits and effectively scrambles the amplitudes [10,14]. The normalized occurrences of the resultant 32 digitized amplitudes are plotted in Fig. 3(b). The distribution of occurrences for FBG feedback (black) approaches the ideal uniform value of 1/32, whereas the distribution for mirror feedback (blue) is much less uniform. This is due to the broader distribution of $I(t)$ for FBG feedback in Fig. 3(a).

As RBG requires absence of correlations between the output bits at different time instances, Fig. 4 examines the autocorrelation functions for the time series in Fig. 2(i), where the total time span of 50 μs is adopted for each time series. Figure 4(a) shows the autocorrelations for the intensity time series $I(t)$. With mirror feedback, the round-trip time-delay information is clearly unveiled by the autocorrelation peaks in the blue curve at the lag time of τ_{RT}. Such a TDS in the autocorrelation function has a large magnitude of 0.53 [20]. The TDS corresponds to the periodicity of τ_{RT}^{-1} in the power spectrum for mirror feedback in Fig. 2(a-iii), according to the Wiener–Khinchin theorem. With the replacement of the mirror by the FBG, the autocorrelation for lag time near τ_{RT} is significantly suppressed for the black curve in Fig. 4(a), where the magnitude of autocorrelation is reduced to about 0.06. Such suppression of the TDS is possible because the FBG distributes the reflection along its length. Distributed reflection in the time domain is linked to chromatic dispersion in the frequency domain, where different optical frequency components experience different feedback delays. The positively detuned FBG yields optimal TDS suppression because of the strong dispersion near the edge of the main lobe of its reflection spectrum [24]. Figure 4(b) then shows the autocorrelations for the output time series $R(t)$. Due to the postprocessing through selecting the LSBs, the signal amplitudes are scrambled [10,14]. So the autocorrelation function of $R(t)$ is essentially a delta function for FBG feedback (black), where the residual autocorrelation is always smaller than 0.005 in magnitude. Nonetheless, for mirror feedback (blue), the autocorrelation function of $R(t)$ still contains a residual TDS at τ_{RT} of over 0.02. Varying the feedback parameters can affect the TDS, but the TDS for mirror feedback is generally larger than that for FBG feedback [24].

To examine RBG at tunable rates, Fig. 5(a) monitors the residual autocorrelation of $R(t)$ as τ_s varies. The residue is defined here as the maximum magnitude of the autocorrelation function within a lag time window between 0 and 25 ns, where the autocorrelation function is averaged 300 times based on 10^6 samples. According to Fig. 1, the value of τ_s affects the output time series $R(t)$, so the measured residual autocorrelation is a function of τ_s in Fig. 5(a). Residual autocorrelation of less than 0.005, as marked by the dashed line in Fig. 5(a), is considered low for RBG of good randomness quality [7,13]. For FBG feedback, the residual autocorrelation is always maintained below 0.005 when τ_s is continuously tuned from 50 ps to over 16 ns. For mirror feedback, the residual autocorrelation degrades significantly, as it exceeds 0.005 for various values of τ_s. At $\tau_s = 50$ ps, the residue of over 0.02 for mirror feedback corresponds to the TDS in Fig. 4(b), after averaging the autocorrelation function. The residue does not reduce to 0.005 until τ_s increases to over 150 ps in Fig. 5(a). As τ_s is further increased, residue peaks are identified for mirror feedback when $\tau_s{:}\tau_{\mathrm{RT}} = 1{:}7$, $1{:}3$, $1{:}2$, $1{:}1$, and $2{:}1$ for $\tau_{\mathrm{RT}} = 7.7$ ns. The residue peaks correspond to rational values of $\tau_s{:}\tau_{\mathrm{RT}}$, because the laser emission at a sampled instant can influence future samples after multiple times of feedback round-trips. Hence, RBG using mirror feedback fails when τ_s is commensurate with τ_{RT}, as previously reported according NIST tests [7,8]. Contrasting FBG and mirror feedback, Fig. 5(a) clearly shows that FBG feedback enables both the continuous tuning of τ_s and the reduction of the minimum τ_s for RBG. Finally, in order to verify the randomness quality of the output bits, the 15 statistical tests in Special Publication 800-22 from NIST are conducted on 1000 1-Mbit sequences for a significance level of 0.01 [13]. Figure 5(b) shows the NIST test results for different values of τ_s, while the number of LSBs selected per sample is varied. The closed symbols for FBG feedback are directly compared to the open symbols for mirror feedback. When $\tau_s = 50$ ps, up to 5 LSBs can be selected per sample in passing all the 15 NIST tests using FBG feedback. Mirror feedback leads to strong residues as Fig. 5(a) indicates, so only 3 LSBs can be selected in order to pass the tests in Fig. 5(b). The reduction of the number of LSBs selected for mirror feedback is due to the need of suppressing the residue through scrambling the signal amplitude [13]. When τ_s is tuned to τ_{RT} or $2\tau_{\mathrm{RT}}$, up to 5 LSBs can be selected per sample for FBG feedback, while only 3 can be selected for mirror feedback. When τ_s is incommensurate with τ_{RT}, FBG provides a similar but less significant improvement. By simply replacing the mirror by the FBG for feedback, the number of LSBs selected for RBG is generally increased.

In summary, a semiconductor laser subject to FBG feedback is demonstrated for RBG. Different from conventional localized feedback using a mirror, the distributed feedback using the properly detuned FBG effectively suppresses the TDS at τ_{RT}. The FBG feedback maintains the randomness of the output when the sampling period τ_s is continuously tuned, as verified by passing all NIST tests even when τ_s and τ_{RT} are commensurate. It reduces the minimum sampling period for low residual autocorrelation. It also increases the maximum number of useful LSBs for RBG. With the simple postprocessing of only self-differencing and selecting LSBs, RBG is demonstrated at a tunable output bit rate from 0.3 to 100 Gbps.

Funding. Research Grants Council of Hong Kong, China (CityU 110712, CityU 111213).

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. Sciamanna and K. A. Shore, Nat. Photonics **9**, 151 (2015).
4. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).
5. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).
6. T. Durt, C. Belmonte, L. P. Lamoureux, K. Panajotov, F. Van den Berghe, and H. Thienpont, Phys. Rev. A **87**, 022339 (2013).
7. R. Takahashi, Y. Akizawa, A. Uchida, T. Harayama, K. Tsuzuki, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, Opt. Express **22**, 11727 (2014).
8. K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, IEEE J. Quantum Electron. **45**, 1367 (2009).
9. N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, Opt. Express **22**, 6634 (2014).
10. X. Fang, B. Wetzel, J. M. Merolla, J. M. Dudley, L. Larger, C. Guyeux, and J. M. Bahi, IEEE Trans. Circuits Syst. I **61**, 888 (2014).
11. A. Wang, Y. Yang, B. Wang, B. Zhang, L. Li, and Y. Wang, Opt. Express **21**, 8701 (2013).
12. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).
13. X. Z. Li and S. C. Chan, IEEE J. Quantum Electron. **49**, 829 (2013).
14. X. Z. Li and S. C. Chan, Opt. Lett. **37**, 2163 (2012).
15. N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, Opt. Lett. **36**, 4632 (2011).
16. M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, Opt. Express **22**, 17271 (2014).
17. A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express **18**, 18763 (2010).
18. M. C. Soriano, J. Garcia-Ojalvo, C. R. Mirasso, and I. Fischer, Rev. Mod. Phys. **85**, 421 (2013).
19. A. P. A. Fischer, M. Yousefi, D. Lenstra, M. W. Carter, and G. Vemuri, IEEE J. Sel. Top. Quantum Electron. **10**, 944 (2004).
20. D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, Opt. Lett. **32**, 2960 (2007).
21. D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, IEEE J. Quantum Electron. **45**, 879 (2009).
22. R. M. Nguimdo, G. Verschaffelt, J. Danckaert, and G. Van der Sande, Opt. Lett. **37**, 2541 (2012).
23. X. Porte, O. D'Huys, T. Jüngling, D. Brunner, M. C. Soriano, and I. Fischer, Phys. Rev. E **90**, 052911 (2014).
24. S. S. Li and S. C. Chan, IEEE J. Sel. Top. Quantum Electron. **21**, 1800812 (2015).
25. A. Wang, P. Li, J. Zhang, J. Zhang, L. Li, and Y. Wang, Opt. Express **21**, 20452 (2013).
26. J. G. Wu, G. Q. Xia, and Z. M. Wu, Opt. Express **17**, 20124 (2009).
27. Y. Hong, Opt. Express **21**, 17894 (2013).
28. S. Xiang, W. Pan, L. Zhang, A. Wen, L. Shang, H. Zhang, and L. Lin, Opt. Commun. **324**, 38 (2014).
29. C. H. Cheng, Y. C. Chen, and F. Y. Lin, Opt. Express **23**, 2308 (2015).