# Randomness evaluation for an optically injected chaotic semiconductor laser by attractor reconstruction

Xiao-Zhou Li,[1] Jun-Ping Zhuang,[1] Song-Sui Li,[1] Jian-Bo Gao,[2] and Sze-Chun Chan[1,3,*]

[1] *Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China*
[2] *Institute of Complexity Science and Big Data Technology, Guangxi University, Nanning, Guangxi, China*
[3] *State Key Laboratory of Millimeter Waves, City University of Hong Kong, Hong Kong, China*

(Received 30 May 2016; revised manuscript received 2 September 2016; published 18 October 2016)

State-space reconstruction is investigated for evaluating the randomness generated by an optically injected semiconductor laser in chaos. The reconstruction of the attractor requires only the emission intensity time series, allowing both experimental and numerical evaluations with good qualitative agreement. The randomness generation is evaluated by the divergence of neighboring states, which is quantified by the time-dependent exponents (TDEs) as well as the associated entropies. Averaged over the entire attractor, the mean TDE is observed to be positive as it increases with the evolution time through chaotic mixing. At a constant laser noise strength, the mean TDE for chaos is observed to be greater than that for periodic dynamics, as attributed to the effect of noise amplification by chaos. After discretization, the Shannon entropies continually generated by the laser for the output bits are estimated in providing a fundamental basis for random bit generation, where a combined output bit rate reaching 200 Gb/s is illustrated using practical tests. Overall, based on the reconstructed states, the TDEs and entropies offer a direct experimental verification of the randomness generated in the chaotic laser.

DOI: 10.1103/PhysRevE.94.042214

## I. INTRODUCTION

Fast physical random bit generation (RBG) is crucial for a range of applications in cryptography, computation, and secure communication [1–9]. As photonic devices support signals of wide bandwidths, they are applicable to generating signals with high-speed fluctuations. The signals with subnanosecond fluctuations have enabled fast RBG at bit rates exceeding hundreds of gigabit per second through various approaches. Different approaches have utilized different physical phenomena, including quantum fluctuations [7], noisy spontaneous emissions [10–12], nonlinear optical instabilities [13–15], optoelectronic oscillations [16–18], and chaos in semiconductor lasers [19–28]. In particular, with inherently nonlinear and fast responses, chaotic semiconductor lasers have been actively investigated for RBG [1–3]. Semiconductor laser chaos-based RBG offers a unique combination of advantages for RBG such as the possibilities of achieving high bit rates [19–22], monolithic integration [26–28], synchronizable consistent responses [8,29], and effective amplification of noise [4–6]. With combinations of different schemes of optical feedback [19–21], optical injection [30–32], distributed feedback [33], mutual coupling [22], and intracavity interactions [25,34], a number of experimental investigations have been thoroughly reported for semiconductor laser chaos-based RBG.

To verify the randomness for semiconductor laser chaos-based RBG, practical tests such as those from the National Institute of Standards and Technology (NIST) can be adopted [1–3], but passing these tests do not fundamentally guarantee randomness. There are examples that pseudorandom bits obtained from properly designed digital algorithms can pass these practical randomness tests, even though the bits are not truly random [35]. Fundamentally, the randomness in laser chaos-based RBG is attributed to the nonlinear dynamical mixing that originates from the diverging trajectories of neighboring states in the attractor [6]. The expansion rates of the separation distances between neighbors are quantified by the Lyapunov exponents, which are time-averaged in the limit of infinitesimally small initial separations [9,36–40]. By numerically simulating noisy perturbations on the initial states, the Lyapunov exponents have been comprehensively estimated for lasers under optical feedback along with injection [9,36–38]. Alternatively, by reconstructing the states from a numerically simulated time series, the Lyapunov exponents have been estimated for a laser under feedback without injection in some recent works [40]. However, it remains interesting to estimate the divergence of the states of the chaotic lasers experimentally.

Besides the divergence of states, the randomness in laser chaos-based RBG can also be evaluated by the Shannon entropy [4–6]. The Shannon entropy refers to the unpredictability of a bit generated from a discretized detection of the laser state. As the evolution time increases, initially neighboring states diverge, causing the bit to become increasingly unpredictable, which in turn increases the Shannon entropy [4–6]. Recently, a theoretical linkage is established between mixing and ergodicity that illustrates entropy generation in a chaotic laser with feedback [4]. By numerical perturbations using different noise series on an initial state, the Shannon entropy of the output bits for a laser under optical feedback has been estimated using a rate-equation model [5], where extensions to a pair of lasers with feedback and a solitary vertical cavity surface-emitting laser have been simulated [24,28]. By experimenting on a mirror-integrated semiconductor laser, the Shannon entropy has also been estimated through switching the optical feedback off and on periodically [6]. When the feedback was off, the laser was reset to the free-running state. When the feedback was on, the laser was forced to evolve away from the free-running state according to the chaotic dynamics

[*] scchan@cityu.edu.hk

with noisy perturbations. After many repetitions, the statistics of the output bits was used to estimate the transient Shannon entropy generated immediately after switching the feedback. However, in practice, a laser for RBG normally stays chaotic without being periodically interrupted by any switching of the operating parameters [2,19,21,28]. The laser does not periodically return to a single free-running state, but rather continuously evolves within the chaotic attractor to different states. So it is of interest to experimentally estimate the continuously generated Shannon entropy for laser chaos-based RBG without the interruptions.

In this paper, the randomness generated from an optically injected chaotic semiconductor laser for RBG is evaluated through state-space reconstruction. The reconstruction is applied to both numerical simulations and experiments using the emission intensity time series of the laser. The reconstructed attractor contains neighboring states that diverge over time as governed by the time-dependent exponents (TDEs), which are estimated for the observations below. First, the mean TDE averaged over the entire attractor is observed to be positive in signifying the divergence of states for randomness generation. It increases with the evolution time at a rate that provides an estimation of the largest Lyapunov exponent. Second, the mean TDE for the chaotic dynamics is observed as being greater than that for a periodic dynamics under the same noise strength. This verifies the effect of noise amplification by chaotic mixing. Third, Shannon entropies associated with the output bits are experimentally estimated based on an ensemble of the reconstructed states. The continually generated Shannon entropies fundamentally enable RBG. With the evaluation of randomness by the TDEs and Shannon entropies, RBG at a combined output bit rate of 200 Gb/s is verified using the practical randomness tests from NIST.

The approach of state-space reconstruction offers some interesting advantages for randomness evaluation. It is applicable to experiments because only the measurable intensity time series is required. It is comprehensive in revealing the divergence of different initial states through obtaining a distribution function of all TDEs. It experimentally estimates the Shannon entropies that are based on the entire attractor instead of just one initial state. The Shannon entropies are calculated without interrupting the laser, thereby directly confirming the continuous generation of randomness in the chaotic laser.

Also, instead of the more common scheme of optical feedback [41–44], optical injection is employed here for inducing chaos [30,31]. The optical feedback scheme often generates a chaotic signal with an observable time-delay signature, which is defined as the nonzero autocorrelation of the signal when the lag time equals the round-trip delay time of the feedback loop [41,42]. The time-delay signature indicates partial repetition of the signal and is thus undesirable in the generation of randomness [33]. The optical injection scheme does not have any feedback loop, so it offers the advantage of generating chaotic signals without any time-delay signatures [30,31,45]. Nonetheless, the approach of attractor reconstruction for randomness evaluation is not limited to the injected lasers as it is applicable to schemes associated with different dimensions [3,46–49]. After this introduction, Sec. II describes the procedure of evaluating randomness through state-space reconstruction, while Sec. III presents the numerical model and experimental setup of chaos generation by optical injection. Numerically, the TDEs for the divergence of states are estimated in Sec. IV. Experimentally, the continuously generated Shannon entropies are estimated with the TDEs in Sec. V. Results of the practical NIST tests are discussed in Sec. VI, which is followed by a conclusion in Sec. VII.

## II. STATE-SPACE RECONSTRUCTION

Although the dynamics of a semiconductor laser involves the intracavity optical field and charge carrier density, only the emission intensity of the laser is measured in most experiments [30,31]. So the state of the laser has to be reconstructed using embedding techniques [46–51]. The scalar time series of the emission intensity $I(t)$ is first recorded and normalized to its free-running value when the laser is solitary [52]. It is then used to construct a time-varying state vector $\boldsymbol{x}(t) = [I(t), I(t+\tau_\mathrm{e}), \ldots, I(t+(m_\mathrm{e}-1)\tau_\mathrm{e})]$, where $m_\mathrm{e}$ and $\tau_\mathrm{e}$ are the embedding dimension and delay time, respectively [53,54]. Practically, $I(t)$ is recorded only at $t = i\tau_\mathrm{s}$ with a fixed sampling period $\tau_\mathrm{s}$ for $i = 1,2,\ldots,N$, where $N$ is the total number of intensity samples [48]. The embedding delay time $\tau_\mathrm{e}$ has to be chosen as a multiple of $\tau_\mathrm{s}$. The $i$th reconstructed state is notated by $\boldsymbol{x}_i = \boldsymbol{x}(i\tau_\mathrm{s})$ for $i = 1,2,\ldots,N-(m_\mathrm{e}-1)\tau_\mathrm{e}/\tau_\mathrm{s}$. These states altogether form the attractor when the laser is in chaos.

Expressing the evolution time as $k\tau_\mathrm{s}$ for an integer $k$. When treating any $\boldsymbol{x}_i$ as an initial state, the corresponding trajectory of evolution is $\boldsymbol{x}_{i+k}$. Likewise, when treating a pair $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ as two initial states, their separation distance is $d_{ij}(k) = \|\boldsymbol{x}_{i+k} - \boldsymbol{x}_{j+k}\|$, where $\|\cdot\|$ denotes the Euclidean norm in the state space. The exponent of the time-dependent increment of the separation is

$$\Lambda_{ij}(k) = \ln \frac{d_{ij}(k)}{d_{ij}(0)}, \tag{1}$$

which is called the TDE of the initial states $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ [49–51]. Here, the TDE is a unitless quantity that describes the divergence of the trajectories of the two states. It is noted that, for initial states lying along an eigendirection of the dynamical evolution, $\Lambda_{ij}(k)/(k\tau_\mathrm{s})$ approximates a finite-time Lyapunov exponent when $d_{ij}(0)$ becomes infinitesimally small [49,55].

Define an ensemble $\mathbb{E}$ as the collection of all possible pairs of neighboring states $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ with initial distances $d_{ij}(0)$ lying within $[r,(1+\delta)r]$ for some small $r$ and $\delta$. A probability distribution function $p(\Lambda,k)$ is used to describe the occurrences of different values of $\Lambda_{ij}(k)$ for all state pairs $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ in $\mathbb{E}$ [51]. As a result, the mean TDE is expressed as

$$\Lambda_0(k) = \int_{-\infty}^{\infty} p(\Lambda,k)\Lambda d\Lambda, \tag{2}$$

which is an ensemble average of the TDEs of all neighboring states collected in $\mathbb{E}$ [48–51,53,54,56,57]. Its rate of change $\Lambda_0(k)/(k\tau_\mathrm{s})$ is denoted as $\lambda$, which approximates the positive largest Lyapunov exponent of the dynamics [5,49,51]. It can also be regarded as an integral form of the scale-dependent Lyapunov exponent (SDLE), which is applicable to both clean and noisy chaotic signals [58–60]. The mean TDE has been calculated for an injected laser using numerical simulations

[53,54], although the distribution of TDEs as well as the extension to experiments need to be further explored.

As for RBG, the state $\boldsymbol{x}(t)$ of the laser is mapped to a binary bit $B$ of either 0 or 1. The mapping is typically done by detecting and discretizing the intensity signal using an analog-to-digital converter (ADC) along with bit selection [19–24], where a specific realization is detailed in Sec. V C. A probability $P_i(B,k)$ governs the value of $B$ as an initial state $\boldsymbol{x}_i$ evolves over time $k\tau_{\rm s}$. The Shannon entropy of the bit from initial state $\boldsymbol{x}_i$ is

$$H_i(k) = -\sum_{B=0}^{1} P_i(B,k)\log_2 P_i(B,k), \tag{3}$$

which maximizes to unity if $P_i(0,k) = P_i(1,k) = 0.5$ [4–6,16]. For estimating $H_i(k)$, consider a subset of pairs $(\boldsymbol{x}_i,\ \boldsymbol{x}_j)$ in $\mathbb{E}$ that share a common $\boldsymbol{x}_i$. This gives a group of neighboring states $\boldsymbol{x}_j$ locating within a small shell centered at $\boldsymbol{x}_i$ with inner and outer radii of $r$ and $(1+\delta)r$, respectively. At the beginning, all states $\boldsymbol{x}_j$ are nearly identical and so they give a same value of $B$. After time $k\tau_{\rm s}$, the evolved states $\boldsymbol{x}_{j+k}$ generally diverge to different parts of the attractor, so the resultant values of $B$ become diversified. The ratios of occurrences of $B = 0$ and 1 are used to respectively estimate the probabilities $P_i(0,k)$ and $P_i(1,k)$, which in turn give $H_i(k)$ through Eq. (3). The accuracy of the estimation obviously improves when the shell becomes infinitesimally small, but it requires increasing the length of the recorded time series in order to maintain a sufficient number of neighbors for the statistics. Nonzero shell radii are useful as long as they are much smaller than the size of the attractor [49,51]. Also, different from the previous experiments that periodically reset the laser to the free-running initial state [6], the estimation using Eq. (3) is applicable to any reconstructed state $\boldsymbol{x}_i$ on the attractor.

Subsequently, by averaging $H_i(k)$ over a collection of states $\boldsymbol{x}_i$ on the attractor, the mean Shannon entropy $H_0(k)$ is estimated. The estimation of entropy through reconstructions is applicable to not only semiconductor lasers but also other photonic systems [16,17]. The entropy is continuously monitored without interrupting the laser chaos-based RBG. The above evaluation of randomness through the TDEs and Shannon entropies are based on state-space reconstruction, which requires merely the intensity time series from either simulations or experiments.

## III. OPTICALLY INJECTED LASER

Optical injection is adopted to induce chaos for obtaining randomness in a semiconductor laser. As shown schematically in Fig. 1, two lasers are arranged in a master-slave configuration. The master laser ML is in continuous-wave operation. Its emission is amplified by an erbium-doped fiber amplifier EDFA and transmitted through a circulator for optically injecting the slave laser SL, which is a single-mode semiconductor laser. The normalized injection strength $\xi_{\rm i}$ is controlled by the EDFA gain, while a polarization controller PC is set to match the polarizations of the injection and SL. The operating point of ML determines its detuning frequency $f_{\rm i}$ with respect to the free-running optical frequency of SL. By adjusting the optical injection parameters ($\xi_{\rm i}$, $f_{\rm i}$), SL can be driven into different nonlinear dynamics such as stable locking, period-one (P1) oscillation, and chaos [52,61]. Similarly to most experiments on laser chaos-based RBG, only the emission intensity $I(t)$ from the slave laser is measured using a photodetector PD in Fig. 1, where an oscilloscope OSC subsequently records the time series with a sampling period $\tau_{\rm s}$ over a long time span for state-space reconstruction.

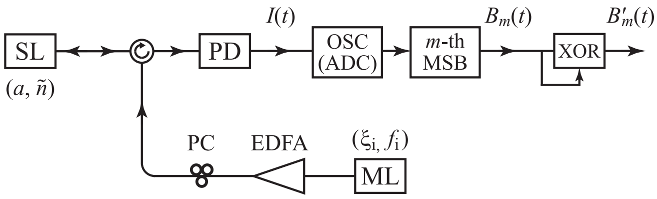

FIG. 1. Schematic of an optically injected semiconductor laser for chaos-based RBG. Continuous-wave light from a master laser ML is injected into the slave laser SL for inducing nonlinear dynamics. The emission intensity time series $I(t)$ from SL is measured by a photodetector PD for recording by an oscilloscope OSC. The $m$th MSB is then selected in yielding a bit stream $B_m(t)$ that is further digitally processed into an output bit stream $B'_m(t)$.

As for RBG, the oscilloscope essentially acts as an ADC for discretization. The ADC outputs 8 bits for each intensity sample, but only the $m$th most significant bit (MSB) is selected to yield a bit stream $B_m(t)$. The bit stream $B_m(t)$ is further digitally processed by an exclusive-or (XOR) operation with a replica of $B_m(t)$ that is delayed by a fixed amount of time. This yields the output bit stream $B'_m(t)$. The selection of bits and the XOR operation are commonly employed to reduce autocorrelations and nonuniformities in distributions of the output bits [14,21,30,62]. Nonetheless, since the digital processing is a deterministic procedure, the output bits cannot be random unless there is a nonzero entropy contained in $I(t)$ of the laser.

### A. Numerical model

For all numerical simulation results, the optically injected semiconductor laser in Fig. 1 is described by a complex intracavity field amplitude $a(t)$ and a real excess charge carrier density $\tilde{n}(t)$, which are normalized with respect to their free-running values [53,63]. The emission intensity time series is then calculated as $I(t) = |a(t)|^2$ [52,53]. Due to the optical injection, the rate-equation model for $(a(t), \tilde{n}(t))$ are expressed as [52,64]

$$\frac{da}{dt} = \frac{1-ib}{2}\left[\frac{\gamma_c\gamma_n}{\gamma_s\tilde{J}}\tilde{n} - \gamma_p(|a|^2-1)\right]a + \xi_i\gamma_c\exp(-i2\pi f_i t) + f_{\rm sp}, \tag{4}$$

$$\frac{d\tilde{n}}{dt} = -(\gamma_s + \gamma_n|a|^2)\tilde{n} - \gamma_s\tilde{J}\left(1 - \frac{\gamma_p}{\gamma_c}|a|^2\right)(|a|^2-1), \tag{5}$$

where $\gamma_c = 5.36\times10^{11}\ {\rm s}^{-1}$ is the cavity decay rate, $\gamma_s = 5.96\times10^{9}\ {\rm s}^{-1}$ is the spontaneous carrier relaxation rate, $\gamma_n = 7.53\times10^{9}\ {\rm s}^{-1}$ is the differential carrier relaxation rate, $\gamma_p = 1.91\times10^{10}\ {\rm s}^{-1}$ is the nonlinear carrier relaxation rate, $b = 3.2$ is the linewidth enhancement factor, and $\tilde{J} = 1.222$

is the normalized bias current above threshold. The laser has a relaxation resonance frequency of $(2\pi)^{-1}(\gamma_c\gamma_n + \gamma_s\gamma_p)^{1/2} = 10\,\text{GHz}$. The values of the parameters were reported for a commercial semiconductor laser [65]. Additionally, the rate-equation model in Eqs. (4) and (5) incorporates a Langevin term $f_{\text{sp}}$, which represents spontaneous emission noise in the slave laser. The real and imaginary parts of $f_{\text{sp}}$ at different time instants are mutually independent, in which ergodicity is observed as detailed in the following averages [64,66]:

$$\langle f_{\text{sp}}(t) f^*_{\text{sp}}(t')\rangle = \frac{4\pi\Delta\nu}{1+b^2}\delta(t-t'), \tag{6}$$

$$\langle f_{\text{sp}}(t) f_{\text{sp}}(t')\rangle = 0, \tag{7}$$

$$\langle f_{\text{sp}}(t)\rangle = 0, \tag{8}$$

where $\Delta\nu = 10$ MHz is the free-running optical linewidth of the slave laser. Introduced in the early works on laser dynamics, the Langevin term $f_{\text{sp}}$ models the noisy disturbances on the complex laser field $a(t)$, resulting in mutually independent perturbation on the amplitude and phase of the laser light [66–69]. The noisy disturbance has a zero mean as Eq. (8) shows. It is also memoryless so that $f_{\text{sp}}$ at different time instants are unrelated as Eqs. (6) and (7) show [67]. Although noise can also be contained in the injection light and bias current, only the spontaneous emission noise is considered because it is inherent to the slave laser. The noise strength is thus fully controlled by the value of $\Delta\nu$.

Using second-order Runge-Kutta integration on Eqs. (4) and (5), the intensity $I(t)$ is recorded with a sampling period of $\tau_s = 2.38$ ps, where a finer integration time step of $\tau_s/4$ is adopted for ensuring accuracy. The injection parameters are chosen as $(\xi_i, f_i) = (0.05, 6.26\text{ GHz})$ for driving the laser into chaos [63,64].

Numerically, the simulated chaotic intensity $I(t)$ is shown by the black curve in Fig. 2(a), followed by the power spectrum in Fig. 3(a). The time series contains chaotic fluctuations faster than 100 ps, which is comparable to the reciprocal of the relaxation resonance frequency of the laser [42]. The time series $I(t)$ is detected by the ADC into 256 digitization values, which observe the probability density function as shown by the black curve in Fig. 2(b). The corresponding power spectrum is shown in Fig. 3(a-i) by applying Fourier transform on $I(t)$. The broadband spectrum is enhanced near 10 GHz due to relaxation resonance [31]. The autocorrelation function of the simulated $I(t)$ is shown in Fig. 3(b-i). It reduces from unity to about 0.5 when the lag time increases from zero to beyond $5\tau_s$.

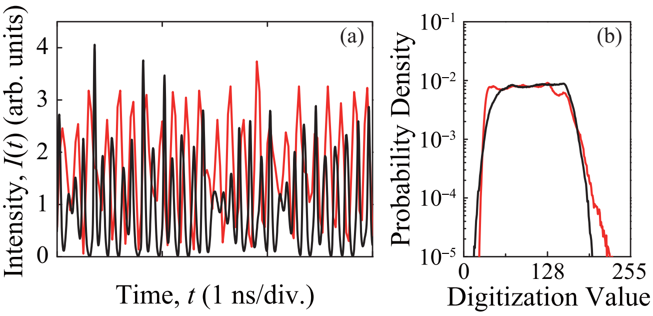

FIG. 2. (a) Chaotic emission intensity time series $I(t)$ of the optically injected semiconductor laser. (b) Probability density functions for the digitized values of $I(t)$ measured after the ADC. The data are recorded from numerical simulations (black) and experiments (red).

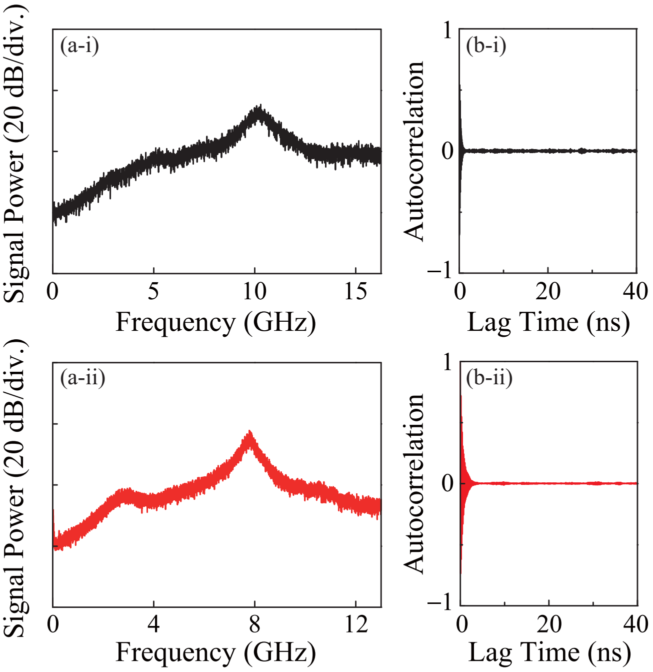

FIG. 3. (a) Power spectra and (b) autocorrelation functions of the chaotic emission intensity time series. The data are recorded from (i) numerical simulations and (ii) experiments.

Moreover, Fig. 4 shows the trajectory of the state vector $\boldsymbol{x}(t)$ that is reconstructed from $I(t)$. The reconstruction uses embedding dimension $m_e = 8$ and embedding delay time $\tau_e = 5\tau_s$, which are consistent with the choices in previous works on optically injected lasers [53,54]. The time-varying vector $\boldsymbol{x}(t)$ is projected to the first three dimensions for visualization, so only its first three components $I(t)$, $I(t+\tau_e)$, and $I(t+2\tau_e)$ are plotted. For clarity, the trajectory

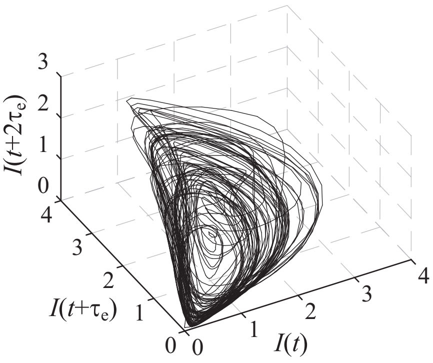

FIG. 4. Reconstructed state trajectory based on the numerically simulated $I(t)$ of the chaotic laser. The time-varying state vector is reconstructed as $\boldsymbol{x}(t) = [I(t), I(t+\tau_e), \ldots, I(t+(m_e-1)\tau_e)]$ with embedding dimension $m_e = 8$ and delay time $\tau_e = 5\tau_s$. Only the first three components of $\boldsymbol{x}(t)$ are plotted.

is shown for only less than 10 ns. The optically injected laser follows a period-doubling route to chaos, so the chaotic trajectory contains reminiscent structures of periodic loops [52,53]. However, the chaotic trajectory does not repeat and so never forms closed loops. Section IV presents the numerical simulation results regarding the TDEs on the divergence of chaotic trajectories for RBG.

### B. Experimental setup

For all experimental results, the setup of optical injection in Fig. 1 is implemented using a 1.55-$\mu$m distributed-feedback semiconductor laser (Nortel LC111-18) as the slave laser SL. The laser is packaged with a fiber pigtail, temperature-stabilized at 20°C for a stable wavelength, and biased at 60 mA, which is above the threshold of 25 mA. The laser gives an emission power of 2.2 mW with a relaxation resonance frequency of 7 GHz when it is free-running. A tunable laser (HP 8168A) is then used as the master laser ML. It emits continuous-wave light that is detuned by $f_i = 4$ GHz from the free-running frequency of SL. The injection light from ML goes through optical amplification by the EDFA (Amonics AEDFA-23-B-FA), polarization controller, and circulator for injecting the slave laser SL, where the injection optical power is adjusted to 0.75 mW for invoking chaotic dynamics [31,70]. Subsequently, the emission from the slave laser passes through the circulator to the photodetector PD (Newport AD-10ir), which measures the time-varying intensity $I(t)$ for recording by a digital real-time oscilloscope OSC (Agilent 81304B). Though the electronic bandwidth of the measurement is limited by the oscilloscope to 13 GHz, it is sufficiently higher than the relaxation resonance frequency of the laser, which roughly corresponds to the chaotic bandwidth [42,71]. The experimental recording of $I(t)$ adopts a sampling period of $\tau_s = 25$ ps. The value is larger than that for the simulations in Sec. III A, although it is already the smallest available value for the oscilloscope.

Experimentally, the recorded intensity $I(t)$ is shown by the red curve in Fig. 2(a). The time series again contains fast and chaotic fluctuations, as in the numerical results in black. The probability density function measured at the ADC for the experimental intensity time series is shown by the red curve in Fig. 2(b), where the maximal probability of $9 \times 10^{-3}$ corresponds to a min-entropy of 6.8 for the ideal case of uncorrelated samples [23]. The corresponding power spectrum is shown in Fig. 3(a-ii). It is again broadband with an enhancement near the relaxation resonance frequency of 7 GHz in the experiments [31]. The autocorrelation function of the experimental $I(t)$ is shown in Fig. 3(b-ii). It reduces to about 0.3 when the lag time increases from zero to $\tau_s$. The magnitudes of the autocorrelation functions in Fig. 3(b) stay less than $10^{-2}$ when lag time is much greater than 1 ns, which is because of the use of optical injection instead of feedback for chaos generation in avoiding the time-delay signatures.

Due to the increased $\tau_s$ in the experiments, embedding dimension $m_e = 5$ and delay time $\tau_e = \tau_s$ are adopted for reconstruction of experimental data. Section V presents the experimental results of the TDEs for the divergence of chaotic trajectories, where the Shannon entropies based on the reconstructed states are directly estimated for RBG.

## IV. NUMERICAL RESULTS

Based on the rate-equation simulations in Sec. III A, a time series $I(t)$ is recorded for reconstruction with $m_e = 8$ and $\tau_e = 5\tau_s$, which equals 11.9 ps, as the sampling period is fixed at $\tau_s = 2.38$ ps. States $\boldsymbol{x}_i$ at time $t = i\tau_s$ are formed as detailed in Sec. II, constituting the chaotic attractor as Fig. 4 shows. Any pair of states $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ are regarded as neighbors if their separation distance $d_{ij}(0)$ falls between $r$ and $(1+\delta)r$, where small values of $r = 0.04$ and $\delta = 50\%$ are adopted [53]. Though the states are initially close to each other, they diverge to $(\boldsymbol{x}_{i+k}, \boldsymbol{x}_{j+k})$ as quantified by the TDE $\Lambda_{ij}(k)$ of Eq. (1) when the evolution time $k\tau_s$ is varied by index $k$.

### A. Distribution of numerical TDEs

Figure 5 shows the probability distribution function $p(\Lambda,k)$ of the simulated TDEs. From Sec. II, $p(\Lambda,k)d\Lambda$ is the relative occurrence for the estimated TDEs that are within $\Lambda$ and $\Lambda + d\Lambda$ when all neighboring pairs of initial states over the entire attractor are considered. In Fig. 5(a), the evolution time is 2.38 ps for $k = 1$. The time is too short for any pair of neighbors to diverge, so most TDEs are concentrated at around zero. In Fig. 5(b), the evolution time increases to about 0.05 ns for $k = 21$. The distribution of the TDEs peaks at 0.4 and spreads beyond 3 because most neighbors diverge through the chaotic dynamics. For any pair of initial states $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ aligned along an eigendirection of the dynamics, their TDE has a rate of change of $\Lambda_{ij}(k)/(k\tau_s)$, which approximates a finite-time Lyapunov exponent [36,51,55]. Neighboring states along different eigendirections lead to different Lyapunov exponents that cause the spread of $p(\Lambda,k)$ in Fig. 5(b). Interestingly, not every exponent is positive, so a small portion of neighboring pairs actually converge over time, as the negative TDEs below the dashed line in Fig. 5(b) show.

Then, in Fig. 5(c), the evolution time further increases to about 0.1 ns for $k = 42$. The vast majority of the neighbors keep diverging so that most TDEs continue to increase. In

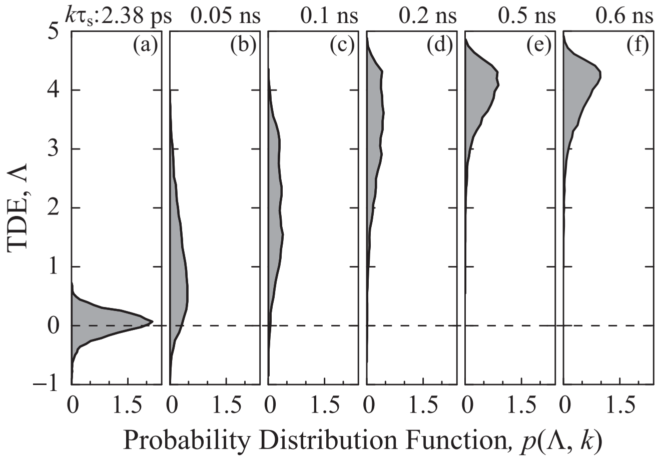

FIG. 5. Numerical probability distribution function $p(\Lambda,k)$ of the TDEs estimated from the reconstructed chaotic attractor. The initially neighboring states evolve over time $k\tau_s$ for $k =$ (a) 1, (b) 21, (c) 42, (d) 84, (e) 210, and (f) 252. The sampling period is $\tau_s = 2.38$ ps in the simulations.

Fig. 5(d), as the evolution time increases to around 0.2 ns for $k = 84$, the TDEs keep increasing in reaching values beyond 4. Due to the sufficiently long evolution time, it is very unlikely for a pair of states to be always aligned to a converging eigendirection throughout their trajectories, so negative TDEs are no longer observed. Now moving on to Fig. 5(e), when the evolution time increases to 0.5 ns for $k = 210$, the distribution function $p(\Lambda,k)$ shows that the TDEs merely increase slowly. There is almost no change for $p(\Lambda,k)$ when the evolution time is further increased to 0.6 ns at $k = 252$ in Fig. 5(f). In fact, for any initially neighboring states $(\boldsymbol{x}_i, \boldsymbol{x}_j)$, their evolved states $(\boldsymbol{x}_{i+k}, \boldsymbol{x}_{j+k})$ are now randomly and independently located on the chaotic attractor. The initial states are completely mixed by the chaotic dynamics in conforming to an invariant probability density for the states [4,27]. So the probability distribution function $p(\Lambda,k)$ for the TDEs also becomes invariant when $k$ is large in Figs. 5(e) and 5(f). In addition, according to Eq. (1), the size of the attractor is roughly comparable to $r \exp(\Lambda)$ for $\Lambda = 4.2$ at the peak of the invariant distribution in Figs. 5(e) and 5(f), so the attractor size is confirmed as being significantly greater than $r$. Therefore, despite the existence of a small portion of neighbors with negative TDEs at short evolution times, Fig. 5 generally shows the increment of TDEs when most neighboring states diverge with chaotic mixing as the evolution time increases.

### B. Evolution of numerical mean TDE

For the ensemble of neighbors on the entire attractor, the overall behavior of the TDEs can be examined by averaging them to $\Lambda_0(k)$ using $p(\Lambda,k)$ through Eq. (2). The mean TDE $\Lambda_0(k)$ varies with the evolution time $k\tau_s$, as the black solid curve in Fig. 6 shows. When $k\tau_s$ increases from zero, $\Lambda_0(k)$ also increases from zero as most neighbors start to diverge according to Figs. 5(a)–5(d). The initial increment of $\Lambda_0(k)$ in Fig. 6 is linear due to the dominance of the positive largest Lyapunov exponent on the divergence. The mean TDE has a slope $\lambda$ defined by $\Lambda_0(k)/(k\tau_s)$, which provides a rough estimation of the largest Lyapunov exponent [49,51,57]. Such a TDE slope quantifies the mixing speed of the states and is estimated as $\lambda \approx 15\ \text{ns}^{-1}$ at $k\tau_s = 0.2$ ns in Fig. 6. When $k\tau_s$ further increases, $\Lambda_0(k)$ increases less quickly and reaches a saturated value of 3.9, corresponding to the invariant $p(\Lambda,k)$ in Figs. 5(e) and 5(f). With the sufficiently long evolution time, the dynamics completely mixes the states and scatters them on the chaotic attractor of a finite size. The average separation between the states no longer expands, which explains the saturation of $\Lambda_0(k)$. Incidentally, $\Lambda_0(k)$ reaches half of its saturated value at $k\tau_s = 0.1$ ns that corresponds to the reciprocal of the relaxation resonance frequency of the laser, which is typically comparable to the chaotic bandwidth [42,71].

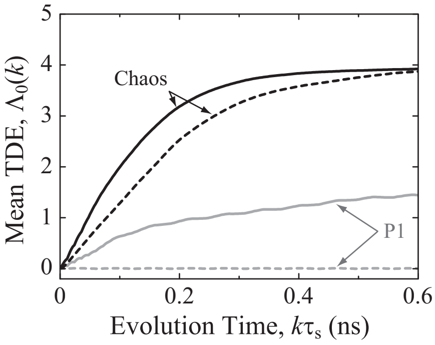

FIG. 6. Numerically estimated mean TDE $\Lambda_0(k)$ versus evolution time $k\tau_s$. The laser is injected into chaotic dynamics (black) and P1 dynamics (gray). The simulations are conducted with and without noise for the solid and dashed curves, respectively.

Besides the chaotic dynamics, however, noise of the slave laser can also contribute to the divergence of neighboring states. The fast increment of $\Lambda_0(k)$ for the black solid curve in Fig. 6 is in fact obtained as the laser states are continually mixed by the chaotic dynamics and constantly perturbed by noise. The noise is in the form of spontaneous emission modeled using $f_{sp}$ in Eq. (4) at a strength specified by $\Delta\nu = 10$ MHz. In order to examine the effect of noise without chaotic mixing, the gray solid curve in Fig. 6 is obtained by simulating the slave laser in P1 dynamics instead of chaotic dynamics. The P1 dynamics is obtained by adjusting the injection strength $\xi_i$ to 0.10, while keeping all other parameters unchanged [63,64,66,72]. The laser state follows a trajectory that loops at a frequency of 16 GHz, so the emission intensity oscillates periodically instead of chaotically. The noise strength is kept at $\Delta\nu = 10$ MHz in perturbing the states, leading to a gradual diffusion of the trajectory and its phase. This causes the eventual separation of neighbors as indicated by the small increase of $\Lambda_0(k)$ as $k\tau_s$ increases, though the increment is slow with $\lambda$ of less than $5\ \text{ns}^{-1}$ due to the lack of chaotic mixing in P1 dynamics. By contrasting the two solid curves in Fig. 6, chaotic dynamics is clearly preferred over P1 dynamics for large TDEs.

In contrast to noise without chaotic dynamics, the effect of the dynamics without noise is also investigated in Fig. 6, as the dashed curves show by setting $\Delta\nu = 0$ for the simulations. On one hand, the black dashed curve is obtained when the laser is in chaos. The chaotic dynamics alone causes the mixing of the neighboring states even without the perturbation of noise. Chaos causes $\Lambda_0(k)$ to quickly rise to its saturated value, though the rise is not as quick as that assisted by noise. At $k\tau_s = 0.2$ ns, the TDE slope $\lambda$ is slightly reduced to about $12\ \text{ns}^{-1}$, which is an improved estimation for the largest Lyapunov exponent of chaos due to the absence of noise. It is possible to calculate the Lyapunov exponents without noise by examining the evolution of small deviations from the trajectory of the state [73,74]. The evolution of the original trajectory is governed by Eqs. (4) and (5), while the evolutions of the deviations are governed by a set of linearized equations around the original trajectory [9,55]. Orthogonalization and normalization are incorporated when the linearized equations are numerically solved for yielding the evolution of the deviations [9]. The exponential growth rates of the deviations then give the Lyapunov exponents, where the largest Lyapunov exponent is found to be about $11.2\ \text{ns}^{-1}$ in close agreement with the TDE slope in Fig. 6 for chaos. On the other hand, the gray dashed curve is obtained when the laser is driven into P1 dynamics. The reconstructed trajectory for the noiseless P1 dynamics is exactly a closed loop of a limit cycle [66]. Any neighboring states are actually just at different phases of the

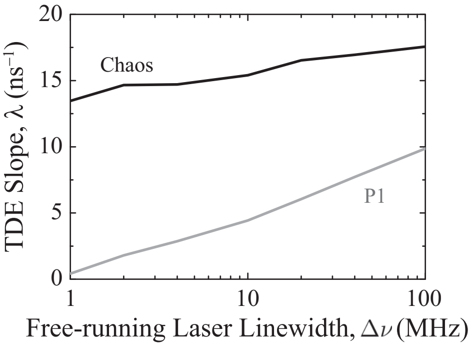

FIG. 7. Numerical TDE slope $\lambda$ as a function of the free-running laser linewidth $\Delta\nu$. The slope is evaluated at $k\tau_s = 0.2$ ns. The laser is injected into chaotic dynamics (black) and P1 dynamics (gray).

loop, so they neither converge nor diverge on average, forcing $\Lambda_0(k)$ to always stay very close to zero. Thus, while chaos provides a positive $\Lambda_0(k)$ without noise, P1 dynamics does not provide randomness at all.

For completeness, Fig. 7 shows the TDE slope $\lambda$ as the noise strength is varied by $\Delta\nu$, while the laser is driven into the chaotic and P1 dynamics for the black and gray curves, respectively. The TDE slope $\lambda$ is evaluated at $k\tau_s = 0.2$ ns in Fig. 7 to quantify the divergence speed. As noise strengthens, the increasing $\Delta\nu$ always causes $\lambda$ to increase, which is consistent with the reduction of memory time in related works [5]. As chaos provides mixing, $\lambda$ for chaotic dynamics is always significantly greater than that for P1 dynamics, which verifies the effect of chaotic noise amplification [4,75].

In short, as Figs. 6 and 7 show, the reconstruction enables the observation of the increase of a positive $\Lambda_0(k)$ over time. Chaos is found to be essential in quickly yielding a large $\Lambda_0(k)$ for generating randomness, which is achieved by the dynamical mixing of states.

### C. Parameters of reconstruction

Reconstruction of the states in Figs. 5–7 adopts embedding dimension $m_e = 8$ and delay time $\tau_e = 5\tau_s$, which equals 11.9 ps. These embedding parameters are chosen to be consistent with previously reported simulations of optically injected lasers [49,53,54]. However, other choices of the embedding parameters are allowed as long as the reconstructed chaotic attractor is not overwhelmed by false neighboring states [49]. The consideration of false neighbors is among the approaches for choosing the embedding parameters [49,59,76,77]. False neighbors appear as being close to each other only in the reconstructed space. They follow drastically different trajectories that can lead to an unrealistically large TDE slope $\lambda$. So the embedding parameters can be determined by minimizing $\lambda$. In this connection, Fig. 8 plots the result of $\lambda$ as the embedding parameters are varied, where $r$ and $\delta$ are kept unchanged. The simulation is conducted for the laser in chaos without noise for simplicity, while $\lambda$ is evaluated at a very short $k\tau_s$ of 0.02 ns. In Fig. 8(a), the embedding dimension $m_e$ is varied for $\tau_e = 11.9$ ps. At $m_e = 2$, the TDE slope $\lambda$ of 68 ns$^{-1}$ is much overestimated because the reconstructed space certainly lacks the dimensions to describe the original laser state, which comprises of the complex field and carrier density. As $m_e$ increases, $\lambda$ reduces monotonically and approaches a constant value asymptotically. Adopting an excessively large $m_e$ only gives redundantly interdependent dimensions and is thus unnecessary [40,49]. So the choice of $m_e = 8$ in the simulations is acceptable under practical computational considerations. In Fig. 8(b), the embedding delay time $\tau_e$ is varied in steps of $\tau_s = 2.38$ ps for $m_e = 8$. The reconstruction of a state involves samples of $I(t)$ over a time window of $(m_e - 1)\tau_e$. At a small $\tau_e$, $\lambda$ is large because the time window is too small to gather much information other than an instant value of $I(t)$ for each reconstructed state. At a large $\tau_e$, $\lambda$ is also large because the state can undergo considerable evolution during the large time window [40,49]. Minimization of $\lambda$ is possible by optimizing $\tau_e$ to around 11.9 ps, as is chosen for the results in Figs. 5–7.

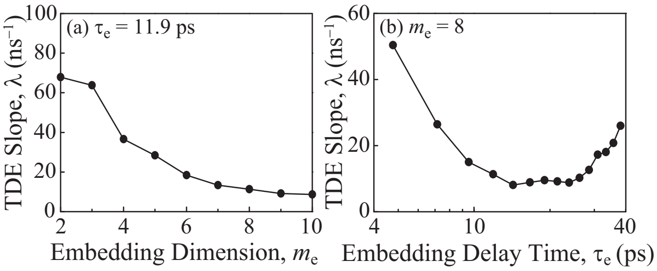

FIG. 8. Numerical TDE slope $\lambda$ for the chaotic dynamics as a function of (a) embedding dimension $m_e$ and (b) embedding delay time $\tau_e$. The slope is evaluated at $k\tau_s = 0.02$ ns. The simulations are conducted without noise.

Summarizing Sec. IV, the estimations of TDEs are enabled by state-space reconstruction with proper embedding parameters when a laser is simulated in chaos. The TDEs for different neighboring states are generally positive, though negative TDEs are found for a small portion of states at very short evolution times. The divergence of states is shown by the positive mean TDE $\Lambda_0(k)$ that increases with the evolution time. Chaotic dynamics always yields a greater $\Lambda_0(k)$ than P1 dynamics, illustrating noise amplification by chaotic mixing for generating randomness.

## V. EXPERIMENTAL RESULTS

Based on the experimental settings in Sec. III B, $I(t)$ is recorded by the oscilloscope in Fig. 1 using its minimal sampling period of $\tau_s = 25$ ps. The experimental reconstruction adopts $m_e = 5$ and $\tau_e = 25$ ps, as any higher multiple of $\tau_s$ cannot yield proper reconstruction in reference to Fig. 8. In the experiments, neighboring states are identified using $r = 0.04$ and $\delta = 20\%$. The inner radius of a shell of neighbors corresponds to about 1.5 mV at the oscilloscope, which has a full range of about 250 mV. The TDEs and Shannon entropies are calculated using Eqs. (1) and (3), respectively, as the evolution time index $k$ varies.

### A. Distribution of experimental TDEs

Figure 9 shows the probability distribution function $p(\Lambda,k)$ of the TDEs estimated by reconstruction using the

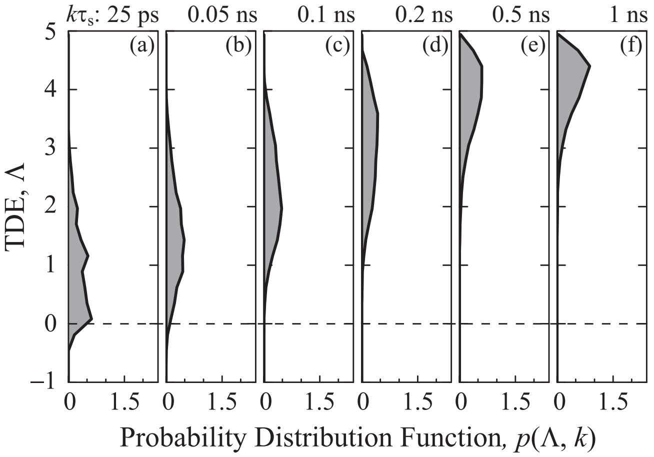

FIG. 9. Experimental probability distribution function $p(\Lambda,k)$ of the TDEs estimated from the reconstructed chaotic attractor. The initially neighboring states evolve over time $k\tau_s$ for $k$ = (a) 1, (b) 2, (c) 4, (d) 8, (e) 20, and (f) 40. The sampling period is $\tau_s = 25$ ps in the experiments.

experimental $I(t)$. In Fig. 9(a), $p(\Lambda,k)$ is shown at the shortest practical evolution time of 25 ps for $k = 1$. The distribution function peaks only at $\Lambda = 0.08$ because the evolution time is relatively short, but the time is already sufficient for some neighbors to diverge with $\Lambda$ spreading beyond 3. In Fig. 9(b), the evolution time increases to about 0.05 ns for $k = 2$. The peak of the distribution function is up-shifted to $\Lambda = 1.4$ when most neighbors continue to diverge. The divergence is attributed to the chaotic dynamics with a positive largest Lyapunov exponent, which amplifies the effect of the noise in the slave laser. However, similarly to the numerical results in Fig. 5(b), the existence of negative TDEs is experimentally unveiled below the dashed line in Figs. 9(a) and 9(b). The negative TDEs correspond to a small portion of neighbors that converge according to negative Lyapunov exponents. The output bits for RBG need to be sampled slower than 0.05 ns for strictly guaranteeing randomness, though some practical randomness tests still allow sampling at a shorter period.

Then, in Fig. 9(c), the evolution time further increases to 0.1 ns for $k = 4$. Most neighboring states diverge and so the TDEs generally increase. In Fig. 9(d), with the increase of the evolution time to 0.2 ns for $k = 8$, the TDEs continue to increase in reaching values beyond 4. Again, similarly to the numerical results in Fig. 5(d), the experimental results in Fig. 9(d) no longer contain negative TDEs. This is because a pair of states cannot be continuously aligned to a converging eigendirection when the evolution time is now sufficiently long. Ultimately, as for Fig. 9(e), the evolution time increases to 0.5 ns for $k = 20$, the general increase of the TDEs is slowed down. The distribution function $p(\Lambda,k)$ becomes invariant as the evolution time increases beyond 1 ns for $k = 40$ in Fig. 9(f), where the peak stays at around $\Lambda = 4.4$. Such an independence of $p(\Lambda,k)$ on $k$ is consistent with the numerical result in Fig. 5(f), which is expected as chaos mixes the states and scatters them according to an invariant probability density on the attractor. The invariant probability density of the states has been theoretically predicted [4] and experimentally verified by resetting a laser to the free-running state periodically [6]. The results in Figs. 9(e) and 9(f) further provide a verification of the invariance of $p(\Lambda,k)$ on large $k$, while all initially neighboring states on the entire reconstructed attractor are considered without resetting the laser. Therefore, in good qualitative agreement with the numerical results in Fig. 5, the experimental results in Fig. 9 illustrate the overall increment of the TDEs with the evolution time, directly verifying the divergence of states for RBG.

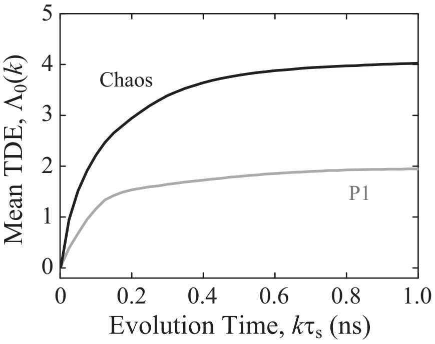

FIG. 10. Experimentally estimated mean TDE $\Lambda_0(k)$ versus evolution time $k\tau_s$. The laser is injected into chaotic dynamics (black) and P1 dynamics (gray).

### B. Evolution of experimental mean TDE

For the ensemble of experimentally reconstructed neighbors, their mean TDE $\Lambda_0(k)$ is again estimated by Eq. (2) using the distribution function $p(\Lambda,k)$. As a function of the evolution time $k\tau_s$, the mean TDE $\Lambda_0(k)$ for the chaotic dynamics is shown by the black curve in Fig. 10. When $k\tau_s$ increases from zero, $\Lambda_0(k)$ also increases from zero as the neighboring states diverge in general. Evaluated at $k\tau_s$ of 0.2 ns, the TDE slope $\lambda = \Lambda_0(k)/(k\tau_s)$ is about 15 ns$^{-1}$, which quantifies the speed of the chaotic mixing and provides an estimation of the largest Lyapunov exponent in the experiments [49,51]. When $k\tau_s$ continues to increase up to 1 ns, $\Lambda_0(k)$ increases and reaches a saturated value of about 4, as $p(\Lambda,k)$ becomes increasingly invariant according to Fig. 9. In good qualitative agreement with the numerical results in Fig. 6, the quick increase of the mean TDE from the experiments in Fig. 10 verifies the fast divergence of states by chaos.

Along with the dynamics, the experiments as detailed in Fig. 1 inevitably contain noise from the detection electronics, injection, and spontaneous emission in the slave laser, which corresponds to its free-running optical linewidth on the order of 10 MHz. The fast increment of $\Lambda_0(k)$, as shown by the black curve in Fig. 10, is actually contributed by both chaos and noise. In order to observe the effect of noise without chaos, the gray curve in Fig. 10 is obtained by driving the slave laser into P1 dynamics. The P1 dynamics is obtained simply by changing the injection power to 1.6 mW, causing the laser emission intensity to oscillate at 9 GHz periodically instead of chaotically, while keeping nearly the same oscillation amplitude [70]. Noise is manifested as amplitude and phase fluctuations of the intensity oscillation, resulting in the increase of $\Lambda_0(k)$ over time. However, by comparing the two curves in

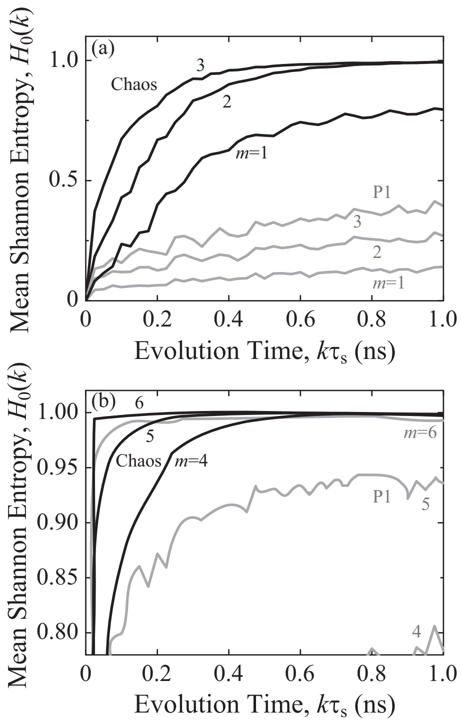

FIG. 11. Mean Shannon entropy $H_0(k)$ versus evolution time $k\tau_s$ estimated from experimental state-space reconstruction. The laser is injected into chaotic dynamics (black) and P1 dynamics (gray). The entropy is calculated for the $m$th MSB $B_m$ from the ADC for $m =$ (a) 1 to 3 and (b) 4 to 6.

Fig. 10, $\Lambda_0(k)$ is much greater for the chaotic dynamics than for the P1 dynamics. It merely increases slowly for the P1 dynamics and does not reach the saturated value even after evolving for over 50 ns.

In short, from Figs. 9 and 10, the experimental reconstruction verifies the role of chaos in attaining a large positive $\Lambda_0(k)$ over a short time, which implies the divergence of states for providing entropy in RBG.

### C. Evolution of Shannon entropy

According to the RBG scheme in Fig. 1, the state of the slave laser determines the intensity $I(t)$. The intensity is discretized by the ADC of 8-bit resolution. Only the $m$th MSB from the ADC, denoted by $B_\mathrm{m}(t)$, is selected. As an initial state evolves, the value of $B_m$ becomes increasingly unpredictable. The uncertainty can be quantified by the Shannon entropy that is associated with the initial state. Averaged over different initial states in the experiments, the mean Shannon entropy $H_0(k)$ of the bit $B_m$ as a function of the evolution time is plotted in Fig. 11.

Figure 11 is obtained through tracing different evolutions of different initial states in the experiments following the procedure in Sec. II. For an initial state $\boldsymbol{x}_i$, a group of 500 neighboring states $\boldsymbol{x}_j$ are identified with initial distances $d_{ij}(0)$ falling within $r$ and $(1+\delta)r$. Basically, these nearly identical neighbors initially give the same value of $B_m$, though they eventually diverge according to their positive TDEs in giving different values of $B_m$. Within the group of the 500 initially neighboring states, the proportion of states having $B_m = 1$ approximates the probability $P_i(1,k)$, whereas the proportion of $B_m = 0$ approximates $P_i(0,k)$ at evolution time $k\tau_\mathrm{s}$. Then, using Eq. (3), the Shannon entropy $H_i(k)$ of bit $B_m$ associated with the one initial state $\boldsymbol{x}_i$ is estimated. Subsequently, in order to cover the reconstructed space, 500 initial states $\boldsymbol{x}_i$ are considered, where the corresponding values of $H_i(k)$ are averaged to the mean Shannon entropy $H_0(k)$ as Fig. 11 shows. Based on the entire reconstructed attractor, the nonzero $H_0(k)$ observed in Fig. 11 illustrates the continuously generated randomness through semiconductor laser dynamics and fundamentally implies the possibility of RBG that is not deterministic.

In Figs. 11(a) and 11(b), the mean Shannon entropy $H_0(k)$ is shown for the bit $B_m$ at $m = 1$ to 3 and 4 to 6, respectively. The black curves are obtained when the laser is injected into chaos. The chaotic mixing of states always causes $H_0(k)$ to quickly increase with $k\tau_\mathrm{s}$ and saturate at unity for maximal randomness. The saturation of $H_0(k)$ normally requires much less than 1 ns, as consistent with the behavior of $\Lambda_0(k)$ in Fig. 10. Increasing the evolution time from zero allows complete mixing of the laser states by the chaotic dynamics. The laser intensity becomes uncorrelated with its initial value according to Fig. 3(b). The intensity ultimately follows the steady-state probability density function in Fig. 2(b), which corresponds to the asymptotic $H_0(k)$ for large $k$ [5,14,78]. Also, as $m$ increases, the black curves in Fig. 11 shows a progressive increment of $H_0(k)$. At $m = 1$ in Fig. 11(a), the entropy is measured for the MSB that is least sensitive to changes of states. So $H_0(k)$ is the lowest for $m = 1$. At $m = 6$ in Fig. 11(b), the bit has a much higher sensitivity to the states and so contains the highest $H_0(k)$, which reaches above 0.995 within an evolution time of merely 25 ps. The increase of entropy by increasing $m$ is consistent with some experiments that realized spectral broadening and scrambling by discarding a number of MSBs in RBG [14,21,33]. Besides, for comparison, the gray curves in Fig. 11 are obtained when the laser is injected into the P1 dynamics. Although experimental noise enables the generation of entropy, the P1 dynamics is periodic in providing no fast mixing of states. Its entropy is always less than that of the chaotic dynamics at any given $m$. Therefore, given the same strength of noise, the experiments illustrate the effectiveness of chaotic dynamics for continuously generating Shannon entropies for RBG.

Summarizing Sec. V, the experimental state-space reconstruction is used for evaluating the randomness associated with the laser in chaos. The diverging chaotic trajectories are observed by estimating the positive mean TDE $\Lambda_0(k)$ that increases with the evolution time $k\tau_\mathrm{s}$. The mean TDE is observed to increase more quickly for chaotic dynamics than for P1 dynamics. The Shannon entropy $H_0(k)$ estimated from the reconstructed states is observed to be continuously generated over time for enabling RBG.

## VI. DISCUSSIONS

Based on the state-space reconstruction, the continuous generation of entropy is verified in Fig. 11. This implies the possibility of RBG passing practical randomness tests such as those stipulated by NIST Special Publication 800-22 [31,33].

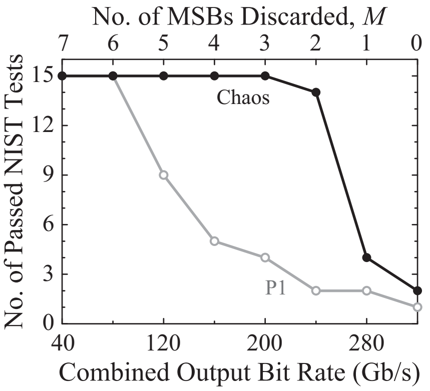

FIG. 12. Number of passes in the 15 NIST tests versus the combined output bit rate. The combined output consists of bits $B'_m(t)$ for $m = M + 1$ to 8, while $M$ MSBs are discarded. The sampling period is $\tau_s = 25$ ps.

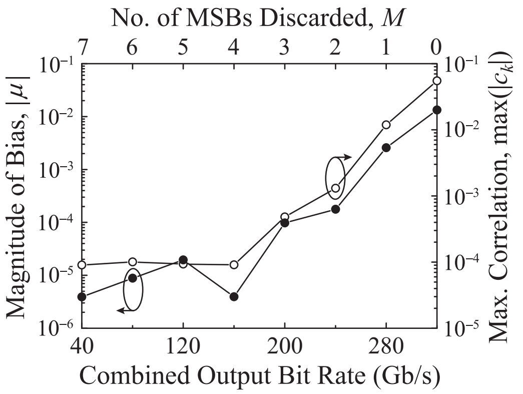

FIG. 13. Magnitude of bias $|\mu|$ and maximum correlation $\max(|c_k|)$ of the output bit stream versus the combined output bit rate. The length of the output bit stream is $10^9$ for the calculation.

The procedure of RBG starts from the detection of the intensity signal $I(t)$ in Fig. 1. The signal is discretized by the ADC into 8 digital channels that correspond to the most significant to the least significant bit, where only the single channel of the $m$th MSB is selected in Fig. 1 for $m = 1, 2, \ldots,$ or 8. The channel gives the bit stream $B_{\mathrm{m}}(t)$, which is subsequently processed through an XOR operation with its 1-ns delayed replica into the output bit stream $B'_m(t)$. Such a delayed XOR operation in Fig. 1 is a standard procedure to suppress any bias of the bits [31,32,62].

Although Fig. 1 shows only one channel of $B'_m(t)$ for a single value of $m$, multiple channels for different values of $m$ can be aggregated for boosting the output bit rate [19,32]. In fact, RBG in Fig. 12 adopts a direct way of sequentially aggregating $B'_m$ with $m = M + 1$ to 8 into a combined output bit stream [26,30], where the channels of $m = 1$ to $M$ are ignored. Here, $M$ denotes the number of MSBs discarded so that the combined output bit rate is $(8 - M)/\tau_s$ for $\tau_s = 25$ ps. Such a discarding of MSBs is commonly employed in RBG [14,21,33]. The discarding of bits of small $m$ is useful for RBG because they have small entropies, as Fig. 11 shows.

Figure 12 shows the results of the 15 standard NIST tests for the combined output bit stream for different choices of $M$. The NIST tests examine the combined output bit streams in batches of 1000 sets of $10^6$ consecutive bits at a significance level of 0.01 [31,33]. For chaotic dynamics, all the 15 tests are passed as long as $M$ is at least 3, which corresponds to a combined output bit rate of 200 Gb/s. By contrast, for P1 dynamics, the combined output can only pass the tests when $M$ is at least 6, which corresponds to retaining only 2 least significant bits. Hence, consistent with the evaluation of TDEs and entropies in Figs. 10 and 11, chaotic dynamics is certainly preferred over P1 dynamics for high-speed generation of random bits.

Besides the standard NIST tests, the output bit stream can also be statistically examined by calculating the bias of the bits $\mu$ and the correlation coefficient $c_k$ as a function of a lag $k$ of the bits [23]. Figure 13 summarizes the results calculated when keeping the length of the output bit stream at $L = 10^9$, where the ideal statistical standard deviations for $\mu$ and $c_k$ are $\sigma_\mu = 0.5/\sqrt{L}$ and $\sigma_c = 1/\sqrt{L}$, respectively [23]. The combined output bit rate is varied in Fig. 13 by varying $M$, as in Fig. 12. The closed symbols in Fig. 13 show the magnitude of bias $|\mu|$, which increases with the combined output bit rate. The magnitude of bias is less than $3\sigma_\mu = 4.7 \times 10^{-5}$ for $M \geqslant 4$, while it marginally exceeds $3\sigma_\mu$ at $M = 3$. The open symbols in Fig. 13 plot the maximum correlation coefficient, which is denoted by $\max(|c_k|)$ as obtained from amongst the correlation coefficients $c_k$ for lag $k$ covering 1 to 300. The maximum correlation coefficient is less than $3\sigma_c = 9.5 \times 10^{-5}$ for $M \geqslant 4$, while it marginally exceeds $3\sigma_c$ at $M = 3$. Such comparisons with three times the standard deviations are often empirically considered as a set of more stringent criteria beside the NIST tests [23,79,80]. In other words, for fulfilling the criteria in addition to the NIST tests, Fig. 13 illustrates that $M$ can be simply increased from 3 to 4, which is equivalent to reducing the combined output bit rate from 200 Gb/s to 160 Gb/s in practice.

Though these practical tests provide a practical quantification of randomness, the Shannon entropies and TDEs estimated from the state-space reconstruction offer a more fundamental evaluation of the randomness for the chaotic laser. The entropy $H_0(k)$ in Fig. 11 quantifies the unpredictability of output bits based on the information of the initial states rather than merely the information of the previous output bits, as in most practical randomness test suites [31,33]. Besides, the entropy $H_0(k)$ is based on a set of initial states rather than only one free-running initial state [6], thereby illustrating the continuous generation of randomness by laser chaos. In addition, the experimental estimation of the entropy and TDEs complements some related works based on simulations [4,5,14,24,28]. Thus, the reconstruction provides a fundamental and experimental confirmation of the continuously generated randomness in the chaotic laser for RBG.

## VII. CONCLUSION

In summary, state-space reconstruction is investigated for evaluating the randomness generated by an optically injected chaotic semiconductor laser. The TDEs are first estimated to quantify the divergence of neighboring states due to chaotic mixing, in which the experimental and numerical results are of good qualitative agreement. The mean TDE $\Lambda_0(k)$ of the entire attractor is found to be positive as it increases with the evolution time $k\tau_s$, while the existence of negative TDEs is unveiled at short $k\tau_s$. Moreover, $\Lambda_0(k)$ for chaotic dynamics is confirmed to be always greater than that for P1 dynamics, illustrating the effect of noise amplification by chaotic mixing of the states. Furthermore, the mean Shannon entropy $H_0(k)$ that quantifies the unpredictability of the output bits is estimated experimentally, where different states of the entire attractor are considered. While RBG at a combined bit rate reaching 200 Gb/s is verified by the practical NIST tests, the continuous generation of the Shannon entropy is fundamentally and experimentally verified by the reconstruction. Based on reconstruction, the approach of randomness evaluation using the TDEs and entropies is readily extended for different chaotic RBG experiments.

## ACKNOWLEDGMENTS

The work described in this paper was fully supported by two grants from the Research Grants Council of Hong Kong, China (Projects No. CityU 111213 and No. CityU 11201014).

[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. Photon. **2**, 728 (2008).

[2] M. Sciamanna and K. Shore, Nat. Photon. **9**, 151 (2015).

[3] M. C. Soriano, J. Garcia-Ojalvo, C. R. Mirasso, and I. Fischer, Rev. Modern Phys. **85**, 421 (2013).

[4] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K.-i. Arai, A. Uchida, and P. Davis, Phys. Rev. E **85**, 046215 (2012).

[5] T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K.-i. Arai, K. Yoshimura, and P. Davis, Phys. Rev. E **85**, 016211 (2012).

[6] S. Sunada, T. Harayama, P. Davis, K. Tsuzuki, K. Arai, K. Yoshimura, and A. Uchida, Chaos **22**, 047513 (2012).

[7] T. Durt, C. Belmonte, L. P. Lamoureux, K. Panajotov, F. Van den Berghe, and H. Thienpont, Phys. Rev. A **87**, 022339 (2013).

[8] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, Phys. Rev. Lett. **108**, 070602 (2012).

[9] K. Kanno and A. Uchida, Phys. Rev. E **86**, 066202 (2012).

[10] T. Butler, C. Durkan, D. Goulding, S. Slepneva, B. Kelleher, S. P. Hegarty, and G. Huyet, Opt. Lett. **41**, 388 (2016).

[11] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, J. Lightwave Technol. **30**, 1329 (2012).

[12] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).

[13] X. Wang, X. Z. Li, S. C. Chan, and K. K. Y. Wong, Opt. Lett. **40**, 2665 (2015).

[14] X. Fang, B. Wetzel, J.-M. Merolla, J. M. Dudley, L. Larger, C. Guyeux, and J. M. Bahi, IEEE Trans. Circuits Syst. I, Reg. Papers **61**, 888 (2014).

[15] B. Wetzel, K. J. Blow, S. K. Turitsyn, G. Millot, L. Larger, and J. M. Dudley, Opt. Express **20**, 11143 (2012).

[16] A. M. Hagerstrom, T. E. Murphy, and R. Roy, Proc. Natl. Acad. Sci. USA **112**, 9258 (2015).

[17] N. Oliver, T. Jungling, and I. Fischer, Phys. Rev. Lett. **114**, 123902 (2015).

[18] T. E. Murphy, A. B. Cohen, B. Ravoori, K. R. B. Schmitt, A. V. Setty, F. Sorrentino, C. R. S. Williams, E. Ott, and R. Roy, Phil. Trans. R. Soc. A **368**, 343 (2010).

[19] T. Yamazaki and A. Uchida, IEEE J. Select. Topics Quantum Electron. **19**, 0600309 (2013).

[20] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).

[21] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, IEEE J. Quantum Electron. **49**, 910 (2013).

[22] X. Tang, Z. M. Wu, J. G. Wu, T. Deng, J. J. Chen, L. Fan, Z. Q. Zhong, and G. Q. Xia, Opt. Express **23**, 33130 (2015).

[23] N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, Opt. Express **22**, 6634 (2014).

[24] A. Wang, B. Wang, L. Li, Y. Wang, and K. A. Shore, IEEE J. Select. Topics Quantum Electron. **21**, 531 (2015).

[25] R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, Opt. Express **20**, 28603 (2012).

[26] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express **18**, 18763 (2010).

[27] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Phys. Rev. A **83**, 031803 (2011).

[28] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, Opt. Express **22**, 17271 (2014).

[29] A. Argyris, E. Pikasis, and D. Syvridis, Proc. SPIE **9773**, 97730K (2016).

[30] X. Z. Li and S. C. Chan, Opt. Lett. **37**, 2163 (2012).

[31] X. Z. Li and S. C. Chan, IEEE J. Quantum Electron. **49**, 829 (2013).

[32] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, Opt. Express **23**, 1470 (2015).

[33] X. Z. Li, S. S. Li, J. P. Zhuang, and S. C. Chan, Opt. Lett. **40**, 3970 (2015).

[34] M. Virte, K. Panajotov, H. Thienpont, and M. Sciamanna, Nat. Photon. **7**, 60 (2013).

[35] F. Arnault and T. P. Berger, IEEE Trans. Comput. **54**, 1374 (2005).

[36] K. Kanno, A. Uchida, and M. Bunsen, Phys. Rev. E **93**, 032206 (2016).

[37] S. Heiligenthal, T. Jungling, O. D'Huys, D. A. Arroyo-Almanza, M. C. Soriano, I. Fischer, I. Kanter, and W. Kinzel, Phys. Rev. E **88**, 012902 (2013).

[38] K. E. Chlouverakis and M. J. Adams, Opt. Commun. **216**, 405 (2003).

[39] T. Fordell and A. M. Lindberg, Opt. Commun. **242**, 613 (2004).

[40] T. Jungling, M. C. Soriano, and I. Fischer, Phys. Rev. E **91**, 062908 (2015).

[41] D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, Opt. Lett. **32**, 2960 (2007).

[42] S. S. Li and S. C. Chan, IEEE J. Sel. Topics Quantum Electron. **21**, 1800812 (2015).

[43] L. Jumpertz, K. Schires, M. Carras, M. Sciamanna, and F. Grillot, Light Sci. Appl. **5**, e16088 (2016).

[44] X. Z. Li, S. S. Li, J. P. Zhuang, J. B. Gao, and S. C. Chan, in *Frontiers in Optics*, OSA Technical Digest (OSA, 2015), paper FTh2G.4.

[45] 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).

[46] M. Sano and Y. Sawada, Phys. Rev. Lett. **55**, 1082 (1985).

[47] J. P. Eckmann, S. O. Kamphorst, D. Ruelle, and S. Ciliberto, Phys. Rev. A **34**, 4971 (1986).

[48] M. T. Rosenstein, J. J. Collins, and C. J. De Luca, Physica D **65**, 117 (1993).

[49] J. Gao and Z. Zheng, Phys. Rev. E **49**, 3807 (1994).

[50] J. B. Gao, S. K. Hwang, and J. M. Liu, Phys. Rev. Lett. **82**, 1132 (1999).

[51] M. Franchi and L. Ricci, Phys. Rev. E **90**, 062920 (2014).

[52] T. B. Simpson, J. M. Liu, A. Gavrielides, V. Kovanis, and P. M. Alsing, Phys. Rev. A **51**, 4181 (1995).

[53] S. K. Hwang, J. B. Gao, and J. M. Liu, Phys. Rev. E **61**, 5162 (2000).

[54] J. B. Gao, S. K. Hwang, and J. M. Liu, Phys. Rev. A **59**, 1582 (1999).

[55] K. Kanno and A. Uchida, Phys. Rev. E **89**, 032918 (2014).

[56] S. Sato, M. Sano, and Y. Sawada, Prog. Theor. Phys. **77**, 1 (1987).

[57] M. Alvaro, M. Carretero, and L. L. Bonilla, Europhys. Lett. **107**, 37002 (2014).

[58] J. B. Gao, J. Hu, W. W. Tung, and Y. H. Cao, Phys. Rev. E **74**, 066204 (2006).

[59] J. B. Gao, Y. H. Cao, W. W. Tung, and J. Hu, *Multiscale Analysis of Complex Time Series: Integration of Chaos and Random Fractal Theory, and Beyond* (Wiley, New York, 2007).

[60] J. B. Gao, J. Hu, W. W. Tung, and E. Blasch, Front. Physiol. **2**, 13 (2012).

[61] T. B. Simpson, J.-M. Liu, M. AlMulla, N. G. Usechak, and V. Kovanis, Phys. Rev. Lett. **112**, 023901 (2014).

[62] D. P. Rosin, D. Rontani, and D. J. Gauthier, Phys. Rev. E **87**, 040902 (2013).

[63] S. C. Chan, IEEE J. Quantum Electron. **46**, 421 (2010).

[64] J. P. Zhuang and S. C. Chan, Opt. Express **23**, 2777 (2015).

[65] S. K. Hwang, J. M. Liu, and J. K. White, IEEE Photon. Technol. Lett. **16**, 972 (2004).

[66] T. B. Simpson, J. M. Liu, K. F. Huang, and K. Tai, Quantum Semiclass. Opt. **9**, 765 (1997).

[67] C. H. Henry, J. Lightwave Technol. **4**, 298 (1986).

[68] T. B. Simpson and J. M. Liu, Opt. Commun. **112**, 43 (1994).

[69] J. M. Liu, H. F. Chen, X. J. Meng, and T. B. Simpson, IEEE Photon. Technol. Lett. **9**, 1325 (1997).

[70] J. P. Zhuang and S. C. Chan, Opt. Lett. **38**, 344 (2013).

[71] F. Y. Lin, Y. K. Chao, and T. C. Wu, IEEE J. Quantum Electron. **48**, 1010 (2012).

[72] M. Pochet, N. A. Naderi, N. Terry, V. Kovanis, and L. F. Lester, Opt. Express **17**, 20623 (2009).

[73] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, Physica D **16**, 285 (1985).

[74] J. P. Eckmann and D. Ruelle, Rev. Mod. Phys. **57**, 617 (1985).

[75] M. Inubushi, K. Yoshimura, and P. Davis, Phys. Rev. E **91**, 022918 (2015).

[76] A. M. Albano, J. Muench, C. Schwartz, A. I. Mees, and P. E. Rapp, Phys. Rev. A **38**, 3017 (1988).

[77] C. J. Cellucci, A. M. Albano, and P. E. Rapp, Phys. Rev. E **67**, 066210 (2003).

[78] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, J. Lightwave Technol. **33**, 2855 (2015).

[79] V. N. Chizhevsky, Phys. Rev. E **82**, 050101 (2010).

[80] W. Wei, G. D. Xie, A. H. Dang, and H. Guo, IEEE Photon. Technol. Lett. **24**, 437 (2012).