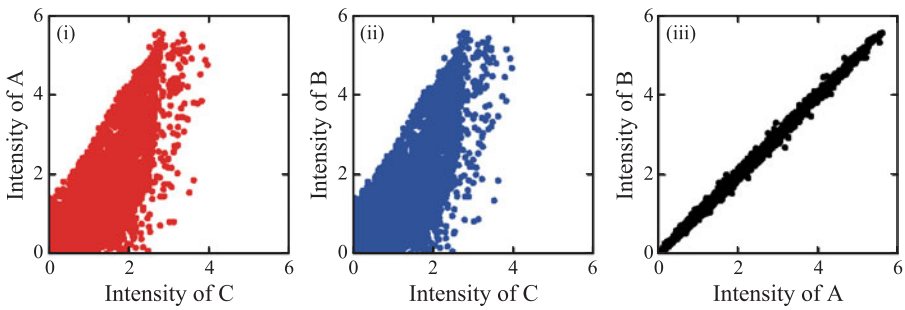
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Correlated Random Bit Generation Using Chaotic Semiconductor Lasers Under Unidirectional Optical Injection

Volume 9, Number 5, October 2017

Xiao-Zhou Li
Song-Sui Li
Sze-Chun Chan, ***Senior Member, IEEE***



DOI: 10.1109/JPHOT.2017.2748978
1943-0655

Correlated Random Bit Generation Using Chaotic Semiconductor Lasers Under Unidirectional Optical Injection

Xiao-Zhou Li,[1] **Song-Sui Li,**[1]
and Sze-Chun Chan,[1,2] ***Senior Member, IEEE***

[1]Department of Electronic Engineering, City University of Hong Kong, Hong Kong
[2]State Key Laboratory of Millimeter Waves, City University of Hong Kong, Hong Kong

DOI:10.1109/JPHOT.2017.2748978

Manuscript received July 16, 2017; revised August 26, 2017; accepted August 31, 2017. Date of publication September 4, 2017; date of current version September 19, 2017. This work was supported by the Grants from the Research Grants Council of Hong Kong, China, under Projects CityU 11260916 and T42-103/16-N. Corresponding author: Sze-Chun Chan (e-mail: scchan@cityu.edu.hk).

Abstract: Correlated random bit generation is investigated using three optically injected chaotic semiconductor lasers. Based on a rate-equation model, a continuous-wave injection first perturbs a common laser into chaos. The common laser then optically injects a pair of response lasers through a public channel unidirectionally. The two response lasers of identical parameters are synchronized. Their chaotic emissions are digitized in yielding correlated random bit streams. As the scheme advantageously involves no feedback loops, the output bits contain no undesirable time-delay information artifacts. Security is ensured as the response lasers produce bits that cannot be extracted using the information in the public channel alone. Output bit streams are generated at a tunable rate of up to about 2 Gbps with randomness verified by a test suite of the National Institute of Standards and Technology. The streams are correlated with a low bit error ratio of less than 4%, which is sensitive to parameter mismatch between the response lasers.

Index Terms: Semiconductor lasers, injection-locked lasers, random bit generation, chaos.

1. Introduction

Secure key distribution between two parties relies on the extraction of correlated information [1]–[9]. Generation of correlated waveforms is possible using synchronized chaotic semiconductor lasers, as they provide wide signal bandwidths for high raw bit rates in key extraction [10]–[14]. Chaos synchronization of two communicating lasers A and B has been achieved through bidirectional coupling in various forms [15]–[23], where the two lasers can be individually perturbed by feedback [16]–[18], the coupling can be realized indirectly through a third laser [20]–[22], and an additional coupling can be applied using a common drive [23]. Bidirectional coupling over a public channel risks exposure of the information of lasers A and B, though the information is usually well hidden by chaotic dynamics.

Alternatively, to completely eliminate the possibility of exposing lasers A and B, unidirectional coupling from a common source has also been devised for chaos synchronization of the two lasers. The consistency of the responses of the two lasers enables the synchronized emission [24]–[27]. The lasers A and B can be simply injected by the common source without additional perturbation [28]–[30], but it can also be subject to self-feedback and with cascaded injection for yielding an increased complexity [3], [6], [31]. The common source can be realized using amplified

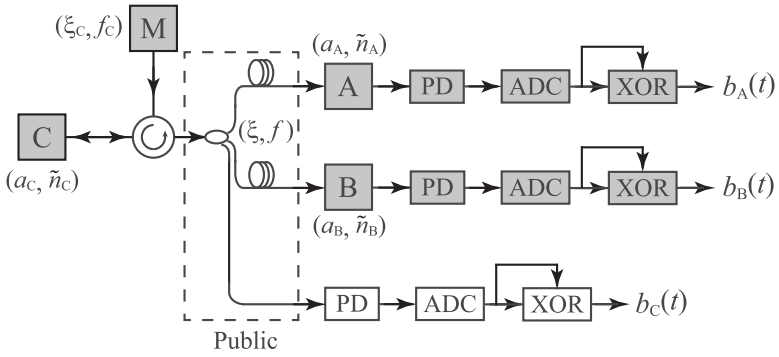


Fig. 1. Schematic of CRBG using semiconductor lasers under unidirectional optical injection. M, master laser; C, common laser; A and B, response lasers; PD, photodetector; ADC, analogue-to-digital converter; XOR, exclusive-or.

spontaneous emission noise or randomly phase-modulated laser light [2], [3], [24], [25]. White noise sources have to be sufficiently strong for inducing synchronization of the chaotic dynamics of lasers A and B, though interesting experimental results have been reported [31].

Recently, the common source was realized by a chaotic laser subject to optical feedback for synchronizing the response lasers [32]–[36]. The common semiconductor laser is driven into chaos by the optical feedback. The response lasers A and B are also in chaos and are synchronized, although their waveforms are significantly different from that of the common laser. Correlated random bit generation (CRBG) was further demonstrated for key distribution by digitizing the chaotic waveforms of the response lasers [2], [3]. However, as the common laser was subject to optical feedback, its waveform inevitably contains residual autocorrelation that reveals the information of the feedback round-trip time [37]–[39]. The residual correlation can also be observed in the injected response lasers as inherited from the common laser under feedback [29], [40]. Such a residual correlation corresponds to artifacts in the random bits, which would in principle impose limitations on the tunability of the output bit rate in CRBG [41], [42]. Although the injection parameters can be optimized for minimizing the residuals, they cannot be simultaneously optimized for maximizing the correlation of the output bits. The elimination of all feedback loops becomes an interesting possibility for CRBG.

In this paper, CRBG is investigated using only unidirectional optical injection of semiconductor lasers based on a rate-equation model. The common laser is first driven into chaos by a continuous-wave (CW) optical injection. The common laser then unidirectionally injects the two response lasers A and B over a public channel. The chaotic emission waveforms from the response lasers are independently digitized into random bit streams, which are correlated when the response lasers are synchronized. Due to the absence of optical feedback, the chaotic waveforms contain no time-delay information, so the randomness of the output bits is sustained over a continuously tunable output bit rate. CRBG with a tunable output bit rate reaching 2 Gbps is shown with randomness verified by a test suite of the National Institute of Standards and Technology (NIST). The correlated random bit streams has a bit error ratio of less than 4% that is sensitive to the parameter mismatch between the two response lasers. Security is also verified as the response lasers share nearly no mutual information with the injection light in the public channel.

2. Setup

Fig. 1 shows the schematic for CRBG using semiconductor lasers under unidirectional optical injection. A total of four single-mode semiconductor lasers are considered. First, through an optical circulator in Fig. 1, a CW master laser M injects a common laser C into chaotic dynamics [42]. The injection into laser C is specified by a normalized strength ξ_C and a detuning frequency f_C. The injection strength ξ_C is proportional to the injection field amplitude. The detuning frequency

f_C is the frequency difference of the master laser M from the free-running optical frequency of the common laser C. Then, the chaotic emission of C is split by a 3-dB coupler into two fiber paths for unidirectional injection into two response lasers A and B. The fibers are in the public domain with a possibility of being tapped by an eavesdropper, but the two response lasers scramble the injected light by their nonlinear dynamics which the eavesdropper cannot access. The response lasers are each subject to the chaotic injection of strength ξ. They are operated at the same free-running optical frequency. So the free-running frequency of the common laser C with respect to that of the response lasers A and B is denoted by one detuning frequency f. As a result of the common injection from C, the response lasers A and B emit chaotically in synchrony. Each of the reponse lasers is detected by a photodetector (PD) that is followed by an electronic analogue-to-digital converter (ADC) of 1-bit resolution and of a sampling rate f_s, where an exclusive-or (XOR) operation is subsequently applied after a delay line for suppressing bias [40]. Thus, using identical postprocessing after the PDs, the synchronized response lasers A and B generate correlated output bit streams $b_A(t)$ and $b_B(t)$, respectively.

Numerically, the dynamics of the common laser C in Fig. 1 is described by the normalized complex intracavity field amplitude $a_C(t)$ and charge carrier density $\tilde{n}_C(t)$. The dynamics for the two response lasers A and B in Fig. 1 are described by their normalized fields $a_A(t)$ and $a_B(t)$, which are associated with charge carrier densities $\tilde{n}_A(t)$ and $\tilde{n}_B(t)$, respectively. The rate equations for the common laser C are [43]–[46]:

$$\frac{da_C}{dt} = \frac{1-ib}{2}\left[\frac{\gamma_c\gamma_n}{\gamma_s J}\tilde{n}_C - \gamma_p(|a_C|^2-1)\right]a_C + \xi_C\gamma_c \exp(-i2\pi f_C t) + F_C, \quad (1)$$

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

where the Langevin noise term $F_C(t)$ represents the spontaneous emission noise within laser C [47]. The term with ξ_C in (1) represents the optical injection from the CW master laser M into the common laser C at a detuning frequency of f_C. Similarly, the rate equations for the response lasers A and B are [30], [33]:

$$\frac{da_{A,B}}{dt} = \frac{1-ib}{2}\left[\frac{\gamma_c\gamma_n}{\gamma_s J}\tilde{n}_{A,B} - \gamma_p(|a_{A,B}|^2-1)\right]a_{A,B} + \xi\gamma_c a_C(t)\exp(-i2\pi f t) + F_{A,B}, \quad (3)$$

$$\frac{d\tilde{n}_{A,B}}{dt} = -(\gamma_s + \gamma_n|a_{A,B}|^2)\tilde{n}_{A,B} - \gamma_s J\left(1-\frac{\gamma_p}{\gamma_c}|a_{A,B}|^2\right)(|a_{A,B}|^2-1). \quad (4)$$

Although (a_A, $\tilde{n}_A$) and (a_B, $\tilde{n}_B$) obey the same (3) and (4), they are stochastically under the influences of different Langevin noise $F_A(t)$ and $F_B(t)$ originating independently within A and B. Synchronization of A and B is possible because of the term with a_C in (3) for the common injection from C [30], [33]. For simplicity, except when mismatches are introduced, all injected lasers in Fig. 1 are modeled using a typical set of dynamical parameters [45]: cavity decay rate $\gamma_c = 5.36 \times 10^{11}\,s^{-1}$, spontaneous carrier relaxation rate $\gamma_s = 5.96 \times 10^{9}\,s^{-1}$, differential carrier relaxation rate $\gamma_n = 7.53 \times 10^{9}\,s^{-1}$, nonlinear carrier relaxation rate $\gamma_p = 1.91 \times 10^{10}\,s^{-1}$, linewidth enhancement factor $b = 3.2$, and normalized bias current above threshold $J = 1.222$. The corresponding relaxation resonance frequency is 10.25 GHz for all of the injected lasers. The Langevin terms F_C, F_A, and F_B have the same strength that corresponds to a 10-MHz free-running linewidth for each laser [42]. Second-order Runge-Kutta integrations are conducted on (1)–(4) with a time step of 2.38 ps and a time

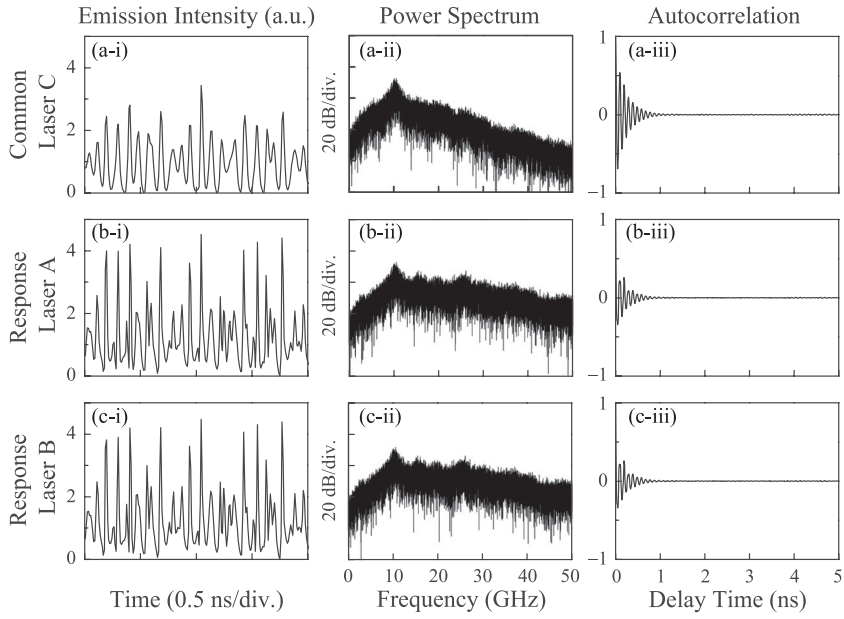


Fig. 2. Chaotic emission (i) intensity time series, (ii) power spectra, and (iii) intensity autocorrelation functions for (a) common laser C, (b) response laser A, and (c) response laser B.

span of 60 μs in yielding normalized emission intensities $|a_C(t)|^2$, $|a_A(t)|^2$, and $|a_B(t)|^2$ for the lasers C, A, and B, respectively.

3. Results

Fig. 2(i) shows the emission intensity time series of the common laser C and the response lasers A and B. The intensity time series can be Fourier-transformed into the power spectra in Fig. 2(ii). Their autocorrelation functions are shown in Fig. 2(iii). The injection parameters from the master laser M into the common laser C are fixed at $(\xi_C, f_C) = (0.05, 6.26\ \text{GHz})$. Such CW injection is sufficient to drive the common laser C into chaotic dynamics, yielding the quickly varying irregular intensity $|a_C(t)|^2$ in Fig. 2(a-i). The corresponding power spectra in Fig. 2(a-ii) is broadband with a peak at around the relaxation resonance frequency of 10.25 GHz for laser C, where the effective chaotic bandwidth is about 7 GHz [48]. The autocorrelation function for the time series $|a_C(t)|^2$ is shown in Fig. 2(a-iii). Interestingly, as the delay time increases from zero, the amplitude of the autocorrelation function rapidly diminishes. There is no residual peaks because the chaotic intensity waveform never repeats, which is attributed to the absence of time-delayed feedback loops in Fig. 1 [49]. Therefore, by using an optically injected common laser, undesired time-delay information is totally absent in the response lasers.

The chaotic emission from the common laser C is then optically injected into the two response lasers A and B, as Fig. 1 indicates, where a common set of injection parameters $(\xi, f) = (0.2, -5\ \text{GHz})$ is adopted. The chaotic injection forces the response lasers into emitting the erratic intensity time series $|a_A(t)|^2$ and $|a_B(t)|^2$ in Figs. 2(b-i) and 2(c-i), respectively. The emission intensity time series of A and B are nearly identical. This is because of the synchrony induced in the two lasers by the common injection from C. However, the emission from A and B in Figs. 2(b-i) and 2(c-i) are different from the emission of C in Fig. 2(a-i) because lasers A and B provide nonlinear dynamical scrambling of the waveform. The power spectra in Figs. 2(b-ii) and 2(c-ii) for the emission from A and B again peak at around the relaxation resonance frequency of 10.25 GHz, but they have a much greater effective bandwidth of 18 GHz due to the bandwidth enhancement by the chaotic optical injection [50], [51]. Thus, the intensity time series for A and B fluctuate more quickly as

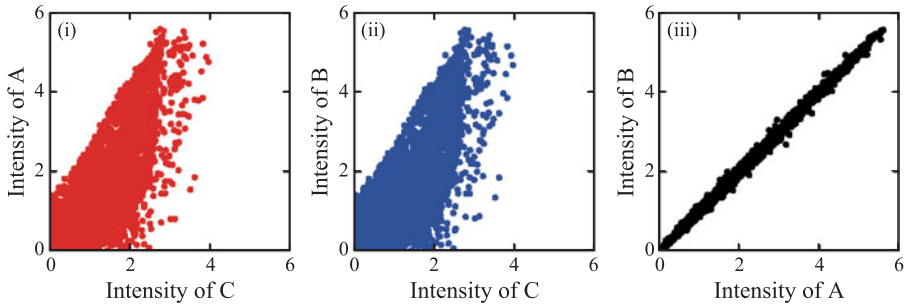


Fig. 3. Correlation plots of the emission intensities from lasers (i) (C, A), (ii) (C, B), and (iii) (A, B).

compare to that for C. The corresponding autocorrelation functions for A and B in Figs. 2(b-iii) and 2(c-iii) again diminish quickly in amplitude, allowing the generation of random bits on the order of Gbps [13]. The time for diminishing is dependent on the relaxation resonance frequency, which can be further increased by increasing the laser bias current. Moreover, no residual peaks are observed due to the absence of time-delayed feedback loops in Fig. 1 [49]. The lack of such time-delay information artifact in the response lasers implies randomness irrespective of the sampling rate f_s of the ADCs [41]. Therefore, CRBG with continuous tunability of the bit rate is enabled by using the optically injected common laser.

To examine the quality of chaos synchronization of lasers A and B through the common injection from C, Fig. 3 shows the correlation plots of the emission intensities, which are sampled every 2.38 ps over a duration of about 0.1 μs. Fig. 3(i) plots $|a_C(t)|^2$ against $|a_A(t)|^2$. The data points are quite scattered because of the nonlinear dynamics of A. The injection from C perturbs A, rather than locking A, so that the cross-correlation coefficient between their emission intensities is only about 0.82 [41]. A weaker cross-correlation of the intensity is possible if the common waveform is hidden in the optical phase of the injection, but the approach requires the usage of external phase modulators [3], [31]. Fig. 3(ii) plots $|a_C(t)|^2$ against $|a_B(t)|^2$ in which similarly scattered data points are observed. By contrast, Fig. 3(iii) reveals a much stronger correlation between A and B. The plot for $|a_A(t)|^2$ against $|a_B(t)|^2$ essentially lies on a straight line, where the cross-correlation coefficient is evaluated as greater than 0.99. Thus, the response lasers A and B are successfully synchronized, while their emissions differ from that of the common laser C. An eavesdropper in the public channel in Fig. 1 can obtain the emission intensity from C, but yet cannot deduce the emission intensities of A and B.

The chaotic emissions from A and B are used to generate binary bit streams $b_A(t)$ and $b_B(t)$, as Fig. 1 shows. The ADCs are assumed to have a limited analogue detection bandwidth of 8 GHz, which is controlled by a digital infinite impulse response (IIR) filter. The sampling rate f_s is set at 2 GHz. The digitization thresholds of the ADCs are set at the time-average of the intensity signals. The delay lines in Fig. 1 for the XOR operations are set at 5 ns as realizable by electrical cables [41]. As a result of the above processing, the output streams $b_A(t)$ and $b_B(t)$ each has a bit rate of 2 Gbps. For analyzing the security of the schematic in Fig. 1, an eavesdropper is assumed to adopt the same configurations for the PD, ADC, and XOR operation such that a binary bit stream $b_C(t)$ is generated directly from the emission of C in the public channel. The three bit streams b_A, b_B, and b_C are compared in Fig. 4. The injection strength ξ is varied under a fixed $f = -5$ GHz in Fig. 4(i), whilst the injection detuning frequency f is varied under a fixed $\xi = 0.2$ in Fig. 4(ii). The bit streams are compared quantitatively by the bit error ratio (closed symbols) and bit mutual information (open symbols). The error ratio between a pair of bit streams measures the proportion of unequal bits amongst all bits. The mutual information between a pair of bit streams measures their mutual dependence [2], [37].

If the nonlinear dynamics of laser A perfectly scrambles the injected waveform, the bit streams (b_A, b_C) become totally independent such that their error ratio and mutual information approach 50% and 0, respectively. Fig. 4(a) shows the actual comparison of b_A and b_C. As ξ increases from

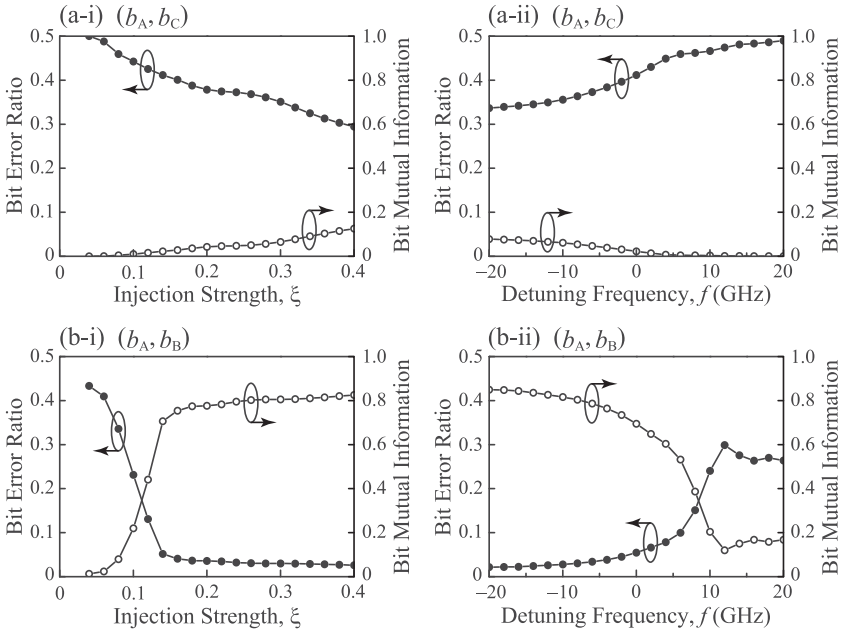


Fig. 4. Bit error ratio and mutual information of (a) (b_A, b_C) and (b) (b_A, b_B). Column (i): The injection strength ξ is varied. Column (ii): The injection detuning frequency f is varied.

0 to 0.4 in Fig. 4(a-i), the bit error ratio slightly reduces from the ideal 50% down to 30%, while the mutual information remains below 0.13. As f is tuned from -20 to 20 GHz in Fig. 4(a-ii), the bit error ratio remains greater than 34%, while the mutual information is less than 0.08. In other words, the eavesdropper is not able to use b_C to obtain much information of b_A, which implies the security of the scheme in Fig. 1.

If perfect identical synchronization is achieved in the response lasers A and B, the bit streams (b_A, b_B) become exactly the same such that their error ratio and mutual information approach 0 and 1, respectively. Fig. 4(b) shows the actual comparison of b_A and b_B, which are subject to the independent noise inside the two response lasers. As ξ slightly increases from 0 to beyond 0.2 in Fig. 4(b-i), the common injection becomes sufficiently strong for synchronizing A and B, causing the bit error ratio to quickly reduce to below 4% and the bit mutual information to rise to the level of 0.8. Such a low error ratio and high mutual information are achieved as f is varied to below -5 GHz in Fig. 4(b-ii). The synchronization is found to prefer negative detuning frequencies because the injection typically causes red-shifting through the antiguidance effect [33], [52]. In short, Fig. 4(b) clearly confirms the correlation of the two bit streams (b_A, b_B) using a sufficiently strong injection with a negative detuning frequency. Moreover, for generality, the bit error ratio of (b_A, b_B) is also examined when the dynamical parameters of the common laser C are different from those of the two response lasers. The bit error ratio in fact remains below 8% even when the parameters γ_c, b, γ_n, γ_p, and γ_s are all varied together by $\pm$20%. The correlation of (b_A, b_B) mainly relies on matching the parameters of lasers A and B, rather than on the parameters of laser C.

If the parameters of lasers A and B are not exactly matched, their synchronization becomes imperfect. Fig. 5(i) compares the bit error ratio between (b_A, b_B) when the two response lasers have a parameter mismatch δ. The common injection is kept at (ξ, f) = (0.2, -5 GHz). The parameters of A are also kept unchanged, but the parameters of B are varied with a percentage change of δ. Mismatch is independently introduced to γ_c, b, γ_n, γ_p, and γ_s for the up-triangles, squares, down-triangles, diamonds, and left-triangles in Fig. 5(i), where only one of the parameter is mismatched for each data point. At $\delta = 0$, there is no parameter mismatch so that the bit error ratio minimizes to about 4%. Errors exist because the two lasers are subject to separate perturbation of their noise. It is worth noting that the error ratio can be reduced by orders of magnitude through adopting various

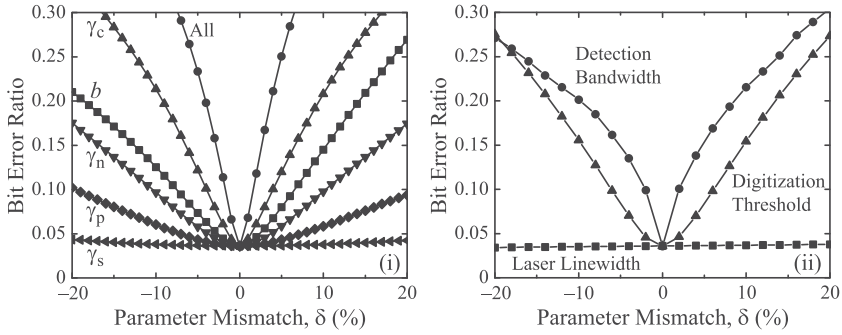


Fig. 5. Bit error ratio of (b_A, b_B) as a function of the parameter mismatch between lasers A and B.

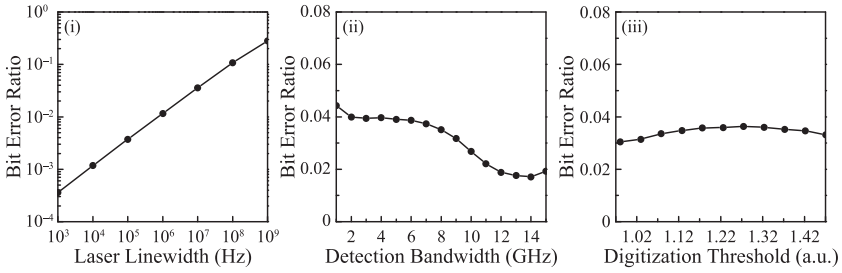


Fig. 6. Bit error ratio of (b_A, b_B) versus (i) free-running laser linewidth, (ii) detection bandwidth, and (iii) digitization threshold for both lasers A and B.

techniques including dual-threshold sampling and forward-error-correction coding [2], [6], [13]. As δ deviates from zero, the parameter mismatch quickly causes a degradation of the synchronization such that the bit error ratio increases. The bit error ratio is most sensitive to γ_c as it governs the rate of photon decay [53]. Furthermore, mismatch is introduced simultaneously to all the five parameters for the circles in Fig. 5(i), where the error ratio increases nearly linearly to 30% with a mismatch δ of only about $\pm$7%. Therefore, highly correlated bit streams can only be generated when the two response lasers are closely matched in parameters.

In addition to the mismatch of the five dynamical parameters of lasers A and B, the output bits in CRBG are sensitive to the process of detection and digitization, as Fig. 1 shows. So Fig. 5(ii) investigates the mismatch in the free-running linewidths of the two lasers, the detection bandwidths of the two ADCs, as well as the digitization thresholds in squares, circles, and triangles, respectively. The five dynamical parameters of lasers A and B are set equal in Fig. 5(ii). The free-running linewidths, as controlled by the noise strengths in lasers A and B, do not significantly affect the error ratio when their mismatch is tuned merely by $\pm$20%. The mismatch of the detection bandwidths or the digitization thresholds, on the other hand, significantly affects the error ratio for bit streams (b_A, b_B). Furthermore, without considering any mismatch, the free-running linewidths of lasers A and B, the detection bandwidths of the ADCs, and the digitization thresholds are independently varied in Figs. 6(i), 6(ii), and 6(iii), respectively. In Fig. 6(i), as the noise strengths are tuned for both response lasers, the linewidths decrease and the bit error ratio reduces accordingly. In Fig. 6(ii), the error ratio generally reduces as the detection bandwidths of the ADCs increase in approaching the effective bandwidths of 18 GHz for the chaotic spectra in Figs. 2(b-ii) and 2(c-ii). As for tuning the digitization thresholds in Fig. 6(iii), the bit error ratio does not vary by much, though the thresholds are known to affect the quality of randomness [42].

The randomness of streams b_A and b_B are individually examined using the NIST statistical tests of Special Publication 800-22 in Table I. The common injection strength and detuning frequency are kept unchanged. The parameter mismatch between the two response lasers is set to zero. The NIST tests are conducted for each stream using 1000 sets of 10^6 bits. At significance level of 0.01 for random bits, the success proportion should be in the range of 0.99 ± 0.0094392. The composite

TABLE 1
NIST Test Results for Output Bit Streams b_A and b_B

	Stream b_A			Stream b_B		
Statistical test	*P*-value	Proportion	Result	*P*-value	Proportion	Result
Frequency	0.022149	0.9840	Pass	0.005166	0.9860	Pass
Block frequency	0.005932	0.9930	Pass	0.004177	0.9900	Pass
Cumulative sums	0.003767	0.9820	Pass	0.010165	0.9840	Pass
Runs	0.670396	0.9950	Pass	0.849708	0.9920	Pass
Longest run	0.725829	0.9890	Pass	0.021849	0.9900	Pass
Rank	0.743915	0.9890	Pass	0.872425	0.9910	Pass
FFT	0.461612	0.9910	Pass	0.618385	0.9920	Pass
Non-overlapping templates	0.003767	0.9810	Pass	0.003795	0.9830	Pass
Overlapping templates	0.003604	0.9840	Pass	0.651693	0.9900	Pass
Universal	0.548314	0.9860	Pass	0.368587	0.9860	Pass
Approximate entropy	0.884671	0.9940	Pass	0.528111	0.9910	Pass
Random excursions	0.005042	0.9851	Pass	0.052160	0.9820	Pass
Random excursions variant	0.024911	0.9834	Pass	0.006935	0.9870	Pass
Serial	0.148653	0.9890	Pass	0.131879	0.9910	Pass
Linear complexity	0.707513	0.9890	Pass	0.036113	0.9960	Pass
Total			15			15

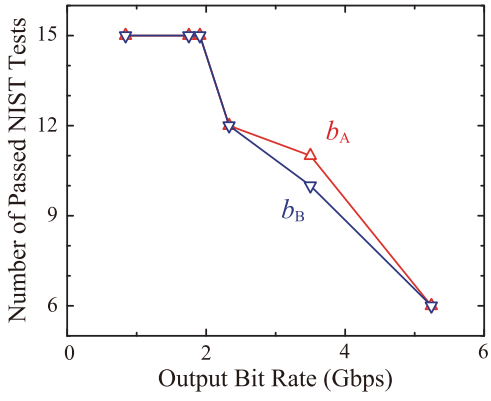


Fig. 7. Number of passed NIST tests for b_A (up-triangles) and b_B (down-triangles). The output bit rate is varied by varying the sampling rate f_s of the ADCs.

P-value should be larger than 0.0001 for uniformity. Both b_A and b_B are observed to pass all the 15 NIST tests in Table I. CRBG is achieved using the scheme of unidirectional optical injection in Fig. 1, where randomness of the bits are verified in Table I and correlations are observed in Fig. 4(b).

Additionally, Fig. 7 shows the number of passes in the NIST tests as the output bit rate is varied by varying the sampling rates f_s of the ADCs in Fig. 1. The results for the output bit streams b_A and b_B are respectively shown as up-triangles and down-triangles in Fig. 7. For each of the bit streams,

all 15 NIST tests are passed as the output bit rate is tuned up to about 2 Gbps, which can be further increased by extracting multiple bits from each sample [41], [42]. The use of optical injection without feedback in Fig. 1 enables such a continuous tunability of the bit rate while maintaining randomness of the output bits [41]. The bit rate can be further increased by utilizing low significant bits of the ADCs with higher resolutions.

4. Discussion

Previously reported approaches for CRBG often utilized optical feedback for yielding the chaotic lasers as the common sources [3], [6]. For comparison, Fig. 1 is modified by removing the master laser M and introducing an optical feedback into the common laser C, while keeping the rest of the settings in the schematic unchanged. Numerical simulation is conducted by replacing the CW injection term $\xi_C \gamma_c \exp(-i2\pi f_C t)$ in (1) by a feedback term $\xi_C \gamma_c a_C(t-\tau)$, where $\tau = 0.5$ ns denotes the feedback delay time. The strength of the feedback is optimized to $\xi_C = 0.06$, which minimizes the residual autocorrelation of the laser at τ [37], [39]. The chaotic emission from C continues to optically inject the response lasers A and B for outputting bit streams (b_A, b_B). Inevitably, despite the optimized suppression of the time-delay signature for the common laser C, the residual time-delay information from C is injected to the response lasers, so the output bit streams (b_A, b_B) are found to fail the NIST randomness tests [41]. Though the injection parameters of the response lasers can be optimized for further suppressing the time-delay information in the output bits, they cannot be simultaneously optimized for minimizing the bit error ratio in CRBG [40]. By contrast, the approach of unidirectional optical injection detailed in Section 2 has the unique advantage of involving no feedback loops, thereby completely avoiding any time-delay information artifacts in the output bits in CRBG.

5. Conclusion

In conclusion, CRBG by the unidirectional optical injection of semiconductor lasers is numerically investigated. Due to chaotic injection from a common laser, the two response lasers are synchronized to successfully generate correlated random bits for a low bit error ratio below 4% and a high mutual information of about 0.8, which are attained by a negatively detuned injection of a sufficiently strong strength. Moreover, the CRBG is secure as it relies on closely matching the parameters of the two response lasers, where a mismatch of all the parameters by 7% drastically increases the error ratio to 30%. Though the injection uses a public channel, an eavesdropper can only attempt to recover the bits with an error ratio as high as 38%. Furthermore, the common laser is itself driven into chaos by CW injection, no feedback loop is involved so that the output rate can be continuously tuned up to 2 Gbps, while randomness is maintained according to the verifications by the NIST tests. The approach of CRBG by optical injection without feedback is potentially applicable to improving chaos-based key distribution schemes.

References

[1] J. Muramatsu, K. Yoshimura, P. Davis, A. Uchida, and T. Harayama, "Secret-key distribution based on bounded observability," *Proc. IEEE*, vol. 103, no. 10, pp. 1762–1780, Oct. 2015.
[2] H. Koizumi *et al.*, "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," *Opt. Exp.*, vol. 21, no. 15, pp. 17869–17893, Jul. 2013.
[3] K. Yoshimura *et al.*, "Secure key distribution using correlated randomness in lasers drivenby common random light," *Phys. Rev. Lett.*, vol. 108, no. 7, Feb. 2012, Art. no. 070602.
[4] I. Kanter *et al.*, "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography," *Opt. Exp.*, vol. 18, no. 17, pp. 18292–18302, Aug. 2010.
[5] L. Wang *et al.*, "Synchronization-based key distribution utilizing information reconciliation," *IEEE J. Quantum Electron.*, vol. 51, no. 12, pp. 1–8, Dec. 2015.
[6] C. Xue, N. Jiang, K. Qiu, and Y. Lv, "Key distribution based on synchronization in bandwidth-enhanced random bit generators with dynamic post-processing," *Opt. Exp.*, vol. 23, no. 11, pp. 14510–14519, 2015.

[7] L. Keuninckx, M. C. Soriano, I. Fischer, C. R. Mirasso, R. M. Nguimdo, and G. Van der Sande, "Encryption key distribution via chaos synchronization," *Sci. Rep.*, vol. 7, 2017, Art. no. 43428.
[8] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, 2014.
[9] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nature Photon.*, vol. 9, no. 3, pp. 151–162, 2015.
[10] L. Jumpertz, K. Schires, M. Carras, M. Sciamanna, and F. Grillot, "Chaotic light at mid-infrared wavelength," *Light Sci. Appl.*, vol. 5, no. 6, 2016, art. no. e16088.
[11] A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol. 2, no. 12, pp. 728–732, Dec. 2008.
[12] M. Virte, K. Panajotov, H. Thienpont, and M. Sciamanna, "Deterministic polarization chaos from a laser diode," *Nature Photon.*, vol. 7, no. 1, pp. 60–65, 2013.
[13] A. Argyris, E. Pikasis, and D. Syvridis, "Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators," *J. Lightw. Technol.*, vol. 34, no. 22, pp. 5325–5331, Nov. 2016.
[14] H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, "Synchronization of bandwidth-enhanced chaos in semiconductor lasers with optical feedback and injection," *Opt. Exp.*, vol. 17, no. 22, pp. 19536–19543, 2009.
[15] M. C. Soriano, J. Garcia-Ojalvo, C. R. Mirasso, and I. Fischer, "Complex photonics: Dynamics and applications of delay-coupled semiconductors lasers," *Rev. Mod. Phys.*, vol. 85, no. 1, pp. 421–470, 2013.
[16] A. Quirce, A. Valle, H. Thienpont, and K. Panajotov, "Chaos synchronization in mutually coupled 1550-nm vertical-cavity surface-emitting lasers with parallel polarizations and long delay time," *J. Opt. Soc. Amer. B*, vol. 33, no. 1, pp. 90–98, 2016.
[17] X. Porte, M. C. Soriano, D. Brunner, and I. Fischer, "Bidirectional private key exchange using delay-coupled semiconductor lasers," *Opt. Lett.*, vol. 41, no. 12, pp. 2871–2874, 2016.
[18] E. Klein *et al.*, "Public-channel cryptography based on mutual chaos pass filters," *Phys. Rev. E*, vol. 74, no. 4, 2006, Art. no. 046201.
[19] M. Virte, M. Sciamanna, and K. Panajotov, "Synchronization of polarization chaos from a free-running VCSEL," *Opt. Lett.*, vol. 41, no. 19, pp. 4492–4495, 2016.
[20] R. Vicente, I. Fischer, and C. R. Mirasso, "Synchronization properties of three delay-coupled semiconductor lasers," *Phys. Rev. E*, vol. 78, no. 6, 2008, Art. no. 066202.
[21] A. Argyris, M. Bourmpos, and D. Syvridis, "Experimental synchrony of semiconductor lasers in coupled networks," *Opt. Exp.*, vol. 24, no. 5, pp. 5600–5614, 2016.
[22] I. Fischer *et al.*, "Zero-lag long-range synchronization via dynamical relaying," *Phys. Rev. Lett.*, vol. 97, no. 12, 2006, Art. no. 123902.
[23] N. Jiang *et al.*, "Chaos synchronization and communication in mutually coupled semiconductor lasers driven by a third laser," *J. Lightw. Technol.*, vol. 28, no. 13, pp. 1978–1986, Jul. 2010.
[24] A. Uchida, R. McAllister, and R. Roy, "Consistency of nonlinear system response to complex drive signals," *Phys. Rev. Lett.*, vol. 93, no. 24, 2004, Art. no. 244102.
[25] S. Sunada, K. Arai, K. Yoshimura, and M. Adachi, "Optical phase synchronization by injection of common broadband low-coherent light," *Phys. Rev. Lett.*, vol. 112, no. 20, 2014, Art. no. 204101.
[26] R. Toral, C. R. Mirasso, E. Hernández-Garcıa, and O. Piro, "Analytical and numerical studies of noise-induced synchronization of chaotic systems," *Chaos*, vol. 11, no. 3, pp. 665–673, 2001.
[27] H. D. Abarbanel, N. F. Rulkov, and M. M. Sushchik, "Generalized synchronization of chaos: The auxiliary system approach," *Phys. Rev. E*, vol. 53, no. 5, pp. 4528–4535, 1996.
[28] N. Jiang, C. Xue, D. Liu, Y. Lv, and K. Qiu, "Secure key distribution based on chaos synchronization of VCSELs subject to symmetric random-polarization optical injection," *Opt. Lett.*, vol. 42, no. 6, pp. 1055–1058, 2017.
[29] J. G. Wu, Z. M. Wu, Y. R. Liu, L. Fan, X. Tang, and G. Q. Xia, "Simulation of bidirectional long-distance chaos communication performance in a novel fiber-optic chaos synchronization system," *J. Lightw. Technol.*, vol. 31, no. 3, pp. 461–467, Feb. 2013.
[30] V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, and S. Merlo, "Private message transmission by common driving of two chaotic lasers," *IEEE J. Quantum Electron.*, vol. 46, no. 2, pp. 258–264, Feb. 2010.
[31] H. Aida *et al.*, "Experiment on synchronization of semiconductor lasers by common injection of constant-amplitude random-phase light," *Opt. Exp.*, vol. 20, no. 11, pp. 11813–11829, 2012.
[32] T. Yamamoto *et al.*, "Common-chaotic-signal induced synchronization in semiconductor lasers," *Opt. Exp.*, vol. 15, no. 7, pp. 3974–3980, 2007.
[33] I. Oowada *et al.*, "Synchronization by injection of common chaotic signal in semiconductor lasers with optical feedback," *Opt. Exp.*, vol. 17, no. 12, pp. 10025–10034, 2009.
[34] C. Xue, N. Jiang, Y. Lv, and K. Qiu, "Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 312–319, Jan. 2017.
[35] V. Annovazzi-Lodi and G. Aromataris, "Privacy in two-laser and three-laser chaos communications," *IEEE J. Quantum Electron.*, vol. 51, no. 7, Jul. 2015, Art. no. 7000405.
[36] J. G. Wu *et al.*, "Isochronous synchronization between chaotic semiconductor lasers over 40-km fiber links," *IEEE Photon. Technol. Lett.*, vol. 23, no. 24, pp. 1854–1856, Dec. 2011.
[37] D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, "Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback," *Opt. Lett.*, vol. 32, no. 20, pp. 2960–2962, 2007.
[38] Y. Z. Liu *et al.*, "Exploiting optical chaos with time-delay signature suppression for long-distance secure communication," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 7900512.
[39] S. S. Li and S. C. Chan, "Chaotic time-delay signature suppression in a semiconductor laser with frequency-detuned grating feedback," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 6, pp. 541–552, Nov./Dec. 2015.
[40] N. Li *et al.*, "Photonic generation of wideband time-delay-signature-eliminated chaotic signals utilizing an optically injected semiconductor laser," *IEEE J. Quantum Electron.*, vol. 48, no. 10, pp. 1339–1345, Oct. 2012.

[41] X. Z. Li, S. S. Li, J. P. Zhuang, and S. C. Chan, "Random bit generation at tunable rates using a chaotic semiconductor laser under distributed feedback," *Opt. Lett.*, vol. 40, no. 17, pp. 3970–3973, 2015.
[42] X. Z. Li, J. P. Zhuang, S. S. Li, J. B. Gao, and S. C. Chan, "Randomness evaluation for an optically injected chaotic semiconductor laser by attractor reconstruction," *Phys. Rev. E*, vol. 94, no. 4, 2016, Art. no. 042214.
[43] C. Wang, K. Schires, M. Osinski, P. J. Poole, and F. Grillot, "Thermally insensitive determination of the linewidth broadening factor in nanostructured semiconductor lasers using optical injection locking," *Sci. Rep.*, vol. 6, 2016, Art. no. 27825.
[44] G. A. Smolyakov, Y. Fichou, and M. Osinski, "Analysis of high-frequency modulation response of strongly injection-locked cascaded semiconductor ring lasers," *IEEE J. Quantum Electron.*, vol. 48, no. 12, pp. 1568–1577, Dec. 2012.
[45] S. C. Chan, "Analysis of an optically injected semiconductor laser for microwave generation," *IEEE J. Quantum Electron.*, vol. 46, no. 3, pp. 421–428, Mar. 2010.
[46] H. F. Chen and J. M. Liu, "Open-loop chaotic synchronization of injection-locked semiconductor lasers with gigahertz range modulation," *IEEE J. Quantum Electron.*, vol. 36, no. 1, pp. 27–34, Jan. 2000.
[47] J. P. Zhuang and S. C. Chan, "Phase noise characteristics of microwave signals generated by semiconductor laser dynamics," *Opt. Exp.*, vol. 23, no. 3, pp. 2777–2797, 2015.
[48] F. Y. Lin, Y. K. Chao, and T. C. Wu, "Effective bandwidths of broadband chaotic signals," *IEEE J. Quantum Electron.*, vol. 48, no. 8, pp. 1010–1014, Aug. 2012.
[49] X. Z. Li and S. C. Chan, "Heterodyne random bit generation using an optically injected semiconductor laser in chaos," *IEEE J. Quantum Electron.*, vol. 49, no. 10, pp. 829–838, Oct. 2013.
[50] A. B. Wang, Y. C. Wang, and H. C. He, "Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback," *IEEE Photon. Technol. Lett.*, vol. 20, no. 19, pp. 1633–1635, Oct. 2008.
[51] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," *Opt. Exp.*, vol. 23, no. 2, pp. 1470–1490, 2015.
[52] H. F. Chen and J. M. Liu, "Complete phase and amplitude synchronization of broadband chaotic optical fields generated by semiconductor lasers subject to optical injection," *Phys. Rev. E*, vol. 71, no. 4, 2005, Art. no. 046216.
[53] H. D. I. Abarbanel, M. B. Kennel, L. Illing, S. Tang, H. F. Chen, and J. M. Liu, "Synchronization and communication using semiconductor lasers with optoelectronic feedback," *IEEE J. Quantum Electron.*, vol. 37, no. 10, pp. 1301–1311, Oct. 2001.