Fast random bits generation based on a single chaotic semiconductor ring laser

Fast random bits generation based on a single chaotic semiconductor ring laser

Romain Modeste Nguimdo,[1,*] **Guy Verschaffelt,**[1] **Jan Danckaert,**[1] **Xaveer Leijtens,**[2] **Jeroen Bolk,**[2] **and Guy Van der Sande**[1]

[1]*Applied Physics Research Group, Vrije Universiteit Brussel, 1050 Brussels Belgium*
[2]*COBRA Research Institute, Eindhoven University of Technology, 5600MB Eindhoven, The Netherlands*
[*]*Romain.Nguimdo@vub.ac.be*

Abstract: The use of the postprocessing method consisting of bitwise Exclusive-OR and least significant bits extraction to generate random bit sequences typically requires two distinct chaotic outputs. While the two signals are, in general, generated using two separated devices, e.g. two Fabry-Perot lasers, a single semiconductor ring laser can be used as an alternative due to its circular symmetry which facilitates lasing in two counterpropagating mode directions. We consider a chaotic semiconductor ring laser and investigate both numerically and experimentally its characteristics for fast random bit generation. In particular, we show that by sampling each directional mode's output signal using a 8-bit analog-digital converter and through Exclusive-OR operation applied to the two resulting signals (after throwing away 4 most significant bits), we can achieve fast random bit-streams with a bit rate $4 \times 10 = 40$ Gbit/s, passing the statistical randomness tests. To optimize the system performance, we also study the dependence of randomness on the main system parameters and on noise.

OCIS codes: (140.3560) Laser, ring; (030.6600) Statistical optics, (060.0060) Fiber optics and optical communications; (140.1540) Chaos.

References and links

1. N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010).
2. W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, "An integrated analog/digital random noise source," IEEE Trans. Circuits Syst. I, **44**, 521-528 (1997).
3. T. Stojanovski and L. Kocarev, "Chaos-based random number generators part I: Analysis [cryptography]," IEEE Trans. Circuits Syst. I: Fundam. Theory Applicat. **48**, 281-288 (2001).
4. R. M. Nguimdo, P. Colet, L. Larger and L. Pesquera, "Digital key for chaos communication performing time delay concealment," Phys. Rev. Lett. **107**, 034103/1-4 (2011).
5. R. M. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," Opt. Express **20**, 25333-25344 (2012).
6. 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, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**, 728-732 (2008).
7. T. E. Murphy, and R. Roy, "The worlds fastest dice, Nat. Photonics **2**, 714-715 (2008).
8. K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," IEEE J. Quantum Electron. **45**, 1367-1379 (2009).
9. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultra high-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**, 024102 (2009).

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

10. A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit," Opt. Express **18**, 18763-18768 (2010).
11. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**, 58-61 (2010).
12. K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," Opt. Express **18**, 5512-5524 (2010).
13. N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation," Opt. Lett. **36**, 4632 (2011).
14. C. R. S. Williams, J. C. Salevan, X.-W. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," Opt. Express **18**, 23584-23597 (2010).
15. R. H. Walden, "Analog-to-digital converter survey and analysis," IEEE J. Sel. Areas Commun. **17**, 539-550 (1999)
16. M. Sorel, G. Giuliani, A. Sciré, R. Miglierina, J. P. R. Laybourn, and S. Donati, "Operating regimes of GaAsAlGaAs semiconductor ring lasers: Experiment and model," IEEE J. Quantum Electron. **39**, 1187-1195 (2003).
17. J. Javaloyes and S. Balle, "Emission directionality of semiconductor ring lasers: A traveling-wave description," IEEE J. Quantum Elect. **45**, 431-438 (2009).
18. S. Sunada, T. Harayama, K. Arai, K. Yoshimura, K. Tsuzuki, A. Uchida, and P. Davis, "Random optical pulse generation with bistable semiconductor ring lasers," Opt. Express **19**, 7439-7450 (2011)
19. I. V. Ermakov, G. Van der Sande and J. Danckaert, "Semiconductor ring laser subject to delayed optical feedback: bifurcations and stability", Commun. Nonlinear Sci. Numer. Simul. **17**, 4767-4779 (2012).
20. R. M. Nguimdo, G. Verschaffelt, J. Danckaert, and G. Van der Sande, "Loss of time-delay signature in chaotic semiconductor ring lasers," Opt. Lett. **37**, 2541-2544 (2012).
21. L. Gelens, S. Beri, G. Van der Sande, G. Mezosi, M. Sorel, J. Danckaert, and G. Verschaffelt, "Exploring multistability in semiconductor ring lasers: theory and experiment," Phys. Rev. Lett. **102**, 193904 (2009).
22. N. Jiang, W. Pan, B. Luo, L. Yan, S. Xiang, L. Yang, D. Zheng, N. Li, "Influence of injection current on the synchronization and communication performance of closed-loop chaotic semiconductor lasers," Opt. Lett. **36**, 3197-3199 (2011).
23. D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: A dynamical point of view," IEEE J. Quantum Electron. **45**, 879-891 (2009).
24. R. M. Nguimdo, M. C. Soriano, and P. Colet, "Role of the phase in the identification of delay time in semiconductor lasers with optical feedback," Opt. Lett. **36**, 4332-4334 (2011).
25. R. Vicente, J. Dauden, P. Colet, R. Toral, "Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop," IEEE J. Quantum Electron. **41**, 541-548 (2005).
26. M. F. Booth, A. Schremer, and J. M. Ballantyne, "Spatial beam switching and bistability in a diode ring laser," Appl. Phys. Lett. **76**, 1095-1097 (2000).
27. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "Towards the generation of random bits at terahertz rates based on a chaotic semiconductor laser," Int. Workshop on Statistical-Mechanical Informatics 1-8 (2010), 5861 (2010).
28. A. Argyris, E. Pikasis, S. Deligiannidis, and Dimitris Syvridis, "Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," J. Lightwave Technol. **30**, 1329-1334 (2010).
29. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, and M. Levenson, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards and Technology, Special Publication 800-22, 2001, Revision 1, 2008 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf.
30. S. J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST statistical test suite for randomness," 2004, arXiv:nlin.CD/0401040v1.
31. X. Leijtens, "JePPIX: the platform for InP-based photonics," IET Optoelectronics **5**, 202-206 (2011).
32. I. V. Ermakov, S. Beri, M. Ashour, J. Danckaert, B. Docter, J. Bolk, X. Leijtens, and G. Verschaffelt, "Semiconductor ring laser with On-Chip Filtered Optical Feedback for discrete wavelength tuning," IEEE J. Quantum Electron. **48**, 129-136 (2012).

1. Introduction

Random numbers are useful for a wide variety of applications including encryption and authentication protocols, stochastic modeling, and online gaming and lotteries [1]. There are two basic types of generators which can be used to produce random sequences: pseudorandom number generators (PRNGs) and random number generators (RNGs). Typically, PRNGs can be implemented on the software platform based on initial seeds and deterministic algorithms. However,

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

sequences of pseudo-random numbers generated deterministically from the same seed will be identical. Therefore, although their effective cost is low, this can lead to serious problems for applications implying parallel computation systems. Still worse, the sequences can be fully predicted once the initial seed or the deterministic algorithm is known. True random numbers should be un-reproducible as well as statistically unbiased. In this viewpoint, random bit generation based on measuring thermal noise may be seen as an efficient way since noise is intrinsically a non-deterministic physical process [2]. However, owing to low signal levels, such systems require extensive broadband amplification and are thus highly susceptible to bias introduced by the non-ideal amplifiers and small non-random external perturbations. As an alternative approach, random bit sequences have been generated by digitizing chaotic signals in electronic circuits [3], however, with the rates much lower than that of PRNGs because of the narrow bandwidth of these physical entropy sources.

Giving the growing applications requiring random bit-streams at high bit rates [4, 5], optical or opto-electronic systems with delay are promising sources of fast non-deterministic random number generations. In fact, their short internal time scales allow for large bandwidth dynamics, and delayed optical feedback can induce strong diverging chaotic trajectories, thus making rapid bit rates possible. Continuous streams of random bit sequences have been generated at fast rates of up to several Gbit/s *in real time* by directly sampling the output of two chaotic semiconductor lasers with one-bit analog-digital converters (ADCs) [6–8]. Subsequently, the efforts to further increase the bit rate [12] or/and to implement more simplified architectures [9–13] have been reported, by using 8-bit ADCs to sample the chaotic signal and to extract multi-bits in order to form the single random sequence.

However, as noted by some researchers [12, 14], it is still unclear to what extent the high-speed chaotic optical signal contributes to the performance, in comparison to the intrinsic noise of the ADC converter, which can often dominate the least significant bits [15]. In particular, the fact that this method can be used to generate very high bit rates, e.g 300 Gb/s, from a single laser developing chaos with bandwidth of only a few GHz [11] has supported the idea that this very good performance is due to intrinsic noise generated by the system components (e.g ADC noise, amplifier noise, etc..) and not to chaos. The main reason for this controversy relies on the fact that all these works are experimental, meaning noisy systems.

In this work, we discuss experiments in a noisy environment and numerical simulations with and without noise to explore the possibility of generating random bit sequences with high bit rate from chaotic semiconductor ring lasers (SRLs). They can be easily implemented on chip. Moreover, the delay line can in principle be integrated on the same chip without requiring on-chip highly reflective mirrors which are technologically challenging. The fact that light can be coupled between these devices and the input/output waveguides via directional couplers facilitates their monolithic integration with other optical components such as delay lines, splitters

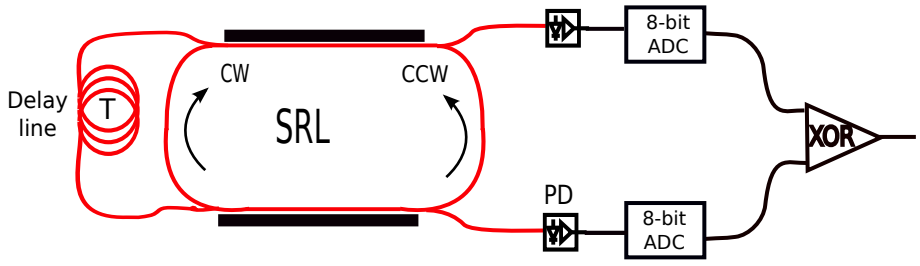

Fig. 1. Schematic of SRL with self-feedback. CW: clockwise mode, CCW: counterclockwise mode, PD: Photodetector, XOR: Exclusive-OR, ADC: analog-digital converter.

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

and detectors providing therefore flexibility and compactness. Moreover their cavity can support lasing in the clockwise (CW) and counterclockwise (CCW) directions [16, 17] and this facilitates post-processing such as bitwise Exclusive-OR operations from a single device. To ensure that chaos is the essential ingredient for random bit generation, we consider in our modeling a noiseless system. Our results indicate that despite relative low chaos bandwidths, post-processing methods allow us to generate ultra-fast deterministic random bits. These results are also verified experimentally. Note that SRLs have been previously used to demonstrate random pulse train generation when they are pulse-modulated by the injection current [18]. In our case a constant current is applied to the SRL and therefore we do not need complicated electronics to drive the device.

2. Dynamics characterization

The scheme used for this work is depicted in Fig. 1. It consists of a semiconductor ring laser (SRL) brought to a chaotic regime by optical self-feedback [19,20]. In the self-feedback configuration, a part of the signal from CW (CCW) mode is injected back in the same mode direction. Thus to implement the feedback, we link two input/output ports of the SRL through an optical fiber, while the two other ports are used to capture the dynamics of the two directional modes. Theoretical analysis of this system can be done based on a single longitudinal-mode SRL model [16, 21] extended with Lang-Kobayashi terms to account for the feedback [19, 20]. Taking into account the effect of spontaneous emission noise, the dynamics can be described, in terms of the mean-field slowly varying complex amplitudes of the electric field associated with the two propagating modes E_{cw} and E_{ccw}, and the carrier number N as

$$\dot{E}_{cw} = \kappa(1+i\alpha)\left[\mathcal{G}_{cw}N-1\right]E_{cw} - (k_d+ik_c)E_{ccw} + \eta E_{cw}(t-T)e^{-i\omega_0 T} + \sqrt{D}\xi_{cw}, \quad (1)$$

$$\dot{E}_{ccw} = \kappa(1+i\alpha)\left[\mathcal{G}_{ccw}N-1\right]E_{ccw} - (k_d+ik_c)E_{cw} + \eta E_{ccw}(t-T)e^{-i\omega_0 T} + \sqrt{D}\xi_{ccw}, \quad (2)$$

$$\dot{N} = \gamma\left[\mu - N - \mathcal{G}_{cw}N\left|E_{cw}\right|^2 - \mathcal{G}_{ccw}N\left|E_{ccw}\right|^2\right], \quad (3)$$

where the parameters are the linewidth enhancement factor α, renormalized bias current μ, field decay rate κ, carrier inversion decay rate γ, solitary laser frequency ω_0, feedback rate η, delay time T, feedback phase $\omega_0 T$, backscattering coefficients $k_d + ik_c$ where k_c and k_d are the conservative and the dissipative couplings, respectively. The relationship between the theoretical parameters and real-world devices are detailed in [16]. The differential gain functions are given by $\mathcal{G}_{cw} = 1 - s\left|E_{cw}\right|^2 - c\left|E_{ccw}\right|^2$ and $\mathcal{G}_{ccw} = 1 - s\left|E_{ccw}\right|^2 - c\left|E_{cw}\right|^2$ where s and c account for the phenomenological self- and cross-saturations, respectively. All the parameters in Eqs. (1)-(3) are needed to reproduce the dynamics encountered in experiments on SRLs [16,21]. As an illustration, while c and s are necessary to get unidirectional emission (i.e emission in only one of the directional modes), k_d and k_c model different reflections on the end-facets of the device, facilitating therefore the emergence of bidirectional emission (i.e emission in both directional modes). The last terms in Eqs. (1) and (2) represent the effect of spontaneous emission noise coupled to the CW/CCW modes [18]: D represents the noise strength expressed as $D = D_m(N + G_0N_0/\kappa)$, where D_m is the spontaneous emission factor, G_0 is the gain parameter, N_0 is the transparent carrier density. $\xi_i(t)$ ($i = cw, ccw$) are two independent complex Gaussian white noises with zero mean and correlation $\langle\xi_i(t)\xi_j^*(t')\rangle = \delta_{ij}(t-t')$. We will set $D_m = 0$ (no noise) unless stated otherwise. We consider the following values for the key parameters which are chosen within the range of experimentally accessible values [20, 21]: $\alpha = 3.5$, $\mu = 1.75$, $s = 0.005$, $c = 0.01$, $\kappa = 100$ ns^{-1}, $\gamma = 0.2$ ns^{-1}, $\omega_0 T = 0$, $k_d = 0.033$ ns^{-1}, $k_{cw} = 0.44$ ns^{-1}, $T = 50$ ns, $\eta = 2.5$ ns^{-1}. With our parameters, the relaxation period of the free-running SRL is $\tau_{R0} \approx 2\pi/\sqrt{2(\mu-1)\gamma\kappa} = 1.14$ ns. Note that τ_{R0} determines how fast the intrinsic dynamics of the system changes.

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

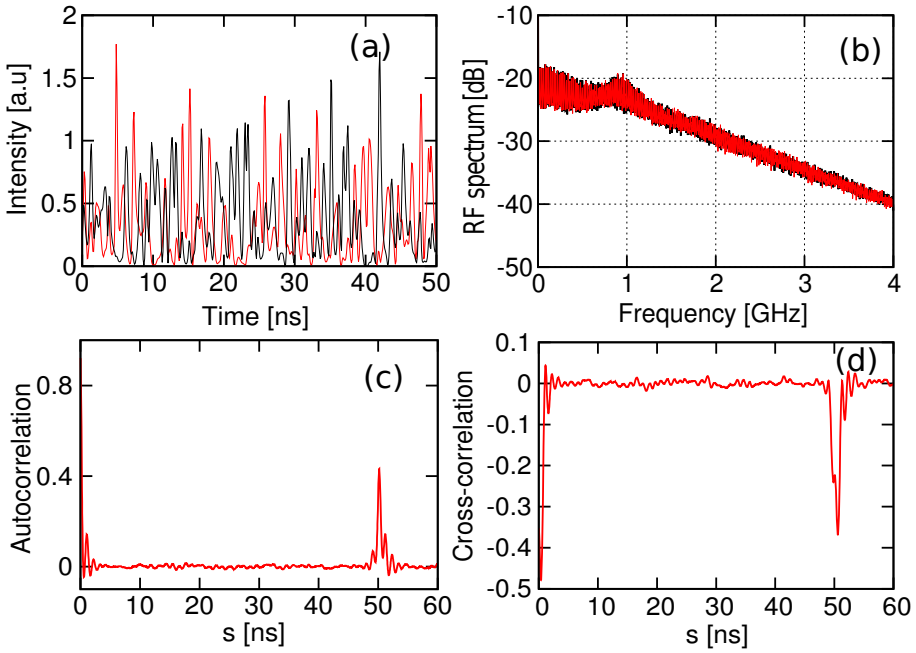

Fig. 2. Left: (a) Part of intensity time series of $|E_{ccw}|^2$ (black) and $|E_{cw}|^2$ (grey, red in color). (b) corresponding RF spectrum in dB. (c) Autocorrelation function computed from $|E_{ccw}|^2$, (d) cross-correlation function between $|E_{cw}|^2$ and $|E_{ccw}|^2$.

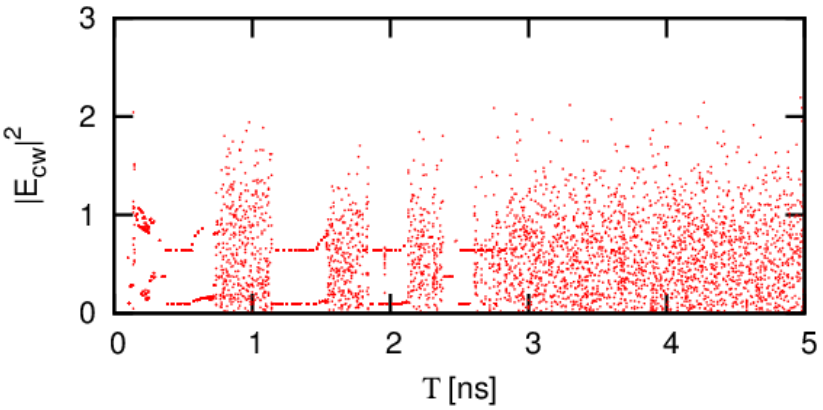

Fig. 3. Bifurcation diagram as a function of the delay time considering $\eta = 2.5$ ns^{-1}

Figure 2(a) displays a part of the CCW (black) and CW (red) intensity time series at the output of the photodiodes. As can be seen, the two modes display similar chaotic behavior. These results are confirmed by the RF power spectra shown in Fig. 2(b) which shows exactly the same spectra for the two signals. This evidences that none of the two modes is favored. Besides, it can be seen that a chaos bandwidth of about 2 GHz is obtained with our parameters. Note that in the chaotic regime, the bandwidth can be increased by increasing the renormalized bias current μ [22]. The finer peak structure observed in the RF spectra corresponds to the delay time signature. These features reveal the existence of certain correlations induced by the feedback. These correlations can be also revealed by computing the autocorrelation function. The results displayed in Fig. 2(c) show peaks around the relaxation and the delay times. The peaks related to the relaxation oscillation are expected to decrease while those related to the

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

delay time increase, with the feedback rate [23, 24]. To estimate the correlation between the two counterpropagating mode signals, we calculate the cross-correlation between $|E_{cw}|^2$ and $|E_{ccw}|^2$. Figure 2(d) displays the results. As can be seen, an anti-correlation of about -0.5 is found around the half of the relaxation period, $\tau_{R0}/2$ while it is close to -0.35 at the delay time. These correlations can be eliminated during post-processing of the signals (see section 3).

Although we consider a long delay for this study (50 ns, i.e 10 m of optical fiber), it should be noted that a short delay can also be used and will be more suitable for on-chip implementations of SRL-based random bit generators. In order to investigate the effect of the length of the feedback loop, we plot in Fig. 3 the bifurcation diagram as a function of the delay time. As can be seen, a delay of 5 ns and even less is enough to bring the system to a chaotic regime similar to that obtained by a long delay. This is in fact expected because it is known that, in chaotic systems, two arbitrary delay times much larger than the intrinsic time scale dynamics induce approximately the same complexity [25]. In our experimental study (see section 5), we did however use a much longer delay as we use a solitary SRL. We thus form the feedback loop externally using optical fibers. Due to the substantial size of the experimentally used components, we implemented a long delay of 10 m .

In some instances, a delay time less than the relaxation time can render the system highly chaotic. We have noted that this can happen only when $T \neq \tau_{RO}/2$ and its near multiples. To illustrate, Fig. 3 shows open windows close to $T \approx \tau_{RO}/2$ and its near multiples, evidencing that the dynamics of the system is either periodic or multi-periodic. Thus the system is more stable for $T \approx \tau_{RO}/2$ meaning that the interplay between the intrinsic dynamics and the external delay is rather destructive so that the system is not destabilized enough to enter in a chaotic regime.

3. Random bit generation

From Fig. 2(c), it can be seen that a random bit sequence generated by directly sampling the CW or CCW laser output using a 1-bit ADC will fail some randomness tests due to the periodicity induced by the feedback in the dynamics. Furthermore, it is also clear from the value of τ_{RO} and confirmed in Fig. 2(b) that the bandwidth of the chaos is small for direct random bits extraction at 10 GSamples/s. The reason is that, if the sampling interval is shorter than τ_{RO}, consecutively extracted points lead to the same value most of the time. As a result, some tests fail.

When multi-bit ADCs are used, consecutive extracted points differ in their least significant bits (LSBs) although their most significant bits (MSBs) remain the same. By throwing away the MSBs, the effect of multi-bit ADCs becomes similar to that obtained through bandwidth

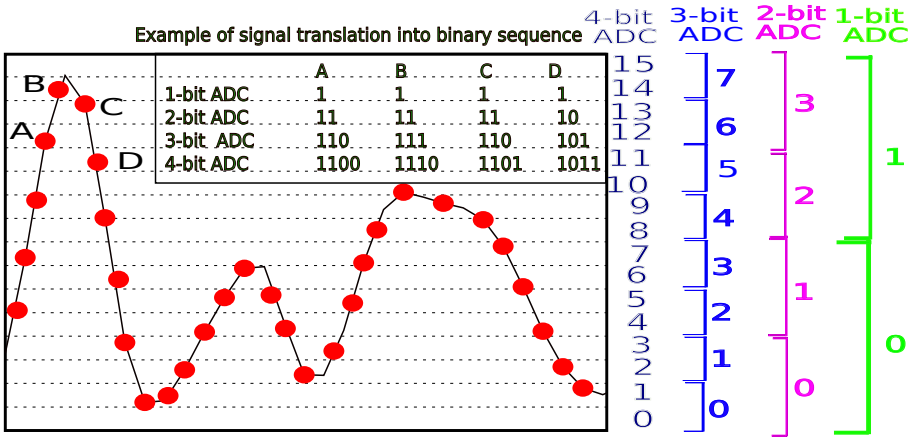

Fig. 4. Operating principle for ADCs. The inset table shows how different ADCs translate the analogic signals A,B,C,D into binary.

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

Table 1. Results of NIST SP 800-22 statistical tests considering $D_m = 0$. For "success" using 1000 samples of 1 Mbit data and significance level $a = 0.01$, the P value (uniformity of p values) should be larger than 0.0001 and the proportion should be greater than 0.9805608 [8]. For the tests which produce multiple P-values and proportions, the worst case is shown.

Statistical	Test P-Value	Proportion	Decision
Frequency	0.715679	0.988	Success
Block frequency	0.775337	0.991	Success
Runs	0.215574	0.989	Success
Longest run	0.864494	0.991	Success
Rank	0.238035	0.990	Success
Fast Fourier transform	0.725829	0.983	Success
Nonoverlapping template	0.003660	0.983	Success
Overlapping template	0.536163	0.989	Success
Universal	0.603841	0.990	Success
Linear complexity	0.078567	0.989	Success
Serial	0.167184	0.991	Success
Approximate entropy	0.079799	0.986	Success
Cumulative sums	0.689019	0.990	Success
Random excursions	0.042632	0.982	Success
Random excursions variant	0.071318	0.995	Success

enhancement. To illustrate, let us consider 4 consecutive points A,B,C, D in an arbitrary portion of the signal triggered simultaneously by 1-, 2-, 3-, 4-bit ADCs at a fixed interval time (Fig. 4). Their binary representations for different ADCs is shown in the inset table of Fig. 4. It can be seen that if they are triggered using a 1-bit ADC, they all lead to the same binary representation. In this case the sequence formed from these extracted bits fails the randomness test. However, as multi-bit ADCs are used, consecutive sample points become completely different in their binary representation when MSBs are ignored. More precisely, it can be seen that A, B, C, D are completely different in their 3-LSBs when a 4-bit ADC is used. By using multiple LSBs per sample, the bit rate of the random sequence will increase proportional to the number of LSBs used. These advantages of multi-bit ADCs suggest that fast random bits can be obtained from a chaotic signal with a small bandwidth. Furthermore, the performance of the system can be further optimized by combining multi-bit ADCs with other post-processing methods such as bitwise Exclusive-OR (XOR) of two independent signals.

We proceed as follows: after the detection of the two chaotic optical signals (CW and CCW modes) by photodetectors, they are digitized by 8-bit ADCs triggered at a sampling rate of 10 GSamples/s (corresponding to a sampling interval of 100 ps). Then, to eliminate the correlations induced by the intrinsic dynamics and delay times and also to enhance uniformity of the generated sequence over short time windows [27, 28], the 4 most significant bits (MSBs) are discarded [9]. According to Fig. 2(c) and (d), the peak size induced by the feedback in the autocorrelation is approximately the same as that in the cross-correlation. Thus, eliminating the delay signature in the directional mode signals will also lead to the elimination of shared information between the two signals, rendering them therefore independent so that they can contribute to the randomness improvement. Effectively to enhance the randomness of our sequence, the two signals constructed from the CW and CCW mode signals (by including the 4

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

Table 2. Results of NIST Special Publication 800-22 statistical tests. Same parameters as in Table 1 considering $D_m = 5 \times 10^6 \text{ns}^{-1}$

Statistical	Test P-Value	Proportion	Decision
Frequency	0.387264	0.984	Success
Block frequency	0.900569	0.987	Success
Runs	0.046269	0.983	Success
Longest run	0.083526	0.993	Success
Rank	0.150340	0.991	Success
Fast Fourier transform	0.150340	0.986	Success
Nonoverlapping template	0.004301	0.983	Success
Overlapping template	0.130369	0.990	Success
Universal	0.951205	0.990	Success
Linear complexity	0.115387	0.992	Success
Serial	0.159910	0.989	Success
Approximate entropy	0.126658	0.996	Success
Cumulative sums	0.725829	0.987	Success
Random excursions	0.036780	0.989	Success
Random excursions variant	0.177727	0.988	Success

least significant bits (LSBs)) are combined using an Exclusive-OR (XOR) gate to form a single bit sequence [6–8]. The randomness of the bit sequence is tested using a standard statistical test suite NIST SP 800-22 [29, 30]. It is composed of 15 statistical tests and the randomness is ensured when all the statistical tests of the NIST test suite are passed.

The results of the NIST SP 800-22 test are shown in Table 1. The tests are performed using 1000 samples of 1 Mbit sequences (i.e. the total amount of test data is 1 Gbit). They are obtained by integrating Eqs. (1)-(3). As can be seen, all the tests pass, verifying that our system produces a statistically random bit-stream. Since the sampling rate is 10 GSamples/s, this system is therefore capable of producing a bit rate of $4 \times 10 = 40$ Gb/s (based on 4 bit). As all NIST tests are passed, this means the noise contribution is not necessary for random bit generation. Thus our main source of entropy is the chaos. Note that for good-quality random bit generation, an incommensurateness between the time-delay and the sampling time is typically required [8].

To investigate the effect of the noise on the randomness statistics, we generate a new sequence by integrating Eqs. (1) and (2) considering the same parameters as were used for Table 1 and noise parameters $D_m = 5 \times 10^6 \text{ns}^{-1}$, $G_0 = 10^{-12}$ m^{3}s^{-1} and $N_0 = 1.4 \times 10^{24}$ m^{-3} [18]. Table 2 shows the results of the NIST SP 800-22 test. Although all the NIST tests pass, it can be noticed that the P-values for some tests in Tables 1 and 2 are different. More specifically, the P-values for the Approximate Entropy and Linear Complexity tests are enhanced due to additional entropy from noise while the P-values for the Frequency, Runs and Long Run tests are worsened by the noise.

4. Influence of parameters on random bit generation

In this section we discuss the influence of the SRL parameters on the randomness of the generated sequences. For our model, the main parameters which can affect the randomness of the generated sequences are the normalized injected current μ, the feedback rate η, the delay time T and the linewidth enhancement factor α. This can be well understood because each of them

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

Table 3. Range of the parameters found to pass all the NIST tests.

Parameter	Fixed parameters	Range of success
Normalized injected current μ	$\eta = 2.5$ ns^{-1}; $\alpha = 3.5$	$1.7 \lesssim \mu \lesssim 4$
Feedback rate η	$\mu = 1.75$; $\alpha = 3.5$	2.2 ns$^{-1} \lesssim \eta \lesssim 2.8$ ns^{-1}
linewidth enhancement factor α	$\mu = 1.75$; $\eta = 2.5$ ns^{-1}	$\gtrsim 3.5$

directly affects the characteristics of the chaotic signals generated by SRLs. While the delay time signatures can be overcome through the digitization and LSB extraction as discussed in section 3, other parameters have to be within a suitable range.

Table 3 shows the suitable range of μ, η and α for which sequences with acceptable randomness can be generated. As already mentioned, the increase (decrease) of μ leads to the increase (decrease) of the generated chaos bandwidth. For our parameters, we have found that random bit sequences pass all the NIST test when μ is in the range of $1.7 \lesssim \mu \lesssim 4$. For $\mu \lesssim 1.7$, the bandwidth is not large enough to generate random numbers at the current bit rate whereas for $\mu \gtrsim 4$ we have found that the system is not chaotic enough. In fact, as μ is increased, the relaxation period decreases, rendering the system more stable. Therefore the current feedback rate is not enough to bring the system into a strongly chaotic regime. Nonetheless, this deteriorating effect for $\mu \gtrsim 4$ can be compensated by increasing the feedback rate so that the system again gets more chaotic. It is worth noting that for two arbitrary values of μ, if the feedback rate is set so that the system operates with the same complexity, better results will be achieved for higher μ because it corresponds to shorter relaxation period, i.e faster intrinsic dynamics. Thus, for random bit generations, it is preferable to operate the SRL with a μ value as high as possible (to get a large bandwidth) and adjust the feedback rate to optimize the system performance.

It is well known that large values of feedback rates produce chaotic time series with clear time-delay signature [20, 23]. If such signatures are very strong, disregarding 4-MSBs may not be enough to completely suppress them. Thus, the generated sequences would still fail the test. We found that randomness of the generated sequences are ensured while $2.2\text{ns}^{-1} \lesssim \eta \lesssim 2.8\text{ns}^{-1}$. Note that for $\eta \lesssim 2.2\text{ns}^{-1}$, the system is not chaotic enough while for $\gtrsim 2.8\text{ns}^{-1}$ the delay time signature is not completely suppressed by disregarding 4 MSBs.

The linewidth enhancement factor α can also play an important role for the randomness of the sequences as increasing α leads to a larger amplitude-phase coupling rendering the system more chaotic. As a consequence the delay signatures are reduced [20]. It is interesting to note that other system parameters, e.g. c, s and k_c only slightly influence the randomness of the sequences.

5. Experiments

We have performed experimental measurements in order to test our numerical predictions.The experiments are performed on an InP-based multi-quantum-well SRL mounted on a brass chuck and thermally controlled by a Peltier element with an accuracy of 0.01^o C. The threshold current of the SRL is 64 mA and the longitudinal mode spacing is 0.305 nm. These lasers have been fabricated using the Joint European Platform for InP-based integrated components and circuits (JePPiX) [31]. More details of the device design, fabrication and operating regimes can be found in [32]. In order to avoid optical feedback from the chip facets, the output waveguides are tilted by 7^o with respect to the chip facets. Light emitted in CW and CCW directions is measured using lensed optical fibers that are angled at 23^o with respect to the chip facets normal in order to maximize the light collection. In our measurements, we use a laser pump current of

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

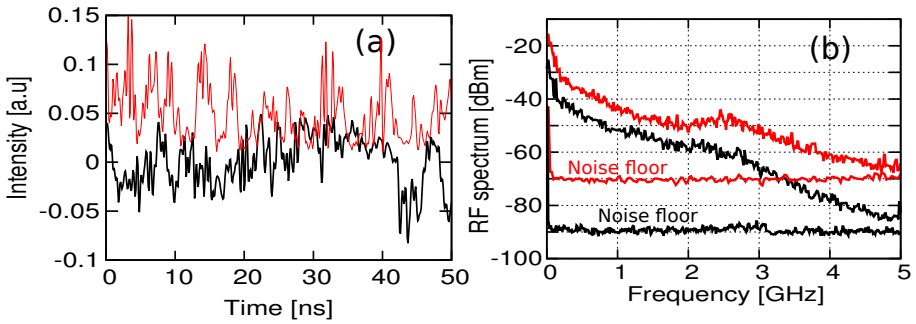

Fig. 5. Left: (a) Part of experimental intensity time series of $|E_{ccw}|^2$ (black) and $|E_{cw}|^2$ (grey, red in color). (b) corresponding RF spectrum and noise floor. The vertical shift (at low frequencies) between the CW and CCW spectra is due to the different responsivity of the different detectors used to measure the two directional modes.

127 mA at which the SRL operates in the bidirectional regime. At this current the laser emits a single longitudinal mode at a wavelength of 1582.17 nm. In the feedback path, we place a semiconductor optical amplifier (SOA), a fiber based polarization controller (PC) and a 50/50 fiber splitter between the lensed fibers that collect the CW and CCW powers. The PC is used to ensure that the feedback light is injected back in the chip with the same polarization direction as the emitted beam. The SOA is used to control the feedback strength by changing the current injection (and hence the amplification) in the SOA. The splitter is used to couple out part of the CW and CCW beams from the feedback loop in order to measure the two directional modes. The total fiber delay length is 14 m corresponding to 70 ns.

Figure 5(a) shows a part of the experimental time traces measured at a sample rate of 10 Gsamples/s on a digital oscilloscope (Tektronix CSA7404). The CCW signal (red) was detected using a Tektronix DC coupled photodetector with a bandwidth of 2.4 GHz while the CW signal was detected using NewFocus photodetector with a bandwidth of 10 GHz (black). In this measurements, the SOA current was set to 295 mA which was found to induce strongly chaotic behavior in CW and CCW directions meanwhile minimizing the delay signatures. As can be seen, these signals are chaotic as evidenced by their RF spectra [Fig. 5(b)]. Furthermore, Fig. 5(b) also shows that, for both modes, the difference between the chaotic signal and noise spectra is greater than 20 dB, indicating that the chaotic signal is much stronger than the detector's noise. Through off-line post-processing, we re-digitize each signal considering a 8-bit ADC. Then a bit sequence is formed from each sample after disregarding the 4-MSBs. Finally, the two bit sequences from CW and CCW signals are combined by bitwise XOR operation and the resulting bit-stream is submitted to the NIST test suite. Table 4 summarizes the results of the NIST tests. All tests pass, confirming therefore our numerical predictions.

As predicted from numerics, we have also checked that data recorded for relative large feedback strength, e.g $I_{OSA} = 600$ mA leads to strong peaks in the autocorrelation and therefore fails the NIST tests. The NIST tests also fail for small feedback strength, e.g $I_{OSA} = 200$ mA because the system is not chaotic enough. We also recorded the time series at higher injection currents (keeping $I_{OSA} = 295$ mA as before). The NIST tests failed for this data as the complexity of the chaos is lowered compared to the previously discussed injection current of 127 mA. As the laser noise, detector's noise and ADC noise are similar for both tested values of the injection current. We can thus conclude that this noise sources are not sufficient to generate random bits, and the chaotic nature of the signal is needed in our system.

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012

Table 4. Results of NIST SP 800-22 statistical tests, generated from experimental data

Statistical	Test P-Value	Proportion	Decision
Frequency	0.414522	0.986	Success
Block frequency	0.332797	0.990	Success
Runs	0.124180	0.982	Success
Longest run	0.382875	0.993	Success
Rank	0.823129	0.989	Success
Fast Fourier transform	0.425552	0.982	Success
Nonoverlapping template	0.035824	0.987	Success
Overlapping template	0.059191	0.992	Success
Universal	0.811542	0.987	Success
Linear complexity	0.387648	0.982	Success
Serial	0.303309	0.995	Success
Approximate entropy	0.218572	0.986	Success
Cumulative sums	0.803890	0.987	Success
Random excursions	0.182977	0.989	Success
Random excursions variant	0.097517	0.982	Success

6. Concluding remarks

We have theoretically and experimentally demonstrated that SRLs can be used to achieve ultra-fast random numbers through bitwise XOR operation and least significant bit extraction operation. While previously ultra-fast random numbers through bitwise XOR operation from deterministic entropy (chaos) have used two lasers to obtain independent chaotic signals [8], SRLs offer a possibility to use a single laser due to their ability of generating simultaneously two chaotic fluctuations though the exploitation of their two directional modes. Interestingly, notwithstanding the relative low bandwidth of the chaos of about 2 GHz, our bit-streams generated from numerical, as well as from experimental data passed all the NIST tests at 40 Gb/s for suitable parameters [See Fig. 2(b) and Fig. 5(b)]. The fact that the numerical bit-streams generated from noiseless simulations passed all tests suggests at least two conclusions: First, successful multi-bit extraction using ADCs shows that the chaotic waveforms are sufficient to random bit generation. Second, this also evidences that by employing post-processing methods such as derivative [11] or ADC [8, 10] methods, chaos with relative low bandwidth can effectively lead to ultra-fast random numbers generation, even without any additional non-deterministic entropy source (noise).

Acknowledgments

The Authors thank M. C. Soriano, B. Docter and P. Colet for valuable discussions. We acknowledge the Research Foundation Flanders (FWO) for project support and fellowships, the Research Council of the VUB and the Belgian Interuniversity Attraction Pole Network photonics@be. This research was supported by the Hercules Foundation under the project ”High-speed real-time characterization of photonic components” and by the European project PHOCUS (EU FET-Open grant: 240763).

#177551 - $15.00 USD Received 5 Oct 2012; revised 16 Nov 2012; accepted 16 Nov 2012; published 10 Dec 2012