Research Article | Vol. 28, No. 24 / 23 November 2020 / Optics Express 36685
Optics EXPRESS

Gbps physical random bit generation based on the mesoscopic chaos of a silicon photonics crystal microcavity

BINGLEI SHI,[1,4] CIWEI LUO,[1,4] JAIME G. FLOR FLORES,[2] GUOQIANG LO,[3] DIM-LEE KWONG,[3] JIAGUI WU,[1,2,5] AND CHEE WEI WONG[2,6]

[1]College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China
[2]Fang Lu Mesoscopic Optics and Quantum Electronics Laboratory, University of California, Los Angeles, CA 90095, USA
[3]Institute of Microelectronics, A*STAR, 117865, Singapore
[4]These authors had equal contribution.
[5]mgh@swu.edu.cn
[6]cheewei.wong@ucla.edu

Abstract: We present an experimental and theoretical physical random bit (PRB) generator using the mesoscopic chaos from a photonic-crystal optomechanical microcavity with a size of ~10μm and very low operating intracavity energy of ~60 Femto-Joule that was fabricated with CMOS compatible processes. Moreover, two kinds of PRB generation were proposed with rates over gigabits per second (Gbps). The randomness of the large PRB strings was further verified using the NIST Special Publication 800-22. In addition, the Diehard statistical test was also used to confirm the quality of the obtained PRBs. The results of this study can offer a new generation of dedicated PRB solutions that can be integrated on Si substrates, which can speed up systems and eliminate reliance on external mechanisms for randomness collection.

1. Introduction

Random bits play an important role in various aspects of science and engineering, such as materials science, biophysics, finance, and information and internet security [1–4]. However, generating truly random bits is not always easy or practical; hence, deterministic mathematical algorithms that generate pseudo-random bits are sometimes used [5,6]. A true random bit generator uses physical entropy sources to produce true random bits that are unpredictable, unreproducible, and statistically unbiased [7]. Some phenomena that show physical random bit (PRB) entropy sources include the thermal noise of resistors [8], frequency jitter of electronic circuits [9], and polarization jitter of single photons [10]. Typical PRB generation rates using these methods are less than 100Mbps, owing to the collection time required, low entropy signal level, and complex digital post-processing.

In recent years, PRB generation using optical chaos entropy sources has drawn great attention because of its large random fluctuations, high bandwidth, and ease of accessibility [7,11–33]. A 1.7Gbps PRB generator using the optical chaos of semiconductor lasers was first demonstrated by Uchida et al. [7]. Subsequently, emphasis has been placed on enhancing the bit rates that can be produced from the optical chaotic signal. One major enhancement that increased the rate to hundreds of Gbps was proposed by I. Kanter in 2010 [12], and in 2015, using the cascaded chaotic semiconductor lasers, it was increased to terabits per second (Tbps) [25]. Parallel PRB schemes have also been presented [14], and parallel Tbps PRB generation was further developed [26]. In addition, recent advancements in the field include Gbps real-time and all-optical PRB generators [19–32]. However, the problem with all these PRB schemes is that they are based

#404923 https://doi.org/10.1364/OE.404923
Journal © 2020 Received 14 Aug 2020; revised 24 Oct 2020; accepted 26 Oct 2020; published 18 Nov 2020

Optics EXPRESS

on III-V compound (such as InGaAsP) semiconductor lasers, which have fabrication problems because of their inherent incompatibility with silicon technologies. Specifically, these problems arise from lattice mismatch, strained material systems, and complicated band structures that result in a challenging integration of semiconductor lasers with silicon complementary metal oxide semiconductor (CMOS) processes.

Fortunately, advances in the field are now offering new schemes for silicon-based PRB generators. In fact, a silicon Mach–Zehnder modulator has been designed for ultrafast PRB generation [33]. Also, silicon oscillators have also been demonstrated for PRB generation from quantum noise, but its speed of this PRB generator is still limited to a megabits per second (Mbps) level [34]. As a solution to these problems, the development of silicon-based optomechanical microcavities, which was done in the previous years, has made it possible for silicon-based PRB generators to be directly fabricated and integrated with the CMOS processes [35–45]. In this study, the researchers demonstrated the optical chaos generation in a photonic-crystal optomechanical (PhC-OM) microcavity [41], enabling the mixing of optical nonlinearities of two-photon absorption, free-carrier absorption and thermo-optic mechanisms in a sub-wavelength volume, with ultra-high quality factor-to-volume ratios (Q/V) and very low operating intracavity energies.

We experimentally demonstrate, for the first time to our knowledge, the generation of a Gbps PRB based on silicon OM chips. Then, theoretical Gbps-PRB generation was proposed by numerically simulating the optical chaos PhC-OM microcavity. Moreover, the working configurations that can be used with this system, high-order derivatives and parallel combinations, were applied. Finally, the randomness of the generated PRB was evaluated using the National Institute of Standard Technology (NIST) [46] and Diehard tests [47].

2. Experimental setup and results

Figure 1(a) shows the experimental setup for random bit generation based on the chaotic silicon OM chip. In the experiments, the externally driven laser (DL, tunable Santec TSL-510C laser, wavelength 1510-1630 nm) had a detuning rate of 2.285 nm, an injection power of 1.26 mW, and a wavelength of 1541.94 nm. As seen in the figure, the optical signal from the driven laser passes through the optical isolator (IO) to ensure forward transmission. Then it passes through the polarizer to adjust the lateral polarization state of the light to the cavity mode. Next, the light is injected into the PhC-OM microcavity, which is fully compatible with the CMOS processes and has sub-wavelength [$\approx 0.05\ (\lambda/n_{air})^3$] modal volumes (V) [41]. The two-dimensional size of the chip is about 10 μm by 10 μm, even taking the large number of photonic crystal hole structures into account. Moreover, it also possesses a high quality factor to volume ratios (Q/V) [38] and very low operating intracavity energy of ~60 Femto-Joule [41]. By adjusting the injected laser power and frequency tuning, a stable nonlinear chaotic oscillation is generated in the PhC-OM microcavity, which is then measured and converted into electricity by a photodetector (PD, New Focus Model 1811). The signal is sent to a digital oscilloscope (Tektronix TDS 7404) and spectrum analyzer (Agilent N9000A) for chaotic data acquisition. The PhC-OM microcavity was fabricated with a CMOS-compatible process on 8-inch silicon wafers, using 248 nm deep-ultraviolet lithography and reactive ion etching on 250 nm thick silicon-on-insulator membranes [41]. A width-modulated line-defect was also introduced into the photonic crystal structure that formed a high Q and an ultra-small modal volume optical resonance cavity. The laser couples into the nanocavity and stimulates chaos through optomechanical oscillation (OMO) and silicon nonlinear oscillation mainly with the help of two-photon absorption and free carrier dissipation. Figure 1(b) shows the temporal waveforms of mesoscopic chaos.

In Fig. 2(a), using the first parallel combination method [1,18], the independent silicon microcavity chips were used to generate several irrelevant chaotic signals that could be linearly combined. Seven intervals from τ_1 to τ_7 as 136.8 ns, 157.6 ns, 205.6 ns, 224.8 ns, 240.8

Optics EXPRESS

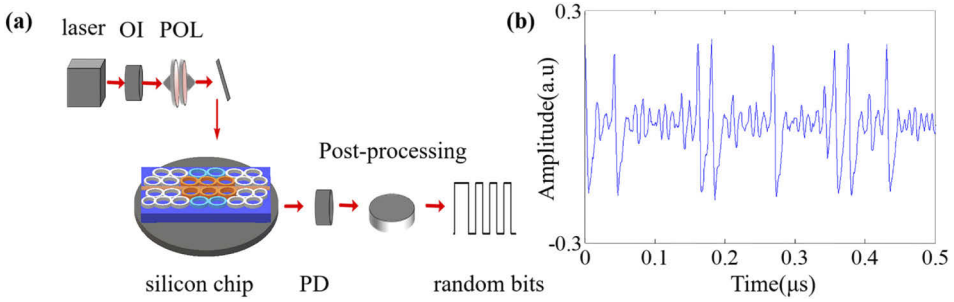

Fig. 1. Experimental setup for optical chaos and PRB generation. (a) Experimental setup for random bits generation, OI: optical isolator; POL: polarizer; PD: photodetector, and (b) Temporal waveforms output directly from microcavity.

ns, 293.6 ns, 317.6 ns were set. Then the 2.5GHz 8-bit analog-to-digital converter (ADC) was implemented for sampling. The 312.5 MHz sampling rate was set to ensure randomness [20]. Next, the self-delay (delay time set to 1 μs) bitwise exclusive-OR (XOR) was operated and the least significant bit (LSB) from each 8-bit sampling was extracted to obtain the PRB sequence. Figures 2(b) to (e) show the results of using combination post-processing. Figures 2(b) presents the processed chaotic waveform and the random sequence generated after thresholding samples were chosen in the processed chaotic waveform. Moreover, as shown in Fig. 2(c), the cumulative probability deviation of the uniform distribution under different LSBs is given, and the probability distribution of the retained 4-LSB is shown in the inset. Here, the cumulative probability deviation of uniform distribution is defined as: $\Delta = \sum_{i=0}^{2^N-1} |P_i - 2^{-N}|$, where the P_i is the distribution probability of retaining N-LSB, and i is the decimal integer between 0 and 2^N-1. Clearly, with an increasing number of retained LSBs, the cumulative probability deviation of the uniform distribution gradually, and to a significant degree, becomes higher than 0.001. This demonstrates that the 1, 2, 3, 4, and 5-LSB cases have good uniform distribution until 6-LSB are retained. As shown in Fig. 2(d), the researchers tested the statistical bias of the retained 4, 5, and 6-LSB sequence. The statistical bias B is defined as: $B = p_1 - 0.5$, where p_1 is the probability of "1" in the bit sequence. The bias level is considered qualified if it is lower than 3-sigma criterion ($3\sigma = 1.5/\sqrt{N}$ where N is the number of random bits) [15,27,28,31]. With an increasing number of retained LSBs, the bias gradually increases above the 3σ standard line. Figure 2(e) shows the autocorrelation coefficient denoted by the 4-LSB bits sequence. The serial autocorrelation coefficient C_k is defined as: $C_k = (a_i - a_i) \times (a_{i+k} - a_i)/(a_i - a_i)^2$, where a_i is the bit of "1" or "0", k is the bit lag, and the averaging (denoted as ...) is performed over index i [19]. In addition, it can be assumed that it is internally independent of the random sequence autocorrelation coefficient, which remains below 3σ line ($3\sigma = (3/\sqrt{N})$ where N is the number of random bits).

The NIST tests were used to evaluate the statistical randomness of bit sequences [46]. For NIST test's 'success', the P-value should be larger than 0.0001 and the proportion should be in the range of 0.99±0.0094392 using 1000 samples of 1 M bit data with a significance level of $\alpha = 0.01$. For the tests that produce multiple P-values and proportions, the worst case is given. As shown in Table 1, the experimental bit sequences for 4-LSB passed all 15 NIST tests, which indicates that the random bits are qualified. But for the 5-LSB case, one part of the NIST test, which is called as nonoverlapping-templates failed. Even the value of cumulative probability deviation of 5-LSB case is lower than 0.001 as shown in Fig. 2(c). Therefore, the 4-LSB was fixed as the system condition for the qualified PRB sequence and the corresponding speed of the PRB is 1.25Gbps (=4bits ×312.5 MHz).

Optics EXPRESS

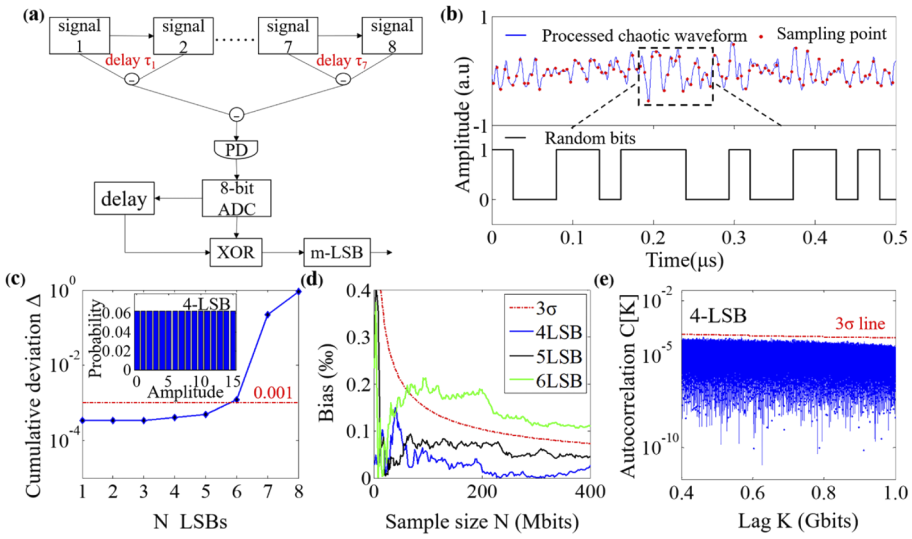

Fig. 2. Schematic diagram and results using the combination processing. (a) The schematic diagram of parallel combination processing, (b) Processed chaotic waveform, and random sequence generated after thresholding samples chosen in chaotic waveform (c) The cumulative probability deviation of uniform distribution under different LSBs, and the inset shows the distribution probability of different intensity values in each unit of 4-LSB, (d) The statistical bias of random sequence with 4, 5, 6-LSB, and (e) Autocorrelation coefficient denoted 4-LSB bits sequence.

Table 1. Results of NIST test for combination processing

NIST Test	4-LSB			5-LSB		
	P-value	Proportion	Result	P-value	Proportion	Result
Frequency	0.088762	0.9880	Success	0.729870	0.9870	Success
Block-frequency	0.254411	0.9900	Success	0.603841	0.9850	Success
Cumulative-sums	0.208837	0.9820	Success	0.579021	0.9880	Success
Runs	0.410055	0.9870	Success	0.616305	0.9890	Success
Longest-run	0.514124	0.9880	Success	0.380407	0.9880	Success
Rank	0.005054	0.9910	Success	0.035640	0.9900	Success
FFT	0.365253	0.9880	Success	0.006379	0.9930	Success
Nonoverlapping-templates	0.001568	0.9920	Success	0.591409	0.9790	Fail
Overlapping-templates	0.741918	0.9870	Success	0.158133	0.9850	Success
Universal	0.801865	0.9900	Success	0.947308	0.9890	Success
Approximate entropy	0.363593	0.9910	Success	0.081013	0.9910	Success
Random-excursions	0.193194	0.9873	Success	0.007127	0.9904	Success
Random-excursions-variant	0.013013	0.9889	Success	0.018934	0.9904	Success
Serial	0.085587	0.9930	Success	0.045971	0.9890	Success
Linear-complexity	0.316052	0.9870	Success	0.516113	0.9930	Success

Optics EXPRESS

Figure 3(a) shows the second PRB scheme using high-order discrete time derivative processing [11,12]. In the high-order derivative method, the chaos was firstly digitized with an 8-bit ADC, and multiple alterable delay digitized signals were used to calculate the *n*th discrete derivative. Then, the processed signal was operated and the *n*th derivative was selected as m-LSB to receive the PRB sequence, in which the selected unit buffer time was 0.6176 μs. Figure 3(b) presents the sampling diagram of the chaotic signal with an 8-bit ADC. The red dots in the figure represents the sampling data points. To reduce the autocorrelation of the chaotic signal, the researchers selected 312.5 MHz sampling rate for data quantization. The calculation of cumulative deviation is also shown in Fig. 3(c). The cumulative deviation increases along the enhancing order of LSB and finally became higher than the criterion, which is 0.001 for 6, 7, 8-LSB cases. Moreover, the inset of Fig. 3(c) shows the static distribution of extracting 5-LSB case, which demonstrated an even probability. In Fig. 3(d), the statistical bias of random sequence is given for 4, 5, 6-LSB cases, and the bias evolutions are all below the 3σ line. Figure 3(e) gives the autocorrelation of bit sequence with 5-LSB, and the value of autocorrelation coefficient is lower than the standard 3-sigma criterion. The detailed NIST test results are shown in Table 2. Both 4-LSB case and 5-LSB case pass all the 15 test terms of NIST, which indicates a better performance of derivative processing in eliminating the possible overlapping pattern of bit sequences. Therefore, the researchers fixed 5-LSB as the condition for the qualified PRB with the corresponding speed of 1.56Gbps (=5bits×312.5 MHz).

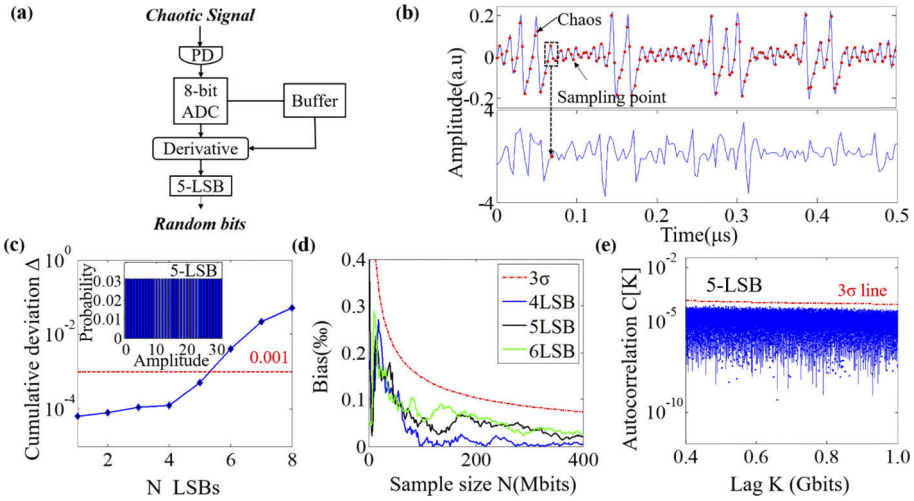

Fig. 3. Schematic diagram and results using 5th-order discrete time derivative processing. (a) Scheme of high-order discrete time derivative processing, (b) A sampling diagram of the chaotic entropy source, (c) The cumulative probability deviation of uniform distribution under different LSBs, and the inset shows the distribution probability of different intensity values in each unit of 5-LSB, (d) The statistical bias of random sequence with 4, 5, 6-LSB, and (e) Autocorrelation coefficient denoted 5-LSB bits sequence.

Optics EXPRESS

Table 2. Results of NIST test for 5th-order discrete time derivative processing

NIST Test	4-LSB			5-LSB		
	P-value	Proportion	Result	P-value	Proportion	Result
Frequency	0.524101	0.9900	Success	0.004365	0.9920	Success
Block-frequency	0.832561	0.9880	Success	0.856359	0.9940	Success
Cumulative-sums	0.211064	0.9920	Success	0.050305	0.9910	Success
Runs	0.478839	0.9880	Success	0.401199	0.9890	Success
Longest-run	0.154629	0.9930	Success	0.761719	0.9930	Success
Rank	0.504219	0.9870	Success	0.725829	0.9940	Success
FFT	0.624627	0.9870	Success	0.618385	0.9900	Success
Nonoverlapping-templates	0.002657	0.9910	Success	0.005091	0.9930	Success
Overlapping-templates	0.892036	0.9860	Success	0.347257	0.9880	Success
Universal	0.908706	0.9880	Success	0.402962	0.9880	Success
Approximate entropy	0.955835	0.9810	Success	0.028434	0.9910	Success
Random-excursions	0.043822	0.9836	Success	0.042595	0.9862	Success
Random-excursions-variant	0.019935	0.9810	Success	0.218563	0.9893	Success
Serial	0.118120	0.9910	Success	0.811080	0.9900	Success
Linear-complexity	0.975012	0.9910	Success	0.542228	0.9910	Success

3. Theoretical simulations

The theoretical model used in the study is based on the nonlinear coupled-mode theory [42–45]. Optical chaos is produced from the OM microcavity due to a series of nonlinearities, mainly by two-photo absorption (TPA), and free carrier dynamical effects. The specific equations are as follows [41]:

$$\frac{d^2x}{dt^2} + \Gamma_m \frac{dx}{dt} + \Omega_m^2 x(t) = \frac{g_0}{\omega_0}\sqrt{\frac{2\Omega_m}{\hbar m_{eff}}}|A(t)|^2 \tag{1}$$

where x is the motional displacement and A is the intracavity E-field amplitude.

$$\begin{aligned}\frac{dA}{dt} =& i\left(-g_0\sqrt{\frac{2m_{eff}\Omega_m}{\hbar}}x(t) + \frac{\omega_0}{n_{Si}}\left(\frac{dn_{Si}}{dT}\Delta T(t) + \frac{dn_{Si}}{dN}N(t)\right) + \sigma\omega\right)A(t) \\ &- \frac{1}{2}\left(\gamma_i + \gamma_e + \frac{\Gamma_{TPA}\beta_{Si}c^2}{V_{TPA}n_g^2}|A(t)|^2 + \frac{\sigma_{Si}cN(t)}{n_g}\right)A(t) + \sqrt{\gamma_e P_{in}}\end{aligned} \tag{2}$$

N is the free-carrier density, and ΔT represents the local-cavity temperature variation.

$$\frac{dN}{dt} = -\frac{N(t)}{\tau_{fc}} + \frac{\Gamma_{FCA}\beta_{Si}c^2}{2\hbar\omega_0 n_g^2 V_{FCA}^2}|A(t)|^4 \tag{3}$$

ω_0 is the photonic-crystal cavity resonance.

$$\frac{d\Delta T}{dt} = -\frac{\Delta T(t)}{\tau_{th}} + \frac{\Gamma_{PhC}}{\rho_{Si}c_p V_{PhC}}\left(\gamma_i + \frac{\Gamma_{PhC}\beta_{Si}c^2}{V_{TPA}n_g^2}|A(t)|^2 + \frac{\sigma_{Si}cN(t)}{n_g}\right)|A(t)|^2 \tag{4}$$

Based on these equations, the researchers simulated the chaos, sampled the waveform using parallel combination of post-processing steps, and finally obtained the PRB. The main parameters are listed in Table 3, and more detailed parameters can be found in Ref. [41].

Optics EXPRESS

Table 3. Results of NIST test for combination processing

Symbol	Meaning	Value
g_0	Vacuum OM coupling strength	690kHz
λ_0	Resonance wavelength	1572.8nm
Γ_{TPA}	TPA confinement factor	0.8012
V_{TPA}	TPA mode volume	$6.4\times10^{-19}m^3$
β_{si}	TPA coefficient	$8.4\times10^{-12}m/W$

Figure 4 shows the results of the model simulation. In Fig. 4(a), it shows that eight chaotic signals were used with the same delay time τ setting as 200 ns. The self-delay time is optimized to 280 ns in XOR operation. Figure 4(b) plots the output waveform of the amplitude with the time-delay module. This time delay was set to 0.5 μs. Figure 4(c) shows the cumulative deviation after sampling and is quantified by the 8-bit ADC, where the inset is the statistical distribution of the 5-LSB case. Figure 4(d) presents the bias evolution of bit sequences with different orders of LSBs. The bias curves of 4, 5, 6-LSB cases are all lower than that of the 3σ criterion. It is interesting that the bias of 6-LSB still meet the 3σ criterion considering the similar parallel combination processing used in Fig. 2. As a result, the theoretical result is little better than that of the experimental result in Fig. 2, and it indicates the experimental possibility of 6-LSB optimization with higher PRB speed in future. Figure 4(e) also shows the autocorrelation coefficient of the 5-LSB case. Furthermore, we tested the simulated bit sequences with both NIST tests (Table 4) and Diehard tests (Table 5). All tested terms show the good P-values and qualified randomness of 1.56 Gbps PRB. Therefore, the theoretical simulation basically is confirmed with the experimental observation, and 5-LSB is an optimized setting for the qualified PRB generation in silicon PhC-OM microcavity scheme.

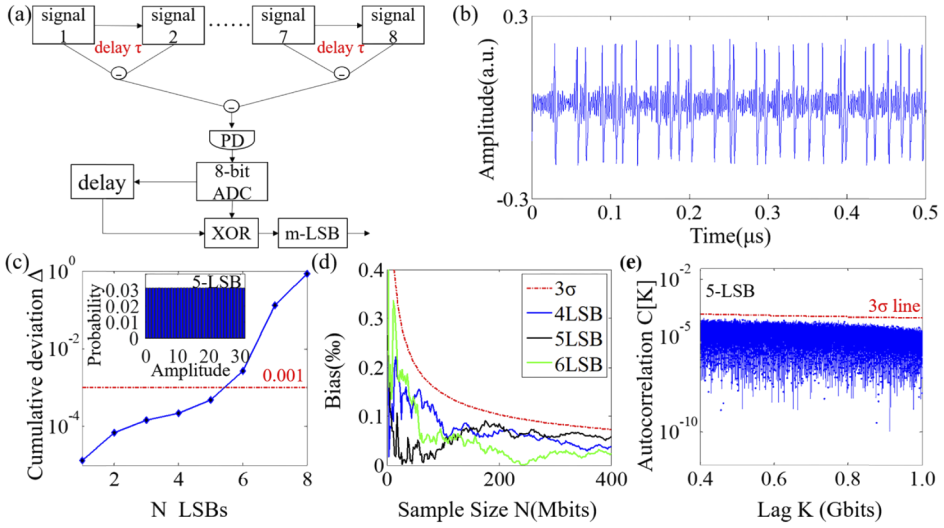

Fig. 4. Results of simulation. (a) The schematic diagram of parallel combination processing in simulation, (b) Chaos output from OM microcavity according to equations, (c) Statistical distribution of extracting 5-LSB after sampling, and the inset shows the distribution probability of different intensity values in each unit of 5-LSB, (d) The statistical bias of random sequences from 4 to 6-LSB, (e) Autocorrelation coefficient denoted 5-LSB bits sequence.

Optics EXPRESS

Table 4. Results of NIST tests for theoretical random bits

NIST Test	5-LSB			6-LSB		
	P-value	Proportion	Result	P-value	Proportion	Result
Frequency	0.046870	0.9820	Success	0.821681	0.9929	Success
Block-frequency	0.310049	0.9920	Success	0.000000	0.9957	Fail
Cumulative-sums	0.262249	0.9820	Success	0.905681	0.9943	Success
Runs	0.322135	0.9960	Success	0.784665	0.9943	Success
Longest-run	0.227180	0.9840	Success	0.229900	0.9886	Success
Rank	0.138860	0.9900	Success	0.007694	0.9829	Success
FFT	0.357000	0.9940	Success	0.359816	0.9814	Success
Nonoverlapping-templates	0.023545	0.9900	Success	0.017051	0.9857	Success
Overlapping-templates	0.973055	0.9960	Success	0.616305	0.9829	Success
Universal	0.747898	0.9960	Success	0.024711	0.9771	Fail
Approximate entropy	0.177628	0.9900	Success	0.403718	0.9929	Success
Random-excursions	0.371778	0.9809	Success	0.082177	0.9978	Success
Random-excursions-variant	0.010913	0.9841	Success	0.060662	0.9802	Success
Serial	0.295391	0.9920	Success	0.291702	0.9929	Success
Linear-complexity	0.331408	0.9940	Success	0.308349	0.9900	Success

Table 5. Typical results of "Diehard" tests and KS – Kolmogorov – Smirnov test for 5, 6-LSB theoretical random bits. Significance level "α=0.01". For tests with multiple P-value, the worst case is shown.

Diehard Test	5-LSB		6-LSB	
	P-value	Result	P-value	Result
Birthday Spacing	0.557335 [KS]	Success	0.142988 [KS]	Success
Overlapping 5-permutation	0.320607	Success	0.000278	Fail
Binary rank for 32×32 matrices	0.404728	Success	0.001549	Fail
Binary rank for 31×31 matrices	0.476911	Success	0.132853	Success
Binary rank for 6×8 matrices	0.271619 [KS]	Success	0.147696 [KS]	Success
Bitstream	0.181557	Success	0.555678	Success
Overlapping-Paris-Sparce-Occupancy	0.090388	Success	0.111576	Success
Overlapping-Quadruples-Sparce-Occupancy	0.065230	Success	0.114424	Success
DNA	0.180568	Success	0.164406	Success
Count-the-1's on a stream of bytes	0.203351	Success	0.330072	Success
Count-the-1's for specific bytes	0.086634	Success	0.142988	Success
Parking lot	0.886162 [KS]	Success	0.557335 [KS]	Success
Minimum distance	0.862823 [KS]	Success	0.616305 [KS]	Success
3D spheres	0.922855 [KS]	Success	0.469505 [KS]	Success
Squeeze	0.603841	Success	0.258494	Success
Overlapping	0.178604 [KS]	Success	0.330072 [KS]	Success
Runs	0.075949 [KS]	Success	0.132858 [KS]	Success
Craps	0.219856	Success	0.276921	Success

Optics EXPRESS

Limited by the chaos bandwidth of current silicon microcavity, less than 2Gbps PRB were generated. It is also noted that, tens GHz silicon optomechanical microcavities have been proposed [48,49,50], and that hundreds Gbps PRB could be expected if using the tens GHz chaos of optomechanical oscillators. When compared to traditional PRB schemes of semiconductor lasers, it is clear that the integrated Si microcavity scheme has a great potential for miniaturization and direct CMOS process compatibility.

4. Conclusion

In conclusion, based on optical chaos from OM silicon microcavity, the researchers experimentally and theoretically developed a physical random bit generator. In the experiments, the parallel combination processing and high-order discrete time derivative processing with 1.25Gbps PRB and 1.56Gbps PRB, respectively were used. They all successfully passed the NIST SP 800-22 standard test. Theoretically, the researchers calculated the model, obtained 1.56Gbps PRB, and qualified it with both NIST SP 800-22 and Diehard tests. This silicon-microcavity based PRB generators could be easily integrated and scaled, which not only helps to greatly reduce the size and cost of PRB generators, but this could also be useful in developing new chip scale physics information security solutions.

Funding

National Natural Science Foundation of China (11474233, 61875168); China Postdoctoral Science Foundation (2017M612885); Chongqing Postdoctoral Science Foundation (Xm2017008); Fundamental Research Funds for the Central Universities (XDJK2019B059).

Disclosures

The authors declare no conflicts of interest.

References

1. S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis* (Springer-Verlag, 2007).
2. N. Metropolis and S. Ulam, "The Monte Carlo method," J. Am. Stat. Assoc. **44**(247), 335–341 (1949).
3. D. R. Stinson, *Cryptography: Theory and Practice* (CRC, 1995).
4. R. G. Gallager, *Principles of Digital Communication* (Cambridge University, 2008).
5. B. A. Wichman and I. D. Hill, "Algorithm AS 183: An Efficient and Portable Pseudo-random-Number Generator," Appl. Stat. **31**(2), 188–190 (1982).
6. M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," ACM Trans. Model. Comput. Simul. **8**(1), 3–30 (1998).
7. 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**(12), 728–732 (2008).
8. C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I **47**(5), 615–621 (2000).
9. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC," IEEE Trans. Comput. **52**(4), 403–409 (2003).
10. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Opt. **47**(4), 595–598 (2000).
11. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**(2), 024102 (2009).
12. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).
13. 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**(6), 5512–5524 (2010).
14. J. G. Wu, X. Tang, Z. M. Wu, G. Q. Xia, and G. Y. Feng, "Parallel generation of 10 Gbits/s physical random number streams using chaotic semiconductor lasers," Laser Phys. **22**(10), 1476–1480 (2012).

Optics EXPRESS

15. Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 850 Gb/s," IEEE Photonics Technol. Lett. **24**(12), 1042–1044 (2012).
16. J. Zhang, Y. Wang, M. Liu, L. Xue, P. Li, A. Wang, and M. Zhang, "A robust random number generator based on differential comparison of chaotic laser signals," Opt. Express **20**(7), 7496–7506 (2012).
17. R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, "Fast random bits generation based on a single chaotic semiconductor ring laser," Opt. Express **20**(27), 28603–28613 (2012).
18. W. Li, I. Reidler, Y. Aviad, Y. Huang, H. Song, Y. H. Zhang, M. Rosenbluh, and I. Kanter, "Fast physical random-number generation based on room-temperature chaotic oscillations in weakly coupled superlattices," Phys. Rev. Lett. **111**(4), 044102 (2013).
19. A. Wang, P. Li, J. Zhang, J. Zhang, L. Li, and Y. Wang, "4.5 Gbps high-speed real-time physical random bit generator," Opt. Express **21**(17), 20452–20462 (2013).
20. X. Z. Li and S. C. Chan, "Heterodyne random bit generation using an optically injected semiconductor laser in chaos," IEEE J. Quantum Electron. **49**(10), 829–838 (2013).
21. N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Fast random bit generation using a chaotic laser: approaching the information theoretic limit," IEEE J. Quantum Electron. **49**(11), 910–918 (2013).
22. X. Fang, B. Wetzel, J. M. Merolla, J. M. Dudley, L. Larger, C. Guyeux, and J. M. Bahi, "Noise and chaos contributions in fast random bit sequence generated from broadband optoelectronic entropy sources," IEEE Trans. Circuits Syst. I **61**(3), 888–901 (2014).
23. M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," Opt. Express **22**(14), 17271–17280 (2014).
24. N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," Opt. Express **22**(6), 6634–6646 (2014).
25. 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. Express **23**(2), 1470–1490 (2015).
26. X. Tang, Z. M. Wu, J. G. Wu, T. Deng, J. J. Chen, L. Fan, Z. Q. Zhong, and G. Q. Xia, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," Opt. Express **23**(26), 33130–33141 (2015).
27. T. Butler, C. Durkan, D. Goulding, S. Slepneva, B. Kelleher, S. P. Hegarty, and G. Huyet, "Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser," Opt. Lett. **41**(2), 388–391 (2016).
28. A. Pandey, A. Sharma, and P. K. Krishnamurthy, "16 Gbps random bit generation using chaos in near-symmetric erbium-doped fiber ring laser," Appl. Opt. **56**(34), 9526 (2017).
29. A. Wang, L. Wang, P. Li, and Y. C. Wang, "Minimal-post-processing 320-Gbps true random bit generation using physical white chaos," Opt. Express **25**(4), 3153–3164 (2017).
30. P. Li, Y. Sun, X. Liu, X. Yi, J. Zhang, X. Guo, Y. Guo, and Y. Wang, "Fully photonics-based physical random bit generator," Opt. Lett. **41**(14), 3347–3350 (2016).
31. P. Li, J. Zhang, L. Sang, X. Liu, Y. Guo, X. Guo, A. Wang, K. A. Shore, and Y. Wang, "Real-time online photonic random number generation," Opt. Lett. **42**(14), 2699–2702 (2017).
32. P. Li, Y. Guo, Y. Guo, Y. Fan, X. Guo, X. Liu, K. Li, K. A. Shore, Y. Wang, and A. Wang, "Ultrafast fully photonic random bit generator," J. Lightwave Technol. **36**(12), 2531–2540 (2018).
33. W. J. Tian, L. Zhang, J. F. Ding, S. Z. Shao, X. Fu, and L. Yang, "Ultrafast physical random bit generation from a chaotic oscillator with a silicon modulator," Opt. Lett. **43**(19), 4839–4842 (2018).
34. Y. Okawachi, M. J. Yu, K. Luke, D. O. Carvalho, M. Lipson, and A. L. Gaeta, "Silicon-chip-based quantum random number generator," in *Conference on Lasers and Electro-Optics*, OSA Technical Digest (online) (Optical Society of America, 2017), paper SM1M.1.
35. T. J. Kippenberg, H. Rokhsari, T. Carmon, A. Scherer, and K. J. Vahala, "Analysis of radiation-pressure induced mechanical oscillation of an optical microcavity," Phys. Rev. Lett. **95**(3), 033901 (2005).
36. T. J. Kippenberg and K. J. Vahala, "Cavity optomechanics: back-action at the mesoscale," Science **321**(5893), 1172–1176 (2008).
37. T. Yamamoto, M. Notomi, H. Taniyama, E. Kuramochi, Y. Yoshikawa, Y. Torii, and T. Kuga, "Design of a high-Q air-slot cavity based on a width-modulated line-defect in a photonic crystal slab," Opt. Express **16**(18), 13809–13817 (2008).
38. J. Gao, J. F. McMillan, M. C. Wu, J. J. Zheng, S. Assefa, and C. W. Wong, "Demonstration of an air-slot mode-gap confined photonic crystal slab nanocavity with ultrasmall mode volumes," Appl. Phys. Lett. **96**(5), 051123 (2010).
39. F. Monifi, J. Zhang, ŞK Özdemir, B. Peng, Y. X. Liu, F. Bo, F. Nori, and L. Yang, "Optomechanically induced stochastic resonance and chaos transfer between optical fields," Nat. Photonics **10**(6), 399–405 (2016).
40. D. Navarro-Urrios, N. E. Capuj, M. F. Colombano, P. D. Garcıa, M. Sledzinska, F. Alzina, A. Griol, A. Martınez, and C. M. Sotomayor-Torres, "Nonlinear dynamics and chaos in an optomechanical beam," Nat. Commun. **8**(1), 14965 (2017).
41. J. G. Wu, S. W. Huang, Y. J. Huang, H. Zhou, J. H. Yang, J. M. Liu, M. B. Yu, G. Q. Lo, D. L. Kwong, S. K. Duan, and C. W. Wong, "Mesoscopic chaos mediated by Drude electron-hole plasma in silicon optomechanical oscillators," Nat. Commun. **8**(1), 15570 (2017).

Optics EXPRESS

42. T. J. Johnson, M. Borselli, and O. Painter, "Self-induced optical modulation of the transmission through a high-Q silicon microdisk resonator," Opt. Express **14**(2), 817–831 (2006).
43. M. Aspelmeyer, T. J. Kippenberg, and F. Marquardt, "Cavity optomechanics," Rev. Mod. Phys. **86**(4), 1391–1452 (2014).
44. M. H. Zadeh and K. J. Vahala, "An optomechanical oscillator on a silicon chip," IEEE J. Sel. Top. Quantum Electron. **16**(1), 276–287 (2010).
45. D. M. Abrams, A. Slawik, and K. Srinivasan, "Nonlinear oscillations and bifurcations in silicon photonic microresonators," Phys. Rev. Lett. **112**(12), 123901 (2014).
46. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dary, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800–22, Revision 1a (2010).
47. G. Marsaglia, DIEHARD: A battery of tests of randomness, (1996). http://stat.fsu.edu/geo
48. X. Sun, J. Zheng, M. Poot, C. W. Wong, and H. X. Tang, "Femtogram doubly clamped nanomechanical resonators embedded in a high-Q two-dimensional photonic crystal nanocavity," Nano Lett. **12**(5), 2299–2305 (2012).
49. H. Li, S. A. Tadesse, Q. Liu, and M. Li, "Nanophotonic cavity optomechanics with propagating acoustic waves at frequencies up to 12GHz," Optica **2**(9), 826–831 (2015).
50. Y. A. V. Espinel, F. G. S. Santos, G. O. Luiz, T. P. M. Alegre, and G. S. Wiederhecker, "Brillouin Optomechanics in Coupled Silicon Microcavities," Sci. Rep. **7**(1), 43423 (2017).