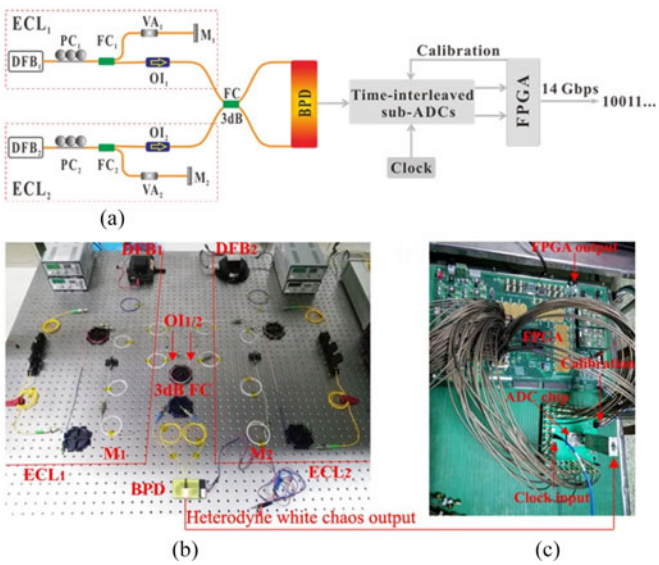
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Real-Time 14-Gbps Physical Random Bit Generator Based on Time-Interleaved Sampling of Broadband White Chaos

Volume 9, Number 2, April 2017

Longsheng Wang
Tong Zhao
Daming Wang
Danyu Wu
Lei Zhou
Jin Wu
Xinyu Liu
Yuncai Wang
Anbang Wang, *Member, IEEE*



DOI: 10.1109/JPHOT.2017.2690462
1943-0655

Real-Time 14-Gbps Physical Random Bit Generator Based on Time-Interleaved Sampling of Broadband White Chaos

Longsheng Wang,[1] Tong Zhao,[1] Daming Wang,[1] Danyu Wu,[2] Lei Zhou,[2] Jin Wu,[2] Xinyu Liu,[2] Yuncai Wang,[2] and Anbang Wang,[1] *Member, IEEE*

[1]Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, and College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China
[2]Institute of Microelectronics of Chinese Academy of Sciences, Beijing 100029, China

DOI:10.1109/JPHOT.2017.2690462

Manuscript received January 30, 2017; revised March 28, 2017; accepted March 30, 2017. Date of publication April 3, 2017; date of current version April 18, 2017. This work was supported in part by the National Nature Science Foundation of China under Grant 61475111 and Grant 61671316, in part by the Natural Science Foundation for Excellent Young Scientists of Shanxi under Grant 2015021004, in part by the Program for the Innovative Talents of Higher Learning Institutions of Shanxi, and in part by the International Science and Technology Cooperation Program of China and Shanxi under Grant 2014DFA50870 and Grant 201603D421008. Corresponding author: A. Wang (e-mail: wanganbang@tyut.edu.cn).

Abstract: We experimentally demonstrate a real-time high-speed physical random bit generator using the time-interleaved sampling of broadband white chaos. The white chaos is generated by optical heterodyning of two external-cavity feedback laser diodes. It has a white-noise-like spectrum with a 3-dB bandwidth of 16.7 GHz and a symmetric amplitude distribution and has no time-delay signatures of the external feedback cavities. An analog-to-digital converter (ADC) chip integrated by two time-interleaved sub-ADCs with a maximum sampling rate of 7 GHz is utilized to discretize the white chaos into parallel binary streams. After real-time interleaving combination and exclusive-OR operation in the field-programmable gate array (FPGA), a 14-Gbps binary stream with verified randomness is achieved.

Index Terms: Semiconductor lasers, heterodyning, ultrafast nonlinear processes.

1. Introduction

Random bit generators (RBGs) are crucial for a broad spectrum of applications in cryptography [1], communications [2], [3] as well as numerical computations and simulations [4], [5]. For above applications, two kinds of RBGs including pseudo RBGs and physical RBGs are considered [6]. Pseudo RBGs can produce random bits with rates of several Gbps in real time using initial seeds and computer algorithms. But they are not perfectly random or unpredictable since the seeds and algorithms are entirely deterministic. Physical RBGs originate from physical stochastic phenomena such as thermal noise from resistor [7] and frequency jitter of oscillator [8] providing high-quality randomness. However, limited by the bandwidth, the real-time generation rates are restricted at the magnitude of Mbps and far from satisfying requirements of practical applications. Especially for security-oriented applications, the high-speed real-time physical RBGs are in great request.

In recent years, photonic broadband entropy sources such as amplified spontaneous emission [9]–[11], laser phase fluctuations [12]–[14], and laser chaos [15]–[17] have been widely investigated for generating high-speed physical random bits. In particular, chaotic external-cavity semiconductor laser (ECL) has attracted intensive attention because of its large amplitude and wide bandwidth [15]–[33]. In 2008, Uchida *et al.* firstly generated 1.7-Gbps random bits using the ECL with single-bit extraction [15]. Shortly afterwards, Reidler *et al.* improved the generation speed to 12.5 Gbps with multi-bit extraction [18]. Since then, many ECL-based schemes with multi-bit extraction were proposed consecutively because of the intriguing generation rates [18]–[29]. For example, Kanter *et al.* demonstrated 300-Gbps (15 bits extracted $\times$ 20 GHz sampling rate) random bit generation [21]. Akizawa *et al.* reported a 400-Gbps (8 bits extracted $\times$ 50 GHz sampling rate) generation rate [23]. However, such fast generation rates were only demonstrated in theory and have not been achieved with real-time output. This is because, in the multi-bit extraction demonstrations, the intensity output of ECL is usually digitized by the commercial oscilloscope and then offline processed with least-significant-bit retention followed by other post-processing methods such as derivative, exclusive-OR (XOR), and bit-order reversal. Differently, for single-bit extraction, the intensity output of ECL can be directly digitized by 1-bit ADC and then processed with XOR device. Such extraction has enabled the real-time generation of random bits with rates of 1.7, 2.08, and 4.5 Gbps [15], [30], [31].

Unfortunately, further increasing the real-time generation rate with single-bit extraction encounters restrictions. This is firstly due to ECL's sharp power spectrum which limits spectral bandwidth and flatness. The narrow bandwidth and uneven spectrum restrict ADC's sampling rate and bandwidth-utilization efficiency in random bit generation, respectively [27]. In addition, two other inherent defects of ECL including asymmetric amplitude distribution and time-delay signature, which introduce disequilibrium and correlation of random bits respectively, are also responsible for restricting the generation rate [32], [33]. Although much effort has been devoted to enhancing bandwidth [19], [23], [27], optimizing amplitude distribution [18], [21], and suppressing time-delay signature [22], [24], [28], simultaneously eliminating these defects to generate faster physical random bits in real time has yet to be achieved.

Our previous work found that optical heterodyning of two ECLs can readily obtain a white-noise-like broadband chaos which not only has a symmetric amplitude distribution but also has no time-delay signature [34]. By harnessing the white chaos as entropy source, we experimentally demonstrate a real-time 14-Gbps physical RBG through single-bit quantization of the time-interleaved sub-ADCs and post-processing of the field-programmable gate array (FPGA).

The remainder of this paper is organized as follows. Section 2 presents the experimental setup of RBG. Section 3 describes the experimental results including generation of white chaos in part A, 7-Gbps parallel RBG in part B, and 14-Gbps RBG in part C. After a discussion offered in Section 4, the paper ends with a brief conclusion in Section 5.

2. Experimental Setup

The schematic diagram of the experimental setup for real-time generation of physical random bits is shown in Fig. 1(a). It includes two parts: generation and quantization of white chaos, corresponding to which the experimental components are shown in Fig. 1(b) and (c), respectively.

For generation of white chaos, two ECLs are constructed, each of which has a distributed feedback (DFB) semiconductor laser subject to optical feedback from a fiber mirror ($M_{1/2}$). The laser facet and the fiber mirror comprise a feedback external cavity. In the feedback cavity, a polarization controller ($PC_{1/2}$) is used to match the polarization state of feedback light to that of the laser, and a variable attenuator ($VA_{1/2}$) is utilized to adjust the feedback strength to change the dynamic state of the laser. After optical isolator ($OI_{1/2}$), the outputs of two ECLs are mixed through a 3-dB fiber coupler (FC), and then the optical heterodyne signal is detected by a balanced photodetector (BPD). The heterodyne signal is expressed as $2(I_1 I_2)^{1/2}\sin(2\pi\Delta\nu t + \varphi_2 - \varphi_1)$, where $I_{1,2}$ and $\varphi_{1,2}$ are the intensity and phase of lasers $DFB_{1/2}$, and $\Delta\nu$ is the optical frequency difference of two lasers.

The heterodyne signal is then differentially coupled into our own ADC chip fabricated with time-interleaved sub-ADCs [35], which is a common way to overcome the limitation of electronic

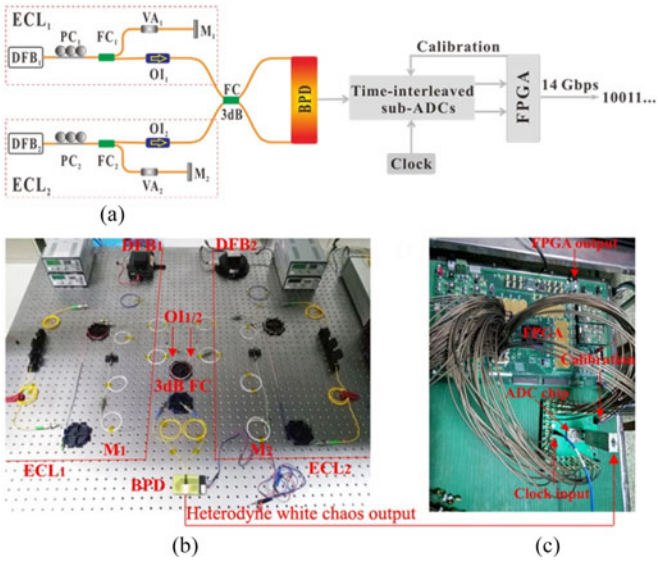


Fig. 1. Structure of RBG. (a) Schematic diagram of real-time physical RBG. (b) Experimental setup of generating white chaos. (c) Experimental setup of quantizing white chaos which includes on-chip ADC and FPGA board. $DFB_{1/2}$: distributed feedback semiconductor laser; $PC_{1/2}$: polarization controller; $FC_{1/2}$, FC: 3-dB fiber coupler; $VA_{1/2}$: variable attenuator; $OI_{1/2}$: optical isolator; $M_{1/2}$: fiber mirror; BPD: balanced photodetector; FPGA: field-programmable gate array. The arrows in Fig. 1(b) indicate the transmission directions of $OI_{1/2}$.

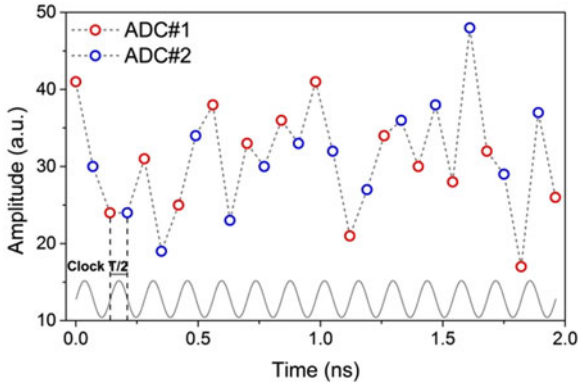


Fig. 2. Schematic diagram of time-interleaved sampling.

bottleneck of ADC and achieve sampling rate over ten GHz. The sampling rate of the ADC chip can be tuned by changing the number of sub-ADCs and the rate of clock signal. In our experiments, two sub-ADCs (ADC#1, ADC#2) and 7-GHz clock rate are utilized to achieve 14-GHz sampling rate. Fig. 2 shows the schematic diagram of time-interleaved sampling. ADC#1 and ADC#2 sample alternately at a constant time interval of T/2, where T is the repetition period of clock. To balance the time interval, the FPGA is programmed for calibration. After sampling, each ADC quantizes respective sampling points into binary stream by comparing with a threshold which equals the mean value of fluctuation amplitude. Then, two raw random bit sequences can be generated and acquired by the FPGA. In FPGA, the bitwise interleaving combination operation is executed to combine the two sequences into a new sequence, which is then processed with self-delay XOR operation. Finally, random bit sequence with a real-time generation rate of 2/T is achieved at the output of FPGA.

In experiments, the lasers DFB_1 and DFB_2 (Eblana, EP1550-DM-B05-FM) have threshold currents of 13.68 mA and 13.88 mA respectively, and are both biased at 34 mA by laser drivers (ILX Lightwave, LDX-3412). Their central wavelengths are slightly tuned by temperature controllers

(ILX Lightwave, LDT-5412) to adjust the frequency difference $\Delta\nu$. The balanced photodetector (u^2t, BPDV2120R) has a bandwidth of 45 GHz. The clock (Agilent, E8257D) has a repetition period of 1/7 ns corresponding to the reciprocal of the maximum sampling rate of sub-ADC. The length of delay bits for self-delay XOR operation in the FPGA (Virtex-7 XC7VX690T) is 70 bits. The optical heterodyne signal is measured by a radio-frequency spectrum analyzer (Agilent, N9030A, 43-GHz bandwidth) and a real-time oscilloscope (LeCroy, SDA806Zi-A, 16-GHz bandwidth, 40 GS/s). The optical spectra of two ECLs are measured by an optical spectrum analyzer with a resolution of 0.02 nm (YOKOGAWA, AQ6370C).

3. Experimental Results

3.1 Generation of White Chaos

The properties of the optical heterodyne signal for different parameters have been investigated in our previous work [34]. Here, we present the conditions for generating the white chaos. First, the two ECLs should have fast phase dynamics which is not dominated by laser relaxation oscillation, so that the heterodyne converting phase into intensity can generate a flat wideband spectrum by controlling the frequency difference. Second, the two feedback delays, i.e. the round-trip time in external cavities, should be incommensurate in principle, so that the external-cavity modes of the two lasers have incommensurate mode frequency intervals. Thus, the heterodyne leads to non-resonance beatings and then totally eliminates the time-delay signatures. It is worth noting that, due to finite external-cavity modes, the delay condition can be eased as $q\tau_1 = p\tau_2$ with large enough integers p and q.

In experiments, the feedback strength defined as the power ratio of the feedback light to the laser output is adjusted to be –10.2 dB for ECL_1 and –11.4 dB for ECL_2. The two feedback delays are $\tau_1 = 107.9$ ns and $\tau_2 = 93.6$ ns. The center wavelengths of DFB_1 and DFB_2 are 1550.486 nm and 1550.390 nm, respectively, which are red shifted by 0.038 nm and 0.030 nm compared to the static-state wavelengths due to optical feedback. With these parameters, we experimentally obtain a white chaos by optical heterodyning.

Fig 3(a) firstly presents the radio-frequency spectra of ECL_1 and ECL_2 used for generating the white chaos. For each spectrum, a peak which appears approximately at the relaxation frequency $\sim$7 GHz can be clearly observed. This peak is much higher than the lowest spectral component and dominates the whole spectrum. As a result, the bandwidth and flatness are greatly restricted: the 3-dB bandwidths for ECL_1 and ECL_2 are only 3.4 GHz and 4.0 GHz, respectively. In addition, as depicted by the fine spectra in a scale of 40 MHz, obvious periodic modulation which equals the reciprocal of feedback delay (τ_1, τ_2) can be clearly observed. Note that the periodic modulation is caused by the resonance of external-cavity feedback and responsible for deteriorating randomness of random bits. By contrast, as shown in Fig. 3(b), the spectrum of white chaos is very flat over a wide frequency band, which leads to a 16.7-GHz bandwidth within 3-dB range. Moreover, as depicted by the inset, the spectrum is also flat without periodic modulation. It is argued that such a wide flat-spectrum could be highly beneficial to generating high-speed and good-quality physical random bits [27].

It is worth noting that the phase noise in two ECLs plays an important role in giving rising to unpredictability of white chaos. But, due to the narrow bandwidth [36], it makes no significant contribution to the wide bandwidth of white chaos, which benefits from the wide and flat spectra of laser phase. While for thermal noise and shot noise of detector as well as radio-frequency spectrum analyzer's noise, their contributions can be ignored owing to that they are independent of the ECLs and have much weaker power than that of white chaos as shown by the noise floor. Moreover, the effects of detector's transit time can also be ignored because the detector's bandwidth used in experiments is wide enough to cover that of white chaos.

Next, the temporal characteristics of white chaos including temporal waveform, amplitude probability distribution, and autocorrelation function (ACF) are investigated. As shown by the temporal waveform of Fig. 4(a), the white chaos has large fluctuation amplitude, which makes it easy to be sampled by ADC. Moreover, we also noticed that the amplitude fluctuates symmetrically with

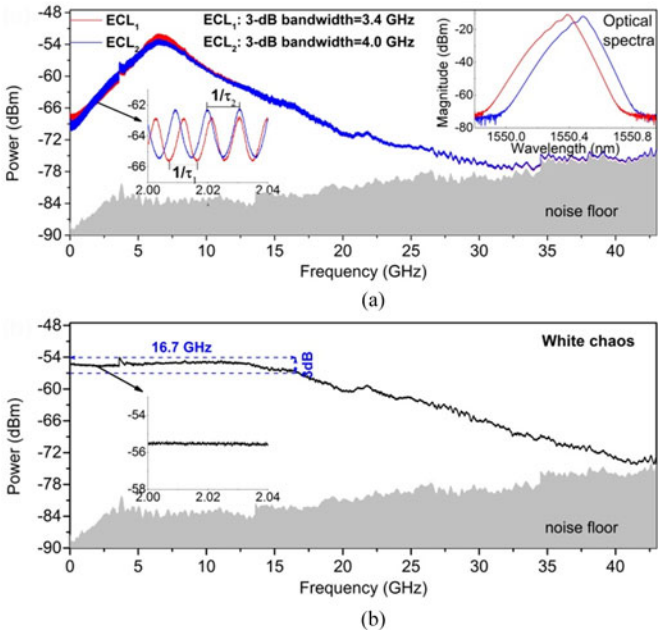


Fig. 3. Characteristics of entropy source in frequency domain. Radio-frequency spectra of (a) $ECL_{1/2}$ and (b) white chaos, resolution bandwidth: 3 MHz; video bandwidth: 3 kHz; sweep time: 1 s; sampling points: 40001; averaged times: 30. The insets plot the radio-frequency spectra of $ECL_{1/2}$ and white chaos in a scale of 40 MHz, as well as the optical spectra of the two ECLs.

respect to its mean value of zero volt. This symmetry can be further verified by the amplitude probability distribution shown in Fig. 4(b). Quantitatively, it has a small skewness of -0.009. As a remark, the asymmetric amplitude distribution is an inherent defect of ECL and will introduce imbalance of bits "0" and "1", which usually requires a careful adjustment of decision voltage of ADC to overcome. Using the white chaos as entropy source, a more balanced generation of bits "0" and "1" can be achieved, and also the careful adjustment of decision voltage can be avoided.

Furthermore, the ACF of white chaos's intensity output, as shown in Fig. 4(c), is plotted to examine the time-delay signature which can be exposed by the peak located at feedback delay. Note that the time-delay signature of ECL is caused by periodic external-cavity resonance shown by the inset of Fig. 3(a). It induces weak periodicity associated with optical feedback cavity and degrades randomness of random bits especially when the sampling period and feedback delay are commensurate. Whereas, for white chaos, the correlation traces have no distinguished peaks at the feedback delays of τ_1 and τ_2. Further zooming the ordinate of ACF shown by the inset, there are still no correlation peaks exceeding the amplitude of background noise at above delays. It indicates that the time-delay signature of white chaos is eliminated. The elimination of time-delay signature not only improves the randomness of random bits but also enables a continuously tunable generation of random bits [28].

3.2 7-Gbps Parallel RBG

In experiments, the random bit sequences of ADC#1 and ADC#2 are separate before merging in the FPGA. It provides an opportunity for generating random bits in a parallel way. In this section, we evaluate the capability of parallel random bit generation. Fig. 5 shows the photographs of temporal waveforms and eye diagrams of the two parallel random bit sequences generated by ADC#1 and ADC#2, respectively. Seen from the temporal waveforms, random bit sequences are in a non-return-to-zero (NRZ) format and seven bits are located within 1-ns division indicating a generation rate of 7 Gbps. Their corresponding eye diagrams are opened well, in which the width between two crossing points is 143.4 ps (23.9×6), which equals the width of minimum code. It is worth

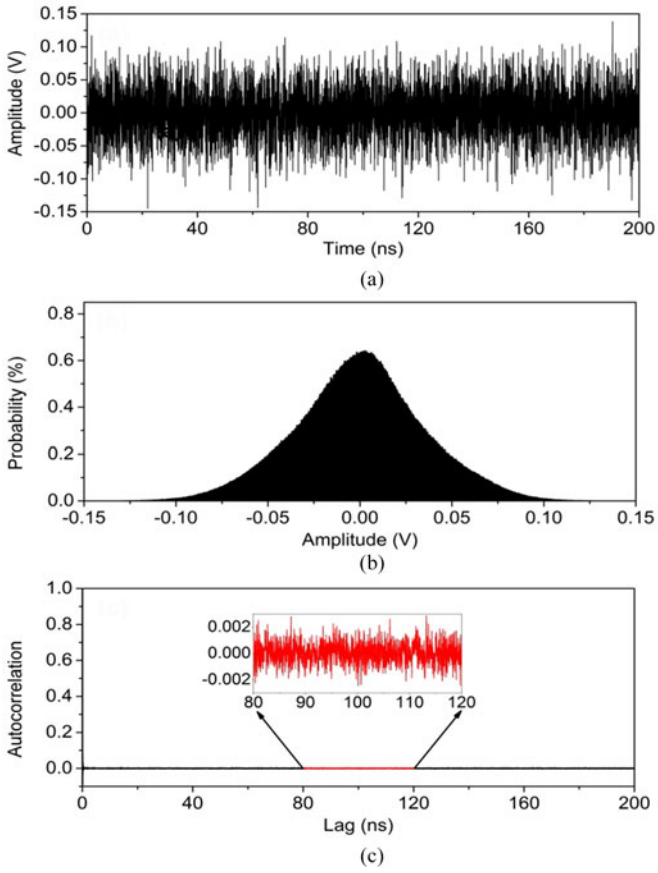


Fig. 4. Characteristics of white chaos in temporal domain. (a) Temporal waveform. (b) Amplitude probability distribution, data length: 2×10^6 points. (c) ACF, correlation length: 2×10^6 points.

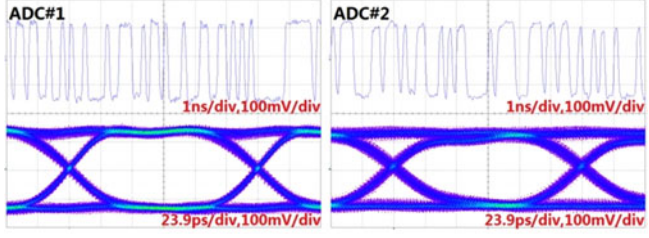


Fig. 5. Temporal waveforms and eye diagrams of random bits generated by ADC#1 and ADC#2 at 7-GHz sampling rate.

noting that the two random bit sequences are directly obtained from sub-ADCs, which are not yet processed by XOR operations.

Furthermore, we examined the statistical randomness of the parallel random bits processed with self-delay XOR operations in the FPGA. Note that a good randomness should refer to that random bits are bias-free and internally independent. Firstly, we qualitatively investigated the bitmap images of random bits of ADC#1 and ADC#2 as shown in Fig. 6. No apparent pattern and bias from the bitmap images are observed. Furthermore, we give a quantitative verification by calculating the bias

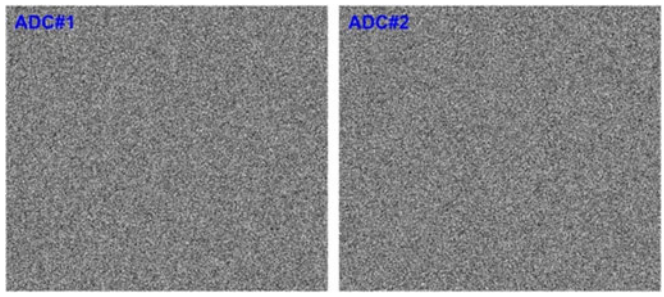


Fig. 6. Bitmap images of random bits generated by ADC#1 and ADC#2. Each bitmap image is constructed using 1000 × 1000 bits with 7-Gbps bit rate. Here, black and white dots denote bits "0" and "1," respectively.

$|e[N]|$ and normalized autocorrelation coefficient $C[K]$, which are, respectively, defined as follows:

$$|e[N]| = |\langle a[N]\rangle - 0.5| \tag{1}$$

$$C[K] = \frac{\langle a[N]\, a[N+K]\rangle - \left\langle a[N]^2\right\rangle}{\langle a^2[N]\rangle - \left\langle a[N]^2\right\rangle} \tag{2}$$

where $a[N]$, $a[N+K]$ are N-bit random sequences, K is the length of delay bits, and $<\cdot>$ denotes a statistical average over N bits. For a random bit sequence with finite length, a Gaussian distribution estimation $N[0, \sigma^2]$ is usually employed to evaluate its randomness, for which the standard deviation σ_e of $e[N]$ equals $(N^{-1/2})/2$, and σ_c of $C[K]$ equals $N^{-1/2}$ [31]. The random bit sequence can be deemed statistically unbiased and internally independent if $e[N]$ and $C[K]$ keep below the level of their own three standard deviation denoted as $3\sigma_e$ and $3\sigma_c$ respectively. Fig. 7 plots the $e[N]$ as a function of sample sizes and the $C[K]$ as a function of delay bits for ADC#1 and ADC#2. It is clearly shown in Fig. 7(a) that the biases keep below the three-standard-deviation levels versus different sample sizes. Moreover, as shown in Fig. 7(b) and (c), autocorrelation coefficients are also well below the significant levels of the three-standard-deviation criterion corresponding to a sample size of 16 Mbits. Above results indicate that the parallel XORed random bits are both unbiased and internally independent.

To better evaluate the statistical randomness, a more stringent industry-standard statistical test suite provided by the National Institute of Standards and Technology (NIST) is used [37]. It consists of 15 statistical tests accomplished using 1000 samples of 1-Mbit sequences and the significance level of 0.01. For "Success," the P-value (uniformity of p-values) should be larger than 0.0001 and the proportion (P) should be in the range of 0.99 ± 0.0094392. Table 1 shows the test results of ADC#1 and ADC#2. For tests which produce multiple P values and proportions, the worst case is shown. Test results show that all of 15 tests can be passed for the XORed random bits of ADC#1 and ADC#2 indicating a good statistical randomness. It is worth noting that passing statistical tests for each random bit sequence cannot guarantee the capability of parallel generation of random bits. The mutual independence between the two random bit sequences should be further checked. This check is presented in part C, which successfully demonstrates the mutual independence. Thus, one can conclude that the 7-Gbps parallel RBG can be achieved.

3.3 14-Gbps RBG

In this section, the mutual independence between random bit sequences of ADC#1 and ADC#2 is firstly evaluated. This is because keeping mutual independence is the precondition not only for parallel output but also for merging output. To assess the mutual independence, cross-correlation

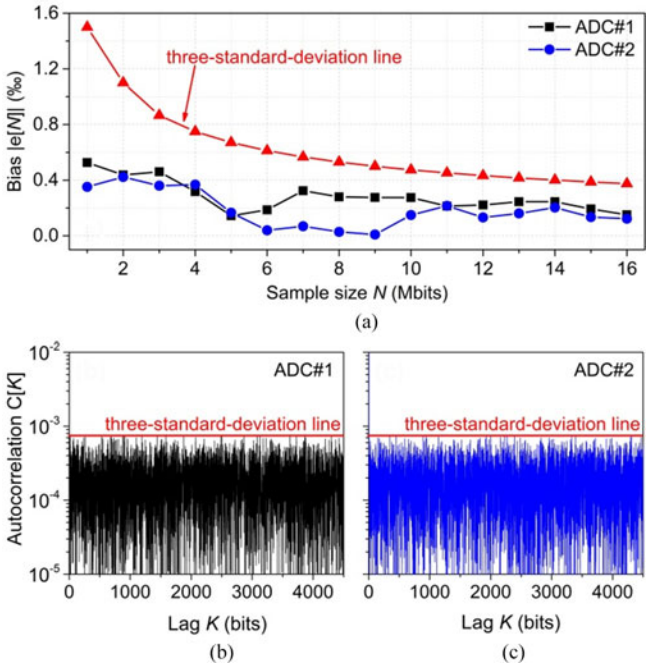


Fig. 7. Quantitative verification of bias and independence for 7-Gbps parallel random bits. (a) Bias $|e[N]|$ as a function of sample size N and (b),(c) autocorrelation coefficient $C[K]$ as a function of delay bit K. The red line in (a) denotes the three standard deviation of $|e[N]|$: $3\sigma_e = (3N^{-1/2})/2$, where $N = 1, 2, 3, \ldots 16$ Mbits. The red lines in (b) and (c) denote the three standard deviations of $C[K]$: $3\sigma_c = 3N^{-1/2}$, where $N = 16$ Mbits. Here, σ_e and σ_c are the standard deviations of $|e[N]|$ and $C[K]$, respectively.

function (CCF) is used which is defined as follows:

$$CCF = \frac{\langle a_1[N]\, a_2[N + K]\rangle - \langle a_1[N]\rangle \langle a_2[N + K]\rangle}{\left(\left[\langle a_1^2[N]\rangle - \left\langle a_1[N]^2\right\rangle\right]\left[\langle a_2^2[N + K]\rangle - \left\langle a_2[N + K]^2\right\rangle\right]\right)^{\frac{1}{2}}} \tag{3}$$

where $a_1[N]$ and $a_2[N + K]$ are N-bit random sequences of ADC#1 and ADC#2 respectively, K is the length of delay bits, and $<\cdot>$ denotes a statistical average over N bits. If no correlation peak is established in the CCF, random bits of ADC#1 and ADC#2 are mutually independent. Otherwise, they are not mutually independent.

The CCFs are shown in Fig. 8. For a clear comparison, we not only show the CCF of random bits when ECL is used as entropy source but also present the CCF of random bits before self-delay XOR operation. Due to the similarity of ECL_1 and ECL_2, the results of ECL_1 are only given. For ECL_1 as shown in the upper trace of Fig. 8(a), the CCF of raw data establishes a high correlation with a value of 0.323 at 0-bit delay. Here, raw data denotes random bits before XOR operation. In addition, the residual correlation at $\pm$755-bit delays caused by time-delay signature is also obvious. After being processed with self-delay XOR operation as shown in the lower trace of Fig. 8(a), the correlation at 0-bit and $\pm$755-bit delays is reduced but remains being distinguished. By contrast, for white chaos as shown in the upper trace of Fig. 8(b), only a weak correlation with a value of 0.024 at 0-bit delay is established between the raw data. With assistance of XOR operation, as shown in the lower trace of Fig. 8(b), this weak correlation can be entirely eliminated. It is worth noting that the correlation caused by time-delay signature is not observed whether with or without XOR operation, which benefits from the elimination of external-cavity resonance for white chaos. Consequently, it can be concluded that the XORed random bit sequences of ADC#1 and ADC#2 generated from white chaos are mutually independent.

TABLE 1
Results of NIST Tests for 7-Gbps Parallel Random Bits Generated by ADC#1 and ADC#2

Statistical test	ADC#1			ADC#2		
	p-value	P	R	p-value	P	R
Frequency	0.076658	0.9830	s	0.006425	0.9830	s
Block Frequency	0.622546	0.9870	s	0.502247	0.9910	s
Cumulative Sums	0.117432	0.9890	s	0.032274	0.9860	s
Runs	0.311542	0.9910	s	0.323668	0.9860	s
Longest Run	0.941144	0.9890	s	0.033362	0.9890	s
Rank	0.618385	0.9900	s	0.140453	0.9940	s
FFT	0.488534	0.9860	s	0.474986	0.9890	s
Non Overlapping Template	0.016488	0.9830	s	0.010911	0.9910	s
Overlapping Template	0.193767	0.9950	s	0.630872	0.9880	s
Universal	0.455937	0.9840	s	0.516113	0.9860	s
Approximate Entropy	0.987492	0.9900	s	0.536163	0.9910	s
Random Excursions	0.009592	0.9950	s	0.238987	0.9936	s
Random Excursions Variant	0.002741	0.9884	s	0.001630	0.9968	s
Serial	0.454053	0.9950	s	0.583145	0.9900	s
Linear Complexity	0.066051	0.9870	s	0.219006	0.9920	s

"R" denotes results, "s" denotes success.

Having confirmed the mutual independence, attention is now turned to examining the statistical randomness of random bits after bitwise interleaving combination. Fig. 9 shows the bitmap which is constructed using 1000 $\times$ 1000 bits with a generation rate of 14 Gbps. No apparent pattern and bias is observed. Note that the 14-Gbps generation rate is realized with the post-processing combination of outputs of ADC#1 and ADC#2 in the FPGA. And the maximum sampling rate of single sub-ADC is 7 GHz. Therefore, the corresponding eye diagram at 14-GHz sampling rate is not presented here. Fig. 10 further shows the quantitative verification of bias and independence for the 14-Gbps random bits. It can be seen that the 14-Gbps random bits are unbiased and internally independent because of obeying the three-standard-deviation criteria. The last evaluation of the statistical randomness using NIST tests is given in Table 2. All of 15 tests are passed, which not only indicates a good statistical randomness but also the capability of real-time 14-Gbps random bit generation. Such a high generation rate also proves a high bandwidth-utilization efficiency $\sim$84% which is the ratio of generation rate and signal bandwidth.

4. Discussion

Time interval (T/2) of sub-ADCs in interleaving sampling affects the mutual correlation of random bits generated by two sub-ADCs as shown in Fig. 8. To avoid high correlation, the time interval should be approximately larger than the reciprocal of the bandwidth of physical entropy source [27]. For white chaos with a 3-dB bandwidth of 16.7-GHz, the time interval of 1/14 ns corresponding to a 7-GHz time-interleaved sampling rate is allowed. Moreover, such a flat power spectrum enables a high bandwidth-utilization efficiency $\sim$84% which indicates that the energies of most frequency components can be used for sampling. Consequently, only a weak correlation of sampling points of

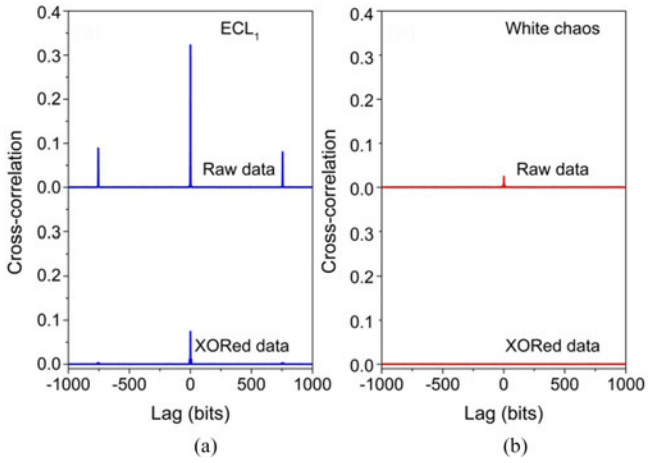


Fig. 8. CCFs of random bits of ADC#1 and ADC#2 using entropy sources of (a) ECL_1 and (b) white chaos. Here, the XORed data and raw data denote random bits with and without XOR operation, respectively. The correlation length is 16×10^6 bits. The $\pm$755-bit delays correspond to $\pm$107.9-ns delays.

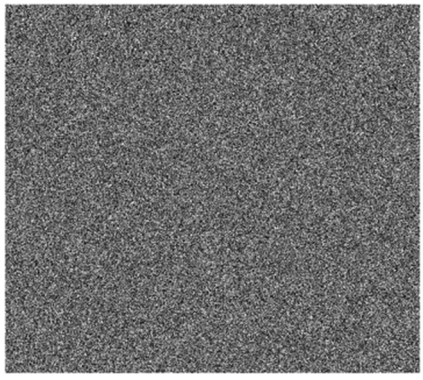


Fig. 9. Bitmap image of random bits after bitwise interleaving combination. The bitmap image is constructed using 1000×1000 bits with 14-Gbps bit rate. Here, black and white dots denote bits "0" and "1," respectively.

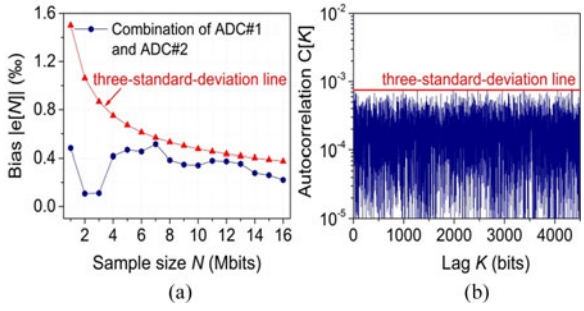


Fig. 10. Quantitative verification of bias and independence for 14-Gbps random bits. (a) Bias $|e[N]|$ as a function of sample size N and (b) autocorrelation coefficient $C[K]$ as a function of delay bit K. The red line in (a) denotes the three standard deviation of $|e[N]|$: $3\sigma_e = (3N^{-1/2})/2$, where $N = 1, 2, 3, \ldots 16$ Mbits. The red lines in (b) denote the three standard deviation of $C[K]$: $3\sigma_c = 3N^{-1/2}$, where $N = 16$ Mbits. Here, σ_e and σ_c are the standard deviations of $|e[N]|$ and $C[K]$, respectively.

TABLE 2
Results of NIST Tests for 14-Gbps Random Bits Generated With Bitwise Interleaving Combination

Statistical test	Combination of ADC#1 and ADC#2		
	p-value	P	R
Frequency	0.018540	0.9870	s
Block Frequency	0.001248	0.9820	s
Cumulative Sums	0.005242	0.9880	s
Runs	0.056426	0.9810	s
Longest Run	0.939005	0.9920	s
Rank	0.242986	0.9900	s
FFT	0.246750	0.9920	s
Non Overlapping Template	0.002322	0.9910	s
Overlapping Template	0.002236	0.9900	s
Universal	0.195864	0.9830	s
Approximate Entropy	0.342451	0.9900	s
Random Excursions	0.000436	0.9884	s
Random Excursions Variant	0.182384	0.9934	s
Serial	0.000349	0.9850	s
Linear Complexity	0.043368	0.9880	s

"R" denotes results, "s" denotes success.

the two ADCs is established. After self-delay XOR, this weak correlation can be eliminated. However, for ECL_1 with a 3-dB bandwidth of 3.4 GHz, the 7-GHz time-interleaved sampling rate is too high for the signal bandwidth. And the sharp spectrum of ECL_1 greatly limits the bandwidth-utilization efficiency resulting in that only the energies nearby relaxation frequency can be used. And thus, much higher correlation of the sampling points of the two sub-ADCs is established. This correlation cannot even be eliminated with XOR operation. The solution is decreasing the interleaved sampling rate, i.e., enlarging the time interval, which however inevitably reduces the generation rate. In addition to bandwidth, time-delay signature of ECL also causes the correlation of sampling points of the two sub-ADCs. Its influence can be usually eliminated by choosing incommensurate sampling rate with feedback delay [15]. However, this hinders the tunable random bit generation and, thus, limits practical use. By comparison, the white chaos has no time-delay signature, which ensures not only the uncorrelation of sampling points but also the tunable generation rate.

It is worth mentioning that the generation rate of random bits based on white chaos can be further improved, which is realized through enhancing the bandwidth of white chaos by optimizing the parameters of ECLs. For example, the feedback strengths of ECLs can be optimized to produce broad optical spectra and the frequency detuning can be tuned to make an appropriate overlap of the optical spectra. Moreover, the generation rate of random bits has not reached the limit of white chaos's bandwidth yet, which is due to the limitation of sampling rate of ADC. An ADC with faster sampling rate will also further improve the generation rate.

5. Conclusion

Real-time high-speed physical RBG based on the time-interleaved sampling of white chaos is experimentally demonstrated. Benefiting from the wide flat-spectrum and no time-delay signature of white chaos, two mutually independent random bit sequences with verified randomness are achieved through single-bit quantization of time-interleaved sub-ADCs and self-delay XOR operation in the FPGA. After bitwise interleaving combination of the two sequences, a real-time 14-Gbps physical RBG with verified randomness is finally achieved.

References

[1] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC, 1995.
[2] R. G. Gallager, *Principles of Digital Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[4] N. Metropolis and S. Ulam, "The monte carlo method," *J. Amer. Stat. Assoc.*, vol. 44, no. 247, pp. 335–341, Sep. 1949.
[5] S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis*. New York, NY, USA: Springer-Verlag, 2007.
[6] [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf FIPS 140-2, May 2001.
[7] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 5, pp. 615–621, Aug. 2000.
[8] 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.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.
[9] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," *Opt. Lett.*, vol. 36, no. 6, pp. 1020–1022, Mar. 2011.
[10] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Opt. Exp.*, vol. 18, no. 23, pp. 23584–23597, Nov. 2010.
[11] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," *J. Lightw. Technol.*, vol. 30, no. 9, pp. 1329–1334, May 2012.
[12] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H. K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Exp.*, vol. 20, no. 11, pp. 12366–12377, May 2012.
[13] Y. Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J. W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Rev. Sci. Instrum.*, vol. 86, no. 6, Jun. 2015, Art. no. 063105.
[14] X. G. Zhang, Y. Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J. W. Pan, "Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction," *Rev. Sci. Instrum.*, vol. 87, no. 7, Jul. 2016, Art. no. 076102.
[15] A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nat. Photon.*, vol. 2, no. 12, pp. 728–732, Nov. 2008.
[16] T. E. Murphy and R. Roy, "Chaotic lasers: The world's fastest dice," *Nat. Photon.*, vol. 2, no. 12, pp. 714–715, Dec. 2008.
[17] M. Sciamanna and K. Alan Shore, "Physics and applications of laser diode chaos," *Nat. Photon.*, vol. 9, no. 3, pp. 151–162, Feb. 2015.
[18] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol. 103, no. 2, Jul. 2009, Art. no. 024102.
[19] K. Hirano *et al.*, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," *Opt. Exp.*, vol. 18, no. 6, pp. 5512–5524, Mar. 2010.
[20] A. Argyris, S. Deglianidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb s–1 true random bit generator based on a chaotic photonic integrated circuit," *Opt. Exp.*, vol. 18, no. 18, pp. 18763–18768, Aug. 2010.
[21] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nat. Photon.*, vol. 4, no. 1, pp. 58–61, Dec. 2010.
[22] 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.*, vol. 36, no. 23, pp. 4632–4634, Dec. 2011.
[23] Y. Akizawa *et al.*, "Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8 × 50 Gb/s," *IEEE Photon. Technol. Lett.*, vol. 24, no. 12, pp. 1042–1044, Jun. 2012.
[24] N. Oliver, M. Soriano, D. Sukow, and I. Fischer, "Fast random bit generation using a chaotic laser: Approaching the information theoretic limit," *IEEE J. Quantum Electron.*, vol. 49, no. 11, pp. 910–918, Nov. 2013.
[25] N. Li *et al.*, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," *Opt. Exp.*, vol. 22, no. 6, pp. 6634–6646, Mar. 2014.
[26] R. Takahashi *et al.*, "Fast physical random bit generation with photonic integrated circuits with different external cavity lengths for chaos generation," *Opt. Exp.*, vol. 22, no. 10, pp. 11727–11740, May 2014.
[27] 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, Jan. 2015.
[28] 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, Sep. 2015.
[29] X. Tang *et al.*, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," *Opt. Exp.*, vol. 23, no. 26, pp. 33130–33141, Dec. 2015.
[30] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," *Phys. Rev. A*, vol. 83, no. 3, Mar. 2011, Art. no. 031803.

[31] A. B. Wang, P. Li, J. G. Zhang, J. Z. Zhang, L. Li, and Y. C. Wang, "4.5 Gbps high-speed real-time physical random bit generator," *Opt. Exp.*, vol. 21, no. 17, pp. 20452–20462, Aug. 2013.
[32] T. Yamazaki and A. Uchida, "Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers," *IEEE J. Sel. Topics Quantum Electron.*, vol. 19, no. 4, Feb. 2013, Art. no. 0600309.
[33] K. Hirano *et al.*, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 45, no. 11, pp. 1367–1379, Nov. 2009.
[34] A. B. Wang, B. J. Wang, L. Li, Y. C. Wang, and K. A. Shore, "Optical heterodyne generation of high-dimensional and broadband white chaos," *J. Sel. Topics Quantum Electron.*, vol. 21, no. 6, pp. 531–540, Apr. 2015.
[35] D. Y. Wu *et al.*, "A 30 GS/s 6 bit SiGe ADC with input bandwidth over 18 GHz and full data rate interface," in *Proc. Bipolar/BiCMOS Circuits Technol. Meet.*, Sep. 2016, pp. 90–93.
[36] H. Guo, W. Z. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E*, vol. 81, no. 5, May 2010, Art. no. 051137.
[37] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Pub. 800–22 Rev. 1a, 2010.