A robust random number generator based on differential comparison of chaotic laser signals

Jianzhong Zhang,1,2 Yuncai Wang,1,2,* Ming Liu,1 Lugang Xue,1 Pu Li,1 Anbang Wang,1,2 and Mingjiang Zhang1,2

1Institute of Optoelectronic Engineering, College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan, 030024, China
2Xi’an Institute of Optics and Precision Mechanics of Chinese Academy of Science, Xi’an 710119, China

Abstract: We experimentally realize a robust real-time random number generator by differentially comparing the signal from a chaotic semiconductor laser and its delayed signal through a 1-bit analog-to-digital converter. The probability density distribution of the output chaotic signal based on the differential comparison method possesses an extremely small coefficient of Pearson’s median skewness (1.5 × 10−6), which can yield a balanced random sequence much easily than the previously reported method that compares the signal from the chaotic laser with a certain threshold value. Moreover, we experimentally demonstrate that our method can stably generate good random numbers at rates of 1.44 Gbit/s with excellent immunity from external perturbations while the previously reported method fails.

OCIS codes: (140.1540) Chaos; (140.5960) Semiconductor lasers; (060.4510) Optical communications.

References and links

1. Introduction

Random numbers play a significant role in a variety of applications such as cryptography [1], spread-spectrum communications [2], Monte Carlo numerical simulations [3], and ranging [4]. There are two basic types of generator to produce random sequences: pseudorandom number generators (PRNGs) and physical random number generators (RNGs). PRNGs can be implemented on the software platform based on initial seeds and certain deterministic algorithms. Although PRNGs are cost effective and, in most cases, efficient, they suffer from the vulnerability that the generators’ output can be potentially predicted if an attacker discovers the seed or the deterministic algorithm. Such weakness may lead to some serious problems in security applications. RNGs are based on physical processes, such as electrical noises [5], frequency jitters in electrical oscillators [6] and chaotic circuits [7, 8], which can produce unpredictable random numbers of high quality yet much lower rates than PRNGs because of the narrow bandwidth of these physical entropy sources. An unconditional secure system should have the communication data encrypted by physical random numbers of the same rates as the data; however, so far the generation rates of these RNG systems are much lower than that of the data.

Recently, the utilization of broadband chaotic laser sources has greatly improved the generation rates of RNGs. In 2008, Uchida et al. [9] for the first time experimentally achieved a 1.7 Gbit/s RNG by comparing the chaotic signal injected into a 1-bit analog-to-digital converter (ADC) with a certain threshold voltage. Such comparison process is relatively sensitive to external perturbations and may cause the practical system of weak stability [10, 11]. To mitigate the robustness of RNG systems, several other schemes have been proposed by using 8-bit ADCs which are free from determining the threshold value. In 2009, Reidler et al. constructed a high-speed stable RNG by combining together multi-bits from an 8-bit ADC [10, 12]. Later, Uchida’s group demonstrated another fast RNG by multi-sampling of experimental bandwidth-enhanced chaotic signals [13]. We have also proposed a high-speed reliable all-optical RNG based on bandwidth-enhanced chaos and all-optical ADCs [14]. Whereas, all of these schemes acquire the random numbers by processing chaotic signals offline, thus the random numbers cannot be real-timely generated. Besides, photonic integrated chaotic semiconductor laser sources can also be utilized to generate high-speed random sequences [11, 15, 16], but to extract the random numbers they face the same problems mentioned above. Therefore, a real-time RNG system of strong robustness is very demanding.

In this paper, we demonstrate such a robust RNG system by differentially comparing two branches of chaotic signals from a chaotic laser source into a 1-bit ADC. Random bit sequences at rates up to 1.44 Gbit/s are finally achieved in real time. In addition, our RNG system is stable with respect to external perturbations with the output performance maintained over multiple trials during continuous operation.

2. Experimental setup

Figure 1 shows the experimental setup of random number generation based on the differential comparison of the chaotic laser signals. A distributed feedback (DFB) laser diode (LDM5S752) subject to external optical feedback is referred to as the chaotic light source.
The laser output is divided into two beams by a fiber coupler (40:60 coupling ratio), one of which is made as the output of the chaotic light source and the other is reflected into the DFB laser by a fiber mirror (FM), inducing high-frequency chaotic oscillations of the optical intensity. The amount and polarization state of the feedback light are adjusted by a variable optical attenuator (VOA) and a polarization controller (PC), respectively. An optical isolator (OI) is used to prevent unwanted optical feedback into the DFB laser diode. The chaotic laser output is detected and converted to an electrical signal by an amplified photodetector (PD, THORLABS, PDA8GS, 9 GHz bandwidth). The converted electrical signal is again divided into two beams through a T-type connector. They are differentially coupled to a 1-bit ADC consisting of a comparator (ADCMP567, 5 GHz equivalent bandwidth) and a D flip-flop (MC10EP52, maximum frequency of 6 GHz). The binary signal is obtained by comparing the differential logic inputs of the comparator. At the same time, an extra electrical delay line of 1.06 m in length is inserted into an input terminal of the comparator to ensure that two differential input chaotic signals are uncorrelated. Finally, to improve the randomness of the random sequence, two binary digital sequences obtained from the two independent chaotic signals are combined using a logical exclusive-OR (XOR) operation. The rate of the random sequence is determined by the input clock frequency of the comparator. The clock module (AD9516-1) can generate multi-frequency clock signals, including 120 MHz, 720 MHz, and 1.44 GHz, with the maximum clock frequency reaching 2.87 GHz. Thus, our random number generator obtains multi-rate random bit sequence output. In our experiment, the temporal waveforms of the chaotic signal and the random sequence are observed and recorded by an oscilloscope with a 20 GHz bandwidth and a 40 GS/s sampling rate (LeCroy SDA 820Zi-A). The corresponding radio-frequency (RF) spectra of the chaotic signal and the random sequence are measured by a spectrum analyzer (Hewlett Packard 8563E, 26.5 GHz bandwidth).

Fig. 1. Experimental setup of random number generation based on the differential comparison of the chaotic laser signals, DFB-LD: distributed feedback laser diode; PC: polarization controller; FM: fiber mirror; VOA, variable optical attenuator; OI: optical isolator; PD: photodetector; T: T-type connector; 1-bit ADC: 1-bit analog-to-digital converter consisting of a comparator and a D flip-flop; OSC: oscilloscope.

3. Experimental results

3.1 Characteristics of chaotic laser signals

The wideband chaotic light source is depicted in the block diagram of Fig. 1. In the experiment, we adjusted the injection current, the length of the external cavity and the external feedback strength to put the laser in a regime of high-bandwidth chaos. When the semiconductor laser was biased at two times its threshold current (22 mA) and the feedback strength was 80% of the laser output power, chaotic signals with the considerably flat RF spectrum were obtained, as shown in Fig. 2(a). According to the bandwidth definition of the chaotic waveform as the span between zero and the frequency within which 80% of the energy is contained, the calculated bandwidth is about 7.3 GHz. For more details, see [17]. The broad chaos bandwidth enables us to generate high-speed random number sequences. The autocorrelation function of the chaotic light source output is illustrated in Fig. 2(b). The peak of the autocorrelation appears at 84 ns, corresponding to the round-trip time of the external cavity for the chaotic semiconductor laser. This indicates that the generated chaotic signal is characteristic of the periodicity induced by the external cavity. The periodicity can be
inherited by the extracted random sequence and can seriously influence the randomness. Thus, the directly extracted random bit sequences from the chaotic light source frequently fail to the statistical tests of randomness. So, the XOR operation on two uncorrelated binary sequences is required to suppress the periodicity.

![Image](Fig. 2. (a) The RF spectrum of the chaotic signal. The red line and blue line denote the chaotic signal and the noise base, respectively. (b) The autocorrelation trace of the chaotic signal.)

### 3.2 Performances of differential comparison

This section firstly analyzes the independence of each other for two differential input chaotic signals into the comparator. This mutual independence not only ensures that two adjacent bits of the generated random sequence has a low correlation, but also is a prerequisite for the symmetric probability density distribution function of the differentiated chaotic signal. Actually, the correlation between the chaotic signal and its time-delay signal can be assessed by the normalized correlation coefficient of the chaotic signal, which is expressed as follows [18]:

$$\rho = \frac{\frac{1}{n} \sum_{i=1}^{n} b_{i-k} - \left( \frac{1}{n} \sum_{i=1}^{n} b_i \right)^2}{\frac{1}{n} \sum_{i=1}^{n} b_i^2 - \left( \frac{1}{n} \sum_{i=1}^{n} b_i \right)^2}$$

(1)

Where $b_i$ denotes the $i$-th sampling value of the chaotic signal, $k$ denotes the delayed sampling dot number, and $n$ is the length of chaotic time series. Chaotic time series for a 500 ns long data stream, i.e., $n = 10000$, is chosen to calculate the correlation trace of the chaotic signal with the maximum delay time of 200 ns, as shown in Fig. 3. It can be seen that when the delay time is larger than 4 ns, the correlation coefficient is decreased to less than 0.01. Here, the delay time is selected to be 5 ns (the delay line length is about 1 m mentioned as before), and the corresponding correlation coefficient is 0.004. Under the condition, the chaotic signal and its delayed signal are considered to be almost independent of each other. Thus, we select the length of about 1 m as the delay line length between two differential chaotic signals into the comparator. From the inset of Fig. 3, we can see that the secondary peak of the overall correlation trace appears at 84 ns corresponding to the external cavity round-trip time, also showing the periodicity induced by the external cavity.
Fig. 3. The correlation trace of the chaotic signal. The inset shows the overall correlation trace of the chaotic signal with the maximum delay time of 200 ns.

Afterwards, we analyze the amplitude distribution of the differentiated chaotic signal. In our scheme, the random bit, 0 or 1, is achieved by comparing the differential logic inputs of the comparator at the corresponding sampling time. That is, the random binary value of 0 or 1 is theoretically assigned according to the sign of the difference between the chaotic signal \( V_1(t) \) and its delayed signal \( V_2(t) \) injected into the comparator. If \( V_1(t) - V_2(t) > 0 \), the random bit 1 is obtained; otherwise, the random bit 0 is obtained. Thus, a good distribution of the differentiated chaotic signal helps to extract high-quality random number sequences. From the above analysis, we find when the delay time between \( V_1(t) \) and \( V_2(t) \) is set to an appropriate value (for example, 5 ns), they are suggested to be mutually independent. Moreover, they obey the same amplitude distribution. Here, we suppose that their probability density functions are \( f(x) \) and \( f(y) \), respectively, and their joint probability density function is \( f(x,y) \), where \( f(x,y) = f(x)f(y) \) due to mutual independence of \( V_1(t) \) and \( V_2(t) \). For the differentiated chaotic signal, a variable \( z \) is introduced to represent it, where \( z = V_1(t) - V_2(t) \). Its amplitude distribution function \( F(z) \) is calculated by the following equation.

\[
F(z) = \int_{\infty}^{\infty} \int_{\infty}^{\infty} f(x, y) dx dy
\]

The corresponding density function \( f_z(z) \) is obtained by the derivation of the distribution function.

\[
f_z(z) = \int_{\infty}^{\infty} f(z + y) dy = \int_{\infty}^{\infty} f(z + y) f(y) dy
\]

Then,

\[
f_z(-z) = \int_{\infty}^{\infty} f(-z + y) f(y) dy
\]

Making the variable substitution by \( v = -z + y \), thus,

\[
f_z(-z) = \int_{\infty}^{\infty} f(v) f(v + z) dv
\]

According to Eq. (3) and Eq. (5), we get:

\[
f_z(z) = f_z(-z)
\]

From Eq. (6), it can be demonstrated that the chaotic signal after the difference operation has a symmetric probability density distribution function. Thus, the amplitude distribution of the chaotic signal can be improved by the differential comparison. Figures 4(a) and 4(b) show statistical histograms of the chaotic signals acquired by the oscilloscope before and after the differential comparison, respectively. Compared with the single chaotic signal, the differential
voltage has a more symmetric distribution. The symmetry of the distribution can be quantitatively evaluated by Pearson’s median skewness coefficient [19].

\[
\gamma = \frac{3 \times (\bar{x} - M)}{\sqrt{\frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})}}
\]  

(7)

Where \(x_i\), \(\bar{x}\), and \(M\) denote the sampling amplitude value, the mean and the median of the chaotic signal, respectively. Closer to zero the skewness coefficient is, the more symmetric the distribution. Specially, \(\gamma = 0\) indicates that the distribution is completely symmetric. For the chaotic signal without the differential comparison, its skewness coefficient is \(\gamma = 0.384\) by calculation. However, for the chaotic signal with the differential comparison, its skewness is decreased to \(\gamma = 1.5 \times 10^{-6}\). The decrease of the skewness coefficient is in agreement with the statistical histograms as shown in Fig. 4.

Finally, we make the comparison between the 0/1 ratios of the extracted random sequences from the chaotic signals before and after the differential comparison. The chaotic signal in Fig. 4(c) is converted to a binary sequence by comparing the chaotic signal with a threshold voltage, where the threshold voltage is set to the mean of the chaotic signal (18.4 mV). Then, a 1-Mbit random sequence is recorded to calculate the proportion of zeros and ones for the overall sequence. The corresponding 0/1 ratio is 579875/420125. The 0/1 deviation is further computed to be about 16%, without meeting the requirement of the frequency test of the standard statistical tests for random number generators provided by the National Institute of Standard Technology (NIST). For the 1-Mbit sequence to pass the frequency test of NIST tests, the 0/1 deviation should locate in the range of \(\pm 0.26\%\). Thus, the generated random sequence can pass the frequency test only when the threshold voltage for the comparator is carefully adjusted around the mean of the chaotic signal. In the experiment, the threshold resolution is required to be as high as 0.1 mV, which has also been stated in supplementary material available for [9]. With such high resolution, the balance of ones and zeros in random sequences is very sensitive to the fluctuations of the chaotic signal or the drift of the threshold voltage. For example, the slight mechanical and thermal fluctuations in the surrounding environment can lead to the large bias of ones and zeros in the generated binary sequence. Figure 4(d) shows the chaotic signal after the differential comparison. Its mean voltage is exactly equal to 0 mV due to the extremely symmetric distribution of the differentiated chaotic signal. The binary sequence is extracted from the difference chaotic signal by comparing with the threshold voltage of 0 mV, which in principle is equivalent to the random sequence extraction by comparing the differential logic inputs of the comparator. The 0/1 ratio of the generated random sequence is 499951/500049. The corresponding 0/1 deviation is 0.0098%, which does not go beyond the range of the 0/1 deviation allowed for the frequency test of NIST tests. Therefore, the differential operation can improve the amplitude distribution of the chaotic signal and make it more symmetric. The generated random sequence has a more balanced distribution of zeros and ones. Moreover, in the extraction course of random numbers, our method does not require the careful tuning of a decision threshold taking into account the unbiased distribution of the differentiated chaotic signal.
Fig. 4. (a) and (b) show statistical histograms of the chaotic signals before and after the differential comparison (The corresponding Pearson’s median skewness coefficients are 0.384 and $1.5 \times 10^{-6}$, respectively). (c) and (d) show time series of the chaotic signals before and after the differential comparison (The corresponding deviations of zeros and ones in the extracted random sequences are 16% and 0.0098%, respectively).

3.3 Random number generation

We generate random numbers by differentially comparing the wideband chaotic laser signals. An example of random bit generation at the maximum rate achievable with the chaotic signal in this setup is given. The generation rate is 1.44 Gbit/s, corresponding to a clock with a frequency of 1.44 GHz. The directly generated random bit sequence has weak periodicity caused by the external cavity. To overcome it, the XOR post-processing is required. Figure 5(a) shows the temporal waveform of the random bit sequence at 1.44 Gbit/s after the XOR operation. The output sequence is in a non-return-to-zero code format, in which the minimum code width is 695 ps and the peak-to-peak voltage value is about 0.7 V. Figure 5(b) depicts an eye diagram of the generated random bit sequence. The measured eye diagram is obviously opening. Figure 5(c) illustrates a random dot diagram with 500 × 500 bits in a two-dimensional plane. Bits “1” and “0” are converted to white and black dots, respectively, and placed from left to right (and from top to bottom). It can be seen that there are no obvious patterns, as we would expect that the ratio of 1 and 0 is roughly equal. To further evaluate the statistical properties of random bit sequences, we used the NIST test suite [20] and the Diehard test suite [21]. The tests were carried out using 1000 samples of 1-Mbit data for NIST tests and using 74-Mbit data for Diehard tests. The sequences passed all of NIST and Diehard tests. The typical results of NIST and Diehard tests are shown in Table 1 and Table 2, respectively.

One critical factor for many applications of RNG is a high bit generation rate. The ultimate rate of our RNG is of course limited. As mentioned before, the rate is determined by the input clock frequency of the comparator. Due to the limitation of 5 GHz equivalent bandwidth of the comparator, the sampling rate is set to 1.44 Gbit/s to reduce the correlation between adjacent sampled points in our experiment. If we choose to use a comparator with higher bandwidth, for example, ADCMP582 (8 GHz equivalent bandwidth), we can further increase the rate of random sequence.
Fig. 5. Typical output signals from RNG experimental system. (a) shows the temporal waveform of the random sequence at 1.44 Gbit/s after the XOR operation; (b) depicts an eye diagram of the random sequence; (c) illustrates a random dot diagram of the random sequence. Random bit patterns with 500 × 500 bits are shown in a two-dimensional plane. Bits “1” and “0” are converted to white and black dots, respectively, and placed from left to right (and from top to bottom).

Table 1. Results of NIST Special Publication 800-22 statistical tests. For ‘success’ using 1000 samples of 1-Mbit data and significance level \( \alpha = 0.01 \), the P-value (uniformity of P-values) should be larger than 0.0001 and the Proportion should be within the range of \( 0.99 \pm 0.0094392 \). For the tests which produce multiple P-values and Proportions, the worst case is shown.

<table>
<thead>
<tr>
<th>Statistical test</th>
<th>P-value</th>
<th>Proportion</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.207730</td>
<td>0.989</td>
<td>Success</td>
</tr>
<tr>
<td>Approximate Entropy</td>
<td>0.169981</td>
<td>0.993</td>
<td>Success</td>
</tr>
<tr>
<td>Block Frequency</td>
<td>0.522005</td>
<td>0.985</td>
<td>Success</td>
</tr>
<tr>
<td>Cumulative Sums</td>
<td>0.378705</td>
<td>0.987</td>
<td>Success</td>
</tr>
<tr>
<td>FFT</td>
<td>0.451626</td>
<td>0.996</td>
<td>Success</td>
</tr>
<tr>
<td>Linear Complexity</td>
<td>0.437636</td>
<td>0.985</td>
<td>Success</td>
</tr>
<tr>
<td>Longest Run</td>
<td>0.715679</td>
<td>0.990</td>
<td>Success</td>
</tr>
<tr>
<td>Non Overlapping Template</td>
<td>0.490483</td>
<td>0.991</td>
<td>Success</td>
</tr>
<tr>
<td>Overlapping Template</td>
<td>0.075719</td>
<td>0.987</td>
<td>Success</td>
</tr>
<tr>
<td>Random Excursions</td>
<td>0.507065</td>
<td>0.986</td>
<td>Success</td>
</tr>
<tr>
<td>Random Excursions Variant</td>
<td>0.760089</td>
<td>0.995</td>
<td>Success</td>
</tr>
<tr>
<td>Rank</td>
<td>0.127393</td>
<td>0.989</td>
<td>Success</td>
</tr>
<tr>
<td>Runs</td>
<td>0.564499</td>
<td>0.992</td>
<td>Success</td>
</tr>
<tr>
<td>Serial</td>
<td>0.576961</td>
<td>0.992</td>
<td>Success</td>
</tr>
<tr>
<td>Universal</td>
<td>0.382115</td>
<td>0.985</td>
<td>Success</td>
</tr>
</tbody>
</table>
4. Analysis of system robustness

In this section, we focus on the system robustness of random number generator. Figures 6(a) and 6(b) depict the chaotic signal with the jamming fluctuation and the corresponding extracted random codes, respectively. The jamming signal is introduced by the ripple effect of laser current source on purpose. In order to enhance the jamming effect, the modulation depth of the jamming signal relative to bias current is set to close to 1. Its average modulation frequency is about 5 MHz. Random binary sequence is generated by comparing with a set threshold value. From Fig. 6(b), it can be seen that the extracted random code sequence has many uninterrupted subsequences containing identical ones or zeros. The occurrence of clusters of ones or zeros leads to the failure of NIST tests. In the experiment, we note that the 0/1 deviation in the generated binary sequence is constantly varied during the course of external interference on chaotic signals. Thus, such RNG system does not steadily work for a long time. Here, the differential comparison method is utilized to improve the system robustness. Figure 6(c) denotes the chaotic signal after the differential comparison of the chaotic signal in Fig. 6(a). The amplitude of the difference chaotic signal is almost 2 times larger than that before the differential operation, suggesting that the difference voltage can be easier compared. It can be seen that the difference chaotic signal has no additional fluctuating
signal corresponding to the external interference. This is because that the fluctuating interference signals can be eliminated by the differential comparison. As mentioned before, the delay time between two chaotic signals into the differential input terminals of the comparator is set to 5 ns, which is far shorter than the average fluctuating period of 200 ns. So, the average fluctuating amplitudes of two jamming signals into the comparator are almost the same, and the external interference signal can be suppressed by doing the subtraction. Under normal circumstances, the frequency of the jamming signal caused by the external mechanical or thermal fluctuation from the real environment is extremely low (at best no more than several hundred hertz). That is, its average fluctuating periodicity remains far greater than the delay time. Therefore, our differential comparison method can effectively eliminate the actual interference signal. Figure 6(d) shows the random code sequence generated from the differentially-processed chaotic signal. Compared with Fig. 6(b), the distribution of random codes is more balanced. At the same time, we demonstrate that the 0/1 deviation remains unchanged under the interference of the external fluctuating signal, which means that the differential RNG system can reliably operate for a long time. A large number of experiments show that the statistical properties of random sequences can be maintained over multiple trials of continuous operation of the devices.

Fig. 6. (a) and (c) show the temporal waveforms of the chaotic signals before and after the differential comparison, respectively; (b) and (d) show the correspondingly extracted random code sequence, respectively. The jamming fluctuations are introduced by the ripple effect of laser current source on purpose. The modulation depth of the jamming signal relative to bias current is close to 1 and its average modulation frequency is about 5 MHz.

5. Conclusions

In conclusion, we have experimentally demonstrated a scheme of real-time robust RNG system by using the chaotic laser signal as the physical entropy source. The chaotic signal from a chaotic semiconductor laser and its delayed signal are differentially coupled into a comparator and then logically compared to produce a series of binary codes. The D flip-flop triggered by a clock samples the output of the comparator. The XOR post-processing is required to eliminate the weak periodicity of random sequences induced by the external feedback delay. Random bit sequences at rates up to 1.44 Gbit/s are finally obtained with verified randomness. The scheme does not require the accurate tuning of a decision threshold voltage, and can effectively improve the probability density distribution of the chaotic signal by the differential comparison. The corresponding Pearson’s median skewness coefficient decreases from 0.384 to $1.5 \times 10^{-6}$. Since the whole experimental system is very robust to the external perturbations and can be maintained for a long time during continuous operation of the devices, it is very useful for practical applications.
Acknowledgments

The authors extend special thanks to Y. X. Cui, G. H. Li, and W. X. Zhang for valuable discussions. We are indebted to LeCroy for the loan of SDA 820Zi-A digital oscilloscope. This work is supported by the National Natural Science Foundation of China (Grant No. 60927007 and 61001114), Shanxi Province Science Foundation for Youths (Grant No. 2010021003-4) and Open Research Fund of State Key Laboratory of Transient Optics and Photonics, Chinese Academy of Sciences (Grant No. SKLST201015).