Real-time 3 Gbit/s true random bit generator based on a super-luminescent diode

Min Huang, Anbang Wang, Pu Li, Hang Xu, Yuncai Wang

A R T I C L E   I N F O

Article history:
Received 13 January 2014
Received in revised form
4 March 2014
Accepted 18 March 2014

Keywords:
Amplified spontaneous emission noise
True random bits generator
Super-luminescent diode

A B S T R A C T

We present a real time random bit generation scheme using broadband amplified spontaneous emission noise from a super-luminescent diode (SLD) as the physical entropy source. Utilizing latch comparators, and an exclusive-or gate, we eventually demonstrate a 3 Gbit/s true random bit sequence with real waveform that can be directly applied to the communication network obtained, and its randomness satisfies all of the NIST statistical tests. Moreover, our system has the scalability so that it can generate multiple channels of true random bits simultaneously. This feature further improves its bit rate to meet the needs of secure communication with higher rate.

© 2014 Published by Elsevier B.V.

1. Introduction

Communication security plays an important role in current highly informational society. In a secure communication system, random bit generator is a crucial component because random bits are used as keys for information encryption and decryption. Besides, random bits also have other widespread applications such as Monte Carlo (MC) simulations, stochastic experiments, lottery games, etc. [1–3].

Random bits can be divided into pseudo-random bits and true random bits. Pseudo-random bits are based on some initial seeds and certain deterministic algorithm and can reach a high generation rate. However, they are deterministic, once eavesdroppers obtain the seed or the algorithm, one can easily crack and even reproduce the generated pseudo-random bits. Therefore, using pseudo-random bits as the key cannot ensure the information security in principle [4].

On the other hand, true random bits are based on a physical stochastic process whose unpredictability can guarantee the absolute security of information. Traditional true random bit generators use thermal noise [5] or photon noise [6] as physical entropy sources, but their bandwidths are so low that the bit rate is at the magnitude of Mbit/s, which cannot meet the needs of modern communication.

In 2008, Uchida et al. confirmed that two chaotic semiconductor lasers and 1-bit ADC can generate high speed physical random bits at the magnitude of Gbit/s [7]. Later, Kanter et al. demonstrated that one chaotic laser and multi-bit ADC can increase the speed of physical random bits significantly [8,9]. Since then, many schemes based on laser chaos appeared [10–16]. These random bit generators (RBGs) based on the chaotic laser required transforming optical signals to electronic signals prior to digitization. In 2013, Li et al. presented an RBG based on chaos from weakly coupled semiconductor superlattices operated at room temperature [17]. This method is robust and its fully electronic implementation indicates scalability and minimal postprocessing in comparison to existing optical implementations.

In recent years, the amplified spontaneous emission (ASE) noise emitted from super-luminescent diodes (SLDs) is another attractive broadband photonic source for high-speed true random bit generation [18–21], because its origin from quantum mechanism can ensure the true randomness of the generated random numbers. There are two main methods to generate true random bits using ASE: one is to use the full-spectrum ASE noise [19–21] and the another is to use the spectrum-sliced ASE noise [18]. Their generation rates have been demonstrated from 8.33 Gbit/s to 1.6 Tbit/s, but these true random bits are all produced in off-line and they are not the real-time random bits with real waveform. Their high-speed generation rates are just some theoretical predictions, because their real achievement in such rates will be very difficult due to the well-known ‘electronic bottleneck’. Actually, the interaction of information is achieved through real waveforms in a practical communication. Thus, these off-line schemes are not suitable for real communication systems.

In this paper, we demonstrate a real time scheme for true random bits generation based on ASE from an SLD. Combine with the differential delay comparison and XOR logic circuit, we eventually...
acquire the real-time true random bit waveform up to 3 Gbit/s with verified randomness by the NIST statistical tests. Moreover, our system is scalable and can use multiple ASE signals with different wavelengths to generate multi-channel high-speed true random bits. This can greatly enhance the generation rate of true random bits to meet the needs of secure communication with higher rate.

2. Experimental setup

The experimental setup of the true random bit generator based on the ASE noise from the SLD is shown in Fig. 1. Black solid line represents the fiber and gray solid line represents the broadband cable. An optical noise signal of the center wavelength $\lambda_1$ can be obtained from the broadband ASE noise emitted from the fiber-coupled SLD (Thorlabs 1005s) using a wavelength division multiplex (WDM). The optical signal is detected and converted into an electrical signal by an amplified photodetector (PD, New Focus 1554-B, 12 GHz bandwidth). Then the electrical signal is divided into two beams through a T-type connector and an extra electrical delay line is inserted into an input terminal of the comparator. The two signals are differentially coupled to a latch comparator consisting of a 1-bit comparator (ADCMPS67, 5 GHz bandwidth) and a D flip-flop (MC10EP52, 6 GHz bandwidth). The DFF is controlled by a clock (TG_C1-A). The electrical signal is converted into random bits after the latch comparator. The rate of the random bits is same as the input clock. Meanwhile, an optical noise signal of the center wavelength $\lambda_2$ can also be obtained from the SLD using the same WDM. And the optical noise signal can produce another sequence of random bits with the same way. The two sequences of random bits are combined with a logical exclusive-or (XOR, MC10EP08, 3 GHz bandwidth) operation to improve the randomness. Finally, the 3 Gbit/s true random bits are produced. The waveforms and eye diagrams of the generated true random bits are observed and recorded by an oscilloscope (OSC, LeCroy SDA8062i-A) with a 6 GHz bandwidth and a 40 GSample/s sampling rate.

3. Experimental results

As mentioned above, the SLD generates broadband ASE noise that is separated into eight nonoverlapping spectral slices with center wavelengths from $\lambda_1$ to $\lambda_8$ using a WDM. Each of the eight spectrally sliced channels has an optical transmission bandwidth of 0.6 nm, and the center wavelength spacing between two adjacent channel is 0.8 nm. In the experiment, it is found that the two optical noise signals with center wavelengths $\lambda_1$ and $\lambda_2$ or $\lambda_1$ and $\lambda_9$ can be used to generate true random bits. In other words, the two signals of center wavelength spacing of 0.8 nm, 1.6 nm,..., 5.6 nm can be used to generate true random bits. Here we just take two optical noise signals with center wavelengths $\lambda_1$ and $\lambda_2$ for example to demonstrate the generation process of true random bits.

The optical spectra of the SLD and the two filtered signals with center wavelengths $\lambda_1$ and $\lambda_2$ are shown in Fig. 2(a) and (b). The injection current of the SLD is set to 350 mA (the threshold is 81 mA) in this experiment, the 3 dB bandwidth of the optical spectra is 54.5 nm. The center wavelengths $\lambda_1$ and $\lambda_2$ of the two filtered signals correspond to 1557.36 nm and 1556.55 nm, respectively. The optical spectra are measured by an optical spectrum analyzer (Agilent 86140B) and the resolution bandwidth (RBW) is 0.06 nm.

The temporal waveforms of the optical noise signals with center wavelengths $\lambda_1$ and $\lambda_2$ are shown in Fig. 3(a) and (b). Both of the temporal waveforms oscillate irregularly. The radio-frequency (RF) spectra of the two optical noise signals and the background noise obtained by extinguishing the optical input signal are shown in Fig. 3(c) and (d). The RF spectra of the filtered signals and the background noise are measured by a spectrum analyzer (Agilent N9020A) with 1 MHz resolution bandwidth. The RF spectra of the two signals are very flat over wide frequency range. Unlike the RF spectra of the chaotic laser signal generated by the semiconductor laser with optical feedback, the filtered signals do not have the characteristics of frequency modulation [22]. The electrical power of the filtered signals is much stronger than the background noise, so the effect of the background noise can be ignored in this experiment.

The autocorrelation function of the optical noise signal with center wavelength $\lambda_1$ and the cross-correlation function of the two filtered signals are shown in Fig. 4(a) and (b). The curve of the autocorrelation function presents a kind of delta function and has no obvious side lobe. It is shown that the optical noise signal had no periodicity. And the case of the autocorrelation function of the optical noise signal with center wavelength $\lambda_2$ is same as that of $\lambda_1$. The temporal waveforms and correlograms show that the two filtered signals are really random, and there is no correlation between them. The low correlation is a good indication of randomness.

In the experiment, the electrical signal output from the PD is divided into two beams through a T-type connector before the ADC, one as the input signal $V(t – r)$ and the other with the delay line as the threshold signal $V(t)$. The introduction of the delay is to realize the differential comparison and thus improve the amplitude distribution of the optical noise signal. Otherwise we had to continuously accuracy adjust the threshold voltage of 1-bit ADC; the whole system would be difficult to operate stably in a long time. In this condition, the output of the 1-bit ADC will be a high level when $V(t) > V(t – r)$ and otherwise a low level. The probability functions (histogram) of the optical noise signal with center wavelength $\lambda_1$ before and after the differential comparison are shown in Fig. 5(a) and (b). From them, it is obvious that the amplitude distribution of the optical noise signal without differential comparison is not symmetrical, while its differential signal

![Fig. 1. Schematic experimental setup of the true random bit generator. WDM: wavelength division multiplex; PD: photodetector; ADC: 1-bit analog to digital converter; DFF: D flip-flop; CLK: clock; XOR: exclusive or; OSC: digital oscilloscope.](image-url)
is symmetrical. This symmetry can guarantee that the output of the 1-bit ADC will be uniform in the proportion of '0' and '1'. This differential comparison operation can improve the amplitude distributions of the two signals and make them more symmetric. Above all, it does not need to adjust the threshold voltage of the comparator precisely. The criterion of the delay length selection is that the correlation coefficient corresponding to the delay time is less than 0.004 [23]. When the delay time is set to 5 ns.

Fig. 2. (a) Optical spectrum of the SLD. (b) Optical spectrum of the two filtered optical noise signals. All measured with a resolution bandwidth (RBW) of 0.06 nm.

Fig. 3. Experimental results of (a), (b) temporal waveforms of the optical noise signal with center wavelengths $\lambda_1$ and $\lambda_2$; (c), (d) RF spectra of the optical noise signal with center wavelength $\lambda_1$ or $\lambda_2$ and the background noise. The RF spectra were measured with a resolution bandwidth of 1 MHz.

Fig. 4. (a) The autocorrelation function of the optical noise signal with center wavelength $\lambda_1$; (b) the cross-correlation function of the two optical noise signals.

Please cite this article as: M. Huang, et al., Optics Communications (2014), http://dx.doi.org/10.1016/j.optcom.2014.03.052
corresponding to the delay line is 1 m, the correlation coefficient is 0.00005.

The temporal waveform and eye diagram of the real-time rate for 3 Gbit/s true random bits are shown in Fig. 6(a) and (b). As shown in Fig. 6(a), the output true random bits is in a non-return-to-zero format, and the smallest random bit width is 334 ps, which means that the rate of true random bits is 3 Gbit/s. In addition, the amplitude range of random bits is 924 mV, and the rise time (20–80%) is 107 ps. The output high-level represents random bit 1 and low-level represents random bit 0. In Fig. 6(b), the eye diagram of random bits is shown well, the intersymbol interference and noise are small. The time between the two corners of the eye is a random bit width of 333 ps, and the rise time of the eye is in accord with random bits. The generated true random bits can be used in communication network.

We use the NIST Special Publication 800-22 (NIST SP 800-22) test provided by the National Institute of Standards and Technology to evaluate the randomness of the generated random bit sequences [24], the test consists of 15 statistical tests. Typical results of the NIST tests are shown in Table 1. From Table 1, we know that the generated 3 Gbit/s true random bit sequences pass all of the NIST statistical tests.

### Table 1

<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>0.417219</td>
<td>0.9910</td>
<td>Success</td>
</tr>
<tr>
<td>Block frequency</td>
<td>0.234373</td>
<td>0.9870</td>
<td>Success</td>
</tr>
<tr>
<td>Cumulative sums</td>
<td>0.546283</td>
<td>0.9920</td>
<td>Success</td>
</tr>
<tr>
<td>Runs</td>
<td>0.463512</td>
<td>0.9880</td>
<td>Success</td>
</tr>
<tr>
<td>Longest run</td>
<td>0.620465</td>
<td>0.9900</td>
<td>Success</td>
</tr>
<tr>
<td>Rank</td>
<td>0.929552</td>
<td>0.9920</td>
<td>Success</td>
</tr>
<tr>
<td>FFT</td>
<td>0.904708</td>
<td>0.9930</td>
<td>Success</td>
</tr>
<tr>
<td>Non-overlapping template</td>
<td>0.737915</td>
<td>0.9870</td>
<td>Success</td>
</tr>
<tr>
<td>Overlapping template</td>
<td>0.697257</td>
<td>0.9830</td>
<td>Success</td>
</tr>
<tr>
<td>Universal</td>
<td>0.755819</td>
<td>0.9860</td>
<td>Success</td>
</tr>
<tr>
<td>Approximate entropy</td>
<td>0.413628</td>
<td>0.9930</td>
<td>Success</td>
</tr>
<tr>
<td>Random excursions</td>
<td>0.987896</td>
<td>0.9883</td>
<td>Success</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>0.142602</td>
<td>0.9850</td>
<td>Success</td>
</tr>
<tr>
<td>Serial</td>
<td>0.288249</td>
<td>0.9900</td>
<td>Success</td>
</tr>
<tr>
<td>Linear complexity</td>
<td>0.908760</td>
<td>0.9880</td>
<td>Success</td>
</tr>
</tbody>
</table>

4. Discussion and conclusion

Firstly, we discuss how an XOR is necessary in our current experiment. The delay lines in the 1-bit ADC may produce some correlations in the sequence of random bits. We record some random bits output from the individual DFF and evaluate their randomness. Typical NIST test results of these bits are shown in Table 2. In our experiment, the random bits before the XOR step usually cannot pass two test items, i.e. Longest Run and FFT, which are linked with correlation in some extent. Comparing with Table 1 which is a typical test result of the final random bits after the XOR gate, we think that the XOR operation will improve the possible correlation in the final true random bits.

The random bit generator is robust and insensitive to external perturbations such as temperature. Its robustness can be reflected well through a good real-time indicator, i.e. the 0/1 ratio of 1-Mbit samples.
wavelength spacing of the signals is not less than 0.8 nm. Considering the 10 dB spectral width of the SLD, it can be separated into 125 nonoverlapping spectral slices. Two signals generate one channel of true random bits, and the SLD can produce 62 channels of true random bits; thus the cumulative generation rate can be 186 Gbit/s. So the rate of the generated true random bits can be improved by increasing the bandwidth of the circuit components or parallel processing on the original experiment device.

The system employs the AES noise generated by SLD as the physical entropy source of the true random bits generator. Including filtering, photoelectric conversion, 1-bit latch comparator and exclusive-or processing, the system can generate 3 Gbit/s true random bits in real time and the random bits pass all of the NIST statistical tests. In the meantime, the system can be used to generate multiple channels of high-speed true random bits and its structure is simple and easy to be integrated, it can be widely used in military, communication, etc.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 60927007, 61001114, 61227016 and 61205142.

References