

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/45924367>

# Truly random number generation via entropy amplification

Article · June 2010

Source: arXiv

---

CITATIONS

2

---

READS

136

3 authors, including:



Hong Guo

Peking University

422 PUBLICATIONS 3,844 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Polarizing Helium-3 atoms [View project](#)



Practical security of quantum key distribution [View project](#)

# Truly random number generation via entropy amplification

Yu Liu, Mingyi Zhu, and Hong Guo\*

*CREAM Group, State Key Laboratory of Advanced Optical Communication Systems and Networks (Peking University) and Institute of Quantum Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*

*\*Corresponding author: hongguo@pku.edu.cn*

We present a simple setup to implement truly random number generator based on the measurement of the laser phase noise. From the entropy point of view, we estimate the number of truly random bits that can be extracted from the sampled Byte. With a simple method of adopting the  $m$ -least-significant-bit, we amplify the entropy of the original bit sequence and realize a truly random bit generation rate of 300 Mbps. © 2010 Optical Society of America

*OCIS codes:* 270.2500, 270.5568.

The application of random number generator (RNG) covers wide areas of cryptography, statistical sampling, computer simulations, etc. Traditionally, RNG is implemented using the algorithm-based pseudo-random number generator (PRNG), while in most application areas, PRNGs are not enough. So far, it is commonly accepted that pure quantum process is the only solution for truly random number generator (TRNG). Recently, two kinds of quantum noise of laser, phase noise and relaxation oscillation noise, are chosen to generate truly random bit sequence with high generation rate [1–4]. Phase noise, directly measured using self-delayed homodyne detection [1,2], can be used to generate random bits with good randomness, but the final random number generation rate is limited by the laser linewidth; relaxation oscillation noise, amplified by chaotic behavior, can be used to achieve ultra-high random bit generation rate [3,4], but the random bits generated by chaotic laser involve more classical noise (not truly random) and so cannot have good results in three-sigma randomness tests [1, 4]. To generate an original random bit sequence, either an oscilloscope [2] or an analog-digital-converter (ADC) [4] is available for high speed multi-bit per measurement data recording, but due to data size limitation in one scan process, using oscilloscope will reduce the generation rate for long random bit sequence. Multi-bit per measurement method

increases the random number generation rate but introduces additional correlations. The proper number of bits extracted from the recorded data can be estimated by randomness evaluation.

In this Letter, we propose a simple method to evaluate the randomness from the entropy point of view, which gives the upper and lower estimations of the maximal bits that can be extracted from one measurement. The laser phase noise (Gaussian random variable [5]) measurement based TRNG scheme is adopted, where a single-mode vertical cavity surface emitting laser (VCSEL) is used and sampled by an ADC. After entropy amplification by bit extraction, we realize a 300 Mbps TRNG, which passes three standard statistical tests. Note that this bit extraction method is also applicable for other random sources.

The schematic setup is shown in Fig. 1 (see also [1]) and the delayed self-homodyne method is used to measure the phase noise of the VCSEL. The beat signal of  $E(t)$  and  $E(t + \tau)$  is detected by the avalanche photodetector (APD) and sampled at  $f_s = 100$  MHz by the 8-bit binary ADC. When the delay time is much longer than the coherence time of laser ( $\tau \gg \tau_{\text{coh}}$ ), the autocorrelation function of the laser electric field is eliminated [6], i.e.,  $\langle E^*(t)E(t + \tau) \rangle \propto \exp(-|\tau|/\tau_{\text{coh}}) \rightarrow 0$ , where  $\tau_{\text{coh}} = (\pi\Delta\nu_{\text{Laser}})^{-1}$  and  $\Delta\nu_{\text{Laser}}$  is the laser linewidth. In this case, the beat signal of these two mutually independent laser fields can be considered as a good candidate to implement TRNG.

Since the phase noise of the laser is inversely proportional to the laser power, while the classical noises are laser power independent [7], we choose working current just above the threshold current to ensure that the phase noise is dominant and the true randomness can thus be guaranteed. In experiment, a 795 nm VCSEL laser works at 1.4 mA (threshold current 1.3 mA), and its linewidth is  $\Delta\nu_{\text{Laser}} = 120$  MHz ( $\tau_{\text{coh}} = 2.65$  ns). With delay time  $\tau = 5$  ns, the power spectral density of the beat signal is shown in Fig. 2 (a). In Fig. 2 (b), we calculate the autocorrelation function  $R_{\text{beat}}(t)$  from the power density spectrum in Fig. 2 (a) using Wiener-Khintchine theorem [8]. Without any post-processing, the autocorrelation of the laser source sampled by 8-bit ADC at 100 MHz (time delay 10 ns) is smaller than  $10^{-2}$ .

Due to the dependence on the external parameters in the experiment, the sampled original data digitized by an 8-bit ADC is biased. To reduce the bias, we perform a simple exclusive-OR post-processing between every two 8-bit original data, which is a common method to improve the randomness of RNG [9]. After the bit extraction, the histogram of the data is shown in Fig. 3 (a), well fitted with a Gaussian profile. Since truly randomness should have a uniform distributed histogram with Shannon entropy of 8 bits per Byte, the randomness in this original data is limited by the correlation within the Byte. To evaluate the randomness, we calculate Shannon entropy using the experiment results (histogram data):  $H_S = -\sum_{i=-128}^{127} p_i \log_2 p_i = 7.1925$ , where  $p_i$  is the probability of the data in the  $i^{\text{th}}$  digi-

tized bin (totally  $2^8$  bins). This can roughly be viewed as that this data can extract 7.1925 random bits out of every Byte using appropriate, yet maybe complicated bit extraction post-processing. To assure that Shannon entropy can evaluate the randomness of the source, we calculate the entropy of laser source according to its Gaussian fitting curve (Fig. 3 (a)) using  $H'_S = \frac{1}{2} \log_2(2\pi e\sigma^2)$ , where  $\sigma$  is the standard deviation of Gaussian profile. The result of the entropy of the laser source is  $H'_S = 7.2685$  bits per Byte, and experiments show these two values of Shannon entropy get closer when the size of the data is larger.

To avoid complicated post-processing, adopting  $m$ -least-significant-bit ( $m$ -LSB) out of each Byte is an efficient method to amplify the randomness. But this method is not strong in eliminating the correlation, and extracting 7-LSB according to Shannon entropy cannot pass the random tests. Therefore, we change the randomness indicator to min-Entropy,  $H_{min} = -\log_2\{\max(p_i)\}$ , which uses only the maximal probability and represents the worst-case scenario [10]. By simply adopting the last 6-bit in each Byte according to the result,  $H_{min} = 6.5083$  bits per Byte, the histogram of the new random bit sequence shows good uniformity (inset of Fig. 3 (a)) and represents good randomness. Hence, we can consider Shannon entropy and min-entropy, respectively, as the upper and lower estimations of the randomness of the laser source.

For true randomness, Shannon entropy and min-entropy have the same value and both equal 8 bits per Byte. In our experiments, after the bit extraction process, the values of these two entropies are amplified to 7.99996 and 7.98333 bits per Byte, respectively. To further illustrate the entropy amplification, we calculate the normalized entropy  $H_{nor} = H(m)/m$  of the random bit sequence before and after bit extraction (Fig. 3 (b)), where  $H(m)$  represents Shannon entropy with the length of tested-bit sequences  $m$ . Since Shannon entropy holds  $H(m) = m$  for true randomness, normalized entropy should be unity for any  $m$ . It can be seen from Fig. 3 (b) that, after bit extraction, the entropy of the random bit sequence is amplified and gets much closer to unity.

For randomness tests, we continuously record a final random bit sequence of 1 Gbit, and it passes all three standard random tests, i.e., ENT: a pseudorandom number sequence test program [11], Diehard: a battery of tests of randomness [12], and NIST-STS: the National Institute of Standards and Technology-Statistical Test Suite [13]. The ENT results are: entropy = 1.000000 bit per bit (the optimum compression would reduce the bit file by 0%).  $\chi^2$  distribution is 0.13 (randomly would exceed this value less than 96.47% of the times). Arithmetic mean value of data bits is 0.5000 (0.5 = random). Monte Carlo value for  $\pi$  is 3.141676275. Serial correlation coefficient is 0.000041. The results of Diehard and STS test are shown in Fig. 4 (a) and (b), respectively.

In summary, we implement a simple and compact TRNG based on the measurement of the laser phase noise, which passes all three standard statistical random tests. To amplify

the entropy, we estimate the maximal bits that can be extracted from each sampled Byte by LSB-adoption, and realize a 300 Mbps truly random number generation rate.

This work is supported by the Key Project of National Natural Science Foundation of China (NSFC) (grant 60837004) and National Hi-Tech Research and Development (863) Program. We acknowledge the help from W. Tang, W. Wei, Y. Li, J. Zhou and J. Zhang.

## References

1. H. Guo, W. Tang, Y. Liu, and W. Wei, “Truly random number generation based on measurement of phase noise of a laser,” *Phys. Rev. E* **81**, 051137 (2010); arXiv: 0908.2893v3 [quant-ph].
2. B. Qi, Y. M. Chi, H. K. Lo, and L. Qian, “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” *Opt. Lett.* **35**, 312 (2010); arXiv: 0908.3351v2 [quant-ph].
3. 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. Photon.* **2**, 728 (2008).
4. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, “Ultrahigh-speed random number generation based on a chaotic semiconductor laser,” *Phys. Rev. Lett.* **103**, 024102 (2009).
5. M. Lax, “Classical noise. V. noise in self-sustained oscillators,” *Phys. Rev.* **160**, 290 (1967).
6. C. H. Henry, “Theory of the linewidth of semiconductor lasers,” *IEEE J. Quantum Electron.* **18**, 259 (1982).
7. K. Vahala and A. Yariv, “Occupation fluctuation noise: a fundamental source of linewidth broadening in semiconductor lasers,” *Appl. Phys. Lett.* **43**, 140 (1983).
8. N. Wiener, *Acta Math.* **55**, 117 (1930).
9. M. Epstein, L. Hars, R. Krasinski, M. Rosner, and H. Zheng, “Design and implementation of a true random number generator based on digital circuit artifacts,” *Lect. Notes Comput. Sci.* **2779**, 152 (2003).
10. M. Wayne, and P. Kwiat, “Low-bias high-speed quantum random number generator via shaped optical pulses,” *Opt. Express* **18**, 9351 (2010).
11. J. Walker, “ENT: a pseudorandom number sequence test program,” <http://www.fourmilab.ch/random/>.
12. G. Marsaglia, “Diehard: a battery of tests of randomness,” <http://www.stat.fsu.edu/pub/diehard/>.
13. NIST, “STS: the National Institute of Standards and Technology-Statistical Test Suite,” [http://csrc.nist.gov/groups/ST/toolkit/rng/stats\\_tests.html](http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html).

## List of Figure Captions

Fig. 1. (Color online) Schematic setup of TRNG based on the laser phase noise measurement using delayed self-homodyne method. BS: beam splitter; APD: Silicon avalanche photodetector with the low (high) cutoff frequency of 50 kHz (1 GHz); ADC: 8-bit binary analog-digital-converter working at  $f_s = 100$  MHz.

Fig. 2. (Color online) (a) The laser phase (detection background) noise of the laser field is observed at 1.4 mA (0 mA), while the threshold current is 1.3 mA. (b) Autocorrelation function of the beat signal vs time delay (red line corresponds to autocorrelation of 0.01). The sampling frequency is  $f_s = 100$  MHz ( $t_s = 10$  ns).

Fig. 3. (Color online) (a) Histogram of the laser intensity digitized by an 8-bit ADC after reducing bias by exclusive-OR post-processing, and after entropy amplification by bit extraction (inset). (b) Normalized entropy  $H(m)/m$  of the random bit sequence when the  $m$ -least-significant-bit ( $m$ -LSB) is adopted.

Fig. 4. (Color online) The results of the randomness tests of (a) Diehard and (b) STS. The Diehard test is considered successful when all  $P$  values satisfy  $0.01 < P < 0.99$ . The STS test is considered successful when all  $P$  values are larger than 0.0001 and the passed portions are between  $0.99 \pm 0.095$ .

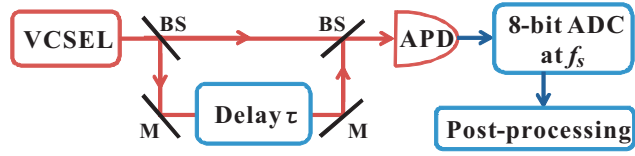


Fig. 1. (Color online) Schematic setup of TRNG based on the laser phase noise measurement using delayed self-homodyne method. BS: beam splitter; APD: Silicon avalanche photodetector with the low (high) cutoff frequency of 50 kHz (1 GHz); ADC: 8-bit binary analog-digital-converter working at  $f_s = 100$  MHz.

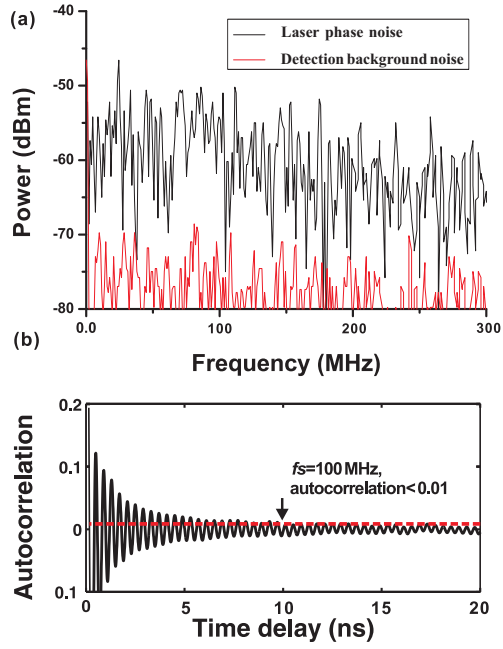


Fig. 2. (Color online) (a) The laser phase (detection background) noise of the laser field is observed at 1.4 mA (0 mA), while the threshold current is 1.3 mA. (b) Autocorrelation function of the beat signal vs time delay (red line corresponds to autocorrelation of 0.01). The sampling frequency is  $f_s = 100$  MHz ( $t_s = 10$  ns).



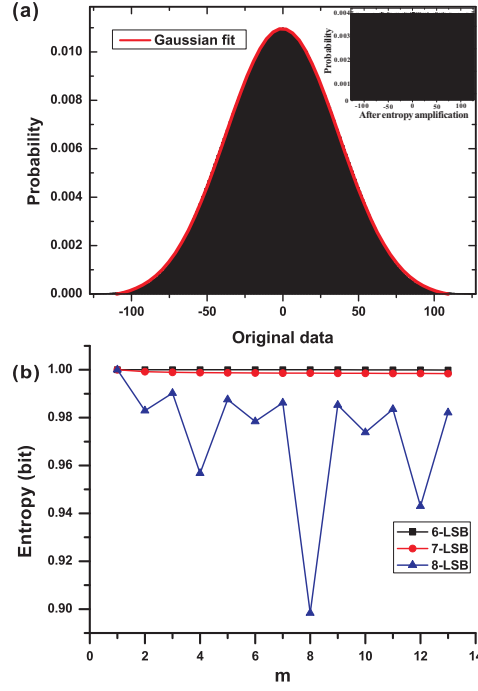


Fig. 3. (Color online) (a) Histogram of the laser intensity digitized by an 8-bit ADC after reducing bias by exclusive-OR post-processing, and after entropy amplification by bit extraction (inset). (b) Normalized entropy  $H(m)/m$  of the random bit sequence when the  $m$ -least-significant-bit ( $m$ -LSB) is adopted.

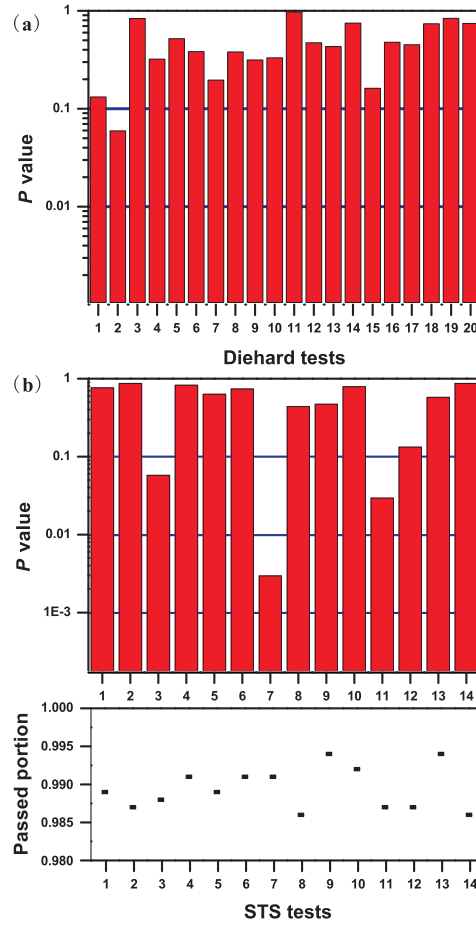


Fig. 4. (Color online) The results of the randomness tests of (a) Diehard and (b) STS. The Diehard test is considered successful when all  $P$  values satisfy  $0.01 < P < 0.99$ . The STS test is considered successful when all  $P$  values are larger than 0.0001 and the passed portions are between  $0.99 \pm 0.095$ .