High-speed quantum random number generation by measuring phase noise of a single-mode laser

Bing Qi,[1,2,*] Yue-Meng Chi,[1,2] Hoi-Kwong Lo,[1,2,3] and Li Qian[1,2]

[1]*Center for Quantum Information and Quantum Control, University of Toronto, Toronto, Ontario, Canada*
[2]*Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada*
[3]*Department of Physics, University of Toronto, Toronto, Ontario, Canada*
**Corresponding author: bqi@physics.utoronto.ca*

Received October 22, 2009; accepted December 7, 2009;
posted December 23, 2009 (Doc. ID 118903); published January 25, 2010

We present a high-speed random number generation scheme based on measuring the quantum phase noise of a single-mode laser operating at a low intensity level near the lasing threshold. A delayed self-heterodyning system has been developed to measure the random phase fluctuation. By actively stabilizing the phase of the interferometer, a random number generation rate of 500 Mbit/s has been demonstrated and the generated random numbers have passed all the DIEHARD tests. © 2010 Optical Society of America

OCIS codes: 270.2500, 270.5565.

Random numbers have been widely used in many branches of science and technology, such as statistical analysis, computer simulation [1], and cryptography [2]. One recent example is quantum key distribution (QKD) [3], where truly random numbers are needed for both quantum state preparation and quantum state detection.

In practice, it is not easy to obtain high-quality random numbers with proven randomness. Conventional pseudorandom generators based on algorithms or physical random generators based on the chaotic behavior of complex systems are not suitable for certain applications owing to their deterministic nature. On the other hand, the probabilistic nature of quantum mechanics suggests that true random numbers can be generated from fundamental quantum processes [4].

To date, most quantum random number generators (QRNGs) are based on performing single photon detections [4,5], and the highest random number generation rate achieved is 16 Mbit/s [6]. Although there is still some room for improvement, the ultimate speed is limited by the performance of the single photon detector (SPD), especially its dead time.

We note that ultrahigh speed random number generators (RNGs) based on chaotic semiconductor lasers have been proposed, and random number generation rates above Gbit/s have been demonstrated [7,8]. However, the observed noise is mainly due to the chaotic behavior of the laser rather than fundamental quantum noise.

Here, we present a QRNG scheme based on measuring the quantum phase noise of a single-mode semiconductor laser [9]. The phase noise of a laser originates from spontaneous emission [10]: each spontaneous emitted photon has a random phase, which in turn contributes a random phase fluctuation to the total electric field and results in a linewidth broadening. The spontaneous emission and the corresponding phase noise are quantum mechanical in origin. We remark that a practical laser source also exhibits additional classical noises. Fortunately, the quantum phase noise (manifested as the fundamental laser linewidth) is inversely proportional to the laser output power [10]. By operating the laser at a low intensity level near the lasing threshold, we measured a 32-fold broadening of its emission spectrum. This ensures that the main contribution to the phase noise is from spontaneous emission, rather than from the chaotic evolution of the macroscopic field [7]. One significant advantage of our scheme is the potential high random number generation rate. In this Letter, we demonstrate a 500 Mbit/s random number generation rate with commercial off-the-shelf components.

The experimental setup is shown in Fig. 1. A 1.5 μm single-mode cw distributed-feedback (DFB) diode laser (ILX Lightwave) is employed as the laser source. Two symmetric fiber couplers are used to construct a fiber Mach–Zehnder interferometer (MZI) with a length imbalance of ΔL. The interference signals from the MZI are fed into two detection channels, Ch1, including a 5 GHz bandwidth InGaAs photodetector (PD_1 in Fig. 1) and a 1 GS/s data acquisition (DAQ) card (DAQ_1 in Fig. 1, implemented with a 3 GHz bandwidth real time oscilloscope), is used to generate random numbers; Ch2 (PD_2 in Fig. 1), which has a bandwidth of 1 MHz, is used to monitor the slow phase drift of the MZI due to temperature changes. The output from PD_2 is sampled by a slow DAQ card (DAQ_2 in Fig. 1, NI PCI6115) at

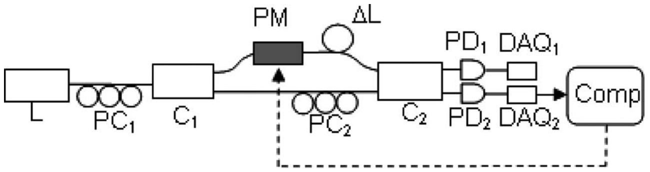

Fig. 1. Experimental setup. L, 1550 nm DFB diode laser; PC_1, PC_2, polarization controllers; PM, phase modulator; C_1, C_2, fiber couplers; PD_1, 5 GHz photodetector for random number generation; PD_2, 1 MHz photo receiver for phase monitoring; DAQ_1, 1 GS/s data acquisition card; DAQ_2, 1 MS/s data acquisition card; Comp, desktop computer. The time delay difference resulting from the length imbalance ΔL is 650 ± 100 ps.

1 MS/s, which in turn provides a feedback control signal to a phase modulator (PM) inside the MZI.

The electric field of a laser beam can be described by

$$E(t) = E_0 \exp\{i[\omega_0 t + \theta(t)]\}, \tag{1}$$

where $\theta(t)$ represents the random phase fluctuation of the laser source.

After removing a constant background term, the interference signal can be described by

$$S(t) \propto \cos[\omega_0 T_d + \Delta\theta(t, T_d)], \tag{2}$$

where $\Delta\theta(t, T_d) \equiv \theta(t) - \theta(t + T_d)$.

In Eq. (2), $T_d = n\Delta L/C$ is the time-delay difference between the two arms of the MZI, n is the refractive index of fiber, and C is the speed of light in vacuum. The term $\omega_0 T_d$ represents a phase delay introduced by the path-length difference, while the term $\Delta\theta(t, T_d)$ represents the quantum phase noise of the laser. $\Delta\theta(t, T_d)$ can be treated as Gaussian white noise with a variance of [11]

$$\langle[\Delta\theta(t, T_d)]^2\rangle = \frac{2T_d}{\tau_c}. \tag{3}$$

Here τ_c is the coherence time of the laser, which is related to its linewidth Δf as $\tau_c \simeq \frac{1}{\pi\Delta f}$ [11].

Equation (3) shows that as long as $T_d \gg \tau_c$, the resulting Gaussian distribution can be treated as a uniform distribution in the range of $[-\pi, \pi)$. Under this condition, the total phase $\omega_0 T_d + \Delta\theta(t, T_d)$ is also uniformly distributed in the range of $[-\pi, \pi)$ regardless of the actual value of $\omega_0 T_d$. Thus we can generate binary random numbers from the sign of $S(t)$.

We define the response time T_{R1} of the photodetection system (PD_1) as the reciprocal of its bandwidth. The sampling period T_S is defined as the reciprocal of the sampling rate. The recommended conditions for random number generation are summarized as (a) $T_d \gg \tau_c$ (see above), (b) $T_S - T_d > T_{R1}$ (to reduce the correlation between adjacent samples due to the finite response time T_{R1} and the length unbalance of the MZI), and (c) $\tau_c > T_{R1}$ (to make sure that the random phase fluctuation will not be averaged out within the response time T_{R1}). Obviously, the maximum sampling rate (or the random number generation rate) is determined by τ_c. Experimentally, by tuning the driving current of the laser, a coherence time of a few nanoseconds has been achieved, corresponding to a maximum sampling rate in the order of 100 MHz.

To go beyond the limitation imposed by τ_c, we have introduced a phase stabilization technique. From Eq. (2), by doing phase feedback control, the $\omega_0 T_d$ term in the cosine function can be stabilized at $2m\pi + \pi/2$ (where m is an integer). Thus, Eq. (2) can be further simplified as $S(t) \propto \sin[\Delta\theta(t, T_d)]$. Since the discrete time series sample $\tilde{S}(t_i)$ has a symmetric distribution around zero, we can generate binary random numbers from the sign of $\tilde{S}(t_i)$. In principle, the sampling rate is limited by T_{R1} but not τ_c. The recommended conditions for random number generation with phase stabilization are summarized as (a) $T_S - T_d > T_{R1}$ and (b) $\tau_c > T_{R1}$.

During the experiment, the driving current of the DFB laser was set to $I = 12$ mA, resulting a coherence time τ_c of 10 ns. As a comparison, the same laser has a coherence time of 320 ns at a higher driving current of 50 mA. From Eq. (3), the variance of the phase noise is proportional to $1/\tau_c$. Thus, the variance of phase noise at $I = 12$ mA is about 32 times larger than that at $I = 50$ mA. We consider this as the evidence that the phase noise at $I = 12$ mA is dominated by spontaneous emissions.

We measured the noise spectrum of $S(t)$ using a spectrum analyzer (HP8564E). Measurements have been performed with time-delay differences: $T_{d1} = 650 \pm 100$ ps and $T_{d2} = 250 \pm 100$ ps. The experiential results are shown in Fig. 2. The electrical noise of the detection system has been measured by blocking the laser output.

In Fig. 2, the electrical noise, which looks quite random in time domain, presents a few dominant spectral lines. These spikes could be due to the environmental electromagnetic noises picked up by our detection system. On the other hand, the phase noise are broadband and much stronger than the electrical noise.

Though the phase noise measured with the 250 ps delay MZI has a flatter band, we chose to use the 650 ps delay MZI for QRNG, as the phase noise is much brighter such that the power of the phase noise overwhelms the power of electrical noise. The output of PD_1 was sampled at 1 GS/s rate. To generate binary random numbers, we simply compare the sampling results $\tilde{S}(t_i)$ with the mean value S_0, the ith bit is assigned as either "1" if $\tilde{S}(t_i) > S_0$ or "0" if $\tilde{S}(t_i) < S_0$.

Two independent random number trains, Bin1 and Bin2, have been generated. The data size for each train is 10^8 bits. The degree of randomness of the raw

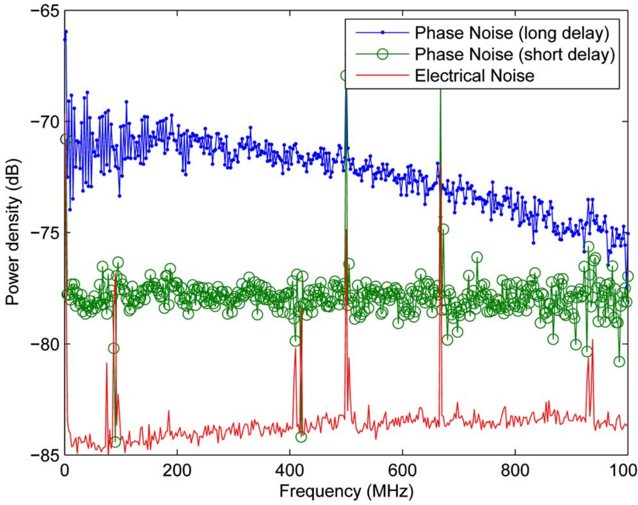

Fig. 2. (Color online) Spectral power density of electrical and phase noise. The solid-line, dot-line, and circle-line represent the spectral power densities of the detection system, the phase noise with a long delay ($T_d = 650 \pm 100$ ps), and the phase noise with a short delay ($T_d = 250 \pm 100$ ps), correspondingly.

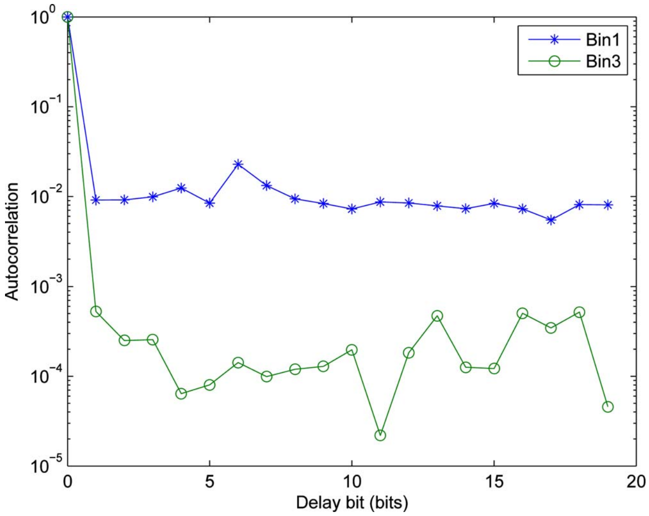

Fig. 3. (Color online) Autocorrelations of the random number trains acquired at 1 Gbit/s. Note for Bin3, the equivalent random number generation rate is 500 Mbit/s.

data trains may be affected by the presence of the spectral spikes (Fig. 2) owing to electromagnetic interference from the environment. By performing a bitwise exclusive OR (XOR) operation between Bin1 and Bin2, another random number train, Bin3, has been generated. This XOR operation has been commonly used on improving randomness of an RNG [12]. The equivalent generation rate of Bin3 is 500 Mbit/s.

Table 1. DIEHARD Test Results (500 Mbits/s)

Statistical Test	p Value	Result
Birthday spacings	0.845968 (KS[a])	Success
Overlapping 5-permutation	0.551420	Success
Binary rank test for 31×31 matrices	0.642062	Success
Binary rank text for 32×32 matrices	0.461672	Success
Binary rank text for 6×8 matrices	0.607744 (KS)	Success
Bitstream	0.98987	Success
OPSO	0.2373	Success
OQSO	0.1860	Success
DNA	0.1439	Success
Count-the-1's test	0.919419	Success
Count-the-1's test for specific bytes	0.751492	Success
Parking lot	0.199468 (KS)	Success
Minimum distance	0.721783 (KS)	Success
3D spheres	0.405683 (KS)	Success
Squeeze	0.305844	Success
Overlapping sums	0.246453 (KS)	Success
Runs	0.829651 (KS)	Success
Craps	0.838686	Success

[a] KS, Kolmogorov–Smirnov test.

The autocorrelations of Bin1 and Bin3 are shown in Fig. 3: the residual correlation of Bin3 is significantly lower than that of Bin1. This suggests that the XOR operation does improve the randomness. We remark that residual correlation of any physical RNG cannot reach zero due to the finite response time of the detection system and other imperfections. One future research direction is to design a "randomness extractor" [13] to further suppress the residual correlation.

We further test the randomness of Bin3 with the DIEHARD test suite [14]. Most of the tests in DIEHARD return a p value, which should be uniform on [0,1) if the input file contains truly independent random bits. The significance level has been chosen to be $\alpha=0.01$, which means that tests with p values within [0.01,0.99] pass the tests [5]. As shown in Table 1, Bin3 passed all the tests.

In summary, we have demonstrated a high-speed random number generation scheme based on measuring the quantum phase noise of a DFB laser diode. With off-the-shelf components, a random number generation rate of 500 Mbit/s has been achieved.

We are thankful for enlightening discussions with Fei Ye and Amr S. Helmy. Financial support from CFI, CIPI, the CRC program, CIFAR, MITACS, NSERC, OIT, and QuantumWorks is gratefully acknowledged.

References

1. N. Metropolis and S. Ulam, J. Am. Stat. Assoc. **44**, 335 (1949).
2. B. Schneier, *Applied Cryptography* (Wiley, 1996).
3. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, 1984), pp. 175–179.
4. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
5. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
6. http://www.idquantique.com.
7. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nat. Photonics **2**, 728 (2008).
8. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).
9. A preliminary version of our results has appeared in B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, in *Proceedings of The 9th Asian Conference on Quantum Information Science* (AQIS, 2009), pp. 64–65.
10. C. H. Henry, IEEE J. Quantum Electron. **18**, 259 (1982).
11. A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications*, 6th ed. (Oxford U. Press, 2007).
12. M. Epstein, L. Hars, R. Krasinski, M. Rosner and H. Zheng, Lect. Notes Comput. Sci. **2779**, 152 (2003).
13. B. Barak, R. Shaltiel, and E. Tromer, Lect. Notes Comput. Sci. **2779**, 166 (2003).
14. http://www.stat.fsu.edu/pub/diehard/.