applied sciences

MDPI

Article

A Phase Fluctuation Based Practical Quantum Random Number Generator Scheme with Delay-Free Structure

Min Huang [1], Ziyang Chen [1], Yichen Zhang [2] and Hong Guo [1,*]

[1] State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China; iqehuangmin@pku.edu.cn (M.H.); chenziyang@pku.edu.cn (Z.C.)

[2] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China; zhangyc@bupt.edu.cn

* Correspondence: hongguo@pku.edu.cn;

Received: 7 March 2020; Accepted: 24 March 2020; Published: 2 April 2020

Abstract: Quantum random number generators are widely used in many applications, ranging from sampling and simulation, fundamental science to cryptography, such as a quantum key distribution system. Among all the previous works, quantum noise from phase fluctuation of laser diodes is one of the most commonly used random source in the quantum random number generation, and many practical schemes based on phase noise with compact systems have been proposed so far. Here, we proposed a new structure of phase noise scheme, utilizing the phase fluctuation from two laser diodes with a slight difference of center wavelength. By analyzing the frequency components and adopting an appropriate band-pass filter, we prove that our scheme extracts quantum noise and filtered other classical noises substantially. Results of a randomness test shows that the extracted random sequences are of good performance. Due to lack of delay-line and the low requirement on other devices in this system, our scheme is promising in future scenarios for miniaturized quantum random number generation systems.

Keywords: quantum random number generator; phase noise; phase fluctuation; delay-free; post-processing

1. Introduction

Random numbers are of great significance in many fields, including statistical analysis, numerical simulation, fundamental science [1] and cryptography [2]. The randomness of a random number generator (RNG) could seriously affect the applications of high security demands, one of the outstanding example is the quantum key distribution (QKD) system in quantum cryptography [3–6]. Based on the determined algorithm, a classical random number generator, also called a pseudo-RNG, could generate pseudo random sequences in an efficient method, expanding the randomness from short random seeds with extremely fast speed, and compatible with portable devices. However, due to the deterministic and predictable intrinsic nature of computational algorithms, pseudo random number generators face severe security issues in applications such as secure communication systems.

In contrast, quantum random number generators (QRNG) [7–9], based on the intrinsic random nature of quantum processes, stand out as a promising alternative for its non-deterministic and unpredictable characteristics. QRNG schemes are classified into three categories, based on various requirements of physical devices, namely full-device-independent [10–12], semi-device-independent [13–18], and full-trusted-device, i.e., practical QRNG schemes. Among the three categories, practical QRNG has been developed rapidly due to its convenience and huge demand.

By adopting a certain post-processing method, practical QRNG scheme is information theoretically proved secure under the trusted-device scenario, which is adequent for the security requirements of most applications.

During the last two decades, plenty of practical QRNG schemes have been realized with high generation rate and relatively low cost, including primarily developed discrete variable schemes, which measure photon path (spatial mode) [19–21], photon arrival time (temporal mode) [22–27], photon number distribution [28–30]. A couple of years later, another category with relatively better performance was proposed, namely the continuous variable schemes. Due to the utilization of conventional high bandwidth photo-detector (PD) and analog-to-digital converter (ADC), continuous variable schemes could reach a generation rate several orders of magnitude higher than its discrete counterpart, while the volume of practical devices is also much more compact, and thus far more popular in recent research. Continuous variable QRNG schemes measure phase fluctuation of laser [31–39], vacuum fluctuation of quantum state [40–45], amplified spontaneous noise (ASE) [46–50] and so on. Among the schemes mentioned above, phase noise, or phase fluctuation, is one of the major schemes adopted as random source (the other is vacuum fluctuation), for its high generation rate and relatively simple implementation setup.

Traditional phase noise schemes utilize a self-delayed interference structure, thus inevitably introducing a delay-line in an unbalanced Mach-Zender interferometer (MZI) in the experimental setup [31,32,38,39]. However, due to the bandwidth of phase noise in the laser, it usually takes several meters for the delay-line to reduce the auto-correlation coefficient of raw data effectively. In practical devices, space for the delay-line is one of the most difficult parts to be compressed, unless this part can be totally removed by adopting a novel scheme.

In this paper, we demonstrate a QRNG scheme based on phase noise with a delay-free structure. We theoretically analyze our scheme, and point out three main frequency components in the electric signal to be measured. After adopting appropriate implementation settings, namely center wavelength of laser diodes and passband of a band-pass filter, we distill phase noise from the original signal for further randomness extraction. Two extraction methods, the m-Least significant bit (m-LSB) method [51] and universal (Toeplitz) hashing method [34,36,44,52] are used in post-processing phase. Our scheme could achieve a generation rate of 600 Mbps, which is six times the sampling rate, and passes widely used randomness test batteries. Compared with previous schemes utilizing phase noise as a random source, our scheme is delay-line free, while the devices are conventional and performance of QRNG remains similar. Thus, it has great potential in compact and portable QRNG devices in the future.

The structure of this article is described as follows. In Section 2, the schematic setup of our scheme is demonstrated, followed by analysis on different noises in the system and the principle to distill the quantum noise of phase fluctuation. An experimental implementation is built according to the scheme. Two post-processing methods are realized, namely the m-LSB method and universal (Toeplitz) hashing method. Section 3 shows the various results of randomness test batteries.

2. Delay-Free Phase Noise QRNG Scheme

2.1. Principle of Scheme

The schematic setup of our scheme is shown in Figure 1. Two laser diodes with very close center wavelength are used as random source. The intensity of lasers are carefully tuned by variable optical attenuator (VOA) to the exact same level, then optical signals of two lasers are injected into a 50:50 beam splitter (BS). Electric fields at the input ports (P1, P2) of the BS could be written as:

$$E_1(t) = \mathbf{E}_1(t) \exp\left[i\left(\omega_1 t + \varphi_1(t)\right)\right] \quad (1)$$

$$E_2(t) = \mathbf{E}_2(t) \exp\left[i\left(\omega_2 t + \varphi_2(t)\right)\right] \quad (2)$$

Since the amplitude of laser is tunable and could be very stable during the experiment, the amplitude part of field could be regarded as a constant in our scheme, which means $\mathbf{E}_i(t) = \mathbf{E}_i, i = 1, 2$. Two signals are interfered at the beam splitter, thus field at the output ports (P3, P4) of the BS could be written as:

$$E_3(t) = \sqrt{T}E_1(t) + \sqrt{1-T}E_2(t) \quad (3)$$

$$E_4(t) = \sqrt{1-T}E_1(t) - \sqrt{T}E_2(t) \quad (4)$$

where T refers to the transmittance, thus $R = 1 - T$ refers to the reflectivity of the beam splitter.

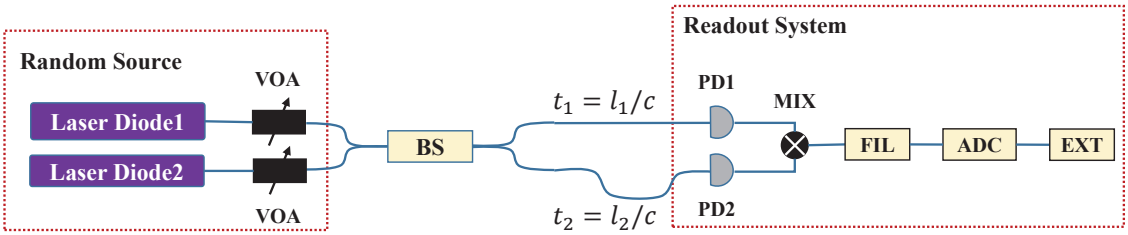

Figure 1. The schematic setup of phase noise QRNG scheme with two lasers. Laser Diode: Distribution Feedback Laser Diode with tunable center wavelength (as random source); VOA: Variable Optical Attenuator; BS: 50:50 Beam Splitter; PD1, PD2: Photodiode detectors; MIX: Frequency Mixer; FIL: Band-pass Filter; ADC: Analog-to-Digital Converter; EXT: Randomness Extractor.

Signals of port P3 and P4 take t_1, t_2 time before arriving at the detectors (D1, D2) respectively. Hence, the intensity of electric signal at detector D1 (which comes from port P3) is:

$$\begin{aligned} I_{D1}(t+t_1) &= E_3(t+t_1)E_3^*(t+t_1) \\ &= TE_1^2 + (1-T)E_2^2 \\ &\quad +2\sqrt{T(1-T)}E_1E_2\exp\left[i\left(\omega_1(t+t_1) + \varphi_1(t+t_1) - \omega_2(t+t_1) - \varphi_2(t+t_1)\right)\right] \end{aligned} \quad (5)$$

while the electric signal at detector D2 (which comes from port P4) has a similar expression:

$$\begin{aligned} I_{D2}(t+t_2) &= (1-T)E_1^2 + TE_2^2 \\ &\quad -2\sqrt{T(1-T)}E_1E_2\exp\left[i\left(\omega_1(t+t_2) + \varphi_1(t+t_2) - \omega_2(t+t_2) - \varphi_2(t+t_2)\right)\right] \end{aligned} \quad (6)$$

Apparently $I_{D1}(t)$ includes both DC term and AC term:

$$I_{D1}(t) = [I_{D1}(t)]_{DC} + [I_{D1}(t)]_{AC} \quad (7)$$

According to (5), the DC term is $TE_1^2 + (1-T)E_2^2$, and AC term is the rest. Therefore, if we use AC coupling photo-detectors in our scheme, we can only keep the AC terms in the following analysis and processing. After being detected by photo-detectors, the optical signal turns into an electric signal and the intensity $I_{D1}(t)$ is converted into optoelectric current $i_{D1}(t)$ proportionally:

$$\begin{aligned} [i_{D1}(t)]_{AC} &\propto [I_{D1}(t)]_{AC} \\ &= +2\sqrt{T(1-T)}E_1E_2\exp\left[i\left((\omega_1-\omega_2)(t+t_1) + (\varphi_1(t+t_1) - \varphi_2(t+t_1))\right)\right] \end{aligned} \quad (8)$$

$$\begin{aligned} [i_{D2}(t)]_{AC} &\propto [I_{D2}(t)]_{AC} \\ &= -2\sqrt{T(1-T)}E_1E_2\exp\left[i\left((\omega_1-\omega_2)(t+t_2) + (\varphi_1(t+t_2) - \varphi_2(t+t_2))\right)\right] \end{aligned} \quad (9)$$

Finally, the voltage signals $V_{D1}(t), V_{D2}(t)$ are combined in a mixer by frequency mixing (only the real part is considered here), and the new signal is denoted as V_{mix}:

$$\begin{aligned} V_{mix} &= [V_{D1}]_{AC}[V_{D2}]_{AC} \\ &\propto -4T(1-T)E_1^2E_2^2\cos\left[(\omega_1-\omega_2)(t+t_1)+\varphi_1(t+t_1)-\varphi_2(t+t_1)\right] \\ &\quad \cos\left[(\omega_1-\omega_2)(t+t_2)+\varphi_1(t+t_2)-\varphi_2(t+t_2)\right] \\ &= -4T(1-T)E_1^2E_2^2\cos\left[\Delta\omega(2t+t_1+t2)+\Delta\varphi(t+t_1)+\Delta\varphi(t+t_2)\right] \\ &\quad -4T(1-T)E_1^2E_2^2\cos\left[\Delta\omega(t_1-t_2)+\Delta\varphi(t+t_1)-\Delta\varphi(t+t_2)\right] \end{aligned} \tag{10}$$

where $\Delta\omega = \omega_1 - \omega_2$, $\Delta\varphi(t) = \varphi_1(t) - \varphi_2(t)$.

It is clear that from (10), the final signal includes several frequency components, in which three of them are dominating. Two of them are from the phase term $\Delta\varphi(t)$, where $\Delta\varphi^{\text{fiber}}$ is due to the fiber jitter, and $\Delta\varphi^{\text{phase}}$ comes from phase noise of laser diode, from which we expect to extract randomness. Another part of frequency term $2\Delta\omega t$ is due to the difference of center wavelength of two laser diodes. In fact, there exist a crucial relationship between these three frequency components in our scheme:

$$f(2\Delta\omega) >> f(\Delta\varphi^{\text{phase}}) >> f(\Delta\varphi^{\text{fiber}}) \tag{11}$$

and all the implementation settings in our experimental setup is based on (11).

2.2. Experimental Setup

We experimentally realized our scheme as Figure 1 shows above, and the setup is described as follows. Two distributed feedback (DFB) laser diodes emit continuous wave (CW) light with center wavelength at around 1550 nm. Specifically, the center wavelength of two DFB laser diodes are originally set at 1549.865 nm and 1549.858 nm respectively, which is 880 MHz separated from each other. The laser output power is set slightly higher than the threshold to obtain highest proportion of quantum noise [31,34,36], which is 1.3 mW in our setup. Intensity of signals from two laser diodes are carefully tuned by variable optical attenuator (VOA) to keep the intensity equal. After the signals interfere at a 50:50 beam splitter (BS), optical signals are detected by two homemade photo-detectors with AC coupling (measurement bandwidth 100 MHz). Electric signals are mixed by a frequency mixer, then the signal is filtered by a band-pass filter with 10–1000 MHz passband range to select the frequency component of phase noise, which is the appropriate frequency range in our scheme decided by the implementation. The electric signal after the filter is sampled by an analog-to-digital converter (ADC, ADS5400, sampling frequency 100 MHz, sampling precision 12 bits and input voltage range 1.5 V peak-to-peak). Finally, a field programmable gate array (FPGA, KC705 evaluation board) is adopted to realize randomness extraction and data precision adjustment. The sampling range is 1.5 V, however the peak-to-peak value of the noise signal is only 190 mV, hence there is approximately three unoccupied bits in raw data, which should be eliminated at the beginning in post-processing.

As mentioned above, we set the difference of center wavelength at around 880 MHz (0.007 nm at 1550 nm wavelength), which is higher than the noise bandwidth from phase fluctuation of laser diodes in our implementation. Noticing that, the difference of center wavelength should not be too large, since the waveform after interfering at the beam splitter may not able to keep stability for heavily mismatched laser diode wavelength, as shown in Figure 2. On the other hand, frequency of fiber jitter noise is usually no greater than 10 MHz. By utilizing a band-pass filter with a 10–1000 MHz passband range at the output port of the mixer, one can substantially eliminate the influence of the fiber jitter term $\Delta\varphi^{\text{fiber}}$, as well as the difference of center wavelength term $2\Delta\omega t$. Hence the term of phase noise is distilled and used for further randomness extraction process.

2.3. Post-Processing Method

The raw data, measured from the phase noise of laser diode, is approximately a Gaussian variable on the probability distribution function (PDF) [53,54]. However, random sequences of general QRNG schemes and applications should be a uniform distribution, hence post-processing is essential. Another function of post-processing is eliminating the unexpected randomness from the environment, which may be utilized by the adversary Eve, specifically the classical noise. Therefore, generally speaking,

a traditional post-processing method includes two phases: entropy estimation and randomness extraction. The entropy estimation phase calculate the upper bound of randomness, which can be extracted from the raw data as a discretized random variable X_{dis}, based on the observable parameters. Then, one can adopt various extractors to distill the randomness calculated before in the randomness extraction phase. There exist two efficient methods in QRNG post-processing, based on different devices in implementation and application requirements, namely the m-least significant bit (m-LSB) method and universal (Toeplitz) hashing method.

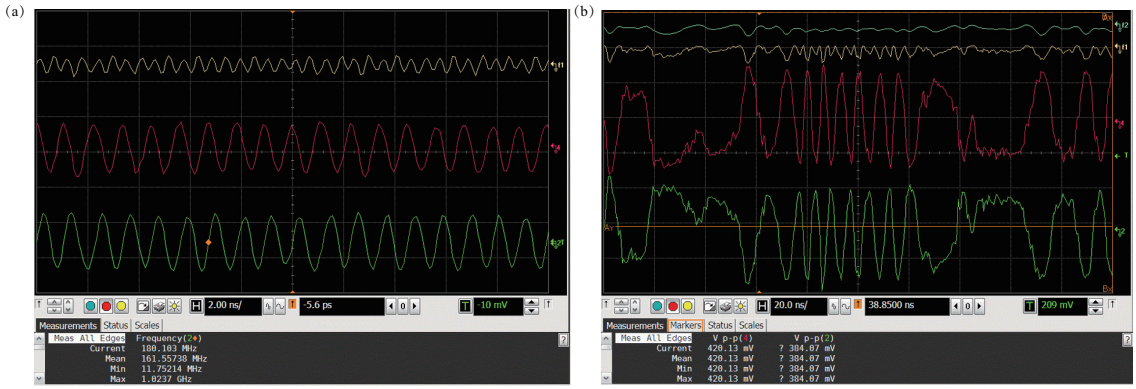

Figure 2. The waveform at photo-detectors in time domain, recorded and shown by oscilloscope (DSAX-91604A, Agilent). Two signals below are the input signal at the frequency mixer, and the signal above with smaller scale is the output signal of mixer. Pictured in (**a**) is the stable waveform with appropriate center wavelength selection. The waveform is very stable during the test, and sine shape phase noise signal is distilled by the frequency mixer and band-pass filter. Pictured in (**b**) is the incorrect waveform when the difference of center wavelength is too large to maintain a regular shape, hence the signal after mixer is also very unstable.

The former one, m-LSB method, belongs to the deterministic extractor. The m-LSB method is extremely simple to implement both on hardware and software, and could run at very high sampling and generation rate. One just truncates the raw data, takes the last m-bit random numbers and outputs the final sequence (logical exclusive OR (XOR) operation is also optional if necessary). The reason for taking the LSB instead of its counterpart, the most significant bit (MSB), is that the LSB has a better distribution and lower auto-correlation coefficient after post-processing, and thus is more difficult to be predicted by the adversary. This method is quite effective if the implementation is trusted and has a relatively high quantum-to-classical noise ratio (QCNR). However, in untrusted device scenarios, one can still extract several bits with high sampling resolution.

We adopt a m-LSB method by treating our implementation as a trusted-device scenario and according to the analysis in [51]. It is secure for m-LSB to truncate four bits out of a 16-bit discretized signal in noise-free cases, and secure to truncate five (seven) bits out of 16 bits with the deviation of classical noise σ_E three (four) times larger than quantum noise σ_Q. In fact, quantum noise is dominate in our implementation, thus truncate a moderate number of six bits from raw data (including the unoccupied three most significant bits) to form the extracted sequence is adequately conservative for our scheme. Therefore, the generation rate of adopting m-LSB method is $100 \times 6 = 600$ Mb/s.

Universal hashing method is another post-processing method often chosen in QRNG schemes, which belongs to the seeded extractor, indicating that this method should consume some short random seed to generate the universal hashing functions. Among these functions, the Toeplitz matrix is an outstanding solution for its low complexity in computation and implementation. For a binary Toeplitz matrix utilized for QRNG post-processing, the size of the original matrix is $M \times N$, where N is the size of raw data, and M is the size of extracted sequence. The ratio M/N is a crucial parameter which is closely related to the min-entropy $H_\infty(X)$ calculated in the entropy estimation phase:

$$H_\infty(X) = -\log_2(\max_{x\in[0,1]^n} Pr(X = x)). \tag{12}$$

The output sequence of Toeplitz hashing, based on the input, is almost unique, for it has a collision probability of only $2^{-M+1}N$ for a different input to share the same output. According to information theory, the security parameter ε should satisfy:

$$M = N \cdot H_\infty - 2\log_2(1/\varepsilon) \tag{13}$$

where ε also indicated the distance between the output sequence and ideal uniform sequence.

Therefore, by designing a Toeplitz matrix with ratio M/N slightly smaller than the min-entropy and adopting different matrix size, the security parameter ε could be arbitrarily close to zero. Noticing that, the seeds consumed in generating Toeplitz matrix is $N + M - 1$. Since the data size is huge in QRNG systems, post-processing should be run by block: $N = Bn, M = Bm$, where $m \times n$ is the size of practical Toeplitz matrix, and B is the number of blocks. After discarding the unoccupied bits in raw data, the min-entropy in our system is 6.60 bits/sample, hence we set our Toeplitz matrix at a moderate size of 1536×3072 and run the post-processing method by block, which means $3072 \div 12 = 256$ consecutive samples are collected and process in one Toeplitz hashing operation. The security parameter is $\varepsilon = 7.6 \times 10^{-24}$ in our implementation. Since the extracting ratio decided by the Toeplitz matrix is also 50%, the generation rate of adopting Toeplitz hashing method is also 600 Mb/s.

3. Test Results

The test is divided into two parts, including 3σ criterion and widely used test batteries such as DIEHARD or NIST-STS. Uniformity are also included in the batteries. Firstly, data are randomly chosen to perform the 3σ test to compare the difference between raw data and extracted numbers. For raw data, the sample size equals the sampling depth of 50 M points/samples with 12-bit resolution in our implementation. While for extracted sequence, the sample size is 420 Mbits, which is consecutive data in 0.7 s after post-processing. The results are shown in Figures 3 and 4. Apparently post-processing methods impressively reduce the low-order auto-correlation coefficient, due to the limited bandwidth of devices may cause some correlation in the adjacent samples of raw data, particularly in oversampled scenarios, where sampling rate and auto-correlation trade-off should be carefully dealed with in practical devices.

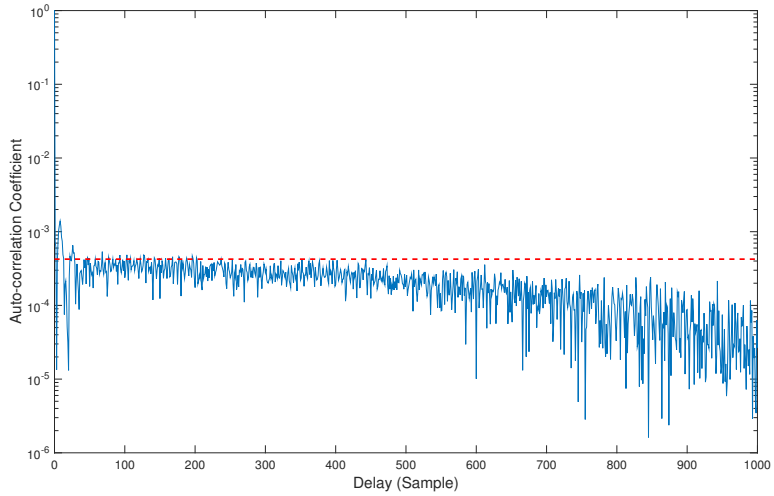

Figure 3. Auto-correlation coefficient a_k of raw data with different self-delay value k, ranging from 1 to 1000 samples ($k = 0$ always leads to $a_k = 1$, thus makes no sense). The dashed line indicates reference calculated by the 3σ criterion. Apparently there exists a relatively high correlation among adjacent 10 samples, that occasionally goes beyond the 3σ reference threshold, due to the limited bandwidth of devices.

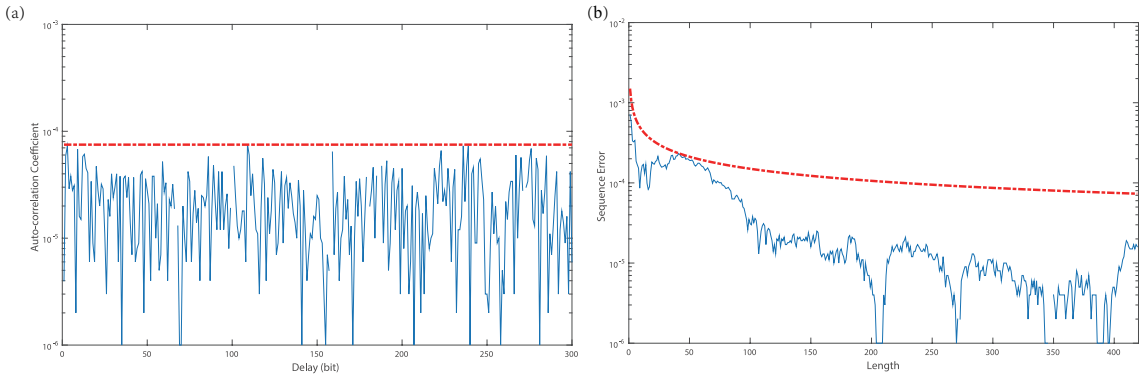

Figure 4. Auto-correlation coefficient a_k of extracted sequences. Pictured in (**a**) is auto-correlation with different self-delay value k, ranging from 1 to 300 bits. Pictured in (**b**) is a first-order auto-correlation coefficient a_1 with different sequence length, ranging from 1 M bit to 420 M bits. The dashed line indicates reference calculated by the 3σ criterion. In contrast to the test of raw data, the parameter shows no bias and does not significantly exceed the reference threshold.

In order to evaluate randomness, we also adopt widely-accepted randomness test batteries, namely DIEHARD and NIST-STS test, both of which are hypothesis tests of a statistically based randomness test, with a couple of p-values indicating whether to accept or reject the hypothesis in each sub-test. Generally speaking, if all the final p-values located between $[0.01, 0.99]$ (with default significance level $\alpha = 0.01$), the whole test is considered successful. Random sequences extracted from either the m-LSB or Toeplitz hashing method should pass both test batteries, and we choose one typical sequence from the Toeplitz hashing method as an example: the result of DIEHARD test is shown in Table 1, and result of NIST-STS test is shown in Table 2.

Table 1. The result of the DIEHARD test after post-processing. DIEHARD includes 18 terms and 20 randomness test results, each with a p-value. For the sub-tests with multiple p-values, a Kolmogorov-Smirnov (KS) test is performed to obtain the final p-value. It is considered successful for certain sub-tests if the final p-value is between $[0.01, 0.99]$ (significance level $\alpha = 0.01$). The length of test sequence is 420 Mbits.

Statistical Test	p-Value	Result
Birthday spacings	0.122824[KS]	success
Overlapping permutations	0.430620	success
Ranks of 31 × 31 matrices	0.605645	success
Ranks of 32 × 32 matrices	0.427548	success
Ranks of 6 × 8 matrices	0.260611[KS]	success
Monkey tests on 20-bit words	0.136669[KS]	success
Monkey test OPSP	0.43930[KS]	success
Monkey test OQSO	0.68062[KS]	success
Monkey test DNA	0.61412[KS]	success
Count 1's in stream of bytes	0.662425	success
Count 1's in specific bytes	0.561794[KS]	success
Parking lot test	0.312073[KS]	success
Minimum distance test	0.377192[KS]	success
Random spheres test	0.440218[KS]	success
Squeeze test	0.019830[KS]	success
Overlapping sums test	0.053688[KS]	success
Run test(up)	0.314213	success
Run test(down)	0.492526	success
Craps test No. of wins	0.420491	success
Craps test throw/game	0.965724	success

Table 2. The result of the NIST-STS test after post-processing. The NIST-STS includes 15 terms and respective test results, each with a p-value. For the sub-tests with multiple p-values, a Kolmogorov-Smirnov (KS) test is performed to obtain final p-value. It is considered successful for certain sub-test if the final p-value is between $[0.01, 0.99]$ and the success proportion is between $[0.9778, 1]$ (significance level $\alpha = 0.01$). The length of test sequence is 420 Mbits.

Statistical Test	p-Value	Proportion	Result
Frequency	0.372076	597	Success
Block Frequency	0.292462	596	Success
Cumulative Sums	0.045724[KS]	590	Success
Runs	0.294970	593	Success
Longest Run	0.940051	592	Success
Rank	0.316426	595	Success
FFT	0.959554	590	Success
Non-overlapping	0.743782[KS]	595	Success
Overlapping	0.065969	596	Success
Universal	0.494772	598	Success
Approx. Entropy	0.908376	596	Success
Excursions	0.558001[KS]	593	Success
Excursions Var.	0.032325[KS]	590	Success
Serial	0.225053[KS]	592	Success
Complexity	0.869431	595	Success

4. Conclusions

We proposed and experimentally realized a QRNG scheme utilizing quantum noise from phase fluctuation of laser diode with a novel structure. Optical signals from two laser diodes with very close center wavelength interfere at a beam splitter before detected by AC coupling photo-detectors. Electric signals from two detectors did frequency mixing with a mixer. After analyzing the frequency components, we pointed out there are three dominating frequency terms in the noise: difference of the center wavelength of laser, phase fluctuation of laser, and fiber jitter of the system. Due to the different frequency range between these components, we found it possible to substantially eliminate the unexpected terms by a well selected band-pass filter, before extracting randomness with the phase noise term. We use two conventional post-processing methods, the m-least significant bit method (m-LSB) and universal (Toeplitz) hashing method, to distill randomness from electric signal, and realize a generation rate of 600 Mb/s on hardware, which is six times higher than the sampling rate.

Our scheme has three major merits. Firstly, the structure of our scheme is delay-line free, which means the space for delay-line in practical system could be removed. Secondly, the requirement for laser diode is not so strict. One only need to make sure the center wavelength of lasers are close enough, and work with a power stabilization module, instead of a possible frequency stabilization module. Thirdly, the post-processing methods, either m-LSB or universal hashing method, can be realized on hardware in real-time. These merits make our scheme highly potential as a compact QRNG system.

We should admit that the generation rate in our scheme is relatively low in contrast to current schemes. However, this is due to building our scheme in a very conservative way and this work is just a demonstration. The bandwidth of photo-detectors and the sampling rate are both set at 100 MHz, where devices used in major schemes of phase noise are one or two orders of magnitude higher than this value. Since the generation rate is mainly limited by the detectors, it still have huge space to improve. In fact, our colleagues have realized balanced detectors with bandwidth over 1 GHz [55]. By utilizing this technique, the generation rate of our scheme is highly potential to be increased to 6 Gbps, which is the level the other QRNG scheme based on vacuum fluctuation proposed before [44]. Furthermore, the corresponding post-processing method can also be more efficient, including carefully setting the driven current of laser diode to achieve a higher quantum-to-classical noise ratio, which could lead to an even tighter upper bound of min-entropy in Toeplitz hashing method.

Author Contributions: Conceptualization, M.H. and H.G.; methodology, Y.Z.; validation, M.H.; formal analysis, M.H. and Z.C.; investigation, M.H., Z.C., Y.Z., and H.G.; resources, Y.Z. and H.G.; writing–original draft preparation, M.H.; writing—review and editing, M.H., Z.C., Y.Z., and H.G.; visualization, M.H.; funding acquisition, Y.Z. and H.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported in part by the Key Program of National Natural Science Foundation of China under Grants 61531003, and the Fund of CETC under Grant No. 6141B08231115.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QRNG	Quantum random number generator
QKD	Quantum Key Distribution
ADC	Analog-to-Digital Converter
MSB/LSB	Most/Least Significant Bit

References

1. Brunner, N.; Cavalcanti, D.; Pironio, S.; Scarani, V.; Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **2014**, *86*, 419. [CrossRef] [CrossRef]
2. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656. [CrossRef] [CrossRef]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
4. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
5. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *arXiv* **2019**, arXiv:1903.09051.
6. Pirandola, S.; Andersen, U.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *arXiv* **2019**, arXiv:1906.01645.
7. Herrero-Collantes, M.; Garcia-Escartin, J.C. Quantum random number generators. *Rev. Mod. Phys.* **2017**, *89*, 015004. [CrossRef]
8. Ma, X.F.; Yuan, X.; Cao, Z.; Qi, B.; Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2016**, *2*, 16021. [CrossRef]
9. Bera, M.N.; Acin, A.; Kus, M.; Mitchell, M.W.; Lewenstein, M. Randomness in quantum mechanics, philosophy, physics and technology. *Rep. Prog. Phys.* **2017**, *80*, 124001. [CrossRef]
10. Pironio, S.; Acin, A.; Massar, S.; de la Giroday, A.B.; Matsukevich, D.N.; Maunz, P.; Olmshenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; et al. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021. [CrossRef] [CrossRef]
11. Colbeck, R.; Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A Math. Theor.* **2011**, *44*, 095305. [CrossRef]
12. Giustina, M.; Mech, A.; Ramelow, S.; Wittmann, B.; Kofler, J.; Beyer, J.; Lita, A.; Calkins, B.; Gerrits, T.; Nam, S. Bell violation using entangled photons without the fair-sampling assumption. *Nature* **2013**, *497*, 227. [CrossRef] [CrossRef] [PubMed]
13. Cao, Z.; Zhou, H.Y.; Ma, X.F. Loss-tolerant measurement-device-independent quantum random number generation. *New J. Phys.* **2015**, *17*, 125011. [CrossRef]
14. Cao, Z.; Zhou, H.Y.; Yuan, X.; Ma, X.F. Source-independent quantum random number generation. *Phys. Rev. X* **2016**, *6*, 011020. [CrossRef]
15. Nie, Y.Q.; Guan, J.Y.; Zhou, H.Y.; Zhang, Q.; Ma, X.F.; Zhang, J.; Pan, J.W. Experimental measurement-device-independent quantum random-number generation. *Phys. Rev. A* **2016**, *94*, 060301. [CrossRef]
16. Vallone, G.; Marangon, D.G.; Tomasin, M.; Villoresi, P. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A* **2014**, *90*, 052327. [CrossRef] [CrossRef]
17. Marangon, D.G.; Vallone, G.; Villoresi, P. Source-Device-Independent Ultrafast Quantum Random Number Generation. *Phys. Rev. Lett.* **2017**, *118*, 060503. [CrossRef]

18. Xu, B.; Chen, Z.; Li, Z.; Yang, J.; Su, Q.; Huang, W.; Zhang, Y.; Guo, H. High speed continuous variable source-independent quantum random number generation. *Quantum Sci. Technol.* **2019**, *4*, 025013. [CrossRef]
19. Jennewein, T.; Achleitner, U.; Weihs, G.; Weinfurter, H.; Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **2000**, *71*, 1675. [CrossRef] [CrossRef]
20. Stefanov, A.; Gisin, N.; Guinnard, O.; Guinnard, L.; Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **2000**, *47*, 595. [CrossRef] [CrossRef]
21. Wang, P.X.; Long, G.L.; Li, Y.S. Scheme for a quantum random number generator. *J. Appl. Phys.* **2006**, *100*, 056107. [CrossRef] [CrossRef]
22. Ma, H.Q.; Xie, Y.J.; Wu, L.A. Random number generation based on the time of arrival of single photons. *Appl. Opt.* **2005**, *44*, 7760. [CrossRef] [CrossRef]
23. Stipčević, M.; Rogina, B.M. Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum.* **2007**, *78*, 045104. [CrossRef] [CrossRef]
24. Dynes, J.F.; Yuan, Z.L.; Sharpe, A.W.; Shields, A.J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **2008**, *93*, 031109. [CrossRef] [CrossRef]
25. Wayne, M.A.; Jeffrey, E.R.; Akselrod, G.M.; Kwiat, P.G. Photon arrival time quantum random number generation. *J. Mod. Opt.* **2009**, *56*, 516. [CrossRef] [CrossRef]
26. Wahl, M.; Leifgen, M.; Berlin, M.; Rohlicke, T.; Rahn, H.J.; Benson, O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Appl. Phys. Lett.* **2011**, *98*, 171105. [CrossRef] [CrossRef]
27. Nie, Y.Q.; Zhang, H.F.; Zhang, Z.; Wang, J.; Ma, X.F.; Zhang, J.; Pan, J.W. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Appl. Phys. Lett.* **2014**, *104*, 051110. [CrossRef] [CrossRef]
28. Wei, W.; Guo, H. Bias-free true random-number generator. *Opt. Lett.* **2009**, *34*, 1876. [CrossRef] [CrossRef]
29. Fürst, M.; Weier, H.; Nauerth, S.; Marangon, D.G.; Kurtsiefer, C.; Weinfurter, H. High speed optical quantum random number generation. *Opt. Express* **2010**, *18*, 13029. [CrossRef] [CrossRef]
30. Ren, M.; Wu, E.; Liang, Y.; Jian, Y.; Wu, G.; Zeng, H.P. Quantum random-number generator based on a photon-number-resolving detector. *Phys. Rev. A* **2011**, *83*, 023820. [CrossRef] [CrossRef]
31. Guo, H.; Tang, W.Z.; Liu, Y.; Wei, W. Truly random number generation based on measurement of phase noise of a laser. *Phys. Rev. E* **2010**, *81*, 051137. [CrossRef] [CrossRef]
32. Qi, B.; Chi, Y.M.; Lo, H.K.; Qian, L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.* **2010**, *35*, 312. [CrossRef] [CrossRef]
33. Jofre, M.; Curty, M.; Steinlechner, F.; Anzolin, G.; Torres, J.P.; Mitchell, M.W.; Pruneri, V. True random numbers from amplified quantum vacuum. *Opt. Express* **2011**, *19*, 20665. [CrossRef] [CrossRef]
34. Xu, F.H.; Qi, B.; Ma, X.F.; Xu, H.; Zheng, H.X.; Lo, H.K. Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express* **2012**, *20*, 12366. [CrossRef] [CrossRef]
35. Yuan, Z.L.; Lucamarini, M.; Dynes, J.F.; Frohlich, B.; Plews, A.; Shields, A.J. Robust random number generation using steady-state emission of gain-switched laser diodes. *Appl. Phys. Lett.* **2014**, *104*, 261112. [CrossRef] [CrossRef]
36. Nie, Y.Q.; Huang, L.L.; Liu, Y.; Payne, F.; Zhang, J.; Pan, J.W. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Rev. Sci. Instrum.* **2015**, *86*, 063105. [CrossRef] [CrossRef]
37. Zhang, X.G.; Nie, Y.Q.; Zhou, H.Y.; Liang, H.; Ma, X.F.; Zhang, J.; Pan, J.W. Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction. *Rev. Sci. Instrum.* **2016**, *87*, 076102. [CrossRef]
38. Yang, J.; Liu, J.L.; Su, Q.; Li, Z.Y.; Fan, F.; Xu, B.J.; Guo, H. 5.4 Gbps real time quantum random number generator with simple implementation. *Opt. Express* **2016**, *24*, 27475–27481. [CrossRef]
39. Liu, J.L.; Yang, J.; Li, Z.Y.; Su, Q.; Huang, W.; Xu, B.J.; Guo, H. 117 Gbits/s Quantum Random Number Generation With Simple Structure. *IEEE Photonics Technol. Lett.* **2017**, *29*, 283–286. [CrossRef]
40. Gabriel, C.; Wittmann, C.; Sych, D.; Dong, R.F.; Mauerer, W.; Andersen, U.L.; Marquardt, C.; Leuchs, G. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* **2010**, *4*, 711. [CrossRef] [CrossRef]
41. Shen, Y.; Tian, L.A.; Zou, H.X. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A* **2010**, *81*, 063814. [CrossRef] [CrossRef]
42. Symul, T.; Assad, S.M.; Lam, P.K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* **2011**, *98*, 231103. [CrossRef] [CrossRef]

43. Haw, J.Y.; Assad, S.M.; Lance, A.M.; Ng, N.H.Y.; Sharma, V.; Lam, P.K.; Symul, T. Maximization of extractable randomness in a quantum random-number generator. *Phys. Rev. Appl.* **2015**, *3*, 054004. [CrossRef]
44. Zheng, Z.Y.; Zhang, Y.C.; N., H.W.; Yu, S.; Guo, H. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Rev. Sci. Instrum.* **2019**, *90*, 043105. [CrossRef]
45. Zhang, J.; Zhang, Y.C.; Zheng, Z.; Chen, Z.; Xu, B.; Yu, S. Finite-size analysis of continuous variable source-independent quantum random number generation. *arxiv* **2020**, arxiv:2002.12767 .
46. Williams, C.R.S.; Salevan, J.C.; Li, X.W.; Roy, R.; Murphy, T.E. Fast physical random number generator using amplified spontaneous emission. *Opt. Express* **2010**, *18*, 23584. [CrossRef] [CrossRef] [PubMed]
47. Li, X.W.; Cohen, A.B.; Murphy, T.E.; Roy, R. Scalable parallel physical random number generator based on a superluminescent LED. *Opt. Lett.* **2011**, *36*, 1020. [CrossRef] [PubMed]
48. Wei, W.; Xie, G.D.; Dang, A.H.; Guo, H. High-speed and bias-free optical random number generator. *IEEE Photonics Technol. Lett.* **2012**, *24*, 437. [CrossRef] [CrossRef]
49. Liu, Y.; Zhu, M.Y.; Luo, B.; Zhang, J.W.; Guo, H. Implementation of 1.6 Tb/s truly random number generation based on a super-luminescent emitting diode. *Laser Phys. Lett.* **2013**, *10*, 045001. [CrossRef] [CrossRef]
50. Martin, A.; Sanguinetti, B.; Lim, C.C.W.; Houlmann, R.; Zbinden, H. Quantum Random Number Generation for 1.25 GHz Quantum Key Distribution Systems. *IEEE J. Lightwave Technol.* **2015**, *33*, 2855. [CrossRef] [CrossRef]
51. Chen, Z.Y.; Li, Z.Y.; Xu, B.J.; Zhang, Y.C.; Guo, H. The m-least significant bits operation for quantum random number generation. *J. Phys. B* **2019**, *52*, 195501. [CrossRef]
52. Ma, X.F.; Xu, F.H.; Xu, H.; Tan, X.Q.; Qi, B.; Lo, H.K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **2013**, *87*, 062327. [CrossRef]
53. Lax, M. Classical Noise. V. Noise in Self-sustained Oscillators. *Phys. Rev.* **1967**, *160*, 290. [CrossRef]
54. Henry, C.H. Theory of the Linewidth of Semiconductor-Lasers. *IEEE J. Quantum Electron.* **1982**, *18*, 259. [CrossRef]
55. Zhang, X.X.; Zhang, Y.C.; Li, Z.Y.; Yu, S.; Guo, H. 1.2-GHz Balanced Homodyne Detector for Continuous-Variable Quantum Information Technology. *IEEE Photonics J.* **2018**, *10*, 6803810. [CrossRef]