Experimental study of a quantum random-number generator based on two independent lasers

Citation: Sun, Shi-Hai and Xu, Feihu. "Experimental study of a quantum random-number generator based on two independent lasers." Physical Review A 96, 6 (December 2017): 062314

As Published: http://dx.doi.org/10.1103/PhysRevA.96.062314

Publisher: American Physical Society

Persistent URL: http://hdl.handle.net/1721.1/112955

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Experimental study of a quantum random-number generator based on two independent lasers

Shi-Hai Sun[1,*] and Feihu Xu[2,3,†]

[1]*College of Science, National University of Defense Technology, Changsha 410073, People's Republic of China*

[2]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*

[3]*Hefei National Laboratory for Physical Sciences at Microscale, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China*

(Received 16 September 2017; published 14 December 2017)

A quantum random-number generator (QRNG) can produce true randomness by utilizing the inherent probabilistic nature of quantum mechanics. Recently, the spontaneous-emission quantum phase noise of the laser has been widely deployed for quantum random-number generation, due to its high rate, its low cost, and the feasibility of chip-scale integration. Here, we perform a comprehensive experimental study of a phase-noise-based QRNG with two independent lasers, each of which operates in either continuous-wave (CW) or pulsed mode. We implement the QRNG by operating the two lasers in three configurations, namely, CW + CW, CW + pulsed, and pulsed + pulsed, and demonstrate their trade-offs, strengths, and weaknesses.

DOI: 10.1103/PhysRevA.96.062314

I. INTRODUCTION

True randomness plays an important role in widespread applications, and it is generally believed to be impossible using only classical processes. A quantum random-number generator (QRNG), however, can generate true and unpredictable random numbers by exploiting the inherent randomness of quantum mechanics [1,2]. During the past decade, QRNGs have been implemented that are based on different types of quantum phenomena including single-photon detection [3–9], vacuum fluctuations [10–13], phase noise [14–21] of amplified spontaneous emission, and quantum nonlocality [22].

Among these implementations, the quantum (spontaneous-emission) phase noise of a laser has the advantages of a high rate and low cost, which has attracted a lot of scientific attention [14–21]. In previous QRNGs, an unbalanced interferometer was generally employed to measure the quantum phase noise. However, such an implementation has two practical drawbacks: first, it requires phase stability of the interferometer; and second, the large footprint of the interferometer makes it unsuitable for chip integration. Very recently, an important scheme which relies upon the interference between two independent lasers—a continuous-wave (CW) laser and a pulsed laser—has been proposed and demonstrated to solve these drawbacks [23–25], although the quantum randomness and the classical noise (e.g., detector's electrical noise) were not rigorously quantified. These recent works [23–25] demonstrate the large potential of practical QRNGs with independent lasers as the quantum entropy source. Besides QRNGs, the interference between two independent lasers is also valuable to the field of quantum cryptography [26,27].

In this paper, we present an extensive experimental study of a QRNG based on two independent lasers. We operate the two lasers in three configurations, i.e., CW + CW, CW + pulsed, and pulsed + pulsed, and analyze their strengths and weaknesses. By using off-the-shelf fiber-optical components, we demonstrate the maximum random-number generation rates under those operating configurations. Moreover, the conditional min-entropy is estimated given a uniform distribution of the practical quantum phase signal. And both the classical electrical noise and the intensity fluctuation noise of the two lasers are also taken into account. Thus, our work provides an important step towards a fast, low-cost, robust QRNG.

II. EXPERIMENTAL SETUP

The experimental setup is shown in Fig. 1. Two independent distributed-feedback lasers (LD1 and LD2), followed by two optical attenuators (Att), interfered at a 50:50 beam splitter (BS). The interference signal was detected by a photodetector (PD) of bandwidth 1 GHz (Newport 1611), whose output was sampled by a high-speed oscilloscope (Agilent DSO9104A). To interfere properly, LD1 and LD2 should be indistinguishable in the dimensions of spatial mode, polarization, spectrum, and arrival time. Because single-mode polarization maintaining fibers were used to connect all the optical devices (LDs, Att, BS), the spatial modes and polarizations of LD1 and LD2 were matched automatically. The spectra of the two lasers were controlled by two independent temperature controllers (TCs). The 3-dB widths of LD1 and LD2 spectra are both $\sim$17 pm. By carefully adjusting the temperature of LD1 and LD2 independently, the difference in the center wavelength between LD1 and LD2 was made to be much smaller than the lasers' 3-dB linewidths. In our experiment, the two lasers were operated in three cases: (I) CW + CW, (II) CW + pulsed, and (III) pulsed + pulsed. Note that the arrival-time mismatch between LD1 and LD2 affects the interference in case III only.

III. MODEL

By controlling the temperature of LD1 and LD2, the center wavelength of LD1 is brought close to that of LD2. After removing the dc background, the output from the photodetector can be written as

$$V(t) \propto E_1 E_2 \cos[\Delta\omega_0 t + \theta_1(t) - \theta_2(t)], \tag{1}$$

*shsun@nudt.edu.cn

†fhxu@mit.edu

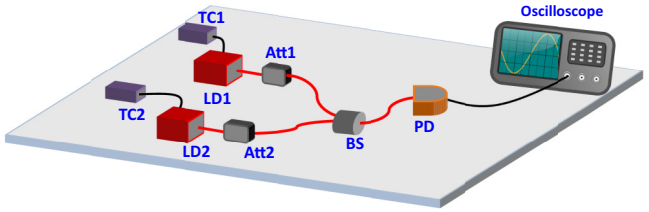

FIG. 1. Experimental setup for the QRNG. Two independent lasers (LD1 and LD2) interfere at a beam splitter (BS) whose output is detected by a photodetector (PD) followed by an oscilloscope. The output voltage of the photodetector is ac-coupled to the oscilloscope, whose sampling rate is determined by the configuration (see the text). Each analog sample is converted to 8 digital bits by an 8-bit analog-to-digital converter.

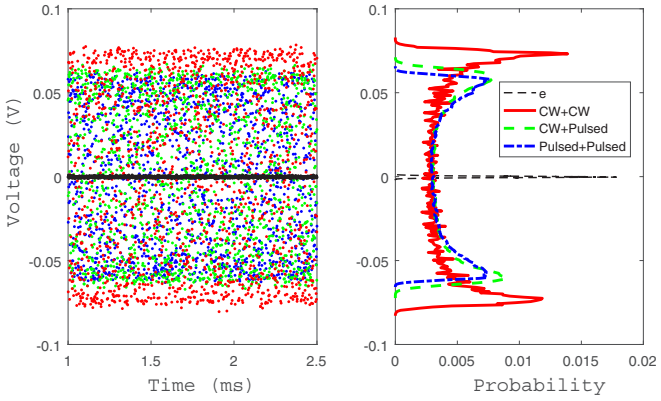

FIG. 2. Measured output voltage (left) and probability density function (right) for electrical (e) noise (dashed black curve) and total phase noise, CW + CW (solid red curve), CW + pulsed (dashed green curve), and pulsed + pulsed (dash-dotted blue curve). The classical noise includes the classical phase noise coming from the interferometer, the intensity fluctuation noise of the two lasers, and the classical electrical noise of the photodetector and oscilloscope. But as in the analysis in the Appendix, the classical phase noise of the interferometer is ignored here, and a detailed figure of the second and third classical noises is given in the Appendix (Fig. 4). In all measurements, the sampling rate of the oscilloscope is 20 GHz, and the recorded sample size is 10^8. The maximal amplitudes of phase noises are 82.9, 70.8, and 65.7 mV for CW + CW, CW + pulsed, and pulsed + pulsed, respectively.

where $\Delta\omega_0 = \omega_1^0 - \omega_2^0$ is the beating frequency, E_j and ω_j^0 ($j = 1,2$) are the amplitude and center frequency of the jth laser, and $\theta_1(t)$ and $\theta_2(t)$ are the phases of LD1 and LD2, which mainly originate from the quantum phase noise due to spontaneous emission photons [29].

This quantum phase noise constitutes our quantum signal. Besides the quantum signal, the output of the PD also contains classical noise, which includes the classical phase noise of the interferometer, the intensity fluctuation noise of the two lasers, and the electrical noise of the detection devices (PD and oscilloscope). Figure 2 and the Appendix report the measured classical noise. In quantum random-number generation, one has to quantify the amount of quantum signal and classical noise in order to extract the genuine quantum randomness in postprocessing [10,12,18,28]. We estimate the conditional min-entropy in all three cases (CW + CW, CW + pulse, and pulse + pulse) given the classical noise taken into account. These details are reported in the Appendix.

A. Case I: CW + CW

In case I, both LD1 and LD2 were operated in CW mode. By carefully controlling the temperature via TC1 and TC2, the difference in the center wavelength between LD1 and LD2 can be made smaller than the 3-dB linewidths of the two lasers. Then $\theta_j(t)$ ($j = 1,2$) can be treated as Gaussian white noise. The variance of $\Delta\theta(t)$ is given by [14,29]

$$\langle[\Delta\theta(t)]^2\rangle = 2T_s\left(\frac{1}{\tau_{c_1}} + \frac{1}{\tau_{c_2}}\right), \tag{2}$$

where T_s is the sampling period and τ_{c_j} is the coherence time of the jth laser.

Here, we remark that only the phase noise coming from spontaneous emission is considered quantum phase noise in Eq. (2). Strictly speaking, the classical phase noise, such as the classical phase noise of the interferometer (due to the mechanical vibration and thermal effect), the intensity fluctuation of light (due to fluctuation of the driving current of the laser and fluctuation of transmittance of the optical setups), and the classical electrical noise of the measured devices (including the photodetector and the oscilloscope), will contribute a small portion of the randomness output. In the Appendix, we show how to remove such classical phase noise.

According to Eq. (2), although the spontaneous emission phase follows Gaussian white noise, if $T_s \gg \tau_{c_j}$, the variance of the $\Delta\theta(t)$ is $\langle[\Delta\theta(t)]^2\rangle \gg 1$. Then the phase of the two adjacent sampling points is close to being independent. In other words, there is no obvious phase correlation between the two adjacent sampling points. Thus, the phase noise $\Delta\theta$ has a close-to-uniform distribution within $(-\pi,\pi]$. In our experiment, the 3-dB linewidths of LD1 and LD2 are 0.0177 and 0.0172 nm, respectively. Thus, the coherent time is 459.78 ps for LD1 and 473.14 ps for LD2. According to Eq. (2), the sampling period should satisfy that $T_s > \tau_{c_1}\tau_{c_2}/2(\tau_{c_1} + \tau_{c_2}) \approx 116.6$ ps. It seems that a sampling rate of about 8.6 GHz can be reached.

However, here we must note that, differently from the previous works that generate quantum random numbers with one CW laser [14], the sampling rate in the CW + CW case is limited not only by the coherent time of the two lasers, but also by the beating frequency of the two lasers. In fact, it is challenging to perfectly match the frequency of the two independent lasers in the CW + CW case, which means that $\Delta\omega_0 \neq 0$ (in the one-laser case, the frequencies of lights, which interfere at the BS, are perfectly matched). Thus, the measured output voltage signal, $V(t)$, is a sine wave with a phase jitter in our experiment. The center frequency of the sine wave comes from the beating frequency $\Delta\omega_0$, and the phase jitter comes from the random phase of the two lasers $\theta_1(t) - \theta_2(t)$. In our experiments, the center frequency of the measured output voltage, $V(t)$, is 278.7 MHz, with a standard deviation of 30.2 MHz [see Fig. 5(a) in the Appendix for details].

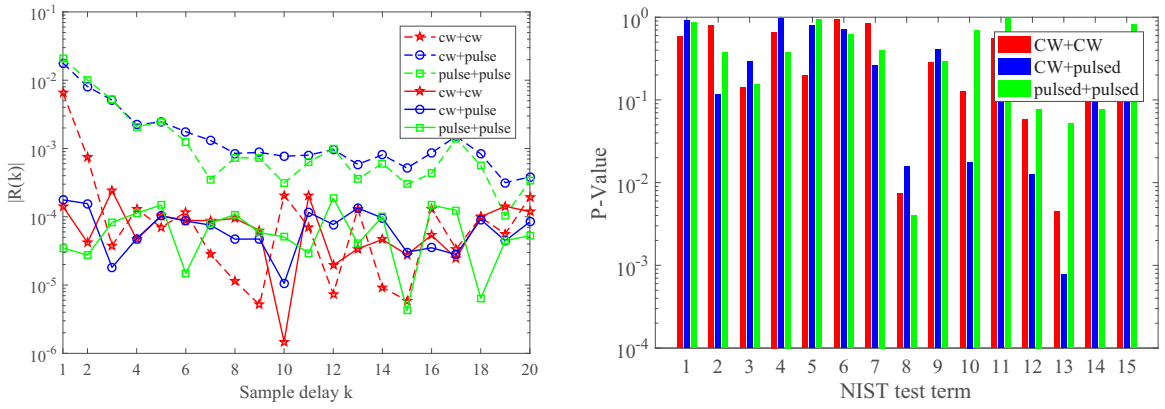

FIG. 3. (a) The Autocorrelation coefficient of raw data (dotted curves) and extracted data (solid curves) for case I (red stars), case II (blue circles), and case III (green squares). The autocorrelation coefficient is calculated with the length of data 10^8 and statistical significance $\alpha = 0.01$. And the calculated P values of the autocorrelation coefficients are given in Fig. 6 (Appendix); all of them are larger than $\alpha = 0.01$. In order to show the autocorrelation coefficient clearly, the absolute value $|R(k)|$ is plotted. The autocorrelation coefficient of extracted data is rather low (normally below 0.001), which means a high-quality random number is obtained after postprocessing. (b) NIST test results for 1 Gbit of extracted data in each case. Labels on the X axis represent the 15 NIST test terms. For each test term, the bar values from left to right represent the P values for the three cases [30]. The extracted data successfully pass all NIST tests in all three cases.

Obviously, the higher the sampling rate is, the higher the correlation between the adjacent sampling points is. Thus, in order to evaluate the sampling rate in the experiment, we calculate the autocorrelation coefficient of the output signal at various sampling frequencies, $f_s = 1/T_s$. The autocorrelation coefficient R of a sequence X is defined as

$$R(k) = \frac{E[(x_i - \mu)(x_{i+k} - \mu)]}{\sigma^2}, \tag{3}$$

where E is the expected value operator, k is the sample delay, and μ and σ are the mean and the standard deviation of X. In Fig. 5(b), we show the measured autocorrelation coefficient of the output signal with different f_s's. In the case where $k = 1$, the autocorrelation coefficients are 0.2319, -0.1497, and 0.008 for $f_s = 100$, 50, and 20 MHz.

Thus, in order to remove the classical correlation of as many sampling points as possible, we select the sampling frequency of 20 MHz in our experiment, i.e., $T_s = 50$ ns. Then the variance of $\Delta\theta(t)$ is $\langle[\Delta\theta(t)]^2\rangle \approx 428.85 \gg 1$, which means the sampling period is much longer than the coherent time of the lasers. Hence, we can treat $\Delta\theta$ as a uniform distribution within $(-\pi,\pi]$; i.e., the probability density function (PDF) of the quantum signal can be written as

$$f_Q(q) = \begin{cases} \frac{1}{\pi\sqrt{A^2-q^2}}, & -A < q < A, \\ 0 & \text{otherwise}, \end{cases} \tag{4}$$

where A is the maximum amplitude of the quantum signal. The solid red curve in Fig. 2 shows the PDF of the measured output voltage of the PD. It follows an arcsine distribution. The maximum (and minimum) output voltage of the PD is 89.2 mV (and -89.2 mV), which is much higher than the amplitude of the classical electrical noise and the intensity fluctuation noise of the lasers (both of them are lower than 2.5 mV; see Fig. 4 for details). For simplicity, we choose $A = 82.9$. Plugging the PDF [Eq. (4)] into the min-entropy model (see the Appendix), we estimate the quantum min-entropy as 4.47 bits per 8-bit sample.

To extract the quantum randomness, a randomness extractor is always required. In practice, two typical extractors, the Toeplitz-hashing extractor [31] and Trevisan's extractor [32], are often used. Both of them have been proven to be information theoretically secure and finite-size effects are taken into account. In this paper, as a proof-of-principle demonstration, only the Toeplitz-hashing extractor is used. And a more rigorous discussion of the randomness extractor can be found in Refs. [1] and [2].

The Toeplitz-hashing randomness extractor extracts random bit string m by multiplying the raw sequence n with the Toeplitz matrix. In our experiment, we set the size of the Toeplitz matrix at $n = 4096$ and $m = 2048$ for simplicity of software implementation, i.e., 4 bits are produced for each sample (8-bit ADC). Finally, the QRNG rate is $20 \times 4 = 80$ Mbp. After extraction, we tested the autocorrelation coefficient [Fig. 3(a)] and ran the National Institute of Standards and Technology (NIST) statistic test suite, with successful passes on all tests [Fig. 3(b)].

B. Case II: CW + pulsed

In the second case, LD1 operates in CW mode, while LD2 operates in pulsed mode. This scheme has been recently demonstrated in [23] and [24]. In our experiment, LD2's repetition rate is 500 MHz, and its 3-dB width is 433.2 ps, with a standard deviation of 27.0 ps. Since the phase of each pulse comes from fresh spontaneous emission photons, $\Delta\theta(t)$ follows a uniform distribution within $(-\pi,\pi]$. This means that the PDF of the quantum signal is the same as Eq. (4).

In our experiment, the interference signal is detected by a PD with bandwidth 1 GHz, followed by an oscilloscope at sampling rate 10 GHz. The dashed green curve in Fig. 2 shows the PDF of the measured output voltage. The maximum (and minimum) output voltage of the PD is 79.2 mV (and

−62.4 mV). Thus, we set the offset of the 8-bit ADC at 8.4 mV, which means that the output number of the ADC is 0 for input voltage −62.4 mV and 255 for input voltage 79.2 mV. In other words, parameter $A = 70.8$ mV in Eq. (4). Note that although the amplitude of the phase noise could be further increased by increasing the power of the CW laser, this would result in almost no change in the conditional quantum min-entropy. Using the same method as in case I, we get the min-entropy of quantum randomness as 4.45 bits, and the final QRNG rate is thus $500 \times 4 = 2$ Gbp. The autocorrelation coefficient and the NIST test results are shown in Figs. 3(a) and 3(b).

C. Case III: Pulsed + pulsed

In this case, both LD1 and LD2 operate in pulsed mode at a repetition rate of 500 MHz. The trigger of the two lasers is generated by an arbitrary waveform generator (Tektronix AWG7092C). To guarantee that the two pulses from the two lasers can properly interfere at the BS, the arrival times of the two pulses should be indistinguishable. This was achieved by delaying the triggers for LD1 and LD2 with a 1-ps time resolution. In the experiment, the 3-dB temporal widths of the pulses from LD1 and LD2 are 530.9 ps with standard deviation 19.1 ps and 563.0 ps with standard deviation 18.9 ps, respectively. By fine-tuning the trigger delay, we can control the overlap of the two pulses at a resolution that is much lower than the temporal width of the pulses.

Since the phase of each pulse comes from different spontaneous emission photons, the phase follows a uniform distribution. The output voltage also follows an arcsine distribution (see dashed-dotted blue curve in Fig. 2). The measured maximum (and minimum) voltage is 111.6 mV (and −19.8 mV). Then by setting the offset of the ADC at 45.9 mV, we get parameter $A = 65.7$ in Eq. (4). Using the same method as in case I, the estimated min-entropy is 4.43 bits, and the final random-number generation rate is $500 \times 4 = 2$ Gbp after postprocessing. The autocorrelation coefficient and NIST test results are shown in Figs. 3(a) and 3(b).

IV. DISCUSSION

We discuss the trade-offs of the three cases for the practical QRNG with independent lasers. First, among the three cases, case I—CW + CW—is the easiest to implement, because it does not require any high-speed electronics to modulate optical pulses. And yet it is difficult to match the frequencies of LD1 and LD2, so the beating frequency limits the maximum QRNG rate. In our experiment, the generation rate is limited to tens of Mbp. Second, case II and case III achieve the same generation rate, 2 Gbp. This is because the generation rate primarily depends on the repetition rate of the pulsed laser and the precision of the ADC. Generally speaking, the repetition rate of the pulsed laser can be increased to a few GHz and a generation rate of tens of Gbp is achievable for both case II and case III with current technology. This rate is much higher than that in case I. Third, case III requires precise matching of the pulse arrival times for LD1 and LD2. This might be a practical challenge for ultrahigh-speed implementations when the repetition rate of the pulsed laser reaches tens of GHz. Therefore, we conclude that case II, CW + pulse, may be the best choice for high-speed implementation of a QRNG based on quantum phase noise (as demonstrated recently in [23] and [24]), while case I is suitable for simple and low-cost applications that may require slow-rate quantum random-number generation only. Note that high-speed implementation of case I is still possible by changing the scheme to a broadband source and homodyne detection [25].

Overall, we have experimentally demonstrated a QRNG based on two independent lasers. We operated the two lasers in three cases (CW + CW, CW + pulsed and pulsed + pulsed), experimentally studied the properties and trade-offs of the QRNG in each case, and generated truly random numbers at rates of 80 Mbp, 2 Gbp, and 2 Gbp, respectively. Our work demonstrates the great potential of quantum phase-noise-based QRNGs using two independent lasers.

ACKNOWLEDGMENTS

The authors thank De-Feng Gu, Connor Henley, and Bing Qi for helpful discussions. This work was supported by National Natural Science Foundation of China Grants No. 11674397 and No. 61771443 and the Canadian NSERC PDF.

APPENDIX: ESTIMATION OF THE MIN-ENTROPY

Taking the classical noise into account, the measured total signal M is $M = Q + N$. Here Q is the quantum signal with probability density function $f_Q(q)$, and N is the classical noise signal with PDF $f_N(n)$. Then the PDF of M is the convolution of $f_Q(q)$ and $f_N(n)$, which is given by

$$f_M(m) = \int_{-\infty}^{\infty} f_Q(m-n) f_N(n) dn. \tag{A1}$$

To evaluate the min-entropy of genuine quantum randomness, we need to estimate the conditional PDF of M given the classical noise N [33]. Using the same method as in Ref. [12], we can get the conditional cumulative distribution function, $F_{M|N}(m|n)$, which can be written as

$$\begin{aligned} F_{M|N}(m|n) &= P\{M \leqslant m | N = n\} = \frac{P\{M \leqslant m, N = n\}}{P\{N = n\}} \\ &= \frac{P\{q \leqslant m - n, N = n\}}{P\{N = e\}} \\ &= \frac{P\{Q \leqslant m - n\} \cdot P\{N = n\}}{P\{N = e\}} \\ &= P\{q \leqslant m - n\} \\ &= F_Q(m - n), \end{aligned} \tag{A2}$$

where $F_Q(q)$ is the cumulative distribution function of the quantum signal Q. Hence it is easy to get the conditional PDF, which is

$$f_{M|N}(m|n) = f_Q(m - n), \tag{A3}$$

where $f_Q(m - n)$ denotes the PDF of the quantum signal Q.

By sampling the output voltage of the photodetector with a k-bit ADC, the discretized conditional probability of the

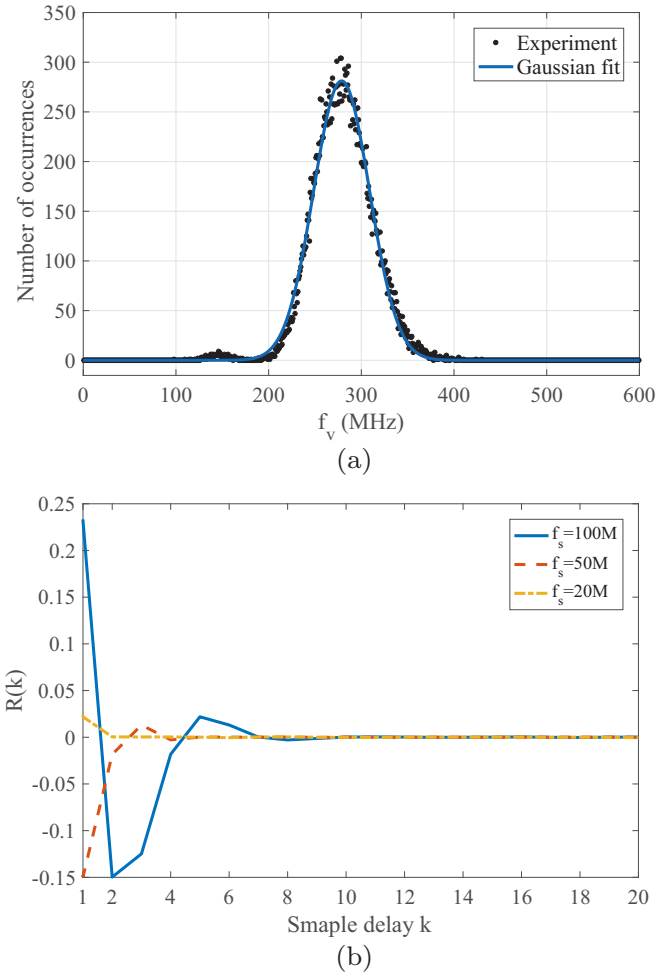

FIG. 4. Measurement results for the CW + CW case. (a) Beating signal's frequency. The sampling rate is 10 GHz in this measurement. The solid line is the Gaussian fitting curve for the experimental data. The beating signal has mean 278.7 MHz and standard deviation 30.2 MHz. (b) Autocorrelation coefficient of the PD's output at sampling frequencies of 100 MHz (solid blue curve), 50 MHz (dashed red curve), and 20 MHz (dash-dotted yellow curve).

measured signal given the classical noise can be written as

$$P_{M_{\mathrm{dis}}|N}(m_i|n) = \int_{V_l+i\delta}^{V_l+(i+1)\delta} f_{M|N}(m|n)dm, \qquad \text{(A4)}$$

where $\delta = (V_u - V_l)/2^k$ and k is the precision of the ADC. V_l and V_u are the lower and upper bounds of the sample range $[V_l, V_u]$. $i = 0, 1, \ldots, 2^k - 1$ is the output digital number of the ADC. Therefore, the worst-case min-entropy conditioned on the classical noise E is given by [12]

$$H_{\min}(M_{\mathrm{dis}|N}) = -\log_2[\max_{n\in[n_{\min},n_{\max}]} \max_{m_i\in M_{\mathrm{dis}}} P_{M_{\mathrm{dis}}|N}(m_i|n)]. \qquad \text{(A5)}$$

Here *worst case* means that, from the adversary's perspective, the classical noise is fully known and controlled by him or her with arbitrary precision. Therefore, if we know the bounds of the classical noise, $n_{\min}$ and $n_{\max}$, we can estimate the min-entropy with Eq. (A5) and then distill the true quantum random number by performing postprocessing.

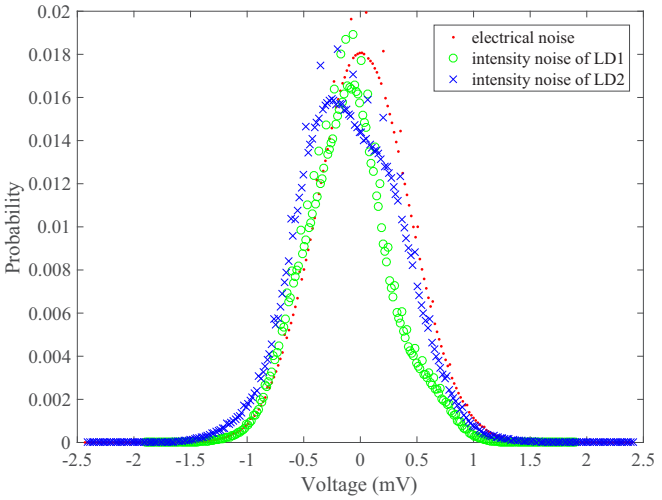

FIG. 5. Observed probability density function (PDF) of the classical noise: electrical noise (red dots), intensity noise of LD1 (green circles), and intensity noise of LD2 (blue x's). The experimental setups are the same as those in the text. But we turn off the two lasers for measurement of the electrical noise and one of the lasers for measurement of the intensity noise of LD1 and LD2. The sampling rate of the oscilloscope is 20 GHz, and the recorded sample size is 10^8.

In order to get the bounds of the classical noise, we should analyze the types of classical noise. In fact, there are three main types of classical noise: classical phase noise of the interferometer, intensity fluctuation of the light (both LD1 and LD2), and classical electrical noise of the measurement devices (photodetector and oscilloscope).

An interferometer is required to measure the phase of the light, but the mechanical vibration and thermal effect will

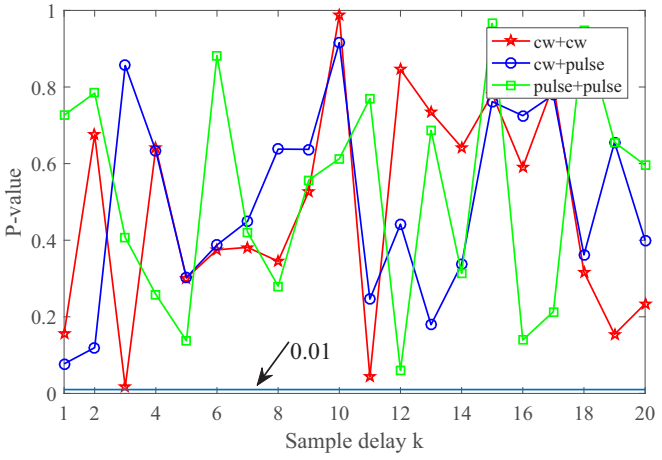

FIG. 6. P value for the autocorrelation coefficient of the extracted bit string. In the calculation, the length of the data is 10^8, and the statistical significance is set at $\alpha = 0.01$. All of them are larger than the statistical significance, which means that there is insufficient evidence to conclude that there is a significant relationship between the bit string $X = [x_i]$ and $X' = [x_{i+k}]$.

affect the stability of the interferometer and introduce classical phase noise. But, in our experiment, such classical phase noise is ignored. This is because the quantum random number is determined by the relative phase of the adjacent sampling point. Thus, we could remove the mechanical vibration and the thermal effect by isolating the interferometer from the environment, as generally done in the phase-encoding QKD system. Using such methods, the time period is about 3 min when the phase of the interferometer changes from 0 to π. Thus, the difference in phase between adjacent sampling points is about $\Delta\theta_c \approx \pi T_s/180$ s. Here T_s is the sampling time. It is easy to get that $\Delta\theta_c$ is much smaller than the random phase coming from spontaneous emission. For example, in our experiment, $\Delta\theta_c \approx \pi 50$ ns/180 s $\approx 2\pi 10^{-10}$ in the CW + CW case with sampling rate 20 MHz, and $\Delta\theta_c \approx \pi 2$ ns/180 s $\approx \pi 10^{-11}$ in the CW + pulse and pulse + pulse cases with repetition 500 MHz. Of course, when the length of the generated bit string is very long, such as larger than 1 Tbit, the classical phase noise of the interferometer will introduce a classical correlation between the first bits and the end bits. Then such classical phase noise must be taken into account in the estimation of the min-entropy. However, in our proof-of-principle experiment, this effect is not considered. In other words, the classical phase noise introduced by the interferometer is ignored in our analysis.

The intensity fluctuation of the light will also affect the randomness of the generated bit string. The intensity fluctuation comes from both the fluctuation of the driven current of the laser and the fluctuation of the optical setups (such as fiber and beam splitter). Furthermore, the classical electrical noise of the measurement devices (photodetector and oscilloscope) will also affect the measured voltage and the output of the analog-to-digital converter. Thus, in this paper, we only consider the two main types of classical noise, since they can be directly measured in experiments. Figure 4 shows the PDF of the measured classical electrical noise and intensity noise of lasers in our experiment. It clearly shows that the classical noises are much lower than the amplitude of the quantum signal.

With the experimental data in Fig. 4, we could directly get the bounds of the classical noise. In fact, with 99.9999% confidence, the bounds are $-2.29\ \text{mV} \leqslant n_e \leqslant 2.29\ \text{mV}$, $-1.88\ \text{mV} \leqslant n_{\text{LD1}} \leqslant 1.88\ \text{mV}$, and $-2.07\ \text{mV} \leqslant n_{\text{LD2}} \leqslant 2.04\ \text{mV}$ for the electrical noise (n_e), intensity noise of LD1 (n_{LD1}), and intensity noise of LD2 (n_{LD2}), respectively. Thus, if we assume that the three types of noise (electrical noise, intensity noise) are independent, the bounds of the total classical noise can be obtained: $n_{\min} = -6.24$ mV and $n_{\max} = 6.21$ mV.

According to the analysis given above, if we know the PDF of the quantum signal, we can estimate the min-entropy of genuine quantum randomness. In the text, based on our experimental results, we adopt this model to calculate the min-entropy of genuine quantum randomness for three QRNG cases: CW + CW, CW + pulse, and pulse + pulse.

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quant. Info. **2**, 16021 (2016).

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[3] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, Quantum random-number generation and key sharing, J. Mod. Opt. **41**, 2435 (1994).

[4] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, Rev. Sci. Instrum. **71**, 1675 (2000).

[5] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, A high speed, postprocessing free, quantum random number generator, Appl. Phys. Lett. **93**, 031109 (2008).

[6] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, Photon arrival time quantum random number generation, J. Mod. Opt. **56**, 516 (2009).

[7] M. Fürst, H. Weier, S. Nauerth, D. Marangon, C. Kurtsiefer, and H. Weinfurter, High speed optical quantum random number generation, Opt. Express **18**, 13029 (2010).

[8] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Ggenerator, Phys. Rev. Lett. **114**, 150501 (2015).

[9] F. Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, Optica **3**, 1266 (2016).

[10] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, A generator for unique quantum random numbers based on vacuum states, Nat. Photonics **4**, 711 (2010).

[11] Y. Shen, L. Tian, and H. Zou, Practical quantum random number generator based on measuring the shot noise of vacuum states, Phys. Rev. A **81**, 063814 (2010).

[12] J. Yaw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Maximization of Extractable Randomness in a Quantum Random-Number Generator, Phys. Rev. Appl. **3**, 054004 (2015).

[13] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, Phys. Rev. Lett. **118**, 060503 (2017).

[14] 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).

[15] 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).

[16] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Opt. Express **19**, 20665 (2011).

[17] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Ultrafast quantum random number generation based on quantum phase fluctuations, Opt. Express **20**, 12366 (2012).

[18] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction, Phys. Rev. A **87**, 062327 (2013).

[19] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Frohlich, A. Plews, and A. J. Shields, Robust random number generation using steady-state emission of gain-switched laser diodes, Appl. Phys. Lett. **104**, 261112 (2014).

[20] Y. Q. Nie, L. L. Huang, Y. Liu, F. Payne, J. Zhang, and J. W. Pan, The generation of 68 gbps quantum random number by measuring laser phase fluctuations, Rev. Sci. Instrum. **86**, 063105 (2015).

[21] C. Abellan, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Generation of Fresh and Pure Random Numbers for Loophole-Free Bell Tests, Phys. Rev. Lett. **115**, 250403 (2015).

[22] S. Pironio, A. Acin, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature **464**, 1021 (2010).

[23] C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Quantum entropy source on an InP photonic integrated circuit for random number generation, Optica **3**, 989 (2016).

[24] Q. Zhou, R. Valivarthi, C. John, and W. Tittel, Practical quantum random number generator based on sampling vacuum fluctuations, arXiv:1703.00559 [quant-ph].

[25] B. Qi, Genuine randomness from an incoherent source, Rev. Sci. Instrum. **88**, 113101 (2017).

[26] M. Curty, X. Ma, B. Qi, and T. Moroder, Passive decoy-state quantum key distribution with practical light sources, Phys. Rev. A **81**, 022310 (2010).

[27] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[28] M. W. Mitchell, C. Abellan, and W. Amaya, Strong experimental guarantees in ultrafast quantum random number generation, Phys. Rev. A **91**, 012314 (2015).

[29] A. Yariv and P. Yeh, Photonics: *Optical Electronics in Modern Communications*, 6th ed. (Oxford University Press, New York, 2007).

[30] In NIST tests, 1000 trails, each with a 1-Mbit sample, are tested. Using the significance level $\alpha = 0.01$, the P value should be larger than 0.0001, and the proportion should be larger than 98.06%. If multiple probability of passing and P values are generated in the tests, the worst cases are given. The X-axis labels 1 to 15 are test terms: Frequency, BlockFrequency, CumultiveSums, Runs, LongestRun, Rank, FFT, NonOverlappingTemplate, OverlappingTemplate, Universal, ApproximateEntropy, RandomExcurisions, RandomExcursionsVariant, Serial, and Linear Complexity.

[31] M. N. Wegman and J. L. Carter, New hash function and their use in authentication and set equality, J. Comput. Syst. Sci. **22**, 265 (1981).

[32] L. Trevisan, Extractors and pseudorandom generators, J. ACM **48**, 860 (2001).

[33] D. Frauchiger, R. Renner, and M. Troyer, True randomness from realistic quantum devices, arXiv:1311.4547.