Randomness generation based on spontaneous emissions of lasers

Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma
Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China
(Received 21 April 2015; published 11 June 2015)

Random numbers play a key role in information science, especially in cryptography. Based on the probabilistic nature of quantum mechanics, quantum random number generators can produce genuine randomness. In particular, random numbers can be produced from laser phase fluctuations with a very high speed, typically in the Gbps regime. In this work, by developing a physical model, we investigate the origin of the randomness in quantum random number generators based on laser phase fluctuations. We show how the randomness essentially stems from spontaneous emissions. The laser phase fluctuation can be quantitatively evaluated from basic principles and qualitatively explained by the Brownian motion model. After taking account of practical device precision, we show that the randomness generation speed is limited by the finite resolution of detection devices. Our result also provides the optimal experiment design in order to achieve the maximum generation speed.

DOI: 10.1103/PhysRevA.91.062316 PACS number(s): 03.67.Dd, 05.40.−a

I. INTRODUCTION

Random numbers have vast applications in a variety of tasks, such as secure communication, numerical simulation, and lotteries. With the development of quantum information science, random numbers are also indispensable in many quantum information tasks. For example, in quantum key distribution (QKD) [1], random numbers are employed for the preparation of quantum states and the choice of measurement bases in order to guarantee its information-theoretical security.

Generally, there are two categories of physical random number generators (RNGs). One type is based on classical physics, whose randomness originates from the incomplete knowledge of the RNG system. For instance, classical RNGs can be based on chaotic behaviors of complicated systems such as semiconductor lasers [2]. Since a full characterization of the randomness generation process may enable an adversary to predict the outcomes, this type of RNG cannot generate provable randomness. The other type with a mechanism of measuring a quantum state is called quantum random number generators (QRNGs). According to the basic principles of quantum mechanics, true random numbers can be generated, which means that the outcomes can never be predicted before the measurement.

QRNGs have developed significantly in the past decade. The simplest QRNG is shown in Fig. 1, which is designed by performing single-photon detections. Here a single-photon $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, which is a superposition of polarization $|H\rangle$ and $|V\rangle$, passes through a balanced polarization beam splitter, and then it is detected by single-photon detectors D_1 and D_2. The event of whether the detector D_1 (D_2) clicks or not for each photon is the desired output random number. Till now, many QRNGs are of this type, but their generation speed is limited by the dead time of the detectors [3,4]. Subsequently, some other types of QRNGs have been proposed. One of them is based on quantum nonlocality, where randomness can be generated with very high security that does not even rely on the implementation [5]. The price to pay for such high security is that the generation speed is so low that the random numbers cannot satisfy most practical necessities. Another type measures the photon arrival time from a CW laser and obtains random numbers from the timing measurement of single-photon detection relative to an external time reference [6–8]. Restricted by the count rate of the detectors and time resolution of the time-to-digital converters, the generation speed cannot be very high. Recently a new type of QRNGs measuring phase fluctuations from lasers [9–13] outperforms most of the existing ones in generation speed. Phase fluctuations are mainly caused by spontaneous emission of excited atoms of the gain medium in a laser. As a direct effect of vacuum state fluctuations, spontaneous emission is an excellent resource for extracting true randomness. In experiments, such a QRNG based on vacuum fluctuation is realized with a very high generation speed, up to 1 Gbps [10,12]. It is also shown that the generation speed has the potential to be extended to 10 Gbps and even 100 Gbps [10].

Such a high speed of the QRNG based on phase fluctuations leads to a natural question of whether there is a limit of the generation speed. To answer this question, in our work, we investigate the randomness generation mechanism by following a derivation from first principles and use the Brownian motion model to support it, which is a starting point to explore the limit of generation speed. We also build a simple model to express the generation speed as a function of some device parameters. We show that the generation speed is finitely limited when considering the precision or resolution of practical experiment instruments and give the optimal experiment design in order to achieve the maximum generation speed.

The rest of this paper is organized as follows. In Sec. II we review the QRNG scheme and its underlying intuitive physical model. In Sec. III we quantitatively derive the randomness output from first principles, which is also qualitatively explained by comparing the similarity with the Brownian motion model. In Sec. IV we show that the generation speed is finitely limited and give the optimal experiment design. Then we explain our result with device imperfection. We discuss another way of quantifying randomness and conclude in Sec. V.

II. QRNG BASED ON VACUUM FLUCTUATIONS

In this section, we review a typical QRNG scheme based on measuring the vacuum fluctuations of a laser [12]. As shown

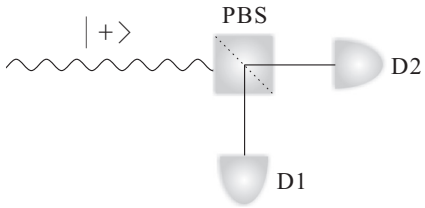

FIG. 1. The simplest QRNG devices: a balanced polarization beam splitter and two single-photon detectors D_1 and D_2.

in Fig. 2, a laser beam passes through a planar light wave circuit Mach-Zehnder interferometer (PLC-MZI). Due to the spontaneous emission, there will be a phase fluctuation in the laser field compared to a plane wave function. The phase fluctuation is transformed into intensity fluctuation by the interferometer and then detected by the photodetector (PD). The output voltage from the PD will be sampled and digitized by an 8-bit analog-to-digital convertor (ADC), which will produce true random numbers.

To get the expression of the output randomness, let us first suppose that the lasing field can be expressed by

$$E(t) = \sqrt{S}\exp\{i[\phi_0(t) + \phi'(t)]\}, \tag{1}$$

where $\phi_0(t)$ represents the phase of a plane wave, $\phi'(t)$ represents the phase fluctuations due to spontaneous emission as well as some other factors, and S represents the photon number intensity of E. Suppose the time delay between the two arms of the PLC-MZI is τ_l, then the measurement output voltage $V(t)$, which is proportional to the interference probability, can be expressed by

$$V(t) \propto 2E^*(t)E(t+\tau_l)\sin[\Delta\phi(t)] \propto P\Delta\phi'(t), \tag{2}$$

where P is the laser output power and $\Delta\phi'(t) = \phi'(t) - \phi'(t+\tau_l)$ is the total phase fluctuations.

The variance of the phase fluctuations is modeled by

$$\langle\Delta\phi'(t)^2\rangle = \frac{Q}{P} + C, \tag{3}$$

where Q/P and C stand for the contributions from spontaneous emission and classical mechanisms, respectively. In experiments, in order to detect such a variance, we transform it into the variance of the output voltage by multiplying Eq. (3)

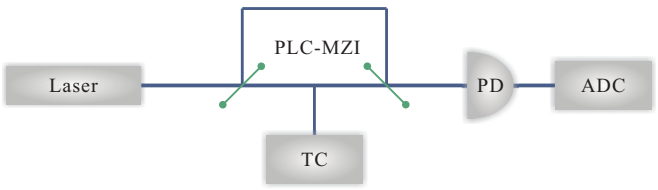

FIG. 2. (Color online) The experiment setup of the QRNG based on phase fluctuation. (1) A 1.55 μm single-mode cw distributed feedback (DFB) diode laser (ILX light wave); (2) a compact planar light wave circuit Mach-Zehnder interferometer (PLC-MZI) with a 500 ps delay difference; (3) a temperature controller used to stabilize the delay difference of PLC-MZI; (4) a 5 GHZ InGaAs photodetector; (5) an 8-bit analog-to-digital converter (ADC).

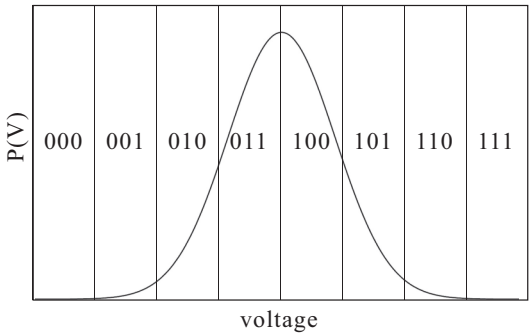

FIG. 3. Probability distribution of the output voltage. The x axis stands for the output voltage, and the y axis stands for the probability density of the voltage. The value range of the output voltage will be divided to eight intervals. If the voltage is measured to be in some interval, a 3-bit sequence of random numbers will be generated accordingly. However, due to the classical noises, we use $\langle V_Q^2\rangle$ instead of $\langle V^2\rangle$ to calculate the maximum probability.

by P^2,

$$\langle V^2\rangle = AQP + ACP^2 + F, \tag{4}$$

where A is a constant coefficient and F is the background noise. The value of AQ, AC, and F can be obtained by fitting experiment data of P and $\langle V^2\rangle$ according to Eq. (4). Then the laser power P is chosen to maximize the quantum signal to classical noise ratio γ:

$$\gamma = \frac{AQP}{ACP^2 + F}. \tag{5}$$

The process to obtain random numbers is shown in Fig. 3, where we use a 3-bit ADC instead of an 8-bit one for simplicity. The output voltage is measured and discretized by dividing its value range into eight intervals. Each voltage interval corresponds to a 3-bit random number sequence. An 8-bit ADC works similarly in practice.

Finally, the method to quantify the random number generation speed is as follows. First it is necessary to quantify the output randomness per sample with the min-entropy function,

$$H_\infty(X) = -\log_2(\max_{x\in\{0,1\}^n}\Pr[X = x]), \tag{6}$$

where X stands for the n random numbers obtained. When assuming that the voltage follows a Gaussian distribution, as the true randomness comes only from the quantum contribution AQP in Eq. (4), the maximum probability $\Pr[X = x]$ can be calculated from the quantum variance $\langle V_Q^2\rangle$:

$$\langle V_Q^2\rangle = \frac{\gamma}{\gamma+1}\langle V^2\rangle. \tag{7}$$

The maximum probability $\Pr[X = x]$ equals the area of the biggest part under the Gaussian function curve $G(0, \sqrt{\langle V_Q^2\rangle})$. Then we can calculate the output randomness per sample R_0, and the generation speed is the product of R_0 and the sampling rate.

Therefore we can obtain the final randomness generation rate by making the following assumptions:

(1) The phase difference $\langle\Delta\phi'(t)^2\rangle$ is assumed to satisfy Eq. (3).

(2) The outputs of quantum signal follow a Gaussian distribution.

(3) The random numbers generated from different samples are mutually independent.

In our work, we start from first principles to theoretically derive these assumptions. In the original experiment [12], the final QRNG speed is given by a product of the sampling frequency and the randomness output in each sample. It seems that the generation speed can infinitely increase with infinite sampling speed. However, we show a contrary result. For given experiment setups, the generation speed is finite and maximized with a finite sampling speed.

III. IMPROVEMENT OF PREVIOUS QRNG PHYSICAL MODEL

In this section, we will start with randomness origin in laser source and then derive assumptions 1 and 2 with basic physical models from first principles. In assumption 1, the quantum contribution of phase fluctuations Q in Eq. (3) is a constant for given experimental parameters. Our result gives an accurate expression of Q and shows a linear relationship between Q and τ_l. For assumption 2, we prove that the output voltage V follows a Gaussian distribution indeed. Moreover, we will use a Brownian motion model to describe the behavior of the random phase and explain our result from an intuitive perspective.

A. Randomness origin in laser source

Let us first introduce the basics of lasers and the origin of the randomness from a laser source. The structure of a laser source mainly consists of an optical resonator and gain medium. The gain medium can be regarded as ensembles of charged particles with two-level energy levels denoted by a ground state $|g\rangle$ and an excited state $|e\rangle$. When a laser source is below the threshold, the population of the particles follow a Boltzmann distribution. If a population inversion is achieved due to some external factors, the laser source is above the threshold and begins to generate the laser. Considering the interaction between atomic electrons and an electromagnetic field, a population inversion will lead to two kinds of photon emissions: stimulated emission and spontaneous emission. The former is of perfect monochromaticity with energy given by

$$h\nu = E_e - E_g, \tag{8}$$

where E_e and E_g are the energies of the excited and ground level, respectively. The latter is the origin of randomness.

The output state of spontaneous emission can be given by

$$|\Psi(t)\rangle = a(t)e^{-i\omega_0 t}|e;0\rangle + \sum_{k,s} b_{ks}(t)e^{-i\omega_k t}|g;1\rangle, \tag{9}$$

according to the Weisskopf-Wigner theory [14]. Here $|0\rangle$ and $|1\rangle$ denote the vacuum and single photon state, respectively, $a(t)$ and $b_{ks}(t)$ are probability amplitudes, k stands for the wave vector, $\omega_k = ck$ is the frequency of the photon, and s refers to the spin of the charged particle.

According to the probabilistic nature of quantum mechanics, a measurement on $|\Psi(t)\rangle$ will lead to a random projection to one of the eigenstates and the corresponding eigenvalue ω_k. The measurement results, photon frequency ω_k, obtained from sequential measurements are mutually independent, and their autocorrelation should be zero. Since ω_k corresponds to the quantum phase fluctuation rate of the laser field $F_{\rm sp}(t)$, we can treat $F_{\rm sp}(t)$ as a white noise.

B. Variance of the quantum phase fluctuations

Now we derive the variance expression in Eq. (3) from first principles. Since the classical phase noise is laser-power independent [15], the quantity C in Eq. (3) can be treated as a constant. As mentioned in Sec. II, it can be calculated by fitting experiment data. Hence, we focus on deriving the quantum part of Eq. (3).

To derive the dynamic evolution of the laser field, let us consider the laser field changes during an infinitesimal time interval δt. Taking account of the stimulated and spontaneous emission, the laser field change can be given by

$$E(t+\delta t) - E(t) = [f(E(t)) + E_{\rm sp}(t)]\delta t, \tag{10}$$

where $E_{\rm sp}(t)$ corresponds to the laser field from spontaneous emission and $f(E(t))$ corresponds to the contributions of stimulated emission and any other factors that may affect the laser field. Thus, the dynamic evolution of the laser field can be given by [16]

$$\frac{dE(t)}{dt} = f(E(t)) + E_{\rm sp}(t). \tag{11}$$

For the laser field E expressed in Eq. (1), the total phase $\phi(t)$ can be rewritten in detail as

$$\phi(t) = \phi_0(t) + \phi_1(t) + \phi_{\rm sp}(t), \tag{12}$$

where $\phi_1(t)$ and $\phi_{\rm sp}(t)$ represent the classical and quantum phase noise, respectively. The total phase dynamically evolves according to

$$\begin{aligned}\frac{d\phi(t)}{dt} &= \frac{1}{S(t)}\mathrm{Im}\left[E^*(t)\frac{dE(t)}{dt}\right] \\ &= \frac{\mathrm{Im}[E^*(t)f(E(t))]}{S(t)} + \frac{\mathrm{Im}[E^*(t)E_{\rm sp}(t)]}{S(t)} \\ &= \frac{\mathrm{Im}[e^{-i\phi(t)}f(E(t))]}{\sqrt{S(t)}} + \frac{\mathrm{Im}[e^{-i\phi(t)}E_{\rm sp}(t)]}{\sqrt{S(t)}}.\end{aligned} \tag{13}$$

The evolution of the phase $\phi_{\rm sp}(t)$ is thus given by

$$\frac{d\phi_{\rm sp}(t)}{dt} = \frac{\mathrm{Im}[e^{-i\phi(t)}E_{\rm sp}(t)]}{\sqrt{S(t)}} = F_{\rm sp}(t). \tag{14}$$

Due to the Weisskopf-Wigner theory, as discussed in Sec. III A, we can regard $F_{\rm sp}(t)$ as a white noise. In fact, they are identically independent distributed (i.i.d.) for different time t.

In the experiment setup in the last section, the time delay between the two arms in the PLC-MZI is τ_l. Then the phase difference $\Delta\phi_{\rm sp}$ induced by quantum spontaneous emission is

$$\Delta\phi_{\rm sp} = \phi_{\rm sp}(t_0+\tau_l) - \phi_{\rm sp}(t_0) = \int_{t_0}^{t_0+\tau_l} F_{\rm sp}(t)\,dt. \tag{15}$$

The variance of the quantum phase fluctuation can be written as

$$\begin{aligned}\langle \Delta\phi_{\rm sp}^2 \rangle &= \left\langle \left[\int_{t_0}^{t_0+\tau_l} F_{\rm sp}(t)\, dt \right]^2 \right\rangle \\ &= \left\langle \left[\int_{t_0}^{t_0+\tau_l} F_{\rm sp}(t)\, dt \right] \left[\int_{t_0}^{t_0+\tau_l} F_{\rm sp}(t')\, dt' \right] \right\rangle \\ &= \int_{t_0}^{t_0+\tau_l} \langle F_{\rm sp}(t) F_{\rm sp}(t') \rangle dt\, dt' \\ &= \frac{R_{\rm sp}}{2\langle S \rangle} \int_{t_0}^{t_0+\tau_l} \delta(t-t')\, dt\, dt' \\ &= \frac{R_{\rm sp}\tau_l}{2\langle S \rangle}. \end{aligned} \tag{16}$$

Here we make use of the autocorrelation of $F_{\rm sp}(t)$,

$$\langle F_{\rm sp}(t) F_{\rm sp}^*(t-\tau_l) \rangle = \frac{R_{\rm sp}\delta(\tau_l)}{2\langle S \rangle}, \tag{17}$$

which is derived from the aforementioned white noise assumption with an autocorrelation function:

$$\langle E_{\rm sp}(t) E_{\rm sp}^*(t-\tau_l) \rangle = R_{\rm sp}\delta(\tau_l). \tag{18}$$

where $R_{\rm sp}$ is a constant factor which can be physically interpreted as the spontaneous emission rate. We refer to Ref. [16] for details of derivation of Eq. (17).

So we can draw a conclusion with the deduction above that the variance of the quantum phase fluctuations $\langle \Delta\phi^2 \rangle \propto \tau_l$. Moreover, the same result can be interpreted physically with a Brownian motion model.

Brownian motion is a physical phenomenon which describes the random motion behavior of tiny particles suspended in a fluid. Due to the collision of the molecules in the fluid, the tiny particles will move randomly. Einstein's theory about the Brownian motion shows that the variance of the displacement of the tiny particles is linearly proportional to the elapsed time, which is very similar to Eq. (20).

Considering the complex laser field as a vector in two-dimensional coordinates, when a photon is added to the field by spontaneous emission, as shown in Fig. 4, there will be a small shift both in phase and in amplitude [17]. Due to the property of spontaneous emission, each increment caused by a photon emitted is completely random in direction and with a constant step length. Thus, the lasing field vector can be regarded as a two-dimensional random walk, which can be proved to be a Brownian motion process [18]. Then we can draw the same conclusion that the variance of the quantum phase fluctuations $\langle \Delta\phi^2 \rangle \propto \tau$ with the characteristics of Brownian motion process.

Generally, when a laser source is above the threshold, its output power P is proportional to the photon number intensity S [16],

$$P = C\langle S \rangle, \tag{19}$$

where C is a constant determined by intrinsic parameters of a laser diode. Thus, we derive the first assumption:

$$\langle \Delta\phi_{\rm sp}^2 \rangle = \frac{C R_{\rm sp}\tau_l}{2P}. \tag{20}$$

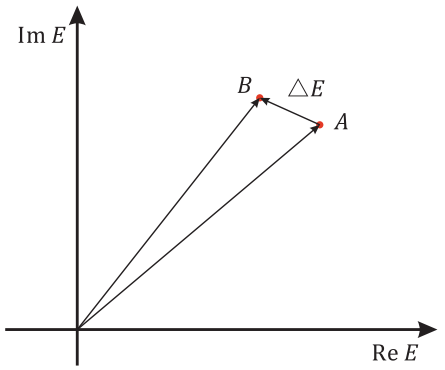

FIG. 4. (Color online) The laser field changes ΔE for the increment of a single photon. The length of ΔE is equal to 1, and the phase of ΔE is completely random. It has the same physical picture as a step of a two-dimensional random walk from A to B, which has been proved to be a Brownian motion.

Compared with Eq. (3), we can easily get

$$Q = \frac{C R_{\rm sp}\tau_l}{2}. \tag{21}$$

As for assumption 2, to see why the voltage V follows a Gaussian distribution, we only need to prove that the phase difference $\Delta\phi_{\rm sp}$ follows the same distribution according to Eqs. (2) and (7). From the definition in Eq. (15), for $F_{\rm sp}(t)$ is i.i.d., the integrals of $F_{\rm sp}(t)$ in the same length of time period are also i.i.d.; therefore we can think that $\Delta\phi_{\rm sp}$ is the sum of N i.i.d. variables, where each one is given by

$$\int_{t}^{t+\tau_l/N} F_{\rm sp}(t')\, dt'. \tag{22}$$

Due to the central limit theorem, we can easily conclude that $\Delta\phi$ follows a Gaussian distribution, and its variance is given in Eq. (16).

IV. MAXIMIZE OUTPUT RANDOMNESS AND GENERATION SPEED

In previous experiments, the random number generation speed is the product of the output randomness per sample and the sampling rate. Even with perfect detectors, the QRNG speed is limited by the sampling rate [19]; that is, the output randomness per sample is finite. On the other hand, it seems that the generation speed will infinitely increase with infinite sampling rate. In this section, we calculate the randomness output for given experiment setups. We show that the output randomness and random number generation speed are maximized with finite sampling rate when other experiment parameters are fixed.

In our analysis, the time delay τ_l and the sampling time interval τ_s are free variables. As the PLC-MZI interferes two laser beams whose emission time difference is τ_l, we can equivalently regard it as that the interference comes from two points in the same beam with time difference τ_l. As shown in Fig. 5(a), we can assume the points A and B interfere, for example.

When $\tau_l \leqslant \tau_s$, the quantum randomness $\Delta\phi_{\rm sp}$ in Eq. (15) is independent between different samples, because the integral

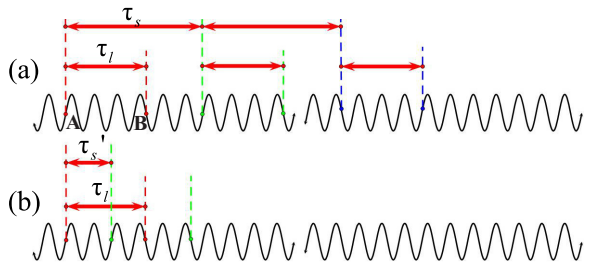

FIG. 5. (Color online) (a) The output of the PLC-MZI in each sample can be regarded as an interference from points A and B in the same beam with time difference τ_l. (b) When the sampling rate increases, there will be an overlap between different samples, and the quantum randomness $\Delta\phi_{\rm sp}$ is not mutually independent for different samples.

of $F_{\rm sp}(t)$, which is i.i.d., does not overlap between different samples. We thus show the assumption 3 is correct for $\tau_l \leqslant \tau_s$. It is straightforward to see that the output randomness will increase with increasing sampling speed as long as the condition $\tau_l \leqslant \tau_s$ holds.

On the other hand, as shown in Fig. 5(b), when $\tau_l > \tau_s$, the random output $\Delta\phi_{\rm sp}$ for successive samples has overlapped integrals, and the quantum phase differences $\Delta\phi_{\rm sp}$ are not independent for different samples. Apparently, assumption 3 cannot be satisfied and the derivation needs to be further adjusted. In this case, one needs to quantify the output randomness and the generation speed. We know that if τ_l is fixed at a certain value, an increasing sampling rate from the situation $\tau_l = \tau_s$ will result in an increasing generation speed. Since the uncertainty (entropy) of the system is finite, as shown later, the generation speed would saturate when the sampling rate is high enough. To find the optimal sampling rate, without loss of generality, we take τ_l as an integer multiple of τ_s. Then as shown in the Appendix, this situation can be regarded as that the random numbers are generated with a smaller τ_l' that $\tau_l' = \tau_s$, and we can equivalently quantify the output randomness with the parameters τ_l' and τ_s.

Thus, when considering the maximum production of randomness, we can always focus on the case of $\tau_l = \tau_s$. Then we just need to optimize τ_l to achieve the most output randomness. First, the coherence time τ_c can be defined by that the variance of $\phi_{\rm sp}$ changes $(2\pi)^2$:

$$\langle \Delta\phi^2 \rangle = \frac{C R_{\rm sp} \tau_c}{2P} = (2\pi)^2. \tag{23}$$

In this case, we can rewrite Eq. (20) by

$$\langle \Delta\phi^2 \rangle = 4\pi^2 \frac{\tau_l}{\tau_c}, \tag{24}$$

and the variance of the output voltage is given by

$$\langle V_Q^2 \rangle = A P^2 \langle \Delta\phi^2 \rangle = 4 A P^2 \pi^2 \frac{\tau_l}{\tau_c}. \tag{25}$$

The output voltage follows a Gaussian distribution, and the output random number is from the voltage in a certain interval. In the practical scenario where there might exist classical noises and potential adversaries, the minimum randomness for each sampling, as shown in Fig. 6, can be expressed as

$$R_0 = -\log_2 {\rm P}_{\rm max},$$

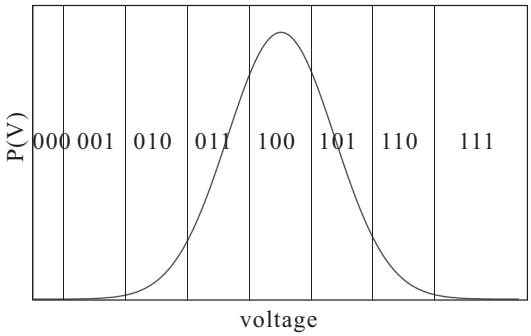

FIG. 6. A shift of the voltage partition caused by classical noise and potential adversaries will always reduce the output randomness per sample, and the randomness has a minimum with the partition here, which represents the worst case.

$$\begin{aligned} &= -\log_2 \left[\Phi'\left(\frac{a}{2}\right) - \Phi'\left(-\frac{a}{2}\right) \right], \\ &= -\log_2 \left[\Phi\left(\frac{a}{2\sqrt{\langle V_Q^2 \rangle}}\right) - \Phi\left(-\frac{a}{2\sqrt{\langle V_Q^2 \rangle}}\right) \right], \\ &= -\log_2 \left[2\Phi\left(\frac{\lambda}{\sqrt{\tau_l}}\right) - 1 \right], \end{aligned} \tag{26}$$

where $\Phi'(x)$ and $\Phi(x)$ are the cumulative distribution functions of a Gaussian distribution $(0, \sqrt{\langle V_Q^2 \rangle})$ and a standard Gaussian distribution, respectively, a is the length of a voltage interval, and λ is a constant determined by experiment parameters according to

$$\lambda = \frac{a}{4\pi P} \sqrt{\frac{\tau_c}{A}}. \tag{27}$$

In a fixed sample time T, the total output randomness is

$$\begin{aligned} R_{\rm tot} &= \frac{T}{\tau_s} R_0, \\ &= -\frac{T}{\tau_l} \log_2 \left[2\Phi\left(\frac{\lambda}{\sqrt{\tau_l}}\right) - 1 \right], \end{aligned} \tag{28}$$

where we make use of the relation $\tau_l = \tau_s$. Moreover, if we multiply Eq. (28) by $1/T$, the result stands for the random number generation speed R_s,

$$R_s = -\frac{1}{\tau_l} \log_2 \left[2\Phi\left(\frac{\lambda}{\sqrt{\tau_l}}\right) - 1 \right]. \tag{29}$$

Here we show the relationship between R_s and τ_l in Fig. 7. We can see that the generation speed R_s has a maximum.

The existence of maximum generation speed can be intuitively explained, which is mainly owing to the finite resolution of the ADC. In Eq. (24), we can see that the variance of the detected random number is linearly proportional to the sampling time interval when $\tau_s = \tau_l$. With increasing sampling speed, the sampling time interval τ_s will decrease. When τ_s is small enough, the detected random numbers will lie almost always in the same interval of the ADC. In other words, we will not detect the quantum noise. In this case, the output randomness in each sample is almost zero as can be inferred from Eq. (26). Therefore, considering the resolution of ADC,

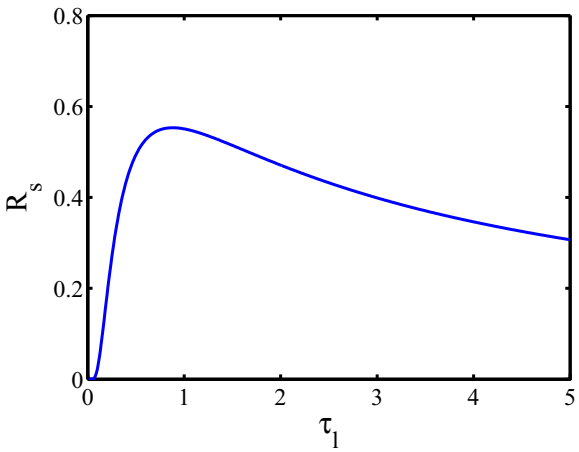

FIG. 7. (Color online) The unit of the random number generation speed R_s and the time delay difference τ_l are bit/s and s, respectively. To merely show their relationship, we set the constant λ to be $1\sqrt{\text{s}}$ for simplicity. Then we can see that R_s has a maximum at $\tau_l = 0.88$˜s. In experiments, the actual value of the optimized τ_l can be calculated similarly with an accurate λ.

the output randomness will be upper bounded with a finite value. Additionally, in experiments, if a high-resolution ADC is not available, we will add a high-gain amplifier after the photodetector, which is equivalent to increasing parameter A in Eq. (4). However, combining Eqs. (4) and (25) we can see that the additional classical noise introduced will increase with sampling rate, that is, the extra noise contributed by the amplifier may overpower the benefit it brings in.

On the other hand, it is interesting to see whether the resolution is the ultimate restriction of the generation speed. When the resolution is almost infinite, can we get infinite randomness output with the discussed experiment setup? Here we show that even if the resolution of the ADC can be infinite, the generation speed will not increase infinitely. Given a perfect photon-number resolving detector, the upper bound of the min-entropy is determined by the photon number within the detection time window [19]. Suppose that the maximum of the photon number detected per sample is N, the total randomness output in the setup, as shown in Fig. 2, is at most $\log_2(N+1) \sim \log_2 N$ (when the photon numbers detected per sample follows a uniform distribution). That is, the upper bound of randomness extracted per sample is about $\log_2 N$. Actually the value of the voltage measured with the ADC is discrete. As the sampling rate increases, the voltage measured by the ADC will finally fix at some certain value, and the output randomness will be zero. Therefore, there still exists a limit of the speed of generating random numbers.

Moreover, here we assume that the response time of the photodetector is small enough to be ignored. In practice, the photodetector has finite bandwidth, so the detection can be understood as an integral process over a certain time interval, which is the origin of detector response time. If we consider it in our model, we only need to replace τ_l with $\tau_l + \tau_r$, where τ_r represents the detector response time satisfying $\tau_s > \tau_r$ and $\tau_c > \tau_r$ [9].

V. DISCUSSION AND CONCLUSION

In randomness evaluation, we quantify it with min-entropy. In a sense, we assume that the classical noise is known to the adversary but not malicious. In a recent work, the malicious classical noise scenario is considered by quantifying the randomness with conditional min-entropy [20]. Assuming the classical noise e also to be Gaussian, in our min-entropy formula, Eq. (6), $\Pr(X)$ should be replaced with a conditional probability $\Pr(X|e)$ to calculate the conditional min-entropy H_c. When the adversary is assumed to have full control over the classical noise, the conditional min-entropy minimizing H_c over e should be used in the worst case scenario. On the other hand, when the adversary is restricted to passive eavesdropping, the conditional min-entropy averaging H_c on the distribution of e is used instead. Here we point out that the quantification of randomness in our model is quite similar to the worst-case conditional min-entropy when the variance of e is small enough, which needs more study in the future work.

In conclusion, by reviewing the QRNG scheme and its underlying intuitive physical model, we derive the assumptions and provide a more rigorous model for the QRNG based on vacuum fluctuation. Our result suggest that random number generation speed in such a QRNG is finitely bounded in practice, and the device parameters can be optimized to maximize the generation speed.

ACKNOWLEDGMENTS

The authors acknowledge insightful discussions with Z. Cao, B. Qi, F. Xu, and Q. Zhao. This work was supported by the National Basic Research Program of China Grants No. 2011CBA00300 and No. 2011CBA00301 and the 1000 Youth Fellowship program in China.

APPENDIX: DEMONSTRATION OF THE EQUIVALENCE OF OUTPUT RANDOMNESS IN TWO SITUATIONS: $\tau_s \ll \tau_l$ AND $\tau_s = \tau_l'$

In this Appendix, we show the output randomness generated in two situations: $\tau_s \ll \tau_l$ and $\tau_s = \tau_l'$ are the same. First, we need to notice that when the sampling rate is high enough, we can think τ_l to be an integer multiple of τ_s; that is, $\tau_l = n\tau_s$, where n is a positive integer.

Here denote the phase by ϕ_k with label k representing the time sequence, then the raw data can be given by

$$\begin{aligned} d_1 &= \phi_{n+1} - \phi_1, \\ d_2 &= \phi_{n+2} - \phi_2, \\ &\cdots . \end{aligned} \tag{A1}$$

In experiments, autocorrelation of the random numbers $\{d_k\}$ in the situation $\tau_s \ll \tau_l$ is very high. To reduce the autocorrelation, "exclusive OR" operations can be applied to every two adjacent sequences of random numbers, as shown in Fig. 8. After the exclusive or operation, we can get new sequences of random numbers:

$$\begin{aligned} d_1' &= d_2 - d_1 = \phi_{n+2} - \phi_{n+1} - (\phi_2 - \phi_1), \\ d_2' &= d_3 - d_2 = \phi_{n+3} - \phi_{n+2} - (\phi_3 - \phi_2), \\ &\cdots . \end{aligned} \tag{A2}$$

Denote $b_k = d_{k+1} - d_k$; then we can see from the main context that b_k are independent random numbers. Then we can

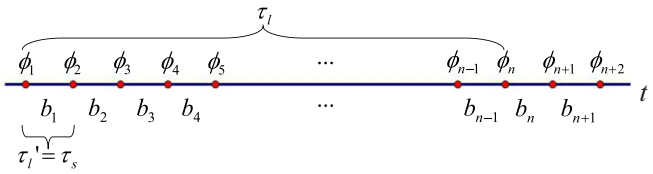

FIG. 8. (Color online) After an exclusive OR operation between every two adjacent sequences of random numbers, the new sequences can be expressed as $b_{n+1} - b_1, b_{n+2} - b_2, \ldots$.

express the d_k' by

$$\begin{aligned} d_1' &= b_{n+1} - b_1, \\ d_2' &= b_{n+2} - b_2, \\ &\cdots . \end{aligned} \tag{A3}$$

Then we can easily see that the randomness of $\{b_k\}$ is the same to that of $\{d_k'\}$ in the asymptotic case, while the randomness of $\{b_k\}$ is generated when we have an equivalent interferometer with $\tau_l' = \tau_s$.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[2] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).

[3] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

[4] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).

[5] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, Nature (London) **464**, 1021 (2010).

[6] M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).

[7] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).

[8] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Appl. Phys. Lett. **104**, 051110 (2014).

[9] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).

[10] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).

[11] T. Symul, S. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).

[12] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).

[13] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, Opt. Express **22**, 1645 (2014).

[14] M. O. Scully, *Quantum Optics* (Cambridge University Press, Cambridge, 1997).

[15] K. Vahala and A. Yariv, Appl. Phys. Lett. **43**, 140 (1983).

[16] K. Petermann, *Laser Diode Modulation and Noise*, Vol. 3 (Springer, New York, 1991).

[17] A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications, Oxford Series in Electrical and Computer Engineering* (Oxford University Press, Oxford, 2006).

[18] S. M. Ross, *Introduction to Probability Models* (Academic Press, New York, 2014).

[19] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).

[20] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Phys. Rev. Applied **3**, 054004 (2015).