Phase randomness in a semiconductor laser: Issue of quantum random-number generation

Roman Shakhovoy,[1,2,3,*] Marius Puplauskis,[4] Violetta Sharoglazova,[1] Alexander Duplinskiy,[1,2,4] Denis Sych,[5] Elizaveta Maksimova,[1] Selbi Hydyrova,[4,6] Alexander Tumachek,[3] Yury Mironov,[3] Vadim Kovalyuk,[2,7] Alexey Prokhodtsov,[7] Grigory Goltsman,[4,7] and Yury Kurochkin[8]

[1]*QRate, Skolkovo 115419, Russia*

[2]*NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*

[3]*Moscow Technical University of Communications and Informatics, Moscow 111024, Russia*

[4]*Russian Quantum Center, Skolkovo 121205, Russia*

[5]*P.N. Lebedev Physical Institute of the Russian Academy of Science, Moscow 119333, Russia*

[6]*Bauman Moscow State Technical University, Moscow 105005, Russia*

[7]*National Research University Higher School of Economics, Moscow 109028, Russia*

[8]*Quantum Research Centre, Technology Innovation Institute, Abu Dhabi 9639, United Arab Emirates*

(Received 4 October 2022; accepted 17 January 2023; published 30 January 2023)

Gain-switched lasers are in demand in numerous quantum applications, particularly in systems of quantum key distribution and in various optical quantum random number generators. The reason for this popularity is natural phase randomization between gain-switched laser pulses. The idea of such randomization has become so familiar that most authors use it without regard to the features of the laser operation mode they use. However, at high repetition rates of laser pulses or when pulses are generated at a bias current close to the threshold, the phase randomization condition may be violated. This paper describes theoretical and experimental methods for estimating the degree of phase randomization in a gain-switched laser. We consider in detail different situations of laser pulse interference and show that the interference signal remains quantum in nature even in the presence of classical phase drift in the interferometer provided that the phase diffusion in a laser is efficient enough. Moreover, we formulate the relationship between the previously introduced quantum reduction factor and the leftover hash lemma. Using this relationship, we develop a method to estimate the quantum noise contribution to the interference signal in the presence of phase correlations. Finally, we introduce a simple experimental method based on the analysis of statistical interference fringes, providing more detailed information about the probabilistic properties of laser pulse interference.

DOI: 10.1103/PhysRevA.107.012616

I. INTRODUCTION

Phase randomness between pulses of a gain-switched semiconductor laser is an essential ingredient of quantum key distribution (QKD) systems and quantum random number generators (QRNGs). Inasmuch as amplified spontaneous emission dominates below threshold in a semiconductor laser [1,2], phase correlations of the electromagnetic field are destroyed very quickly between laser pulses under the gain switching. Therefore, many authors often assume implicitly that pulses from a gain-switched laser have no phase relationship with each other. The security analysis of QKD protocols, particularly decoy-BB84 protocol [3–5], assumes that the laser emits light pulses that are a mixture of coherent states with uniformly distributed phases. A similar assumption is usually made when considering laser pulse interference as a quantum entropy source for some optical QRNGs [6–12]. In real experiments, however, phase correlations may still occur and may thus lead to loss of security. Therefore, phase diffusion between laser pulses should be treated carefully in these applications.

The main reason for correlations between phases of pulses emitted by a gain-switched semiconductor laser is an insufficient delay between subsequent pulses, during which the phase does not have enough time to "diffuse." Also, a high value of the bias current does not allow the attenuation between laser pulses to be high enough to provide fast decoherence. It was estimated in [6] that enough for application in QRNG randomness could be achieved with the laser pulse repetition rate up to 20 GHz under the assumption that attenuation between pulses reaches 100 dB. The same authors demonstrated later an optical QRNG with the distributed feedback (DFB) gain-switched laser operating at a pulse repetition rate of 5.825 GHz [7]. In [13] the phase randomness between pulses with the repetition rate of 10 GHz was demonstrated to be enough for QKD applications.

The issue of the phase randomness of attenuated laser pulses used as quantum states for QKD has been widely discussed in the literature [13–16]. It was shown that phase correlations enhance the distinguishability of quantum states [14], which is directly related to the security of the decoy-BB84 protocol; therefore, when the phase between coherent states is not well randomized, the performance of the QKD system will be substantially reduced. In fact,

*r.shakhovoy@goqrate.com

it was demonstrated experimentally that Eve could employ phase correlations to compromise the quantum key [15,16]. The dependence of the state distinguishability (imbalance of the quantum coin [17]) on the degree of phase correlations between laser pulses or rather on the value of the standard deviation σ_φ of phase fluctuations has been investigated numerically in [13]. The authors demonstrated that the imbalance decreases as the standard deviation increases converging to finite values for large σ_φ.

Reference [12] introduced the concept of the quantum reduction factor, which allows estimating the contribution of classical noise to the interference of laser pulses. The proposed approach assumes that σ_φ is large enough ($\sigma_\varphi > 2\pi$), such that one may consider any classical contribution to phase fluctuations to be buried under the noise of spontaneous emission. The situation $\sigma_\varphi < 2\pi$ has not been considered in [12]; however, the definition of the quantum reduction factor now should be modified to take the lack of phase randomness into account. In this paper we propose a method which allows including these correlations into the model for a QRNG based on the interference of laser pulses. We discuss this in Sec. II C.

Another motivation for this paper was that there is no well-established theoretical approach in the literature that would allow estimating the pulse repetition rate and appropriate values of the pump current at which the phase randomness could be still considered purely quantum and thus sufficient for application in a QRNG. Here we intend to formulate a theoretical approach which provides a clear criterion for the phase diffusion efficiency at any pulse repetition rate and any value of the pump current.

In addition to a theoretical model, which allows analyzing the dependence of σ_φ on laser parameters, it is useful to have a reliable experimental method to measure the phase diffusion between pulses of a gain-switched laser. A standard approach is to use visibility of interference fringes as a criterion of phase randomness (see, e.g., [13]). Such an approach provides a useful experimental probe to estimate the effectiveness of the phase diffusion. However, it does not allow distinguishing various noise contributions to the interference signal, such as the photodetector noise or intrinsic fluctuations of laser pulse intensity. We will demonstrate here that it is possible to set up the experiment in such a way that the experimental data would be sensitive to the mentioned classical noises, so that they could be separated from the phase fluctuations by choosing an appropriate mathematical model. We discuss this in Sec. IV (for more details see [12]).

In Sec. II we consider the most essential features of the interference of laser pulses with random phases, provide a method to estimate the quantum noise contribution to the interference signal in the presence of phase correlations, and develop a numerical approach to follow the dependence of the phase diffusion on the pump current and the pulse repetition rate. In Sec. III we provide the reader with experimental results on the phase diffusion measurements. Finally, in Secs. IV and V discussions and conclusions are given.

II. THEORETICAL CONSIDERATIONS

A. On the interference of laser beams

1. Monochromatic plane wave

In most textbooks on optics, the interference of light in a Mach-Zehnder interferometer is usually considered using the example of a plane-polarized monochromatic wave, which is divided by a first beam splitter and gets into the interferometer arms. In the general case, one of the arms can be longer or, e.g., may contain some object. After passing through the interferometer arms, the two resulting waves are then met at the second beam splitter, where the interference occurs. The result of the interference depends on the phase acquired by the wave in the long arm of the interferometer (or rather by the phase difference between the arms). In the case of a quasimonochromatic wave, the result of the interference will also depend on the relationship between the time delay ΔT of the long arm and the coherence time τ_c of light. If $\Delta T \ll \tau_c$, one may assume that electric fields meeting at the second beam splitter have the form

$$E_1(t) = E_0 \exp(i\varphi_0 + i\omega_0 t),$$
$$E_2(t) = E_0 \exp[i\varphi_0 + i\omega_0(t + \Delta T)], \tag{1}$$

where ω_0 is the midfrequency of the field and where we assume for simplicity that both beam splitters of the interferometer are ideal 50:50 beam splitters. We also assume that losses in the interferometer arms are the same (or may be neglected), so that the real amplitudes of the interfering fields are equal to E_0. The result of the interference S in one of the output ports of the interferometer will then be written as follows:

$$S \equiv |E_1 + E_2|^2 = 4E_0^2 \cos^2\left(\frac{\omega_0 \Delta T}{2}\right). \tag{2}$$

It is clear from Eq. (2) that the interference depends on the carrier frequency of the field, which is a standard result.

2. Two independent monochromatic waves

A somewhat different result is obtained when considering the interference of the two monochromatic waves from independent laser sources [18]. To observe the interference in this case, it is sufficient to take a single beam splitter and to send laser beams into its input ports. If the intensities of the two laser beams are the same, then the monochromatic waves interfering at the beam splitter can be written as follows:

$$E_1(t) = E_0 \exp\left(i\varphi_1^0 + i\omega_0 t\right),$$
$$E_2(t) = E_0 \exp\left[i\varphi_2^0 + i\omega_0(t + \tau)\right], \tag{3}$$

where φ_1^0 and φ_2^0 are random initial phases of the fields and $\omega_0\tau$ corresponds to a phase difference due to the optical path difference of the light beams. The result of the interference in one of the output ports of the beam splitter can be written as follows:

$$S = 4E_0^2 \cos^2\left[\tfrac{1}{2}(\omega_0\tau + \Delta\varphi)\right], \tag{4}$$

where $\Delta\varphi = \varphi_2^0 - \varphi_1^0$. In the general case, the phase difference $\Delta\varphi$ is a random function of time, and for incoherent beams it fluctuates very quickly, so that the interference cannot be observed. In the case of independent quasimonochromatic laser beams, $\Delta\varphi$ is still a function of time, but its variations occur quite slowly, so that the interference can be easily observed.

Note that if the two independent laser beams with fields, as in Eq. (3), are brought into the same input port of an unbalanced interferometer, the result of the interference will be determined by the following relation:

$$S = 4E_0^2\cos^2\left(\frac{\omega_0\Delta T}{2}\right)\cos^2\left[\frac{1}{2}(\omega_0\tau + \Delta\varphi)\right]. \tag{5}$$

An important difference between the interference of independent coherent laser beams [Eq. (5)] from the interference of a monochromatic wave with itself [Eq. (2)] is that the former depends on the phase difference $\Delta\varphi$, as well as on the additional phase change $\omega_0\tau$ associated with the "prehistory" of the interfering beams.

3. Laser pulses from a continuous beam

Let us now consider the interference of pulses from a semiconductor laser when the pump current does not fall below threshold, i.e., when the laser operates in a continuous mode, and the modulation current "cuts out" pulses from the continuous laser beam (we neglect the effect of chirp). We will further assume that the sequence of laser pulses obtained in this way is fed into the unbalanced interferometer with the time delay equal to the pulse repetition period ($\Delta T = 1/f_p$; f_p is the pulse repetition frequency). With such an interferometer, we will observe the interference of the two neighboring pulses. Obviously, this case is similar to the interference of a monochromatic wave with itself with the only difference that the envelopes of the interfering components now depend on time, and instead of Eq. (1) we should write

$$\begin{aligned} E_1(t) &= \sqrt{Q_1(t)}\exp\left(i\varphi_0 + i\omega_0 t\right), \\ E_2(t) &= \sqrt{Q_2(t)}\exp\left[i\varphi_0 + i\omega_0(t+\Delta T)\right], \end{aligned} \tag{6}$$

where Q_1 and Q_2 are field intensities. Here we will assume that optical pulses have a Gaussian shape:

$$Q_1(t) = Q_0 e^{-\frac{t^2}{2w^2}}, \quad Q_2(t) = Q_0 e^{-\frac{(t-\Delta t)^2}{2w^2}}, \tag{7}$$

where w is the width of the pulse and Δt takes into account the inaccuracy of the pulse overlap. In the general case, Δt can be associated with a difference between the pulse repetition period and the time delay in the interferometer, as well as with the time jitter of laser pulses. Below we will assume that Δt is associated only with jitter, whereas the time delay ΔT in the long arm of the interferometer ideally matches the pulse repetition period.

The result of the interference of laser pulses with fields from Eq. (6) is

$$S = Q_1 + Q_2 + 2\sqrt{Q_1 Q_2}\cos(\omega_0\Delta T). \tag{8}$$

In the case of the pulse interference, it is useful to determine the integral signal $\tilde{S}$ corresponding to the "area" under the interference pulse normalized to the "area" of the signal passing through one of the interferometer arms:

$$\tilde{S} = \frac{\int_{-\Delta T/2}^{\Delta T/2} S(t)\,dt}{\int_{-\Delta T/2}^{\Delta T/2} Q_1(t)\,dt}, \tag{9}$$

whence using Eqs. (7) and (8) and extending integration limits up to $\pm\infty$ (this can be done if the width w is significantly smaller than the pulse repetition period ΔT) we will have

$$\tilde{S} = 2[1 + \eta\cos(\omega_0\Delta T)], \tag{10}$$

where visibility $\eta = \exp[-\Delta t^2/(8w^2)]$ depends on the ratio between jitter Δt and the pulse width w. It is important to note here that visibility of the interference in this extreme case does not depend on the spectral composition of light, but depends only on jitter, i.e., on the quality of the electrical pattern that sets the sequence of laser pulses. However, if the time jitter is small, $\Delta t \ll w$, one may assume that $\eta \approx 1$, which yields $\tilde{S} = 4\cos^2(\omega_0\Delta T/2)$, and the result of the pulse interference is determined by the phase evolution $\omega_0\Delta T$ and *does not depend* on jitter.

4. Independent laser pulses

Now let us consider the above scheme of laser pulse interference ($\Delta T = 1/f_p$), but now with the semiconductor laser operating under the gain switching. If the coherence of radiation in the cavity is destroyed during the time while the laser is under the threshold, then we may assume that the pulses meeting at the interferometer's output originate from independent sources. The result of the interference, therefore, should be similar to that obtained in Eq. (4). In fact, by analogy with Eq. (3), let us write the fields in the interfering pulses:

$$\begin{aligned} E_1(t) &= \sqrt{Q_1(t)}\exp\left(i\varphi_1^0 + i\omega_0 t\right), \\ E_2(t) &= \sqrt{Q_2(t)}\exp\left[i\varphi_2^0 + i\omega_0(t+\Delta t)\right], \end{aligned} \tag{11}$$

where the phase change $\omega_0\tau$ from Eq. (3) is replaced here by $\omega_0\Delta t$ since the "prehistory" is related in this case with jitter, due to which different pairs of pulses do not always arrive at the second beam splitter simultaneously. Moreover, we will assume that Q_1 and Q_2 in Eq. (11) are again defined by Eq. (7).

Let us first consider the case when there is no jitter. The integral signal $\tilde{S}$ will then have a simple form:

$$\tilde{S} = 4\cos^2\frac{\Delta\varphi}{2}. \tag{12}$$

As can be seen from a comparison of Eqs. (12) and (10), the result of the interference of independent laser pulses does not include the carrier frequency of the electromagnetic field. This means that if we take a laser of another wavelength and use it to prepare a similar pair of pulses with the same initial phases, then the result of the interference of this new pair of pulses will be the same as in the previous case. This result differs significantly from the interference of a continuous monochromatic wave in an unbalanced interferometer, for which the shift of the carrier frequency leads to the change in the result of the interference.

Now let us consider the interference of independent pulses in the presence of jitter. In this case, the result of the interference of fields from Eq. (11) will have the following

form:

$$\tilde{S} = 2[1 + \eta \cos(\omega_0 \Delta t + \Delta\varphi)]. \tag{13}$$

If $\Delta t \ll w$, we may put $\eta \approx 1$, which yields $\tilde{S} = 4\cos^2[(\omega_0 \Delta t + \Delta\varphi)/2]$, whence it is clear that the result of the interference is strongly dependent on jitter since the latter is included in the cosine argument. Moreover, for a fixed $\Delta\varphi$, the interference of pulses in this case will, in essence, be determined by jitter. Indeed, for frequencies commonly used in telecommunications, $\omega_0/(2\pi) \sim 10^{14}$ Hz, even highly stable frequency oscillators with jitter of hundreds of femtoseconds, $\Delta t \sim 10^{-13}$, will not allow obtaining the stable interference (at fixed $\Delta\varphi$), because $\omega_0 \Delta t \gg 1$. It should be noted here that the time jitter of laser pulses from a gain-switched laser is generally much larger than the intrinsic jitter of the driving electrical signal. This fact is related to a delay between the leading edge of the pump current pulse and the onset of lasing (the so-called turn-on delay [19]), which depends on the amplitude (peak-to-peak value I_p) of the modulation current. Due to fluctuations in I_p, the turn-on delay will also fluctuate, which will lead to an additional contribution to jitter.

Comparing Eqs. (13) and (10), we may write the following condition (on the assumption that the influence of jitter on visibility can be neglected):

$$4\cos^2\left(\frac{\omega_0 \Delta t + \Delta\varphi}{2}\right) \to 4\cos^2\left(\frac{\omega_0 \Delta T}{2}\right), \tag{14}$$

which determines the transition of the laser from the gain-switching mode to continuous generation. It is important to note that the left-hand side of Eq. (14) is valid when the bias current I_b is significantly below threshold current I_{th}, whereas the right-hand side is valid when I_b is much higher than I_{th}. Obviously, the transition given by Eq. (14) is equivalent to the following conditions: $\Delta\varphi \to \omega_0 \Delta T$ and $\Delta t \to 0$, which are satisfied if we assume that $\Delta\varphi$ and Δt are random variables with Gaussian distributions, whose average values are $\omega_0 \Delta t$ and 0, respectively, and whose standard deviations $\sigma_\varphi \equiv \sigma_\varphi(I_b)$ and $\sigma_{\Delta t} \equiv \sigma_{\Delta t}(I_b)$ are decreasing functions of the bias current, and they tend to zero when I_b is much higher than I_{th}.

In a QRNG based on the interference of laser pulses, the phase difference $\Delta\varphi$ plays the role of a quantum entropy source since its random values are determined by quantum nature of spontaneous emission. In contrast, the jitter-related phase change $\omega_0 \Delta t$ should be treated as classical noise. For typical jitter values (10^{-12} s), the phase evolution $\omega_0 \Delta t$ can take on very large values, significantly exceeding $\Delta\varphi$; therefore, at first glance, it seems that randomness obtained from the interference of laser pulses cannot be considered quantum. This could be true if, with a large range of $\omega_0 \Delta t$ values, the spread of $\Delta\varphi$ values was small enough. However, the influence of jitter on the phase difference between laser pulses can be also ignored at small values of σ_φ (small spread of $\Delta\varphi$ values). Indeed, in this case, adjacent laser pulses cannot be considered as pulses from two independent sources since they are now phase correlated. This means that such pulses should be considered "cut out" from a continuous quasimonochromatic wave (albeit with a short coherence time), for which the effect of jitter on the phase evolution is absent.

The above reasoning shows that substantiation of quantum nature of laser pulse interference is a "thin place" of QRNG implementation. Indeed, continuing the above reasoning, one can come to the conclusion that for a sufficiently large value of σ_φ (at least for $\sigma_\varphi > \pi$) interfering laser pulses can be considered independent and one should take into account the jitter-related phase change $\omega_0 \Delta t$. Inasmuch as classical contribution from $\omega_0 \Delta t$ can significantly exceed quantum contribution from $\Delta\varphi$, a reasonable question arises: does the QRNG cease to be quantum in this case? In fact, it is easy to see that QRNG still should be considered quantum. Indeed, inasmuch as the sum $\omega_0 \Delta t + \Delta\varphi$ is in the argument of the cosine, an adversary who knows all the Δt values in advance or may even control them will not be able to say anything definite about the result of the interference (beyond what he *a priori* knows about the probability density of the interference signal), if $\Delta\varphi$ exhibits a large spread of values. In other words, even in the presence of a classical contribution from $\omega_0 \Delta t$ the result of the interference from Eq. (13) remains nondeterministic, unpredictable, and uncontrollable, i.e., satisfies the requirements for the quantum noise [12]. This means that when considering the interference of laser pulses with random phases in the context of a QRNG, the phase change associated with jitter can be excluded from consideration.

Finally, note that the result of interference is also influenced by the spread in the intensities of laser pulses associated with fluctuations of the pump current. We will assume below that such fluctuations are sufficiently small, so that we can neglect the change in the shape of the laser pulse and assume that only its "area" changes slightly from pulse to pulse. Thus, the fields in interfering pulses can be written in the following form:

$$\begin{aligned} E_1(t) &= \sqrt{s_1 Q_1(t)} \exp\left(i\varphi_1^0 + i\omega_0 t\right), \\ E_2(t) &= \sqrt{s_2 Q_2(t)} \exp\left(i\varphi_2^0 + i\omega_0 t\right), \end{aligned} \tag{15}$$

where we have introduced two independent random variables, s_1 and s_2, associated with the spread of intensities of interfering pulses. For simplicity, we may assume that both s_1 and s_2 exhibit Gaussian distribution with the mean value $\bar{s}_1 = \bar{s}_2 = 1$ and a standard deviation of σ_s. The integral interference signal $\tilde{S}$ for the fields from Eq. (15) will then have the form

$$\tilde{S} = s_1 + s_2 + 2\eta\sqrt{s_1 s_2}\cos(\Delta\varphi). \tag{16}$$

B. Probability density function and the quantum reduction factor

Probabilistic properties of laser pulse interference are well described by the probability density function (PDF) of the interference signal. In this section we will consider it both for the case of efficient phase diffusion ($\sigma_\varphi > 2\pi$) and for correlated neighboring laser pulses ($\sigma_\varphi < 2\pi$).

The PDF $f_{\tilde{S}}$ of the integral signal $\tilde{S}$ can be defined as a derivative of a corresponding cumulative distribution function. The latter represents an integral of the PDF defining joint fluctuations of $\Delta\varphi$, s_1, s_2, ζ, and η, where ζ is the Gaussian classical detector noise, which should be added to the integral signal: $\tilde{S} \to \tilde{S} + \zeta$, and fluctuations of η are caused by the jitter. The influence of chirp, jitter, and relaxation oscillations on the probability density of the integral interference signal $\tilde{S}$

has been considered in [20]. In particular, the chirp has been shown to enhance the influence of jitter on visibility η, so that the condition $\Delta t \ll w$ does not always allow neglecting fluctuations of η. Nevertheless, it was shown that the "chirp + jitter" effect could be significantly decreased for relatively short laser pulses by cutting off the high-frequency part of the spectrum. As for sufficiently long laser pulses, the effect of the chirp on the interference can be neglected (even without spectral filtering) if the "area" under the main relaxation peak is much smaller than the "area" under the rest of the pulse. With this in mind, we will assume below that we deal with quite long laser pulses or use spectral filtering, so that the chirp has no significant effect on the interference. We will thus neglect jitter-related fluctuations of the visibility. However, even in this case an analytical expression for $f_{\tilde{S}}$ cannot be found; therefore, the analysis of various contributions to $f_{\tilde{S}}$ is performed numerically with Monte Carlo simulations.

1. Uniform distribution of $\Delta\varphi$

It was shown in [12] that one can extract quantum noise from the interference signal by introducing the parameter called the quantum reduction factor (QRF) Γ. This parameter shows how much the raw random sequence should be reduced (or compressed) by the randomness extractor in order to filter out possible hidden correlations associated with classical noise. The idea of the QRF is based on a comparison of the experimentally observed PDF $f_{\tilde{S}}$ with ideal (or quantum) PDF $f_{\tilde{S}}^{Q}$. The latter can be found from Eq. (16) on the assumption that the only random variable is $\Delta\varphi$ (whereas s_1 and s_2 are fixed to their average values), and

$$f_{\Delta\varphi} = \begin{cases} 1/\pi, & \Delta\varphi \in [0,\pi) \\ 0, & \Delta\varphi \notin [0,\pi) \end{cases}. \tag{17}$$

One can easily show that

$$f_{\tilde{S}}^{Q}(y) = \left[\pi\sqrt{(y-\tilde{S}_{\min})(\tilde{S}_{\max}-y)}\right]^{-1}, \tag{18}$$

where

$$\begin{aligned} \tilde{S}_{\min} &= s_1 + s_2 - 2\eta\sqrt{s_1 s_2}, \\ \tilde{S}_{\max} &= s_1 + s_2 + 2\eta\sqrt{s_1 s_2}. \end{aligned} \tag{19}$$

The function given by Eq. (18) with $s_1 = s_2 = 1$ and $\eta = 1$ is shown in Fig. 1 with black dashed lines; one can see that $f_{\tilde{S}}^{Q}$ is U-shaped and tends to infinity at $\tilde{S}_{\min}$ and $\tilde{S}_{\max}$ (in the case under consideration, $\tilde{S}_{\min} = 0$ and $\tilde{S}_{\max} = 4$).

It was shown that the definition of Γ depends on the method of digitizing the random signal [12]. When digitizing with a comparator, one can define Γ as follows:

$$\Gamma = \frac{1}{2 - H_{\infty}}, \tag{20}$$

where the min-entropy is defined as

$$H_{\infty} = -\log_2\left(\int_{\tilde{S}_{\min}}^{\tilde{S}_{\text{th}}} f_{\tilde{S}}(y)\,dy\right), \tag{21}$$

and $\tilde{S}_{\text{th}}$ is a threshold value, which should be chosen such that the area under the PDF curve to the left and to the right of $\tilde{S}_{\text{th}}$ was 1/2. (With such a definition, we may also treat $\tilde{S}_{\text{th}}$ as a mean value of the distribution.) The quantum PDF $f_{\tilde{S}}^{Q}$ is implicitly contained in Eq. (21) via the lower limit of the integral. If we insert $f_{\tilde{S}}^{Q}$ instead of $f_{\tilde{S}}$ into Eq. (21), the min-entropy will have the sense of an ideal or quantum min-entropy, which we denote as H_{∞}^{Q} and which, obviously, equal to 1. Note that generally $H_{\infty} > 1$ inasmuch as the experimental PDF is broadened due to fluctuations of s_1 and s_2 as well as due to the detector noise ζ. In this case $\tilde{S}_{\min}$ lies inside the experimental PDF, and the integral under the logarithm in Eq. (21) is less than 1/2. Note also that definitions of the quantum reduction factor [Eq. (20)] and the min-entropy [Eq. (21)] are valid only when digitization is performed with the comparator. Other definitions should be chosen when the signal is digitized with an analog-to-digital converter (see [12] for more details).

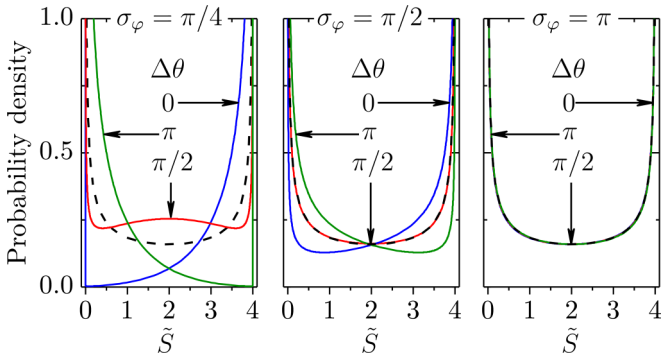

FIG. 1. Probability density functions $\tilde{f}_{\tilde{S}}^{Q}$ defined by Eq. (29) at different values of σ_φ and $\Delta\theta$.

2. Gaussian distribution of $\Delta\varphi$

It is important to keep in mind that the definition of the QRF given by Eqs. (20) and (21) is directly related to the assumption that $f_{\Delta\varphi}$ is uniform. In the general case, however, $f_{\Delta\varphi}$ is Gaussian:

$$\tilde{f}_{\Delta\varphi}(x) = \frac{1}{\sigma_\varphi\sqrt{2\pi}}\exp\left(-\frac{(x-\Delta\theta)^2}{2\sigma_\varphi^2}\right), \tag{22}$$

where $\Delta\theta = \omega_0\Delta T$, and the value of the random variable $\Delta\varphi$ we have denoted as x. [The tilde sign above f in Eq. (22) means also that in contrast to Eq. (17) the PDF depends now on $\Delta\theta$.] To find the quantum PDF $\tilde{f}_{\tilde{S}}^{Q}$ in this case, we use a well-known theorem applicable to monotonic functions, according to which the probability density $f_Y(y)$ of a random variable $Y = g(X)$ is given by the following formula:

$$f_Y(y) = f_X\big(g^{-1}(y)\big)\left|\frac{d}{dy}\big(g^{-1}(y)\big)\right|, \tag{23}$$

where y is the value of a random variable Y, f_X is a PDF of a random variable X, and $g^{-1}(y)$ is the inverse function. To apply this theorem to a random function $\tilde{S}(\Delta\varphi)$ defined by Eq. (16), we have to divide the domain of $\tilde{S}(\Delta\varphi)$ into intervals, where it is piecewise monotonic. Obviously, $\tilde{S}(\Delta\varphi)$ is monotonically decreasing in the intervals $\Delta\varphi \in I_{\downarrow}^{m} \equiv [2m\pi, (2m+1)\pi)$ (m is integer), whereas it is monotonically increasing in the intervals $\Delta\varphi \in I_{\uparrow}^{m} \equiv [(2m-1)\pi, 2m\pi)$ (we introduced here the notation $I_{\downarrow}^{m}$ and $I_{\uparrow}^{m}$ for the intervals of

monotonicity). In the intervals of monotonicity, there exist inverse functions, which we will denote as $\tilde{S}^{-1}_{I^m_\downarrow} \equiv \tilde{S}^{-1}_\downarrow(y)$ and $\tilde{S}^{-1}_{I^m_\uparrow} \equiv \tilde{S}^{-1}_\uparrow(y)$. It is easy to see from Eq. (16) that

$$\tilde{S}^{-1}_{\downarrow,\uparrow}(y) = \pm \arccos\left(\frac{2y - \tilde{S}_{\max} - \tilde{S}_{\min}}{\tilde{S}_{\max} - \tilde{S}_{\min}}\right) + 2\pi m, \tag{24}$$

where the "plus" sign refers to $\tilde{S}^{-1}_\downarrow$, and the "minus" sign refers to $\tilde{S}^{-1}_\uparrow$ (the value of the random variable $\tilde{S}$ we have denoted as y). According to Eq. (23), the PDF of a piecewise monotonic function defined in such a way can be written in the following form:

$$\tilde{f}^Q_{\tilde{S}} = \sum_{i=I^m_\downarrow, I^m_\uparrow} f_{\Delta\varphi}\left(\tilde{S}^{-1}_i\right)\left|\left(\tilde{S}^{-1}_i\right)'\right|, \tag{25}$$

where

$$(\tilde{S}^{-1}_{\downarrow,\uparrow})' \equiv \frac{d}{dy}\tilde{S}^{-1}_{\downarrow,\uparrow}(y) = \mp\left[\sqrt{(y - \tilde{S}_{\min})(\tilde{S}_{\max} - y)}\right]^{-1}, \tag{26}$$

and where the "minus" sign refers to the derivative of $\tilde{S}^{-1}_\downarrow$, whereas the "plus" sign refers to the derivative of $\tilde{S}^{-1}_\uparrow$. Substituting Eq. (26) into Eq. (25) and using Eqs. (22) and (24) we will obtain

$$\tilde{f}^Q_{\tilde{S}}(y) = \left[\sigma_\varphi\sqrt{2\pi(y - \tilde{S}_{\min})(\tilde{S}_{\max} - y)}\right]^{-1} \times \sum_{p=\pm1}\sum_{m=-\infty}^{+\infty} \exp\left[-\frac{1}{2\sigma^2_\varphi}\left(pa_y + 2\pi m - \Delta\theta\right)^2\right], \tag{27}$$

where we used the shorthand notation

$$a_y = \arccos\left(\frac{2y - \tilde{S}_{\max} - \tilde{S}_{\min}}{\tilde{S}_{\max} - \tilde{S}_{\min}}\right). \tag{28}$$

The sum in Eq. (27) converges to

$$\tilde{f}^Q_{\tilde{S}}(y) = \sum_{p=\pm1} \frac{J\left(\frac{pa_y}{2} - \frac{\Delta\theta}{2}, e^{-\sigma^2_\varphi/2}\right)}{2\pi\sqrt{(y - \tilde{S}_{\min})(\tilde{S}_{\max} - y)}}, \tag{29}$$

where $J(u, q)$ is the Jacobi θ function:

$$J(u, q) = 1 + 2\sum_{j=1}^{\infty} q^{j^2}\cos(2ju). \tag{30}$$

An important difference between PDFs given by Eqs. (18) and (29) is that the latter depends on $\Delta\theta$. The form of the $\tilde{f}^Q_{\tilde{S}}$ function at various values of $\Delta\theta$ for the cases $\sigma_\varphi = \pi/4, \pi/2, \pi$ is shown in Fig. 1, where it is assumed that $s_1 = s_2 = 1$ and $\eta = 1$. When $\sigma_\varphi = \pi/4$, the function $\tilde{f}^Q_{\tilde{S}}$ substantially differs from $f^Q_{\tilde{S}}$ at any value of $\Delta\theta$ [recall that the $f^Q_{\tilde{S}}$ function given by Eq. (18) is shown with the black dashed line]. The values $\Delta\theta = 0$ and $\Delta\theta = \pi$ yield in the substantial shift of the PDF into the region of constructive and destructive interference, respectively, whereas at $\Delta\theta = \pi/2$ the PDF exhibits a maximum at $\tilde{S} = 2$. When $\sigma_\varphi = \pi/2$, the shift is still clearly visible at $\Delta\theta = 0$ and $\Delta\theta = \pi$, whereas $\tilde{f}^Q_{\tilde{S}}$ and $f^Q_{\tilde{S}}$ become almost indistinguishable at $\Delta\theta = \pi/2$. Finally, when $\sigma_\varphi = \pi$, the $\tilde{f}^Q_{\tilde{S}}$ function is weakly dependent on $\Delta\theta$ and is almost indistinguishable from $f^Q_{\tilde{S}}$ at any value of $\Delta\theta$.

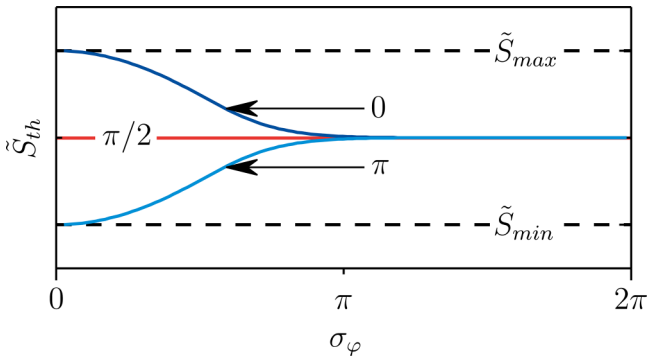

FIG. 2. Calculated dependences $\tilde{S}_{\text{th}}(\sigma_\varphi)$ for the three values of $\Delta\theta$: 0, $\pi/2$, and π.

Let us return to the definition of the QRF. At first glance, we are not prohibited from using formulas (20) and (21) in the case when σ_φ is quite small. The only difference here would be the dependence of the threshold value $\tilde{S}_{\text{th}}$ in Eq. (21) on both σ_φ and $\Delta\theta$. To clarify this, let us consider the calculated dependences $\tilde{S}_{\text{th}}(\sigma_\varphi)$ for the three values of $\Delta\theta$ shown in Fig. 2. One can see from the figure that $\tilde{S}_{\text{th}}$ is almost independent on both σ_φ and $\Delta\theta$ when $\sigma_\varphi > \pi$; in addition, the threshold value remains equal to $(\tilde{S}_{\max} + \tilde{S}_{\min})/2$ and does not depend on σ_φ, when $\Delta\theta = \pi/2$. However, $\tilde{S}_{\text{th}}$ differs significantly from $(\tilde{S}_{\max} + \tilde{S}_{\min})/2$ at smaller values of σ_φ, if $\Delta\theta$ is far from $\pi/2$. Thus, $\tilde{S}_{\text{th}} \to \tilde{S}_{\max}$ at $\Delta\theta = 0$ and $\tilde{S}_{\text{th}} \to \tilde{S}_{\min}$ at $\Delta\theta = \pi$ when σ_φ approaches zero. It seems that such a dependence of $\tilde{S}_{\text{th}}$ on σ_φ and $\Delta\theta$ should not affect the quantum noise extraction method itself since $\tilde{S}_{\text{th}}$ is explicitly included in the definition of Γ. Nevertheless, one can show that the use of Eqs. (20) and (21) is hardly possible when $\sigma_\varphi < \pi$.

The main reason for this statement is that $\tilde{f}^Q_{\tilde{S}}$ function averaged over $\Delta\theta$ becomes equal to $f^Q_{\tilde{S}}$:

$$\frac{1}{2\pi}\int_0^{2\pi} \tilde{f}^Q_{\tilde{S}}\, d(\Delta\theta) = f^Q_{\tilde{S}}. \tag{31}$$

It follows from Eq. (31) that an adversary may "mimic" the large-σ_φ PDF via controlling $\Delta\theta$, such that the user employing $f_{\tilde{S}}$ to monitor the contribution of classical noise will believe that he or she is still working with a quantum entropy source. In fact, the phase $\Delta\theta$ in the long arm of the interferometer should be considered as a "classical" parameter, which can be predicted or even controlled (at least in principle) by a third party. Indeed, since $\Delta\theta$ is related to the optical path difference of the interferometer arms, it is enough for an adversary to control the temperature near the device to gain insight into the value of the signal $\tilde{S}$. Thus, using the dependence of $\tilde{S}_{\text{th}}$ on $\Delta\theta$, an adversary may predict (with a probability different from 1/2) each bit of the random sequence digitized by a comparator when $\sigma_\varphi < \pi$.

In contrast, it can be shown that the PDF of the phase difference $\Delta\varphi$ may be assumed uniform with high accuracy when $\sigma_\varphi > 2\pi$; in other words, we may neglect the difference between $\tilde{f}^Q_{\tilde{S}}$ and $f^Q_{\tilde{S}}$ in this case. Indeed, inasmuch as $\Delta\varphi$ is in the argument of the cosine in Eq. (16), the Gaussian PDF

$f_{\Delta\varphi}$ from Eq. (22) may be substituted for $x \in [0, \pi)$ by the following one (see the Appendix in [12]):

$$\tilde{f}_{\Delta\varphi}(x) = \frac{1}{2\pi} \sum_{p=\pm 1} J\left(\frac{x}{2} + \frac{p\Delta\theta}{2}, e^{-\sigma_\varphi^2/2}\right) \tag{32}$$

and should be put to 0 when $x \notin [0, \pi)$. Here $J(u, q)$ is again the Jacobi θ function defined by Eq. (30). Inasmuch as $q < 1$ in this case, the series in Eq. (32) rapidly converges, so the value of the θ function may be estimated with just the two first terms: $J(u, q) \approx 1 + 2q\cos(2u)$, whence one can see that $J(u, q)$ deviates from 1 by a value $2q \sim 10^{-8}$ at $\sigma_\varphi = 2\pi$.

Thus, we may conclude that fluctuations of the phase difference $\Delta\varphi$ in Eq. (16) can be considered quantum when $\sigma_\varphi > 2\pi$, whereas they become highly sensitive to variations of $\Delta\theta$ when $\sigma_\varphi < \pi$ and cannot be used as a quantum entropy source. But what about the range from π to 2π? We may just look at Fig. 1 and Fig. 2 and repeat again that $\tilde{f}_{\tilde{S}}^{Q}$ is almost indistinguishable from $f_{\tilde{S}}^{Q}$, when σ_φ is in this range. At first sight, one may just soften the restriction imposed on the values of σ_φ and assume for simplicity that everything still works and the formulas (18), (20), and (21) are valid when $\sigma_\varphi > \pi$. Nevertheless, it would be useful to have a quantitative estimate for the difference between $\tilde{f}_{\tilde{S}}^{Q}$ and $f_{\tilde{S}}^{Q}$ when σ_φ is in the range from π to 2π and, if necessary, to modify the QRF in order to take into account the possible influence of an adversary.

3. Nonuniformity in terms of statistical distance

In the information theory, the difference between the two distributions, P_X and P_Y, is generally measured in terms of a statistical distance d, which for the countable set Ω of elementary events can be defined as follows [21]:

$$d = \frac{1}{2} \sum_{a \in \Omega} |P_X(a) - P_Y(a)|, \tag{33}$$

where $P_{X(Y)}(a)$ is a probability that the random variable $X(Y)$ takes a value a. By analogy with Eq. (33), the statistical distance between the PDFs $\tilde{f}_{\tilde{S}}^{Q}$ and $f_{\tilde{S}}^{Q}$ can be written in the form of the following integral:

$$d = \frac{1}{2} \int_{\tilde{S}_{\min}}^{\tilde{S}_{\max}} \left|\tilde{f}_{\tilde{S}}^{Q}(y) - f_{\tilde{S}}^{Q}(y)\right| dy, \tag{34}$$

where $\tilde{f}_{\tilde{S}}^{Q}$ and $f_{\tilde{S}}^{Q}$ are defined by Eqs. (29) and (18), respectively. It is not very convenient, however, to calculate numerically the integral in Eq. (34) since $\tilde{f}_{\tilde{S}}^{Q}$ and $f_{\tilde{S}}^{Q}$ have singularities at $\tilde{S}_{\min}$ and $\tilde{S}_{\max}$; therefore, it is reasonable to define d as a statistical distance between $\tilde{f}_{\Delta\varphi}$ and $f_{\Delta\varphi}$, namely,

$$d = \frac{1}{2} \int_0^\pi \left|\tilde{f}_{\Delta\varphi}(x) - \pi^{-1}\right| dx, \tag{35}$$

where $\tilde{f}_{\Delta\varphi}$ is defined by Eq. (32). One can check (e.g., numerically) that both definitions, Eqs. (34) and (35), are equivalent.

The dependence of the statistical distance defined by Eq. (35) on σ_φ and $\Delta\theta$ in the form of a color map is shown in Fig. 3(a). The slices of the map at different values of $\Delta\theta$ are shown in Fig. 3(b). First of all, it is clear that the statistical distance is highly sensitive to the value of $\Delta\theta$. Thus, d is at least seven orders of magnitude smaller at $\Delta\theta = \pi(m + 1/2)$ than at $\Delta\theta = \pi m$. In fact, one can see from Fig. 3(b) that $d \approx 10^{-9}$ at $\Delta\theta = \pi/2$ and $d \approx 10^{-2}$ at $\Delta\theta = 0$ when $\sigma_\varphi = \pi$. Another interesting feature is that the $d(\sigma_\varphi)$ curves are not significantly different from each other in the range of $\Delta\theta$ close to πm, whereas significant difference between them is clearly seen in the vicinity of $\Delta\theta = \pi(m + 1/2)$ [compare, e.g., curves at $\Delta\theta = 90°$ and $\Delta\theta = 89.9°$ in Fig. 3(b)]. It is also seen from Fig. 3(b) that the greatest value of d does not exceed 10^{-9} when $\sigma_\varphi > 2\pi$, which confirms that $f_{\Delta\varphi}$ can be considered uniform at these values of σ_φ. On the other hand, d has quite high values in the range of σ_φ between π and 2π, particularly when $\Delta\theta$ is close to πm. Random numbers obtained at such d cannot be considered enough random in terms of cryptographic security. Therefore, one should additionally improve the randomness of the digitized interference signal when $\pi < \sigma_\varphi < 2\pi$. As far as we know, such an analysis has not been yet carried out in the literature. In the next section, we show how this can be performed in terms of the QRF.

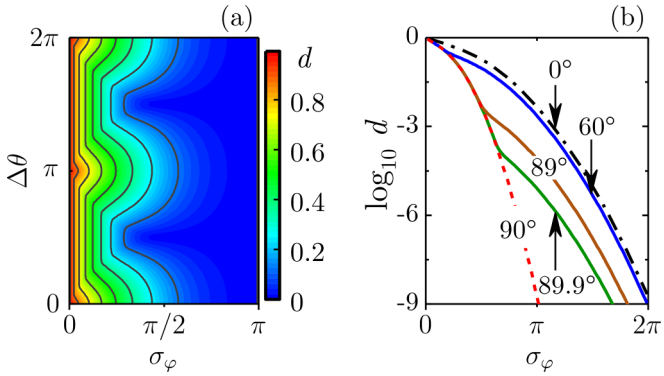

FIG. 3. The dependence of the statistical distance d defined by Eq. (35) on σ_φ and $\Delta\theta$ in the form of a color map (a). The slices of the map at different values of $\Delta\theta$ are shown in (b).

C. Improving randomness in the range $\pi < \sigma_\varphi < 2\pi$

The choice of the statistical distance as a measure of the deviation of $\tilde{f}_{\tilde{S}}^{Q}$ from $f_{\tilde{S}}^{Q}$ is also convenient because d is used in the definition of a randomness extractor and in the formulation of the leftover hash lemma (see below), which can be used to relate d with the QRF. To demonstrate this relation more consistently, let us first provide some necessary definitions.

Recall that the two distributions, P_X and P_Y, are called ε-close if their statistical distance defined by Eq. (33) does not exceed ε: $d \leqslant \varepsilon$. Roughly speaking, one can distinguish ε-close distributions only with the probability not exceeding ε, such that ε may be also considered as an error parameter. If a distribution P_X is ε-close to the uniform distribution, then P_X is referred to as quasiuniform. Recall further that a random variable X is called a k source (k is a some real number), if the min-entropy H_∞ of X does not exceed k or, equivalently, $P_X(x) \leqslant 2^{-k}$ for any value x of a random variable X. If the discrete random variable X is defined on a set of elementary events representing binary vectors of a length n, then such a set is denoted as $\Omega = \{0, 1\}^n$. Such a random variable is also called the (n, k) source, if X obeys the inequality

$H_\infty(X) \geqslant k/n$, where H_∞ is a min-entropy per bit. Thus, the random signal digitized with an eight-bit analog-to-digital converter (ADC) can be considered as an $(8, k)$ source if the min-entropy of the obtained binary sequence does not exceed k. Here the value of n in the definition of the (n, k) source was put to a bit resolution b of an ADC; however, the digitized random signal may be also grouped into much longer binary sequences with arbitrary n, which will be then considered as a random variable on $\{0, 1\}^n$ with $n > b$.

Using the above definitions, we may now give a strict definition of a (seeded) randomness extractor. Let us first recall that a *seed* is an additional random binary sequence with (quasi-) uniform distribution. Further, let there be an (n, k)-source X with distribution P_X and a seed having a uniform distribution on $\{0, 1\}^l$. Then the function $E(P_X)$: $\{0, 1\}^n \times \{0, 1\}^l \to \{0, 1\}^m$ is called a (k, ε) extractor if the resulting distribution on $\{0, 1\}^m$ is ε-close to uniform. Obviously, the length l of a seed should be quite small, or at least it should be shorter than the output, $l < m$, because otherwise the extractor would become trivial, i.e., it would be possible to output the seed itself.

Seeded randomness extractors are generally implemented via the so-called 2-universal hash functions, whose effectiveness is guaranteed by the leftover hash lemma (LHL) [21]. According to this lemma, the transformation $\{0, 1\}^n \to \{0, 1\}^m$ defined by a set of 2-universal hash functions and performed on the (n, k) source is a (k, ε) extractor if

$$m = k - 2\log_2(1/\varepsilon), \tag{36}$$

where ε is the required error parameter. The sense of this theorem can be roughly reformulated as follows. If there is a binary string of length n obtained from a weak entropy source, then one can extract m truly random bits with the use of a set of 2-universal hash functions, and the upper bound for m is the value of the min-entropy of the raw sequence. Generally, nH_∞ bits could be extracted from the raw sequence with a hypothetical ideal randomness extractor; however, according to the LHL, 2-universal hash functions allow extracting such a number of bits ($m = k = nH_\infty$) only with $\varepsilon = 1$, which does not guarantee the uniformity of the output sequence. In other words, the number of truly random bits that can be extracted with the use of 2-universal hash functions is less than nH_∞; however, we can guarantee the uniformity of the resulting distribution (up to the error parameter ε). In cryptographic applications, ε is chosen over a wide range of values: $\varepsilon \sim 10^{-10}$–$10^{-30}$.

Instead of the error parameter ε one can use the ratio between the lengths of the input and output binary sequences, which is sometimes referred to as a reduction factor: $\gamma = n/m$. Using the leftover hash lemma, one can easily find the relationship between ε and γ. Indeed, inserting $m = n/\gamma$ into Eq. (36) we will find

$$\varepsilon = 2^{-nr}, \tag{37}$$

where

$$r = \frac{k\gamma/n - 1}{2\gamma}. \tag{38}$$

In a similar way, we can find the relationship between the QRF and ε. However, it should be noted here that the raw binary sequence, obtained by digitizing (with a comparator) a random interference signal, is already uniform from the point of view of classical randomness (of course, with the proper choice of the threshold voltage on the comparator). Obviously, such a raw sequence does not require additional postprocessing; therefore, the LHL is not applicable here in the usual sense. That is why the definition of the QRF dispenses with LHL. Nevertheless, we can formally insert $m = n/\Gamma$ into Eq. (36) taking also into account that we are interested in quantum entropy, so that we should write $k = nH_\infty^Q = n$, which yields

$$\frac{n}{\Gamma} = n - 2\log_2(1/\varepsilon_c), \tag{39}$$

where we have introduced an effective error parameter ε_c, which is related with the contribution of classical noise and not with the nonuniformity of the raw binary sequence. One can easily find from Eq. (39) that

$$\varepsilon_c = 2^{-nR}, \tag{40}$$

where

$$R = \frac{\Gamma - 1}{2\Gamma}. \tag{41}$$

Continuing to develop this approach, we can use Eq. (39) to solve the problem indicated in the title of this section. First, we note that to consider the classical contribution from $\Delta\theta$ in $\tilde{S}$, it is necessary to increase the value of the QRF introducing a modified factor $\tilde{\Gamma}$, such that $\tilde{\Gamma} > \Gamma$ at $\sigma_\varphi \in [\pi, 2\pi]$ and $\tilde{\Gamma} = \Gamma$ at $\sigma_\varphi > 2\pi$. As was shown in the previous section, the statistical distance between $f_{\Delta\varphi}$ and the uniform distribution exhibits maximum when $\Delta\theta = \pi m$ [let us denote the corresponding value of d as $d_{\pi m}(\sigma_\varphi)$]; therefore, it makes sense to use $d_{\pi m}(\sigma_\varphi)$ as a parameter characterizing the nonuniformity of $f_{\Delta\varphi}$. Since we neglect the nonuniformity of $f_{\Delta\varphi}$ at $\sigma_\varphi > 2\pi$, it seems appropriate to determine the error parameter as

$$\varepsilon_Q \equiv \varepsilon_Q(\sigma_\varphi) = \frac{d_{\pi m}(2\pi)}{d_{\pi m}(\sigma_\varphi)}. \tag{42}$$

The modified quantum reduction factor $\tilde{\Gamma}$ can be then defined as follows:

$$\frac{n}{\tilde{\Gamma}} = n - 2\log_2(1/\varepsilon_c) - 2\log_2(1/\varepsilon_Q), \tag{43}$$

whence, using Eq. (40), we may find the relation between $\tilde{\Gamma}$ and Γ:

$$\tilde{\Gamma}(\sigma_\varphi) = \frac{n\Gamma}{n - 2\Gamma\log_2(1/\varepsilon_Q)}. \tag{44}$$

One can see from Eqs. (42) and (44) that $\varepsilon_Q = 1$ at $\sigma_\varphi = 2\pi$, so $\tilde{\Gamma}$ becomes equal to Γ. We may thus write for QRF:

$$\mathrm{QRF} = \begin{cases} \infty, & \sigma_\varphi < \pi; \\ \tilde{\Gamma}, & \sigma_\varphi \in [\pi, 2\pi]; \\ \Gamma, & \sigma_\varphi > 2\pi. \end{cases} \tag{45}$$

D. Stochastic rate equations

A fundamental noise source in the output of a laser is the quantum shot noise due to the random electron transitions producing spontaneous emission events [22–26]. Probability properties of spontaneous transitions are determined by their

relation to zero-point (vacuum) fluctuations of the electromagnetic field [27,28], which are generally considered to be perfectly uncorrelated and broadband. Therefore phase fluctuations in a semiconductor laser are generally assumed to have the same properties. It is sometimes argued that the description of quantum noise in a semiconductor laser should be performed with the method developed by Lax [29,30]. Namely, one should use a Markovian model for a set of atoms and a radiation field interacting with some reservoirs, which are defined mathematically by a set of damping constants and a set of noncommuting noise operators (quantum Langevin forces). In many cases, however, it is preferable to employ the simple model developed by Henry [22], who showed how the spontaneous emission should be incorporated into the classical field rate equation for a semiconductor laser, such that the drift and diffusion coefficients for the field intensity and the phase remained consistent with the fully quantum description. For our purposes, a standard system of laser rate equations with classical Langevin terms [1,22,26,31,32] is well suited; therefore, we will use here this approach. (See Appendix A for more details on stochastic rate equations we use here for simulations.)

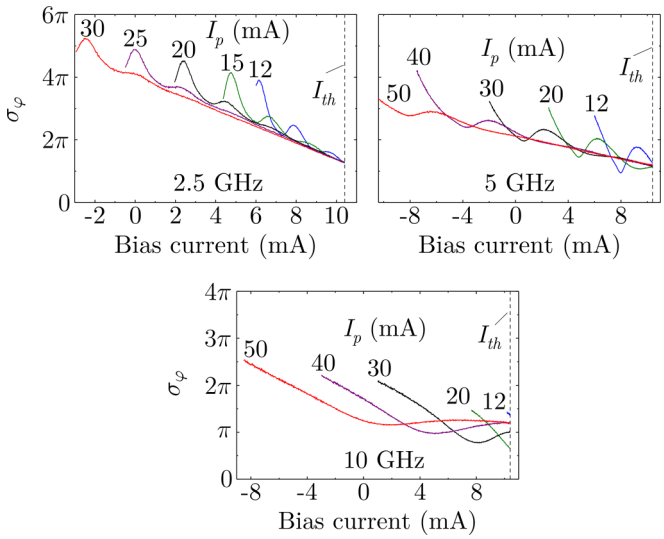

FIG. 4. Theoretical dependences of the phase diffusion standard deviation (σ_φ) on the bias current I_b and modulation current amplitude I_p at different pulse repetition rates.

E. Phase diffusion: Monte Carlo simulations

For the numerical study of the phase diffusion between the pulses of a single-mode gain-switched semiconductor laser, we performed Monte Carlo simulations of the phase evolution between adjacent optical pulses using Eq. (A16). The pump current was assumed to have a form of a square wave, $I(t) = I_b + I_p(t)$, where I_b is the bias current and $I_p(t)$ changed abruptly from 0 to I_p. We performed integration of Eq. (A16) from 0 to time T_p corresponding to a period of pulse repetition, i.e., the phase was allowed to diffuse during the time between two adjacent pulses. Initial conditions (N_0, Q_0 and φ_0) were chosen so that there were no transients. After each such integration, we obtained a value $\varphi(T_p)$ of a random phase, which exhibited Gaussian distribution, whose standard deviation we have denoted as $\sigma_\varphi(T_p) \equiv \sigma_\varphi$. Fifty iterations [random values of $\varphi(T_p)$] were found to be enough to find a value of σ_φ for given values of I_b, I_p and a given set of laser parameters. In Fig. 4 we present the dependence of σ_φ on the bias current I_b at different values of the pulse repetition rate $f_p = 1/T_p$; we used three different values of f_p: 2.5 GHz, 5 GHz, 10 GHz. At each pulse repetition rate, we calculated several curves corresponding to different values of I_p. For each I_p, we chose the range of the bias current variation from the value $I_b^{\min}$ corresponding to stable pulsation at a given I_p up to the threshold value defined by $I_{\text{th}} = N_{\text{th}} e/\tau_e$. The gain compression factor γ_P in Fig. 4 was put to 20 W^{-1}. Other laser parameters used in simulations are listed in Table I. In order to achieve high performance and reduce the computation time, we performed computations on a Compute Unified Device Architecture (CUDA) platform with the Nvidia video card equipped by a CUDA-powered graphics processing unit.

One can see from Fig. 4 that σ_φ increases towards lower values of the bias current. This reflects the fact that the number of carriers decreases faster at a lower pump current between laser pulses, which leads to a faster decrease of the field intensity inside the laser cavity and, consequently, to a faster decoherence due to spontaneous emission. An interesting feature here is a nonmonotonic behavior of $\sigma_\varphi(I_b)$ curves, which exhibit "damped oscillations." In Sec. IV we will discuss this result and provide an explanation of these "oscillations."

A comparison of simulations in Fig. 4 may also provide some insight into the dependence of σ_φ on the modulation frequency at fixed I_b and I_p. Thus, one can see that for $I_b = 8$ mA and $I_p = 30$ mA, the standard deviation of the phase diffusion decreases from $\sigma_\varphi \approx 1.9\pi$ at 2.5 GHz to $\sigma_\varphi \approx 1.4\pi$ at 5 GHz and to $\sigma_\varphi \approx 0.8\pi$ at 10 GHz. Although the dependence of σ_φ on the modulation frequency is complicated by the "oscillations," the general trend towards a decrease in σ_φ with an increase in f_p can be clearly seen. Note that this result should be used with caution, since in a real experiment, a change in the pulse repetition rate generally changes the peak-to-peak value of the modulation current (see the end of the Sec. III B 1), such that the increase of f_p may lead to a much more pronounced decrease of σ_φ.

TABLE I. Laser parameters used in simulations.

Parameter	Value
Photon lifetime τ_{ph}, ps	1.0
Electron lifetime τ_e, ns	1.0
Quantum differential output η	0.3
Transparency carrier number N_{tr}	6.0×10^7
Threshold carrier number N_{th}	6.5×10^7
Spontaneous emission coupling factor C_{sp}	10^{-5}
Confinement factor Γ	0.12
Linewidth enhancement factor α	6
Central lasing frequency $\omega_0/(2\pi)$, THz	193.548

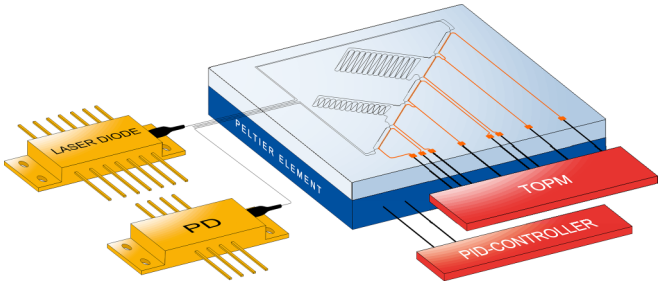

FIG. 5. Schematic representation of the experimental setup to measure phase diffusion in a gain-switched laser.

III. EXPERIMENT

A. Experimental setup description

An obvious way to measure the phase diffusion between pulses of a gain-switched laser is to measure the pulse interference using an unbalanced Mach-Zehnder interferometer (uMZI), whose time delay is chosen to be equal to the laser pulse repetition period. It should be noted that it is difficult to use a fiber-optic interferometer for phase diffusion measurements due to the temperature drift in the fiber. In fact, due to its relatively large size, it is quite problematic to stabilize it in temperature; therefore, thermal fluctuations may introduce significant errors to the measured values of σ_φ, especially if a measurement takes a long time. Also, it is difficult to make the fiber-optic delay line that would precisely correspond to a predetermined value of the pulse repetition rate using just a fiber fusion splicer. Because of this, we used an integrated uMZI, where it is quite simple to implement active temperature stabilization and to perform fine adjustment of the phase difference between the interferometer arms.

Schematic representation of the experimental setup used to measure phase diffusion between laser pulses is shown in Fig. 5. We employed the 1550 nm distributed feedback (DFB) laser module (Gooch & Housego, AA0701) of 12 Gbps modulation bandwidth. The bias current was controlled by the high-stability laboratory power supply, whereas modulation signals of 2.5 and 1.25 GHz were generated by a phase-locked loops followed by a broadband amplifier. The optical signal was detected with the InGaAs fixed gain amplified detector (Thorlabs, PDA8GS) of 9.5 GHz bandwidth (PD in Fig. 5), and the signal processing was performed using the Teledyne Lecroy digital oscilloscope (WaveMaster 808Zi-A) with 8 GHz bandwidth and temporal resolution of 25 ps.

The laser diode with the polarization-maintaining fiber output was coupled to the photonic integrated circuit (PIC) containing a cascade of uMZIs. For simplicity, we present in Fig. 5 only two uMZIs with delay lines of 400 and 800 ps. The PIC contained also additional balanced MZIs (three of them are shown in Fig. 5), which were used to control the splitting ratios of the interferometers, as well as to choose the uMZI with the desired delay line. Each MZI on the chip was equipped by a thermo-optical phase modulator (TOPM) in the form of a resistive heater (a metal band) deposited over a waveguide corresponding to one of the interferometer arms. Heaters were controlled via a multichannel digital-to-analog converter (DAC) indicated as a TOPM controller in Fig. 5.

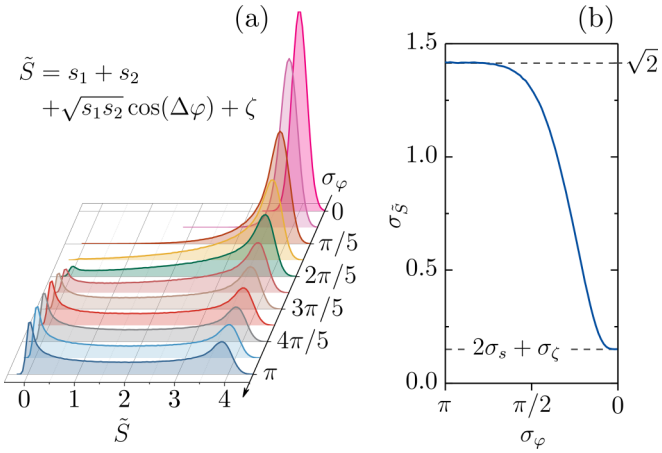

FIG. 6. Theoretical dependence of the probability density function of the normalized interference signal $\tilde{S}$ [Eq. (16)] on the standard deviation of phase fluctuations σ_φ (a) and the corresponding dependence of its standard deviation $\sigma_{\tilde{S}}$ (b).

To set the desired configuration of DAC voltages, we applied to the laser a low-frequency (312.5 MHz) modulation signal, which yielded in a train of short laser pulses with the repetition period of 3.2 ns. We then set up the controller so that each of these pulses was split at the output of the chip into a pair of pulses of the same intensity. The time delay between the pulses in a pair was set either to 400 ps or to 800 ps depending on the choice of the delay line. (Some details concerning the control over delay lines are given in Appendix B.)

To maintain a stable temperature, the chip was mounted on the Peltier thermoelectric cooler controlled by a commercially available temperature controller (PID controller in Fig. 5). Note that the Peltier element can be used along with TOPMs to control the phase difference between the interferometer arms; moreover, the change in the chip temperature allowed for much greater modulation depth than resistive heaters, although the latter allowed for much faster phase modulation (up to several kilohertz). Since for our experiments there was no need to change the phase with such a frequency, we used the Peltier element to vary the phase in the interferometer arms.

B. Phase diffusion measurements

The main object of measurements in our experiments was the probability density function of laser pulse interference $f_{\tilde{S}}$. Before proceeding to the study of experimental PDFs, it seems appropriate to simulate the interference statistics. For simulations, we used Eq. (16) with $\eta = 1$, and random amplitudes s_1, s_2 with Gaussian PDFs: $\bar{s}_1 = \bar{s}_2 = 1$ and $\sigma_s = 0.05$. The same value of the standard deviation was assumed for the additive Gaussian noise: $\sigma_\zeta = 0.05$. We varied the standard deviation of phase diffusion σ_φ from π to 0 with a step of $\pi/10$. The theoretical evolution of the interference PDF with such a change of σ_φ is shown in Fig. 6(a). One can see that when σ_φ is close to π, the PDF has two pronounced maxima near $\tilde{S} = 0$ and $\tilde{S} = 4$ with the left maximum noticeably thinner and higher than the right one. When decreasing σ_φ (and assuming that the phase change $\Delta\theta$ in the interferometer is

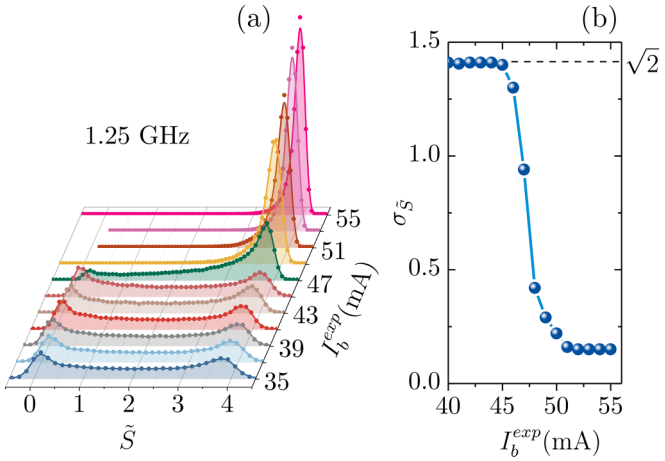

FIG. 7. Experimental dependence of the probability density function of the normalized interference signal $\tilde{S}$ on the bias current $I_b^{\rm exp}$ (on the left) and the corresponding dependence of its standard deviation $\sigma_{\tilde{S}}$ (on the right) at pulse repetition frequency $f_p = 1.25$ GHz.

zero), the right maximum of the PDF starts to grow, and when σ_φ tends to zero, the PDF turns into Gaussian curve with standard deviation equal to $2\sigma_s + \sigma_\zeta$. Corresponding evolution of $\sigma_{\tilde{S}}$ (standard deviation of $f_{\tilde{S}}$) is shown in Fig. 6(b): when $\sigma_\varphi > \pi$, $\sigma_{\tilde{S}}$ tends to the value $\sigma_{\tilde{S}} = \sqrt{2}$, which corresponds to the standard deviation of the quantum PDF $f_{\tilde{S}}^{Q}$ defined by Eq. (18).

1. Experimental PDFs

Figures 7 and 8(a) show experimental statistics of the normalized interference signal, which were recorded as histograms with the oscilloscope at a laser pulse repetition rate of 1.25 and 2.5 GHz, respectively, at various bias currents $I_b^{\rm exp}$ (the procedure of normalization is explained in Appendix C). As was shown in Sec. II E (see Fig. 4), at sufficiently high values of the modulation current ($I_p > 30$ mA) and not very

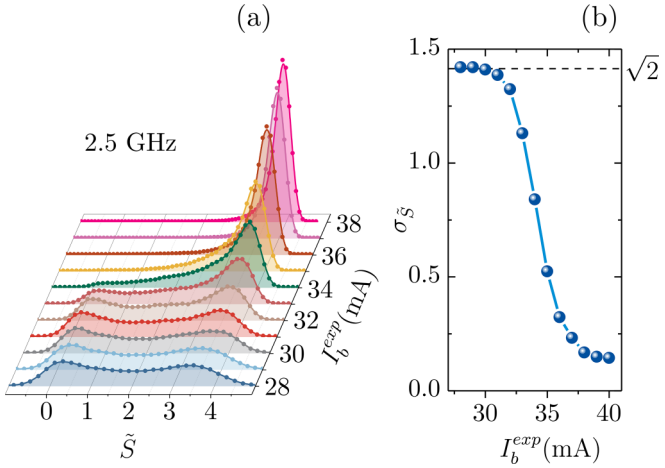

FIG. 8. Experimental dependence of the probability density function of the normalized interference signal $\tilde{S}$ on the bias current $I_b^{\rm exp}$ (a) and the corresponding dependence of its standard deviation $\sigma_{\tilde{S}}$ (b) at pulse repetition frequency $f_p = 2.5$ GHz.

high values of the pulse repetition frequency ($f_p < 5$ GHz), σ_φ below the 2π value decreases linearly when increasing the bias current I_b. So we may consider that the linear increase of the bias current in the experiment is equivalent to a linear decrease in σ_φ.

One can see that experimental PDFs repeat the evolution shown in Fig. 6. Note, however, that experimental statistics (particularly in case of short optical pulses without spectral filtering) is generally affected by the "chirp + jitter" effect [20]. Therefore, to achieve a good correspondence between theoretical and experimental PDFs, we put the optical filter between the interferometer output and the photodetector. (We used the Santec OTF-980 optical tunable filter; the bandpass was put to 6.25 GHz.)

When performing simulations in Fig. 4, it was convenient to define the bias current I_b as the minimum value of the pump current. (The peak-to-peak value I_p of the modulation current was "measured" from I_b.) However, in the experiment, it was convenient to define the pump current as $I^{\rm exp}(t) = I_b^{\rm exp} + I_p^{\rm exp}(t)$, where $I_p^{\rm exp}(t)$ is changed from $-I_p^{\rm exp}/2$ to $I_p^{\rm exp}/2$. In this case, the minimum value of the pump current is $I_b^{\rm exp} - I_p^{\rm exp}/2$. In Fig. 7 the pump current axes are plotted in terms of $I_b^{\rm exp}$.

The dependences of the standard deviation $\sigma_{\tilde{S}}$ of the normalized signal $\tilde{S}$ on the bias current at $f_p = 1.25$ and $f_p = 2.5$ GHz are shown in Figs. 7 and 8(b). (For each value of $I_b^{\rm exp}$ we set $\Delta\theta = 0$ by adjusting the temperature of the interferometer.) One can see that the experimental dependences $\sigma_{\tilde{S}}(I_b^{\rm exp})$ are in a good agreement with the theoretical dependence $\sigma_{\tilde{S}}(\sigma_\varphi)$ shown in Fig. 6. Comparing theoretical dependence $\sigma_{\tilde{S}}(\sigma_\varphi)$ in Fig. 6 with experimental dependences $\sigma_{\tilde{S}}(I_b^{\rm exp})$ in Figs. 7 and 8, one can easily estimate (just by eye) what value of the bias current approximately corresponds to $\sigma_\varphi = \pi/2$ [at this value the curve $\sigma_{\tilde{S}}(I_b^{\rm exp})$ starts to bend] and to $\sigma_\varphi = \pi$ [at this value the curve $\sigma_{\tilde{S}}(I_b^{\rm exp})$ reaches the maximum].

We can also employ the $\sigma_{\tilde{S}}(I_b^{\rm exp})$-curves to estimate the peak-to-peak value of the modulation current. In fact, the bend in these curves in Figs. 7 and 8(b) occurs when $I_b^{\rm exp} - I_p^{\rm exp}/2 = I_{\rm th}$. The threshold current $I_{\rm th}$ of our laser was approximately 10 mA, so, at 1.25 GHz we had $I_p^{\rm exp} \approx 70$ mA, whereas at 2.5 GHz we had $I_p^{\rm exp} \approx 40$ mA.

2. Interference fringes

A more accurate estimate of σ_φ can be obtained by analyzing conventional interference fringes (the dependences of the mean value $\langle\tilde{S}\rangle$ on the phase change $\Delta\theta$ in the interferometer) and by investigating the curves $\sigma_{\tilde{S}}(\Delta\theta)$, which we refer here to as $\sigma_{\tilde{S}}$ fringes or *statistical* interference fringes. To measure fringes at a given value of the bias current, we varied the temperature of the interferometer (with the step of 10 mK for the delay line of 800 ps and with the step of 20 mK for the delay line of 400 ps) and for each temperature recorded the PDF. The result of such measurements at $f_p = 1.25$ GHz for $I_b^{\rm exp} = 54$ mA is shown in Fig. 9 as an example. Experimental fringes extracted from these data at some selected values of the bias current are shown in Fig. 10 for $f_p = 1.25$ GHz and in Fig. 11 for $f_p = 2.5$ GHz.

It can be easily shown [13,33] that standard deviation of the phase diffusion σ_φ can be calculated via the relation

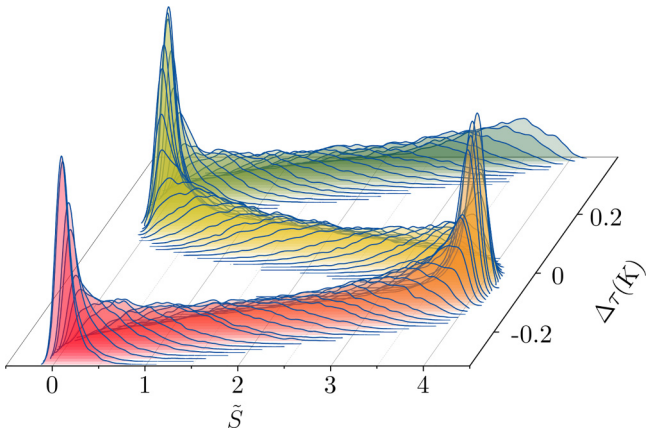

FIG. 9. An example of measured probability density function of the laser pulse interference as a function of the interferometer temperature. Pulse repetition rate was 1.25 GHz; the bias current was $I_b^{\rm exp} = 54$ mA. The temperature shift $\Delta\tau$ was measured with respect to 300 K.

$\sigma_\varphi = \sqrt{-2\ln\eta}$, where η is the visibility of the pulse interference. Visibility, in turn, can be obtained by fitting interference fringes (filled circles in Figs. 10 and 11) with the formula $\langle\tilde{S}\rangle = 2[1 + 2\eta\sin(\Delta\theta + \varphi_0)]$, where φ_0 is an auxiliary fitting parameter, which allows taking into account the "initial phase" of the fringe. However, we will use here another approach; namely, we will perform the joint fit of both $\langle\tilde{S}\rangle$ and $\sigma_{\tilde{S}}$ dependences on $\Delta\theta$ with the use of Eqs. (16) and (22). The main advantage of such an approach is that it allows determining not only σ_φ but also σ_s (standard deviation of normalized laser pulse intensity fluctuations). In the context of a QRNG, this is extremely useful because intensity fluctuations are generally treated as classical noise, which should be properly taken into account when extracting quantum noise from the interference of laser pulses. The result of the joint fit for each pair of curves is shown in Figs. 10 and 11 with solid red lines.

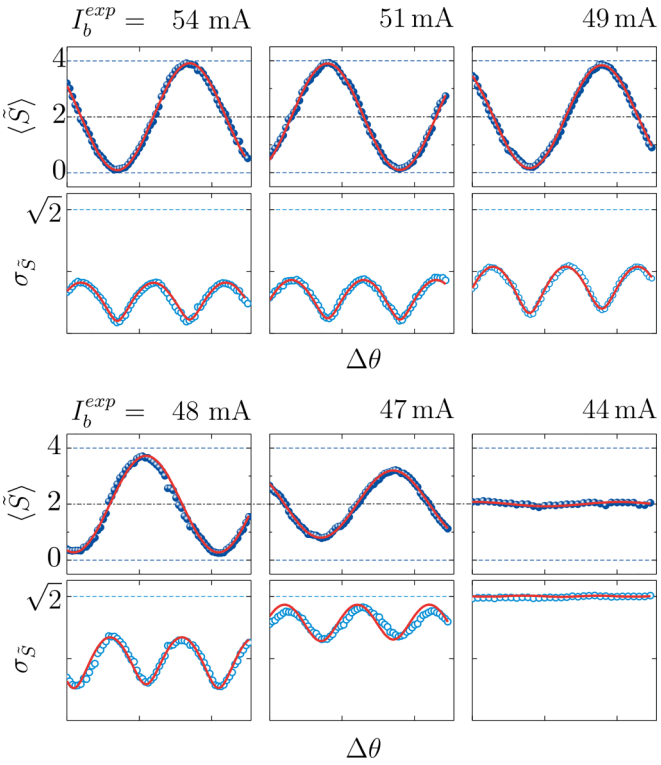

FIG. 10. Experimental dependences of the mean value $\langle\tilde{S}\rangle$ of the interference signal on the phase shift $\Delta\theta$ (filled circles) and corresponding statistical interference fringes $\sigma_{\tilde{S}}(\Delta\theta)$ (empty circles) at pulse repetition frequency of 1.25 GHz. In all panels one division on the $\Delta\theta$ axis equals to π.

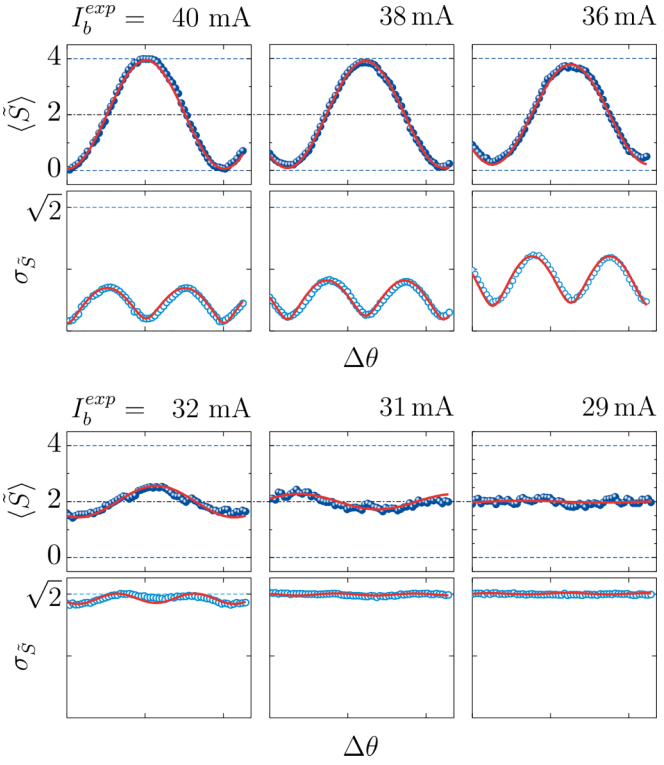

FIG. 11. Experimental dependences of the mean value $\langle\tilde{S}\rangle$ of the interference signal on the phase shift $\Delta\theta$ (filled circles) and corresponding statistical interference fringes $\sigma_{\tilde{S}}(\Delta\theta)$ (empty circles) at pulse repetition frequency of 2.5 GHz. In all panels one division on the $\Delta\theta$ axis equals to π.

Statistical interference fringes differ significantly from the sinusoid and cannot be generally fitted as conventional interference fringes. Particularly, they may exhibit different depth of a dip at constructive and destructive interference, which is clearly seen in some experimental curves (see, e.g., the curve in Fig. 10 at $I_b^{\rm exp} = 49$ mA). (To demonstrate that this is not related to experimental imperfections, we plotted some theoretical statistical fringes in Fig. 14 in Appendix D.)

The results obtained by fitting the curves in Figs. 10 and 11 are presented in Fig. 12. As was discussed above, experimental PDFs at various values of σ_φ (or rather at various values of $I_b^{\rm exp}$) are almost indistinguishable when $\sigma_\varphi > \pi$; therefore, we may measure the standard deviation of phase diffusion with acceptable precision only when $\sigma_\varphi < \pi$. However, assuming linear evolution of σ_φ and σ_s with $I_b^{\rm exp}$ (at least in the range from π to 2π), we may always extrapolate these dependences as shown in Fig. 12 with dashed lines.

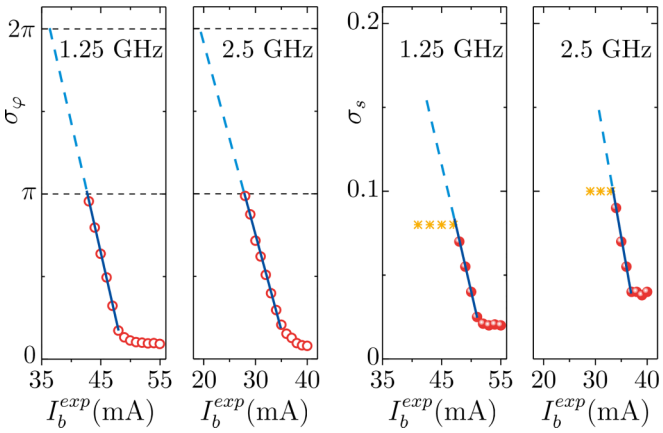

FIG. 12. Experimentally measured standard deviations of phase diffusion (σ_φ) and normalized pulse intensity fluctuations (σ_s) as functions of the bias current at 1.25 and 2.5 GHz of pulse repetition rate. Orange asterisks denote values of σ_s that were used when fitting $\sigma_{\tilde{S}}$ fringes at $I_b^{\rm exp} < 47$ mA (for 1.25 GHz) and $I_b^{\rm exp} < 33$ mA (for 2.5 GHz).

IV. DISCUSSION

In the context of a QRNG, the main result of the phase diffusion measurements is dependences $\sigma_\varphi(I_b^{\rm exp})$ and $\sigma_s(I_b^{\rm exp})$ shown in Fig. 12. These dependences clearly show what $I_b^{\rm exp}$ values should be used to ensure that interference of laser pulses acts as uncorrelated quantum entropy source. We see from Fig. 12 that for 1.25 GHz the bias current values $I_b^{\rm exp} >$ 43 mA yield $\sigma_\varphi < \pi$. According to Eq. (45), this means that the phase between neighboring laser pulses correlates significantly, such that these pulses cannot be used for QRNG. In the range between 43 and 37 mA, σ_φ belongs to the range $[\pi, 2\pi]$, such that we should use the factor $\tilde{\Gamma}$ [Eq. (44)] for randomness extraction. Finally, when $I_b^{\rm exp} < 37$ mA, we may neglect any phase correlations between laser pulses and assume that $f_{\Delta\varphi}$ is uniform, which allows employing the factor Γ from Eq. (20). At 2.5 GHz the laser should be employed at values $I_b^{\rm exp} < 28$ mA: between 19 and 28 mA we should use the QRF $\tilde{\Gamma}$, whereas at $I_b^{\rm exp} < 19$ mA one may use Γ.

Equally important are dependencies $\sigma_s(I_b^{\rm exp})$. As was shown in [12], experimental estimation of the QRF is hampered by the fact that the definition of the min-entropy [Eq. (21)] contains the quantity $\tilde{S}_{\rm min}$, which is difficult to determine in practice. It was therefore proposed to determine Γ via precalculated curves $\Gamma(B)$, where B is defined by the following ratio:

$$B = \frac{\text{whole PDF width}}{\text{distance between PDF maxima}}. \tag{46}$$

The curve $\Gamma(B)$ can be computed with the use of Eqs. (16) and (17) in assumption of a certain value of σ_s. Experimentally measured dependencies $\sigma_s(I_b^{\rm exp})$ thus allow computing proper dependencies $\Gamma(B)$.

The nature of the damped oscillations in theoretical curves $\sigma_\varphi(I_b)$ in Fig. 4 can be understood by referring to the work of Henry [34], where the author provides an explanation for the additional peaks appearing in a spectrum of a semiconductor laser. The satellite peaks were related to the time dependence of the mean square phase change $\langle\Delta\varphi^2\rangle$, which, in addition to a linear dependence, exhibits damped periodical variations caused by relaxation oscillations. It was shown that

$$\langle\Delta\varphi^2\rangle \propto \exp(-\gamma_d t)\cos(\omega_r t - 3\delta), \tag{47}$$

where γ_d and ω_r are the damping rate and the angular frequency of relaxation oscillations, respectively, and $\cos\delta = \omega_r/\sqrt{\omega_r^2+\gamma_d^2}$. Obviously, the quantity σ_φ we have considered so far corresponds to $\sqrt{\langle\Delta\varphi^2\rangle}$; however, the mean square phase change $\langle\Delta\varphi^2\rangle$ in Eq. (47) was derived for the continuous wave lasing (i.e., above threshold), whereas the standard deviation plotted in Fig. 4 was calculated for the "large signal." In other words, σ_φ in Fig. 4 contains the evolution of the phase below threshold (when the laser does not emit) as well as above threshold (when the laser emits the pulse). We may thus divide σ_φ into two parts: the one part is related to the phase evolution below threshold and should decrease monotonically with the increase of I_b, whereas the second part is related to the phase diffusion above threshold (during the laser pulse emission) and should exhibit oscillations according to Eq. (47). In fact, increase of the bias current leads to the increase of the laser pulse duration, which is equivalent to the increase of time t in Eq. (47). So damped oscillation in the $\sigma_\varphi(I_b)$ curves is driven by the competition between the oscillating growth of $\langle\Delta\varphi^2\rangle$ with I_b during laser pulse emission and monotonic decrease of $\langle\Delta\varphi^2\rangle$ with I_b between laser pulses. At sufficiently high values of I_b, when the width of the laser pulse becomes approximately equal to the width of the electric pulse and thus ceases to grow with increasing I_b, the dependence $\sigma_\varphi(I_b)$ becomes monotonically decreasing.

V. CONCLUSIONS

In this work we provided a general description of a quantum entropy source based on the interference of laser pulses. We have considered in detail the different modes of laser pulse interference and have shown that the interference signal remains quantum in nature even in the presence of classical phase drift in the interferometer if the phase diffusion obeys the relation $\sigma_\varphi > 2\pi$. In other words, correlations between lasers pulses are absent if this inequality holds. We also emphasize that the influence of jitter as a source of classical noise can be neglected for large as well as for small values of σ_φ. In the former case, the classical noise of jitter is buried under the quantum noise, whereas in the latter case, laser pulses should be considered "cut out" from a continuous quasimonochromatic wave, for which the effect of jitter on the phase evolution is absent.

From an experimental point of view, the optimal mode of operation of a semiconductor laser in a quantum random number generator is achieved by using the lowest possible bias current, I_b, and the highest possible modulation current, I_p, for which the laser may generate pulses of the required intensity. At not very high pulse repetition rates (<2–3 GHz) and with laser drivers providing high enough modulation currents ($I_p \sim$ 70–100 mA), such a choice automatically provides efficient phase diffusion, which allows neglecting interpulse correlations. Insufficiently high values of the modulation cur-

rent do not allow the use of high pulse repetition rates due to an insufficient delay between subsequent pulses and the requirement to use small bias currents (or even the reverse-biased laser diode). As a first approximation for estimating phase diffusion, one can use the PDF of the interference signal: if the form of the PDF does not vary when changing the bias current, then one can definitely conclude that $\sigma_\varphi > \pi$. If it is suspected that available modulation current does not allow reaching the desired value of σ_φ, one may use techniques described in Sec. III to estimate it experimentally.

We have explicitly formulated the relationship between the previously introduced quantum reduction factor [12] and the leftover hash lemma, which allows us to develop a method to estimate the quantum noise contribution to the interference signal when $\pi < \sigma_\varphi < 2\pi$. With this approach, even in the presence of (partial) interpulse correlations, one can use laser pulse interference as a quantum entropy source with reduced entropy rate determined by the modified quantum reduction factor $\tilde{\Gamma}$. Also, in addition to conventional interference fringes, we proposed to use statistical interference fringes to obtain more detailed information about the probabilistic properties of laser pulse interference. We hope that the theoretical and experimental results presented here will be useful for the developers of QRNGs and may also help in the preparation of probabilistic models necessary for the certification of such devices.

ACKNOWLEDGMENTS

We are grateful to A. Losev and V. Zavodilenko for assistance in the development of the laser driver and to A. Udaltsov for the development of the TOPM controller.

APPENDIX A: DERIVATION OF STOCHASTIC RATE EQUATIONS

According to Henry [22], a spontaneous emission event is described as a randomly occurring increase of the field amplitude and an accompanying random change in the phase φ of the optical field. The complex field amplitude $E(t)$ is assumed to increase by ΔE_k, which has an absolute value equal to 1 and the phase $\varphi + \theta_k$, i.e., $\Delta E_k = \exp[i(\varphi + \theta_k)]$, where θ_k is a random angle. Note that the electric field E is assumed here to be normalized such that its absolute square corresponds to the average photon number Q inside the laser cavity: $Q = |E|^2$ or $E = \sqrt{Q}\exp(i\varphi)$. It is important to emphasize that despite its correspondence to the average photon number, the quantity should be referred to as a *normalized intensity* rather than to as a photon number, $N_{\rm ph}$. This feature is not relevant when considering dynamics of averaged quantities since $\langle Q\rangle = \langle N_{\rm ph}\rangle$ (here angular brackets denote ensemble averaging); however, it becomes relevant when considering stochastic equations, inasmuch as $N_{\rm ph}$ and Q have different distributions and diffusion coefficients [26].

It is assumed that different events producing the change ΔE_k are uncorrelated, such that the spontaneous emission noise $F_E(t)$ may be written as a sequence of δ pulses:

$$F_E(t) = \sum_k \Delta E_k \delta(t - t_k) \tag{A1}$$

with uncorrelated t_k. The rate of these events obviously corresponds to the average rate of radiative spontaneous emission into the lasing mode, which can be written as $C_{\rm sp}R_{\rm sp}$, where $R_{\rm sp}$ is the total average rate of radiative spontaneous emission and the $C_{\rm sp}$ factor corresponds to the fraction of spontaneously emitted photons that end up in the active mode under consideration. According to a general approach, the spontaneous emission noise may be introduced just by adding the complex Langevin force $F_E(t)$ to the right-hand side of the single-mode laser rate equation for the complex slowly varying electric field amplitude [1,22,26,31,32]:

$$dE = \frac{1}{2\tau_{\rm ph}}(1 + i\alpha)(G_L - 1)E\,dt + F_E(t)\,dt, \tag{A2}$$

where α is the linewidth enhancement factor (the Henry factor [22]), $\tau_{\rm ph}$ corresponds to the inverse decay rate of the field intensity and is generally treated as a photon lifetime, and the normalized dimensionless linear gain $G_L = (N - N_{\rm tr})/(N_{\rm th} - N_{\rm tr})$ depends on the carrier number N, where $N_{\rm tr}$ and $N_{\rm th}$ are the carrier numbers at transparency and threshold, respectively. According to Eq. (A1), $F_E(t)$ satisfies the general relations

$$\langle F_E(t)\rangle = 0, \quad \langle F_E(t)F_E(t-\tau)\rangle = 0 \tag{A3}$$

and

$$\langle F_E(t)F_E^*(t-\tau)\rangle = 2D_{EE}\delta(\tau), \tag{A4}$$

where the asterisk means the complex conjugate. To determine the coefficient D_{EE} one should compute $\langle F_E(t)F_E^*(u)\rangle$, where $u = t - \tau$. According to Eq. (A1), this quantity is the product of two sums of δ functions, where all cross terms are zero since $\delta(t - t_k)\delta(u - t_l)$ is zero unless $t_k = t_l$; hence

$$F_E(t)F_E^*(u) = \sum_k \delta(t - u)\delta(u - t_k). \tag{A5}$$

Finally, the averaging can be performed by replacing $\sum_k$ in Eq. (A5) by $C_{\rm sp}R_{\rm sp}\int dt_k$. Thus, we have after averaging

$$\langle F_E(t)F_E^*(t-\tau)\rangle = C_{\rm sp}R_{\rm sp}\delta(\tau). \tag{A6}$$

Comparing this to Eq. (A4) we obtain $2D_{EE} = C_{\rm sp}R_{\rm sp}$, such that we can write

$$F_E = \sqrt{\frac{C_{\rm sp}R_{\rm sp}}{2}}(\xi_1 + i\xi_2), \tag{A7}$$

where ξ_1 and ξ_2 are independent random variables representing the normalized white Gaussian noise and obey the following relations:

$$\langle \xi_i(t)\rangle = 0, \quad \langle \xi_i(t)\xi_j(t-\tau)\rangle = \delta_{ij}\delta(\tau). \tag{A8}$$

Writing the normalized electric field as $E = x_1 + ix_2$ and separating the real and imaginary parts of Eq. (A2) we will obtain the following system:

$$\begin{aligned} dx_1 &= h_1 dt + g_{11}\xi_1\,dt + g_{12}\xi_2\,dt, \\ dx_2 &= h_2 dt + g_{21}\xi_1\,dt + g_{22}\xi_2\,dt, \end{aligned} \tag{A9}$$

where

$$h_1 = \frac{1}{2\tau_{\rm ph}}(G_L - 1)x_1 - \frac{\alpha}{2\tau_{\rm ph}}(G_L - 1)x_2,$$
$$h_2 = \frac{1}{2\tau_{\rm ph}}(G_L - 1)x_2 + \frac{\alpha}{2\tau_{\rm ph}}(G_L - 1)x_1, \qquad \text{(A10)}$$
$$g_{11} = g_{22} = \sqrt{\frac{C_{\rm sp}R_{\rm sp}}{2}}, \quad g_{12} = g_{21} = 0.$$

Introducing variables x_1' and x_2' by the relations

$$x_1' = u_1(x_1, x_2) \equiv Q = x_1^2 + x_2^2,$$
$$x_2' = u_2(x_1, x_2) \equiv \varphi = \arctan(x_2/x_1), \qquad \text{(A11)}$$

and using the Itô formula [35] written for our case as

$$dx'_i = \left(\frac{\partial u_i}{\partial t} + \sum_{k=1}^{2} h_k \frac{\partial u_i}{\partial x_k} + \frac{1}{2}\sum_{j=1}^{2}\sum_{k,m=1}^{2} g_{mj}g_{kj}\frac{\partial^2 u_i}{\partial x_m \partial x_k}\right)dt$$
$$+ \sum_{j=1}^{2}\sum_{k=1}^{2} g_{kj}\frac{\partial u_i}{\partial x_k}\,dW_j, \qquad \text{(A12)}$$

we will obtain the following set of stochastic rate equations:

$$dQ = (G_L - 1)\frac{Q}{\tau_{\rm ph}}dt + C_{\rm sp}R_{\rm sp}\,dt + F_Q\,dt,$$
$$d\varphi = \frac{\alpha}{2\tau_{\rm ph}}(G_L - 1)dt + F_\varphi\,dt \qquad \text{(A13)}$$

with

$$F_Q\,dt = \sqrt{2C_{\rm sp}R_{\rm sp}Q}[\cos(\varphi)\,dW_1 + \sin(\varphi)\,dW_2],$$
$$F_\varphi\,dt = \sqrt{\frac{C_{\rm sp}R_{\rm sp}}{2Q}}[\cos(\varphi)\,dW_2 - \sin(\varphi)\,dW_1], \qquad \text{(A14)}$$

where W_1, W_2 are two independent Wiener processes, which may be defined via the notation $dW_1 = \xi_1\,dt$ and $dW_2 = \xi_2\,dt$. [It should be remembered, however, that the Wiener process $W(t)$ is nowhere differentiable, so the equality $dW(t) = \xi(t)\,dt$ cannot be treated as a differential in the usual sense, and it is better to consider it just as a symbolic notation [35].]

Since the gain G_L depends on the carrier number N, Eqs. (A13) should be supplemented by the rate equation for N. If one can neglect carrier diffusion effects, such as in index-guided lasers, the rate equation for the carrier number can be written in the following form:

$$dN = \frac{I}{e}\,dt - \frac{N}{\tau_e}\,dt - \frac{G_L Q}{\Gamma\tau_{\rm ph}}\,dt + F_N\,dt, \qquad \text{(A15)}$$

where I is the pump current, e is the absolute value of the electron charge, τ_e is the effective carrier lifetime, and Γ is the confinement factor, which can be estimated as a ratio between the cross-sectional areas of the transverse mode and the active layer. We also added in Eq. (A15) the Langevin force F_N, which drives fluctuations of N; however, due to relatively short (∼1 ns) carrier lifetime, perturbations to the carrier density do not persist long enough to make significant low-frequency contributions, while at higher frequencies they are damped by diffusion [36]. Therefore, carrier fluctuations are usually assumed to be negligible when modeling stochastic properties of laser radiation. We will thus assume below that $F_N = 0$.

Finally, rate equations for N and Q should be modified to take into account the gain saturation [37,38]. This can be performed by substituting G_L by $G = G_L/\sqrt{1 + 2\gamma_Q Q} \approx G_L(1 - \gamma_Q Q)$, where γ_Q is the dimensionless gain compression factor. (The rate equation for the phase is generally left unchanged.) Sometimes, it is more convenient to use instead of γ_Q the gain compression factor γ_P related to the output optical power P, which can be defined as $\gamma_P = 2\gamma_Q\Gamma\tau_{\rm ph}/(\eta_d\hbar\omega_0)$, where η_d is the differential quantum output (don't confuse it with visibility, for which we used similar notation above), and $\hbar\omega_0$ is the photon energy. For typical semiconductor lasers, γ_P may reach a few dozens of W^{-1} [20]; here we will assume that it is in the range 10–40 W^{-1}.

The system of stochastic differential equations (SDEs) (A13) and (A15) with stochastic terms given by Eq. (A14) can be solved numerically with the Euler-Maruyama method [35], which is the simplest time discrete approximation used for integration of SDEs. In this method, each component of the solution of the vector-valued SDE is approximated by a continuous time stochastic process defined via the iterative scheme with the time differential dt substituted by the conventional time increment $\Delta = t_{n+1} - t_n$ and the independent "differentials" dW_1 and dW_2 approximated by the increments $\Delta W_{1,2} = W_{1,2}(t_{n+1}) - W_{1,2}(t_n)$, which are assumed to be normally distributed with zero mean value and variance equal to Δ. We can write $\Delta W_{1,2} = \xi_{1,2}\sqrt{\Delta}$, where $\xi_{1,2}$ are discrete Gaussian random variables with zero mean and variance equal to 1. Thereby, our system of SDEs can be written in the following form suitable for the direct numerical integration:

$$Q_{n+1} = Q_n + \left(\frac{N_n - N_{\rm tr}}{N_{\rm th} - N_{\rm tr}}\frac{1}{\sqrt{1 + 2\gamma_Q Q_n}} - 1\right)\frac{Q_n}{\tau_{\rm ph}}\Delta + C_{\rm sp}\frac{N_n}{\tau_e} + 2\sqrt{\frac{C_{\rm sp}N_n Q_n}{2\tau_e}}\left(\xi_1^n\cos\varphi_n + \xi_2^n\sin\varphi_n\right)\sqrt{\Delta},$$
$$\varphi_{n+1} = \varphi_n + \frac{\alpha}{2\tau_{\rm ph}}\left(\frac{N_n - N_{\rm tr}}{N_{\rm th} - N_{\rm tr}} - 1\right)\Delta + \sqrt{\frac{C_{\rm sp}N_n}{2\tau_e Q_n}}\left(\xi_2^n\cos\varphi_n - \xi_1^n\sin\varphi_n\right)\sqrt{\Delta},$$
$$N_{n+1} = N_n + \frac{I_n}{e}\Delta - \frac{N_n}{\tau_e}\Delta - \frac{Q_n}{\Gamma\tau_{\rm ph}}\frac{N_n - N_{\rm tr}}{N_{\rm th} - N_{\rm tr}}\frac{1}{\sqrt{1 + 2\gamma_Q Q_n}}\Delta, \qquad \text{(A16)}$$

where we used the notations $Q_n \equiv Q(t_n)$, $N_n \equiv N(t_n)$, $\varphi_n \equiv \varphi(t_n)$, $I_n \equiv I(t_n)$, $\xi_{1,2}^n \equiv \xi_{1,2}(t_n)$.

It should be taken into account that direct implementation of the Euler-Maruyama scheme may lead to an unphysical

result, namely, to negative values of N and Q; therefore, Eq. (A16) should be solved with constraint that N and Q are nonnegative. Note that this feature persists for the second order scheme (e.g., the Milstein scheme [35]), albeit the latter somewhat minimizes such unphysical trajectories. In simulations shown below, we used the first order (Euler-Maruyama) scheme. Note that we performed integration at different reasonable integration steps $\Delta < 0.1\tau_{\rm ph}$; the results obtained at different Δ were the same for all simulations.

APPENDIX B: CONTROLLING THE INTERFEROMETERS

As was discribed in Sec. III A, we used for measurements a chip with a cascade of unbalanced Mach-Zehnder interferometers (two of them are shown in Fig. 5). To choose the desired delay line, we used an additional balanced interferometers placed between the unbalanced ones; there were seven interferometers on the chip in total: four balanced and three unbalanced with the delay lines $\Delta T_1 = 200$ ps, $\Delta T_2 = 400$ ps, and $\Delta T_3 = 800$ ps (each MZI was also equipped by a thermo-optical phase modulator). Due to such a configuration, the evolution of phase in the interferometers have a cumulative effect, such that splitting ratios depend on the set of phases in all four balanced interferometers. To determine the phases that must be set on thermo-optical modulators in order to select the required delay line, let us write a system of recursive equations that describe propagation of an optical pulse through a cascade of interferometers:

$$\begin{aligned}
E_{12}^{\pm}(t) &= E_{\rm in}(t)\big(1 \pm e^{i\varphi_c^1}\big)/4,\\
E_{23}^{\pm}(t) &= \big[E_{12}^{-}(t-\Delta T_1) \pm E_{12}^{+}(t)e^{i\varphi_u^1}\big]/\sqrt{2},\\
E_{34}^{\pm}(t) &= \big[E_{23}^{-}(t) \pm E_{23}^{+}(t)e^{i\varphi_c^2}\big]/\sqrt{2},\\
E_{45}^{\pm}(t) &= \big[E_{34}^{-}(t-\Delta T_2) \pm E_{34}^{+}(t)e^{i\varphi_u^2}\big]/\sqrt{2},\\
E_{56}^{\pm}(t) &= \big[E_{45}^{-}(t) \pm E_{45}^{+}(t)e^{i\varphi_c^3}\big]/\sqrt{2},\\
E_{67}^{\pm}(t) &= \big[E_{56}^{-}(t-\Delta T_3) \pm E_{56}^{+}(t)e^{i\varphi_u^3}\big]/\sqrt{2},\\
E_{\rm out}^{\pm}(t) &= \big[E_{67}^{-}(t) \pm E_{67}^{+}(t)e^{i\varphi_c^4}\big]/\sqrt{2},
\end{aligned} \tag{B1}$$

where $E_{\rm in}(t)$ is the electric field in the input laser pulse, $E_{mn}^{\pm}(t)$ stands for the electric field in the laser pulse being between the mth and nth interferometers at time t, and the signs "+" and "−" correspond to different ports of the corresponding directional coupler. Photodetectors connected to the output ports + and − measure the intensities $|E_{\rm out}^{+}|$ and $|E_{\rm out}^{-}|$, respectively. [We will assume for simplicity that $|E_{\rm in}(t)|^2$ is defined by the Gaussian curve: $|E_{\rm in}(t)|^2 = \exp[-t^2/(2w^2)]$, where w is the rms width of the pulse.]

It is easy to see that configuration of splitting ratios, which defines the choice of the delay line, does not depend on phases φ_u^k determining phase shifts in unbalanced interferometers; therefore, for simplicity, they can be put to zero. It is interesting to note that if we put also $\varphi_c^1 = \varphi_c^2 = \varphi_c^3 = \varphi_c^4 = 0$, we will obtain using (B1)

$$|E_{\rm out}^{-}| = 0, \quad |E_{\rm out}^{+}| = \exp\left[-\frac{(t-\Delta T_2)^2}{2w^2}\right], \tag{B2}$$

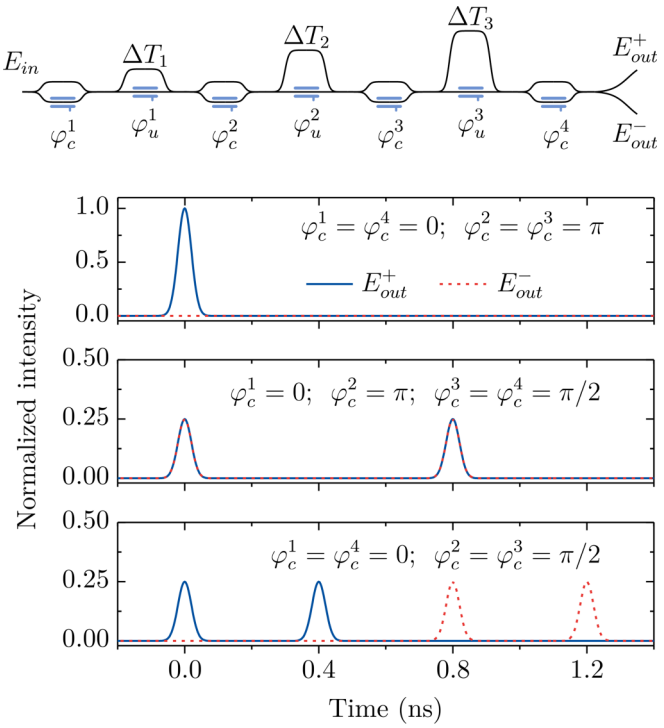

FIG. 13. Schematic representation of a cascade of interferometers on the chip we used in the experiment (on the top) and the output of the system for various configurations of phases φ_c^k in assumption that a single laser pulse of the Gaussian shape with the rms width of 20 ps arrives at the input of the interferometer.

i.e., the incoming laser pulse passes through the delay line $\Delta T_2 = 400$ ps and outputs to the port "+" (and nothing is output to the port "−").

To "close" all the delay lines, the following phase configuration should be used: $\varphi_c^1 = \varphi_c^4 = 0$, $\varphi_c^2 = \varphi_c^3 = \pi$, which yields

$$|E_{\rm out}^{-}| = 0, \quad |E_{\rm out}^{+}| = \exp[-t^2/(2w^2)]. \tag{B3}$$

To choose the interferometer with $\Delta T_3 = 800$ ps, one should put $\varphi_c^1 = 0$, $\varphi_c^2 = \pi$, $\varphi_c^3 = \varphi_c^4 = \pi/2$, which provides

$$|E_{\rm out}^{\pm}|^2 = \frac{1}{4}\left[e^{-\frac{t^2}{4w^2}} + e^{-\frac{(t-\Delta T_3)^2}{4w^2}}\right]^2. \tag{B4}$$

To choose the interferometer with $\Delta T_2 = 400$ ps, one may use $\varphi_c^1 = \varphi_c^4 = 0$, $\varphi_c^2 = \varphi_c^3 = \pi/2$, which gives

$$\begin{aligned}
|E_{\rm out}^{+}|^2 &= \frac{1}{4}\left[e^{-\frac{t^2}{4w^2}} + e^{-\frac{(t-\Delta T_2)^2}{4w^2}}\right]^2,\\
|E_{\rm out}^{-}|^2 &= \frac{1}{4}\left[e^{-\frac{(t-\Delta T_3)^2}{4w^2}} + e^{-\frac{(t-\Delta T_2-\Delta T_3)^2}{4w^2}}\right]^2.
\end{aligned} \tag{B5}$$

The results corresponding to Eqs. (B3)–(B5) are shown in Fig. 13 on the assumption that a single laser pulse of the Gaussian shape with the rms width of 20 ps arrives at the input of the interferometer.

APPENDIX C: SIGNAL NORMALIZATION

When constructing experimental PDFs, it is extremely important to perform proper normalization. To obtain the normalized signal defined by Eq. (9), it was taken into account that even in the absence of optical power, the "area" under the signal from the photodetector (i.e., the measured energy contained in the pulse) can be different from zero; therefore, in all experiments we preliminary determined the "origin" S_{zero}. In addition, we estimated the losses in the interferometer arm. For this, we set the pulse repetition rate to 312.5 MHz (the repetition period of 3.2 ns) and set the voltage on the TOPM-controller such that the optical pulse does not enter any of the delay lines, and all the corresponding optical power goes out to the port connected to the photodetector. The optical energy per pulse was determined as the area under the photodetector signal (in picowebers) in the range from 0 to 3.2 ns (the position of zero on the time axis was chosen arbitrarily). (S_{zero} was measured as the area of the photodetector signal in the same range, but with the laser turned off.) Then the delay line of 800 ps was selected, and the area under the photodetector signal was again measured in the same range, the value of which we designated now S_{800}. It is clear from Eq. (B4) (see also Fig. 13) that the insertion loss of the delay line $\Delta T_3 =$ 800 ps (in dB) can be estimated using the formula $\alpha_{800} = 10\log_{10}\{(S_0 - S_{\text{zero}})/[2(S_{800} - S_{\text{zero}})]\}$. We obtained $\alpha_{800} \approx$ 1.3 dB. The pulse repetition rate was then set to 1.25 GHz and the pulse energy S_0 (without entering the delay line) was measured in the range from 0 to 800 ps. Then, the histogram of the interference PDF (over the pulse area) was recorded. Each value along the x axis was normalized according to the formula

$$\tilde{S} = 10^{\alpha_{800}/10}\frac{x - S_{\text{zero}}}{S_0 - S_{\text{zero}}}. \tag{C1}$$

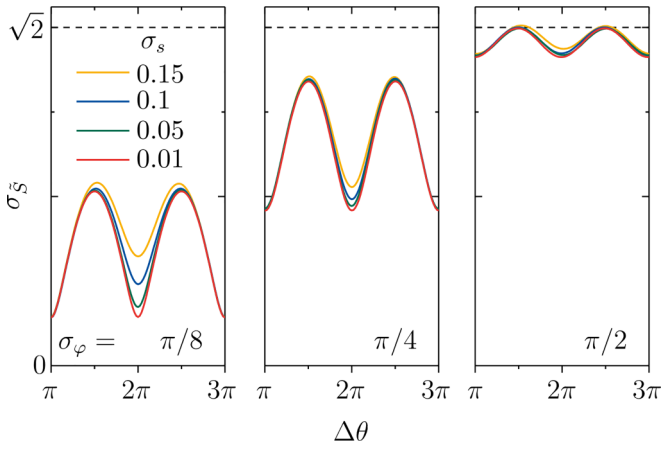

FIG. 14. Theoretical statistical fringes at various values of σ_φ and σ_s.

In a similar way, we normalized the signal at 2.5 GHz. For the delay line $\Delta T_2 = 400$ ps we obtained $\alpha_{400} \approx 0.7$ dB.

APPENDIX D: $\sigma_{\tilde{S}}$ FRINGES

Figure 14 demonstrates theoretical statistical interference fringes at various values of σ_φ and σ_s. One can see that the depth of the dip in the $\sigma_{\tilde{S}}$ curve at constructive interference ($\Delta\theta = 0$) decreases when increasing σ_s, and such an asymmetry of the fringe is more pronounced at smaller σ_φ. Although the analysis of $\sigma_{\tilde{S}}$ fringes is not as straightforward as fitting conventional interference fringes, it allows gaining deeper insight into statistical features of the pulse interference and can be thus a useful tool.

[1] K. Petermann, *Laser Diode Modulation and Noise* (Kluwer Academic Publishers, Dordrecht, 1988).

[2] O. Svelto, *Principles of Lasers* (Springer, New York, 2010).

[3] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[4] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[5] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[6] 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).

[7] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Opt. Express **22**, 1645 (2014).

[8] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, 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).

[9] C. Abellán, 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).

[10] D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-term test of a fast and compact quantum random number generator, J. Lightwave Technol. **36**, 3778 (2018).

[11] Q. Zhou, R. Valivarthi, C. John, and W. Tittel, Practical quantum random-number generation based on sampling vacuum fluctuations, Quantum Eng. **1**, e8 (2019).

[12] R. Shakhovoy, D. Sych, V. Sharoglazova, A. Udaltsov, A. Fedorov, and Y. Kurochkin, Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator, Opt. Express **28**, 6209 (2020).

[13] T. Kobayashi, A. Tomita, and A. Okamoto, Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser, Phys. Rev. A **90**, 032320 (2014).

[14] H.-K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Inf. Comput. **7**, 431 (2007).

[15] S.-H. Sun, M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, Partially random phase attack to the practical two-way quantum-key-distribution system, Phys. Rev. A **85**, 032304 (2012).

[16] Y. L. Tang, H. L. Yin, X. Ma, C. H. F. Fung, Y. Liu, H. L. Yong, T. Y. Chen, C. Z. Peng, Z. B. Chen, and J. W. Pan, Source attack of decoy-state quantum key distribution using phase information, Phys. Rev. A **88**, 022308 (2013).

[17] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[18] G. Magyar and L. Mandel, Interference fringes produced by superposition of two independent maser light beams, Nature (London) **198**, 255 (1963).

[19] K. Konnerth and C. Lanza, Delay between current pulse and light emission of a gallium arsenide injection laser, Appl. Phys. Lett. **4**, 120 (1964).

[20] R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference, IEEE J. Quantum Electron. **57**, 1 (2021).

[21] N. Nisan and A. Ta-Shma, Extracting randomness: A survey and new constructions, J. Comput. Syst. Sci. **58**, 148 (1999).

[22] C. Henry, Theory of the linewidth of semiconductor lasers, IEEE J. Quantum Electron. **18**, 259 (1982).

[23] H. Haug, Quantum-mechanical rate equations for semiconductor lasers, Phys. Rev. **184**, 338 (1969).

[24] D. E. McCumber, Intensity fluctuations in the output of CW laser oscillators. I, Phys. Rev. **141**, 306 (1966).

[25] D. J. Morgan and M. J. Adams, Quantum noise in semiconductor lasers, Phys. Status Solidi A **11**, 243 (1972).

[26] C. Henry, Phase noise in semiconductor lasers, J. Lightwave Technol. **4**, 298 (1986).

[27] R. Loudon, *The Quantum Theory of Light* (Oxford University Press, New York, 2000).

[28] R. J. Glauber, Nobel lecture: One hundred years of light quanta, Rev. Mod. Phys. **78**, 1267 (2006).

[29] M. Lax, Quantum noise. IV. Quantum theory of noise sources, Phys. Rev. **145**, 110 (1966).

[30] M. Lax, Quantum noise. X. Density-matrix treatment of field and population-difference fluctuations, Phys. Rev. **157**, 213 (1967).

[31] G. H. M. van Tartwijk and D. Lenstra, Semiconductor lasers with optical injection and feedback, Quantum Semiclass. Opt. **7**, 87 (1995).

[32] G. P. Agrawal and N. K. Dutta, *Semiconductor Lasers* (Kluwer Academic Publishers, Dordrecht, 1993).

[33] E. Eichen and P. Melman, Semiconductor laser lineshape and parameter determination from fringe visibility measurements, Electron. Lett. **20**, 826 (1984).

[34] C. Henry, Theory of the phase noise and power spectrum of a single-mode injection laser, IEEE J. Quantum Electron. **19**, 1391 (1983).

[35] P. E. Kloeden and E. Platen, *Numerical Solution of Stochastic Differential Equations* (Springer, New York, 1995).

[36] R. Lang, K. Vahala, and A. Yariv, The effect of spatially dependent temperature and carrier fluctuations on noise in semiconductor lasers, IEEE J. Quantum Electron. **21**, 443 (1985).

[37] G. P. Agrawal, Spectral hole–burning and gain saturation in semiconductor lasers: Strong-signal theory, J. Appl. Phys. **63**, 1232 (1988).

[38] G. P. Agrawal, Effect of gain and index nonlinearities on single-mode dynamics in semiconductor lasers, IEEE J. Quantum Electron. **26**, 1901 (1990).