Eight-port homodyne detector: The effect of imperfections on quantum random-number generation and on detection of quadratures

Alberto Barchielli [*]
Istituto Nazionale di Fisica Nucleare (INFN), Sezione di Milano, 20133 Milan, Italy

Alberto Santamato [†]
Photonics Networks and Technologies Lab, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, 56124 Pisa, Italy

(Received 29 April 2022; accepted 3 August 2022; published 30 August 2022)

The eight-port homodyne detector is an optical circuit designed to perform the monitoring of two quadratures of an optical field: the signal. By using quantum Bose fields and quantum stochastic calculus, we give a complete quantum description of this apparatus, when used as quadrature detector in continuous time. We can treat either the traveling waves in the optical circuit or the observables involved in the detection part: two couples of photodiodes, postprocessing of the output currents …. The analysis includes imperfections, such as not perfectly balanced beam splitters, detector efficiency, electronic noise, phase and intensity noise in the laser acting as local oscillator; this last noise is modeled by using mixtures of field coherent states as statistical operator of the laser component. Due to the monitoring in continuous time, the output is a stochastic process and its full probability distribution is obtained. When the output process is sampled at discrete times, the quantum description can be reduced to discrete mode operators, but at the price of having random operators, which contain also the noise of the local oscillator. Consequently, the local oscillator noise has a very different effect on the detection results with respect to an additive noise, such as the noise in the electronic components. As an application, the problem of secure random-number generation is considered, based on the local oscillator shot noise. The rate of random bits that can be generated is quantified by the min-entropy; the possibility of classical and quantum side information is taken into account by suitable conditional min-entropies. The final rate depends on which parts of the apparatus are considered to be secure and on which ones are considered to be exposed to the intervention of an intruder. In some experimentally realistic situations, the entropy losses are computed, depending on the values of the parameters quantifying the imperfections.

DOI: 10.1103/PhysRevA.106.022620

I. INTRODUCTION

Sources of true random numbers, those that are not generated from algorithms but from stochastic processes, are of great interest especially in areas such as cryptography, simulation, and secure communication. Particularly interesting are those random-number generators which rely on stochastic processes of quantum origin; these are fundamentally unpredictable due to the aleatory nature of the measurement outcome of quantum states. A single photon traveling through a balanced beam splitter and detected at the two outputs with single-photon detectors [1] is a paradigmatic example of quantum random-number generator (QRNG); the randomness is quantified by the entropy of the superposition of being in one output or the other. The entropy in this case is maximal for a perfectly balanced beam splitter since the probability distribution of the two outcomes is a uniform distribution of the two values (say 0 and 1). Quite recently, QRNGs that do not require single photons, but based on continuous variable (CV) measurements, have been proved to be very efficient and technologically less demanding [2–10]; these devices perform homodyne detection and exploit the entropy of the stochastic process underpinning the shot noise generated from balanced receivers when the signal input is the vacuum state. Improvements of this approach have also been demonstrated [11]; the simultaneous measurement of complementary quadratures of the vacuum state with double homodyne detection generates not only genuine but also secure random numbers. In fact, following this technique it is possible to counteract the influence of an adversary that is trying to exploit untrusted elements of the system to steer the statistics of the random numbers towards his own benefits.

The eight-port homodyne detector [12–16] is a combination of an optical circuit and photodetectors, devised to "measure" two quadratures of a quantum "signal," possibly two complementary quadratures. The quantum treatment of both single- and double-homodyne detection is usually done by using discrete bosonic modes [4,11–15,17,18]; thanks to the use of continuous Bose fields we allow for a more general description in terms of traveling waves and of detection in continuous time [19–23]. In this work we want to focus our

[*]Also at Istituto Nazionale di Alta Matematica (INDAM-GNAMPA); Politecnico di Milano, Dipartimento di Matematica, piazza Leonardo da Vinci 32, 20133 Milano, Italy; alberto.barchielli@polimi.it
[†]asantamato@cnit.it

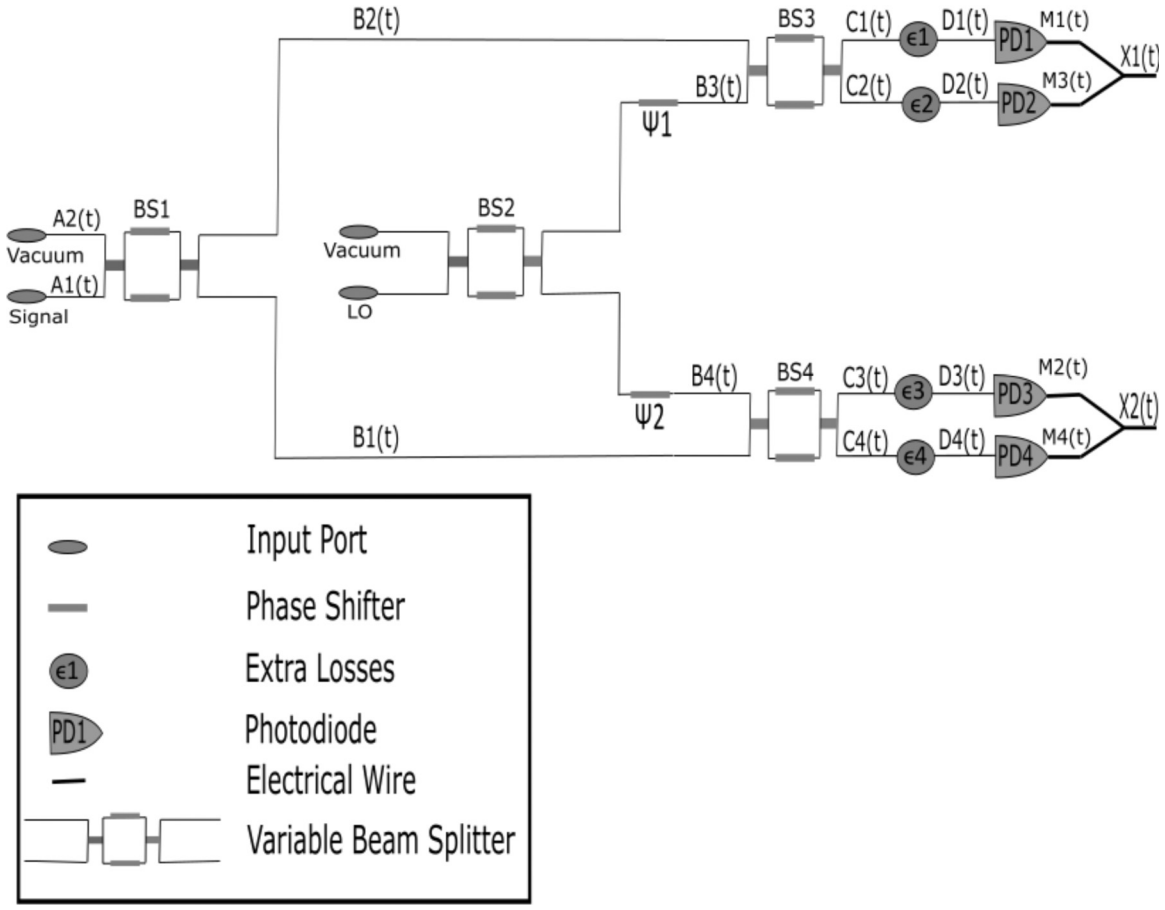

FIG. 1. The eight-port optical circuit for a double-homodyne detection. Input fields: $A_j(t)$. Transformed fields: stage 1 $B_j(t)$, stage 2 $C_j(t)$. Detected fields: $D_j(t)$. Detector outputs: $M_j(t)$. Balanced outputs: $X_j(t)$.

attention on the detailed analysis of the eight-port apparatus, described in Fig. 1: it is composed by four beam splitters and four photodiodes, one at each output of the beam splitters 3 and 4. The inputs are the *signal* (port 1) and the *local oscillator* (LO, port 3); the beam splitter 1 mixes the signal with a vacuum input, while beam splitter 2 mixes the LO with another vacuum input. We include imperfections and noises in the analysis of this circuit and we show that it is still possible to use it as a detector apparatus. We also produce formulas useful to calibrate nonideal experimental implementations of QRNG modules.

The purpose of the device is to measure two field quadratures of the input signal and this is realized when the LO power is much larger than the signal power (i.e., in the limit of infinitely strong local oscillator). We are interested in the distribution of the two output currents generated by the difference of the pairs of photocurrents produced by each couple of photodiodes. In the limit of strong LO, as we shall see, it is possible to demonstrate that the apparatus is indeed monitoring in continuous time two quadratures; when the signal is in the vacuum state, the variance of the each quadrature is reduced to pure shot noise (up to imperfections to be discussed), which is an ideal source of entropy. This noise is the source of randomness that is used to produce random bits. The distribution of the measured photocurrent is approximately Gaussian centered around a zero mean with a variance dependent on the power of the local oscillator. Continuous time observations of real signals are involved in the description; however, when this apparatus is used for QRNG, the signals are sampled at discrete times and the CV outputs are discretized in their turn. This is due to the natural discrete sampling that an oscilloscope or an ADC (analog to digital converter) operates on the input signals. The discrete distribution obtained this way can be used to produce the actual uniform distribution of independent samples needed for true random-number generators. The transformation from the output statistics (which is close to a Gaussian distribution) to a uniform distribution can be done using established techniques described, for example, in [2].

Independently from the application as detector or as random-number generator, the system we are considering consists of linear optical elements with traveling light waves, constantly monitored by the four photodiodes. To give a full quantum description of this system we shall use quantum Bose fields and *quantum stochastic calculus* (QSC) [24–26]. An important aim of this work is also to use this concrete application to show how to construct a consistent quantum theory of optical circuits [27,28] and *photodetection in continuous time* [22,29,30], even when imbalanced beam splitters, detector response functions, laser, and electronic noises have to be taken into account. Here, quantum and classical noises find a consistent description, based on general quantum measurement

theory [17,20,31–34]. The whole approach presented here can be generalized also to other optical circuits, such as those presented in [12,35], or to problems of quantum communication, such as *quantum key distribution* (QKD) [8,36,37].

Plan of the paper

In Sec. II we discuss the quantum treatment of the eight-port detector. We introduce the necessary quantum fields and the unitary operators representing the beam splitters and other linear components in the circuit. The measurement stage, the photodetectors, is represented by projection-valued measures (pvm) and positive operator-valued measures (POVM) in continuous time. We allow for not balanced beam splitters. The circuits also include a variable phase shifter between the beam splitters 2 and 3 and another one between the beam splitters 2 and 4. At one input of beam splitter 2 there is a laser (the local oscillator, LO) which we consider of very strong power with respect to a possible signal in the other inputs. The laser state is a mixture of field coherent states; phase fluctuations and intensity noise are included in the formulation of such a state. The action of the photodetectors is described by the pvm associated with the photocounting operators; this counting process is smoothed in time by the photodiodes and the resulting photocurrents are subtracted in order to implement the balanced homodyne detection. More precisely we work with the characteristic operators (Fourier transform) [20–22] of the counting pvm in continuous time and of the POVM describing the subtracted photocurrents. The theoretical results are rooted in QSC, which is essential in the whole construction. In the main text we present the relevant results and give a physical interpretation of the formulas, while some mathematical details are left to the Appendixes A, B 1, and B 2.

The limit of strong LO is done in Sec. III. Here we have to prove the existence of this limit for the full probability distribution of the scaled photocurrents; again the mathematical proofs are left to Appendix B 3. For a suitable choice of the two phases ψ_j, the two subtracted currents become proportional to two complementary quadrature operators, meaning that the circuit considered in the strong intensity limit is indeed measuring simultaneously the two quadratures. In the ideal case, this result shows that this circuit is a physical implementation of the theoretical POVM introduced in [20] for time continuous measurements; however, now we take into account also the effects of imbalanced beam splitters, inefficiencies of the photodiodes, and LO noises. We also discuss how the increase of phase noises can degrade the homodyne detection into heterodyne detection in a continuous way.

The outputs of the apparatus of Fig. 1 are often sampled at discrete times, either when it is used for QRNG or as a detection apparatus for the signal quadratures. The previous general results are particularized to this situation in Sec. IV. Moments and probability distributions of the involved observables are obtained; again mathematical computations are left to Appendixes B 4 and C. In this situation it is possible to express the various physical quantities through discrete mode operators, but, thanks to our general approach in continuous time, one sees that these mode operators are random because their structure is based on the function describing the coherent state of the LO and this function is random due to the intensity noise and phase fluctuations.

In Sec. V we apply the previous results to the problem of QRNG. Now the signal is in the vacuum state and the outputs are sampled at discrete times; moreover, the CV outputs are naturally discretized by the ADC apparatus. Following a common approach presented in other works, we use the classical min-entropy and the conditional min-entropy [2,5,11,38] to evaluate the rate of secure bits that can be extracted from the system under practical and nonideal situations (not perfect balancing of the beam splitters, some inefficiency of the detectors, presence of laser intensity and phase noises). Our work generalizes and enlarges the analysis presented in [8] and [11] since we allow for an imperfect realization of the double-homodyne detection scheme, not only for additive electronic noise. By choosing some realistic values for the free parameters we give also examples where the number of secure bits per sample can be computed. The problem of QRNG is not only that the extracted bits must be truly random, but also that they must be unknown to a possible adversary. There are subtleties to be taken into consideration depending on what it is assumed to be "secure" and "trusted," with respect to what is "untrusted," due to the possibility that an eavesdropper takes advantage of this untrusted part of the system to gain knowledge on the generated data or to simply corrupt the generation process [6,7,36]. In a first approach we consider untrusted only the classical noise: the laser noise and the the electronic noise due to the amplification chain after the photodiodes; the apparatus and, in particular, the input ports are trusted. Then, we consider also the case in which the signal port is not secure and the so-called *quantum side information* has to be taken into account. Via the introduction of a conditional min-entropy, this classification influences the quantification of the secure rate of random bits that can be extracted from the system. In the examples we show also how the generation rate of "secure bits" is influenced by the imperfections in the circuit, as imbalance of the beam splitters and not unit efficiency of the photodiodes. In this section we discuss also the different roles of the LO fluctuations and of the electronic noise, which is a purely additive noise.

As a particular case, the circuit of Fig. 1 includes also the case of single homodyning. In Sec. VI we explain how to obtain this case and we discuss its application to the QRNG problem; again quantitative examples are given. Some final comments are in Sec. VII.

II. OPTICAL CIRCUIT AND PHOTON DETECTION

To give a quantum description of optical circuits, such as the one of Fig. 1, and of the photon detection scheme, we need to introduce suitable quantum fields representing the traveling waves inside the circuit and some notions of QSC, needed to handle the equations used in the description of the detection stage [20–23,26]. Let us stress that the original motivation for the introduction of QSC was related to quantum open system theory [21,24–26].

We introduce d Bose fields $a_j(t)$ satisfying the canonical commutation rules (CCRs)

$$[a_i(s), a_j(t)] = 0, \quad [a_i(s), a_j^\dagger(t)] = \delta_{ij}\delta(t-s). \tag{1}$$

In quantum field theory, the CCRs admit inequivalent representations. In order to have the existence of the vacuum and of the coherent states we fix the Fock representation and denote by $\Gamma = \Gamma_1 \otimes \Gamma_2 \otimes \cdots$ the *symmetric Fock space* [see (A1) in Appendix A], the Hilbert space where the fields $a_j(t)$ act. The *coherent vectors* $e_j(f) \in \Gamma_j$, with $f \in L^2(\mathbb{R})$, are defined by (A2) and satisfy

$$a_j(t)e_j(f) = f(t)e_j(f); \tag{2}$$

this equation shows that $e_j(f)$ is indeed a coherent vector for the annihilation operators. Note that $e_j(0)$ represents the vacuum state for the field component $a_j(t)$.

To develop the theory of quantum stochastic differential equations, the integral version of the a_j fields is needed, together with the integral of quadratic expressions preserving the number of quanta:

$$A_j(t) = \int_0^t a_j(s)ds, \quad \Lambda_{ij}^A(t) = \int_0^t a_i^\dagger(s)a_j(s)ds. \tag{3}$$

The operators $\Lambda_{ij}^A(t)$ were named *gauge process* [24]; note that $\Lambda_{jj}^A(t)$ is the *number process* for the field j (indeed it has the integer numbers as eigenvalues). By (2) we get $\langle e_j(f)|\Lambda_{jj}^A(t)|e_j(f)\rangle = \int_0^t |f(s)|^2 dt$ and this quantity represents the mean number of photons in the time interval $(0, t)$; then, $|f(t)|^2$ is the instantaneous mean number of photons per unit of time.

The approximations involved in the use of these fields to represent the electromagnetic field are justified when the interactions and the refraction indices are little dependent on frequency in a large band around a principal frequency ω_0; this is the so-called "broadband, quasimonochromatic approximation." Moreover, to use these fields in an optical circuit means to use a "quantum traveling wave formulation," an approximation which is in some way opposed to the use a single mode or a few discrete modes. By using these fields and QSC it is also possible to develop a theory of direct, homodyne, heterodyne detection in continuous time [21,22,27–30,32,37,39,40].

By suitable unitary transformations, which preserve the canonical commutation relations, it is possible to represent the optical linear devices which compose an optical circuit [27,28]. In particular, we shall need the transformation generated by a beam splitter of transmissivity $\eta \in [0, 1]$: two input fields $A_1(t)$ and $A_2(t)$ are mixed together and transformed in the fields $B_1(t)$ and $B_2(t)$, given by

$$\begin{aligned} B_1(t) &= \sqrt{\eta}\, A_1(t) + i\sqrt{1-\eta}\, A_2(t), \\ B_2(t) &= i\sqrt{1-\eta}\, A_1(t) + \sqrt{\eta}\, A_2(t). \end{aligned} \tag{4}$$

In the optical circuit that we shall analyze, the polarization does not play any role; when it is not so, polarization can be taken into account by doubling the fields and also linear devices depending on the polarization can be introduced [27].

A. Optical circuit

The circuit under study is drawn in Fig. 1. It presents four input ports, into which the input fields $A_j(t)$ enter, and four output ports, from which the four output fields $D_j(t)$ leave the circuit; the output fields are detected by four photodiodes.

The field $A_1(t)$ carries the *input signal*, and it is split in two fields by mixing it at the beam splitter BS1 with the field $A_2(t)$ in the vacuum state. The field $A_3(t)$ carries the laser light playing the role of local oscillator (LO), and it is split in two fields by mixing it at the beam splitter BS2 with the field $A_4(t)$ in the vacuum state. As discussed in Sec. II A 2, to model the light losses in the circuit and the efficiency of the detectors we add before the output ports four fictitious beam splitters and four auxiliary input fields $A_{j+}(t)$ in the vacuum state. So, to analyze the circuit of Fig. 1 we use $d = 8$ field components.

This circuit is suggested as a realization of a double-homodyne detection in [12, Sec. 5.6.1], [32, Sec. 4.5.1], [18, Fig. 5], for instance. Here we want to perform a fully quantum analysis of this circuit, taking into account noise sources and imperfections (e.g., laser noise and unbalancing of the beam splitters), as suggested in [8] for the case of a single-homodyne apparatus.

1. Beam splitters and phase shifters

The circuit is composed by four beam splitters BSj of transmissivity η_j, $j = 1, \ldots, 4$, and by two tunable phase shifters. All the optical paths from the inputs to the outputs are assumed to be equal; this allows to neglect the delays in passing from a beam splitter to the other. By suitable chosen phase shifts in the fields, also imperfections in the optical paths could be taken into account in our formalism.

At the beam splitter BS1 the signal field $A_1(t)$ is mixed with the vacuum field $A_2(t)$ and produces the output fields $B_1(t)$ and $B_2(t)$, which turn out to be given by

$$\begin{aligned} B_1(t) &= \sqrt{\eta_1}\, A_1(t) + i\sqrt{1-\eta_1}\, A_2(t), \\ B_2(t) &= i\sqrt{1-\eta_1}\, A_1(t) + \sqrt{\eta_1}\, A_2(t). \end{aligned} \tag{5a}$$

At the beam splitter BS2 the LO field $A_3(t)$ is mixed with the vacuum field $A_4(t)$ and, after the two tunable phase shifts ψ_j, it gives rise to the output fields $B_3(t)$ and $B_4(t)$, given by

$$\begin{aligned} B_3(t) &= e^{i\psi_1}[\sqrt{\eta_2}\, A_3(t) + i\sqrt{1-\eta_2}\, A_4(t)], \\ B_4(t) &= e^{i\psi_2}[i\sqrt{1-\eta_2}\, A_3(t) + \sqrt{\eta_2}\, A_4(t)]. \end{aligned} \tag{5b}$$

It will be useful to have a notation for the difference of the tunable phases:

$$\phi = \psi_2 - \psi_1. \tag{6}$$

Then, the fields $B_1(t)$ and $B_3(t)$ are mixed together at the beam splitter BS3, giving rise to the fields $C_1(t)$ and $C_3(t)$, while the fields $B_2(t)$ and $B_4(t)$ are mixed at BS4 and give rise to $C_2(t)$ and $C_4(t)$. The output fields turn out to be given by

$$C_1(t) = \sqrt{\eta_3}\, B_1(t) + i\sqrt{1-\eta_3}\, B_3(t), \tag{7a}$$

$$C_3(t) = i\sqrt{1-\eta_3}\, B_1(t) + \sqrt{\eta_3}\, B_3(t), \tag{7b}$$

$$C_2(t) = \sqrt{\eta_4}\, B_2(t) + i\sqrt{1-\eta_4}\, B_4(t), \tag{7c}$$

$$C_4(t) = i\sqrt{1-\eta_4}\, B_2 + \sqrt{\eta_4}\, B_4(t). \tag{7d}$$

2. Losses and efficiency of the detectors

To model the field losses in an optical path and/or in a photodetector and to maintain the CCRs (1) for the fields,

it is usual to insert a virtual beam splitter of transmissivity less than one [8]. The beam enters a first input port, while the vacuum enters the second input port. The attenuated beam comes out from the transmission output port, while the lost light comes out from the other port.

In our case we add four input fields $A_{j+}(t)$ in the vacuum state and four beam splitters of transmissivity $\epsilon_j \in (0, 1]$; at the eight outputs we have the observed field $D_j(t)$, which reach the photodetectors, and the lost fields $D_{j+}(t)$, $j = 1, \ldots, 4$. The transformation of the field operators is

$$D_j(t) = \sqrt{\epsilon_j}\, C_j(t) + i\sqrt{1-\epsilon_j}\, A_{j+}(t),$$
$$D_{j+}(t) = i\sqrt{1-\epsilon_j}\, C_j(t) + \sqrt{\epsilon_j}\, A_{j+}(t). \tag{8}$$

Let us stress that preserving the CCRs (1) is needed to have a consistent quantum description; this means that the attenuation of the optical signal goes together an increase of the noise due to the new vacuum inputs.

Remark 1. As suggested in [8], the efficiency coefficients ϵ_j can be considered partially tunable; indeed, by inserting a variable optical attenuator in series before each output port we can diminish the efficiency coefficient. So, if $\epsilon_j^{\max} \in (0, 1]$ is the coefficient value due to light losses and inefficiency of the detector, the effective coefficient ϵ_j is (roughly) tunable in the interval $(0, \epsilon_j^{\max}]$.

By combining Eqs. (5), (7), and (8) we can express the output fields $D_j(t)$ in terms of the input fields $A_j(t)$ and of the auxiliary fields $A_{j+}(t)$; the total transformation for the field densities is given in Eqs. (A4). From these densities one can also express, in terms of the input fields $a_j(t)$, $a_{j+}(t)$, the components $\Lambda_{ij}^D(t) = \int_0^t d_i^\dagger(s) d_j(s)\, ds$ of the gauge process; the number operators $\Lambda_{jj}^D(t)$ will be used in Sec. II C in modeling the photodetectors.

B. Field state

As already noticed, the fields $A_2(t)$, $A_4(t)$, $A_{j+}(t)$ are in the vacuum state. Then, if we denote by ρ_{13}^T the reduced state of signal and LO [in the time interval $(0, T)$], the total state of the field is

$$\rho^T = \rho_{13}^T \otimes \rho^\perp,$$
$$\rho^\perp = |e_2(0)\rangle\langle e_2(0)| \otimes |e_4(0)\rangle\langle e_4(0)| \otimes \prod_{j=1}^{4}{}^{\otimes} |e_{j+}(0)\rangle\langle e_{j+}(0)|. \tag{9}$$

To represent the laser light of the LO we use the mixture of coherent states

$$\rho_3^T = \mathbb{E}_f[|e_3(f_T)\rangle\langle e_3(f_T)|], \quad f_T(t) = f(t)1_{(0,T)}(t), \tag{10}$$

where $f(t)$ is a complex stochastic process; by the comments after Eq. (3), $|f(t)|^2$ is the instantaneous laser intensity. As for a monochromatic wave, a typical trajectory of this process is not in $L^2(\mathbb{R})$, as required to define a field coherent vector. However, it can be assumed to be locally square integrable and by multiplying it by the indicator function $1_{(0,T)}(t)$ we get $f_T \in L^2(\mathbb{R})$. The time T is taken to be large and sent to $+\infty$ in the final physical formulas.

Remark 2. For the means and other moments done under the law P_f of the process f and of the other correlated processes we use the notation $\mathbb{E}_f$, Var_f, $\mathrm{Cov}_f \ldots$. On the other side, for means and moments with respect to the probability law P obtained from the total field state and the various positive operator-valued measures (POVM) representing the quantum observables we shall use the notation $\mathbb{E}_P$, Var_P, $\mathrm{Cov}_P \ldots$.

Remark 3. In some applications of homodyne detection, when squeezing can be relevant, a good phase coherence between signal and LO must be maintained in time, the LO must be *phase locked* to the signal [19]. To guarantee this, the same laser is used to produce the LO and to stimulate the quantum system of interest (an atom [33,34], a quantum oscillator [28], a nonlinear medium [41], ...). This means that signal and LO can be correlated; to model this situation, we take as signal-LO state

$$\rho_{13}^T = \mathbb{E}_f\big[\rho_{13}^{f,T}\big], \quad \rho_{13}^{f,T} = \rho_1^{f,T} \otimes |e_3(f_T)\rangle\langle e_3(f_T)|, \tag{11}$$

where $\rho_1^{f,T}$ is a random statistical operator for the signal field, depending on the process f or correlated in some way with it.

We already introduced the reduced random signal-LO state $\rho_{13}^{f,T}$; it is useful to introduce also the random total state and some simplified notations

$$\rho_f^T = \rho_{13}^{f,T} \otimes \rho^\perp, \quad \langle\cdot\rangle_T^f = \mathrm{Tr}\left\{\cdot\,\rho_f^T\right\},$$
$$\langle\cdot\rangle_T = \mathrm{Tr}\{\cdot\,\rho^T\} = \mathbb{E}_f\big[\langle\cdot\rangle_T^f\big]. \tag{12}$$

Laser models

The process $f(t)$ plays the role of reference wave when the whole apparatus is used as a detector for the signal light. To represent a laser of nominal frequency ω_0 we can take $f(t) = \lambda e^{-i\omega_0 t} \times \cdots$, where the ellipsis stands for other contributions representing the main noises affecting the laser light. The first important noise is the *phase noise* and a good model for this is the *phase-diffusion model of a laser* [42, Sec. 11.4.1], [43, Sec. 2.7.3]: a term proportional to a Wiener process is added to the phase $\omega_0 t$, whose effect is to give a finite coherence length. Another important noise is the one generated by the fluctuations of the laser intensity, often represented by the *relative intensity noise* (RIN) [8,43,44]:

$$n_{\mathrm{RIN}}(t) = \frac{|f(t)|^2 - \mathbb{E}_f[|f(t)|^2]}{\mathbb{E}_f[|f(t)|^2]}. \tag{13}$$

As explained in [43, Sec. 2.8], lasers are constructed in such a way that they do not have other peaks in a large frequency band around their carrier frequency and the proposed noise models should be compliant with these requirements.

We collect all these features in a single model for the laser, a modification of the phase-diffusion model:

$$f(t) = \lambda e^{-i\omega_0 t - i\sqrt{2\gamma_0}\, W(t)}\, u(t), \quad \lambda = |\lambda| e^{i\theta},$$
$$\theta \in \mathbb{R}, \quad \omega_0 > 0, \quad \gamma_0 > 0, \tag{14}$$

where $W(t)$ is a standard Wiener process. Moreover, we take $u(t)$ to be a real Gaussian process, independent of $W(t)$, such

that

$$\mathbb{E}_f[u(t)] = w, \quad \mathrm{Cov}_f[u(t), u(s)] = v(t-s),$$
$$\mathbb{E}_f[u(t)^2] \equiv w^2 + v(0) = 1. \tag{15}$$

The processes $W(t)$, $u(t)$ and the random variable θ are taken to be independent. Computations of some moments of $f(t)$ are given in Appendix A 2. By the comments below Eq. (3), $f(t)$ has the dimensions of a time to $-\frac{1}{2}$. By the last requirement in (15), w and $u(t)$ are taken to be pure numbers, so that λ has the dimensions of a time to $-\frac{1}{2}$.

By (14) and (15), the mean intensity of the laser is constant in time:

$$\mathbb{E}_f[|f(t)|^2] = |\lambda|^2; \tag{16}$$

$|\lambda|^2$ is the mean number of photons per unit of time. By (A5d), the RIN correlations turn out to have the expression

$$\mathrm{Cov}_f\,[n_{\mathrm{RIN}}(t), n_{\mathrm{RIN}}(s)] = \mathbb{E}_f[n_{\mathrm{RIN}}(t) n_{\mathrm{RIN}}(s)]$$
$$= 2v(t-s)^2 + 4w^2 v(t-s). \tag{17}$$

The correlation function $v(t)$, defined in (15), turns out to be even, $v(-t) = v(t) \in \mathbb{R}$, and positive definite; so, we have $v(0) \geqslant 0$ and

$$v(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} e^{i\nu t} \tilde{v}(\nu)\, d\nu, \quad \tilde{v}(\nu) = \tilde{v}(-\nu) \geqslant 0; \tag{18}$$

we assume also $\tilde{v}(\nu) \in L^1(\mathbb{R})$.

An important feature of the laser model is the intensity spectrum of the process $f(t)$, defined by

$$\Pi_f(\mu) = \lim_{T\to+\infty} \mathbb{E}_f\left[\left|\frac{1}{\sqrt{T}} \int_0^T e^{i\mu t} f(t) dt\right|^2\right]; \tag{19}$$

note that $\Pi_f(\mu)$ turns out to be a pure number. By using (14), (18), and (A5a), we get

$$\Pi_f(\mu) = \frac{2|\lambda|^2 w^2 \gamma_0}{\gamma_0^2 + (\mu-\omega_0)^2} + \int_{\mathbb{R}} d\nu\, \frac{|\lambda|^2 \tilde{v}(\nu)\gamma_0/\pi}{\gamma_0^2 + (\mu-\omega_0-\nu)^2}. \tag{20}$$

If needed, the laser parameters $\gamma_0, \omega_0, \tilde{v}(\nu)$ could be estimated in a calibration stage, for instance by measuring the intensity spectrum.

Similarly, we can introduce the spectrum of the intensity fluctuations; from (17) and (18), by straightforward computations we get

$$\Pi_{\mathrm{RIN}}(\mu) = \lim_{T\to+\infty} \frac{1}{T} \int_0^T dt \int_0^T ds\, e^{i\mu(t-s)} \times \mathbb{E}_f[n_{\mathrm{RIN}}(t) n_{\mathrm{RIN}}(s)]$$
$$= 4w^2 \tilde{v}(\mu) + \int_{\mathbb{R}} \frac{\tilde{v}(\nu)\tilde{v}(\mu-\nu)}{\pi}\, d\nu.$$

To agree with the request that the intensity fluctuations do not introduce new peaks in the laser spectrum we need $\tilde{v}(\nu)$ to be sufficiently flat.

C. Photodetectors

Let us consider now the monitoring of the photon flux intensity at the four output ports; we start by considering direct detection (in continuous time) of the photons [21,22,30,32,39,40].

When the detectors at the output ports are perfect photocounters, we can say that we are measuring the quantum observables represented by the number operators

$$\hat{N}_j(t) = \Lambda^D_{jj}(t) = \int_0^t d_j^\dagger(s) d_j(s)\, ds,$$
$$0 \leqslant t \leqslant T, \quad j = 1, \ldots, 4. \tag{21}$$

Remark 4. The essential point is that, by the CCRs satisfied by the fields $d_j(t)$, these are compatible observables: the set $\{\hat{N}_j(t),\ 0 \leqslant t \leqslant T,\ j = 1, 2, 3, 4\}$ is a family of commuting self-adjoint operators to which a projection-valued measure (pvm) is associated. The commutativity also for different times is the key point which allows for a quantum theory of measurements in continuous time [20,22]. All the observables we shall introduce in the following will be functions of the number operators, and, so, also these other observables will be represented by commuting operators.

The family of number operators is a continuity of operators (with respect to the index "time"); so, the associated pvm is a measure on an infinite-dimensional value space. Apart from this, by the usual rules of a quantum theory, this measure and the system state (introduced in Sec. II B) give rise to a probability measure P for the observed counts $N_j(t)$. To handle this implicitly defined pvm, it is useful to introduce its Fourier transform, the *characteristic operator* [20–22], which we discuss in Appendix B 1. In any case, as the probabilities are given by the pvm of the commuting number operators, all the moments of the observed counts can be expressed by means the usual quantum expectations; by using the notations introduced in Remark 2 and in Eq. (12), we have

$$\mathbb{E}_P[N_{j_1}(t_1) N_{j_2}(t_2) \ldots] = \langle \hat{N}_{j_1}(t_1) \hat{N}_{j_2}(t_2) \ldots \rangle_T. \tag{22}$$

Remark 5. In the case of vanishing signal, as shown in Appendix B 1 a, the counting processes $N_j(t)$ are a mixture of Poisson processes with random intensities

$$J_1^f(t) = \eta_2(1-\eta_3)\epsilon_1 |f(t)|^2,$$
$$J_2^f(t) = (1-\eta_2)(1-\eta_4)\epsilon_2 |f(t)|^2. \tag{23}$$

In Appendix B 1 a, it is also shown that we get a mixture of Poisson processes also when the signal is in a coherent state.

Photodiodes

In the following we shall be interested in a generic signal and a strong LO; so we expect an intense flux of photons at the output ports and we cannot rely on single-photon counters. We consider as detectors general photodiodes, whose output is some kind of time average of the photon arrivals in a time interval. The output photocurrent of a photodiode can be seen as a smoothed version of the rate of arrival of the photons; this signal and its associated operator can be represented by

$$M_j(t) = \int_0^t F_j(t,s) dN_j(s),$$
$$\hat{M}_j(t) = \int_0^t F_j(t,s) d\hat{N}_j(s), \tag{24}$$

where $F_j(t,s)$ is the *response function* of the jth detector.

The response functions contain an unavoidable smoothing on time; a good and general choice is to take

$$F_j(t,s) = \xi_j h(t-s), \quad \xi_j > 0, \quad h(t) \geqslant 0, \quad \int_0^{+\infty} h(t)dt = 1. \tag{25}$$

The function $h(t)$ represents the *impulse response* of the photodiode; it decays as time grows and it is taken to be the inverse of a time and normalized as indicated in (25). Moreover, the conversion factors ξ_j are dimensional coefficients, containing possible amplification contributions. The four detectors cannot be exactly equal; however, for simplicity, we took the same time behavior of the four response functions, while we left the freedom of having different conversion factors ξ_j.

Again, the output signals $M_j(t)$ are represented by the commuting self-adjoint operators $\hat{M}_j(t)$, $t \in (0,T)$, $j = 1,\dots,4$, and their probability law and moments are obtained by the usual rules of quantum mechanics. The characteristic operator of the family of the $\hat{M}$ operators is presented in Appendix B 1 b, while the moments can be obtained directly from (22) and (24). By using the field densities and putting them in normal order, we get

$$\begin{aligned}\mathbb{E}_P[M_j(t)] &= \langle \hat{M}_j(t)\rangle_T = \int_0^t F_j(t,r)\langle d\hat{N}_j(r)\rangle_T \\ &= \xi_j \int_0^t dr\, h(t-r)\langle d_j^\dagger(r) d_j(r)\rangle_T, \end{aligned} \tag{26}$$

$$\begin{aligned}\mathbb{E}_P[M_j(t)M_i(s)] &= \langle \hat{M}_j(t)\hat{M}_i(s)\rangle_T \\ &= \delta_{ij}\xi_j^2 \int_0^{t\wedge s} dr\, h(t-r)h(s-r) \\ &\quad \times \langle d_j^\dagger(r) d_j(r)\rangle_T \\ &\quad + \xi_j\xi_i \int_0^t dr \int_0^s dr'\, h(t-r)h(s-r') \\ &\quad \times \langle d_j^\dagger(r) d_i^\dagger(r') d_i(r') d_j(r)\rangle_T; \end{aligned} \tag{27}$$

we are using the notation $t \wedge s \equiv \min\{t,s\}$. Some more explicit expressions of means and correlations are given in Appendix A 3.

D. Postprocessing of the outputs

To realize the balanced homodyne detection scheme [21,22,30,32,39,40] we need to subtract the two output photocurrents from each couple of photodiodes (1, 3 and 2, 4); then, the limit of strong LO will be considered (after a possible scaling of the output signals). So, we end with the two output signals

$$X_j(t) = M_j(t) - M_{j+2}(t) = \xi_j \int_0^t h(t-s)dN_j(s) - \xi_{j+2}\int_0^t h(t-s)dN_{j+2}(s), \quad j = 1,2. \tag{28}$$

By (24) we see that the two stochastic processes $X_j(\cdot)$ are linear combinations of the counting processes $N_i(\cdot)$; again they represent the observed values of the compatible quantum observables

$$\hat{X}_j(t) = \int_0^t F_j(t,s)d\hat{N}_j(s) - \int_0^t F_{j+2}(t,s)d\hat{N}_{j+2}(s). \tag{29}$$

Remark 6. The usual scheme is to amplify the two difference currents, for instance, by a *transimpedance amplifier*, and to apply some suitable frequency filter [8,37]. This means that the processes $X_j(t)$ are modified by a second convolution; however, this procedure is equivalent to a single convolution with a modified response function and its effects are included in the structure (28). This electronic postprocessing gives the dimensions of a voltage to the observed processes; so, the physical dimension of the parameters ξ_j is that of a time multiplied by a voltage. The second amplification or deamplification stage can be used also to scale the total output signal. If some amplification is introduced also before the difference is taken, we can partially tune the coefficients ξ_j, in order to get a better balancing in the final output.

A typical choice is to include in $h(t)$ a Butterworth filter [8]; as a simple example we shall use an exponential response function

$$h(t) = \varkappa e^{-\varkappa t}. \tag{30}$$

As discussed again in [8], the amplification process inside the photodiodes produces some extra additive noise. Being additive and dependent only on the response function, we do not consider the electronic noise in the following, but we add it only in Sec. V A.

Again, the probability law of the stochastic processes is uniquely determined by their characteristic functional (Appendix B 2); here below we give means and correlations.

1. Means and correlations of the observed processes

The first moments can be obtained directly from the definition (28) and the moments of the photocurrents (A13) and (A14). First, we define the following coefficients:

$$\kappa_{11} = \eta_1\left[\eta_3\epsilon_1\xi_1^2 + (1-\eta_3)\epsilon_3\xi_3^2\right], \tag{31a}$$
$$\kappa_{21} = (1-\eta_1)\left[\eta_4\epsilon_2\xi_2^2 + (1-\eta_4)\epsilon_4\xi_4^2\right], \tag{31b}$$
$$\kappa_{12} = \eta_2\left[(1-\eta_3)\epsilon_1\xi_1^2 + \eta_3\epsilon_3\xi_3^2\right], \tag{31c}$$
$$\kappa_{22} = (1-\eta_2)\left[(1-\eta_4)\epsilon_2\xi_2^2 + \eta_4\epsilon_4\xi_4^2\right], \tag{31d}$$
$$\kappa_{13} = \sqrt{\eta_1\eta_2\eta_3(1-\eta_3)}(\epsilon_1\xi_1 + \epsilon_3\xi_3), \tag{31e}$$
$$\kappa_{23} = \sqrt{(1-\eta_1)(1-\eta_2)\eta_4(1-\eta_4)}(\epsilon_2\xi_2 + \epsilon_4\xi_4), \tag{31f}$$

$$\Delta_{11} = \eta_1[\eta_3\epsilon_1\xi_1 - (1-\eta_3)\epsilon_3\xi_3], \tag{32a}$$
$$\Delta_{21} = (1-\eta_1)[\eta_4\epsilon_2\xi_2 - (1-\eta_4)\epsilon_4\xi_4], \tag{32b}$$
$$\Delta_{12} = \eta_2[(1-\eta_3)\epsilon_1\xi_1 - \eta_3\epsilon_3\xi_3], \tag{32c}$$
$$\Delta_{22} = (1-\eta_2)[(1-\eta_4)\epsilon_2\xi_2 - \eta_4\epsilon_4\xi_4], \tag{32d}$$
$$\Delta_{13} = \sqrt{\eta_1\eta_2\eta_3(1-\eta_3)}\left(\epsilon_1\xi_1^2 - \epsilon_3\xi_3^2\right), \tag{32e}$$
$$\Delta_{23} = \sqrt{(1-\eta_1)(1-\eta_2)\eta_4(1-\eta_4)}\left(\epsilon_2\xi_2^2 - \epsilon_4\xi_4^2\right). \tag{32f}$$

Then, by using the field state introduced in Sec. II B, the definitions (A11), and the notation $:\cdot:$ for normal order, we

get easily, for $i, j = 1, 2$,

$$\mathbb{E}_P[X_j(t)] = \int_0^t dr\, h(t-r)\Big\{\kappa_{j3}(ie^{i\psi_j}\mathbb{E}_f\big[f(r)\langle a_1^\dagger(r)\rangle_T^f\big] + \text{c.c.}) + \Delta_{j1}\langle a_1^\dagger(r)a_1(r)\rangle_T + \Delta_{j2}\mathbb{E}_f[|f(r)|^2]\Big\}, \tag{33}$$

$$\begin{aligned}\mathbb{E}_P[X_j(t)X_i(s)] = {}& \delta_{ij}\int_0^{t\wedge s} dr\, h(t-r)h(s-r)\Big\{\kappa_{j1}\langle a_1^\dagger(r)a_1(r)\rangle_T + \kappa_{j2}\mathbb{E}_f[|f(r)|^2] + \Delta_{j3}(ie^{i\psi_j}\mathbb{E}_f\big[f(r)\langle a_1^\dagger(r)\rangle_T^f\big] + \text{c.c.})\Big\} \\ & + \int_0^t dr \int_0^s dr'\, h(t-r)h(s-r')\mathbb{E}_f\big[\langle: \{\Delta_{j1}a_1^\dagger(r)a_1(r) + \Delta_{j2}|f(r)|^2 + \kappa_{j3}(ie^{i\psi_j}f(r)a_1^\dagger(r) + \text{H.c.})\} \\ & \times \{\Delta_{i1}a_1^\dagger(r')a_1(r') + \Delta_{i2}|f(r')|^2 + \kappa_{i3}(ie^{i\psi_i}f(r')a_1^\dagger(r') + \text{H.c.})\} :\rangle_T^f\big].\end{aligned} \tag{34}$$

By these two equations one can write also the expression of $\mathrm{Cov}_P[X_j(t),\, X_i(s)]$.

Remark 7. Let us stress that the term starting by δ_{ij} in (34) comes out from the reordering of the creation and annihilation operators and, so, it represents the shot noise. Moreover, note that the phases ψ_j appear only in the terms containing the interference between signal and LO; so, they disappear when the signal vanishes.

In the expression of the means (33), the last two terms are due to some imbalance in the circuit, while the first term is an indication that the whole detection apparatus is a way to "measure" two quadratures of the signal field operator $a_1(t)$, even complementary quadratures (when $\phi \equiv \psi_2 - \psi_1 = \pm\pi/2$). The fact that these two observables do not commute implies the presence of some extra noise.

2. Balanced case

To gain some insight on the effects of imperfections it is useful to fix the perfectly balanced case:

$$\eta_j = 1/2, \quad \epsilon_j = \epsilon, \quad \xi_j = \xi. \tag{35}$$

This gives

$$\kappa_{j1} = \kappa_{j2} = \epsilon\xi^2/2, \quad \kappa_{j3} = \epsilon\xi/2, \quad \Delta_{ij} = 0. \tag{36}$$

As an example, Eqs. (33) and (34) become

$$\mathbb{E}_P[X_j(t)] = \frac{\epsilon\xi}{2}\, ie^{i\psi_j}\int_0^t dr\, h(t-r)\mathbb{E}_f\big[f(r)\langle a_1^\dagger(r)\rangle_T^f\big] + \text{c.c.}, \tag{37}$$

$$\begin{aligned}\mathbb{E}_P[X_j(t)X_i(s)] = {}& \delta_{ij}\frac{\epsilon\xi^2}{2}\int_0^{t\wedge s} dr\, h(t-r)h(s-r)\{\langle a_1^\dagger(r)a_1(r)\rangle_T + \mathbb{E}_f[|f(r)|^2]\} \\ & + \frac{\epsilon^2\xi^2}{4}\int_0^t dr\int_0^s dr'\, h(t-r)h(s-r')\mathbb{E}_f[\langle: (ie^{i\psi_j}f(r)a_1^\dagger(r) + \text{H.c.})(ie^{i\psi_i}f(r')a_1^\dagger(r') + \text{H.c.}) :\rangle_T^f].\end{aligned} \tag{38}$$

Remark 8 (Rebalancing). An intermediate case, suggested in [8], is when we are able to fine tune the efficiencies ϵ_j and/or the coefficients ξ_j (see Remarks 1 and 6), and we get $\Delta_{j2} = 0$. In this way we would eliminate the problem of a mean growing with the LO intensity [the last term in (33)]. At the same time the contribution of the laser intensity noise $\mathrm{Cov}_f[|f(r)|^2, |f(r')|^2]$ would disappear from the fluctuations of the observed processes.

III. STRONG LO AND DOUBLE-HOMODYNE DETECTION

When the interest is in the measurement of the two signal quadratures or in the secure QRNG protocol introduced in [11], we need to have a strong LO and to scale the observed processes.

Assumption 1. We assume the LO laser to have a constant mean intensity, as it holds for the model of Sec. II B,

$$\mathbb{E}_f\big[|f(t)|^2\big] = |\lambda|^2, \tag{39}$$

and we set

$$\tilde f(t) = f(t)\big/|\lambda|. \tag{40}$$

Then, we scale the outputs with respect to this mean intensity:

$$Y_j(t) = \frac{X_j(t)}{|\lambda|} = \int_0^t \frac{h(t-s)}{|\lambda|}[\xi_j dN_j(s) - \xi_{j+2}dN_{j+2}(s)]. \tag{41}$$

Recall that also the probability law P of the counting processes $N_j(t)$ depends on λ because the field state depends on f (see Sec. II B).

From (33) we get

$$\begin{aligned}\mathbb{E}_P[Y_j(t)] = \int_0^t dr\, h(t-r)\Big\{\kappa_{j3}\big(ie^{i\psi_j}\mathbb{E}_f\big[\tilde f(r)\langle a_1^\dagger(r)\rangle_T^f\big] \\ + \text{c.c.}\big) + \frac{\Delta_{j1}}{|\lambda|}\langle a_1^\dagger(r)a_1(r)\rangle_T + \Delta_{j2}|\lambda|\Big\}.\end{aligned} \tag{42}$$

If $\Delta_{j2} \neq 0$, the last term explodes when the laser intensity grows. We do not assume to be able to get a perfect rebalancing as in Remark 8, but only to limit the growth with the laser intensity of the terms containing the expression Δ_{j2},

so to have a moderate effect of the laser fluctuations at the working intensity of LO. By working at vanishing signal, we manage to tune the efficiency and transmissivity coefficients so to maintain a small mean up to the maximal LO power; this means to have $\Delta_{j2} \propto 1/|\lambda|_{\max}$.

Assumption 2. In mathematical terms, we set

$$G_{j2} = \Delta_{j2}|\lambda|/\kappa_{j3} \tag{43}$$

and we assume G_{j2} to be independent of λ. We also take η_j different from 0 and 1.

Now, we can take the limit $|\lambda| \to +\infty$ and the mean (42) becomes

$$\mathbb{E}_P[Y_j(t)] = \kappa_{j3} \int_0^t dr\, h(t-r)\Big\{\big(ie^{i\psi_j}\mathbb{E}_f\big[\tilde{f}(r)\langle a_1^\dagger(r)\rangle_T^f\big] + \text{c.c.}\big) + G_{j2}\Big\}, \tag{44}$$

while (34), (41), and (43) give, by direct calculations,

$$\text{Cov}_P\,[Y_j(t),\ Y_i(s)] = \delta_{ij}\kappa_{j2}\int_0^{t\wedge s} h(t-r)h(s-r)\,dr + \kappa_{j3}\kappa_{i3}\int_0^t dr\int_0^s dr'\, h(t-r)h(s-r')[C_f(j,r;i,r') + \mathtt{C}(j,r;i,r')], \tag{45}$$

where the first term is the shot-noise contribution and the two matrices in the double integral have the expressions

$$C_f(j,r;i,r') = \text{Cov}_f\left[G_{j2}|\tilde{f}(r)|^2 + \big(ie^{i\psi_j}\tilde{f}(r)\langle a_1^\dagger(r)\rangle_T^f + \text{c.c.}\big),\ G_{i2}|\tilde{f}(r')|^2 + \big(ie^{i\psi_i}\tilde{f}(r')\langle a_1^\dagger(r')\rangle_T^f + \text{c.c.}\big)\right], \tag{46}$$

$$\begin{aligned}\mathtt{C}(j,r;i,r') = \mathbb{E}_f\big[&e^{i(\psi_j-\psi_i)}\tilde{f}(r)\overline{\tilde{f}(r')}\big(\langle a_1^\dagger(r)a_1(r')\rangle_T^f - \langle a_1^\dagger(r)\rangle_T^f\langle a_1(r')\rangle_T^f\big)\\ &- e^{i(\psi_i+\psi_j)}\tilde{f}(r)\tilde{f}(r')\big(\langle a_1^\dagger(r)a_1^\dagger(r')\rangle_T^f - \langle a_1^\dagger(r)\rangle_T^f\langle a_1^\dagger(r')\rangle_T^f\big) + \text{c.c.}\big].\end{aligned} \tag{47}$$

The matrix (47) vanishes when the signal is in a coherent state, and it can be not positive definite when the signal is in a squeezed state. It is important to stress that only the sum of the shot noise plus the contribution of (47) is guaranteed to be a positive-definite matrix.

A. Reduced description and the probability law in the limit of strong LO

Up to now we have considered only observables represented by commuting self-adjoint operators and the associated pvm in the Fock space Γ, a Hilbert space with the tensor product structure (A1). Indeed, also to the processes $Y_j(t)$ we can associate the self-adjoint operators $\hat{Y}_j(t)$ by the operator version of (41); these are again compatible observables, as they are linear combinations of the compatible number operators (see Remark 4). POVMs enter into play when a reduced description is considered: the characteristic operator is reduced to the factor Γ_1, where the signal lives, by using the fact that the state in the complementary factor is fixed. By this technique we can show that the limit for $|\lambda| \to +\infty$ exists for the whole law of the processes $Y_j(\cdot)$, not only for the first moments, and that this probability law is linked to a POVM describing the joint measurement of two quadratures of the signal field.

To have a clear picture of the underlying POVM, it is convenient to suitably decompose the coefficients κ_{j2}, which appear in the shot-noise term in (45). By direct computations based on (31) and (32), one can check that the following equality holds:

$$\kappa_{j2} = \kappa_{j3}^2\big(G_{j3} + V_j^{\,2} + \sigma_j^{\,2} + 1\big), \tag{48}$$

where

$$G_{13} = \frac{1-\eta_1}{\eta_1}, \quad G_{23} = \frac{\eta_1}{1-\eta_1}, \tag{49a}$$

$$V_1^{\,2} = \frac{\Delta_{12}^2}{\eta_2\kappa_{13}^2} = \frac{\tilde{V}_1^{\,2}}{\eta_1},$$

$$V_2^{\,2} = \frac{\Delta_{22}^2}{(1-\eta_2)\kappa_{23}^2} = \frac{\tilde{V}_2^{\,2}}{1-\eta_1}, \tag{49b}$$

$$\tilde{V}_j^{\,2} = \frac{[(1-\eta_{j+2})\epsilon_j\xi_j - \eta_{j+2}\epsilon_{j+2}\xi_{j+2}]^2}{\eta_{j+2}(1-\eta_{j+2})(\epsilon_j\xi_j + \epsilon_{j+2}\xi_{j+2})^2}, \tag{49c}$$

$$\sigma_1^{\,2} = \frac{\tilde{\sigma}_1^{\,2}}{\eta_1}, \quad \sigma_2^{\,2} = \frac{\tilde{\sigma}_2^{\,2}}{1-\eta_1},$$

$$\tilde{\sigma}_j^{\,2} = \frac{\frac{\epsilon_j(1-\epsilon_j)}{\eta_{j+2}}\xi_j^{\,2} + \frac{\epsilon_{j+2}(1-\epsilon_{j+2})}{1-\eta_{j+2}}\xi_{j+2}^{\,2}}{(\epsilon_j\xi_j + \epsilon_{j+2}\xi_{j+2})^2}. \tag{49d}$$

The contribution $\sigma_j^{\,2}$ represents some extra noise due to the presence of optical losses, as it vanishes when $\epsilon_j = \epsilon_{j+2} = 1$; this noise is of quantum origin because it is due to the need of preserving CCRs as discussed in Sec. II A 2. The contribution $V_j^{\,2}$ is due to the unbalancing and, by Assumption 2, it is small.

Proposition 1. With the above assumptions, the characteristic functional of the processes $Y_j(\cdot)$ admits a limit for $|\lambda| \to +\infty$; so, we can write

$$\Phi_T^Y[\vec{k}] = \lim_{|\lambda|\to+\infty}\mathbb{E}_P\left[\exp\left\{\frac{i}{|\lambda|}\sum_{j=1}^2\int_0^T k_j(s)X_j(s)ds\right\}\right]. \tag{50}$$

The structure of the characteristic functional (50) turns out to be given by

$$\Phi_T^Y[\vec{k}] = \mathbb{E}_f\big[\Phi_T^Z[\vec{k}^T; f]\big],$$

$$k_j^T(t) = \kappa_{j3}\int_t^T h(s-t)k_j(s)ds, \tag{51a}$$

$$\Phi_T^Z[\vec{k}; f] = \Phi_T^Q[\vec{k}; f]\Gamma_T[\vec{k}; f], \tag{51b}$$

$$\Phi_T^Q[\vec{k};f] = \mathrm{Tr}_{\Gamma_1}\left\{\hat{\Psi}_T^Q[\vec{k};f]\rho_1^{f,T}\right\}, \tag{51c}$$

$$\Gamma_T[\vec{k};f] = \exp\left\{\int_0^T ds\left|\tilde{f}(s)\right|^2 \sum_{j=1}^{2}\left[ik_j(s)G_{j2} - \frac{\sigma_j^2 + V_j^2}{2}k_j(s)^2\right]\right\}. \tag{51d}$$

With a fixed $\tilde{f}(t)$, the quantity $\hat{\Psi}_T^Q[\vec{k};f]$ is the characteristic operator of a POVM on the Hilbert space Γ_1, having the expression

$$\hat{\Psi}_T^Q[\vec{k};f] = \exp\int_0^T\left\{i\sum_{j=1}^{2}k_j(t)d\hat{Q}_j(t) - \frac{1}{2}\sum_{i,j=1}^{2}k_j(t)\Xi_{ji}k_i(t)\left|\tilde{f}(t)\right|^2 dt\right\}, \tag{52a}$$

$$d\hat{Q}_j(t) = ie^{i\psi_j}\tilde{f}(t)dA_1^\dagger(t) + \mathrm{H.c.},$$

$$\Xi = \begin{pmatrix} G_{13} & -\cos\phi \\ -\cos\phi & G_{23}\end{pmatrix}. \tag{52b}$$

In the formulas above, $\tilde{f}$ and G_{j2} are introduced in Assumptions 1 and 2, the phase ϕ is defined in (6), the expressions of κ_{j3} and σ_j^2 are given in (31) and (49d); the matrix Ξ is non-negative definite.

The proof of the proposition above is given in Appendix B 3, where also the following corollary is proved.

Corollary 2. Let the signal state be a mixture of coherent states, given by $\rho_1^{f,T} \to \rho_1^{f_s,T} = |e_1(f_s)\rangle\langle e_1(f_s)|$, where $f_s(t)$ is a stochastic process and P_f is the joint probability distribution of the processes f_s and $\tilde{f}$, as in Appendix B 1 a. By using the notations of Proposition 1, we have

$$\Phi_T^Z[\vec{k};f] = \exp\sum_{j=1}^{2}\int_0^T dt\left\{ik_j(t)[G_{j2}|\tilde{f}(t)|^2 + (ie^{i\psi_j}\overline{f_s(t)}\tilde{f}(t) + \mathrm{c.c.})] - \frac{\kappa_{j2}}{2\kappa_{j3}^2}k_j(t)^2|\tilde{f}(t)|^2\right\}. \tag{53}$$

1. Structure of the observed processes

When $|\tilde{f}(s)|$ is a nonrandom given function, the expression (51d) is the characteristic functional of the increments of a bidimensional Gaussian process, which we denote by $L_j^f(t)$, which can be expressed as

$$L_j^f(t) = G_{j2}\int_0^t|\tilde{f}(s)|^2 ds + \sigma_j\int_0^t|\tilde{f}(s)|dW_{j1}(s) + V_j\int_0^t|\tilde{f}(s)|dW_{j2}(s), \tag{54}$$

where the four processes W_{ji} are independent, standard Wiener processes (their formal time derivatives are white noises).

Let us consider now the POVM (in continuous time) determined by the characteristic operator (52) and let us denote by $Q_j^f(t)$ the corresponding observables, measured in the signal state $\rho_1^{f,T}$. Then, the quantity $\Phi_T^Q[\vec{k};f]$, given by (51c), is the characteristic functional of the random processes $Q_j^f(t)$.

As the product of two characteristic functionals is the characteristic functional of the sum process, the quantity $\Phi_T^Z[\vec{k};f]$ in (51b) is the characteristic functional of the processes

$$Z_j^f(t) = Q_j^f(t) + L_j^f(t). \tag{55}$$

Then, $\Phi_T^Z[\vec{k}^T;f]$, with $\vec{k}^T$ defined in (51a), is the characteristic functional of the processes

$$Y_j^f(t) = \kappa_{j3}\int_0^t h(t-s)dZ_j^f(s). \tag{56}$$

Let us summarize the physical meaning of these results. The first equality in (51a) says that the probability law of the observed processes $Y_j(t)$ is a *mixture* of the probability laws of the processes $Y_j^f(t)$ with respect to the law of the random function f (see Remark 2), i.e., with respect to the LO fluctuations. Then, by the results (56) and (55), the processes $Y_j^f(t)$ are a smoothed and noisy versions of the processes $Q_j^f(t)$, whose characteristic functional is given by (51c) and the associated characteristic operator by (52a). Finally, by the structure of this characteristic operator (52a), we can interpret the associated POVM as a joint measurement of the "dilated quadratures" (52b). In some sense, the whole apparatus gives a joint noisy measurement of the field quadratures (52b).

2. Measured quadratures

The measured field quadratures (52b) satisfy the commutation relations

$$\left[\frac{d\hat{Q}_1(t)}{dt}, \frac{d\hat{Q}_2(s)}{ds}\right] = 2i\sin\phi|\tilde{f}(t)|^2\delta(t-s),$$

$$[\hat{Q}_j(t), \hat{Q}_j(s)] = 0. \tag{57}$$

Note that these quadratures are not complementary when $|\sin\phi| \neq 1$ and that they are random operators, as they contain the random process $\tilde{f}(t)$ [Eqs. (14) and (40)]. For $\sin\phi \neq 0$ the two quadratures do not commute and a joint pvm does not exist; indeed, the second term in (52a) represents some noise needed to have a true POVM. However, in general, this noise is not minimal. For instance, for $\phi = n\pi$ the two quadratures (52b) are compatible quantum observables and the whole noise in (52a) is due to the way the measurement is realized, but it is not necessary on a pure mathematical ground.

For $\phi = n\pi + \pi/2$, instead, the quadratures (52b) are orthogonal and (52a) can be written as

$$\hat{\Psi}_T^Q[\vec{k};f] = \exp\int_0^T\left\{i[\tilde{f}(t)k(t)ie^{i\psi_2}dA_1^\dagger(t) + \mathrm{H.c.}] - \frac{1}{2}|\alpha k(t) + \alpha(1-2\eta_1)\overline{k(t)}|^2|\tilde{f}(t)|^2 dt\right\}, \tag{58}$$

$$k(t) = k_1(t) + ik_2(t), \quad \alpha = \frac{1}{\sqrt{4\eta_1(1-\eta_1)}}$$

$$\Rightarrow \quad \alpha \geqslant 1, \quad \alpha|1-2\eta_1| = \sqrt{\alpha^2-1}.$$

The associated POVM was already introduced in [20, Sec. III]; the case with $\alpha = 1$, i.e., $\eta_1 = \frac{1}{2}$, it is a generalization to fields in continuous time of the POVM constructed from coherent states of a single mode, having the Husimi function as probability density.

B. Homodyne and heterodyne detection

As observed in Remark 7, the phases ψ_j disappear from the moments of the observed processes in the case of vanishing signal. Similarly, also the contributions of the LO phase fluctuations disappear from the distributions of the processes $X_j(\cdot)$, $Y_j(\cdot)$ [see (33), (34), (44)–(47), (B13), (52), and (57)]. This is due to the fact that we are taking equal the optical paths arriving to the various interference points (the beam splitters). Things are different when the circuit is used as detection apparatus and there is interference between LO and signal. To detect squeezing in homodyne spectra, it is necessary to maintain phase coherence for a sufficiently long time; the LO must be phase locked to the signal [19] and this can be realized by taking as signal the light generated by some system stimulated by the same laser which produces the LO (mathematically, both LO and signal depend on f [33], see Remark 3).

To understand the effect of the phase fluctuations, let us consider the case of a signal state totally independent of f; we take the laser model of Secs. II B and A 2 and we study means and fluctuations of the processes $Y_j(\cdot)$. In Eqs. (44)–(47) the f dependence in the signal state disappears; then, by the expressions of the f moments (A5), we get

$$\mathbb{E}_P[Y_j(t)] = \kappa_{j3}\int_0^t dr\, h(t-r)\{we^{-\gamma_0 r}(ie^{i(\psi_j+\theta-\omega_0 r)}\langle a_1^\dagger(r)\rangle_T + \text{c.c.}) + G_{j2}\}, \tag{59a}$$

$$\begin{aligned} C_f(j,r;i,r') = {} & G_{j2}G_{i2}\frac{v(r-r')}{2}[2w^2 + v(r-r')] + 2iG_{j2}v(r-r')we^{i(\psi_i+\theta-\omega_0 r')-\gamma_0 r'}\langle a_1^\dagger(r')\rangle_T \\ & + 2iG_{i2}v(r-r')we^{i(\psi_j+\theta-\omega_0 r)-\gamma_0 r}\langle a_1^\dagger(r)\rangle_T \\ & + e^{i(\psi_i+\psi_j+2\theta)-(i\omega_0+\gamma_0)(r+r')}\langle a_1^\dagger(r)\rangle_T\langle a_1^\dagger(r')\rangle_T\{w^2 - [w^2+v(r-r')]e^{-2\gamma_0(r\wedge r')}\} \\ & + e^{i(\psi_j-\psi_i)+i\omega_0(r'-r)-\gamma_0|r-r'|}\langle a_1^\dagger(r)\rangle_T\langle a_1(r')\rangle_T[w^2 + v(r-r') - w^2e^{-2\gamma_0(r\wedge r')}] + \text{c.c.}, \end{aligned} \tag{59b}$$

$$\begin{aligned} \mathtt{C}(j,r;i,r') = {} & e^{i[\psi_j-\psi_i+\omega_0(r'-r)]-\gamma_0|r-r'|}[w^2+v(r-r')](\langle a_1^\dagger(r)a_1(r')\rangle_T - \langle a_1^\dagger(r)\rangle_T\langle a_1(r')\rangle_T) \\ & - e^{i[\psi_i+\psi_j+2\theta-\omega_0(r+r')]-\gamma_0[4(r\wedge r')+|r-r'|]}[w^2+v(r-r')](\langle a_1^\dagger(r)a_1^\dagger(r')\rangle_T - \langle a_1^\dagger(r)\rangle_T\langle a_1^\dagger(r')\rangle_T) + \text{c.c.} \end{aligned} \tag{59c}$$

Let us consider now the extreme case of an incoherent LO (the coherence time $1/\gamma_0$ is small); this means to take the relevant times to be large: $t, s \gg 1/\gamma_0, t, s \gg \tau$, where τ is the decaying time of $h(t)$. From Eqs. (59) and (45) we get

$$\mathbb{E}_P[Y_j(t)] = \kappa_{j3}\int_0^t dr\, h(t-r)G_{j2} \simeq \kappa_{j3}G_{j2}, \tag{60a}$$

$$\begin{aligned} \text{Cov}_P[Y_j(t), Y_i(s)] \simeq {} & \delta_{ij}\kappa_{j2}\int_0^{t\wedge s} h(t-r)h(s-r)\,dr + \kappa_{j3}G_{j2}\kappa_{i3}G_{i2}G_v(t,s) \\ & + \kappa_{j3}\kappa_{i3}\int_0^t dr\int_0^s dr'\, h(t-r)h(s-r')e^{-\gamma_0|r-r'|}[e^{i[\psi_j-\psi_i+\omega_0(r'-r)]}\langle a_1^\dagger(r)a_1(r')\rangle_T[w^2+v(r-r')] + \text{c.c.}], \end{aligned} \tag{60b}$$

$$G_v(t,s) = \int_0^t dr\int_0^s dr'\, h(t-r)h(s-r')v(r-r')[2w^2+v(r-r')]. \tag{60c}$$

In this limit, the terms with two annihilators or two creators disappear from the matrix (59c) and each of the three terms (60b) is a positive-definite matrix for every choice of the signal state; so, it is not possible to detect squeezing. We can say that this is the limit of heterodyne detection: the phase fluctuations in the LO destroy any phase coherence [32,33]. Let us note that in (45) and (47) the contribution of $\langle a_1^\dagger(r)a_1^\dagger(r')\rangle_T$ is cut again when its frequency spectrum is far from ω_0; we can speak of heterodyne detection also in this case.

The other extreme case is pure homodyning. Without correlations between signal and LO to attenuate the coherence losses, we need to have a highly coherent LO ($1/\gamma_0$ is very large), say $\gamma_0 = 0$ or $t, s \ll 1/\gamma_0$. Now, the terms with two annihilators or two creators survive and the possible presence of negative eigenvalues of the matrix $\mathtt{C}(j,r;i,r')$ can allow to detect squeezing [28,34].

Let us stress that we are speaking of homodyne detection when the measurement is phase sensitive, independently from the fact that a single quadrature or two orthogonal ones are monitored; essentially this terminology is used also in [12,18,32], while in [11] they use the term "heterodyne detection" for the case of monitoring of two complementary quadratures.

An application of detection in continuous time is to construct a consistent quantum theory of the various types of spectra for the signal. In the heterodyne regime, by varying the frequency of the LO, the *power spectrum* of the signal

can be studied [34,45,46], while in the homodyne regime we have the *homodyne spectrum* and the *spectrum of squeezing* [28,34,45,46]. By using the eight-port circuit we get in the same run the spectra of two complementary quadratures.

IV. DISCRETE SAMPLING

The output of the apparatus of Fig. 1 is in continuous time, but in many experimental situations it is sampled at discrete times. This can happen both when it is used for QRNG [5,11], and when it is used as a detection apparatus for the signal quadratures, as it is done for the outputs of various optical circuits [43]. Sometimes a pulsed laser can be used as LO [6,8,19,37]; in this situation, even a single detection per pulse is considered.

For instance, in the case of QRNG, the output of the difference photocurrents [the couple of processes $X_j(t)$] is sampled by an oscilloscope; the laser can be either CW or pulsed. The sampling rate will determine the maximum generation rate of the random numbers, while the ADC that digitizes the signal determines the number of bits per sample and also limits the maximum level of output photocurrents that can be used without saturating the instrument.

In QRNG we need the samples at different times to be independent; eventually, this result can be obtained by undersampling when some correlation is detected in the experimental data. In view of this, we take the sampling times such that correlations for observations at different times can be due only to the signal. This choice is not necessary when the apparatus is used for signal detection, but even in this case it simplifies some mathematical expressions.

Assumption 3. We assume that the sampling process is done at m times $t_1, t_2, \dots, t_m$ with $t_1 > t_0 \geqslant 0$ and with an intertime $t_l - t_{l-1} \geqslant \tau$, where τ is such that the response function and the intensity correlations are nearly completely decayed:

$$h(t) \simeq 0, \quad t \geqslant \tau,$$
$$\mathrm{Cov}_f[|f(t)|^2, |f(s)|^2] \simeq 0, \quad |t-s| \geqslant \tau. \tag{61}$$

For the laser model of Sec. II B, by Eq. (A5d), the decaying of the correlations is equivalent to $v(t) \simeq 0$ for $|t| \geqslant \tau$.

A. Observed processes

We start by considering the sampling of the observed processes $X_j(\cdot)$, introduced in Sec. II D. Means and correlations of the observed samples can be obtained by Eqs. (33) and (34). By Assumption 3, the covariance of two observations at different times can be different from zero only due to correlations introduced by the signal state. In particular, when the signal state is a coherent one, the covariance of observations at different times vanishes.

For QRNG it is of main interest the case of pure noise; when the signal is in the vacuum state, from (33), (34), (39), (40), and (13) we get

$$\mathbb{E}_P[X_j(t_l)] \simeq \Delta_{j2}|\lambda|^2 \int_{t_l-\tau}^{t_l} dr\, h(t_l - r) \simeq \Delta_{j2}|\lambda|^2, \tag{62a}$$
$$\mathrm{Cov}_P[X_j(t_l),\, X_i(t_{l'})] \simeq \delta_{ll'}(\delta_{ij}\kappa_{j2}|\lambda|^2 S_0 + \Delta_{j2}\Delta_{i2}|\lambda|^4 C_0), \tag{62b}$$
$$S_0 = \int_{t_l-\tau}^{t_l} dr\, h(t_l - r)^2 \simeq \int_0^{+\infty} dr\, h(r)^2, \tag{62c}$$
$$C_0 = \int_{t_l-\tau}^{t_l} dr \int_{t_l-\tau}^{t_l} dr'\, h(t_l - r)h(t_l - r')\mathbb{E}_f[n_{\mathrm{RIN}}(r)n_{\mathrm{RIN}}(r')]. \tag{62d}$$

If the intensity fluctuations vanish, $X_1(t_l)$ and $X_2(t_l)$ become uncorrelated. In the case of the laser model of Sec. II B, the RIN contribution C_0 becomes

$$\begin{aligned} C_0 &= 2\int_{t_l-\tau}^{t_l} dr \int_{t_l-\tau}^{t_l} dr'\, h(t_l - r)h(t_l - r')v(r - r')[2w^2 + v(r - r')] \\ &\simeq 2\int_0^{+\infty} ds \int_0^{+\infty} ds'\, h(s)h(s')v(s - s')[2w^2 + v(s - s')]. \end{aligned} \tag{63}$$

As an example, we can consider the case of an exponential response function (30) and exponential correlations (A6); then, we have

$$S_0 = \frac{\varkappa}{2}, \quad C_0 = \frac{2\varkappa(1-w^2)}{\varkappa + 2\gamma_1}\left(1 + w^2 + \frac{2\gamma_1 w^2}{\varkappa + \gamma_1}\right), \tag{64}$$

where $w^2 \leqslant 1$. Independently of the laser model, S_0 and C_0 are two parameters to be estimated from the data. As noted in Remark 7, phases no longer play any role. So, if we are only interested in the shot noise for random-number generation, the relative phases do not have any effect on the statistics of the generated numbers.

In the case of signal in the vacuum state, the observables $X_j(t_l)$ come from a mixture of distributions of linear combinations of Poisson processes [Remark 5, Eq. (28)]. However, by the effect of an LO intensity $|\lambda|^2$ not too small and of the smoothing on time due to the detector response function, we can rely on a normal approximation of the distribution of the observed processes. Therefore, the observations $(X_1(t_l), X_2(t_l))$ can be considered a random sample from an (approximately) bi-variate normal distribution with means and covariances given by (62).

B. Scaled processes

We consider now the discrete sampling of the scaled processes $Y_j(t)$ in the case of strong LO; this is the situation considered, for instance, in [8,11]. Means and covariances of the random variables $Y_j(t_l)$ are obtained immediately by particularizing Eqs. (44)–(47) and by taking into account Assumption 3. In the case of vanishing signal as above, we get means and covariances simply by applying the scaling (41) to Eqs. (62):

$$\mathbb{E}_P[Y_j(t_l)] \simeq \kappa_{j3} G_{j2},$$
$$\mathrm{Cov}_P[Y_j(t_l),\, Y_i(t_l')] \simeq \delta_{ll'}(\delta_{ij}\kappa_{j2}S_0 + \kappa_{j3}G_{j2}\kappa_{i3}G_{i2}C_0). \quad (65)$$

The coefficients $\kappa_{j2},\ \kappa_{j3},\ G_{j2}$ are defined in (31) and (43).

In the case of the observables $Y_j(t_l)$, by the results of Sec. III A, we can obtain their characteristic function and, so, their full probability distribution.

1. Discrete mode operators

To get explicitly the characteristic function of the observables $Y_j(t_l)$ and the associated POVM, it is convenient to introduce suitable bosonic mode operators. Moreover, this construction gives a link between the quantum field approach to optical circuits and the more usual discrete mode approach.

We define the operators

$$a_l = \frac{-i}{R_l(f)} \int_{t_l-\tau}^{t_l} h(t_l - s)\overline{\tilde{f}(s)}\, e^{-i\psi_1} dA_1(s), \quad (66a)$$

$$\hat{q}_1^l = \hat{q}_1^l(\phi) = \frac{1}{\sqrt{2}}(a_l^\dagger + a_l), \quad (66b)$$

$$\hat{q}_2^l(\phi) = \frac{1}{\sqrt{2}}(e^{i\phi}a_l^\dagger + e^{-i\phi}a_l), \quad (66c)$$

$$R_l(f) = \left(\int_0^\tau dr\, h(r)^2 \left|\tilde{f}(t_l - r)\right|^2 \right)^{1/2}. \quad (66d)$$

Let us note that the normalization constant (66d) is a random quantity and that, by (62c), (66d), and (16), we have

$$\mathbb{E}_f[R_l(f)^2] = S_0. \quad (67)$$

Remark 9. The operators a_l and $a_l^\dagger$ are discrete mode operators, satisfying the CCRs, while $\hat{q}_1^l$ and $\hat{q}_2^l(\phi)$ are two quadratures, not complementary in general:

$$[a_{l'},\, a_l^\dagger] = \delta_{ll'}, \quad [a_{l'},\, a_l] = 0, \quad [\hat{q}_1^l,\, \hat{q}_2^l(\phi)] = i\,\sin\phi. \quad (68)$$

All these operators contain $\tilde{f}$: *they are random operators*.

The operators $\hat{q}_j^l(\phi)$ can be expressed in terms of the quantum observables (52b), introduced in Sec. III; indeed, we have

$$\hat{q}_j^l(\phi) = \frac{1}{\sqrt{2}R_l(f)} \int_{t_l-\tau}^{t_l} h(t_l - s) d\hat{Q}_j(s).$$

To give the structure of our POVM, we shall need also squeezed coherent states; here we introduce some notation. First, we decompose the Hilbert space Γ_1 and the vacuum state into the tensor product forms

$$\Gamma_1 = \Gamma_1^\perp \otimes \prod_l{}^{\otimes} \Gamma_1^l, \quad e_1(0) = e_1^\perp(0) \otimes \prod_l{}^{\otimes} e_1^l(0).$$

The component Γ_1^l is such that $\{a_l,\, a_l^\dagger,\, \Gamma_1^l\}$ gives an irreducible representation of the CCRs for a single mode. Then, we introduce the displacement operator and the squeezing operator

$$D_l(z) = \exp\left\{z a_l^\dagger - \bar{z}\, a_l\right\},$$
$$S_{\alpha,\beta}^l = \exp\left\{\frac{\xi}{2}\, a_l^{\dagger 2} - \frac{\bar{\xi}}{2}\, a_l^2\right\}, \quad \xi = \frac{\beta}{|\beta|}\cosh^{-1}\alpha; \quad (69a)$$

to have a well-defined squeezing operator the coefficients $\alpha,\ \beta$ must satisfy

$$\alpha \in \mathbb{R}, \quad \beta \in \mathbb{C}, \quad \alpha^2 - |\beta|^2 = 1. \quad (69b)$$

By introducing also the unitary operator

$$U_l(\phi) = \exp\left\{ i\left(\phi - \frac{\pi}{2}\right) a_l^\dagger a_l \right\},$$

we define the squeezed mode operator

$$b_l = S_{\alpha,\beta}^l U_l(\phi) a_l U_l(\phi)^\dagger S_{\alpha,\beta}^{l\,\dagger} = ie^{-i\phi}\left(\alpha a_l + \beta a_l^\dagger\right). \quad (70)$$

Finally, we introduce the coherent states for the mode b_l:

$$\psi_l(z;\alpha,\beta) = S_{\alpha,\beta}^l U_l(\phi) D_l(z) e_1^l(0),$$
$$b_l\psi_l(z;\alpha,\beta) = z\psi_l(z;\alpha,\beta), \quad \psi_l(0;1,0) = e_1^l(0). \quad (71)$$

2. Probability distribution in case of strong LO

The *characteristic function* of the $2m$ random variables $Y_j(t_l)$,

$$\Phi^{\vec{Y}}(\vec{k}) = \mathbb{E}_P\left[\exp\left\{ i \sum_{jl} k_j^l Y_j(t_l) \right\} \right], \quad (72)$$

is directly obtained from the *characteristic functional* $\Phi_T^Y[\vec{k}]$ [Eq. (50)] of the stochastic process $Y_j(\cdot)$ by taking $k_j(s) = \sum_{l=1}^m k_j^l \delta(s - t_l)$. To understand the structure of these random variables, we elaborate this characteristic function.

Proposition 3. Under Assumption 3, the characteristic function (72) of the random variables $Y_j(t_l)$ is given by

$$\Phi^{\vec{Y}}(\vec{k}) = \mathbb{E}_f[\Gamma^{\mathcal{L}}(\vec{k};f)\Phi^{\mathcal{Q}}(\vec{k};f)],$$
$$\Phi^{\mathcal{Q}}(\vec{k};f) = \mathrm{Tr}_{\Gamma_1}\left\{\hat{\Psi}^q(\vec{k};f)\rho_1^{f,T}\right\}, \quad (73)$$
$$\Gamma^{\mathcal{L}}(\vec{k};f) = \prod_{l=1}^m \Gamma_l^{\mathcal{L}}(\vec{k}^l;f),$$
$$\hat{\Psi}^q(\vec{k};f) = \prod_{l=1}^m \hat{\Psi}_l^q(\vec{k}^l;f), \quad (74)$$

$$\Gamma_l^{\mathcal{L}}(\vec{k}^l;f) = \exp\left\{ \sum_{j=1}^2 \left[ik_j^l\, \mu_{\mathcal{L}}^{jl}(f) - \frac{{k_j^l}^2}{2}\, \sigma_{\mathcal{L}}^{jl}(f)^2 \right] \right\}, \quad (75a)$$

$$\mu_{\mathcal{L}}^{jl}(f) = G_{j2}\kappa_{j3}\int_0^\tau ds|\tilde{f}(t_l - s)|^2 h(s), \tag{75b}$$

$$\sigma_{\mathcal{L}}^{jl}(f)^2 = \left(\sigma_j^{\,2} + V_j^{\,2}\right)\kappa_{j3}^{\,2}\int_0^\tau ds|\tilde{f}(t_l - s)|^2 h(s)^2 = \left(\sigma_j^{\,2} + V_j^{\,2}\right)\kappa_{j3}^{\,2} R_l(f)^2, \tag{75c}$$

$$\hat{\Psi}_l^q(\vec{k}^l; f) = \exp\left\{ i\sqrt{2}\,R_l(f)\left[\kappa_{13}k_1^l\hat{q}_1^l + \kappa_{23}k_2^l\hat{q}_2^l(\phi)\right] - \frac{R_l(f)^2}{2}\left|\sqrt{\frac{1-\eta_1}{\eta_1}}\,\kappa_{13}k_1^l - e^{-i\phi}\sqrt{\frac{\eta_1}{1-\eta_1}}\,\kappa_{23}k_2^l\right|^2\right\}. \tag{76}$$

For fixed $\tilde{f}$, the operator $\hat{\Psi}_l^q(\vec{k}^l; f)$ is the characteristic operator of a POVM on the Hilbert space Γ_1; the same statement holds for the product $\hat{\Psi}^q(\vec{k}; f)$.

The proof of Proposition 3 is given in Appendix B 4.

When $\sin\phi = 0$, i.e., $\phi = n\pi$, one has $\hat{q}_2^l(2n\pi) = \hat{q}_1^l$, $\hat{q}_2^l(2n\pi + \pi) = -\hat{q}_1^l$. In this case, a measurement of the two quadratures is trivially represented by a pvm; the part with the squared modulus in (76) is some additive noise.

In the case $\sin\phi \neq 0$ instead, we shall see that the characteristic operator $\hat{\Psi}_l^q(\vec{k}^l; f)$ can be expressed through the Fourier transform of a POVM density based on squeezed coherent states; this measure is in a class which generalizes the POVM constructed starting from the Husimi transform [20, Eqs. (3.4)–(3.10)], [31, Chap. 4].

Proposition 4. Let us take the case $\sin\phi \neq 0$ and fix the squeezing parameters (69b) by

$$\alpha = \frac{1}{2\sqrt{\eta_1(1-\eta_1)}\,\sin\phi},$$
$$\beta = \frac{e^{2i\phi}(1-\eta_1) + \eta_1}{2\sqrt{\eta_1(1-\eta_1)}\,\sin\phi}. \tag{77}$$

Then, the characteristic operator (76) can be written as

$$\hat{\Psi}_l^q(\vec{k}^l; f) = \exp\left\{ i(u_l b_l^\dagger + \overline{u_l}\,b_l) - \tfrac{1}{2}|u_l|^2\right\}, \tag{78a}$$

where b_l is defined in (70) and

$$u_l = R_l(f)\left[\sqrt{\frac{1-\eta_1}{\eta_1}}\,\kappa_{13}k_1^l - e^{-i\phi}\sqrt{\frac{\eta_1}{1-\eta_1}}\,\kappa_{23}k_2^l\right]. \tag{78b}$$

Moreover, we have

$$\hat{\Psi}_l^q(\vec{k}^l; f) = \int_{\mathbb{C}} d^2z\, e^{i(u_l\,\bar{z} + \overline{u_l}\,z)}\hat{g}_{\alpha,\beta}^l(z),$$
$$\hat{g}_{\alpha,\beta}^l(z) = \frac{1}{\pi}|\psi_l(z;\alpha,\beta)\rangle\langle\psi_l(z;\alpha,\beta)|; \tag{79}$$

$\hat{g}_{\alpha,\beta}^l(z)$ is a POVM density on $\mathbb{C}$ with respect to the Lebesgue measure d^2z.

The proof of Proposition 4 is given in Appendix B 4.

Remark 10. Let us note that, when $\eta_1 = \frac{1}{2}$ and $\phi = \pi/2$ we get $(\alpha, \beta) = (1, 0)$ and $b_l = a_l$; then, the POVM (79) reduces to the usual measure based on the coherent states of the "random" modes a_l (cf. Remark 9). So, squeezed states appear in the measurement operators when $|\sin\phi| \neq 1$, which means that two not exactly complementary quadratures are involved, and/or that $\eta_1 \neq \frac{1}{2}$, which means an imbalance in the beam splitter which divides the signal into the two measured components.

C. Probability density

By the results of Sec. IV B 2, we can write explicitly the POVM density and the probability distribution of the observables $(Y_1(t_l), Y_2(t_l))$, when $\sin\phi \neq 0$, $\eta_1 \neq 0,\ 1$. From Eqs. (73) and (74) we get the characteristic operator

$$\hat{\Psi}_l^Y(\vec{k}^l; f) = \Gamma_l^{\mathcal{L}}(\vec{k}^l; f)\hat{\Psi}_l^q(\vec{k}^l; f), \tag{80}$$

where the two factors are given in (75) and (79). We assume also $\sigma_{\mathcal{L}}^{jl}(f)^2 > 0$; let us note that the electronic noise can be taken into account by increasing the variances (75c).

As proved in Appendix B 4, the POVM density associated with the characteristic operator (80) has the expression

$$\hat{g}_Y^l(y_1, y_2; f) = \frac{1}{2\pi\sigma_{\mathcal{L}}^{1l}(f)\sigma_{\mathcal{L}}^{2l}(f)}\int_{\mathbb{C}} d^2z\,\hat{g}_{\alpha,\beta}^l(z)$$
$$\times \exp\left\{-\frac{\left[\mu_{\mathcal{L}}^{2l}(f) + 2K_2^l(f)(z_2\sin\phi - z_1\cos\phi) - y_2\right]^2}{2\sigma_{\mathcal{L}}^{2l}(f)^2}\right\}$$
$$\times \exp\left\{-\frac{\left[\mu_{\mathcal{L}}^{1l}(f) + 2K_1^l(f)z_1 - y_1\right]^2}{2\sigma_{\mathcal{L}}^{1l}(f)^2}\right\}, \tag{81}$$

where $\mu_{\mathcal{L}}^{jl}(f)$ and $\sigma_{\mathcal{L}}^{jl}(f)$ are given in (75), $z = z_1 + iz_2$, and

$$K_1^l(f) = R_l(f)\kappa_{13}\sqrt{\frac{1-\eta_1}{\eta_1}}, \quad K_2^l(f) = R_l(f)\kappa_{23}\sqrt{\frac{\eta_1}{1-\eta_1}}. \tag{82}$$

As expected, the density (81) is a convolution of a Gaussian with the POVM introduced in Proposition 4. Then, the probability density of the observables $Y_j(t_l)$, $j = 1, 2$, $l = 1, \ldots, m$, is given by

$$g_{\vec{Y}}(\vec{y}) = \mathbb{E}_f\left[\mathrm{Tr}_{\Gamma_1}\left\{ \rho_1^{f,T} \prod_l \hat{g}^l_Y\left(y^l_1, y^l_2; f\right)\right\}\right]. \tag{83}$$

Signal in the vacuum state. An explicit expression of this density can be given when the signal is in a mixture of coherent states as in Corollary 2 (see Appendix C 1). When the signal is in the vacuum state the density (83) and (C1) take the form

$$g_{\vec{Y}}(\vec{y}) = \prod_{l=1}^{m} g^l_Y\left(y^l_1, y^l_2\right), \tag{84a}$$

$$g^l_Y(y^l_1, y^l_2) = \mathbb{E}_f\left[g^l_Y\left(y^l_1, y^l_2; f\right)\right], \tag{84b}$$

$$g^l_Y(y^l_1, y^l_2; f) = \prod_{j=1}^{2} \frac{\exp\left\{ -\frac{\left(y^l_j - \mu^{jl}_{\mathcal{L}}(f)\right)^2}{2\kappa_{j2} R_l(f)^2}\right\}}{\sqrt{2\pi\kappa_{j2} R_l(f)^2}}, \tag{84c}$$

where $\mu^{jl}_{\mathcal{L}}(f)$ is given in (75b). In getting the product structure, Assumption 3 is involved.

V. MIN-ENTROPY AND RANDOM-NUMBER GENERATION

In this section we discuss a specific application of the full quantum theory of an eight-port homodyne detection scheme presented in this work: random-number generation. As we stated in Sec. IV A, for QRNG applications we are interested in pure noise (shot noise); in particular, we want to show the effects of unbalancing and LO fluctuations with respect to the perfect case discussed in [11]. To capture the characteristic features of a good random-number generator we extract the random bits from the sampled joint distribution of $(X_1(t_l), X_2(t_l))$, $l = 1, \ldots, m$; when the signal is in the vacuum state, they are independent and identically distributed (i.i.d.) by Assumption 3. If some dependence would be left, we can generate the random numbers after a suitable undersampling.

We want the generated bits to be truly random and known only to the users of the QRNG. The requirement of true randomness can be synthesized by the leftover Hash lemma, which relates the maximum number of extractable i.i.d. bits from a given string to an entropic quantity called min-entropy $H_{\min}$. Instead, to have secure and private random bits we have to rely on the quantum-classical conditional min-entropy, which takes into account possible side information held by an eavesdropper [11,38,47]. On the basis of the computed value of the min-entropy the truly random and secure bits are obtained from the raw data by employing a suitable algorithm, a randomness extractor [2,10,11].

Given a discrete probability distribution $P = \{p_j,\ j \in I\}$ the (classical) *min-entropy* is

$$H_{\min}(P) = -\log_2 \max_{j\in I} p_j \geqslant 0; \tag{85}$$

the quantity $P_{\text{guess}} = \max_{j\in I} p_j$ is known as *guessing probability*. Obviously $0 < P_{\text{guess}} \leqslant 1$ and the inequality in (85) follows. Then, the maximal number of i.i.d. bits extractable per measurement is given by $H_{\min}(P)$ [3,6,11,38,47].

When the sampled quantity is a continuous one, it has to be discretized; this is automatically done because any real measuring apparatus has a finite resolution. To state the problem, let us think to the univariate case and fix one of our sampled observables, say $X_1(t_l) \equiv X_1$, and denote by $f_1(x)$ its probability density. An n-bit ADC as a finite range $2R_1$ and a resolution $\delta_1 = 2R_1/2^n$. If possible, the discretization range has to be placed symmetrically around the mean μ_1. We set $x_0 \simeq \mu_1 - R_1$, and $x_j = x_0 + j\delta_1$ for $j = 1, \ldots, 2^n$; so, we get the discrete distribution

$$p_0 = \int_{-\infty}^{x_0} f_1(y)dy, \quad p_{2^n+1} = \int_{x_{2^n}}^{+\infty} f_1(y)dy,$$
$$p_j = \int_{x_{j-1}}^{x_j} f_1(y)dy, \quad 1 \leqslant j \leqslant 2^n.$$

The length and the position of the discretization interval must be such that the *saturation probabilities* p_0 and p_{2^n+1} are negligible (cf. the discussion in [48]). Then, the guessing probability turns out to be

$$P_{\text{guess}}(X_1, \delta_1) = \sup_{j=1,\ldots,2^n} \int_{x_{j-1}}^{x_j} f_1(y)dy \leqslant \delta_1 \times \sup_{x\in\mathbb{R}} f_1(x), \tag{86}$$

and for the min-entropy we get

$$H_{\min}(X_1, \delta_1) = -\log_2 P_{\text{guess}}(X_1, \delta_1)$$
$$\geqslant \log_2\left(\delta_1 \sup_{x\in\mathbb{R}} f_1(x)\right)^{-1}. \tag{87}$$

The lower bound above could be also negative; in this case it gives no information because the min-entropy is always positive. However, in usual situations δ_1 is sufficiently small in order to have that the lower bound is positive and it is a good estimation of the min-entropy. In the case of a Gaussian distribution, Ref. [3] contains also a discussion on how to optimize the choice of the discretization interval.

A. Total min-entropy

Let us denote by $p^l_X(x_1, x_2)$ the probability density of the observed sample $(X_1(t_l), X_2(t_l))$ at time t_l; the signal is in the vacuum state and we include also the electronic noise.

We assume this distribution to be approximately Gaussian, as discussed at the end of Sec. IV A. By (62a) and (62b), the means are given by $\mu_j = \Delta_{j2}|\lambda|^2$ and the covariance matrix by

$$\mathbf{C} = \begin{pmatrix} \Sigma_1^2 & \Delta_{12}\Delta_{22}|\lambda|^4 C_0 \\ \Delta_{12}\Delta_{22}|\lambda|^4 C_0 & \Sigma_2^2 \end{pmatrix},$$
$$\Sigma_j^2 = \kappa_{j2}|\lambda|^2 S_0 + \Delta_{j2}^2|\lambda|^4 C_0 + \sigma_j^{\mathrm{el}2}. \tag{88}$$

The quantities S_0, C_0 are given in (62c) and (62d), and κ_{j2}, Δ_{j2} in (31) and (32). The variances Σ_j^2 are expressed by the sum of the shot-noise contribution $\kappa_{j2}|\lambda|^2 S_0$, the RIN contribution $\Delta_{j2}^2|\lambda|^4 C_0$, and the electronic-noise contribution $\sigma_j^{\mathrm{el}2}$. Here and in the following it is useful to have a short notation for the noise ratios; so, we set

$$\Upsilon_j = \frac{\Delta_{j2}^2|\lambda|^2 C_0}{\kappa_{j2} S_0}, \quad \Theta_j = \frac{\sigma_j^{\mathrm{el}2}}{\kappa_{j2}|\lambda|^2 S_0}. \tag{89}$$

Then, we have $(X_1(t_l),\ X_2(t_l)) \sim \mathcal{N}(\vec{\mu}; \mathbf{C})$ and

$$\sup_{\vec{x}\in\mathbb{R}^2} p_X^l(\vec{x}) = (2\pi\sqrt{\det \mathbf{C}})^{-1}, \tag{90}$$
$$\begin{aligned} \det \mathbf{C} &= \Sigma_1^2\Sigma_2^2 - \Delta_{12}^2\Delta_{22}^2|\lambda|^8 C_0^2 \\ &= \kappa_{12}\kappa_{22}|\lambda|^4 S_0^2 E_{12}, \end{aligned} \tag{91}$$
$$\begin{aligned} E_{12} &= \frac{\det \mathbf{C}}{\kappa_{12}\kappa_{22}|\lambda|^4 S_0^2} = (1+\Theta_1)(1+\Theta_2) \\ &\quad + (1+\Theta_1)\Upsilon_2 + (1+\Theta_2)\Upsilon_1. \end{aligned} \tag{92}$$

As already said in Remark 6, the two signals are suitably filtered in order to eliminate the nonflat part of the spectrum and, then, to digitize the two components of each sample, two n-bits ADCs are employed, with two ranges $2R_j$ and resolutions $\delta_j = 2R_j/2^n$. The two ranges are placed around the means and are such that the saturation probability is negligible. Possibly, the two ADCs are identical and this would give $\delta_1 = \delta_2$. Under these hypotheses, the guessing probability for the single sample is

$$\begin{aligned} P_{\mathrm{guess}}(X,\delta) &\simeq \sup_{x_1,x_2} \int_{x_1-\delta_1/2}^{x_1+\delta_1/2} dy_1 \int_{x_2-\delta_2/2}^{x_2+\delta_2/2} dy_2\, p_X^l(\vec{y}) \\ &\leqslant \delta_1\delta_2 \sup_{\vec{x}\in\mathbb{R}^2} p_X^l(\vec{x}). \end{aligned} \tag{93}$$

We assume also δ_1 and δ_2 to be small enough to have $P_{\mathrm{guess}}(X,\delta) \simeq \delta_1\delta_2 \sup_{\vec{x}\in\mathbb{R}^2} p_X^l(\vec{x})$. Then, the min-entropy per sample is given by

$$H_{\min}(X,\delta) = -\log_2 P_{\mathrm{guess}}(X,\delta) \simeq \log_2 \frac{2\pi\sqrt{\det \mathbf{C}}}{\delta_1\delta_2}. \tag{94}$$

When the step lengths δ_j are not sufficiently small, the final expression on the right is only a lower bound and the guessing probability has to be expressed by using the error function [3,6,10].

Let us stress that the min-entropy (94) is independent of η_1, as one can see from (31) and (32), where the expressions of the coefficients κ_{j2} and Δ_{j2} are given. This is due to the fact that the signal is in the vacuum state and that η_1 is the transmissivity of the beam splitter which mixes the signal with another vacuum. Similarly, there is no dependence on ϕ because the probabilities do not depend on the phases when there is no interference between signal and LO (Remark 7). When $\Delta_{j2} = 0$ as in case of rebalancing (Remark 8), the means and the terms with the RIN contribution C_0 disappear; in this case the placement of the discretization interval is easier, as it must be symmetric around zero due to the vanishing of the mean.

1. Entropy losses due to correlations

To put in evidence the entropy losses due to the presence of correlations in the covariance matrix (88), it is useful to introduce the *reference entropy*

$$H_{\mathrm{ref}} = \log_2 \frac{2\pi\,\Sigma_1\Sigma_2}{\delta_1\delta_2}. \tag{95}$$

By comparing this formula with (94), we see that we have replaced the determinant of the covariance matrix with the product of the variances; so, H_{ref} represents the min-entropy when the correlations are not taken into account.

Then, by Eqs. (88), (89), (92), (94), and (95), we obtain

$$\begin{aligned} &H_{\mathrm{ref}} - H_{\min}(X,\delta) \\ &\quad \simeq -\frac{1}{2}\log_2\left[1 - \frac{\Upsilon_1\Upsilon_2}{(1+\Theta_1+\Upsilon_1)(1+\Theta_2+\Upsilon_2)}\right]. \end{aligned} \tag{96}$$

This difference is positive and represents the entropy loss due to the correlations introduced by the RIN; this loss vanishes in the case of rebalancing (see Remark 8). It is important to note that the difference (96) does not depend on the resolution parameters δ_j.

2. Optimization of the discretization range

From (94) we see that the min-entropy increases when the discretization steps δ_j decrease. On the other side, this expression of the min-entropy is based on the hypothesis that the probability of saturation is negligible, but this probability increases with the decrease of the discretization range. We can try to quantify this tradeoff by saying that there is saturation when the signal $(X_1(t_l),\ X_2(t_l))$ falls outside the discretization rectangle; this is a conservative choice, as we do not make a finer subdivision of the saturation region. Then, the saturation probability is given by

$$P_{\mathrm{saturation}}(X,\delta) \simeq 1 - \int_{\mu_1-R_1}^{\mu_1+R_1} dy_1 \int_{\mu_2-R_2}^{\mu_2+R_2} dy_2\, p_X^l(\vec{y}). \tag{97}$$

To be negligible, the saturation probability must satisfy

$$P_{\mathrm{saturation}}(X,\delta) < P_{\mathrm{guess}}(X,\delta). \tag{98}$$

By suitably tuning the ADC apparatus and the laser intensity, we can manage the range R_j to be proportional to the standard deviation of the observed voltage (at least approximately); so, by (88), we can write

$$R_j = x_j\Sigma_j, \quad \delta_j = \frac{2R_j}{2^n} = \frac{x_j\Sigma_j}{2^{n-1}}. \tag{99}$$

We have considered the same n for both ADCs; eventually, also the proportionality constants x_j could be independent from the index j. To apply the condition (98) in a simple way, we consider the Gaussian approximation and we neglect

TABLE I. The entropy contribution $H_{\rm ref}$ [Eq. (102)] as a function of the proportionality parameter $x = x_1 = x_2$ [Eq. (99)] and of the ADC number of bits n. A blank value means that the condition (101) is not satisfied.

$n\backslash x$	3.8	4.0	4.6	5.1	6.0	8.9	9.5
8		12.65	12.25	11.95	11.48	10.34	10.16
10			16.25	15.95	15.48	14.34	14.16
12				19.95	19.48	18.34	18.16
16					27.48	26.34	26.16
32						58.34	58.16

the correlations; we add a tilde to denote the guessing and saturation probabilities in this approximation:

$$\tilde{P}_{\rm guess}(X,\delta) = \frac{\delta_1\delta_2}{2\pi\,\Sigma_1\Sigma_2} = \frac{x_1x_2}{\pi\,2^{2n-1}}, \tag{100}$$

$$\begin{aligned}\tilde{P}_{\rm saturation}(X,\delta) &= 1 - P[-R_1 < X_1(t_l) - \mu_1 < R_1] \\ &\quad \times P[-R_2 < X_2(t_l) - \mu_2 < R_2] \\ &= 1 - 4\left(\Phi(x_1) - \frac{1}{2}\right)\left(\Phi(x_2) - \frac{1}{2}\right),\end{aligned}$$

where $\Phi(x)$ is the cumulative distribution function of a standard Gaussian random variable. Then, condition (98) (approximately) becomes

$$1 - 4\left(\Phi(x_1) - \frac{1}{2}\right)\left(\Phi(x_2) - \frac{1}{2}\right) < \frac{x_1x_2}{\pi\,2^{2n-1}}. \tag{101}$$

Let us note that the quantity $H_{\rm ref}$ [Eq. (95)] is just the min-entropy associated with the approximate guessing probability (100) and that we have

$$H_{\rm ref} = -\log_2 \tilde{P}_{\rm guess}(X,\delta) = 2n - 1 - \log_2 \frac{x_1x_2}{\pi}. \tag{102}$$

To have an idea of the values of the min-entropy and of good choices of x_j and n, let us consider the case $x_1 = x_2 = x$. Table I gives the values of $H_{\rm ref}$ (the main contribution to the total min-entropy) as a function of the parameters n and x.

For a given n the best choice for QRNG is to take the smallest x compatible with condition (101); however, if we want to use the apparatus also for detection, or if we want to be more sure to avoid saturation, we need x to be bigger. In Table II we report the ratio $\tilde{P}_{\rm saturation}(X,\delta)/\tilde{P}_{\rm guess}(X,\delta)$. The good choice for QRNG is to take the parameters which give this ratio near 1; however, by comparing the two tables, we see that we can make this ratio very small without a strong decreasing of $H_{\rm ref}$.

In the computations of Tables I and II we have assumed that the ranges are centered on the means. When this is not possible, the saturation probability increases and it is convenient to enlarge the range with respect to the variance and to chose a value for x giving a ratio well below 1 in Table II.

In [11] the equilibrated case is considered and experimentally implemented; by using a 10-bit ADC, they obtain a value of about 14 for the min-entropy. So, by looking at Table I, we can say that values from 14 to 26 for $H_{\rm ref}$ are experimentally reasonable, depending on the characteristics of the ADC and of the electronic part of the apparatus. A much higher value can be obtained, if a 32-bit ADC is available.

As already written, to tune the ADC ranges to the noise variances one could increase the LO intensity. The shot-noise intensity can be increased also by using two lasers, one at the LO port and one at the signal port. To use two similar lasers is nearly the same as doubling the LO intensity; explicit computations can be done by starting from the results of Appendix C 1. In any case, the most important ingredient to increase the bit generation rate is the ADC resolution.

In the following, we assume that the instrumentation has been chosen and calibrated; so, n and the ADC ranges are fixed, which means that also the values of δ_1 and δ_2 have been fixed.

B. Side information: Classical noise

When all the noise contributions, classical and quantum, are trusted, the randomness extractor can be calibrated on the value of the total min-entropy $H_{\rm min}(X,\delta)$. Fast random-number generators based on various types of physical noise have been proposed and realized (see [48] for an example based on laser noise). However, doubts have been raised on some of the noise components involved in homodyne-based random-number generators (see, for instance, [4,6,9–11]). The presence of untrusted noise or of possible side information forces to calibrate the randomness extractor on suitable conditional min-entropies, as discussed here and in the next subsection.

In our formulation of the double-homodyne detector we have included two sources of classical noise: the electronic noise and the laser fluctuations. The classical noise can be considered untrusted because not truly random and not well modeled, but even because it could be known to some intruder and it could convey some side information. To get secure

TABLE II. The ratio $\tilde{P}_{\rm saturation}(X,\delta)/\tilde{P}_{\rm guess}(X,\delta)$ as a function of the proportionality parameter $x = x_1 = x_2$ [Eq. (99)] and of the ADC number of bits n. A value greater than 1 means that the condition (101) is not satisfied.

$n\backslash x$	3.8	4.0	4.6	5.1	6.0	8.9	9.5
8	2.1	0.82	4.1×10^{-2}	2.7×10^{-3}	1.1×10^{-5}	1.5×10^{-15}	4.8×10^{-18}
10	33	13	0.66	4.3×10^{-2}	1.8×10^{-4}	2.3×10^{-14}	7.7×10^{-17}
12	5.3×10^{2}	2.1×10^{2}	11	0.69	2.9×10^{-3}	3.7×10^{-13}	1.2×10^{-15}
16	$14 times 10^{4}$	5.3×10^{4}	2.7×10^{3}	1.8×10^{2}	0.74	9.5×10^{-11}	3.1×10^{-15}
32	5.8×10^{14}	2.3×10^{14}	1.2×10^{13}	7.6×10^{11}	3.2×10^{9}	0.41	1.3×10^{-3}

random bits with respect to not certified noise and to side information, the *average conditional min-entropy* [3, Sec. C] has to be used to calibrate the randomness extractor: the guessing probability has to be computed with respect to the probability distribution conditioned on laser fluctuations and electronic noise; then, the mean is taken.

Let us denote by $N_{\mathrm{el}}^{j,l}$ the contribution of the electronic noise to the observation at time t_l; we have assumed the electronic noise to be normal, $N_{\mathrm{el}}^{j,l} \sim \mathcal{N}(0;\sigma_j^{\mathrm{el}\,2})$, and independent of any other noise contribution. Then, for fixed f, the sampled observables can be written as

$$X_j^f(t_l) = |\lambda| Y_j^f(t_l) + N_{\mathrm{el}}^{j,l}, \tag{103}$$

where the $Y_j^f(t)$ are the scaled processes introduced in (41). We assume the LO intensity to be sufficiently high, so that the probability density of the random variables $Y_j^f(t_l)$ is the one discussed in Sec. IV C. When the signal is in the vacuum state and f and $N_{\mathrm{el}}^{j,l}$ are given, we get from (84c) that the conditional probability density for a single sample is

$$p_X^l(x_1,x_2;f,N_{\mathrm{el}}) = \frac{1}{|\lambda|^2}\, g_Y^l\big((x_1^l - N_{\mathrm{el}}^{1,l})/|\lambda|,\,(x_2^l - N_{\mathrm{el}}^{2,l})/|\lambda|;f\big).$$

In this situation the average guessing probability, conditional on the classical noise, is given by

$$\begin{aligned} P_{\mathrm{guess}}(X,\delta|\mathcal{E}_{\mathrm{cl}}) &= \mathbb{E}_{f,N_{\mathrm{el}}}\left[\sup_{x_1,x_2}\int_{x_1-\delta_1/2}^{x_1+\delta_1/2} dy_1 \int_{x_2-\delta_2/2}^{x_2+\delta_2/2} dy_2\, p_X^l(y_1,y_2;f,N_{\mathrm{el}})\right] \\ &\leqslant \frac{\delta_1\delta_2}{|\lambda|^2}\,\mathbb{E}_f\left[\sup_{y_1,y_2} g_Y^l\big(y_1^l/|\lambda|, y_2^l/|\lambda|;f\big)\right] = \mathbb{E}_f\left[\frac{\delta_1\delta_2}{2\pi\sqrt{\kappa_{12}\kappa_{22}}|\lambda|^2 R_l(f)^2}\right]. \end{aligned} \tag{104}$$

Accordingly, the average conditional min-entropy per sample is given by

$$H_{\min}(X,\delta|\mathcal{E}_{\mathrm{cl}}) = -\log_2 P_{\mathrm{guess}}(X,\delta|\mathcal{E}_{\mathrm{cl}}) \simeq \log_2 \frac{2\pi|\lambda|^2\sqrt{\kappa_{12}\kappa_{22}}}{\delta_1\delta_2\mathbb{E}_f[R_l(f)^{-2}]}, \tag{105}$$

where we have again simplified the computations of the Gaussian integrals by assuming the δ_j to be sufficiently small. From these definitions we have immediately $P_{\mathrm{guess}}(X,\delta) \leqslant P_{\mathrm{guess}}(X,\delta|\mathcal{E}_{\mathrm{cl}})$ and $H_{\min}(X,\delta) \geqslant H_{\min}(X,\delta|\mathcal{E}_{\mathrm{cl}})$.

Remark 11. Let us note that the electronic noise disappears from the expression (105) of the classically conditioned min-entropy, as this noise is purely additive. This is not the case of the RIN, which contributes through the expression $\mathbb{E}_f[R_l(f)^{-2}]$. The reason is that the laser fluctuations are involved in the definition (66a) of the discrete mode operators, where $R_l(f)$ is the (random) normalization constant. Moreover, we have $\mathbb{E}_f[R_l(f)^2] = S_0$ [see (67)], and

$$\mathbb{E}_f\big[R_l(f)^{-2}\big] = \frac{1}{S_0} + \mathbb{E}_f\left[\frac{[R_l(f)^2 - S_0]^2}{R_l(f)^2 S_0^2}\right] \geqslant \frac{1}{S_0}, \tag{106}$$

which gives $S_0\mathbb{E}_f[R_l(f)^{-2}] \geqslant 1$. Consistently with the laser models discussed in Sec. II B, we assume $\mathbb{E}_f[R_l(f)^{-2}]$ to be independent from l and we set

$$S_- = 1\big/\mathbb{E}_f[R_l(f)^{-2}] \leqslant S_0. \tag{107}$$

Remark 12. By definition (66d), $R_l(f)$ turns out to be a time smoothing of the function f realized through the response function $h(t)$. If the involved integration time interval is not too short, it is realistic to have $R_l(f)^2 \simeq S_0$, by ergodic properties of the process $f(t)$; in this case $S_- \simeq S_0$. In any case their difference should be small. From (64) we see that to have the decay time of RIN correlations much shorter than the decay time of $h(t)$ gives also $C_0 \ll 1$.

In the works on QRNG from homodyne detection it is usual to express the min-entropy by scaling the involved noise to the vacuum noise ($\frac{1}{2}$ in standard units) [6,11]. If we have a good estimate of $2\kappa_{j2}|\lambda|^2 S_0$ from the calibration stage, we can introduce the "scaled" resolutions and min-entropy:

$$\delta_j^0 = \frac{\delta_j}{|\lambda|\sqrt{2\kappa_{j2}S_0}}, \quad H_0 = \log_2\frac{\pi}{\delta_1^0\delta_2^0}. \tag{108}$$

The scaled resolutions δ_j^0 turn out to be pure numbers; even in the case $\delta_1 = \delta_2$, the presence of any imbalance should give $\delta_1^0 \neq \delta_2^0$. From (31) and (108), we can see that when the ϵ_j decrease (more losses) the parameters δ_j^0 increase (worst scaled resolution). Then, by comparing (105) with the reference min-entropy (108), we get

$$H_0 - H_{\min}(X,\delta|\mathcal{E}_{\mathrm{cl}}) \simeq \log_2(S_0/S_-) \geqslant 0. \tag{109}$$

Under the conditions of Remark 12, this entropy difference is small. Also, the total min-entropy (94) can be expressed in a similar way:

$$H_{\min}(X,\delta) \simeq H_0 + \frac{1}{2}\log_2\frac{\det\mathbf{C}}{|\lambda|^4\kappa_{12}\kappa_{22}S_0^2}; \tag{110}$$

only the min-entropy H_0 depends on the discretization steps δ_j, not the last term.

The price in considering untrusted the classical noise is a loss of entropy quantified by

$$H_{\min}(X,\delta) - H_{\min}(X,\delta|\mathcal{E}_{\mathrm{cl}}) \simeq \tfrac{1}{2}\log_2 E_{12} + \log_2(S_0/S_-), \tag{111}$$

where E_{12} is defined in (92) and depends on the noise ratios (89). Note that the entropy loss does not depend on the resolutions δ_j. By increasing the laser intensity $|\lambda|^2$ and the coefficients ϵ_j (less optical losses), we can make the electronic-noise contributions Θ_j to decrease, but one has to pay attention to the tradeoff with respect to the RIN (the terms

with Υ_j). Indeed, these contributions increase with $|\lambda|^2$, while they can be made to decrease by some rebalancing which can be obtained by decreasing some of the ϵ_j (see Remark 8). This tradeoff is more evident if we consider the entropy loss with respect to $H_{\rm ref}$ because, by Eqs. (96) and (111), this loss takes the simpler expression

$$H_{\rm ref} - H_{\min}(X,\delta|\mathcal{E}_{\rm cl}) \simeq \log_2(S_0/S_-) + \log_2\sqrt{(1+\Theta_1+\Upsilon_1)(1+\Theta_2+\Upsilon_2)}. \tag{112}$$

If the laboratory is "secure" and we trust in our detection apparatus and in the LO laser, we can rely on the conditional min-entropy $H_{\min}(X,\delta|\mathcal{E}_{\rm cl})$ to calibrate the randomness extractor. To be sure that no intruder can violate the privacy of the generated random bits, we can physically block the vacuum input ports, represented in Fig. 1 by the channel 1 (signal) and the channels 2 and 4 (vacuum); to block the unused ports is suggested also in [3,5].

C. Side information: The signal

In [11] one of the reasons to propose double-homodyne detection for QRNG was that one can obtain secure random bits even if an intruder can manipulate the signal (but in the same paper this possibility is referred to as a "paranoid scenario"). Indeed, in QRNG the eight-port circuit is not used to detect a signal coming from the external world, as in QKD, and it can be blocked to external influences, as noticed above. Moreover, if the intruder is sending too strong signals, as in a blinding attack [36], the intrusion is easily detected. On another side, to conduct a successful eavesdropping attack, one needs to send a signal phase locked to the LO laser [7] and this means to have access to the laboratory. In any case, it is possible to extend the approach of [11] and to take into account the quantum side information which an intruder could gain by manipulating the signal.

From (103) and (83), the probability density for the m sample turns out to be

$$p_{\vec{X}}(\vec{x}) = \mathbb{E}_{f,N_{\rm el}}\left[\mathrm{Tr}_{\Gamma_1}\left\{\rho_1^{f,T}\prod_{l=1}^{m}\frac{1}{|\lambda|^2}\,\hat{g}_Y^l\big((x_1^l - N_{\rm el}^{1,l})/|\lambda|,\,(x_2^l - N_{\rm el}^{2,l})/|\lambda|;f\big)\right\}\right], \tag{113}$$

where $\hat{g}_Y^l(y_1,y_2;f)$ is given by (81). By setting

$$\hat{P}_l\big(x_1^l,x_2^l;f,N_{\rm el},\delta\big) = \frac{1}{|\lambda|^2}\int_{x_1^l-\delta_1/2}^{x_1^l+\delta_1/2}dx_1'\int_{x_2^l-\delta_1/2}^{x_2^l+\delta_1/2}dx_2'\,\hat{g}_Y^l\big((x_1'-N_{\rm el}^{1,l})/|\lambda|,\,(x_2'-N_{\rm el}^{2,l})/|\lambda|;f\big),$$

we can introduce a classical and quantum "worst-case" conditional guessing probability for the full m sample:

$$P_{\rm guess}^{\rm full}(\vec{X},\delta|\mathcal{E}_{\rm cl\&qu}) = \mathbb{E}_{f,N_{\rm el}}\left[\sup_{\rho_1}\sup_{\vec{x}_1,\vec{x}_2}\mathrm{Tr}_{\Gamma_1}\left\{\rho_1\prod_{l=1}^{m}\hat{P}_l(x_1^l,x_2^l;f,N_{\rm el},\delta)\right\}\right] \tag{114}$$

(cf. [3,6,11,38,47]); then, the related min-entropy is

$$H_{\min}^{\rm full}(\vec{X},\delta|\mathcal{E}_{\rm cl\&qu}) = -\log_2 P_{\rm guess}^{\rm full}(\vec{X},\delta|\mathcal{E}_{\rm cl\&qu}) \geqslant 0. \tag{115}$$

By comparing these definitions with (93), (94), (104), and (105), we get

$$mH_{\min}(X,\delta) \geqslant mH_{\min}(X,\delta|\mathcal{E}_{\rm cl}) \geqslant H_{\min}^{\rm full}(\vec{X},\delta|\mathcal{E}_{\rm cl\&qu}).$$

Now, let us consider the (normalized) squeezed coherent states $|\psi_l(z;\alpha,\beta)\rangle$ [Eq. (71)] and the POVM density $\hat{g}_{\alpha,\beta}^l(z)$, which is defined by the second equality in (79) and is involved in the definition (81) of $\hat{g}_Y^l(y_1,y_2;f)$. The operator $\pi\,\hat{g}_{\alpha,\beta}^l(z) = |\psi_l(z;\alpha,\beta)\rangle\langle\psi_l(z;\alpha,\beta)|$ is a rank-one orthogonal projection (for every choice of α, β, z) and, so,

$$\hat{g}_{\alpha,\beta}^l(z) \leqslant \mathbb{1}/\pi. \tag{116}$$

The results about secure QRNG developed in [11] are based on the bound (116) in the particular case $\alpha = 1$, $\beta = 0$. As it is proved in Appendix C 2, this bound implies

$$p_{\vec{X}}(\vec{x}) \leqslant \frac{1}{(4\pi\kappa_{13}\kappa_{23}|\lambda|^2|\sin\phi|S_-)^m}. \tag{117}$$

By introducing the *entropy lower bound* per sample

$$H_{\rm lb}(X,\delta|\mathcal{E}_{\rm cl\&qu}) = \log_2\frac{4\pi\kappa_{13}\kappa_{23}|\sin\phi||\lambda|^2S_-}{\delta_1\delta_2}, \tag{118}$$

from (114), (115), and (117), we obtain

$$H_{\min}^{\rm full}(\vec{X},\delta|\mathcal{E}_{\rm cl\&qu}) \geqslant m\,H_{\rm lb}(X,\delta|\mathcal{E}_{\rm cl\&qu}). \tag{119}$$

Even in the case of a possible variant of the definition of conditional min-entropy with respect to the quantum side information, inequality (119) would be valid because the lower bound is independent of any kind of signal the intruder could send. Then, the entropy lower bound per sample (118) can be safely used to calibrate the randomness extractor; this bound holds even in the case of a coherent attack. However, let us note that the quantity (118) is not guaranteed to be positive; so, to be useful it needs $|\sin\phi|$ to be not too small.

The dependence on $|\sin\phi|$ implies a decrease of the min-entropy bound (118) when the two observed quadratures are not perfectly complementary. Moreover, with respect to the transmissivities, the bound (118) is maximum for $\eta_j = \frac{1}{2}$; indeed, by (31) we have

$$4\kappa_{13}\kappa_{23} = 4\sqrt{\prod_{j=1}^{4}\eta_j(1-\eta_j)(\epsilon_1\xi_1+\epsilon_3\xi_3)(\epsilon_2\xi_2+\epsilon_4\xi_4)} \leqslant 4\kappa_{13}\kappa_{23}\big|_{\eta_j=1/2} = \frac{\epsilon_1\xi_1+\epsilon_3\xi_3}{2}\times\frac{\epsilon_2\xi_2+\epsilon_4\xi_4}{2}. \tag{120}$$

With respect to the entropy losses (111), to ask for independence from any quantum intrusion gives a further loss of min-entropy:

$$H_{\min}(X,\delta|\mathcal{E}_{\rm cl}) - H_{\rm lb}(X,\delta|\mathcal{E}_{\rm cl\&qu}) \simeq \log_2 \frac{\sqrt{\kappa_{12}\kappa_{22}}}{2\kappa_{13}\kappa_{23}|\sin\phi|}$$
$$= \log_2 \frac{\sqrt{(1+\tilde V_1^{\,2}+\tilde\sigma_1^{\,2})(1+\tilde V_2^{\,2}+\tilde\sigma_2^{\,2})}}{\sqrt{4\eta_1(1-\eta_1)}|\sin\phi|} \geqslant 0; \qquad (121)$$

here we have used Eqs. (105), (118), (48), and (49). In a more explicit way we can write

$$1+\tilde V_j^{\,2}+\tilde\sigma_j^{\,2} = \frac{(1-\eta_{j+2})\epsilon_j\xi_j^{\,2}+\eta_{j+2}\epsilon_{j+2}\xi_{j+2}^{\,2}}{\eta_{j+2}(1-\eta_{j+2})(\epsilon_j\xi_j+\epsilon_{j+2}\xi_{j+2})^2}. \qquad (122)$$

In the entropy loss (121) we can identify a first contribution, $\log_2(\sqrt{4\eta_1(1-\eta_1)}|\sin\phi|)^{-1} \geqslant 0$, due to the fact that the intruder is allowed to send any kind of squeezed states, such as the eigenstates of the squeezed modes b_l (70) (see Remark 10). The second contribution is $\frac{1}{2}\sum_{j=1}^2 \log_2(1+\tilde V_j^{\,2}+\tilde\sigma_j^{\,2}) \geqslant 0$; note that $\tilde V_1^{\,2}$ and $\tilde V_2^{\,2}$ vanish in the rebalancing case of Remark 8, while $\tilde\sigma_1^{\,2}$ and $\tilde\sigma_2^{\,2}$ vanish when there are no optical losses, i.e., $\epsilon_j = 1$. So, by using the entropy lower bound (118), one gets secure random bits also with respect to possible intrusions through the optical losses, which is one of the points raised in [10].

D. Examples

An interesting question is to understand the effects on the min-entropies of the various imperfections with respect to the balanced case of Sec. II D 2.

Remark 13. In the case of the perfect balancing (35), Eqs. (31), (32), (49), (89), and (92) give

$$\tilde V_j^{\,2} = 0, \quad \tilde\sigma_j^{\,2} = \frac{1-\epsilon}{\epsilon}, \quad \Upsilon_j = 0,$$
$$\Theta_j = \frac{2\sigma_j^{\rm el\,2}}{\epsilon\xi^2|\lambda|^2 S_0}, \quad E_{12} = (1+\Theta_1)(1+\Theta_2).$$

Then, (94), (96), (112), and (121) reduce to

$$H_{\min}(X,\delta) = H_{\rm ref} \simeq \log_2 \frac{\pi\epsilon|\lambda\xi|^2 S_0\sqrt{(1+\Theta_1)(1+\Theta_2)}}{\delta_1\delta_2},$$

$$H_{\rm ref} - H_{\min}(X,\delta|\mathcal{E}_{\rm cl}) \simeq \log_2(S_0/S_-) + \log_2\sqrt{(1+\Theta_1)(1+\Theta_2)},$$

$$H_{\min}(X,\delta|\mathcal{E}_{\rm cl}) - H_{\rm lb}(X,\delta|\mathcal{E}_{\rm cl\&qu}) \simeq -\log_2(\epsilon|\sin\phi|).$$

If, in addition, we have perfectly complementary quadratures, $|\sin\phi| = 1$, and totally efficient detectors, $\epsilon = 1$, the conditional min-entropy $H_{\min}(X,\delta|\mathcal{E}_{\rm cl})$ and the lower bound $H_{\rm lb}(X,\delta|\mathcal{E}_{\rm cl\&qu})$ become equal, which is the case of [11].

To have an idea of the effects of unbalancing and losses, we particularize the choice of the various parameters. First, we take $\epsilon_j = \epsilon$ and $\xi_j = \xi$, which means that the quantum efficiencies and the conversion factors of the four detectors are equal. We take also the same unbalancing in the two detection channels, i.e., $\eta_3 = \eta_4 = \eta$, while the first two beam splitters are taken well balanced, $\eta_1 = \eta_2 = \frac{1}{2}$. We take equal also the variances of the two electronic noises $\sigma_j^{\rm el\,2} = \sigma_{\rm el}^{\,2}$. Then, Eqs. (31), (32), (88), (89), and (122) give

$$\kappa_{j2} = \frac{\epsilon}{2}\xi^2, \quad \Delta_{j2} = \frac{\epsilon}{2}\xi(1-2\eta), \quad \Upsilon_j = \epsilon\Upsilon,$$
$$\Theta_j = \frac{\Theta}{\epsilon}, \quad \Upsilon = (1-2\eta)^2\frac{|\lambda|^2 C_0}{2S_0},$$
$$\Theta = \frac{2\sigma_{\rm el}^{\,2}}{|\xi\lambda|^2 S_0}, \quad 1+\tilde V_j^{\,2}+\tilde\sigma_j^{\,2} = \frac{1}{4\eta(1-\eta)\epsilon},$$
$$\Sigma_j^2 = \Sigma^2 = \frac{|\xi\lambda|^2}{2}S_0\big(\Theta+\epsilon+\epsilon^2\Upsilon\big). \qquad (123)$$

Finally, Eqs. (95), (96), (112), and (121) reduce to

$$H_{\rm ref} = \log_2\frac{2\pi\Sigma^2}{\delta_1\delta_2} = \log_2\left[\frac{\pi|\xi\lambda|^2 S_0}{\delta_1\delta_2}\big(\Theta+\epsilon+\epsilon^2\Upsilon\big)\right], \qquad (124)$$

$$H_{\rm ref} - H_{\min}(X,\delta) = -\frac{1}{2}\log_2\left[1-\left(1+\frac{1}{\epsilon\Upsilon}+\frac{\Theta}{\epsilon^2\Upsilon}\right)^{-2}\right], \qquad (125)$$

$$H_{\rm ref} - H_{\min}(X,\delta|\mathcal{E}_{\rm cl}) \simeq \log_2(S_0/S_-) + \log_2(1+\epsilon\Upsilon+\Theta/\epsilon), \qquad (126)$$

$$H_{\min}(X,\delta|\mathcal{E}_{\rm cl}) - H_{\rm lb}(X,\delta|\mathcal{E}_{\rm cl\&qu}) \simeq -\log_2[4\eta(1-\eta)\epsilon|\sin\phi|]. \qquad (127)$$

The reference entropy (124) decreases when ϵ or $|1-2\eta|$ decrease. However, its value can be kept constant by tuning the instrumentation, as discussed in Sec. V A 2, and reasonable values for $H_{\rm ref}$ go from 14 to 26 bits (see Table I). So, here we study the behavior of the entropy differences (125)–(127).

We take the parameters ϵ and η free, and we fix some reasonable values for the other parameters; let us recall that $|1-2\eta|$ measures the unbalancing in the detectors, while ϵ is the effective quantum efficiency of the photodiodes. The parameter S_0, given in (62c) and (64), is linked to the detection bandwidth and we can take $S_0 = 10\ \text{GHz} = 10^{10}\ \text{s}^{-1}$; we take also $S_- \simeq S_0$ [see Eq. (107) and Remark 12]. With lasers of a power of 1.25 mW and wavelength around 1550 nm, we can get the mean number of photons per unit of time $|\lambda|^2 = 10^{16}\ \text{s}^{-1}$; higher values are also possible. By assuming the decay time of the RIN correlations much shorter of the decay time of the detector response function $h(t)$, from Eqs. (62d) and (64) and Remark 12 we see that C_0 must be small and we take $C_0 = 0.01$. Finally, we can take $\Theta = \frac{2\sigma_{\rm el}^{\,2}}{|\lambda\xi|^2 S_0} = 0.12$, which comes out by taking a variance for the electronic noise compatible with the values reported in [11]. With these choices we get also $\frac{|\lambda|^2 C_0}{2S_0} = 0.5\times 10^4$.

Let us start with the entropy losses (125), due to the correlations introduced by the RIN. We plot this entropy loss with respect to the "quantum loss percentage $= 100(1-\epsilon)$" of

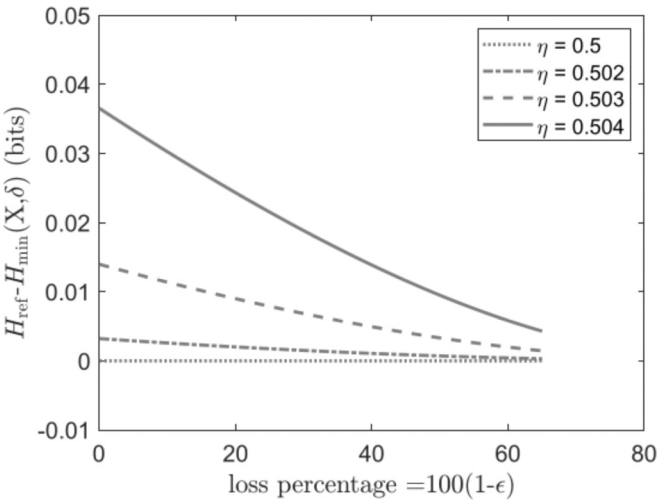

FIG. 2. Entropy loss $H_{\text{ref}} - H_{\min}(X, \delta)$ [Eq. (125)] for small unbalancing $|1 - 2\eta| \leqslant 0.008$.

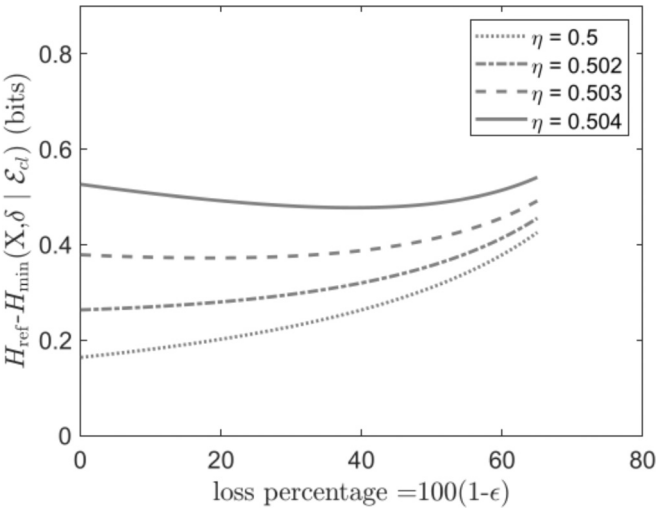

FIG. 4. Entropy loss $H_{\text{ref}} - H_{\min}(X, \delta|\mathcal{E}_{\text{cl}})$ [Eq. (126)] for small unbalancing $|1 - 2\eta| \leqslant 0.008$.

the photodiodes for small values of the detector unbalancing $|1 - 2\eta|$ in Fig. 2, and for bigger unbalancing in Fig. 3. From Figs. 2 and 3 we see that the entropy loss (125) can be made to decrease by increasing the detector losses $1 - \epsilon$ (apart from the balanced case $\eta = \frac{1}{2}$), a phenomenon which is evident also from formula (125), but not *a priori* expected. Note a change of curvature in going from the cases of Fig. 2 to the cases of Fig. 3. We see also that the entropy loss decreases with the decreasing of the distance of η from $\frac{1}{2}$. Moreover, this loss is acceptably small for small unbalancing as in Fig. 2, while it can take values of even two bits per sample in the cases of Fig. 3.

When the contributions of the classical noises (RIN and electronic noise) are considered not secure, the entropy loss is given by (126); the behavior is plotted in Figs. 4 and 5 for the same values of η as before. Now, we have again a decrease of the entropy loss with the increase of $1 - \epsilon$ in the case of large imbalance (see Fig. 5). However, for small imbalance (Fig. 4), the behavior is more complex. For $\eta = 0.5$ and 0.502, the entropy loss monotonically grows with $1 - \epsilon$, while for $\eta = 0.503$ and 0.504 we have a nonmonotonic behavior, first a decreasing and then an increasing of the entropy loss.

To avoid losses of some bits in the case of large unbalancing, as in the case of Figs. 3 and 5, one has to rely on a partial rebalancing (see Remark 8) or on a change of the detector response in order to decrease the coefficient C_0.

In the extreme case of Sec. V C, when we consider not secure even the signal port, we have to add a further entropy loss represented by (127). Now the behavior is very simple: minus the logarithm of a product. For $4\eta(1 - \eta)\epsilon|\sin\phi| = 0.5$ the entropy loss is 1 bit; we can think to arrive to 2 bits by increasing a little the imperfections (and such a loss is not small). However, with reasonable values of the involved parameters, we can remain below 1 bit.

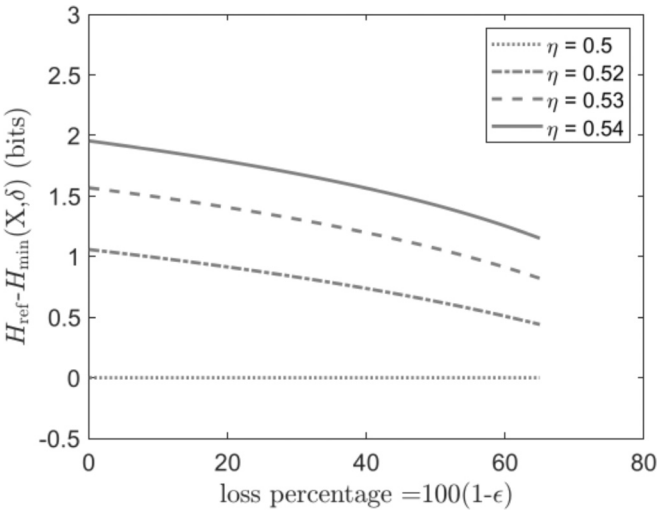

FIG. 3. Entropy loss $H_{\text{ref}} - H_{\min}(X, \delta)$ [Eq. (125)] for big unbalancing $0.04 \leqslant |1 - 2\eta| \leqslant 0.08$.

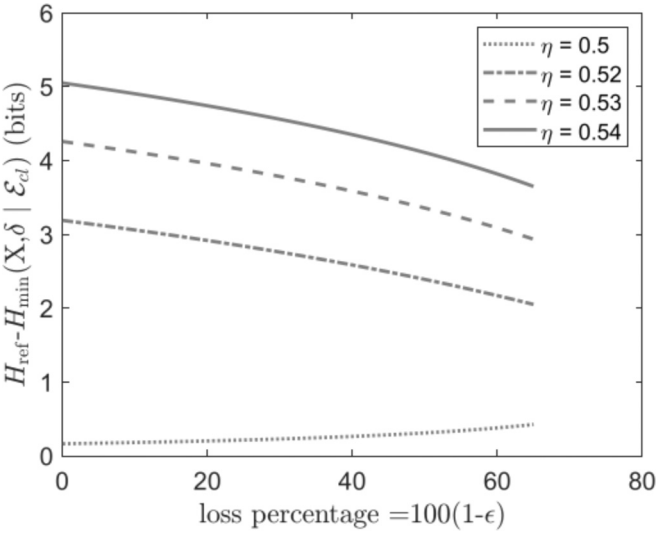

FIG. 5. Entropy loss $H_{\text{ref}} - H_{\min}(X, \delta|\mathcal{E}_{\text{cl}})$ [Eq. (126)] for big unbalancing $0.04 \leqslant |1 - 2\eta| \leqslant 0.08$.

VI. QRNG FROM SINGLE HOMODINING

The whole construction of the previous sections can be particularized to the case of a single homodyning and this allows to see the effect of imperfections either when the apparatus works as a detector, as in [21,22,30,32,37], or when it is used for QRNG, as in [2,3,5–10,36].

One can get single homodyning from the circuit of Fig. 1 by eliminating the beam splitters BS1 and BS2, which means to take $\eta_1 = \eta_2 = 1$. Then, no light arrives to the photodiodes PD2 and PD4 and we can eliminate them; so, we are left with a single detected process $X_1(t)$ [Eq. (28)] and the scaled process $Y_1(t)$ [Eq. (41)].

The first two moments of the process $X_1(t)$ are given by Eqs. (33) and (34), where the coefficients, defined in (31) and (32), reduce to

$$\begin{aligned}
\kappa_{11} &= \eta_3\epsilon_1{\xi_1}^2 + (1-\eta_3)\epsilon_3{\xi_3}^2,\\
\kappa_{12} &= (1-\eta_3)\epsilon_1{\xi_1}^2 + \eta_3\epsilon_3{\xi_3}^2,\\
\kappa_{13} &= \sqrt{\eta_3(1-\eta_3)}(\epsilon_1\xi_1 + \epsilon_3\xi_3),\\
\Delta_{11} &= \eta_3\epsilon_1\xi_1 - (1-\eta_3)\epsilon_3\xi_3,\\
\Delta_{12} &= (1-\eta_3)\epsilon_1\xi_1 - \eta_3\epsilon_3\xi_3,\\
\Delta_{13} &= \sqrt{\eta_3(1-\eta_3)}\big(\epsilon_1{\xi_1}^2 - \epsilon_3{\xi_3}^2\big).
\end{aligned} \tag{128}$$

Moreover, the characteristic functional of the process $Y_1(t)$ in the limit of strong LO is given by Proposition 1, where one has to take $k_2(s) = 0$. The various quantities introduced in Eqs. (49) reduce to

$$G_{13} = 0, \quad {V_1}^2 = {\tilde V_1}^2 = \frac{\Delta_{12}^2}{\kappa_{13}^2},$$
$$\sigma_1^2 = \tilde\sigma_1^2 = \frac{(1-\eta_3)\epsilon_1(1-\epsilon_1){\xi_1}^2 + \eta_3\epsilon_3(1-\epsilon_3){\xi_3}^2}{\eta_3(1-\eta_3)(\epsilon_1\xi_1 + \epsilon_3\xi_3)^2}.$$

Let us stress that the POVM with characteristic operator (52a) becomes the pvm associated to the single quadrature $\hat Q_1(t)$.

Then, one can consider the discrete sampling as in Sec. IV; if interested in QRNG, we have to consider the case of no signal as in the double-homodyne setup. From (62) and (88) we get

$$\mathbb{E}_P[X_1(t_l)] \simeq \Delta_{12}|\lambda|^2, \tag{129a}$$
$$\mathrm{Cov}_P[X_1(t_l),\, X_1(t_l')] \simeq \delta_{ll'}\Sigma_1^2 = \delta_{ll'}\kappa_{12}|\lambda|^2 S_0(1 + \Upsilon_1 + \Theta_1), \tag{129b}$$

where Υ_1 and Θ_1 are given in (89). However, the coefficients take the expressions (128), which means that their values are nearly two times the values in the double-homodyne scheme.

A. Total min-entropy

For a sufficiently intense LO and signal in the vacuum, $X_1(t_l)$ has a distribution which is nearly Gaussian with mean $\mu_1 = \Delta_{12}|\lambda|^2$ and variance Σ_1^2, given in (129). Let us denote by $p_{X_1}(x)$ the density of this Gaussian distribution. Now, the guessing probability and the associated min-entropy per sample (93) and (94) become

$$P_{\mathrm{guess}}(X_1, \delta_1) \simeq \sup_x \int_{x-\delta_1/2}^{x+\delta_1/2} dy\, p^l_{X_1}(y) \simeq \frac{\delta_1}{\sqrt{2\pi}\,\Sigma_1}, \tag{130}$$
$$H_{\min}(X_1, \delta_1) = -\log_2 P_{\mathrm{guess}}(X_1, \delta_1) \simeq \log_2 \frac{\sqrt{2\pi}\,\Sigma_1}{\delta_1}. \tag{131}$$

In the univariate case correlations are not involved; so, the analogous of H_{ref} [Eq. (95)] coincides with the total min-entropy [Eq. (131)].

As discussed in Sec. V A 2, we can try to optimize the discretization range $2R_1$ by acting on the ADC and on the laser power. Analogously to (99), we can write $R_1 = x\Sigma_1$, which gives

$$\delta_1 = \frac{x\Sigma_1}{2^{n-1}}, \quad \tilde P_{\mathrm{guess}}(X_1, \delta_1) \simeq \frac{x}{\sqrt{\pi}\,2^{n-1/2}},$$
$$H_{\min}(X_1, \delta_1) \simeq n - \frac{1}{2} + \log_2\frac{\sqrt{\pi}}{x};$$

these expressions are the analog of (100) and (102). Now, the saturation probability (97) and the condition (98) become

$$\begin{aligned}
P_{\mathrm{saturation}}(X_1, \delta_1) &= 1 - P[-R_1 < X_1(t_l) - \mu_1 < R_1]\\
&= 2[1 - \Phi(x)] < P_{\mathrm{guess}}(X_1, \delta_1).
\end{aligned} \tag{132}$$

As done in Table I for H_{ref}, we can give the min-entropy $H_{\min}(X_1, \delta_1)$ for some values of x and n.

By comparing Table III with Table I, we see that, for the same values of x and n, the min-entropy $H_{\min}(X_1, \delta_1)$ is half of H_{ref}, as expected because in H_{ref} the correlations between the two outputs are not taken into account. Moreover, by the positions of the blank values we see that the inequality in (132) is a less stringent condition than (98).

TABLE III. The min-entropy $H_{\min}(X_1, \delta_1)$ as a function of the proportionality parameter x and of the ADC number of bits n. A blank value means that the inequality in (132) is not satisfied.

$n\backslash x$	3.0	3.4	4.0	4.6	6.1	8.9	9.5
8	6.74	6.56	6.33	6.12	5.72	5.17	5.08
10		8.56	8.33	8.12	7.72	7.17	7.08
12			10.33	10.12	9.72	9.17	9.08
16				14.12	13.72	13.17	13.08
32					29.72	29.17	29.08

B. Side information

When the classical noise is not trusted, as in Sec. V B, we have to rely on the conditional min-entropy. The analogs of (104) and (105) are now

$$P_{\mathrm{guess}}(X_1, \delta_1|\mathcal{E}_{\mathrm{cl}}) \simeq \mathbb{E}_f\left[\frac{\delta_1}{\sqrt{2\pi\kappa_{12}}|\lambda|R_l(f)}\right],$$
$$H_{\min}(X_1, \delta_1|\mathcal{E}_{\mathrm{cl}}) \simeq \log_2\frac{|\lambda|\sqrt{2\pi\kappa_{12}}}{\delta_1\mathbb{E}_f[R_l(f)^{-1}]}. \tag{133}$$

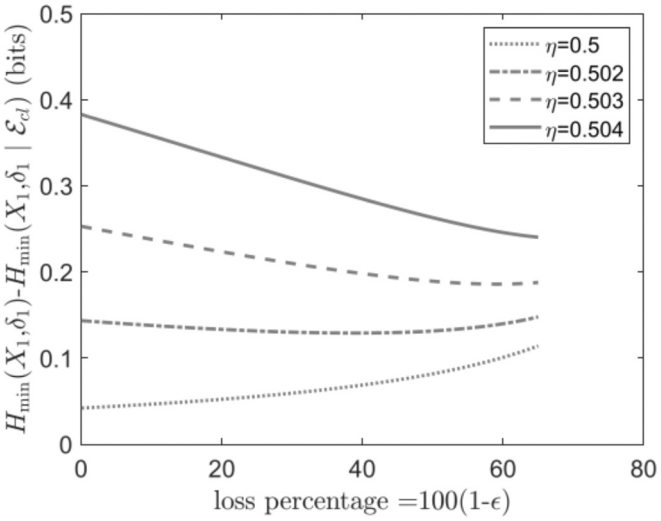

FIG. 6. Entropy loss $H_{\min}(X_1,\delta_1) - H_{\min}(X_1,\delta_1|\mathcal{E}_{\rm cl})$ [Eq. (135)]. Small unbalancing $|1-2\eta| \leqslant 0.008$.

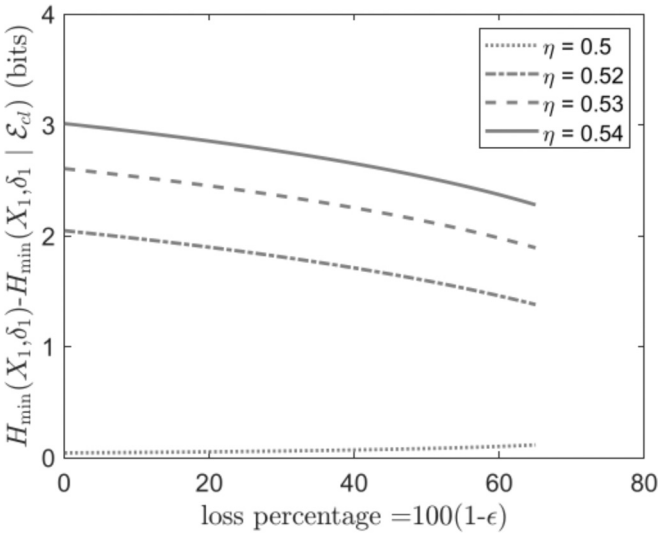

FIG. 7. Entropy loss $H_{\min}(X_1,\delta_1) - H_{\min}(X_1,\delta_1|\mathcal{E}_{\rm cl})$ [Eq. (135)]. Big unbalancing $0.04 \leqslant |1-2\eta| \leqslant 0.08$.

As in (111) and (112), by considering unreliable the classical noise we have the entropy loss

$$H_{\min}(X_1,\delta_1) - H_{\min}(X_1,\delta_1|\mathcal{E}_{\rm cl}) \simeq \tfrac{1}{2}\log_2(1+\Upsilon_1+\Theta_1) + \log_2(\mathbb{E}_f[R_l(f)^{-1}]\sqrt{S_0}), \tag{134}$$

where the expressions of Υ_1 and Θ_1 are given in (89).

To have examples of the effects of the various imperfections on this entropy loss, we take $\epsilon_1 = \epsilon_3 = \epsilon$ and $\xi_1 = \xi_3 = \xi$ as in Sec. V D and we set also $\eta = \eta_3$. By assuming $\log_2(\mathbb{E}_f[R_l(f)^{-1}]\sqrt{S_0}) \simeq 0$ and by using the expressions (128) of the various parameters, we get

$$H_{\min}(X_1,\delta_1) - H_{\min}(X_1,\delta_1|\mathcal{E}_{\rm cl}) \simeq \tfrac{1}{2}\log_2(1+2\epsilon\Upsilon+\Theta/2\epsilon), \tag{135}$$

where Υ and Θ are defined in (123). With the numerical choices for the various parameters discussed in Sec. V D we get $2\epsilon\Upsilon = 10^4\epsilon(1-2\eta)^2$ and $\Theta/2\epsilon = 0.06/\epsilon$. The analogous entropy loss for the double-homodyne case is given in (126), when $\log_2(S_0/S_-) \simeq 0$. Note the different expressions of the coefficients in front of the RIN contribution Υ and the electronic noise contribution Θ. In Figs. 6 and 7 we give the plots of the entropy loss (135) with the same choice for the values of the involved parameters as in the analog figures 4 and 5. The qualitative behavior is very similar in the two cases of double- and single-homodyne scheme. By comparing Table III with Figs. 6 and 7, again we see that the most important parameter for the rate of random bit production is n, giving the ADC resolution.

The single-homodyne scheme is considered experimentally simpler than the double scheme [6,10], but now we have not some analog of what is done in Sec. V C. However, as already discussed at the end of Sec. V B, we can rely on the conditional min-entropy $H_{\min}(X_1,\delta_1|\mathcal{E}_{\rm cl})$ to calibrate the randomness extractor because we can physically block the vacuum input port. Even in the case in which an intruder can send a signal through the signal port we can follow the strategy suggested in [6]. By using a pulsed laser we can make the measured quadrature at time t_l to be characterized by a new random phase [see θ in (14)] not known to the intruder. This prevents the intruder to be capable of sending eigenstates of the measured quadrature and to have some knowledge of the produced random numbers.

An alternative strategy, which can be applied also in our general case, is the one proposed in [4]: one samples a fixed quadrature, but, to avoid a possible eavesdropping, the orthogonal quadrature is sampled at *random times*; then, an entropy lower bound is estimated by an entropic version of the uncertainty relations. A variant of this strategy is discussed in [49], where also the detector inefficiency is taken into account. However, this strategy is not so simpler than the use of the double homodyning. The eight-port circuit needs two ADC components and four photodiodes; the random sampling strategy needs only an ADC and two photodiodes, but a component which switches the phases at random times, with its own source of randomness, has to be added.

VII. DISCUSSION

By using the example of the eight-port optical circuit, we have shown how to use QSC to give a fully quantum treatment of traveling waves in the circuit and of direct, homodyne, heterodyne detection in continuous time. A key point is that the number operators of the quantum fields used in QSC are a family of commuting self-adjoint operators and their joint pvm can be introduced (see Remark 4). Then, the POVMs related to the field quadratures enter into play when the Hilbert space component associated with the LO field is traced out and the system is reduced to the Hilbert component associated with the signal alone. Moreover, we have shown how to introduce imperfections such as imbalanced beam splitters, phase and intensity noise in the LO laser, inefficiency of the photodetectors, and electronic noise. In this way we have a complete quantum description of the apparatus of Fig. 1

monitoring in continuous time the quantum field entering the signal port.

We consider also the case in which the continuous output is sampled at discrete times. Now, discrete mode operators can be introduced, but they result to be random operators because the LO fluctuations are involved in the definition of such operators (see Remark 9). So, even in this case, the description in continuous time is an essential step, as already suggested in [8].

Finally, we study the case in which the apparatus is used as QRNG, both in the cases of double- and single-homodyne detection. Our treatment allows for taking into account the various imperfections on the detected noise. By the use of the conditional min-entropy the effect of untrusted parts of the noise can be eliminated. While the electronic noise is treated as additive noise as usual, a very peculiar role is played by the LO intensity noise which is involved in the construction of the discrete quadrature operators and its effect is less straightforward (see Remark 11). We show how the random bit generation rate decreases when we consider that side information could be gained by an intruder through the classical noise or when he could have also access to the input signal port (quantum side information). Some experimentally reasonable examples are treated and the entropy losses are numerically computed, depending on some parameters characterizing the imperfections in the circuit and in the detection part of the apparatus.

Our quantum analysis of the apparatus of Fig. 1 could be applied when it is employed as a detector, for instance, in problems of quantum teleportation and quantum dense coding (see [18]) or of QKD (see [8]). Note that in QKD and QRNG the security instances are completely different. In QRNG the unused ports can be physically blocked (see the discussion at the end of Sec. V B), while QKD is a problem of secure communication and an intruder could have access to the transmitted signal.

ACKNOWLEDGMENT

The authors acknowledge support from the Italian Space Agency (ASI) Contract No. 2020-23-HH.

APPENDIX A: PROPERTIES OF THE BOSE FIELDS AND SOME QUANTUM EXPECTATIONS

Let us recall some properties of the Bose fields $a_j(t)$ introduced in Sec. II [26]. We work in the Fock representation, which means that the CCRs are realized in the Hilbert space

$$\Gamma = \prod_{j=1}^{d}{}^{\otimes} \Gamma_j, \quad \Gamma_j = \mathbb{C} \oplus \sum_{n=1}^{\infty} L^2(\mathbb{R})^{\otimes_s n}; \tag{A1}$$

Γ_j is the *symmetric Fock space* over the one-particle space $L^2(\mathbb{R})$ and the direct sum on the right is its decomposition in the n-particle spaces. In all developments, a key role is played by the coherent vectors $e_j(f) \in \Gamma_j$, or normalized *exponential vectors*, which can be introduced by giving their components in the n-particle spaces: for $f \in L^2(\mathbb{R})$,

$$e_j(f) = e^{-\frac{1}{2}\|f\|^2}\left(1, f, \frac{f\otimes f}{\sqrt{2!}}, \dots, \frac{f^{\otimes n}}{\sqrt{n!}}, \dots\right). \tag{A2}$$

These vectors are completely analogous to the coherent vectors of the case of discrete modes, as one sees by comparing the representations in the spaces with fixed number of photons.

Finally, let us recall that QSC [26] is an Itô-type calculus involving the integral form (3) of the quantum fields; by this calculus a theory of quantum stochastic differential equations has been developed. In handling the "stochastic differentials" a "promemoria" is given by the Itô table:

$$\begin{aligned} dA_k(t)dA_l^\dagger(t) &= \delta_{kl}dt, & dA_i(t)d\Lambda_{kl}^A(t) &= \delta_{ik}dA_l(t), \\ d\Lambda_{kl}^A(t)dA_i^\dagger(t) &= \delta_{li}dA_k^\dagger(t), & d\Lambda_{kl}^A(t)d\Lambda_{ij}^A(t) &= \delta_{li}d\Lambda_{kj}^A(t), \end{aligned} \tag{A3}$$

all the other products vanish. This table has the same role as the heuristic rule $[dW(t)]^2 = dt$ in classical Itô stochastic calculus. The rigorous definition of field and gauge operators (3) is through their action on the exponential vectors.

1. Output fields

By combining Eqs. (5), (7), and (8) we express the output fields $D_j(t)$ in terms of the fields $A_j(t)$ and $A_{j+}(t)$; in terms of field densities we get

$$\begin{aligned} d_1(t) &= \sqrt{\eta_3\epsilon_1}[\sqrt{\eta_1}\,a_1(t) + i\sqrt{1-\eta_1}\,a_2(t)] \\ &\quad + e^{i\psi_1}\sqrt{(1-\eta_3)\epsilon_1}[i\sqrt{\eta_2}\,a_3(t) - \sqrt{1-\eta_2}\,a_4(t)] + i\sqrt{1-\epsilon_1}\,a_{1+}(t), \end{aligned} \tag{A4a}$$

$$\begin{aligned} d_3(t) &= \sqrt{(1-\eta_3)\epsilon_3}[i\sqrt{\eta_1}\,a_1(t) - \sqrt{1-\eta_1}\,a_2(t)] \\ &\quad + e^{i\psi_1}\sqrt{\eta_3\epsilon_3}[\sqrt{\eta_2}\,a_3(t) + i\sqrt{1-\eta_2}\,a_4(t)] + i\sqrt{1-\epsilon_3}\,a_{3+}(t), \end{aligned} \tag{A4b}$$

$$d_2(t) = \sqrt{\eta_4\epsilon_2}[i\sqrt{1-\eta_1}\,a_1(t) + \sqrt{\eta_1}\,a_2(t)] + e^{i\psi_2}\sqrt{(1-\eta_4)\epsilon_2}[-\sqrt{1-\eta_2}\,a_3(t) + i\sqrt{\eta_2}\,a_4(t)] + i\sqrt{1-\epsilon_2}\,a_{2+}(t), \tag{A4c}$$

$$d_4(t) = \sqrt{(1-\eta_4)\epsilon_4}[-\sqrt{1-\eta_1}\,a_1(t) + i\sqrt{\eta_1}\,a_2(t)] + e^{i\psi_2}\sqrt{\eta_4\epsilon_4}[i\sqrt{1-\eta_2}\,a_3(t) + \sqrt{\eta_2}\,a_4(t)] + i\sqrt{1-\epsilon_4}\,a_{4+}(t). \tag{A4d}$$

2. Properties of the laser

Let us collect here some features of the laser model of Sec. II B. By the definition of the various processes we have easily (16) and

$$\mathbb{E}_f[f(t)] = \lambda w e^{-i\omega_0 t-\gamma_0 t}, \quad \mathbb{E}_f[\overline{f(s)}f(t)] = |\lambda|^2\exp\{i\omega_0(s-t) - \gamma_0|t-s|\}[w^2 + v(t-s)], \tag{A5a}$$

$$\mathbb{E}_f[f(s)f(t)] = \lambda^2 e^{-(i\omega_0+\gamma_0)(t+s)-2\gamma_0(t\wedge s)}[w^2 + v(t-s)], \tag{A5b}$$

$$\mathbb{E}_f[|f(t)|^2 f(s)] = |\lambda|^2\lambda w[1 + 2v(t-s)]e^{-(i\omega_0+\gamma_0)s}, \tag{A5c}$$

$$\mathrm{Cov}_f[|f(t)|^2, |f(s)|^2] = 2|\lambda|^4 v(t-s)[2w^2 + v(t-s)]. \tag{A5d}$$

The relative intensity noise (13) reduces to $n_{\mathrm{RIN}}(t) = u(t)^2 - 1$, which has zero mean and covariance (17). The RIN is not normally distributed, but it is the square of a Gaussian process, due to the $u(t)^2$ contribution. By the choice of the function $v(t)$ we can make its correlations to decay very fast. As a measure of this noise, an effective RIN coefficient can be introduced by integrating the correlations (17) over time:

$$\mathrm{RIN}_{\mathrm{eff}} = \int_{\mathbb{R}} ds\,\mathbb{E}_f[n_{\mathrm{RIN}}(t)n_{\mathrm{RIN}}(t-s)] = 4w^2\tilde{v}(0) + \frac{1}{\pi}\int_{\mathbb{R}}\tilde{v}(\nu)^2\,d\nu,$$

where we have used (17) and (18).

A simple choice is to take an exponential behavior for the correlations $v(t)$:

$$v(t) = v(0)e^{-\gamma_1|t|}, \quad v(0) \geqslant 0, \quad \gamma_1 > 0. \tag{A6}$$

This gives

$$\mathbb{E}_f[n_{\mathrm{RIN}}(t)n_{\mathrm{RIN}}(s)] = 4w^2 v(0)e^{-\gamma_1|t-s|} + 2v(0)^2 e^{-2\gamma_1|t-s|}, \tag{A7}$$

$$\tilde{v}(\nu) = \frac{2v(0)\gamma_1}{\gamma_1^2 + \nu^2}, \quad \mathrm{RIN}_{\mathrm{eff}} = \frac{2}{\gamma_1}(1-w^2)(1+3w^2). \tag{A8}$$

Moreover, the intensity spectrum, introduced in (19), turns out to be

$$\Pi_f(\mu) = \frac{2|\lambda|^2 w^2\gamma_0}{\gamma_0^2 + (\mu-\omega_0)^2} + \frac{2|\lambda|^2(1-w^2)(\gamma_0+\gamma_1)}{(\gamma_0+\gamma_1)^2 + (\mu-\omega_0)^2}. \tag{A9}$$

Finally, the RIN spectrum takes the expression

$$\Pi_{\mathrm{RIN}}(\mu) = 8(1-w^2)\gamma_1\left[\frac{w^2}{\gamma_1^2+\mu^2} + \frac{1-w^2}{4\gamma_1^2+\mu^2}\right]. \tag{A10}$$

3. Moments of the photocurrents

Let us introduce the following combinations of transmissivity and efficiency parameters:

$$g_{11} = \eta_1\eta_3\epsilon_1, \qquad g_{22} = (1-\eta_2)(1-\eta_4)\epsilon_2, \tag{A11a}$$

$$g_{12} = \eta_2(1-\eta_3)\epsilon_1, \quad g_{21} = (1-\eta_1)\eta_4\epsilon_2, \tag{A11b}$$

$$g_{31} = \eta_1(1-\eta_3)\epsilon_3, \quad g_{32} = \eta_2\eta_3\epsilon_3, \tag{A11c}$$

$$g_{j3} = \sqrt{g_{j1}g_{j2}}, \qquad g_{41} = (1-\eta_1)(1-\eta_4)\epsilon_4, \tag{A11d}$$

$$g_{42} = (1-\eta_2)\eta_4\epsilon_4. \tag{A11e}$$

By using the input and output expressions of the fields (A4), the state (9), and the notation (A11) we get

$$d_1(r)\rho_f^T = [\sqrt{g_{11}}\,a_1(r) + ie^{i\psi_1}\sqrt{g_{12}}\,f(r)]\rho_f^T, \tag{A12a}$$

$$d_3(r)\rho_f^T = [i\sqrt{g_{31}}\,a_1(r) + e^{i\psi_1}\sqrt{g_{32}}\,f(r)]\rho_f^T, \tag{A12b}$$

$$d_2(r)\rho_f^T = [i\sqrt{g_{21}}\,a_1(r) - e^{i\psi_2}\sqrt{g_{22}}\,f(r)]\rho_f^T, \tag{A12c}$$

$$d_4(r)\rho_f^T = [-\sqrt{g_{41}}\,a_1(r) + ie^{i\psi_2}\sqrt{g_{42}}\,f(r)]\rho_f^T. \tag{A12d}$$

From these equations, we can compute the quantum expectation of any normal ordered function of the fields $d_i^\dagger(\cdot)$, $d_j(\cdot)$.

By using (11), (12), (26), (27), (A5), and (A12) we get easily

$$\mathbb{E}_P[M_j(t)] = \xi_j \int_0^t dr\, h(t-r)\big\{g_{j1}\langle a_1^\dagger(r)a_1(r)\rangle_T + g_{j2}\mathbb{E}_f[|f(r)|^2] + s_j g_{j3}\big(ie^{i\psi_j}\mathbb{E}_f\big[f(r)\langle a_1^\dagger(r)\rangle_T^f\big] + \text{c.c.}\big)\big\}, \tag{A13}$$

$$\begin{aligned}\mathbb{E}_P[M_j(t)M_i(s)] = {}& \delta_{ij}\xi_j^2 \int_0^{t\wedge s} dr\, h(t-r)h(s-r)\{g_{j1}\langle a_1^\dagger(r)a_1(r)\rangle_T + g_{j2}\mathbb{E}_f[|f(r)|^2] \\ & + s_j g_{j3}\big(ie^{i\psi_j}\mathbb{E}_f\big[f(r)\langle a_1(r)\rangle_T^f\big] + \text{c.c.}\big)\} + \xi_j\xi_i \int_0^t dr \int_0^s dr'\, h(t-r)h(s-r') \\ & \times \mathbb{E}_f[(: \{g_{j1}a_1^\dagger(r)a_1(r) + g_{j2}|f(r)|^2 + s_j g_{j3}(ie^{i\psi_j}f(r)a_1^\dagger(r) + \text{H.c.})\} \\ & \times \{g_{i1}a_1^\dagger(r')a_1(r') + g_{i2}|f(r')|^2 + s_i g_{i3}(ie^{i\psi_i}f(r')a_1^\dagger(r') + \text{H.c.})\} :\rangle_T^f];\end{aligned} \tag{A14}$$

the constants g_{ij} are defined in (A11) and $s_1 = s_2 = +1$, $s_3 = s_4 = -1$; the notation $: \cdot :$ means normal order.

APPENDIX B: PROBABILITY LAW AND CHARACTERISTIC OPERATOR

For stochastic processes the probability law is uniquely determined by its Fourier transform, the *characteristic functional* [50]; the same holds for pvms and POVMs, whose Fourier transform is called *characteristic operator* [20–22].

1. Characteristic operator for the counts of photons and of the output photocurrents

In the case of the increments of the commuting self-adjoint number operators (21), the characteristic operator in the time interval $(0, t)$ and the characteristic functional of the associated counting processes $N_j(t)$ in the interval $(0, T)$ are given by

$$\hat\Phi_t^N[\vec k] = \exp\left\{i\sum_{j=1}^4 \int_0^t k_j(s)d\hat N_j(s)\right\} = \prod_{j=1}^4 \exp\left\{i\int_0^t k_j(s)d\hat N_j(s)\right\}, \tag{B1a}$$

$$\Phi_T^N[\vec k] = \mathbb{E}_P\left[\exp\left\{i\sum_{j=1}^4 \int_0^T k_j(t)dN_j(t)\right\}\right] = \big\langle \hat\Phi_T^N[\vec k]\big\rangle_T; \tag{B1b}$$

we have used the notation (12) for the quantum expectations. The functions $k_j(t)$ are called test functions and are the analog of the variables which are introduced in the definition of an usual Fourier transform. A very important point is that the characteristic operator $\hat\Phi_t^N[\vec k]$ satisfies a closed evolution equation, represented by the quantum stochastic equation

$$d\hat\Phi_t^N[\vec k] = \hat\Phi_t[\vec k]\sum_{j=1}^4 (e^{ik_j(t)} - 1)d\hat N_j(t), \tag{B2}$$

which can be obtained by using the heuristic rules (A3).

a. Case of a coherent signal

Let us consider the case of a coherent state for the signal or a mixture of coherent states. The system state is given by (9)–(12) with $\rho_1^{f,T} \to \rho_1^{f_s,T} = |e_1(f_s)\rangle\langle e_1(f_s)|$, where $f_s(t)$ is a stochastic process. Now P_f denotes the joint probability law of the two processes, so that (11) becomes

$$\rho_{13}^T = \mathbb{E}_f\big[\rho_{13}^{\vec f,T}\big], \qquad \rho_{13}^{\vec f,T} = |e_1(f_{s,T})\rangle\langle e_1(f_{s,T})| \otimes |e_3(f_T)\rangle\langle e_3(f_T)|. \tag{B3}$$

Given f and f_s fixed, by the factorization properties of the exponential vectors and of the Fock space [22,26], Eqs. (B1b), (B2), and (A12) give

$$\frac{d\Phi_t^N[\vec k;\vec f]}{dt} = \Phi_t[\vec k;\vec f]\sum_{j=1}^4 \big(e^{ik_j(t)} - 1\big)J_j(t;\vec f),$$

$$J_j(t;\vec f) = |\sqrt{g_{j1}}f_s(t) + s_j ie^{i\psi_j}\sqrt{g_{j2}}f(t)|^2, \quad s_1 = s_2 = +1, \quad s_3 = s_4 = -1, \quad \psi_{j+2} = \psi_j. \tag{B4}$$

Then, we have

$$\Phi_T^N[\vec k;\vec f] = \exp\left\{\sum_{j=1}^4 \int_0^T \big(e^{ik_j(t)} - 1\big)J_j(t;\vec f)dt\right\}, \tag{B5}$$

which is the characteristic functional of four Poisson processes of intensities $J_j(t;\vec{f})$. When f and f_s are random, the total characteristic functional turns out to be

$$\Phi_T^N[\vec{k}] = \mathbb{E}_f\big[\Phi_T^N[\vec{k};\vec{f}]\big] = \mathbb{E}_f\left[\exp\left\{\sum_{j=1}^4 \int_0^T \big(e^{ik_j(t)}-1\big)J_j(t;\vec{f})dt\right\}\right], \tag{B6}$$

and we have a mixture of Poisson processes, as reported in Remark 5, where the notation $J_j^f(t) = J_j(t;f,0)$ is used.

b. Output currents

In the case of the processes $M_j(t)$ and of the pvm of the commuting self-adjoint operators $\{\hat{M}_j(t),\ j=1,\dots,4,\ t\in(0,T)\}$, the characteristic operator and the characteristic functional are given by

$$\hat{\Phi}_T^M[\vec{k}] = \exp\left\{i\sum_{j=1}^4 \int_0^T ds\, k_j(s)\hat{M}_j(s)\right\}, \tag{B7a}$$

$$\Phi_T^M[\vec{k}] = \mathbb{E}_P\left[\exp\left\{i\sum_{j=1}^4 \int_0^T ds\, k_j(s)M_j(s)\right\}\right] = \big\langle\hat{\Phi}_T^M[\vec{k}]\big\rangle_T. \tag{B7b}$$

By inserting the expressions (24) into (B7) we immediately find

$$\hat{\Phi}_T^M[\vec{k}] = \hat{\Phi}_T^N[\vec{k}], \quad \Phi_T^M[\vec{k}] = \Phi_T^N[\vec{l}], \tag{B8a}$$

$$l_j(r) = \int_r^T ds\, F_j(s,r)k_j(s) = \xi_j\int_r^T ds\, h(s-r)k_j(s), \tag{B8b}$$

where the characteristic operator of the number operators and the characteristic functional of the counting processes are given by (B1).

2. Characteristic operator of the observed processes

Similarly, the characteristic functional of the observed processes $X_j(t)$ [Eq. (28)] is defined by

$$\Phi_T^X[\vec{k}] = \mathbb{E}_P\left[\exp\left\{i\sum_{j=1}^2 \int_0^T dt\, k_j(t)X_j(t)\right\}\right], \tag{B9a}$$

while the characteristic operator of the compatible operators (29) is

$$\hat{\Phi}_T^X[\vec{k}] = \exp\left\{i\sum_{j=1}^2 \int_0^T dt\, k_j(t)\hat{X}_j(t)\right\}. \tag{B9b}$$

Then, we get

$$\Phi_T^X[\vec{k}] = \Phi_T^N[\vec{l}], \quad \hat{\Phi}_T^X[\vec{k}] = \hat{\Phi}_T^N[\vec{l}], \quad \Phi_T^X[\vec{k}] = \big\langle\hat{\Phi}_T^X[\vec{k}]\big\rangle_T; \tag{B10a}$$

Φ_T^N and $\hat{\Phi}_T^N$ are given by Eqs. (B1), while the functions $l_j(r)$ are defined by Eqs. (B8) together with

$$k_3(s) = -k_1(s), \quad k_4(s) = -k_2(s). \tag{B10b}$$

Characteristic functional in the case of signal in a coherent state. In the case of the mixture of coherent states as in Appendix B 1 a, we get from (B10) the characteristic functional of the observed processes $X_j(t)$:

$$\Phi_T^X[\vec{k}] = \mathbb{E}_f\left[\exp\left\{\sum_{j=1}^4 \int_0^T (e^{il_j(t)}-1)J_j(t;\vec{f})dt\right\}\right], \tag{B11}$$

where $l_j(t)$ is given in (B8) and $J_j(t;\vec{f})$ in (B4).

3. Characteristic operator in the limit of strong LO

To analyze the structure of the processes $Y_j(\cdot)$ and to get their probability law in the strong LO limit, we introduce the processes

$$Z_j(t) = \frac{\xi_j N_j(t) - \xi_{j+2}N_{j+2}(t)}{|\lambda|\kappa_{j3}}, \quad j=1,2. \tag{B12}$$

By (28) and (41) we have

$$Y_j(t) = \kappa_{j3} \int_0^t h(t-r) dZ_j(r). \tag{B13}$$

By using the processes $Z_j(\cdot)$ we can prove Proposition 1 and Corollary 2:

Proof. The probability law of the processes $Z_j(\cdot)$ is uniquely determined by the characteristic functional of their increments, defined by

$$\Phi_t^Z[\vec{k}] = \mathbb{E}_P\left[\exp\left\{ i \sum_{j=1}^2 \int_0^t k_j(s) dZ_j(s) \right\}\right]. \tag{B14}$$

By (B12), this functional can be expressed in terms of the characteristic functional and characteristic operator (B1) of the increments of the four counting processes $N_j(\cdot)$:

$$\Phi_t^Z[\vec{k}] = \Phi_T^N[\vec{\ell}/|\lambda|] = \left\langle \hat{\Phi}_T^N[\vec{\ell}/|\lambda|] \right\rangle_T, \quad \ell_j(s) = \frac{\xi_j k_j(s)}{\kappa_{j3}}, \quad \ell_{j+2}(s) = -\frac{\xi_{j+2} k_j(s)}{\kappa_{j3}}. \tag{B15}$$

By using the structures (9)–(12) of the field state, we can introduce the *reduced characteristic operator* of the Z observables:

$$\hat{\Psi}_t^Z[\vec{k}; f] = \mathrm{Tr}_{\Gamma_3 \otimes \Gamma^\perp}\left\{ \hat{\Phi}_t^N[\vec{\ell}/|\lambda|] \left(\rho_3^{f,T} \otimes \rho^\perp \right) \right\}. \tag{B16}$$

Then, the Z functional (B14) can be written as

$$\Phi_t^Z[\vec{k}] = \mathbb{E}_f\left[\mathrm{Tr}_{\Gamma_1}\left\{ \hat{\Psi}_t^Z[\vec{k}; f] \rho_1^{f,T} \right\} \right]. \tag{B17}$$

By construction, $\hat{\Psi}_t^Z[\vec{k}; f]$ is the Fourier transform of a POVM on the signal Hilbert space Γ_1.

By using the differential of the characteristic operator of the number operators (B2) and the factorization properties of Fock spaces and exponential vectors [22,26], we get a quantum stochastic differential equation for the reduced characteristic operator (B16):

$$d\hat{\Psi}_t^Z[\vec{k}; f] = \hat{\Psi}_t^Z[\vec{k}; f] \sum_{j=1}^4 \left(e^{i\ell_j(t)/|\lambda|} - 1 \right) \mathrm{Tr}_{\Gamma_3 \otimes \Gamma^\perp}\left\{ d\hat{N}_j(t) \left(\rho_3^{f,T} \otimes \rho^\perp \right) \right\}, \tag{B18}$$

where the ℓ functions are given in (B15). Then, we can expand the exponential up to the second order in $1/|\lambda|$. By the assumption of G_{j2} [Eq. (43)] independent of λ, we get, in the limit $|\lambda| \to +\infty$,

$$\begin{aligned} &\frac{i\ell_j(t)}{|\lambda|} \mathrm{Tr}_{\Gamma_3 \otimes \Gamma^\perp}\left\{ d\hat{N}_j(t) \left(\rho_3^{f,T} \otimes \rho^\perp \right) \right\} + \frac{i\ell_{j+2}(t)}{|\lambda|} \mathrm{Tr}_{\Gamma_3 \otimes \Gamma^\perp}\left\{ d\hat{N}_{j+2}(t) \left(\rho_3^{f,T} \otimes \rho^\perp \right) \right\} \\ &\quad \simeq ik_j(t)[G_{j2}|\tilde{f}(t)|^2 dt + (ie^{i\psi_j} \tilde{f}(t) dA_1^\dagger(t) + \mathrm{H.c.})], \end{aligned}$$

$$-\frac{\ell_j(t)^2}{2|\lambda|^2} \mathrm{Tr}_{\Gamma_3 \otimes \Gamma^\perp}\left\{ d\hat{N}_j(t) \left(\rho_3^{f,T} \otimes \rho^\perp \right) \right\} - \frac{\ell_{j+2}(t)^2}{2|\lambda|^2} \mathrm{Tr}_{\Gamma_3 \otimes \Gamma^\perp}\left\{ d\hat{N}_{j+2}(t) \left(\rho_3^{f,T} \otimes \rho^\perp \right) \right\} \simeq -k_j(t)^2 \frac{\kappa_{j2}}{2\kappa_{j3}^2} |\tilde{f}(t)|^2 dt.$$

By using these expressions, we have that the limit for $|\lambda| \to +\infty$ of Eq. (B18) exists and, by using (52b), it is given by

$$d\hat{\Psi}_t^Z[\vec{k}; f] = \hat{\Psi}_t^Z[\vec{k}; f] \sum_{j=1}^2 \left\{ ik_j(t)[G_{j2}|\tilde{f}(t)|^2 dt + d\hat{Q}_j(t)] - \frac{\kappa_{j2}}{2\kappa_{j3}^2} |\tilde{f}(t)|^2 k_j(t)^2 dt \right\}. \tag{B19}$$

By the rules of QSC, this equation can be integrated and we get

$$\hat{\Psi}_t^Z[\vec{k}; f] = \exp \int_0^t \left\{ \sum_{j=1}^2 ik_j(s)(G_{j2}|\tilde{f}(s)|^2 ds + d\hat{Q}_j(s)) - \frac{1}{2}\left[\sum_{j=1}^2 \left(\frac{\kappa_{j2}}{\kappa_{j3}^2} - 1 \right) k_j(s)^2 - 2k_1(s)k_2(s)\cos\phi \right] |\tilde{f}(s)|^2 ds \right\}. \tag{B20}$$

To check this result one has to differentiate (B20) by using the rules (A3); in this way, (B19) is obtained. These computations prove also the existence of the limit in (50).

By using (B20), (B13), and (B17), we obtain the expressions (51) and (52). The expression $\hat{\Psi}_T^Q[\vec{k}; f]$ [Eq. (52a)] is the characteristic operator which we would have obtained in the case of perfect efficiency, $\epsilon_j = 1$, balanced outputs, i.e., $G_{j2} = 0$ and $\Delta_{j2} = 0$, and nonrandom laser; as these parameters are arbitrary, also $\hat{\Psi}_T^Q[\vec{k}; f]$ is the characteristic operator of a POVM. This ends the proof of Proposition 1.

To prove Corollary 2 the easiest way is to take the characteristic functional (B11), (B8), and (B4) and to compute the limit (50). Then, the characteristic functional of the Y processes turns out to be given by (51a) and (53). ■

4. Characteristic operator and probability density for the case of discrete sampling

In this Appendix we prove Propositions 3 and 4, giving the structure of the characteristic function of the random variables $Y_j(t_l)$.

a. Proof of Proposition 3

Proof. To get the characteristic function $\Phi^{\vec{Y}}(\vec{k})$ [Eq. (72)] we insert $k_j(s) = \sum_l k_j^l \delta(s - t_l)$ into the characteristic functional $\Phi_T^Y[\vec{k}]$ [Eq. (50)]. From (51a), (51b), and Assumption 3 we get

$$\Phi_T^Y(\vec{k}) = \mathbb{E}_f\big[\Phi_T^Q[\vec{u}; f]\Gamma_T[\vec{u}; f]\big], \quad u_j(s) = \kappa_{j3} \sum_l k_j^l h(t_l - s)1_{(t_l-\tau,t_l)}(s).$$

From (51d) we obtain

$$\Gamma_T[\vec{u}; f] = \exp\left\{\sum_{j,l} \int_{t_l-\tau}^{t_l} ds|\tilde{f}(s)|^2 \left[ik_j^l G_{j2}\kappa_{j3}h(t_l - s) - \frac{\sigma_j^2 + V_j^2}{2} \kappa_{j3}^2 {k_j^l}^2 h(t_l - s)^2\right]\right\};$$

this expression gives (74) and (75). Moreover, from (51c) and (52), we get

$$\Phi_T^Q[\vec{u}; f] = \mathrm{Tr}_{\Gamma_1}\left\{\hat{\Psi}_T^Q[\vec{u}; f]\rho_1^{f,T}\right\},$$

$$\hat{\Psi}_T^Q[\vec{u}; f] = \exp\sum_l \left\{ i \sum_{j=1}^2 \int_{t_l-\tau}^{t_l} \kappa_{j3}k_j^l h(t_l - s)\, d\hat{Q}_j(s) - \frac{1}{2}\int_{t_l-\tau}^{t_l} h(t_l - s)^2 \big|\tilde{f}(s)\big|^2 ds \sum_{i,j=1}^2 k_j^l \kappa_{j3}\, \Xi_{ji}\kappa_{i3}k_i^l \right\}.$$

By using Eqs. (66) and the fact that the quadrature operators commute for different values of l, we get the product structure and by expressing the quantity in square brackets as a squared modulus, this equation gives (76).

Once again, the expression $\hat{\Psi}^q(\vec{k}; f)$ [Eq. (76)] is the characteristic operator which we would have obtained in the case of perfect efficiency, $\epsilon_j = 1$, balanced outputs, i.e., $G_{j2} = 0$ and $\Delta_{j2} = 0$, and nonrandom laser; as these parameters are arbitrary, also $\hat{\Psi}^q(\vec{k}; f)$ is the characteristic operator of a POVM. By taking a single time t_l we have that also each one of the factors is the characteristic operator of a POVM. ■

b. Proof of Proposition 4

Proof. First, we define the parameter

$$v_l = R_l(f)\big[\kappa_{13}k_1^l + e^{i\phi}\kappa_{23}k_2^l\big].$$

By using the parameters v_l and $\alpha,\ \beta$ [Eq. (77)], we can check by direct computations that the characteristic operator (76) can be written as

$$\hat{\Psi}_l^q(\vec{k}^l; f) = \exp\left\{i(v_l a_l^\dagger + \overline{v_l}\, a_l) - \tfrac{1}{2}|\alpha v_l - \beta\overline{v_l}|^2\right\}.$$

Again by direct computations, by using (70) and (78b), we can verify that

$$a_l = -i(e^{i\phi}\alpha b_l + e^{-i\phi}\beta b_l^\dagger), \quad u_l = ie^{-i\phi}(\alpha v_l - \beta\,\overline{v_l}).$$

This gives $v_l a_l^\dagger + \overline{v_l}\, a_l = u_l b_l^\dagger + \overline{u_l}\, b_l$ and $|\alpha v_l - \beta\overline{v_l}|^2 = |u_l|^2$ and (78a) is proved.

Then, by using CCRs and the overcompleteness property of the coherent states for the mode b_l we have

$$\begin{aligned}\hat{\Psi}_l^q(\vec{k}^l; f) &= e^{i\,\overline{u_l}\,b_l} e^{iu_l b_l^\dagger} \\ &= e^{i\,\overline{u_l}\,b_l}\frac{1}{\pi}\int_{\mathbb{C}} d^2\zeta\ |\psi_l(\zeta;\alpha,\beta)\rangle\langle\psi_l(\zeta;\alpha,\beta)|e^{iu_l b_l^\dagger} \\ &= \frac{1}{\pi}\int_{\mathbb{C}} d^2\zeta\ e^{i\,\overline{u_l}\,\zeta}|\psi_l(\zeta;\alpha,\beta)\rangle\langle\psi_l(\zeta;\alpha,\beta)|e^{iu_l\,\overline{\zeta}};\end{aligned}$$

this proves (79). ■

c. Proof of Eq. (81)

Proof. First, the parameter (78b), needed in (79), can be written as

$$u_l = K_1^l(f)k_1^l - e^{-i\phi}K_2^l(f)k_2^l.$$

Then, we can compute the anti-Fourier transform of (80):

$$\begin{aligned}\hat{g}^l_Y(y_1,y_2;f) &= \frac{1}{4\pi^2}\int_{\mathbb{R}^2} dk_1dk_2\, e^{-i(y_1k_1+y_2k_2)}\hat{\Psi}^{\vec{Y}}_l(k_1,k_2)\\ &= \frac{1}{4\pi^2}\int_{\mathbb{C}} d^2z\,\hat{g}^l_{\alpha,\beta}(z)\int_{\mathbb{R}^2} dk_1dk_2\,\exp\left\{-i(y_1k_1+y_2k_2)+i(u_l\,\overline{z}+\overline{u_l}\,z)+\sum_j\left[ik_j\mu^{jl}_{\mathcal{L}}(f)-\frac{1}{2}\,\sigma^{jl}_{\mathcal{L}}(f)^2\,{k_j}^2\right]\right\}\\ &= \frac{1}{4\pi^2}\int_{\mathbb{C}} d^2z\,\hat{g}^l_{\alpha,\beta}(z)\int_{\mathbb{R}^2} dk_1dk_2\,\exp\left\{-\frac{1}{2}\sum_j\sigma^{jl}_{\mathcal{L}}(f)^2\,{k_j}^2\right\}\\ &\quad\times\exp\left\{ik_1\left[\mu^{1l}_{\mathcal{L}}(f)+2z_1x^l_1(f)-y_1\right]+ik_2\left[\mu^{2l}_{\mathcal{L}}(f)+2x^l_2(f)(z_2\sin\phi-z_1\cos\phi)-y_2\right]\right\},\end{aligned}$$

where we have used $z=z_1+iz_2$. By computing the Gaussian integral in dk_1dk_2, we get the POVM density $\hat{g}^l_Y(y_1,y_2;f)$ [Eq. (81)]. ■

APPENDIX C: THE POVM AND THE PROBABILITY DENSITY OF THE Y OBSERVABLES

1. Signal in a mixture of coherent states

The density (83) can be explicitly computed, for instance, in the case of the signal in a mixture of coherent states as in Corollary 2. By using (53) and (51) we get the characteristic function, from which we see that the density turns out to be a mixture of normal distributions. We define

$$\mu^l_j(\vec{f}) = \mu^{jl}_{\mathcal{L}}(f)+\kappa_{j3}\int_0^\tau dt\,h(t)(ie^{i\psi_j}\overline{f_s(t_l-t)}\tilde{f}(t_l-t)+\text{c.c.}),$$

where $\mu^{jl}_{\mathcal{L}}(f)$ is given in (75b). Then, the probability density can be written as

$$g_{\vec{Y}}(\vec{y}) = \mathbb{E}_f\left[\prod_{l=1}^m\prod_{j=1}^2\frac{1}{\sqrt{2\pi\kappa_{j2}R_l(f)^2}}\exp\left\{-\frac{\left(y^l_j-\mu^l_j(\vec{f})\right)^2}{2\kappa_{j2}R_l(f)^2}\right\}\right]. \tag{C1}$$

Let us note that (48), (49a), and (75c) give the following decomposition of the variances:

$$\kappa_{j2}R_l(f)^2 = \sigma^{jl}_{\mathcal{L}}(f)^2+\kappa^2_{j3}(G_{j3}+1)R_l(f)^2,\quad G_{13}+1=\frac{1}{\eta_1},\quad G_{23}+1=\frac{1}{1-\eta_1}. \tag{C2}$$

2. A density bound

Proposition 5. The POVM density (81) is bounded by

$$\hat{g}^l_Y(y_1,y_2;f)\leqslant\frac{\mathbb{1}}{4\pi R_l(f)^2\kappa_{13}\kappa_{23}|\sin\phi|}. \tag{C3}$$

Moreover, the total probability density (83) is bounded by

$$g_{\vec{Y}}(\vec{y})\leqslant\frac{1}{(4\pi\kappa_{13}\kappa_{23}|\sin\phi|)^m}\prod_{l=1}^m\mathbb{E}_f[R_l(f)^{-2}], \tag{C4}$$

$\forall\,\vec{y}\in\mathbb{R}^{2m}$. This bound holds for any choice of the signal state ρ^f_1 in the expression (83).

Proof. By using the bound (116) we have

$$\begin{aligned}\hat{g}^l_Y(y_1,y_2;f) &\leqslant \frac{1}{2\pi^2\sigma^{1l}_{\mathcal{L}}(f)\sigma^{2l}_{\mathcal{L}}(f)}\int_{\mathbb{C}} d^2z\,\exp\left\{-\frac{\left[\mu^{1l}_{\mathcal{L}}(f)+2z_1K^l_1(f)-y_1\right]^2}{2\sigma^{1l}_{\mathcal{L}}(f)^2}\right\}\\ &\quad\times\exp\left\{-\frac{\left[\mu^{2l}_{\mathcal{L}}(f)+2K^l_2(f)(z_2\sin\phi-z_1\cos\phi)-y_2\right]^2}{2\sigma^{2l}_{\mathcal{L}}(f)^2}\right\}\mathbb{1}\\ &= \frac{1}{2\pi\sqrt{2\pi}\,\sigma^{1l}_{\mathcal{L}}(f)\left|K^l_2(f)\sin\phi\right|}\int_{\mathbb{R}} dz_1\,\exp\left\{-\frac{\left[\mu^{1l}_{\mathcal{L}}(f)+2z_1K^l_1(f)-y_1\right]^2}{2\sigma^{1l}_{\mathcal{L}}(f)^2}\right\}\mathbb{1} = \frac{1}{4\pi\left|K^l_1(f)K^l_2(f)\sin\phi\right|}\,\mathbb{1}.\end{aligned}$$

By inserting the expressions of $K^l_j(f)$ [Eq. (82)] we get (C3). As the POVM densities (81) act, for different values of l, on different factors of the Hilbert space, the analogous bound holds for the total probability density (83), for any choice of the signal state (even if not factorized), and this proves (C4). ■

Let us note that, by inserting the bound (C3) into (113), we get (117).

[1] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, J. Mod. Opt. **47**, 595 (2000).

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

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

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

[5] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, Quantum Sci. Technol. **3**, 025003 (2018).

[6] P. R. Smith, D. G. Marangon, M. Lucamarini, Z. L. Yuan, and A. J. Shields, Simple source device-independent continuous-variable quantum random number generator, Phys. Rev. A **99**, 062326 (2019).

[7] J. Thewes, C. Lüders, and M. Assmann, Eavesdropping attack on a trusted continuous-variable quantum random-number generator, Phys. Rev. A **100**, 052318 (2019).

[8] M. Almeida, D. Pereira, M. Facao, A. N. Pinto, and N. A. Silva, Impact of imperfect homodyne detection on measurements of vacuum states shot noise, Opt. Quantum Electron. **52**, 503 (2020).

[9] W. Huang, Y. Zhang, Z. Zheng, Y. Li, B. Xu, and S. Yu, Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator, Phys. Rev. A **102**, 012422 (2020).

[10] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. J. T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information, Nat. Commun. **12**, 605 (2021).

[11] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, Nat. Commun. **9**, 5365 (2018).

[12] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Naples, 2005).

[13] J. Kiukas and P. Lahti, A note on the measurement of phase space observables with an eight-port homodyne detector, J. Mod. Opt. **55**, 1891 (2008).

[14] U. Leonhardt, *Essential Quantum Optics. From Quantum Measurements to Black Holes* (Cambridge University Press, Cambridge, 2010).

[15] P. Lahti, J.-P. Pellonpää, and J. Schultz, Realistic eight-port homodyne detection and covariant phase space observables, J. Mod. Opt. **57**, 1171 (2010).

[16] G. Dmochowski, A. Feizpour, and X. Xing, 8-port homodyne detection of optical fields using IQ demodulation, Meas. Sci. Technol. **30**, 095201 (2019).

[17] J. Kiukas and P. Lahti, On the moment limit of quantum observables, with an application to the balanced homodyne detection, J. Mod. Opt. **55**, 1175 (2008).

[18] M. Ban, S. Kitajimaa, and F. Shibataa, Quadrature operators with arbitrary phase and applications to phase-space distribution and quantum communication, J. Mod. Opt. **61**, 582 (2014).

[19] M. G. Raymer, J. Cooper, H. J. Carmichael, M. Beck, and D. T. Smithey, Ultrafast measurement of optical-field statistics by dc-balanced homodyne detection, J. Opt. Soc. Am. B **12**, 1801 (1995).

[20] A. Barchielli, Measurement theory and stochastic differential equations in quantum mechanics, Phys. Rev. A **34**, 1642 (1986).

[21] P. Zoller and C. W. Gardiner, Quantum noise in quantum optics: the stochastic Schrödinger equation, in *Fluctuations Quantiques (Les Houches 1995)*, edited by S. Reynaud, E. Giacobino, and J. Zinn-Justin (North-Holland, Amsterdam, 1997), pp. 79–136.

[22] A. Barchielli, Continual Measurements in Quantum Mechanics and Quantum Stochastic Calculus, in *Open Quantum Systems III*, edited by S. Attal, A. Joye, and C.-A. Pillet, Lecture Notes in Math 1882 (Springer, Berlin, 2006), pp. 207–291.

[23] S. Zippilli, G. Di Giuseppe, and D. Vitali, Entanglement and squeezing of continuous-wave stationary light, New J. Phys. **17**, 043025 (2015).

[24] R. L. Hudson and K. R. Parthasarathy, Quantum Itô's formula and stochastic evolutions, Commun. Math. Phys. **93**, 301 (1984).

[25] C. W. Gardiner and M. J. Collet, Input and output in damped quantum systems: Quantum stochastic differential equations and the master equation, Phys. Rev. A **31**, 3761 (1985).

[26] K. R. Parthasarathy, *An Introduction to Quantum Stochastic Calculus* (Birkhäuser, Basel, 1992).

[27] A. Santamato, A quantum theory of photodetection and other optical devices, Master thesis, University of Milan, 2010, doi:10.13140/RG.2.2.36655.48801.

[28] A. Barchielli and M. Gregoratti, Quantum optomechanical system in a Mach-Zehnder interferometer, Phys. Rev. A **104**, 013713 (2021).

[29] A. Barchielli, Direct and heterodyne detection and other applications of quantum stochastic calculus to quantum optics, Quantum Opt. **2**, 423 (1990).

[30] A. Barchielli, Detection theory in quantum optics and quantum stochastic calculus, in *Quantum Aspects of Optical Communications*, edited by C. Bendjaballah, O. Hirota, and S. Reynaud, Lecture Notes in Physics Vol. 378 (Springer, Berlin, 1991), pp. 179–189.

[31] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982); *Probabilistic and Statistical Aspects of Quantum Theory*, 2nd ed. (Edizioni della Normale, Pisa, 2011).

[32] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, Cambridge 2010).

[33] A. Barchielli and M. Gregoratti, Quantum measurements in continuous time, non-Markovian evolutions and feedback, Philos. Trans. R. Soc. A **370**, 5364 (2012).

[34] A. Barchielli and M. Gregoratti, Quantum continuous measurements: The stochastic Schrödinger equations and the spectrum of the output, Quantum Meas. Quantum Metrol. **1**, 34 (2013).

[35] C. Dorrer, D. C. Kilper, H. R. Stuart, G. Raybon, and M. G. Raymer, Linear optical sampling, IEEE Photon. Technol. Lett. **15**, 1746 (2003).

[36] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, Phys. Rev. A **98**, 012312 (2018).

[37] Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, and L. Tian, A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution, New J. Phys. **13**, 013003 (2011).

[38] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[39] J. H. Shapiro, H. P. Yuen, and J. A. Machado Mata, Optical communication with two-photon coherent states—Part II: Photoemissive detection and structured receiver performance, IEEE Trans. Inf. Theory **25**, 179 (1979).

[40] H. P. Yuen and J. H. Shapiro, Optical communication with two-photon coherent states—Part III: Quantum measurements realizable with photoemissive detectors, IEEE Trans. Inf. Theory **26**, 78 (1980).

[41] M. Asjad, S. Zippilli, and D. Vitali, Mechanical Einstein-Podolsky-Rosen entanglement with a finite-bandwidth squeezed reservoir, Phys. Rev. A **93**, 062307 (2016).

[42] M. O. Scully and M. S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, 1997).

[43] S. Bottacchi, *Noise and Signal Interference in Optical Fiber Transmission Systems* (Wiley, Hoboken, NJ, 2008).

[44] D. Meschede, *Optics, Light and Lasers* (Wiley, Hoboken, NJ, 2007).

[45] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).

[46] H. J. Carmichael, *Statistical Methods in Quantum Optics*, Vol. 2 (Springer, Berlin, 2008).

[47] N. Datta and R. Renner, Smooth entropies and the quantum information spectrum, IEEE Trans. Inf. Theory **55**, 2807 (2009).

[48] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, Fast Random Bit Generation Using a Chaotic Laser: Approaching the Information Theoretic Limit, IEEE J. Quantum Electron. **49**, 910 (2013).

[49] W. O. Krawec, Quantum random number generation with practical device imperfections, in *Proceedings of SPIE 12093, Quantum Information Science, Sensing, and Computation XIV* (SPIE, Bellingham, WA, 2022), p. 1209307.

[50] D. J. Daley and D. Vere-Jones, *An Introduction to the Theory of Point Processes. Volume II: General Theory and Structure*, 2nd ed. (Springer, Berlin, 2008).