# Self-coherent phase reference sharing for continuous-variable quantum key distribution

Adrien Marie[*] and Romain Alléaume

*Télécom ParisTech, LTCI, CNRS, 46 Rue Barrault, 75013 Paris, France*

(Received 1 September 2016; published 17 January 2017)

We develop a comprehensive framework to model and optimize the performance of continuous-variable quantum key distribution (CV-QKD) with a local local oscillator (LLO), when phase reference sharing and QKD are jointly implemented. We first analyze the limitations of the only existing approach, called LLO-sequential, and show that it requires high modulation dynamics and can only tolerate small phase noise. Our main contribution is to introduce two designs to perform LLO CV-QKD, respectively called LLO-delayline and LLO-displacement, and to study their performance. Both designs rely on a self-coherent approach, in which phase reference information and quantum information are coherently obtained from a single optical wavefront. We show that these designs can lift some limitations of the existing LLO-sequential approach. The LLO-delayline design can in particular tolerate much stronger phase noise and thus appears to be an appealing alternative to LLO-sequential in terms of network integrability. We also investigate, with the LLO-displacement design, how phase reference information and quantum information can be multiplexed within a single optical pulse. By studying the trade-off between phase reference recovery and phase noise induced by displacement, we, however, demonstrate that this design can only tolerate low phase noise. On the other hand, the LLO-displacement design has the advantage of minimal hardware requirements and provides a simple approach to multiplex classical and quantum communications, opening a practical path towards the development of ubiquitous coherent classical-quantum communications systems compatible with next-generation network requirements.

DOI: 10.1103/PhysRevA.95.012316

## I. INTRODUCTION

Quantum key distribution (QKD) [1–3] is a promising technology that has reached the commercialization step in the past decade [4,5]. Targeting deployment over large-scale networks, next-generation QKD should rely on affordable optical components. It will in particular consist of highly integrated systems able to operate at high rate and able to be deployed over modern optical networks. Relying on standard telecommunication equipment, continuous-variable (CV) QKD is an attractive approach towards this next step of QKD development [6,7]. While first results towards CV-QKD practical photonics chip integration have been pursued [8,9], the possibility of effectively deploying CV-QKD in coexistence with intense wavelength-division multiplexing classical channels has been demonstrated [10]. Furthermore, high repetition rates (up to the order of hundreds of MHz) [11,12] in CV-QKD systems have also been demonstrated recently. Although they are more sensitive to optical losses than discrete-variable based QKD, long-distance CV-QKD has, however, been demonstrated by controlling excess noise [13] and developing high-efficiency error correction codes [14]. These important steps in the recent development of CV-QKD are, in addition, likely to benefit from the rise of classical coherent communications [15], with the prospect of convergence of classical and quantum communication techniques and simplified photonic integration. This positions CV-QKD and more generally quantum coherent communications as an appealing technology for the the development of modern quantum communications.

### A. Sharing a reference frame in CV-QKD

Quantum coherent communication protocols have to address one specific challenge, namely phase reference sharing. As a matter of fact, the receiver must perform a phase-sensitive detection using an optical beam usually called a "local oscillator" whose phase drift with respect to the emitter must be controlled, or estimated, and corrected. The problem of sharing a reference frame is specific in the sense that reference frame information constitutes *unspeakable information* that can only be shared through physical carriers exchanged between emitter and receiver [16]. On the other hand, it is important to emphasize that although quantum mechanics gives a precise framework to formulate the question of reference frame sharing, in relation with quantum metrology [16], this question can be solved classically, using macroscopic signals to exchange reference frame information. The type of question related to phase reference sharing is not whether it is possible but whether it can be achieved given resource constraints, dictated by the hardware resources and by the characteristics of the channel, such as losses and noise. In line with the recent work on LLO CV-QKD [17–19], we will focus on in this article on the issue of jointly performing, with the same hardware, phase reference sharing and CV-QKD. We will, in particular, focus on the Gaussian-modulated coherent state (GMCS) [20] protocol.

### B. The transmitted local oscillator design

In most implementations of CV-QKD performed so far [12,21–23], the phase reference is directly transmitted from Alice to Bob through the optical channel as a bright optical pulse with each quantum signal pulse and is used as the LO pulse at reception. Such implementation is detailed in Fig. 1 and is referred to as the transmitted LO (TLO) design. The main advantage of this scheme is the guarantee, by

[*] adrien.marie@telecom-paristech.fr

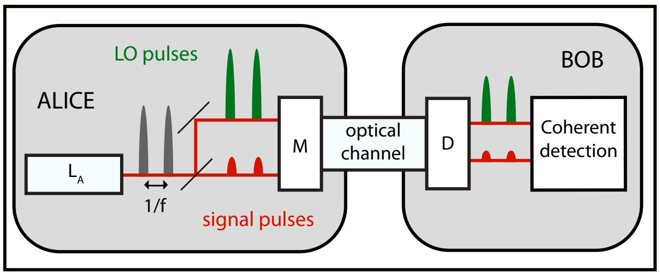

FIG. 1. Transmitted local oscillator (TLO) design. In the TLO design, the phase reference (green pulse) and the quantum signal (red pulse) are derived from the same optical pulse and sent from Alice to Bob using multiplexing and demultiplexing (MD) techniques.

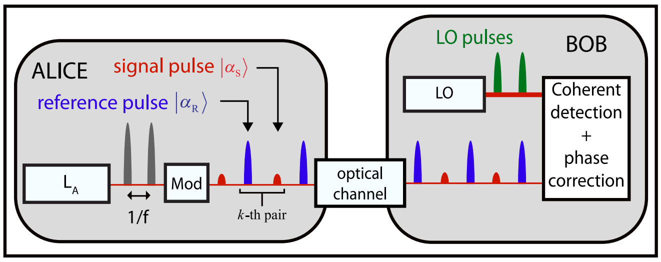
ALICE
signal pulse $|\alpha_S\rangle$
reference pulse $|\alpha_R\rangle$
$L_A$
1/f
Mod
$k$-th pair
optical channel
LO pulses
BOB
LO
Coherent detection + phase correction

FIG. 2. Local local oscillator (LLO) sequential design. In the LLO-sequential design, Alice sequentially sends weak quantum signal (red pulse) and bright phase reference (blue pulse) pulses. At reception, Bob performs consecutive coherent detections of each pulse received using is own LO pulses (green pulse).

design, of a stable relative phase between quantum signal and LO at reception by producing both of them from a single laser $L_A$ placed at Alice's side. Although it is the most implemented GMCS protocol, limitations of this design have been pointed out in Refs. [17–19]. Security weaknesses of such implementations have, however, been demonstrated in practice by manipulating the LO intensity [24–26] or wavelength [27] on the quantum channel. Furthermore, such protocols rely on the use of a bright LO at reception. For long distance or high speed (where the pulse duration is short), the requirements in terms of launch power at emission creates practical issues. This will, in particular, limit the possibility of using the TLO design on shared optical fibers at long distance and high-rate operation, i.e., situations where the requirements on LO power at emission would be extremely large.

### C. The local local oscillator method

In order to lift the limitations of CV-QKD implementations relying on the TLO design, a CV-QKD method relying on a so-called local local oscillator (LLO) has recently been independently introduced in Refs. [17–19]. This method, implementing the Gaussian modulated coherent state protocol, consists in using a second laser at Bob's side in order to produce local LO pulses for coherent detections. One crucial advantage of implementing CV-QKD in a LLO configuration is to close, by design, any potential security loophole linked to the possibility of manipulating the LO as it propagates on the public optical channel between Alice and Bob. Implementing LLO CV-QKD allows us, on the other hand, to ensure by design that the LO is fully trusted, and in particular that the LO amplitude (that requires careful calibration) cannot be manipulated. Another important advantage of LLO CV-QKD stems from the fact that in this configuration, repetition rate and distance do not affect the LO intensity at detection. A LO power sufficient to ensure high electronic-to-shot-noise ratio may thus be obtained, independently of the propagation distance.

Implementing CV-QKD in the LLO configuration, however, comes with experimental challenges. The main issue in LLO-based CV-QKD is to be able to perform CV-QKD despite the potentially important drift of the relative phase between Alice's emitter laser $L_A$ and Bob's local oscillator laser $L_B$; see Fig. 2. The relative phase at reception is, in the case of LLO-based CV-QKD, the relative phase between the two free-running lasers $L_A$ and $L_B$. As such, Bob's raw measurement outcomes are *a priori* decorrelated from Alice's quadratures and a phase correction process has to be performed in order to allow secret key generation. The goal of the phase reference sharing in the context of LLO CV-QKD is then to ensure a phase noise low enough so that the excess noise is significantly below the threshold imposed by security proofs [7].

### D. The LLO-sequential method

Recent works [17–19] have demonstrated the possibility of implementing the GMCS protocol using a local local oscillator, by introducing an experimental design, depicted on Fig. 2, that we will call LLO-sequential. In the LLO-sequential design, Alice sequentially sends, at a repetition rate $f/2$, consecutive pairs $(|\alpha_S\rangle,|\alpha_R\rangle)$ of coherent states, where $|\alpha_S\rangle$ is a GMCS quantum signal pulse and $|\alpha_R\rangle = |E_R\rangle$ is a phase reference pulse with a fixed phase set to 0 and an amplitude $E_R$. Phase reference pulses are relatively bright pulses compared to the signal and have a fixed phase in Alice's phase reference frame, which is publicly known so that it carries information on Alice's reference frame. At reception, Bob performs sequential coherent detections of quantum signal and phase reference, using a single detector, operated with a local local oscillator, placed at Bob. Bob can thus estimate the relative phase using the phase reference pulse and a phase correction can be performed on Alice and Bob's signal data in order to generate the secret key.

In Ref. [18] a 250-kHz-clocked proof-of-principle experiment of the LLO-sequential designed is performed, however, with only one single laser playing the role of both emitter and LO and two consecutive uses of a homodyne detector used to emulate a heterodyne measurement. In Ref. [17], another proof-of-principle experiment with two lasers and Alice and Bob connected by a 25-km optical fiber is performed with a 50-MHz-clocked system. The authors demonstrate that phase correction can be implemented with a residual excess noise compatible with CV-QKD security threshold. Joint operation of CV-QKD (requiring weak quantum signals) together with the phase correction mechanism (requiring bright phase reference pulses) was studied through a simulation, which left aside the question of the hardware requirements for both CV-QKD and phase reference sharing. Reference [19] provides a whole experimental demonstration of an implementation of LLO-sequential CV-QKD over 25 km, with a 100-MHz-clocked system, and a 1-GHz-bandwidth shot-noise limited homodyne detection. We should, however, emphasize that these strong experimental performances have been obtained with two external-cavity lasers (ECL), as emitter and LO, and an amplitude modulator with 60 dB of dynamics. We show in this work that adopting some alternative experimental schemes allows us to perform CV-QKD and phase reference sharing with same hardware and yet lighter requirements, thanks to better phase noise tolerance.

### E. Contributions of this work

We identify and discuss the existing approaches to the phase reference sharing problem for LLO CV-QKD. Recent works [17–19] all rely on time-multiplexed quantum signals pulses with reference pulses in order to jointly perform phase recovery and quantum communication. In this work, we introduce new elements in the standard noise model of CV-QKD analysis, considering practical constraints imposed by the simultaneous quantum signal and phase reference transmission of LLO-based CV-QKD. In particular, we show that the amplitude modulator dynamics is a key parameter in order to compare performance of realistic implementations of LLO-based CV-QKD. Based on this comprehensive model, we show that there exist fundamental and practical limitations in the phase noise tolerance of the design introduced in Refs. [17–19] that we designate as LLO-sequential.

In order to go beyond that phase noise limit, we introduce the idea of self-coherence in phase reference sharing for CV-QKD implementations based on a local local oscillator. Self-coherent designs consist in ensuring the phase coherence between pairs of quantum signal and phase reference pulses by deriving both of them from the same optical wavefront at emission. This allows us to perform relative phase recovery schemes with better sensitivity than in the LLO-sequential design. In particular, we propose a design, called LLO-delayline, that implements a self-coherent phase sharing design. It ensures the self-coherence using a balanced delay-line interferometer split between emitter and receiver sides. We analyze how self-coherence is obtained and study the performance reachable with this design, demonstrating that they exhibit a much stronger resilience to high phase noise than the LLO-sequential design under realistic experimental parameters. While previous experimental proposals of LLO CV-QKD are limited to slowly varying reference frames regimes (i.e., based on very stable lasers or high repetition rates), our newly introduced design allows phase reference sharing resilient to high phase noise regimes, using the idea of self-coherence.

A second self-coherent design, referred to as LLO-displacement, relies on an original multiplexing allowing to transmit both the quantum signal and the reference pulse within each optical pulse. The simultaneous transmission of quantum signal and phase reference can be seen as an original cryptographic primitive, considered in Ref. [28], that can be used with different modulation schemes. In particular, this allows us to optimize the resources—in terms of required hardware and repetition rate—in LLO-based CV-QKD experiments. We also emphasize that an important advantage of our LLO-displacement design is its experimental simplicity as we show that the multiplexing can be perform numerically on Alice's variables. As such, no specific hardware devices are required. We study the theoretical performance of such design and exhibit its limitations.

In Sec. II, we introduce the CV-QKD model. In particular, the phase reference sharing issue in CV-QKD is formally introduced and discussed and we also introduce our comprehensive noise model. In Sec. III, we highlight practical limitations of existing local local oscillator–based CV-QKD and introduce the idea of self-coherence for reference sharing in CV-QKD. In Secs. IV and V, we respectively introduce the LLO-delayline and LLO-displacement designs and study their performance. Conclusion and perspectives are presented in Sec. VI.

## II. CV-QKD: NOISE MODEL

We introduce new elements in the standard noise model in order to account for the important constraints that drive the performance of CV-QKD in the regime of a local local oscillator implemented with shared standard hardware. In particular, we consider several contributions to the phase noise as well as practical limitations of the amplitude modulator dynamics, which have not been studied in CV-QKD regimes so far. This in particular allows us to discuss the limitations of LLO-sequential design when implemented with realistic hardwares.

### A. Phase noise

In Ref. [17], the authors consider perfect phase measurement and, in Ref. [18], the performance analysis is performed in the regime of no relative phase drift. However, in order to study the overall influence of the phase noise, we need to jointly consider those contributions. In this work, we analyze CV-QKD performance considering these two contributions at the same time. We also consider the optical phase drift during the propagation of optical pulses on the optical channel, thus resulting in a comprehensive model for analyzing all the considered designs. In LLO-based CV-QKD, the main challenge is to create a reliable phase reference between emitter and receiver because the relative phase drift between the two involved lasers may fully decorrelate Alice's variables and Bob's measurements, thus preventing any secret key rate generation. We define the *signal relative phase* $\theta_S$ as the phase difference between the LO pulse $|\alpha_{LO}\rangle$ and the signal pulse $|\alpha_S\rangle$ at reception:

$$\theta_S = \varphi_{LO} - \varphi_S, \tag{1}$$

where $\varphi_S$ is the signal phase and $\varphi_{LO}$ is the phase of the local oscillator at reception. Using the notations of Eq. (A1) and in the presence of a relative phase $\theta_S$, we can write Bob's measurement outcomes, when performing a heterodyne, as

$$\begin{pmatrix} x_B \\ p_B \end{pmatrix} = \sqrt{\frac{G}{2}}\left[\begin{pmatrix} \cos\theta_S & \sin\theta_S \\ -\sin\theta_S & \cos\theta_S \end{pmatrix}\begin{pmatrix} x_A \\ p_A \end{pmatrix} + \begin{pmatrix} x_0 + x_c \\ p_0 + p_c \end{pmatrix}\right], \tag{2}$$

where $x_c$ and $p_c$ capture all excess noise sources but the phase noise. The relative phase $\theta_S$ acts as the selector of the measured quadrature. In the TLO design, the relative phase $\theta_{\mathrm{S}}$ is, by design, always close to 0. However, in the case of two free-running lasers, $\theta_{\mathrm{S}}$ depends on the relative phase $\theta$ between the two lasers. Assuming that the two lasers $\mathrm{L}_A$ and $\mathrm{L}_B$ are centered around the same optical frequency and have spectral linewidths $\Delta\nu_A$ and $\Delta\nu_B$, we can model [29–31] the relative phase $\theta = \varphi_B - \varphi_A$ ($\varphi_A$ and $\varphi_B$ are respectively the phase of $\mathrm{L}_A$ and $\mathrm{L}_B$) as a Gaussian stochastic process $\{\theta_t\}_t$ characterized by the variance of the drift between two times $t_i$ and $t_{i+1}$:

$$\mathrm{var}(\theta_{i+1}|\theta_i) = 2\pi(\Delta\nu_A + \Delta\nu_B)|t_{i+1} - t_i|, \tag{3}$$

where $\theta_i$ and $\theta_{i+1}$ correspond to the relative phase at consecutive times $t_i$ and $t_{i+1}$.

We can see from Eq. (2) that this implies a decorrelation between Alice's data and Bob's measurements, which can be seen as a contribution, noted $\xi_{\mathrm{phase}}$, to the excess noise $\xi$. The principle of phase reference sharing schemes considered in the article consists in using a reference pulse to build an estimate $\hat{\theta}_{\mathrm{S}}$ of the actual relative phase $\theta_{\mathrm{S}}$ of the signal (relative means relative with respect to local oscillator) and to apply a phase correction $-\hat{\theta}_{\mathrm{S}}$ on the signal, in order to compensate for the phase drift. In a reverse reconciliation scheme, this correction has to be performed on Alice's data as a rotation of her data:

$$\begin{pmatrix} \tilde{x_A} \\ \tilde{p_A} \end{pmatrix} = \begin{pmatrix} \cos\hat{\theta}_{\mathrm{S}} & \sin\hat{\theta}_{\mathrm{S}} \\ -\sin\hat{\theta}_{\mathrm{S}} & \cos\hat{\theta}_{\mathrm{S}} \end{pmatrix} \begin{pmatrix} x_A \\ p_A \end{pmatrix}. \tag{4}$$

We can show from Eqs. (A2), (2), and (4) that the remaining excess noise $\xi_{\mathrm{phase}}$ due to phase noise (after correction) depends on the modulation format and is, in general, not symmetric on the two quadratures. However, in the case of the GMCS protocol (with modulation variance $V_A$) and assuming that the remaining phase noise $\theta_{\mathrm{S}} - \hat{\theta}_{\mathrm{S}}$ after correction is Gaussian, the phase noise $\xi_{\mathrm{phase}}$ can then be written as

$$\xi_{\mathrm{phase}} = 2V_A(1 - e^{-V_{\mathrm{est}}/2}), \tag{5}$$

where we define the variance $V_{\mathrm{est}}$ of the *remaining phase noise* (after reference quadrature measurement, relative phase estimation and correction) as

$$V_{\mathrm{est}} \hat{=} \mathrm{var}(\theta_{\mathrm{S}} - \hat{\theta}_{\mathrm{S}}). \tag{6}$$

Equation (5) (derived in the Appendix) is a generalization of the phase noise expression given in Refs. [18,28] for the case of small phase noise.

An important challenge to perform LLO-based CV-QKD is therefore to calculate a precise estimator $\hat{\theta}_{\mathrm{S}}$ of the relative phase $\theta_{\mathrm{S}}$ in order to minimize $V_{\mathrm{est}}$ and thus $\xi_{\mathrm{phase}}$. The general scheme for phase reference sharing design in LLO CV-QKD can be modeled in the following way: Alice generates two coherent states, a quantum signal pulse $|\alpha_{\mathrm{S}}\rangle$ and a reference pulse $|\alpha_{\mathrm{R}}\rangle$, and sends them on the optical channel using some multiplexing scheme. At reception, Bob performs demultiplexing, and uses the received reference pulse to derive an estimate $\hat{\theta}_{\mathrm{R}}$ of the relative phase $\theta_{\mathrm{R}}$ between the reference pulse and the local oscillator at reception. The phase sharing designs (cf. Secs. III, IV, and V) give guarantees that the relative phase of the reference pulse is close to the relative phase of the quantum signal, i.e., that $\theta_{\mathrm{R}} \approx \theta_{\mathrm{R}}$. Therefore, the estimated value $\hat{\theta}_{\mathrm{R}}$ can be used to approximate and then correct the relative phase of the signal $\theta_{\mathrm{S}}$.

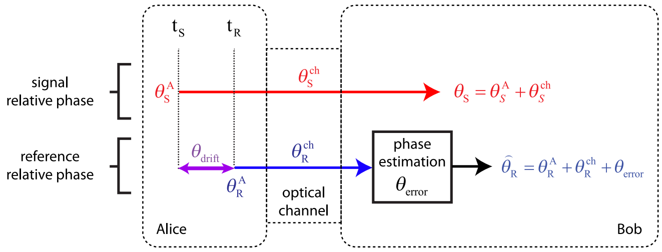

FIG. 3. Schematic representation of a general relative phase estimation process. The relative phase $\theta_{\mathrm{S}}$ at reception (red), which is defined with respect to the $LO$ phase [Eq. (1)], is estimated at reception with the estimator $\hat{\theta}_{\mathrm{R}}$ inferred from specific reference phase information evaluation (blue).

A general picture of the phase estimation process, and of the sources of deviations, is depicted in Fig. 3. We can express the quantum signal relative phase $\theta_{\mathrm{S}}$ (with respect to local oscillator) as the sum of the relative phase $\theta_{\mathrm{S}}^{\mathrm{A}}$ at emission and the phase $\theta_{\mathrm{ch}}^{\mathrm{S}}$ accumulated by the coherent state $|\alpha_{\mathrm{S}}\rangle$ on the optical channel:

$$\theta_{\mathrm{S}} = \theta_{\mathrm{S}}^{\mathrm{A}} + \theta_{\mathrm{S}}^{\mathrm{ch}}. \tag{7}$$

Similarly, using the same notations for the reference pulse $|\alpha_{\mathrm{R}}\rangle$, we can express the relative phase $\theta_{\mathrm{R}}$ at reception of a reference pulse $|\alpha_{\mathrm{R}}\rangle$ as

$$\theta_{\mathrm{R}} = \theta_{\mathrm{R}}^{\mathrm{A}} + \theta_{\mathrm{R}}^{\mathrm{ch}}. \tag{8}$$

At reception, Bob measures both quadratures of $|\alpha_{\mathrm{R}}\rangle$ using a heterodyne detection (in the remaining of the paper, we only consider heterodyne detections at reception with $\delta_{\mathrm{det}} = 2$). The estimator $\hat{\theta}_{\mathrm{R}}$ of $\theta_{\mathrm{R}}$ can be calculated from the heterodyne measurement outcomes $x_B^{(\mathrm{R})}$ and $p_B^{(\mathrm{R})}$ as

$$\hat{\theta}_{\mathrm{R}} = \tan^{-1}\left(\frac{p_B^{(\mathrm{R})}}{x_B^{(\mathrm{R})}}\right). \tag{9}$$

Due to the fundamental shot noise and the experimental noise on the heterodyne detection, $\hat{\theta}_{\mathrm{R}}$ differs from $\hat{\theta}_{\mathrm{R}}$ by an error $\theta_{\mathrm{error}}$ characterized by its variance:

$$V_{\mathrm{error}} \hat{=} \mathrm{var}\big(\hat{\theta}_{\mathrm{R}} - \theta_{\mathrm{R}}\big). \tag{10}$$

We can show that, in the case of a reference pulse of the form $|\alpha_{\mathrm{R}}\rangle = |E_{\mathrm{R}}\rangle$,

$$V_{\mathrm{error}} = \frac{\chi + 1}{E_{\mathrm{R}}^2}, \tag{11}$$

where $E_{\mathrm{R}} = |\alpha_{\mathrm{R}}|$ is the amplitude of the reference pulse and $\chi$ is defined in Eq. (A2). Finally, Bob uses the relative phase estimate $\hat{\theta}_{\mathrm{S}}$ to apply a phase correction $-\hat{\theta}_{\mathrm{R}}$ to the quantum signal. The overall process is schematically represented in Fig. 3. It results, after phase correction, to a remaining phase noise $V_{\mathrm{est}} = \mathrm{var}(\hat{\theta}_{\mathrm{R}} - \theta_{\mathrm{S}})$, which can be expressed using Eqs. (7) and (8) as

$$V_{\mathrm{est}} = V_{\mathrm{error}} + V_{\mathrm{drift}} + V_{\mathrm{channel}}, \tag{12}$$

where

$$V_{\mathrm{drift}} \hat{=} \mathrm{var}\big(\theta_{\mathrm{R}}^{\mathrm{A}} - \theta_{\mathrm{S}}^{\mathrm{A}}\big), \tag{13}$$

$$V_{\mathrm{channel}} \hat{=} \mathrm{var}\big(\theta_{\mathrm{R}}^{\mathrm{ch}} - \theta_{\mathrm{S}}^{\mathrm{ch}}\big). \tag{14}$$

The term $V_{\text{drift}}$ corresponds to the variance of the relative phase drift $\theta_{\text{drift}} = \theta_{\text{R}}^{\text{A}} - \theta_{\text{S}}^{\text{A}}$ between the two free-running lasers $\text{L}_A$ and $\text{L}_B$ between time $t_{\text{S}}$ at which $|\alpha_{\text{S}}\rangle$ is emitted and time $t_{\text{R}}$ at which $|\alpha_{\text{R}}\rangle$ is emitted. From Eq. (3), we can express the phase noise due to laser phase drift between times $t_{\text{S}}$ and $t_{\text{R}}$ as

$$V_{\text{drift}} = 2\pi(\Delta\nu_A + \Delta\nu_B)|t_{\text{R}} - t_{\text{S}}|. \tag{15}$$

We can observe that the time delay between signal and phase reference emissions implies a decorrelation between the corresponding relative phases and, thus, introduce a noise on the phase estimation process. This leads to the main limitation of the LLO-sequential approach as explained in next section.

The term $V_{\text{channel}}$ corresponds to the relative phase drift due to the difference of the phase accumulated by $|\alpha_{\text{S}}\rangle$ and $|\alpha_{\text{R}}\rangle$ during propagation. In practice, we assume that this term is dominated by the difference between the optical path lengths of $|\alpha_{\text{S}}\rangle$ and $|\alpha_{\text{R}}\rangle$.

In the remaining of this article we will study and discuss the performance of existing as well as newly introduced LLO-based CV-QKD designs, relying on different relative phase sharing designs. For each of these designs, we will explicitly show the expressions of the different contributions to the remaining phase noise $V_{\text{est}}$ of Eq. (12).

### B. Amplitude modulator finite dynamics

Amplitude modulators' efficiencies are limited by their dynamics restricting the range of the achievable transmission coefficient. Recent works [17–19] have proposed to conjointly communicate weak quantum signals and relatively bright reference pulses using a single experimental setup and, in particular, a single amplitude modulator (AM). This directly addresses the issue of the AM dynamics at emission, limiting the maximal amplitude that Alice can output and introducing a leakage on the modulated amplitude. This limitation has not been taken into account in LLO CV-QKD analysis so far and we will show that this is a key parameter in the LLO regime.

The ratio between the maximal and minimal amplitudes $E_{\max}$ and $E_{\min}$ that Alice can output is characterized by the dynamics $d_{\text{dB}}$ of the AM defined as

$$d_{\text{dB}} = 10\log_{10}\left(\frac{E_{\max}^2}{E_{\min}^2}\right). \tag{16}$$

From this equation, one can model Alice's modulator imperfection as an amplitude leakage on each optical pulse, resulting in an excess noise, which can be approximated as

$$\xi_{\text{AM}} = E_{\max}^2 10^{-d_{\text{dB}}/10}, \tag{17}$$

where $E_{\max}$ is the maximal amplitude to be modulated. The finite dynamics of Alice's AM thus adds a noise proportional to the amplitude $E_{\max}$. This imperfection is then a limitation to the maximal amplitude of the phase reference pulses in LLO-based CV-QKD designs.

The necessity of exchanging both weak and intense optical signals in CV-QKD based on a local local oscillator using only one experimental setup is limited by the finite AM dynamics. These effects are not considered in standard TLO designs because only weak quantum signals are modulated and detected but we will show that they are key parameters in order to compare realistic implementations of LLO-based CV-QKD in terms of secret key rate. To our knowledge, the amplitude modulator issue has not been taken into account so far in CV-QKD analysis. Based on this refined model, we first analyze practical limitations of the LLO-sequential design and, then, we compare the LLO-sequential implementations with our newly proposed designs.

## III. TOWARDS IMPROVED PHASE REFERENCE SHARING DESIGNS

In this section, we highlight limitations of the LLO-sequential design in terms of tolerable phase noise due to the underlying phase reference sharing scheme. We then propose the idea of self-coherence to go beyond that phase noise limit.

### A. Limitations of the LLO-sequential design

Since signal and reference pulses follow the same optical path, the estimation process in the LLO-sequential design can be schematically shown using Fig. 3 where $\theta_{\text{S}}^{\text{ch}} = \theta_{\text{R}}^{\text{ch}}$. Thus, we have $V_{\text{channel}} \approx 0$ and the phase noise stems from two contributions: $V_{\text{est}} = V_{\text{drift}} + V_{\text{error}}$.

One important motivation of the present work is related to the fact that there exists a minimal amount of phase noise $V_{\text{est}}$ [Eq. (12)] that can be reached with the LLO-sequential design. The main limitation is due to the fact that signal and reference pulses are emitted with a time delay $1/f$, leading to a phase noise that cannot be compensated, of variance

$$V_{\text{drift}} = 2\pi\frac{\Delta\nu_A + \Delta\nu_B}{f}. \tag{18}$$

The phase variance associated to reference pulse phase estimation error, $V_{\text{error}}$, can be minimized by choosing the amplitude $E_{\text{R}}$ as large as possible. However, the value $E_{\text{R}}$ that can be chosen in practice is limited by the finite dynamics of her amplitude modulator, and the existence of an associated optical leakage, whose excess noise $\xi_{\text{AM}}$ is proportional to the amplitude $E_{\text{R}}$, as discussed in Eq. (17). This in practice leads to a compromise regarding the value of $E_{\text{R}}$, in order to minimize the total excess noise.

The excess noise due to imperfect phase reference sharing reads as [Eq. (5)]

$$\xi_{\text{phase}} = 2V_A(1 - e^{-V_{\text{est}}/2}). \tag{19}$$

In the regimes of low $V_{\text{est}}$, it simplifies to $\xi_{\text{phase}} = V_A V_{\text{est}}$. In order to ensure a tolerable value $\xi_{\text{phase}} \leqslant 0.1$ (typical value of the null key threshold according to security proofs [21,32]), this imposes that $V_{\text{drift}} \lesssim 0.1/V_A$.

We can finally express a lower bound on the total excess noise, sum of the excess noise $\xi_{\text{phase}}$, and the excess noise $\xi_{\text{AM}}$ in the LLO-sequential design as

$$\xi_{\text{phase}} + \xi_{\text{AM}} \geqslant V_A\left(V_{\text{drift}} + \frac{\chi + 1}{E_{\text{R}}^2}\right) + E_{\text{R}}^2 \times 10^{-d_{\text{dB}}/10}. \tag{20}$$

We can quantitatively understand from Eq. (20) that increasing the amplitude $E_{\text{R}}$ can reduce the $\xi_{\text{phase}}$ contribution at the cost of increasing the $\xi_{\text{AM}}$ contribution. The LLO-sequential design is then restricted to the experimental regimes

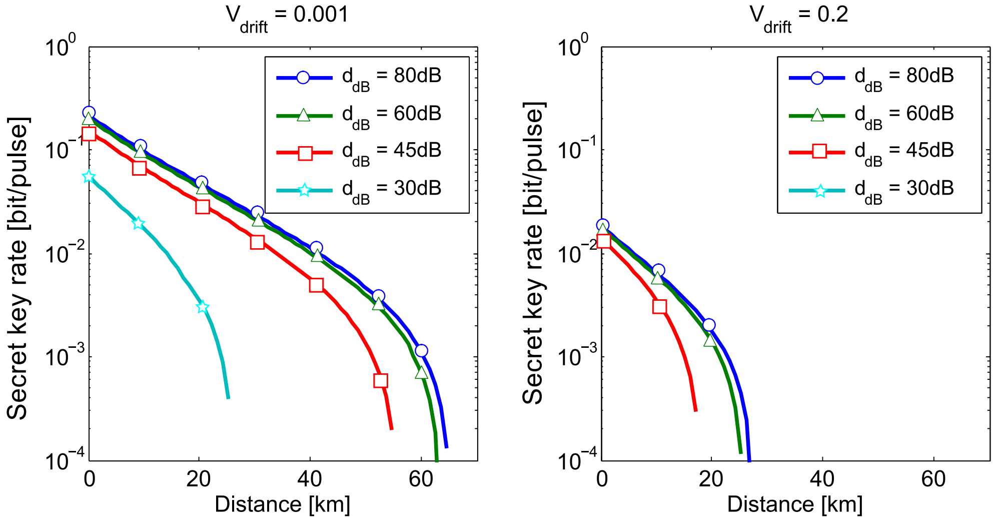

FIG. 4. Secret key rates of the LLO-sequential design for two different values of $V_{\rm drift}$ in the presence of AM finite dynamics $d_{\rm dB}$. Simulations are performed in the individual attacks and pessimistic (Eve can control Bob's detection) model [18]. The values of $V_A$ and $E_{\rm R}$ are chosen to optimize the secret key rate with $\beta = 0.95$, $\eta = 0.7$, $v_{\rm elec} = 0.01$, and $\xi_{\rm tech} = 0.01$.

where $V_{\rm drift} \ll 1$ and where the amplitude modulator dynamics is large. In other words, the LLO-sequential has to be implemented with performance hardware. Current bandwidth limitation of shot-noise limited coherent detectors typically leads researchers to choose $f$ below 100 MHz. This imposes in return requirements on the spectral linewidth of the lasers that can be used in order to perform LLO-sequential CV-QKD: The linewidth of the lasers must be at most of 200 kHz to ensure an excess noise $\xi_{\rm phase}$ lower than 0.1. As a consequence, only low-phase-noise lasers, such as external-cavity lasers (ECL), whose typical spectral linewidth is of a few kHz, are suitable to implement the LLO-sequential design. This is actually illustrated in Ref. [18], where the performance analysis is made in the low-phase-noise regime where $f \gg \Delta\nu_A + \Delta\nu_B$ (i.e., in a regime where $V_{\rm drift} \approx 0$) and in Ref. [19] with the experimental choice of ultra-low-noise of ECL lasers of 1.9 kHz linewidth.

Another issue is actually that finite modulation dynamics has not been taken into account in Ref. [18], allowing the authors to choose arbitrary large amplitudes $E_{\rm R}$. For instance, they show that, by choosing $E_{\rm R}^2 = 500\ V_A$, a distance of 40 km is achievable while a more realistic value $E_{\rm R}^2 = 20 V_A$ ($\xi_{\rm AM} \approx 10^{-2}$ for $d_{\rm dB} = 40$ dB) restricts the protocol to less than 10 km. This indicates that AM dynamics is an important parameter for analyzing CV-QKD within the LLO framework and that the LLO-sequential performances are moreover affected by finite AM dynamics. This hinders its practical use over coherent communication links already equipped with standard telecom AM.

In Fig. 4, we plot the secret key rates of the LLO-sequential design with finite AM dynamics. We can see that the AM dynamics is an important parameter as it allows us to recover the relative phase with good efficiency while ensuring a low excess noise $\xi_{\rm AM}$. Below an AM dynamics of 30 dB, no secret key rate can be produced beyond a distance of around 20 km, even for a moderate relative phase drift $V_{\rm drift} = 10^{-3}$. On the other hand, because of the fundamental limit $V_{\rm drift}$, the LLO-sequential design has to be run at a minimal repetition rate to produce secret key, even in large AM dynamics regimes.

In Table I, we summarize the main characteristics of the two existing implementations of the GMCS protocol proposed so far. Although strong security loopholes have been demonstrated on the TLO implementation, the GMCS protocol has mainly been implemented by directly sending the LO from Alice to Bob. Recent works have however introduced the idea of LLO-based CV-QKD by proposing the experimental LLO-sequential design, hence fixing security weaknesses by generating the LO pulses at Bob side. We have, however, shown that the LLO-sequential design has strong limitations in terms of implementation in realistic regimes. In the next sections, we investigate how these limitations in term of hardware requirements can be lifted by proposing the idea of self-coherence for phase reference sharing designs.

TABLE I. Summary of the advantages and drawbacks of all the different CV-QKD designs considered in this work.

| Design | Trusted LO | Tolerable phase noise | Hardware requirements |
|---|---|---|---|
| Transmitted LO (Fig. 1) [12,21–23] | No | $\Delta\nu/f \sim 10$ | Stable interferometric setup |
| LLO-sequential (Fig. 2) [17–19] | Yes | $V_{\rm drift} \sim 10^{-1}$ (60 dB AM)<br>$V_{\rm drift} \sim 10^{-3}$ (30 dB AM) | High AM dynamics |

### B. Self-coherent phase reference sharing schemes

Performing CV-QKD protocols in the LLO regime can be seen as the issue of conjointly—in the sense of using the same hardware—sharing a phase reference between two remote lasers and performing CV-QKD between the two parties Alice and Bob holding lasers $L_A$ and $L_B$. A first method to perform such task is the LLO-sequential design [17–19]. Indeed, the specific modulation of the sequential optical pulses allows one to perform CV-QKD on signal pulses while sharing the phase reference on specific pulses. We have, however, shown in Sec. III A a fundamental limitation in terms of tolerable relative phase drift in the LLO-sequential design. As an unspeakable information, the phase reference has to be encoded over physical carriers, photons in this case. However, by design, the time delay between the emission of quantum signal photons and phase reference photons introduce a decoherence between signal and reference which can prevent any secret key generation in high-phase-noise regimes.

We now introduce the idea of self-coherence for quantum coherent communication protocols. In order to prevent the phase decorrelation between signal and reference due to sequential emissions, we propose to derive both the signal and reference from the same optical wavefront at emission, thus ensuring the physical coherence between signal and phase reference pulses and ensuring that the relative phase drift from Eq. (12) is $V_{\text{drift}} = 0$. We call such a design *self-coherent*. The relative phase between signal and phase reference is then not affected by the relative phase drift of the lasers and a stable relation between the quantum signal and the LO phases at reception can be provided. As the relative phase estimation no longer depends on the relative phase drift, self-coherent designs allow Alice and Bob to perform more efficient phase reference sharings. This method, however, comes with the challenge of coherently sending—i.e., by conserving the stable phase relation—the quantum signal and the phase reference from Alice to Bob. This challenge can be seen as a multiplexing issue. In the remaining of this work, we propose two designs to realize GMCS CV-QKD, relying on such self-coherent phase reference sharing designs.

Our first proposal to implement self-coherent CV-QKD is to split a single optical pulse into two pulses used to respectively carry signal and reference information. As output of the same optical pulse, the relative phase between the two pulses at reception only depends on the phases accumulated on their optical paths between emission and reception. This phase reference sharing design relies on the balancing of remote delay line interferometers and we refer to it as the LLO-delayline design. We describe and study its performance in Sec. IV.

A second idea, that we introduced in Ref. [33], to directly ensure self-coherence between signal and phase reference is to encode both of them within the same optical pulse at emission while recovering both information at reception. In Sec. V, we propose such a design, the LLO-displacement, in which the phase reference information is encoded over a displacement of the quantum signal modulation. Although we show that LLO-displacement is restricted to low phase noise, an advantage of this design is that the experimental setup is drastically simplified compare to LLO-delayline, which is a major advantage in the optics of the integration of LLO-based CV-QKD.

## IV. SELF-COHERENT DESIGN BASED ON DELAY-LINE INTERFEROMETER

The idea of the LLO-delayline design is to derive consecutive pulse pairs with fixed relative phase, using a balanced delay line interferometer, hence ensuring a self-coherence property. This design does not suffer from the drift limitation of LLO-sequential and can allow Bob to recover the relative phase with better precision.

### 1. The protocol

The protocol can be decomposed in successive cycles at the repetition rate $f/2$. We note $2\tau = 2/f$ is the time interval between two consecutive cycles. Each cycle consists in producing and measuring a self-coherent pair of pulses: one quantum signal pulse and one phase reference pulse. We here describe the protocol for one cycle while Fig. 5 details the overall design.

At the beginning of a cycle, Alice produces a coherent state $|\alpha_{\text{source}}\rangle$, which has an optical phase $\varphi^A_{\text{source}}$. From that single optical pulse, she derives two coherent optical pulses in the following way: She splits the state $|\alpha_{\text{source}}\rangle$ into two optical pulses, using an unbalanced delayline interferometer:

(1) The weak pulse $|\alpha_{\text{S}}\rangle$ is modulated as the GMCS quantum signal and propagates through an optical path of length $l_A$.

(2) The strong pulse $|\alpha_{\text{R}}\rangle$ is delayed by a time $\tau = 1/f$ on a optical path of length $l_A + \delta l_A$ and is referred to as the reference pulse.

Alice then recombines the two pulses $|\alpha_{\text{S}}\rangle$ and $|\alpha_{\text{R}}\rangle$ resulting in consecutive optical pulses. A major point is that the relative phase between phase reference and quantum signal no longer depends on the phase drift between Alice's and Bob's lasers. An other advantage of this scheme is that the amplitude modulator only modulates the quantum signal, which removes the constraints on the AM dynamics. The two optical pulses are then successively sent to Bob through the optical channel, resulting in a repetition rate $f$.

At reception, Bob produces coherent LO pulse pairs using a similar delay line technique used at Alice side. He produces an optical pulse $|\beta_{\text{source}}\rangle$ with phase $\varphi^B_{\text{source}}$ and derives two pulses on a 50:50 beamsplitter:

(1) The pulse $|\beta_{\text{S}}\rangle$ that goes through an optical path of length $l_B$.

(2) The pulse $|\beta_{\text{R}}\rangle$ that is delayed and follows an optical path of length $l_B + \delta l_B$.

Bob uses the $|\beta_{\text{S}}\rangle$ and $|\beta_{\text{R}}\rangle$ pulses as LO pulses to successively measure the received $|\alpha_{\text{S}}\rangle$ and $|\alpha_{\text{R}}\rangle$ pulses. This experimental setup can thus be seen as a remote delay-line interferometer split between Alice and Bob sides.

The reference pulse measurement outcomes allows Bob to calculate an estimation $\hat{\theta}_{\text{R}}$ of the relative phase $\theta_{\text{R}}$ at reference measurement and, thus, infer an estimation of the relative phase $\theta_{\text{S}}$ at signal measurement. Alice can then correct her data to decrease the induced excess noise according to Eq. (4).

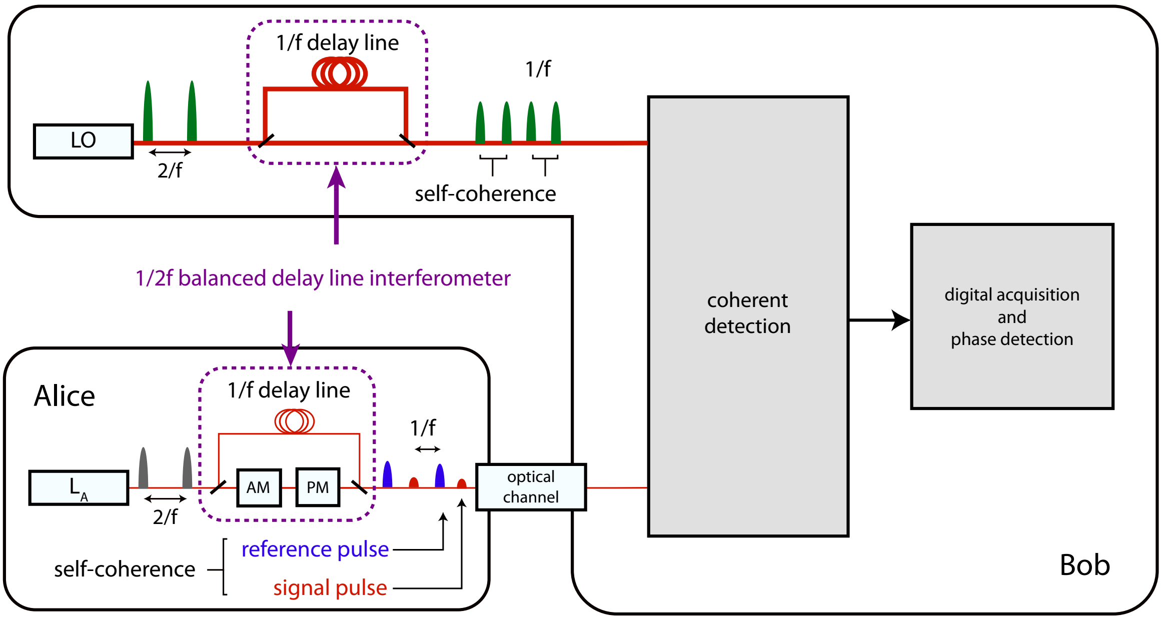

FIG. 5. Full experimental scheme of the LLO-delayline design. Alice sends consecutive phase-coherent signal/reference pulses pairs to Bob based on a balanced delay line interferometer. On his side, Bob uses his own laser as the LO for coherent detections using the same delay line technique to produce phase-coherent LO pulses. Phase estimation and phase correction are digitally performed after measurement acquisition.

### 2. *Excess noise evaluation*

In order to study the performance of the LLO-delayline design and calculate the achievable secret key rate, one can note that Alice modulates the quantum signal according to the standard GMCS modulation. Thus, the usual secret key rates formulas of Ref. [34] can be used. We then have to express the excess noise of the propagating channel in this design, in particular the amplitude modulator noise and the remaining relative phase noise $V_{\mathrm{est}}$.

In the LLO-delayline design, the finite dynamics of Alice's amplitude modulator only induces a small contribution to the excess noise $\xi$ in standard hardware regimes. As it only modulates the quantum signal, the maximal amplitude $E_{\max}$ of Eq. (17) does not depend on the reference pulse amplitude. The excess noise $\xi_{\mathrm{AM}}$ is then independent of the reference amplitude $E_{\mathrm{R}}$ and the intensity $E_{\max}^2$ of Eq. (17) only has to be a few times larger than $V_A$ [34], resulting in a moderate contribution of $\xi_{\mathrm{AM}}$ to the excess noise $\xi$ ($\xi_{\mathrm{AM}} \sim 10^{-2}$ for $V_A = 4$, $E_{\max}^2 = 10\ V_A$, and $d_{\mathrm{dB}} = 30$).

We now quantify the excess noise $\xi_{\mathrm{phase}}$ by expressing the remaining phase noise $V_{\mathrm{est}}$ on Bob's estimation of the relative phase. By design, the simultaneous emission on the source pulse of $|\alpha_{\mathrm{S}}\rangle$ and $|\alpha_{\mathrm{R}}\rangle$, i.e., $t_{\mathrm{S}} = t_{\mathrm{R}}$, implies $\theta_{\mathrm{drift}} = 0$ and, thus, $V_{\mathrm{drift}} = 0$, which corresponds to the self-coherence property. The variance $V_{\mathrm{est}}$ can then be written as the sum of the phase estimation efficiency $V_{\mathrm{error}}$ [given in Eq. (11)] and the variance $V_{\mathrm{channel}}$ [Eq. (14)] of the difference between the accumulated phases on the channel:

$$V_{\mathrm{est}} = V_{\mathrm{error}} + V_{\mathrm{channel}}. \tag{21}$$

In this design, signal and phase reference pulses propagate through different optical paths. Then, the former term depends on the stability of the delayline interferometer. As introduced in Sec. II, this corresponds to the variance:

$$V_{\mathrm{channel}} = \mathrm{var}\big(\theta_{\mathrm{R}}^{\mathrm{ch}} - \theta_{\mathrm{S}}^{\mathrm{ch}}\big), \tag{22}$$

where $\theta_{\mathrm{S}}^{\mathrm{ch}}$ and $\theta_{\mathrm{R}}^{\mathrm{ch}}$ respectively correspond to the phases accumulated by $|\alpha_{\mathrm{S}}\rangle$ and $|\alpha_{\mathrm{R}}\rangle$ through their propagation. Therefore, one wants to express the quantity $\theta_{\mathrm{channel}} = \theta_{\mathrm{R}}^{\mathrm{ch}} - \theta_{\mathrm{S}}^{\mathrm{ch}}$. Using the definition of the relative phase of Eq. (1), we can first write the relative phase as the difference between the phases respectively accumulated by the two interfering LO and signal pulses:

$$\begin{aligned} \theta_{\mathrm{S}}^{\mathrm{ch}} &= \varphi_{\beta,\mathrm{S}}^{\mathrm{acc}} - \varphi_{\alpha,\mathrm{S}}^{\mathrm{acc}}, \\ \theta_{\mathrm{R}}^{\mathrm{ch}} &= \varphi_{\beta,\mathrm{R}}^{\mathrm{acc}} - \varphi_{\alpha,\mathrm{R}}^{\mathrm{acc}}, \end{aligned} \tag{23}$$

where, for instance, $\varphi_{\beta,\mathrm{S}}^{\mathrm{acc}}$ stands for the phase accumulated by the LO pulse $|\beta_{\mathrm{S}}\rangle$ during its propagation. We model the accumulated phase as a linear function $\varphi^{\mathrm{acc}}(l)$ of the optical path length $l$, and then we can derive the following expressions:

$$\begin{aligned} \varphi_{\alpha,\mathrm{S}}^{\mathrm{acc}} &= \varphi^{\mathrm{acc}}(l_A), \\ \varphi_{\alpha,\mathrm{R}}^{\mathrm{acc}} &= \varphi^{\mathrm{acc}}(l_A) + \varphi^{\mathrm{acc}}(\delta l_A), \\ \varphi_{\beta,\mathrm{S}}^{\mathrm{acc}} &= \varphi^{\mathrm{acc}}(l_B), \\ \varphi_{\beta,\mathrm{R}}^{\mathrm{acc}} &= \varphi^{\mathrm{acc}}(l_B) + \varphi^{\mathrm{acc}}(\delta l_B). \end{aligned} \tag{24}$$

Using the previous equations, we can finally express $\theta_{\mathrm{channel}} = \theta_{\mathrm{R}}^{\mathrm{ch}} - \theta_{\mathrm{S}}^{\mathrm{ch}}$ as

$$\theta_{\mathrm{channel}} = \varphi^{\mathrm{acc}}(\delta l_B) - \varphi^{\mathrm{acc}}(\delta l_A). \tag{25}$$

As we can see, the relative phase drift $\theta_{\mathrm{channel}}$ only depends on the difference of the accumulated phases between the delayline optical paths $\delta l_A$ and $\delta l_B$. Due to experimental imperfections as thermal fluctuations, we model $\delta l_A$ and $\delta l_B$ as a stochastic processes over time around the same mean value

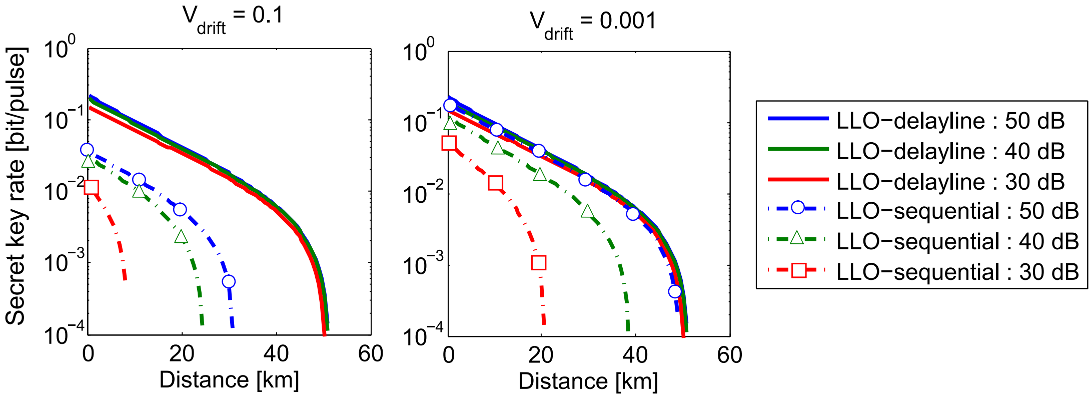

FIG. 6. Secret key rate comparison between the LLO-sequential and the LLO-delayline designs for different AM dynamics and relative phase drift $V_{\rm drift}$.

$\langle\delta l_A\rangle = \langle\delta l_B\rangle = c\tau$ ($c$ being the speed of the light). The phase $\theta_{\rm channel}$ then only depends on the fluctuations of the processes $\delta l_A$ and $\delta l_B$ corresponding to the interferometer balancing efficiency. An important point is that previous experimental demonstrations of CV-QKD [21–23] with transmitted LO, that rely on such delay line interferometers, have proven that phase fluctuations (with frequency typically of order of Hz) associated to interferometer path length fluctuations can be kept low in frequency and amplitude when sampled at CV-QKD repetition rate and do not prevent performing CV-QKD with repetition rates in the MHz (or above) and we consider that $V_{\rm channel} = {\rm var}(\theta_{\rm channel}) \approx 0$. We can then consider that the variance $V_{\rm est}$ from Eq. (21) is dominated by the phase measurement efficiency:

$$V_{\rm est} = V_{\rm error}. \tag{26}$$

The LLO-delayline design ensures self-coherence at interference using delayline interferometers and the dependence on the relative phase drift of the lasers is removed. Bob gets self-coherent outcome measurements and is able to estimate the phase drift in the same way as in the LLO-sequential design but with higher efficiency. Finally, this results in the following excess noise:

$$\xi_{\rm phase} = 2V_A(1 - e^{-V_{\rm error}/2}). \tag{27}$$

### 3. *Performance analysis*

Based on the previous excess noise analysis, we can now study the performance of the LLO-delayline design in terms of secret key rate and compare its performance with the LLO-sequential design. As the quantum signal modulation is the same as in the LLO-sequential, we can equivalently compare the achievable secret key rate or the excess noise contributions.

The LLO-delayline design allows us to remove the relative phase drift $V_{\rm drift}$ from the excess noise expression. However, the relative phase drift between the two lasers should be stable within the duration of a single optical pulse and imposes that $V_{\rm drift} \lesssim 10$. The remaining phase noise is only limited by the efficiency $V_{\rm error}$ of the phase reference estimation. In particular, the LLO-delayline allows us to perform a stronger CV-QKD phase noise regime than the LLO-sequential design. Furthermore, as the amplitude modulator excess noise $\xi_{\rm AM}$ does not depend on the phase reference amplitude, the AM dynamics do no longer restrict the relative phase measurement efficiency $V_{\rm error}$. The reference amplitude $E_{\rm R}$ can then be chosen as large as possible in the limit of the saturation limit of Bob's detector and of the launched power limit without increasing the excess noise $\xi_{\rm AM}$. In practice, these limits allow an very efficient phase measurement.

In Fig. 6, we plot the expected key rates for both the LLO-sequential and LLO-delayline designs for different relative phase drift and AM dynamics. We can see that the LLO-delayline design is more resilient to both a decrease of the AM dynamics and an increase of the relative phase drift. The self-coherence between quantum signal and phase reference allows us to reach stronger phase noise regime than LLO-sequential with similar optical hardware. We can see on the left panel of Fig. 6 that with a 50-dB AM, the LLO-delayline design allows secret key generation at 50 km with $V_{\rm drift} = 0.1$ when LLO-sequential can only reach 30 km. Furthermore, in the LLO-delayline design, the amplitude of the reference pulses can be much larger than in the LLO-sequential design because it does not increase the excess noise $\xi_{\rm AM}$. Thus, the relative phase is estimated with better precision, reducing the induced excess noise. For instance, the LLO-delayline allows us to perform CV-QKD at a distance of 50 km with standard 30-dB amplitude modulators even in the regime of standard DFB lasers (linewidths of order of MHz), which is not possible with the LLO-sequential design. We have thus shown that the LLO-delayline allows us to perform LLO-based CV-QKD in the regime of standard optical hardware regimes, which is an improvement on LLO-based CV-QKD based on standard optical equipments. This work has recently been presented in Ref. [35].

## V. SELF-COHERENT DESIGNS BASED ON A MODULATION DISPLACEMENT

In this section, we propose a second design (proposed in Ref. [33]), the LLO-displacement design, implementing CV-QKD with a self-coherent phase reference sharing. This design is based on a method for jointly encoding both quantum signal and phase reference information over each optical pulse produced by Alice's laser $\rm L_A$ at emission.

### A. The protocol

The main idea is to displace, in the phase space, the modulation sent by Alice with a fixed displacement of amplitude $\Delta$ and phase $\phi_\Delta$. Given her standard GMCS variables $(x_A, p_A)$, Alice produces and sends to Bob the displaced coherent state:

$$|\alpha\rangle_{\vec{\Delta}} = |x_A + \Delta\cos\phi_\Delta, p_A + \Delta\sin\phi_\Delta\rangle. \tag{28}$$

The amplitude $\Delta$ and the phase $\phi_\Delta$ of the displacement are publicly known so that it carries information on Alice's phase reference. At reception, Bob measures both $\hat{x}$ and $\hat{p}$ quadratures of each received optical pulse using a heterodyne detection and gets measurement outcomes $(x_B, p_B)$:

$$\begin{aligned} x_B &= \sqrt{\frac{G}{2}}[(x_A + \Delta\cos\theta_\Delta)\cos\theta \\ &\quad + (p_A + \Delta\sin\theta_\Delta)\sin\theta + x_0 + x_c], \\ p_B &= \sqrt{\frac{G}{2}}[-(x_A + \Delta\cos\theta_\Delta)\sin\theta \\ &\quad + (p_A + \Delta\sin\theta_\Delta)\cos\theta + p_0 + p_c]. \end{aligned} \tag{29}$$

Using the displacement of Alice's modulation, Bob is able to measure an estimator $\hat{\theta}_S$ of the relative phase $\theta_S$ by using his measurement outcomes $(x_B, p_B)$. Furthermore, using the $i$ indexes for successive pulses, Bob can calculate a more precise estimator $\hat{\theta}_{\text{filter}}^{(i)}$ by averaging each estimator $\hat{\theta}_S^{(i)}$ with the previous filtered estimator $\hat{\theta}_{\text{filter}}^{(i-1)}$ using optimized weighted coefficients. Finally, the estimator $\hat{\theta}_{\text{filter}}^{(i)}$ allows Alice and Bob to correct their data using Eq. (4).

### B. Security of the protocol

In order to study the security of the design LLO-displacement and calculate the secret key rate, one can observe that security proofs for the GMCS protocols [36,37] do not rely on the mean value of Alice's quadrature because it is fully described using the covariance matrices formalism. However, as we will show, the excess noise induced by the phase noise on a displaced modulation is asymmetric. The secret key rates then has to be calculated using a specific method which is detailed in the Appendix.

We now quantify the remaining phase noise $V_{\text{est}}$ of Eq. (12). As both quantum signal and phase reference are encoded and transmitted within the same optical pulse, we can directly write $V_{\text{drift}} = 0$ and $V_{\text{channel}} = 0$. Finally, the only term contributing to the remaining phase noise $V_{\text{est}}$ is the variance $V_{\text{error}}$. Due to the the particular modulation scheme, however, the variance of the estimates $\hat{\theta}_S^{(i)}$ is not expressed as Eq. (14). In this case, Alice's modulation can be seen as a noise in the phase estimation process, resulting in

$$V_{\text{error}} = \frac{V_A + \chi + 1}{\Delta^2}. \tag{30}$$

Furthermore, the filtering technique—hence based on all previous relative phase estimates—allows us to use correlations of the phase drift over time to recover the relative phase with better precision than $V_{\text{error}}$. In the asymptotic regime (when $i$ is large), we can show that the successive variances $V_{\text{filter}}^{(i)}$ tend to an asymptotic limit and, finally, one can write

$$V_{\text{est}} = \sqrt{V_{\text{error}}}\sqrt{V_{\text{drift}}}, \tag{31}$$

where $V_{\text{drift}}$ is the relative phase drift between lasers $L_A$ and $L_B$ between two consecutive pulses; i.e., it is expressed as Eq. (18).

We can now express the excess noise $\xi_{\text{phase}}$ due to phase noise in the LLO-displacement regime (using the appendix). It can be simplified when $V_{\text{est}} \ll 1$ and reads as

$$\begin{aligned} \xi_{\text{phase}}^{(x)} &= (V_A + \Delta^2\sin^2\phi_\Delta)V_{\text{est}}, \\ \xi_{\text{phase}}^{(p)} &= (V_A + \Delta^2\cos^2\phi_\Delta)V_{\text{est}}, \end{aligned} \tag{32}$$

where the expression of $V_{\text{est}}$ is defined using Eq. (31). A crucial point in the noise analysis of the LLO-displacement design is that the displacement of Alice's modulation creates an asymmetry on the excess noise on each quadrature. For instance, if $\phi_\Delta = 0$ (displacement according to the $\hat{x}$ quadrature), the displacement induces an increasing of the excess noise on the $\hat{p}$ quadrature.

Furthermore, in this design, the maximal amplitude $E_{\max}$ of the AM excess noise [Eq. (17)] can be approximate as $\sqrt{V_A + \Delta^2}$, resulting in

$$\xi_{AM} = (V_A + \Delta^2)10^{-d_{\text{dB}}}. \tag{33}$$

However, one can note that the excess noise $\xi_{\text{phase}}$ is a more restricting limitation to the displacement amplitude than the excess noise $\xi_{AM}$ for realistic parameters and, in practice, the AM dynamics do not restrict the amplitude displacement.

### C. Performance analysis

In Ref. [33], we only considered the $\xi_{\text{phase}}^{(x)}$ contribution in the case of $\phi_\Delta = 0$, resulting in a too optimistic key rate. Although the displacement decreases the variance $V_{\text{error}}$ and, thus, the remaining phase noise $V_{\text{est}}$, it also increases its impact on the excess noise according to Eq. (32). Unfortunately, this result is a strong limitation to the achievable $\Delta$ and, thus, to the tolerable phase noise in the LLO-displacement design.

We here consider the case where $\phi_\Delta = 0$ (other cases can be treated in a similar way by observing that the sum $\xi_{\text{phase}}^{(x)} + \xi_{\text{phase}}^{(p)}$ does not depend on $\phi_\Delta$). From Eq. (32), one can note that the phase excess noise induced on the $\hat{p}$ quadrature is proportional to the displacement mean photon number $\Delta^2$. This sets a strong constraints on the achievable value of $\Delta$ and, thereby, on the achievable value of $V_{\text{error}}$. There is a trade-off in terms of the $\Delta$ value between the remaining phase noise $V_{\text{est}}$—the displacement $\Delta$ decreases $V_{\text{error}}$—and the excess noise $\xi_{\text{phase}}^{(p)}$. An optimal value for the displacement can be found and is calculated in our simulations. However, the optimal value of the $\Delta$ only allows secret key generation for low values of $V_{\text{drift}}$. This means that, solely based on the single estimates $\hat{\theta}_S$, the LLO-displacement design does not allow a low enough excess noise $\xi_{\text{phase}}$ and, as such, requires strong correlations, i.e., low values of $V_{\text{drift}}$, between consecutive relative phases to recover phase information based on filtering techniques.

In Fig. 7, we plot the expected key rates for both the LLO-sequential and the LLO-displacement designs. The displacement value is optimized to maximize the overall

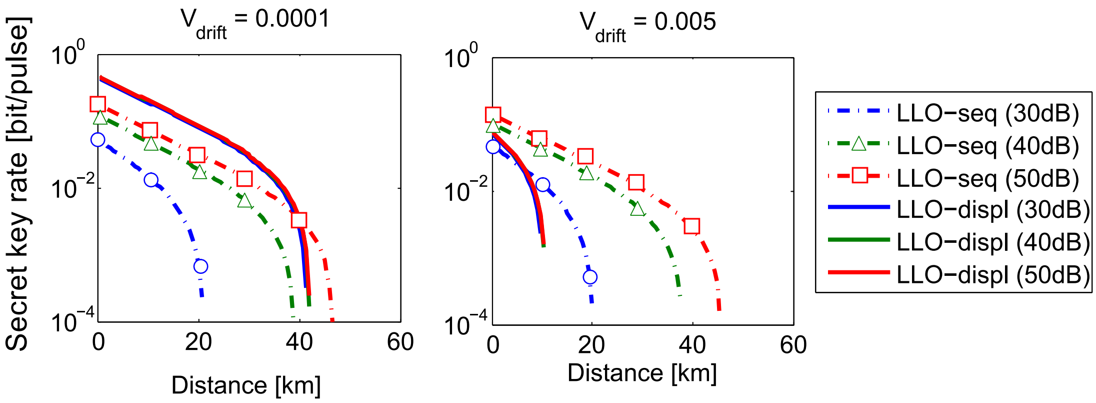

FIG. 7. Secret key rate comparison between the LLO-sequential and the LLO-displacement designs for two relative phase drift $V_{\text{drift}}$ and for different AM dynamics.

secret key rate. In low-phase-noise regimes, we can see that the LLO-displacement is better in terms of secret key rate generation. This is due to the fact that the LLO-displacement relies on the whole repetition rate to generate secret key and the filtering technique combined to the displacement allows a more efficient relative phase recovery. For higher phase noise regimes, however, the displacement value required to estimate the relative phase is limited by the excess noise $\xi_{\text{phase}}^{(p)}$ and, finally, the relative phase estimation cannot be performed with a good efficiency.

We have shown that the coherence coming from the simultaneous encoding of both the quantum signal and phase reference in this design comes with new challenges. In particular, the displacement of the modulation increases the excess noise induced by the relative phase noise and creates an asymmetry on the excess noise on each quadratures. An interesting issue is then to optimize the LLO-displacement design in order to increase its performance, especially in terms of phase noise resilience. This study is, however, kept for future works. We emphasize that LLO-displacement design relies on an extremely convenient experimental scheme as the phase reference encoding is performed simultaneously with the quantum signal modulation. The simultaneous quantum signal and phase reference transmission introduced in the LLO-displacement design can be applied to different signal modulations as BPSK or higher order modulations. Since both quantum signal and phase reference information are sent over the same optical pulse, the key rate obtained with the LLO-displacement design is moreover not lowered by time multiplexing, as it is the case with LLO-sequential. Thereby, unlike all other proposals for locally generated local oscillator based CV-QKD designs, it allows us to use the whole repetition rate for secret key generation.

## VI. CONCLUSION AND PERSPECTIVES

In order to lift security loophole issues, the local oscillator should not be directly sent through the optical channel in CV-QKD experiments and LLO-based CV-QKD protocols have been introduced. The main challenge of LLO CV-QKD is that the phase drift between emitter laser and local oscillator laser, placed at reception, induces a phase noise on the quantum communication that has to be efficiently corrected. In Table II, we summarize the performance and requirements of existing and proposed designs for CV-QKD. The approach considered so far, i.e., the LLO-sequential design [17–19], is intrinsically limited to low-phase-noise regimes. This puts important constraints on the type of lasers that can be used both as emitter and LO. Another limitation of the LLO-sequential is the efficiency of the relative phase estimation process, which is limited in practice by Alice's amplitude modulator dynamics. This can be seen as a limitation of the integrability of such design.

Our results imply that next-generation CV-QKD, implemented with a local LO, is possible even with low-cost DFB lasers and standard amplitude modulators. Such features are made possible by the newly introduced self-coherent phase reference sharing design, the LLO-delayline design, and are

TABLE II. Summary of all the CV-QKD designs discussed in this work. We compare them in terms of tolerable phase noise and on their experimental limitations.

| Design | Trusted LO | Tolerable phase noise | Hardware requirements |
|---|---|---|---|
| Transmitted LO [12,21–23] | No | $\Delta\nu/f \sim 10$ | Stable interferometric setup |
| LLO-sequential [17–19] | Yes | $V_{\text{drift}} \sim 10^{-2}$ | High AM dynamics |
| LLO-delayline (Sec. IV) | Yes | $V_{\text{drift}} \sim 10$ | Stable interferometric setup |
| LLO-displacement (Sec. V) | Yes | $V_{\text{drift}} \sim 10^{-4}$ | |

essential to progress towards photonic integration and wide deployment of CV-QKD. The LLO-delayline design relies on the self-coherence between the quantum signal and phase reference and on the interferometric stability of two delay lines at a short time scale. The finite dynamics of the amplitude modulator no longer restricts the reference pulse amplitude and, by consequence, the relative phase estimation process. These characteristics allow the LLO-delayline design to be more resilient to phase noise than the previously proposed LLO-sequential design. In Fig. 6, we can see that the LLO-delayline design is able to reach a distance of 50 km in a regime of high phase noise, $V_{\text{drift}} = 0.1$, while the reachable distance with the LLO-sequential design is below 25 km even with large AM dynamics. Furthermore, we emphasize that remote delay-line interferometric stability has already been demonstrated in practice on several CV-QKD implementations [21,22], paving the way to the demonstration of LLO CV-QKD with cheap hardware, using the LLO-delayline design.

As another contribution, we have investigated a scheme, LLO-displacement, allowing us to simultaneously transmit the quantum signal and the phase reference information on the same optical pulse. We have, however, observed that the implementation of the LLO-displacement design with Gaussian modulated coherente states (GMCS CV-QKD protocol) leads to an overall excess noise that increases with displacement, which restricts its use to low-phase-noise regimes. Simultaneous transmission of quantum and phase reference information had, however, not been studied so far and our results can be of interest in view of performing a joint optimization of classical and quantum coherent communication systems, operating with the same hardware. The optimization of such protocols is then an interesting open question and is kept for future works.

## ACKNOWLEDGMENTS

The authors thank Bing Qi for noticing an important limitation of the LLO-displacement design, in terms of additional excess noise, as well as for the fruitful exchanges and discussions on the LLO-displacement design.

## APPENDIX

### 1. The GMCS protocol

In the Gaussian-modulated coherent states protocol, Alice encodes classical Gaussian variables $(x_A, p_A)$ on the mean values of the two conjugate quadratures of coherent states $|\alpha\rangle = |x_A, p_A\rangle$. Coherent states are then sent to Bob through an insecure channel controlled by an eavesdropper Eve. At reception, Bob performs a coherent detection of either one quadrature (homodyne detection) or both quadratures (heterodyne detection) of the received pulse and calculates estimators $(x_B, p_B)$ of Alice's variables. As Eve's optimal attacks are Gaussian [36,37], we can model the logical channels between Alice and Bob's data as additive white Gaussian noise channels [34]:

$$x_B = \sqrt{\frac{G}{\delta_{\text{det}}}}(x_A + x_0 + x_c),$$
$$p_B = \sqrt{\frac{G}{\delta_{\text{det}}}}(p_A + p_0 + p_c), \tag{A1}$$

where $(x_c, p_c)$ is the total noise of the channel and we note $(\chi_x, \chi_p)$ its variance. In Eq. (A1), $G$ is the total intensity transmission of the channel, $\delta_{\text{det}}$ stands for the detection used at reception ($\delta_{\text{det}} = 1$ for a homodyne detection and $\delta_{\text{det}} = 2$ for a heterodyne detection), and $x_0$ and $p_0$ are Gaussian variables of variance $N_0$ modeling the shot noise quadratures. In general [36], it is assumed that the channel noise is symmetric and $\chi = \chi_x = \chi_p$, where the variance $\chi$ is referred to Alice's input. The variance $\chi$ of the total noise can be expressed as [34,37]

$$\chi = \frac{\delta_{\text{det}} - G}{G} + \xi, \tag{A2}$$

where the first term is the loss-induced vacuum noise and $\xi$ is the overall excess noise variance of the channel referred to Alice's input. Thereby, using Eqs. (A1) and (A2), we can see that the Gaussian channel between Alice and Bob is fully characterized by the two parameters $G$ and $\xi$. In a real-world experiment, Alice and Bob can estimate $G$ and $\xi$ from the correlations between their respective variables by revealing a fraction of their data and are then able to characterize the propagation channel and generate secret key. We discuss and model the different contributions to the excess noise $\xi$ in practical CV-QKD in the next paragraph. Finally, the secret key rate available to Alice and Bob in the reverse reconciliation scheme can be expressed as [34,37]

$$k = \beta I_{AB} - Q_{BE}, \tag{A3}$$

where $0 \leqslant \beta \leqslant 1$ is the reconciliation efficiency, $I_{AB}$ is the mutual information between Alice and Bob's classical variables, and $Q_{BE}$ stands for Eve's maximal accessible information on Bob's measurements, capturing assumptions on Eve's behavior [37]. In this work, we restrict the security analysis to individual attacks [34,37] and $Q_{BE}$ is then the classical information $I_{BE}$ between Bob's measurements and Eve's data. In Refs. [17,22], it is assumed that Eve does not have access to Bob's electronics. In this work, however, we use the stronger security model of Ref. [18], assuming that Eve is able to control the noise of Bob's detector.

### 2. Excess noise due to phase noise

Alice sends the coherent state $|\alpha\rangle = |x_A + x_0, p_A + p_0\rangle$, where, in the general case, we suppose that $x_A \sim \mathcal{N}(0, V_x)$ and $p_A \sim \mathcal{N}(0, V_p)$, while Bob uses a heterodyne detection at reception. In order to estimate the phase-noise-induced excess noise, we consider in this analysis that the relative phase noise is the only noise source. Bob then gets the following measurement outcomes $(x_m, p_m)$:

$$\begin{pmatrix} x_m \\ p_m \end{pmatrix} = \sqrt{\frac{G}{2}}\left[\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} x_A + x_0 \\ p_A + p_0 \end{pmatrix}\right]. \tag{A4}$$

We suppose that Bob gets an estimator $\hat{\theta} \sim \mathcal{N}(\theta, V_\varphi)$. He sends his estimator to Alice, which corrects her data and, in the reverse reconciliation scheme, Alice then estimates Bob's measurements as

$$\begin{pmatrix} \tilde{x_A} \\ \tilde{p_A} \end{pmatrix} = \sqrt{\frac{G}{2}}\begin{pmatrix} \cos\hat{\theta} & \sin\hat{\theta} \\ -\sin\hat{\theta} & \cos\hat{\theta} \end{pmatrix}\begin{pmatrix} x_A + x_0 \\ p_A + p_0 \end{pmatrix}. \tag{A5}$$

We can then express the excess noise on each quadrature as

$$\begin{aligned}\xi_x &= \mathrm{var}(x_m - \tilde{x}_A),\\ \xi_p &= \mathrm{var}(p_m - \tilde{p}_A).\end{aligned} \tag{A6}$$

These two quantities depends on the remaining relative phase $\varphi = \theta - \hat{\theta}$. Assuming that the variable $\varphi$ is a Gaussian variable such that $\varphi \sim \mathcal{N}(0, V_\varphi)$, the above expressions can be calculated from the characteristic function of the Gaussian function and, after calculations, we obtain the following expressions:

$$\begin{aligned}\xi^{(x)}_{\text{phase}} &= V_x(1 + e^{-V_\varphi} - 2e^{-V_\varphi/2}) + \left(V_x + x_0^2\right)\\ &\quad\times\left(\tfrac{1}{2} + \tfrac{1}{2}e^{-2V_\varphi} - e^{-V_\varphi}\right) + \left(V_p + p_0^2\right)\left(\tfrac{1}{2} - \tfrac{1}{2}e^{-2V_\varphi}\right),\\ \xi^{(p)}_{\text{phase}} &= V_p(1 + e^{-V_\varphi} - 2e^{-V_\varphi/2}) + \left(V_p + p_0^2\right)\\ &\quad\times\left(\tfrac{1}{2} + \tfrac{1}{2}e^{-2V_\varphi} - e^{-V_\varphi}\right) + \left(V_x + x_0^2\right)\left(\tfrac{1}{2} - \tfrac{1}{2}e^{-2V_\varphi}\right).\end{aligned} \tag{A7}$$

### 3. Imperfections of the detector

#### *a. Electronic noise*

Electronic noise of Bob's detector induces a noise of variance $v_{\text{elec}}$ on Bob's quadrature raw measurements. In general, the electronic noise variance $v_{\text{elec}}$ depends on the detection circuit as well as on the repetition rate of the experiment. As the shot noise value scales with the LO intensity while $v_{\text{elec}}$ is constant with the LO intensity, it is, however, possible to reduce the effective electronic to shot noise ratio $\xi_{\text{elec}}$ by increasing the LO intensity. In this work, we consider that $\xi_{\text{elec}}$ referred to Alice in SNU is modeled as

$$\xi_{\text{elec}} = \frac{\delta_{\text{det}}}{G}\frac{E^2_{\text{LO,cal}}v_{\text{elec}}}{E^2_{\text{LO}}}, \tag{A8}$$

where $E^2_{\text{LO,cal}}$ is the photon number in the LO at which $\xi_{\text{elec}} = (\delta_{\text{det}}/G)v_{\text{elec}}$ and $E^2_{\text{LO}}$ is the actual photon number per LO pulse at reception. The variable $\delta_{\text{det}}$ stands for the detection method as $\delta_{\text{det}} = 1$ for a homodyne receiver and $\delta_{\text{det}} = 2$ for a heterodyne receiver. In general, the variance $v_{\text{elec}}$ increases with the repetition rate, for a given detection circuit. For instance, in Ref. [21], the same detector has an electronic to shot noise ratio of −6 dB at 50 MHz, −4 dB at 200 MHz, and −1 dB at 1 GHz. In the following, we consider an electronic to shot noise ratio, which is independent of the repetition rate. We have consider the typical values $v_{\text{elec}} = 0.01$ for $E^2_{\text{LO,cal}} = 10^8$.

#### *b. Linearity range of the detector*

We consider that Bob relies on a single coherent detector, which addresses the issue of the linearity range of the detector when considering both quantum signal and phase reference transmission. A typical homodyne detector is presented in Fig. 8. The response of the integrator circuit is proportional to the incoming number of electrons over a finite range. Beyond a certain threshold, the response of the integrator circuit is no longer linear and the security can be broken by specific attacks [32]. We define this threshold as the maximal number of electrons $N_{\text{sat}}$ per electrical pulses that can be detected in a linear regime. The number of electrons in each electrical pulse is $N_e = 0.5GE_{\text{S}}E_{\text{LO}}$ (see Fig. 8), where $E_{\text{S}}$ and $E_{\text{LO}}$ are the amplitudes of the signal and the LO so that the saturation hypothesis imposes:

$$\frac{G}{2}E_{\text{S}}E_{\text{LO}} \leqslant N_{\text{sat}}. \tag{A9}$$

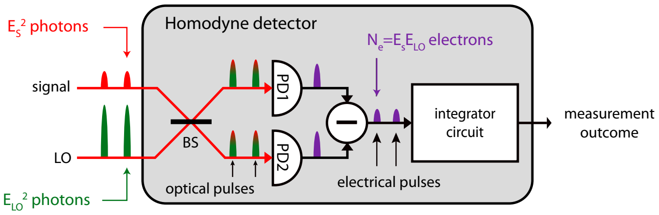

FIG. 8. Scheme of a typical homodyne detector. Signal and local oscillator pulses interfere on a 50:50 beamsplitter (BS). Both resulting fields are detected on two photodiodes (PD1 and PD2), which convert photons into electrons. The electrical pulses (purple pulses) produced by the photodiodes are then substracted (−) and the resulting quadrature electrical pulse intensity is measured using a integrator circuit. The outcome of the integrator circuit is proportional to $N_e = E_{\text{S}}E_{\text{LO}}$ up to an intensity threshold $N_{\text{sat}}$.

A example of saturation threshold $N_{\text{sat}} = 10^6$ has been experimentally evaluated in Ref. [32]. For quantum signal of intensity of order of the shot noise, this threshold is not important and has not been considered so far in CV-QKD analysis. In LLO-based CV-QKD, however, the relatively large amplitude of phase reference pulses imposes to consider the saturation threshold as a limit on the reference pulse amplitude.

Equation (A9) implies a trade-off, in the LLO-sequential design, between the signal amplitude—in particular the reference amplitude $E_{\text{R}}$—and the local oscillator amplitude—used to decrease the electronic to shot noise ratio. If we want to maximize these two quantities, one has to saturate Eq. (A9) by choosing

$$E_{\text{LO}} = \frac{2}{G}\frac{N_{\text{sat}}}{E_{\text{R}}}, \tag{A10}$$

The effective electronic to shot noise ratio $\xi_{\text{elec}}$ defined in Eq. (A8) can then be expressed in the case of a heterodyne detection ($\delta_{\text{det}} = 2$) as

$$\xi_{\text{elec}} = \frac{G10^6}{2}\frac{E^2_{\text{R}}}{N^2_{\text{sat}}} \tag{A11}$$

where $v_{\text{elec}} = 0.01$ and $E^2_{\text{LO,cal}} = 10^8$. In Fig. 9, we plot the expected key rate of the LLO-sequential design for different values of the threshold $N_{\text{sat}}$. As we can see, only low values of $N_{\text{sat}}$ (two order of magnitude lower than the experimental value of Ref. [32]) are limitations to this design. As a typical value of $N_{\text{sat}} = 10^6$ photons is sufficiently large to allow a precise relative phase sharing, the saturation threshold will not be a limitation to the reference amplitude.

### 4. Secret key rate formulas for CV-QKD

In this work, we focus on the Gaussian-modulated coherent state (GMCS) protocol. In this protocol, Alice encodes zero-mean Gaussian classical variables $x_A$ and $p_A$ on both the $\hat{x}$ and $\hat{p}$ quadratures of coherent states [6] before sending

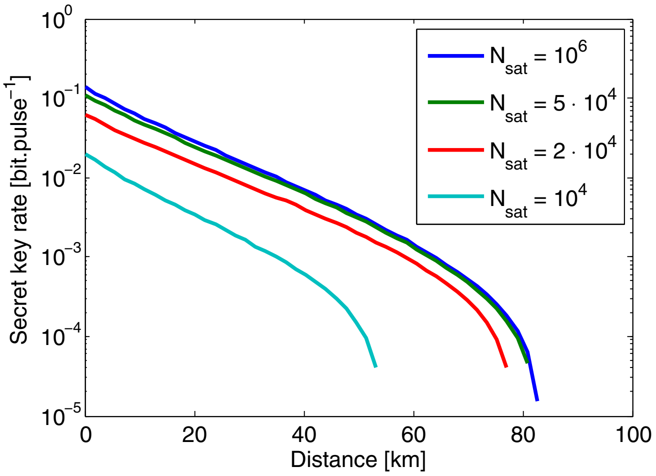

FIG. 9. Expected secret key rates for the LLO-sequential design for different value of linearity threshold $N_{\text{sat}}$.

them to Bob through an insecure optical channel controlled by an eavesdropper Eve. In the Gaussian model, the channel between Alice and Bob is fully characterized by the intensity transmission $G$ and the excess noise $\xi_x$ and $\xi_p$ (*a priori* different on each quadratures. We also assume that Bob uses a heterodyne detection at reception.

### *a. Symmetric channel*

We first detail the secret key rate formulas used for symmetric excess noise $\xi = \xi_x = \xi_p$. This formulas are used for the LLO-sequential and the LLO-delayline designs. We consider that Eve controls the whole excess noise and we also consider individual attacks. The secret key rates is written as [34]

$$k = \beta I_{AB} - I_{BE}, \tag{A12}$$

where

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{V+\chi}{1+\chi}\right), \tag{A13}$$

$$I_{BE} = \frac{1}{2}\log_2\left(\frac{G(V+\chi)(V+\chi_E)}{(\chi_E+1)(V+1)}\right), \tag{A14}$$

with

$$V = V_A + 1, \tag{A15}$$

$$\chi = \frac{2-G}{G} + \xi, \tag{A16}$$

$$\chi_E = \frac{G(2-\xi)^2}{(\sqrt{2-2G+G\xi}+\sqrt{\xi})^2} + 1. \tag{A17}$$

### *b. Asymmetric channel*

We have shown in Sec. V that the excess noise induced by the phase noise in the case of the displaced modulation is asymmetric in the two quadratures. We then need to derive specific secret key rate expressions. From Refs. [34,37], we can write

$$k = k_x + k_p, \tag{A18}$$

where $k_x$ and $k_p$ represent the respective key rates on the logical channel corresponding to each quadrature. Each of these two key rates can then be obtained using the secret key formulas from Eq. (A12), using the corresponding expression $\xi_x$ and $\xi_p$ from Eq. (32).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).

[3] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Information **2**, 16025 (2016).

[4] www.sequrenet.com

[5] www.idquantique.com

[6] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[7] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security, and implementations, Entropy **17**, 6072 (2015).

[8] M. Ziebell, M. Persechino, N. Harris, C. Galland, D. Marris-Morini, L. Vivien, E. Diamanti, and P. Grangier, Towards on-chip continuous-variable quantum key distribution, in *Conference on Lasers and Electo-optics/European Quantum Electronics Conference (CLEO/Europe-EQEC)*, 2015.

[9] A. Orieux and E. Diamanti, Recent advances on integrated quantum communications, J. Opt. **18**, 083002 (2016).

[10] R. Kumar, H. Qin, and R. Alléaum, Coexistence of continuous variable QKD with intense dwdm classical channels, New J. Phys. **17**, 043027 (2015).

[11] 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).

[12] D. Huang, J. Fang, D. Wang, P. Huang, and G. Zeng, A wideband balanced homodyne detector for high speed continuous-variable quantum key distribution systems, QCrypt, 2013.

[13] D. Lin D. Huang, P. Huang, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[14] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Long-distance continuous-variable quantum key distribution with a Gaussian modulation, Phys. Rev. A **84**, 062317 (2011).

[15] K. Kikuchi, Fundamentals of coherent optical fiber communications, J. Lightwave Technol. **34**, 1 (2016).

[16] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Reference frames, superselection rules, and quantum information, Rev. Mod. Phys. **79**, 555 (2007).

[17] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the Local Oscillator Locally in Continuous-Variable Quantum Key Distribution Based on Coherent Detection, Phys. Rev. X **5**, 041009 (2015).

[18] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-Referenced Continuous-Variable Quantum Key Distribution Protocol, Phys. Rev. X **5**, 041010 (2015).

[19] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, Opt. Lett. **40**, 3695 (2015).

[20] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[21] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Continuous-variable quantum key distribution with 1 mbps secure key rate, Opt. Express **23**, 17511 (2015).

[22] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, Nat. Photon. **7**, 378 (2013).

[23] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, Phys. Rev. A **76**, 052323 (2007).

[24] A. Ferenczi, P. Grangier, and F. Grosshans, Calibration attack and defense in continuous variable quantum key distribution, in *Lasers and Electro-Optics, 2007 and the International Quantum Electronics Conference: CLEOE-IQEC 2007* (IEEE, 2007).

[25] X. C. Ma, S. H. Sun, M. S. Jiang, M. Gui, Y. L. Zhou, and L. M. Liang, Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator, Phys. Rev. A **89**, 032310 (2014).

[26] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, Phys. Rev. A **87**, 062313 (2013).

[27] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, Phys. Rev. A **87**, 062329 (2013).

[28] B. Qi, Simultaneous quantum and classical communication using continuous variable, Phys. Rev. A **94**, 042340 (2016).

[29] H. Schulze, Stochastic model for phase noise (2005), http://www.fh-meschede.de/public/schulze/docs/OFDM2005_schulze_rev1.pdf.

[30] A. Yariv and P. Yeh, Photonics: Optical Electronics in Modern Communications The Oxford Series in Electrical and Computer Engineering (Oxford University Press, Inc., New York, NY, 2006).

[31] S. Bittner, S. Krone, and G. Fettweis, Tutorial on discrete time phase noise modeling for phase locked loops (2010), https://www.researchgate.net/publication/228572264_Tutorial_on_discrete_time_phase_noise_modeling_for_phase_locked_loops.

[32] H. Qin, R. Kumar, and R. Alléaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, Phys. Rev. A **94**, 012325 (2016).

[33] A. Marie and R. Alléaume, Self-coherent phase reference sharing for continuous-variable quantum key distribution, arXiv:1605.03642.

[34] S. Fossier, Mise en oeuvre et évaluation de dispositifs de cryptographie quantique à longueur d'onde télécom, Ph.D. thesis, Thales Research & Technology France, 2009 (unpublished).

[35] L. T. Vidarte, A. Marie, A. Alléaume, and E. Diamanti, Proof-of-principle study of self-coherent continuous-variable quantum key distribution, QCrypt, 2016.

[36] A. Leverrier, Theoretical study of continuous-variable quantum key distribution, Ph.D. thesis, Télécom ParisTech, Paris, 2010 (unpublished).

[37] R. Garcia-Patron, Quantum information with optical continuous variables: From bell tests to key distribution, Ph.D. thesis, Université Libre de Bruxelles, Bruxelles, 2008 (unpublished).