Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection

Roberto Corvaja*

Department of Information Engineering, University of Padova, Via G. Gradenigo 6/B, 35131, Padova, Italy

(Received 16 May 2016; revised manuscript received 1 December 2016; published 9 February 2017)

In continuous-variables quantum key distribution with coherent states, the advantage of performing the detection by using standard telecoms components is counterbalanced by the lack of a stable phase reference in homodyne detection due to the complexity of optical phase-locking circuits and to the unavoidable phase noise of lasers, which introduces a degradation on the achievable secure key rate. Pilot-assisted phase-noise estimation and postdetection compensation techniques are used to implement a protocol with coherent states where a local laser is employed and it is not locked to the received signal, but a postdetection phase correction is applied. Here the reduction of the secure key rate determined by the laser phase noise, for both individual and collective attacks, is analytically evaluated and a scheme of pilot-assisted phase estimation proposed, outlining the tradeoff in the system design between phase noise and spectral efficiency. The optimal modulation variance as a function of the phase-noise amount is derived.

DOI: 10.1103/PhysRevA.95.022315

I. INTRODUCTION

In quantum key distribution (QKD) a current trend towards the deployment of continuous variables (CV) is driven mainly by the advantage of using standard components for optical fiber communications [1]. Moreover higher rates are expected by the use of CV [2] and the efficiency of the measurement is higher than in single-photon schemes. CV protocols have been developed for nonclassical states-of-light-like squeezed states [3], but also coherent states can be employed [4,5], which are produced more easily and, unlike squeezed states, propagate through the fiber channel without loosing their main characteristics. Reverse reconciliation is more suited to CV-QKD [4–6] and a proof of the composable security for CV-QKD with coherent states is given in [7].

However, a major problem, common to all the coherent detection schemes where the incoming signal phase carries some data information, is the phase-locking between the local laser carrier and the transmit laser. In almost all the studies and experimental works, the same laser used at the transmitter is employed also at the demodulation side [4,5,8]: an unmodulated signal is sent through a parallel channel, for example, on a different polarization or by time-division multiplexing. This is a great limitation since it requires a high power signal at the transmitter to get a sufficiently strong signal at the receiver, for the combination and the subsequent homodyne detection. Another side effect is the reduction of the useful capacity to transmit also the reference carrier, namely the spectral efficiency is reduced by the transmission of the reference signal.

Recent *self-referenced* experiments [2,9,10] show the feasibility of a scheme where the local oscillator is actually generated "locally" at the receiver by an independent laser and it is not *phase-locked* by complex optical phase-locked loops. Instead, a postdetection phase correction is applied to the photodiodes outputs. This is implemented by transmitting pilot-symbols interlaced in time-division with the useful data symbols. The pilots are used to retrieve a common phase reference.

Here the scheme of [9,10] is modified to reduce the number of pilot symbols, thus increasing the spectral efficiency, and the effect of phase noise is considered on the secure rate of CV-QKD with homodyne detection employing hybrid balanced detectors [11] and postdetection phase correction. The secure rate is considered for both individual and collective attacks based on the secure rate analysis of [7,9]. With respect to [9,10], here the analytical expression of the phase-noise degradation is provided and it is related to a practical system parameter such as the laser bandwidth. Moreover the design of a more spectral efficient pilot-data structure is proposed and practical system design criteria provided.

II. SYSTEM MODEL

A CV-QKD system is considered, where Alice modulates the amplitude and phase of a laser, producing a coherent state $|x_A + jy_A\rangle$ every symbol period T, where the in-phase x_A and quadrature y_A components are Gaussian random variables with zero mean and variance V_A (expressed in shot-noise units). The quantum state is applied to a fiber and Bob at the receiving side performs homodyne detection obtaining the components x_B and y_B.

The channel introduces additive noise and is characterized in terms of the relations

$$x_{\text{out}} = \sqrt{G}(x_{\text{in}} + e_x), \tag{1}$$

$$y_{\text{out}} = \sqrt{G}(y_{\text{in}} + e_y), \tag{2}$$

where G is the channel gain ($G < 1$) and e_x, e_y represent the line noises with variance χ_l, related to the losses and to the excess noise ϵ.

Then a reverse reconciliation protocol is implemented: Bob randomly chooses either component in-phase x or quadrature y and sends back to Alice through an authenticated channel a part of the bits corresponding to the quantization of x or y. This step is followed by classical data processing for the privacy amplification [1] to share a secure key between Alice and Bob.

*corvaja@dei.unipd.it

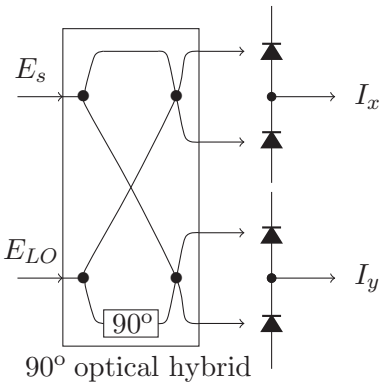

FIG. 1. Homodyne receiver with 90° optical hybrid and balanced detectors: The dots in the optical hybrid denote beam-splitters.

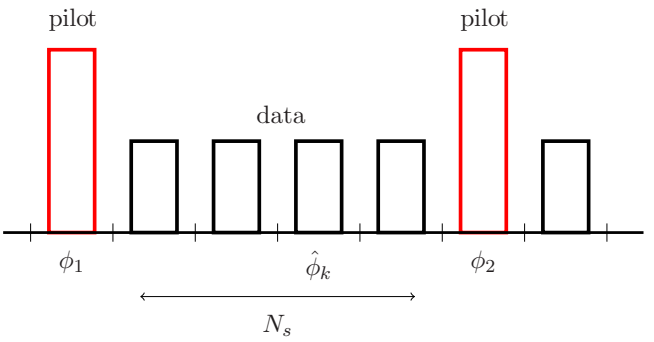

FIG. 2. Pilot-assisted phase estimation and compensation: The high-power received signal during pilot slots is used to estimate ϕ_1 and ϕ_2, which are used for the phase compensation by $\hat{\phi}_k$ during the kth symbol.

III. HOMODYNE DETECTION

The homodyne receiver is depicted in Fig. 1: It is composed by a passive 90° optical hybrid, which combines the local laser signal with the received optical signal, both in phase or after a phase shift of 90°, by using beam-splitters, which are denoted by dots in the optical hybrid scheme of Fig. 1. The outputs are then sent to a balanced photodetector, as in classical coherent homodyne receivers [11].

The optical 90° hybrid combines the local oscillator

$$E_{LO} = \sqrt{P_{LO}}\,\cos\left(\omega_{LO}t + \theta_{LO}(t)\right), \tag{3}$$

and the modulated signal corresponding to the coherent state prepared by Alice received from the channel $|x_{\text{out}} + jy_{\text{out}}\rangle = |\sqrt{P_s}e^{j\phi_s}\rangle$

$$E_s = \sqrt{P_s}\,\cos\left(\omega_s t + \phi_s + \theta_s(t)\right). \tag{4}$$

In (3) and (4) the terms $\theta_s(t)$ and $\theta_{LO}(t)$ represent the laser phase noises at the transmitter and receiver, respectively. The four hybrid outputs are sent to two balanced photodetectors, giving the photocurrents

$$I_x = R\sqrt{P_{LO}P_s}\eta\,\cos(\phi_s + \theta_s(t) - \theta_{LO}(t)), \tag{5}$$

$$I_y = R\sqrt{P_{LO}P_s}\eta\,\sin(\phi_s + \theta_s(t) - \theta_{LO}(t)), \tag{6}$$

where R is the equivalent resistance. In typical applications the power of the local oscillator is much larger than the received signal $P_{LO} \gg P_s$, so that the shot-noise is dominated by the local oscillator.

We note that with respect to the state prepared by Alice, Bob observes a coherent state $|x_B + jy_B\rangle$ which is degraded by the channel noise and by the phase noise which introduces the rotation $e^{j\phi}$ with $\phi = \theta_s(T) - \theta_{LO}(T)$.

A postdetection phase correction scheme can be applied by rotating the detected value by the angle $(-\phi)$, using a pilot assisted channel equalization, as common in radio communications [12] and proposed recently in [10] also for optical fiber CV-QKD. The protocol for phase estimation and correction proposed in [10] is that Alice transmits the nonmodulated carrier with power P_s, which is considered the pilot symbol, for each data symbol. This is used to estimate the phase difference ϕ between the local laser and the incoming signal. The solution proposed in this work is modified with respect to [10], in that a pilot symbol is transmitted for several payload symbols N_s, as shown in Fig. 2, thus increasing the spectral efficiency (the ratio between the useful symbols and the total transmitted symbols) from 1/2 to $N_s/(N_s+1)$ and correspondingly the energy efficiency from $P_s/(P_s+P_p)$ to $N_sP_s/(N_sP_s+P_p)$. This scheme has the advantage of enabling homodyne detection without transmitting the reference carrier together with the information coherent states, while a really "local" laser is employed, with the sufficient power required to perform the demodulation, not affected by the fiber losses. Moreover, the postdetection phase correction removes the need of locking between the local laser and the incoming signal by complex devices, such as optical phase locked loops. The main advantage with respect to [10] is the fact that a phase reference pilot is shared among several payload symbols, thus increasing the spectral efficiency.

Two successive pilot symbols can be employed to enhance the accuracy of the phase reference estimation: the values ϕ_1 and ϕ_2 are obtained by by $\phi_i = \arctan(y_i/x_i)$, $i = 1,2$. Then a linear combination of the estimates is applied in the correction, to compensate the phase error during the kth symbol by $\hat{\phi}_k$. Considering that, due to the Wiener model for the phase noise, the variance of the phase noise increases with time, the best linear combination of the estimations ϕ_1 and ϕ_2, in terms of minimum estimation variance, is given by

$$\hat{\phi}_k = \frac{N_s+1-k}{N_s+1}\phi_1 + \frac{k}{N_s+1}\phi_2 \quad k = 1,\ldots,N_s. \tag{7}$$

After the phase compensation, the residual phase error on the equalized values corresponds to the phase-noise evolution of both the local laser and the signal laser between the estimation points and the compensation point. Thus, the kth variable used by Bob for the QKD protocol is still rotated by the residual phase-noise error

$$\Theta_k = \hat{\phi}_k - \theta_{LO}(kT) + \theta_s(kT). \tag{8}$$

This reflects on the in-phase and quadrature components measured by Bob as a multiplicative factor, namely $\cos\Theta_k$ on the kth in-phase value x_B and $\sin\Theta_k$ on the quadrature y_B.

Effect of phase noise on the variance of detected variables

The phase noise of lasers is suitably modeled by a Wiener process so that the corresponding power spectral density of the baseband equivalent of the noisy carrier is described by a Lorentzian line

$$\mathcal{P}_\theta(f) = \frac{1}{\pi B}\frac{1}{1+\left(\frac{f}{B}\right)^2}, \tag{9}$$

with 3-dB carrier bandwidth B. The amount of phase noise of lasers is usually expressed by the bandwidth B, normalized to the symbol period $B_T = B\,T$. The characteristic of the Wiener process is to have independent increments over disjoint time intervals, so that the variance of the phase noise over the symbol period T is given by

$$\sigma_\theta^2 = 2\pi B_T. \tag{10}$$

In the following the normalized bandwidth B_T is the parameter used to quantify the amount of phase noise. The effect on the detected sample is represented by the multiplicative factor $\cos^2\Theta_k$ (or $\sin^2\Theta_k$) at the output. We have

$$E[\cos^2(\Theta_k)] = \tfrac{1}{2} + \tfrac{1}{2}e^{-2\sigma^2_{\Theta_k}}, \tag{11}$$

where $E[\cdot]$ denotes the expectation and $\sigma^2_{\Theta_k}$ is the variance of the residual phase noise Θ_k. Note that (11) can derived from the characteristic function of a Gaussian random variable. Then, according to (7) and (10), for independent phase noises $\theta_{LO}(t)$ and $\theta_s(t)$, the variance of Θ_k is

$$\sigma^2_{\Theta_k} = E\left[\Theta_k^2\right] = 4\pi B_T\left[k\left(\frac{N_s+1-k}{N_s+1}\right)^2 + \left(\frac{k}{N_s+1}\right)^2(N_s-k+1)\right]. \tag{12}$$

Note that the reference values ϕ_1 and ϕ_2 estimated on the pilots are affected in principle by en error. However, as shown in [10], the estimation error limited by the shot-noise becomes negligible as soon as the number of photons associated to the pilot symbols is greater than 100.

IV. SECURE KEY RATE

Reverse reconciliation [6] is considered, where Bob reveals a fraction of the bits to Alice. Eve needs to guess the measurements of Bob without introducing too much noise or degradation. Several attacks could be considered and in general it is assumed the entangling-cloner model for Eve, in which the best estimates of Eve are only limited by Heisenberg relations [4]. A proof of the composable security against collective attacks for CV-QKD with coherent states has been proposed in [7].

A. Security against individual attacks

According to the proofs of [4,13] the *raw secret key rate* is given by

$$R_0 = I_{AB} - I_{BE}. \tag{13}$$

Taking into account the efficiency of the reconciliation protocol and of the pilot symbols, the practical *net secret key rate* is given by

$$R = \frac{N_s}{N_s+1}[\beta I_{AB} - I_{BE}], \tag{14}$$

where β represents the efficiency of the reconciliation protocol, with typical values that can reach 87% [5], by the use of LPDC codes.

As outlined in [5], Alice-Bob mutual information is given by

$$I_{AB} = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_t}\right), \tag{15}$$

where χ_t is the total noise variance referred to the input

$$\chi_t = \chi_l + \frac{\chi_d}{G}, \tag{16}$$

which includes the "line" noise χ_l, including the excess noise ϵ

$$\chi_l = \frac{1-G}{G} + \epsilon, \tag{17}$$

and the detection noise variance χ_d, which is due to: photodetector efficiency η, electronic noise variance $\nu_{\rm el}$, and the phase noise contribution χ_θ,

$$\chi_d = \frac{1-\eta}{\eta} + \frac{\nu_{\rm el} + V_A\chi_\theta}{\eta}. \tag{18}$$

From the analysis in the previous section, the phase-noise contribution (referred to the input) is

$$\chi_\theta = \tfrac{1}{2}\left(1-e^{-2\sigma^2_\Theta}\right). \tag{19}$$

On the other hand, Eve's information I_{BE} is [5]

$$I_{BE} = \frac{1}{2}\log_2\left[G^2\frac{(1+\chi_t+V_A)\left(\chi_l+\frac{1}{1+V_A}\right)}{1+G\chi_d\left(\chi_l+\frac{1}{1+V_A}\right)}\right]. \tag{20}$$

B. Security against collective attacks

In the case of *collective attacks* an analysis of the conditions for the composable security and an upper bound on the the secure rate have been derived in [7]. In [9] the secure rate is evaluated and the main results are reported also in [10].

In particular we have that the mutual information between Alice and Bob is lower bounded by [9]

$$I_{AB} \geqslant \log_2\left(\frac{V_A+1+\chi_t}{1+\chi_t}\right) \tag{21}$$

with

$$\chi_t = \chi_l + + V_A\chi_\theta \tag{22}$$

where the variance of the "line" noise is

$$\chi_l = \frac{1-G\eta}{G\eta} + \epsilon + \frac{\nu_{\rm el}}{G\eta}, \tag{23}$$

where χ_θ is given by (19).

On the other hand, Eve's information I_{BE} in this case is the Holevo accessible information and is obtained by the symplectic eigenvalues of the covariance matrices. As

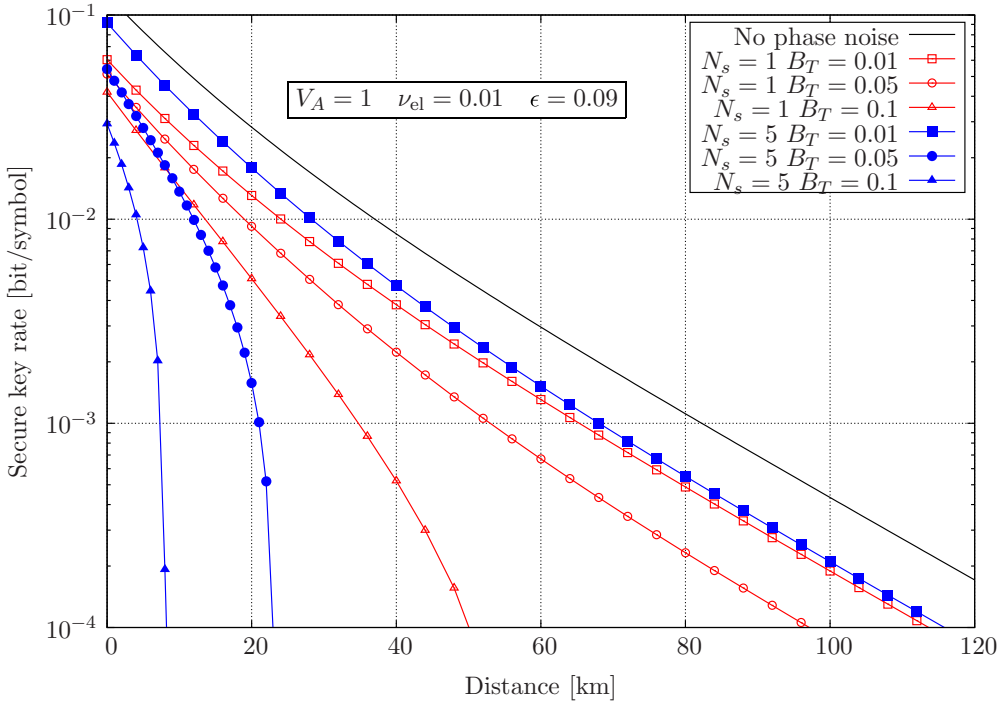

FIG. 3. Secure key rate R against individual attacks as a function of the distance for three values of B_T and symbols $N_s = 1$ or $N_s = 5$ ($V_A = 1$).

presented in [9,10], it is given by

$$I_{BE} = \sum_{i=1}^{2}\left[\frac{\lambda_i+1}{2}\log_2\left(\frac{\lambda_i+1}{2}\right) - \frac{\lambda_i-1}{2}\log_2\left(\frac{\lambda_i-1}{2}\right)\right] - \frac{\lambda_3+1}{2}\log_2\left(\frac{\lambda_3+1}{2}\right) + \frac{\lambda_3-1}{2}\log_2\left(\frac{\lambda_3-1}{2}\right). \tag{24}$$

The terms λ_i are given by [9]

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}, \tag{25}$$

$$\lambda_3 = \sqrt{(V_A+1)\frac{(V_A+1)\chi_l + 1 + ((V_A+1)^2-1)\chi_\theta}{V_A - 1 + \chi_l}} \tag{26}$$

with

$$A = (V_A+1)^2(1-2G\eta) + (G\eta)^2(V_A+1+\chi_l)^2 + 2G\eta[(V_A+1)^2 - 1]\chi_\theta), \tag{27}$$

$$B = G\eta[(V_A+1)\chi_l + 1 + ((V_A+1)^2-1)\chi_\theta]. \tag{28}$$

V. NUMERICAL RESULTS

A. With individual attacks

The effects of phase noise are first considered in terms of net secure rate as a function of the distance, for a fiber with specific attenuation 0.2 dB/km and system parameters in a typical range of a realistic scenario, used also in [4,8,10], namely, the efficiency of the reconciliation procedure $\beta = 0.8$, photodetector efficiency $\eta = 0.5$, electronic noise $\nu_{\rm el} = 0.01$, and excess noise $\epsilon = 0.09$. The estimation error on ϕ_1 and ϕ_2 is neglected. The secure rate is shown in Fig. 3 for different values of the phase-noise bandwidth B_T and two values of the symbol length, namely $N_s = 1$ and $N_s = 5$. The modulation variance is $V_A = 1$. We can see that the reduction of the secure rate is limited for values of the phase-noise-normalized bandwidth up to $B_T = 0.05$. Note that for a sufficiently high symbol rate $1/T$, commercial lasers can achieve a bandwidth with $B_T \approx 0.01$. Thus the degradation introduced by the phase noise is acceptable also for $N_s = 5$, the value for which the spectral efficiency can increase from 50% as in [10] to about 83%. We should note that the modulation variance V_A can be optimized, within the power limitation of the transmitter. Then, to show the actual degradation introduced by the phase noise, one can take as reference the distance at which a certain secure key rate R is obtained in the absence of phase noise, for example, the value $R = 10^{-3}$. Then the degradation introduced by the phase noise is accounted for by the relative reduction in the distance to achieve the same rate R, for the best value of V_A. Namely, if d_0 is the distance at which the secure rate R is obtained with no phase noise and d in the presence of phase noise, the distance penalty P_D is given by

$$P_D = \min_{V_A}\left(\frac{d_0 - d}{d_0}\right). \tag{29}$$

This penalty is shown in Fig. 4 together with the corresponding optimum value of the modulation variance $V_{\rm opt}$ for the same parameter values as in the previous figure and three values of the data symbol length N_s. A value of penalty of 100% means that the degradation introduced by the phase noise is

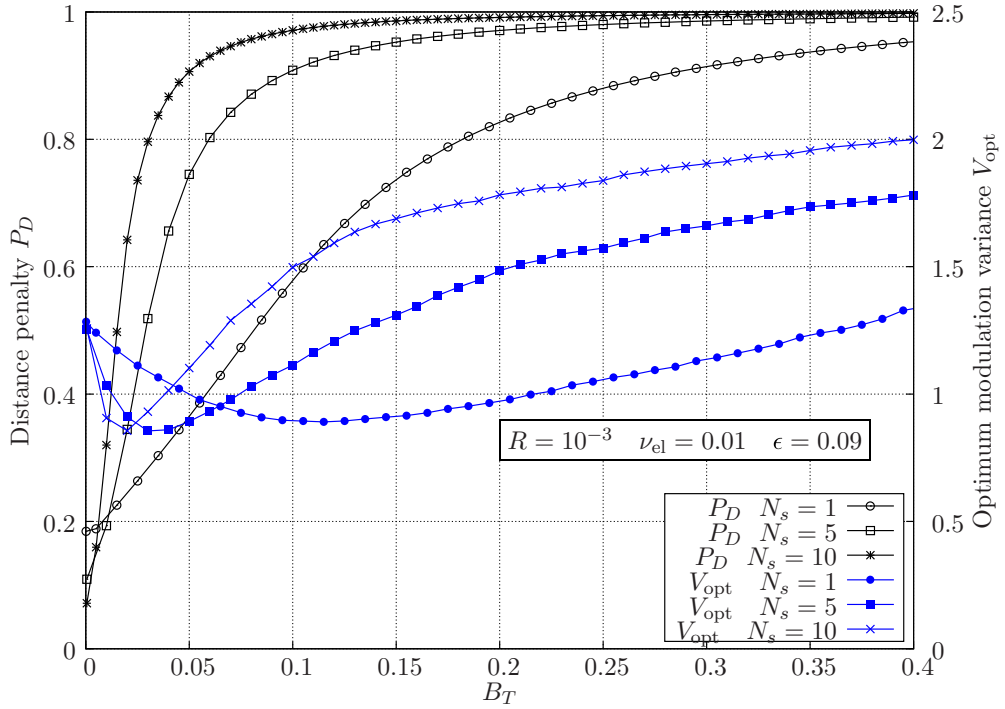

FIG. 4. Distance penalty and optimum modulation variance $V_{\rm opt}$ as a function of the normalized phase noise bandwidth B_T ($\beta = 0.8$, $\eta = 0.5$, $\nu_{\rm el} = 0.01$, $\epsilon = 0.09$).

so high that the reference secure rate cannot be reached at any distance. The curves of P_D show that the impossibility of achieving the secure rate of 10^{-3}, thus a distance penalty equal to 100%, is obtained for values of B_T which are quite reasonable, of the order of 0.1. For example, a system with a symbol rate of 100 MHz would require a laser with linewidth of 10 MHz. However, the penalty introduced by phase noise cannot be neglected in general, especially if a higher spectral efficiency is sought, for example, with $N_s = 5$. In other words, the penalty due to phase noise is noticeable, but a proper choice of the symbol rate and laser linewidth permits the exchange of a secure key with a good spectral efficiency. As

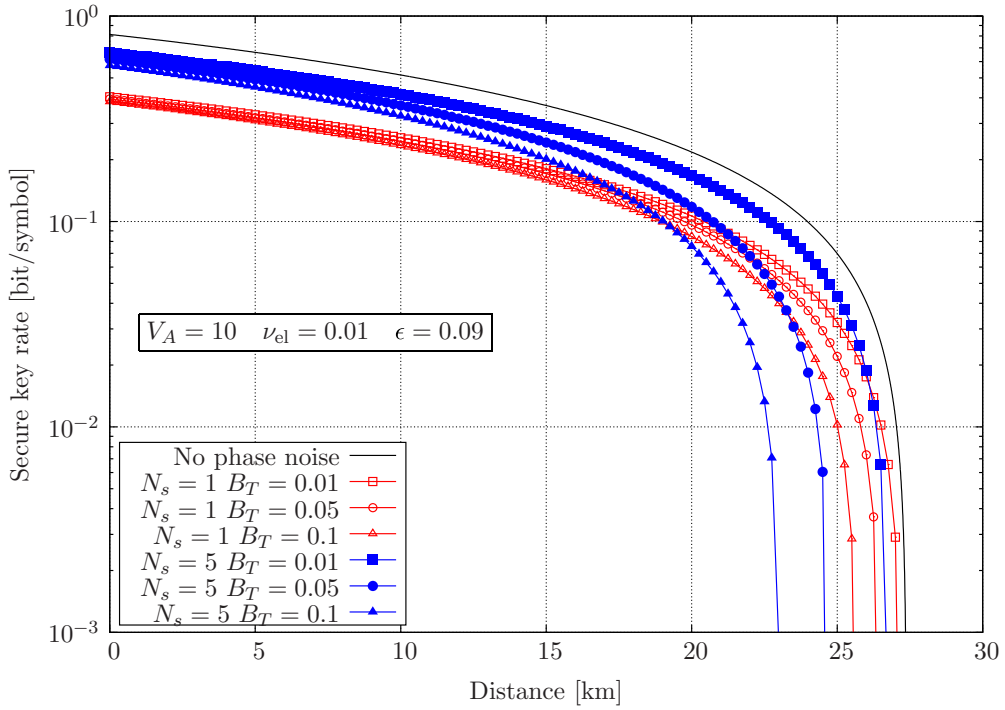

FIG. 5. Secure key rate R against collective attacks as a function of the distance for three values of B_T and useful symbols $N_s = 1$ or $N_s = 5$ ($V_A = 100$).

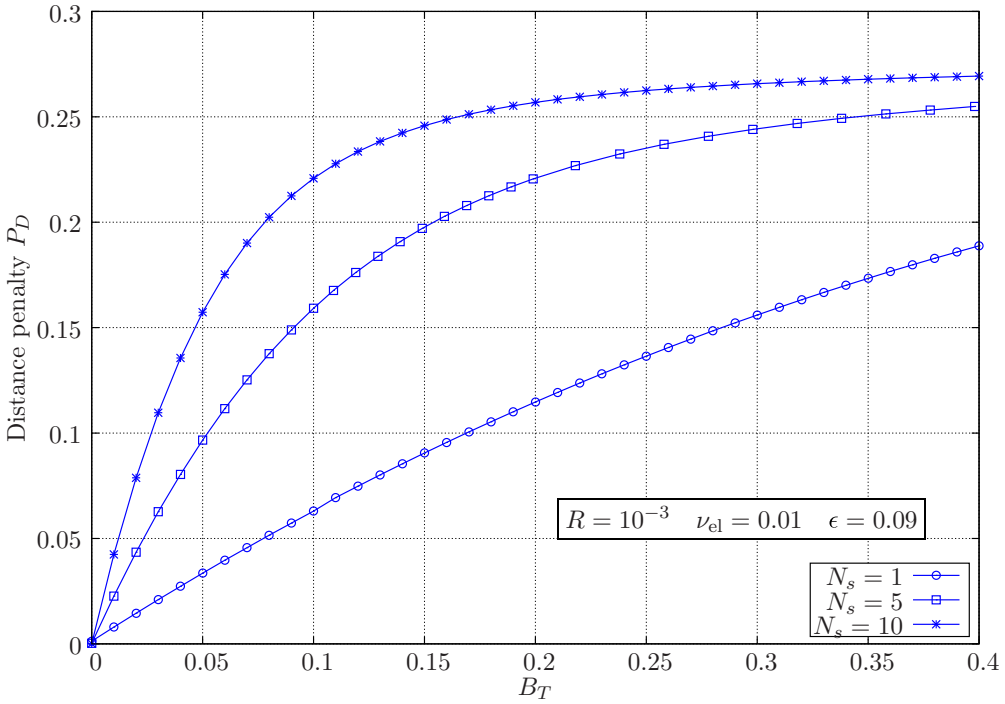

FIG. 6. Distance penalty as a function of the normalized phase noise bandwidth B_T ($\beta = 0.8$, $\eta = 0.5$, $\nu_{\rm el} = 0.01$, $\epsilon = 0.09$, $V_A = 100$).

the optimal modulation variance V_A is concerned, it can be noted that $V_{\rm opt}$ is not far from unity in general. After a first decrease with increasing phase noise, a minimum is obtained, then as the phase noise increases again a higher modulation variance is needed. However, for the corresponding values of the phase noise, the system becomes almost useless since the distance to achieve the secure rate becomes too small.

B. With collective attacks

In the case of collective attacks, the secure rate is lower and shows a behavior with a drop, corresponding to a limit distance, as shown in Fig. 5, for a fiber with specific attenuation 0.2 dB/km. As in the previous results, the other parameters are as follows: reconciliation efficiency $\beta = 0.8$, photodetector efficiency $\eta = 0.5$, electronic noise $\nu_{\rm el} = 0.01$, and excess noise $\epsilon = 0.09$. Note, however, that to get similar values of distance and rate a greater value of the modulation variance, namely $V_A = 100$, is considered in this results. Also with collective attacks, the penalty introduced by the phase noise can be accounted for by the reduction in the distance to achieve the same secure rate as in the absence of phase noise, namely P_D. In Fig. 6 the distance penalty is presented as a function of the laser phase-noise bandwidth B_T. Note that in this case the rate increases with the modulation variance so that optimum is always the maximum value for V_A, which in this case is $V_A = 100$. The same system parameters as in Fig. 5 are used. In this case the penalty is lower, but we should note that the reference key rate is taken close to the limit value, where it drops to zero. Note that the value of the modulation variance is much larger than in the previous case where the security against individual attacks is considered.

VI. CONCLUSION

The effect of phase noise has been considered in CV-QKD, showing that high symbol-rate systems can sustain a limited degradation due to phase noise, even with off the shelf components as lasers, if a pilot-assisted estimation and compensation method is employed. However, if security against collective attacks must be guaranteed, then the system requirements in terms of modulation variance are more compelling and the protocol exhibits a limit distance, i.e., a maximum channel attenuation, where the secure key rate rate drops to zero. A tradeoff between spectral efficiency and phase-noise penalty occurs, in terms of the number of data symbols between two pilots.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, Opt. Lett. **40**, 3695 (2015).
[3] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).
[4] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[5] N. J. Cerf and P. Grangier, J. Opt. Soc. Am. B **24**, 324 (2007).
[6] G. V. Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[7] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).

[8] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).

[9] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).

[10] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).

[11] K. Kikuchi, *High Spectral Density Optical Communication Technologies* (Springer, Berlin, 2010), Chap. 2, pp. 11–49.

[12] J. K. Cavers, IEEE Trans. Veh. Technol. **40**, 686 (1991).

[13] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303 (2005).