Continuous-variable quantum key distribution in non-Markovian channels

Vasile, Ruggero; Olivares, Stefano; Paris, Matteo G. A; Maniscalco, Sabrina

Published in:
Physical Review A (Atomic, Molecular, and Optical Physics)

DOI:
10.1103/PhysRevA.83.042321

Publication date:
2011

Continuous-variable quantum key distribution in non-Markovian channels

Ruggero Vasile,[1,*] Stefano Olivares,[2,3,4,†] Matteo G. A. Paris,[4,‡] and Sabrina Maniscalco[5,1,§]

[1]*Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, FI-20014 Turun yliopisto, Finland*

[2]*Dipartimento di Fisica, Università degli Studi di Trieste, I-34151 Trieste, Italy*

[3]*CNISM, Unitá di Ricerca di Milano Università, I-20133 Milano, Italy*

[4]*Dipartimento di Fisica, Università degli Studi di Milano, I-20133 Milano, Italy*

[5]*School of Engineering & Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

(Received 1 November 2010; published 15 April 2011)

We address continuous-variable quantum key distribution (QKD) in non-Markovian lossy channels and show how the non-Markovian features may be exploited to enhance security and/or to detect the presence and the position of an eavesdropper along the transmission line. In particular, we suggest a coherent-state QKD protocol which is secure against Gaussian individual attacks based on optimal $1 \rightarrow 2$ asymmetric cloning machines for arbitrarily low values of the overall transmission line. The scheme relies on specific non-Markovian properties, and cannot be implemented in ordinary Markovian channels characterized by uniform losses. Our results give a clear indication of the potential impact of non-Markovian effects in QKD.

DOI: 10.1103/PhysRevA.83.042321 PACS number(s): 03.67.Dd, 03.65.Yz

I. INTRODUCTION

Quantum key distribution (QKD) is a fundamental area of quantum technology [1]. The aim of any QKD protocol is to allow two parties, the sender Alice and the receiver Bob, to exchange a secret key using quantum and/or classical channels, avoiding a possible eavesdropper (Eve) from acquiring information on the key. Discrete-variable QKD protocols are based on transmission and measurements of single- or entangled-photon states, and therefore are limited by the efficiency of single-photon generation and detection. On the contrary, continuous-variable (CV) QKD [2] is a potentially high-bit-rate technique for at least two reasons. On the one hand, the key is encoded into continuous-spectrum quantum observables as the quadrature components of a light field, and thus the number of bits per pulse can be high. On the other hand, it employs a homodyne detection technique based on standard photodiodes, which are much faster than the avalanche photodiodes used in photon-counting discrete QKD schemes. Different proposals for CV QKD have been put forward, either based on single-mode coherent [3,4] and squeezed [5–11] signals or Einstein-Podolsy-Rosen (EPR) correlated beams [12,13]. Experimental demonstrations have been reported for coherent [3,4,14–16], squeezed [10], and EPR beams-based [13] protocols, and unconditional security proofs have also been investigated [17,18].

The coherent-state protocol is perhaps the most interesting for practical applications. In this case, Alice encodes a key into amplitudes of pure coherent states and sends them through a quantum channel to Bob, who randomly chooses a coding quadrature basis in which to measure them via homodyne detection. Binary data is extracted from the homodyne sample using bit-slice reconciliation methods and privacy amplification [19].

The unavoidable losses occurring along the channel must be taken into account for the realistic description of QKD protocols and for the analysis of their security. In fact, it has been shown that losses can be exploited by eavesdroppers to hide themselves and acquire information about the key [3]. Security of the protocol is defined, e.g., ensuring that the information of Alice and Bob about the key is higher than the one acquired by Eve (direct or reverse reconciliation). Lossy channels considered so far are Markovian, i.e., characterized by a constant damping rate along the transmission line. This is usually an approximation and, in practice, channels may show non-Markovian losses, i.e., a damping rate which is not uniform along the line, being dependent on the spectral structure of the environment coupled to the propagating mode [20,21]. Moreover, the increasing success of reservoir engineering techniques paves the way for the realization of optical channels in which the losses due to the interaction with the environment can be appropriately manipulated. Recently non-Markovian signatures in semiconductor quantum wires have been experimentally observed [22].

Non-Markovian effects in CV systems have indeed been analyzed in some detail in recent years [23], with focus on the dynamics of purity, entanglement [24–26], and more general quantum correlations [27] in either independent or common baths.

In this paper, we address the effects of non-Markovian channel losses on the performance of a CV QKD protocol. In particular, we focus on a specific coherent-state protocol showing how the non-Markovian features may be exploited to enhance security, i.e., to reduce the information available for Eve and/or to detect her presence and position along the transmission line. In our scheme, a suitable engineering of the channel decay rate allows us to obtain secure QKD for arbitrarily low values of the overall transmission line. We also show that the same result cannot be obtained with ordinary Markovian channels characterized by uniform losses.

*ruggero.vasile@utu.fi
†stefano.olivares@ts.infn.it
‡matteo.paris@fisica.unimi.it
§s.maniscalco@hw.ac.uk

The best eavesdropping strategy in Markovian channels depends on the chosen reconciliation scheme by Alice and Bob [28]. Direct reconciliation-based protocols are known to be secure for channel losses not exceeding 50%, while with reverse reconciliation protocols, security is in principle achieved for any amount of loss [4]. Assuming that this is also the best strategy in the non-Markovian case, we show that our proposal enhances security independent of the choice of reconciliation method.

This paper is structured as follows. In the next section, we briefly review the coherent-state protocol in a Markovian channel and describe the eavesdropping strategy based on $1 \to 2$ asymmetric optimal cloning machines. In Sec. III we introduce a relevant class of non-Markovian channels and generalize the protocol to this case, whereas in Sec. IV, we describe in detail our proposal to enhance security and show how it is possible to detect the eavesdropper by a post-communication comparison of a part of the data sent by Alice to Bob. In Sec. V we discuss how to optimize the decay properties of the channel for a specific type of structured environment. In Sec. VI we analyze the effects of finite resolution in the detection stage. Finally, Sec. VII is devoted to extending our analysis to the case of channels with excess noise and/or to reverse reconciliation protocols. Section VIII closes the paper with some concluding remarks.

II. QKD USING COHERENT STATES

In QKD with coherent states [3], Alice draws pairs of independent real random numbers (x_A, p_A) from two Gaussian distributions with zero mean and the same variance, and then generates the coherent states $|\alpha_A\rangle = |x_A + ip_A\rangle$, which are finally sent to Bob through a quantum channel. The propagation along the channel is, in general, noisy and losses are described as the interaction of the light mode with an environment made of an ensemble of independent harmonic oscillators at temperature T under the Born-Markov approximation [29]. The evolution is thus governed by a master equation in the Lindblad form,

$$\begin{aligned}\dot{\varrho} = {} & \gamma(N+1)(2a\varrho a^\dagger - a^\dagger a\varrho - \varrho a^\dagger a) \\ & + \gamma N(2a^\dagger \varrho a - aa^\dagger \varrho - \varrho aa^\dagger),\end{aligned} \tag{1}$$

where $\gamma > 0$ is the damping rate and $N \geqslant 0$ is the mean number of thermal photons of the bath at the signal frequency, i.e., the temperature parameter of the bath. The coherent state sent by Alice evolves into a displaced thermal state of the form

$$|\alpha_A\rangle\langle\alpha_A| \to D(\alpha\sqrt{\eta_M})\nu(\mu/2)D^\dagger(\alpha\sqrt{\eta_M}), \tag{2}$$

where $D(\beta) = \exp\{\beta a^\dagger - \beta^* a\}$ is the displacement operator,

$$\eta_M \equiv \eta_M(t) = e^{-2\gamma t} \tag{3}$$

is the total channel transmission,

$$\mu \equiv \mu(t) = 2N[1 - \eta_M(t)] \tag{4}$$

is the total added excess noise, and $\nu(x)$ is a thermal state of thermal parameter x. We denote by $\tau \equiv L$ (hitherto $c = 1$) the total transmission time (channel length). After the propagation, Bob receives the states (2) and arbitrarily decides to measure one of two orthogonal quadratures. Since the key is encoded in the mean value of the signal sent by Alice, he needs to rescale the measured observables by an amount equal to $\eta_M(\tau)^{-1/2}$, thus also amplifying the noise. For the sake of clarity, we begin our analysis discussing the particular but fundamental case of $N = 0$, i.e., a damping channel without added excess noise μ, and we focus on the situation in which the key is extracted via the direct reconciliation method. The generalization to channels with thermal excess noise and reverse reconciliation will be discussed in Sec. VII.

Under the above hypothesis, the best eavesdropping attack is obtained using a passive asymmetric $1 \to 2$ cloning machine [28,30–32]: this process can be modeled with Eve intercepting the signal with a beam splitter of transmissivity η_E at position $L_E = t_E$ along the line. We assume that Eve has perfect knowledge of relevant properties of the quantum channel, i.e., the length τ and the loss rate γ, and that she can tune, with arbitrary precision, both the value of the transmissivity η_E and the attack time t_E. The reflected part of the beam is stored by Eve, whereas the other part is sent to Bob through a lossless channel. Under these conditions, the best strategy is to attack immediately ($t_E = 0$) with a beam splitter of transmissivity $\eta_E = \eta_M(\tau)$ [3] equal to the overall transmissivity of the channel. In this way, Eve is introducing the same amount of losses as the overall line: Bob will receive the same state as in the absence of any attack, and the eavesdropper is not detectable. If, however, $\eta_M(\tau) \geqslant 1/2$, then, even if not detected, Eve cannot achieve the same information as Bob about the secret key, and the protocol is secure under direct reconciliation [3].

III. COHERENT-STATE PROTOCOL IN NON-MARKOVIAN CHANNELS

Markovian evolutions are approximate dynamical models for channel losses, and more realistic situations can be described with master equations derived without the Markov assumption. For example, the inclusion of the nonresonant coupling to phonons in the description of propagation in fused silica fibers leads to delayed nonlinearity due to the non-Markovian phonon bath, in addition to spontaneous and thermal noise [21]. In the following, we consider the non-Markovian master equation (NME)

$$\dot{\varrho} = \gamma(t)\,(2a\rho a^\dagger - a^\dagger a\rho - \rho a^\dagger a), \tag{5}$$

which corresponds to a model in which the light mode interacts weakly with a structured bosonic reservoir at zero temperature. The functional form of the coefficient $\gamma(t)$ depends on the spectral structure of the environment in which the system is embedded. In the weak-coupling regime, and for times larger than the typical reservoir correlation time scale τ_R, the coefficient tends to the Markovian constant value, i.e., $\gamma(t) \to \gamma_M$. By changing the reservoir spectral properties, one may engineer the functional form of $\gamma(t)$ as well as modify the value of τ_R. It is worth noticing that the key feature in our scheme is the inhomogeneity in the rate of loss γ. This can also be achieved by a suitably engineered position-dependent coupling to the reservoir along the optical channel, since

$\gamma(x) = \gamma(ct)$. In the non-Markovian (NM) channel (5), an initial coherent state evolves as

$$|\alpha_A\rangle \to |\alpha_A e^{-\Gamma(t)/2}\rangle = |\alpha_A \sqrt{\eta_{NM}}\rangle\,,$$

where $\eta_{NM}(t) = e^{-\Gamma(t)}$ is the channel transmissivity, with $\Gamma(t) = 2\int_0^t \gamma(s)ds$. This channel does not introduce excess noise and therefore can be considered the non-Markovian analog of (1) with $N = 0$. However, because of the time dependence of the coefficient $\gamma(t)$, we have, in general, $\Gamma(t) \not\propto t$, i.e., the damping is not uniform as in the Markovian case. The eavesdropping strategy described above works in the same way if we let Eve know the analytic form of the decay rate $\gamma(t)$. In this case, the best strategy is still to attack at the beginning of the channel and to choose properly the beam-splitter transmissivity to have $\eta_E = \eta_{NM}(\tau)$. In this way, her presence is still nondetectable and the results about the security of the channel reported in [3,4] still hold.

IV. SECURITY AND EAVESDROPPING DETECTION IN NON-MARKOVIAN DAMPING CHANNELS

One of the main assumptions in QKD is that everything that Alice communicates to Bob using public channels is also known by Eve. This means that, in order to detect a possible eavesdropper, Alice needs to perform independently a certain operation during the transmission, leading to different results at Bob's side when Eve is present or not. In our protocol, Alice still encodes the key into coherent signals, but now she can act on the channel length by adding a delay Δt at the first stage of the signal propagation, as depicted in Fig. 1. For the sake of simplicity, although we have only one physical channel, we will refer to the two possible choices as two channels with the same time-dependent loss rate $\gamma(t)$ but different length. The key signal is always sent through the ordinary channel of length τ, but now Alice may also send a reference coherent state $|\alpha_0\rangle$ by choosing randomly, with the same probability, between the ordinary and the longer channel of length $\tau + \Delta t$. As we will see, although this is not changing the optimal eavesdropping strategy, it allows detection of Eve in NM channels.

Let us start by considering the situation of a clean channel (no eavesdropper) and focus on the results of the quadrature measurements for the reference state. Fifty percent of the time,

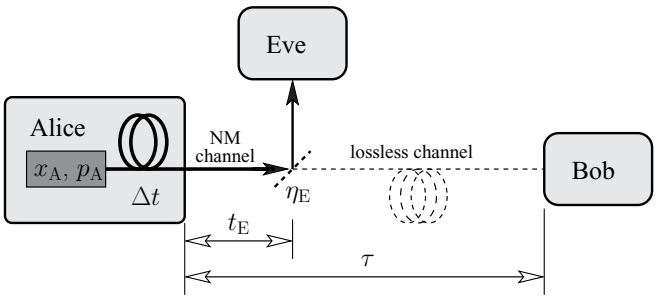

FIG. 1. Schematic diagram of the QKD protocol in a NM channel with the relevant elements of Eve's attack scheme. The solid channel line refers to the NM channel, and the dashed line refers to the lossless channel used by Eve. Without the eavesdropper, the channel is non-Markovian throughout its whole length.

Bob is receiving the state $|\alpha_0 e^{-\Gamma(\tau)/2}\rangle$ when it is sent through the ordinary line, whereas the rest of the copies evolve into $|\alpha_0 e^{-\Gamma(\tau+\Delta t)/2}\rangle$. Since Bob is not aware of which channel has been chosen by Alice, his quadrature measurements must be independent from this choice. Therefore he measures quadratures scaled according to the total ordinary channel losses $e^{-\Gamma(\tau)/2}$. After the completion of the session, Alice informs Bob about which channel each reference state has been sent through. Bob can now distinguish among the two sets of states and study the statistics of the two measurement distributions. It is easy to show that these distributions are Gaussian with the same width, but they differ in the mean value by an amount

$$\delta x_{NE} = |\alpha_0(1 - e^{-[\Gamma(\tau+\Delta t)-\Gamma(\tau)]/2})| \simeq |\alpha_0 \gamma(\tau)\Delta t|\,, \quad (6)$$

where we assumed that Δt is small compared to the variation of $\gamma(t)$. Moreover the difference in mean value increases as the amplitude α_0 increases. The situation changes when Eve is attacking the line. Because she also cannot distinguish between the reference signals and the key ones, as well as between the choice of channel by Alice, she has to treat every state the same. She then keeps unchanged the attacking time t_E and the beam-splitter transmissivity $\sqrt{\eta_E}$. If she attacks at t_E, the transmissivity must be chosen in a way that

$$e^{-\Gamma(t_E)/2}\sqrt{\eta_E} = e^{-\Gamma(\tau)/2},$$

so as to be undetectable when the ordinary channel is used. If Alice uses the longer channel, Eve's attack time is forcefully shifted to $t_E + \Delta t$. The same calculation as before for the difference in the mean values of the quadrature measurement distribution at Bob's side leads to

$$\delta x_E = |\alpha_0(1 - e^{-[\Gamma(t_E+\Delta t)-\Gamma(t_E)]/2})| \simeq |\alpha_0 \gamma(t_E)\Delta t|. \quad (7)$$

Because of the time dependence of the loss rate $\gamma(t)$, the quantities in Eqs. (6) and (7) are, in general, different. Therefore, if after the communication Alice and Bob perform a check of the mean values of the distributions using a public channel, they are able to detect the presence of Eve whenever $\gamma(t_E) \neq \gamma(\tau)$. This condition cannot be satisfied in a Markovian channel.

For non-Markovian channels that also introduce thermal noise [33], the added noise is time dependent and thus, besides the mean values, the widths of the distributions at Bob's side are also different in the presence or absence of an eavesdropper. In turn, this may be exploited to further enhance security via checking the sample variances (see Sec. VII).

V. CHANNEL OPTIMIZATION

Our proposal is based on the fact that, in a non-Markovian channel, $\Gamma(t + s) \neq \Gamma(t) + \Gamma(s)$ for generic $t, s \geqslant 0$. The lack of the semigroup property immediately implies that the integral expression $\int_t^{t+\Delta t} \gamma(s)ds$ for fixed Δt is not a constant function of t. Therefore, the two quantities in Eqs. (6) and (7) do not coincide, and the only way Eve can avoid detection is to attack the channel when $\gamma(t_E) \simeq \gamma(\tau)$. As a consequence, it is crucial to engineer appropriately the environment surrounding the channel to obtain the desired decay properties. We do not discuss here possible specific realizations of the protocol;

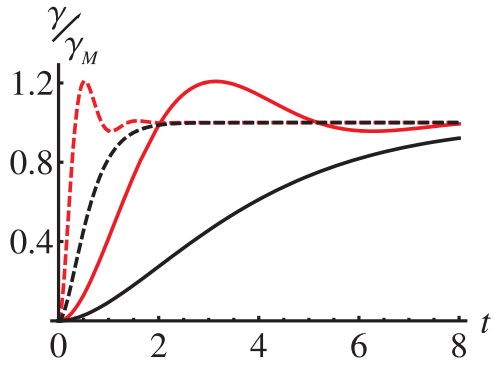

FIG. 2. (Color online) Normalized decay rates (see text) as a function of time. Red lines correspond to $\omega_c/\omega_0 = 0.5$ and black lines to $\omega_c/\omega_0 = 3.0$. Also, solid lines correspond to $\omega_c = 0.5$ and dashed lines to $\omega_c = 3.0$.

however, as a concrete example, we consider here the decay rate evaluated for an Ohmic reservoir with Lorentz-Drude cutoff [34], i.e.,

$$\gamma(t) = \gamma_M[1 - e^{-\omega_c t}\cos\omega_0 t - (\omega_c/\omega_0)e^{-\omega_c t}\sin\omega_0 t], \quad (8)$$

where ω_0 is the mode frequency, ω_c is the cut-off frequency of the environment spectrum, and γ_M is the asymptotic decay rate. The reservoir correlation time is here identified with $\tau_R = \omega_c^{-1}$.

In Fig. 2 we show the behavior of the normalized decay rate $\gamma(t)/\gamma_M$ for different values of light and cut-off frequencies ω_0 and ω_c. The red lines are evaluated for the same ratio, $\omega_c/\omega_0 = 0.5$, and differ for the value of $\omega_c = 0.5$ (solid line) and $\omega_c = 3.0$ (dashed line). The black lines instead correspond to the ratio $\omega_c/\omega_0 = 5.0$, and also differ for the value of $\omega_c = 0.5$ (solid line) and $\omega_c = 3.0$ (dashed line). Decay rates of this second class (regime $\omega_c > \omega_0$) are exactly what is needed for our scheme to work, because the relation $\gamma(t_E) < \gamma(\tau)$ holds for any allowed value of the attack time t_E, and Eve has in principle no way to hide herself from the security protocol. Moreover, since for $\omega_c > \omega_0$ the function $\gamma(t)$ is invertible, Alice and Bob can also find the exact position of the eavesdropper along the line. On the other hand, decay functions corresponding to red lines in Fig. 2 exhibit oscillations before approaching the stationary value and thus they are not invertible. In this case, Eve may find several places, or "hiding locations," at the beginning of the line where she can perform the attack while avoiding detection, i.e., when $\gamma(t_E) = \gamma_M$.

VI. EFFECTS OF IMPERFECT DETECTION

Our detection method relies on checking whether the distributions of homodyne data from the two channels of different lengths are shifted by each other by an amount δx_{NE} rather than δx_E. The ability to detect an eavesdropper thus depends on the precision and the resolution of quadrature measurements made by Bob. A finite precision implies that Bob would not be able to discriminate the results when

$$|\alpha_0 \Delta t[\gamma(t_E^*) - \gamma(\tau)]| < \epsilon,$$

with ϵ a threshold depending on the precision. In practice, this means that whenever Eve places the attack at $t_E > t_E^*$, she is not revealed by our method. According to Ref. [3], the channel is then secure when

$$\Gamma(t_E) \geqslant -\log 2\eta_{NM},$$

with $\eta_{NM} = \exp\{-\Gamma(\tau)\}$ being the overall transmission of the non-Markovian channel. In other words, security is ensured if the overall transmission is larger than

$$\eta_{NM} \geqslant \tfrac{1}{2}\exp\{-\Gamma(t_E^*)\} \equiv \eta_{th}.$$

For any given ϵ, we can make t_E^* in principle arbitrarily close to τ by a suitable engineering of the environment spectrum. In turn, this allows one to decrease the threshold and make the channel secure for arbitrarily low values of the overall transmission η_{NM}. Notice also that, being t_E is of the order of the reservoir correlation time scale τ_R, if $\tau_R \ll \tau$, then the amount of losses accumulated before the attack is negligible compared to the overall losses, and the advantage given by our protocol cannot be appreciated. In order to obtain a consistent improvement, we need τ_R to be of the order of the total transmission time τ.

VII. EXTENSION OF THE PROTOCOL TO CHANNELS WITH EXCESS NOISE AND TO REVERSE RECONCILIATION

The extension of our proposal to non-Markovian channels with added excess noise and/or to reverse reconciliation protocols is straightforward if we keep in mind the main idea behind our protocol, that is, to force a discrepancy on some result at Bob's side when the eavesdropper is present. This discrepancy is implemented through the random transmission of the reference states $|\alpha_0\rangle$ along two different lines characterized by a difference in the overall loss η and, in the present case, also in the added excess noise μ. For the sake of concreteness, and in order to make the discussion as clear as possible, we refer in the following to the case considered in [28], where different kinds of eavesdropping attacks in protocols using coherent states and reverse reconciliation have been investigated and compared.

Our prototype of a non-Markovian channel with added excess noise is described by the following master equation:

$$\dot{\varrho} = [\Pi(t) + \gamma(t)](2a\varrho a^\dagger - a^\dagger a\varrho - \varrho a^\dagger a) \quad (9)$$

$$+ [\Pi(t) - \gamma(t)](2a^\dagger \varrho a - aa^\dagger\varrho - \varrho aa^\dagger), \quad (10)$$

characterized by a time-dependent loss rate $\gamma(t)$ and a time-dependent excess-noise density $\Pi(t)$. In the presence of this channel of length τ, a pure coherent state will evolve into a displaced thermal state, as in Eq. (2). In terms of mean values of first and second quadrature moments, we have

$$\bar{X}(\tau) = \sqrt{\eta(\tau)}\bar{X}(0), \quad \sigma(\tau) = [\mu(\tau) + 1]\sigma(0), \quad (11)$$

where $\mu(\tau) = \int_0^\tau \Pi(s)ds$ is the added excess noise, $\eta(\tau) = \exp\{-\Gamma(\tau)\}$ is the channel transmission with $\Gamma(\tau) = \int_0^\tau \gamma(s)ds$, and $\sigma(0) = \mathbb{I}/2$ is the covariance matrix of a coherent state, with $\mathbb{I}$ being the 2×2 identity matrix.

We start analyzing the situation in the absence of any eavesdropper. In this case, Alice sends the key states along the channel of length τ, while the reference coherent states $|\alpha_0\rangle$ may be randomly sent along the normal channel or the

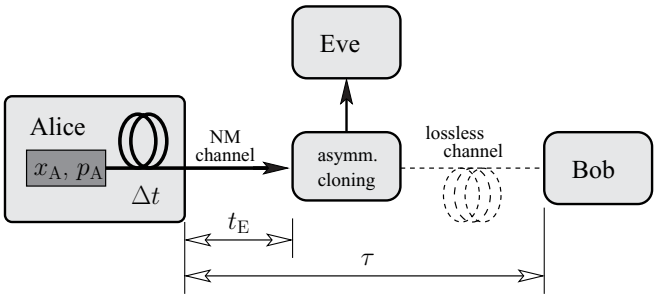

FIG. 3. Schematic diagram of the QKD protocol in a NM channel with excess noise. During the attack, Eve simulates both the noise and the damping by means of an active asymmetric cloning machine.

longer one of length $\tau + \Delta t$. A straightforward calculation shows that, in the absence of Eve, at Bob's side there will be a discrepancy on the mean value and variance of the quadrature measurements for the reference states, whose amount is given by

$$\delta x_{NE} = |\alpha_0(1 - e^{-[\Gamma(\tau+\Delta t)-\Gamma(\tau)]/2})| \simeq |\alpha_0 \gamma(\tau)\, \Delta t|, \quad (12a)$$

$$\Delta x_{NE} \simeq \frac{|\Pi(\tau)|}{\eta(\tau)}\, \Delta t, \quad (12b)$$

respectively.

Let us consider what happens in the presence of an eavesdropper attacking at a certain time t_E. It is worth stressing that, whatever attack is performed, the net effect can now be modeled as an active asymmetric cloning machine, in order to simulate the effect of both the damping and the noise (see Fig. 3). If Alice now switches between the channels, it will result in a different discrepancy at Bob's side when Eve attacks, and the new discrepancies on mean values and variance read

$$\delta x_E = |\alpha_0(1 - e^{-[\Gamma(t_E+\Delta t)-\Gamma(\tau)]/2})| \simeq |\alpha_0 \gamma(t_E)\Delta t|, \quad (13a)$$

$$\Delta x_E \simeq \frac{|\Pi(t_E)|}{\eta(\tau)}\Delta t, \quad (13b)$$

respectively. Therefore our result works for general kinds of eavesdropping attacks in protocols using coherent states, provided that the non-Markovian channel does not contain "hiding locations" where $\gamma(t_E) \simeq \gamma(\tau)$. If Eve attacks at these hiding locations, indeed, she can always hide her presence. Nevertheless, even in the case of an eavesdropping attack at the hiding locations, our scheme may always be used to enhance the security of coherent-state protocols based on direct or reverse reconciliation. This can be proved by focusing once more on the main effect of the channel switching performed by Alice, that is, to force Eve to attack in the hiding locations. If the non-Markovian channel is suitably designed and engineered, it is possible to shift Eve's attacks at times $t_E \gg 0$. In this way, the signal is already partially damped and decohered when arriving at the eavesdropper's location, thus forcing Eve to reduce the interference with the communication and, therefore, reduce its added noise (reducing μ) and losses (increasing η). If we consider, as a peculiar example, the optimal individual Gaussian attack for the reverse reconciliation reported in Ref. [28], this constraint corresponds to an increase of the conditional variance between Eve's and Bob's data, thus resulting in a decrease of the correlations.

VIII. CONCLUSION

We have analyzed continuous-variable QKD with coherent states in the presence of non-Markovian effects along the transmission line and suggested a method to improve security based on the nonuniform time dependence of the losses. In particular, we focused on a coherent-state QKD protocol, which is secure against Gaussian individual attacks based on optimal $1 \to 2$ cloning machines.

Our method ensures security for arbitrarily low transmissivity of the channel and allows one to detect the presence and the position of the eavesdropper upon both a suitable engineering of the channel decay properties and the use of an additional reference coherent signal. The eavesdropper can manage to hide her presence by reducing the extracted amount of information, but the legitimate users can reduce to zero her information by tuning the reservoir correlation time. Our scheme to reveal an eavesdropper is based on a specific non-Markovian property, and it cannot be implemented in ordinary Markovian channels characterized by uniform losses. In addition, since it is based on channel properties rather than on specific features of the distribution scheme, we foresee its application to other CV QKD protocols, such as those based on squeezed or entangled states.

Our results pave the way for future investigations on security against even more general non-Markovian attacks, and give a clear indication of the potential impact of non-Markovian effects in QKD.

ACKNOWLEDGMENTS

This work has been supported by the Finnish Cultural Foundation (Science Workshop on Entanglement), the Emil Aaltonen Foundation, and the CNR-CNISM agreement.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] N. J. Cerf and Ph. Grangier, J. Opt. Soc. Am. B **24**, 324 (2007).
[3] F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, Nature (London) **421**, 238 (2003).
[5] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[6] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999); **62**, 062306 (2000).
[7] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).

[8] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[9] K. Bencheikh, Th. Symul, A. Jankovic, and J. A. Levenson, J. Mod. Opt. **48**, 19031920 (2001).
[10] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[11] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[12] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[13] Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[14] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).
[15] B. Qi, L. L. Huang, L. Qian, and H. K. Lo, Phys. Rev. A **76**, 052323 (2007).
[16] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303 (2007).
[17] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[18] A. Leverrier, E. Karpov, Ph. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).
[19] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[20] P. D. Drummond and J. F. Corney, J. Opt. Soc. Am. B **18**, 139 (2001).
[21] J. F. Corney, P. D. Drummond, J. Heersink, V. Josse, G. Leuchs, and U. L. Andersen, Phys. Rev. Lett. **97**, 023606 (2006).
[22] V. Lopez-Richard, J. C. Gonzalez, F. M. Matinaga, C. Trallero-Giner, E. Ribeiro, M. RebelloSousa Dias, L. Villegas-Lelovsky, and G. E. Marques, Nano Lett. **9**, 3129 (2009).
[23] M. Ban, J. Phys. A **39**, 1927 (2006).
[24] S. Maniscalco, S. Olivares, and M. G. A. Paris, Phys. Rev. A **75**, 062119 (2007).
[25] K-L. Liu and H-S. Goan, Phys. Rev. A **76**, 022312 (2007).
[26] R. Vasile, S. Olivares, M. G. A. Paris, and S. Maniscalco, Phys. Rev. A **80**, 062324 (2009).
[27] R. Vasile, P. Giorda, S. Olivares, M. G. A. Paris, and S. Maniscalco, Phys. Rev. A **82**, 012313 (2010).
[28] R. Namiki, M. Koashi, and N. Imoto, Phys. Rev. A **73**, 032302 (2006).
[29] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems* (Oxford University Press, Oxford, 2002).
[30] S. L. Braunstein, V. Buzek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
[31] F. Grosshans and Ph. Grangier, Phys. Rev. A **64**, 010301 (2001).
[32] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[33] S. Maniscalco, J. Piilo, F. Intravaia, F. Petruccione, and A. Messina, Phys. Rev. A **70**, 032113 (2004).
[34] U. Weiss, *Quantum Dissipative Systems*, 2nd ed. (World Scientific, Singapore, 1999).