Continuous variable quantum key distribution in non-Markovian channels

Ruggero Vasile,[1,*] Stefano Olivares,[2] Matteo G. A. Paris,[3] and Sabrina Maniscalco[1]

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

[2] *CNISM UdR Milano Università, I-20133 Milano, Italy*

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

(Dated: November 2, 2010)

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 states QKD protocol which is secure against individual attacks for arbitrarily low values of the overall transmission line. Our scheme relies on specific non-Markovian properties, and cannot be implemented in ordinary Markovian channels characterized by uniform losses.

PACS numbers: 03.67.Dd, 03.65.Yz,89.70.+c

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) to acquire information on the key. Discrete variable QKD protocols are based on transmission and measurements of single or entangled photons states, and therefore they 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. One 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 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 EPR correlated beams [12, 13]. Experimental demonstrations have been reported for coherent state [3, 4, 14–16], squeezed [10] and EPR beams [13] based protocols, and unconditional security proofs have been also given [17]. In the coherent state protocol, which is the most interesting for practical applications, 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 via homodyne detection. Binary data is extracted from the homodyne sample using the bit-slice reconciliation method and privacy amplification [18].

The unavoidable losses occurring along the channel must be taken into account for a realistic description of any QKD protocol. In fact, it has been shown that losses can be exploited by eavesdroppers to hide themselves [3]. Security of the protocol is then defined through the equivalent noise referred to the input, i.e. on ensuring that the information of Bob about the key to be higher than the one acquired by Eve. Lossy channels considered so far are Markovian, i.e. characterized by a damping rate which is constant 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 transmission line, being dependent on the spectral structure of the environment coupled to the propagating mode [19, 20]. Moreover, the increasing success of reservoir engineering techniques paves the way to the realization of optical channels in which the losses due to the interaction with the environment can be appropriately manipulated. Recently, e.g., non-Markovian signatures in semiconductor quantum wires have been experimentally observed [21].

In this Letter we address for the first time the effects of non-Markovian channel losses on the performances of a CV QKD protocol. In particular, we focus on the coherent state protocol and show 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. In the following, we briefly review the coherent state protocol in a Markovian channel and describe the eavesdropping strategy. We then introduce a relevant class of non-Markovian channel and generalize the protocol to this case. Finally, 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 part of the data sent by Alice to Bob. We also discuss how to optimize the decay properties of the channel for a specific type of structured environment.

QKD using coherent states — In QKD with coherent states [3], Alice draws pairs of indepedent real random numbers (x_A, p_A) from two Gaussian distributions with zero mean and the same variance, and then generates the coherent states $|\alpha_\mathrm{A}\rangle = |x_\mathrm{A} + ip_\mathrm{A}\rangle$, 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 a zero temperature ensemble of independent harmonic oscillators under the Born-Markov approximation [22]. The evolution is thus governed by a Master equation in the Lindblad form $\dot{\varrho} = \gamma(2a\varrho a^\dagger - a^\dagger a\varrho - \varrho a^\dagger a)$. The state sent by Alice evolves as $|\alpha_\mathrm{A}\rangle \to |\alpha_\mathrm{A} e^{-\gamma t}\rangle \equiv |\alpha_\mathrm{A}\sqrt{\eta_M}\rangle$, where $\eta_M \equiv \eta_M(t) = e^{-2\gamma t}$ is the channel transmission. We denote by $\tau \equiv L$ (hitherto $c = 1$) the total transmission time/channel length. After the propagation Bob receives the damped states 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.

Eavesdropping strategy — Due to the very nature of the protocol, the best passive attack Eve may perform is the use of an optimal asymmetric $1 \to 2$ cloning machine [23–25]. 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 Eve knows the features of the quantum channel (the lenght 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 eavesdropping 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 $\eta_M(\tau) \geq 1/2$ then, even if not detected, Eve cannot achieve the same information as Bob about the secret key and the protocol is secure [3].

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. As for example, including the non-resonant 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 [20]. In the following we consider the non-Markovian master equation (NME) $\dot{\varrho} = \gamma(t)(2a\rho a^\dagger - a^\dagger a\rho - \rho a^\dagger a)$, 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 a non-Markovian channel an initial coherent state evolves as $|\alpha_\mathrm{A}\rangle \to |\alpha_\mathrm{A} e^{-\Gamma(t)/2}\rangle = |\alpha_\mathrm{A}\sqrt{\eta_{NM}}\rangle$ where $\eta_{NM}(t) = e^{-\Gamma(t)}$ is the channel transmissivity, with $\Gamma(t) = 2\int_0^t \gamma(s)ds$. 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 known 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 non detectable and the results about the security of the channel reported in [3, 4] still hold. On the other hand, the time-dependent losses may be exploited to detect the presence of the eavesdropper and, in some cases, its position along the line.

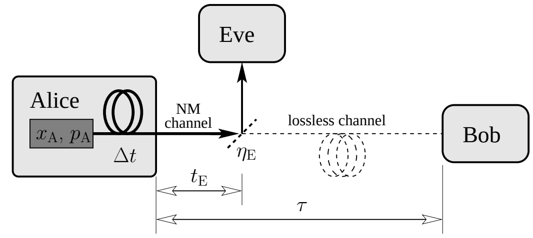

FIG. 1: Diagram of the QKD protocol in NM channel with the relevant elements of Eve's attack scheme. The solid channel line refers to the NM channel, the dashed one refers to the lossless channel used by Eve. Without the eavesdropper, the channel is non-Markovian throughout its whole length.

Eavesdropping detection in NM channels — One of the main assumptions in QKD is that everything 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 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, though 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 $\tau + \Delta t$.

Let us start by considering the situation of clean channel (no eavesdropper) and focus to the results of the quadrature measurements for the reference state. Bob is receiving fifty percent of the time 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 same width but they differ in the mean value by an amount

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

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 on the same foot. 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 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 side leads to

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

Because of the time dependence of the loss rate $\gamma(t)$ the quantities in Eqs. (1) and (2) 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.

Certain types of non-Markovian channels also introduce thermal noise [27]. Since the added noise is time dependent, besides the mean values also the widths of the distributions at Bob side are different in the presence or absence of an eavesdropper. In turn, this may be exploited to further enhance security via checking the sample variances.

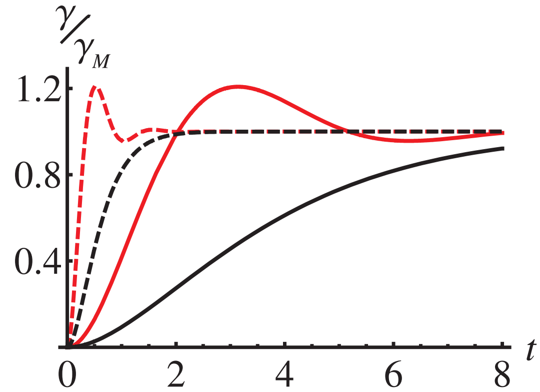

FIG. 2: (Colors online) Normalized decay rates (see text) as a function of time. Red lines correspond to $\omega_c/\omega_0 = 0.5$ and black lines to $\omega_c/\omega_0 = 3$. $\omega_c = 0.5$ for solid lines, and $\omega_c = 3$ for dashed lines.

Discussion — Our proposal is based on the fact that, in a non-Markovian channel, $\Gamma(t+s) \neq \Gamma(t) + \Gamma(s)$ for generic $t, s \geq 0$. 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. (1) and (2) 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. As a concrete example we consider here the decay rate evaluated for an Ohmic reservoir with Lorentz-Drude cutoff [28], i.e. $\gamma(t) = \gamma_M\big[1 - e^{-\omega_c t}\cos\omega_0 t - (\omega_c/\omega_0)e^{-\omega_c t}\sin\omega_0 t\big]$, ω_0 being the mode frequency, ω_c the cut-off frequency of the environment spectrum, and γ_M 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 $\omega_c = 3$ (dashed line). The black lines instead correspond to $\omega_c/\omega_0 = 5$ and $\omega_c = 0.5$ (solid line), $\omega_c = 3$ (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 represented by the red lines present oscillations before relaxing to the stationary value and are not invertible. In this case Eve may find several places at the beginning of the line where she can perform the attack while avoiding detection, i.e. when $\gamma(t_E) = \gamma_M$.

Our detection method relies on checking whether the distributions of homodyne data from the two channels of different lengths are shifted each other by an amount δx_{NE} rather than δx_E. The ability of detecting an eavesdropper thus depends on the precision and the resolution of quadrature measurements made by Bob. A finite precision implies that Bob could 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 $\Gamma(t_E) \geq -\log 2\eta_{NM}$, $\eta_{NM} = \exp\{-\Gamma(\tau)\}$ being the overall transmission of the non-Markovian channel. In other words, security is ensured if the overall transmission is larger than $\eta_{NM} \geq \frac{1}{2}\exp\{-\Gamma(t_E^*)\} \equiv \eta_{th}$. 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 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 are 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.

Conclusion — We have analyzed continuous variable QKD with coherent states in the presence of non-Markovian effects along the transmission line and suggested a novel method to improve security based on the non uniform time dependence of the losses. 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 detection scheme is based on a specific non-Markovian property, and it cannot be implemented in ordinary Markovian channel characterized by uniform losses. Besides, 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, as those based on squeezed or entangled states.

This work has been supported by the Turku Collegium of Science and Medicine, the Finnish Cultural Foundation (Science Workshop on Entanglement), the Magnus Ehrnrooth Foundation, the Emil Aaltonen Foundation, and partially supported by the CNR-CNISM agreement.

* Electronic address: ruggero.vasile@utu.fi

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] N. J. Cerf, Ph. Grangier, J. Opt. Soc. Am. B **24**, 324 (2007).
[3] F. Grosshans, 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, J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[8] N. J. Cerf, M. Levy, G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[9] K. Bencheikh, Th. Symul, A. Jankovic, J. A. Levenson, J. Mod. Opt. **48**, 19031920 (2001).
[10] Ch. Silberhorn, T.C. Ralph, N. Lutkenhaus, G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[11] R. Garcia-Patron, N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[12] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[13] Ch. Silberhorn, N. Korolkova, G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[14] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, R. Namiki, Phys. Rev. A **68**, 042331 (2003).
[15] B. Qi, L. Huang, L. Qian, H. Lo, Phys. Rev. A **76**, 052323 (2007).
[16] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, P. K. Lam, Phys. Rev. A **76**, 030303 (2007).
[17] A. Leverrier, E. Karpov, Ph. Grangier, N. J. Cerf, New J. Phys. **11**, 115009 (2009).
[18] G. Van Assche, J. Cardinal , N. J. Cerf, IEEE Trans. Inform. Th. **50**, 394 (2004).
[19] P. D. Drummond and J. F. Corney, J. Opt. Soc. Am. B **18**, 139 (2001).
[20] J. F. Corney, P. D. Drummond, J. Heersink, V. Josse, G. Leuchs, U. L. Andersen, Phys. Rev. Lett. **97**, 023606 (2006).
[21] V. Lopez-Richard, J. C. Gonzalez, F. M. Matinaga, C. Trallero-Giner, E. Ribeiro, M. Rebello Sousa Dias, L. Villegas-Lelovsky, and G. E. Marques, Nano Lett. **9**, 3129 (2009).
[22] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems* (Oxford University Press, 2002).
[23] S. L. Braunstein, V. Buzek and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
[24] F. Grosshans and Ph. Grangier, Phys. Rev. A **64**, 010301 (2001).
[25] R. Namiki, M. Koashi, and N. Imoto, Phys. Rev. A **73**, 032302 (2006).
[26] N.J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[27] S. Maniscalco, J. Piilo, F. Intravaia, F. Petruccione, and A. Messina Phys. Rev. A **70**, 032113 (2004).
[28] U. Weiss, *Quantum Dissipative Systems, 2nd edition* (World Scientific Publishing, Singapore, 1999).