Multiphoton communication in lossy channels with photon-number entangled states

Vladyslav C. Usenko[1,2,*] and Matteo G. A. Paris[2,†]
[1]*Bogolyubov Institute for Theoretical Physics of the National Academy of Sciences, Kyiv, Ukraine*
[2]*Dipartimento di Fisica dell'Università di Milano, Milan, Italy*

(Received 14 December 2006; revised manuscript received 6 February 2007; published 20 April 2007)

We address binary and quaternary communication channels based on correlated multiphoton two-mode states of radiation in the presence of losses. The protocol are based on photon number correlations and realized upon choosing a shared set of thresholds to convert the outcome of a joint photon number measurement into a symbol from a discrete alphabet. In particular, we focus on channels built using feasible photon-number entangled states (PNES) as two-mode coherently-correlated (TMC) or twin-beam (TWB) states and compare their performances with that of channels built using feasible classically correlated (separable) states. We found that PNES provide larger channel capacity in the presence of loss, and that TWB-based channels may transmit a larger amount of information than TMC-based ones at fixed energy and overall loss. Optimized bit discrimination thresholds, as well as the corresponding maximized mutual information, are explicitly evaluated as a function of the beam intensity and the loss parameter. The propagation of TMC and TWB in lossy channels is analyzed and the joint photon number distribution is evaluated, showing that the beam statistics, either sub-Poissonian for TMC or super-Poissonian for TWB, is not altered by losses. Although entanglement is not strictly needed to establish the channels, which are based on photon-number correlations owned also by separable mixed states, purity of the support state is relevant to increase security. The joint requirement of correlation and purity individuates PNES as a suitable choice to build effective channels. The effects of losses on channel security are briefly discussed.

DOI: 10.1103/PhysRevA.75.043812 PACS number(s): 42.50.Dv, 03.67.−a, 03.67.Hk, 03.67.Dd

I. INTRODUCTION

Communication protocols based on quantum signals have attracted increasing interest in recent years, since they offer the possibility of enhancing either the communication capacity or the security by exploiting the very quantum nature of the information carriers. Information may be indeed conveyed from a sender to a receiver through quantum channels. In order to achieve this goal a transmitter prepares a quantum state drawn from a collection of known states and sends it through a given quantum channel. The receiver retrieves the information by measuring the channel in order to discriminate among the set of possible preparations and, in turn, to determine the transmitted signal. The encoding states are generally not orthogonal and also when orthogonal signals are transmitted, they usually lose orthogonality because of noisy propagation along the communication channel. Therefore, in general, no measurement allows the receiver to distinguish perfectly between the signals [1,2] and the need of optimizing the detection strategy unavoidably arises.

A different approach, which will be used in this paper, is to encode information in the degrees of freedom of a correlated state shared by the two parties. In this framework, the two parties jointly (and independently) measure the state and extract the transmitted symbol according to a previously agreed inference rule. This kind of scheme, which may be symmetric or asymmetric depending on the nature of the channels, may serve either to send a message or to share a cryptographic key. In particular, entanglement-based protocols with nonlocal correlations between spatially separated locations have been proved very effective to provide a pair of legitimate users with methods to share a secure cryptographic key via quantum key distribution (QKD). Besides, the nonclassicality of entangled states can be used to improve the monitoring of a state against disturbance and/or decoherence, which, in turn, made entanglement useful to detect unwanted measurement attempts, i.e., increasing the security of communication. Indeed, several quantum-based cryptographic protocols [3] have been suggested and implemented either for qubits or continuous variable (CV) systems.

Communication protocols and QKD schemes have been first developed for single qubit [4] or entangled qubit pairs [5], and practically implemented using faint laser pulses or photon pairs from spontaneous parametric down conversion (SPDC) in a pumped nonlinear crystal [6]. Recently, much attention has been devoted to investigating the use of CV systems in quantum-information processing. In fact, continuous-spectrum quantum variables may be easily manipulated in order to perform various quantum-information processes. This is the case of multiphoton Gaussian state of light, e.g., squeezed-coherent beams and twin beams, by means of linear optical circuits, photodetection, and homodyne detection. In addition, non-Gaussian CV states of two modes may be generated either by conditional measurements [7,8] or concurrent nonlinearities. In turn, CV multiphoton states [9], may be used to increase the effectiveness and reliability of quantum communications and QKD. Several CV QKD protocols have already been developed on the basis of quadrature modulations coding of single squeezed [10], coherent [11], and entangled beam pairs [12–15]. Protocols using the sub-shot-noise fluctuations of photon-number difference of two correlated beams [16], the sub-shot-noise

*Electronic address: usenko@iop.kiev.ua
†Electronic address: matteo.paris@fisica.unimi.it

modulations [17], and the sub-shot-noise fluctuations of the photon numbers in each of the correlated modes [18] have been proposed. Although for CV protocols unconditional security proofs have not been obtained yet [19], they are of interest and deserve investigations mostly due to the potential gain in communication effectiveness.

In this paper we address binary and quaternary communication channels based on photon-number continuous-variable multiphoton entangled states (PNES), in particular we consider two-mode coherently-correlated (TMC) or twin-beam (TWB) states. The communication protocol is based on photon number correlations and realized upon choosing a shared (set of) threshold(s) to convert the outcome of a joint photon number measurement into a symbol from a discrete alphabet.

Notice that, in principle, entanglement itself is not needed to establish this class of communication channels, which are based on photon-number correlations owned also by separable mixed states. On the other hand, purity of the support state is relevant to increase security of the channel. In fact, if the information is encoded in classically correlated (mixed) states an intruder can easily measure the number of photons in either of the modes and then recreate the mixed state mode by activating the corresponding number of single-photon or photon-pair sources (the latter case with the degenerate SPDC process is already quite realistic). Thus the information encoded in the photon number of a mixed state mode can be effectively intercepted. On the other hand, this attack is not effective in the case of PNES-based channels, since the destruction of the mutual second order coherence of a PNES state can be revealed by a joint measurement on the two modes, which can be accomplished if the receiver, instead of or besides extracting the bit value, randomly sends his mode or part of it back to the sender to let her check the presence of an eavesdropper, analogously to "two-way" quantum cryptography based on individually coherent entangled beams [20]. For the PNES-based protocols, although no strict proofs of security can be offered, TMC-based protocols may be proved secure against realistic intercept-resend eavesdropping. The security mostly relies on the fact that the generation of traveling Fock states of radiation, despite several theoretical proposals based on tailored nonlinear interactions [21], conditional measurements [22], or state engineering [23,24], is still extremely challenging from the experimental point of view. Overall, it is the joint requirement of correlation and purity that leads to individuate PNES as a suitable choice for building effective and, to some extent, secure communication channels.

The main goal of the paper is twofold. On the one hand, we consider communication channels based on a realistic class of PNES and analyze the effects of losses on the performances of the protocol. On the other hand, we optimize the performances of our protocol and compare the results of PNES-based schemes to that obtained using a realistic kind of classically correlated (mixed, separable) states as a support. The evolution of TMC and TWB in lossy channels, as well as that of classically correlated states, is analyzed to calculate the joint photon number distribution and evaluate the survival of correlations. Using these results we determine the optimized bit discrimination thresholds and the corresponding channel capacity (maximized mutual information) for binary and quaternary alphabets. The effects of losses on security of the protocols against intercept-resend attacks are briefly discussed.

The paper is structured as follows: in Sec. II we describe the communication protocol and introduce the correlated states, either PNES or classically correlated, that will be considered as a support. In Sec. III we analyze the propagation of the above states in a lossy channel, and evaluate the joint photon number distribution and the correlations. In Sec. IV we optimize the bit discrimination threshold for binary and quaternary alphabets and evaluate the corresponding channel capacity. Finally, in Sec. V we briefly discuss security and close the paper with some concluding remarks.

II. COMMUNICATION CHANNELS BASED ON PHOTON-NUMBER CORRELATIONS

Quantum optical communication channels can be established using multiphoton entangled states of two field mode, which provide the necessary correlations between the two parties. In this work we investigate the information capacity of quantum channels built using as a support a specific class of bipartite entangled states, which we refer to as photon-number entangled states (PNES). In the Fock number basis, PNES may be written as

$$|\Psi\rangle\rangle = \sum_n c_n |n,n\rangle\rangle, \tag{1}$$

where $|n,n\rangle\rangle = |n\rangle_1 \otimes |n\rangle_2$ and $\Sigma_n |c_n|^2 = 1$. As we will see an effective channel may be established exploiting the strong correlation between the photon number distributions of the two modes. Indeed, PNES show perfect (total) correlations in the photon number, i.e., the correlation index

$$\gamma = \frac{\langle n_1 n_2 \rangle - \langle n_1 \rangle \langle n_2 \rangle}{\sqrt{\sigma_1^2 \sigma_2^2}}, \tag{2}$$

with $n_j = a_j^\dagger a_j$, $j=1,2$, and $\sigma_j^2 = \Delta n_j^2$, is equal to one for any PNES. On the other hand, the degree of entanglement strongly depends on the profile c_n. PNES may be generated by means of parametric optical oscillator exploiting seeded PDC process in a nonlinear crystal placed in and optical cavity [25]. Several implementations have already been reported, with the generation of PNES with photon number statistics varying from super-Poissonian to sub-Poissonian after postselection [26–28]. Meanwhile, several quantum communication schemes and QKD protocols were proposed using PNES, with information encoded in the beam intensity [17,29] or intensity difference [16,30].

The bits coding or decoding for a PNES-based communication protocol is rather natural: In the binary case each of the legitimate users measure the incoming photon number in a predetermined time slot and compare the obtained value to a given bit threshold. If the detected value is above the threshold the corresponding bit value is assigned to one, zero otherwise,

$$B_2 = \begin{cases} n \le T \to 0, \\ n > T \to 1. \end{cases} \tag{3}$$

The scheme may be also extended to an M-letter protocol by introducing different thresholds

$$B_M = \begin{cases} n \le T_1 \to 0, \\ T_1 < n \le T_2 \to 1, \\ T_2 < n \le T_3 \to 2, \\ \cdots \quad \cdots \\ n > T_{M-1} \to M. \end{cases} \tag{4}$$

The effectiveness of these generalizations depends of course on the beam intensity and on the resolution thresholds of the detectors. PNES-based protocols of this kind have been suggested [18] and analyzed in the ideal case using two-mode coherently correlated (TMC) states using, in the binary case, a threshold value equal to the integer part of the average photon number. In the Fock basis TMC states [31,32] are written as follows:

$$|\lambda\rangle\rangle = \frac{1}{\sqrt{I_0(2|\lambda|)}} \sum_n \frac{\lambda^n}{n!} |n,n\rangle\rangle, \tag{5}$$

where $\lambda \in \mathbb{C}$ and $I_0(x)$ denotes a modified Bessel' function of the first kind. Without loss of generality we will consider λ as real throughout the paper. The average photon number of the state $|\lambda\rangle\rangle$ is given by

$$N_\lambda = \frac{2\lambda I_1(2\lambda)}{I_0(2\lambda)}.$$

TMC are eigenstates of the product of the annihilation operators of the two radiation modes $a_1 a_2 |\lambda\rangle\rangle = \lambda |\lambda\rangle\rangle$ and for this reason they are also referred to as pair-coherent states. The two partial traces

$$\rho_1 \equiv \mathrm{Tr}_2[|\lambda\rangle\rangle\langle\langle\lambda|] = \rho_2 \equiv \mathrm{Tr}_1[|\lambda\rangle\rangle\langle\langle\lambda|] = \frac{1}{I_0(2\lambda)} \sum_n \frac{\lambda^{2n}}{n!^2} |n\rangle\langle n|, \tag{6}$$

show sub-Poissonian photon statistics. In fact, the Mandel parameter $Q = \sigma^2/\langle n\rangle - 1$ is given by

$$Q_\lambda = \lambda \frac{I_0^2(2\lambda) - I_1^2(2\lambda)}{I_0(2\lambda) I_1(2\lambda)} - 1 \tag{7}$$

and it is negative for any value of λ.

A communication channel based on TMC relies on the strong photon number correlations, which allow to decode a random bit sequence by carrying out independent and simultaneous intensity measurements at two remote locations. On the other hand, the security of the scheme is based on checking the beam statistics coming from the measurement results against the (sub-Poissonian) expected one. It was shown that any realistic eavesdropping attempts introduce perturbations that are significant enough to be detected, thus making eavesdropping ineffective [18]. In addition, the extension to $M = 2^d$-letter alphabets was shown to be effective, i.e., increase the information capacity to d bits per measurements, also making the protocol more secure against intercept-resend attacks [29].

Another relevant class of PNES is given by the so-called twin-beam state (TWB)

$$|x\rangle\rangle = \sqrt{(1-x^2)} \sum_n x^n |n,n\rangle\rangle, \tag{8}$$

where $x \in \mathbb{C}$ and $0 \le |x| \le 1$, which are entangled two-mode Gaussian states of the field and represent the crucial ingredient for CV teleportation and dense coding. Without loss of generality we assume x as real; the average photon number of TWB is thus given by

$$N_x = \frac{2x^2}{1-x^2}.$$

The two partial traces of $|x\rangle\rangle$ are equal to thermal states $\nu_{N/2} = (1+N/2)^{-1}[N/(2+N)]^{a^\dagger a}$ with $N/2$ average photon number each. The Mandel parameter is positive and equal to $Q = N/2$ for both the modes. As we will see, also TWB may be employed to build a CV communication protocol analogous to that described above. The channel capacity is generally larger than for TMC, though the super-Poissonian statistics of the partial traces make the security issue more relevant.

In Fig. 1 we show the typical photon number distribution $|c_n|^2$ of TMC and TWB partial traces. We also report the degree of entanglement of the two states, evaluated as the Von Neumann (VN) entropy $S[\varrho] = -\mathrm{Tr}[\varrho \log \varrho]$ of the partial traces, i.e., $\epsilon = S[\varrho_1] = S[\varrho_2]$, as a function of the average photon number. Notice that TWBs show larger entanglement; indeed they are maximally entangled states for a CV two-mode system at fixed energy [33].

Classically correlated states

As already mentioned in the Introduction, the communication protocols expressed by Eqs. (3) and (4) may, in principle, be implemented also without entanglement, e.g., using mixed separable states of the form

$$R = \sum_{n=0}^{\infty} P_{nm} |n \times n| \otimes |m \times m|,$$

with any nonfactorized profile $P_{nm} \neq p_n p_m$, as, for example, $P_{nm} = \delta_{nm} |c_n|^2$, c_n being the amplitude of a PNES. This kind of classically correlated separable mixed states may have the necessary correlations to establish the channel but, on the other hand, have serious disadvantages compared to PNES in terms of security of the quantum channel. Thus in the following we will consider classically correlated states to assess the improvement of the channel capacity using PNES, however keeping in mind that any kind of classically correlated mixed state does not provide reliable security of the transmitted information.

As a paradigm of classically correlated state we consider the state obtained at the output of a balanced beam splitter fed by a thermal state (and with the second port unexcited).

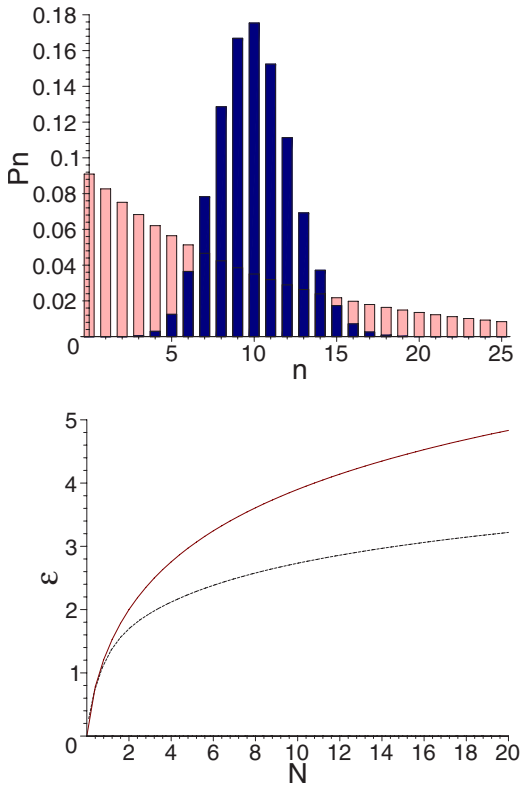

FIG. 1. (Color online) Top: Comparison between the mode photon number profiles $P_n \equiv |c_n|^2$ of TMC (dark gray) and TWB (light gray) with state average photon number $N=20$. Bottom: Entanglement (VN entropy of the partial traces) of TMC (lower, dotted line) and TWB (upper, solid line) states as a function of the state average photon number N.

This is a feasible class of states, which we refer to as two-mode thermal (TTH) states, that have been proved very effective to implement the so-called ghost imaging by classical means. In turn, this opened a debate about the usefulness of entanglement in protocols based on photon correlations [34,35]. As we will see, although TTH perform well in ghost imaging, PNES-based communication protocols achieve a larger channel capacity.

The density matrix of TTH is given by

$$R_H = U_{\pi/4} \nu_N \otimes |0\rangle\langle 0| U_{\pi/4}^{\dagger}, \tag{9}$$

where $U_{\pi/4}=\exp\{\pi/4(a^{\dagger}b+b^{\dagger}a)\}$ is the evolution operator of the balanced beam splitter and ν_N is a thermal state with N average photons. R_H is a mixed separable Gaussian state with correlation index given by $\gamma=N/(N+2)$. For large N the correlation index approaches one, in agreement with the strong correlations observed in ghost imaging experiments. The partial traces of R_H are both thermal states with $N/2$ average photons and Mandel parameter $Q=N/2$, whereas the two-mode photon distribution is given by [36]

$$P_H(p,q) = \frac{1}{1+N}\binom{p+q}{p}\left[\frac{N}{2(1+N)}\right]^{p+q}. \tag{10}$$

III. CORRELATED STATES IN A LOSSY CHANNEL

In order to assess the performances of our protocol in realistic conditions we investigate the propagation of the support states in lossy optical media, as the evolution in a fiber. We model the loss mechanism by the standard quantum optical Master equation, i.e., as the interaction with a bath of oscillators. We also assume that the noisy environment is acting independently on the two modes. At zero temperature the evolution of a two-mode state described by the density matrix R is given by

$$\dot{R} = (L[a_1] + L[a_2])R, \tag{11}$$

where dots denote time derivative and the Lindblad superoperator $L[a]$ acts as follows:

$$L[a]\varrho = \frac{\Gamma}{2}(2a\rho a^{+} - a^{+}a\rho - \rho a^{+}a). \tag{12}$$

Assuming that R_0 denotes the initial density matrix, the evolved state, i.e., the solution of the master equation (11), is given by

$$R_{\eta} = \sum_{n,k=0}^{\infty} A_n^{(1)} A_k^{(2)} R_0 A_k^{(2)\dagger} A_n^{(1)\dagger}, \tag{13}$$

where the elements of the maps are given by

$$A_n^{(j)} = \frac{(\eta_j^{-1}-1)^{n/2}}{\sqrt{n!}} a_j^n \eta_j^{(1/2)a_j^{\dagger}a_j}, \quad j=1,2, \tag{14}$$

and $\eta_j=\exp(-\Gamma_j t)$ will be referred to as the loss parameter. The evolution of TMC and TWB corresponds to the evolution of pure states of the form $R_0=|\psi_0\rangle\rangle\langle\langle\psi_0|$ with $|\psi_0\rangle\rangle$ being the PNES of Eq. (1). The joint photon number distribution after the propagation corresponds to the diagonal matrix elements of the evolved state $P_{\eta}(p,q)=\langle\langle p,q|R_{\eta}|p,q\rangle\rangle$. Assuming that the coefficients c_n in Eq. (1) are real and using Eqs. (13) and (14) we arrive at

$$P_{\eta}(p,q) = \sum_{n,k}\sum_{i,j} c_i c_j \langle p|A_n^{(1)}|i\rangle\langle q|A_k^{(2)}|i\rangle\langle j|A_n^{(1)\dagger}|p\rangle\langle j|A_k^{(2)\dagger}|q\rangle \tag{15}$$

with

$$\langle p|A_n^{(j)}|i\rangle = \frac{(\eta_j^{-1}-1)^{n/2}}{\sqrt{n!}} \eta_j^{(p+n)/2} \sqrt{\frac{(p+n)!}{p!}} \delta_{i,p+n} \tag{16}$$

and analogously for the other terms. Upon substituting in Eq. (15) the expression of the coefficients c_n for the TMC and TWB we obtain the output joint photon distributions

$$P_{\lambda,\eta_1,\eta_2}(p,q) = (I_0(2|\lambda|)p\,!\,q\,!)^{-1} I_{|p-q|}[2|\lambda|\sqrt{(1-\eta_1)(1-\eta_2)}] \times \lambda^{p+q}\eta_1^p\eta_2^q(1-\eta_1)^{(q-p)/2}(1-\eta_2)^{(p-q)/2}, \tag{17}$$

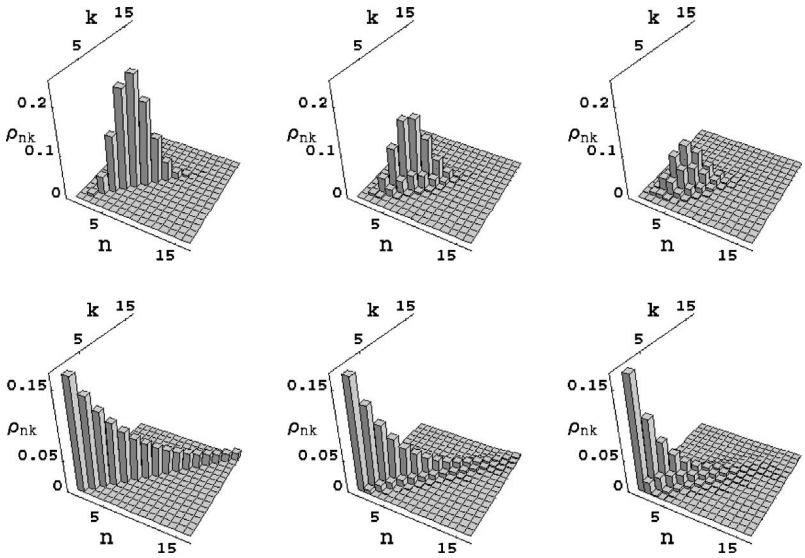

FIG. 2. Effect of losses on the joint photon-number distribution $P_\eta(p,q)$ of TMC and TWB with average photon number $N=10$. The plots on the top line refer to TMC and on the bottom line to TWB. From left to right the distributions for $\eta=1$ (no loss), $\eta=0.95$, and $\eta=0.85$.

$$P_{x,\eta_1,\eta_2}(p,q) = (1-x^2)\left(\frac{\eta_1}{1-\eta_1}\right)^p \left(\frac{\eta_2}{1-\eta_2}\right)^q \times [x^2(1-\eta_1)(1-\eta_2)]^M \binom{M}{m} {}_2F_1 \times [\{1+M,1+M\},\{1+d\};x^2(1-\eta_1)(1-\eta_2)], \tag{18}$$

where $d=|p-q|$, $M=\max(p,q)$, $m=\min(p,q)$, $I_d(x)$ is the dth modified Bessel function of the first kind, and ${}_2F_1[\{a,b\},\{c\};x]$ denotes a hypergeometric function. Equation (15) can be easily generalized to mixed input: For TTH states the evolution of the state R_H corresponds to a joint photon number distribution given by

$$P_{N,\eta_1,\eta_2}(p,q) = 2\eta_1^p \eta_2^q \frac{N^{p+q}}{[2+N(\eta_1+\eta_2)]^{p+q+1}} \binom{p+q}{p}. \tag{19}$$

The correlation index γ decreases with losses. Upon the evaluation of the first moments using Eqs. (17)–(19) we arrive at

$$\gamma_\lambda = \sqrt{\eta_1 \eta_2}, \tag{20}$$

$$\gamma_x = \frac{(2+N_x)\sqrt{\eta_1\eta_2}}{\sqrt{(2+N_x\eta_1)(2+N_x\eta_2)}}, \tag{21}$$

$$\gamma_\nu = \frac{N\sqrt{\eta_1\eta_2}}{\sqrt{(2+N\eta_1)(2+N\eta_2)}}. \tag{22}$$

For TMC the correlation index does not depend on the input energy. In Fig. 2 we show the joint photon-number distribution of TMC and TWB for different loss parameter and $N=10$. We also notice that the Mandel parameter of the partial traces shows a simple rescaling $Q_j \to \eta_j Q_j$ and thus the sub-Poissonian statistics of TMC and the super-Poissonian one of TWB are not altered by the propagation.

IV. OPTIMIZED BIT THRESHOLDS AND CHANNEL CAPACITIES

A. Symmetric channels

Once the joint probability distribution is known we may evaluate the mutual information between the two parties and optimize it against the threshold(s) for the different channels. Let us illustrate the procedure for the case of a binary alphabets assuming a symmetric lossy channel, i.e., $\eta_1=\eta_2=\eta$. The effects of asymmetry will be discussed in the next subsection. Upon adopting the decoding rule (3) the two parties infer the same symbol with probabilities

$$p_{00} = \sum_{p=0}^{T}\sum_{q=0}^{T} P_\eta(p,q), \tag{23}$$

$$p_{11} = \sum_{p=T}^{\infty}\sum_{q=T}^{\infty} P_\eta(p,q). \tag{24}$$

In the ideal case, i.e., with no losses, PNES-based protocols achieve $p_{00}+p_{11}=1$, due to perfect correlations between the two modes. On the other hand, if $\eta \neq 1$ the unwanted inference events "01" and "10" may occur with probabilities

$$p_{01} = \sum_{p=0}^{T}\sum_{q=T}^{\infty} P_\eta(p,q), \tag{25}$$

$$p_{10} = \sum_{p=T}^{\infty}\sum_{q=0}^{T} P_\eta(p,q). \tag{26}$$

The probabilities are not independent since the normalization condition $p_{00}+p_{10}+p_{01}+p_{11}=1$ holds. The mutual information between the two alphabets reads as follows:

$$I_2 = \sum_{i=0}^{1}\sum_{j=0}^{1} p_{ij} \log_2 \frac{p_{ij}}{q_i r_j}, \tag{27}$$

where

$$q_i = p_{i0} + p_{i1}, \quad i=0,1, \tag{28}$$

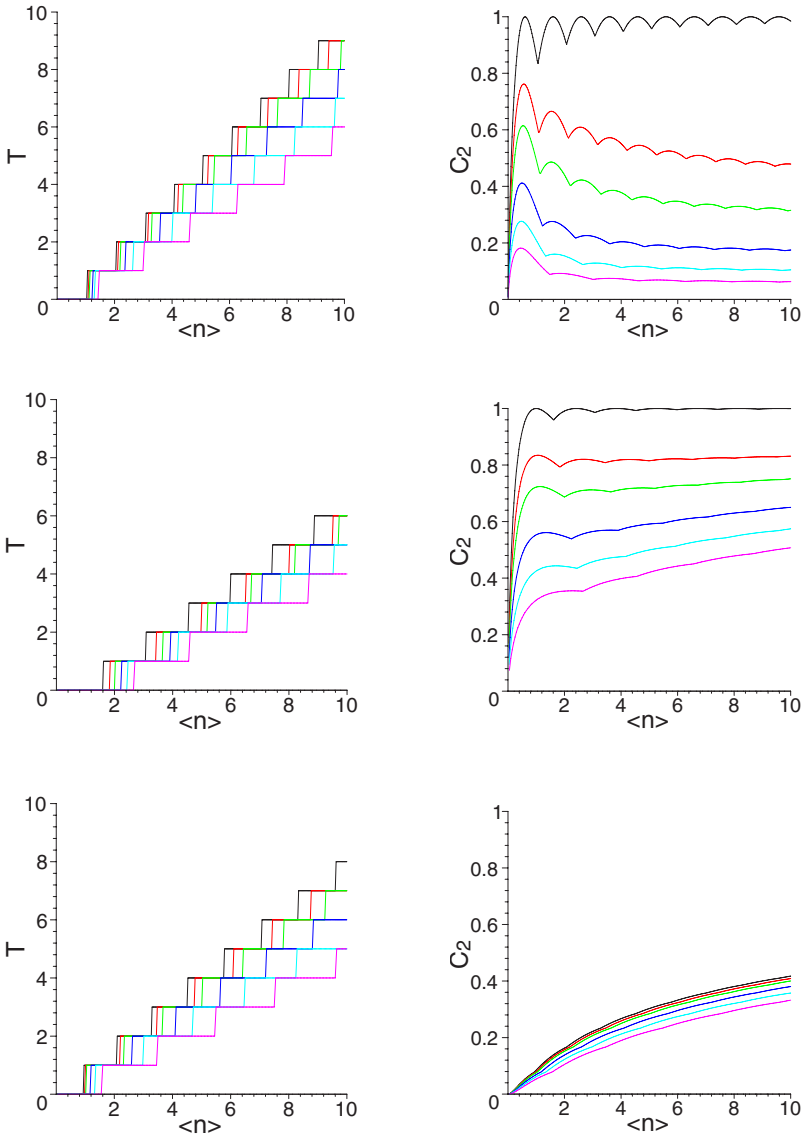

FIG. 3. (Color online) Optimized threshold (left) and channel capacity (right) for TMC-, TWB-, and TTH-based two-letter protocols as a function of the mode average photon number at the input and for different values of the loss parameter η (symmetric channels). In all the plots, from bottom to top: $\eta=0.6$, $\eta=0.7$, $\eta=0.8$, $\eta=0.9$, $\eta=0.95$, and $\eta=1$; the upper curves correspond to the ideal case with no losses.

$$r_j = p_{0j} + p_{1j}, \quad j = 0,1, \tag{29}$$

represents the marginal probabilities, i.e., the unconditional probabilities of inferring the symbol "i" ("j") for the first (second) party. The mutual information, once the average number of input photons and the loss parameter have been set, depends only on the threshold value T. The channel capacity $\mathcal{C}_2=\max_T I_2$ corresponds to the maximum of the mutual information over the threshold.

The mutual information has been maximized numerically by looking for the optimal bit discrimination threshold as a function of the input energy. The optimal thresholds and the corresponding channel capacities are shown in Fig. 3. Notice that the threshold for TMC only slightly increases with loss and it is always larger than the one for TWB. On the other hand, the threshold for TTH is smaller, and the resulting channel capacity is smaller than for PNES-based schemes as far as the loss is not too strong. At fixed energy the channel capacity is larger for TWB than for TMC. Notice that the capacity for a single-mode two-letter intensity modulation–direct detection (IMDD) channel is always smaller than $\mathcal{C}_2$ in the (relevant) low photon-number regime [37]. IMDD reaches the unity effectiveness for the mode average photon number $\langle n\rangle \approx 6$, giving just about 0.04 bits for $\langle n\rangle \approx 1$, while PNES schemes perform maximally already at $\langle n\rangle \approx 1$. Thus the PNES-based protocols are more convenient in terms of energy expenditure.

The channel capacity for a PNES based M-letter protocol may be analogously derived by maximizing the mutual information versus the $M-1$ bit thresholds. In the ideal case (no loss) the capacity obviously increases with M (as $\log_2 M$). A question arises on whether this effect is robust against losses. In Fig. 4 we report the rescaled capacity $\mathcal{C}_4/2$ as it results from the threshold optimization of the four-letter TMC-, TWB-, and TTH-based protocols, respectively. Besides the dubbing of the capacity due to the alphabet dimension, one can easily see that the four-letter protocol shows less oscillations in the low photon number regime (TMC and TWB) than the two-letter one for a large range of loss value, at the price of a slightly reduced capacity per letter. On the other hand, no appreciable improvement can be noticed for TTH states, thus confirming that photon-number correlations

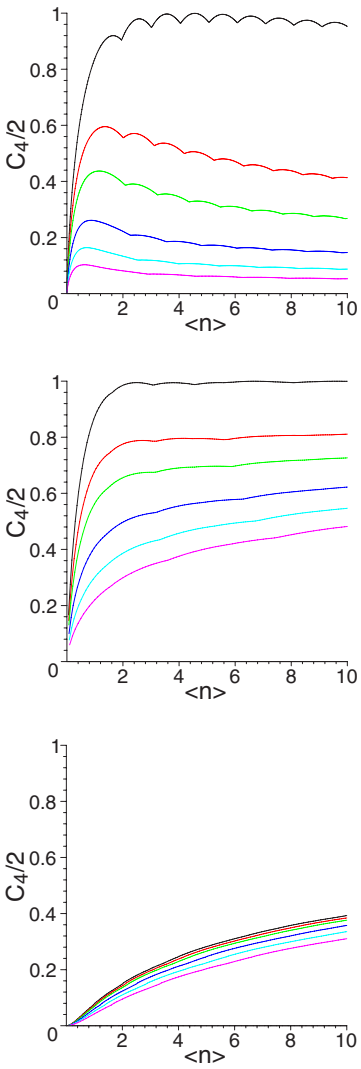

FIG. 4. (Color online) Optimized normalized channel capacity for TMC-, TWB-, and TTH-based four-letter protocols as a function of the mode average photon number at the input and for different values of the loss parameter η (symmetric channels). In all the plots, from bottom to top: $\eta=0.6$, $\eta=0.7$, $\eta=0.8$, $\eta=0.9$, $\eta=0.95$, and $\eta=1$; the upper curves correspond to the ideal case with no losses.

carried by PNES are more effective for quantum communication in lossy channel. We conclude that, thanks to their large stability, quaternary alphabets should be used in cases when the mean photon number of the support cannot be precisely fixed. In a four-letter protocol three thresholds should be used to extract the bit values. The optimization shows that for TWB and TTH states the distances between the three thresholds increase with the beam intensity whereas for TMC states there are three consecutive numbers for any value of the input energy. This behavior is due to the super-Poissonian photon-number distributions of TWB and TTH.

B. Asymmetric channels

In this section we analyze whether, and to what extent, different losses on the two beams affect the performances of the channel. In comparing symmetric to asymmetric channels we set the overall loss $\eta=\sqrt{\eta_1\eta_2}$ and the beam energy and evaluate the bit threshold and the channel capacity by varying the asymmetry, i.e., the loss of one channel, say η_1, in the range $\eta^2\leq\eta_1\leq 1$. This scheme corresponds to set the overall distance between the two parties and move the source of PNES from one ($\eta_1=1$) to the other ($\eta_1=\eta^2$). In Fig. 5 we show the channel capacities as a function of the single-channel loss η_1 for different values of the overall loss η and a fixed value of the input beam energy. At first we notice that asymmetry is not dramatically affecting the performances of the channels, especially for the case of small overall loss (i.e., for $\eta\rightarrow 1$). On the other hand, it is apparent from the plot that asymmetry acts in an opposite way on the TMC- and TWB-based protocols. In fact, the channel capacity increases with asymmetry for TMC and decreases for TWB. This behavior depends on the different correlation properties of TMC and TWB. On the one hand, the correlation index of TMC remains unchanged [compare to Eq. (20)] in asymmetric channels whereas that of TWB decreases. On the other hand, asymmetry acts in opposite ways on the probability of coincidence counts in the two channels. Upon expanding Eqs. (17) and (18) up to second order in the asymmetry we have

$$P_{\lambda,\eta_1,\eta_2}(n,n)=P_{\lambda,\eta,\eta}(n,n)+A_n(\eta,\lambda)\delta\eta^2, \tag{30}$$

$$P_{x,\eta_1,\eta_2}(n,n)=P_{x,\eta,\eta}(n,n)+B_n(\eta,x)\delta\eta^2, \tag{31}$$

where $\delta\eta=\eta_1-\eta_2$, $A>0\,\forall\,\eta,\lambda,n$, and $B<0\,\forall\,\eta,x,n$. Overall, placing the source of entanglement closer to one of the two parties results in a slight increase of the capacity for TMC and a slight decrease for TWB.

V. DISCUSSION AND CONCLUSIONS

A question arises on whether security may be proved for PNES based communication channels. In the ideal case of no loss, the intercept-resend strategy has been considered assuming that Eve is able to produce strongly correlated beams source (optimally the TMC source [29]) and it has been shown that the state-cloning attempts can be revealed by checking the beam statistics, which is modified from sub-Poissonian to super-Poissonian by any eavesdropping attempt. Since, as we have proved in this paper, the statistical properties are not changed by the propagation, TMC-based protocols are secure also in the presence of loss. As concern TWB, security, remarkably security against intercept-resend attacks, cannot be guaranteed through a check of the beam statistics. The TWB-based protocols require the use of additional degrees of freedom, as for example binary randomization of polarization [17] to guarantee security and to reveal eavesdropping actions. This may also be useful for TMC-based protocols, in order to achieve unconditional security. Overall, there is a trade-off between the quantity of information one is able to transmit at fixed energy and the security of this transmission, with TMC offering more security at the price of decreasing the channel capacity.

In conclusion, we have analyzed lossy communication channels based on photon number entangled states and real-

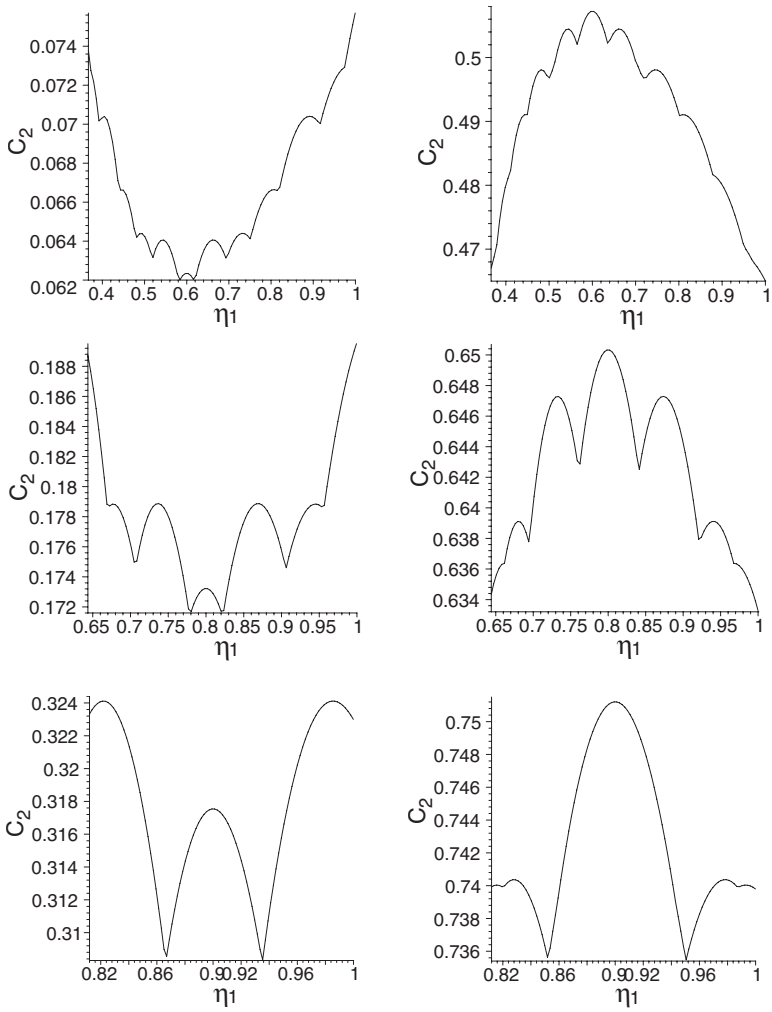

FIG. 5. Channel capacity for the TMC- (left) and TWB-based (right) two-letter CV coding in an asymmetric channel as a function of loss parameter in one of the channels. In all the plots the mode average photon number at the input is $\langle n \rangle = 10$. The overall channel loss is given, from left to right: $\eta=0.6$, $\eta=0.8$, and $\eta=0.9$.

ized upon choosing a shared set of thresholds to convert the outcome of a joint photon number measurement into a symbol from a binary or a quaternary alphabet. We have focused on channels built using two-mode coherently-correlated or twin-beam states a support. The explicit optimization of the bit discrimination thresholds have been performed and the corresponding channel capacities have been compared to that of channels built using classically correlated (separable) states. We found that PNES are useful to improve capacity in the presence of noise, and that TWB-based channels may transmit a larger amount of information than TMC-based ones at fixed energy and overall loss.

The evolution of the entangled support, either TMC or TWB, in lossy channels have been analyzed in detail, showing that the beam statistics, either sub-Poissonian for TMC or super-Poissonian for TWB, is not altered during propagation. The preservation of sub-Poissonian statistics indicates that TMC-based protocols are secure against intercept-resend eavesdropping attacks, whereas TWB-based protocols require the use of additional degrees of freedom, as for example binary randomization of polarization.

We have analyzed the effects of asymmetric losses on the two beams, showing that (i) asymmetry of the channel does not dramatically affect the performances and (ii) placing the source of entanglement closer to one of the two parties results in a slight increase of the capacity for TMC-based protocols and a slight decrease for TWB-based ones.

We conclude that photon-number entangled states, either Gaussian or non-Gaussian ones, are useful resources to implement effective quantum-enhanced communication channels in the presence of loss.

ACKNOWLEDGMENTS

This work has been supported by MIUR through the project PRIN-2005024254-002. The work of V.U. has been supported by the Landau Network through the Cariplo Foundation and by NATO through Grant No. CPB.NUKR.EV 982379.

[1] C. W. Helstrom, J. W. S. Liu, and J. P. Gordon, Proc. IEEE **58**, 1578 (1970).
[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] C. H. Bennett and G. Brassard, in Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[6] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, UK, 1995), pp. 816–827.
[7] T. Opatrný, G. Kurizki, and D.-G. Welsch, Phys. Rev. A **61**, 032302 (2000); M. Dakna, T. Anhut, T. Opatrny, L. Knoll, and D. G. Welsch, *ibid.* **55**, 3184 (1997); P. T. Cochrane, T. C. Ralph, and G. J. Milburn, *ibid.* **65**, 062306 (2002); S. Olivares, M. G. A. Paris, and R. Bonifacio, *ibid.* **67**, 032314 (2003).
[8] J. Wenger, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **92**, 153601 (2004); M. S. Kim, E. Park, P. L. Knight, and H. Jeong, Phys. Rev. A **71**, 043805 (2005); S. Olivares and M. G. A. Paris, J. Opt. B: Quantum Semiclassical Opt. **7**, S616 (2005); Phys. Rev. A **70**, 032112 (2004); J. Opt. B: Quantum Semiclassical Opt. **7**, S392 (2005); H. Nha and H. J. Carmichael, Phys. Rev. Lett. **93**, 020401 (2004); R. Garcíá-Patrón, J. Fiurášek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *ibid.* **93**, 130409 (2004); R. Garcíá-Patrón, J. Fiurášek, and N. J Cerf, Phys. Rev. A **71**, 022105 (2005); S. Daffer and P. L. Knight, *ibid.* **72**, 034101 (2005). C. Invernizzi, S. Olivares, M. G. A. Paris, and K. Banaszek, *ibid.* **72**, 042105 (2005).
[9] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2004).
[10] M. Hillery, Phys. Rev. A **61**, 022309 (1999).
[11] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[12] S. F. Pereira, Z. Y. Ou, and H. J. Kimble, Phys. Rev. A **62**, 042311 (2000).
[13] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).
[14] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[15] C. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[16] A. C. Funk and M. G. Raymer, Phys. Rev. A **65**, 042307 (2002).
[17] A. Porzio, V. D'Auria, P. Aniello, M. G. A. Paris, and S. Solimeno, Opt. Lasers Eng. **45**, 463 (2007).
[18] V. C. Usenko and C. V. Usenko, in *Quantum Communication, Measurement, and Computing*, edited by S. M. Barnett, E. Andersson, J. Jeffers, P. Ohberg, and O. Hirota, AIP Conf. Proc. No. 734 (AIP, Melville, NY, 2004), p. 319.
[19] A proof may be obtained under additional security amplification assumptions; see D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[20] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, e-print quant-ph/0611167.
[21] S. Y. Kilin and D. B. Horoshko, Phys. Rev. Lett. **74**, 5206 (1995); W. Leonski, S. Dyrting, and R. Tanas, J. Mod. Opt. **44**, 2105 (1997); A. Vidiella-Barranco and J. A. Roversi, Phys. Rev. A **58**, 3349 (1998); W. Leonski, *ibid.* **54**, 3369 (1999).
[22] M. G. A. Paris, Int. J. Mod. Phys. B **11**, 1913 (1997); M. Dakna, T. Anhut, T. Opatrny, L. Knoll, and D. G. Welsch, Phys. Rev. A **55**, 3184 (1997).
[23] K. Vogel, V. M. Akulin, and W. P. Schleich, Phys. Rev. Lett. **71**, 1816 (1993).
[24] G. M. D'Ariano, L. Maccone, M. G. A. Paris, and M. F. Sacchi, Phys. Rev. A **61**, 053817 (2000).
[25] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Heidelberg, 1995), pp. 146–157.
[26] J. Laurat, T. Coudreau, N. Treps, A. Maitre, and C. Fabre, Phys. Rev. Lett. **91**, 213601 (2003).
[27] O. Haderka, J. Perina, Jr., M. Hamar, and J. Perina, Phys. Rev. A **71**, 033815 (2005).
[28] K. Hayasaka, Y. Zhang, and K. Kasai, Opt. Lett. **29**, 1665 (2004).
[29] V. C. Usenko and B. I. Lev, Phys. Lett. A **348**, 17 (2005).
[30] Y. Zhang, K. Kasai, and K. Hayasaka, Opt. Express **11**, 3592 (2003).
[31] G. S. Agarwal, Phys. Rev. Lett. **57**, 827 (1986).
[32] G. S. Agarwal and A. Biswas, J. Opt. B: Quantum Semiclassical Opt. **7**, 350 (2005).
[33] M. G. A. Paris, Phys. Rev. A **59**, 1615 (1999).
[34] A. Gatti *et al.*, J. Mod. Opt. **53**, 739 (2006).
[35] M. Bache, D. Magatti, F. Ferri, A. Gatti, E. Brambilla, and L. A. Lugiato, Phys. Rev. A **73**, 053802 (2006).
[36] A. Agliati, M. Bondani, A. Andreoni, G. De Cillis, and M. G. A. Paris, J. Opt. B: Quantum Semiclassical Opt. **7**, 652 (2005).
[37] S. Olivares and M. G. A. Paris, J. Opt. B: Quantum Semiclassical Opt. **6**, 69 (2004).