PAPER • OPEN ACCESS

Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel

To cite this article: M N Notarnicola *et al* 2023 *New J. Phys.* **25** 103014

View the article online for updates and enhancements.

New Journal of Physics

The open access journal at the forefront of physics

PAPER

Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel

M N Notarnicola[1] ⬤, M Jarzyna[2,*] ⬤, S Olivares[1] ⬤ and K Banaszek[2,3] ⬤

[1] Dipartimento di Fisica 'Aldo Pontremoli', Università degli Studi di Milano and INFN Sezione di Milano, via Celoria 16, I-20133 Milano, Italy
[2] Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warszawa, Poland
[3] Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warszawa, Poland
[*] Author to whom any correspondence should be addressed.

E-mail: m.jarzyna@cent.uw.edu.pl

Keywords: continuous-variable quantum key distribution, quantum state discrimination, wiretap channels

Abstract

We address a continuous-variable quantum key distribution protocol employing quaternary phase-shift-keying of coherent states and a non-Gaussian measurement inspired by quantum receivers minimizing the error probability in a quantum-state-discrimination scenario. We consider a pure-loss quantum wiretap channel, in which a possible eavesdropper is limited to collect the sole channel losses. We perform a characterization of state-discrimination receivers and design an optimized receiver maximizing the asymptotic secure key rate (SKR), namely the key-rate optimized receiver (KOR), comparing its performance with respect to the pretty good measurement and the heterodyne-based protocol. We show that the KOR increases the SKR for metropolitan-network distances. Finally, we also investigate the implementations of feasible schemes, such as the displacement feed-forward receiver, obtaining an increase in the SKR in particular regimes.

1. Introduction

Quantum key distribution (QKD) is the art of sharing a secure key between two distant parties in the presence of an untrusted channel [1–4]. In a QKD scenario, a transmitter (Alice) sends quantum states through a quantum channel to a receiver (Bob), who performs a suitable measurement to extract a set of correlated data. The security of this scheme against any potential attack by an eavesdropper (Eve) is guaranteed by the laws of quantum mechanics [5, 6].

Within the field, continuous-variable QKD (CV-QKD) [7] is of particular interest due to its feasibility with the technologies commonly employed in optical communications [8]. Indeed, in CV-QKD information is encoded onto coherent states [9], that is, laser pulses, just as in classical communication systems. Several CV-QKD protocols have been proposed in literature, employing either Gaussian modulation of coherent states [10–14] or discrete modulation formats [15–26]. Nevertheless, all these schemes assume homodyne or heterodyne (equivalent to double homodyne) detection at Bob's side, and unconditional security proofs are currently established only for Gaussian measurements [27–29].

On the other hand, in many other frameworks non-Gaussian measurements often outperform Gaussian ones, and this makes it interesting to investigate their role also for CV-QKD. A relevant example is provided by quantum state discrimination theory, in which Alice encodes information onto non-orthogonal states and the task is to design an efficient receiver minimizing the error probability of Bob's decision [30–34]. This optimal receiver has been shown to be non-Gaussian, whereas Gaussian receivers are limited by the so-called shot noise limit (SNL) [32]. However, deriving the optimum measurement is rather cumbersome as it requires convex semidefinite programming [32, 35, 36]. As a consequence, there have also been developed suboptimal methods such as the pretty good measurement (PGM) method, which provides an upper bound to the minimum error probability and still beats the SNL [32, 37, 38]. Finally, feasible receivers have been

proposed for both binary [39–42] and quaternary [43–46] coherent-state discrimination, exploiting linear optics and photodetection, thus being easier to implement into practice. Beside quantum communications, in the existing literature state-discrimination receivers have also been investigated for CV-QKD [47].

In this paper, we propose a new quantum state-discrimination receiver for CV-QKD, namely, the key-rate optimized receiver (KOR). In more detail, we consider a CV-QKD protocol employing a quaternary phase-shift-keying (QPSK) modulation of coherent states [15, 19–23, 25] in which Bob implements the KOR rather than a Gaussian measurement. We compute the secure key rate (SKR), that is, the asymptotic length of the secret key per unit time slot, assuming a quantum wiretap channel [48–50], which represents a realistic paradigm for many different situations, e.g. free-space optical communications [51]. For the sake of simplicity, we consider a pure-loss channel, in order to deal with discrimination of pure states at Bob's side. This latter assumption depicts a simplified scenario, providing a cornerstone fostering more advanced developments. We design the KOR to maximize the SKR of the addressed protocol and compare it with the PGM, showing that both these non-Gaussian measurements improve the SKR in the metropolitan-network distance regime with respect to the heterodyne-based protocol. We also investigate the performance of some feasible quantum receivers, by considering the feed-forward displacement receiver proposed in [43].

The structure of the paper is the following. First, in section 2 we briefly outline the general structure of quantum state-discrimination receivers that will be employed throughout the work. Thereafter, section 3 presents the scheme of the protocol under investigation and describes the construction of the KOR. Then, in section 4 we compare the performance of the designed receiver with the same protocol employing heterodyne detection, whereas in section 5 we compute the SKR for the feed-forward displacement receiver. Finally, in section 6 we summarize the results and draw some conclusions and outlooks.

2. General structure of a state-discrimination receiver

In this paper, we investigate the potentiality of state-discrimination receivers for secure quantum communications and propose a new quantum receiver, the KOR, for CV-QKD protocols employing discrete modulation. To begin with, in this section, we present the general structure of a state-discrimination receiver within the framework of quantum state discrimination theory, or quantum decision theory [32–38].

Generally speaking, we have a source emitting M non-orthogonal linearly independent quantum states $\{|\gamma_k\rangle\}_k, k = 0, \ldots, M-1$, with *a priori* probabilities $q_k, 0 \leqslant q_k \leqslant 1$, and the task is to design a quantum receiver. That is, we look for a positive-operator-valued measure (POVM) $\{\Pi_j\}_j, j = 0, \ldots, M-1, \Pi_j \geqslant 0$ and $\sum_j \Pi_j = \hat{\mathbb{1}}, \hat{\mathbb{1}}$ being the identity operator over the whole Hilbert space, such that registering the outcome j infers the state generated by the source to be $|\gamma_j\rangle$. When the outcome j is obtained, we underline that the receiver makes the decision j even if the state $k \neq j$ was sent, resulting in a decision error.

For the decision between pure states, the Kennedy theorem [32, 39] proves an optimum POVM to be 1-rank, namely, $\Pi_j = |\mu_j\rangle\langle\mu_j|$, expressed in terms of a set of measurement vectors $\{|\mu_j\rangle\}_j$. As a consequence, the problem may be recast into a geometric optimization task. Indeed, we introduce the state and measurement (row) matrices

$$\Gamma = (|\gamma_0\rangle, \ldots, |\gamma_{M-1}\rangle) \quad \text{and} \quad \mathbb{M} = (|\mu_0\rangle, \ldots, |\mu_{M-1}\rangle), \tag{1}$$

respectively. Moreover, it is not restrictive to reduce the problem to the M dimensional subspace spanned by the encoded states, $\mathcal{S} = \text{span}\{|\gamma_k\rangle : k = 0, \ldots, M-1\}$ [32, 52]. Accordingly, the measurement vectors are expressible as a linear combination of the state vectors, $|\mu_j\rangle = \sum_k a_{kj}|\gamma_k\rangle, a_{kj} \in \mathbb{C}$, or equivalently,

$$\mathbb{M} = \Gamma A, \tag{2}$$

with A being an $M \times M$ matrix with coefficients $(a_{kj})_{k,j}$. The identity resolution constraint now becomes $\sum_j \Pi_j = \mathbb{P}_{\mathcal{S}}, \mathbb{P}_{\mathcal{S}}$ being the projection operator onto subspace $\mathcal{S}$.

In turn, the conditional probability of obtaining outcome j if the kth state is probed is given by

$$p(j|k) = \text{Tr}\left[|\gamma_k\rangle\langle\gamma_k|\Pi_j\right] = |B_{kj}|^2, \tag{3}$$

where

$$B = \mathbb{M}^\dagger \Gamma = A^\dagger G, \tag{4}$$

G being the $M \times M$ Gram matrix:

$$G = \Gamma^\dagger \Gamma = (\langle\gamma_l|\gamma_k\rangle)_{l,k=0,\ldots,M-1}, \tag{5}$$

that is the matrix of the overlaps between the encoded states. Thus, a quantum receiver is completely characterized by its corresponding matrix A, subject to the constraint

$$AA^\dagger = G^{-1},\tag{6}$$

guaranteeing the identity resolution of the resulting POVM, as derived in appendix A.

The scenario may be further simplified if the constellation of states $\{|\gamma_k\rangle\}_k$ exhibits the geometric uniform symmetry (GUS) [32], namely if there exists a symmetry operator S such that

$$|\gamma_k\rangle = S^k |\gamma_0\rangle \quad \text{and} \quad S^M = \hat{\mathbb{1}}, \qquad (k = 0,\dots,M-1).\tag{7}$$

In this case, we may safely assume also the measurement vectors to exhibit the GUS for the same operator S, thus the POVM $\{\Pi_j\}_j$ is identified by a single 'reference' measurement vector

$$|\mu_0\rangle = \sum_{k=0}^{M-1} a_{k0} |\gamma_k\rangle,\tag{8}$$

$a_{k0} \in \mathbb{C}$, while all the others will be retrieved as $|\mu_j\rangle = S^j|\mu_0\rangle, j = 0,\dots,M-1$. Consequently, A is a circulant matrix, having the form

$$A = \begin{pmatrix} a_{00} & a_{M-10} & \dots & a_{10} \\ a_{10} & a_{00} & \dots & a_{20} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M-10} & a_{M-20} & \dots & a_{00} \end{pmatrix},\tag{9}$$

which is diagonalizable by the unitary matrix $U = \mathbb{F}^{-1}$, $\mathbb{F} = (e^{-i2\pi jk/M}/\sqrt{M})_{jk}, j,k = 0,\dots,M-1$, being the discrete Fourier transform matrix [53]. Its eigendecomposition is given by $A = U\Lambda U^\dagger$, where $\Lambda = \text{diag}(\lambda_0,\dots,\lambda_{M-1})$, is the diagonal matrix composed of the eigenvalues $\{\lambda_j\}_j$ of A. Furthermore, circulant matrices form a commutative algebra [53], thus $A^\dagger$ is also circulant and $[A,A^\dagger] = 0$. Thereby, $A^\dagger = U\Lambda^\dagger U^\dagger$ and equation (6) becomes:

$$U|\Lambda|^2 U^\dagger = G^{-1},\tag{10}$$

where $|\Lambda|^2 = \text{diag}(|\lambda_0|^2,\dots,|\lambda_{M-1}|^2)$. We conclude that A and G^{-1} are simultaneously diagonalizable and $|\lambda_j|^2 = g_j^{-1}$, $\{g_j\}_j$ being the eigenvalues of the Gram matrix (5) listed in increasing order, that is, $g_0 \geqslant g_1 \geqslant \dots \geqslant g_{M-1}$. In conclusion, the matrix A may be re-expressed in the following form:

$$A \equiv A_\phi = U\Lambda_\phi U^\dagger,\tag{11}$$

where

$$\Lambda_\phi = \text{diag}\left(\left\{\lambda_j^{(\phi)}\right\}_{j=0,\dots,M-1}\right),\tag{12}$$

and

$$\lambda_j^{(\phi)} = e^{i\phi_j} g_j^{-1/2},\tag{13}$$

in which the relative phases $\phi = (\phi_0,\dots,\phi_{M-1})$ provide the only free parameters. Furthermore, the matrix A_ϕ is defined up to an overall phase due to (2), therefore we may fix $\phi_0 = 0$, ending up with $M-1$ phases whose value can be arbitrarily chosen.

We conclude that, in the presence of GUS, every quantum receiver is ultimately identified by the set of phases ϕ, which may be properly chosen to optimize a desired figure of merit, according to the context under investigation. In the existing literature, the typical figure of merit of quantum discrimination theory is the error probability

$$P_{\text{err}} = 1 - \sum_{k=0}^{M-1} q_k p(k|k),\tag{14}$$

representing the probability of inferring a symbol $j \neq k$ if the kth state is sent. In this case, the optimal matrix A minimizing (14) may be retrieved via convex semidefinite programming [32, 35, 36]. Alternatively, simpler

suboptimal schemes have been proposed, providing an upper bound of the minimum error probability. The most relevant is the PGM method [32, 37, 38], leading to a suboptimal POVM which coincides with the optimal measurement for constellations exhibiting GUS [32]. The matrix A for the PGM reads:

$$A_{\mathrm{PGM}} = G^{-1/2}, \tag{15}$$

which may be retrieved from (11) by setting all phases to zero, $\phi = (0, \dots, 0)$.

In the following section, we discuss a different approach and adopt a quantum receiver described by (11) to maximize the SKR of the four-state CV-QKD protocol, optimizing the free phases to design the optimized discrete receiver for CV-QKD, namely, the KOR.

3. CV-QKD with state-discrimination receivers over a wiretap channel

As mentioned in the previous section, we design the KOR to optimize the SKR of the four-state protocol depicted in figure 1, in which the sender, Alice, employs the QPSK modulation. The latter is a special case of phase-shift keying (PSK) modulation in which information is encoded in one of M coherent states

$$|\alpha_k\rangle = |\alpha\, e^{i\pi\,(2k+1)/M}\rangle, \qquad (k = 0, \dots, M-1), \tag{16}$$

where $\alpha \geqslant 0$, generated with equal *a priori* probabilities $q_k = 1/M$. That is, the PSK constellation is composed of M coherent states with the same energy α^2 and phase-shifted by $\theta = 2\pi/M$; therefore, it satisfies the GUS for the phase-shift symmetry operator $S_\theta = \exp(-i\theta\,\hat{n})$, $\hat{n}$ being the photon-number quantum operator [32]. The QPSK is a special case of PSK with $M = 4$.

After the modulation stage, Alice injects the signals into an untrusted quantum channel and the receiver, Bob, probes the received pulses via a state-discrimination receiver, namely, a finite-valued POVM $\{\Pi_j\}_j$ with the properties described in section 2. However, already existing protocols [10–15, 17–19, 22] usually assume Gaussian POVMs at the receiver, either homodyne or heterodyne detection, and unconditional security proofs are guaranteed only for Gaussian measurements [27–29]. In fact, under the unconditional security paradigm, one considers the most powerful eavesdropping attack, where an eavesdropper, Eve, performs any arbitrary channel manipulation that preserves the local statistics at Alice's and Bob's sides. Physical layer security is then addressed via a constrained functional optimization over all possible channels, leading to the Devetak–Winter (DW) bound [54]. This task has been obtained for protocols employing Gaussian measurements under the assumption of either a linear [15] or nonlinear channel [19], thanks to the optimality of Gaussian attacks [27–29]. Recently, a tight lower bound to the DW bound has also been obtained via nonlinear convex optimization algorithms and without invoking Gaussian optimality [20].
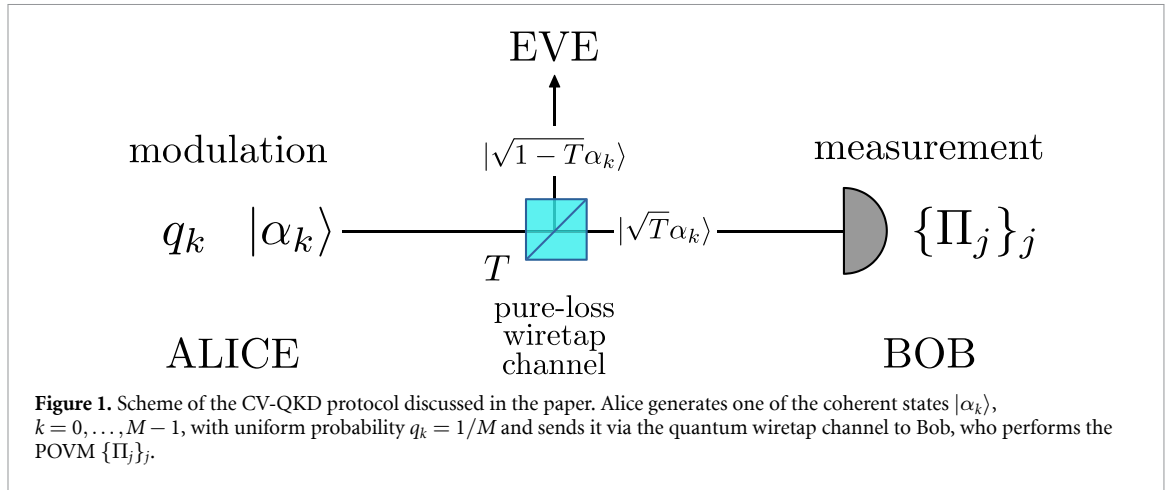
Nevertheless, in practical scenarios it is justified to address physical layer security under a wider set of assumptions, including restricted eavesdropping [50] and different trust levels of the infrastructure [55], computing the SKR under the so-called composable security paradigm. For instance, in a typical satellite QKD attack, Eve intercepts a part of the signal not being captured by Bob's telescope [56]. Similarly, in the fiber based protocols we may assume an attack to be performed without breaking the structure of the fiber to implement arbitrary signal manipulation. In the recent literature, secure key distillation in these practical conditions is gaining much interest, with particular reference to wiretap channels [50] modeling the previous realistic assumptions, and passive eavesdropping [57, 58], which have also been tested experimentally [59].

Given the present scenario, CV-QKD with non-Gaussian measurements still remains an open problem since the Gaussian optimality theorem does not hold anymore, and the DW bound can only be directly evaluated with the advanced methods presented in [20]. In light of this, here we start from scratch and address composable security, by considering a quantum wiretap channel [48–50]. In this scenario, we consider a restricted eavesdropping strategy where Eve may only collect the lost fraction of the encoded signals without performing arbitrary channel manipulation. Once again, we remark that this represents a realistic scenario which is worth of interest for practical conditions, but does not guarantee unconditional security. In turn, the purpose of our research is to show that, in particular conditions, it is possible to theoretically design a suitable measurement outperforming the conventional quadrature detection schemes.

Moreover, we also perform a further assumption and consider a pure-loss channel, described as a beam splitter with transmissivity

$$T = 10^{-\kappa d/10}, \tag{17}$$

d being the transmission distance (expressed in km) and $\kappa = 0.2\,\mathrm{dB\,km^{-1}}$ is the loss rate of common fibers at telecom wavelength [60–64]. This case is worth of investigation for a twofold reason. At first, in the recent literature there has been a revived interest in passive eavesdropping strategies [51, 57, 58, 65–67]. Secondly,

Figure 1. Scheme of the CV-QKD protocol discussed in the paper. Alice generates one of the coherent states $|\alpha_k\rangle$, $k = 0, \ldots, M - 1$, with uniform probability $q_k = 1/M$ and sends it via the quantum wiretap channel to Bob, who performs the POVM $\{\Pi_j\}_j$.

passive eavesdropping can be used as the first stepping stone to identify scenarios where a potential advantage of quantum receivers may be substantial, even in the possible presence of nonzero excess noise.

Provided these two assumptions, in the following we construct the optimized POVM that describes the KOR, and show it to bring advantages in some particular regimes.

In the presence of a pure-loss quantum wiretap channel, if Alice generates the state $|\alpha_k\rangle$, the transmitted fraction $|\alpha_k^{(t)}\rangle = |\sqrt{T}\alpha_k\rangle$ reaches Bob, whereas Eve receives the reflected part $|\alpha_k^{(r)}\rangle = |\sqrt{1-T}\alpha_k\rangle$, as shown in figure 1. Accordingly, the dimensional reduction holds [32, 52], and we restrict our attention to the M-dimensional subspace spanned by the transmitted pulses, namely, $\mathcal{S} = \text{span}\{|\alpha_k^{(t)}\rangle : k = 0, \ldots, M - 1\}$ and apply the results of section 2.

To form a truly identity-resolving set, the POVM elements $\{\Pi_j\}_j$, $j = 0, \ldots, M - 1$, shall be complemented with an $(M + 1)$th inconclusive element $\Pi_M = \hat{\mathbb{1}} - \mathbb{P}_\mathcal{S}$, $\mathbb{P}_\mathcal{S}$ being the projection operator onto $\mathcal{S}$. For the case under investigation, Π_M is irrelevant, and we will neglect it in the following. However, this would not be true anymore in the presence of a channel excess noise; thus, registering a zero probability for this additional outcome may provide a useful way to check the reasonableness of the pure-loss hypothesis in a realistic implementation of the proposed protocol.

3.1. Construction of the KOR

In our protocol Bob shall employ an optimized POVM to perform discrimination among the transmitted pulses, described by the state vector $\Gamma = (|\alpha_0^{(t)}\rangle, \ldots, |\alpha_{M-1}^{(t)}\rangle)$ and the Gram matrix:

$$G = \left(\langle \alpha_l^{(t)} | \alpha_k^{(t)} \rangle \right)_{l,k=0,\ldots,M-1}, \tag{18}$$

in which the overlap $G_{lk} = \langle \alpha_l^{(t)} | \alpha_k^{(t)} \rangle$ reads [68]:

$$G_{lk} = \exp\left\{ -\frac{1}{2} \left| \alpha_k^{(t)} - \alpha_l^{(t)} \right|^2 + \frac{1}{2} \left[\alpha_k^{(t)} \left(\alpha_l^{(t)} \right)^* - \left(\alpha_k^{(t)} \right)^* \alpha_l^{(t)} \right] \right\}$$

$$= \exp\left(-T\alpha^2 \left\{ 1 - \cos\left[\frac{2\pi}{M}(k - l) \right] \right\} + \mathrm{i}\, T\alpha^2 \sin\left[\frac{2\pi}{M}(k - l) \right] \right). \tag{19}$$

The constellation of transmitted pulses maintains the GUS for the phase-shift operator S_θ, thus the set of measurement vectors $\mathbb{M} = \{|\mu_j\rangle\}_j$, $j = 0, \ldots, M - 1$, also satisfies the GUS, and the corresponding matrix A is in the form (11), according to the results of section 2. The KOR is obtained by optimizing the phases ϕ to maximize the SKR, and is described by the optimized 'reference' measurement vector:

$$|\mu_0^{(\phi)}\rangle = \sum_{k=0}^{M-1} (A_\phi)_{k0} \left| \alpha_k^{(t)} \right\rangle \tag{20}$$

$$= \mathrm{e}^{-T\alpha^2/2} \sum_{n=0}^{\infty} \frac{\left(\sqrt{T}\alpha_0 \right)^n}{\sqrt{n!}} \lambda_{(n-1) \bmod M}^{(\phi)} |n\rangle, \tag{21}$$

where $a \bmod b$ is the modulo operation, returning the reminder of the division a/b, $a, b \in \mathbb{Z}$, and $\{|n\rangle\}_n$ is the photon-number basis.

Given the previous considerations, we compute the SKR of the discussed protocol, considering a reverse reconciliation scenario, which guarantees higher security in many existing protocols [10–12]. Moreover, for the sake of simplicity, we perform the asymptotic key-rate calculation, where the channel parameters are known with no uncertainty. Under this paradigm, for a generic state-discrimination receiver described by the phase vector ϕ, the SKR reads:

$$K\left(\phi,\alpha^2\right) = \beta I_{AB}\left(\phi,\alpha^2\right) - \chi_{BE}\left(\phi,\alpha^2\right), \tag{22}$$

where I_{AB} and χ_{BE} are the mutual information between Alice and Bob and the Holevo information [69] between Bob and Eve, respectively, and $\beta \leqslant 1$ is the reconciliation efficiency [15, 17].

The mutual information reads:

$$I_{AB}\left(\phi,\alpha^2\right) = H\left[p_B^{(\phi)}(j)\right] - \frac{1}{M}\sum_{k=0}^{M-1} H\left[p_{B|\alpha_k}^{(\phi)}(j)\right], \tag{23}$$

where

$$p_{B|\alpha_k}^{(\phi)}(j) = \left\langle \sqrt{T}\alpha_k \left| \Pi_j \right| \sqrt{T}\alpha_k \right\rangle = \left| \left(A_\phi^\dagger G\right)_{kj} \right|^2, \tag{24}$$

G being the Gram matrix (18), and

$$p_B^{(\phi)}(j) = \frac{1}{M}\sum_{k=0}^{M-1} p_{B|\alpha_k}^{(\phi)}(j), \tag{25}$$

are the conditional and overall probabilities of Bob's detection associated with outcome $j = 0, \ldots, M-1$, respectively, and $H[p(x)] = -\sum_x p(x)\log_2 p(x)$ is the Shannon entropy of the probability distribution $p(x)$.

To compute the Holevo information shared between Bob and Eve, that is the maximum amount of information accessible to Eve, we approach the problem in the prepare-&-measure picture [7, 10, 11] and obtain:

$$\chi_{BE}\left(\phi,\alpha^2\right) = S[\rho_E] - \sum_{j=0}^{M-1} p_B^{(\phi)}(j)\, S\left[\rho_{E|j}^{(\phi)}\right], \tag{26}$$

where $\rho_{E|j}^{(\phi)}$ and ρ_E are the conditional and overall Eve's state, respectively, $p_B^{(\phi)}(j)$ is Bob's probability distribution (25) and $S[\rho] = -\mathrm{Tr}[\rho\log_2\rho]$ represents the von Neumann entropy associated with state ρ. These two states may be retrieved from the joint state of Bob and Eve after the channel, that is:

$$\begin{aligned}
\rho_{BE} &= U_{BS}(T)\,\rho_A \otimes |0\rangle\langle 0|\, U_{BS}(T)^\dagger \\
&= \frac{1}{M}\sum_{k=0}^{M-1} \left|\alpha_k^{(t)}\right\rangle\left\langle\alpha_k^{(t)}\right| \otimes \left|\alpha_k^{(r)}\right\rangle\left\langle\alpha_k^{(r)}\right|,
\end{aligned} \tag{27}$$

where $\rho_A = \sum_k q_k |\alpha_k\rangle\langle\alpha_k|$ is Alice's overall state, $|0\rangle$ is the vacuum state and $U_{BS}(T)$ is unitary operator associated with a beam splitter with transmissivity T [9], as displayed in figure 1. In turn, we have:

$$\rho_E = \mathrm{Tr}_B[\rho_{BE}] = \frac{1}{M}\sum_{k=0}^{M-1} \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|, \tag{28}$$

and

$$\begin{aligned}
\rho_{E|j}^{(\phi)} &= \frac{1}{p_B^{(\phi)}(j)}\mathrm{Tr}_B\left[\rho_{BE}\,\Pi_j \otimes \hat{\mathbb{1}}_E\right] \\
&= \frac{1}{M p_B^{(\phi)}(j)}\sum_{k=0}^{M-1} p_{B|\alpha_k}^{(\phi)}(j)\left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|,
\end{aligned} \tag{29}$$

Tr_B being the partial trace over Bob's mode and $\hat{\mathbb{1}}_E$ being the identity operator over Eve's mode. Finally, the von Neumann entropy of states (28) and (29) may be computed with the methods outlined in appendix B.

In our analysis, we are interested in the maximum achievable SKR as a function of the transmission distance d, therefore, in the end we will perform optimization over the free parameters, namely the phases ϕ and the constellation energy α^2. The final, optimized, SKR is therefore equal to

$$K_{\text{KOR}} = \max_{\phi, \alpha^2} K\left(\phi, \alpha^2\right), \tag{30}$$

with the optimized phases and modulation energy denoted by $\phi_{\text{KOR}} = (0, \phi_1^{(\text{KOR})}, \ldots, \phi_{M-1}^{(\text{KOR})})$ and α^2_{KOR}. As a consequence, we define the KOR via equation (11), as the quantum receiver associated with the optimized phase vector ϕ_{KOR}. Furthermore, we compare the performance of the KOR with that associated with the PGM, for which the optimized SKR reads:

$$K_{\text{PGM}} = \max_{\alpha^2} K\left(\phi = \mathbf{0}, \alpha^2\right), \tag{31}$$

with zero phases and the optimized energy α^2_{PGM}. The results obtained for the above two receivers are discussed in the following section, where we compare both SKRs with the key rate of the heterodyne-based protocol in order to highlight the advantages brought by the two non-Gaussian measurements.

The heterodyne-based protocol is analogous to the one discussed above and employs double homodyne detection at Bob's side, that is, a measurement of both field quadratures q and p, retrieving a pair of real outcomes $\mathbf{x} = (x_B, y_B) \in \mathbb{R}^2$. We underline that, while both the KOR and the PGM are described in terms of a finite-valued POVM with M possible outcomes, in the presence of heterodyne detection we have a continuous-variable measurement. Therefore, in this case Bob's conditional probability reads:

$$p_{B|\alpha_k}^{(\text{het})}(\mathbf{x}) = \frac{1}{4\pi\sigma_0^2} \exp\left\{-\left[x_B - 2\sigma_0\sqrt{T}\text{Re}\left(\alpha_k\right)\right]^2 / \left(4\sigma_0^2\right)\right\}$$
$$\times \exp\left\{-\left[y_B - 2\sigma_0\sqrt{T}\text{Im}\left(\alpha_k\right)\right]^2 / \left(4\sigma_0^2\right)\right\}, \tag{32}$$

σ_0^2 being the shot-noise variance [9], which from now on will be taken equal to 1, meaning, we perform calculations in shot-noise units (SNU). The obtained mutual information is, similarly as in (23), given by:

$$I_{AB}^{(\text{het})}\left(\alpha^2\right) = H\left[p_B^{(\text{het})}(\mathbf{x})\right] - \frac{1}{M}\sum_{k=0}^{M-1} H\left[p_{B|\alpha_k}^{(\text{het})}(\mathbf{x})\right], \tag{33}$$

with $p_B^{(\text{het})}(\mathbf{x}) = M^{-1}\sum_k p_{B|\alpha_k}^{(\text{het})}(\mathbf{x})$. Instead, the Holevo information becomes:

$$\chi_{BE}\left(\alpha^2\right) = S\left[\rho_E\right] - \int_{\mathbb{R}^2} \mathrm{d}^2\mathbf{x}\, p_{B|\alpha_k}^{(\text{het})}(\mathbf{x})\, S\left[\rho_{E|\mathbf{x}}\right], \tag{34}$$

with ρ_E given in (28) and

$$\rho_{E|\mathbf{x}} = \frac{1}{Mp_B^{(\text{het})}(\mathbf{x})} \sum_{k=0}^{M-1} p_{B|\alpha_k}^{(\text{het})}(\mathbf{x}) \left|\sqrt{1-T}\alpha_k\right\rangle\left\langle\sqrt{1-T}\alpha_k\right|. \tag{35}$$

The integration in (34) can been performed numerically by exploiting the Simpson's rule [70]. Finally, the resulting SKR is obtained as

$$K_{\text{het}} = \max_{\alpha^2}\left[\beta I_{AB}^{(\text{het})}\left(\alpha^2\right) - \chi_{BE}^{(\text{het})}\left(\alpha^2\right)\right], \tag{36}$$

with the optimized modulation energy α^2_{het}.

As a final remark, towards a realistic implementation of the present protocol, we underline that both the KOR and the PGM may not represent appropriate POVMs for the channel evaluation stage. Indeed, assuming that the channel properties do not change, Alice and Bob must estimate the channel parameters, which in the present case is limited to the sole transmissivity T. However, unlike homodyne and heterodyne detection, in principle the designed POVM $\{\Pi_j\}_j$ does not guarantee full channel characterization. This problem may be circumvented, at least for the asymptotic key rate calculation, by performing Gaussian detection on a small fraction of the exchanged pulses and reserving it for the channel estimation stage, whilst exploiting the non-Gaussian receiver only for the key extraction. On the contrary, in the presence of a finite-size scenario, Alice and Bob estimate the channel transmissivity T with a finite uncertainty ΔT, thus leaving more space for Eve's intervention. Therefore, they employ a conservative strategy and compute the

SKR by considering a lower value of the transmissivity, namely $T - \Delta T$. However, the main effect of this lower effective transmissivity is to reduce the range of distances for which the state-discrimination receivers outperforms the heterodyne protocol. Furthermore, the dataset for the key extraction is also finite, resulting in a lower SKR with respect to the asymptotic case.

4. Results

In this section, we compare the results derived previously. In figure 2(a) we plot the SKRs (30), (31) and (36) as a function of the transmission distance d, expressed in km. The reconciliation efficiency is fixed to $\beta = 0.95$ [22, 61, 62]. It can be seen in the plot that both PGM and KOR beat the heterodyne-based protocol, that is $K_{\mathrm{p}} \geqslant K_{\mathrm{het}}$, p = PGM, KOR. The improvement in the SKR is more relevant for metropolitan-network distances, in particular for $d \leqslant 100\,\mathrm{km}$, whereas for larger ones both K_{KOR} and K_{PGM} approach K_{het} and achieve the same asymptotic scaling. To quantify this improvement we compute the ratio

$$\mathcal{R}_{\mathrm{p}} = \frac{K_{\mathrm{p}}}{K_{\mathrm{het}}}, \qquad (\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}), \tag{37}$$

reported in figure 2(b). Both the ratios exhibit peaks for $d \leqslant 40\,\mathrm{km}$ and then decrease towards 1 in the long-distance regime, but the behaviour is rather different between the two cases. In fact, $\mathcal{R}_{\mathrm{PGM}}$ achieves a single maximum at $\approx 5\,\mathrm{km}$, increasing the SKR with respect to K_{het} by more than 42%, and then decays monotonously to 1. On the contrary, K_{KOR} is not a monotonic function of the transmission distance and, in turn, the associated ratio exhibits two separated peaks. The KOR coincides with the PGM up to its first maximum, that is $\mathcal{R}_{\mathrm{KOR}} = \mathcal{R}_{\mathrm{PGM}}$ for $d \lesssim 7\,\mathrm{km}$, while for larger d we have $\mathcal{R}_{\mathrm{KOR}} \geqslant \mathcal{R}_{\mathrm{PGM}}$. Thereafter, $\mathcal{R}_{\mathrm{KOR}}$ reaches a local minimum and then achieves a second maximum at $\approx 23\,\mathrm{km}$, with $\approx 47\%$ increase in the SKR. Ultimately, the curve decreases to 1, approaching the heterodyne-based protocol together with $\mathcal{R}_{\mathrm{PGM}}$.
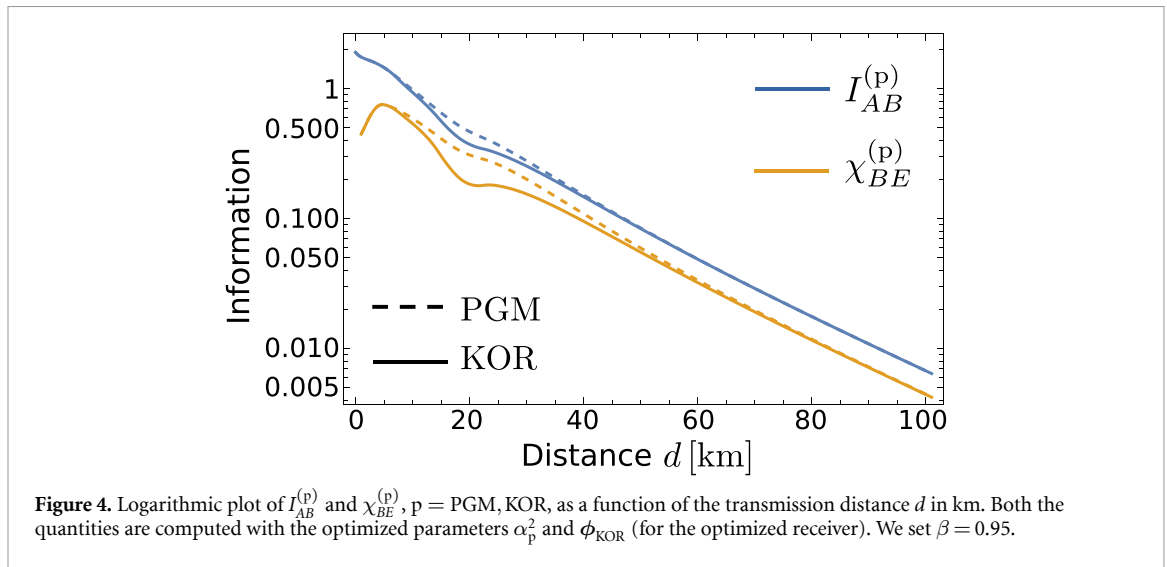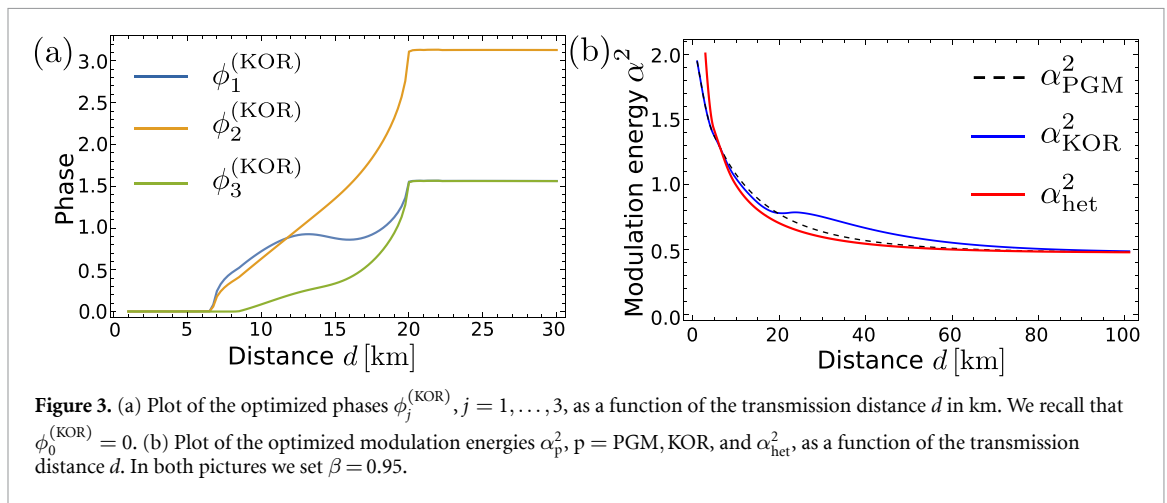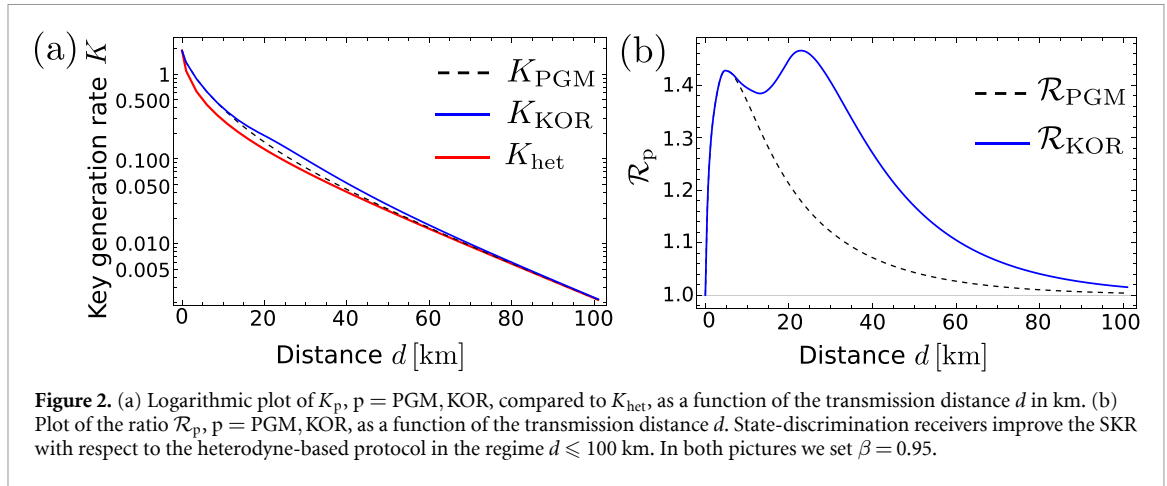
The behavior of K_{KOR} is a consequence of the resulting optimized phases $\phi_j^{(\mathrm{KOR})}$, depicted in figure 3(a). We recall that $\phi_0^{(\mathrm{KOR})} = 0$ by definition. For $d \lesssim 7\,\mathrm{km}$ we have $\phi_{\mathrm{KOR}} = \mathbf{0}$ and the optimized receiver is identical to the PGM, whereas for larger distances the optimized phases are nonzero and $\mathcal{R}_{\mathrm{KOR}} \geqslant \mathcal{R}_{\mathrm{PGM}}$. Interestingly, for $d \gtrsim 20\,\mathrm{km}$ the optimized phase tuple becomes distance-independent and reads $\phi_{\mathrm{KOR}} = (0, \pi/2, \pi, \pi/2)$. This choice allows to reach the second maximum in figure 2(b), after which the KOR approaches the heterodyne-based protocol. For completeness, figure 3(b) reports also the optimized energies α_{p}^2, p = PGM, KOR, and α_{het}^2. All curves converge to 0.5 average number of photons in the long-distance regime but, differently from the other cases, α_{KOR}^2 shows the same non-monotonic trend of K_{KOR}.

The previous results prove non-Gaussian receivers as a potential tool for improving the key rate of the QPSK protocol, at least in the present composable security approach. Remarkably, they also highlight that the discrete-valued POVM minimizing the error probability, namely the PGM, does not coincide with the discrete-valued POVM maximizing the SKR, namely the KOR. The reason becomes evident when comparing separately the mutual and the Holevo information appearing in the SKR (22). In figure 4 we plot the quantities $I_{AB}^{(\mathrm{p})}$ and $\chi_{BE}^{(\mathrm{p})}$, p = PGM, KOR, computed with the same optimized energy and phases previously obtained and depicted in figure 3. As we can see, in the metropolitan-network distance regime the optimized receiver is associated with a reduced mutual information with respect to the PGM but, at the same time, reducing the mutual information induces also a reduction of the Holevo information extractable by Eve, thus resulting in a higher SKR. As a consequence, differently from the state-discrimination scenario, in CV-QKD there emerges a tradeoff between the goal of increasing the information accessible to Bob and the necessity of making the encoded symbols less 'distinguishable' to weaken Eve's attack.
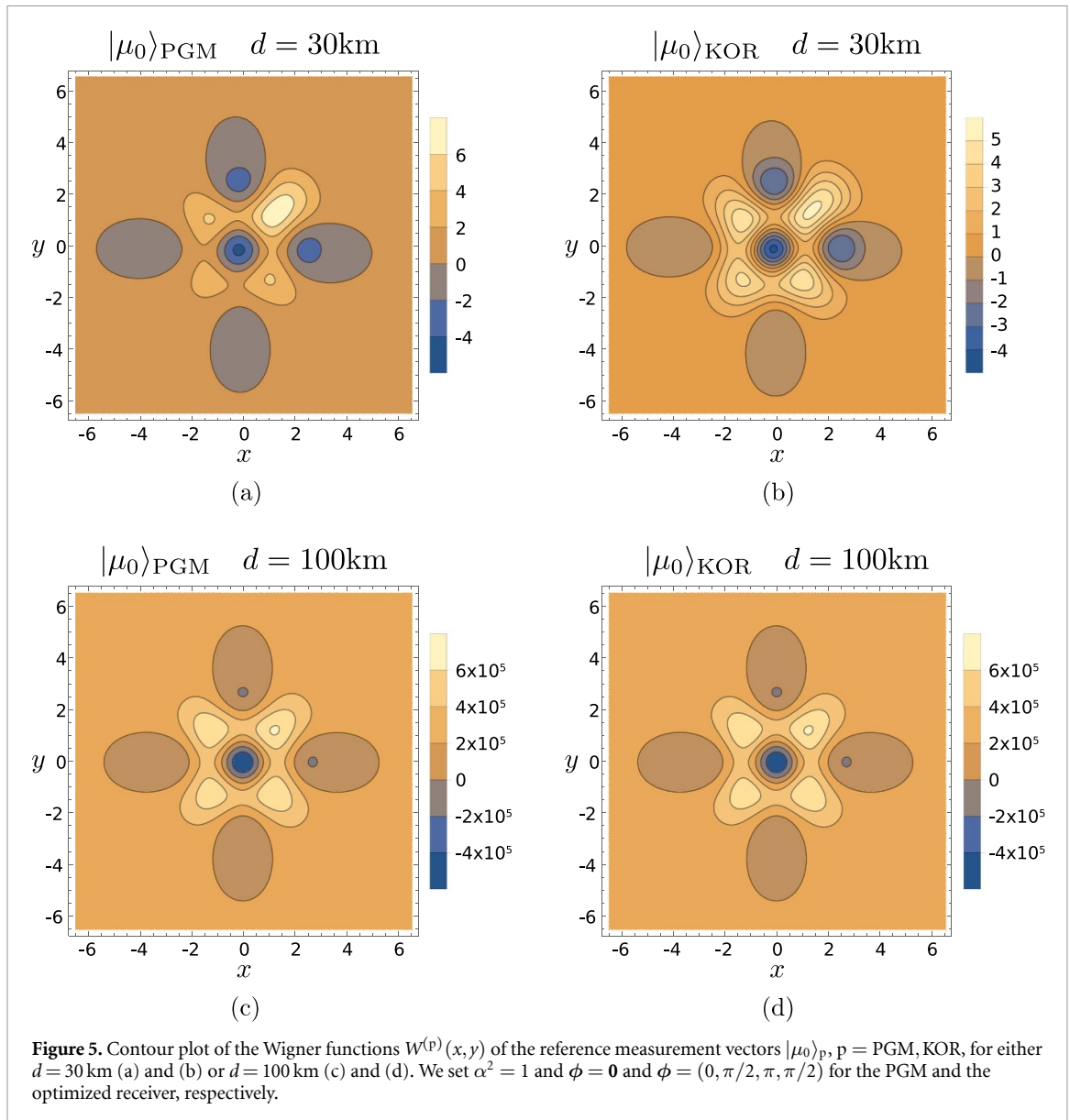
In light of this, we may interpret the physical meaning of the optimized phases as follows. For small transmission distances $\kappa d \ll 1$, Eve's intercepted signals are too weak to give her sufficient knowledge on which symbol was sent and the two different goals of reducing the error probability and maximizing the SKR are compatible, therefore the KOR coincides with the PGM. On the contrary, for larger d the compatibility does not hold anymore, and Bob has to sacrifice part of his potential information and to reduce the mutual information shared with Alice to the detriment of the eavesdropper.

The discussed tradeoff may be qualitatively appreciated by comparing the phase-space representations of the PGM and the KOR effects. More in detail, we consider the two reference measurement vectors $|\mu_0\rangle_{\mathrm{p}}$, p = PGM, KOR, computed from (20) with the phases $\phi = \mathbf{0}$ and $\phi = (0, \pi/2, \pi, \pi/2)$, respectively, and compute the associated Wigner function

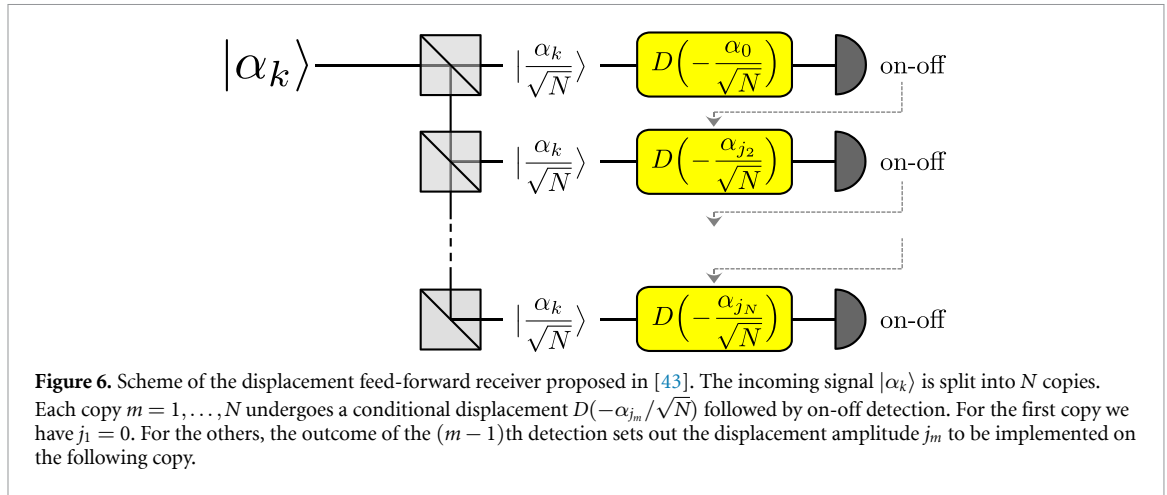$$W^{(\mathrm{p})}(x, y) = \frac{2}{\pi} \sum_{n=0}^{\infty} (-1)^n \langle n | D^\dagger(\zeta) \rho_{\mathrm{p}} D(\zeta) | n \rangle, \quad (\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}), \tag{38}$$

Figure 2. (a) Logarithmic plot of K_{p}, p = PGM, KOR, compared to K_{het}, as a function of the transmission distance d in km. (b) Plot of the ratio $\mathcal{R}_{\mathrm{p}}$, p = PGM, KOR, as a function of the transmission distance d. State-discrimination receivers improve the SKR with respect to the heterodyne-based protocol in the regime $d \leqslant 100$ km. In both pictures we set $\beta = 0.95$.

Figure 3. (a) Plot of the optimized phases $\phi_j^{(\mathrm{KOR})}$, $j = 1, \ldots, 3$, as a function of the transmission distance d in km. We recall that $\phi_0^{(\mathrm{KOR})} = 0$. (b) Plot of the optimized modulation energies α_{p}^2, p = PGM, KOR, and α_{het}^2, as a function of the transmission distance d. In both pictures we set $\beta = 0.95$.

Figure 4. Logarithmic plot of $I_{AB}^{(\mathrm{p})}$ and $\chi_{BE}^{(\mathrm{p})}$, p = PGM, KOR, as a function of the transmission distance d in km. Both the quantities are computed with the optimized parameters α_{p}^2 and ϕ_{KOR} (for the optimized receiver). We set $\beta = 0.95$.

where $\zeta = (x + \mathrm{i}y)/2$ expressed in SNU, $\rho_{\mathrm{p}} = |\mu_0\rangle_{\mathrm{p}\,\mathrm{p}}\langle\mu_0|$ and $D(\zeta)$ is the displacement operator [9, 68]. The contour plots of $W^{(\mathrm{p})}(x, y)$ are depicted in figure 5 for $\alpha^2 = 1$ and two different transmission distances $d = 30$ km and $d = 100$ km. If $d = 30$ km, that is for metropolitan-network distances, there is a qualitative difference between the two compared cases, see figures 5(a) and (b). Both Wigner functions exhibit four peaks, corresponding to the four transmitted states $|\alpha_k^{(t)}\rangle$. However, $W^{(\mathrm{PGM})}(x, y)$ is well concentrated around state $|\alpha_0^{(t)}\rangle$, while $W^{(\mathrm{KOR})}(x, y)$ is more delocalized over the four states and the peaks are less distinguishable. This implies a reduced distinguishability of the states and, in turn, a reduced mutual

Figure 5. Contour plot of the Wigner functions $W^{(\mathrm{p})}(x,y)$ of the reference measurement vectors $|\mu_0\rangle_{\mathrm{p}}$, $\mathrm{p} = \mathrm{PGM}, \mathrm{KOR}$, for either $d = 30\,\mathrm{km}$ (a) and (b) or $d = 100\,\mathrm{km}$ (c) and (d). We set $\alpha^2 = 1$ and $\phi = \mathbf{0}$ and $\phi = (0, \pi/2, \pi, \pi/2)$ for the PGM and the optimized receiver, respectively.

information $I_{AB}^{(\mathrm{KOR})}$. On the contrary, when the distance is larger, e.g. $d = 100\,\mathrm{km}$, the transmitted states are weak coherent states with a greater overlap between one another. As a consequence, $W^{(\mathrm{p})}(x,y)$ for respective receivers are equally delocalized over the four peaks and the differences between PGM and KOR become negligible; see figures 5(c) and (d). In turn, the associated SKRs converge to the same value, corresponding also to the rate of the heterodyne-based protocol, as depicted in figure 2. Furthermore, in all cases we observe a Wigner-negativity, proving both $|\mu_0\rangle_{\mathrm{p}}$ to be non-classical (as well as non-Gaussian) states at all distances [9, 68, 71].

5. Employing feasible receivers

Even though both PGM and KOR discussed in the previous sections have shown interesting potentialities for CV-QKD, from a practical point of view there is no clear idea on their experimental implementation. Differently from the case of binary discrimination where the PGM is implemented via the Dolinar receiver [72, 73], in the presence of QSPK designing a feasible optimum receiver is an open problem. In fact, the Dolinar receiver has been generalized, obtaining the so-called Bondurant receiver [74], which, unfortunately, is not optimum. As a consequence, it is not known how to reach the minimum error probability with optical feedback and linear optics. Nevertheless, at the state of the art many feasible quantum receivers are based on displacement operations and photon counting [39–41, 43–46]. Therefore, it is worth of interest to investigate also the performance of these receivers for CV-QKD. Here, in particular, we focus on the proposal of the

Figure 6. Scheme of the displacement feed-forward receiver proposed in [43]. The incoming signal $|\alpha_k\rangle$ is split into N copies. Each copy $m = 1, \dots, N$ undergoes a conditional displacement $D(-\alpha_{j_m}/\sqrt{N})$ followed by on-off detection. For the first copy we have $j_1 = 0$. For the others, the outcome of the $(m-1)$th detection sets out the displacement amplitude j_m to be implemented on the following copy.

displacement feed-forward receiver (DFFRx) presented in [43] and depicted in figure 6. Its functioning will be presented in detail in the following subsection.

5.1. Description of the displacement feed-forward receiver

The DFFRx, presented schematically in figure 6, aims at QPSK discrimination of coherent states in the form $|\alpha_k\rangle = |\alpha\, e^{i\pi\,(2k+1)/M}\rangle$, $k = 0, \dots, M-1$, with $M = 4$. It is based on the slicing property of coherent states: indeed, thanks to an array of splitters, the incoming signal $|\alpha_k\rangle$ is split into $N \geqslant M-1$ identical copies with reduced amplitude $|\alpha_k/\sqrt{N}\rangle$. Then, each mth copy, $m = 1, \dots, N$, undergoes a conditional displacement operation followed by an on–off detection which returns a click-no click result. The first copy is displaced by $D(-\alpha_{j_1}/\sqrt{N})$, with $j_1 = 0$, being mapped into the coherent state $|(\alpha_k - \alpha_{j_1})/\sqrt{N}\rangle$. In turn, if $k = 0$ the incoming signal is displaced into the vacuum and the subsequent on-off detector will not click, whereas if $k \neq 0$ the detector is more likely to click with a probability $1 - p_k$, where

$$p_0 = 1\,,$$
$$p_1 = p_3 = e^{-2\alpha^2/N}\,,$$
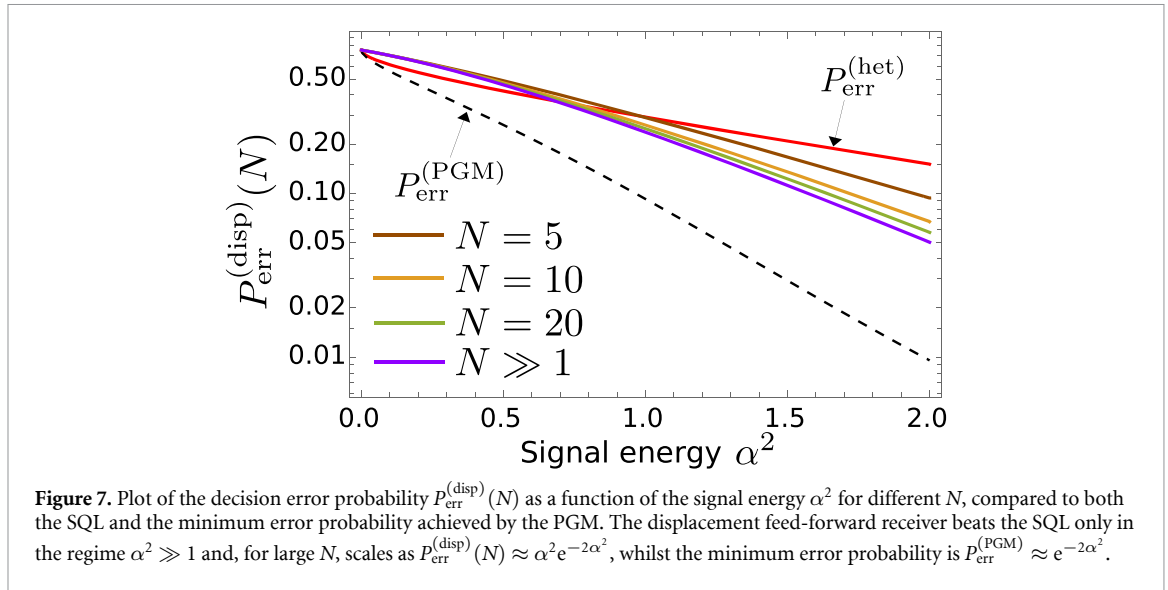$$p_2 = e^{-4\alpha^2/N}\,. \tag{39}$$

According to the result of the first detection, we decide what would be the value of the amplitude of the displacement $D(-\alpha_{j_2}/\sqrt{N})$ applied to the second copy: if an 'off' result is registered, that is the detector does not click, we set $j_2 = j_1 = 0$; otherwise we discard hypothesis '$k = 0$', set $j_2 = j_1 + 1$ and probe the final hypothesis from the remaining set $k = 1, 2, 3$. We proceed iteratively in this way until the last copy is processed, following the feed-forward rule: if the $(m-1)$th detection gives outcome 'off' we displace the mth copy by $D(-\alpha_{j_m}/\sqrt{N})$ with $j_m = j_{m-1}$, if an 'on' is obtained we set $j_m = j_{m-1} + 1$, discard all states $j \leqslant j_{m-1}$ and restrict the decision to the states $j_m, \dots, M-1$. The outcome of the last detection determines the final decision. If an 'off' is retrieved, we decide the state $j = j_m$ has been sent, otherwise we perform a random decision among the remaining states.

The conditional probabilities of inferring the state $j = 0, \dots, M-1$ if state $k = 0, \dots, M-1$ was sent read:

$$p_{B|\alpha_k}^{(N)}(0) = p_0^N\,, \tag{40a}$$

$$p_{B|\alpha_k}^{(N)}(1) = \sum_{t=0}^{N-2} p_k^t\,(1-p_k)\,p_{(k-1)\bmod M}^{N-1-t} + \frac{p_k^{N-1}\,(1-p_k)}{3}\,, \tag{40b}$$

$$p_{B|\alpha_k}^{(N)}(2) = \sum_{t=0}^{N-3}\sum_{s=0}^{N-3-t} p_k^t\,(1-p_k)\,p_{(k-1)\bmod M}^s\,\left(1-p_{(k-1)\bmod M}\right)p_{(k-2)\bmod M}^{N-2-t-s}$$
$$+ \sum_{t=0}^{N-2} p_k^t\,(1-p_k)\,\frac{p_{(k-1)\bmod M}^{N-2-t}\,\left(1-p_{(k-1)\bmod M}\right)}{2} + \frac{p_k^{N-1}\,(1-p_k)}{3}\,, \tag{40c}$$

Figure 7. Plot of the decision error probability $P_{\text{err}}^{(\text{disp})}(N)$ as a function of the signal energy α^2 for different N, compared to both the SQL and the minimum error probability achieved by the PGM. The displacement feed-forward receiver beats the SQL only in the regime $\alpha^2 \gg 1$ and, for large N, scales as $P_{\text{err}}^{(\text{disp})}(N) \approx \alpha^2 e^{-2\alpha^2}$, whilst the minimum error probability is $P_{\text{err}}^{(\text{PGM})} \approx e^{-2\alpha^2}$.

$$p_{B|\alpha_k}^{(N)}(3) = \sum_{t=0}^{N-3} \sum_{s=0}^{N-3-t} \sum_{u=0}^{N-3-t-s} p_k^t (1-p_k) \, p_{(k-1) \bmod M}^s \left(1 - p_{(k-1) \bmod M}\right) p_{(k-2) \bmod M}^u$$

$$\times \left(1 - p_{(k-2) \bmod M}\right) p_{(k-3) \bmod M}^{N-3-t-s-u} + \sum_{t=0}^{N-2} p_k^t (1-p_k) \frac{p_{(k-1) \bmod M}^{N-2-t} \left(1 - p_{(k-1) \bmod M}\right)}{2}$$

$$+ \frac{p_k^{N-1}(1-p_k)}{3} . \tag{40d}$$

The overall Bob's probability can then be written as:

$$p_B^{(N)}(j) = \frac{1}{M} \sum_{k=0}^{M-1} p_{B|\alpha_k}^{(N)}(j), \quad (j = 0,\dots,M-1). \tag{41}$$

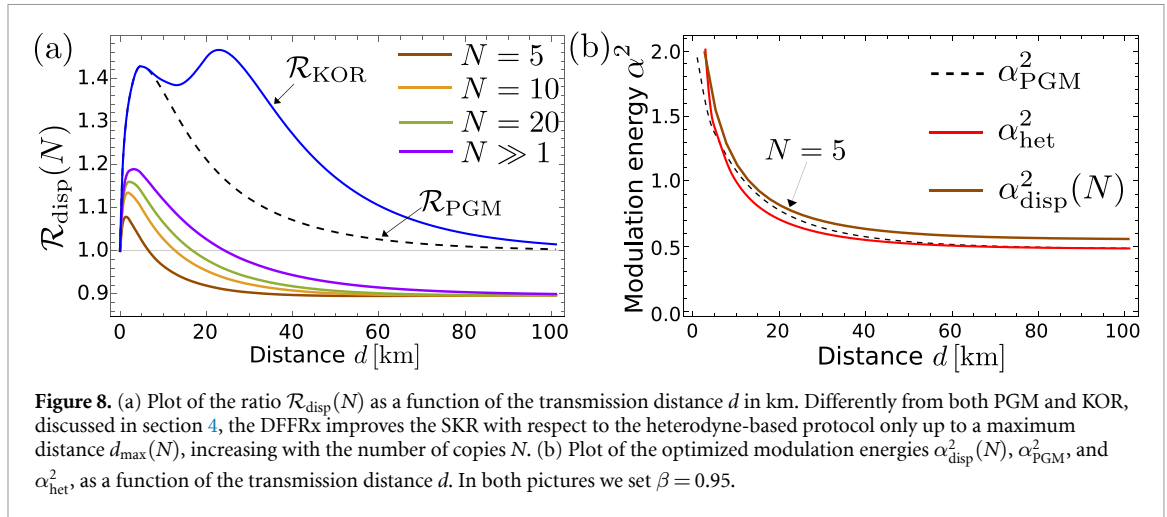In the context of quantum-state discrimination, the associated decision error probability reads:

$$P_{\text{err}}^{(\text{disp})}(N) = 1 - \frac{1}{M} \sum_{k=0}^{M-1} p_{B|\alpha_k}^{(N)}(k), \tag{42}$$

depicted in figure 7 as a function of α^2 for different N. As emerges from the plot, the present displacement receiver outperforms the SNL achieved with heterodyne detection, namely $P_{\text{err}}^{(\text{het})} = 1 - [1 + \text{erf}(\alpha/\sqrt{2})]^2/4$, only in the high-energy regime $\alpha^2 \gg 1$. We also note that, in the limit $N \gg 1$, we have $P_{\text{err}}^{(\text{disp})}(N) = e^{-2\alpha^2}(\alpha^2 + 3/4)$, and the DFFRx reaches the Bondurant receiver [74]. Nevertheless, it does not provide a near-optimum receiver. In fact, the minimum error probability, associated with the PGM, reads

$$P_{\text{err}}^{(\text{PGM})} = 1 - \frac{1}{M^2} \left(\sum_{k=0}^{M-1} \sqrt{\lambda_k} \right)^2, \tag{43}$$

with $\lambda_{0(1)} = 2e^{-\alpha^2}[\cosh(\alpha^2) \pm \cos(\alpha^2)]$ and $\lambda_{2(3)} = 2e^{-\alpha^2}[\sinh(\alpha^2) \pm \sin(\alpha^2)]$, which for $\alpha^2 \gg 1$ scales only exponentially, $P_{\text{err}}^{(\text{PGM})} \approx e^{-2\alpha^2}$.

When Bob employs the DFFRx in the protocol of figure 1, the previous conditional probabilities shall be modified accordingly by substituting $\alpha^2 \to T\alpha^2$ in the p_k in (39), as Bob receives only the transmitted fraction of Alice's signals.

Figure 8. (a) Plot of the ratio $\mathcal{R}_{\text{disp}}(N)$ as a function of the transmission distance d in km. Differently from both PGM and KOR, discussed in section 4, the DFFRx improves the SKR with respect to the heterodyne-based protocol only up to a maximum distance $d_{\max}(N)$, increasing with the number of copies N. (b) Plot of the optimized modulation energies $\alpha^2_{\text{disp}}(N)$, α^2_{PGM}, and α^2_{het}, as a function of the transmission distance d. In both pictures we set $\beta = 0.95$.

5.2. Calculation of the SKR

We now compute the SKR $K_{\text{disp}}(N; \alpha^2)$ associated with the DFFRx by exploiting equations (22), (23) and (26), provided the substitutions $p^{(\phi)}_{B|\alpha_k} \to p^{(N)}_{B|\alpha_k}$ and $p^{(\phi)}_B \to p^{(N)}_B$, and optimize over the modulation energy, obtaining:

$$K_{\text{disp}}(N) = \max_{\alpha^2} K_{\text{disp}}(N; \alpha^2). \tag{44}$$

Moreover, we also compute the ratio with respect to the heterodyne-based protocol, namely,

$$\mathcal{R}_{\text{disp}}(N) = \frac{K_{\text{disp}}(N)}{K_{\text{het}}}, \tag{45}$$

reported in figure 8(a) for different number of copies N. Unlike the PGM and the KOR, the DFFRx outperforms the heterodyne-based protocol only up to a maximum transmission distance $d_{\max}(N)$ whose value increases with N. Afterwards, $K_{\text{disp}}(N) \leqslant K_{\text{het}}$ and, in turn, $\mathcal{R}_{\text{disp}}(N)$ saturates to an asymptotic value $\leqslant 1$. The best performance is achieved in the limit of infinite copies, $N \gg 1$, where the receiver approximates the Bondurant receiver, obtaining a maximum increase in the SKR of about $\lesssim 20\%$ and $d_{\max}(N) \lesssim 25$ km.

This behaviour is a direct consequence of the optimized modulation $\alpha^2_{\text{disp}}(N)$, reported in figure 8(b). In fact, $\alpha^2_{\text{disp}}(N)$ is a decreasing function of d, which in the long-distance regime, $\kappa d \gg 1$, reaches an asymptotic value $\gtrsim 0.5$. Numerical calculations also show this asymptote to be independent of the number of copies N. In these conditions, Bob receives a signal with $T\alpha^2_{\text{disp}}(N) \ll 0.5$ mean photons, for which the DFFRx does not beat the SQL, as depicted in figure 7. In turn, even the SKR of the CV-QKD protocol is lower than the corresponding heterodyne protocol. On the other hand, for $\kappa d \ll 1$, the optimized modulation is of few photons, the DFFRx outperforms the SQL and we observe an increase also in the SKR.

In conclusion, despite its feasibility, the present displacement feed-forward scheme is not optimal for CV-QKD, just as it is not optimal for coherent state discrimination. Nevertheless, it still provides an improvement of the resulting key rate in the short-distance regime, being a candidate for experimental realizations of the present protocol.

6. Conclusions and outlooks

In this paper we have investigated the role of state-discrimination receivers for CV-QKD. In particular, we have addressed a QPSK protocol based on a pure-loss wiretap channel assumption, and proposed an optimized non-Gaussian state-discrimination receiver, the KOR, to be employed by Bob in place of the commonly exploited Gaussian measurements. We have compared the performance of both the KOR and PGM with respect to the heterodyne-based protocol and obtained an increase in the SKR for metropolitan-network distances. Moreover, we have also discussed the role of feasible schemes, such as the displacement feed-forward receiver, obtaining an increased SKR in the short-distance regime up to a maximum transmission distance.

The results obtained in this paper suggest suitable non-Gaussian receivers as a resource to increase the key rate in the CV-QKD framework. Nevertheless, they only provide a first step towards the analysis of CV-QKD with non-Gaussian measurements and leave many points as open problems. At first, the extension

of the present analysis to the more realistic case of a thermal-loss channel remains a challenging task. In fact, in the presence of thermal mixed states, designing the receiver achieving the minimum error probability is non-trivial. The general structure of quantum receivers derived in section 2 does not hold anymore, as the M mixed states now span the whole infinite dimensional Hilbert space. Moreover, from the perspective of quantum communications, the optimum receiver achieving the minimum error probability can only be obtained numerically via linear convex semidefinite programming [32]. There exists an extension of the PGM method, where the Gram matrix is obtained via the 'factor decomposition' of the quantum states [32, 36, 75, 76]. However, the resulting POVM is not optimal anymore, even in the presence of GUS, and only provides a non-tight upper bound of the minimum error probability. As a consequence, the search of the KOR could only be obtained via a brute-force functional optimization over all possible POVMs, being a nonlinear and non-convex problem.

Secondly, the sketch of an unconditional security proof may be designed, identifying which is the optimal Eve's attack. To do so, we should optimize over all the possible attacks compatible with Alice and Bob's statistics, retrieving the DW bound [22, 54] by extending the methods of [20]. Indeed, the question whether or not protocols employing non-Gaussian measurement guarantee higher security than Gaussian ones is an interesting open problem.

Finally, we should investigate the scalability of the present scheme with discrete-modulation formats of higher order, like PSK schemes with $M \geqslant 4$ encoded states or quadrature-amplitude-modulation (QAM) constellations, in which the GUS is not satisfied anymore [26, 32].

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgment

Appendix A. Derivation of the constraint on matrix A

As discussed in section 2, the optimal receiver for pure-state discrimination is a 1-rank POVM $\{\Pi_j\}_j$, $\Pi_j = |\mu_j\rangle\langle\mu_j|, j = 0, \ldots, M-1$, where $|\mu_j\rangle = \sum_k a_{kj}|\gamma_k\rangle$, $a_{kj} \in \mathbb{C}$ and

$$\mathcal{N} \equiv \sum_{j=0}^{M-1} |\mu_j\rangle\langle\mu_j| = \mathbb{P}_{\mathcal{S}}. \tag{A.1}$$

The previous condition may be turned into the constraint (6) as follows. Equation (A.1) is an equality of quantum operators, therefore it shall be

$$\mathcal{N}|\psi\rangle = |\psi\rangle \qquad \forall|\psi\rangle \in \mathcal{S}, \tag{A.2}$$

where $|\psi\rangle = \sum_s b_s|\gamma_s\rangle$, $b_s \in \mathbb{C}$. Accordingly, the following equations hold:

$$\left[\sum_j \left(\sum_{k,l} a_{kj}a_{lj}^*|\gamma_k\rangle\langle\gamma_l|\right)\right]\sum_s b_s|\gamma_s\rangle = \sum_t b_t|\gamma_t\rangle, \tag{A.3}$$

$$\sum_k \left(\sum_{j,l,s} a_{kj}a_{jl}^\dagger G_{ls}b_s\right)|\gamma_k\rangle = \sum_t b_t|\gamma_t\rangle, \tag{A.4}$$

where $G_{ls} = \langle\gamma_l|\gamma_s\rangle$. In the matrix notation we have $AA^\dagger G\mathbf{b} = \mathbf{b}$ to be satisfied for all $\mathbf{b} = (b_0, \ldots, b_{M-1})$. In turn,

$$AA^\dagger G = \mathbb{1}_M, \tag{A.5}$$

$\mathbb{1}_M$ being the $M \times M$ identity matrix and, ultimately, $AA^\dagger = G^{-1}$.

Appendix B. Computation of the von Neumann entropy of Eve's states

To perform the SKR analysis outlined in section 3.1 we need to compute the von Neumann entropies of states (28) and (29). Both of them are in the following form:

$$\rho = \sum_{k=0}^{M-1} c_k |\alpha_k^{(r)}\rangle\langle\alpha_k^{(r)}|, \tag{B.1}$$

for some coefficients $c_k \in \mathbb{C}$. To compute the associated entropy we need to diagonalize state (B.1). If $|\psi\rangle$ is the eigenvector of ρ associated with eigenvalue λ, we have $|\psi\rangle = \sum_m b_m |\alpha_m^{(r)}\rangle$ and the following equations hold:

$$\rho|\psi\rangle = \lambda|\psi\rangle \tag{B.2}$$

$$\left(\sum_k c_k |\alpha_k^{(r)}\rangle\langle\alpha_k^{(r)}|\right)\sum_m b_m|\alpha_m^{(r)}\rangle = \lambda\sum_s b_s|\alpha_s^{(r)}\rangle \tag{B.3}$$

$$\sum_k c_k \left(\sum_m G_{km}b_m\right)|\alpha_k^{(r)}\rangle = \lambda\sum_s b_s|\alpha_s^{(r)}\rangle, \tag{B.4}$$

where $G_{km} = \langle\alpha_k^{(r)}|\alpha_m^{(r)}\rangle$.

As a consequence, we have a set of equations:

$$\lambda b_k = c_k \left(\sum_{m=0}^{M-1} G_{km}b_m\right), \quad (k=0,\dots,M-1), \tag{B.5}$$

or, equivalently,

$$\left(\frac{\lambda}{c_k}-1\right)b_k - \sum_{m\neq k} G_{km}b_m = 0. \tag{B.6}$$

This defines the homogeneous linear system $M\mathbf{b} = 0$, where $\mathbf{b} = (b_0,\dots,b_{M-1})$ and

$$M = \begin{pmatrix} \frac{\lambda}{c_0}-1 & -G_{01} & -G_{02} & -G_{03} \\ -G_{10} & \frac{\lambda}{c_1}-1 & -G_{12} & -G_{13} \\ -G_{20} & -G_{21} & \frac{\lambda}{c_2}-1 & -G_{23} \\ -G_{30} & -G_{31} & -G_{32} & \frac{\lambda}{c_3}-1 \end{pmatrix}. \tag{B.7}$$

The equation $M\mathbf{b} = 0$ always admits a trivial solution $\mathbf{b} = 0$, therefore to obtain a nonzero eigenvector we shall impose the condition $\det M = 0$. This provides us with the four eigenvalues $\{\lambda_j\}_j$ and the corresponding von Neumann entropy $S[\rho] = -\sum_j \lambda_j \log_2 \lambda_j$.

For state ρ_E in (28), for which $c_k = M^{-1}$, the equation $\det M = 0$ may be solved analytically, leading to:

$$\lambda_{0(1)} = \frac{e^{-(1-T)\alpha^2}}{2}\left\{\cosh\left[(1-T)\alpha^2\right] \pm \cos\left[(1-T)\alpha^2\right]\right\},$$

$$\lambda_{2(3)} = \frac{e^{-(1-T)\alpha^2}}{2}\left\{\sinh\left[(1-T)\alpha^2\right] \pm \left|\sin\left[(1-T)\alpha^2\right]\right|\right\}. \tag{B.8}$$

ORCID iDs

M N Notarnicola ● https://orcid.org/0000-0002-7492-6143
M Jarzyna ● https://orcid.org/0000-0001-9989-1648
S Olivares ● https://orcid.org/0000-0002-9251-0731
K Banaszek ● https://orcid.org/0000-0002-5389-6897

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Pirandola S *et al* 2020 *Adv. Opt. Photon.* **12** 1012–236
[4] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 *Rev. Mod. Phys.* **92** 025002

[5] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[6] Grosshans F and Grangier P 2001 *Phys. Rev. A* **64** 010301(R)
[7] Laudenbach F, Pacher C, Fung C H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P and Hübel H 2018 *Adv. Quantum Technol.* **1** 1800011
[8] Braunstein S L and van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[9] Olivares S 2021 *Phys. Lett. A* **418** 127720
[10] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[11] Grosshans F, Van Assche G, Wenger J, Tualle-Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[12] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2003 *Quantum Inf. Comput.* **3** 535
[13] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Koy Lam P 2004 *Phys. Rev. Lett.* **93** 170504
[14] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504
[15] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[16] Sych D and Leuchs G 2010 *New J. Phys.* **12** 053019
[17] Leverrier A and Grangier P 2011 *Phys. Rev. A* **83** 042312
[18] Becir A, El-Orany F A A and Wahiddin M R B 2012 *Int. J. Quantum Inf.* **10** 1250004
[19] Ghorai S, Grangier P, Diamanti E and Leverrier A 2019 *Phys. Rev. X* **9** 021059
[20] Lin J, Upadhyaya T and Lütkenhaus N 2019 *Phys. Rev. X* **9** 041064
[21] Liao Q, Xiao G, Xu C-G, Xu Y and Guo Y 2020 *Phys. Rev. A* **102** 032604
[22] Denys A, Brown P and Leverrier A 2021 *Quantum* **5** 540
[23] Upadhyaya T, van Himbeeck T, Lin J and Lütkenhaus N 2021 *PRX Quantum* **2** 020325
[24] Liu W-B, Li C-L, Xie Y-M, Weng C-X, Gu J, Cao X-Y, Lu Y-S, Li B-H, Yin H-L and Chen Z-B 2021 *PRX Quantum* **2** 040334
[25] Lupo C and Ouyang Y 2022 *PRX Quantum* **3** 010341
[26] Notarnicola M N, Olivares S, Forestieri E, Parente E, Potí L and Secondini M 2023 *IEEE Trans. Commun.* (https://doi.org/10.1109/TCOMM.2023.3317259)
[27] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
[28] Leverrier A 2009 Theoretical study of continuous-variable quantum key distribution *PhD Thesis* Télécom ParisTech
[29] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[30] Helstrom C W 1976 *Quantum Detection and Estimation Theory Mathematics in Science and Engineering* (Elsevier, Academic)
[31] Bergou J A 2010 *J. Mod. Opt.* **57** 160–80
[32] Cariolaro G 2015 *Quantum Communications* (Springer)
[33] Holevo A S 1973 *J. Multivariate Anal.* **3** 337–94
[34] Yuen H P, Kennedy R and Max L 1975 *IEEE Trans. Inf. Theory* **21** 125–34
[35] Eldar Y C, Megretski A and Verghese G C 2003 *IEEE Trans. Inf. Theory* **49** 1017–1012
[36] Assalini A, Cariolaro G and Pierobon G 2010 *Phys. Rev. A* **81** 012315
[37] Eldar Y C and Forney G D 2001 *IEEE Trans. Inf. Theory* **47** 858–72
[38] Eldar Y C and Forney G D 2002 *IEEE Trans. Inf. Theory* **48** 599–610
[39] Kennedy R S 1973 A near-optimum receiver for the binary coherent state quantum channel *MIT Research Laboratory of Electronics Quarterly Progress Report* vol 108 pp 219–25
[40] DiMario M T and Becerra F E 2018 *Phys. Rev. Lett.* **121** 023603
[41] Notarnicola M N, Paris M G A and Olivares S 2023 *J. Opt. Soc. Am. B* **40** 705–14
[42] Notarnicola M N, and Olivares S 2023 Beating the standard quantum limit for binary phase-shift-keying discrimination with a hybrid feed-forward receiver (arXiv:2308.04146 [quant-ph])
[43] Izumi S, Takeoka M, Fujiwara M, Dalla Pozza N, Assalini A, Ema K and Sasaki M 2012 *Phys. Rev. A* **86** 042328
[44] Becerra F E, Fan J, Baumgartner G, Goldhar J, Kosloski J T and Migdall A 2013 *Nat. Photon.* **7** 147–52
[45] DiMario M T, Carrasco E, Jackson R A and Becerra F E 2018 *J. Opt. Soc. Am. B* **35** 568–74
[46] Izumi S, Neergaard-Nielsen J S, Miki S, Terai H and Andersen U L 2020 *Phys. Rev. Appl.* **13** 054015
[47] Liao Q, Guo Y, Huang D, Huang P and Zeng G 2018 *New J. Phys.* **20** 023015
[48] Cai N, Winter A and Yeun R W 2004 *Probl. Inf. Transm.* **40** 318–36
[49] Holevo A S and Giovannetti V 2012 *Rep. Prog. Phys.* **75** 04600
[50] Pan Z, Seshadreesan K P, Clark W, Adcock M R, Djordjevic I B, Shapiro J H and Guha S 2020 *Phys. Rev. Appl.* **14** 024044
[51] Banaszek K, Jachura M, Kolenderski P and Lasota M 2021 *Opt. Express* **29** 43091–103
[52] Cariolaro G, Corvaja R and Pierobon G 2011 Compression of Pure and Mixed States in Quantum Detection *2011 IEEE Global Telecommunications Conf. - GLOBECOM* (*Houston, USA*, *05–09 December 2011*) (IEEE) pp 1–5
[53] Davis P J 1970 *Circulant Matrices* (Wiley)
[54] Devetak I and Winter A 2005 *Proc. R. Soc. A* **461** 207–35
[55] Pirandola S 2021 *Phys. Rev. Res.* **3** 043014
[56] Pirandola S 2021 *Phys. Rev. Res.* **3** 013279
[57] Derkach I and Usenko V C 2021 *Entropy* **23** 55
[58] Kundu N K, McKay M R, Conti A, Mallik R K and Win M Z 2023 *IEEE Trans. Quantum Eng.* **4** 1–15
[59] Fujiwara M *et al* 2018 *Opt. Express* **26** 19513–23
[60] Banaszek K, Kunz L, Jachura M and Jarzyna M 2020 *J. Light. Technol.* **38** 2741–54
[61] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev. A* **72** 050303
[62] Lodewyck J *et al* 2007 *Phys. Rev. A* **76** 042305
[63] Agrawal G P 2002 *Fiber-Optic Communications Systems* (Wiley)
[64] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti P 2013 *Nat. Photon.* **7** 378–81
[65] Medlock E T H 2021 Continuous Variable Quantum Key Distribution in presence of emulated atmospheric turbulence and with passive eavesdropping *PhD Thesis* University of York
[66] Ghalaii et al 2022 Satellite-Based quantum key distribution in the presence of bypass channels (arXiv:2212.04807 [quant-ph])
[67] Jarzyna M, Jachura M and Banaszek K 2023 *IEEE Commun. Lett.* **27** 1699–703
[68] Serafini A 2017 *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press)
[69] Holevo A S 1998 *IEEE Trans. Inf. Theory* **44** 269–73

[70] Press W H, Teukolsky S A, Vetterling W T and Flannery B P 2007 *Numerical Recipes : The Art of Scientific Computing* 3rd edn (Cambridge University Press)
[71] Genoni M G, Palma M L, Tufarelli T, Olivares S, Kim M S and Paris M G A 2013 *Phys. Rev. A* **87** 062104
[72] Dolinar S J 1973 An optimum receiver for the binary coherent state quantum channel *MIT Research Laboratory of Electronics Q. Prog. Rep.* **11** 115–20
[73] Assalini A, Dalla Pozza N and Pierobon G 2011 *Phys. Rev. A* **84** 022342
[74] Bondurant R S 1993 *Opt. Lett.* **18** 1896–8
[75] Eldar Y C, Megretski A and Verghese G C 2004 *IEEE Trans. Inform. Theory* **50** 1198–207
[76] Cariolaro G and Pierobon G 2010 *IEEE Trans. Commun.* **58** 623–30