Research Article | Vol. 32, No. 22 / 21 Oct 2024 / Optics Express 39846
Optics EXPRESS

Assessing a binary quantum channel exploiting a silicon photomultiplier based hybrid receiver

ALBERTO SANVITO,[1] SILVIA CASSINA,[1,*] MARCO LAMPERTI,[1,2] MICHELE N. NOTARNICOLA,[3] STEFANO OLIVARES,[3] AND ALESSIA ALLEVI[1,2]

[1] University of Insubria, Via Valleggio 11, I-22100 Como, Italy
[2] Institute for Photonics and Nanotechnologies, IFN-CNR, Via Valleggio 11 I-22100 Como, Italy
[3] University of Milan and INFN Section of Milan, Via Celoria 16, I-20133 Milan, Italy
[*] s.cassina@uninsubria.it

Abstract: In quantum communication protocols, the use of photon-number-resolving detectors could open new perspectives by broadening the way to encode and decode information and merging the properties of discrete and continuous variables. In this work, we consider a quantum channel exploiting a silicon-photomultiplier-based receiver and evaluate its performance for quantum communication protocols under three possible configurations, defined by different post-processing of the detection outcomes. We investigate two scenarios: information transmission over the channel, quantified by the mutual information, and continuous-variable quantum key distribution, quantified by the key generation rate. The preliminary results encourage further use of this detection scheme in extended networks.

1. Introduction

In the context of optical quantum communication, the encoding of information can be carried out either in discrete or continuous variables [1]. While in the former case, the typical detection system is based on the use of single-photon detectors [2], in the latter one the signal detection is performed by means of homodyne detection schemes [3–5]. In this second kind of detectors, the state to be characterized interferes at a balanced beam splitter with a high-intensity coherent state, the local oscillator (LO), and then the two outputs of the interferometer are detected by two photodiodes, whose photocurrent difference is measured as a function of the LO phase [6]. Years ago, some of us have proposed to merge the two above-mentioned detection strategies in a hybrid scheme, in which photodiodes are substituted by photon-number-resolving detectors [7], and the LO has an energy comparable to that of the signal under investigation [8]. The scheme has been already exploited to perform quantum state tomography [9] as well as coherent-state discrimination with binary phase-shift keying (BPSK) [10]. Furthermore, theoretical works proved the adoption of photon-number-resolving receivers for quantum communication protocols with coherent-state encoding to be beneficial, both for information transmission [11–14] and continuous-variable quantum key distribution (CVQKD) [15,16]. A first experimental verification has been recently carried out by DiMario and Becerra, who adopted a displacement photon-number-resolving receiver, inspired on the Kennedy receiver for BPSK discrimination [17], to assess the information transmission over realistic quantum channels, optimizing also the encoding strategy [18,19]. Anyway, the performance of a hybrid receiver, probing both the particle- and wave-like properties of radiation, has been so far limited to the quantum-state discrimination framework.

In this work, we investigate the applicability of the hybrid scheme introduced in [8] to the more general context of quantum communication with coherent states affected by loss. To this aim, we consider Silicon photomultipliers (SiPMs) [20] as photon-number-resolving detectors instead of the previously-used hybrid photodetectors [21], since they are more compact and with higher

#534910 https://doi.org/10.1364/OE.534910
Journal © 2024 Received 5 Jul 2024; revised 30 Aug 2024; accepted 19 Sep 2024; published 17 Oct 2024

Optics EXPRESS

dynamic range [22]. In particular, we evaluate the performance of the quantum channel exploiting the SiPM-based receiver under two different scenarios. At first, we address the transmission of classical information over the channel, quantified by the mutual information (MI), while, thereafter we consider CVQKD context, proving conditional security under the wiretap channel assumption [23]. In this latter framework, we compute the amount of secure information shared by Alice and Bob both in direct (DR) and reverse reconciliation (RR) for individual and collective attacks. In both cases, we calculate the MI as a function of the parameters characterizing the system, and investigate the role of both the LO intensity [24] and the losses affecting the encoded coherent states. In this way, we can characterize the communication channel and test its robustness to loss and detector inefficiencies. Thanks to the features of our detection system, we consider three possible scenarios according to the output reading. In the first case we consider the detection system as a weak-field (WF) receiver, in which we have direct access to the output of the two employed photon-number-resolving detectors. In the second case, we treat it as a homodyne-like (HL) receiver, where we evaluate the photon-number difference between the two outputs and use it to calculate the MI similarly to the procedure of a standard homodyne detection. Finally, in the third case, we employ a binary discrimination strategy (BDS), which is based on the sign of the photon-number difference in the case of a binary alphabet. In both applications, we consider BPSK encoding, providing the basic case for further implementation of more elaborated protocols with larger alphabets; we compare the experimental results to the corresponding figures of merit and demonstrate the feasibility of the proposed receiver for quantum communication protocols. Our results prove that, in the presence of BPSK modulation, the WF and HL strategies are equivalent, while the BDS method is less performing, according to the data processing inequality. The obtained outcomes encourage further exploitation of the SiPM-based detection scheme in extended networks [25].

2. Theoretical description

In this work, we address a BPSK protocol, being one of the basic strategies to transmit information between two distant parties: a sender, usually called Alice, and a receiver, usually called Bob [1,26,27]. BPSK can be easily implemented by encoding two classical symbols $k = 0, 1$ onto the coherent states:

$$|\alpha_k\rangle = |e^{i\pi(k+1)}\alpha\rangle\,, \qquad (k = 0, 1)\,, \tag{1}$$

with $\alpha>0$, such that $|\alpha_0\rangle = |-\alpha\rangle$ and $|\alpha_1\rangle = |+\alpha\rangle$, generated with equal a priori probabilities $q_k = 1/2$. The encoded pulses have the same energy, i.e. mean number of photons, equal to α^2, but are phase-shifted by π [28,29]. We note that the choice of coherent-state encoding provides robustness against losses, since with respect to nonclassical states of radiation, coherent states remain coherent under a lossy dynamics [30]. The encoded pulses are then injected into the quantum channel, here considered as a pure-loss channel associated with transmissivity $T<1$, until to reach Bob, who performs a suitable measurement on the received signal $|\sqrt{T}\alpha_k\rangle$.

The adopted detection scheme is based on an interferometric setup, where the received quantum state $|\sqrt{T}\alpha_k\rangle$ interferes at a balanced beam splitter with a low-intensity LO prepared in the coherent state $|z\rangle$ with amplitude $z>0$. Thereafter, we perform photon-number-resolving detection at each beam splitter output, and reconstruct the local photon-number distributions on both arms. In particular, if state $|\alpha_k\rangle$ is sent, the conditional photon-number distributions of the transmitted and reflected beams are given by Poisson distribution:

$$\mathcal{P}_n(\mu|\alpha_k) = e^{-\mu}\frac{\mu^n}{n!}\,, \tag{2}$$

with rates $\mu_k^{(t)}$ and $\mu_k^{(r)}$, respectively, in which

$$\mu_k^{(t)} = \frac{1}{2}\left(T\alpha^2 + z^2 + 2\xi\sqrt{T}\alpha_k z\right) \quad \text{and} \quad \mu_k^{(r)} = \frac{1}{2}\left(T\alpha^2 + z^2 - 2\xi\sqrt{T}\alpha_k z\right)\,, \tag{3}$$

Optics EXPRESS

where $\xi \leq 1$ represents the interference visibility, quantifying the overlap between the signal and the LO beams interacting with each other [18,25].

Given the previous setup, we identify three different strategies, that, ultimately, correspond to three different types of receivers. In the former, referred to as weak-field (WF) receiver, we have access to the single detector outputs n and m on the transmitted and reflected arm of the beam splitter, respectively. Therefore, the outcome of the measurement is provided by the tuple of integers (n, m). The conditional probability given state $|\alpha_k\rangle$ is the bi-variate Poisson distribution:

$$p_{\mathrm{WF}}(n, m|\alpha_k) = \mathcal{P}_n\left(\mu_k^{(t)}|\alpha_k\right)\mathcal{P}_m\left(\mu_k^{(r)}|\alpha_k\right) . \tag{4}$$

In the second strategy, referred to as homodyne-like (HL) receiver, we use the single photon-number-resolving outputs to only evaluate, in post-processing, the photon-number difference, $\Delta = n - m$, $\Delta \in Z$. In turn, the probability distribution $p_{\mathrm{HL}}(\Delta|\alpha_k)$ follows a Skellam distribution [10]:

$$\begin{aligned} p_{\mathrm{HL}}(\Delta|\alpha_k) &= \sum_{m=0}^{\infty}\mathcal{P}_{m+\Delta}\left(\mu_k^{(t)}|\alpha_k\right)\mathcal{P}_m\left(\mu_k^{(r)}|\alpha_k\right) \\ &= e^{-\mu_k^{(t)}-\mu_k^{(r)}}\left(\mu_k^{(t)}\right)^{\Delta}\sum_{m=0}^{\infty}\frac{\left(\mu_k^{(t)}\mu_k^{(r)}\right)^m}{m!(\Delta+m)!} \\ &= e^{-\mu_k^{(t)}-\mu_k^{(r)}}\left[\frac{\mu_k^{(t)}}{\mu_k^{(r)}}\right]^{\Delta/2} I_{\Delta}\left(2\sqrt{\mu_k^{(t)}\mu_k^{(r)}}\right) , \end{aligned} \tag{5}$$

where $I_{\Delta}(x)$ is the modified Bessel function of the first kind. Moreover, as demonstrated in [10,14], the Skellam distribution converges to a homodyne (Gaussian) distribution in the limit of macroscopic LO, $z^2 \to \infty$. Finally, the last strategy requires further post-processing on the HL data, drawing inspiration on the methods of quantum-state discrimination theory, and, thus, referred to in the following as binary discrimination strategy (BDS) [1,27,31,32]. In more detail, in the BDS we design a binary positive-operator-valued measurement (POVM), retrieving the two integer outcomes $j = 0, 1$, that directly infers which was the state $|\alpha_k\rangle$ generated by the sender. This binary POVM is constructed by evaluating the sign of the measured photon-number difference $\Delta = n - m$. In particular, given the phase space representation associated with BPSK encoding, we set outcome $j = 0$ if a negative difference $\Delta<0$ is obtained, and $j = 1$ if the measured difference is positive, *i.e.* $\Delta>0$, while, in the case $\Delta = 0$, we perform a random decision between $j = 0$ and $j = 1$, with equal probability. The corresponding conditional probability $p_{\mathrm{BDS}}(j|\alpha_k)$ then reads:

$$\begin{aligned} p_{\mathrm{BDS}}(0|\alpha_k) &= \sum_{\Delta<0} p_{\mathrm{HL}}(\Delta|\alpha_k) + \frac{p_{\mathrm{HL}}(\Delta = 0|\alpha_k)}{2} \\ p_{\mathrm{BDS}}(1|\alpha_k) &= 1 - p_{\mathrm{BDS}}(0|\alpha_k) . \end{aligned} \tag{6}$$

We also note that, due to the non-orthogonality of the encoded coherent states, the distribution $p_{\mathrm{BDS}}(j|\alpha_k)$ is nontrivial, since there is always a nonzero probability to infer the wrong symbol, i.e. $p_{\mathrm{BDS}}(j \neq k|\alpha_k) \neq 0$, which, in the context of BPSK discrimination, leads to a nonzero decision error probability [1,27,31,32].

In the following, we address the performance of these three strategies in two different quantum communication contexts. At first, we address a genuine communication protocol and quantify the information transmission between Alice and Bob over the proposed channel. Thereafter, we consider possible applications to CVQKD.

Optics EXPRESS

2.1. Information transmission over the channel

To begin with, we compute the information rate transmitted over the channel, quantified by the MI, which yields the amount of information encoded at the source that Bob is effectively able to extract from his probed statistics. In general, given two stochastic variables A and B, associated with probabilities $p_A(x_A)$, $x_A \in A$, and $p_B(x_B)$, $x_B \in B$, and a communication channel $X \to Y$ described by the conditional probability distribution $p_{B|A}(x_B|x_A)$, the MI is defined as [33]:

$$I(A;B) = H(B) - H(B|A)\,, \tag{7}$$

expressed in bits per channel use, where $H(B) = \mathsf{H}[p_B(x_B)]$ is the overall entropy of B, with $p_B(x_B) = \sum_{x_A \in A} p_A(x_A) p_{B|A}(x_B|x_A)$, and $H(B|A) = \sum_{x_A \in A} p_A(x_A) \mathsf{H}[p_{B|A}(x_B|x_A)]$ is the average conditional Shannon entropy of B if A is given, in which

$$\mathsf{H}[p(x)] = -\sum_x p(x) \log_2 p(x) \tag{8}$$

represents the Shannon entropy of a probability distribution $p(x)$ [33].

Keeping this in mind, we now compare the MI for the three methods under the assumption that Alice encodes binary information on symbols $k = 0, 1$, with equal a priori probability $q_k = 1/2$, while Bob performs different measurement strategies, associated with different conditional probabilities, and different amounts of MI. In more detail, for the WF receiver we have:

$$\begin{aligned} I_{\mathrm{WF}}(A;B) &= \mathsf{H}\left[\sum_{k=0,1} q_k p_{\mathrm{WF}}(n,m|\alpha_k)\right] - \sum_{k=0,1} q_k\, \mathsf{H}\left[p_{\mathrm{WF}}(n,m|\alpha_k)\right] \\ &= -\sum_{n,m=0}^{\infty} \left(\sum_k q_k p_{\mathrm{WF}}(n,m|\alpha_k)\right) \log_2 \left(\sum_k q_k p_{\mathrm{WF}}(n,m|\alpha_k)\right) \\ &\qquad + \sum_k q_k \left[\sum_{n,m=0}^{\infty} p_{\mathrm{WF}}(n,m|\alpha_k) \log_2 p_{\mathrm{WF}}(n,m|\alpha_k)\right], \end{aligned} \tag{9}$$

while for the HL:

$$\begin{aligned} I_{\mathrm{HL}}(A;B) &= \mathsf{H}\left[\sum_{k=0,1} q_k p_{\mathrm{HL}}(\Delta|\alpha_k)\right] - \sum_{k=0,1} q_k\, \mathsf{H}\left[p_{\mathrm{HL}}(\Delta|\alpha_k)\right] \\ &= -\sum_{\Delta=-\infty}^{\infty} \left(\sum_k q_k p_{\mathrm{HL}}(\Delta|\alpha_k)\right) \log_2 \left(\sum_k q_k p_{\mathrm{HL}}(\Delta|\alpha_k)\right) \\ &\qquad + \sum_k q_k \left[\sum_{\Delta=-\infty}^{\infty} p_{\mathrm{HL}}(\Delta|\alpha_k) \log_2 p_{\mathrm{HL}}(\Delta|\alpha_k)\right], \end{aligned} \tag{10}$$

and, eventually, for the BDS:

$$\begin{aligned} I_{\mathrm{BDS}}(A;B) &= \mathsf{H}\left[\sum_{k=0,1} q_k p_{\mathrm{BDS}}(j|\alpha_k)\right] - \sum_{k=0,1} q_k\, \mathsf{H}\left[p_{\mathrm{BDS}}(j|\alpha_k)\right] \\ &= -\sum_{j=0,1} \left(\sum_k q_k p_{\mathrm{BDS}}(j|\alpha_k)\right) \log_2 \left(\sum_k q_k p_{\mathrm{BDS}}(j|\alpha_k)\right) \\ &\qquad + \sum_k q_k \left[\sum_{j=0,1} p_{\mathrm{BDS}}(j|\alpha_k) \log_2 p_{\mathrm{BDS}}(j|\alpha_k)\right]. \end{aligned} \tag{11}$$

Given these expressions, it is worth to investigate which strategy yields the highest value of MI. Therefore, we remind a fundamental result of information theory, namely the data processing

Optics EXPRESS

inequality, stating that any post-processing of data implies a loss of bits, and thus a reduction of MI [14,33]. In our scenario we expect the following hierarchy to hold: $I_{\mathrm{WF}}(A;B) \geq I_{\mathrm{HL}}(A;B) \geq I_{\mathrm{BDS}}(A;B)$. Nevertheless, in the presence of PSK modulation, the WF and HL are equivalent in terms of MI. In fact, implementing WF detection, retrieving the outcome (n,m) is equivalent to perform joint measurement of both the sum and difference photocurrents $\sigma = n+m$, and $\Delta = n-m$, respectively, with $\sigma \in \mathbb{N}$ and $\Delta \in \mathbb{Z}$. In turn, the joint probability $P(\sigma,\Delta|\alpha_k)$ contains the same amount of information on the encoded signal as $p_{\mathrm{WF}}(n,m|\alpha_k)$. Moreover, the distribution can be re-expressed as $P(\sigma,\Delta|\alpha_k) = p_{\mathrm{HL}}(\Delta|\alpha_k)f(\sigma,\Delta)$, for a suitable function $f(\sigma,\Delta)$, being independent of α_k and satisfying $\sum_\sigma f(\sigma,\Delta) = 1$. Accordingly, information on the signal phase is only carried by the difference photocurrent, and, after straightforward calculation, we get $I_{\mathrm{WF}}(A;B) = I_{\mathrm{HL}}(A;B)$.

However, in practical implementations, one should also design suitable reconciliation codes to practically extract a finite number of bits from the output statistics of the receivers, which would introduce further loss of bits, thus making the analysis of suboptimal methods like BDS still worth of investigation.

3. Experimental implementation

3.1. Setup and preliminary characterization

In this paragraph, we give a more detailed description of the detector based on SiPMs. In particular, we are interested in demonstrating that such a scheme can be embedded in quantum communication protocols, both for information transmission and CVQKD.

The experimental setup is shown in Fig. 1. The second-harmonic pulses (at 515 nm, 190 fs pulse duration) of a Yb:KGW laser operated at 5 kHz are sent to a Mach-Zehnder interferometer, whose input beam splitter divides the light beam into two parts: in one arm we have the signal, while in the other arm the LO. The length of one arm of the interferometer is controlled in steps by means of a piezoelectric movement (Pz) in order to modify the LO phase through the whole 2π range. Indeed, the selection of the states $|\alpha\rangle$ and $|-\alpha\rangle$ is obtained in post-processing by the comparative analysis of the mean value of the light as a function of the LO phase and of the photon-number difference distribution, as already explained in Refs. [8,10]. This operation is performed for different attenuations of the signal and LO obtained by means of two variable neutral density (ND) filters. To optimize the overlap between the signal and the LO beams in the second beam splitter of the interferometer, we worked on the control of the polarization of the beams as well as on their spatio-temporal superposition. In particular, we reduced the beam size to make its attenuation uniform on the variable density filter. Concerning the temporal superposition, we used a piezoelectric movement of the translation stage in one arm of the interferometer to optimize it (see Fig. 1).

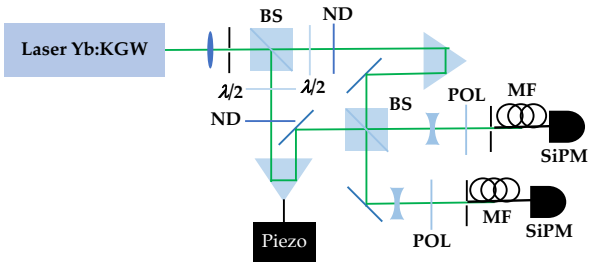

Fig. 1. Sketch of the experimental setup to realize the SiPM-based receiver: BS, beam splitter; $\lambda/2$, half-wave plate; ND, variable neutral-density filter; Piezo, piezoelectric mounted on a translation stage; POL, polarizer; MF, multi-mode fiber; SiPM, Silicon photomultiplier.

Optics EXPRESS

At the two outputs of the second beam splitter two collection systems are placed. They are formed by a pin-hole with a fixed aperture and a multi-mode fiber with a 1 mm core that delivers the light to two SiPMs. The model that we use is the MPPC S13360-1350CS produced by Hamamatsu Photonics [34], which consists of 667 pixels in a 1.3×1.3 mm^2 photosensitive area, with a pixel pitch equal to 50 μm. This kind of detector is endowed with a good photon-number-resolving capability and is operated at room temperature. The output of each detector is amplified by a fast inverting amplifier with a gain of 24 dB embedded in the computer-based Caen SP5600 Power Supply and Amplification Unit, synchronously integrated by a boxcar-gated integrator, and digitized. We choose an integration gate of 15 ns centered around the peak of the amplified signal [20]. This kind of detector is known to have a high dark-count rate, corresponding to 90 kHz for the model used in this experiment. Considering the 15 ns integration time, this corresponds to 1.3 $10^{(-3)}$ dark-count events per measured pulse, on average. To consider the effect of the whole acquisition chain, we performed an experimental dark measurement of 10^5 samples, and obtained a value of about 0.3% of dark counts for both the detectors. Also taking into account this second value, in the theoretical description of the receiver dark-count contribution can be considered negligible compared with the introduced losses.

To perform the experimental acquisition, for each condition of signal and LO, 10^5 pulses are collected. A typical trace, for a given value of signal and LO, and a typical reconstructed pulse-height spectrum are shown in Fig. 2(a) and (b), respectively [22].

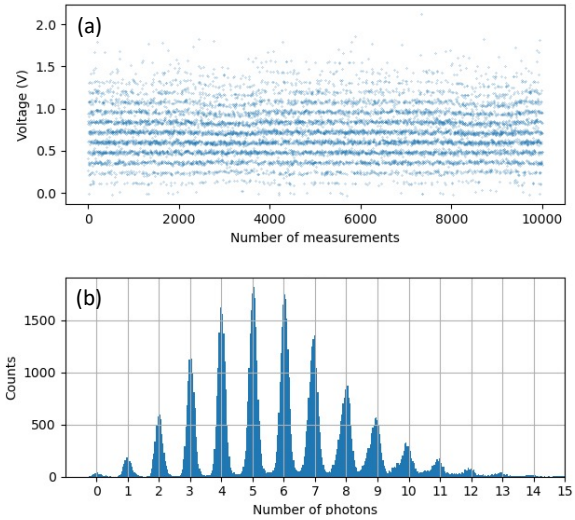

Fig. 2. (a) Typical trace of 10^4 shots acquired by a SiPM embedded in the hybrid scheme; (b) example of pulse-height spectrum corresponding to a mean value $\langle m \rangle = 5.77$.

3.2. *Experimental results on information transmission*

The characterization of the SiPM-based receiver used for state discrimination can be obtained as a function of some important parameters, namely the energy of the LO and the losses affecting the signal. In particular, in Fig. 3 we consider the behavior of $I(A;B)$ as a function of the mean number of LO photons for a fixed mean number of signal photons ($\langle m_{\mathrm{sig}} \rangle = 3.07$). The data obtained from the WF receiver are shown as green dots, those from the HL receiver as red dots, and those from the BDS receiver as blue dots. We immediately note that the first two methods give the same results since the corresponding data are perfectly superimposed, while the data corresponding to BDS are lower. The experimental results are superimposed on the numerical expectations (see the highlighted bands in the same figure), calculated according to

Optics EXPRESS

Eqs. (9)-(11) with an overlap ranging from $\xi = 0.86$ to $\xi = 0.91$. The colored dashed curves represent the theoretical expectation limits for $\xi = 0.86$ (lower curve) and $\xi = 0.91$ (upper curve). The variation of ξ is caused by the fact that changing the LO intensity by means of the ND filter could slightly change the overlap between the interfering beams at the beam splitter. Despite these imperfections, from the analysis of Fig. 3 we can observe that MI reaches values larger than 0.98 quite rapidly. Indeed, the asymptotic value that can be achieved for $\langle m_{\mathrm{LO}} \rangle \to \infty$ is equal to 1 in the case of BPSK protocols. Experimentally, the maximum value of MI is obtained for the highest mean value we measured, namely $\langle m_{\mathrm{LO}} \rangle = 12.17$.

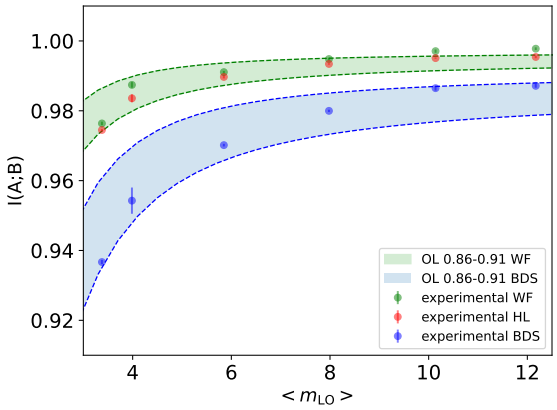

Fig. 3. MI as a function of the mean value of LO, for a fixed mean value of the signals, $\langle m_{\mathrm{sig}} \rangle = 3.07$: green dots refer to the WF receiver, red dots to the HL receiver, and blue dots to the BDS receiver. Dots + error bars: experimental data; dashed lines: results from numerical expectations, in which we assumed $\xi = 0.86$ (lower curve) and $\xi = 0.91$ (higher curve). The highlighted bands were calculated according to Eqs. (9)-(11) with an overlap ranging from $\xi = 0.86$ to $\xi = 0.91$.

As a second step of investigation, we consider the effect of losses affecting the signal. To this aim, we set the mean value of LO at $\langle m_{\mathrm{LO}} \rangle = 12.15$, and vary the energy of the signal by means of the variable ND filter shown in Fig. 1 from $\langle m_{\mathrm{sig}} \rangle = 3.20$ to $\langle m_{\mathrm{sig}} \rangle = 0.14$, thus considering a maximum 13.44 dB loss. The experimental results corresponding to MI are shown in Fig. 4 as functions of the losses affecting the signal. The experimental data are shown as colored dots, respectively, while the numerical expectations are presented as solid curves with the same color choice. As in the case of Fig. 3, green dots refer to the WF receiver, red dots to the HL receiver, and blue dots to the BDS receiver. Again, the agreement between the experimental data and numerical expectations is achieved assuming a non-perfect overlap, that in this kind of investigation is $\xi = 0.94$. While we observe that there is a perfect overlap between the data corresponding to WF and HL methods (and the same holds for the theoretical expectations), lower values of MI are obtained through the BDS, as already discussed in the previous Section. Moreover, in the same figure we plot, as cyan line, the expected results obtained from a standard homodyne receiver, having the same overlap as our experimental receiver. We can notice that the performance of the two detection systems is quite similar, despite the fact that our detector is based on discrete quantities (numbers of photons), while standard homodyne detection relies on continuous variables. This means that the proposed receiver can be considered as a valid alternative to the more common technique, having the advantage of a low-energy LO.

3.3. *Towards applications in continuous-variable quantum key distribution*

The interest in investigating a SiPM-based detection scheme can be further extended to the field of CVQKD, with nontrivial consequences. In fact, it has been recently demonstrated that the

Optics EXPRESS

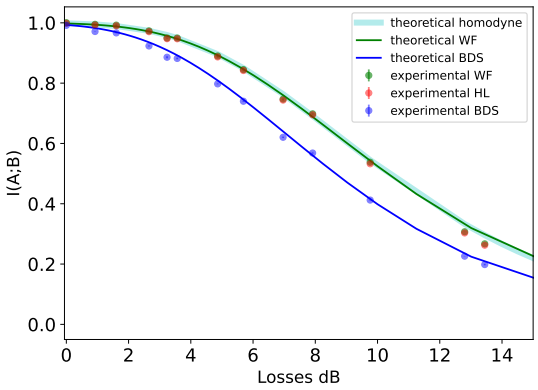

Fig. 4. MI as a function of the losses affecting the signal arm, for a fixed mean value of the LO, $\langle m_{\mathrm{LO}} \rangle = 12.15 \sim 4\langle m_{\mathrm{sig}} \rangle_{\mathrm{MAX}}$. Green dots refer to the WF receiver, red dots to the HL receiver, and blue dots to the BDS receiver. Dots + error bars: experimental data; colored lines: results from numerical expectations (HL and WF correspond to the same curve); cyan line: theoretical prediction of the standard homodyne receiver. In the numerical and homodyne predictions we assumed $\xi = 0.94$.

optimal strategies for state discrimination, information transmission and CVQKD differ from one another, even if based on the same kind of detection system [16]. For instance, the POVM that optimizes the MI is not the same as minimizing the error probability in a discrimination problem. In fact, it is well-known that in the case of a homodyne-like scheme exploited for state discrimination the best strategy corresponds to the BDS one [10].

Now, let us consider the communication channel between Alice and Bob to be eavesdropped by a third party, Eve. Alice and Bob's goal is to share a common random secure key. In the simplest case, Alice generates randomly one of the two symbols $k = 0, 1$, with corresponding probability $q_k = 1/2$, and Bob retrieves a set of data correlated to Alice's ones.

The key is tipically extracted from Alice and Bob's datasets after a reconciliation stage, which can be performed according to either Alice's data (DR) or Bob's data (RR).

In this work, since we did not experimentally perform the reconciliation protocol, we consider as a figure of merit the key generation rate (KGR), defined as the difference between the MI between Alice and Bob and the one acquired by Eve. We investigate security by considering both individual attacks (IA) and collective attacks (CA). In the first case, the eavesdropper measures individually each sent pulse, in the second a final joint collective measurement is performed over many transmitted signals according to either DR or RR, respectively [35].

In general, the security can be addressed under different paradigms, according to the level of trust of the quantum channel [36]. Here, we assume a restrictive eavesdropping scenario under a wiretap channel. In other words, we assume the transmission channel to be completely characterized in terms of a pure-loss channel, so that Eve has only access to the fraction of the signals lost during transmission, without either performing any arbitrary channel manipulation or injecting noise in the system [16,23]. Given this consideration, when Alice sends the state $|\alpha_k\rangle$, Bob and Eve receive the transmitted and reflected fractions $|\sqrt{T}\alpha_k\rangle$ and $|\sqrt{1-T}\alpha_k\rangle$, respectively.

We start with the IA scenario for the receiver that guarantees higher values of MI, that is the WF receiver. In this case, we assume Eve to hold the same receiver as Bob in its best performing solution. Thus, Eve has at her disposal a WF receiver with unit visibility $\xi_E = 1$. For the sake of simplicity, in this scenario we also consider Bob to hold a WF receiver, albeit with reduced visibility $\xi_B < 1$. The corresponding KGR reads

$$\Delta I_{\mathrm{WF}}^{(\mathrm{IA})} = I_{\mathrm{WF}}(A;B) - I_{\mathrm{WF}}(A;E) \qquad \text{for DR}\,, \tag{12}$$

Optics EXPRESS

with $I_{\rm WF}(A;E)$ computed according to Eq. (9), with the substitutions $T \to 1-T$ and $\xi_E = 1$, and:

$$\Delta I_{\rm WF}^{\rm (IA)} = I_{\rm WF}(A;B) - I_{\rm WF}(B;E) \qquad \text{for RR}\,, \tag{13}$$

in which the MI $I_{\rm WF}(B;E)$ is derived from the joint probability distribution of Alice, Bob and Eve:

$$p_{ABE}(k;n_B,m_B;n_E,m_E) = q_k p_{\rm WF}^{(B)}(n_B,m_B|\alpha_k) p_{\rm WF}^{(E)}(n_E,m_E|\alpha_k)\,, \tag{14}$$

in which $p_{\rm WF}^{(B(E))}$ is given in (4) with the parameters T and ξ_B for Bob's side, and $1-T$ and $\xi_E = 1$ for Eve's. Ultimately, we have $I_{\rm WF}(B;E) = H(E) - H(E|B) = H(B) + H(E) - H(BE)$, where $H(BE)$, $H(B)$ and $H(E)$ are the Shannon entropy of the distributions $p_{BE}(n_B,m_B;n_E,m_E) = \sum_k p_{ABE}(k;n_B,m_B;n_E,m_E)$, $p_B(n_B,m_B) = \sum_k q_k p_{\rm WF}^{(B)}(n_B,m_B|\alpha_k)$, and $p_E(n_E,m_E) = \sum_k q_k p_{\rm WF}^{(E)}(n_E,m_E|\alpha_k)$, respectively.

On the other hand, in the presence of CA, the MI at Eve's side should be replaced by the Holevo information $\chi(A;E)$ and $\chi(B;E)$ for DR and RR, respectively, providing the maximum amount of information extractable from the ensemble of eavesdropped signals compatible with quantum mechanics laws. However, since DR is inevitably associated with a bound of 3 dB transmission (see the next Section), due to the symmetry of the channel, here we only consider the RR case, providing a more effective solution. Then, we have:

$$\Delta I_{\rm p}^{\rm (CA)} = I_{\rm p}(A;B) - \chi_{\rm p}(B;E), \qquad ({\rm p} = {\rm WF, HL, BDS}), \tag{15}$$

where

$$\chi_{\rm p}(B;E) = S(E) - S_{\rm p}(E|B) \tag{16}$$

is the Holevo information between Bob and Eve [16]. In the former expression, $S(E) = S[\rho_E]$, where $\rho_E = \sum_k q_k |\sqrt{1-T}\alpha_k\rangle\langle\sqrt{1-T}\alpha_k|$, and $S[\rho] = -{\rm Tr}[\rho \log_2(\rho)]$ is the Von-Neumann entropy of the state ρ, whereas $S_{\rm p}(E|B)$ is Eve's entropy conditioned to Bob. In particular, for the WF case we have:

$$S_{\rm WF}(E|B) = \sum_{n_B,m_B} p_{\rm WF}^{(B)}(n_B,m_B)\, S[\rho_{E|(n_B,m_B)}]\,, \tag{17}$$

in which $p_{\rm WF}^{(B)}(n_B,m_B) = \sum_k q_k p_{\rm WF}^{(B)}(n_B,m_B|\alpha_k)$ is the overall distribution of the WF receiver, and

$$\rho_{E|(n_B,m_B)} = \frac{1}{2p_{\rm WF}^{(B)}(n_B,m_B)} \sum_{k=0,1} p_{\rm WF}^{(B)}(n_B,m_B|\alpha_k) \left|\sqrt{1-T}\alpha_k\right\rangle \left\langle\sqrt{1-T}\alpha_k\right| \tag{18}$$

is the corresponding conditional state received by Eve [15,16]. Also in this context, we show that WF and HL are again equivalent, as $\rho_{E|(n_B,m_B)} = \rho_{E|\Delta}$, with $\Delta = n_B - m_B$, thus $S_{\rm WF}(E|B) = S_{\rm HL}(E|B)$, while the conditional entropy in the presence of BDS is:

$$S_{\rm BDS}(E|B) = \sum_{j=0,1} p_{\rm BDS}(j)\, S[\rho_{E|j}]\,, \tag{19}$$

in which $p_{\rm BDS}(j) = \sum_k q_k p_{\rm BDS}(j|\alpha_k)$ and the state $\rho_{E|j}$ is computed from (18), provided the substitution $p_{\rm WF}^{(B)}(n_B,m_B|\alpha_k) \to p_{\rm BDS}(j|\alpha_k)$.

3.4. Experimental results

In Fig. 5, we show the MI as a function of channel transmittance in the presence of individual attacks. For the sake of completeness, we consider both DR and RR strategies, and we assume that both Bob and Eve employ photon-number-resolving detectors, and in particular WF method. However, to test the possible advantages of Eve over Bob, we consider a perfect overlap for the

Optics EXPRESS

eavesdropper compared to the non-perfect overlap ($\xi = 0.94$) corresponding to Bob. Moreover, we assume that all the losses experienced by Bob correspond to the signal intercepted by Eve. In panel (a) we compare the experimental values of $I_{\mathrm{WF}}(A;B)$ with the numerical expectations of $I_{\mathrm{WF}}(A;E)$, which correspond to the case of DR, and those of $I_{\mathrm{WF}}(B;E)$, which correspond to the case of RR. In particular, from the figure we can easily appreciate for which values the MI between Alice and Bob surpasses that between Alice (or Bob) and Eve. As expected, the more effective strategy is to use RR instead of DR. Indeed, the communication rapidly drops in the case of DR becoming negative for losses values close to 3 dB, while it decreases more smoothly in the case of RR. In this second case, $I_{\mathrm{WF}}(A;B)>I_{\mathrm{WF}}(B;E)$ even for large values of losses. In panels (b) and (c) of the same figure, we show the modulus of the quantities K_{DR} and K_{RR}, respectively, defined as the normalized KGR between Alice and Bob in the presence of individual attacks, namely

$$K_{\mathrm{DR}} = \frac{I_{\mathrm{WF}}(A;B) - I_{\mathrm{WF}}(A;E)}{I_{\mathrm{WF}}(A;B)}$$
$$K_{\mathrm{RR}} = \frac{I_{\mathrm{WF}}(A;B) - I_{\mathrm{WF}}(B;E)}{I_{\mathrm{WF}}(A;B)}. \tag{20}$$

We point out that the full circles correspond to positive values of K_{DR} and K_{RR}, while open symbols to negative ones. Indeed, the calculation of the quantities in Eqs. (20) starting from real data is quite delicate when the absolute values become small, namely smaller than 10^{-3}. In that case, the effect of noise due to the detection system, such as the cross talk of SiPM or the electronic noise of the boxcar-gated integrators [20], could play a detrimental role, which is instead not visible in the pure calculation of MI.

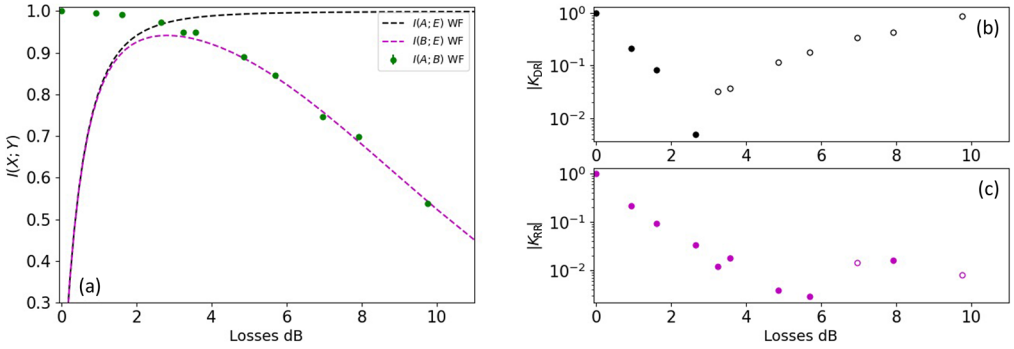

Fig. 5. IA scenario. (a) MI $I_{\mathrm{WF}}(A;B)$ (experimental data, green dots), $I_{\mathrm{WF}}(A;E)$ (numerical expectation, black curve) and $I_{\mathrm{WF}}(B;E)$ (numerical expectation, magenta curve) as functions of the losses affecting the signal arm, for a fixed mean value of the LO, $\langle m_{\mathrm{LO}} \rangle = 12.15$, in a semi-logarithmic scale. In the numerical expectations we assumed $\xi_{\mathrm{B}} = 0.94$ and $\xi_{\mathrm{E}} = 1$. (b) and (c): $|K_{\mathrm{DR}}|$ and $|K_{\mathrm{RR}}|$ as functions of the losses affecting the signal arm, respectively. Full (open) symbols refer to positive (negative) values of K_{DR} and K_{RR}.

As a further investigation, we consider collective attacks. In this case, we have to calculate the Holevo bound, which is an upper limit for MI. Indeed, this definition is useful to define a lower bound for the KGR. By following Ref. [15], we consider the asymptotic limit in which infinitely many signals are shared between Alice and Bob, thus neglecting any possible finite-size effect arising with finite datasets. Similarly to the case of individual attacks, also for collective ones we exploit the experimental data for the calculation of the MI between Alice and Bob, while we use the numerical expectation for the calculation of the Holevo bound. In particular, we only consider RR since it is more effective than DR. We remark that these results are obtained as theoretical definitions of the considered figures of merit and not from a real implementation of

Optics EXPRESS

the protocol. The results are shown in Fig. 6 both for WF, coinciding with HL, and BDS methods. As expected, the former method must be preferred to the other one since it guarantees higher values of MI. Moreover, for both the receivers $I(A;B)$ surpasses the Holevo bound for small values of losses, while the situation becomes more critical for larger values. This can be better appreciated by the evaluation of the normalized KGR between Alice and Bob in the presence of collective attacks, that is

$$K = \frac{I_{\mathrm{p}}(A;B) - \chi_{\mathrm{p}}(B;E)}{I_{\mathrm{p}}(A;B)}, \tag{21}$$

with p =WF or BDS. The experimental values of $|K|$ are shown in panels (b) and (c) of the same figure for WF and BDS receivers, respectively. Again, full circles correspond to positive values of K and open symbols to negative ones. We can easily observe that, at increasing losses, the values of K are more negative. As already discussed about Fig. 5, we ascribe this behavior to the possible noise sources affecting the detection chain. In principle, further improvements of the setup and a more optimal choice of the parameters could lead to more stable results. In light of these results, it is also instructive to make a comparison between the WF receiver and standard homodyne detection in terms of KGR. To this aim, in Fig. 7(a) we show the numerical expectations of KGR for individual attacks both in the case of DR and RR. In general, we can observe that the two receivers behave similarly as a function of the losses affecting the signal. Indeed, in the case of DR there is an abrupt drop in communication for losses around 3 dB, while in the case of RR the decrease is gentler. The same holds for collective attacks, shown in Fig. 7(b) in the case of RR. The KGR as a function of losses obtained by means of standard homodyne detection is indistinguishable from that achieved by using the WF receiver and both smoothly decrease at increasing values of losses. We can therefore conclude that even for applications to CVQKD, our receiver represents a viable alternative to the conventional technique, but it has the advantage of using fewer resources and being less critical of possible instabilites and balancing issues. Moreover, in view of a real implementation of a CVQKD protocol, optimization procedures will be adopted to increase the absolute values of KGR.

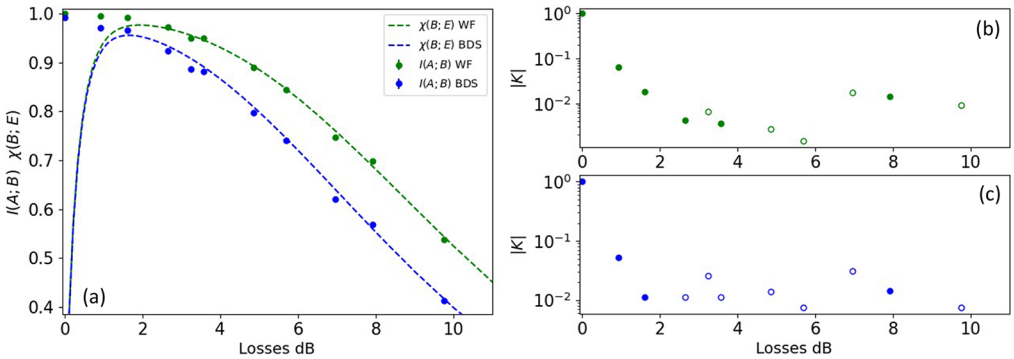

Fig. 6. CA scenario. (a) MI $I_{\mathrm{WF}}(A;B)$ and $I_{\mathrm{BDS}}(A;B)$ (experimental data, green and blue dots, respectively), $\chi_{\mathrm{WF}}(B;E)$ and $\chi_{\mathrm{BDS}}(B;E)$ (numerical expectations, green and blue curve, respectively) as functions of the losses affecting the signal arm, for a fixed mean value of the LO, $\langle m_{\mathrm{LO}} \rangle = 12.15$, in a semi-logarithmic scale. In the numerical expectations we assumed $\xi_{\mathrm{B}} = 0.94$ and $\xi_{\mathrm{E}} = 1$. (b) and (c) $|K|$ as a function of the losses affecting the signal arm for WF and BDS receiver, respectively. Full (open) symbols refer to positive (negative) values of K.

Optics EXPRESS

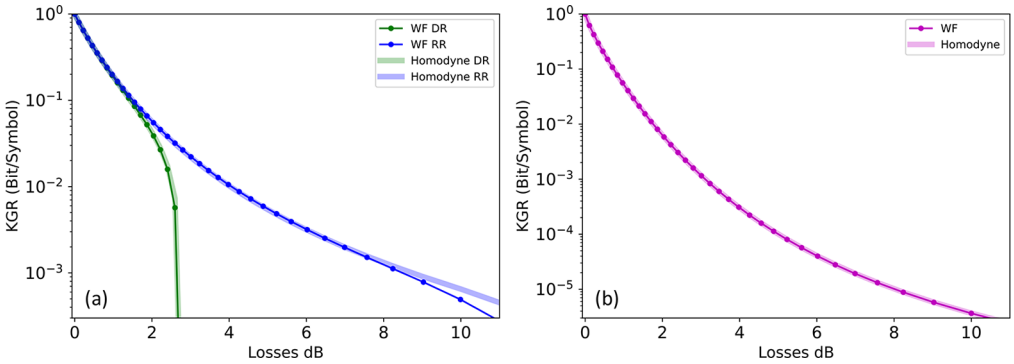

Fig. 7. (a) KGR as a function of the losses affecting the signal arm in a semi-logarithmic scale in the IA scenario. Solid line + symbol: theoretical prediction of the WF receiver; highlighted line: theoretical prediction of the standard homodyne receiver. Green tones refer DR, while blue tones to RR. (b) The same as in (a) in the CA scenario in the case of RR. In both panels and for both receivers, we assumed a fixed mean value of the LO, $\langle m_{\mathrm{LO}} \rangle = 12.15$, $\xi_{\mathrm{B}} = 0.94$ and $\xi_{\mathrm{E}} = 1$.

4. Conclusion

In this work, we investigated the performance of SiPM detectors in the context of quantum communication. In particular, we considered a receiver exploiting the interference of a coherent signal with a LO before photodetection. As a figure of merit, we evaluated the MI in a BPSK protocol in the presence of losses and low intensity LO. Our results concerning the information transmission over the channel highlight its robusness with respect to losses taking also into account the non-unit visibility of the receiver. This represents the basic element to develop more complex setups, such as the HYNORE receiver [25], to perform quasi-optimal discrimination strategies. In this case, the application of the BDS receiver is the first step, depending on which the second step, given by the use of a photon-number-resolving detector, and thus of a WF receiver, is implemented. In this respect, the HYNORE receiver has a very hybrid nature. In this view we plan to extend our analysis to higher order modulation formats, such as the amplitude PSK, and more advanced detection schemes.

Eventually, we studied a possible development towards CVQKD in the simplest case of a binary alphabet, where the obtained, though limited, promising results related to the evaluation of the KGR suggest further investigations with larger alphabets up to a continuous modulation. Moreover, in the case of a real implementation of a CVQKD protocol, optimization stages, such as practical reconciliation or privacy amplification, will be properly adopted to improve the absolute values of KGR.

From the practical point of view, to make the scheme more versatile, we plan to explore its extension in the telecom wavelengths range, for instance, realizing the optical part of the setup into optical fibers, while leaving the detection in the visible region and by using a sum-frequency generation process before the detection stage.

Funding. Ministero dell'Università e della Ricerca (PNRR D.D.M.M. 351/2022, PNRR D.D.M.M. 737/2021).

Acknowledgments. We thank Maristella Crotti (University of Insubria) for her assistance in the early stage of the experiment and Maria Bondani (Institute for Photonics and Nanotechnologies, CNR) for fruitful discussions.

Disclosures. The authors declare no conflicts of interest.

Data availability. The datasets generated and analyzed during the current study are available from the corresponding authors on reasonable request.

Optics EXPRESS

References

1. G. Cariolaro, *Quantum Communications* (Springer International Publishing, 2015).
2. F. Flamini, N. Spagnolo, and F. Sciarrino, "Photonic quantum information processing: a review," Rep. Prog. Phys. **82**(1), 016001 (2019).
3. F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Phys. Rev. Lett. **88**(5), 057902 (2002).
4. E. Diamanti, H.-K. Lo, and B. Qi, "Practical challenges in quantum key distribution," Npj Quantum Inf. **2**(1), 16025 (2016).
5. S. Olivares, S. Cialdi, and F. Castelli, "Homodyne detection as a near-optimum receiver for phase-shift-keyed binary communication in the presence of phase diffusion," Phys. Rev. A **87**(5), 050303 (2013).
6. A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," Rev. Mod. Phys. **81**(1), 299–332 (2009).
7. G. Donati, T. J. Bartley, and X.-M. Jin, "Observing optical coherence across Fock layers with weak-field homodyne detectors," Nat. Commun. **5**(1), 5584 (2014).
8. A. Allevi, M. Bina, and S. Olivares, "Homodyne-like detection scheme based on photon-number-resolving detectors," Int. J. Quantum Inform. **15**(08), 1740016 (2017).
9. S. Olivares, A. Allevi, and G. Caiazzo, "Quantum tomography of light states by photon-number-resolving detectors," New J. Phys. **21**(10), 103045 (2019).
10. M. Bina, A. Allevi, and M. Bondani, "Homodyne-like detection for coherent state-discrimination in the presence of phase noise," Opt. Express **25**(9), 10685 (2017).
11. A. Martinez, "Spectral efficiency of optical direct detection," J. Opt. Soc. Am. B **24**(4), 739–749 (2007).
12. M. Cheraghchi and J. Ribeiro, "Improved upper bounds and structural results on the capacity of the discrete-time Poisson channel," IEEE Trans. Inform. Theory **65**(7), 4052–4068 (2019).
13. K. Łukanowski and M. Jarzyna, "Capacity of a Lossy Photon Channel With Direct Detection," IEEE Trans. Commun. **69**(8), 5059–5068 (2021).
14. M. N. Notarnicola and S. Olivares, "Employing weak-field homodyne detection for quantum communications," arXiv, 2024.
15. M. Cattaneo, M. G. A. Paris, and S. Olivares, "Hybrid quantum key distribution using coherent states and photon-number-resolving detectors," Phys. Rev. A **98**(1), 012333 (2018).
16. M. N. Notarnicola, M. Jarzyna, and S. Olivares, "Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel," New J. Phys. **25**(10), 103014 (2023).
17. R. S. Kennedy, "A Near-Optimum Receiver for the Binary Coherent State Quantum Channel," Quarterly Progress Report. **108**, 219–225 (1973).
18. M. T. DiMario and F. E. Becerra, "Robust Measurement for the Discrimination of Binary Coherent States," Phys. Rev. Lett. **121**(2), 023603 (2018).
19. M. T. DiMario, L. Kunz, and K. Banaszek, "Optimized communication strategies with binary coherent states over phase noise channels," npj Quantum Inf. **5**(1), 65 (2019).
20. G. Chesi, L. Malinverno, and A. Allevi, "Measuring nonclassicality with silicon photomultipliers," Opt. Lett. **44**(6), 1371 (2019).
21. M. Bondani, A. Allevi, and A. Agliati, "Self-consistent characterization of light statistics," J. Mod. Opt. **56**(2-3), 226–231 (2009).
22. S. Cassina, A. Allevi, and V. Mascagna, "Exploiting the wide dynamic range of silicon photomultipliers for quantum optics applications," EPJ Quantum Technol. **8**(1), 4 (2021).
23. Z. Pan, K. P. Seshadreesan, and W. Clark, "Secret-Key Distillation across a Quantum Wiretap Channel under Restricted Eavesdropping," Phys. Rev. Applied **14**(2), 024044 (2020).
24. S. Olivares, A. Allevi, and M. Bondani, "On the role of the local oscillator intensity in optical homodyne-like tomography," Phys. Lett. A. **384**(17), 126354 (2020).
25. M. N. Notarnicola, M. G. A. Paris, and S. Olivares, "Hybrid near-optimum binary receiver with realistic photon-number-resolving detectors," J. Opt. Soc. Am. B **40**(4), 705 (2023).
26. C. W. Helstrom and J. Love, *Quantum Detection and Estimation Theory* (Elsevier, Academic Press, 1976).
27. J. A. Bergou, "Discrimination of quantum states," J. Mod. Opt. **57**(3), 160–180 (2010).
28. S. Izumi, M. Takeoka, and M. Fujiwara, "Displacement receiver for phase-shift-keyed coherent states," Phys. Rev. A **86**(4), 042328 (2012).
29. C. R. Müller and C. H. Marquardt, "A robust quantum receiver for phase shift keyed signals," New J. Phys. **17**(3), 032003 (2015).
30. S. Olivares, "Introduction to generation, manipulation and characterization of optical quantum states," Phys. Lett. A **418**, 127720 (2021).
31. F. E. Becerra, J. Fan, and G. Baumgartner, "Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination," Nat. Photonics **7**(2), 147–152 (2013).
32. F. E. Becerra, J. Fan, and A. Migdall, "Implementation of generalized quantum measurements for unambiguous discrimination of multiple non-orthogonal coherent states," Nat. Commun. **4**(1), 2028 (2013).
33. T. M. Cover, *Elements of information theory* (John Wiley Sons, 1999).

Optics EXPRESS

34. https://www.hamamatsu.com/content/dam/hamamatsu-photonics/sites/documents/99_SALES_LIBRARY/ssd/s13360_series_kapd1052e.pdf.
35. S. Pirandola, "Advances in Quantum Cryptography," Adv. Opt. Photon. **12**(4), 1012–1236 (2020).
36. S. Pirandola, "Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks," Phys. Rev. Res. **3**(4), 043014 (2021).