

PAPER • OPEN ACCESS

Hybrid discrimination strategy in quantum communication based on photon-number-resolving detectors and mesoscopic twin-beam states

To cite this article: Luca Razzoli *et al* 2025 *Quantum Sci. Technol.* **10** 045036

View the [article online](#) for updates and enhancements.

You may also like

- [Enhanced Oxidation Resistance of CrSi-SiC Ceramic Coatings on SiC coated C/C Composites via SiC Nanowires Reinforcement](#)
Xinfa Qiang, Xiangyu Chen, Maoheng Dong et al.
- [Smarter usage of measurement statistics can greatly improve continuous variable quantum reservoir computing](#)
Markku Hahto and Johannes Nokkala
- [Artificial Intelligence Techniques for Precise Current Sensor Fault Diagnosis in Battery Systems Using Enhanced Equivalent Circuit Models](#)
S Mohana Devi and Bagyaveereswaran V

Quantum Science and Technology



PAPER

Hybrid discrimination strategy in quantum communication based on photon-number-resolving detectors and mesoscopic twin-beam states

OPEN ACCESS

RECEIVED
11 June 2025

REVISED
9 August 2025

ACCEPTED FOR PUBLICATION
10 September 2025

PUBLISHED
18 September 2025

Original Content from this work may be used under the terms of the [Creative Commons Attribution 4.0 licence](#).

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



Luca Razzoli^{1,2,4} , Alex Pozzoli³ and Alessia Allevi^{3,*}

¹ Center for Nonlinear and Complex Systems, Department of Science and High Technology, University of Insubria, Via Valleggio 11, I-22100 Como, Italy

² INFN, Sezione di Milano, Via Celoria 16, I-20133 Milano, Italy

³ Como Lake Institute of Photonics, Department of Science and High Technology, University of Insubria, Via Valleggio 11, I-22100 Como, Italy

⁴ Currently at Department of Physics 'Alessandro Volta', University of Pavia, Via Bassi 6, I-27100 Pavia Italy; INFN, Sezione di Pavia, Via Bassi 6, I-27100 Pavia, Italy.

* Author to whom any correspondence should be addressed.

E-mail: alessia.allevi@uninsubria.it

Keywords: twin-beam states of light, state discrimination, mesoscopic intensity regime, photon-number-resolving detectors

Abstract

State discrimination is a key challenge in the implementation of quantum communication protocols. Most optical communication protocols rely on either coherent states of light or fragile single-photon states, making it often difficult to achieve robustness and security simultaneously. In this work, we propose a hybrid strategy that operates in the mesoscopic intensity regime, leveraging robust quantum states of light. Our approach combines classical and quantum features: reliable state discrimination based on a classical property of light, and security stemming from nonclassical correlations. Specifically, the receiver uses photon-number-resolving detectors to access the mean photon number of the binary thermal signals encoding the information. The communication channel exploits twin-beam states, inherently sensitive to eavesdropping attacks, to provide a layer of security. This strategy is scalable, allowing for straightforward extension to more complex signal alphabets, and offers a promising route for robust and secure quantum communication in the mesoscopic intensity domain.

1. Introduction

In communication protocols, the discrimination of the alphabet in which a message is encoded represents a fundamental step [1]. Depending on the complexity of the message and the security of the transmission channel, different strategies can be employed. In particular, the chosen alphabet could involve either discrete [2] or continuous variables [3]. Usually, the main requirement is to develop a receiver that is able to discriminate the sent signals by minimizing the error probability in the discrimination process. To this aim, both direct and homodyne detection systems are commonly used [4, 5]. More recently, hybrid detection systems have also been developed and successfully employed [6–9]. In such schemes, photon-number-resolving (PNR) detectors are embedded in interferometric setups, enabling the use of both discrete and continuous variables.

In most cases, optical communication protocols involve coherent states of light since they are more robust than nonclassical states [10]. However, the use of quantum resources could improve the security of the transmission channels by enabling the detection of eavesdropping attempts [11]. Actually, the main limitation in fully leveraging quantum states lies in their fragility. Indeed, at the single-photon level losses can significantly reduce the rate at which information is sent. Instead, in the mesoscopic intensity domain the optical states contain larger numbers of photons, thus being more robust against external degradation, while still exhibiting the nonclassical properties essential to the successful implementation of the protocol [12, 13]. In this respect, here we introduce a communication protocol, whose transmission channel relies on

the use of mesoscopic twin-beam (TWB) states and the alphabet adopted to encode information consists of two thermal signals with different mean values, superimposed on a twin portion of the above-mentioned TWB [14]. The information thus encoded is transmitted by Alice, the sender, to Bob, whose detector is equipped with PNR capability. This choice allows for direct discrimination based on the mean value of light, assuming no eavesdropping occurs. However, in the case of an intercept-resend attack [15], where Eve intercepts a portion of light transmitted through the communication channel and re-sends a different signal with the same mean value, the discrimination does not guarantee the communication security. Nevertheless, exploiting nonclassical features can reveal the presence of an eavesdropping attack. In that case, the sequence under attack can be discarded and the communication interrupted. Specifically, we leverage the existence of nonclassical correlations in the number of photons of TWB states. This enables Bob to implement a hybrid discrimination strategy, in which he exploits a classical property (the mean value of light) to discriminate and a nonclassical one (the noise reduction factor between the two arms of the TWB) to ensure security.

The reliability of the method is evaluated both in terms of error probability and by adopting figures of merit commonly used in binary classification, which provide insights into the type of error occurring within the communication channel. The investigation is performed as a function of the size of the data samples used to encode the message bits, a critical parameter that significantly impacts the performance of the system. Our results open new perspectives in the use of mesoscopic quantum resources to improve the security of communication channels.

2. Theoretical framework

2.1. Thermal states and mesoscopic TWB states

The communication protocol we propose in this work is based on a binary alphabet, in which the bits 0 and 1 are encoded in two thermal states with different mean values, called noise signals hereafter. The choice leverages the PNR capability of the detection system, consisting of two Silicon photomultipliers (SiPMs) [16–18]: Alice uses one, while Bob uses the other. To be sufficiently general and to take into account the possible nonidealities in the experimental generation of the noise signals to be transmitted, we assume that such states are characterized by a multi-mode thermal distribution (MMTD). In terms of detected photons, to which we have direct access, it can be expressed as [19]

$$P^\mu(m) = \frac{(m + \mu - 1)!}{m! (\mu - 1)! (\langle m \rangle / \mu + 1)^\mu (\mu / \langle m \rangle + 1)^m}, \quad (1)$$

where μ is the effective number of modes, while $\langle m \rangle$ is the mean number of detected photons. The photon-number statistics is super-Poissonian and can be also discriminated by means of the Fano factor. The latter is defined in terms of detected photons as $F(m) = \sigma^2(m) / \langle m \rangle = \eta F(n) + (1 - \eta)$, where $\sigma^2(m)$ is the variance of the distribution of the number of detected photons and η is the quantum efficiency of the detector [20]. It is well known that $F = 1$ in the case of Poissonian light, $F < 1$ for sub-Poissonian light (nonclassical), and $F > 1$ for super-Poissonian light.

The two noise signals are sent in an alternative way through a communication channel together with a portion of a multi-mode TWB state [21], which is a quantum-correlated optical state. If the μ modes of each of the two parties of the TWB are equally populated, then the multi-mode TWB state is ideally described by a tensor product of μ identical TWB states [22, 23],

$$|\Psi_{\text{TWB}}^\mu\rangle = \bigotimes_{k=1}^{\mu} \sqrt{1 - \lambda^2} \sum_{\nu=0}^{\infty} \lambda^\nu |\nu_k\rangle \otimes |\nu_k\rangle, \quad (2)$$

where k labels the modes, ν is the photon number in each mode, λ is defined through $\lambda^2 = \langle n \rangle / (\mu + \langle n \rangle)$, and $\langle n \rangle$ is the mean total number of photons in either of the two parties of the TWB, with $n = \sum_{k=1}^{\mu} \nu_k$. The state in equation (2) is characterized by perfect photon-number correlations between the two parties of the TWB in each mode k . It is possible to prove that the probability of observing an overall number of photons n in each arm of the TWB is given by MMTD in equation (1) written in terms of the number n of incident photons [21, 24, 25]. The measurements performed by Bob return a mean value that is given by the sum of the mean value of the thermal signal and that of the TWB portion. The other TWB portion is retained and measured by Alice herself. The presence of the TWB in the communication channel allows for revealing possible eavesdropping attacks. For instance, this can be achieved by applying nonclassicality criteria involving the number of photons, such as that based on the noise reduction factor, R . In terms of the number of detected photons, it reads as [26]

$$R = \frac{\sigma^2(m_1 - m_2)}{\langle m_1 \rangle + \langle m_2 \rangle}, \quad (3)$$

where $\sigma^2(m_1 - m_2)$ is the variance of the distribution of the photon-number difference between the two parties of the TWB and $(\langle m_1 \rangle + \langle m_2 \rangle)$ is the shot-noise level. Values of R lower than 1 prove that the states are sub-shot-noise correlated. It has been demonstrated that this is also a sufficient criterion for entanglement [17]. For the purpose of the protocol, it is useful to express the noise reduction factor in the presence of the thermal noise signal to be transmitted. To model a more realistic scenario, we also assume that the communication channel is affected by losses, described by the imbalance parameter t between the two arms of the TWB [13, 21]:

$$R = 1 - \frac{2\eta t \langle m \rangle}{(1+t)\langle m \rangle + \langle m_N \rangle} + \frac{(1-t)^2 \langle m \rangle^2}{\mu[(1+t)\langle m \rangle + \langle m_N \rangle]} + \frac{\langle m_N \rangle^2}{\mu_N[(1+t)\langle m \rangle + \langle m_N \rangle]}, \quad (4)$$

where $\langle m \rangle$ is the mean number of detected photons in a TWB arm, η is the global quantum efficiency of the detection system (including the detection efficiency and the coupling of light into fibers), $t \in [0, 1]$ is the transmission efficiency quantifying the balancing between the two arms, while $\langle m_N \rangle$ and μ_N are the mean value and the effective number of modes of the thermal noise signal, respectively. This means that, in general, the value of R increases in the presence of noise, since the latter is not correlated with the TWB, and also in the presence of losses, as $t < 1$. In this scenario, nonclassical correlations, i.e. $R < 1$, can be detected provided that

$$\langle m_N \rangle < \sqrt{\mu_N [2\eta t \mu - (1-t)^2 \langle m \rangle]} \langle m \rangle / \mu. \quad (5)$$

Physically, this inequality can be interpreted as follows: in the case of perfect balance between the TWB arms (i.e. for $t = 1$), the nonclassicality condition requires that the mean value of the signal noise, $\langle m_N \rangle$, be less than a term proportional to $\sqrt{2\langle m \rangle}$, where $2\langle m \rangle$ is the shot-noise level, corresponding to the total mean number of detected photons in the two TWB arms; for $t < 1$, the presence of an imbalance imposes a more stringent constraint on the thermal noise signal, requiring $\langle m_N \rangle$ to be lower than that in the balanced case.

2.2. Discrimination of the noise signal as a binary classification problem

The binary alphabet adopted to encode the information comprises two noise signals, characterized by different mean values and encoding, respectively, the logical bits 0 and 1. Letting x be a scalar quantity that characterizes the noise signal and according to which we discriminate the latter, we label noise signals with values $x < x_{\text{th}}$ ($x \geq x_{\text{th}}$) as bit 0 (bit 1), where x_{th} is an arbitrary discrimination threshold value.

Discriminating between the two noise signals can be framed as a binary classification problem, whose performance can be assessed using various figures of merit, the most intuitive being the error probability, $P^{(\text{err})}$. Assuming that the two noise signals are characterized by equal prior probability, i.e.

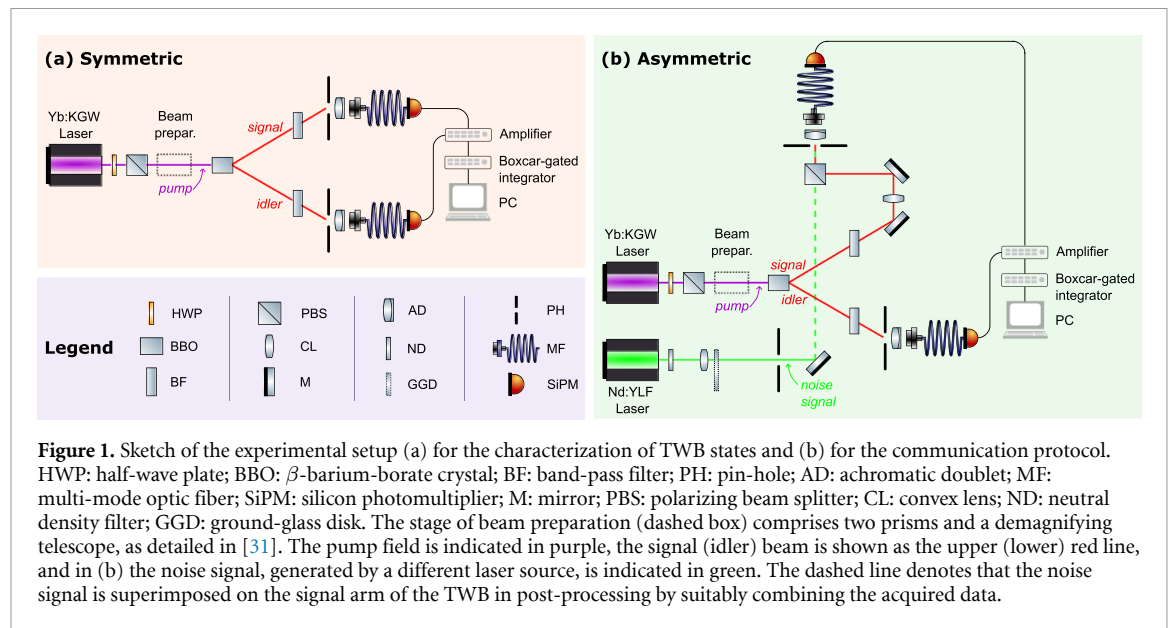
$p(0) = p(1) = 1/2$, $P^{(\text{err})}$ is expressed as [27]

$$P^{(\text{err})} = \frac{1}{2} [p(0|1) + p(1|0)], \quad (6)$$

where $p(i|j)$ is the conditional probability of detecting i having sent j .

To better characterize the performance of the binary classifier, we also consider the receiver operating characteristic (ROC) curve [28, 29], a parametric plot that shows *true positive rate* $\text{TPR} = \text{TP}/(\text{TP} + \text{FN})$ against the *false positive rate* $\text{FPR} = \text{FP}/(\text{FP} + \text{TN})$ at varying discrimination threshold values. By definition, $\text{TPR}, \text{FPR} \in [0, 1]$. In our setting, we treat bit 1 as the positive class and bit 0 as the negative. Thus, true positives (TPs) and true negatives (TNs) refer respectively to the number of correctly classified 1s and 0s, while FP (false positives) and FN (false negatives) to the number of 0s misclassified as 1s and of 1s misclassified as 0s, respectively. For completeness, the false negative rate is $\text{FNR} = 1 - \text{TPR}$ and the TN rate is $\text{TNR} = 1 - \text{FPR}$. Note that the number of T/F P/N, as well as the error probability in equation (6), which can be expressed as $P^{(\text{err})} = (\text{FNR} + \text{FPR})/2$, are determined at fixed threshold value. Based on these definitions, the perfect classifier corresponds to the point $(\text{FPR}, \text{TPR}) = (0, 1)$ (no false negatives and no false positives), while a random classifier is any point along the line $\text{TPR} = \text{FPR}$. Accordingly, points above this diagonal represent better-than-random classifiers. Regarding the discrimination threshold, low threshold values correspond to points near (1, 1) (most instances are labeled as positives), while high threshold values correspond to points near (0, 0) (very few instances are labeled as positives).

The area under the ROC curve (AUC) score [30] is a single, threshold-independent value which is often used to capture the overall performance of a binary classifier: $\text{AUC} = 1$ for the perfect classifier and $\text{AUC} = 0.5$ for a random one.



In the following, we address the binary discrimination based either on the mean value or the noise reduction factor and we investigate the figures of merit introduced above for representative sizes of the sample used to encode a single logical bit.

3. Experimental setup

3.1. Communication channel

The investigation of the communication protocol consists of two consecutive steps. First, we characterize the communication channel based on the multi-mode TWB state. In particular, we study both classical and nonclassical features of the TWB, such as the photon-number statistics and the strength of nonclassical correlations. Second, we investigate the performance of state discrimination superimposing the two noise signals on the portion of TWB sent to Bob.

The experimental setup we realized to accomplish these two steps is shown in figure 1: the sub-picosecond third-harmonic pulses at 344 nm of a tunable Yb:KGW laser are optically tilted by a system composed of two prisms and a demagnifying telescope before impinging on a β -barium-borate crystal (BBO), where they produce parametric down conversion. As described in [31], the tilting of the pulses is necessary to improve their group-velocity matching [32, 33] so as to obtain the phase-matching condition in the nonlinear crystal around frequency degeneracy (i.e. at 694 nm). The energy of the pump beam, and thus of the generated TWB, is changed by means of a half-wave plate (HWP) followed by a polarizing cube beam splitter (PBS) placed at the output of the laser.

Outside the BBO, spatial and spectral filtering (identical in the two arms) allows to select two entangled regions. As to the spectral filtering, we use two band-pass filters, having a central wavelength of 692 nm on one arm and 697 nm on the other arm, and both having a width of ~ 20 nm. For the spatial filtering, we use an adjustable pin-hole having a diameter of 1 cm. The filtered light in each arm is then focused by an achromatic doublet into a multi-mode optical fiber having a 1-mm-core diameter, and then delivered to the detector. The detection is performed by means of two SiPMs (model S13360–3050CS, Hamamatsu Photonics) [34]. These are solid-state PNR detectors endowed with hundreds of cells (pixels), operated in the Geiger-Müller regime. Under the assumption that each cell is fired by at most one photon impinging on it, each SiPM yields a single output that is proportional to the number of fired cells. The SiPM model used in this work is characterized by a quantum efficiency $\sim 16\%$ at 693 nm, which can reach higher values, $\sim 40\%$, in the blue-green spectral region [31]. The detectors are plugged into a power supply and amplification unit (model SP5600, CAEN) that supplies a bias voltage of 56 V to the SiPMs and amplifies the output by 17 dB. Each output is synchronously integrated over an interval of 10 ns by a boxcar-gated integrator and acquired.

3.2. Binary noise signal

The experimental setup for the study of the discrimination protocol is sketched in figure 1(b). It is equivalent to the previous one (figure 1(a)) except for the additional optical elements required to generate the noise signal and to superimpose it on the signal arm of the TWB. The thermal noise is generated by sending

picosecond pulses at 523 nm to a GGD. A single speckle is selected in far field by an iris 300 μm large. The energy of the laser beam is changed by means of a variable ND filter. In this way, it is possible to produce the two noise signals with different mean values, necessary to encode the logical bits 0 and 1, that can be superimposed in an alternative way on the portion of TWB sent to Bob. In the present study, we superimpose the noise signals in post-processing (see the dashed line in figure 1(b)), following a similar procedure already adopted in [35, 36] to merge the data corresponding to TWB states and those corresponding to noise signals. In a practical realization of the protocol, the superposition of one of the two noise signals on the signal arm of TWB could represent a critical point. In fact, even though an imperfect overlap, due for instance to mode matching, could be included in the expression in equation (4), its presence could make the two signals more distinguishable, thus degrading the security of the protocol [37]. However, it has been demonstrated that this issue could be mitigated through the use of a homodyne scheme with a strong local oscillator [38] or by employing non-Gaussian modulations [39]. Moreover, superimposing two beams by means of optical elements, such as beam splitters and dichroic mirrors, could introduce further losses, because both the signal of TWB and the thermal states could be attenuated. However, this effect is not particularly detrimental since it can be included in the parameter t for the TWB and would act in the same way for the two thermal states at different mean values. To take into account the role played by $t < 1$ in the practical implementation of the communication channel based on TWB, we decide to insert in the setup some optical elements that increase its length and introduce some losses. Despite the latter, nonclassical correlations can still be detected by Bob, thus enabling the devised communication protocol.

4. Results

4.1. Measurements and data processing

The quantities we are interested in—the mean number of detected photons $\langle m \rangle$ and the noise reduction factor R —ultimately depend on the intensity of the light that impinges on the two detectors. Therefore, it is necessary to preliminarily characterize the TWB states for different values of their intensity in the mesoscopic intensity domain, and the two noise signals we superimpose on the signal arm to encode the bits. Concerning the first aspect, we use a combination of HWP and PBS (figure 1(a)) as a knob to tune the intensity of the pump beam and so, ultimately, to change the mean value of TWB. In more detail, we consider four angle values of the HWP placed on the pump beam path to investigate the statistical properties of the TWB alone as a function of the pump beam intensity. The TWB is then investigated in the presence of losses by using the asymmetric setup in figure 1(b). The two noise signals are also preliminarily characterized in order to verify that we have at our disposal single-mode thermal states. Their mean values are properly selected in order to satisfy equation (5), thus ensuring $R < 1$.

Following the analysis procedure previously described in [40], for all the considered configurations the two outputs of the detection chain are suitably processed to reconstruct the statistical properties of light in terms of detected photons. Specifically, we process the data acquired by each SiPM in every conditions by computing the pulse-height spectrum [41] (see, e.g. figure 2). From the latter we determine the gain of each detector as the average distance between the peaks of the histograms. Finally, the amplitude is converted from volts (units of the measured outputs) to number of detected photons by dividing each column of data by the corresponding gain and rounding the results to the nearest integer value.

4.2. Characterization of the communication channel

As explained in section 2, many properties of the TWB that qualify the communication channel can be determined starting from the number of detected photons m_k in each arm, signal ($k = s$) and idler ($k = i$). Among them, here we consider the photon-number distribution, the Fano factor, and the noise reduction factor. For all the four increasing values of the pump intensity, our results are consistent with the expected behavior of the TWB. The two arms are well balanced, $\langle m_s \rangle \approx \langle m_i \rangle$, and each detected-photon distribution is well fitted by the MMTD in equation (1), as shown in figure 3(a). The super-Poissonian nature of the measured light is also evidenced by the Fano factor, which is larger than 1 for all the datasets shown in figure 3(b). Finally, the noise reduction factor is $R < 1$ (see figure 3(c)) in all cases, denoting the presence of nonclassical photon-number correlations in the mesoscopic intensity domain. By fitting the latter results using equation (4) with $t = 1$ (lossless configuration, the two arms are balanced) and $\langle m_N \rangle = 0$ (noiseless configuration), we can estimate the detection efficiency $\eta = (8.5 \pm 0.7)\%$, which is lower than the expected one ($\eta \sim 16\%$ at 693 nm, according to the datasheet [34]). The discrepancy between our estimate and the expected value is likely due to possible losses in the collection of light including a non perfect coupling into fibers. Remarkably, despite its low value, this efficiency is still sufficient to detect nonclassical correlations.

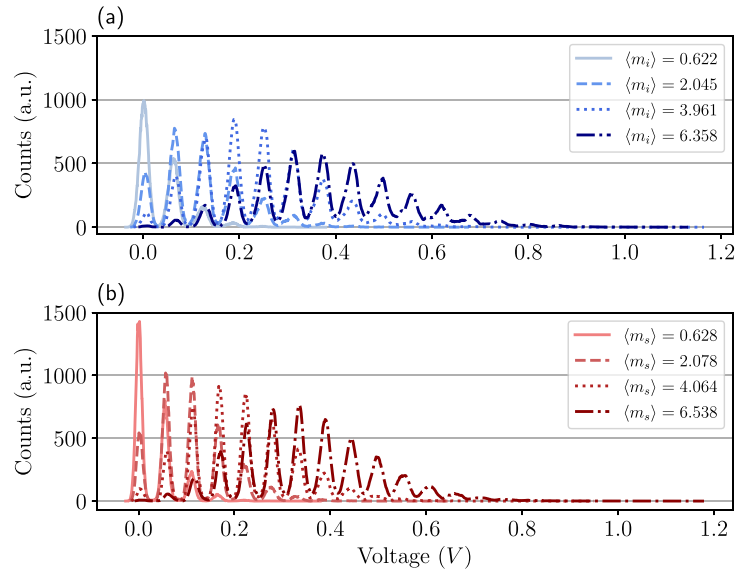


Figure 2. Pulse-height spectra of idler (a) and signal (b) at different mean numbers of detected photons $\langle m \rangle$. Results are obtained from 10^5 data for each mean value.

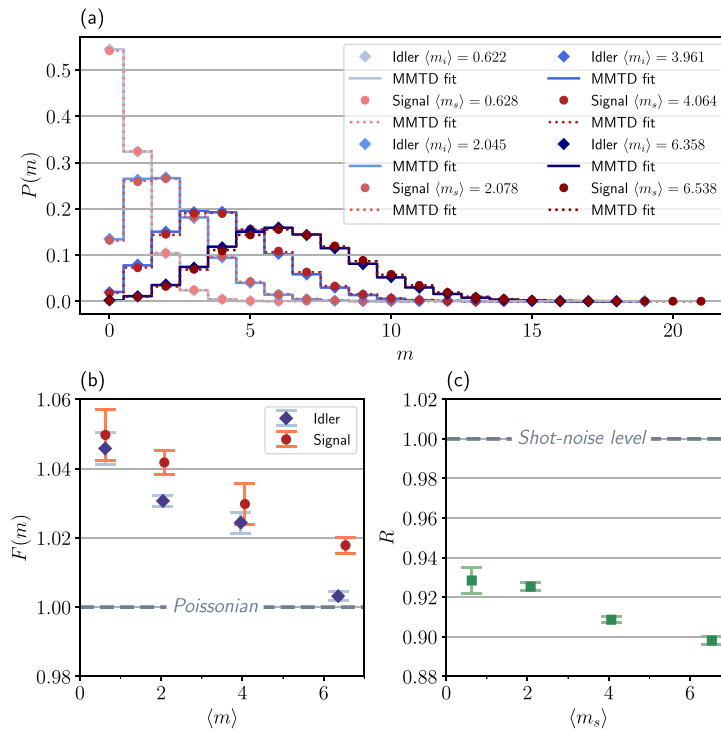


Figure 3. Characterization of the symmetric TWB. (a) Detected-photon distribution $P(m_k)$ in the idler $k = i$ (blue-scale-colored diamonds) and signal $k = s$ (red-scale-colored circles). The fitting function (line) is the MMTD in equation (1). Light (dark) colors correspond to low (high) $\langle m_k \rangle$. (b) Fano factor $F(m_k) > 1$ of each arm as a function of $\langle m_k \rangle$. (c) Noise reduction factor $R < 1$ as a function of $\langle m_s \rangle$. Results in (b) and (c) are obtained by dividing the 10^5 data of each dataset into 4 batches of 25 000 shots: the marker with its error bar represents the mean and the associated standard error computed from the batches of the considered dataset.

Due to the additional optical elements required to mimic the losses in the communication channel, in the configuration shown in figure 1(b) the TWB is no longer symmetric: The optical length of the signal has increased, while that of the idler is almost unchanged. These differences determine the presence of losses, especially in the signal arm. Losses can be easily estimated in terms of the transmission efficiency $t = \langle m_s \rangle / \langle m_i \rangle \approx 47\%$, where the mean number of detected photons in the signal and idler arms is $\langle m_s \rangle = 3.44 \pm 0.01$ and $\langle m_i \rangle = 7.37 \pm 0.01$, respectively. Again, in each arm the detected-photon distribution is well described by the MMTD in equation (1) (see figure 4(a), where the asymmetry

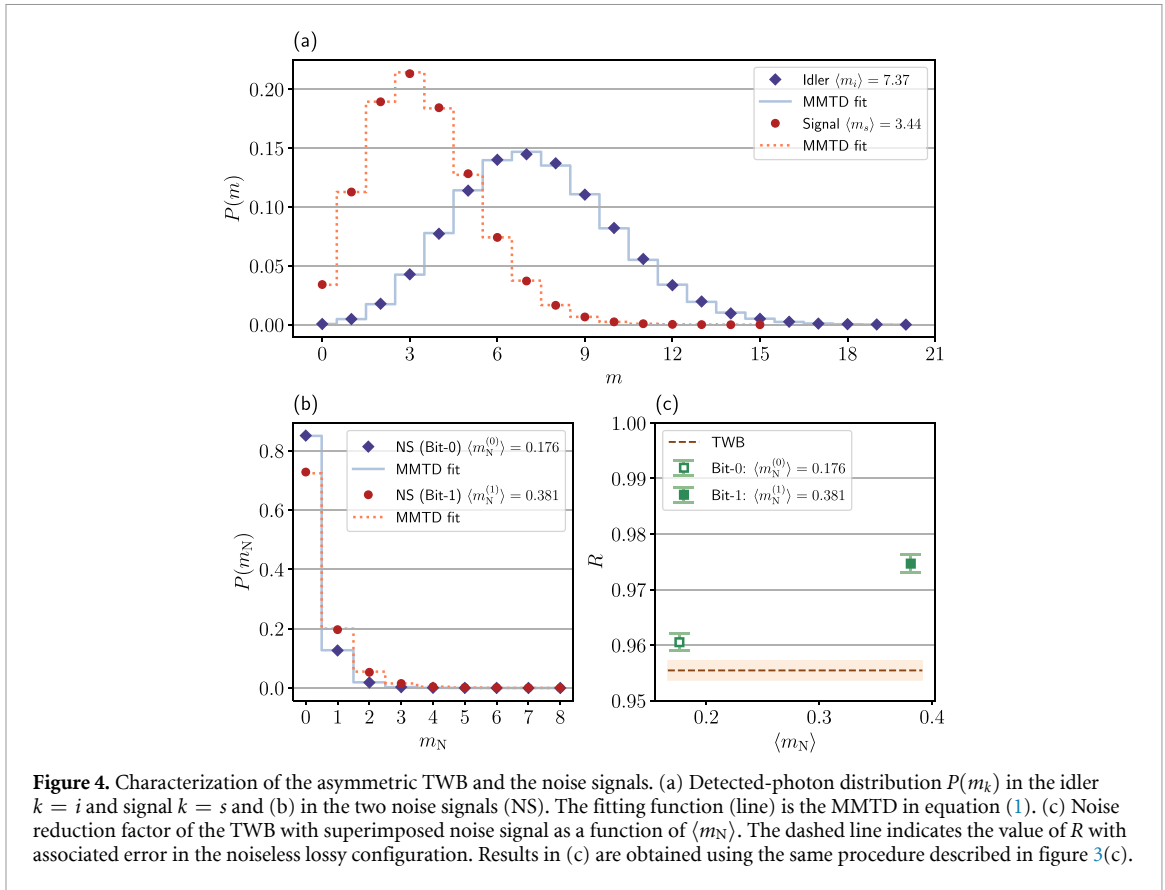


Figure 4. Characterization of the asymmetric TWB and the noise signals. (a) Detected-photon distribution $P(m_k)$ in the idler $k = i$ and signal $k = s$ and (b) in the two noise signals (NS). The fitting function (line) is the MMTD in equation (1). (c) Noise reduction factor of the TWB with superimposed noise signal as a function of $\langle m_N \rangle$. The dashed line indicates the value of R with associated error in the noiseless lossy configuration. Results in (c) are obtained using the same procedure described in figure 3(c).

introduced by the transmission channel is evident), with Fano factor $F(m_i) = (1.012 \pm 0.002) > 1$ and $F(m_s) = (1.036 \pm 0.005) > 1$, respectively. Despite the losses, we can still detect sub-shot-noise correlations. Indeed, the noise reduction factor is $R = 0.955 \pm 0.002$, from which we can estimate the effective quantum efficiency in this asymmetric configuration to be $\eta = (7.0 \pm 0.2)\%$. This value, slightly lower than that in the symmetric configuration (i.e. 8.5%), accounts for additional losses introduced in both arms as a result of increasing the distance from the nonlinear crystal to allow for the insertion of optical elements in the signal arm.

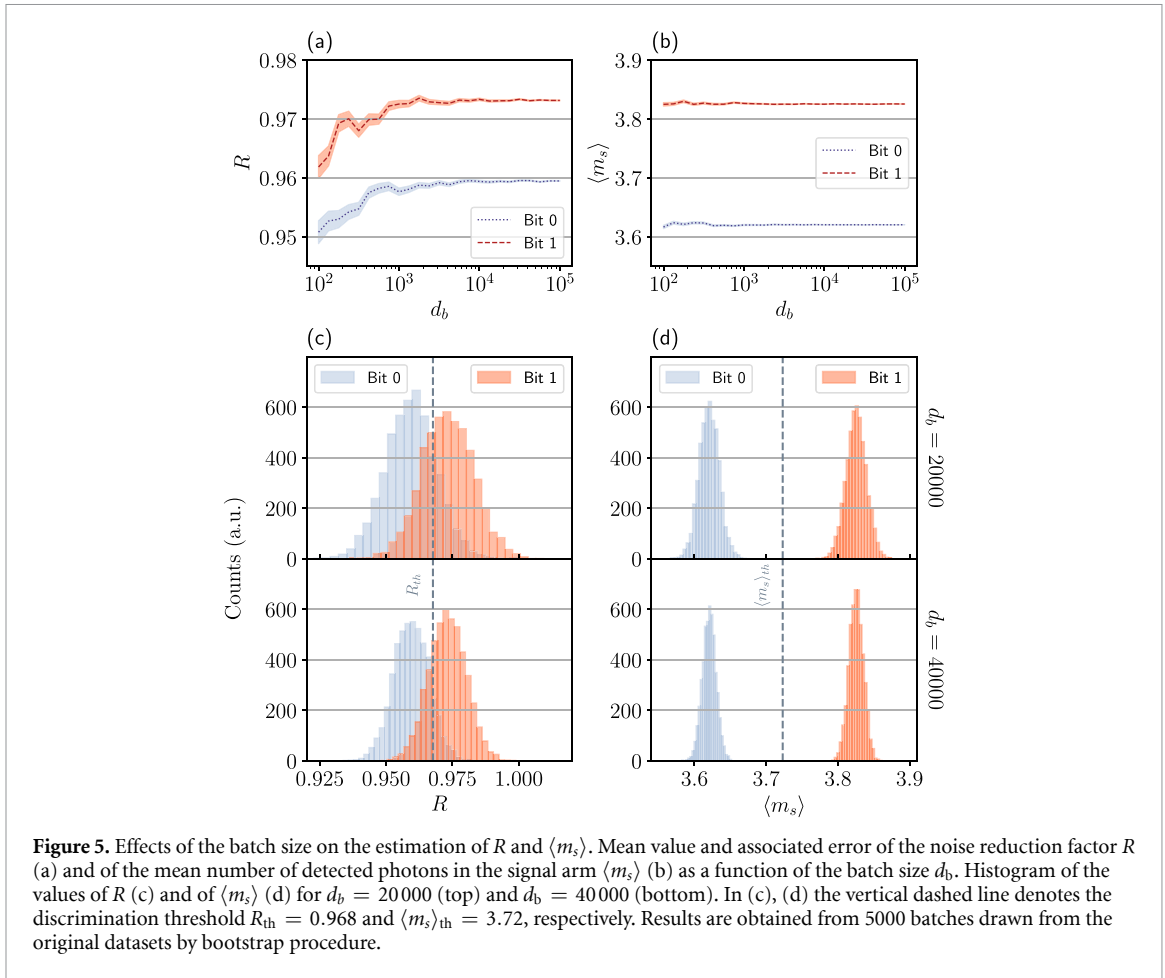
Concerning the two noise signals, we consider two quasi-single-mode thermal states with mean values $\langle m_N^{(0)} \rangle = 0.176 \pm 0.001$ encoding the logical bit value 0, and $\langle m_N^{(1)} \rangle = 0.381 \pm 0.005$ encoding the logical bit value 1. Their photon-number distributions are shown together in figure 4(b). When either noise signal is superimposed on the lossy transmission channel, the value of R measured by Bob increases compared to the noiseless case (see equation (4)), though it remains below 1, as shown in figure 4(c). Specifically, the superposition of the two noise signals yields two values— $R^{(0)} = 0.962 \pm 0.002$ and $R^{(1)} = 0.975 \pm 0.002$, respectively—that are different within 2σ .

It is worth noting that the fact that all these values are below 1, but not by much, makes the discrimination strategy particularly intriguing: under these conditions, a potential intercept-resend attack by Eve can easily raise the value of R above 1 or, at least, above a given threshold of uncertainty, thus providing a clear and readily applicable criterion for detecting the attack. From the experimental point of view, these conditions can be easily attained by properly choosing the wavelength of the produced TWB or the model of SiPMs, i.e. by suitably tuning the detection efficiency η (see equation (4)).

4.3. Performance of the discrimination strategy

In the proposed communication protocol, we assume that Alice prepares the TWB, chooses the binary sequence of noise signals to superimpose on the signal arm, and sends it to Bob. While Alice measures the light in the idler arm, Bob does the same in the signal arm and compares his results with Alice's, evaluating either $\langle m_s \rangle$ or R to decode the received bits. In this section, we compare the performance of these two decoding strategies, one based on a classical feature, $\langle m_s \rangle$, and the other on a nonclassical one, R .

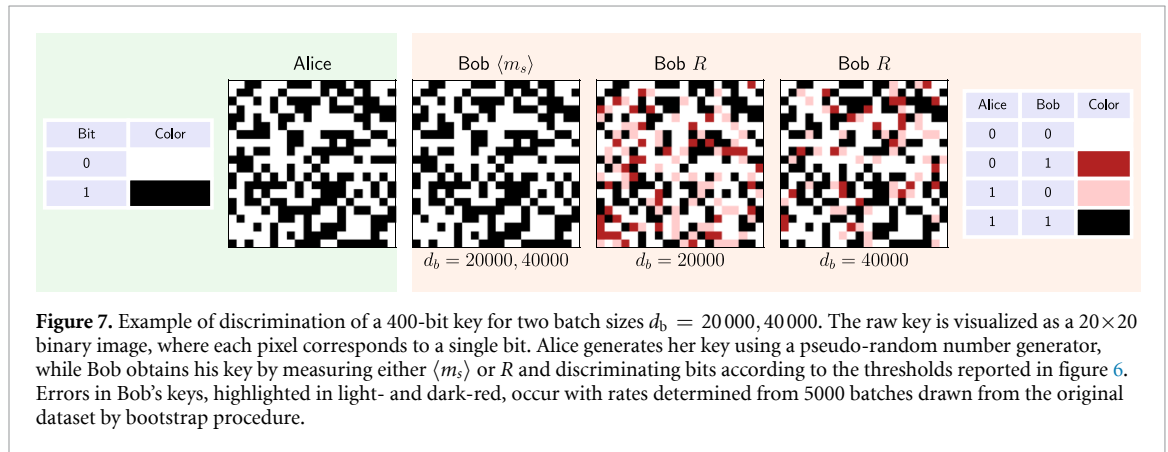
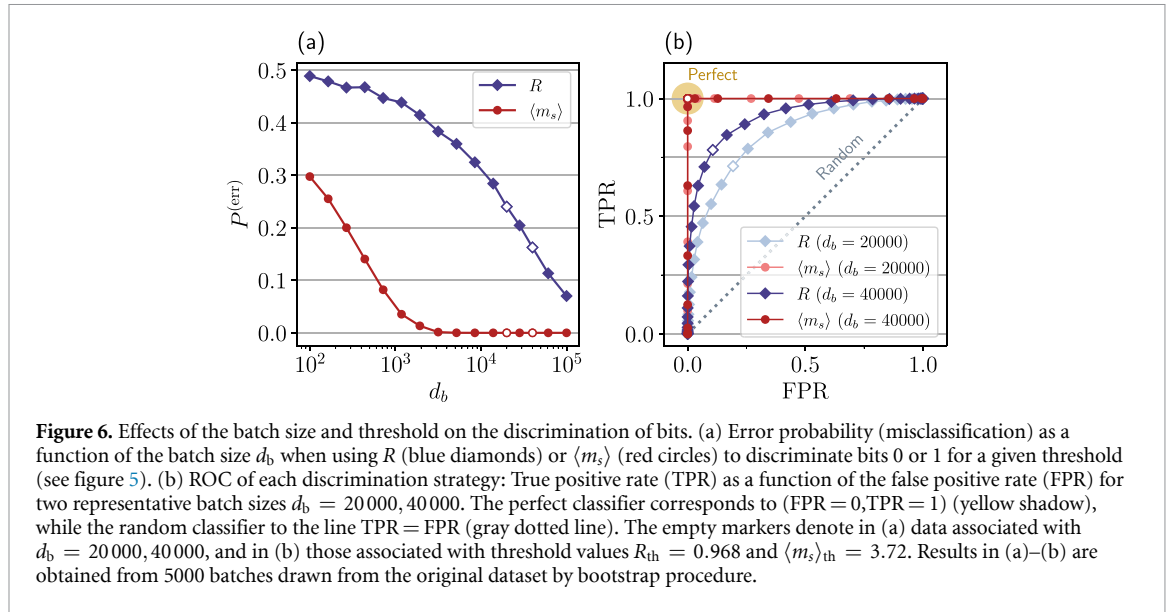
For this analysis, a remark is in order. The 10^5 shots we measured for each dataset (lossy TWB and noise signal with $\langle m_N^{(0)} \rangle$ and $\langle m_N^{(1)} \rangle$) are not sufficient to properly test the performance of the discrimination strategy, because a reliable estimate of $\langle m_s \rangle$ and R requires at least $O(10^4)$ measurements, as shown in



figures 5(a) and (b). This is particularly necessary for evaluating the noise reduction factor, which depends on second-order moments of statistical distributions (see equation (3)). To overcome this limitation, we apply the bootstrap procedure [42, 43] to the original experimental datasets from which we draw samples. Each batch we draw represents a possible realization of the experiment. In the following, we evaluate and discuss the performance of the discrimination strategies based either on R or on $\langle m_s \rangle$ using 5000 batches for representative values of the batch size d_b .

To illustrate the different discrimination capabilities of R and $\langle m_s \rangle$, it is instructive to focus on the distribution of their values for two representative batch sizes $d_b = 20000, 40000$, as shown in figures 5(c) and (d). Letting $x = R, \langle m_s \rangle$ be the discrimination parameter, here we define the discrimination threshold as $x_{th} \equiv (x^{(0)} + x^{(1)})/2$, where $x^{(b=0,1)}$ is the value obtained from the original datasets (values are reported in section 4.2). Discriminating the superimposed noise signal (i.e. decoding the bits) via R leads to misclassification errors: the two histograms representing bits 0 and 1 overlap (figure 5(c)). In contrast, the outstanding PNR capabilities of SiPMs enable the exact discrimination when using $\langle m_s \rangle$: there is no overlap of the two histograms representing bits 0 and 1 (figure 5(d)).

As discussed in section 2.2, to better understand how the batch size d_b affects the discrimination of bits, we consider the following figures of merit at varying d_b : (i) The error probability $P_x^{(err)}$ defined in equation (6), according to which a bit 0 is misclassified as bit 1 or vice versa, (ii) the ROC curve, and (iii) the associated AUC. (i) The error probability in figure 6(a) clearly shows how the discrimination via $\langle m_s \rangle$ outperforms that via R even at low d_b , where discrimination via R is basically random guessing. Focusing on $d_b \sim 10^4$, we have $P_{\langle m_s \rangle}^{(err)} \approx 0$, while $P_R^{(err)} \approx 16\%$ for $d_b = 40000$. (ii) The ROC curves in figure 6(b) reveal that for $d_b = 20000, 40000$ both discrimination strategies perform better than random guessing, though with significant differences. The ROC curves related to $\langle m_s \rangle$ for the two d_b overlap and perfect discrimination is enabled, $(FPR, TPR) = (0, 1)$, for various threshold values. Instead, the ROC curve related to R improves upon increasing the batch size, but this discrimination strategy requires a fine-tuning of the threshold value, and yet it performs worse than the strategy based on the mean value. (iii) Analogous conclusions can be drawn by evaluating the area under the ROC curve: $AUC \approx 1$ (perfect classifier) when



discriminating via $\langle m_s \rangle$ for both the batch sizes considered, while $AUC \approx 0.843$ if $d_b = 20\,000$ and $AUC \approx 0.918$ if $d_b = 40\,000$ when discriminating via R .

To summarize, reliably encoding a bit requires a batch size at least $d_b \sim O(10^4)$, in particular when using R rather than $\langle m_s \rangle$ (see figures 5(a) and (b)). This is also reflected in the error probability for decoding a bit (i.e. discriminating the noise signals) (see figure 6(a)). As evidenced by the analysis of the ROC curve (see figure 6(b)) and the AUC, the $\langle m_s \rangle$ -based discrimination strategy exactly distinguishes the noise signals without requiring a fine-tuning of the threshold, in contrast to the R -based strategy, which is prone to errors.

5. Proof-of-principle test

In light of the results presented in section 4 for the two discrimination criteria, it is interesting to investigate the performance of each discrimination strategy. We point out that while $\langle m_s \rangle$ -based discrimination strategy relies only on Bob's measurement outcomes, the R -based one requires Bob and Alice to share, over a different communication channel, their measurement outcomes with each other (see equation (3)). As a proof-of-principle test, we generate a binary string (Alice's raw key) with a pseudo-random number generator [44]. The rates of true/false positive/negatives—estimated over 5000 batches drawn from the original datasets—define the probabilities that govern the decoding of each bit in Bob's raw key. Figure 7 shows an example of a 400-bit raw key decoded using the two discrimination strategies, for two batch sizes $d_b = 20\,000, 40\,000$.

As expected, Bob can exactly decode Alice's raw key using the $\langle m_s \rangle$ -based discrimination strategy, while the raw key he obtains using the R -based strategy is affected by errors. In particular, the error probability decreases from $P_R^{(err)} \approx 24\%$ to $\approx 16\%$ upon increasing the batch size from $d_b = 20\,000$ to $40\,000$ (see also figure 6(a)). In detail, the false positive/negative rates decreases from $FPR \approx 19\%$ to $\approx 11\%$ and $FNR \approx 29\%$ to $\approx 22\%$. Therefore, a bit-1 decoded as a bit-0 (i.e. a false negative) constitutes a misclassification error that

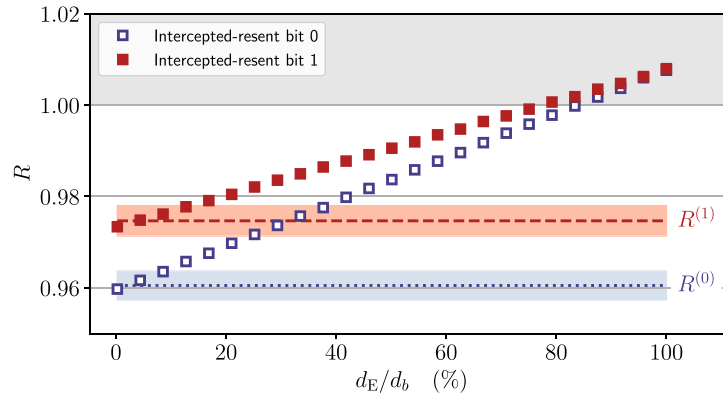


Figure 8. An ideal intercept-resend attack can be revealed by the values of the noise reduction factor R . Eve intercepts d_E shots of a batch encoding a bit ($d_b = 40000$) and resends, in place of the intercepted light, d_E shots belonging to a Poissonian light having the same mean value as that of the intercepted light. While the mean value measured by Bob is not affected by this attack (data not shown), the value of the noise reduction factor is. Blue color refers to bit 0, while red color refers to bit 1. The blue dotted line + blue highlighted band corresponds to $R^{(0)} \pm 2\sigma$, while the red dashed line + red highlighted band corresponds to $R^{(1)} \pm 2\sigma$. The values of R corresponding to the intercepted-resent bit 0 (1) are shown as blue open squares (full red squares). Results are averaged over 5000 realizations of the intercept-resend attack.

occurs systematically more often than the opposite case, where a bit-0 is decoded as a bit-1 (i.e. a false positive). This asymmetry in error rates arises from the choice of the discrimination threshold R_{th} in the present example. According to the analysis of the ROC curve, and recalling that $FNR \equiv 1 - TPR$, the condition $FNR = FPR$ corresponds to points lying along the anti-diagonal $TPR = 1 - FPR$. However, as illustrated in figure 6(b), the points associated with $R_{th} = 0.968$ lie below the anti-diagonal, thus indicating $FNR > FPR$ (see also figure 5(c), which shows that the threshold R_{th} lies closer to one distribution than to the other). Since this protocol requires estimating R , each bit must be encoded using a batch size at least $d_b \sim O(10^4)$. In this regard, $d_b \approx 40000$ represents a suitable batch size to reliably estimate R while keeping the number of shots per bit reasonably limited.

In light of these results, one might thus be tempted to choose the discrimination strategy based on $\langle m_s \rangle$ and to use a lower batch size, which in turn saves resources and can increase the bit rate, given the mild impact of batch size on discriminative power. However, the $\langle m_s \rangle$ -based protocol is vulnerable to eavesdropping, e.g. to intercept-resend attacks, which can instead be readily detected by the values of R . Therefore, the hybrid discrimination strategy we propose is devised to leverage a classical property—the mean value of the detected light, $\langle m_s \rangle$ —for bit discrimination, while harnessing a nonclassical feature—the noise reduction factor R between the two arms of the TWB—to ensure security. In practice, Bob constructs his raw key by decoding the received light using $\langle m_s \rangle$, and retains each bit only if the corresponding measurement satisfies $R < 1$ (nonclassical correlations) and the value of R falls within a reasonable uncertainty range.

To better investigate the feasibility of the strategy, we simulate an eavesdropping attack by assuming that Eve intercepts part of a batch encoding either 0 or 1, and re-sends a signal with the same mean value as the stolen portion of light. In doing so, Eve replaces a portion of the shots in the signal arm (Bob)—originally nonclassically correlated with those in the idler arm (Alice)—with others from a different light source, which is uncorrelated with Alice's. This degradation of nonclassical correlations due to the intercept-resend attack is therefore expected to increase the noise reduction factor (see equation (4)). In particular, we consider a synthetic signal generated according to a Poissonian distribution, since this is the statistical distribution that better approximates the distribution of the signal received by Bob in the absence of eavesdropping. The results of this intercept-resend attack are shown in figure 8, where the noise reduction factor is shown as a function of the ratio d_E/d_b between the batch size changed by Eve and that encoding either 0 or 1. The linear dependence of R on d_E/d_b can be proved analogously to the derivation of equation (4). The highlighted bands indicate the uncertainty corresponding to $\pm 2\sigma$. It can be noticed that for bit 0 the value of R exceeds $R^{(0)} + 2\sigma$ and 1 at $d_E/d_b \approx 9\%$ and $\approx 84\%$, respectively. Instead, for bit 1 it exceeds $R^{(1)} + 2\sigma$ and 1 at $d_E/d_b \approx 14\%$ and $\approx 78\%$, respectively. This means that Bob can easily detect the presence of Eve by simply checking whether the values of R are larger than 2σ . On the contrary, values $R > 1$ are more difficult to observe, at least when Eve, as in the present example, is equipped with an ideal detector that allows perfect estimation of the mean value of the intercepted signal. At the same time, this proof-of-principle test does not take into account possible optimization strategies, such as practical reconciliation or privacy amplification, devised by Bob to improve his receiver.

Moreover, in view of a realistic application of the communication protocol, the scheme can be implemented at telecom wavelengths [45, 46], while leaving the detection in the visible region and using a sum-frequency generation process [47, 48] before the detection stage. Work on this phase is ongoing precisely on a SiPM-based detection scheme.

6. Conclusions

In this work, we investigated a hybrid state discrimination strategy in the mesoscopic intensity domain, where information is encoded in the photon number of two single-mode thermal states. The proposed method employs a receiver that uses PNR detectors, while the communication channel exploits mesoscopic TWB states. The PNR capability provides direct access to the mean photon number, which is essential for effective discrimination. Simultaneously, the use of nonclassically correlated TWB states, characterized through the noise reduction factor, enables the detection of eavesdropping attacks, thereby enhancing communication security. Our analysis focuses on the error probability and the ROC curve, both evaluated as functions of the batch size of transmitted signals.

The results demonstrate the existence of a batch-size threshold above which the chosen discrimination metric becomes reliable. Specifically, discrimination based on the mean number of photons achieves lower error rates and requires fewer measurements, but does not provide inherent security. Conversely, discrimination based on the noise reduction factor R can reveal eavesdropping activity, although it is more error-prone and demands a larger number of measurements per bit. Furthermore, the analysis of the ROC curve offers insights into the nature of errors occurring in the communication channel.

The overall robustness of the proposed discrimination strategy paves the way to further enhancements, particularly in the encoding scheme. For example, one promising direction would be to adopt an alphabet with more than two symbols [49], encoded either in single-mode thermal states with distinct mean values or in superthermal states [36].

Data availability statement

The data cannot be made publicly available upon publication because no suitable repository exists for hosting data in this field of study. The data that support the findings of this study are available upon reasonable request from the authors.

Acknowledgments

We thank Silvia Cassina (University of Insubria) for fruitful discussions. A A acknowledges support from Grant No. PNRR D.D.M.M. 737/2021. Scientific support from CRIETT centre of University of Insubria (instrument code: MAC27) is greatly acknowledged. L R acknowledges support from INFN through the project 'QUANTUM'.

Conflict of interest

The authors have no conflicts to disclose.

Author contributions

Luca Razzoli: Data curation (equal); Formal analysis (lead); Methodology (equal); Writing—Original draft (equal); Review and editing (equal). **Alex Pozzoli:** Investigation (equal); Software (lead); Data curation (equal); Review and editing (equal). **Alessia Allevi:** Conceptualization (lead); Investigation (lead); Supervision (lead); Methodology (equal); Funding acquisition (lead); Writing—Original draft (equal); Review and editing (equal).

ORCID iDs

Luca Razzoli  0000-0002-9129-2154

Alex Pozzoli  0009-0003-8917-7725

Alessia Allevi  0000-0002-1972-3124

References

- [1] Cariolaro G 2015 *Quantum Communications* (Springer)
- [2] Flamini F, Spagnolo N and Sciarrino F 2019 Photonic quantum information processing: a review *Rep. Prog. Phys.* **82** 016001
- [3] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Phys. Rev. Lett.* **88** 057902
- [4] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 Practical challenges in quantum key distribution *npj Quantum Inf.* **2** 16025
- [5] Olivares S, Cialdi S, Castelli F and Paris M G A 2013 Homodyne detection as a near-optimum receiver for phase-shift-keyed binary communication in the presence of phase diffusion *Phys. Rev. A* **87** 050303
- [6] DiMario M T and Becerra F E 2018 Robust measurement for the discrimination of binary coherent states *Phys. Rev. Lett.* **121** 023603
- [7] DiMario M T, Kunz L, Banaszek K and Becerra F E 2019 Optimized communication strategies with binary coherent states over phase noise channels *npj Quantum Inf.* **5** 65
- [8] Sanvito A, Cassina S, Lamperti M, Notarnicola M N, Olivares S and Allevi A 2024 Assessing a binary quantum channel exploiting a silicon photomultiplier based hybrid receiver *Opt. Express* **32** 39846–59
- [9] Cassina S, Notarnicola M N, Olivares S and Allevi A 2025 On the application of a silicon photomultiplier-based receiver for binary phase-shift-keying protocols *Phys. Lett. A* **541** 130403
- [10] Bergou J A 2010 Discrimination of quantum states *J. Mod. Opt.* **57** 160–80
- [11] Benenti G, Casati G, Rossini D and Strini G 2019 *Principles of Quantum Computation and Information: A Comprehensive Textbook* (World Scientific)
- [12] Allevi A and Bondani M 2019 Preserving nonclassical correlations in strongly unbalanced conditions *J. Opt. Soc. Am. B* **36** 3275–81
- [13] Allevi A and Bondani M 2021 Effect of noisy channels on the transmission of mesoscopic twin-beam states *Opt. Express* **29** 32842–52
- [14] Allevi A and Bondani M 2022 Novel scheme for secure data transmission based on mesoscopic twin beams and photon-number-resolving detectors *Sci. Rep.* **12** 15621
- [15] Usenko V C et al 2025 Continuous-variable quantum communication (arXiv:2501.12801)
- [16] Akindinov A V, Martemianov A N, Polozov P A, Golovin V M and Grigoriev E A 1997 New results on MRS APDs *Nucl. Instrum. Methods Phys. Res. A* **387** 231–4
- [17] Agliati A, Bondani M, Andreoni A, De Cillis G and Paris M G A 2005 Quantum and classical correlations of intense beams of light investigated via joint photodetection *J. Opt. B: Quantum Semiclass. Opt.* **7** S652–63
- [18] Ramilli M, Allevi A, Chmill V, Bondani M, Caccia M and Andreoni A 2010 Photon-number statistics with silicon photomultipliers *J. Opt. Soc. Am. B* **27** 852–62
- [19] Mandel L and Wolf E 1995 *Optical Coherence and Quantum Optics* (Cambridge University Press)
- [20] Allevi A and Bondani M 2017 Nonlinear and quantum optical properties and applications of intense twin-beams *Adv. At. Mol. Opt. Phys.* **66** 49–110
- [21] Allevi A and Bondani M 2022 Multi-mode twin-beam states in the mesoscopic intensity domain *Phys. Lett. A* **423** 127828
- [22] Allevi A, Andreoni A, Beduini F, Bondani M, Genoni M G, Olivares S and Paris M G A 2010 Conditional measurements on multimode pairwise entangled states from spontaneous parametric downconversion *Europhys. Lett.* **92** 20007
- [23] Harder G, Bartley T J, Lita A E, Nam S W, Gerrits T and Silberhorn C 2016 Single-mode parametric-down-conversion states with 50 photons as a source for mesoscopic quantum optics *Phys. Rev. Lett.* **116** 143601
- [24] Paleari F, Andreoni A, Zambra G and Bondani M 2004 Thermal photon statistics in spontaneous parametric downconversion *Opt. Express* **12** 2816–24
- [25] Mauerer W, Avenhaus M, Helwig W and Silberhorn C 2009 How colors influence numbers: photon statistics of parametric down-conversion *Phys. Rev. A* **80** 053815
- [26] Heidmann A, Horowicz R J, Reynaud S, Giacobino E, Fabre C and Camy G 1987 Observation of quantum noise reduction on twin laser beams *Phys. Rev. Lett.* **59** 2555–7
- [27] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (Academic)
- [28] Fawcett T 2006 An introduction to ROC analysis *Pattern Recognit. Lett.* **27** 861–74
- [29] Canbek G, Taskaya Temizel T and Sagiroglu S 2022 PToPI: a comprehensive review, analysis and knowledge representation of binary classification performance measures/metrics *SN Comput. Sci.* **4** 13
- [30] Hanley J A and McNeil B J 1982 The meaning and use of the area under a receiver operating characteristic (ROC) curve *Radiology* **143** 29–36
- [31] Pozzoli A, Lamperti M, Clerici M, Bondani M and Allevi A 2025 Optimal generation of mesoscopic twin-beam states by means of a natively femtosecond laser system *APL Photon.* **10** 036116
- [32] Smith A V 2001 Group-velocity-matched three-wave mixing in birefringent crystals *Opt. Lett.* **26** 719–21
- [33] Schimpf D N, Rothhardt J, Limpert J, Tünnermann A and Hanna D C 2007 Theoretical analysis of the gain bandwidth for noncollinear parametric amplification of ultrafast pulses *J. Opt. Soc. Am. B* **24** 2837–46
- [34] (Available at: www.hamamatsu.com/content/dam/hamamatsu-photonics/sites/documents/99_SALES_LIBRARY/ssd/s13360_series_kapd1052e.pdf)
- [35] Peřina Jr J, Černoř A and Soubusta J 2021 Compound twin beams without the need of genuine photon-number-resolving detection *Phys. Rev. Applied* **16** 024061
- [36] Allevi A and Bondani M 2023 Thermal and superthermal noise signals as resources for underwater quantum communication *Phys. Lett. A* **492** 129207
- [37] Usenko V C, Ruppert L and Filip R 2015 Quantum communication with macroscopically bright nonclassical states *Opt. Express* **23** 31534
- [38] Kovalenko O, Spasibko K Y, Chekhova M V, Usenko V C and Filip R 2019 Feasibility of quantum key distribution with macroscopically bright coherent light *Opt. Lett.* **27** 36154–63
- [39] Bose S and Jeong H 2023 Multimode non-Gaussian secure communication under mode mismatch *Phys. Rev. A* **108** 042412
- [40] Bondani M, Allevi A, Agliati A and Andreoni A 2009 Self-consistent characterization of light statistics *J. Mod. Opt.* **56** 226–31
- [41] Cassina S, Allevi A, Mascagna V, Prest M, Vallazza E and Bondani M 2021 Exploiting the wide dynamic range of silicon photomultipliers for quantum optics applications *EPJ Quantum Technol.* **8** 4
- [42] Efron B 1979 Bootstrap methods: another look at the jackknife *Ann. Stat.* **7** 1–26

- [43] BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP, and OIML 2008 *Evaluation of Measurement Data—Supplement 1 to the “Guide to the Expression of Uncertainty in Measurement”—Propagation of Distributions Using a Monte Carlo Method (JCGM 101)* (available at: www.bipm.org/en/doi/10.59161/jcgm101-2008)
- [44] (Available at: <https://docs.python.org/3/library/random.html>)
- [45] Sharping J E, Fiorentino M and Kumar P 2001 Observation of twin-beam-type quantum correlation in optical fiber *Opt. Lett.* **26** 367–9
- [46] Eckstein A, Christ A, Mosley P J and Silberhorn C 2011 Highly efficient single-pass source of pulsed single-mode twin beams of light *Phys. Rev. Lett.* **106** 013603
- [47] Bai P, Zhang Y H and Shen W Z 2017 Infrared single photon detector based on optical up-converter at 1550 nm *Sci. Rep.* **7** 15341
- [48] Chae J-W, Kim J-H, Jeong Y-C and Kim Y-H 2023 Tunable up-conversion single-photon detector at telecom wavelengths *Nanophotonics* **12** 495
- [49] Becerra F E, Fan J and Migdall A 2013 Implementation of generalized quantum measurements for unambiguous discrimination of multiple non-orthogonal coherent states *Nat. Commun.* **4** 2028