

This is a repository copy of *Testing the photon-number statistics of a quantum key distribution light source*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/167338/>

Version: Published Version

---

**Article:**

Dynes, J. F., Lucamarini, M. [orcid.org/0000-0002-7351-4622](https://orcid.org/0000-0002-7351-4622), Patel, K. A. et al. (4 more authors) (2018) Testing the photon-number statistics of a quantum key distribution light source. Optics Express. pp. 22733-22749. ISSN 1094-4087

<https://doi.org/10.1364/OE.26.022733>

---

**Reuse**

Other licence.

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.



# Testing the photon-number statistics of a quantum key distribution light source

J. F. DYNES, M. LUCAMARINI,<sup>\*</sup> K. A. PATEL, A. W. SHARPE,  
M. B. WARD, Z. L. YUAN, AND A. J. SHIELDS

Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK

<sup>\*</sup>marco.lucamarini@crl.toshiba.co.uk

**Abstract:** A commonly held tenet is that lasers well above threshold emit photons in a coherent state, which follow Poissonian statistics when measured in photon number. This feature is often exploited to build quantum-based random number generators or to derive the secure key rate of quantum key distribution systems. Hence the photon number distribution of the light source can directly impact the randomness and the security distilled from such devices. Here, we propose a method based on measuring correlation functions to experimentally characterize a light source's photon statistics and use it in the estimation of a quantum key distribution system's key rate. This promises to be a useful tool for the certification of quantum-related technologies.

© 2018 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

## 1. Introduction

Quantum random number generators (QRNGs) [1,2] and quantum key distribution (QKD) [3–5] are the first quantum-related technology to leap out of the lab and reach the maturity necessary for the market. The goal of a QRNG is to generate unpredictable numbers based on the laws of quantum physics. The typical example is a single, indivisible, photon impinging on a beam splitter [1,6,7], which ideally provides a uniformly distributed random bit, 0 or 1, depending on the output port it emerges from. By measuring the photons with a pair of photodetectors, it is possible to extract random strings that can be suitably post-processed and employed for cryptographic applications as well as for lotteries, gambling and scientific simulations. Other common implementations are based on events that are expected to follow a Poissonian distribution, for example the arrival time of photons emitted by a coherent light source [2,8–11]. In other cases, as for QRNGs based on the phase noise of a laser [12–16], the Poissonian nature of the source can provide evidence of the correct functioning of the randomness-generating mechanism.

On the other hand, the aim of QKD is to generate shared randomness between two distant parties, traditionally called Alice and Bob, through the exchange of quantum signals. The most common light source in QKD systems is a laser followed by an attenuator. The attenuation level depends on the particular protocol implemented, but in general it is set so that the intensity of the emitted pulses approaches the single-photon regime, which is captured by the following condition:

$$\mu = \sum_n p_n n < 1. \quad (1)$$

In Eq. (1),  $\mu$  is the mean photon number of each emitted pulse and  $p_n$  is the probability to emit  $n$  photons. The calibration of the mean photon number is essential to guarantee the security of QKD systems. If  $\mu$  is too large, the secret information is redundantly encoded in  $n > 1$  photons, allowing an eavesdropper (Eve) to access the secret information. Therefore  $\mu$  has to be carefully set and it is typically monitored in real time in existing QKD systems [17].

However, this is not the only security requirement and the statistics of the source, represented by  $p_n$  in Eq. (1), also plays a crucial role. To gain some insight into this problem, consider Fig. 1, where three different types of photon number distributions are depicted, all displaying an average photon number  $\mu = 1$ . Figure 1(a) is the Poissonian case, with  $p_n = e^{-\mu} \mu^n / n!$ , which

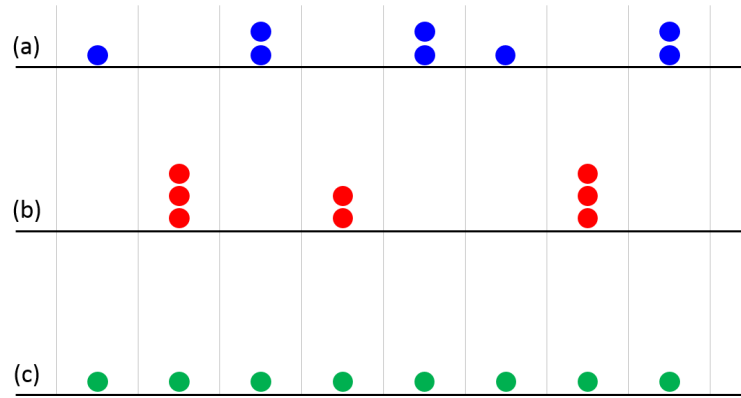


Fig. 1. Schematic of photon number distributions in a train of optical pulses with average photon number  $\mu = 1$ . (a) Poissonian source; (b) super-Poissonian source; (c) single-photon source. Each colored dot represents a single photon. Vertical lines identify the optical pulses in the same time slot.

typically stems from a laser operated well above threshold [18]. The resulting distribution is composed of statistically independent events and the number of photons in each pulse varies in a random way. In the super-Poissonian case, on the other hand, represented in Fig. 1(b), the light is composed of photons bunched in the same optical pulse. The typical example is a thermal source, which features photon number statistics equal to  $p_n = \mu^n / (1 + \mu)^{1+n}$ . Finally, we show in Fig. 1(c) the ideal case of a true single-photon source, which features  $p_1 = 1$ ,  $p_{n \neq 1} = 0$  and displays deterministic emission of exactly one photon per pulse.

Loosely speaking, case (c) is the most secure, as there never is more than one photon carrying the secret information, whereas case (b) is the least secure, because the photon bunching effect favors the redundant encoding of the information. More accurately, for a given photon generation rate and for a fixed security level guaranteed by the three cases above, case (c) and (b) provide, respectively, the best and the worst performance, as they are the closest to and the farthest from the ideal case. This shows that even if the mean photon number  $\mu$  is known, the photon number distribution probability  $p_n$  can still affect the performance of a QKD system and is therefore important to find ways to properly characterize it.

For that, one method would be to use photon number resolving detectors or, equivalently, space-multiplexed or time-multiplexed threshold detectors [19–21]. However, in this case, a precise calibration of the detection efficiency would be required, which is far from trivial. A second, more practical, method is the one proposed here. We perform a generalized Hanbury Brown-Twiss (HBT) experiment [22, 23] to estimate the normalized correlation functions  $g^{(m)}(\tau)$  [24, 25] of the light source, with  $m = \{2, 3, 4\}$ . These functions, evaluated at time delay  $\tau = 0$ , are closely related to the photon statistics of the light source. For example, it is well-known that if  $p_n$  follows a Poissonian statistics, the light source has all the  $g^{(m)}(0)$  equal to unity [18], irrespective of the order  $m$ . Although experimentally it is not possible to measure the correlation functions to all orders, we will show that measuring them up to the fourth order is sufficient to determine tight bounds on the secure key rate of a QKD system.

To apply this method, we consider a scenario where the characterization of the light source is done off-line, at a different time to the QKD transmission, in an environment that has been reasonably cleared of the presence of Eve. Moreover, we will work in the low detection efficiency approximation. This allows us to treat our threshold detectors as linear and makes our estimate independent of the exact efficiency of the detectors used in the experiment. The details of this approach are given in the next Sec. 2. In Sec. 3 we will describe the experimental implementation,

whereas in Sec. 4 we will exploit our experimental results to estimate the secure key rate of a QKD system [26].

## 2. Normalized correlation functions

In the present work, we are interested in the characterization of the photon statistics  $p_n$  of a light source that is suitable for quantum-related technologies like a QRNG or a QKD system. We consider a scenario where the characterization is worked out using detectors that are only loosely calibrated. In particular, we assume that the tester has guarantees that the efficiency of his detectors is positive but, at the same time, smaller than a certain threshold  $\eta_0$ . This allows us to treat threshold detectors as if they were linear and makes our result independent of the exact value of the detectors' efficiency. This assumption is perfectly reasonable if the source is tested in a trusted environment, where there is no eavesdropping ongoing during the test. It is then reasonable to assume that the tester has a certain control over his detectors and can arbitrarily decrease their efficiency below  $\eta_0$  using a suitable attenuator.

Under this assumption, we can write the “normalized correlation functions” [24, 25], or “degrees of coherence” [18],  $g^{(2)}(0)$ ,  $g^{(3)}(0)$ ,  $g^{(4)}(0)$  of a stationary light source as:

$$g^{(2)}(0) = \langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rangle / \langle \hat{a}^\dagger \hat{a} \rangle^2 \quad (2)$$

$$g^{(3)}(0) = \langle \hat{a}^\dagger \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \hat{a} \rangle / \langle \hat{a}^\dagger \hat{a} \rangle^3 \quad (3)$$

$$g^{(4)}(0) = \langle \hat{a}^\dagger \hat{a}^\dagger \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \hat{a} \hat{a} \rangle / \langle \hat{a}^\dagger \hat{a} \rangle^4 \quad (4)$$

where  $\hat{a}^\dagger$  and  $\hat{a}$  are the boson creation and annihilation operators of a single quantum of light, respectively, and the bra-ket notation indicates the average over the states emitted by the source represented by the density matrix  $\rho$ , i.e.,  $\langle \Theta \rangle = \text{tr}\{\rho\Theta\}$ .

When the source is pulsed, which is often the case in QKD systems, the above relations can be written in a discrete form [27, 28]:

$$g^{(2)}[0] = \langle \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k \hat{a}_k \rangle / \langle \hat{a}_k^\dagger \hat{a}_k \rangle^2 \quad (5)$$

$$g^{(3)}[0] = \langle \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k \hat{a}_k \hat{a}_k \rangle / \langle \hat{a}_k^\dagger \hat{a}_k \rangle^3 \quad (6)$$

$$g^{(4)}[0] = \langle \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k \hat{a}_k \hat{a}_k \hat{a}_k \rangle / \langle \hat{a}_k^\dagger \hat{a}_k \rangle^4 \quad (7)$$

where  $k$  denotes the integer value representing the pulse number. In the following, we will use a compressed notation  $g_m$  to indicate the quantity  $g^{(m)}[0]$ , dropping the zero time delay whenever it is unnecessary to specify it.

The normalized photon correlation functions in Eqs. (5)-(7) represent the quantities measured in our experiment. Under the low detection efficiency approximation they are attractive from an experimental point of view as they can be measured using threshold single photon detectors. We point the reader to the prior art in [18] and [28] for the proof that the measurement of the  $g_m$  is not affected by the loss or by the imbalance in the beamsplitters or in the detectors unequal efficiency.

To connect the discrete correlation functions  $g_m$  with the photon statistics  $p_n$ , we express the density matrix of the state emitted by the source,  $\rho$ , as a sum of photon number states:

$$\rho = \sum_{n=0}^{\infty} p_n |n\rangle \langle n|. \quad (8)$$

The form of  $\rho$ , diagonal in the photon number states, is due to our use of a phase-randomized laser source [29].

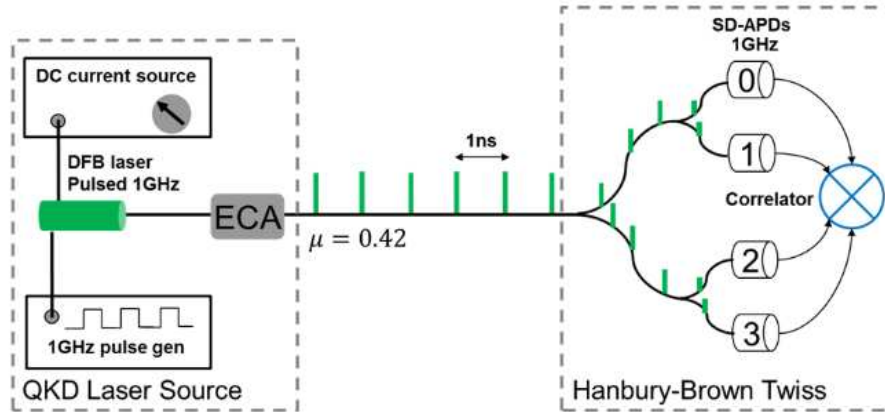


Fig. 2. Schematic of the experimental arrangement for measuring normalized correlation functions up to the fourth order. ECA: electronically controlled attenuator, SD-APD: self-differencing avalanche photodiode.

Upon rewriting Eqs. (5)-(7) in terms of the density matrix and using the compressed notation previously introduced, we obtain:

$$g_2 = \sum_{n=0}^{\infty} p_n [n(n-1)] / \mu^2 \quad (9)$$

$$g_3 = \sum_{n=0}^{\infty} p_n [n(n-1)(n-2)] / \mu^3 \quad (10)$$

$$g_4 = \sum_{n=0}^{\infty} p_n [n(n-1)(n-2)(n-3)] / \mu^4 \quad (11)$$

where  $\mu$  has been defined in Eq. (1). From the above equations, it is apparent that the value of  $\mu$  is necessary to find out the  $n$ -photon probability  $p_n$ . For example, it is intuitive that for large  $\mu$  the  $p_n$  will be centered around larger values of  $n$ . However, the exact determination of  $\mu$  is not necessary for estimating the correlation functions  $g_m$ . Therefore we can treat  $\mu$  as a parameter of the theory, known to the user Alice who prepares the states for the QKD protocol. It is worth noting that in existing QKD systems  $\mu$  is usually measured quite easily and precisely by means of a calibrated power meter, whose output is fed into a feedback loop to guarantee the high stability of the measured value.

### 3. Experimental setup and results

A schematic of the experimental arrangement used to characterize the  $g_m$  functions is shown in Fig. 2. In order to connect our method with a prominent application, the light source to be characterized has been taken directly from a GHz-clocked QKD prototype [17].

It consists of a DFB laser diode linked to a 1 GHz pulse generator and driven by a DC current source. A small DC current is supplied to the laser diode from the DC current source, which causes a minor amount of spontaneous emission. The pulse generator produces a square wave so the on-period is 500ps followed by a 500ps off-period. The square wave has an amplitude of approximately 2V which modulates the DFB laser diode on top of the DC current. Note the AC and DC parts of the electrical biasing are combined using an integrated bias tee inside the DFB laser diode. Under normal operating conditions, the modulation drives the laser diode in a gain switched mode, i.e., above and below lasing threshold. Here laser threshold intensity is defined as the resulting optical intensity at which the laser gain equals the loss [30]. In addition the laser threshold here refers to the pulsed laser threshold and represents a time-averaged photocurrent include both DC and AC pulsed currents. The DC driving current is set well below

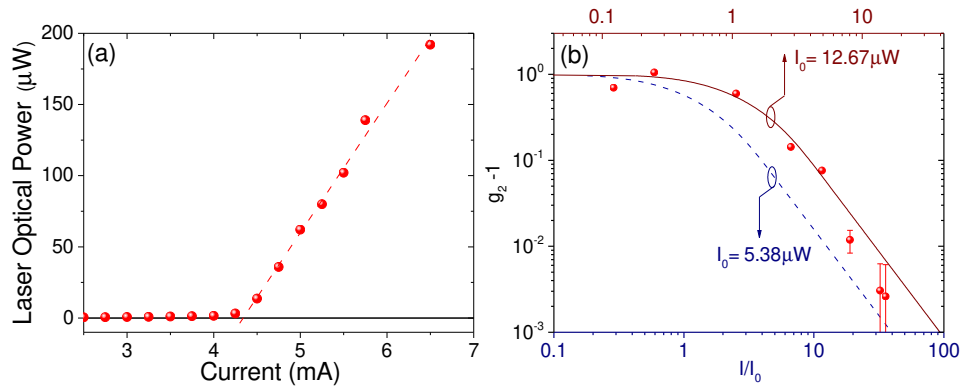


Fig. 3. (a): Laser DC current vs optical output power from DFB laser diode. Above threshold, around 4.5 mA, there is a steep rise in output power. (b):  $g_2 - 1$  as a function of laser optical intensity  $I$ , normalized to threshold optical intensity  $I_0$  with  $I_0 = 12.67 \mu\text{W}$ . Points: Experimental data. Solid curve: fit of the non-linear oscillator model using  $I_0$  as a free parameter. Dashed curve: non-linear oscillator model with  $I_0 = 5.38 \mu\text{W}$ .

the conventional DC threshold current thus fulfilling the requirement of gain switching. The effect of the modulation is to cause a train of phase-randomized optical pulses to be produced at a frequency of 1 GHz [16]. The resulting optical pulses are then attenuated to the single photon level using an electronically controlled attenuator (ECA), so that the condition expressed by Eq. (1) is satisfied in our experiments.

To analyze the correlation functions, a four channel HBT interferometer was constructed. Photons from the QKD laser source under test are transmitted into a 50:50 beamsplitter whereupon they encounter a second 50:50 beamsplitter. Four self-differencing avalanche photodiodes (SD-APD) [31] synchronized to the QKD laser source detect the transmitted photons. Care was taken in the experiment to guarantee a detection efficiency well below 1% in each detector. The subsequent electrical output from each SD-APD is then discriminated before being sent to a correlator card where time stamps are assigned to the photon arrivals. The time stamps from the correlator were analyzed by a custom built program. The program constructed two, three and four-fold photon coincidences from the photon arrival times. From this data, the resulting correlation functions up to the fourth order were evaluated.

### 3.1. Dependence on laser drive current

We start our analysis by examining the effect of changing the laser drive current on the normalized second order correlation function  $g_2$ . This allows us to gain some insight on how the photon statistics might change for a laser diode under different operating conditions.

Figure 3(a) shows the DC laser current vs optical output power dependence for the QKD laser source. The 1 GHz square wave modulation is applied at all times. Note the optical power is measured before the ECA using a standard optical power meter. As expected, the optical output rises sharply after the lasing threshold, around 4.5 mA, has been exceeded. Figure 3(b) (points) shows the resulting normalized second order correlation function minus one ( $g_2 - 1$ ) as measured in the single photon regime (i.e. after the ECA). Below lasing threshold,  $g_2 - 1 \approx 1$ , indicating photon bunching, as might be expected for a thermal-like source. Around threshold,  $g_2 - 1$  starts to reduce. As the DC current is further increased, the fluctuations begin to die out and  $g_2 - 1$  tends to 0, indicating the laser emission is approaching Poissonian-like photon statistics, for which  $g_2 = 1$ .

To gain more insight into the functional dependence of  $g_2 - 1$  on laser intensity, we fit



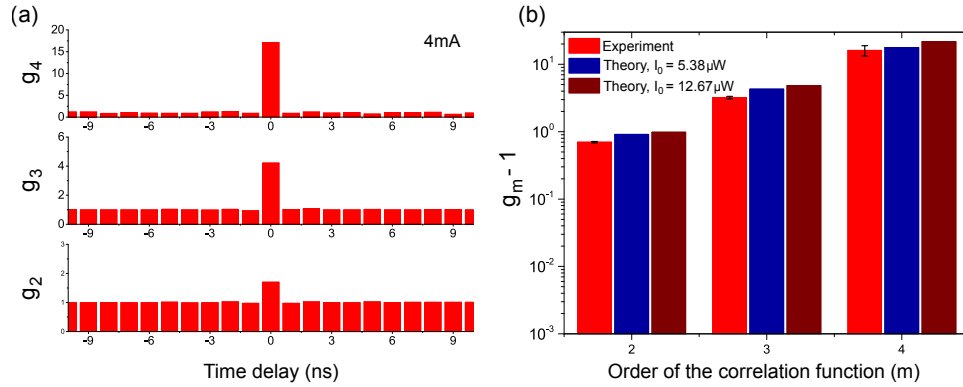


Fig. 4. (a): Measured normalized correlation functions  $g_2$ ,  $g_3$  and  $g_4$  for a DC current of 4.0 mA. (b):  $m$ -th order  $g_m - 1$  as a function of the order  $m$ . Red bars: experimental data; blue bars: prediction of non-linear oscillator model when  $I_0 = 5.38 \mu\text{W}$ ; wine bars: prediction of non-linear oscillator model when  $I_0 = 12.67 \mu\text{W}$ .

the experimental data in Fig. 3(b) with a non-linear oscillator model [30], using a single free parameter, the laser threshold intensity  $I_0$ . This model has been successful in describing  $g_2$  around lasing threshold for gas lasers [32] provided the lasers under study can be approximated as single mode. The fit gives  $I_0 = 12.67 \mu\text{W}$  corresponding to a DC current of 4.49 mA (solid curve in Fig. 3(b)). The fit appears reasonable for the experimental points around  $I = I_0$  and up to  $I = 6I_0$ . Beyond this laser intensity, the model overestimates  $g_2 - 1$ . Alternatively, we can extract a rough indication of lasing threshold  $I_0$  from Fig. 3(a) whereby we fit the experimental data above  $I_0$  using a straight line, yielding  $I_0 = 5.38 \mu\text{W}$ , corresponding to a DC current of 4.34 mA. This gives the dashed curve in Fig. 3(b), now obtained with no free fitting parameters. In this case the experimental points in the range  $1 < I/I_0 < 10$  are above the dashed curve although the points  $I/I_0 > 10$  are closer to the prediction of this model.

The above analysis suggests the underlying model of the non-linear oscillator qualitatively describes the experimental data, if not quantitatively. Most likely the ideal model lies between the two curves in Fig. 3(b). Note, as we show below, we do not rely on any physical model to construct bounds on the secure bit rate, see Sec. 4.

For use in QKD, it is important to choose an appropriate DC current level. Too low gives large photon bunching and therefore a high incidence of multi-photon events, which greatly facilitates photon number splitting attacks by an eavesdropper. Too high a DC current yields Poissonian behavior but increases the laser CW optical background. A high CW optical background increases the phase correlation between successive optical pulses and destroys the phase randomization of the QKD laser source [16].

We choose a compromise such that under normal operating conditions, i.e. during QKD, the DC current is set to approximately 6.5 mA which corresponds to  $g_2 - 1$  of the order of  $10^{-3}$ , as shown in Fig. 3(b).

Next we characterize higher order correlations. By way of comparison higher order correlations are measured for two cases. Firstly, below lasing threshold at a DC current of about 4.0 mA. Secondly, above lasing threshold, where the DC current is 6.5 mA corresponding to normal operating conditions.

### 3.1.1. Variation of $g_m$ for laser below threshold

We first examine the variation of the higher order correlation functions when the laser is operated below threshold. A DC current of 4.0 mA is selected.

Figure 4(a) shows the measured normalized correlation functions  $g_2$ ,  $g_3$  and  $g_4$  and the numerical values are listed in the following equations:

$$g_2 = 1.6985 \pm 0.0138 \quad (12)$$

$$g_3 = 4.21 \pm 0.13 \quad (13)$$

$$g_4 = 17.11 \pm 2.84 \quad (14)$$

The source displays a high level of bunching, approaching a thermal distribution, hence we term it “quasi-thermal”. The peak at time zero grows with the order  $m$ , as shown with red bars in Fig. 4(b). Also plotted are the predictions of the non-linear oscillator model for the two laser threshold intensities shown in Fig. 3(b). Both scenarios predict slightly stronger correlations for all orders compared to what was experimentally measured. This behavior can be intuitively understood by assuming the source is mainly bunched but also possesses a smaller Poissonian component since the measured  $g_2 = 1.6985$  is less than the value  $g_2 = 2$  expected for a purely thermal source. The bunching contribution naturally gives stronger correlation values  $g_m$  as  $m$  is increased but at the same time the smaller Poissonian component contributes to reducing these correlation values. In Fig. 4(a), small fluctuations are visible around the central peak, suggesting negatively correlated intensity fluctuations. This agrees with the findings in Ref. [33], which reports anti-correlated intensity fluctuations from gain-switched lasers in the proximity of the lasing threshold. These fluctuations become negligible when the laser is operated well above threshold.

### 3.1.2. Variation of $g_m$ for laser above threshold

We now turn our attention to the variation of the higher order correlation functions when the laser is operated above threshold. A DC current of 6.5 mA is selected for this purpose. The acquisition period for the experiment time was approximately 24 hours in order to reduce the error bar size for  $g_4$ . Figure 5(a) shows the measured normalized correlation functions  $g_2$ ,  $g_3$

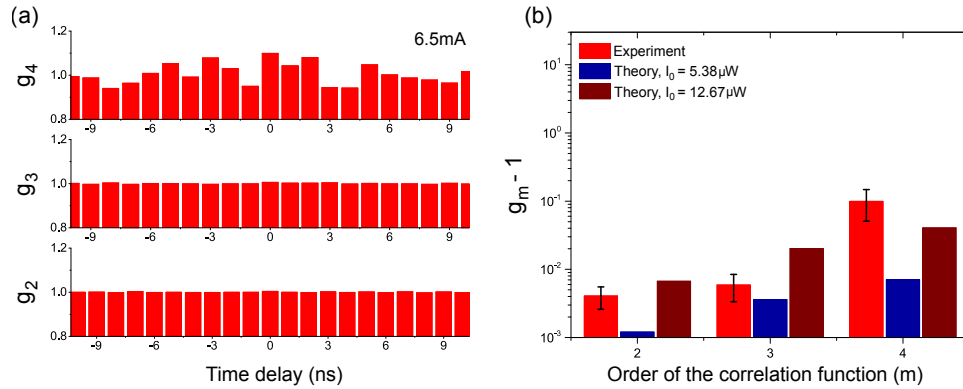


Fig. 5. (a): Measured normalized correlation functions  $g_2$ ,  $g_3$  and  $g_4$  for a DC current of 6.5 mA. (b):  $n$ -th order normalized correlation functions as a function of the order  $n$ . Red bars: experimental data; blue bars: prediction of non-linear oscillator model when  $I_0 = 5.38 \mu\text{W}$ ; wine bars: prediction of non-linear oscillator model when  $I_0 = 12.67 \mu\text{W}$ .

and  $g_4$  and the numerical values are:

$$g_2 = 1.0041 \pm 0.0039 \quad (15)$$

$$g_3 = 1.0059 \pm 0.0056 \quad (16)$$

$$g_4 = 1.099 \pm 0.049 \quad (17)$$



On this occasion there is no clear peak at time zero, which indicates the laser is qualitatively Poissonian. However, plotting the  $g_m$  as a function of  $m$  reveals an ever so slight increase in correlation despite the large error bars, associated with the red bars in Fig. 5(b). On this occasion the source appears to have a minor bunched-like component, hence much weaker correlation values  $g_m$  are observed as the order  $m$  is increased, compared to the previous case.

Again we plot the predictions of the non-linear oscillator model for the two laser threshold intensities shown in Fig. 3(b). The non-linear oscillator model qualitatively follows the trend of the experiment but not quantitatively. This implies some correction of the non-linear oscillator model is demanded. However, as we show below, an exact model isn't required for quantifying QKD security; just the measured correlation functions  $g_m$  and their associated error bars are required.

Note for the measured correlation functions we have also considered corrections from afterpulsing, dark counts and dead time. However these corrections are well within the size of one error bar, so have consequently been safely neglected in the current analysis.

#### 4. Worst-case bounds from correlation functions and secure key rate

Let us now consider how the experimental results from the previous section can be used to determine the secure key rate of a QKD system. For that, we rewrite the key rate equation for the efficient [34,35] decoy-state [36–38] BB84 protocol [3] in the finite-size scenario [26,39,40] in the following way:

$$R \geq p_u p_Z^2 \{ \underline{p}_1 \underline{y}_{1,Z} [1 - h(\bar{e}_{1,X})] - f Q_Z h(E_Z) - \Delta \}. \quad (18)$$

With minor modifications, Eq. (18) can be easily adapted to other BB84-like protocols. To write it, we considered a protocol where Alice prepares phase-randomized weak coherent states in the two bases  $Z$  and  $X$ , randomly chosen with probabilities  $p_Z$  and  $p_X = 1 - p_Z$ , respectively, and in the three intensity classes  $u$  (signal),  $v$  (decoy) and  $w$  (vacuum), randomly chosen with probabilities  $p_w$ ,  $p_v$  and  $p_u = 1 - p_v - p_w$ , respectively. However, the users extract the secure key bits only from the basis  $Z$  and from the class  $u$ . The quantity  $R$  is the fraction of secure bits per signal distilled by the system; when multiplied by the system's clock rate, it provides the amount of secure bits in the time unit;  $\bar{e}_{1,X}$  is the upper bound for the phase error rate associated to the single-photon events in the  $Z$  basis, estimated from the counts in the  $X$  basis and  $\underline{y}_{1,Z}$  is the lower bound to the 1-photon yield in the  $Z$  basis. This last quantity is multiplied by the lower bound to the 1-photon probability,  $\underline{p}_1$ , thus providing an overall lower bound to the 1-photon gain of the protocol. Finally,  $f$  is the inefficiency of error correction,  $Q_Z$  and  $E_Z$  are the gain and the QBER, respectively, measured in the  $Z$  basis and  $\Delta$  is a parameter related to the finite-size effect.

The crucial difference between the rate in Eq. (18) and previous QKD key rates resides in the term  $\underline{p}_1$ . Usually, a Poissonian distribution is assumed for decoy-state QKD, entailing that  $p_1 = \mu e^{-\mu}$  [36–38]. However, by applying our method, we can now drop this assumption and replace it with the lower bound  $\underline{p}_1$  that is retrieved from measured in the experimental characterization of the light source. Similar bounds can be obtained for the other probabilities  $p_0$ ,  $p_{\geq 2}$ , as well as for the other parameters  $y_0$ ,  $y_1$ ,  $e_1$  usually present in decoy-state QKD. The details on the constrained numerical optimization providing such bounds are given in the Appendix. Here and in the following, we outline the main steps.

First, we target the derivation of  $\underline{p}_1$  under the constraints represented by Eqs. (15)-(17). We treat the experimentally determined  $g_m$  as normally-distributed random variables, with mean values  $g_m^*$  and standard deviations  $\sigma_{g_m}$ , both specified in Eqs. (15)-(17). This is reasonable due to the central limit theorem and to the fact that the repeated runs in these measurements are largely independent. This allows us to write the quantile  $\gamma_{1-\epsilon}$ , which gives us the probability  $2\epsilon$  that the true value of the random variable lies outside the confidence interval  $[g_m^* - \gamma_{1-\epsilon} \sigma_{g_m}, g_m^* + \gamma_{1-\epsilon} \sigma_{g_m}]$ .

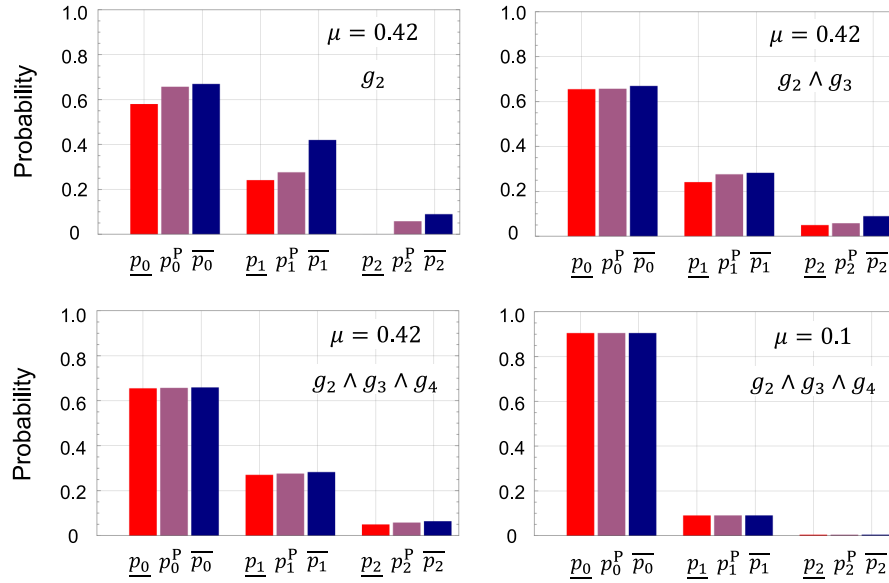


Fig. 6. Bounds to the photon probabilities  $p_0, p_1, p_2$  for various experimental conditions. In the top right corner of each diagram, the correlation functions used in the estimation of the bounds and the mean photon number  $\mu$  are indicated. Underlined (overlined) quantities are for lower (upper) bounds obtained from the experimental data given in Sec. 3.1.2, Eqs. (15)-(17), for a confidence interval of 7 standard deviations. The superscript P refers to the ideal Poissonian distribution. **Numerical Values.** Poissonian:  $p_n^P = e^{-\mu} \mu^n / n!$ , with  $\mu = \{0.42, 0.1\}$ . Bounds – clockwise starting from top-left diagram:  $p_0 = \{0.580; 0.655; 0.905; 0.655\}$ ;  $\overline{p_0} = \{0.670; 0.669; 0.905; 0.659\}$ ;  $p_1 = \{0.2411; 0.2411; 0.0903; 0.2702\}$ ;  $\overline{p_1} = \{0.4203; 0.2826; 0.0906; 0.2826\}$ ;  $\underline{p_2} = \{0; 0.04973; 0.00446; 0.04973\}$ ;  $\overline{p_2} = \{0.08947; 0.08947; 0.00461; 0.06405\}$ .

When the three constraints of Eqs. (15)-(17) are taken into account, the overall probability to fall outside the confidence interval raises to  $6\epsilon$ .

It is worth recalling that in our security model this part of the procedure is carried out off-line in a protected environment. So the assumption on the independence of repeated measurements and the statistical fluctuations of the data sample can only indirectly affect the security of the system. In particular, the measurement of the  $g_m$  does not require the typical real-time finite-size analysis of a QKD data sample. This measurement can even last for a long time under stable experimental conditions. We also notice that, in principle, the  $p_n$ 's depend on the mean photon number. So we should repeat the same procedure outlined above for each of the mean photon number values used in the QKD experiment, e.g., for  $\mu = \{u, v, w\}$  if we refer to the decoy-state BB84 protocol. While this would be straightforward in our experiment, we find that the resulting photon statistics for typical values of  $v$  and  $w$  is virtually indistinguishable from the ideal Poissonian distribution, so we simply assume a Poissonian distribution in this case.

As an example, we provide in Fig. 6 the bounds for  $p_0, p_1$  and  $p_2$  drawn from the experimental values reported in Eqs. (15)-(17) and we compare them with the corresponding probabilities from the Poissonian distributions, for various experimental conditions. On the top-left diagram, we consider the case where Alice prepares a mean photon number  $\mu = u = 0.42$ , a common value for the signal state in decoy-state QKD, and uses only the  $g_2$  function from Eq. (15) as a constraint. In this case, the comparison with the ideal Poissonian probabilities normally used in decoy-state QKD shows that the bounds are quite loose. Therefore, we expect a dramatic reduction of the key

rate obtained by assuming that the distribution is Poissonian. However, if more constraints are added, the bounds become tighter and tighter, as can be noted from the top-right and bottom-left diagrams in Fig. 6. This should entail a close-to-ideal key rate in these cases. Finally, when the mean photon number is decreased to  $\mu = \nu = 0.1$ , a value commonly used for decoy states in QKD, and all the constraints are applied, the match with the Poissonian probabilities is nearly perfect (see bottom-right diagram in Fig. 6), implying a negligible reduction in the key rate.

In the estimation leading to Fig. 6, we have considered a quantile  $\gamma_{1-\epsilon} = 7$ , which corresponds to a probability  $\epsilon = 2.56 \times 10^{-12}$  that the true experimental value falls outside the confidence interval. In turn, once all the confidence intervals related to the constrained optimization are taken into account [41], this probability generates a global security parameter for the QKD protocol in the finite-size scenario equal to  $3.3 \times 10^{-11}$ .

Once the bounds to the photon statistics have been obtained, we proceed to determine the bounds for the single-photon quantities that enter the key rate equation, Eq. (18). In this case, we need to include constraints that explicitly deal with the statistical fluctuations of the data sample. This is done by counting the total signals exchanged in the QKD session as well as the counts and the errors detected by the receiving user. Then, under the assumption of identically and independently distributed variables, the Clopper-Pearson statistical analysis [42] is adopted to determine the confidence intervals for the yields  $Y^{(\mu)} \in [\underline{Y}^{(\mu)}, \bar{Y}^{(\mu)}]_{\epsilon}$  and the error rates  $E^{(\mu)} \in [\underline{E}^{(\mu)}, \bar{E}^{(\mu)}]_{\epsilon}$  of the QKD session, respectively [26], where  $\epsilon$  denotes the failure probability. For each basis of the BB84 protocol, the yield is the ratio of the counts detected by the receiving user to the number of preparations sent by the transmitter, whereas the error rate is the ratio between the errors and the detected counts. In the final optimization problem we have six constraints for the yields and one for the error rate (see Appendix), contributing with  $7\epsilon$  to the overall failure probability. The lower and upper bounds of the confidence intervals are then used to write the constraints leading to the single-photon yield lower bound,  $\underline{y}_1$ , and to the single-photon phase error rate upper bound,  $\bar{e}_1$ , through the decoy-state equations (see Eqs. (56), (57) and (60) in the Appendix).

As a prominent application of our method, we use the bounds just derived to estimate the secure key rate of a QKD system according to Eq. (18). The results are shown in Fig. 7. It can be seen that when the  $g_2$  function is the only constraint in the problem (wine-colored line), there is a considerable decrease in key rate and maximum distance achieved by protocol. On the contrary, when also the  $g_3$  and  $g_4$  are taken into account (green and blue lines), the key rate is very close to the ideal one. Intuitively, this can be explained by the fact that each additional constraint improves the bounds on the  $p_n$ . When only  $g_2$  is considered, we can only reliably bound the first term in the photon statistics,  $p_0$ , which does not enter the key rate equation (18), or it plays only a minor role in other versions of the BB84 protocol [40]. However, when both  $g_2$  and  $g_3$  are considered, we can bound  $p_0$  and  $p_1$ , the latter being the most important term in the secure key rate. This explains the large gap in the plotted key rates between the orange line ( $g_2$  only) and the red line ( $g_2$  and  $g_3$  together).

In the same figure, we also plot in red color the key rate corresponding to the quasi-thermal source described in Sec. 3.1.1, which is obtained by plugging Eqs. (12)–(14) into the corresponding optimization problem. The upper and lower bounds are shown in the inset of Fig. 7. It can be noticed that the lower bound for the zero-photon fraction of this distribution (leftmost yellow bar) is higher than the corresponding Poisson probability (brown bar), clearly showing that the distribution is not Poissonian. Nevertheless, it is still possible to extract from it a key rate that remains positive up to a distance of about 40 km in optical fibre. Larger distances might be achieved upon optimization of the system's parameters. This positive key rate is remarkable given the highly bunched nature of the source and represents an experimental evidence of a positive key rate drawn from a quasi-thermal source.

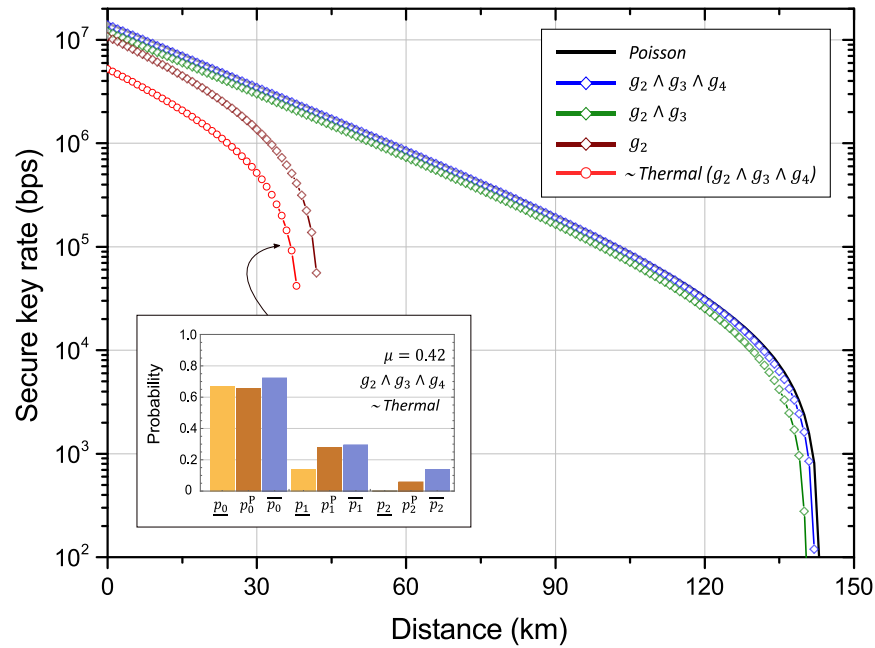


Fig. 7. Secure key rate of the efficient decoy-state BB84 protocol in the finite-size scenario, for the ideal case of a Poissonian source (black line) and for the real case where the correlation functions up to the fourth order have been measured. The values of the correlation functions have all been drawn from the experiments. The blue, green and wine lines correspond to the source described in Sec. 3.1.2, Eqs. (15)–(17), whereas the red line is for the source in Sec. 3.1.1, Eqs. (12)–(14). The bounds for this latter source, which displays a quasi-thermal distribution, are given in the inset, together with the Poisson probabilities for comparative purposes. The mean photon number for the signal and the decoy states in the protocol have been set to  $\mu = 0.42$  and  $\nu = 0.02$ , respectively. The security parameter is  $\epsilon < 10^{-10}$  and the finite-size sample is drawn from a minimum of  $1.2 \times 10^{12}$  initial pulses.

On the other hand, this result should be treated as a caveat for the correct operation of a laser source. If the laser is unconsciously operated close-to-threshold, the users will not realize that the correct key rate is the one corresponding to a quasi-thermal source (red line in Fig. 7) and will keep using the privacy amplification corresponding to a Poissonian source. This entails that less privacy amplification than necessary will be performed, compromising the security of the system. The calibration of the QKD system's light source and the detailed description of its operative parameters represent a desirable best practice to prevent these kind of security risks.

## 5. Conclusion

In quantum-related technology, claims about randomness and security crucially depend on a set of assumptions that have to be carefully met in the implementation. In the present work, we introduced and experimentally realized a test for one of the most common assumptions in QRNG devices and QKD systems, i.e., the Poissonian nature of the light source.

The method is based on a generalized HBT experiment [22] with single-photon detectors in the low-efficiency approximation. If the detection efficiency is known to be small, the exact efficiency of each detector simplifies in the corresponding expressions of the normalized correlation functions, Eqs. (5)–(7). This lets us bypass an accurate calibration of the detectors, which is often a cumbersome process.

On the other hand, our method makes it possible to test a light source upon which the tester has some limited prior knowledge. For example, we showed that the source in this work qualitatively follows a well-established laser model. However, the technique does not make use of this model and makes no stringent assumptions on the physics underlying the photon source under test. This identifies a practical way to undertake calibration tests, which are normally performed in the protected environment of a laboratory, where the assumptions on the potential presence of a malevolent agent are mild.

The results of the experimental tests, given in Eqs. (12)-(14) for a laser operated close to threshold and in Eqs. (15)-(17) for a laser above threshold, show that photon statistics of the light source crucially depend on the driving current. When the laser is operated above threshold, the photon distribution is very close to Poissonian, which is especially true when the mean photon number is low. In this case, the normalized correlation functions up to the fourth order are all close to 1. This implies that the bounds to the Poissonian distribution, depicted in Fig. 6, are quite tight. Nevertheless, when plugged in a typical key rate equation for a QKD system, these bounds generate a key rate that can deviate from the ideal one. This is shown in Fig. 7, which suggests that measuring at least the  $g_2$  and  $g_3$  correlation functions is essential to avoid a major reduction of the secure key rate. This is feasible and practical, as we have shown, thus promoting the present method as a useful tool to guarantee the security of QKD systems. Close to threshold, the distribution of the emitted photons becomes quasi-thermal and displays a highly bunched behavior. However, even without optimizing the system's parameters, we could obtain a positive key rate over a few tens of kilometers of optical fiber.

## A. Bounds for the photon statistics

In this section we show how to bound the photon probabilities  $p_n$  using the experimentally measured correlation functions  $g_m$ , with  $m = \{2, 3, 4\}$ . This is a constrained optimization problem that can be cast in linear form, so that it is efficient and provides a global solution.

In this problem, the probabilities  $p_n$  are the objective functions and the experimental correlation functions are the constraints. We will consider in the following a specific problem, i.e., the minimization of the single-photon probability  $p_1$  when Alice emits optical pulses with mean photon number  $\mu = u$  (signal in the decoy-state BB84 protocol). Other problems related to the maximization of  $p_1$ , or to the optimization of the other  $p_n$ 's, with  $n \neq 1$ , are analogous and can be straightforwardly obtained from the one described here. Moreover, as we noted in the main text, we assume that the photon statistics is Poissonian when  $\mu = \{v, w\}$ , as the difference from a Poissonian distribution is negligible in this case (see bottom-right diagram in Fig. 6, where the mean photon number is 0.1, i.e., 5 times bigger than the value considered here). Hence, in what follows we will use  $p_n$  in lieu of  $p_n^{(u)}$  whenever it is unnecessary to specify the mean photon

number label. With this notation, the optimization problem can be written as:

$$\text{minimize } \hat{p}_1 \quad (19)$$

$$\text{subject to } 1 = \sum_{n=0}^{\infty} \hat{p}_n \quad (20)$$

$$\hat{g}_2 = \sum_{n=0}^{\infty} \hat{p}_n n(n-1) / \mu^2 \quad (21)$$

$$\hat{g}_3 = \sum_{n=0}^{\infty} \hat{p}_n n(n-1)(n-2) / \mu^3 \quad (22)$$

$$\hat{g}_4 = \sum_{n=0}^{\infty} \hat{p}_n n(n-1)(n-2)(n-3) / \mu^4 \quad (23)$$

$$0 \leq \hat{p}_n \leq 1 \quad (24)$$

$$\underline{g}_2 \leq \hat{g}_2 \leq \overline{g}_2 \quad (25)$$

$$\underline{g}_3 \leq \hat{g}_3 \leq \overline{g}_3 \quad (26)$$

$$\underline{g}_4 \leq \hat{g}_4 \leq \overline{g}_4 \quad (27)$$

where we have used hatted letters to indicate the variables of the problem and underlined or over-lined letters to indicate lower or upper bounds to the corresponding physical quantities, respectively. These bounds are specified as follows:

$$\underline{g}_2 = g_2^* - \gamma_{1-\epsilon} \sigma_{g_2} ; \quad \overline{g}_2 = g_2^* + \gamma_{1-\epsilon} \sigma_{g_2} \quad (28)$$

$$\underline{g}_3 = g_3^* - \gamma_{1-\epsilon} \sigma_{g_3} ; \quad \overline{g}_3 = g_3^* + \gamma_{1-\epsilon} \sigma_{g_3} \quad (29)$$

$$\underline{g}_4 = g_4^* - \gamma_{1-\epsilon} \sigma_{g_4} ; \quad \overline{g}_4 = g_4^* + \gamma_{1-\epsilon} \sigma_{g_4} \quad (30)$$

where the experimental quantities are taken from Eqs. (15)-(17) and  $\gamma_{1-\epsilon}$  is the already introduced quantile of the normally-distributed random variables associated to the experimental results.

The above optimization problem is linear in the unknowns and can be readily solved to find the global minimum for  $\hat{p}_1$ . However, it contains sums that run on an infinite number of terms. This is impractical to treat, so we turn it into a problem that contains a finite number of terms. The idea behind this is that when Eq. (1) is fulfilled, only the first few terms in the sums give a relevant contribution. To write this problem, we will limit the number of photons  $n$  to the interval  $[0, N_{\text{cut}}]$ , with  $N_{\text{cut}}$  a natural number chosen large enough to satisfy the following condition:

$$\sum_{n=0}^{N_{\text{cut}}} p_n \geq \sum_{n=N_{\text{cut}}}^{\infty} p_n. \quad (31)$$

By choosing  $N_{\text{cut}}$  large enough, the condition in Eq. (31) can always be fulfilled. On the practical side, we choose  $N_{\text{cut}} = 25$  in our solution. This entails that we are discarding all the photon distributions where the probability of having more than 25 photons in a single pulse is larger than the probability of having less than 25 photons in a single pulse. We believe that this assumption is met in all the distributions of practical interest. For example, if we consider a source where the measured average photon number  $\mu$  is smaller than one, as in Eq. (1), our solution rules out a distribution where one optical pulse contains 25 photons and the following 24 pulses are empty, whereas it includes the three distributions depicted in Fig. 1. Moreover, also the most exotic photon distributions could be covered by further increasing the value of  $N_{\text{cut}}$ , which is feasible, due to the linearity of the problem.

By using the closure condition  $\sum_{n=0}^{\infty} p_n = 1$  we can rewrite the assumption in Eq. (31) as  $\sum_{n=0}^{N_{\text{cut}}} p_n \geq 1/2$ . This, in turn, provides the following bounds for the sum of the variables  $\hat{p}_n$ 's in the finite-size scenario:

$$1 \geq \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n \geq \frac{1}{2}. \quad (32)$$



The lower bound in the above equation can be used to rewrite the lower bounds for the other constraints of the optimization problem:

$$\sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n \geq \mu/2, \quad (33)$$

$$\sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^2 \geq (\mu^2 \hat{g}_2 + \mu)/2, \quad (34)$$

$$\sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^3 \geq (\mu^3 \hat{g}_3 + 3\mu^2 \hat{g}_2 + \mu)/2, \quad (35)$$

$$\sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^4 \geq (\mu^4 \hat{g}_4 + 6\mu^3 \hat{g}_3 + 7\mu^2 \hat{g}_2 + \mu)/2. \quad (36)$$

To upper bound the finite sum related to the average photon number, we exploit the following chain of relations:

$$\mu = \sum_{n=0}^{\infty} \hat{p}_n n \quad (37)$$

$$= \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n + \sum_{n=N_{\text{cut}}+1}^{\infty} \hat{p}_n n \quad (38)$$

$$\geq \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n + (N_{\text{cut}} + 1) \sum_{n=N_{\text{cut}}+1}^{\infty} \hat{p}_n. \quad (39)$$

Similar relations can be easily found for the constraints involving the correlation functions. The resulting upper bounds, to be paired with the lower bounds in Eqs. (33)-(36), are:

$$\mu - (N_{\text{cut}} + 1) \left(1 - \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n\right) \geq \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n \quad (40)$$

$$\mu^2 \hat{g}_2 + \mu - (N_{\text{cut}} + 1) \left(\mu - \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n\right) \geq \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^2 \quad (41)$$

$$\mu^3 \hat{g}_3 + 3\mu^2 \hat{g}_2 + \mu - (N_{\text{cut}} + 1) \left(\mu^2 \hat{g}_2 + \mu - \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^2\right) \geq \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^3 \quad (42)$$

$$\mu^4 \hat{g}_4 + 6\mu^3 \hat{g}_3 + 7\mu^2 \hat{g}_2 + \mu - (N_{\text{cut}} + 1) \left(\mu^3 \hat{g}_3 + 3\mu^2 \hat{g}_2 + \mu - \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^3\right) \geq \sum_{n=0}^{N_{\text{cut}}} \hat{p}_n n^4 \quad (43)$$

As a result, the optimization problem for  $\hat{p}_1$  becomes:

$$\text{minimize } \hat{p}_1 \quad (44)$$

$$\text{subject to } (32) - (36) \quad (45)$$

$$(40) - (43) \quad (46)$$

$$(24) - (27). \quad (47)$$

## B. Optimization of the photon number yields

In this section, we bound the photon number yields  $y_n$  estimated through the decoy-state technique. As in the previous section, we only consider a specific problem, i.e., the minimization of the single-photon yield  $y_1$ , which is the most relevant contribution to the key rate in Eq. (18). Other problems related to the maximization of  $y_1$  or to the optimization of the other  $y_n$ 's, with  $n \neq 1$ , can be treated in a similar manner.

The objective function in the constrained-minimization problem is  $y_1$  and the constraints are



given by the usual decoy-state equations, so that we can write the optimization problem as

$$\text{minimize } \hat{y}_1 \quad (48)$$

$$\text{subject to } 0 \leq \hat{y}_n \leq 1 \quad (49)$$

$$Y^{(u)} = \sum_{n=0}^{\infty} \hat{p}_n \hat{y}_n \quad (50)$$

$$Y^{(v)} = \sum_{n=0}^{\infty} e^{-v} \frac{v^n}{n!} \hat{y}_n \quad (51)$$

$$Y^{(w)} = \sum_{n=0}^{\infty} e^{-w} \frac{w^n}{n!} \hat{y}_n \quad (52)$$

$$\underline{p}_n \leq \hat{p}_n \leq \bar{p}_n, \quad (53)$$

which should hold for all  $n$ . In the above equations, the hatted quantities are the unknowns. Moreover, we remind that  $\underline{p}_n$  and  $\bar{p}_n$  are the lower and upper bounds, respectively, for the probability that an  $n$ -photon pulse is emitted by the light source when the mean photon number  $u$  is prepared. These bounds are calculated from problems analogous to the one in Eqs. (19)-(27) for the probabilities  $p_0, p_1, p_2$  and  $p_3$ . The lower (upper) bounds for the remaining probabilities for the signal state with intensity  $u = 0.42$  are conservatively assumed to be equal to 0 (to 1). The probabilities for the decoy state with intensity  $v = 0.02$  and for the vacuum state with intensity  $w = 10^{-4}$  are explicitly taken equal to the corresponding Poissonian distribution. As already stated, this is justified by the fact that when the mean photon number is so small, we did not observe any practical deviation from a Poissonian distribution.

The constraint in Eq. (50) defines an optimization problem that is nonlinear in the unknowns. This obstacle can be overcome by replacing  $\hat{p}_n$  with the bounds  $\underline{p}_n$  and  $\bar{p}_n$  in Eq. (53). Moreover, the sums contain an infinite number of terms, which is not suitable for a practical scenario. This can be easily circumvented using the same technique demonstrated for the problem in Sec. A and in the literature [44], i.e., by cutting the sums to a finite value  $N_{\text{cut}}$  and then bounding the residual. Finally, we have to include in the problem the finite-size bounds for the yield,  $\underline{Y}^{(\mu)}, \bar{Y}^{(\mu)}$ , obtained from the QKD experiment as described in Sec. 4 of the main text. As a result, we obtain the following constraints:

$$\text{minimize } \hat{y}_1 \quad (54)$$

$$\text{subject to } 0 \leq \hat{y}_n \leq 1 \quad (55)$$

$$\bar{Y}^{(\mu)} \geq \sum_{n=0}^{N_{\text{cut}}} \bar{p}_n^{(\mu)} \hat{y}_n \quad (56)$$

$$\underline{Y}^{(\mu)} \leq \sum_{n=0}^{N_{\text{cut}}} \underline{p}_n^{(\mu)} \hat{y}_n + \bar{\Gamma}_\mu \quad (57)$$

$$\bar{\Gamma}_\mu = 1 - \sum_{n=0}^{N_{\text{cut}}} \underline{p}_n^{(\mu)}, \quad (58)$$

which should hold for all  $n$  and for  $\mu = \{u, v, w\}$ . The bounds  $\underline{p}_n^{(\mu=u)}$  and  $\bar{p}_n^{(\mu=u)}$  are calculated from problems analogous to the one in Eqs. (19)-(27) for  $n = \{0, 1, 2, 3\}$  and conservatively assumed equal to 0 and 1, respectively, for all the remaining values of  $n$ . For the remaining bounds we have  $\underline{p}_n^{(\mu=v)} = \bar{p}_n^{(\mu=v)} = e^{-v} v^n / n!$  and  $\underline{p}_n^{(\mu=w)} = \bar{p}_n^{(\mu=w)} = e^{-w} w^n / n!$ .

### C. Optimization of the photon number error rates

The optimization problem for the single-photon error rate  $e_1$  follows similar lines as in the previous sections. In QKD, and in the key rate equation (18), it is important to find an upper bound to the error rate. This can be achieved by replacing the bounds  $\underline{Y}^{(\mu)}$  and  $\bar{Y}^{(\mu)}$  in the previous

section with the bounds for the bit error rate  $\underline{B}^{(\mu)} = \underline{Y}^{(\mu)} \underline{E}^{(\mu)}$  and  $\overline{B}^{(\mu)} = \overline{Y}^{(\mu)} \overline{E}^{(\mu)}$ , respectively, and  $\hat{y}_n$  with  $\hat{b}_n$ . Then, after maximizing  $\hat{b}_1$ ,  $\bar{e}_1$  will be given by:

$$\bar{e}_1 = \frac{\bar{b}_1}{y_1}, \quad (59)$$

where  $y_1$  has been obtained from the yield optimization problem. After straightforward steps, we obtain an explicit upper bound for the single-photon error rate [41] which is the one used to draw the plots in Fig. 7:

$$\bar{e}_1 = \frac{\overline{B}^{(u)} - \underline{p}_{-0-0} e_0}{\underline{p}_{-1} y_1}. \quad (60)$$

## Funding

EMPIR programme co-financed by the Participating States and from the European Union Horizon 2020 research and innovation programme.

## Acknowledgments

During the completion of this work, a paper on a closely-related subject appeared in [43]. We acknowledge useful discussions with Toshihiro Sasaki. The present work was supported by the project EMPIR 14IND05 MIQC2. This project has received funding from the EMPIR programme co-financed by the Participating States and from the European Unions Horizon 2020 research and innovation programme.

## References

1. J. G. Rarity, P. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," *J. Mod. Opt.* **41**, 2435–2444 (1994).
2. Y. Yoshizawa, H. Kimura, H. Inoue, K. Fujita, M. Toyama, and O. Miyatake, "Physical random numbers generated by radioactivity," *J. Jpn. Soc. Comput. Stat.* **12**, 67–81 (1999).
3. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. on Comput. Syst. Signal Process.* (IEEE, New York, 1984), p. 175. (1984).
4. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.* **67**, 661–663 (1991).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145–195 (2002).
6. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and a. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instruments* **71**, 1675 (2000).
7. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *J. Mod. Opt.* **47**, 595–598 (2000).
8. M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Rev. Sci. Instruments* **78**, 045104 (2007).
9. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Appl. Phys. Lett.* **93**, 031109 (2008).
10. M. Fürst, H. Weier, S. Nauwerth, D. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Opt. Express* **18**, 13029–13037 (2010).
11. Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Appl. Phys. Lett.* **104**, 051110 (2014).
12. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. review. E, Stat. nonlinear, soft matter physics* **81**, 051137 (2010).
13. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. letters* **35**, 312–314 (2010).
14. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," *Opt. Express* **19**, 20665–20672 (2011).
15. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Opt. Express* **22**, 1645–1654 (2014).
16. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Appl. Phys. Lett.* **104**, 261112 (2014).

17. A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "High speed prototype quantum key distribution system and long term field trial," *Opt. Express* **23**, 7583–7592 (2015).
18. R. Loudon, *The quantum theory of light* (Oxford University, Oxford, 2000), 3rd ed.
19. R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nat. Photonics* **3**, 696–705 (2009).
20. E. A. Goldschmidt, F. Piacentini, I. R. Berchera, S. V. Polyakov, S. Peters, S. Kück, G. Brida, I. P. Degiovanni, A. Migdall, and M. Genovese, "Mode reconstruction of a light field by multiphoton statistics," *Phys. Rev. A* **88**, 013822 (2013).
21. F. Piacentini, M. P. Levi, A. Avella, M. López, S. Kück, S. V. Polyakov, I. P. Degiovanni, G. Brida, and M. Genovese, "Positive operator-valued measure reconstruction of a beam-splitter tree-based photon-number-resolving detector," *Opt. Lett.* **40**, 1548–1551 (2015).
22. R. Hanbury Brown and R. Q. Twiss, "A test of a new type of stellar interferometer on sirius," *Nature* **178**, 1046–1048 (1956).
23. R. Hanbury Brown and R. Q. Twiss, "Interferometry of the intensity fluctuations in light. i. basic theory: The correlation between photons in coherent beams of radiation," *Proc. IEEE Int. Conf. on Comput. Syst. Signal Process.* (IEEE, New York, 1984), p. 175. **242**, 300–324 (1957).
24. R. J. Glauber, "The quantum theory of optical coherence," *Phys. Rev.* **130**, 2529–2539 (1963).
25. R. J. Glauber, "Coherent and incoherent states of the radiation field," *Phys. Rev.* **131**, 2766–2788 (1963).
26. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Pentty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express* **21**, 24550–24565 (2013).
27. C. Santori, D. Fattal, J. Vučković, G. S. Solomon, E. Waks, and Y. Yamamoto, "Submicrosecond correlations in photoluminescence from inas quantum dots," *Phys. Rev. B* **69**, 1110 (2004).
28. M. J. Stevens, S. Glancy, S. W. Nam, and R. P. Mirin, "Third-order antibunching from an imperfect single-photon source," *Opt. Express* **22**, 3244–3260 (2014).
29. H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *Eur. Phys. J. D* **41**, 599–627 (2007).
30. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University, Cambridge, 1995), 1st ed.
31. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," *Appl. Phys. Lett.* **91**, 041114 (2007).
32. A. W. Smith and J. A. Armstrong, "Laser photon counting distributions near threshold," *Phys. Rev. Lett.* **16**, 1169–1172 (1966).
33. K. Nakata, A. Tomita, M. Fujiwara, K.-i. Yoshino, A. Tajima, A. Okamoto, and K. Ogawa, "Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution systems," *Opt. Express* **25**, 622 (2017).
34. H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *J. Cryptol.* **18**, 133–165 (2005).
35. V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Phys. Rev. Lett.* **100**, 200501 (2008).
36. W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.* **91**, 057901 (2003).
37. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.* **94**, 230503 (2005).
38. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**, 230504 (2005).
39. M. Hayashi and R. Nakayama, "Security analysis of the decoy method with the bennett–brassard 1984 protocol for finite key lengths," *New J. Phys.* **16**, 063009 (2014).
40. C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A* **89**, 374 (2014).
41. M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical treatment of quantum bugs," (SPIE, 2012), *SPIE Proceedings*, p. 85421K.
42. C. J. Clopper and E. S. Pearson, "The use of confidence or fiducial limits illustrated in the case of the binomial," *Biometrika* **26**, 404–413 (1934).
43. M. Kumazawa, T. Sasaki, and M. Koashi, "Rigorous calibration method for photon-number statistics," eprint arXiv:1710.00457 (2017).
44. K. Tamaki, M. Curty, and M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," *New J. Phys.* **18**, 065008 (2016).