Security of Decoy-State Quantum Key Distribution with Correlated Intensity Fluctuations

Xoel Sixto,[1,2,*] Víctor Zapatero,[1,2,†] and Marcos Curty[1,2]

[1] *Department of Signal Theory and Communications, Escuela de Ingeniería de Telecomunicación, University of Vigo, Vigo E-36310, Spain*

[2] *AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*

(Received 5 July 2022; revised 12 September 2022; accepted 19 September 2022; published 27 October 2022)

One of the most prominent techniques to enhance the performance of practical quantum key distribution (QKD) systems with laser sources is the decoy-state method. Current decoy-state QKD setups operate at gigahertz repetition rates, a regime where memory effects in the modulators and electronics that control them create correlations between the intensities of the emitted pulses. This translates into information leakage about the selected intensities, which cripples a crucial premise of the decoy-state method, thus invalidating the use of standard security analyzes. To overcome this problem, a security proof that exploits the Cauchy-Schwarz constraint has been introduced recently. Its main drawback is, however, that the achievable key rate is significantly lower than that of the ideal scenario without intensity correlations. Here, we improve this security proof technique by combining it with a fine-grained decoy-state analysis, which can deliver a tight estimation of the relevant parameters that determine the secret key rate. This results in a notable performance enhancement, being now the attainable distance double that of previous analyzes for certain parameter regimes. Also, we show that when the probability density function of the intensity fluctuations, conditioned on the current and previous intensity choices, is known, our approach provides a key rate very similar to the ideal scenario, which highlights the importance of an accurate experimental characterization of the correlations.

DOI: 10.1103/PhysRevApplied.18.044069

I. INTRODUCTION

Quantum key distribution (QKD) offers a way to distribute a secret key over the distance between two communicating parties, Alice and Bob [1–3]. When used in conjunction with the one-time-pad encryption scheme [4], QKD allows for information-theoretically secure communications, regardless of the future evolution of classical or quantum computers. This is so because its security is based on the laws of quantum mechanics and does not rely on computational assumptions. In recent years, QKD has progressed very rapidly both in theory and in practice, turning into a flourishing commercial technology that is being deployed in metropolitan and intercity fiber-based networks worldwide [5–8], including also satellite links [9–13] and chip-based technology [14–17].

One of the most successful QKD protocols for long-distance transmission is undoubtedly the decoy-state QKD scheme [18–20]. It uses phase-randomized weak coherent pulses (PRWCPs) emitted by laser sources to provide a secret key rate that scales linearly with the channel transmission [21]. Since its theoretical proposal, numerous experimental implementations have been reported in recent years [22–30], being the actual distance record over fiber of 421 km [31]. Decoy-state QKD has also been demonstrated over satellite links [9,11,12], and various companies currently implement it in their commercial products. Importantly, the use of decoy states is also an essential ingredient for other QKD schemes that use laser sources, like, e.g., measurement-device-independent (MDI) QKD [32] or twin-field (TF) QKD [33], the latter presently holding a distance record over fiber of 833 km [34].

However, despite these achievements, there are still certain challenges that need to be overcome for QKD to become a widely used technology. One of these challenges is to increase the secret key rate delivered by current experimental setups, which is severely affected by the limited transmissivity of single photons in optical fibers, as well as by the dead time of the detectors at the receiver. Possible approaches for this include the use of multiplexing techniques—like, e.g., wavelength division

*xsixto@com.uvigo.es
†vzapatero@com.uvigo.es

multiplexing—that simultaneously transmit several QKD channels over the same fiber [35,36], the adoption of high-dimensional QKD, which can encode many bits of information on a single photon [37], and the increase of the pulse repetition rate of the sources [38]. Indeed, current decoy-state QKD experimental setups operate at gigahertz repetition rates [26,29–31], and the trend is to increase their clock frequency even further. However, in such a high-speed regime, memory effects in the modulators and electronics that control them create correlations between the generated optical pulses [38–41]. That is, the state of a quantum signal emitted by the source at a certain time instant depends not only on the state preparation settings selected by Alice in that time instant, but also on those selected by her in previous time instants. Importantly, if this effect is not properly taken into account in the security proof of QKD, it might open a security loophole in the form of information leakage [42]. This is so because the settings chosen to encode each quantum signal are also partially leaked through the quantum states of subsequent signals.

So far, most security proofs of QKDs have neglected the effect of pulse correlations and assume independent and identically distributed emitted pulses. Therefore, they cannot be used to guarantee the security of high-speed QKD implementations. Only a few recent theoretical works partially address this problem. Precisely, the authors of Refs. [43,44] studied the case of setting-choice-independent pulse correlations, in which the emitted pulses can be arbitrarily correlated between them, but these correlations do not depend on the state preparation setting choices. This scenario may occur, for example, when the temperature of Alice's laser drifts slowly over time due to thermal effects, or when her modulators' power supply fluctuates in time. Moreover, various results that address the problem of setting-choice-dependent pulse correlations have also been reported. In particular, the authors in Ref. [42] introduced a security proof that can handle arbitrary correlations that originate from the phase modulator that encodes the bit and basis information of each generated signal. Likewise, a restricted class of nearest-neighbor pulse correlations that arise from the intensity modulator used to prepare decoy states has been studied in Ref. [41], where a postprocessing technique to treat these correlations is also provided. Also, the authors of Ref. [45] introduced a general methodology to treat arbitrary intensity correlations in a decoy-state QKD setup. For this, they exploit a fundamental constraint that is a direct consequence of the Cauchy-Schwarz (CS) inequality in Hilbert spaces [42,46]. The case of correlations between the global phases of the coherent states emitted by a laser when it is operated under gain-switching conditions has been studied in Ref. [47].

On the experimental side, a few recent works have quantified the strength of pulse correlations (affecting the phase-randomization process, and/or the bit, basis, and intensity encoding of the signals) for various particular QKD setups that operate at the gigahertz regime [38–41], and showed that such correlations are in general not negligible. All these works, however, limit their study to nearest-neighbor pulse correlations. More experimental efforts are needed to accurately characterize the pulse correlations (of arbitrary length) that are created by a QKD source as a function of its experimental configuration and repetition rate.

A main limitation of the security proof technique presented in Ref. [45] is that the delivered secret key rate is significantly lower than that of the ideal scenario without correlations. Only when the intensity correlations are very tiny, the resulting performance can approximate the ideal scenario. In this paper we improve the general methodology introduced in Ref. [45], based on the CS constraint, by combining it with a fine-grained decoy-state analysis. In doing so, we achieve a much tighter estimation procedure to determine the relevant parameters that enter the secret key rate formula. This results in a notable enhancement of the achievable secret key rate in the presence of intensity correlations. Indeed, for certain parameter regimes, the maximum attainable distance can be double that of Ref. [45]. In addition, we show that when the probability density function of the intensity fluctuations, conditioned on the current and previous intensity setting choices, is known, our analysis can provide a secret key rate that is very close to that of the ideal scenario. This highlights the importance of properly characterizing intensity correlations in QKD experimental setups. Most importantly, our results can be readily applied to guarantee the security of high-speed decoy-state QKD realizations with current technology, without much penalization on their secret key rate.

The paper is organized as follows. In Sec. II we present the problem of intensity correlations, and explain why the standard decoy-state analysis cannot be directly applied to this scenario. Here, we also emphasize our main contributions in relation to previous results. Next, in Sec. III we provide the main assumptions that we consider in the security analysis. Then, in Sec. IV we introduce a fine-grained decoy-state parameter estimation method that can be used in the presence of intensity correlations to tightly estimate the relevant parameters that determine the secret key rate. This estimation procedure is then applied to two different scenarios in the following two sections. Precisely, in Sec. V we consider the general case where Alice and Bob only know the intervals where the intensity fluctuations lie. The results for the case where they know the probability density function of the intensity fluctuations are presented in Sec. VI, followed by the conclusions in Sec. VII. To improve the readability of the paper, certain derivations are omitted in the main text and are included in a series of appendices.

II. RELATION WITH PREVIOUS WORK

As already mentioned, intensity correlations refer to the fact that the intensity of an optical pulse generated in a certain round of a QKD protocol depends not only on the intensity setting selected for that round, but also on the intensity settings selected for previous rounds. This effect has been experimentally quantified in Refs. [38,40,41]. It is illustrated in Fig. 1 with a simple example. In general, an eavesdropper (Eve) could exploit these correlations to learn information about the intensity settings selected in previous rounds by measuring the intensity of the pulses emitted in subsequent rounds. This could allow her to make the photon-number detection statistics (i.e., the yields and error rates associated to n-photon pulses) dependent on the intensity setting selected, in so breaking the elementary security premise of the standard decoy-state method [18–20]. This situation is similar to that of a Trojan-horse attack [48–50], in which Eve can learn partial information about the intensities selected to generate the different pulses.

To overcome this problem, there are two main complementary approaches. Precisely, one could implement hardware countermeasures to try to reduce (or even eliminate) the correlations, and one could also include their effect in the security proof of QKDs. An example of the first type of approach could be to use various intensity modulators, each of them acting on different nonconsecutive signals, such that their modulation rate effectively decreases to a regime where no correlations are created. An example of the second approach has been provided in Ref. [41], where the authors studied a restricted type of nearest-neighbor intensity correlation (i.e., this refers to the fact that the actual intensity of each pulse only depends on the intensity settings selected for that time instant and for the previous time instant). In particular, Ref. [41] analyzes the case where only certain intensity settings have a significant effect on the actual intensity of a subsequent pulse, and introduces a postprocessing technique to guarantee security in this scenario. In addition, an experimental characterization of the probability density function of the correlations is provided, which seems to indicate that it essentially follows a Gaussian-shaped form, though this knowledge is not exploited by the postprocessing technique introduced.

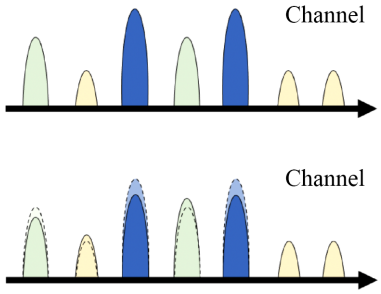

FIG. 1. Illustration of the effect of intensity correlations. The upper subfigure shows a train of optical pulses sent by Alice to the channel with three different intensity values selected at random, which are indicated with the different colours and amplitudes of the pulses. In the absence of intensity correlations, the intensity of each signal is determined only by the intensity setting selected in the corresponding time instant. In the lower subfigure we show a specific example of nearest-neighbor intensity correlations. Solid lines indicate the pulses actually emitted, while dashed lines indicate the selected intensity settings. Precisely, this example assumes that, for illustration purposes, when the intensity setting of the previous pulse is lower (higher) than that of the actual pulse, then the actual intensity generated is a bit lower (higher) than that indicated by the setting selected.

Recently, in Ref. [45], the authors presented an asymptotic security proof that can deal with intensity correlations of arbitrary range (i.e., not necessarily nearest-neighbor pulse correlations) in the decoy-state parameter estimation procedure. Their method is rather general and can be applied when all previous intensity settings can influence the actual intensity of subsequent pulses. The main idea in Ref. [45] is to pose a restriction on the maximum bias that Eve can induce between the n-photon yields and error rates associated to different intensity settings, by using the CS constraint [42,46]. Notably, only two parameters, the correlation range ξ and the maximum deviation $\delta_{\max}$ between the physical intensity and the selected intensity setting, are needed. However, despite the fact that this work is quite simple and experimentally friendly, it treats the deviation of each pulse independently of the previous sequence of selected intensities, but instead it takes the maximum possible deviation for the worst-case scenario, thus providing loose bounds. Indeed, the resulting bounds on the secret key rate are significantly lower than those obtained in the absence of correlations. Therefore, the question arises of whether this damaging effect on the key rate is a fundamental feature of the correlations, or rather an artifact of a loose parameter estimation procedure.

In this paper we preserve the essence of the approach in Ref. [45] to deal with arbitrary intensity correlations—i.e., we exploit the CS constraint to quantify the maximum bias that Eve may induce between the photon-number detection statistics associated to different intensity settings—but sharpen the decoy-state method with a finer-grained analysis of the yields and errors that keeps explicit track of the record of settings. This, in turn, allows us to incorporate finer-tuned CS constraints to the parameter estimation procedure. Putting it all together, our approach enables a noticeable enhancement of the secret key rate when compared with the results in Ref. [45].

In addition, we show that, when the probability density function of the intensity fluctuations is known, our fine-grained decoy-state analysis is rather tight, as it can produce a secret key rate that is comparable to that obtainable in the absence of intensity correlations. This is explicitly

illustrated by considering a Gaussian-shaped probability density function for the correlations, following the preliminary results in Ref. [41] (see also Ref. [51]). In this scenario, the principal improvement mainly comes from the fact that the knowledge of the probability density function now permits us to calculate certain quantities—that are necessary to determine the secret key rate—precisely, avoiding the need to use looser bounds that exploit monotonicity arguments.

III. ASSUMPTIONS

For concreteness, below we shall consider a typical polarization encoding decoy-state BB84 protocol with three intensity settings. Nevertheless, our results apply to other encoding schemes, and can be straightforwardly adapted to other decoy-state-based QKD protocols with a different number of intensity settings.

In the first place, let us fix the notation that is used throughout the paper. In each round k of the protocol, with $k = 1, \ldots, N$, Alice selects an intensity setting $a_k \in A = \{\mu, \nu, \omega\}$ with probability p_{a_k}, a basis $x_k \in B = \{X, Z\}$ with probability q_{x_k}, and a uniform raw key bit $r_k \in \mathbb{Z}_2 = \{0, 1\}$. Without loss of generality, we impose that the intensity settings satisfy $\mu > \nu > \omega \geq 0$. Then, she encodes the BB84 state defined by x_k and r_k in a PRWCP with intensity setting a_k, and sends it to Bob through the quantum channel. Importantly, the actual mean photon number of the pulse might not match the setting a_k due to the presence of intensity correlations. To finish with, we assume perfect phase randomization, perfect polarization encoding, and that there are no side channels beyond intensity correlations for simplicity.

On the other hand, Bob selects a basis $y_k \in B$ with probability q_{y_k} and performs a measurement described by a positive operator-valued measure (POVM) $\{\hat{M}_{B_k}^{y_k,s_k}\}_{s_k \in \{0,1,f\}}$ on the incident pulse. Here, B_k denotes Bob's kth incoming pulse, s_k stands for Bob's classical outcome, and f stands for "no click." As usual, the basis-independent detection efficiency condition is assumed, *i.e.,* $\hat{M}_{B_k}^{Z,f} = \hat{M}_{B_k}^{X,f}$, and thus, we shall simply denote these two operators by $\hat{M}_{B_k}^{f}$. Also, we disregard any potential memory effect in the detectors [52]. These assumptions could be removed by the use of MDI-QKD [32] or TF-QKD [33].

Let $\vec{a}_k = a_k, a_{k-1}, \ldots, a_1$ symbolize the record of intensity settings up to round k, where $a_j \in A$ for every j, and let α_k stand for the actual intensity emitted in round k. We consider that α_k is a continuous random variable whose probability density function is fixed by the record of settings $\vec{a}_k$. From now on, we denote such correlation function as $g_{\vec{a}_k}(\alpha_k)$. Three additional elementary assumptions of our work are listed below.

Assumption 1: The presence of correlations does not compromise the Poissonian character of the photon-number statistics of the source conditioned on the value of the actual intensity, α_k. Mathematically, this amounts to saying that, for any given round k, and for all $n_k \in \mathbb{N}$,

$$p\,(n_k|\alpha_k) = \frac{e^{-\alpha_k}\alpha_k^{n_k}}{n_k!}. \tag{1}$$

Notably, this assumption is supported by recent high-speed QKD experiments [38,41]. Still, we remark that our analysis could be easily adapted to consider any other photon-number statistics conditioned on the value of α_k.

Assumption 2: The intensity correlations have a finite range ξ, meaning that the value of the physical intensity of round k, α_k, is not affected by those previous settings a_j with $k - j > \xi$.

Assumption 3: The correlation function $g_{\vec{a}_k}(\alpha_k)$ is only nonzero for $\alpha_k \in \left[a_k^-, a_k^+\right]$ with $a_k^{\pm} = a_k\left(1 \pm \delta_{\vec{a}_k}^{\pm}\right)$, where $\delta_{\vec{a}_k}^{\pm}$ are the relative deviations. Note that, in virtue of Assumption 2, $\delta_{\vec{a}_k}^{+}$ and $\delta_{\vec{a}_k}^{-}$ only depend on a_k and the previous ξ intensity settings.

From these three assumptions, it follows that the photon-number statistics for a given round k and a given record of settings $\vec{a}_k$ are

$$p_{n_k}|_{\vec{a}_k} = \int_{a_k^-}^{a_k^+} g_{\vec{a}_k}(\alpha_k)\frac{e^{-\alpha_k}\alpha_k^{n_k}}{n_k!}d\alpha_k \quad \text{for all } n_k \in \mathbb{N}. \tag{2}$$

Note that Assumption 2 is not explicitly imposed here.

IV. QUANTIFYING THE EFFECT OF INTENSITY CORRELATIONS ON THE DECOY-STATE PARAMETER ESTIMATION PROCEDURE

With the three assumptions stated above and to account for the influence of intensity correlations in the decoy-state analysis, we use the fundamental CS constraint [42,46]. This result poses a natural constraint between the measurement statistics of two nonorthogonal states. Hence, in particular, one can use it to restrict the possible bias that Eve may induce between the yields (error probabilities) associated to different records of settings. The reader is directed to Appendix A for a definition of this statement. The limits we derive with it are shown below.

We define both the yield and the error probability, for any given round k, photon number $n \in \mathbb{N}$, and record of settings $v_0, \ldots, v_\xi \in A$, as

$$\begin{aligned} Y_{n,v_0,\ldots,v_\xi}^{(k)} &= p(s_k \neq f\,|n_k = n, a_k = v_0, \ldots, \\ &\quad a_{k-\xi} = v_\xi, x_k = Z, y_k = Z), \\ H_{n,v_0,\ldots,v_\xi,r}^{(k)} &= p(s_k \neq f\,, s_k \neq r_k|n_k = n, a_k = v_0, \cdots, \\ &\quad a_{k-\xi} = v_\xi, x_k = X, y_k = X, r_k = r). \end{aligned} \tag{3}$$

In virtue of the CS constraint, for any two distinct intensity settings v_0 and w_0 that could be selected in round k, and for any record of previous settings $v_1,\ldots,v_\xi$, in Appendix A it is shown that the associated yields and error probabilities satisfy

$$G_-\left(Y^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\le Y^{(k)}_{n,w_0\cdots v_\xi}\le G_+\left(Y^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) \tag{4}$$

and

$$G_-\left(H^{(k)}_{n,v_0\cdots v_\xi,r},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\le H^{(k)}_{n,w_0\cdots v_\xi,r}\le G_+\left(H^{(k)}_{n,v_0\cdots v_\xi,r},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right), \tag{5}$$

where

$$G_-(y,z)=\begin{cases}g_-(y,z) & \text{if } y>1-z,\\ 0 & \text{otherwise,}\end{cases}\qquad G_+(y,z)=\begin{cases}g_+(y,z) & \text{if } y<z,\\ 1 & \text{otherwise,}\end{cases} \tag{6}$$

with the function $g_\pm(y,z)=y+(1-z)(1-2y)\pm 2\sqrt{z}(1-z)y(1-y)$. That is, Eqs. (4) and (5), state, respectively, how much $Y^{(k)}_{n,w_0\cdots v_\xi}$ and $H^{(k)}_{n,w_0\cdots v_\xi,r}$ can deviate from $Y^{(k)}_{n,v_0\cdots v_\xi}$ and $H^{(k)}_{n,v_0\cdots v_\xi,r}$. Crucially, the parameters $\tau^{\xi}_{v_0w_0\cdots v_\xi,n}$ are a lower bound on the squared overlap of the two quantum states with which the two yields are calculated. Explicit expressions for the parameters $\tau^{\xi}_{v_0w_0\cdots v_\xi,n}$ are derived in Appendix B 2 for the two different scenarios that we consider in Secs. V and VI.

To enable the use of linear programming for the decoy-state parameter estimation procedure, a linear version of the constraints given by Eq. (4) is needed. As shown in Appendix A, the linearized versions of the CS constraints for the yields and error probabilities can be expressed as

$$\begin{aligned}&G_-\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)+G'_-\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\left(Y^{(k)}_{n,v_0\cdots v_\xi}-\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}\right)\le Y^{(k)}_{n,w_0\cdots v_\xi}\\ &\le G_+\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)+G'_+\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\left(Y^{(k)}_{n,v_0\cdots v_\xi}-\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}\right)\end{aligned} \tag{7}$$

and

$$\begin{aligned}&G_-\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)+G'_-\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\left(H^{(k)}_{n,v_0\cdots v_\xi}-\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}\right)\le H^{(k)}_{n,w_0\cdots v_\xi}\\ &\le G_+\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)+G'_+\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi},\tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\left(H^{(k)}_{n,v_0\cdots v_\xi}-\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}\right),\end{aligned} \tag{8}$$

where both $\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}$ and $\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}$ are the reference parameters of the linear approximations, introduced in Appendix C. Finally, the functions $G'_\pm$ are defined as

$$G'_-(y,z)=\begin{cases}g'_-(y,z) & \text{if } y>1-z,\\ 0 & \text{otherwise,}\end{cases}\qquad G'_+(y,z)=\begin{cases}g'_+(y,z) & \text{if } y<z,\\ 0 & \text{otherwise,}\end{cases} \tag{9}$$

with $g'_\pm(y,z)=-1+2z\pm(1-2y)\sqrt{z(1-z)/y(1-y)}$.

V. MODEL-INDEPENDENT CORRELATIONS

A. Characterization

In this section we now consider a general scenario in which the correlation function $g_{\vec{a}_k}(\alpha_k)$ given by Eq. (2) is unknown. This implies that one cannot compute the photon-number statistics of the emitted pulses explicitly, and, thus, must impose bounds on them by invoking monotonicity arguments. We consider two cases.

In the first one, the maximum relative deviations $\delta^{+}_{(a_k\ldots a_{k-\xi})}$ and $\delta^{-}_{(a_k\ldots a_{k-\xi})}$ depend on the intensity setting choices corresponding to all the previous ξ rounds and the

present round, and define an interval that is in general not symmetric with respect to the value of the selected setting.

$$\sqrt{\tau^{\xi}_{v_0,w_0,\ldots,v_\xi,n}} = \sum_{a_{k+1}^{\min\{k+\xi,N\}}} \prod_{i=k+1}^{\min\{k+\xi,N\}} p_{a_i} \left[e^{(1/2)(-a_i^{(w_0)+}-a_i^{(v_0)+})} + e^{(1/2)(-a_i^{(w_0)-}-a_i^{(v_0)-})} \left(e^{\sqrt{a_i^{(w_0)-} a_i^{(v_0)-}}} - 1 \right) \right], \tag{10}$$

where the terms $a_i^{(v_0)\pm}$ satisfy $a_i^{(v_0)\pm} = a_i(1 \pm \delta^{\pm}_{(a_i\ldots a_{k+1},a_k=v_0,a_{k-1}=v_1\ldots a_{i-\xi}=v_{\xi+k-i})})$ and analogously for $a_i^{(w_0)\pm}$. Note that, with this notation, settings a_1 to a_k are fixed to a certain value, while settings a_{k+1} to a_i are not. Also, note that the bound given by Eq. (10) does not depend on the photon number n, i.e., it holds for all n.

Secondly, we consider as well a simplified situation where only a worst-case deviation $\delta_{\max}$ is known for every possible record of settings. That is, it holds that $\delta_{\max} \geq \delta^{\pm}_{(a_i\cdots a_{k+1},a_k=w_0,v_0,a_{k-1}=v_1\cdots a_{i-\xi}=v_{\xi+k-i})}$ for all $k = 1,\ldots,N$ and all $i \in [k+1, \min\{k+\xi, N\}]$. In this case, the bound simply reads

$$\sqrt{\tau^{\xi}_{v_0,w_0,\ldots,v_\xi,n}} = \left[1 - \sum_{a_i \in A} p_{a_i} \left(e^{-a_i^-} - e^{-a_i^+} \right) \right]^{\xi}, \tag{11}$$

where $a_i^{\pm} = a_i(1 \pm \delta_{\max})$. This derivation is also presented in Appendix B 2. Note that Eq. (10) can only be used if one is able to experimentally characterize the maximum relative deviation for every possible combination of settings.

From now on, and in order to keep the discussion simple, we focus on the case of nearest-neighbor intensity correlations. That is, we set $\xi = 1$. For this purpose, it is convenient to do a slight change of notation, by calling $v_0 = a$; $w_0 = b$ and $v_1 = c$ as this makes the following section easier to follow. Note that the analysis below can be easily adapted for the case of $\xi > 1$, and we include simulations for this latter scenario in Sec. V D.

B. Decoy-state method

To introduce the linear programs that perform the parameter estimation, we shall now provide a decoy-state analysis.

Let us start by defining the Z basis gain for a certain pair of intensity settings a and c, and a number of rounds N, as

$$Z_{a,c,N} = \sum_{k=1}^{N} Z^{(k)}_{a,c}, \tag{12}$$

As shown in Appendix B 2, and denoting $a_1^N = a_1 \ldots a_N$, the bound for this case reads

with $Z^{(k)}_{a,c} = \mathbb{I}_{\{a_k=a,a_{k-1}=c,x_k=y_k=Z,s_k\neq f\}}$. That is, $Z^{(k)}_{a,c} = 1$ if in round k, Alice selects an intensity setting a that is preceded by an intensity setting c (in round $k-1$), both Alice and Bob select the Z basis, and a click occurs at Bob's side. Thus,

$$\begin{aligned} \left\langle Z^{(k)}_{a,c} \right\rangle &= p^{(k)}(a,c,Z,Z,\text{click}) \\ &= q_Z^2 p_a p_c \sum_{n=0}^{\infty} p^{(k)}(n,\text{click}|a,c,Z,Z) \\ &= q_Z^2 p_a p_c \sum_{n=0}^{\infty} p^{(k)}(n|a,c) Y^{(k)}_{n,a,c}. \end{aligned} \tag{13}$$

Straightforward monotonicity arguments lead to the following bounds on the photon-number statistics $p^{(k)}(n|a,c)$:

$$\begin{aligned} p^{(k)}(0|a,c) &\in \left[e^{-a_c^+}, e^{-a_c^-} \right], \\ p^{(k)}(n|a,c) &\in \left[\frac{e^{-a_c^-}(a_c^-)^n}{n!}, \frac{e^{-a_c^+}(a_c^+)^n}{n!} \right] (n \geq 1). \end{aligned} \tag{14}$$

Here $a_c^{\pm} = a(1 \pm \delta^{\pm}_{(a_k=a,a_{k-1}=c)})$. Note that, despite the fact that this notation is similar to that used in Eq. (10), the parameters $a_c^{\pm}$ are actually not equal to $a_i^{(\gamma)\pm}$ with $\gamma \in A$. This is so because here, only the settings a_k and a_{k-1} matter, and they are respectively fixed to a and c.

Now, using these intervals in Eq. (13), one obtains

$$\begin{aligned} \frac{\left\langle Z^{(k)}_{a,c} \right\rangle}{q_Z^2 p_a p_c} &\geq e^{-a_c^+} Y^{(k)}_{0,a,c} + \sum_{n=1}^{\infty} \frac{e^{-a_c^-}(a_c^-)^n}{n!} Y^{(k)}_{n,a,c}, \\ \frac{\left\langle Z^{(k)}_{a,c} \right\rangle}{q_Z^2 p_a p_c} &\leq e^{-a_c^-} Y^{(k)}_{0,a,c} + \sum_{n=1}^{\infty} \frac{e^{-a_c^+}(a_c^+)^n}{n!} Y^{(k)}_{n,a,c}, \end{aligned} \tag{15}$$

for all $a, c \in A$ and $k = 1,\ldots,N$. Selecting a threshold photon number for the numerics, n_{cut}, and using the fact that

$$\sum_{n=n_{\text{cut}}+1}^{\infty} \frac{Y^{(k)}_{n,a,c} e^{-a_c^+} a_c^{+n}}{n!} \leq 1 - \sum_{n=0}^{n_{\text{cut}}} \frac{e^{-a_c^+}(a_c^+)^n}{n!}, \tag{16}$$

we have

$$\begin{aligned}\frac{\langle Z^{(k)}_{a,c}\rangle}{q_Z^2 p_a p_c} &\geq e^{-a_c^+} Y^{(k)}_{0,a,c} + \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^-}(a_c^-)^n}{n!} Y^{(k)}_{n,a,c},\\ \frac{\langle Z^{(k)}_{a,c}\rangle}{q_Z^2 p_a p_c} &\leq 1 - e^{-a_c^+} + e^{-a_c^-} Y^{(k)}_{0,a,c}\\ &\quad - \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^+}(a_c^+)^n}{n!}\left(1 - Y^{(k)}_{n,a,c}\right).\end{aligned} \tag{17}$$

Note how replacing Z by X everywhere, one obtains the corresponding analysis for the X basis gains in a certain round k.

We now have to impose similar constraints to the error counts. For that matter, we define the number of X basis error counts with settings a in round k and c in round $k-1$ as

$$E_{a,c,N} = \sum_{k=1}^{N} E^{(k)}_{a,c}, \tag{18}$$

with $E^{(k)}_{a,c} = X^{(k)}_{a,c}\mathbb{I}_{\{r_k \neq s_k\}}$. Then, we have

$$\begin{aligned}\langle E^{(k)}_{a,c}\rangle &= p^{(k)}(a,c,X,X,\text{err})\\ &= q_X^2 p_a p_c \sum_{n=0}^{\infty} p^{(k)}(n,\text{err}\,|a,c,X,\text{X})\\ &= q_X^2 p_a p_c \sum_{n=0}^{\infty} p^{(k)}(n|a,c) H^{(k)}_{n,a,c},\end{aligned} \tag{19}$$

where we have defined

$$\begin{aligned}H^{(k)}_{n,a,c} &= p^{(k)}(\text{err}\mid n,a,c,X,X)\\ &= \frac{H^{(k)}_{n,a,c,0} + H^{(k)}_{n,a,c,1}}{2}.\end{aligned} \tag{20}$$

With the same steps as before, it follows that

$$\begin{aligned}\frac{\langle E^{(k)}_{a,c}\rangle}{q_X^2 p_a p_c} &\geq e^{-a_c^+} H^{(k)}_{0,a,c} + \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^-}(a_c^-)^n}{n!} H^{(k)}_{n,a,c},\\ \frac{\langle E^{(k)}_{a,c}\rangle}{q_X^2 p_a p_c} &\leq 1 - e^{-a_c^+} + e^{-a_c^-} H^{(k)}_{0,a,c}\\ &\quad - \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^+}(a_c^+)^n}{n!}\left(1 - H^{(k)}_{n,a,c}\right).\end{aligned} \tag{21}$$

Now, summing over k and dividing by N in both Eqs. (17) and (21), one obtains bounds for the average parameters

$$\begin{aligned}y_{n,a,c,N} &= \sum_{k=1}^{N} \frac{Y^{(k)}_{n,a,c}}{N},\\ h_{n,a,c,N} &= \sum_{k=1}^{N} \frac{H^{(k)}_{n,a,c}}{N},\end{aligned} \tag{22}$$

from the round-dependent bounds. Thus, defining

$$\begin{aligned}\bar{Z}_{a,c,N} &= \frac{Z_{a,c,N}}{N},\\ \bar{E}_{a,c,N} &= \frac{E_{a,c,N}}{N},\end{aligned} \tag{23}$$

we obtain that the final bounds are

$$\begin{aligned}\frac{\langle \bar{Z}_{a,c,N}\rangle}{q_Z^2 p_a p_c} &\geq e^{-a_c^+} y_{0,a,c,N} + \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^-}(a_c^-)^n}{n!} y_{n,a,c,N},\\ \frac{\langle \bar{Z}_{a,c,N}\rangle}{q_Z^2 p_a p_c} &\leq 1 - e^{-a_c^+} + e^{-a_c^-} y_{0,a,c,N}\\ &\quad - \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^+}(a_c^+)^n}{n!}\left(1 - y_{n,a,c,N}\right),\\ \frac{\langle \bar{E}_{a,c,N}\rangle}{q_X^2 p_a p_c} &\geq e^{-a_c^+} h_{0,a,c,N} + \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^-}(a_c^-)^n}{n!} h_{n,a,c,N},\\ \frac{\langle \bar{E}_{a,c,N}\rangle}{q_X^2 p_a p_c} &\leq 1 - e^{-a_c^+} + e^{-a_c^-} h_{0,a,c,N}\\ &\quad - \sum_{n=1}^{n_{\rm cut}} \frac{e^{-a_c^+}(a_c^+)^n}{n!}\left(1 - h_{n,a,c,N}\right).\end{aligned} \tag{24}$$

C. Linear programs for parameter estimation

In this section we present the linear programs that allow us to estimate the relevant single-photon parameters by putting together the decoy-state constraints, already introduced above, and the linearized CS constraints with the notation presented in Eq. (A6).

To begin with, note that the quantities that go into the secret key rate are the average number of single-photon counts associated to the case where Alice selects the signal intensity setting, which we shall denote by $\bar{Z}_{1,\mu,N}$, and the average number of phase errors associated to these single-photon counts (which in the case of the BB84 protocol, without state preparation flaws and assuming the asymptotic limit, match the average number of single-photon error counts in the X basis). Moreover, since below we shall consider the asymptotic secret key regime where $p_\mu \approx 1$, for simplicity, we can restrict our estimation to the

number of single-photon error counts in the X basis when Alice selects the intensity setting, which we shall denote by $\bar{E}_{1,\mu,N}$.

Let us consider $\bar{Z}_{1,\mu,N}$ first. Formally,

$$\bar{Z}_{1,\mu,N} = \sum_{k=1}^{N} \frac{Z_{1,\mu}^{(k)}}{N}, \tag{25}$$

where, for each k, $Z_{1,\mu}^{(k)} = Z_{\mu}^{(k)} \mathbb{I}_{\{n_k=1\}}$ is the probability that Alice selects the signal intensity setting μ, both Alice and Bob select the Z basis, and a click occurs at Bob's side. In turn, it is clear that $Z_{1,\mu}^{(k)}$ decomposes as

$$Z_{1,\mu}^{(k)} = \sum_{h\in A} Z_{1,\mu,h}^{(k)}, \tag{26}$$

where of course $Z_{1,\mu,h}^{(k)} = Z_{1,\mu}^{(k)} \mathbb{I}_{\{a_{k-1}=h\}}$. Then it trivially follows that

$$\begin{aligned}
\langle \bar{Z}_{1,\mu,N} \rangle &= \frac{1}{N} \sum_{k=1}^{N} \langle Z_{1,\mu}^{(k)} \rangle = \frac{1}{N} \sum_{k=1}^{N} \sum_{h\in A} \langle Z_{1,\mu,h}^{(k)} \rangle \\
&= \frac{1}{N} \sum_{k=1}^{N} \sum_{h\in A} q_Z^2 p_\mu p_h p^{(k)}(1|\mu,h) Y_{1,\mu,h}^{(k)} \\
&\geq \frac{1}{N} \sum_{k=1}^{N} \sum_{h\in A} q_Z^2 p_\mu p_h \mu_h^- e^{-\mu_h^-} Y_{1,\mu,h}^{(k)} \\
&= \sum_{h\in A} q_Z^2 p_\mu p_h \mu_h^- e^{-\mu_h^-} y_{1,\mu,h,N}.
\end{aligned} \tag{27}$$

Note that the above equation lower bounds the expected value of the quantity of interest $\bar{Z}_{1,\mu,N}$ using the yields $y_{1,a,b,N}$ introduced in the previous section. Thus, the linear program of interest is

$$\begin{aligned}
\min \quad & q_Z^2 p_\mu \sum_{h\in A} p_h \mu_h^- e^{-\mu_h^-} y_{1,\mu,h,N} \\
\text{such that} \quad & \frac{\langle \bar{Z}_{a,c,N} \rangle}{q_Z^2 p_a p_c} \geq e^{-a_c^+} y_{0,a,c,N} + \sum_{n=1}^{n_{\text{cut}}} \frac{e^{-a_c^-} (a_c^-)^n}{n!} y_{n,a,c,N} \quad (a,c \in A), \\
& \frac{\langle \bar{Z}_{a,c,N} \rangle}{q_Z^2 p_a p_c} \leq 1 - e^{-a_c^+} + e^{-a_c^-} y_{0,a,c,N} - \sum_{n=1}^{n_{\text{cut}}} \frac{e^{-a_c^+} (a_c^+)^n}{n!} \left(1 - y_{n,a,c,N}\right) \quad (a,c \in A), \\
& c_{abc,n}^+ + m_{abc,n}^+ y_{n,a,c,N} \geq y_{n,b,c,N} \; (a,b,c \in A, b \neq a, n = 0,\ldots,n_{\text{cut}}), \\
& c_{abc,n}^- + m_{abc,n}^- y_{n,a,c,N} \leq y_{n,b,c,N} \; (a,b,c \in A, b \neq a, n = 0,\ldots,n_{\text{cut}}), \\
& 0 \leq y_{n,a,b,N} \leq 1 \; (a,b \in A, n = 0,\ldots,n_{\text{cut}}),
\end{aligned} \tag{28}$$

where the parameters $c_{abc,n}^{\pm}$ and $m_{abc,n}^{\pm}$ represent, respectively, the intercepts and slopes from the linear version of the CS constraints given in Appendix A. We recall that we use such linearization for convenience, to be able to use linear programming to estimate the relevant parameters in the decoy-state analysis. The precise form of these parameters is provided by Eq. (A6) in Appendix A; we do not explicitly include it in Eq. (28) to keep the notation simple. We shall denote the lower bound on $\langle \bar{Z}_{1,\mu,N} \rangle$ obtained with the linear program above by $\bar{Z}_{1,\mu,N}^L$.

Naturally, substituting Z for X everywhere yields the equivalent program for the average number of signal-setting single-photon counts in the X basis.

Proceeding analogously for the average number of signal-setting single-photon error counts in the X basis we have

$$\bar{E}_{1,\mu,N} = \sum_{k=1}^{N} \frac{E_{1,\mu}^{(k)}}{N}, \tag{29}$$

where, for each round k, $E_{1,\mu}^{(k)} = E_{\mu}^{(k)} \mathbb{I}_{\{n_k=1\}}$. As before, $E_{1,\mu}^{(k)}$ decomposes as

$$E_{1,\mu}^{(k)} = \sum_{h\in A} E_{1,\mu,h}^{(k)}, \tag{30}$$

where $E^{(k)}_{1,\mu,h} = E^{(k)}_{1,\mu}\mathbb{I}_{\{a_{k-1}=h\}}$. Therefore, we obtain

$$\begin{aligned}\langle \bar{E}_{1,\mu,N}\rangle &= \frac{1}{N}\sum_{k=1}^{N}\langle E^{(k)}_{1,\mu}\rangle = \frac{1}{N}\sum_{k=1}^{N}\sum_{h\in A}\langle E^{(k)}_{1,\mu,h}\rangle = \frac{1}{N}\sum_{k=1}^{N}\sum_{h\in A} q_X^2 p_\mu p_h p^{(k)}(1|\mu,h) H^{(k)}_{1,\mu,h} \\ &\leq \frac{1}{N}\sum_{k=1}^{N}\sum_{h\in A} q_X^2 p_\mu p_h \mu_h^+ e^{-\mu_h^+} H^{(k)}_{1,\mu,h} = \sum_{h\in A} q_X^2 p_\mu p_h \mu_h^+ e^{-\mu_h^+} h_{1,\mu,h,N}. \end{aligned} \tag{31}$$

Then an upper bound $\bar{E}^U_{1,\mu,N}$ on the quantity $\langle \bar{E}_{1,\mu,N}\rangle$ is achieved by using the linear program

$$\begin{aligned} \max \quad & q_X^2 p_\mu \sum_{h\in A} p_h \mu_h^+ e^{-\mu_h^+} h_{1,\mu,h,N} \\ \text{such that} \quad & \frac{\langle \bar{E}_{a,c,N}\rangle}{q_X^2 p_a p_c} \geq e^{-a_c^+} h_{0,a,c,N} + \sum_{n=1}^{n_{\text{cut}}} \frac{e^{-a_c^-}(a_c^-)^n}{n!} h_{n,a,c,N} \quad (a,c\in A), \\ & \frac{\langle \bar{E}_{a,c,N}\rangle}{q_X^2 p_a p_c} \leq 1 - e^{-a_c^+} + e^{-a_c^-} h_{0,a,c,N} - \sum_{n=1}^{n_{\text{cut}}} \frac{e^{-a_c^+}(a_c^+)^n}{n!}\left(1 - h_{n,a,c,N}\right) \quad (a,c\in A), \\ & t^+_{abc,n} + s^+_{abc,n} h_{n,a,c,N} \geq h_{n,b,c,N} \; (a,b,c\in A, b\neq a, n = 0,\ldots,n_{\text{cut}}), \\ & t^-_{abc,n} + s^-_{abc,n} h_{n,a,c,N} \leq h_{n,b,c,N} \; (a,b,c\in A, b\neq a, n = 0,\ldots,n_{\text{cut}}), \\ & 0 \leq h_{n,a,b,N} \leq 1 \; (a,b\in A, n = 0,\ldots,n_{\text{cut}}), \end{aligned} \tag{32}$$

with the parameters $t^{\pm}_{abc,n}$ and $s^{\pm}_{abc,n}$ representing again, respectively, the intercepts and slopes that arise from the linear CS constraints. We refer the reader to Appendix A for further details, and to Eq. (A6) for the explicit definition of these parameters.

D. Simulations

As shown in Ref. [45], the asymptotic secret key rate is well approximated by

$$K_\infty = \bar{Z}^L_{1,\mu,N}\left[1 - h\left(\frac{\bar{E}^U_{1,\mu,N}}{\bar{X}^L_{1,\mu,N}}\right)\right] - f_{\text{EC}}\bar{Z}_{\mu,N} h\left(E_{\text{tol}}\right) \tag{33}$$

for large enough N, as long as the variances of the experimental averages vanish asymptotically (see Ref. [45] for a precise meaning of this statement). Here, $h(x)$ denotes the binary entropy function, f_{EC} is the error-correction efficiency, the parameter $\bar{Z}_{\mu,N}$ is the gain in the Z basis defined as

$$\bar{Z}_{\mu,N} = \sum_{h\in A}\bar{Z}_{\mu,h,N}, \tag{34}$$

and E_{tol} is the overall error rate observed in the Z basis.

Note that here one cannot simply use the asymptotic secret key rate formula against collective attacks due to the presence of intensity correlations. To be precise, we have the fact that the asymptotic equivalence between the collective and the coherent settings is typically established on the basis of the so-called postselection technique [53] built on the De Finetti theorem [54,55]. However, the round-exchangeability property required to apply the postselection technique is generally invalidated by pulse correlations.

Even though simulations with real data from Ref. [41] are presented in Sec. VI, in order to compare our fine-grained analysis with the previous results in Ref. [45], we fix the experimental inputs of the linear programs $\bar{Z}_{a,c,N}/q_Z^2 p_a p_c$, $\bar{X}_{a,c,N}/q_X^2 p_a p_c$, and $\bar{E}_{a,c,N}/q_X^2 p_a p_c$ to their expected values according to a typical channel model, which is provided in Appendix C.

For that matter, let η_{det} denote the common detection efficiency of Bob's detectors, and let $\eta_{\text{ch}} = 10^{-\alpha_{\text{att}}L/10}$ be the transmittance of the quantum channel, where α_{att} (dB/km) is its attenuation coefficient and L (km) is the distance. Also, let p_d denote the dark count probability of each of Bob's detectors and let δ_A stand for the polarization misalignment occurring in the channel. This model yields the results (see Appendix C)

$$\frac{\langle \bar{Z}_{a,c,N}\rangle}{q_Z^2 p_a p_c} = \frac{\langle \bar{X}_{a,c,N}\rangle}{q_X^2 p_a p_c} = 1 - (1-p_d)^2 e^{-\eta a}, \tag{35}$$

and

$$\frac{\langle \bar{E}_{a,c,N}\rangle}{q_X^2 p_a p_c} = \frac{\langle \bar{E}_{a,c,N(Z)}\rangle}{q_Z^2 p_a p_c} = \frac{p_d^2}{2} + p_d\,(1-p_d)\left(1+h_{\eta,a,c,\delta_A}\right) + (1-p_d)^2 \times \left(\frac{1}{2} + h_{\eta,a,c,\delta_A} - \frac{1}{2}e^{-\eta a}\right), \quad (36)$$

for $a, c \in A$ and where $\eta = \eta_{\rm det}\eta_{\rm ch}$. Here, we define the parameter h_{η,a,c,δ_A} as

$$h_{\eta,a,c,\delta_A} = \frac{e^{-\eta a \cos^2\delta_A} - e^{-\eta a \sin^2\delta_A}}{2}. \quad (37)$$

We also introduce the parameter $\bar{E}_{a,c,N(Z)}$, which is equivalent to $\bar{E}_{a,c,N}$ but accounts for the Z basis error clicks. The tolerated bit error rate of the sifted key is set to $E_{\rm tol} = \langle \bar{E}_{\mu,N(Z)}\rangle / \langle \bar{Z}_{\mu,N}\rangle$. Also, the reference parameters for the linearized CS constraints are fixed by the channel model as well, as indicated in Appendix C.

In particular, in the simulations we take $\eta_{\rm det} = 0.65$ and $p_d = 7.2 \times 10^{-8}$ [56]. The attenuation coefficient of the channel is set to $\alpha_{\rm att} = 0.2$ dB/km, the error-correction efficiency to $f_{\rm EC} = 1.16$, and a channel misalignment of $\delta_A = 0.08$ is used. As for the intensities, the weakest intensity setting is set to $\omega = 10^{-4}$ due to the finite extinction ratio of intensity modulators. For simplicity, due to the large number of constraints included in the linear programs, instead of optimizing both μ and ν to maximize the asymptotic secret key rate K_∞ as a function of the distance L, we select a pair (μ, ν) that roughly maximizes the achievable distance and use that pair for all values of L. Notably, since we are considering the asymptotic regime, K_∞ does not depend on the probabilities of the decoy settings, p_ν and p_ω, nor on the probability of selecting the X basis, q_X, in such a way that setting $p_\mu \approx 1$ and $q_Z \approx 1$ maximizes K_∞.

In Fig. 2 we illustrate the effect of the intensity correlations in a rate-distance representation for various values of the maximum relative deviation $\delta_{\rm max} \in \{10^{-2}, 10^{-3}, 10^{-4}\}$, and for $\xi = 1$ (i.e., for the case of nearest-neighbor pulse correlations) and $\xi = 2$ (corresponding to pulse correlations of range two). The simulations show that the secret key rate is very sensitive to the deviation $\delta_{\rm max}$. What is more, with realistic experimental data [41], we find that the maximum distance attainable is less than 50 km. Moreover, it is important to remark that, as expected, the fine-grained analysis presented here outperforms the coarse-grained analysis introduced in Ref. [45] regardless of the value of $\delta_{\rm max}$. Indeed, Fig. 2 shows that when $\delta_{\rm max} = 10^{-2}$, now the attainable distance is approximately double that in Ref. [45]. Also, note that this figure assumes a single worst-case deviation parameter $\delta_{\rm max}$ [following Eq. (11)]. The case corresponding to Eq. (10) is illustrated in the next section, when we compare this model with the one where Alice and Bob know the probability density function of the correlations.

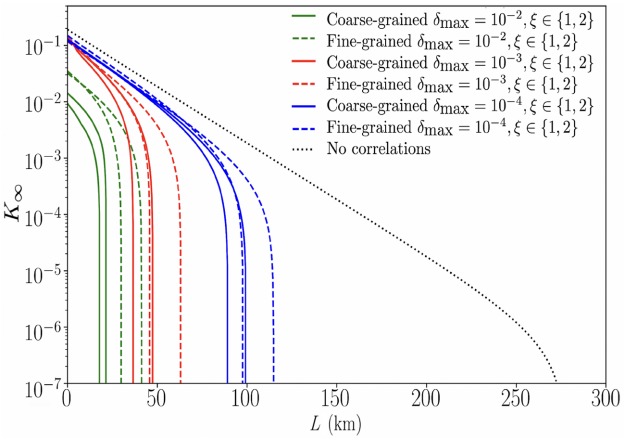

FIG. 2. Secret key rate given by Eq. (33) using the analysis provided by Eq. (11). We consider different values for the maximum deviation $\delta_{\rm max} \in \{10^{-2}, 10^{-3}, 10^{-4}\}$ between the actual physical intensity α_k and the selected intensity setting a_k, and two values of the parameter ξ. Precisely, we consider $\xi = 1$ (i.e., corresponding to the case of nearest-neighbor pulse correlations) and $\xi = 2$ (corresponding to pulse correlations of range two). The coarse-grained analysis follows the techniques presented in Ref. [45].

VI. TRUNCATED NORMAL MODEL

A. Characterization

In this section we show that a significant improvement on the secret key rate presented in Fig. 2 can be obtained when Alice and Bob know the probability density function given by Eq. (2). By assuming this, the analysis that we present now is similar to that of the previous section but simpler, as we do not have to bound the photon-number statistics, but we can solve them numerically.

The main motivation to consider this scenario is that recent decoy-state QKD experiments [41] performed in the high-speed regime seem to indicate that the correlation function is not arbitrary but Gaussian-shaped (see also Ref. [51]). Triggered by this observation, for concreteness and illustration purposes, we shall assume here a truncated Gaussian (TG) distribution for the correlations, which follows from renormalizing a Gaussian distribution to a fixed finite interval $[\lambda, \Lambda]$. We note, however, that the analysis presented in this section could be straightforwardly adapted to any other probability density function of the correlations. To be precise, given both the mean and the variance—say, γ and σ^2, respectively—of the parental Gaussian distribution together with the truncation interval

$[\lambda, \Lambda]$, the TG model reads

$$g_{\vec{a}_k}(\gamma,\sigma,\lambda,\Lambda;\alpha_k) = \begin{cases} 0 & \text{if } \alpha_k \le \lambda, \\ \frac{\phi\left(\gamma,\sigma^2;\alpha_k\right)}{\Phi\left(\gamma,\sigma^2;\Lambda\right)-\Phi\left(\gamma,\sigma^2;\lambda\right)} & \text{if } \lambda < \alpha_k < \Lambda, \\ 0 & \text{if } \Lambda \le \alpha_k, \end{cases} \tag{38}$$

where

$$\begin{aligned} \phi\left(\gamma,\sigma^2;x\right) &= \frac{1}{\sigma\sqrt{2\pi}} e^{-((x-\gamma)^2/2\sigma^2)}, \\ \Phi\left(\gamma,\sigma^2;x\right) &= \int_{-\infty}^{x} \frac{1}{\sigma\sqrt{2\pi}} e^{-((t-\gamma)^2/2\sigma^2)} dt. \end{aligned} \tag{39}$$

From now on, we shall denote by $\tilde{\gamma}$ and $\tilde{\sigma}^2$ the mean and variance of the TG distribution. We also call $\gamma_{\vec{a}_k}$, the average intensity given the sequence $\vec{a}_k$, and $\sigma_{\vec{a}_k}$, the standard deviation given the sequence $\vec{a}_k$ of the parental normal distribution, although below the subscript indicating the record of settings will be omitted unless it can lead to confusion. More details on the truncation model are given in Appendix D.

Importantly, under suitable truncation conditions, this model reproduces the observed Gaussian-shaped correlations in a finite support $[\lambda, \Lambda]$ (in contrast to the unbounded support of nontruncated Gaussian distributions). We note as well that the relevant parameters can be estimated experimentally by monitoring the intensities in long sequences of rounds.

From Eq. (38), the photon-number statistics now read

$$p_{n_k}|_{\vec{a}_k} = \int_{\lambda}^{\Lambda} \frac{\phi\left(\gamma_{\vec{a}_k},\sigma^2_{\vec{a}_k};\alpha_k\right) e^{-\alpha_k}\alpha_k^{n_k}}{\left[\Phi\left(\gamma_{\vec{a}_k},\sigma^2_{\vec{a}_k};\Lambda\right)-\Phi\left(\gamma_{\vec{a}_k},\sigma^2_{\vec{a}_k};\lambda\right)\right] n_k!} d\alpha_k. \tag{40}$$

In general, as has been experimentally observed in Ref. [38], $\gamma_{\vec{a}_k} \neq a_k$ for $a_k \in \{\mu,\nu,\omega\}$, i.e., a certain displacement in the mean intensity typically occurs. We account for this shift in the signal and the decoy intensity settings, while we neglect it for the vacuum intensity setting following the observations of Ref. [41]. Notably as well, $\sigma^2_{\vec{a}_k}$ generally depends on the previous intensity settings, and so far no assumption about the range of the correlations has been made. In this sense, despite the fact that the analysis is valid for an arbitrary range, for simplicity here, we only consider nearest-neighbor correlations for illustration purposes, i.e., below we assume that $\xi = 1$.

Following the calculations in Appendix B 2, and combining the analysis above with the TG model here presented, the bound on the squared overlap in the nearest-neighbor setting simply reads

$$\begin{aligned} &\sum_{a_{k+1}\in A} p_{a_{k+1}} \sum_{n_i=0}^{\infty} \sqrt{p_{n_i|a_{k+1},a} p_{n_i|a_{k+1},b}} \\ &\quad \ge \sum_{a_{k+1}\in A} p_{a_{k+1}} \sum_{n_i=0}^{n_{\text{cut}}} \sqrt{p_{n_i|a_{k+1},a} p_{n_i|a_{k+1},b}} \equiv \sqrt{\tau^{\xi=1}_{a,b,c,n}}, \end{aligned} \tag{41}$$

where we have introduced a threshold photon number n_{cut} for the numerics.

B. Linear programs for parameter estimation

The techniques for calculating the relevant parameters to evaluate the secret key rate formula using the decoy-state constraints in this model are common with those deployed in the model-independent case evaluated in the previous section. The only difference is that certain steps such as the one that leads to Eq. (14) are no longer necessary. Here we solve the photon-number statistics given by Eq. (40) numerically and there is no need to invoke monotonicity arguments to bound them. The resulting linear program for the relevant single-photon yield (error click probability in the X basis) reads

$$\begin{aligned} \min \quad & q_Z^2 p_\mu \sum_{h\in A} p_h p^{(k)}(1|\mu,h) y_{1,\mu,h,N} \\ \text{such that} \quad & \frac{\langle Z^{(k)}_{a,c}\rangle}{q_Z^2 p_a p_c} \ge \sum_{n=0}^{n_{\text{cut}}} p_{n|a,c} y_{n,a,c,N}, \\ & \frac{\langle Z^{(k)}_{a,c}\rangle}{q_Z^2 p_a p_c} \le 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|a,c} + \sum_{n=0}^{n_{\text{cut}}} p_{n|a,c} y_{n,a,c,N}, \\ & c^+_{abc,n} + m^+_{abc,n} y_{n,a,c,N} \ge y_{n,b,c,N} \ (a,b,c\in A, b\neq a, n=0,\ldots,n_{\text{cut}}), \\ & c^-_{abc,n} + m^-_{abc,n} y_{n,a,c,N} \le y_{n,b,c,N} \ (a,b,c\in A, b\neq a, n=0,\ldots,n_{\text{cut}}), \\ & 0 \le y_{n,a,b,N} \le 1 \ (a,b\in A, n=0,\ldots,n_{\text{cut}}), \end{aligned} \tag{42}$$

and

$$\begin{aligned}
\max \quad & q_X^2 p_\mu \sum_{h\in A} p_h p^{(k)}(1|\mu,h) h_{1,\mu,h,N} \\
\text{such that} \quad & \frac{\langle E_{a,c}^{(k)}\rangle}{q_X^2 p_a p_c} \geq \sum_{n=0}^{n_{\text{cut}}} p_{n|a,c} h_{n,a,c,N}, \\
& \frac{\langle E_{a,c}^{(k)}\rangle}{q_X^2 p_a p_c} \leq 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|a,c} + \sum_{n=0}^{n_{\text{cut}}} p_{n|a,c} h_{n,a,c,N}, \\
& t^+_{abc,n} + s^+_{abc,n} h_{n,a,c,N} \geq h_{n,b,c,N} \; (a,b,c \in A, b \neq a, n = 0,\ldots,n_{\text{cut}}), \\
& t^-_{abc,n} + s^-_{abc,n} h_{n,a,c,N} \leq h_{n,b,c,N} \; (a,b,c \in A, b \neq a, n = 0,\ldots,n_{\text{cut}}), \\
& 0 \leq h_{n,a,b,N} \leq 1 \; (a,b \in A, n = 0,\ldots,n_{\text{cut}}).
\end{aligned} \tag{43}$$

C. Simulations

The TG model requires us to experimentally determine all of its parameters, namely, the truncation ranges, the mean intensities, and the standard deviations of the distribution for every combination of pulses in rounds k and $k-1$ (if one assumes, as already mentioned, nearest-neighbor intensity correlations), which in turn should be experimentally accessible by monitoring the output of the transmitter in long sequences of rounds.

As discussed in Appendix D, regardless of the value of the mean intensity and the standard deviation, which in principle depend on the present and previous settings, for illustration purposes, we determine the truncation range for these simulations as $(\lambda,\Lambda) = (\tilde{\gamma} - t\tilde{\sigma}, \tilde{\gamma} + t\tilde{\sigma})$, where $\tilde{\gamma}$ is the measured mean intensity of the TG distribution and $\tilde{\sigma}$ is the measured standard deviation of the TG distribution. Note that ideally, the truncation range could be measured experimentally. We can now make a direct comparison between this model in which we assume that Alice and Bob know the probability density function of the correlations, and the one that uses a maximum relative deviation defined in Eq. (10).

For this, we use Eq. (33) and the channel model presented in Appendix C to evaluate the performance. Moreover, regarding the mean and the standard deviations as a function of the intensity settings in rounds k and $k-1$, we take the experimental values reported in Ref. [41]. The only exception is the normalized standard deviation $\hat{\sigma} = \tilde{\sigma}/\tilde{\gamma}$ corresponding to vacuum, where Ref. [41] does not report any value and we select, for illustration purposes, 10^{-5} for all possible intensities in the round $k-1$. This is so because the fluctuation of the vacuum setting seems to be essentially negligible. In addition, for simplicity, we do not optimize the intensity settings, but fix them to $\mu = 0.5$, $\nu = 0.2$, and $\omega = 10^{-4}$, which are the values considered in Ref. [41], and we select the parameter $t = 4$. The relevant parameters are summarized in Table I.

To facilitate a fair comparison between this model and that of Eq. (10), we take

$$\delta_{(a_k=i,a_{k-1}=j)} = t\hat{\sigma}_{i,j} = t\frac{\tilde{\sigma}_{i,j}}{\tilde{\gamma}_{i,j}}, \tag{44}$$

as explained in Appendix D, where $i,j \in A$. Here, $\tilde{\gamma}_{i,j}$ ($\tilde{\sigma}_{i,j}$) refers to the average mean intensity (standard deviation) of round k associated to the record $(a_{k-1},a_k) = (j,i)$, while $\hat{\sigma}_{i,j} = \tilde{\sigma}_{i,j}/\tilde{\gamma}_{i,j}$ are the normalized standard deviations of the TG model. In this way, we ensure that the physical intensity is bounded in the same interval in both cases. These parameters are obtained from Table I.

Figure 3 illustrates the improvement in the secret key rate when the correlation function is known and corresponds to a TG distribution according to the model that was just introduced. We find that now the results are comparable to those of the ideal case without intensity correlations, which highlights the importance of characterizing the probability density function of the correlations. When comparing the two models studied in this paper, we

TABLE I. Values for the average intensity $\tilde{\gamma}$ and normalized standard deviations $\hat{\sigma} = \tilde{\sigma}/\tilde{\gamma}$ reported in Ref. [41]. The only exception is the normalized standard deviation $\hat{\sigma}$ corresponding to vacuum, where Ref. [41] does not report any value and we select for illustration purposes 10^{-5}. In our simulations we consider that they characterize a TG distribution.

Pattern (a_{k-1},a_k)	Average intensities ($\tilde{\gamma}$)	Normalized SD ($\hat{\sigma}$)
μ,μ	0.500	0.032
ν,μ	0.510	0.032
ω,μ	0.503	0.034
μ,ν	0.210	0.070
ν,ν	0.172	0.090
ω,ν	0.165	0.091
$\mu/\nu/\omega,\omega$	10^{-4}	10^{-5}

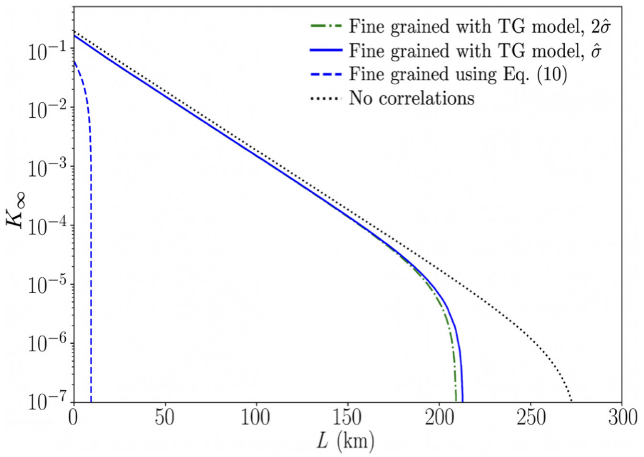

FIG. 3. Secret key rate within the TG model assuming the parameters from Table I (solid blue line), and when the normalized standard deviations are twice those illustrated in that table (dash-dotted green line). For comparison, this figure also includes the model-independent case (dashed blue line) where the maximum relative deviation is taken as $\delta_{(a_k=i,a_{k-1}=j)} = t\hat{\sigma}_{i,j}$ for every $i,j \in A$, where $\hat{\sigma}_{i,j}$ stands for the normalized standard deviations in the TG model, and we select $t = 4$. When we consider twice the normalized standard deviations provided in Table I, this latter model provides no key.

conclude that knowing the distribution $g_{\vec{a}_k}(\alpha_k)$ allows for a significant improvement of the resulting performance. This is due to the fact that in this scenario one can evaluate the photon-number statistics exactly, which makes the parameter estimation much tighter, improving both the decoy-state constraints and the CS constraints. Finally, Fig. 3 also includes a representation where the standard deviations are twice the values given in Table I, to evaluate the effect that this parameter has on the secret key rate. The fine-grained analysis described in Eq. (10) does not provide the key in this latter scenario. Likewise, if we use Eq. (11) in the model-independent case, no key is obtained in neither case.

VII. CONCLUSIONS

When combining high-speed clock rate QKD transmitters with the decoy-state technique, the presence of intensity correlations in the generated pulses invalidate the central security assumption of this method, namely, that the yields and error rates associated to n-photon pulses are independent of the intensity settings. This problem can be solved by imposing constraints on the intensity setting dependence of these parameters, which is done here by invoking the so-called Cauchy-Schwarz constraints. Essentially, these constraints arise from the indistinguishability of nonorthogonal quantum states and can be derived on the basis of a minor characterization of the correlations.

In this work, by using a standard decoy-state BB84 protocol with three possible intensity settings, we evaluate the effect that such correlations have in the secret key rate. We do so by introducing a *fine-grained analysis* able to handle arbitrary long-range correlations. This approach leads to significantly tighter constraints for the parameter estimation and notably improves the secret key rate achieved by previous works. Also, we show that the characterization of the probability density function of the correlations permits us to notably improve the resulting performance, which now becomes comparable to that of the ideal scenario without intensity correlations. Putting it all together, the present work provides a solid step forward towards full implementation security in QKD with high performance.

ACKNOWLEDGMENTS

This work is supported by Cisco Systems Inc., the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2020-118178RB-C21, and MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with their own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication.

APPENDIX A: CAUCHY-SCHWARZ CONSTRAINT

The CS constraint can be stated as follows.

Theorem 1: *Let* $|u\rangle$ *and* $|v\rangle$ *be pure states of a certain quantum system. Then, for all positive operators* $\hat{O} \leq I$,

$$G_-\left(\langle u|\hat{O}|u\rangle, |\langle v|u\rangle|^2\right) \leq \langle v|\hat{O}|v\rangle \leq G_+\left(\langle u|\hat{O}|u\rangle, |\langle v|u\rangle|^2\right), \tag{A1}$$

where the functions $G_\pm$ *are given in Eq. (6).*

Proof : See supplementary materials of Ref. [42]. ■

This constraint can be used to impose a restriction on the maximum bias that Eve can induce between the n-photon yields and error probabilities associated to different intensity settings. Here we derive a linear version of Eq. (4), enabling the use of linear programming for the decoy-state parameter estimation procedure. Following Ref. [45], we have that in virtue of the convexity or concavity of the functions that define the constraints, their first-order expansions around any given reference value provide valid linear bounds as well. Thus, if we focus on the yields, the linearization provides the bounds

$$\begin{aligned} G_-(Y^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}) &\geq G_-(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}) + G'_-(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau_{v_0w_0\cdots v_\xi,n})(Y^{(k)}_{n,v_0\cdots v_\xi} - \tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}), \\ G_+(Y^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}) &\leq G_+(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}) + G'_+(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau_{v_0w_0\cdots v_\xi,n})(Y^{(k)}_{n,v_0\cdots v_\xi} - \tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}), \end{aligned} \tag{A2}$$

for every $Y^{(k)}_{n,v_0\cdots v_\xi} \in [0,1]$ independently of which reference $\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi} \in [0,1]$ is selected.

Note that the derivative functions $G'_\pm$ are well defined for all $Y^{(k)}_{n,v_0\cdots v_\xi} \in [0,1]$; their expression is given by Eq. (9). Thus, given a reference yield $\tilde{Y}^{(k)}_{n,w_0\cdots v_\xi}$, the linearized bounds read

$$\begin{aligned} G_-\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) + G'_-\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\left(Y^{(k)}_{n,v_0\cdots v_\xi} - \tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}\right) &\leq Y^{(k)}_{n,w_0\cdots v_\xi}, \\ G_+\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) + G'_+\left(\tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{aw_0\cdots v_\xi,n}\right)\left(Y^{(k)}_{n,v_0\cdots v_\xi} - \tilde{Y}^{(k)}_{n,v_0\cdots v_\xi}\right) &\geq Y^{(k)}_{n,w_0\cdots v_\xi}. \end{aligned} \tag{A3}$$

Similarly for the error probabilities, and assuming that we select reference parameters independent of Alice's bit value r_k (for a more detailed analysis, see Ref. [45]), we have

$$\begin{aligned} G_-\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) + G'_-\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\left(H^{(k)}_{n,v_0\cdots v_\xi} - \tilde{H}^{(k)}_{n,v_0\cdots v_\xi}\right) &\leq H^{(k)}_{n,w_0\cdots v_\xi}, \\ G_+\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) + G'_+\left(\tilde{H}^{(k)}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{aw_0\cdots v_\xi,n}\right)\left(H^{(k)}_{n,v_0\cdots v_\xi} - \tilde{H}^{(k)}_{n,v_0\cdots v_\xi}\right) &\geq H^{(k)}_{n,w_0\cdots v_\xi}. \end{aligned} \tag{A4}$$

To finish with, note that one can restrict the reference parameters to be round independent, in such a way that, summing over k and dividing by N in Eqs. (7) and (8), we obtain the average parameters

$$\begin{aligned} y_{n,w_0\cdots v_\xi,N} &= \sum_{k=1}^{N} \frac{Y^{(k)}_{n,w_0\cdots v_\xi}}{N}, \\ h_{n,w_0\cdots v_\xi,N} &= \sum_{k=1}^{N} \frac{H^{(k)}_{n,w_0\cdots v_\xi}}{N}, \end{aligned} \tag{A5}$$

and similarly for the other terms that appear below.

We define the intercepts and slopes as

$$\begin{aligned} c^{\pm}_{v_0w_0\cdots v_\xi,n} &= G_\pm\left(\tilde{y}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) - G'_\pm\left(\tilde{y}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\tilde{y}_{n,v_0\cdots v_\xi}, \\ m^{\pm}_{v_0w_0\cdots v_\xi,n} &= G'_\pm\left(\tilde{y}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right), \\ t^{\pm}_{v_0w_0\cdots v_\xi,n} &= G_\pm\left(\tilde{h}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right) - G'_\pm\left(\tilde{h}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right)\tilde{h}_{n,v_0\cdots v_\xi}, \\ s^{\pm}_{v_0w_0\cdots v_\xi,n} &= G'_\pm\left(\tilde{h}_{n,v_0\cdots v_\xi}, \tau^{\xi}_{v_0w_0\cdots v_\xi,n}\right). \end{aligned} \tag{A6}$$

The linear CS constraints for the round independent case are

$$\begin{aligned} c^{+}_{v_0w_0\cdots v_\xi,n} + m^{+}_{v_0w_0\cdots v_\xi,n} y_{n,v_0\cdots v_\xi,N} &\geq y_{n,w_0\cdots v_\xi,N}\left(v_0, w_0, \ldots, v_\xi \in A, w_0 \neq v_0\right), \\ c^{-}_{v_0w_0\cdots v_\xi,n} + m^{-}_{v_0w_0\cdots v_\xi,n} y_{n,v_0\cdots v_\xi,N} &\leq y_{n,w_0\cdots v_\xi,N}\left(v_0, w_0, \ldots, v_\xi \in A, w_0 \neq v_0\right), \\ 0 \leq y_{n,v_0\cdots v_\xi,N} &\leq 1\left(v_0, \cdots, v_\xi \in A\right), \end{aligned} \tag{A7}$$

and

$$\begin{aligned} t^{+}_{v_0w_0\cdots v_\xi,n} + s^{+}_{v_0w_0\cdots v_\xi,n} h_{n,v_0\cdots v_\xi,N} &\geq h_{n,w_0\cdots v_\xi,N}\left(v_0, w_0, \ldots, v_\xi \in A, w_0 \neq v_0\right), \\ t^{-}_{v_0w_0\cdots v_\xi,n} + s^{-}_{v_0w_0\cdots v_\xi,n} h_{n,v_0\cdots v_\xi,N} &\leq h_{n,w_0\cdots v_\xi,N}\left(v_0, w_0, \ldots, v_\xi \in A, w_0 \neq v_0\right), \\ 0 \leq h_{n,v_0\cdots v_\xi,N} &\leq 1\left(v_0, \cdots ., v_\xi \in A\right). \end{aligned} \tag{A8}$$

Note that the characterization of the quantum channel is essential, as the tightness of these linear bounds is subject to the adequacy of the selected reference parameters, and so it relies on it. The selected reference values are presented in Appendix C.

APPENDIX B: DERIVATION OF $\tau^{\xi}_{v_0,w_0,\ldots v_\xi,n}$

In an entanglement-based view of the protocol, the global input state describing all the protocol rounds reads

$$|\Psi\rangle = \left[\sum_{a_1^N}\sum_{x_1^N}\sum_{r_1^N}\left(\prod_{i=1}^{N}\sqrt{\frac{p_{a_i}q_{x_i}}{2}}\right)\left(\bigotimes_{i=1}^{N}|a_i\rangle_{A_i}|x_i\rangle_{\tilde{A}_i}|r_i\rangle_{A_i'}\left|\psi_{\tilde{a}_i}^{x_i,r_i}\right\rangle_{B_iC_i}\right)\right]\otimes|0\rangle_E, \tag{B1}$$

where $a_1^N = a_1\ldots a_N$ and equivalently for x_1^N and r_1^N. Also, for every round i, $\{|a_i\rangle_{A_i}\,|a_i\in A\}$, $\{|x_i\rangle_{\tilde{A}_i}\,|x_i\in B\}$, and $\{|r_i\rangle_{A_i'}\,|r_i\in\mathbb{Z}_2\}$ are orthonormal bases of Alice's ith registers A_i, $\tilde{A}_i$, and A_i'. The state $|0\rangle_E$ stands for the initial state of Eve's ancillary system. We also define

$$\left|\psi_{\tilde{a}_i}^{x_i,r_i}\right\rangle_{B_iC_i} = \sum_{n_i=0}^{\infty}\sqrt{p_{n_i|\tilde{a}_i}}\left|t_{n_i}\right\rangle_{C_i}\left|n_i^{x_i,r_i}\right\rangle_{B_i}, \tag{B2}$$

where C_i denotes an inaccessible purifying system with orthonormal basis $\{\left|t_{n_i}\right\rangle_{C_i}\,|n_i\in\mathbb{N}\}$ (C_i stores the photon-number information of the ith signal that Alice sends to Bob), B_i denotes the system delivered to Bob, $|n_i^{x_i,r_i}\rangle_{B_i}$ stands for a Fock state with n_i photons encoding the BB84 polarization state defined by (x_i,r_i), and the photon-number statistics $p_{n_i}\big|_{\tilde{a}_i}$ are defined in Eq. (2).

Let us denote by $\hat{U}_{BE}$ Eve's coherent interaction with systems $B_1,\ldots,B_N$ and E so that $\hat{U}_{BE}|\Psi\rangle$ represents the global state prior to Bob's measurements. We also refer to Bob's click POVM element in round k as

$$\hat{M}_{B_k}^{\text{click}} = \mathbb{I}_{B_k} - \hat{M}_{B_k}^{f}. \tag{B3}$$

The joint probability $p^{(k)}(\text{click}, n, v_0,\ldots,v_\xi,Z)$ is computed as

$$\begin{aligned} p^{(k)}(\text{click}, n, v_0,\ldots,v_\xi,Z) &= \text{Tr}\left\{\hat{P}_{|v_0,\ldots,v_\xi,Z,t_n\rangle_{A_k\cdots A_{k-\xi}\tilde{A}_kC_k}}\hat{M}_{B_k}^{\text{click}}\,\hat{U}_{BE}|\Psi\rangle\langle\Psi|\hat{U}_{BE}^{\dagger}\right\}\\ &= \text{Tr}\left\{\hat{U}_{BE}^{\dagger}\hat{M}_{B_k}^{\text{click}}\,\hat{U}_{BE}\hat{P}_{|v_0,\ldots,v_\xi,Z,t_n\rangle_{A_k\cdots A_{k-\xi}\tilde{A}_kC_k}}|\Psi\rangle\langle\Psi|\hat{P}_{|v_0,\ldots,v_\xi,Z,t_n\rangle_{A_k\cdots A_{k-\xi}\tilde{A}_kC_k}}\right\}\\ &= \text{Tr}_{\underline{A_k}\underline{\tilde{A}_k}\underline{C_k},A_1'^NB_1^NE}\left\{\hat{U}_{BE}^{\dagger}\hat{M}_{B_k}^{\text{click}}\,\hat{U}_{BE}\left|\widetilde{\Psi}_{v_0,\ldots,v_\xi Z,n}^{(k,\ldots,k-\xi)}\right\rangle\left\langle\widetilde{\Psi}_{v_0,\ldots,v_\xi,Z,n}^{(k,\ldots,k-\xi)}\right|\right\}, \end{aligned} \tag{B4}$$

where

$$\hat{P}_{|v_0,\ldots,v_\xi,Z,t_n\rangle_{A_k\tilde{A}_k\cdots A_{k-\xi}C_k}} = |v_\xi\rangle\langle v_\xi|_{A_{k-\xi}}\otimes\cdots\otimes|v_0\rangle\langle v_0|_{A_k}\otimes|Z\rangle\langle Z|_{\tilde{A}_k}\otimes|t_n\rangle\langle t_n|_{C_k}, \tag{B5}$$

$\underline{A_k} = \{A_j\,|j\neq k,..,k-\xi\}$, $\underline{\tilde{A}_k} = \{\tilde{A}_j\,|j\neq k\}$, and $\underline{C_k} = \left\{C_j\,|j\neq k\right\}$. Note that, for round k, we project on the intensity setting, the basis and the photon number, and for all previous rounds, we only project on the intensity setting. The unnormalized pure state is defined as

$$\left|\widetilde{\Psi}_{v_0,\ldots,v_\xi,Z,n}^{(k,\ldots,k-\xi)}\right\rangle = \langle v_\xi|_{A_{k-\xi}}\cdots\langle v_0|_{A_k}\langle Z|_{\tilde{A}_k}\langle t_n|_{C_k}|\Psi\rangle. \tag{B6}$$

We now restate Eq. (B4) in terms of the normalized state

$$\left|\Psi_{v_0,\ldots,v_\xi,Z,n}^{(k,\ldots,k-\xi)}\right\rangle = \frac{\left|\widetilde{\Psi}_{v_0,\ldots,v_\xi,Z,n}^{(k,\ldots,k-\xi)}\right\rangle}{\left\|\left|\widetilde{\Psi}_{v_0,\ldots,v_\xi,Z,n}^{(k,\ldots,k-\xi)}\right\rangle\right\|}, \tag{B7}$$

which leads to

$$p^{(k)}(\text{click}, n, v_0, \ldots, v_\xi, Z) = \left\| \left| \widetilde{\Psi}^{(k,\ldots,k-\xi)}_{v_0,\ldots,v_\xi,Z,n} \right\rangle \right\|^2 \mathrm{Tr}\left\{ \hat{U}^\dagger_{BE} \hat{M}^{\text{click}}_{B_k} \hat{U}_{BE} \left| \Psi^{(k,\ldots,k-\xi)}_{v_0,\ldots v_\xi,Z,n} \right\rangle \left\langle \Psi^{(k,\ldots,k-\xi)}_{v_0,\ldots v_\xi,Z,n} \right| \right\}. \tag{B8}$$

We note that $p^{(k)}(n, v_0, \ldots, v_\xi, Z)$ is given by $p^{(k)}(n, v_0, \ldots, v_\xi, Z) = \mathrm{Tr}\{\hat{P}_{|v_0,\ldots,v_\xi,Z,t_n\rangle_{A_k C_k}} \hat{U}_{BE}|\Psi\rangle\langle\Psi|\hat{U}^\dagger_{BE}\} = \left\| \left| \widetilde{\Psi}^{(k,\ldots,k-\xi)}_{v_0,\ldots,v_\xi,Z,n} \right\rangle \right\|^2$. Therefore, in virtue of Bayes rule we obtain

$$p^{(k)}(\text{click}|n, v_0, \ldots, v_\xi, Z) = \left\langle \Psi^{(k,\ldots,k-\xi)}_{v_0,\ldots,v_\xi,Z,n} \right| \hat{O}^{(k)}_{\text{click}} \left| \Psi^{(k,\ldots,k-\xi)}_{v_0,\ldots,v_\xi,Z,n} \right\rangle, \tag{B9}$$

where we have defined

$$\hat{O}^{(k)}_{\text{click}} = \hat{U}^\dagger_{BE} \hat{M}^{\text{click}}_{B_k} \hat{U}_{BE}. \tag{B10}$$

Now, from Eq. (3), we recall that the quantity defined above is actually the n-photon yield of round k associated to the record of settings $v_0, \ldots, v_\xi$. From the CS constraint, it follows that

$$G_-\left(Y^{(k)}_{n,v_0\cdots v_\xi}, \left| \left\langle \Psi^{(k,\ldots,k-\xi)}_{w_0\cdots v_\xi,Z,n} | \Psi^{(k,\ldots,k-\xi)}_{v_0\cdots v_\xi,Z,n} \right\rangle \right|^2 \right) \leq Y^{(k)}_{n,w_0\cdots v_\xi} \leq G_+\left(Y^{(k)}_{n,v_0\cdots v_\xi}, \left| \left\langle \Psi^{(k,\ldots,k-\xi)}_{w_0\cdots v_\xi,Z,n} | \Psi^{(k,\ldots,k-\xi)}_{v_0\cdots v_\xi,Z,n} \right\rangle \right|^2 \right), \tag{B11}$$

for all $n \in \mathbb{N}$, $w_0, v_0, \ldots, v_\xi \in A$ where $v_0 \neq w_0$ and $k = 1, \ldots, N$. Note that the closer the inner product between the states is to one, the tighter the bounds of the inequality are.

Having reached this stage, we recall that the goal is to set a lower bound on the inner product $\langle \Psi^{(k,\ldots,k-\xi)}_{w_0\cdots v_\xi,Z,n} \mid \Psi^{(k,\ldots,k-\xi)}_{v_0\cdots v_\xi,Z,n} \rangle$. From Eqs. (B1) and (B6), direct calculation shows that

$$\begin{aligned}
\left| \widetilde{\Psi}^{(k,\ldots,k-\xi)}_{v_0,v_1\cdots v_\xi,Z,n} \right\rangle = \sqrt{\frac{q_z p_{v_0}\cdots p_{v_\xi}}{2^N}} \Bigg[& \sum_{\underline{a_k}} \sum_{\underline{x_k}} \sum_{r_1^N} \left(\prod_{i\neq k} \sqrt{q_{x_i}} \right) \left(\prod_{i\neq k\cdots k-\xi} \sqrt{p_{a_i}} \right) \bigotimes_{i=1}^{k-\xi-1} |a_i\rangle_{A_i} |x_i\rangle_{\tilde{A}_i} |r_i\rangle_{A'_i} \left| \psi^{x_i,r_i}_{\vec{a}_i} \right\rangle_{B_i C_i} \\
& \otimes |x_{k-\xi}\rangle_{\tilde{A}_{k-\xi}} |r_{k-\xi}\rangle_{A'_{k-\xi}} \left| \psi^{x_{k-\xi},r_{k-\xi}}_{\vec{a}_{k-\xi}(a_{k-\xi}=v_\xi)} \right\rangle_{B_{k-\xi}C_{k-\xi}} |x_{k-\xi+1}\rangle_{\tilde{A}_{k-\xi+1}} |r_{k-\xi+1}\rangle_{A'_{k-\xi+1}} \\
& \otimes \left| \psi^{x_{k-\xi+1},r_{k-\xi+1}}_{\vec{a}_{k-\xi+1}(a_{k-\xi+1}=v_{\xi-1},a_{k-\xi}=v_\xi)} \right\rangle_{B_{k-\xi+1}C_{k-\xi+1}} \cdots |x_{k-1}\rangle_{\tilde{A}_{k-1}} |r_{k-1}\rangle_{A'_{k-1}} \\
& \otimes \left| \psi^{x_{k-1},r_{k-1}}_{\vec{a}_{k-1}(a_{k-1}=v_1\cdots a_{k-\xi}=v_\xi)} \right\rangle_{B_{k-1}C_{k-1}} \sqrt{p_n|_{v_0,v_1,\ldots,v_\xi,\vec{a}_{k-\xi-1}}} |r_k\rangle_{A'_k} |n^{Z,r_k}\rangle_{B_k} \\
& \bigotimes_{i=k+1}^{N} |a_i\rangle_{A_i} |x_i\rangle_{\tilde{A}_i} |r_i\rangle_{A'_i} \left| \psi^{x_i,r_i}_{\vec{a}_i(a_k=v_0,\ldots,a_{k-\xi}=v_\xi)} \right\rangle_{B_i C_i} \Bigg] \otimes |0\rangle_E,
\end{aligned} \tag{B12}$$

where $\underline{x_k} = \{x_j | j \neq k, \}$ and $\underline{a_k} = \{a_j | j \neq k, \ldots, k-\xi\}$. Then, computing the inner product yields

$$\begin{aligned}
\left\langle \widetilde{\Psi}^{(k,\ldots,k-\xi)}_{w_0,v_1,\ldots,v_\xi,Z,n} | \widetilde{\Psi}^{(k,\ldots,k-\xi)}_{v_0,v_1,\ldots,v_\xi,Z,n} \right\rangle = & \frac{q_z \sqrt{p_{v_0}\cdots p_{v_\xi} p_{w_0}\cdots p_{v_\xi}}}{2^N} \sum_{\underline{a_k}} \sum_{\underline{x_k}} \sum_{r_1^N} \left(\prod_{i\neq k} q_{x_i} \right) \left(\prod_{i\neq k,\ldots,k-\xi} p_{a_i} \right) \\
& \times \left\langle \psi^{x_{k-\xi},r_{k-\xi}}_{\vec{a}_{k-\xi}(a_{k-\xi}=v_\xi)} | \psi^{x_{k-\xi},r_{k-\xi}}_{\vec{a}_{k-\xi}(a_{k-\xi}=v_\xi)} \right\rangle_{B,C_{k-\xi}} \left\langle \psi^{x_{k-\xi+1},r_{k-\xi+1}}_{\vec{a}_{k-\xi+1}(a_{k-\xi+1}=v_{\xi-1},a_{k-\xi}=v_\xi)} | \psi^{x_{k-\xi+1},r_{k-\xi+1}}_{\vec{a}_{k-\xi+1}(a_{k-\xi+1}=v_{\xi-1},a_{k-\xi+1}=v_{\xi-1})} \right\rangle_{B,C_{k-\xi+1}} \\
& \cdots \left(\sqrt{p_n|_{v_0,v_1,\ldots,v_\xi} p_n|_{w_0,v_1,\ldots,v_\xi}} \right) \left(\prod_{i=k+1}^{\min\{k+\xi,N\}} \left\langle \psi^{x_i,r_i}_{\vec{a}_i(a_k=w_0,\ldots,a_{k-\xi}=v_\xi)} | \psi^{x_i,r_i}_{\vec{a}_i(a_k=v_0,\ldots,a_{k-\xi}=v_\xi)} \right\rangle_{B_i C_i} \right),
\end{aligned} \tag{B13}$$

where we have omitted the subscript $\vec{a}_{k-\xi-1}$ in the square root term in parentheses because the photon-number statistics are independent of this substring of settings. Since all the factors previous to round k are equal to 1, and the sums over x_k

and r_1^N yield $\sum_{\underline{x_k}}\sum_{r_1^N}\left(\prod_{i\neq k} q_{x_i}\right)=\sum_{r_1^N}\left\{\sum_{\underline{x_k}}\left(\prod_{i\neq k} q_{x_i}\right)\right\}=2^N$, the previous equation reduces to

$$\left\langle \widetilde{\Psi}^{(k,\ldots,k-\xi)}_{w_0,v_1,\ldots,v_\xi,Z,n}|\widetilde{\Psi}^{(k,\ldots,k-\xi)}_{v_0,v_1,\ldots,v_\xi,Z,n}\right\rangle = q_z\sqrt{p_{v_0}p_{w_0}}p_{v_1}\cdots p_{v_\xi}\sum_{a^{k-\xi-1}_{\max\{1,k-2\xi\}}}\left(\prod_{i=\max\{1,k-2\xi\}}^{k-\xi-1}p_{a_i}\right)\sqrt{p_n|_{v_0,\ldots,w_\xi}p_n|_{w_0,\ldots,w_\xi}}$$
$$\times\left[\sum_{a^{\min\{k+\xi,N\}}_{k+1}}\left(\prod_{i=k+1}^{\min\{k+\xi,N\}}p_{a_i}\left\langle\psi^{x_i,r_i}_{\vec{a}_i(a_k=w_0,\ldots,a_{k-\xi}=v_\xi)}|\psi^{x_i,r_i}_{\vec{a}_i(a_k=v_0,\ldots a_{k-\xi}=v_\xi)}\right\rangle_{B_iC_i}\right)\right]. \tag{B14}$$

In terms of the normalized states, we obtain

$$\left\langle \Psi^{(k,\ldots,k-\xi)}_{w_0,\ldots,v_\xi,Z,n}|\Psi^{(k,\ldots,k-\xi)}_{v_0,\ldots,v_\xi,Z,n}\right\rangle = \sum_{a^{\min\{k+\xi,N\}}_{k+1}}\left(\prod_{i=k+1}^{\min\{k+\xi,N\}}p_{a_i}\right)\left\langle\psi^{x_i,r_i}_{\vec{a}_i(a_k=w_0,\ldots,a_{k-\xi}=v_\xi)}|\psi^{x_i,r_i}_{\vec{a}_i(a_k=v_0,\ldots a_{k-\xi}=v_\xi)}\right\rangle_{B_iC_i}. \tag{B15}$$

We can express Eq. (B15) in terms of the photon-number statistics instead, i.e.,

$$\left\langle \Psi^{(k,\ldots,k-\xi)}_{w_0,\ldots,v_\xi,Z,n}|\Psi^{(k,\ldots,k-\xi)}_{v_0,\ldots,v_\xi,Z,n}\right\rangle = \sum_{a^{\min\{k+\xi,N\}}_{k+1}}\left(\prod_{i=k+1}^{\min\{k+\xi,N\}}p_{a_i}\right)\sum_{m=0}^{\infty}\sqrt{p_m|_{a_i\cdots v_0\cdots v_{\xi+k-i}}p_m|_{a_i\cdots w_0\cdots v_{\xi+k-i}}}. \tag{B16}$$

That is, this quantity takes the same value given by Eq. (B16) for all n.

1. Model-independent correlations

Equation (B16) provides a general formula that can be used as the input of the CS constraint regardless of the correlation function. Here we consider the model-independent scenario where the correlation function is assumed to be unknown. This implies that we cannot evaluate the photon-number statistics on which Eq. (B16) depends. Therefore, we bound these statistics by invoking monotonicity arguments.

Only to keep the notation simple, we consider that the mean physical intensity matches the actual intensity setting, even though according to experiments there might to be a certain displacement between these two quantities [41]. We emphasize, however, that such a shift could be straightforwardly included in our analysis. Let us start by introducing the following shorthand notation:

$$a_i^{(\tau)\pm}=a_i\left(1\pm\delta^{\pm}_{(a_i,\ldots,a_{k+1},a_k=\tau,a_{k-1}=v_1,\ldots,a_{i-\xi}=v_{\xi+k-i})}\right) \tag{B17}$$

with $\tau\in\{v_0,w_0\}$.

From the definition of the photon-number statistics and by noting that $e^{-x}x^n$ is strictly decreasing for $n=0$ and increasing for $n\geq 1$ in $x\in(0,1)$, we have

$$\begin{aligned} p_0|_{\vec{a}_i(a_k=v_0)} &\geq e^{-a_i^{(v_0)+}},\\ p_{n\geq 1}|_{\vec{a}_i(a_k=v_0)} &\geq e^{-a_i^{(v_0)-}}\frac{\left(a_i^{(v_0)-}\right)^n}{n!}. \end{aligned} \tag{B18}$$

Therefore, we can bound the square root of Eq. (B16) as (where, for convenience, we now use the variable n to name the index of the sum)

$$\sum_{n=0}^{\infty}\sqrt{p_n|_{a_i\cdots v_0\cdots v_{\xi+k-i}}p_n|_{a_i\cdots w_0\cdots v_{\xi+k-i}}}=\sqrt{p_0|_{a_i\cdots v_0\cdots v_{\xi+k-i}}p_0|_{a_i\cdots w_0\cdots v_{\xi+k-i}}}+\sum_{n=1}^{\infty}\sqrt{p_n|_{a_i\cdots v_0\cdots v_{\xi+k-i}}p_n|_{a_i\cdots w_0\cdots v_{\xi+k-i}}}$$
$$\geq\left[e^{(1/2)(-a_i^{(w_0)+}-a_i^{(v_0)+})}+e^{(1/2)(-a_i^{(w_0)-}-a_i^{(v_0)-})}\left(e^{\sqrt{a_i^{(w_0)-}a_i^{(v_0)-}}}-1\right)\right]. \tag{B19}$$

By combining Eqs. (B16)–(B19), we obtain the bound given by Eq. (10).

A simpler bound given by Eq. (11) arises by considering that the relative deviation parameters are all equal. It can be obtained directly from Eq. (10).

It is also worth mentioning that one could use a more exhaustive approach by considering different records of settings for each of the two yields (or error probabilities) to be compared via the CS constraint. However, our numerical simulations suggest that the improvement achieved by doing so is not really significant, while the analysis is much more cumbersome to implement numerically.

If we focus our attention on nearest-neighbor intensity correlations only, and call $v_0 = a$, $w_0 = b$, and $v_1 = c$, then from Eqs. (10) and (11), respectively, one trivially obtains

$$\left\langle \Psi_{b,c,Z,n} \mid \Psi_{a,c,Z,n} \right\rangle \geq \sum_{a_i \in A} p_{a_i} \left[e^{(1/2)(-a_i^{(b)+} - a_i^{(a)+})} + e^{(1/2)(-a_i^{(b)-} - a_i^{(a)-})} \left(e^{\sqrt{a_i^{(b)-} a_i^{(a)-}}} - 1 \right) \right] \equiv \sqrt{\tau_{a,b,c,n}^{\xi=1}} \tag{B20}$$

and

$$\left\langle \Psi_{b,c,Z,n} \mid \Psi_{a,c,Z,n} \right\rangle \geq \left[1 - \sum_{a_i \in A} p_{a_i} \left(e^{-a_i^-} - e^{-a_i^+} \right) \right] \equiv \sqrt{\tau_{a,b,c,n}^{\xi=1}}. \tag{B21}$$

2. Truncated normal model

Following Eq. (B16) and using the same notation as in the previous section for nearest-neighbor intensity correlations, we have that the bound for the different possible combinations of settings when the correlation function is a TG distribution is given by

$$\left[\sum_{a_{k+1} \in A} p_{a_{k+1}} \sum_{n_{k+1}=0}^{\infty} \sqrt{p_{n_{k+1}|a_{k+1},a} p_{n_{k+1}|a_{k+1},b}} \right]^2 \geq \left[\sum_{a_{k+1} \in A} p_{a_{k+1}} \sum_{n_{k+1}=0}^{n_{\text{cut}}} \sqrt{p_{n_{k+1}|a_{k+1},a} p_{n_{k+1}|a_{k+1},b}} \right]^2 \equiv \tau_{a,b,c,n}^{\xi=1}. \tag{B22}$$

For instance, we have

$$p_{n_{k+1}|a_{k+1},a} = \int_{\lambda}^{\Lambda} \frac{e^{-\alpha_{k+1}} \alpha_{k+1}^{n_{k+1}}}{n_{k+1}!} \frac{\phi\left(\gamma_{a_{k+1},a}, \sigma_{a_{k+1},a}^2; \alpha_{k+1} \right)}{\left[\Phi\left(\gamma_{a_{k+1},a}, \sigma_{a_{k+1},a}^2; \Lambda \right) - \Phi\left(\gamma_{a_{k+1},a}, \sigma_{a_{k+1},a}^2; \lambda \right) \right]} d\alpha_{k+1}, \tag{B23}$$

where $\sigma_{a_{k+1},a}$ and $\gamma_{a_{k+1},a}$, respectively, are the parental standard deviation and the parental mean value of the random variable α_{k+1}, given that $a_k = a$. Similarly, λ and Λ define the truncation intervals of the TG distribution.

APPENDIX C: REFERENCE VALUES FOR THE LINEARIZED CAUCHY-SCHWARZ CONSTRAINTS

We now present the reference values $\tilde{y}_{n,a,c}$ and $\tilde{h}_{n,a,c}$. For the moment, we neglect the effect of the dark counts of Bob's detectors and the random assignments of the double clicks that he performs. This means that the possible genuine detection outcomes for an n-photon pulse emitted by Alice are "no click" (00), "error" (01), "no error" (10), and "double click" (11). Their probabilities are (see Fig. 4 below)

$$\begin{aligned} p_{00} &= (1-\eta)^n, \\ p_{01} &= \left(\eta \sin^2 \delta_A + 1 - \eta \right)^n - (1-\eta)^n, \\ p_{10} &= \left(\eta \cos^2 \delta_A + 1 - \eta \right)^n - (1-\eta)^n, \\ p_{11} &= 1 - p_{00} - p_{01} - p_{10}. \end{aligned} \tag{C1}$$

We now need to incorporate the dark counts and the random assignments of the double clicks, so let us introduce the mutually exclusive events $A = \{\text{no dark counts}\}$, $B = \{\text{dark count in } D1\}$, $C = \{\text{dark count in } D2\}$, and $D = \{\text{dark count in both } D1 \text{ and } D2\}$, where we follow the detector notation of the figure above. The conditional error probabilities read

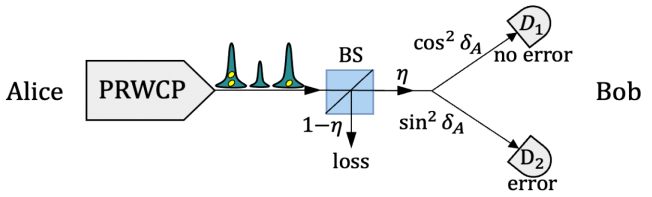

FIG. 4. Representation of the channel model considered for the simulations when Alice uses a PRWCP source. We recall that η stands for the overall system efficiency (i.e., it includes the loss in the channel and the finite detection efficiency of the detectors), and δ_A stands for the polarization misalignment introduced by the channel. We assume that Bob uses an active BB84 receiver with two detectors, D_1 and D_2. In the figure BS stands for beam splitter.

$$\begin{aligned} p_{\text{err}}|_A &= p_{01} + \frac{1}{2}p_{11}, \\ p_{\text{err}}|_B &= \frac{1}{2}\left(p_{01} + p_{11}\right), \\ p_{\text{err}}|_C &= p_{00} + p_{01} + \frac{1}{2}\left(p_{10} + p_{11}\right), \\ p_{\text{err}}|_D &= \frac{1}{2}, \end{aligned} \tag{C2}$$

so that

$$\begin{aligned} \tilde{h}_{n,a,c} = (1-p_d)^2 p_{\text{err}}|_A + p_d(1-p_d)\left(p_{\text{err}}|_B + p_{\text{err}}|_C\right) \\ + p_d^2 p_{\text{err}}|_D \end{aligned} \tag{C3}$$

for all $n \in \mathbb{N}$ and $a, c \in A$. Note that these quantities depend only on round k, so that they are independent of c or the intensity setting of round $k-1$. Regarding the yield, we have

$$\tilde{y}_{n,a,c} = 1 - (1-p_d)^2 p_{00}. \tag{C4}$$

APPENDIX D: THE TRUNCATED NORMAL MODEL

In this appendix we present the link between the mean and variance of the parent normal distribution (γ and σ^2), and the mean and variance of the truncated normal distribution ($\tilde{\gamma}$ and $\tilde{\sigma}^2$). For this purpose, we define

$$\alpha = \frac{\lambda - \gamma}{\sigma} \quad \text{and} \quad \beta = \frac{\Lambda - \gamma}{\sigma}, \tag{D1}$$

so that we can make a mapping between the two [57], having

$$\tilde{\gamma} = \gamma - \sigma \frac{\phi(0,1;\beta) - \phi(0,1;\alpha)}{\Phi(0,1;\beta) - \Phi(0,1;\alpha)},$$

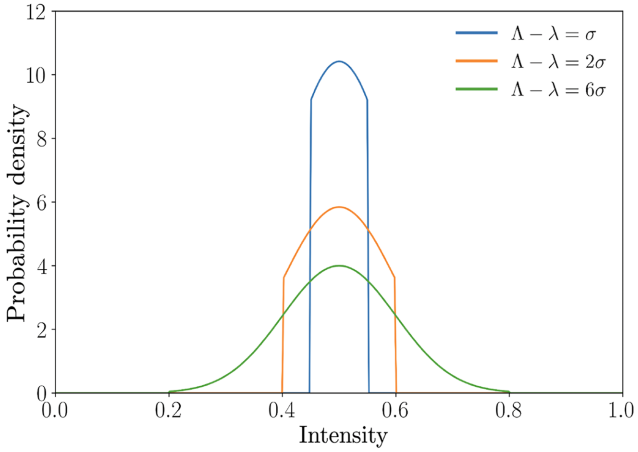

FIG. 5. Representation of a TG distribution with $\gamma = 0.5$ and $\sigma = 0.1$ for three different values of the truncation range. Shorter truncation intervals lead to a larger difference between σ and $\tilde{\sigma}$. Note that, with $\Lambda - \lambda = 6\sigma$, the Gaussian shape of the distribution is preserved after truncation.

$$\begin{aligned} \tilde{\sigma}^2 = \sigma^2\Bigg[1 - \frac{\beta\phi(0,1;\beta) - \alpha\phi(0,1;\alpha)}{\Phi(0,1;\beta) - \Phi(0,1;\alpha)} \\ - \left(\frac{\phi(0,1;\beta) - \phi(0,1;\alpha)}{\Phi(0,1;\beta) - \Phi(0,1;\alpha)}\right)^2\Bigg], \end{aligned} \tag{D2}$$

where $\Phi(0,1;\alpha)$ and $\phi(0,1;\alpha)$ are defined in Eq. (39).

To gain intuition about the form of this distribution and the effect that the truncation range has on $\tilde{\sigma}$, in Fig. 5 we plot it for a couple of different intervals $[\lambda, \Lambda]$ centered in the mean value. Note that, in this way, the mean is not affected by the truncation.

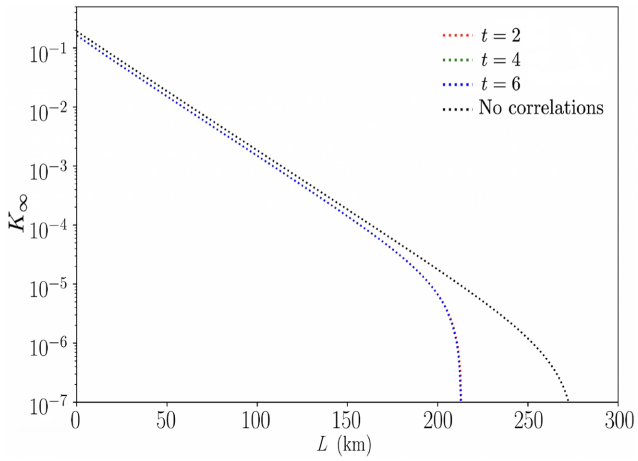

FIG. 6. Effect of the parameter t in the secret key rate corresponding to the TG model. The curves with $t = 2, 4$, and 6 essentially overlap with each other. A bigger t leads to a greater $\delta_{\max}$ and, as a consequence, the results corresponding to the model-independent case are worse. The three cases assume the same input values: $\tilde{\gamma}$, $\tilde{\sigma}$, and $[\lambda, \Lambda]$.

To compare this model with the model-independent case, we need to relate the truncation interval and $\delta_{\max}$, which we recall that fully characterizes the model-independent setting. For this matter, we take $(\lambda, \Lambda) = (\tilde{\gamma} - t\tilde{\sigma}, \tilde{\gamma} + t\tilde{\sigma})$. We state the relation between $\delta_{\max}$ and the parameter t as $\tilde{\gamma}(1 - \delta_{\max}) = \tilde{\gamma} - t\tilde{\sigma}$. In other words, we demand that the maximum relative deviation matches the extreme of the truncation. Note that, ideally, the interval (λ, Λ) could be measured experimentally.

Regarding the value of t, for the sake of comparison with the model-independent case in the main text, we use $t = 4$. It is also worth mentioning that modifying the value of t has a negligible effect on the secret key rate K_∞, as shown in Fig. 6.

[1] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, and C. Ottaviani, *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[3] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[4] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, Trans. Am. Inst. Electr. Eng. **XLV**, 295 (1926).

[5] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, and A. Tanaka, *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[6] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, and P. Monbaron, *et al.*, Long-term performance of the swissquantum quantum key distribution network in a field environment, New J. Phys. **13**, 123001 (2011).

[7] J. F. Dynes, A. Wonfor, W. W. S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, and J. Cho, *et al.*, Cambridge quantum network, npj Quantum Inf. **5**, 101 (2019).

[8] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, and Z. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[9] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, and Z.-P. Li, *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[10] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nat. Photonics **11**, 502 (2017).

[11] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, and W.-Y. Liu, *et al.*, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120**, 030501 (2018).

[12] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, and S.-L. Li, *et al.*, Entanglement-based secure quantum cryptography over 1120 km, Nature **582**, 501 (2020).

[13] X. Wang, X. Sun, Y. Liu, W. Wang, B. Kan, P. Dong, and L. Zhao, Transmission of photonic polarization states from geosynchronous Earth orbit satellite to the ground, Quantum Eng. **3**, e73 (2021).

[14] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. Tanner, C. Natarajan, R. Hadfield, J. O'Brien, and M. Thompson, Chip-based quantum key distribution, Nat. Commun. **8**, 13984 (2017).

[15] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, Metropolitan Quantum Key Distribution with Silicon Photonics, Phys. Rev. X **8**, 021009 (2018).

[16] T. Paraïso, I. De Marco, T. Roger, D. Marangon, J. Dynes, M. Lucamarini, Z. Yuan, and A. Shields, A modulator-free quantum key distribution transmitter chip, npj Quantum Inf. **5**, 42 (2019).

[17] L.-C. Kwek, L. Cao, W. Luo, Y. Wang, S. Sun, X. Wang, and A. Q. Liu, Chip-based quantum key distribution, AAPPS Bull. **31**, 15 (2021).

[18] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[19] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[20] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[21] 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**, 022307 (2014).

[22] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Experimental Quantum Key Distribution with Decoy States, Phys. Rev. Lett. **96**, 70502 (2006).

[23] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Unconditionally secure one-way quantum key distribution using decoy pulses, Appl. Phys. Lett. **90**, 011118 (2007).

[24] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber, Phys. Rev. Lett. **98**, 10503 (2007).

[25] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding, Phys. Rev. Lett. **98**, 010505 (2007).

[26] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, and J. G. Rarity, *et al.*, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. **98**, 10504 (2007).

[27] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate, Opt. Express **16**, 18790 (2008).

[28] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, and L. Yang,

et al., Decoy-state quantum key distribution with polarized photons over 200 km, Opt. Express **18**, 8587 (2010).

[29] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).

[30] Z. Yuan, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, A. J. Shields, A. Plews, R. Takahashi, and K. Doi, *et al.*, 10-mb/s quantum key distribution, J. Lightwave Tech. **36**, 3427 (2018).

[31] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, and M.-J. Li, *et al.*, Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 502 (2018).

[32] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[33] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[34] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, and Y.-G. Zhu, *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[35] K. I. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, *et al.*, High-speed wavelength-division multiplexing quantum key distribution system, Opt. Lett. **37**, 223 (2012).

[36] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. G. Muñoz, and J. Capmany, Simultaneous transmission of 20 × 2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON, Opt. Express **20**, 16358 (2012).

[37] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably-secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[38] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, Appl. Phys. Lett. **117**, 144003 (2020).

[39] T. Kobayashi, A. Tomita, and A. Okamoto, Evaluation of the phase randomness of a light source in quantum- key-distribution systems with an attenuated laser, Phys. Rev. A **90**, 032320 (2014).

[40] G. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution, Opt. Lett. **43**, 5110 (2018).

[41] K.-I. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses, npj Quantum Inf. **4**, 8 (2018).

[42] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, 9 (2020).

[43] Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki, Security of quantum key distribution with light sources that are not independently and identically distributed, Phys. Rev. A **93**, 042325 (2016).

[44] A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H.-K. Lo, and K. Tamaki, Quantum key distribution with setting-choice-independently correlated light sources, npj Quantum Inf. **5**, 8 (2019).

[45] V. Zapatero, A. Navarrete, K. Tamaki, and M. Curty, Security of quantum key distribution with intensity correlations, Quantum **5**, 602 (2021).

[46] H.-K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Inf. Comput. **7**, 431 (2007).

[47] S. Nahar and N. Lütkenhaus, in *Poster Presented at the International Conference on Quantum Cryptography (QCRYPT)* (Amsterdam, 2021).

[48] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, and A. J. Shields, Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

[49] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

[50] A. Navarrete and M. Curty, Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks, Quantum Sci. Technol. **7**, 035021 (2022).

[51] A. Huang, A. Mizutani, H.-K. Lo, V. Makarov, and K. Tamaki, Characterisation of state preparation uncertainty in quantum key distribution, ArXiv:2205.11870 (2022).

[52] G.-J. Fan-Yuan, S. Wang, Z. Yin, W. Chen, D. He, G. Guo, and H.-W. Li, Afterpulse analysis for passive decoy quantum key distribution, Quantum Eng. **2**, e56 (2020).

[53] M. Christandl, R. König, and R. Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 020504 (2009).

[54] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nat. Phys. **3**, 645 (2007).

[55] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).

[56] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, and W.-J. Zhang, *et al.*, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[57] N. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions*, Vol. 1 (Wiley-Interscience, New York, 1994), 1st edn.