Heralded single-photon sources for quantum-key-distribution applications

Matteo Schiavon,[*] Giuseppe Vallone, Francesco Ticozzi, and Paolo Villoresi
Dipartimento di Ingegneria dell'Informazione, Università di Padova, via Gradenigo 6/B, 35131 Padova, Italy

(Received 8 September 2015; published 20 January 2016)

Single-photon sources (SPSs) are a fundamental building block for optical implementations of quantum information protocols. Among SPSs, multiple crystal heralded single-photon sources seem to give the best compromise between high pair production rate and low multiple photon events. In this work, we study their performance in a practical quantum-key-distribution experiment, by evaluating the achievable key rates. The analysis focuses on the two different schemes, symmetric and asymmetric, proposed for the practical implementation of heralded single-photon sources, with attention on the performance of their composing elements. The analysis is based on the protocol proposed by Bennett and Brassard in 1984 and on its improvement exploiting decoy state technique. Finally, a simple way of exploiting the postselection mechanism for a passive, one decoy state scheme is evaluated.

DOI: 10.1103/PhysRevA.93.012331

I. INTRODUCTION

The goal of quantum-key distribution (QKD) is to allow two distant parties, Alice and Bob, to share a secret key even in the presence of an eavesdropper, Eve. Since in quantum mechanics measurements irremediably perturb the systems, it is impossible for an eavesdropper to extract useful information without being noticed. Quantum-key-distribution protocols, like the Bennett-Brassard 1984 (BB84) protocol [1], are proven to be unconditionally secure, when using single photons. However, due to the spread of laser systems and the difficulty of realizing true single-photon sources, most QKD implementations use attenuated pulsed lasers as sources. The need to avoid multiphoton pulses, that can leak information through the photon number splitting (PNS) attack [2], requires a low mean photon number per pulse. This, however, increments the incidence of pulses containing no photons, thus limiting the key generation rate. The incidence of the PNS attack can be limited using the decoy state technique [3–5], at the expense of the necessity to modulate the laser intensity. These limitations have encouraged the research of sources emitting a single photon for each pulse.

One possible implementation of these sources is based on localized quantum structures, such as color centers [6], quantum dots [7,8], atoms [9], or ions [10] in a cavity. These schemes, however, show some major drawbacks: the need of expensive equipment for their operation and limitations in wavelength and bandwidth selection [11]. An alternative scheme for single-photon sources exploits the process of spontaneous parametric down conversion (SPDC) in a nonlinear crystal. An intense laser pump on a nonlinear crystal leads to the probabilistic emission of pairs of photons, called signal and idler. The idler photon can be used to "herald" the presence of the signal photon, giving the so-called heralded source (HS). If the duration of the pulse is much greater than the reciprocal of the phase-matching bandwidth the statistics of the pairs is still poissonian [11]. There are some strategies for improving the single-photon character of the heralded source. One strategy consists of using a single HS with photon number resolving detector on the idler channel and selecting the pulses where only one photon has been detected [12]. An alternative strategy uses parallel HS units and postselection: each unit is pumped with low intensity to suppress multiphoton events, while keeping the overall rate at an acceptable level. The scheme of multiple HS with postselection (MHPS) has been originally proposed by Migdall *et al.* [13]: it used an m-to-1 optical switch triggered by a detector on the idler photon of each HS. Migdall *et al.* took into account also the finite efficiency of single-photon detectors but, as pointed out by Shapiro and Wong [11], the current low efficiency of m-to-1 optical switches strongly limits the performance of this architecture. To overcome this limitation, they proposed a symmetric scheme (SMHPS) using m HS units linked by $m-1$ binary polarization-based photon switches in a tree structure [11]; see Fig. 1. They studied the probability of single-photon and multiphoton pulses, with real detectors and optical switches. Their scheme has been subsequently implemented using four crystals, both with bulk optics [14] and using hybrid photonic circuits [15].

A thorough analysis of multiple heralded sources with postselection has been performed in Ref. [16]. From their work, it emerges that, in the case of imperfect devices, the symmetric scheme suffers from a scalability issue, with a decrease in one photon probability when increasing the number of crystals. In Ref. [16], an asymmetric scheme (AMHPS) that does not present this problem was also proposed. The scheme is shown in Fig. 2 for completeness. The SMHPS and AMHPS schemes were also referred to respectively as *log-tree* and *chained scheme* in Ref. [17].

Subpoissonian sources have already been demonstrated to give an improvement over poissonian ones in the key rate of a QKD system [12,18]. This article specializes the analysis to the case of the multiple-crystal heralded photon sources studied in Ref. [16], parametrizing them using their design parameters instead of the more experimentally relevant efficiency and second-order correlation. Moreover, the security analysis is extended to the case of general attacks by Eve [19].

In this work, we follow [16], and compare the performances of the different architectures and their efficacy in a practical QKD implementation. An ideal MHPS in the configuration proposed by Migdall *et al.*, with perfect heralding efficiency

[*] matteoschiav@yahoo.it

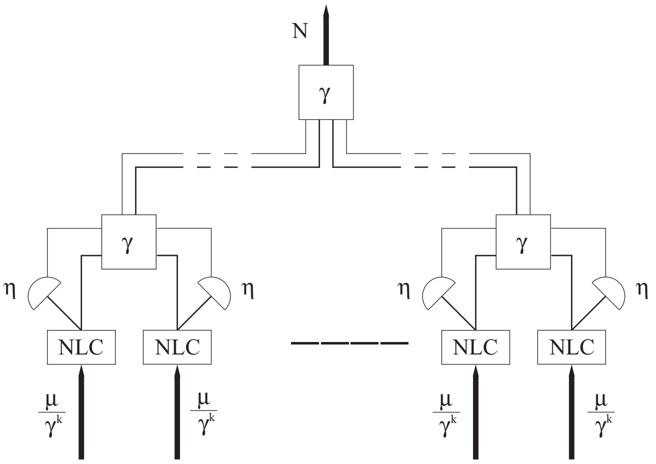

FIG. 1. Schematic of the SMHPS [11]. Each nonlinear crystal (NLC) is fed with pulses such that the mean number of generated pair per pulse is μ/γ^k, with $k = \log_2 m$ and γ is the transmittance of 2-to-1 optical switches. The idler of each NLC is fed into a detector with quantum efficiency η.

and an m-to-1 optical switch with no losses, is studied first, in order to give an account of the maximum performance that can be obtained with this kind of source. Next, two architectures for implementing a multiplexed source in a realistic scenario are analyzed, based on *symmetric* and *asymmetric* networks of 2-to-1 switches. Finite heralding efficiency and optical switch transmittance are considered in order to illustrate the potential of these source with state-of-the-art technology. The different types of sources are inserted in a common model of QKD, based on the BB84 protocol and taking into account channel and detector inefficiencies [19]. The optimization maximizes the key generation rate for the different architectures, with different numbers of HS units, for a wide range of channel losses. The obtained values are then compared with the key generation rate of both an ideal single-photon source and an attenuated laser.

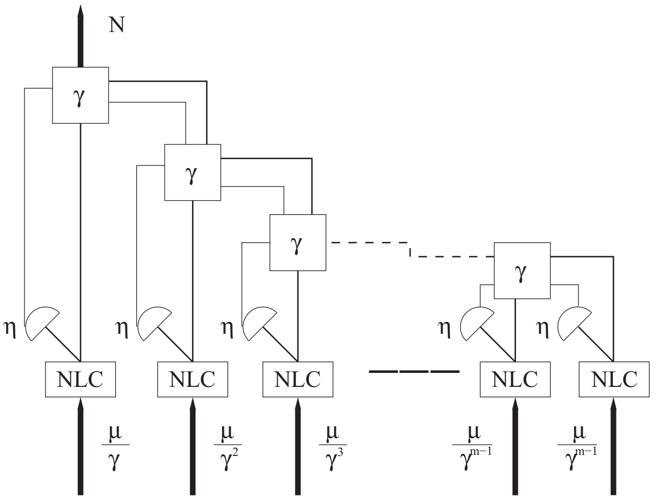

FIG. 2. Schematics of the AMHPS [16]. Each nonlinear crystal (NLC) is pumped with a different intensity in order to compensate the different number of traversed 2-to-1 optical switches, each characterized by its transmittance γ. The idler of each NLC is fed into a detector with quantum efficiency η.

The symmetric and asymmetric schemes are also optimized when used with decoy states [3,4], both in an active [5] and in a passive scheme [20,21]. The active scheme, where Alice actively changes the output statistics of its apparatus, allows her to choose an arbitrary number of decoy states, giving her the ability to estimate channel parameters with arbitrary precision. Passive decoy, on the other hand, is implemented by exploiting photon number correlations of the two outputs of nonlinear crystals [20]. This gives less flexibility in the choice of the decoy states, thus limiting the precision of parameter estimation, but allows us to reach a key generation rate comparable with active decoy without introducing further complexity in Alice's apparatus.

II. MODEL

To evaluate the performances of the heralded single-photon sources, we consider the Bennett-Brassard 1984 (BB84) QKD protocol [1] with polarization encoding. Alice, the transmitter, encodes the random bits into the $Z \equiv \{|H\rangle,|V\rangle\}$ or the $X \equiv \{|D\rangle,|A\rangle\}$ basis, where H, V, D, and A refer to the horizontal, vertical, diagonal, and antidiagonal polarization respectively. Bob randomly measures the incoming photon into the Z or X basis. After the transmission, Alice and Bob discard the events in which the sent and measured bases are different. On the remaining events, they evaluate the secret key rate, namely the amount of unconditional secret bits that they have produced.

The single-photon source held by Alice is completely described by its output statistics. We indicate the probability of emitting n photon by $P_n^M(\mu;m)$ for the MHPS and $P_n^S(\mu;m,\eta,\gamma)$ and $P_n^A(\mu;m,\eta,\gamma)$ for the SMHPS and the AMHPS, respectively [16] (see Appendix A for a more detailed description of the different architectures and the explicit expressions of P_n^M, P_n^S, and P_n^A). The source is pumped by a pulsed laser, with phase randomization between each pulse [19]. The variable μ is proportional to the intensity of the pump laser, which is related to the mean number of pairs generated by each HS per pulse. The sources are parametrized by the number of nonlinear crystals (i.e., of HS units) m and, for the SMHPS and the AMHPS, by the efficiency of the heralding detectors η and the transmittance of the optical switches γ. For $\gamma \to 1$, the scheme used in the switching network is no longer significant, therefore the output statistics of the two architectures coincide. If the heralding efficiency $\eta \to 1$ as well, the two architectures become equivalent to the ideal MHPS.

We used as a model for the QKD channel a depolarizing lossy channel (DLC), characterized by a transmittance $t = 10^{-L/10}$, with L the loss level in decibel, and a depolarization effect with visibility V, that takes into account also alignment and stability issues.

The receiver consists of an optical apparatus, characterized by transmittance t_B, and two single-photon detectors, each with quantum efficiency η_B and dark count probability p_d. They are threshold detectors, i.e., they cannot discriminate the number of incident photons. Assuming the effects of the channel on each photon of an n-photon pulse are independent, the probability that a detector clicks, when an n-photon signal is sent, is

$$\eta_n = 1 - (1 - \eta_D t_B t)^n. \qquad (1)$$

The parameters used for the evaluation of the secret key rate are the *gain* Q, defined as the probability that a pulse gives a click in Bob's measurement apparatus, and the *quantum bit error rate* (QBER) E, i.e., the error probability in Bob's detection events. These are the only measurable parameters during a QKD experiment. For the DLC they can be estimated as follows (see also Ref. [5]).

The gain is defined as

$$Q = \sum_{n=0}^{\infty} Y_n P_n, \qquad (2)$$

where P_n is the probability of having n photons in a pulse and Y_n is the yield of an n-photon signal, i.e., the conditional probability of a detection event at Bob's side given that Alice sends n photons. Assuming independence between signal and background, the yield of an n-photon pulse for a DLC can be predicted to be

$$\widetilde{Y}_n = \widetilde{Y}_0 + \eta_n - \widetilde{Y}_0\eta_n \simeq \widetilde{Y}_0 + \eta_n, \qquad (3)$$

where Y_0 is the probability of a dark count event, which is $\widetilde{Y}_0 \simeq 2p_d$ in the case of two independent detectors and small dark count probability. From now on we use the convention of indicating with a tilde the predicted parameters for a DLC. The negative term, coming from the fact that real detection events and dark counts are not mutually exclusive, can be neglected, since $Y_0 \ll 1$.

The QBER is defined by

$$E = \frac{1}{Q}\sum_{n=0}^{\infty} e_n Y_n P_n, \qquad (4)$$

where e_n is the n-photon error rate, i.e., the probability of an error when Alice sends a n-photon state. For a DLC the n-photon error rate can be predicted to be

$$\widetilde{e}_n = \frac{\widetilde{e}_0\widetilde{Y}_0 + \widetilde{e}_d\eta_n}{\widetilde{Y}_n}, \qquad (5)$$

where $\widetilde{e}_0 = \frac{1}{2}$ is the error probability of a dark count event, which is assumed to be random, and $\widetilde{e}_d = \frac{1-V}{2}$ is the probability that a photon hits the wrong detector.

III. SECRET KEY RATE

After the transmission, Alice and Bob use postprocessing to extract a shared, secret key from the exchanged symbols. The secret key rate R is defined as the fraction of pulses that produce a secret bit (without counting those discarded in the sifting phase) [19]. Its high dependence on source statistics makes it the most suitable parameter for the comparison of the different configurations.

A. BB84 without decoy state

The rate of the BB84 protocol is limited by the fact that Eve can, in principle, obtain full information from a multiphoton pulse through the photon number splitting (PNS) attack, without introducing any error [2]. In the asymptotic limit of infinite key, the achievable key rate is

$$R = Q\left\{(1-\Delta)\left[1 - h\left(\frac{E}{1-\Delta}\right)\right] - f_{EC}h(E)\right\}, \qquad (6)$$

where Δ is the multiphoton rate, defined as

$$\Delta = \frac{1 - P_0 - P_1}{Q}, \qquad (7)$$

f_{EC} is the error correction efficiency, and $h(x)$ is the binary Shannon entropy [19,22]. For true single-photon sources $\Delta = 0$ and the secret key rate is written as $R = Q[1 - h(E) - f_{EC}h(E)]$: the correction term $1 - \Delta$ in (6), indeed, takes into account the possible PNS attack on the multiphoton pulses.

B. BB84 with active decoy

The decoy state technique has been introduced to counteract the PNS attack [4]. It consists of randomly varying the source statistic, so that Eve can no longer adapt her attack to Alice's state. After the transmission, Alice communicates to Bob the state she used for every pulse, allowing them to estimate channel parameters conditioned to that knowledge.

The decoy state technique is active in the sense that Alice chooses the output statistics using a random number generator and (typically) a variable attenuator after the source. In principle, she can choose an arbitrary number of decoy states: however it has been shown that just using the vacuum and a weak decoy state gives tight bounds on the relevant parameters [5]. In the asymptotic limit of infinite key, the key rate is

$$R = P_0Y_0 + P_1Y_1[1 - h(e_1)] - Qf_{EC}h(E), \qquad (8)$$

where P_0 and P_1 are given by the source statistics in the signal state and the parameters e_1, Y_0, and Y_1 are the channel parameters estimated using decoy states [5,23]. Following [19], we make the simplifying assumption that the parameters have been determined exactly.

C. BB84 with passive decoy

In passive decoy state QKD, the source statistics is not under Alice's direct control, but is conditioned on some random event at Alice's side. A typical example consists of an attenuate coherent state passing through a 50/50 beam splitter (BS) with a single-photon detector at the reflected output: the photon statistic at the transmitting output of the BS changes when Alice detects or not a photon. In the case of heralded sources, we denote by $P_n^{(c)}$ or $P_n^{(nc)}$ the output statistics if, respectively, at least one detector or no detector clicks (see Appendix B for the explicit form of these probabilities for the different architectures). We note that $P_n^{(nc)}$ is not trivial since in both schemes the postselection mechanism outputs the first HS if no detector fires [16]. This feature can be used to implement a passive decoy state, since Eve has no way of distinguishing the statistics of each pulse before it is publicly announced.

Assuming the postprocessing is done separately for each statistics, the key rate is

$$R = P^cR^c + P^{nc}R^{nc}, \qquad (9)$$

where R^c and R^{nc} are the key rates for, respectively, the case of at least one detector and no detector clicking. The key rate is, in the limit of infinite key,

$$R^{\xi} = P_0^{(\xi)} Y_0^L + P_1^{(\xi)} Y_1^L \left[1 - h\left(e_1^U\right)\right] - Q^{\xi} f_{EC} h(E^{\xi}), \quad (10)$$

where $\xi \in \{c,nc\}$, Q^{ξ} and E^{ξ} are the parameters estimated from the pulses in the corresponding statistics and Y_0^L, Y_1^L, e_1^U are the lower (L) and upper (U) bounds for the parameters estimated from $\{Q^c, E^c, Q^{nc}, E^{nc}\}$ and the known source statistics. The explicit formulas for parameter estimation, derived from [24], are given in Appendix B in Eqs. (B10), (B13), and (B19).

IV. RESULTS

In the present section we compare the performances of the SMHPS and AMHPS sources for different values of m, namely the number of HS units considered. The parameter μ, related to the number of generated pairs per pulse, is the free parameter used to numerically maximize the rate.

For the channel and detector parameters, we used typical values of present day fiber-based QKD systems [19]. We consider a channel with visibility $V = 0.99$ and losses ranging from 0 to 55 dB (we note that 55 dB corresponds to 275 km if we consider the typical fiber attenuation of $\alpha = 0.2$ dB/km). Bob's apparatus is characterized by optical transmittance $t_B = 1$ and detectors with quantum efficiency $\eta_B = 0.25$ and dark count probability $p_d = 2 \times 10^{-7}$, corresponding to the state-of-the-art of infrared semiconductor single-photon detectors [25]. The efficiency of the error correction code is $f_{EC} = 1.05$ [26].

All the simulated key rates are compared with the one obtained with an weak coherent source (WCS) of poissonian output statistics $P_n = e^{-\mu}\mu^n/n!$, where μ is the mean number of photons per pulse, both without and with a decoy state. In the passive scheme, the comparison is extended to the one decoy state with attenuated laser described in Ref. [5], where also the inefficiencies in parameter estimation are taken into account. Furthermore, all schemes are compared with the single-photon case, representing an upper bound of the rate attainable in a given configuration.

In the following subsections the performances of the heralded single-photon source are compared in different cases.

A. Performances of BB84 without decoy state

The ideal MHPS gives the maximum key rate attainable with this kind of source [16]. This value is shown in Fig. 3. The key rate increases with the number of HS units and approaches the single-photon case for $m = 128$, in the low loss regime. Indeed, for $m \to \infty$, $\Delta = O(\mu)$ and $Q \simeq 1$, approximating the single-photon case for $\mu \ll 1$. At increasing losses, however, the contribution of multiphoton pulses increases and the source shows the same behavior as the attenuated laser. This had already been observed in Ref. [18], with the difference that, for low m, not only is the fraction of multiphoton pulses higher, determining the lower maximum tolerable loss level, but also the incidence of pulses with zero photons is stronger, determining the lower key rate at $L = 0$ dB.

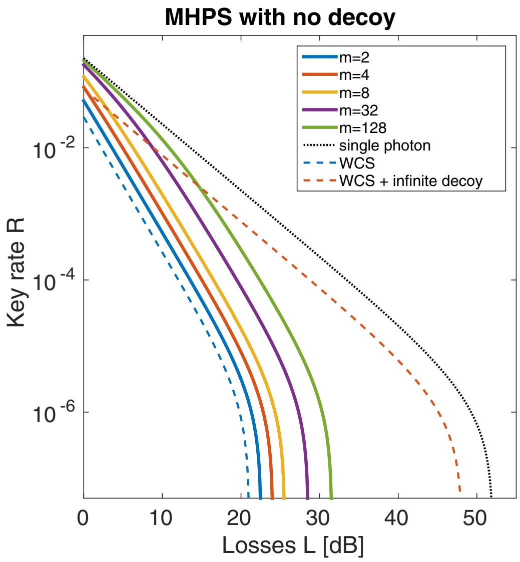

FIG. 3. Key rate for the MHPS architecture in function of channel losses.

While these limitations are proper of the multiple-crystal architecture itself, the implementation using finite efficiency devices further reduces the key generation rate. Using $\eta = 0.7$ and $\gamma = 0.5$ as, respectively, heralding efficiency and switch transmittance [16], the key generation rate of the SMHPS and the AMHPS has the values shown in Fig. 4. Both the key rate and the maximum tolerable losses are lower than for the ideal MHPS, since the low switch transmittance requires a higher mean number of generated pairs per pulse in order to avoid zero-photon pulses, thus increasing also the incidence of multiphoton pulses. This effect is particularly evident in the case of the SMHPS, where, independently from the HS unit triggered to output, the number of switches crossed scales as $k = \log_2 m$. For few HS units, where the number of crossed switches is low, the predominant effect is the suppression of multiphoton events, therefore the key rate increases with m. For a higher number of HS units (such as $m = 32$ or $m = 128$), the source shows a low key rate for low losses (not much higher than the attenuated laser one) and a high maximum tolerable loss level. In the limit $m \to \infty$, any advantage over the attenuated laser is lost.

On the other hand, the AMHPS has a more stable behavior, since its key rate never decreases by increasing m, but reaches an optimal value and then remains unchanged (the key rates for $m = 8$ and $m = 128$ are almost equal). This is due to the fact that, when a certain number of HS units has been reached, the addition of further HS units does not yield significant improvement, since the probability that the rightmost HS units are triggered to the output is negligible and the output is given only by the leftmost HS units, whose configuration does not change (see Fig. 2).

The different behavior of the two architectures is even more evident when studying their key rate at the variation of the two relevant source parameters, the detection efficiency η and the switch transmittance γ. The key rate of the SMHPS and the AMHPS is shown, respectively, in Figs. 5 and 6, when fixing $\eta = 0.7$ and changing γ on the left and with fixed $\gamma = 0.5$ and changing η on the right. The behavior of the SMHPS is

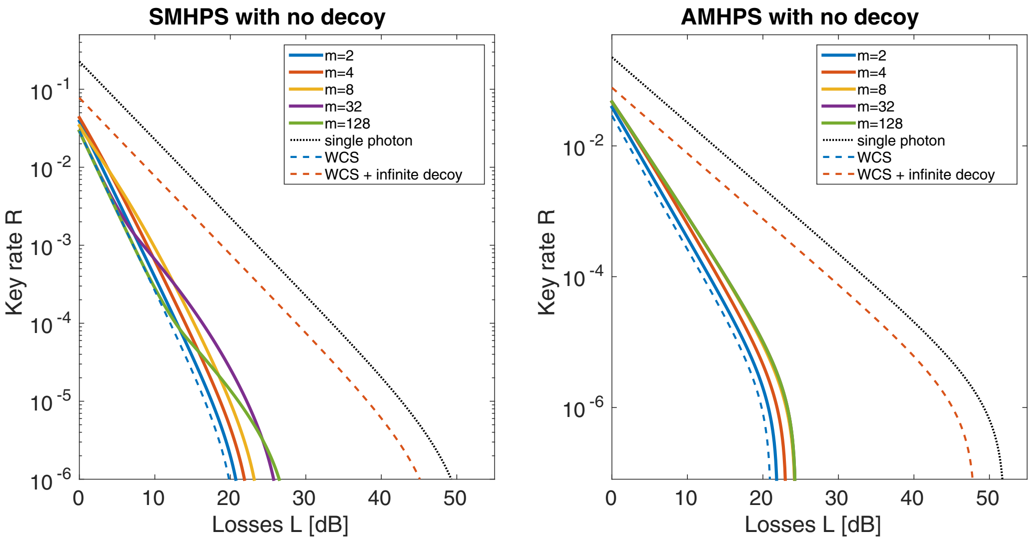

FIG. 4. Key rate of the SMHPS (left) and the AMHPS (right), with $\eta = 0.7$ and $\gamma = 0.5$ for BB84 without decoy state. For the AMHPS (right), the curves for $m = 8$, $m = 32$, and $m = 128$ are superposed.

highly dependent on the switch transmittance. For low γ, the benefits deriving from multiple HS units do not compensate the higher absorption rate. As evident from Fig. 5, for $\gamma < 0.5$ the SMHPS does not perform much better than the attenuated laser. This is consistent with the results from [16], where it has been shown that, in the asymptotic limit $m \to \infty$, the SMHPS performs better than the attenuated laser for $\gamma \geqslant 0.5$. The curve $\gamma = 0.5$ corresponds to the transition between the laserlike regime and the MHPS-like one.

The effect of the detector efficiency η is evident in the high loss regime, where the influence of the lower number of multiphoton pulses is more important. This can be evinced from the right plot of Fig. 5, where the detection efficiency η is varied for the case $\gamma = 0.5$. In the low loss regime, the key rate is the same for all values of η, showing that in this region the dominating effect is photon absorption in the optical routing. On the other hand, the high loss regime shows an improvement in the maximum tolerable loss level from 21 dB for $\eta = 0.1$ to 26 dB for $\eta = 1$. The increased detection efficiency allows a better choice of the HS unit to route to output, thus allowing the HS units to be pumped with less intensity and decreasing the incidence of multiphoton pulses.

The key rate curves of the AMHPS, on the contrary, show the same trend for all tested combinations (η,γ). In the asymmetric scheme, indeed, photons emitted by the leftmost HS units pass a low number of optical switches before being routed to output, therefore the effect of photon absorption never dominates over multiphoton pulses.

B. Performances of BB84 with decoy state

The key rate for active decoy is obtained by using Eq. (8), with e_1, Y_0, and Y_1 calculated by using the channel parameters

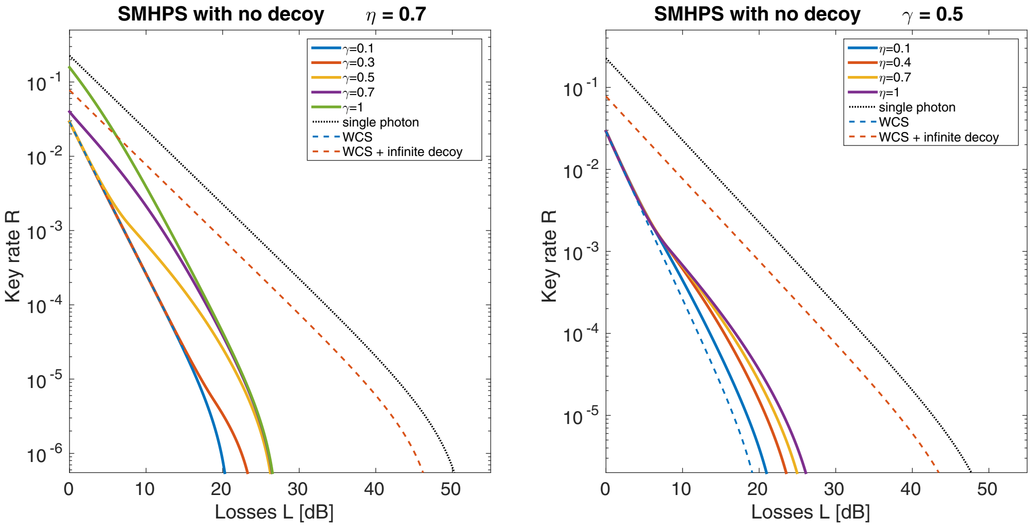

FIG. 5. Key rate (without decoy state) for the SMHPS for $m = 32$ and (left) $\eta = 0.7$ and different values of γ, (right) $\gamma = 0.5$ and different values of η.

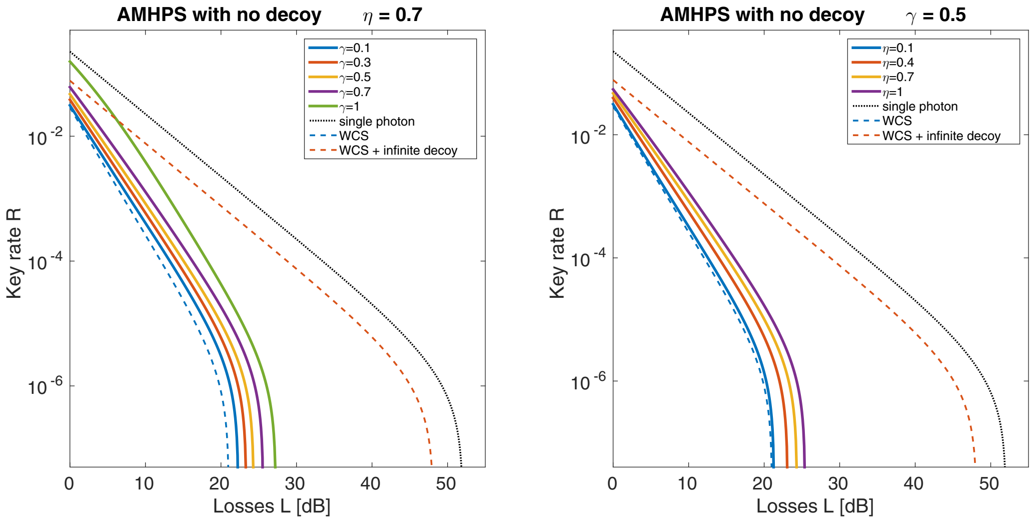

FIG. 6. Key rate (without decoy state) for the AMHPS for $m = 32$ and (left) $\eta = 0.7$ and different values of γ, (right) $\gamma = 0.5$ and different values of η.

given in (5) and (3). The results of simulations are shown in Fig. 7. The normalized mean number of generated pairs that maximizes the key rate is almost constant for both sources in the range ~0.6–0.9, with a steep fall in the regime where dark counts become important. The rate of the SMHPS decreases as the number of crystals increases, thus further underlining the detrimental effect of the increased absorption in optical switches. The AMHPS, on the other hand, does not show any improvement for more than four HS units, because the probability of triggering the rightmost HS units is negligible (see Appendix A).

Since in the proposed implementation of passive decoy the bound on channel parameters is no longer optimal, simulations have to take into account also this effect on the key rate. Therefore, the key rate is calculated by inserting the bounds for e_1, Y_0, and Y_1 into (10) and taking into account the fraction of pulses using each statistics with Eq. (9). Simulation results are shown in Fig. 8. The use of just two different statistics gives a nonoptimal parameter estimation, so a lower key rate than the schemes using active decoy. To account for this, the rates in Fig. 8 are compared also with a similar, one decoy scheme implemented with attenuated laser pulses [5]. The worse bound on the parameters gives a worse estimation of the information leaked to Eve, thus requiring the sources to be pumped with lower intensity than in the case of active decoy (the normalized mean number of generated pairs oscillates, in this case, between 0.2 and 0.3). The performance of the SMHPS is comparable, or slightly worse, to the one of decoy state with attenuated lasers, because of the already discussed detrimental effect on the source caused by optical switch attenuation. On the other hand, the key rate of the AMHPS is always higher than the one obtained with the attenuated laser in the one decoy scheme and almost reaches the maximum tolerable loss level of the attenuated laser with decoy. As in all

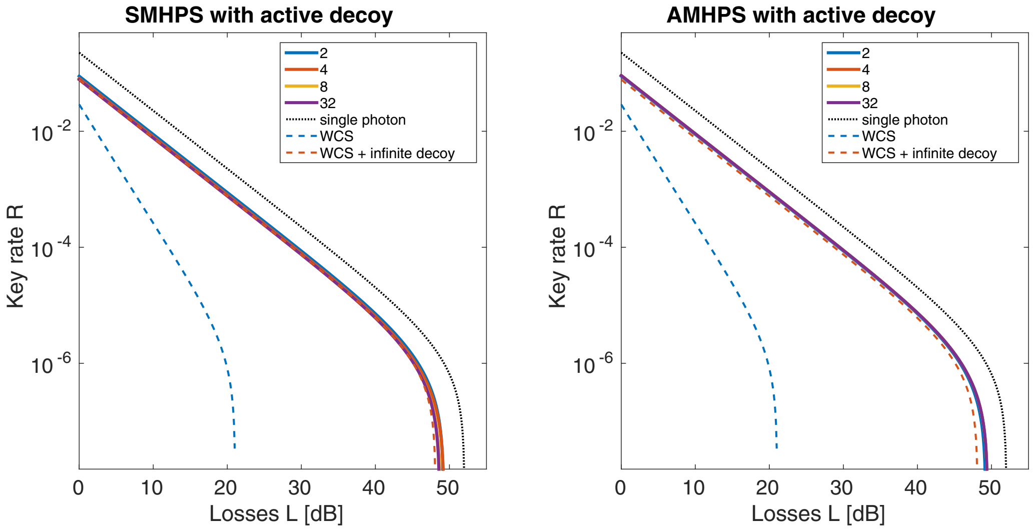

FIG. 7. Key rate of active decoy state QKD for the SMHPS (left) and the AMHPS (right), with $\eta = 0.7$ and $\gamma = 0.5$. For the SMHPS (left), the curves are very close, with $m = 32$ the lowest curve. In the AMHPS case (right), the lowest curve has $m = 2$, while all the others are superposed.

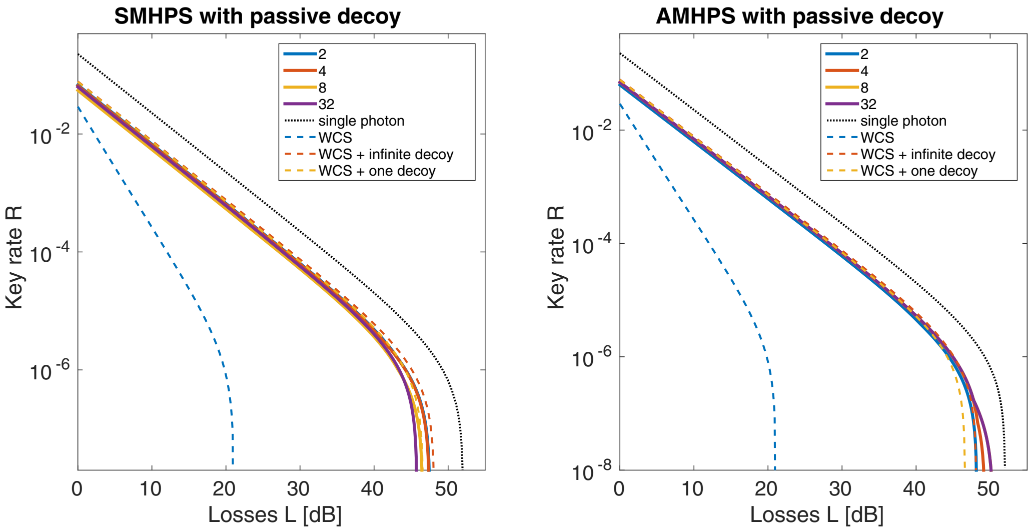

FIG. 8. Key rate for passive decoy state QKD for the SMHPS (left) and the AMHPS (right), with $\eta = 0.7$ and $\gamma = 0.5$.

previous schemes, the AMHPS shows no improvement after a certain threshold of HS units is reached (in this case, $m = 4$).

The comparison of the two sources in the two different decoy schemes of Fig. 9 directly shows the advantage of the AMHPS over the SMHPS. Indeed, the asymmetric scheme performs better than the passive one in both active and passive decoy. Furthermore, the key rate of the AMHPS in the passive scheme almost equals both the SMHPS and the attenuated laser with decoy, despite the worse parameter estimation caused by the use of just one decoy state.

V. CONCLUSION

The multiple-crystal heralded sources have shown better performance than the attenuated laser in all the studied cases, with the only exception of the SMHPS in the one decoy scheme, where the high absorption in optical switches, together with an imperfect parameter estimation, completely overrules the enhancement given by the multiple crystal configuration. The AMHPS shows better scalability than the SMHPS, since in the latter the addition of HS units can degrade the performance while in the former it has, in the worst case scenario, no effect.

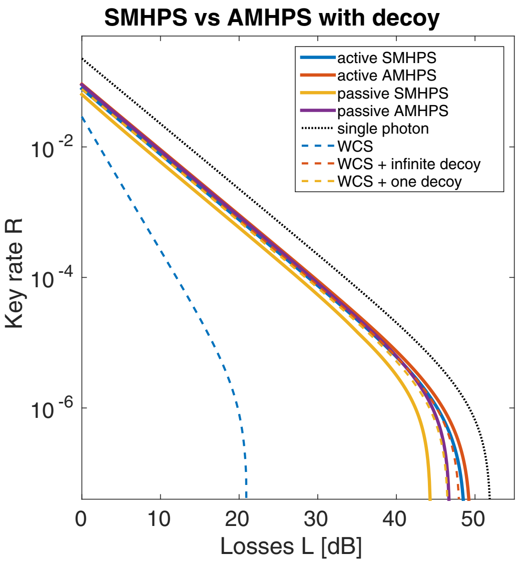

FIG. 9. Key rate for the SMHPS and the AMHPS for both active and passive decoy with $m = 8$, $\eta = 0.7$, and $\gamma = 0.5$.

In addition to this, the key rate of the AMHPS is generally higher than for the SMHPS. The asymmetric structure of the AMHPS, on the other hand, makes its implementation harder than the SMHPS, since each crystal much be fed a different pump intensity and the different HS units must be carefully synchronized. Both architectures have shown a stronger dependence of the key rate on optical switch transmittance than on detector efficiency.

The effect of multiphoton pulses, even if less important than for the attenuated laser, still limits the maximum tolerable loss level. The use of the decoy state solves this problem also for multiple-crystal heralded sources. The best results are given by active decoy, where a variable optical attenuator and a random number generator are used to change the output statistics. The much more complex statistics of these sources, however, makes the calculations needed for the determination of the optimal decoy parameters impractical. Therefore, the simplifying assumption of exact determination of the parameters has been adopted and the obtained results just give a superior limit on the attainable key rate. The optimal decoy parameters must be calculated on a case by case basis, once the characteristics of the source have been chosen.

These limitations might make it preferable the use of a passive decoy scheme, which can be easily implemented in both sources by exploiting the postselection mechanism. In this case, the optimization has taken into account also the inefficiencies of parameter estimation, thus the obtained results give the effective key rate attainable with each configuration and not just a superior limit.

All the results here presented are subjected to the approximation of infinitely long key. We leave finite key effects for future studies. These effects are important especially for the schemes with decoy state, since each photon statistics requires a sufficiently high number of events. In the passive decoy scheme the effect is still more important, since the need of considering also the relative frequency of the two photon statistics can drastically change the optimal source parameters.

The recent advances in integrated photonics suggest an increasing role of multiple-crystal heralded sources. If built into a single chip, they might be a valid alternative to lasers in quantum-key distribution and other quantum information tasks requiring single photons to work properly. Our analysis shows the supremacy of the asymmetric scheme with respect to the symmetric one for QKD applications.

ACKNOWLEDGMENTS

The authors acknowledge the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova and the Strategic- Research-Project QUANTUMFUTURE of the University of Padova. M.S. acknowledges the Center of Studies and Activities for Space (CISAS) "Giuseppe Colombo" for financial support.

APPENDIX A: MULTIPLE CRYSTAL HERALDED SOURCES WITH POSTSELECTION

The multiple crystal heralded source with postselection (MHPS) consists of an array of m HS units, simultaneously pumped with a laser pulse with intensity such that the mean number of generated pairs per pulse is μ [13]. For each HS unit, labeled with index $i = 1 \dots m$, the idler photon is used as a trigger for the signal one, which is injected into an optical switch, as shown in Fig. 10. In the ideal case of perfect detector and optical switch, a postselection mechanism that selects one of the channels whose detector has fired gives the output statistics

$$P_n^M(\mu;m) = \frac{\mu^n}{n!}e^{-\mu}\frac{1-e^{-m\mu}}{1-e^{-\mu}}(1-\delta_n) + \delta_n e^{-m\mu}, \qquad \text{(A1)}$$

where δ_n is the Kronecker δ ($\delta_0 = 1$ and $\delta_{n>0} = 0$) [16].

Taking into account real devices, the MHPS would face the low efficiency of m-to-1 optical switches. This can be avoided by replacing the m-to-1 switch with a tree structure of 2-to-1 switches, giving the symmetric MHPS (SMHPS) [11] shown in Fig. 1.

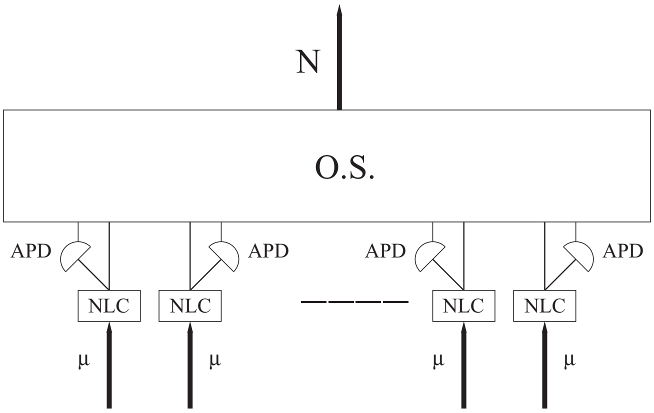

FIG. 10. Schematic of the MHPS [13]. Each nonlinear crystal (NLC) is fed with a pulse such that the mean number of generated pairs is μ. The idler photon is fed into a detector (APD), while the signal one is routed through an optical switch (O.S.) to the output.

The structure of this scheme requires the number of HS units m to be a power of 2. The idler photon of each HS unit is fed into a detector with quantum efficiency η, while the signal photon is directed to a 2-to-1 optical switch of transmittance γ. Since the photons produced by each HS unit pass $k = \log_2 m$ switches before reaching the output, the crystals are pumped with an intensity such that the mean number of generated pairs per pulse is μ/γ^k. The postselection mechanism in each optical switch gives priority to the left HS unit and, in case no HS unit triggers, always outputs the left one [16]. The photon statistics at the output is

$$\begin{aligned} P_n^S(\mu;m,\eta,\gamma) = {} & \frac{(1-\eta)\mu e^{-(1-\eta)\mu}}{n!}e^{-\eta\mu(2^k/\gamma^k)} \\ & + \frac{\mu^n e^{-\mu}}{n!}\frac{1-(1-\eta)^n e^{-\eta(1/\gamma^k-1)\mu}}{1-e^{-\eta(\mu/\gamma^k)}} \\ & \times \left(1-e^{-\eta\mu(2^k/\gamma^k)}\right). \qquad \text{(A2)} \end{aligned}$$

In the asymmetric MHPS (AMHPS), the m HS units are arranged following the scheme shown in Fig. 2 [16]. Each HS unit, whose idler photon is fed into a detector of efficiency η, is pumped with an intensity such that the mean number number of generated pair per pulse is μ/γ^{k_i}, with

$$k_i = \begin{cases} i & i \leqslant m-1 \\ m-1 & i = m \end{cases}, \qquad \text{(A3)}$$

in order to compensate the different number of traversed 2-to-1 optical switches. The postselection mechanism of each optical switch is the same as for the SMHPS, i.e., it gives priority to the left HS unit and, if none triggers, outputs the left one. Differently from the SMHPS, this architecture requires delay lines to be introduced, in order to compensate the longer transmission time of the rightmost HS units [16]. The statistics at the output is

$$\begin{aligned} P_n^A(\mu;m,\eta,\gamma) = {} & \frac{[(1-\eta)\mu]e^{-(1-\eta)\mu}}{n!} \\ & \times e^{-\eta\mu\{[(2-\gamma)\gamma^{1-m}-1]/(1-\gamma)\}} \\ & + \frac{\mu^n e^{-\mu}}{n!}\sum_{i=1}^{m} e^{-\eta\mu[(\gamma^{1-i}-1)/(1-\gamma)]} \\ & \times \left[1-(1-\eta)^n e^{\eta\mu} e^{-\eta\mu/\gamma^{k_i}}\right]. \qquad \text{(A4)} \end{aligned}$$

APPENDIX B: PARAMETER ESTIMATION IN PASSIVE DECOY STATE QKD

The parameters Y_0, Y_1, and e_1, necessary in postprocessing, are not directly measured during the key exchange session, but must be estimated from the experimental data Q and E. If Alice registers, for each pulse, whether at least one or no detector has clicked, a different gain and QBER for each case can be measured and these can be used for parameter estimation. Since both statistics depend on the same μ, parameter estimation can be included in the general optimization process, thus giving the real key rate and not just a superior limit.

The probability that no detector clicks in a pulse is

$$P^{nc}(\mu;m,\eta,\gamma) = e^{-\mu\eta(2^k/\gamma^k)} \tag{B1}$$

for the SMHPS and

$$P^{nc}(\mu;m,\eta,\gamma) = e^{-\mu\eta\{[(2-\gamma)\gamma^{1-m}-1]/(1-\gamma)\}} \tag{B2}$$

for the AMHPS, where $k = \log_2 m$. The statistics in the case of no click is the same for both sources (in both cases the first HS unit is routed to the output) and is

$$P_n^{(nc)} = \frac{[\mu(1-\eta)]^n}{n!} e^{-\mu(1-\eta)}, \tag{B3}$$

while the statistics for the case of at least a detector click is

$$P_n^{(c)} = \frac{\mu^n e^{-\mu}}{n!}[1-(1-\eta)^n e^{-\eta\mu(1/\gamma^k-1)}]\frac{1}{1-e^{-\mu\eta/\gamma^k}} \tag{B4}$$

for the SMHPS and

$$P_n^{(c)} = \frac{\mu^n e^{-\mu}}{n!}\sum_{i=1}^{m}[1-(1-\eta)^n e^{-\mu\eta[(1/\gamma^{k_i})-1]}]\frac{e^{-\mu\eta[(\gamma^{1-i}-1)/(1-\gamma)]}}{1-e^{-\mu\eta\{[(2-\gamma)\gamma^{1-m}-1]/(1-\gamma)\}}} \tag{B5}$$

for the AMHPS [16].

After the key exchange session, Alice tells Bob for which pulses at least one detector has clicked, so that they can estimate the gain and the QBER separately for the two cases. From these values, referenced to as $\{Q^c,E^c,Q^{nc},E^{nc}\}$, and the known source statistics $P_n^{(c)}$ and $P_n^{(nc)}$, they can estimate the parameters of the channel using the method described in Ref. [24].

The first parameter to be estimated is Y_0. Its upper bound Y_0^U can be calculated starting from the relations

$$Q^c E^c = \sum_{n=0}^{\infty} P_n^{(c)} Y_n e_n \geqslant P_0^{(c)} Y_0 e_0, \tag{B6}$$

$$Q^{nc} E^{nc} = \sum_{n=0}^{\infty} P_n^{(nc)} Y_n e_n \geqslant P_0^{(nc)} Y_0 e_0. \tag{B7}$$

Since both inequalities must hold, the parameter Y_0 is upper bounded by

$$Y_0 \leqslant Y_0^U = \min\left\{\frac{Q^c E^c}{P_0^{(c)} e_0}, \frac{Q^{nc} E^{nc}}{P_0^{(nc)} e_0}\right\}. \tag{B8}$$

Its lower bound Y_0^L can be calculated from

$$P_1^{(c)} Q^{nc} - P_1^{(nc)} Q^c = \sum_{n=0}^{\infty}\big(P_1^{(c)} P_n^{(nc)} - P_1^{(nc)} P_n^{(c)}\big) Y_n \leqslant \big(P_1^{(c)} P_0^{(nc)} - P_1^{(nc)} P_0^{(c)}\big) Y_0, \tag{B9}$$

that gives

$$Y_0 \geqslant Y_0^L = \max\left\{\frac{P_1^{(c)} Q^{nc} - P_1^{(nc)} Q^c}{P_1^{(c)} P_0^{(nc)} - P_1^{(nc)} P_0^{(c)}}, 0\right\}, \tag{B10}$$

since, for both the SMHPS and the AMHPS,

$$P_1^{(c)} P_n^{(nc)} - P_1^{(nc)} P_n^{(c)} = A_{n,1}[(1-\eta)^n - (1-\eta)]\begin{cases}\leqslant 0 & \text{for} \quad n \geqslant 2\\ \geqslant 0 & \text{for} \quad n = 0\text{'}\end{cases} \tag{B11}$$

with $A_{n,1}$ a positive constant.

The lower bound on the single-photon yield Y_0 is calculated starting from

$$P_2^{(c)} Q^{nc} - P_2^{(nc)} Q^c = \sum_{n=0}^{\infty}\big(P_2^{(c)} P_n^{(nc)} - P_2^{(nc)} P_n^{(c)}\big) Y_n \leqslant \sum_{n=0}^{1}\big(P_2^{(c)} P_n^{(nc)} - P_2^{(nc)} P_n^{(c)}\big) Y_n, \tag{B12}$$

which leads to

$$Y_1 \geqslant Y_1^L = \max\left\{\frac{P_2^{(c)} Q^{nc} - P_2^{(nc)} Q^c - \big(P_2^{(c)} P_0^{(nc)} - P_2^{(nc)} P_0^{(c)}\big) Y_0^U}{P_2^{(c)} P_1^{(nc)} - P_2^{(nc)} P_1^{(c)}}, 0\right\}, \tag{B13}$$

since

$$P_2^{(c)}P_n^{(nc)} - P_2^{(nc)}P_n^{(c)} = A_{n,2}[(1-\eta)^n - (1-\eta)^2]\begin{cases}\leqslant 0 & \text{for} \quad n \geqslant 2\\ \geqslant 0 & \text{for} \quad n \leqslant 1\end{cases} \tag{B14}$$

with $A_{n,2}$ positive.

Similarly, the upper bound on e_1 is calculated from

$$P_0^{(nc)}Q^cE^c - P_0^{(c)}Q^{nc}E^{nc} = \sum_{n=0}^{\infty}\left(P_0^{(nc)}P_n^{(c)} - P_0^{(c)}P_n^{(nc)}\right)e_nY_n \geqslant \left(P_0^{(nc)}P_1^{(c)} - P_0^{(c)}P_1^{(nc)}\right)e_1Y_1, \tag{B15}$$

since

$$P_0^{(nc)}P_n^{(c)} - P_0^{(c)}P_n^{(nc)} = A_{n,0}[1-(1-\eta)^n] \geqslant 0 \tag{B16}$$

for all n, and

$$Q^cE^c = \sum_{n=0}^{\infty}P_n^{(c)}Y_ne_n \geqslant P_0^{(c)}Y_0e_0 + P_1^{(c)}Y_1e_1, \tag{B17}$$

$$Q^{nc}E^{nc} = \sum_{n=0}^{\infty}P_n^{(nc)}Y_ne_n \geqslant P_0^{(nc)}Y_0e_0 + P_1^{(nc)}Y_1e_1, \tag{B18}$$

thus obtaining

$$e_1 \leqslant e_1^U = \min\left\{\frac{P_0^{(nc)}Q^cE^c - P_0^{(c)}Q^{nc}E^{nc}}{\left(P_0^{(nc)}P_1^{(c)} - P_0^{(c)}P_1^{(nc)}\right)Y_1^L}, \frac{Q^cE^c - P_0^{(c)}Y_0^Le_0}{P_1^{(c)}Y_1^L}, \frac{Q^{nc}E^{nc} - P_0^{(nc)}Y_0^Le_0}{P_1^{(nc)}Y_1^L}\right\}. \tag{B19}$$

[1] C. H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.

[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[3] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[4] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[5] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[6] I. Aharonovich, S. Castelletto, D. A. Simpson, C.-H. Su, A. D. Greentree, and S. Prawer, Rep. Prog. Phys. **74**, 076501 (2011).

[7] M. Pelton, C. Santori, J. Vučković, B. Zhang, G. S. Solomon, J. Plant, and Y. Yamamoto, Phys. Rev. Lett. **89**, 233602 (2002).

[8] J. Ayesha *et al.*, Appl. Phys. Lett. **104**, 101108 (2014).

[9] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, Science **303**, 1992 (2004).

[10] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, Nature (London) **431**, 1075 (2004).

[11] J. H. Shapiro and F. N. Wong, Opt. Lett. **32**, 2698 (2007).

[12] M. Lasota, R. Demkowicz-Dobrański, and K. Banaszek, Int. J. Quantum Inf. **11**, 1350034 (2013).

[13] A. L. Migdall, D. Branning, and S. Castelletto, Phys. Rev. A **66**, 053805 (2002).

[14] X.-S. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, Phys. Rev. A **83**, 043814 (2011).

[15] T. Meany, L. A. Ngah, M. J. Collins, A. S. Clark, R. J. Williams, B. J. Eggleton, M. J. Steel, M. J. Withford, O. Alibart, and S. Tanzilli, Laser Photon. Rev. **8**, L42 (2014).

[16] L. Mazzarella, F. Ticozzi, A. V. Sergienko, G. Vallone, and P. Villoresi, Phys. Rev. A **88**, 023848 (2013).

[17] D. Bonneau, G. J. Mendoza, J. L. O'Brien, and M. G. Thompson, New J. Phys. **17**, 043057 (2015).

[18] E. Waks, C. Santori, and Y. Yamamoto, Phys. Rev. A **66**, 042315 (2002).

[19] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[20] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).

[21] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Opt. Lett. **34**, 3238 (2009).

[22] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).

[23] H.-K. Lo, Quant. Inf. Comput. **5**, 413 (2005).

[24] M. Curty, X. Ma, B. Qi, and T. Moroder, Phys. Rev. A **81**, 022310 (2010).

[25] ID230 datasheet, *ID Quantique*, http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf (online: 11/2015).

[26] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Quant. Inf. Comput. **15**, 453 (2015).