Fully passive measurement-device-independent quantum key distribution

Jinjie Li,[1] Wenyuan Wang,[1,2,*] and Hoi-Kwong Lo[3,4,5,6,†]

[1] *Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *HK Institute of Quantum Science & Technology, University of Hong Kong, Pokfulam Road, Hong Kong*
[3] *Dept. of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada*
[4] *Centre for Quantum Information and Quantum Control (CQIQC), University of Toronto, Toronto, Ontario M5S 1A7, Canada*
[5] *Dept. of Physics, University of Toronto, Toronto, Ontario M5S 1A7, Canada*
[6] *Quantum Bridge Technologies, Inc., 100 College Street, Toronto ON M5G 1L5, Canada*

(Received 6 December 2023; revised 26 April 2024; accepted 17 May 2024; published 25 June 2024)

A recently proposed fully passive quantum key distribution (QKD) removes all source modulator side channels. In this work, we combine fully passive sources with measurement-device-independent (MDI) QKD to simultaneously remove side channels from source modulators and detectors. We show a numerical simulation of passive MDI QKD, and we obtain an acceptable key rate while achieving much better implementation security, as well as ease of implementation, compared with a recently proposed fully passive twin-field QKD, paving the way towards more secure and practical QKD systems. We prove that a fully passive protocol is compatible with MDI QKD and we propose a novel idea that can improve the sifting efficiency.

DOI: 10.1103/PhysRevApplied.21.064056

I. INTRODUCTION

The laws of quantum mechanics ensure theoretically secure communication using quantum key distribution (QKD) between two parties [1,2]. However, practically implementing QKD systems is still a challenge due to the lack of perfect equipment [3–7]. Hence, physicists have been working on eliminating side channels arising from these imperfections. The concept of measurement-device-independent (MDI) QKD, introduced in 2012, is automatically immune to attacks on detectors. In other words, it completely removes the risk of side channels at detectors [8].

To perform MDI QKD, the two verified users, Alice and Bob, desire to communicate and send signals to a third party, Charlie. Charlie can even be untrusted, and he should perform a Bell state measurement and publicly announce the successful outcomes. The decoy-state analysis technique [9–11] could be used when there are no available single-photon sources. A review of MDI QKD can be found in Appendix A [8].

While side channels from the detector side can be eliminated, sources remain a vulnerable part in QKD implementations. Active modulations on laser's phases or intensities are one of the vulnerabilities in the sources. Specifically, they may either leak information directly to an eavesdropper or compromise the security of the decoy-state analysis. Meanwhile, an eavesdropper may hack the information using, for example, a Trojan-horse attack or pattern effect [3,6].

A fully passive QKD protocol proposed in 2022 [12,13] offers a way to remove side channels from the source modulator, so that the abovementioned vulnerabilities can be prevented. In the recently proposed fully passive QKD, the fully passive source setup is essentially a combination of a passive decoy-state and a passive encoding setup [12]. A passive decoy state [14,15] uses a 50:50 beam splitter (BS) to interfere with two incoming signals; the intensity of the output signal is determined by the phase difference of the incoming signals while maintaining a randomized global phase. In the passive encoding setup [15], a polarizing beam splitter (PBS) is used. The polarization of the output signal is determined by the phase difference of the two incoming signals, again with a randomized global phase.

The fully passive QKD source setup is shown in Fig. 1 [12]. Each user prepares four laser sources with independent random phases; the pairwise phase difference determines the intensities of the two arms. Subsequently, the phase and intensity difference of the two arms yield an output with random polarization. This output can be represented by a state on a Bloch sphere [12]. The signals coming out of the fully passive source can then be postselected by users to perform QKD [12].

*Corresponding author: wenyuanw@hku.hk
†Corresponding author: hklo@ece.utoronto.ca

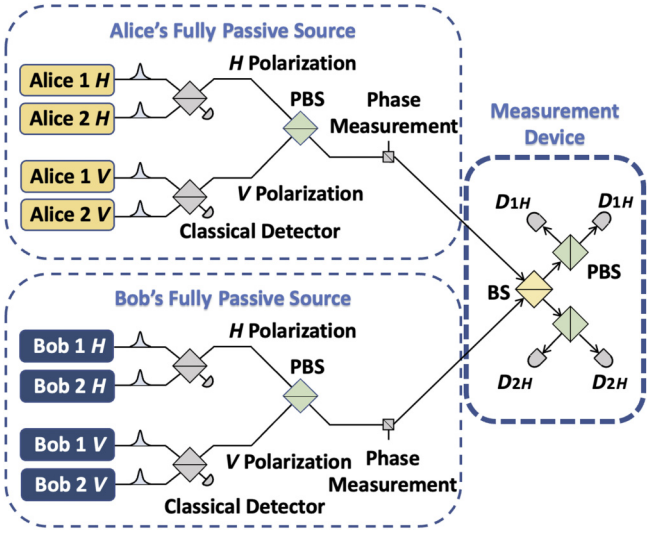

FIG. 1. Fully passive MDI-QKD setup. Alice and Bob each possess a fully passive source, and Charlie possesses the usual MDI measurement device. The fully passive sources and Charlie's setup are reproduced from Refs. [12] and [8], respectively. Figure is reproduced with modifications from Fig. 1 in W. Wang *et al.*, Phys. Rev. Lett. 130, 220801 (2023) with permission. Copyright 2023, American Physical Society.

It is a natural progression to consider combining MDI QKD with passive QKD, in order to ensure that both detector and source modulator sides can simultaneously avoid side channels. This notion inspired this work, which we have named passive MDI QKD. This work mainly entails the following key contributions. (1) In this work, we generalize the fully passive source proposed in Ref. [12] to MDI QKD. Since MDI QKD involves single-photon pairs, it is nontrivial to apply the decoy-state analysis based on passively prepared mixed states to MDI QKD; we present a proof to show that decoy-state analysis is applicable to fully passive MDI QKD. (2) We develop a new channel model for fully passive MDI QKD that caters for arbitrary source state polarizations on a Bloch sphere [i.e., perfect polarizations undergoing arbitrary three-dimensional (3D) rotations]. Such a model has never been explicitly studied in previous works for active MDI QKD, which usually consider perfectly prepared signal states and only 2D rotations of polarizations on the X-Z plane caused by channel misalignment. (3) The main challenge in simulating the channel statistics is efficiently calculating high-dimensional integrations, such as Eq. (3); we use a high-speed numerical integration library [16] to implement efficient simulations. Because of the double sifting nature of MDI QKD, working with very small numbers throughout the project is inevitable; additionally, the higher-dimensional integrations cost significant computational power, which brings additional technical challenges for numerical simulation and key rate optimization. (4) To address the relatively low sifting efficiency, we propose a novel sifting method that can further improve the key rate.

In the work that originally proposed this idea, this fully passive source was applied to a BB84 protocol [12]. Most recently, a fully passive twin-field (TF) QKD protocol has also been proposed, which can also remove side channels from both modulators and detectors [17]. However, TF QKD is significantly more challenging experimentally compared to MDI QKD due to the requirement of remote frequency stabilization. The same applies to passive TF QKD, while the requirement on frequency stability will be much less stringent for MDI QKD, which we discuss in this work.

In this paper, the details of the passive MDI-QKD protocol will be discussed in Sec. II, including the passive sources, channel model, decoy-state analysis, and key rate calculation. In Sec. III, a simulation result is shown with some interpretation. In Sec. IV, we provide some discussion and propose a novel idea to improve the key rate.

II. THE PROTOCOL

In this section, there are four subsections that cover the discussion on the fully passive sources and detectors, postselection, channel model, decoy-state analysis, and key rate calculation.

A. Fully passive sources and detection

A fully passive source setup [8,12] is shown in Fig. 1, Alice and Bob each hold one fully passive setup to perform passive MDI QKD. As shown in Fig. 1, each of Alice and Bob needs four light sources, and they join in pairs at a 50:50 BS to yield the signals at the H and V arms. The two arms then combine at a PBS to generate the final output signal, whose polarization is fully passively chosen [12]. The phases of the four sources, $\phi_1, \phi_2, \phi_3, \phi_4$, are entirely random; hence, each user has four degrees of freedom (DOFs). While Alice (or Bob) makes measurements of intensities and phases of the light signals at the H and V arms, represented as $\mu_H, \mu_V, \phi_H, \phi_V$, they correspond one to one with a Bloch sphere coordinate $\mu, \theta_{HV}, \phi_{HV}$, and a global phase via [12]

$$\theta_{HV} = 2\cos^{-1}\left(\sqrt{\frac{\mu_H}{\mu_H+\mu_V}}\right), \qquad \phi_{HV} = \phi_V - \phi_H. \tag{1}$$

So the four DOFs that Alice possesses convert from the beginning four phases to the Bloch sphere coordinates

$$\phi_1, \phi_2, \phi_3, \phi_4 \rightarrow \mu_H, \mu_V, \phi_H, \phi_V \rightarrow \mu, \theta_{HV}, \phi_{HV}, \phi_{\text{global}}. \tag{2}$$

Since all of the four phases at the beginning are randomly chosen, the final signal can be any state on the Bloch

sphere. The output states are then ready for users, Alice and Bob, to postselect.

Charlie, the untrusted third party, possesses the usual MDI-QKD measurement devices; see Fig. 1 [8]. The four detectors Charlie uses are single-photon detectors (SPDs).

B. Postselection

The output signals from the sources can be any state on a Bloch sphere. The users determine regions on the Bloch sphere to represent the four states $H, V, +, -$. Alice and Bob postselect only those signals that lie within those regions. More specifically, the regions in $(\mu_H, \mu_V, \phi_{HV})$ space are shown in Fig. 2. One could subdivide the regions into smaller ones to perform decoy-state analysis [12]. This point will be discussed further in Sec. II D.

Within a given region, S_i, there is a mixture of Bloch sphere states. Hence, observables are described by their expectation values, for example, for an observable A, its expectation value (in a fully passive MDI-QKD protocol) within given regions, S_i for Alice and S_j for Bob, is given by

$$\begin{aligned}\langle A\rangle_{S_iS_j} &= \frac{1}{2}\left(\frac{1}{P_{S_iS_j}}\right)\\ &\times \int_{0,\phi_R'}^{2\pi}\iiint_{S_i}\iiint_{S_j} p_A(\mu_{HA},\mu_{VA},\phi_{HVA})\\ &\times p_B(\mu_{HB},\mu_{VB},\phi_{HVB})\\ &\times A(\mu_{HA},\mu_{VA},\phi_{HVA},\mu_{HB},\mu_{VB},\phi_{HVB})\\ &\times d\mu_{HA}d\mu_{VA}d\phi_{HVA}d\mu_{HB}d\mu_{VB}d\phi_{HVB}d\phi_R', \quad (3)\\ P_{S_iS_j} &= \iiint_{S_i}\iiint_{S_j} p_A(\mu_{HA},\mu_{VA},\phi_{HVA})\\ &\times p_B(\mu_{HB},\mu_{VB},\phi_{HVB})\\ &\times d\mu_{HA}d\mu_{VA}d\phi_{HVA}d\mu_{HB}d\mu_{VB}d\phi_{HVB}.\end{aligned}$$

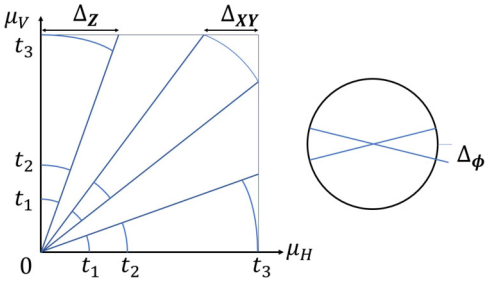

FIG. 2. Alice's postselection regions and decoy settings shown in μ_H, μ_V, ϕ space. Three decoys are used. The whole setup is determined by six parameters, $\{\Delta_Z, \Delta_{XY}, \Delta_\phi, t_1, t_2, t_3\}$. Bob possesses the same decoy setting. This figure is reproduced from [12]. Figure is reproduced with modifications from Fig. 2 in W. Wang *et al.*, Phys. Rev. Lett. 130, 220801 (2023) with permission. Copyright 2023, American Physical Society.

Here, the integration of phase, ϕ_R', will be discussed in the next section. The probability distribution p_A for Alice is simply a classical probability, given by [12]

$$p_A(\mu_{HA},\mu_{VA},\phi_{HVA}) = p_{\mu A}(\mu_{HA},\mu_{VA})p_{\phi A}(\phi_{HAV}), \quad (4)$$

$$\begin{aligned}p_{\mu A}(\mu_{HA},\mu_{VA}) &= \frac{1}{\pi^2\sqrt{\mu_{HA}(\mu_{\max}-\mu_{HA})}}\\ &\times \frac{1}{\sqrt{\mu_{VA}(\mu_{\max}-\mu_{VA})}}, \quad (5)\end{aligned}$$

$$p_{\phi A}(\phi_{HVA}) = \frac{1}{2\pi}, \quad (6)$$

and Bob has the same distribution. Therefore, for one observable in fully passive MDI QKD, a seven-dimensional integration is required (three for Alice and Bob each, with an additional dimension on phase randomization), which consumes significant computational power. Throughout the project, all high-dimensional integrations were performed using the CUBA library [16].

In our protocol, Alice and Bob need to perform an additional postselection, whose probability distribution depends on the intensities for Alice or Bob:

$$q_\mu(\mu_{HA/B},\mu_{VA/B}). \quad (7)$$

This means that Alice and Bob discard some of the signals according to q_μ. In this case, the overall probability distribution used to calculate the expectation value is the product of p and q_μ. In this work, q_μ is chosen to be [12]

$$\begin{aligned}&q_\mu(\mu_{HA/B},\mu_{VA/B})\\ &= C\pi^2\sqrt{\mu_{HA/B}(\mu_{\max}-\mu_{HA/B})}\\ &\times \sqrt{\mu_{VA/B}(\mu_{\max}-\mu_{VA/B})}e^{(\mu_{HA/B}+\mu_{VA/B})}, \quad (8)\end{aligned}$$

so the overall probability distribution is an exponential

$$p_\mu = Ce^{\mu_H+\mu_V}. \quad (9)$$

One may find this "modulation" of postselection useful while doing decoy-state analysis. This will be covered in detail while discussing decoy-state analysis.

C. Channel model

In active MDI QKD, the two bases (X and Z) consist of a two-dimensional plane, while in the fully passive case, signals are represented on a three-dimensional Bloch sphere. This poses additional difficulties when simulating its channel model.

The signals coming from Alice and Bob's fully passive setup go through the fiber channel to reach Charlie. Alice and Bob may prepare the states with slight misalignment. At the same time, the signals may gain some rotation

while traveling through the channels. A model was built to describe the misalignment and rotations based on the 3D Rodrigues formula [18].

The two signals arriving at Charlie from Alice and Bob interfere at a 50:50 BS, described by the interference formula. Therefore, we could calculate the probability of a detection event happening at each of the four detectors. The probabilities can then be used to calculate the gains, G, and error gains, QE, given the set of input parameters $\{\mu_{HA}, \mu_{VA}, \phi_{HVA}, \mu_{HB}, \mu_{VB}, \phi_{HVB}\}$, which describes the states coming from Alice and Bob's fully passive source. A detailed mathematical explanation of the channel model is given in Appendix E.

D. Decoy-state analysis

In QKD, the conventional decoy-state analysis solves a set of linear equations to find the lower and upper bounds of the single-photon yield Y_{11} and the error yield $e_{11}Y_{11}$, for example, in MDI QKD [19],

$$\begin{aligned} Q_{\mu_A\mu_B} &= \sum_{n,m=0}^{\infty} P_n^A P_m^B Y_{\mu_A\mu_B}^{nm}, \\ Q_{\mu_A\mu_B}E_{\mu_A\mu_B} &= \sum_{n,m=0}^{\infty} P_n^A P_m^B Y_{\mu_A\mu_B}^{nm} e_{\mu_A\mu_B}^{nm}, \end{aligned} \tag{10}$$

where P is the Poisson distribution, and μ_A, μ_B are Alice and Bob's decoy intensity choices.

While in the passive MDI-QKD case, the gains and quantum bit error rates (QBERs) are of the forms

$$\begin{aligned} \langle Q\rangle_{S_i^A S_j^B} &= \sum_{n,m=0}^{\infty} \langle P_n^A P_m^B Y_{nm}\rangle_{S_i^A S_j^B}, \\ \langle QE\rangle_{S_i^A S_j^B} &= \sum_{n,m=0}^{\infty} \langle P_n^A P_m^B e_{nm} Y_{nm}\rangle_{S_i^A S_j^B}, \end{aligned} \tag{11}$$

where the expectation value of any observable in passive MDI QKD is described in Eq. (3).

One could note that the single-photon yield Y_{11} or the error yield $e_{11}Y_{11}$ is within the whole sevenfold integration, and hence cannot be directly "decoupled" to a linear programming form [19].

It is important to find a way to transform this "coupled" form into a "decoupled" form, so that one can apply a linear program (which is what is usually used in decoy-state analysis to find the single-photon parameter bounds), and, subsequently, it is also important to prove that the bounds derived from the "decoupled" form can be used to calculate the key rate. In the "decoupling" process, we propose a novel postselection method that can effectively decouple the parameters, The details of the derivation are shown in Appendix B [12]. The "decoupled" forms are

$$\langle Q\rangle_{S_i^A S_j^B} = \langle P_n^A\rangle_{S_i^A}\langle P_n^B\rangle_{S_j^B} \times Y_{nm}^{\text{mixed}}, \tag{12}$$

$$\langle QE\rangle_{S_i^A S_j^B} = \langle P_n^A\rangle_{S_i^A}\langle P_n^B\rangle_{S_j^B} \times e_{nm} Y_{nm}^{\text{mixed}}. \tag{13}$$

Though linear programs can be applied to Eqs. (12) and (13) to bound the single-photon yield Y_{11} and error yield $e_{11}Y_{11}$, one might note that in Eqs. (12) and (13), the yield is "mixed," that is, a mixture of signals that are slightly polarized [12]. However, in the key rate calculation, the "perfectly prepared single-photon" yield and error yield are required. From here, we denote them Y_{11}^{mixed} and Y_{11}^{perfect}. We argue that the bounds for the "mixed" quantities are actually the bounds for the "perfectly prepared" ones by explicitly writing and making comparisons to their density matrices [12].

For the single-photon yield Y_{11}, we find that the lower bound of the mixed single-photon yield term is actually the lower bound of the "perfect encoding state" [12]. Mathematically,

$$Y_{11}^{\text{mixed,Lower}} \le Y_{11}^{\text{mixed}} = Y_{11}^{\text{perfect}}. \tag{14}$$

More specifically, we prove that the mixed single-photon yield is actually equal to the perfectly encoded one. Therefore, lower bounds solved from linear programming can be used to calculate the key rate.

For the single-photon error yield $e_{11}Y_{11}$, the upper bound of the mixed error yield, $e_{11}Y_{11}^{\text{mixed}}$, is actually the upper bound of the "perfect encoding state" error yield, $e_{11}Y_{11}^{\text{perfect}}$ [12]:

$$e_{11}Y_{11}^{\text{mixed,Upper}} \ge e_{11}Y_{11}^{\text{mixed}} \ge e_{11}Y_{11}^{\text{perfect}}. \tag{15}$$

In this way, we can apply the linear programming technique to find the lower bound of the single-photon yield and the upper bound of the single-photon error rate and, subsequently, use them to calculate the key rate. Detailed derivations of the results in this section are given in Appendices C and D.

E. Key rate

The key rate for passive MDI QKD is given by [8,12,19]

$$\begin{aligned} R = P_Z^A P_Z^B \Big\{ &\langle P_1^A\rangle_{S_z}\langle P_1^B\rangle_{S_z} Y_{11}^{Z,\text{Lower,mixed}} \\ &\times \left[1 - h_2\left(e_{11}^{X,\text{Upper,mixed}}\right)\right] \\ &- f\,\langle Q_Z^{AB}\rangle_{S_z} h_2\left(\langle Q_Z^{AB}E_Z^{AB}\rangle_{S_z}/\langle Q_Z^{AB}\rangle_{S_z}\right)\Big\}, \end{aligned} \tag{16}$$

where $P_Z^{A/B}$ represents the probability for Alice or Bob to choose the key generation basis, the Z basis; $\langle P_1^{A/B}\rangle_{S_z}$

denotes the average probability for Alice or Bob to send a single-photon state in the key generation region; $Y_{11}^{Z,\mathrm{Lower,mixed}}$ is the lower bound of single-photon states in the X basis, found from linear programming; $e_{11}^{X,\mathrm{Upper,mixed}}$ is the upper bound of the error rate in the X basis; and Q_Z^{AB} and E_Z^{AB} are the Z-basis gain and QBER.

III. SIMULATED RESULTS

In this section, we show the simulated results of the key rate for asymptotic passive MDI QKD. In Fig. 3, we plot the key rate against communication distance for both an active and a passive MDI-QKD system. Both systems used three decoy settings. We see that the key rate of passive sources is 2–3 orders of magnitude lower than active MDI QKD. This difference is mainly due to the double-sifting nature of passive MDI QKD, where both Alice and Bob discarded many signals while doing postselection. In the result shown, the parameters t_3 and Δ_Z were optimized.

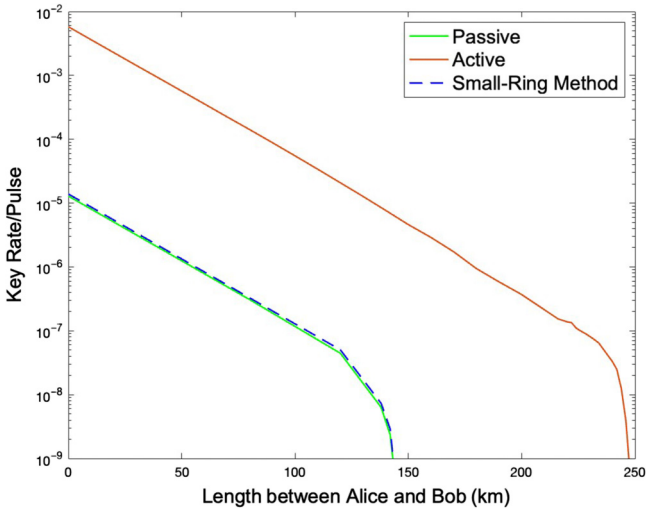

FIG. 3. Key rate of passive MDI QKD (green) and active MDI QKD (red), along with the key rate of the newly proposed method (dashed blue line; see Sec. IV). There is a misalignment of 1% (Alice and Bob 0.5% each) on the X-Z plane, and three decoy settings are used in both passive and active schemes. In the passive cases, Δ_Z is optimized within the range $[0.01, 0.05]$ and t_3 is optimized within the range $[0.1, 0.99]$. The other parameters used are fixed: $\Delta_{XY} = 0.2, \Delta_\phi = 0.2, t_1 = 0.02/u_{\max}, t_2 = 0.04/u_{\max}$. In the active case, the three intensities $[\mu, \nu, \omega]$ are used; all three intensities are optimized within the range $[0, 1.0]$. In both cases, we use a channel loss coefficient of 0.2 dB km^{-1} and a detector dark count of 10^{-6}. The passive MDI QKD's key rate is reasonable. It is about 2–3 orders of magnitude lower than the active one. However, it possesses the advantage of the removal of all source modulator side channels. In the "small-ring" method key rate calculation, the three decoy-state intensities used are the same as the passive one. We see an improvement in the key rate by about 6%.

But we chose fixed small values of $\Delta_{XY} = \Delta_\phi = 0.2$ [20]. Passive MDI QKD could reach a maximum communication distance of about 143 km. However, sacrificing some key rate performance, passive MDI QKD allows the removal of side channels from both source modulators and detectors.

IV. DISCUSSIONS

In this paper, we proposed a QKD scheme that implements the recently developed fully passive sources on MDI QKD—a passive MDI QKD that compromises some performance with the removal of all source modulator side channels. Recently, a fully passive TF QKD [17] was also proposed, which could also eliminate source modulator side channels. However, our protocol is easier to implement because it does not require a global phase reference. The key rate of passive MDI QKD is 2–3 orders of magnitude lower than active MDI QKD (see Fig. 3), mainly due to the double-sifting nature of the passive sources. Further efforts could be made to tackle the sifting problem, which could improve the key rate performance significantly. Meanwhile, an experimental realization of the proposed scheme is also planned in our subsequent research.

The protocol proposed in this paper differs from a typical MDI-QKD setup in that it involves the preparation of a fully passive source for both users. Note that here we still have to make a few assumptions about the practical preparation of the fully passive source [12]. (1) The phase of each pulse emitted must be random and uniformly distributed, and there is no correlation between consecutive pulses or between any two sources. (2) The classical detectors locally at Alice and Bob's site should give secure and accurate measurements of the intensities and polarization of the output states. (3) In addition to the remote Hong-Ou-Mandel interference between Alice and Bob, they need to achieve reliable interference between their local sources. Additionally, the passive scheme only removes side channels from active modulation devices, so one still needs to avoid potential side channels that might arise from the classical detectors and the fixed-pattern modulators [21].

Nonetheless, previous works have shown that the above-mentioned assumptions can either be successfully verified in experimental demonstrations or be bounded by a revised theoretical analysis. (1) Experimentally, previous works verified the phase uniformness and randomness, as well as the feasibility of achieving good interference, particularly using the aforementioned single-laser implementation [22,23]. (2) Theoretically, it has been shown [12,13] that, in principle, one could bound the security impact of phase measurement inaccuracy and intensity modulator leakage and obtain a lower bound on the key rate. (3) We can prevent the injection of strong light by Eve by using an optical isolator. Our passive sources and local detectors operate at

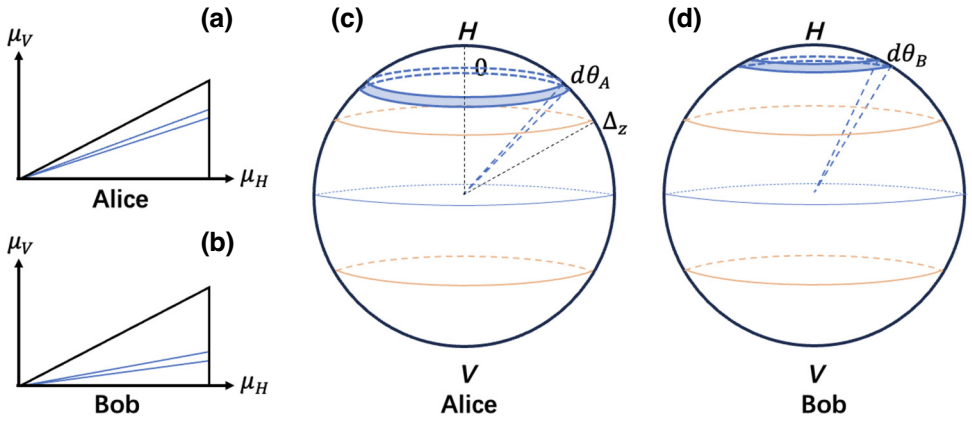

FIG. 4. An additional method that could improve the key rate. The key generation regions, H and V, are subdivided into smaller rings (shaded regions between dark blue lines), and the key rate of each "ring" is calculated and integrated together; see Eq. (17). Panels (a) and (b) show the ring's corresponding regions in $\mu_H - \mu_V$ space for Alice and Bob, respectively. Panels (c) and (d) show the rings on the Bloch spheres for Alice and Bob, respectively. The rings are labeled by the polar angle, θ, and have a thickness of $d\theta$. On Alice's Bloch sphere, the integration limits of Eq. (17), 0 and Δ_Z, are labeled. Bob's integration limits are the same.

classical strong light levels. So the injected but attenuated light from Eve will have negligible effect on the classical local detectors [12,13].

Also, our current work focuses on the asymptotic regime with infinite data sizes. While a rigorous finite-size analysis will be a subject of future studies, here we remark that, like for the BB84 protocol, our passive MDI-QKD scheme does not introduce any fundamental theoretical difference from standard MDI QKD that might prevent its standard finite-size analysis (such as Ref. [24]) from being applied to our scheme. (1) As discussed in Ref. [12], the passive selection of the intensity setting (i.e., photon-number distribution) introduces one more step before the selection of the actual photon number. This random two-step drawing still results in an identical and independent photon-number distribution for each signal. (2) Although the single-photon components in the X and Z bases both have mixed polarizations, they still average to fully mixed states and are mutually unbiased, so this does not prevent the random sampling assumption used commonly in finite-size analysis that bounds Z-basis phase errors with X-basis bit errors.

In terms of an estimation of the finite-size performance of our scheme, an X-basis slice size of $\Delta_{XY} = \Delta_\phi = 0.2$ can be selected, resulting in 0.022% of X-basis signals passing the postselection. By selecting moderately larger data sizes, for instance, of the order of 10^{12}, we could achieve similar levels of the limits of statistical fluctuation in active MDI QKD, which require a data size of the order of 10^{10} [25]. If we are willing to accept a decrease in key rate performance of approximately 35%, we can increase the values of Δ_{XY} and Δ_ϕ to 0.5. This expansion would result in a significant increase in X-basis signals, specifically from 0.022% to 0.42%. Consequently, we would be able to utilize a data size of approximately 10^{11} to achieve a comparable level of statistical fluctuation to that described in Ref. [25]. However, this is only an estimation, and the actual simulation of key rates under finite-size effects will be addressed in future work.

We propose one more method that could improve the key rate (Fig. 4). In this method, we divide the key generation regions (H and V regions) into small rings, which can in principle be infinitesimally small, and one can calculate the key rate of each ring. In other words, each ring is represented by a polar angle θ_{HV}; hence, the key rate of each ring is $R(\theta_{HV})$. One then integrates the key rates

$$R_{\text{improved}} = \int_0^{\Delta_Z}\int_0^{\Delta_Z} R(\theta_{HVA},\theta_{HVB}) \times p(\theta_{HVA})p(\theta_{HVB})d\theta_{HVA}d\theta_{HVB}, \tag{17}$$

where the limits of the integration are the key generation region and $p(\theta_{HV})$ is the marginal of the intensity probability distribution [Eq. (5)] in terms of the polar angle. Intuitively, one might obtain an improved key rate because we make use of more information. Some "rings" of too large of a θ_{HV} will have a too-big QBER, thus having a zero key rate. Using this method, those "zero key rate regions" would be excluded from the overall key rate calculation. However, while calculating the key rate of one bulk region, those regions would increase the QBER, while making no contribution to the key rate. Specifically, the privacy amplification term remains the same because the lower bound of the single-photon yield and upper bound of the single-photon error yield (from a decoy-state analysis) remains the same, so summing the privacy amplification term comes down to just summing the number of single photons [which is multiplied by a constant $Y_{11}^{Z,\text{Lower,mixed}}[1 - h_2(e_{11}^{X,\text{Upper,mixed}})]$], the total number of which is independent of the binning method. However,

less error correction is required for the small-ring method, because the binary entropy function is convex. Because of Jensen's inequality [26], the average of the entropy functions of respective errors in each ring is always less than the entropy function of the average error, $\langle h_2(E)\rangle < h_2(\langle E\rangle)$, thus making the small-ring method advantageous.

The key rate using this new method is shown in Fig. 3 (blue dashed line). Comparing it to the passive MDI-QKD key rate, we observe an improvement of about 6%. This method is applicable to all protocols that use fully passive sources, like the fully passive BB84 protocol [12], not just to MDI QKD.

Note added.—Recently, it has come to our attention that another work on fully passive MDI QKD is being prepared [27], which is independently completed from our work.

ACKNOWLEDGMENTS

We thank H. F. Chau, R. Wang, C. Hu, and X. Lin for helpful discussions. This project is financially supported by the University of Hong Kong start-up grant and NSERC. H.K.L. also acknowledges support from MITACS and Innovative Solutions Canada. W.W. acknowledges support from the Hong Kong RGC General Research Fund (GRF) and the University of Hong Kong Seed Fund for Basic Research for New Staff.

APPENDIX A: MDI QKD [8]

In 2012, a novel QKD scheme, termed MDI QKD, was introduced to remove all detector side channels [8].

Alice and Bob individually and randomly prepare one of the BB84 states using weak coherent pulse sources, transferring them to an untrusted third party, Charlie. Intensity modulators are applied to perform decoy-state analysis [9–11]. Charlie carries out a Bell state measurement (BSM), resulting in one of the Bell states as the outcome. Specifically, Charlie could arrange the measurement setup as depicted in Fig. 1 (Charlie's side), where the two signals received from Alice and Bob could be interfered with at a 50:50 BS, and at each end of the BS, a PBS could project the signal into either a horizontal or vertical polarization state. At the end of each path, there is an SPD. Charlie publicly broadcasts the successful detection results. If precisely two detectors' clicks are observed, it is counted as one successful BSM, yielding two different types of Bell states. If detectors $1H$ and $2V$ or $1V$ and $2H$ click, it signifies a projection on the singlet Bell state $|\psi^-\rangle$. If detectors $1H$ and $1V$, or $2H$ and $2V$ click, it indicates a projection on the triplet Bell state, $|\psi^+\rangle$ [8].

When Alice and Bob receive Charlie's measurement results, they keep only those light signals that correspond to the successful measurements. Then they postselect those signals where Alice and Bob both use the same basis [8]. The details of the implementation of MDI QKD can be found in Ref. [8].

Two bases are utilized separately: the rectilinear basis is employed for key generation, and the diagonal basis is used for testing. Consequently, the gain and QBER for the two bases should be calculated independently. The key rate is given by [8]

$$R = Q^{11}_{\text{rect}}[1 - H(e^{11}_{\text{diag}})] - Q_{\text{rect}} f\,(E_{\text{rect}}) H(E_{\text{rect}}), \quad \text{(A1)}$$

where $H(x) = -x\log(x) - (1-x)\log(1-x)$ is the Shannon entropy function.

APPENDIX B: DECOY-STATE ANALYSIS—LINEAR PROGRAMMING CONSTRUCTION [12]

In passive MDI QKD, the gain and error gain relations are

$$\begin{aligned}\langle Q\rangle_{S_i^A S_j^B} &= \sum_{n,m=0}^{\infty} \langle P_n^A P_m^B Y_{nm}\rangle_{S_i^A S_j^B},\\ \langle QE\rangle_{S_i^A S_j^B} &= \sum_{n,m=0}^{\infty} \langle P_n^A P_m^B e_{nm} Y_{nm}\rangle_{S_i^A S_j^B},\end{aligned} \quad \text{(B1)}$$

where S_i^A and S_j^B are postselection regions chosen by Alice and Bob, $P_n^{A/B}$ are Poisson distributions, and are functions of $(\mu_H^{A/B}, \mu_V^{A/B})$, and Y_{nm} or $e_{nm}Y_{nm}$ are functions of $(\mu_H^A, \mu_V^A, \phi_{HV}^A, \mu_H^B, \mu_V^B, \phi_{HV}^B)$, observables of both Alice and Bob. We can rewrite the coordinates in polar coordinates, (μ_H^A, μ_H^A) to (r^A, θ^A), and similarly for Bob. We denote ϕ_{HV}^A by ϕ^A.

We can now explicitly write

$$\begin{aligned}\langle P_n^A P_m^B Y_{nm}\rangle_{S_i^A S_j^B} &= \frac{1}{P^{\mu^A,\mu^B,\phi^A,\phi^B}_{S_i^A S_j^B}}\\ &\times \iiint \iiint_{S_i^A S_j^B} p_\mu^A(r^A,\theta^A) p_\mu^B(r^B,\theta^B) p_\phi^A(\phi^A) p_\phi^B(\phi^B)\\ &\times P_n^A(r^A,\theta^A) P_m^B(r^B,\theta^B)\\ &\times Y_{nm}(\theta^A,\phi^A,\theta^B,\phi^B) r^A r^B dr^A dr^B d\theta^A d\theta^B d\phi^A d\phi^B,\end{aligned} \quad \text{(B2)}$$

$$\begin{aligned}\langle P_n^A P_m^B e_{nm} Y_{nm}\rangle_{S_i^A S_j^B} &= \frac{1}{P^{\mu^A,\mu^B,\phi^A,\phi^B}_{S_i^A S_j^B}}\\ &\times \iiint \iiint_{S_i^A S_j^B} p_\mu^A(r^A,\theta^A) p_\mu^B(r^B,\theta^B) p_\phi^A(\phi^A) p_\phi^B(\phi^B)\\ &\times P_n^A(r^A,\theta^A) P_m^B(r^B,\theta^B) e_{nm} Y_{nm}(\theta^A,\phi^A,\theta^B,\phi^B)\\ &\times r^A r^B dr^A dr^B d\theta^A d\theta^B d\phi^A d\phi^B.\end{aligned} \quad \text{(B3)}$$

Note that here Y_{nm} depends on θ and ϕ, the polarization. Since Y_{nm} and $e_{nm}Y_{nm}$ are of similar form, from here, we

just focus on the calculation of Y_{nm}. The other one follows the same procedure. The following procedure is largely inspired by Wang *et al.* [12].

One could take out the integrals of the ϕ^A and ϕ^B parts:

$$\begin{aligned}\langle P_n^A P_m^B Y_{nm}\rangle_{S_i^A S_j^B} = \frac{1}{P_{S_i^A S_j^B}} \iint \iint_{S_i^A S_j^B} p_\mu^A(r^A,\theta^A) p_\mu^B(r^B,\theta^B) \\ \times P_n^A(r^A,\theta^A) P_m^B(r^B,\theta^B) \\ \times Y_{nm}(\theta^A,\theta^B) r^A r^B dr^A dr^B d\theta^A d\theta^B.\end{aligned} \tag{B4}$$

Here, we partially integrate Y_{nm} over ϕ^A, ϕ^B:

$$\begin{aligned}Y_{nm}(\theta^A,\theta^B) = \frac{1}{P^{\phi^A,\phi^B}_{S_i^A S_j^B}} \iint_{\phi^A,\phi^B} p_\phi^A(\phi^A) p_\phi^B(\phi^B) \\ \times Y_{nm}(\theta^A,\phi^A,\theta^B,\phi^B) d\phi^A d\phi^B.\end{aligned} \tag{B5}$$

From the above, we can rearrange the integrals by collecting terms related to $r^{A/B}$:

$$\begin{aligned}&\langle P_n^A P_m^B Y_{nm}\rangle_{S_i^A S_j^B} = \frac{1}{P_{S_i^A S_j^B}} \iint \iint_{S_i^A S_j^B} p_\mu^A(r^A,\theta^A) p_\mu^B(r^B,\theta^B) \\ &\times P_n^A(r^A,\theta^A) P_m^B(r^B,\theta^B) \\ &\times Y_{nm}(\theta^A,\theta^B) r^A r^B dr^A dr^B d\theta^A d\theta^B \\ &= \iint_{\theta^{A/B}} \left(\frac{\int_{r^A(\theta^A)} p_\mu^A(r^A,\theta^A) P_n^A(r^A,\theta^A) r^A dr^A}{P_{S_i^A}} \right) \\ &\times \left(\frac{\int_{r^B(\theta^B)} p_\mu^B(r^B,\theta^B) P_m^B(r^B,\theta^B) r^B dr^B}{P_{S_i^A}} \right) \\ &\times Y_{nm}(\theta^A,\theta^B) d\theta^A d\theta^B \\ &= \langle P_n^A\rangle_{S_i^A} \langle P_n^B\rangle_{S_j^B} \iint_{\theta^{A/B}} \frac{p_{\theta^A,n,S_i^A}(\theta^A)}{\langle P_n^A\rangle_{S_i^A}} \frac{p_{\theta^B,m,S_j^B}(\theta^A)}{\langle P_n^B\rangle_{S_j^B}} \\ &\times Y_{nm}(\theta^A,\theta^B) d\theta^A d\theta^B \\ &= \langle P_n^A\rangle_{S_i^A} \langle P_n^B\rangle_{S_j^B} \times Y^{\text{mixed}}_{nm,S_iS_j}.\end{aligned} \tag{B6}$$

Here

$$P_{S_i^A} = \iint_{S_i^A} p_\mu^A(r^A,\theta^A) r^A dr^A d\theta^A \tag{B7}$$

and

$$P_{S_i^A} P_{S_j^B} = P_{S_i^A S_j^B}, \tag{B8}$$

and we have set

$$p_{\theta^A,n,S_i^A}(\theta^A) = \frac{\int_{r^A(\theta^A)} p_\mu^A(r^A,\theta^A) P_n^A(r^A,\theta^A) r^A dr^A}{P_{S_i^A}} \tag{B9}$$

and [12]

$$\begin{aligned}Y^{\text{mixed}}_{nm,S_iS_j} = \iint_{\theta^{A/B}} \frac{p_{\theta^A,n,S_i^A}(\theta^A)}{\langle P_n^A\rangle_{S_i^A}} \frac{p_{\theta^B,m,S_j^B}(\theta^A)}{\langle P_n^B\rangle_{S_j^B}} \\ \times Y_{nm}(\theta^A,\theta^B) d\theta^A d\theta^B.\end{aligned} \tag{B10}$$

Up to this point, we have effectively decoupled the functions:

$$\langle P_n^A P_m^B Y_{nm}\rangle_{S_i^A S_j^B} = \langle P_n^A\rangle_{S_i^A} \langle P_n^B\rangle_{S_j^B} \times Y^{\text{mixed}}_{nm,S_iS_j}. \tag{B11}$$

However, linear programming is not yet applicable because $Y^{\text{mixed}}_{nm,S_iS_j}$ depends on the decoy regions $S_{i/j}$; therefore, $Y^{\text{mixed}}_{nm,S_iS_j}$ is not constant, so one could not bound them using linear programming.

To solve the problem, we cleverly construct a decoy setting so that the yield $Y^{\text{mixed}}_{nm}(\theta)$ is independent of the decoy settings, namely, it is consistent across all decoy settings so that a normal linear program can be used [12]. The key is to let Alice and Bob perform an additional postselection to "shape" the probability distribution into the desired form [12].

More concretely, for both Alice and Bob, they perform an additional postselection to make the overall probability distribution $p'_\mu = Ce^{r(\sin\theta+\cos\theta)}$ [12]. In this way, the exponential part in the Poisson term can be canceled out. Finally, we have [12]

$$Y^{\text{mixed}}_{nm} = \frac{\iint_{\theta^{A/B}} (\sin\theta^A + \cos\theta^A)^n (\sin\theta^B + \cos\theta^B)^m Y_{nm}(\theta^A,\theta^B) d\theta^A d\theta^B}{\iint_{\theta^{A/B}} (\sin\theta^A + \cos\theta^A)^n (\sin\theta^B + \cos\theta^B)^m d\theta^A d\theta^B}. \tag{B12}$$

Meanwhile, they also need to constrain the decoy regions to sector-shaped regions; see Fig. 2.

Now, the linear program can be written as

$$\langle Q\rangle_{S_i^A S_j^B} = \langle P_n^A\rangle_{S_i^A} \langle P_n^B\rangle_{S_j^B} \times Y^{\text{mixed}}_{nm}, \tag{B13}$$

and, similarly, for the error yield, we have

$$\langle QE\rangle_{S_i^A S_j^B} = \langle P_n^A\rangle_{S_i^A}\langle P_n^B\rangle_{S_j^B} \times e_{nm} Y_{nm}^{\text{mixed}}. \tag{B14}$$

APPENDIX C: DECOY-STATE ANALYSIS—YIELD BOUNDS [12]

We argue that the lower bounds of the "mixed" single-photon yield are actually those of the "perfectly encoding" yield:

$$Y_{11}^{\text{mixed,Lower}} \le Y_{11}^{\text{mixed}} = Y_{11}^{\text{perfect}}. \tag{C1}$$

In passive MDI QKD, we need both Alice and Bob to get an H state or a V state; we label the coordinates $\theta_{A/B}$ and $\phi_{A/B}$, respectively [12]. We should have the mixed state

$$\begin{aligned}\rho^{\text{mixed}} = {} & |H'H'\rangle\langle H'H'| + |H'V'\rangle\langle H'V'| \\ & + |V'H'\rangle\langle V'H'| + |V'V'\rangle\langle V'V'|.\end{aligned} \tag{C2}$$

We simplify the derivation by setting $\phi_A = 0$ and $\phi_B = \phi$, because the global phase does not really matter, and we set the global phase to Alice's phase so that $\phi_A = 0$.

Starting with the first term, we have

$$\begin{aligned}|H'H'\rangle &= |H'\rangle_A \otimes |H'\rangle_B \\ &= \left[\cos\left(\frac{\theta_A}{2}\right)|H\rangle_A + \sin\left(\frac{\theta_A}{2}\right)|V\rangle_A\right] \otimes \left[\cos\left(\frac{\theta_B}{2}\right)|H\rangle_B + e^{i\phi}\sin\left(\frac{\theta_B}{2}\right)|V\rangle_B\right].\end{aligned} \tag{C3}$$

The other terms follow similar constructions. Therefore, the density matrix

$$\begin{aligned}|H'H'\rangle\langle H'H'| = {} & \left[\cos\left(\frac{\theta_A}{2}\right)\cos\left(\frac{\theta_B}{2}\right), e^{-i\phi}\cos\left(\frac{\theta_A}{2}\right)\sin\left(\frac{\theta_B}{2}\right), \sin\left(\frac{\theta_A}{2}\right)\cos\left(\frac{\theta_B}{2}\right), e^{-i\phi}\sin\left(\frac{\theta_A}{2}\right)\sin\left(\frac{\theta_B}{2}\right)\right] \\ & \otimes \begin{pmatrix} \cos(\theta_A/2)\cos(\theta_B/2) \\ e^{i\phi}\cos(\theta_A/2)\sin(\theta_B/2) \\ \sin(\theta_A/2)\cos(\theta_B/2) \\ e^{i\phi}\sin(\theta_A/2)\sin(\theta_B/2) \end{pmatrix}.\end{aligned} \tag{C4}$$

Similarly, we can construct another basis

$$|H'V'\rangle\langle H'V'|, \tag{C5}$$

$$|V'H'\rangle\langle V'H'|, \tag{C6}$$

$$|V'V'\rangle\langle V'V'|; \tag{C7}$$

adding them all together, it is not hard to spot that the diagonal terms are all 1 and the nondiagonal terms are all 0. Hence, the whole matrix is a four-dimensional identity matrix:

$$\begin{aligned}\rho' &= |H'H'\rangle\langle H'H'| + |H'V'\rangle\langle H'V'| \\ &\quad + |V'H'\rangle\langle V'H'| + |V'V'\rangle\langle V'V'| \\ &= \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \\ &= I.\end{aligned} \tag{C8}$$

Note that we have used the trigonometry identity $\sin^2(x) + \cos^2(x) = 1$. Up to now, we have shown that the "mixed" state is actually a fully mixed state, I, so that it is equivalent to the "perfect encoding state," which is just

$$|HH\rangle\langle HH| + |HV\rangle\langle HV| + |VH\rangle\langle VH| + |VV\rangle\langle VV| = I. \tag{C9}$$

So, the "mixed" state and the "perfect" state, ρ^{perfect}, should share a lower bound. Hence, we could use the lower bound of Y_{nm}^{mixed}, denoted $Y_{nm}^{\text{mixed,Lower}}$, as the lower bound of the "perfectly encoded" state:

$$Y_{11}^{\text{mixed,Lower}} \le Y_{11}^{\text{mixed}} = Y_{11}^{\text{perfect}}. \tag{C10}$$

APPENDIX D: DECOY-STATE ANALYSIS—ERROR YIELD BOUNDS [12]

We only consider the HH state here (both Alice and Bob send an H state) [12]. We would like to compute

$$\begin{aligned}\rho^{HH} = {} & |H_1H_1^\perp\rangle\langle H_1H_1^\perp| + |H_1H_2^\perp\rangle\langle H_1H_2^\perp| \\ & + |H_2H_1^\perp\rangle\langle H_2H_1^\perp| + |H_2H_2^\perp\rangle\langle H_2H_2^\perp|,\end{aligned} \tag{D1}$$

where $|H_1H_1^\perp\rangle$ is $|H_1\rangle \otimes |H_1^\perp\rangle$, and we define $|H_1\rangle$ as just a "polarized" H state, which has the coordinate (θ_A, ϕ_A)

on the Bloch sphere. State $|H_1^{\perp}\rangle$ is the "pair state" with coordinate $(\theta_A, \phi_A + \pi)$. Similarly, states $|H_2\rangle$ and $|H_2^{\perp}\rangle$ are Bob's analog states, with coordinates (θ_B, ϕ_B) and $(\theta_B, \phi_B + \pi)$, respectively [12]. We again offset the phases so that Alice has no phase, and Bob simply has a ϕ phase.

Therefore, we can write down each of the four states in terms of

$$|H_1\rangle = \cos\left(\frac{\theta_A}{2}\right)|H\rangle_A + \sin\left(\frac{\theta_A}{2}\right)|V\rangle_A. \tag{D2}$$

The remaining three states can be written down in a similar form.

Hence, we could compute the terms, $|H_1H_1^{\perp}\rangle\langle H_1H_1^{\perp}|$,$|H_1H_2^{\perp}\rangle\langle H_1H_2^{\perp}|$, $|H_2H_1^{\perp}\rangle\langle H_2H_1^{\perp}|$,$|H_2H_2^{\perp}\rangle\langle H_2H_2^{\perp}|$ individually. They should each be a 4×4 matrix.

Adding them up, we end up with the matrix

$$\rho = \begin{pmatrix} \cos^2\left(\frac{\theta_A}{2}\right)\cos^2\left(\frac{\theta_B}{2}\right) & & & \\ & \cos^2\left(\frac{\theta_A}{2}\right)\sin^2\left(\frac{\theta_B}{2}\right) & & \\ & & \sin^2\left(\frac{\theta_A}{2}\right)\cos^2\left(\frac{\theta_B}{2}\right) & \\ & & & \sin^2\left(\frac{\theta_A}{2}\right)\sin^2\left(\frac{\theta_B}{2}\right) \end{pmatrix}. \tag{D3}$$

We could rewrite the matrix as a combination of states:

$$\begin{aligned} \rho = & \left[\cos^2\left(\frac{\theta_A}{2}\right) - \sin^2\left(\frac{\theta_A}{2}\right)\right]\left[\cos^2\left(\frac{\theta_B}{2}\right)\sin^2\left(\frac{\theta_B}{2}\right)\right]\begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \\ & + \left[\cos^2\left(\frac{\theta_A}{2}\right) - \sin^2\left(\frac{\theta_A}{2}\right)\right]\sin^2\left(\frac{\theta_B}{2}\right)\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \\ & + \left[\cos^2\left(\frac{\theta_B}{2}\right) - \sin^2\left(\frac{\theta_B}{2}\right)\right]\sin^2\left(\frac{\theta_A}{2}\right)\begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix} + \sin^2\left(\frac{\theta_A}{2}\right)\sin^2\left(\frac{\theta_B}{2}\right)\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \\ = & \left[\cos^2\left(\frac{\theta_A}{2}\right) - \sin^2\left(\frac{\theta_A}{2}\right)\right]\left[\cos^2\left(\frac{\theta_B}{2}\right)\sin^2\left(\frac{\theta_B}{2}\right)\right](|HH\rangle\langle HH|) \\ & + \left[\cos^2\left(\frac{\theta_A}{2}\right) - \sin^2\left(\frac{\theta_A}{2}\right)\right]\sin^2\left(\frac{\theta_B}{2}\right)(|H\rangle\langle H|_A \otimes I_B) \\ & + \left[\cos^2\left(\frac{\theta_B}{2}\right) - \sin^2\left(\frac{\theta_B}{2}\right)\right]\sin^2\left(\frac{\theta_A}{2}\right)(I_A \otimes |H\rangle\langle H|_B) + \sin^2\left(\frac{\theta_A}{2}\right)\sin^2\left(\frac{\theta_B}{2}\right)(I_A \otimes I_B). \end{aligned} \tag{D4}$$

We note that the last three terms all have a QBER of 50%, and we also note that the first term is the "perfect" encoding state, which must have a smaller QBER than the "mixed" state [12].

For the H state alone (for both Alice and Bob), if we integrate over all possible pairs of polarized states [12], each has a density matrix like Eq. (D4), the overall density matrix for the HH scenario (when Alice has an H state and

Bob has an H state) would be the sum of some sort of mixture [the latter three terms in Eq. (D4)] and the perfectly encoding state [the first term in Eq. (D4)]. The mixture terms have a QBER of 50%, Therefore, we conclude that

$$e_{11}Y_{11}^{\text{mixed}} \geq e_{11}Y_{11}^{\text{perfect}}; \tag{D5}$$

similar reasoning applies for the VV, HV, and VH states. A similar argument could be proved for the $++$, $--$, $+-$, and $-+$ states in the X basis.

In conclusion, the upper bound of the mixed state, $e_{nm}Y_{nm}^{\text{mixed,Upper}}$, which can be obtained from linear programming, is indeed the upper bound of the "perfect" state, eY^{perfect}:

$$e_{11}Y_{11}^{\text{mixed,Upper}} \geq e_{11}Y_{11}^{\text{mixed}} \geq e_{11}Y_{11}^{\text{perfect}}. \tag{D6}$$

APPENDIX E: CHANNEL MODEL

The signals immediately coming out from Alice's fully passive source are described by four DOFs, $(\mu_A, \theta_{HVA}, \phi_{HVA}, \phi_{\text{global},A})$, and a similar set for Bob. The signals can be slightly polarized after they travel through the channel. Writing the Bloch sphere state in terms of coordinates [12]

$$\vec{s}_A = (\sin\theta_{HVA}\cos\phi_{HVA}, \sin\theta_{HVA}\sin\phi_{HVA}, \cos\theta_{HVA}). \tag{E1}$$

This polarization rotation is described by Rodrigues' formula [18]

$$\vec{s'}_A = \cos\alpha\vec{s} + \sin\alpha(\vec{r}\times\vec{s}) + (\vec{s}\cdot\vec{r})(1-\cos\alpha)\vec{r}, \tag{E2}$$

where α is the rotation angle and $\vec{r}$ is the rotation axis (unit length). We can then convert the coordinate back into the Bloch sphere coordinates $\{\mu'_A, \theta'_{HVA}, \phi'_{HVA}, \phi'_{GA}\}$, where the superscripts denote postrotation. It is worth noting that the global phase is also rotated; however, it does not affect the physics—it will eventually be integrated over.

The former two postrotation parameters for Alice (μ_A, θ'_{HVA}) can be reconverted into H and V leg intensities, (μ'_{HA}, μ'_{VA}). Considering the channel loss and detector efficiency, the intensity arriving at the detectors becomes $\mu'_{HA} \to \mu'_{HA}\eta = \mu'_{HA}\eta_L\eta_d = \mu'_{HA}10^{-\alpha L/10}\eta_d$, where α is the loss coefficient, typically about 0.2 dB/km, and η_d is the detector efficiency. The other intensities follow the same format.

The postrotation signals travel through the channels and arrive at the 50:50 BS for interference. The interference can be partitioned into H and V components, each adhering to the interference formula

$$|\sqrt{\mu_1}e^{i\phi_1}\rangle_a|\sqrt{\mu_2}e^{i\phi_2}\rangle_b \to$$
$$|\sqrt{\mu_1/2}e^{i\phi_1} + i\sqrt{\mu_2/2}e^{i\phi_2}\rangle_c|i\sqrt{\mu_1/2}e^{i\phi_1} + \sqrt{\mu_2/2}e^{i\phi_2}\rangle_d. \tag{E3}$$

We can derive the output intensity for leg c as

$$\mu_1/2 + \mu_2/2 - \sqrt{\mu_1\mu_2}\sin(\phi), \tag{E4}$$

where ϕ represents the phase difference between the two signals. Meanwhile, the output intensity for leg d is given by

$$\mu_1/2 + \mu_2/2 + \sqrt{\mu_1\mu_2}\sin(\phi). \tag{E5}$$

The intensities applied here are μ'_{HA}, μ'_{HB} and μ'_{VA}, μ'_{VB} for the H and V interferences, respectively. For the H leg, the phase difference used is $\phi'_{HA} - \phi'_{HB} = \phi'_R$. For the V leg, the phase difference is determined by $\phi'_{VA} - \phi'_{VB} = \phi'_R + \phi'_{HVA} - \phi'_{HVB}$. Using the formula, we can compute the intensities reaching detectors $3H$ and $4H$ from the H leg interference, as well as the $3V$ and $4V$ intensities from the V leg interference.

Because the phase differences ϕ'_R and $\phi'_R + \phi'_{HVA} - \phi'_{HVB}$ are randomized, in order to calculate the average gain, one needs to integrate the phases from 0 to 2π; this explains the phase integration in Eq. (3). The phase integration should also be separate for H and V; however, the phase difference in the V interference is also a function of ϕ'_R. Therefore, to derive the average gain, it suffices to integrate ϕ'_R from 0 to 2π.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

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

[5] J. E. Bourassa, A. Gnanapandithan, L. Qian, and H.-K. Lo, Measurement-device-independent quantum key distribution with passive time-dependent source side channels, Phys. Rev. A **106**, 062618 (2022).

[6] K. ichiro 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).

[7] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).
[8] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[9] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[10] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).
[11] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[12] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Fully passive quantum key distribution, Phys. Rev. Lett. **130**, 220801 (2023).
[13] V. Zapatero, W. Wang, and M. Curty, A fully passive transmitter for decoy-state quantum key distribution, Quantum Sci. Technol. **8**, 025014 (2023).
[14] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution, Opt. Lett. **34**, 3238 (2009).
[15] M. Curty, X. Ma, B. Qi, and T. Moroder, Passive decoy-state quantum key distribution with practical light sources, Phys. Rev. A **81**, 022310 (2010).
[16] T. Hahn, Cuba–a library for multidimensional numerical integration, Comput. Phys. Commun. **168**, 78 (2005).
[17] W. Wang, R. Wang, and H.-K. Lo, Fully-passive twin-field quantum key distribution, arXiv:2304.12062.
[18] R. Friedberg, Rodrigues, olinde: "des lois géométriques qui régissent les déplacements d'un système solided'ots", translation and commentary, arXiv:2211.07787.
[19] F. Xu, M. Curty, B. Qi, and H. K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).
[20] In principle, in the asymptotic regime, one can choose arbitrarily small Δ_{XY} and Δ_{ϕ} to obtain the highest key rate. However, here we used reasonably small values of 0.2 (considering that one has to obtain a reasonable data size after the postselection). The other reason is that choosing too-small slice sizes often result in numerical instability, since one has to perform numerical integrations over very small regions simultaneously for Alice's and Bob's sources.
[21] As proposed in Ref. [12], one can use an intensity modulator with a fixed pattern combined with delays to simulate the effect of four laser sources with just a single laser source, which makes it easier to maintain good interference visibility.
[22] C. Hu, W. Wang, K.-S. Chan, Z. Yuan, and H.-K. Lo, Proof-of-principle demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110801 (2023).
[23] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Experimental demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110802 (2023).
[24] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).
[25] R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. L. Yuan, and A. J. Shields, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Inf. **7**, 58 (2021).
[26] J. L. W. V. Jensen, Sur les fonctions convexes et les inégalités entre les valeurs moyennes, Acta Math. **30**, 175 (1906).
[27] X. Wang, F.-Y. Lu, Z.-H. Wang, Z.-Q. Yin, S. Wang, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Fully passive measurement device independent quantum key distribution, arXiv:2309.07576.