Measurement-device-independent quantum key distribution with asymmetric sources

Jia-Ju Deng,[1,2,*] Feng-Yu Lu,[1,2,3,*] Zhen-Qiu Zhong,[1,2,3] Xiao-Hai Zhan,[1,2,3] Zhen-Qiang Yin,[1,2,3,†] Shuang Wang,[1,2,3,‡] Wei Chen,[1,2,3] De-Yong He,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[3] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Received 24 April 2025; revised 30 July 2025; accepted 18 September 2025; published 15 October 2025)

Measurement-device-independent quantum key distribution (MDI QKD), which eliminates all the attacks from the eavesdropper to the measurement party, has been one of the most promising technologies for the implementation of end-to-end quantum networks. In practice, the asymmetry of both sources and channels is generally inevitable. Therefore, we propose a theory to analyze the performance when any two MDI users in networks communicate using asymmetric sources in distinct single or multiple temporal modes. As a specific application, we model to obtain the key rate of MDI QKD with a weak-coherent pulse source and a spontaneous parametric down-conversion source, and compare the performance to the cases with symmetric (i.e., identical) sources. The result demonstrates that the actual performance does not degrade due to the asymmetry of sources. On the contrary, it maintains at a good level over the entire distance we study. This work provides a theoretical basis for analyzing and optimizing MDI-QKD networks with asymmetric sources, thus paving the way for the practical deployment of completely asymmetric MDI-QKD networks.

DOI: 10.1103/zw9s-ywd6

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] has achieved enormous development in the past 40 years. The inherent security of QKD originates from the principle of quantum mechanics [4–7], and thus it allows two remote users, Alice and Bob, to exchange secret keys with information-theoretical security. Moreover, QKD is the fundamental step towards the future quantum Internet [8–12].

Although this technology is theoretically secure, practical implementations of QKD inherently suffer from device imperfections, which lead to potential security risks. Measurement-device-independent (MDI) QKD [13] allows an untrusted third party to perform measurements and announces the results, which eliminates all the attacks from the eavesdropper to the measurement party [14]. MDI QKD is mature and easy to implement, so it has been studied worldwide with numerous remarkable achievements in theory and experiment [15–40]. Particularly, in MDI-QKD networks, the star topology is quite suitable, in which the measurement unit is located at the central relay [28,41,42]. Therefore, MDI QKD is a promising scheme for metropolitan networks [28,43,44], and simultaneously an achievable and specific solution for upgrading the trusted repeater quantum network [10,41].

However, these studies share a common limitation that they assume symmetric channels and symmetric (i.e., identical) sources. In practical networks, it is unreasonable and impossible to require all users to distribute symmetrically at equal distances around the relay, and inconvenient for network users to employ customized transmitters with the same parameters. The countermeasure against asymmetry channels has been solved by separately choosing intensities to compensate for different channel loss [16,45,46]. Nevertheless, research on asymmetric source communication, that is, communication using sources with distinct waveforms in the frequency domain, is still lacking. In previous work on quantum interference [47–51], the case of multiple photons is ignored or avoided. And their theories only give the two-fold coincidence probability, without considering the polarization degree of freedom. Simultaneously, it is challenging to extend the theoretical framework

*These authors contributed equally to this work.
†Contact author: yinzq@ustc.edu.cn
‡Contact author: wshuang@ustc.edu.cn

 © 2025 American Physical Society

to include such information. Besides, how distinct multiple temporal modes (see Appendix A for a specific concept) match is still an unanswered question. All these problems are obstacles to the construction of the MDI-QKD model with asymmetric sources.

Now in this paper, we propose an alternative theory to analyze how two parties communicate with asymmetric sources in the MDI-QKD protocol, and attempt to extend the protocol to the fully asymmetric scenario, refer to Fig. 1. This theory studies the interference of multiple photons in different temporal modes on beam splitter (BS). In this process, polarization information can be naturally contained. Generally, for two arbitrary light fields with given wave functions in time or frequency domain, it can be used to obtain the final state after BS. In principle, this advantage allows us to perform the theoretical analysis and optimization of the lower bound of the key rate in MDI QKD with any asymmetric sources. Furthermore, we decouple the intensity and the wave function of a practical signal, so the method of enhancing the key rate with asymmetric channels proposed in Ref. [16] is still effective. It is noted that the theoretical framework we proposed can provide valuable theoretical fundamentals for implementing the practical large-scale quantum network, in which users usually hold diverse sources in communications. Based on this, we can experimentally optimize the parameter settings to attain the key rate nearly as high as the simulation result.

This paper is structured as follows. In Sec. II, we first introduce the theory of the interference of two single photons in different single modes, then we extend the method to the multimode case, and give several examples as verification. In Sec. III, as a specific application, we consider the communication scenario where one party uses a weak-coherent pulse (WCP) source and the other uses a spontaneous parametric down-conversion (SPDC) source. We start from a simplified scheme of the experiment setup, then we give some details in this protocol and the simulation result, the curves of key rate versus distance and data size. Simultaneously, we fix the detection efficiency and dark count at the measurement party, and compare this result with the key rates when both parties use identical WCP sources and use identical SPDC sources. Finally, we construct a hypothetical case where the experiment parameters are attempted without the theoretical guidance. We arbitrarily choose several fixed parameters to compare the performance of this system with the optimized one.

II. INTERFERENCE THEORY OF MULTIPLE TEMPORAL MODES

Although there has been extensive studies [47–51] on the Hong-Ou-Mandel interference [52] between a pair of photons in different modes on the 50:50 BS, these studies share a common limitation that they consider only a single photon on a path, or even a single mode. Therefore, we propose an alternative general quantum interference theory to calculate the output results after BS.

In this section, we first introduce from the single-mode case, and then extend the conclusion to the multimode case. Finally, we simply verify this theory through several examples with experimental evidence.

A. Single-mode interference

First, we define the creation operator in the temporal mode (TM) $\psi(\omega)$ [47,53]:

$$\hat{a}_{\psi}^{\dagger} = \int \mathrm{d}\omega \psi(\omega)\hat{a}^{\dagger}(\omega), \tag{1}$$

where the wave function in frequency domain $\psi(\omega)$ is probability normalized, i.e., $\int \mathrm{d}\omega|\psi(\omega)|^2 = 1$. See Appendix A for the specific concept of "temporal modes." This expression can be seen as the coherent superposition of the single-photon state around the frequency ω. In other words, a single photon can be "created" around the frequency ω with the probability $|\psi(\omega)|^2\mathrm{d}\omega$.

Now we consider a creation operator in mode φ. Generally, $\hat{a}_{\psi}^{\dagger}$ and $\hat{a}_{\varphi}^{\dagger}$ do not commute. Similar to the method used in Ref. [50,51], we define

$$\begin{aligned} c &= \langle 1,\psi|1,\varphi\rangle = \langle 0|\hat{a}_{\psi}\hat{a}_{\varphi}^{\dagger}|0\rangle \\ &= \int \mathrm{d}\omega \int \mathrm{d}\omega' \psi^*(\omega)\varphi(\omega')\langle 0|\hat{a}(\omega)\hat{a}^{\dagger}(\omega')|0\rangle \\ &= \int \mathrm{d}\omega \psi^*(\omega)\varphi(\omega) \end{aligned} \tag{2}$$

as the description of their temporal overlap, formulated using Eq. (A2). Similarly, it can be calculated that

$$\begin{aligned} [\hat{a}_{\psi},\hat{a}_{\varphi}^{\dagger}] &= \int \mathrm{d}\omega \int \mathrm{d}\omega' \psi^*(\omega)\varphi(\omega')[\hat{a}(\omega),\hat{a}^{\dagger}(\omega')] \\ &= \int \mathrm{d}\omega \psi^*(\omega)\varphi(\omega) = c. \end{aligned} \tag{3}$$

Now we can decompose $\hat{a}_{\varphi}^{\dagger}$ into components "parallel" and "orthogonal" to $\hat{a}_{\psi}$, that is,

$$\hat{a}_{\varphi}^{\dagger} = c\hat{a}_{\psi}^{\dagger} + \sqrt{1-|c|^2}\hat{a}_{\perp}^{\dagger}. \tag{4}$$

We prove the following three properties of the "orthogonal" component $\hat{a}_{\perp}^{\dagger}$ below.

(1) **Commutativity** $\hat{a}_{\psi}$ and $\hat{a}_{\perp}^{\dagger}$ commute:

$$\begin{aligned} [\hat{a}_{\psi},\hat{a}_{\perp}^{\dagger}] &= (1-|c|^2)^{-1/2}[\hat{a}_{\psi},\hat{a}_{\varphi}^{\dagger} - c\hat{a}_{\psi}^{\dagger}] \\ &= (1-|c|^2)^{-1/2}(c - c\times 1) = 0. \end{aligned} \tag{5}$$

(2) **Orthogonality** $\hat{a}_{\perp}^{\dagger}|0\rangle$ is orthogonal to $\hat{a}_{\psi}^{\dagger}|0\rangle$:

$$\begin{aligned}\langle 1,\psi|1,\perp\rangle &= (1-|c|^2)^{-1/2}\langle 0|\hat{a}_{\psi}(\hat{a}_{\varphi}^{\dagger}-c\hat{a}_{\psi}^{\dagger})|0\rangle \\ &= (1-|c|^2)^{-1/2}(c-c\times 1)=0. \end{aligned} \tag{6}$$

(3) **Canonical commutation relation**

$$\begin{aligned}[\hat{a}_{\perp},\hat{a}_{\perp}^{\dagger}] &= (1-|c|^2)^{-1}[\hat{a}_{\varphi}-c^{*}\hat{a}_{\psi},\hat{a}_{\varphi}^{\dagger}-c\hat{a}_{\psi}^{\dagger}] \\ &= (1-|c|^2)^{-1}(1-c^{*}\times c-c\times c^{*}+|c|^2\times 1) \\ &= 1. \end{aligned} \tag{7}$$

Based on these three properties above, we conclude that operators $\hat{a}_{\psi}^{\dagger}$ and $\hat{a}_{\perp}^{\dagger}$ are creation operators in distinct Hilbert spaces. This conclusion explains why the states obtained after TM decomposition are product states.

It should be emphasized that $\hat{a}_{\perp}^{\dagger}$ is defined from two modes $\psi(\omega)$ and $\varphi(\omega)$. In other words, we do not care about whether $\hat{a}_{\perp}^{\dagger}$ contains any other modes $\phi(\omega)$. Even if $\phi(\omega)$ is concluded, the three properties proved above remain correct.

B. Multimode interference

In this subsection, we generalize the distinct single-mode decomposition method from the previous subsection to the multimode case. Let $\{\psi_n(\omega)\}_{n=1}^{N}$ and $\{\varphi_n(\omega)\}_{n=1}^{N}$ be two sets of orthonormal function bases, and

$$\hat{A}_{\boldsymbol{\psi}}^{\dagger}=\sum_{\mathbf{n}=0}^{\infty}\alpha_{\mathbf{n}}\prod_{i=1}^{N}\left(\hat{a}_{\psi,i}^{\dagger}\right)^{n_i}, \tag{8}$$

$$\hat{A}_{\boldsymbol{\varphi}}^{\dagger}=\sum_{\mathbf{n}=0}^{\infty}\beta_{\mathbf{n}}\prod_{i=1}^{N}\left(\hat{a}_{\varphi,i}^{\dagger}\right)^{n_i} \tag{9}$$

are two multimode creation operators, where

$$\hat{a}_{\psi,i}^{\dagger}=\int \mathrm{d}\omega\psi_i(\omega)\hat{a}^{\dagger}(\omega), \tag{10}$$

$$\hat{a}_{\varphi,i}^{\dagger}=\int \mathrm{d}\omega\varphi_i(\omega)\hat{a}^{\dagger}(\omega) \tag{11}$$

are the creation operators of each mode; $\mathbf{n}=(n_1,\ldots,n_N)$ means there are n_i photons in the ith mode; $\boldsymbol{\psi}$ and $\boldsymbol{\varphi}$, respectively, represent the set $\{\psi_n(\omega)\}_{n=1}^{N}$ and $\{\varphi_n(\omega)\}_{n=1}^{N}$.

Note that the so-called "single-mode decomposition" actually involves two TMs, ψ and $\perp$, then the approach is to express each basis function in set $\{\varphi_n(\omega)\}_{n=1}^{N}$ as a linear combination of the basis functions in another set $\{\psi_n(\omega)\}_{n=1}^{N}$, that is, to connect the two sets of basis functions via a unitary transformation matrix $\mathbf{c}$: $\boldsymbol{\varphi}(\omega)=\mathbf{c}\boldsymbol{\psi}(\omega)$.

Another view is that we can decompose $\hat{a}_{\perp,i}^{\dagger}$ step by step (let $\hat{a}_{\perp,0}^{\dagger}=\hat{a}_{\varphi,j}^{\dagger}$). Now we can rewrite $\hat{A}_{\boldsymbol{\varphi}}^{\dagger}$:

$$\begin{aligned}\hat{A}_{\boldsymbol{\varphi}}^{\dagger} &= \sum_{\mathbf{n}=0}^{\infty}\beta_{\mathbf{n}}\prod_{i=1}^{N}\left(\sum_{j=1}^{N}c_{ij}\hat{a}_{\psi,j}^{\dagger}\right)^{n_i} \\ &= \sum_{\mathbf{n}=0}^{\infty}\beta_{\mathbf{n}}\prod_{i=1}^{N}n_i!\sum_{\|\mathbf{m}_i\|_1=n_i}\prod_{j=1}^{N}\frac{(c_{ij}\hat{a}_{\psi,j}^{\dagger})^{m_{ij}}}{m_{ij}!}, \end{aligned} \tag{12}$$

where multinomial theorem and Eq. (A2) has been applied in the last line, and now $\hat{A}_{\boldsymbol{\varphi}}^{\dagger}$ can be expressed as the form similar to Eq. (8). In particular, if $\hat{A}_{\boldsymbol{\varphi}}^{\dagger}$ has a more simplified expression, such as the displacement operator of coherent state, we do not have to perform Taylor series expansion on it. A simpler approach is to directly decompose the creation operators of this simplified form.

It should be emphasized that the equivalence in the number of basis functions between sets $\{\psi_n(\omega)\}_{n=1}^{N}$ and $\{\varphi_n(\omega)\}_{n=1}^{N}$ is imposed solely to simplify the summation notation; this is not a strict requirement in practice.

When interference occurs, coherent interference emerges exclusively between $\psi_n(\omega)$ within the same mode, while no cross-mode coherent interference takes place. The resultant state manifests as a product state of independently interfered modes.

C. Several HOM interference examples

We make three assumptions about the experimental structure of HOM interference: (1) the transformation on the creation operators by BS [54]

$$\hat{a}^{\dagger}\xrightarrow{\text{BS}}\frac{\hat{a}^{\dagger}+\hat{b}^{\dagger}}{\sqrt{2}}, \tag{13}$$

$$\hat{b}^{\dagger}\xrightarrow{\text{BS}}\frac{\hat{a}^{\dagger}-\hat{b}^{\dagger}}{\sqrt{2}} \tag{14}$$

acts exclusively on the spatial (here path-encoded) modes, leaving other degrees of freedom (TMs, polarization modes, etc.) unaffected [50]. Therefore, the polarization compatibility of our theory is natural; (2) the dark counts of the detectors a and b, with detection efficiency η_1 and η_2, respectively, are both zero; (3) all incident photons share identical polarization.

Additionally, the last assumption is included only for simplicity in the following discussion. If polarization information is needed, a polarization degree of freedom independent of the temporal mode can be attached to the creation operator. A specific polarization-involved interference result can be seen in Sec. III.

1. Single-photon single-mode interference

As a simple introduction, we consider the case that there is only a single photon in TM ψ in path a, while another single photon in TM φ in path b. Then we can decompose the creation operation in path b:

$$\hat{b}_{\varphi}^{\dagger} = c\hat{b}_{\psi}^{\dagger} + \sqrt{1-|c|^2}\hat{b}_{\perp}^{\dagger}, \tag{15}$$

where $c = \langle 0|\hat{b}_{\psi}\hat{b}_{\varphi}^{\dagger}|0\rangle$. The input state can be written as

$$\begin{aligned}|\Psi_{\text{in}}\rangle &= |1,\psi\rangle_a\,|1,\varphi\rangle_b = \hat{a}_{\psi}^{\dagger}\hat{b}_{\varphi}^{\dagger}\,|0\rangle \\ &= \hat{a}_{\psi}^{\dagger}(c\hat{b}_{\psi}^{\dagger} + \sqrt{1-|c|^2}\hat{b}_{\perp}^{\dagger})\,|0\rangle\,.\end{aligned} \tag{16}$$

Then the output state after BS is

$$\begin{aligned}|\Psi_{\text{out}}\rangle = \Bigg[& c\frac{(\hat{a}_{\psi}^{\dagger})^2 - (\hat{b}_{\psi}^{\dagger})^2}{2} + \sqrt{1-|c|^2} \\ & \times \frac{\hat{a}_{\psi}^{\dagger} + \hat{b}_{\psi}^{\dagger}}{\sqrt{2}}\frac{\hat{a}_{\perp}^{\dagger} - \hat{b}_{\perp}^{\dagger}}{\sqrt{2}}\Bigg]|0\rangle\,.\end{aligned} \tag{17}$$

The state containing coincident count events is

$$|\Psi_{\text{coin}}\rangle = \frac{\sqrt{1-|c|^2}}{2}\left(\hat{a}_{\perp}^{\dagger}\hat{b}_{\psi}^{\dagger} - \hat{a}_{\psi}^{\dagger}\hat{b}_{\perp}^{\dagger}\right)|0\rangle\,, \tag{18}$$

and the corresponding coincidence probability is

$$\begin{aligned}P(\text{coin}) &= \eta_1\eta_2\,\langle\Psi_{\text{coin}}|\Psi_{\text{coin}}\rangle = \frac{\eta_1\eta_2}{2}(1-|c|^2) \\ &= \frac{\eta_1\eta_2}{2}\left(1 - \int \mathrm{d}\omega_1\psi^*(\omega_1)\varphi(\omega_1)\right. \\ &\quad \left.\times \int \mathrm{d}\omega_2\psi(\omega_2)\varphi^*(\omega_2)\right).\end{aligned} \tag{19}$$

If $\eta_1 = \eta_2 = 100\%$, this result is consistent with the result in Ref. [47,51].

2. Multiphoton single-mode interference

Now we consider the coherent sources α in mode ψ and β in mode φ, and the corresponding displacement operator is denoted as $\hat{D}_{a,\psi}(\alpha)$ and $\hat{D}_{b,\varphi}(\beta)$. Similarly, we decompose the initial state in path b:

$$\begin{aligned}|\beta,\varphi\rangle_b &= \hat{D}_{b,\varphi}(\beta)\,|0\rangle = \exp(\beta\hat{b}_{\varphi}^{\dagger} - \beta^*\hat{b}_{\varphi})\,|0\rangle \\ &= \exp\Big([(\beta c\hat{b}_{\psi}^{\dagger} - \text{H.c.}) \\ &\quad + (\beta\sqrt{1-|c|^2}\hat{b}_{\perp}^{\dagger} - \text{H.c.})]\Big)\,|0\rangle \\ &= \hat{D}_{b,\psi}(\beta c)\hat{D}_{b,\perp}(\beta\sqrt{1-|c|^2})\,|0\rangle \\ &= |\beta c,\psi\rangle_b\,|\beta(1-|c|^2)^{-1/2},\perp\rangle_b\,,\end{aligned} \tag{20}$$

where Baker-Campbell-Hausdorff formula [54] and Eq. (5) has been applied in the third line. For an intuitive description of asymmetry reflected by c, we assume Gaussian-shaped $\psi(\omega)$ and $\varphi(\omega)$:

$$\psi(\omega) = \frac{1}{\pi^{1/4}\sigma_1^{1/2}}\mathrm{e}^{-(\omega-\omega_1)^2/2\sigma_1^2}, \tag{21}$$

$$\varphi(\omega) = \frac{1}{\pi^{1/4}\sigma_2^{1/2}}\mathrm{e}^{-(\omega-\omega_2)^2/2\sigma_2^2}, \tag{22}$$

where σ_i^2 is twice the variance. Particularly, if there exists a time delay τ between these two spectra $\psi(\omega)$ and $\varphi(\omega)$, the latter (or former) one should be revised into $\varphi(\omega)\mathrm{e}^{\mathrm{i}\omega\tau}$. By definition,

$$\begin{aligned}c &= \int \psi^*(\omega)\varphi(\omega)\mathrm{e}^{\mathrm{i}\omega\tau}\,\mathrm{d}\omega \\ &= \exp\left[-\frac{(\Delta\omega)^2 + \sigma_1^2\sigma_2^2\tau^2}{2(\sigma_1^2+\sigma_2^2)}\right]\exp\left[\mathrm{i}\frac{\sigma_2^2\omega_1 + \sigma_1^2\omega_2}{\sigma_1^2+\sigma_2^2}\tau\right],\end{aligned} \tag{23}$$

where $\Delta\omega = \omega_2 - \omega_1$. As the difference between two central frequency and the delay increase, the coefficient c reflecting overlap will decrease exponentially. For given and fixed nonzero $\Delta\omega$ and τ, it can be proved that $|c| \leqslant \exp(-\Delta\omega\tau/2)$ with equality if and only if $\sigma_1 = \sigma_2 = \sqrt{\Delta\omega/\tau}$. In extreme asymmetric case, c will severely degrade to zero, where no interference occurs.

The output state can be written as

$$\begin{aligned}|\Psi_{\text{out}}\rangle = &\left|\frac{\alpha+\beta c}{\sqrt{2}},\psi\right\rangle_a\left|\frac{\alpha-\beta c}{\sqrt{2}},\psi\right\rangle_b \\ &\bigotimes\left|\beta\sqrt{\frac{1-|c|^2}{2}},\perp\right\rangle_a\left|-\beta\sqrt{\frac{1-|c|^2}{2}},\perp\right\rangle_b.\end{aligned} \tag{24}$$

Let

$$\begin{aligned}\mu_a &= \frac{|\alpha+\beta c|^2}{2} + |\beta|^2\frac{1-|c|^2}{2}, \\ \mu_b &= \frac{|\alpha-\beta c|^2}{2} + |\beta|^2\frac{1-|c|^2}{2}.\end{aligned} \tag{25}$$

Because mode ψ is independent of mode $\perp$, based on Eq. (B2) and Eq. (B5), the probability that there exist n_i $(i = a,b)$ photons in path i is

$$P_i(n_i) = \frac{1}{n_i!}\frac{\partial^{n_i}}{\partial z^{n_i}}\mathrm{e}^{(z-1)\mu_i}\Big|_{z=0} = \mathrm{e}^{-\mu_i}\frac{\mu_i^{n_i}}{n_i!}. \tag{26}$$

When n_i photons are incident on the detector, the click probability [55] is $P_{n_i}(\text{click}) = 1-(1-\eta)^{n_i}$. So the coincidence probability is

$$\begin{aligned} P(\text{coin}) &= \sum_{m=0}^{\infty} P_a(m)[1-(1-\eta_1)^m] \\ &\quad \times \sum_{n=0}^{\infty} P_b(n)[1-(1-\eta_2)^n] \\ &= \left(1-\mathrm{e}^{-\eta_1\mu_a}\right)\left(1-\mathrm{e}^{-\eta_2\mu_b}\right). \end{aligned} \tag{27}$$

If the coherent states input in two paths are completely indistinguishable, i.e., $|c|=1$, then $\mu_a = |\alpha+\beta|^2/2$, $\mu_b = |\alpha-\beta|^2/2$, and thereby

$$P(\text{coin})\big|_{|c|=1} = (1-\mathrm{e}^{-\eta_1|\alpha+\beta|^2/2})(1-\mathrm{e}^{-\eta_2|\alpha-\beta|^2/2}), \tag{28}$$

where we attribute the phase of c to β. If they are completely distinguishable, i.e., $c=0$, then $\mu_a = \mu_b = (|\alpha|^2+|\beta|^2)/2$, and thereby

$$\begin{aligned} P(\text{coin})\big|_{c=0} &= \left[1-\mathrm{e}^{-\eta_1(|\alpha|^2+|\beta|^2)/2}\right] \\ &\quad \times \left[1-\mathrm{e}^{-\eta_2(|\alpha|^2+|\beta|^2)/2}\right]. \end{aligned} \tag{29}$$

These two results are consistent with the result in Ref. [56].

3. Single-photon multimode interference

We consider the interference of a pair of entangled photons generated in the SPDC process, which is detailed in Appendix A. Given by Ref. [47,48], the initial state can be written as

$$\begin{aligned} |\Psi_{\text{in}}\rangle &= \int \mathrm{d}\omega_s \int \mathrm{d}\omega_i f(\omega_s,\omega_i)\hat{a}_s^\dagger(\omega_s)\hat{a}_i^\dagger(\omega_i)\,|0\rangle \\ &= \sum_{m=1}^{N} \sqrt{\lambda_m}\hat{a}_{\psi,m}^\dagger \hat{b}_{\varphi,m}^\dagger\,|0\rangle\,, \end{aligned} \tag{30}$$

where Eqs. (A5)–(A7) has been applied in the last line. The next step is to introduce a unitary transformation matrix $\mathbf{c}$ to decomposition $\hat{b}_{\varphi,m}^\dagger$:

$$\hat{b}_{\varphi,m}^\dagger = \sum_{n=1}^{N} c_{mn}\hat{b}_{\psi,n}^\dagger, \tag{31}$$

where $c_{mn} = \langle 0|\hat{b}_{\psi,n}\hat{b}_{\varphi,m}^\dagger|0\rangle$. At this time, the initial state can be rewritten as

$$|\Psi_{\text{in}}\rangle = \sum_{m,n=1}^{N} c_{mn}\sqrt{\lambda_m}\hat{a}_{\psi,m}^\dagger \hat{b}_{\psi,n}^\dagger\,|0\rangle\,. \tag{32}$$

Note that now $\hat{a}_{\psi,n}^\dagger$ and $\hat{b}_{\psi,n}^\dagger$ are in the same TM, for simplicity, we omit the subscript ψ. After BS, the final state and the containing coincident count events are

$$|\Psi_{\text{out}}\rangle = \sum_{m,n=1}^{N} c_{mn}\sqrt{\lambda_m}\frac{\hat{a}_m^\dagger+\hat{b}_m^\dagger}{\sqrt{2}}\frac{\hat{a}_n^\dagger-\hat{b}_n^\dagger}{\sqrt{2}}\,|0\rangle\,, \tag{33}$$

$$|\Psi_{\text{coin}}\rangle = \frac{1}{2}\sum_{m,n=1}^{N} c_{mn}\sqrt{\lambda_m}(\hat{a}_n^\dagger\hat{b}_m^\dagger - \hat{a}_m^\dagger\hat{b}_n^\dagger)\,|0\rangle\,. \tag{34}$$

Therefore, for ideal detectors ($\eta_1=\eta_2=100\%$), the coincidence probability is

$$\begin{aligned} P(\text{coin}) &= \langle\Psi_{\text{coin}}|\Psi_{\text{out}}\rangle \\ &= \frac{1}{2}\sum_{m,n,k,l=1}^{N} c_{mn}^* c_{kl}\sqrt{\lambda_m\lambda_k}(\delta_{mk}\delta_{nl}-\delta_{nk}\delta_{ml}) \\ &= \frac{1}{2}\left(\sum_{m=1}^{N}\lambda_m\sum_{n=1}^{N}|c_{mn}|^2 - \sum_{m,n=1}^{N} c_{mn}^* c_{nm}\sqrt{\lambda_m\lambda_n}\right) \\ &= \frac{1}{2} - \frac{1}{2}\sum_{m,n=1}^{N}\sqrt{\lambda_m\lambda_n}\int \mathrm{d}\omega_1\psi_n(\omega_1)\varphi_m^*(\omega_1) \\ &\quad \times \int \mathrm{d}\omega_2\psi_m^*(\omega_2)\varphi_n(\omega_2) \\ &= \frac{1}{2} - \frac{1}{2}\int \mathrm{d}\omega_1 \int \mathrm{d}\omega_2 \sum_{m=1}^{N}\sqrt{\lambda_m}\psi_m^*(\omega_2)\varphi_m^*(\omega_1) \\ &\quad \times \sum_{n=1}^{N}\sqrt{\lambda_n}\psi_n(\omega_1)\varphi_n(\omega_2) \\ &= \frac{1}{2} - \frac{1}{2}\int \mathrm{d}\omega_1 \int \mathrm{d}\omega_2 f^*(\omega_2,\omega_1)f(\omega_1,\omega_2), \end{aligned} \tag{35}$$

where the unitary property of matrix $\mathbf{c}$ has been applied in the third line. This result is consistent with the result in Ref. [47,48].

III. MDI QKD WITH ASYMMETRIC SOURCES

In this section, we formally analyze the asymmetric MDI-QKD protocol where the two communication parties use a WCP source and a SPDC source, respectively. First, we introduce an experimental setup for implementation. Secondly, we decompose the coherent state in the TMs of the signal photons from certain SPDC source, and calculate the interference result. Thirdly, we consider the finite-size effect, which introduce statistic fluctuations, leading to lower key rate and necessarily more optimization parameters. Finally, we present a comparative analysis of the key

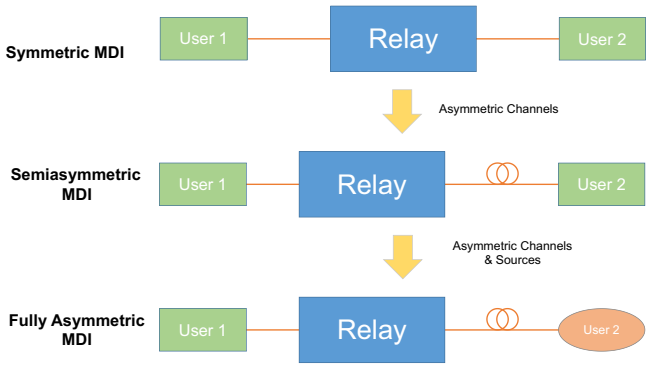


FIG. 1. Scheme of the evolution of the asymmetric MDI QKD. The structure at the top is the typical symmetric MDI QKD, in which two users have identical sources and distribute at equal distances. The next structure shows that the distances from the two users to the relay differ. Now we take this asymmetry of MDI QKD a step further: we consider that the sources of the two users are asymmetric. This is what the structure at the bottom demonstrates.

rate simulations for symmetric WCP sources, symmetric SPDC sources, and asymmetric sources mentioned above.

A. Expected experimental structure

According to the experimental setup in Ref. [57], we give a simplified scheme of the structure in Fig. 2. To facilitate simulation, we assume that the probability normalized laser waveform of in the frequency domain is independent of the laser intensity. Therefore, the waveform of the WCP source and the pump pulse in the SPDC process are the same, which is assumed to be Gaussian shaped:

$$\alpha_0(\omega) = \frac{1}{\pi^{1/4}\sigma^{1/2}} \exp\left[-\frac{(\omega-\bar{\omega})^2}{2\sigma^2}\right]. \tag{36}$$

The Gaussian filter is used to suppress noise and obtain higher spectral purity [58], whose mathematical form is

$$F_n(\omega) = \exp\left[-2^{2n-1}\ln 2\left(\frac{\omega-\omega_0}{\omega_{\mathrm{FWHM}}}\right)^{2n}\right], \tag{37}$$

where n is a positive integer and ω_{FWHM} is the full width at half power, i.e., $|F_n(\pm\omega_{\mathrm{FWHM}}/2)|^2 = 1/2$. The final waveform of WCP source and SPDC source are $\alpha(\omega) = \alpha_0(\omega)F(\omega)$ and $g(\omega_s,\omega_i) = f(\omega_s,\omega_i)F_s(\omega_s)F_i(\omega_i)$, respectively.

B. Interference of WCP source and SPDC source

As a specific example of the MDI QKD with asymmetric sources, we let the signal photons from an SPDC source and coherent photons interfere on BS. It is the interference of single-mode photons and multimode photons. We choose the TMs of signal photons shown in Eq. (A3) as a

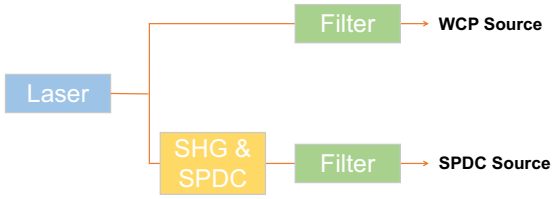


FIG. 2. A simplified scheme of experimental setup. The emitted pulse laser beam is split into two components: one is utilized as the WCP source after a Gaussian filter, while the other is employed as the pump pulse in the SPDC process. SHG means second-harmonic generation process. These two beams are then subjected to MDI-QKD protocol implementation, with interference occurring at a 50:50 BS.

set of orthonormal function bases. From Eqs. (12) and (20), the initial state of the WCP source can be decomposed into

$$|\alpha\rangle_b = \bigotimes_{i=1}^{N} |\alpha c_i\rangle_b, \tag{38}$$

where

$$c_i = \langle 0|\hat{b}_{\psi,i}\hat{b}_\alpha^\dagger|0\rangle = \int \mathrm{d}\omega \psi_i^*(\omega)\alpha(\omega). \tag{39}$$

We assume that the dark count rate d_S and detection efficiency η_S of the detectors at the measurement party (Charlie) of the MDI-QKD protocol are also identical. In such a case, we can attribute the detection efficiency to the channel loss [59], and the PND of n photons and the probability of $\mathbf{k}$ photons after the channel are

$$P_\mu(n) = \frac{1}{n!}\frac{\partial^n}{\partial z^n}\prod_{i=1}^{N} \mathrm{e}^{(z-1)|\alpha c_i|^2}\Big|_{z=0} = \mathrm{e}^{-\mu}\frac{\mu^n}{n!}, \tag{40}$$

$$\begin{aligned} f_\mu(\mathbf{k}) &= \sum_{\mathbf{m}\geqslant\mathbf{k}}\prod_{i=1}^{N}\binom{m_i}{k_i}\eta_S^{k_i}(1-\eta_S)^{m_i-k_i}P_i(m_i) \\ &= \mathrm{e}^{-\eta_S\mu}\prod_{i=1}^{N}\frac{(\eta_S\mu_i)^{k_i}}{k_i!}, \end{aligned} \tag{41}$$

where $\mu_i = |\alpha c_i|^2$ and $\mu = |\alpha|^2 = \sum_{i=1}^{N}\mu_i$. See Appendix C for the detailed derivation process of these two results above.

C. Optimization with finite-size effect

We use the general framework for multimode-photon interference proposed in Ref. [60], and apply the three-intensity decoy-state method [61,62] to get the overall gain and quantum bit error rate (QBER) in rectilinear (or Z) and

diagonal (or X) bases, respectively. In practice, the number of communication rounds N are experimentally finite, then the finite-size effect, essentially the statistic fluctuation, should be considered.

First, the product of the calculated total data size N and the overall gain Q corresponds to the counts of successful events measured in the experiment; and the product of N and QBER E corresponds to the number of error bits. We denote μ, ν as the intensities from two parties, Alice and Bob. Because the formulas [13]

$$Q_{\mu\nu} = \sum_{m,n=0}^{\infty} P_\mu(m) P_\nu(n) Y_{mn}, \tag{42}$$

$$E_{\mu\nu} Q_{\mu\nu} = \sum_{m,n=0}^{\infty} P_\mu(m) P_\nu(n) Y_{mn} e_{mn} \tag{43}$$

are applicable only to asymptotic cases, that is, the size of data is infinite. Therefore, we must estimate the lower and upper bound of the expected value $E(X)$ with the measured value X [63]:

$$E^L(X,\xi) = \frac{X}{1+\delta_1(X,\xi)}, \tag{44}$$

$$E^U(X,\xi) = \frac{X}{1-\delta_2(X,\xi)}, \tag{45}$$

where δ_1, δ_2 satisfy the following equations:

$$\delta_1 - (1+\delta_1)\left[\ln(1+\delta_1) + \frac{\ln\xi}{X}\right] = 0, \tag{46}$$

$$\delta_2 + (1-\delta_2)\left[\ln(1-\delta_2) + \frac{\ln\xi}{X}\right] = 0, \tag{47}$$

where ξ is the failure probability.

Consider that $Y_{mn}, e_{mn} < 1$, we set a cutoff number of photons $N_{\max}$, then the linear programming problem is

$$\begin{aligned} 0 < Q_{\mu\nu} - \sum_{m,n=0}^{N_{\max}} P_\mu(m) P_\nu(n) Y_{mn} \\ < 1 - \sum_{m,n=0}^{N_{\max}} P_\mu(m) P_\nu(n), \end{aligned} \tag{48}$$

$$\begin{aligned} 0 < E_{\mu\nu} Q_{\mu\nu} - \sum_{m,n=0}^{N_{\max}} P_\mu(m) P_\nu(n) Y_{mn} e_{mn} \\ < 1 - \sum_{m,n=0}^{N_{\max}} P_\mu(m) P_\nu(n). \end{aligned} \tag{49}$$

After we obtain the lower bound of the expected value of Y_{11} and the upper bound of the expected value of $Y_{11}e_{11}$, it should be noted that the experimentally measured values still exhibit statistical fluctuations relative to the expected values. So we use the Chernoff bound [63] to estimate a lower Y_{11} and a higher $Y_{11}e_{11}$:

$$O^U(Y,\xi) = [1+\delta_1'(Y,\xi)]Y, \tag{50}$$

$$O^L(Y,\xi) = [1-\delta_2'(Y,\xi)]Y, \tag{51}$$

where O is the observed value, $Y = E(O)$ is the expected value, and δ_1', δ_2' satisfy the following equations:

$$\delta_1' - (1+\delta_1')\ln(1+\delta_1') - \frac{\ln\xi}{Y} = 0, \tag{52}$$

$$\delta_2' + (1-\delta_2')\ln(1-\delta_2') + \frac{\ln\xi}{Y} = 0. \tag{53}$$

Finally, we obtain the key rate as conservative as possible in the experiment.

D. Simulation results

In this subsection, we give a clear comparison curve of key rates from different sources. We denote W as WCP source and S as SPDC source. To determine the proportion of each mode in the SPDC source, we consider the down-conversion process 532 nm $\rightarrow$ 1064 nm + 1064 nm. For simplicity and intuitiveness, we assume phase matching. The standard deviation of the Gaussian-shaped pump pulse is 5 ps, and the FWHM of the filter $\omega_{\text{FWHM}} = 600$ GHz. The frequency spectrum and the corresponding spectrum of the first and second modes have been shown in Fig. 6.

In simulation, we set $\eta_S = 60\%$, $d_S = 10^{-6}$ for Charlie, and $\eta_I = 90\%$, $d_I = 10^{-6}$ for both Alice and Bob; the loss per kilometer is $\alpha = 0.2$ dB/km; the misalignment error is $e_d = 1.5\%$; the failure probability when estimating Chernoff bound is $\xi = 10^{-7}$; the cutoff number of photons in linear programming is $N_{\max} = 6$.

We optimize the intensities of decoy and signal states ν, μ, respectively, and the four probabilities that Alice and Bob choose μ or ν in Z or X basis. The parameters to be optimized amount to 6 in symmetric W-W and S-S communications, and 12 in W-S communication. We apply the particle swarm optimization (PSO) method to obtain the initial (i.e., lossless) global optimal point. As channel loss increases, an improved search algorithm is applied, and each point to be optimized starts with the previous optimal value. Based on Gottesman-Lo-Lütkenhaus-Preskill (GLLP) formula [64], the key rate formula [63] we utilize is

$$\begin{aligned} R \geqslant p^Z_{\mu_A} p^Z_{\mu_B} \{ P_{\mu_A}(1) P_{\mu_B}(1) Y^Z_{11} [1 - H_2(e^X_{11})] \\ - Q^Z_{\mu_A\mu_B} f(E^Z_{\mu_A\mu_B}) H(E^Z_{\mu_A,\mu_B}) \}, \end{aligned} \tag{54}$$

where $p^Z_{\mu_A}$ and $p^Z_{\mu_B}$ denote the probability that Alice and Bob choose signal state in Z basis, respectively; $H_2(x) =$

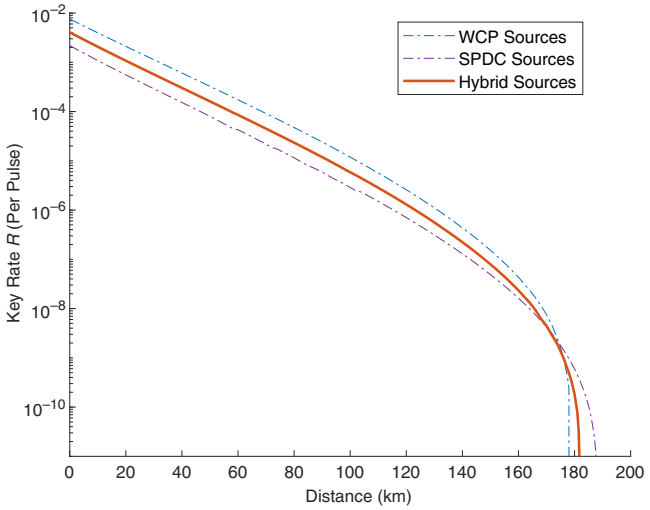


FIG. 3. This figure shows the key rates variation with distance between Alice and Bob. The blue dashdot line, purple dashdot line and the red solid line represent *W*-*W*, *S*-*S*, and *W*-*S* communications, respectively. We set the data size $N_{\text{tot}} = 10^{12}$.

$-x\log_2 x-(1-x)\log(1-x)$ is the binary Shannon entropy; Y_{11}^Z and e_{11}^X denote the single-photon yield in Z basis and QBER in X basis, which can be seen as the phase error in Z basis; $Q_{\mu_A\mu_B}^Z$ and $E_{\mu_A\mu_B}^Z$ denote the overall gain and QBER in Z basis; $f\,(E_{\mu_A\mu_B}^Z)\approx 1.16$ is an inefficiency function for the error-correction process [13]. The simulation results are in Fig. 3 and 4.

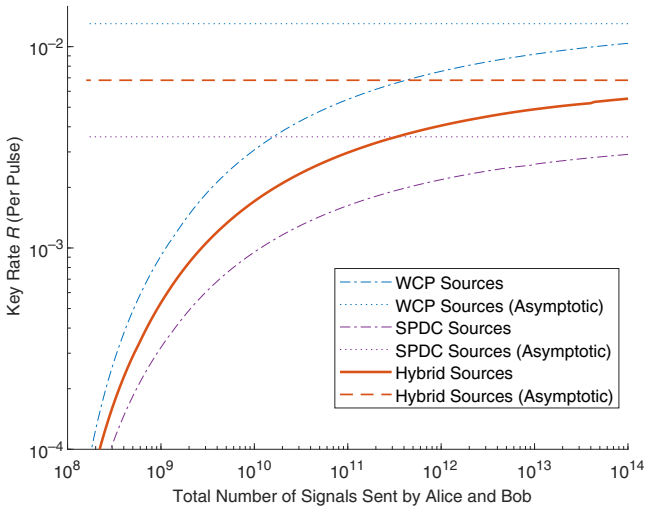


FIG. 4. This figure shows the key rates' variation with the total number of signals sent by Alice and Bob, ranging from 10^8 to 10^{14}. The blue dashdot line, purple dashdot line, and the red solid line represent *W*-*W*, *S*-*S*, and *W*-*S* communications, respectively. And the blue dotted line, purple dotted line, and the red dashed line represent the corresponding asymptotic key rates. We set the detection efficiency $\eta_S = 60\%$.

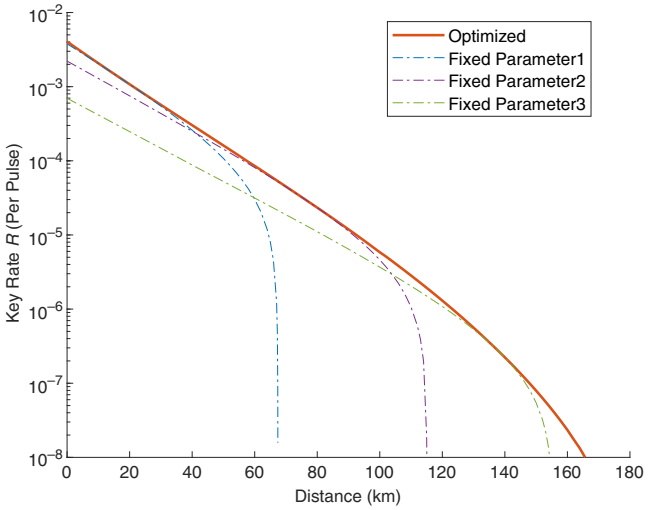


FIG. 5. This figure shows the key rates variation with distance from Alice to Bob. The red solid line, blue dashdot line, green dashdot line and purple dashdot line represent the key rates optimized and calculated in three arbitrarily given parameters, respectively. All simulation parameters remain unchanged. The fixed parameters we choose are from the optimal parameters at distances of 20 km, 80 km, and 140 km.

Figure 3 demonstrates that at low loss, the single-photon yield Y_{11} plays a dominant role in GLLP formula. Since the heralded single-photon source (here, an SPDC source) requires joint response monitoring with local detectors, its single-photon yield in Z basis Y_{11}^Z reduces. Consequently, the key rates of *W*-*W*, *W*-*S*, and *S*-*S* communications decrease sequentially. As the loss increases, the number of successful events decreases, and the effect of QBER becomes gradually significant. At this point, if the local detector triggers, the probability of vacuum emitted by signal or decoy state is equal to d_I, which is tiny, thus lowering the QBER. Therefore, at a long distance, the key-rate result is exactly the opposite. Overall, *W*-*S* communication combines the features of the WCP source and the SPDC source, which manifests not quite low key rate over the entire selected distance range.

Figure 4 demonstrates that the variation of the data size does not affect the relative relationship of the key rates in different communications (at least at low loss). And the overall growth trends of all key rates are similar, slowing when the data size exceeds 10^{12}.

In addition, we choose the tenth, fortieth, and seventieth optimal parameters, that is, parameters at distances of 20, 80, and 140 km (see Appendix E), and fix them at any distance. That is the reason why the optimal curve and each of the curves with fixed parameters Fig. 5 have an intersection. The result shows that, if we conduct the experiment of MDI QKD with asymmetric sources without this theoretical guidance, the performance at short or long distance

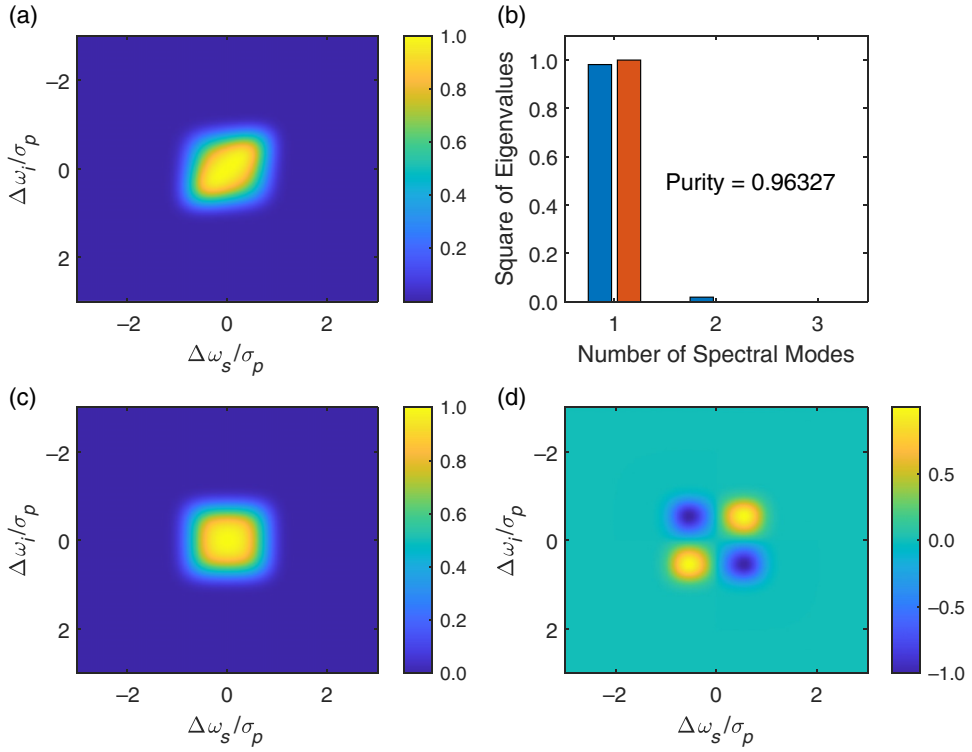


FIG. 6. We consider a simple case of phase matching (i.e., $\Delta k = 0$) and use Gaussian filters $F(\omega)$ to suppress noise, that is, the JSA is now $f(\omega_s, \omega_i) = \alpha(\omega_s + \omega_i)\, F_s(\omega_s) F_i(\omega_s)$. The specific expression of Gaussian filters is shown in Sec. III A. For Gaussian-shaped $\alpha(\omega)$, (a) shows the JSA relative to its maximum value; (b) shows the mode proportion comparison between SPDC source (blue bar) and WCP source (orange bar), in which the purity of the SPDC source is defined as $\sum_{i=1}^{N} \lambda_i^2$. The "multiple modes" of coherent state originates from the decomposition under the modes of SPDC source; (c),(d) show the first and second mode of the JSA to their maximum values after Schmidt decomposition.

becomes significantly worse. Besides, all the cut-off distances with fixed parameters fall far short of the optimized cut-off distance.

At the end of the main text, we consider the practical scene and make a brief discussion. In principle, any type of data postprocessing could not rebuild the detailed original information of the two spectra $\psi(\omega)$ and $\varphi(\omega)$. Actually, c eliminates the details of two spectra, yet all observables relate to c at most. In other words, it is impossible to deduce the specific waveforms of the frequency spectra from these observables. In fact, the thing to be most concerned about is not the spectra themselves, but their differences (or overlaps), that is, the coefficient $c = \int \psi^*(\omega)\varphi(\omega)\mathrm{d}\omega$.

Since our expression is general with no assumption, for local test, we can estimate the expected visibility according to our priori knowledge on or parameters of the apparatus in advance, or directly conduct a simple interference experiment. If it is feasible experimentally, we can go further considering the possible performance in QKD.

For practical and large-scale applications, we believe that users usually have no approach for local test. Therefore, fundamental information such as the trusted ranges of waveform, central wavelength (ideally Gaussian, or typically Lorentzian) and linewidth should be provided by the device suppliers. Before two users connect, the communication relay estimates the most conservative performance and distributes corresponding extra sources.

IV. CONCLUSION

In summary, we propose a general theory of quantum networks for analyzing and optimizing the interference of any different sources in different temporal modes. This method would be the theoretical basis for addressing the key-rate degradation due to the asymmetry of sources in future applications.

As a practical application, this theory demonstrates the performance of *W*-*W*, *S*-*S*, and *W*-*S* communications. This result demonstrates that the features of the asymmetric sources from both parties are reflected in the key rate. It means that the asymmetry of sources might not be an obstacle for the implementation of quantum networks. Furthermore, this theory manifests that for better performance, it may be a possible scheme to modulate two sources to make their TMs match.

ACKNOWLEDGMENTS

This work has been supported by the National Natural Science Foundation of China (Grants No. 62171424, 62425507, No. 62271463, No. 62301524, No. 62105318, and No. 61961136004), the Fundamental Research Funds for the Central Universities, the China Postdoctoral Science Foundation (Grant No. 2022M723064), Natural Science Foundation of Anhui (Grant No. 2308085QF216), and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300700).

DATA AVAILABILITY

The data that support the findings of this article are not publicly available. The data are available from the authors upon reasonable request.

APPENDIX A: BASIC PRINCIPLE OF SPDC SOURCE

In this section, we will give an introduction to the basic principle of SPDC source and the photon number distribution (PND) of this entanglement source. Starting form the Maxwell's equations, the effective interaction Hamiltonian of the SPDC process has been given in Ref. [65] in detail. Considering that the effective Hamiltonian of the SPDC process has been studied widely [58,60,66–69], here we only care about the specific mathematical form of the effective Hamiltonian:

$$\hat{H}_I = C\int \mathrm{d}\omega_s \int \mathrm{d}\omega_i f\left(\omega_s,\omega_i\right)\hat{a}_s^{\dagger}(\omega_s)\hat{a}_i^{\dagger}(\omega_i) + \mathrm{H.c.}, \tag{A1}$$

where C is a constant, ω_x $(x = s, i)$ are the frequency of the signal and idler photons, respectively, and $\hat{a}_x^{\dagger}(\omega_x)$ are the corresponding creation operators at the frequency ω_x, which satisfy the commutative relation

$$[\hat{a}_x(\omega_x), \hat{a}_y^{\dagger}(\omega_y')] = \delta_{x,y}\delta(\omega_x - \omega_y'). \tag{A2}$$

In particular, the joint spectral amplitude (JSA) $f\left(\omega_s,\omega_i\right)$ reflect the probability amplitude of this entangled photon pair in frequency, which can be expressed as

$$f\left(\omega_s,\omega_i\right) = \alpha(\omega_s+\omega_i)\Phi(\omega_s,\omega_i), \tag{A3}$$

where $\alpha(\omega)$ is the pump envelope function, and $\Phi(\omega_s,\omega_i)$ is the phase-matching function [66]. $\alpha(\omega_s+\omega_i)$, $\Phi(\omega_s,\omega_i)$ reflect the conservation conditions of energy and momentum, respectively. In a uniformly polarized nonlinear crystal,

$$\Phi(\omega_s,\omega_i) = \mathrm{sinc}\frac{\Delta k(\omega_s,\omega_i)L}{2}\exp\left(\mathrm{i}\frac{\Delta k(\omega_s,\omega_i)L}{2}\right), \tag{A4}$$

where $\Delta k = k_s(\omega_s) + k_i(\omega_i) - k_p(\omega_p)$.

Now we choose the JSA to be probability normalized, i.e., $\int\int \mathrm{d}\omega_s\mathrm{d}\omega_i|f\left(\omega_s,\omega_i\right)|^2 = 1$, and then apply the Schmidt decomposition [70] to Eq. (A3):

$$f\left(\omega_s,\omega_i\right) = \sum_{n=1}^{\infty}\sqrt{\lambda_n}\psi_n(\omega_s)\varphi_n(\omega_i), \tag{A5}$$

where $\{\psi_n(\omega)\}_{n=1}^{\infty}$ and $\{\varphi_n(\omega)\}_{n=1}^{\infty}$ are two sets of orthonormal bases. Intuitive results of these spectra are shown in Fig. 6. In fact, the eigenvalues $\{\lambda_n\}_{n=1}^{\infty}$, which satisfy $\sum_{n=1}^{\infty}\lambda_n = 1$, decay rapidly with the subscript n for SPDC source, we usually set a cutoff mode number N. This expression reflects the inherent entanglement properties of SPDC sources. Law *et al.* [70] named $\{\psi_n(\omega)\}_{n=1}^{N}$ and $\{\varphi_n(\omega)\}_{n=1}^{N}$ as the "temporal modes" (TMs) of signal and idler photons as early as 2000, after that numerous research on TMs of SPDC sources has emerged [53,71–73]. From this perspective, we can regard JSA as the coherent superposition of these TMs. For a given subscript n, $\psi_n(\omega)$, or $\varphi_n(\omega)$ represent a frequency-domain wave function.

From Eq. (A5), we can define effective single-mode field operators by

$$\hat{a}_n^{\dagger} = \int \mathrm{d}\omega_s\psi_n(\omega_s)\hat{a}_s^{\dagger}(\omega_s), \tag{A6}$$

$$\hat{b}_n^{\dagger} = \int \mathrm{d}\omega_i\varphi_n(\omega_i)\hat{a}_i^{\dagger}(\omega_i). \tag{A7}$$

It is easy to see from Eq. (A2) that

$$[\hat{a}_m, \hat{a}_n^{\dagger}] = [\hat{b}_m, \hat{b}_n^{\dagger}] = \delta_{mn}. \tag{A8}$$

We assume that the initial state is vacuum state, then the finial state after evolution time t [67] is

$$\begin{aligned}|\Psi\rangle &= \exp\left(\frac{\hat{H}_I}{\mathrm{i}\hbar}\right)|0\rangle \\ &= \bigotimes_{n=1}^{N}\exp\left[\frac{C}{\mathrm{i}\hbar}\left(\sqrt{\lambda_n}\hat{a}_n^{\dagger}\hat{b}_n^{\dagger} + \mathrm{H.c.}\right)\right]|0\rangle .\end{aligned} \tag{A9}$$

Let $\eta_k = \mathrm{i}C\sqrt{\lambda_k}/\hbar$, and denote $\exp(-\eta_k\hat{a}_k^{\dagger}\hat{b}_k^{\dagger} + \eta_k^{*}\hat{a}_k\hat{b}_k)$ as $\hat{S}_k(\eta_k)$, then the state of the kth mode

$$|\Psi_k\rangle = \hat{S}_k(\eta_k)\,|0\rangle = \sum_{n_k=0}^{\infty}\sqrt{P_k(n_k)}\,|n_k, n_k\rangle \tag{A10}$$

is a two-mode squeezed state [54], whose probability of n_k-photon pair is

$$P_k(n_k) = \frac{\mu_k^{n_k}}{(1+\mu_k)^{n_k+1}}, \tag{A11}$$

where $\mu_k = \sinh^2|\eta_k| = \sinh^2(C\sqrt{\lambda_k}/\hbar)$.

APPENDIX B: GENERATING FUNCTIONS

For a given discrete probability distribution $P(n)$, its generating function is defined as

$$g(z) = \sum_{n=0}^{\infty} P_n(z) z^n. \tag{B1}$$

For example, if discrete random variable X follows the Poisson distribution with parameter μ, then its generating function is

$$g(z) = \mathrm{e}^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} z^n = \mathrm{e}^{(z-1)\mu}. \tag{B2}$$

The generating function of thermal distribution $P(n) = \mu^n/(1+\mu)^{n+1}$ is

$$g(z) = \sum_{n=0}^{\infty} \frac{(\mu z)^n}{(1+\mu)^{n+1}} = \frac{1}{1+\mu-z\mu}. \tag{B3}$$

Generating function possesses a desirable property. If the probability mass function of random variable X_i $(i = 1, \cdots, N)$ is $P_{X_i}(n)$, then the distribution of the random variable $Z = \sum_{i=1}^{N} X_i$ can be calculated as

$$P_Z(n) = \sum_{\|\mathbf{n}\|_1 = n} \prod_{i=1}^{N} P_{X_i}(n_i) = P_{X_1}(n) * \cdots * P_{X_N}(n), \tag{B4}$$

where $\mathbf{n}\|_1 = \sum_{i=1}^{N} n_i$, the symbol "$*$" means convolution. The generating function can be written concisely:

$$\begin{aligned} g_Z(z) &= \sum_{n=0}^{\infty} z^n \sum_{\|\mathbf{n}\|_1 = n} \prod_{i=1}^{N} P_{X_i}(n_i) \\ &= \sum_{\mathbf{n}=0}^{\infty} \prod_{i=1}^{N} P_{X_i}(n_i) z^{n_i} = \prod_{i=1}^{N} g_{X_i}(z). \end{aligned} \tag{B5}$$

That is, the generating function of the sum is the product of all the individual generating functions.

APPENDIX C: CALCULATION OF THE PND OF WCP AND SPDC SOURCES BEFORE AND AFTER THE CHANNEL

We utilize the MDI-QKD framework proposed in Ref. [59,60] to obtain the overall gain for multimode input. In the following discussion, we denote the conditional probability $P(A|B)$ as $P_B(A)$. Assuming a local threshold detector with dark count rate d_I and detection efficiency η_I, the triggering probability when k photons are incident is [60]

$$P_k(\text{trigger}) = 1 - (1-d_I)(1-\eta_I)^k. \tag{C1}$$

It is reasonable to posit that the response of the local detector to k photons states is independent of the intensity μ of the SPDC source generating such k photons, i.e., $P_k(\text{trigger}) = P_{\mu,k}(\text{trigger})$. We denote $\mathbf{k} = (k_1, \ldots, k_N)$ as the event that there are k_n photon pairs in the k_nth mode from SPDC source, and denote $\|*\|_1$ as 1-norm of a vector. From Eq. (A11) and the discussion of the independence of different TMs in Sec. II A, the total PND of SPDC source is

$$P_\mu(\mathbf{k}) = P_\mu(k_1, \ldots, k_N) = \prod_{i=1}^{N} \frac{\mu_i^{k_i}}{(1+\mu_i)^{1+k_i}}. \tag{C2}$$

From Eqs. (B3), (B5), and (C2), the generating function of the probability distribution $\{P_\mu(k)\}_{k=0}^{\infty}$ that SPDC source emit $k = \|\mathbf{k}\|_1$ $(k = 1, 2, \ldots)$ photons is

$$g(z) = \prod_{i=1}^{N} \frac{1}{1+\mu_i-z\mu_i}, \tag{C3}$$

where $\mu_i = \sinh^2(C\sqrt{\lambda_i})$, and thus

$$P_\mu(n) = \frac{1}{n!} \left. \frac{\partial^n g(z)}{\partial z^n} \right|_{z=0} = \frac{1}{n!} \frac{\partial^n}{\partial z^n} \prod_{i=1}^{N} \frac{1}{1+\mu_i-z\mu_i} \Bigg|_{z=0}. \tag{C4}$$

It should be noted that this expression is only suitable for theoretical analysis. When simulating, numerical convolution

$$P_\mu(n) = \frac{\mu_1^{n_1}}{(1+\mu_1)^{1+n_1}} * \cdots * \frac{\mu_N^{n_N}}{(1+\mu_N)^{1+n_N}} \tag{C5}$$

is a more computationally tractable solution.

We assume that the dark count rate d_S and detection efficiency η_S of the detectors at the measurement party of the MDI-QKD protocol are also identical. In such a case, we can attribute the detection efficiency to the channel loss

[59], and the probability of **k** photons after the channel is

$$\begin{aligned} f_\mu(\mathbf{k}) &= \sum_{\mathbf{n}\geqslant\mathbf{k}} P_{\mathbf{n}}(\text{trigger}) \\ &\quad\times \prod_{i=1}^{N} \binom{n_i}{k_i} \eta_S^{k_i}(1-\eta_S)^{n_i-k_i} P_\mu(\mathbf{n}) \\ &= \prod_{i=1}^{N} \frac{(\eta_S\mu_i)^{k_i}}{k_i!(1+\mu_i)^{1+k_i}} \\ &\quad\times \sum_{\mathbf{n}\geqslant 0} \left[1-(1-d_I)(1-\eta_I)^{\sum_{i=1}^{N}(n_i+k_i)}\right] \\ &\quad\times \prod_{i=1}^{N} \frac{(n_i+k_i)!}{n_i!} \left[\frac{(1-\eta_S)\mu_i}{1+\mu_i}\right]^{n_i}, \end{aligned} \tag{C6}$$

where $\mathbf{n}\geqslant\mathbf{k}$ means that for each mode i, $n_i \geqslant k_i$ holds true. We denote $C_{N-1} = (1-d_I)(1-\eta_I)^{\sum_{i=1}^{N} k_i}(1-\eta_I)^{\sum_{i=1}^{N-1} n_i}$, $x = (1-\eta_S)\mu_N/(1+\mu_N) < 1$, $y = (1-\eta_I)x < 1$, and consider the sum

$$\begin{aligned} &\sum_{n_N\geqslant 0} \frac{(n_N+k_N)!}{n_N!}\left(x^{n_N} - C_{N-1}y^{n_N}\right) \\ &= \frac{\partial^{k_N}}{\partial z^{k_N}}\left(\frac{x_N^{k_N}}{1-x_N} - C_{N-1}\frac{y_N^{k_N}}{1-y_N}\right) \\ &= \sum_{m=0}^{k_N}\binom{k_N}{m}(-1)^m \frac{\partial^{k_N}}{\partial z^{k_N}}\left[(1-x_N)^{m-1}\right. \\ &\quad \left. - C_{N-1}(1-y_N)^{m-1}\right] \\ &= k_N!\left[\frac{1}{(1-x)^{k_N+1}} - \frac{C_{N-1}}{(1-y)^{k_N+1}}\right] \\ &= k_N!\left\{\left(\frac{1+\mu_N}{1+\eta_S\mu_N}\right)^{k_N+1} - C_{N-1}\right. \\ &\quad \left.\times\left[\frac{1+\mu_N}{1+(\eta_I+\eta_S-\eta_I\eta_S)\mu_N}\right]^{k_N+1}\right\}. \end{aligned} \tag{C7}$$

Similarly, each factor $(1-\eta_I)^{n_i}$ in C_{N-1} can provide a sum result

$$k_i!\left[\frac{1+\mu_i}{1+(\eta_I+\eta_S-\eta_I\eta_S)\mu_i}\right]^{k_i+1}. \tag{C8}$$

Therefore, the final calculation result of Eq. (C6) is

$$\begin{aligned} f_{\mu,\text{trigger}}(\mathbf{k}) &= \prod_{i=1}^{N}\frac{(\eta_S\mu_i)^{k_i}}{(1+\eta_S\mu_i)^{1+k_i}} - (1-d_I) \\ &\quad\times\prod_{i=1}^{N}\frac{[(1-\eta_I)\eta_S\mu_i]^{k_i}}{[1+(\eta_S+\eta_I-\eta_S\eta_I)\mu_i]^{1+k_i}}. \end{aligned} \tag{C9}$$

For WCP source decomposed in orthonormal temporal modes in Eq. (38), we adopt the same approach and obtain

$$\begin{aligned} f(\mathbf{k}) &= \sum_{\mathbf{n}\geqslant\mathbf{k}}\prod_{i=1}^{N}\binom{n_i}{k_i}\eta_S^{k_i}(1-\eta_S)^{n_i-k_i}P_\mu(\mathbf{n}) \\ &= \prod_{i=1}^{N}\mathrm{e}^{-\mu_i}\frac{(\eta_S\mu_i)^{k_i}}{k_i!}\sum_{n_i=0}^{\infty}\frac{[(1-\eta_S)\mu_i]^{n_i}}{n_i!} \\ &= \mathrm{e}^{-\eta_S\mu}\prod_{i=1}^{N}\frac{(\eta_S\mu_i)^{k_i}}{k_i!}, \end{aligned} \tag{C10}$$

where $\mu_i = |\alpha c_i|^2$ and $\mu = |\alpha|^2 = \sum_{i=1}^{N}\mu_i$. The total PND is $P_\mu(n) = \mathrm{e}^{-\mu}\mu^n/n!$.

APPENDIX D: THEORETICAL ANALYSIS OF THE VISIBILITY WITH WCP SOURCE AND SPDC SOURCE

Since the expressions of overall gain and QBER are tough for theoretical analysis due to the over generality in Ref. [59], we will apply a more simplified method for given PND.

The local detection operator can be described as the projector

$$\Pi_k = |\boldsymbol{k}\rangle\langle\boldsymbol{k}| = \bigotimes_{k_1+\cdots+k_N=k}|\boldsymbol{k}_i\rangle\langle\boldsymbol{k}_i| \tag{D1}$$

with corresponding probability $1-(1-d_I)(1-\eta_I)^k$, followed by a partial trace operation on the system of idler photons. Note another fact that the quantum channel can be equivalently regarded as a beam splitter [47] with transmittance η, while the remainder of the signal is leaked or consumed. In other words, for the export we concern, the transformation on the creation operator is $\hat{a}^\dagger \to \sqrt{\eta}\hat{a}^\dagger$. In this case, for simplicity, we temporarily attribute η to η_S and omit η_S. After temporal-mode decomposition, the joint state after 50:50 BS in the ith mode can be expressed as

$$\begin{aligned} |\Psi_i\rangle_A|\alpha c_i\rangle_B &= \hat{S}_{A,i}(\eta_i)\hat{D}_{B,i}(\alpha c_i)|0\rangle \\ &\xrightarrow{\text{BS}} \hat{S}_{A,i}\left(\frac{\eta_i}{\sqrt{2}}\right)\hat{S}_{B,i}\left(\frac{\eta_i}{\sqrt{2}}\right) \\ &\quad\times\hat{D}_{A,i}\left(\frac{\alpha}{\sqrt{2}}\right)\hat{D}_{B,i}\left(-\frac{\alpha}{\sqrt{2}}\right)|0\rangle, \end{aligned} \tag{D2}$$

where A, B represent the sides belong to Alice and Bob, respectively. For side (or path) A, now we execute the

TABLE I. The fixed parameters chosen from the optimal parameter of asymmetric sources.

	ν_1	μ_1	$P^Z_{\nu_1}$	$P^Z_{\mu_1}$	$P^X_{\nu_1}$	$P^X_{\mu_1}$	ν_2	μ_2	$P^Z_{\nu_2}$	$P^Z_{\mu_2}$	$P^X_{\nu_2}$	$P^X_{\mu_2}$
Parameter 1	0.0066	0.4225	0.0358	0.8754	0.0788	0.0091	0.0542	0.5774	0.0344	0.8757	0.0500	0.0055
Parameter 2	0.0082	0.2671	0.0680	0.7453	0.1612	0.0200	0.0624	0.4287	0.0703	0.7466	0.1035	0.0147
Parameter 3	0.0134	0.1588	0.1249	0.5094	0.3124	0.0411	0.0812	0.3583	0.1177	0.5144	0.2014	0.0412

projective measurements on idler photons:

$$\rho_{s,i}(k) = \mathrm{Tr}_{\mathrm{idler}}\left[\Pi_k \hat{S}_{A,i}\left(\frac{\eta_i}{\sqrt{2}}\right)|0\rangle\langle 0|\hat{S}^\dagger_{A,i}\left(\frac{\eta_i}{\sqrt{2}}\right)\right] = \bigotimes_{k_1+\cdots+k_N=k} P_i(k_i)\,|\boldsymbol{k}_i\rangle\langle\boldsymbol{k}_i|\,, \tag{D3}$$

where $P_i(k_i) = \mu_i^{k_i}/(1+\mu_i)^{k_i+1}$ and $\mu_i = \sinh^2|\eta_i/\sqrt{2}|$, then the density operator of the system of signal photons can be written as

$$\rho_{\mathrm{sigal}} = \sum_{k=0}^{\infty}\left[1-(1-d_I)(1-\eta_I)^k\right]\rho_{s,i}(k) = \bigotimes_{i=1}^{N}\sum_{k_i=0}^{\infty}\left[1-(1-d_I)(1-\eta_I)^{k_i}\right]P_i(k_i)\,|\boldsymbol{k}_i\rangle\langle\boldsymbol{k}_i|\,, \tag{D4}$$

and the total probability of local triggering is

$$P(\mathrm{trigger}) = \mathrm{Tr}\rho_{\mathrm{signal}} = 1-(1-d_I)\prod_{i=1}^{N}\frac{1}{1+\eta_I\mu_i}. \tag{D5}$$

We denote the ith mode of ρ_{signal} as $\rho_{s,i}$, that is,

$$\rho_{s,i} = \sum_{k_i=0}^{\infty}\left[1-(1-d_I)(1-\eta_I)^{k_i}\right]P_i(k_i)\,|\boldsymbol{k}_i\rangle\langle\boldsymbol{k}_i|\,. \tag{D6}$$

Since the majority of noncoincidence is caused by vacuum, we only concern the vacuum probability of the ith mode:

$$P_{A,i}(0) = \langle 0|\hat{D}_{A,i}(\alpha_i)\rho_{s,i}\hat{D}^\dagger_{A,i}(\alpha_i)|0\rangle = \frac{1}{1+\mu_i}\left[\mathrm{e}^{-|\alpha_i|^2/(1+\mu_i)} - (1-d_I)\mathrm{e}^{-(1+\eta_I\mu_i)|\alpha_i|^2/(1+\mu_i)}\right], \tag{D7}$$

where $\alpha_i = \alpha c_i/\sqrt{2}$. Therefore, the total probability of vacuum is $P_A(\mathrm{vac}) = \prod_{i=1}^{N} P_{A,i}(0)$. By replacing α, η_i to $\alpha\sqrt{\eta_S}, \eta_i\sqrt{\eta_S}$, the final click probability, $P_A(\mathrm{click})$, of Charlie's detector in path A can be expressed as

$$P_A(\mathrm{click}) = 1-(1-d_S)\prod_{i=1}^{N}\frac{1}{1+\mu_i}\left[\mathrm{e}^{-\eta_S|\alpha|^2|c_i|^2/2(1+\mu_i)} - (1-d_I)\mathrm{e}^{-(1+\eta_I\mu_i)\eta_S|\alpha|^2|c_i|^2/2(1+\mu_i)}\right], \tag{D8}$$

where $\mu_i = \sinh^2|\eta_i\sqrt{\eta_S/2}|$. Consider the function $f(x) = \mathrm{e}^{-x} - (1-d_I)\mathrm{e}^{-(1+\eta_I\mu)x}$ $(x \geqslant 0)$. Usually $d_I \ll \eta_I\mu_i < 1$, and therefore, when $x_0 = \ln[(1-d_I)(1+\eta_I\mu)]/(\eta_I\mu)$, function $f(x)$ achieves the maximum. Thus, for any temporal mode of WCP source, the click probability for path A is lower bounded by

$$P_A(\mathrm{click}) \geqslant 1-(1-d_S)\max_i\left\{\frac{\eta_I\mu_i}{(1+\mu_i)(1+\eta_I\mu_i)}\left[\frac{1}{(1-d_I)(1+\eta_I\mu_i)}\right]^{1/\eta_I\mu_i}\right\}. \tag{D9}$$

It is similar for path B. With this simplified expression, if we can have a prior knowledge or estimation of c_i (e.g., experimental measurement), we can further judge whether MDI QKD with these two asymmetric sources is feasible through a predetermined lower bound of the visibility.

APPENDIX E: FIXED PARAMETERS CHOSEN FROM THE OPTIMAL PARAMETERS

Here we list the fixed parameters used in Fig. 5. The symbol used in Table I is as follows. ν, μ are, respectively, the (intensities of) the decoy and signal state; P^β_α $(\alpha = \mu, \nu,\ \beta = Z, X)$ is the probability that the state α in β basis is chosen; the subscripts 1 and 2, respectively, represent the parameters of the SPDC source and the WCP source.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014). Theoretical Aspects of Quantum Cryptography—celebrating 30 years of BB84.

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

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and

P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).
[4] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).
[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).
[6] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).
[8] H. J. Kimble, The quantum internet, Nature **453**, 1023 (2008).
[9] D. Castelvecchi, The quantum internet has arrived (and it hasn't), Nature **554**, 289 (2018).
[10] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, eaam9288 (2018).
[11] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions, IEEE Commun. Surv. Tutorials **23**, 2218 (2021).
[12] Z. Li, K. Xue, J. Li, L. Chen, R. Li, Z. Wang, N. Yu, D. S. Wei, Q. Sun, and J. Lu, Entanglement-assisted quantum networks: Mechanics, enabling technologies, challenges, and research directions, IEEE Commun. Surv. Tutorials **25**, 2133 (2023).
[13] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[14] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).
[15] 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).
[16] W. Wang, F. Xu, and H.-K. Lo, Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks, Phys. Rev. X **9**, 041012 (2019).
[17] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A—At., Mol. Opt. Phys. **86**, 062319 (2012).
[18] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A **87**, 012320 (2013).
[19] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).
[20] 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).
[21] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method, Phys. Rev. A **91**, 032318 (2015).
[22] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A **93**, 042324 (2016).
[23] F.-Y. Lu, Z.-Q. Yin, G.-J. Fan-Yuan, R. Wang, H. Liu, S. Wang, W. Chen, D.-Y. He, W. Huang, B.-J. Xu, *et al.*, Efficient decoy states for the reference-frame-independent measurement-device-independent quantum key distribution, Phys. Rev. A **101**, 052318 (2020).
[24] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, *et al.*, Experimental measurement-device-independent quantum key distribution, Phys. Rev. Lett. **111**, 130502 (2013).
[25] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Measurement-device-independent quantum key distribution over 200 km, Phys. Rev. Lett. **113**, 190501 (2014).
[26] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photonics **9**, 397 (2015).
[27] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phase-reference-free experiment of measurement-device-independent quantum key distribution, Phys. Rev. Lett. **115**, 160502 (2015).
[28] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, *et al.*, Measurement-device-independent quantum key distribution over untrustful metropolitan network, Phys. Rev. X **6**, 011024 (2016).
[29] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).
[30] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, *et al.*, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).
[31] G. Roberts, M. Lucamarini, Z. Yuan, J. Dynes, L. Comandar, A. Sharpe, A. Shields, M. Curty, I. Puthoor, and E. Andersson, Experimental measurement-device-independent quantum digital signatures, Nat. Commun. **8**, 1 (2017).
[32] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, Optica **4**, 1016 (2017).
[33] H. Liu, J. Wang, H. Ma, and S. Sun, Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration, Optica **5**, 902 (2018).
[34] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Chip-based measurement-device-independent quantum key distribution, Optica **7**, 238 (2020).
[35] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, *et al.*, High-speed

measurement-device-independent quantum key distribution with integrated silicon photonics, Phys. Rev. X **10**, 031030 (2020).

[36] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. Paraïso, M. Lucamarini, Z. Yuan, and A. Shields, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Inf. **7**, 1 (2021).

[37] X.-Y. Zhou, H.-J. Ding, M.-S. Sun, S.-H. Zhang, J.-Y. Liu, C.-H. Zhang, J. Li, and Q. Wang, Reference-frame-independent measurement-device-independent quantum key distribution over 200 km of optical fiber, Phys. Rev. Appl. **15**, 064016 (2021).

[38] F.-Y. Lu, Z.-H. Wang, Z.-Q. Yin, S. Wang, R. Wang, G.-J. Fan-Yuan, X.-J. Huang, D.-Y. He, W. Chen, Z. Zhou, *et al.*, Unbalanced-basis-misalignment-tolerant measurement-device-independent quantum key distribution, Optica **9**, 886 (2022).

[39] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, *et al.*, Hacking measurement-device-independent quantum key distribution, Optica **10**, 520 (2023).

[40] Ö. Erkılıç, L. Conlon, B. Shajilal, S. Kish, S. Tserkis, Y.-S. Kim, P. K. Lam, and S. M. Assad, Surpassing the repeaterless bound with a photon-number encoded measurement-device-independent quantum key distribution protocol, npj Quantum Inf. **9**, 29 (2023).

[41] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution for nonstandalone networks, Photonics Res. **9**, 1881 (2021).

[42] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, *et al.*, Robust and adaptable quantum key distribution network without trusted nodes, Optica **9**, 812 (2022).

[43] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4600 km, Nature **589**, 214 (2021).

[44] G.-Z. Tang, S.-H. Sun, and C.-Y. Li, Experimental point-to-multipoint plug-and-play measurement-device-independent quantum key distribution network, Chin. Phys. Lett. **36**, 070301 (2019).

[45] F.-Y. Lu, Z.-Q. Yin, C. Wang, C.-H. Cui, J. Teng, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, *et al.*, Parameter optimization and real-time calibration of a measurement-device-independent quantum key distribution network based on a back propagation artificial neural network, JOSA B **36**, B92 (2019).

[46] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, *et al.*, Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels, Phys. Rev. Lett. **122**, 160501 (2019).

[47] A. M. Brańczyk, Hong-Ou-Mandel interference, ArXiv:1711.00080.

[48] R.-B. Jin, Z.-Q. Zeng, C. You, and C. Yuan, Quantum interferometers: Principles and applications, Prog. Quantum Electron. **96**, 100519 (2024).

[49] H. Takesue and K. Shimizu, Effects of multiple pairs on visibility measurements of entangled photons generated by spontaneous parametric processes, Opt. Commun. **283**, 276 (2010).

[50] M. C. Tichy, Interference of identical particles from entanglement to boson-sampling, J. Phys. B: At., Mol. Opt. Phys. **47**, 103001 (2014).

[51] Y.-S. Ra, M. C. Tichy, H.-T. Lim, O. Kwon, F. Mintert, A. Buchleitner, and Y.-H. Kim, Nonmonotonic quantum-to-classical transition in multiparticle interference, Proc. Natl. Acad. Sci. **110**, 1227 (2013).

[52] C.-K. Hong, Z.-Y. Ou, and L. Mandel, Measurement of subpicosecond time intervals between two photons by interference, Phys. Rev. Lett. **59**, 2044 (1987).

[53] B. Brecht, D. V. Reddy, C. Silberhorn, and M. G. Raymer, Photon temporal modes: A complete framework for quantum information science, Phys. Rev. X **5**, 041017 (2015).

[54] M. O. Scully and M. S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, 1997).

[55] J. Rarity, P. Tapster, and R. Loudon, Non-classical interference between independent sources, J. Opt. B: Quantum Semiclassical Opt. **7**, S171 (2005).

[56] H. Chen, X.-B. An, J. Wu, Z.-Q. Yin, S. Wang, W. Chen, and Z.-F. Han, Hong–Ou–Mandel interference with two independent weak coherent states, Chin. Phys. B **25**, 020305 (2016).

[57] H. Takesue, S. D. Dyer, M. J. Stevens, V. Verma, R. P. Mirin, and S. W. Nam, Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors, Optica **2**, 832 (2015).

[58] Z.-Q. Zhong, S. Wang, X.-H. Zhan, Z.-Q. Yin, W. Chen, G.-C. Guo, and Z.-F. Han, Realistic and general model for quantum key distribution with entangled-photon sources, Phys. Rev. A **106**, 052606 (2022).

[59] Q. Wang and X.-B. Wang, Simulating of the measurement-device independent quantum key distribution with phase randomized general sources, Sci. Rep. **4**, 4612 (2014).

[60] X.-H. Zhan, Z.-Q. Zhong, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution with practical spontaneous parametric down-conversion sources, Phys. Rev. Appl. **20**, 034069 (2023).

[61] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[62] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A—At., Mol. Opt. Phys. **87**, 012320 (2013).

[63] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Higher key rate of measurement-device-independent quantum key distribution through joint data processing, Phys. Rev. A **103**, 012402 (2021).

[64] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings* (IEEE, Chicago, Illinois, USA, 2004), p. 136.

[65] J. A. Crosse and S. Scheel, Effective nonlinear hamiltonians in dielectric media, Phys. Rev. A **81**, 033815 (2010).

[66] W. P. Grice and I. A. Walmsley, Spectral information and distinguishability in type-II down-conversion with a broadband pump, Phys. Rev. A **56**, 1627 (1997).

[67] W. Mauerer, M. Avenhaus, W. Helwig, and C. Silberhorn, How colors influence numbers: Photon statistics of parametric down-conversion, Phys. Rev. A—At., Mol. Opt. Phys. **80**, 053815 (2009).

[68] X. Ma, C.-H. F. Fung, and H.-K. Lo, Quantum key distribution with entangled photon sources, Phys. Rev. A—At., Mol. Opt. Phys. **76**, 012307 (2007).

[69] P. Kok and S. L. Braunstein, Postselected versus nonpostselected quantum teleportation using parametric down-conversion, Phys. Rev. A **61**, 042304 (2000).

[70] C. K. Law, I. A. Walmsley, and J. H. Eberly, Continuous frequency entanglement: Effective finite Hilbert space and entropy control, Phys. Rev. Lett. **84**, 5304 (2000).

[71] V. Ansari, J. M. Donohue, B. Brecht, and C. Silberhorn, Tailoring nonlinear processes for quantum optics with pulsed temporal-mode encodings, Optica **5**, 534 (2018).

[72] M. G. Raymer and I. A. Walmsley, Temporal modes in quantum optics: Then and now, Phys. Scr. **95**, 064002 (2020).

[73] D. V. Reddy, M. G. Raymer, C. J. McKinstrie, L. Mejling, and K. Rottwitt, Temporal mode selectivity by frequency conversion in second-order nonlinear optical waveguides, Opt. Express **21**, 13840 (2013).