Security research on practical measurement-device-independent quantum key distribution

Wei Li [1,2,3,*] and Shengmei Zhao [2,3]

[1] *National Laboratory of Solid State Microstructures, Nanjing University, Nanjing 210093, China*

[2] *Nanjing University of Posts and Telecommunications, Institute of Signal Processing and Transmission, Nanjing 210003, China*

[3] *Nanjing University of Posts and Telecommunications, Key Lab Broadband Wireless Communication and Sensor Network, Ministy of Education, Nanjing 210003, China*

(Received 15 March 2022; accepted 9 September 2022; published 28 October 2022)

The ideal measurement-device-independent quantum key distribution (MDI-QKD), which is immune to all detector side-channel attacks, is built on the Bell state measurement of two single-photon states. However, in practical MDI-QKD where phase-randomized weak coherent pulses (PR-WCPs) are used, the mismatch between states preparation and measurement in X basis leads to the bit error rate of more than 25%, which poses a challenge to the security of QKD. In this paper, we provide a security analysis of practical MDI-QKD based on polarization coding. We analyze the Hong-Ou-Mandel interference of PR-WCPs and Poisson-distributed photon number states (PNs), and find that these two sources are equivalent in MDI-QKD. The security analysis based on entanglement distillation is carried out on PNs, and the measurement results in Z basis and X basis are averaged to overcome the noncorrelation of the error rates in these two bases. Compared with GLLP scheme, a tighter key rate is obtained in this work, and the key rate deviates from the linear key rate bound in a short distance due to the finite proportion of multiphoton terms.

DOI: 10.1103/PhysRevA.106.042445

I. INTRODUCTION

Quantum key distribution (QKD) is a way to generate a set of shared random numbers for two far separated parties, Alice and Bob, for encrypted communication through the transmission and measurement of quantum states [1–3]. Its unconditional security is guaranteed by the principle of quantum mechanics. However, the gap between ideal devices and realistic devices in real-life implementation of QKD, such as imperfection of source and detector, may provide the eavesdropper, Eve, with opportunities to carry out source-side [4–6] and detection-side attacks [7–11]. The combination of decoy-state method [12–15] and measurement-device-independent QKD (MDI-QKD) [15–23] ensures the security of practical QKD despite the imperfect source and detector. Inspired by MDI-QKD, twin-field QKD (TF-QKD) [24–26], phase-matching QKD (PM-QKD) [27–29], and sending-or-not sending QKD (SNS-QKD) [30–33], have been proposed, where information is carried by wavelike state. The security of these QKDs have been studied based on entanglement distillation protocol (EDP), which can be used to verify the security of a QKD against the most powerful channel attacks. However, the practical MDI-QKD with imperfect source and detection still needs further detailed EDP-based security analysis.

MDI-QKD is a time-reversed version of entanglement-based QKD protocol [29,34–36], in which correlation measurement based on two-photon coincidence counting is used to eliminate all the detector generated side-channel information about the transmitted quantum states. The core component of MDI-QKD is Bell state measurement (BSM), which involves two-photon Hong-Ou-Mandel (HOM) interference [37,38] in some of its measurements. The visibility of HOM interference will have a non-negligible impact on the BSM results, so the key rate will be affected accordingly. The ideal MDI-QKD is built on the single-photon sources [16] where 100% visibility of HOM interference can be reached. Due to the lack of mature commercial single-photon sources, the phase randomized weakly coherent pulses (PR-WCPs) are always used as the source, for which the HOM interference visibility is only about 50%. This will lead to the mismatch between state preparation and measurement in X basis, and a large bit error rate (BER) will be caused in X basis [17,18,39]. The imperfection of BSM of PR-WCPs will also cause the noncorrelation of error rate between Z basis and X basis, which will bring challenges to security analysis. In principle, all errors may provide shield for eavesdroppers and cause the loss of information. Thus, security analysis should take all errors into account.

In this paper, we give a theoretical study on the security of PR-WCPs-based MDI-QKD with polarization coding. The core of this work is to analyze all possible decoding errors caused by the imperfection of BSM of PR-WCPs, and take them into account in security analysis. First, we analyze the HOM interference of PR-WCPs and the Poisson distributed photon number state (PNs), so as to establish the equivalence of these two light sources in MDI-QKD. Next, according to the BSM results of PR-WCPs, we construct *a posteriori* probability decoding table to analyze the possible BER in Z basis and X basis. Finally, we use PNs to analyze the BER and phase error rate (PER) in Z and X bases in the security

*alfred_wl@njupt.edu.cn

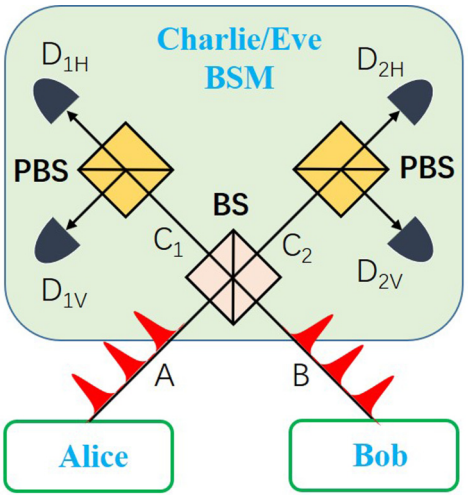

FIG. 1. Schematic diagram of MDI-QKD.

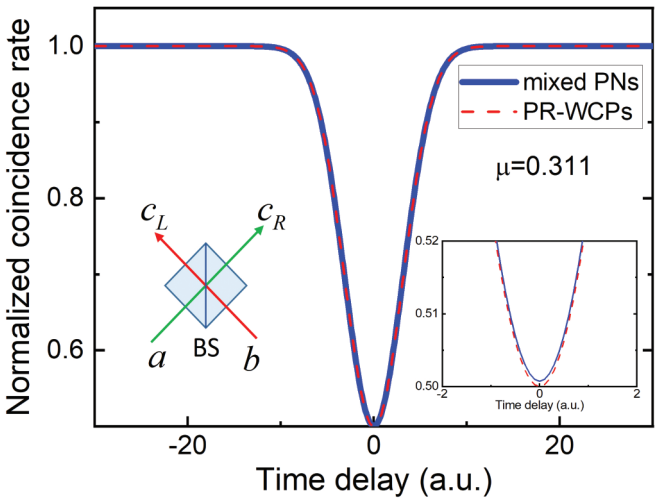

FIG. 2. Comparison of the HOM interference for single-photon source, Poisson distributed PNs and PR-WCPs.

proof based on entanglement distillation protocol (EDP), and take them into account in the extraction of the final key.

II. REVIEW OF MDI-QKD

Figure 1 is the schematic diagram of MDI-QKD, in which Alice and Bob each prepare a single-photon state randomly selected from two mutually unbiased bases (MUBs), and then send them to the third party Charlie for BSM. In MDI-QKD, BSM of the states does not need basis switch, so any attack on the side information about detection can be eliminated. In fact, in polarization coding, the joint states in Z basis are the eigenstates of BSM in Fig. 1, which is why the BER can be very low in Z basis even if Alice and Bob send non-single-photon states [39]. While in X basis, the correlation measurement of BSM strongly depends on the visibility of HOM interference, which is determined by the indistinguishability of modes and the fidelity of the single-photon state. In the ideal MDI-QKD, the HOM interference with 100% visibility can ensure that the joint states in X basis are the eigenstates of the correlation measurement of BSM. While in the practical MDI-QKD where both Alice and Bob send PR-WCPs, the BSM in X basis will produce a non-negligible BER. The large difference in the BSM results between Z basis and X basis implies that in the security analysis based on EDP, we should not directly use the key rate formula obtained from BB84-QKD. PR-WCPs are usually regarded as Poisson distributed PNs because they have the same density of states. This model has achieved a great success in the security analysis of BB84-QKD. However, whether these two light sources are equivalent in BSM still needs further proof.

Here we first compare HOM interference of PR-WCPs and Poisson distributed PNs, which is the decisive factor in BSM measurement. We assume that the single-photon state, the basic unit of these two light sources, has a Gaussian spectral distribution centered on ω_0

$$|\Psi(\omega_0)\rangle = (2\pi\Gamma)^{\frac{1}{4}} \int_{-\infty}^{\infty} \exp\left[\frac{-(\omega-\omega_0)^2}{4\Gamma}\right] \hat{a}_\omega^\dagger |0\rangle d\omega, \quad (1)$$

where Γ is the shape factor of the Gaussian envelope, $\hat{a}_\omega^\dagger$ is the generating operator at frequency ω. Its time domain counterpart can be obtained by Fourier transform

$$|\Psi(t_0)\rangle = \left(\sqrt{\frac{2\Gamma}{\pi}}\right)^{\frac{1}{4}} \int_{-\infty}^{\infty} \exp[-\Gamma(t-t_0)^2 + i\omega_0(t-t_0)] \times \hat{a}_t^\dagger |0\rangle dt, \quad (2)$$

which is a Gaussian-shaped pulse centered on t_0, where $\hat{a}_t^\dagger$ is the generating operator at time t. Therefore, we have the time domain WCP

$$|\Psi_{t_0}\rangle_{\mathrm{C}} = \left(\frac{2\Gamma}{\pi}\right)^{\frac{1}{4}} \int_{-\infty}^{\infty} |\sqrt{\mu_{t-t_0}} e^{i\theta_{t-t_0}}\rangle_{\mathrm{C}} dt, \quad (3)$$

where $|\sqrt{\mu}e^{i\theta}\rangle_{\mathrm{C}} = e^{-\frac{\mu}{2}} \sum_{k=0}^{\infty} \frac{\mu^{\frac{k}{2}} e^{ik\theta}}{k!} (\hat{a}^\dagger)^k |0\rangle$ is the coherent state with an average photon number of μ and a phase of θ, $\mu_{t-t_0} = \mu \exp[-2\Gamma(t-t_0)^2]$ is the Gaussian-shaped amplitude factor, $\theta_{t-t_0} = \omega_0(t-t_0)$ is the time-dependent phase of the WCP. In the slowly varying amplitude approximation with $\Gamma \ll \omega_0$, the amplitude μ_{t-t_0} can be regarded as a constant when θ_{t-t_0} continuously varies from 0 to 2π. In Fock representation, the PR-WCPs is equivalent to the Poisson distributed PNs [40],

$$\hat{\rho}_M = e^{-\mu_{t-t_0}} \sum_{k=0}^{\infty} \frac{\mu_{t-t_0}^k}{k!} \hat{\rho}_k, \quad (4)$$

where $\hat{\rho}_k = |k\rangle\langle k|$ is the density of state with k photons and its probability is $p_k = e^{-\mu_{t-t_0}} \frac{\mu_{t-t_0}^k}{k!}$. If the value of μ is small enough, the single-photon state accounts for a large proportion except the vacuum state. This is the most commonly used light source model in practical BB84-QKD.

The HOM interference can be expressed by the joint probability of the two outputs of the interferometer, as shown in the left inset of Fig. 2. For Poisson distributed PNs, the photon number state $|n\rangle$ is sent to the interferometer with a probability of $p_n = e^{-\mu} \frac{\mu^n}{n!}$, where μ is the average photon number of PNs. We denote the joint probability as p_{n_a,n_b}

when there are n_a and n_b photons incident on the a-side and b-side of the 50 : 50 beam splitter (BS). Here it should be noted that even though the single-photon state occupies a large proportion in the PNs for μ small enough, but the multiphoton terms also have comparable contributions in the HOM interference. For example, the joint probabilities that one side of the incident end is a vacuum state while the other side is a two-photon state is equal to that both sides are single-photon states. In this case, the total joint probability p_{PNs} is the weighted sum of the terms of different photon number combination

$$p_{\mathrm{PNs}}(\Delta) \approx \sum_{m+n=2}^{m+n=4} p_m p_n p_{m,n}(\Delta) + O(p_{m+n>4}), \tag{5}$$

where $O(p_{m+n>4})$ is the high-order infinitesimal term with $m+n>4$. This term can be omitted in the simulation when μ is small enough. The details of the derivation of $p_{m,n}$ are given in Appendix A.

For PR-WCPs, the probability of photon state detection is proportional to the average number of photons μ in the WCP, which can be reflected from the linear bound in BB84-QKD. Therefore, the HOM interference of this light source can also be regarded as the second-order correlation of the light intensities,

$$\begin{aligned} p_{\mathrm{WCP}} &\propto \int_0^{2\pi} d\theta_a \int_0^{2\pi} d\theta_b I_L(\theta_a - \theta_b, \Delta) I_R(\theta_a - \theta_b, \Delta) \\ &= \frac{1}{2}\left[1 - \frac{1}{2}\exp(-\Gamma\Delta^2)\right], \end{aligned} \tag{6}$$

where I_{L} and I_{R} are the light intensities on the left-hand side and right-hand side of the outputs of the BS, θ_{a} and θ_b are the global phases of the PR-WCPs incident on the a-side and b-side of the BS. A detailed derivation of Eq. (6) is given in Appendix B.

Figure 2 shows the comparison of time domain HOM interference for Poisson distributed PNs and PR-WCPs from Eqs. (5) and (6). These two light sources are assumed to have the same pulse width, and all the joint probabilities are normalized to their maximum values. In this figure, the average number μ is set to 0.311, which is the optimal value for key extraction in Sec. IV. We can see that the two curves almost coincide, which directly proves the equivalence of the two light source models in BSM. The right inset shows the amplification of the dip of the HOM curves, the omission of the high-order terms will almost cause 0.15% deviation between the curves of these two models. As the average photon number μ continues to decrease, we can expect that the deviation between them will tend to 0. This means that the security analysis of practical MDI-QKD from the perspective of Poisson distributed PNs and PR-WCPs are equivalent.

III. VIRTUAL PROTOCOL OF MDI-QKD

In polarization encoded MDI-QKD, Alice and Bob decode the key according to Charlie's BSM results and their bases information. For ideal single-photon sources, there are only four coincidence detection events, which are $\mathrm{D_{1H}D_{1V}}$, $\mathrm{D_{2H}D_{2V}}$, $\mathrm{D_{1H}D_{2V}}$, and $\mathrm{D_{2H}D_{1V}}$. In practical MDI-QKD with PR-WCPs as the source, Alice and Bob send the WCPs $|\sqrt{\mu}e^{i\alpha}\rangle_{A,P_A}$ and $|\sqrt{\mu}e^{i\beta}\rangle_{B,P_B}$ to Charlie for BSM, where α and β are the randomized phases, the subscripts P_A, P_B denote the polarizations of the MUBs with $P_A, P_B \in \{H, V\}$ in Z basis and $P_A, P_B \in \{+, -\}$ in X basis. Here, H, V represent the horizontal and vertical polarizations, $+$, $-$ represent the $+45^\circ$ and -45° polarizations, and they satisfy $|\pm\rangle = \frac{\sqrt{2}}{2}[|H\rangle \pm |V\rangle]$. Because the WCPs, can be regarded as a semiclassical light source, so the joint detection probability is proportional to the second correlation of the light intensity at each output,

$$p(D_{j,P}, D_{j',P'}) \propto \langle I_{j,P} I_{j',P'} \rangle, \tag{7}$$

with the subscripts $j, j' \in \{1, 2\}$ and $P, P' \in \{H, V\}$. A detailed calculation of the joint probabilities is given in Appendix C. Here, in addition to the detection events in ideal MDI-QKD, there are other two detection events $\mathrm{D_{1H}D_{2H}}$ and $\mathrm{D_{1V}D_{2V}}$. It is easy to prove that these two detection events are invalid here. If the WCPs are prepared in Z basis, when Alice and Bob use the same polarization, these two detection events will provide information about the key for the eavesdropper, and when Alice and Bob use different polarizations, these two detection events cannot provide the correct decoding information for Alice and Bob. If the WCPs are prepared in X basis, by comparing Eqs. (C5) and (C7), we can see that these two detection events will not provide any information for Alice's and Bob's key extraction.

TABLE I. The normalized *a posteriori* probability of key decoding $p(AB|C)$ for Alice and Bob based on Charlie's BSM results. Here, C is taken from four effective joint detection events $\mathrm{D_{1H}D_{1V}}$, $\mathrm{D_{2H}D_{2V}}$, $\mathrm{D_{1H}D_{2V}}$, and $\mathrm{D_{2H}D_{1V}}$, $AB \in \{|\Phi\rangle, |\Psi\rangle\}$. If $|\Psi\rangle$ is decoded, Alice or Bob need to flip her or his bit, otherwise they do nothing to their bits.

	$p(AB\|C)$	$\mathrm{D_{1H}D_{1V}}$	$\mathrm{D_{2H}D_{2V}}$	$\mathrm{D_{1H}D_{2V}}$	$\mathrm{D_{2H}D_{1V}}$
Z	Φ	0	0	0	0
basis	Ψ	1	1	1	1
X	Φ	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
basis	Ψ	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{3}{4}$	$\frac{3}{4}$

Accordingly, the normalized *a posteriori* probability of key decoding $p(AB|C)$ based on these four effective detection events can be obtained, as shown in Table I. Here, the symbols Φ and Ψ learn from the writing habits of the Bell states, which determine the bit correlation between Alice and Bob. If Φ is inferred, than Alice and Bob are assumed to have the same bit, or else their bits are assumed to be different. In this table we can see that the BER in Z basis is 0, while the BER in X basis is 25% due to the imperfection of the BSM of PR-WCPs. The large BER difference between the two bases caused by BSM is what we need to consider in the security analysis.

Here, the security of PR-WCPs-based MDI-QKD with the *a posteriori* probability in Table I will be analyzed with EDP. This security analysis method has achieved remarkable success in BB84-QKD [41,42]. Although MDI-QKD evolved from BB84-QKD, there are great differences between them at

the detection end, which requires special attention in security analysis. In BB84-QKD, the measurement of quantum states is carried out by one of the communication participants with properly selected basis, where no additional errors will be caused by measurement, and the PER in Z basis is equal to the BER in X basis. While in MDI-QKD, there is no basis switch for the measurement of quantum states. Especially in X basis, PR-WCPs is not the eigenstate of BSM, and a large BER will be produced by in X basis, as shown in Table I. In addition, the effective detection events of Z basis and X basis have different gains. In the security analysis, all these problems should be taken into account.

Here, we will analyze and compare the virtual protocols of BB84-QKD and MDI-QKD based on the virtual entanglement with an ancillary state, so as to find a solution to these problems in practical MDI-QKD.

Virtual protocol of BB84-QKD. B1: Alice generates N ancillary qubits A' initialized to $|+\rangle = \frac{\sqrt{2}}{2}[|0\rangle + |1\rangle]$, N polarization encoded states A initialized to $|H\rangle$ and a random string $K = k_1, k_2, \ldots, k_N$ of length N. Alice applies the CNot gate to qubits A' and states A to generate the EPR pair $|\Phi_Z^+\rangle_{A'A} = \frac{\sqrt{2}}{2}[|0\rangle|H\rangle + |1\rangle|V\rangle]$. She keeps A' and sends A to Bob via a quantum channel. Before sending, she performs a Hadamard operation on A to transform the ith EPR pair to $|\Phi_X^+\rangle_{A'A} = \frac{\sqrt{2}}{2}[|0\rangle|+\rangle + |1\rangle|-\rangle]$ when the value of the random number k_i is 1, or else she does nothing.

B2: After Bob receives all the states A, Alice announce the random number string K publicly. For each time, Bob performs Hadamard operation on the received state when the value of K is 1.

B3: Alice and Bob use EDP or quantum Calderbank-Shor-Steane (CSS) codes to distill m EPR pairs with fidelity of almost 100% from those EPR pairs polluted by channel noise. Finally, Alice and Bob conduct Z measurement on the distilled EPR pairs to obtain a set of shared random numbers. Here we extend the virtual protocol of BB84-QKD directly to MDI-QKD.

Virtual protocol of MDI-QKD. M1: Similar to the state preparation in BB84-QKD, Alice first generates N ancillary qubits A' initialized to $|+\rangle_A = \frac{\sqrt{2}}{2}[|0\rangle + |1\rangle]$, N polarization encoded states A initialized to $|H\rangle_A$ and a random string $K^A = k_1^A, k_2^A, \cdots, k_N^A$ of length N. Alice applies the CNot gate to qubits A' and states A to generate the EPR pair $|\Phi_Z^+\rangle_{A'A} = \frac{\sqrt{2}}{2}[|0\rangle_{A'}|H\rangle_A + |1\rangle_{A'}|V\rangle_A]$. Whenever the value of k_i^A is 1, Alice performs a Hadamard operation on A to transform the i-th EPR pair to $|\Phi_X^+\rangle_{A'A} = \frac{\sqrt{2}}{2}[|0\rangle_{A'}|+\rangle_A + |1\rangle_{A'}|-\rangle_A]$. Similarly, Bob generates N ancillary qubits B', N polarization encoded states B, a random number K^B, and he applies the CNot gate to B' and B to obtain the EPR pairs $|\Phi_Z^+\rangle_{B'B}^{(N)} = \frac{\sqrt{2}}{2}[|0\rangle_{B'}|H\rangle_B + |1\rangle_{B'}|V\rangle_B]$. Whenever the value of k_i^B is 1, Bob performs a Hadamard operation on B. Alice and Bob keep A' and B', and send A and B to the third party Charlie for BSM through two identical quantum channels.

M2: After Charlie completes the BSM of all states, Alice and Bob publicly announce K^A an K^B. At each time j, when $k_j^A \neq k_j^B$, that is, they use different bases, they discard the corresponding ancillary qubits. If both of them use Z bases, and detectors $D_{LH}D_{LV}$ or $D_{RH}D_{RV}$ click, they need do nothing to their ancillary qubits. If detectors $D_{LH}D_{RV}$ or $D_{RH}D_{LV}$ click, Alice or Bob performs σ_Z on his ancillary qubit. If both of them use X bases, and detectors $D_{LH}D_{LV}$ or $D_{RH}D_{RV}$ click, Alice or Bob performs σ_Z on his ancillary qubit. If detectors $D_{LH}D_{RV}$ or $D_{RH}D_{LV}$ click, one of them perform $\sigma_X\sigma_Z$ on the ancillary qubit. After this step, A' and B' are quantum correlated.

M3: Alice and Bob use EDP or quantum CSS code to distill EPR pairs with fidelity of 100% from $A'B'$ polluted by channel noise. Finally, Alice and Bob conduct Z measurement on the distilled EPR pairs to obtain a set of shared random numbers.

In conventional BB84-QKD and MDI-QKD, the use of MUBs is to ensure the security of quantum key by the uncertainty principle of quantum mechanics. In the above protocols based on virtual entanglement, we can see that both Z basis and X basis can be used to estimate the BER and PER of the channels, and these two bases play the same role in the generation of key.

IV. SECURITY ANALYSIS OF MDI-QKD BASED ON ENTANGLEMENT DISTILLATION PROTOCOL

In the following, we will use the virtual protocol to analyze the security of practical MDI-QKD. Since PR-WCPs is equivalent to the Poisson distributed PNs in BSM, we will deduce the EDP-based key rate of MDI-QKD in Fock state representation. In Z basis, the non normalized joint state sent by Alice and Bob to Charlie is

$$|\Upsilon\rangle_{m,n}^Z = \frac{A_m A_n}{2\sqrt{m!n!}}[|0\rangle_{A'}(\hat{a}_H^+)^m + |1\rangle_{A'}(\hat{a}_V^+)^m] \otimes [|0\rangle_{B'}(\hat{b}_H^+)^m + |1\rangle_{B'}(\hat{b}_V^+)^m]|0\rangle, \tag{8}$$

where m, n are the photon numbers sent by Alice and Bob, A_m, A_n are the probability amplitudes of the corresponding photon number states, $\hat{a}_H^+, \hat{a}_V^+$ are the generation operators of the photon state of horizontal and vertical polarizations at Alice, and $\hat{b}_H^+, \hat{b}_V^+$ are the generation operators at Bob. Considering the effective detection events in Table I, after the PNs passing through the BSM setup, the following state can be obtained

$$\begin{aligned}|\Upsilon\rangle_{m,n}^Z = \frac{\sqrt{2}A_m A_n}{\sqrt{m!n!}}\left(\frac{\sqrt{2}}{2}\right)^{m+n} &[(|\Psi^+\rangle + |\Psi^-\rangle)(i\hat{d}_{1H}^+ + \hat{d}_{2H}^+)^m \\ &\times (\hat{d}_{1V}^+ + i\hat{d}_{2V}^+)^n + (|\Psi^+\rangle - |\Psi^-\rangle)(i\hat{d}_{1V}^+ + \hat{d}_{2V}^+)^m \\ &\times (\hat{d}_{1H}^+ + i\hat{d}_{2H}^+)^n]|0\rangle,\end{aligned} \tag{9}$$

where $\hat{d}_{jH}^+, \hat{d}_{jV}^+$ are the generation operators of the states at D_{jH}, D_{jV} with $j = 1, 2$. For $m = n = 1$, this is equivalent to the ideal MDI-QKD

$$\begin{aligned}|\Upsilon\rangle_{1,1}^Z = \frac{\sqrt{2}A_1 A_1}{2}&[(\hat{d}_{1H}^+\hat{d}_{1V}^+ + \hat{d}_{2H}^+\hat{d}_{2V}^+)|\Psi^+\rangle \\ &+ (\hat{d}_{1H}^+\hat{d}_{2V}^+ + \hat{d}_{2H}^+\hat{d}_{1V}^+)|\Psi^-\rangle]|0\rangle,\end{aligned} \tag{10}$$

so that Eq. (10) is equivalent to the BSM of the Z basis in Table I, and the symbol Ψ denotes the anticorrelation between ancillary qubits A' and B'. Here we set $|\Phi^+\rangle$ as the standard Bell state, that is, the final Bell state to be obtained by entan-

glement distillation. Hence, if $D_{1H}D_{1V}$ or $D_{2H}D_{2V}$ click, Alice or Bob need to perform σ_X operation on the ancillary qubit, if $D_{1H}D_{2V}$ or $D_{2H}D_{1V}$ click, Alice or Bob need to perform $\sigma_X\sigma_Z$ operation on the ancillary qubit. For Poisson distributed PNs, in addition to the single-photon state, there will be the situations that Alice or Bob send a multiphoton state. Actually, Alice and Bob can not tell the number of photons they have sent at each time, but only know the probability distribution of the photon number states. Therefore, they treat every effective detection result as generated by single-photon states. Besides, in Z basis, sending vacuum state on either side can not produce effective detection events.

In WCPs assumption, we only focus on the joint states with $m \geqslant 1, n \geqslant 1$ and $m+n \leqslant 4$, any contributions from $m+n>4$ can be incorporated into the high-order infinitesimal term $O(\rho^Z_{m+n>4})$. If $m \neq n$, after Charlie's measurement, the joint state of Alice and Bob will reduce to the mixed state of $|\Phi^+\rangle + |\Phi^-\rangle$ and $|\Phi^+\rangle - |\Phi^-\rangle$. Before entanglement distillation, Alice and Bob first use bilateral rotation operation to transform the mixed state into the mixture of Bell states. After this step, we can get the following non-normalized density of state with Bell state diagonalization in Z basis conditioned on Charlie's detection results:

$$\begin{aligned}
\rho^Z_{1,1} &= \frac{Q_{1,1}}{2}\rho_{\Phi^+}, \quad \rho^Z_{1,2} = \rho^Z_{2,1} = \frac{Q_{1,2}}{8}(\rho_{\Phi^+} + \rho_{\Phi^-}),\\
\rho^Z_{1,3} &= \rho^Z_{3,1} = \frac{Q_{1,3}}{16}(\rho_{\Phi^+} + \rho_{\Phi^-}),\\
\rho^Z_{2,2} &= \frac{Q_{2,2}}{16}(\rho_{\Phi^+} + \rho_{\Phi^-}),\\
O(\rho^Z_{m+n>4}) &\leqslant \frac{1}{2}(1 - \sum_{m+n=0}^{m+n=4} Q_{m,n})\frac{I}{4},
\end{aligned} \tag{11}$$

where $Q_{m,n} = Q_{n,m} = A_m^2 A_n^2$ is the collision probability when the state of A is $|m\rangle$ and the state of B is $|n\rangle$, $\rho_\Phi = |\Phi\rangle\langle\Phi|$ with $\Phi = \{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$, I is the identity operator $I = \rho_{\Phi^+} + \rho_{\Phi^-} + \rho_{\Psi^+} + \rho_{\Psi^-}$. In practical QKDs where the light is transmitted in fibers, then the probability amplitude is $A_m = e^{-\mu}\frac{\mu^m}{m!}$ with $\mu = \mu_0\eta_l\eta_d$, where μ_0 is the average photon number of the PR-WCPs sent by Alice and Bob, η_l is the transmittance of the quantum channel, η_d is the detection efficiency of the single-photon detectors. As all the transmission losses are incorporated into μ, the triple detectors click events are regarded as invalid. Then the total non-normalized density of states of $A'B'$ is the sum of each term in Eq. (11)

$$\rho^Z = \sum_{m=1,n=1}^{m+n=4} \rho^Z_{m,n} + O\big(\rho^Z_{m+n>4}\big). \tag{12}$$

We can see that even though no bit flip error occurs in Z basis, there are still phase flip errors caused by multiphoton states.

If the PNs are prepared in X basis, Alice and Bob perform Hadamard operations on A and B to transform Eq. (8) into the following form:

$$\begin{aligned}
|\Upsilon\rangle^X_{m,n} = \frac{A_m A_n}{2\sqrt{m!n!}}&[|0\rangle_{A'}(\hat{a}^+_+)^m + |1\rangle_{A'}(\hat{a}^+_-)^m]\\
&\otimes [|0\rangle_{B'}(\hat{b}^+_+)^n + |1\rangle_{B'}(\hat{b}^+_-)^n]|0\rangle,
\end{aligned} \tag{13}$$

where $\hat{a}^+_+, \hat{a}^+_-$ are the generation operators of states $|+\rangle$ and $|-\rangle$ at Alice, and $\hat{b}^+_+, \hat{b}^+_-$ are the generation operators at Bob. Here it should be noted that even though the PR-WCPs are prepared in $\pm 45^\circ$ polarizations, but the final measurement of BSM is completed in Z basis. This leads to the fact that the BSM of PNs in X basis is more complex than that in Z basis, and the gains and error rates may differ in these two bases. For example, in X basis, the cases that one of Alice and Bob sends a two-photon state while the other sends a vacuum state also contribute to the effective detection events. In WCPs approximation, we may reasonably assume that the effective detection events in X basis are mainly contributed by the cases of $2 \leqslant m+n \leqslant 4$. We first discuss the case of $m = n = 1$, which is also equivalent to the ideal case. The joint state after the PNs passing through the BSM setup is

$$\begin{aligned}
|\Upsilon\rangle^X_{1,1} = -\frac{\sqrt{2}A_1A_1}{4}&[|\Phi^-\rangle(d^+_{1H}d^+_{1V} + d^+_{2H}d^+_{2V}) + i|\Psi^-\rangle\\
&\times (d^+_{1H}d^+_{2V} + d^+_{2H}d^+_{1V})]|0\rangle.
\end{aligned} \tag{14}$$

In the assumption that $|\Phi^+\rangle$ is the standard Bell state, when $D_{1H}D_{1V}$ or $D_{2H}D_{2V}$ click, Alice or Bob perform the σ_Z operation on the ancillary qubit, and if $D_{1H}D_{2V}$ or $D_{2H}D_{1V}$ click, Alice or Bob perform the $\sigma_X\sigma_Z$ operation. Cases such as $m = 0, n = 2$ or $m = 2, n = 0$ are also of concern because they have the same collision probability as $m = n = 1$ in the light source, and they are the main sources of BER and PER in X basis. The non-normalized joint state with $m = 0, n = 2$ after PNs passing through the BSM setup is

$$\begin{aligned}
|\Upsilon\rangle^X_{0,2} = -\frac{A_0A_2}{4}&(|\Phi^-\rangle - |\Psi^-\rangle)(-id^+_{1H}d^+_{1V} + id^+_{2H}d^+_{2V}\\
&+ d^+_{1H}d^+_{2V} + d^+_{2H}d^+_{1V})|0\rangle,
\end{aligned} \tag{15}$$

the ancillary qubits reduce to a pure state $(|\Phi^-\rangle - |\Psi^+\rangle)$ conditioned on Charlie's effective detection results. Since the values of m and n are unknown, Alice and Bob can only perform appropriate operations according to the measurement results announced by Charlie. Then Alice and Bob use bilateral rotation to transform $A'B'$ into a mixture of Bell states. Following the same steps, we can get the density of states in different cases

$$\begin{aligned}
\rho^X_{1,1} &= \frac{Q_{1,1}}{2}\rho_{\Phi^+},\\
\rho^X_{0,2} &= \rho^X_{2,0} = \frac{Q_{0,2}}{4}(\rho_{\Phi^+} + \rho_{\Psi^+}),\\
\rho^X_{0,3} &= \rho^X_{3,0} = \frac{3Q_{0,3}}{32}(\rho_{\Phi^+} + \rho_{\Phi^-} + \rho_{\Psi^+} + \rho_{\Psi^-}),\\
\rho^X_{1,2} &= \rho^X_{2,1} = \frac{Q_{1,2}}{32}(9\rho_{\Phi^+} + 9\rho_{\Phi^-} + \rho_{\Psi^+} + \rho_{\Psi^-}),\\
\rho^X_{0,4} &= \rho^X_{4,0} = \frac{Q_{0,4}}{64}(4\rho_{\Phi^+} + 3\rho_{\Phi^-} + 4\rho_{\Psi^+} + 3\rho_{\Psi^-}),\\
\rho^X_{1,3} &= \rho^X_{3,1} = \frac{Q_{1,3}}{16}(4\rho_{\Phi^+} + 3\rho_{\Phi^-} + \rho_{\Psi^+}),\\
\rho^X_{2,2} &= \rho^X_{2,2} = \frac{Q_{2,2}}{64}(12\rho_{\Phi^+} + 18\rho_{\Phi^-} + \rho_{\Psi^-}),\\
O\big(\rho^X_{m+n>4}\big) &= O\big(\rho^Z_{m+n>4}\big).
\end{aligned} \tag{16}$$

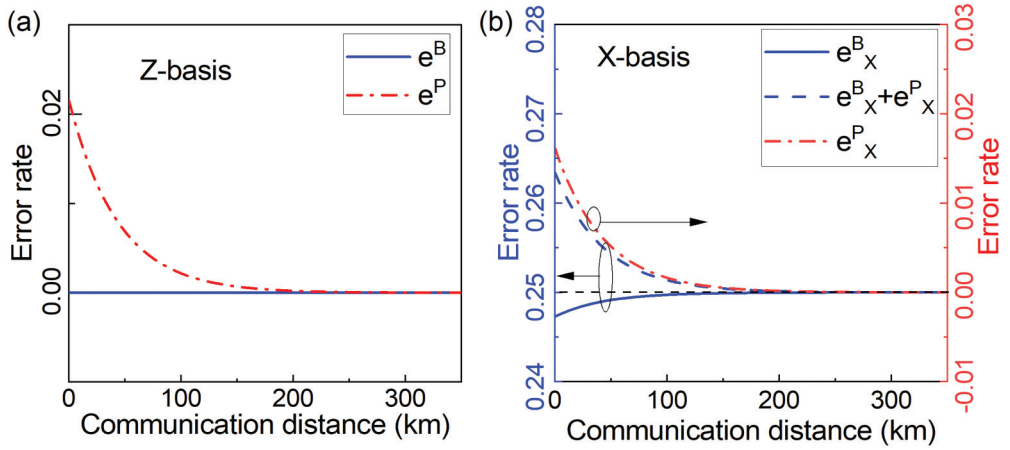

FIG. 3. Comparison of BER and PER in (a) Z basis and (b) X basis. In this figure, the average photon number μ is set to 0.3 when the communication distance is 0 km.

The total density of states of $A'B'$ for entanglement distillation in X basis is

$$\rho^X = \sum_{m+n=2}^{m+n=4} \rho^X_{m,n} + O\left(\rho^X_{m+n=4}\right). \tag{17}$$

By comparing Eqs. (16), (17) and Eqs. (11), (12), we can find that the density of states for $A'B'$ in X basis is different from that in Z basis, so the parameters such as BER, PER, and measurement gain between these two bases are not correlated.

V. KEY RATE OF MDI-QKD

From the viewpoint of security analysis based on EDP, there are two factors that affect the key rate of QKD: the gain of the measurement; the BER and PER caused by various channel noise. There has been a lot of evidence that in PR-WCPs-based MDI-QKD, the measurement parameters in Z basis and X basis are not correlated. This can be reflected in the large error rate difference between these two bases. Figure 3 shows the BER and PER with respect to the communication distance in Z basis and X basis, the simulation data in this figure are taken from Eqs. (11) and (16). Here, the photons are assumed to be transmitted in two identical optical fibers with a transmission loss coefficient of $\beta_l = 0.2$ dB/km, and the corresponding quantum channel transmittance is $\eta_l = 10^{-\frac{\beta_l L}{10}}$ where L is the transmission distance. In addition, we only consider the influence of BSM of PNs on entanglement distillation, and ignore the influence of any noise from quantum channel and detection. Then one can find that the transmission distance is actually related to the intensity of the PR-WCPs. The average photon number μ is set to 0.3 at the transmission distance of 0 km.

In this figure, we can see that the virtual channel for EDP is asymmetrical in both bases, and the BER and PER between these two bases are not correlated. In Z basis, as shown in Fig. 3(a), the PER e^P_Z is almost 0 at low light intensity and increases with the light intensity, while BER e^B_Z is equal to 0 in the whole communication distance, which is consistent with the prediction of the BER in Table I. Therefore, in Z basis, the BSM of PR-WCPs could generate finite PER that will influence the rate of entanglement distillation. In X basis, as shown in Fig. 3(b), the maximum value of BER e^B_X is 0.25 and decreases with light intensity. While the value of e^P_X has the similar light intensity dependence as e^P_Z but with a lower increasing rate. In X basis, as the total error rate $e^B_X + e^P_X$ increases with the light intensity, so the rate of entanglement distillation will decrease at a higher value of μ. Considering the practical error correction inefficiency, almost no Bell states can be distilled in X basis.

By comparing Fig. 3 and Table I, we find a counterintuitive phenomenon that under a relative high light intensity, the BER obtained by EDP deviates from that obtained by prepare-and-measure schemes. Here, the prepare-and-measure scheme is that both Alice and Bob prepare a quantum state, and send them to Charlie for measurement. In Table I, we have $e^B_Z = 0$ and $e^B_X = 25\%$ and both of them are light intensity independent, the BER in Z basis is consistent with that in Fig. 3, but the BER in X basis is inconsistent with that in Fig. 3. This means that due to the imperfection of BSM, the commutation relation between bit measurement and quantum operations, such as bit error correction and phase error correction, in EDP-based security proof is not always valid. The results in Table I corresponding to the case that bit measurement is conducted before entanglement swapping, while the results in Fig. 3 correspond to the case that Z basis is conducted after entanglement swapping. This deviation is totally caused by multiphoton terms and it will disappear when the light intensity decreases.

Another factor that affects the key rate is the gain of the measurement results. Figure 4 shows the comparison of the measurement gains between Z basis and X basis for $\mu = 0.2$ and $\mu = 0.5$ in logarithmic coordinate. In this figure, we can see that all the measurement gains satisfy the linear bound of QKDs with the particle nature of light as the information carrier and they are proportional to the channel transmittance. Under the same light intensity, the Z basis and the X basis have different measurement gains, Q_X is almost twice that of Q_Z. Therefore, not only the bit error rates and phase error rates are uncorrelated between these two bases, but also their

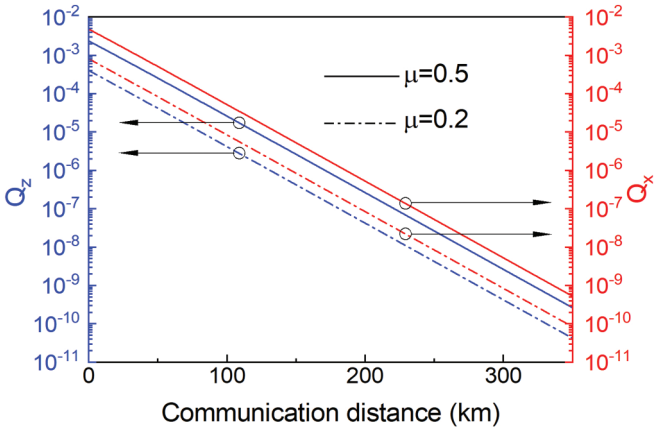

FIG. 4. Gain comparison between Z basis (blue curves) and X basis (red curves) for $\mu = 0.2$ and $\mu = 0.5$ in logarithmic coordinate.

measurement gains are unequal. So, the conventional conjugation measurement in the EDP-based security proof is questionable here.

According to the virtual protocol of MDI-QKD, one way to solve the above problems is to mix the measurement results of Z basis and X basis. In this case, the total density of states of $A'B'$ is the average of that in Z basis and X basis,

$$\begin{aligned}\rho &= \tfrac{1}{2}(\rho^Z + \rho^X)\\ &= p_{\Phi^+}\rho_{\Phi^+} + p_{\Phi^-}\rho_{\Phi^-} + p_{\Psi^+}\rho_{\Psi^+} + p_{\Psi^-}\rho_{\Psi^-},\end{aligned} \tag{18}$$

where p_Φ is the gain of state ρ_Φ. In addition to the errors caused by BSM of PR-WCPs, there are also other errors due to the imperfection of practical experiments, such as dark counts of single-photon detectors, optical misalignment errors. Assume that the four independent single-photon detectors have the same dark count rate p_d, and the error rate of dark counts is $\frac{1}{2}$, and the gain contributed by dark counts is $4p_d^2$. The optical misalignment rate e_d caused bit flip error rate and phase flip error rate are

$$\begin{aligned}e^B_{\text{mis}} &= (p_{\Phi^+} + p_{\Phi^-} - p_{\Psi^+} - p_{\Psi^-})e_d,\\ e^P_{\text{mis}} &= (p_{\Phi^+} + p_{\Psi^+} - p_{\Phi^-} - p_{\Psi^-})e_d.\end{aligned} \tag{19}$$

Equation (19) is the state density of entanglement swapping for virtual entanglement protocol. From Fig. 3, we know that the multiphoton terms will cause the decrease of e^B_X. Thus, in order to make the bit error correction consistent with the experiment results, as predicted in Table I, we set the BER and PER as

$$\begin{aligned}e^B &= \frac{0.25 \times 0.5 \times Q_X + e^B_{\text{mis}} + 2p_d^2}{Q},\\ e^P &= \frac{p_{\Phi^-} + p_{\Psi^-} + e^P_{\text{mis}} + 2p_d^2}{Q},\end{aligned} \tag{20}$$

where 0.25 is the BER in X basis measured in experiment, as shown in Table I, 0.5 is the probability that the quantum state is prepared in X basis, Q is the total gain

$$Q = p_{\Phi^+} + p_{\Phi^-} + p_{\Psi^+} + p_{\Psi^-} + 4p_d^2. \tag{21}$$

As the PER e^P increases with the average photon number, thus e^P in Eq. (20) sets the upper bound of the privacy amplification. So the key rate is lower bound by

$$r \geqslant Q[1 - f * H(e^B) - H(e^P)], \tag{22}$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy of the variable x, f is the error correction efficiency, which always satisfies $f \geqslant 1$.

Figure 5 shows the simulation of the light-intensity-dependent key rate of PR-WCPs based MDI-QKD and its comparison with the GLLP scheme. The parameters used for simulation fully consider the current laboratory technology, in which the dark count rate $p_d = 8 \times 10^{-8,}$, the error correction inefficiency $f = 1.15$, detector efficiency $\eta_d = 14.5\%$, misalignment error $e_d = 1.5\%$. In Fig. 5(a), we can see that at long communication distance the key rate satisfies the linear bound. While at short communication distance, the key rate deviates from the linear bound with the increase of light intensity. Due to the linear relationship between the average photon number μ and the channel transmittance, as well as the explicit functional dependence of the measurement gain, BER and PER on μ, so the key rate curve under different light intensities can be obtained by translating one of them in the horizontal direction. Under high light intensity, the rate first increases and then decreases with the communication distance, this is due to the increased proportion of the multiphoton terms. However, this phenomenon is contrary to the nonincreasing of information in the process of information processing and transmission, and this will also bring the risk of beam-separation (BS) attacks. Here we choose the maximum value of the key rate as the starting point of communication. In this simulation, we find that the maximum value of the key rate corresponds to $\mu = 0.311$.

In Fig. 5(b), we give the comparison between the key rate of this work and that obtained by GLLP scheme with infinite decoy-state method [27,43]. In this figure, it can be seen that in most of the communication distance, the key rate obtained in this work is less than that obtained by the GLLP bound. Actually, the GLLP scheme also uses the idea of entanglement distillation, and this scheme assumes that all the absolutely secure information is carried by the single-photon states. In this way, it seems that our work should get a higher key rate than GLLP scheme. The main reason for this opposite result is the way these two models deal with the imperfection of the BSM caused by nonideal sources. Our work makes the worst assumption about the imperfection of these experimental devices in key extraction, and considers that the imperfection of BSM caused large values of BER and PER to be able to be utilized by the eavesdroppers. While in GLLP scheme, the noncorrelation of the measurement results between Z basis and X basis are not considered in key generation. Therefore, a tighter key rate bound is obtained in this work, and our work proves that even in the case of imperfect BSM, the PR-WCPs-based MDI-QKD is still secure.

The imperfection of the light source will also provide Eve with the opportunity of photon-number-splitting (PNS) attacks, where Eve is assumed to be able to control the probability distribution, error rate and the yield of the photon number states. At present, the best tool to deal with PNS attacks is the decoy-state method [12–14,40], which is widely used in BB84-QKD [13,40], MDI-QKD [16,17,43], and PM-QKD [27], and has achieved great success. In stan-

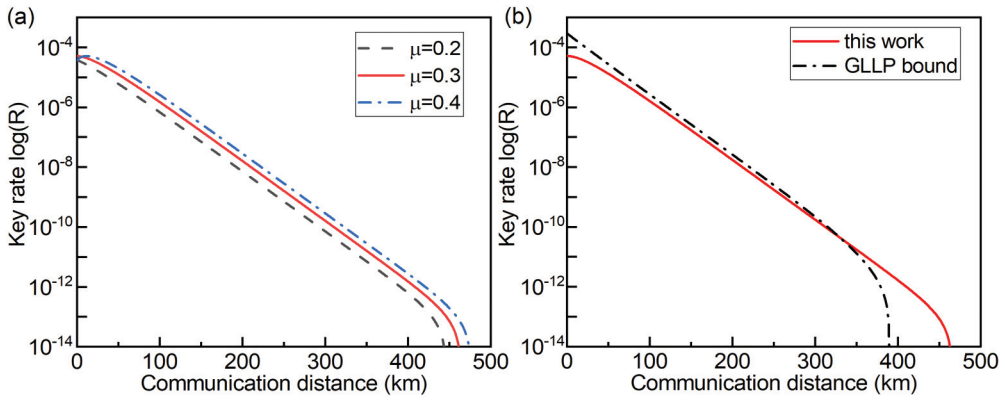

FIG. 5. (a) Dependence of key rate on the average photon number μ, (b) Key rate comparison for MDI-QKD between this work and that obtained by GLLP scheme with decoy state method [43].

dard decoy-state QKD systems, the probability distribution is considered to be known, while the error rate and yield of the photon number states need to be determined from the experiment results, so as to exclude Eve's invasion. According to Eqs. (11), (16), it can be seen that the measurement gain Q, BER e^B and PER e^P in Eq. (22) are related to parameters $Q_{i,j}$ with $i, j \in \{0, 1, 2, 3, 4\}$, which we need to estimate through decoy-state method. The details of the estimation of these parameters is provided in Appendix D.

VI. CONCLUSION

In this paper, we have given the security analysis of PR-WCPs-based MDI-QKD, and derive the corresponding key rate. By analyzing the HOM effect of PR-WCPs and PNs, we get that these two light source are equivalent in MDI-QKD, that is to say, the security of practical MDI-QKD can be equivalently analyzed in these two source models. We then use the BSM results of PR-WCPs to construct the *a posteriori* decoding probability table of MDI-QKD, and find that the BER in X basis is larger than 25%, which is caused by the mismatch between state preparation and measurement. The large error rate difference between Z basis and X basis caused by measurement indicates that the key rate formula derived in BB84-QKD can not be directly used in MDI-QKD. The security analysis of MDI-QKD based on EDP is carried out on PNs, where the final virtual ancillary qubits is the mixed average of that obtained in Z basis and X basis, so as to ensure that the finite key rate can be extracted under the given BER and PER. Finally, we compare the key rate in this work with that obtained by GLLP scheme. The key rate in this work deviates from the linear key rate bound in a short communication distance and is lower than that obtained by GLLP scheme. Because we consider all inevitable errors caused by imperfect measurement as possible eavesdropping risks, this work provides a tighter key rate bound for practical PR-WCPs-based MDI-QKD.

ACKNOWLEDGMENTS

This work is supported by China Postdoctoral special funding project (2020T130289), the National Natural Science Foundation of China (No. 61871234).

APPENDIX A: HOM INTERFERENCE OF GAUSSIAN-SHAPED PNs

The experimental setup of HOM interference of the PNs is given in the inset of Fig. 2. PNs is the mixture of photon number state that at each time photon number state $|m\rangle$ is sent out, m is the number of photons. Assume that at one time there are m photons incident on tha a-side of the BS and n photons incident on the b-side of the BS, the incident photon number state is $|m\rangle_a|n\rangle_b = \frac{1}{\sqrt{m!n!}}(a^+)^m(b^+)^n|0\rangle$, and all the photon states have the same spatial mode and frequency spectrum. For Gaussian-shaped pulses, then the photon state in time domain can be written as

$$|\Psi_{m,n}\rangle = \left(\frac{2\Gamma}{\pi}\right)^{\frac{m+n}{4}} \int_{-\infty}^{\infty} dt_1 \cdots \int_{-\infty}^{\infty} dt_m \int_{-\infty}^{\infty} dt_{m+1} \cdots \int_{-\infty}^{\infty} dt_n e^{-\Gamma(t_1-t_0)^2} \cdots e^{-\Gamma(t_m-t_0)^2} e^{-\Gamma(t_{m+1}-\tau_0)^2} \cdots e^{-\Gamma(t_{m+n}-\tau_0)^2} a^+_{t_1} \cdots a^+_{t_m} b^+_{t_{m+1}} \cdots b^+_{t_{m+n}}|0\rangle, \tag{A1}$$

where t_0 and τ_0 are the centers of the pulses sent by Alice and Bob in the time domain, respectively. For the convenience of discussion, here we use the function $f(t)$ to represent $e^{-\Gamma(t-t_0)^2}$ and $g(t)$ to represent $e^{-\Gamma(t-\tau_0)^2}$. In the case of $m = n = 1$, which is the most standard HOM interference, then we have

$$|\Psi_{1,1}\rangle = \sqrt{\frac{2\Gamma}{\pi}} \int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 f(t_1) g(t_2) a^+_{t_1} b^+_{t_2}|0\rangle. \tag{A2}$$

Because there are two time variables in Eq. (A2), it is not a good form to analyze HOM interference. Here we first make a transform to the integral in Eq. (A2),

$$\begin{aligned}\Psi_{1,1} &= \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{-\infty}^{\infty}dt_2 f(t_1)g(t_2)\\ &= \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{-\infty}^{t_1}dt_2 f(t_1)g(t_2)+\sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{t_1}^{\infty}dt_2 f(t_1)g(t_2)\\ &= \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{-\infty}^{0}d\tau f(t_1)g(t_1+\tau)+\sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau f(t_1)g(t_1+\tau),\end{aligned} \tag{A3}$$

where τ is the time difference between t_1 and t_2, and Eq. (A3) can be further transformed to

$$\begin{aligned}\Psi_{1,1} &= \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau f(t_1)g(t_1-\tau)+\sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau f(t_1)g(t_1+\tau)\\ &= \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau f(t_1+\tau)g(t_1)+\sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau f(t_1)g(t_1+\tau)\\ &= \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau[f(t_1+\tau)g(t_1)+f(t_1)g(t_1+\tau)].\end{aligned} \tag{A4}$$

Here we denote $f(t_1+\tau)g(t_1)$ as A_1 and $f(t_1)g(t_1+\tau)$ as A_2, after the photon states passing through the BS, the joint state is

$$|\Psi_{1,1}\rangle = \sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau A_1\frac{ic^{+}_{L,t_1+\tau}+c^{+}_{R,t_1+\tau}}{\sqrt{2}}\frac{c^{+}_{L,t_1}+ic^{+}_{R,t_1}}{\sqrt{2}}|0\rangle+\sqrt{\frac{2\Gamma}{\pi}}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau A_2\frac{ic^{+}_{L,t_1}+c^{+}_{R,t_1}}{\sqrt{2}}\frac{c^{+}_{L,t_1+\tau}+ic^{+}_{R,t_1+\tau}}{\sqrt{2}}|0\rangle \tag{A5}$$

Then the coincidence count rate is

$$\begin{aligned}p_{1,1} &= \langle\Psi_{1,1}|\hat{P}(1_{L,t_1},1_{R,t_1+\tau})+\hat{P}(1_{L,t_1+\tau},1_{R,t_1})|\Psi_{1,1}\rangle = \frac{\Gamma}{\pi}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau|A_1-A_2|^2\\ &= \frac{\Gamma}{\pi}\int_{-\infty}^{\infty}dt_1\int_{0}^{\infty}d\tau(|A_1|^2+|A_2|^2-A_1^*A_2-A_1A_2^*),\end{aligned} \tag{A6}$$

where $\hat{P}(1_{L,t},1_{R,t'})=|1_{L,t},1_{R,t'}\rangle\langle 1_{L,t},1_{R,t'}|$ is the projection operator that one photon appears at time t on the left side and the other photon appears at time t' on the right side. As

$$|A_1|^2+|A_2|^2 = e^{-4\Gamma\left(t_1+\frac{\tau-t_0-\tau_0}{2}\right)}(e^{-\Gamma(\tau-t_0+\tau_0)}+e^{-\Gamma(\tau+t_0-\tau_0)}), \tag{A7}$$

and

$$A_1^*A_2+A_1A_2^* = 2e^{-4\Gamma\left(t_1+\frac{\tau-t_0-\tau_0}{2}\right)^2}e^{-\Gamma\tau^2}e^{-\Gamma(t_0-\tau_0)^2}, \tag{A8}$$

then we have

$$\begin{aligned}p_{1,1} &= \frac{\Gamma}{\pi}\int_{-\infty}^{\infty}\infty_0^{\infty}\left(|A_1|^2+|A_2|^2-A_1^*A_2-A_1A_2^*\right)\\ &= \frac{\Gamma}{\pi}\int_{-\infty}^{\infty}e^{-4\Gamma\left(t_1+\frac{\tau-t_0-\tau_0}{2}\right)}dt_1\int_{-\infty}^{\infty}e^{-\Gamma(\tau-t_0+\tau_0)}d\tau-\frac{\Gamma}{\pi}\int_{-\infty}^{\infty}e^{-4\Gamma\left(t_1+\frac{\tau-t_0-\tau_0}{2}\right)^2}dt_1\int_{-\infty}^{\infty}e^{-\Gamma\tau^2}d\tau e^{-\Gamma(t_0-\tau_0)^2}\\ &= \frac{1}{2}\left(1-e^{-\Gamma(t_0-\tau_0)^2}\right).\end{aligned} \tag{A9}$$

In the three-photon HOM interference, the case of $m=1,n=2$ is equivalent to the case of $m=2,n=1$. In the following, we will analyze the first case,

$$|\Psi_{1,2}\rangle = \left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}}\int_{-\infty}^{\infty}dt_1\int_{-\infty}^{\infty}dt_2\int_{-\infty}^{\infty}dt_3 f(t_1)g(t_2)g(t_3)a^{+}_{t_1}b^{+}_{t_2}b^{+}_{t_3}|0\rangle. \tag{A10}$$

According to the method above, we should first perform a transformation on the integral form in Eq. (A10). For the triple integral A of any three functions, we first transform the integral variables of the first and second functions like that in Eq. (A4)

$$\begin{aligned} A &= \int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 \int_{-\infty}^{\infty} dt_3 f(t_1) g(t_2) h(t_3) \\ &= \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{-\infty}^{\infty} dt_3 f(t_1) g(t_1 - \lambda) h(t_3) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{-\infty}^{\infty} dt_3 f(t_1) g(t_1 + \lambda) h(t_3). \end{aligned} \tag{A11}$$

By changing the variable t_1 to $t_1 + \lambda$ in the second line of Eq. (A11), we obtain

$$A = \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{-\infty}^{\infty} dt_3 f(t_1 + \lambda) g(t_1) h(t_3) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{-\infty}^{\infty} dt_3 f(t_1) g(t_1 + \lambda) h(t_3). \tag{A12}$$

Following the same procedures, we can obtain the transformation of the third variable,

$$\begin{aligned} A = &\int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda) g(t_1) h(t_1 + \lambda - \gamma) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda) g(t_1) h(t_1 + \lambda + \gamma) \\ &+ \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1) g(t_1 + \lambda) h(t_1 + \lambda - \gamma) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1) g(t_1 + \lambda) h(t_1 + \lambda + \gamma). \end{aligned} \tag{A13}$$

By changing the variable t_1 to $t_1 + \gamma$ in the first and third lines of Eq. (A13), we obtain

$$\begin{aligned} A = &\int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda + \gamma) g(t_1 + \gamma) h(t_1 + \lambda) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda) g(t_1) h(t_1 + \lambda + \gamma) \\ &+ \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \gamma) g(t_1 + \lambda + \gamma) h(t_1 + \lambda) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1) g(t_1 + \lambda) h(t_1 + \lambda + \gamma). \end{aligned} \tag{A14}$$

According to the transformation order of integral variables, the above integral can also be transformed into

$$\begin{aligned} A = &\int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 \int_{-\infty}^{\infty} dt_3 f(t_1) g(t_2) h(t_3) \\ = &\int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda + \gamma) g(t_1 + \lambda) h(t_1 + \gamma) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda) g(t_1 + \lambda + \gamma) h(t_1) \\ &+ \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \gamma) g(t_1 + \lambda) h(t_1 + \lambda + \gamma) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1) g(t_1 + \lambda + \gamma) h(t_1 + \lambda), \end{aligned} \tag{A15}$$

and

$$\begin{aligned} A = &\int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 \int_{-\infty}^{\infty} dt_3 f(t_1) g(t_2) h(t_3) \\ = &\int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda) g(t_1 + \lambda + \gamma) h(t_1 + \gamma) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda + \gamma) g(t_1 + \lambda) h(t_1) \\ &+ \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda) g(t_1 + \gamma) h(t_1 + \lambda + \gamma) + \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma f(t_1 + \lambda + \gamma) g(t_1) h(t_1 + \lambda). \end{aligned} \tag{A16}$$

It is found that there are 12 integrands after transformation. According to the order in which the integrands appear above, we mark the ith integrand as A_i. As $g(x) = h(x)$, we have $A_1 = A_5, A_2 = A_6, A_3 = A_7, A_4 = A_8, A_9 = A_{11}$, and $A_{10} = A_{12}$. In addition, the integral transformation does not change the normalization of the integrand function, so we have

$$\begin{aligned} \left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma \left(A_1^2 + A_2^2 + A_3^2 + A_4^2\right) = 1, \\ \left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma \left(A_5^2 + A_6^2 + A_7^2 + A_8^2\right) = 1, \\ \left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \int_{-\infty}^{\infty} dt_1 \int_{0}^{\infty} d\lambda \int_{0}^{\infty} d\gamma \left(A_9^2 + A_{10}^2 + A_{11}^2 + A_{12}^2\right) = 1. \end{aligned} \tag{A17}$$

Then the joint state of Eq. (A10) can be written as

$$
\begin{aligned}
|\Psi_{1,2}\rangle = {} & \sqrt{6}\left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \iiint dt_1 d\lambda d\gamma (A_1 + A_5) a^+_{t_1+\lambda+\gamma} b^+_{t_1+\lambda} b^+_{t_1+\gamma} + \sqrt{6}\left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \iiint dt_1 d\lambda d\gamma (A_2 + A_6) a^+_{t_1+\lambda} b^+_{t_1+\lambda+\gamma} b^+_{t_1} \\
& + \sqrt{6}\left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \iiint dt_1 d\lambda d\gamma (A_3 + A_7) a^+_{t_1+\gamma} b^+_{t_1+\lambda} b^+_{t_1+\lambda+\gamma} + \sqrt{6}\left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \iiint dt_1 d\lambda d\gamma (A_4 + A_8) a^+_{t_1} b^+_{t_1+\lambda+\gamma} b^+_{t_1+\lambda} \\
& + \sqrt{6}\left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \iiint dt_1 d\lambda d\gamma (A_9 + A_{11}) a^+_{t_1+\lambda} b^+_{t_1+\gamma} b^+_{t_1+\lambda+\gamma} + \sqrt{6}\left(\frac{2\Gamma}{\pi}\right)^{\frac{3}{4}} \iiint dt_1 d\lambda d\gamma (A_{10} + A_{12}) a^+_{t_1+\lambda+\gamma} b^+_{t_1} b^+_{t_1+\lambda}.
\end{aligned}
\tag{A18}
$$

In Eq. (A18), the integral ranges of the three variables are the same as that in Eqs. (A15)–(A17), and $\sqrt{6}$ is the normalization constant. Here, the transformation matrix of the BS is

$$
\begin{pmatrix} c_L^+ \\ c_R^+ \end{pmatrix} = \frac{\sqrt{2}}{2} \begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix} \begin{pmatrix} a^+ \\ b^+ \end{pmatrix}. \tag{A19}
$$

After the photon states pass through the BS, the coincidence count rate for $m = 1, n = 2$ is

$$
\begin{aligned}
p_{1,2} = {} & \langle \Psi_{1,2}| \sum_i P^i \hat{P}_{L,R}(1_{j,t_1}, 1_{j',t_1+\lambda}, 1_{j'',t_1+\lambda+\gamma}) \\
& + \sum_i P^i \hat{P}_{L,R}(1_{k,t_1+\lambda}, 1_{k',t_1+\gamma}, 1_{k'',t_1+\lambda+\gamma}) |\Psi_{1,2}\rangle,
\end{aligned}
\tag{A20}
$$

where $\hat{P}_{L,R}(1_{j,t_1}, 1_{j',t_2}, 1_{j'',t_3}) = |1_{j,t_1}, 1_{j',t_2}, 1_{j'',t_3}\rangle\langle 1_{j,t_1}, 1_{j',t_2}, 1_{j'',t_3}|$ is the projection operator of three photons at three different times on the left side and right side of the BS with $j, j', j'' \in \{L, R\}$, P^i is the permutation operator of L and R, but it should be ensured that all L or all R cannot occur. After complicated and lengthy calculations, we can get

$$
p_{1,2} = p_{2,1} = \tfrac{1}{4}\left(3 - 2e^{-\Gamma(t_0-\tau_0)^2}\right). \tag{A21}
$$

Similarly, we can also obtain the following HOM interference:

$$
\begin{aligned}
& p_{1,3} = p_{3,1} = \tfrac{1}{8}\left(7 - 3e^{-\Gamma(t_0-\tau_0)^2}\right), \\
& p_{2,2} = \tfrac{1}{8}\left(7 - 4e^{-\Gamma(t_0-\tau_0)^2} - e^{-2\Gamma(t_0-\tau_0)^2}\right), \\
& p_{0,2} = p_{2,0} = \tfrac{1}{2}, \quad p_{0,3} = p_{3,0} = \tfrac{3}{4}, \quad p_{0,4} = p_{4,0} = \tfrac{7}{8}.
\end{aligned}
\tag{A22}
$$

APPENDIX B: HOM INTERFERENCE OF PR-WCPs

Alice and Bob each prepare a Gaussian-shaped PR-WCPs, as given in Eq. (3), and send them to the BS for HOM interference. After passing the BS, the joint state is

$$
|\Upsilon\rangle_C = \left(\frac{2\Gamma}{\pi}\right)^{\frac{1}{4}} \int dt \left| i\sqrt{\frac{\mu_{t-t_0}}{2}} e^{i\theta_A} + \sqrt{\frac{\mu_{t-\tau_0}}{2}} e^{i\theta_B} \right\rangle_L \left| \sqrt{\frac{\mu_{t-t_0}}{2}} e^{i\theta_A} + i\sqrt{\frac{\mu_{t-\tau_0}}{2}} e^{i\theta_B} \right\rangle_R, \tag{B1}
$$

where θ_A and θ_B are the global random phases of Alice and Bob's PR-WCPs with $\theta_A, \theta_B \in [0, 2\pi]$. In the slow varying amplitude approximation, the time-dependent amplitudes μ_{t-t_0} and $\mu_{t-\tau_0}$ can be viewed as constants when θ_A and θ_B vary from 0 to 2π. When the light intensity μ is low enough, the detection probability of a WCP is proportional to μ, which can be reflected from the linear key rate bound in BB84-QKD. For any given θ_A, θ_B, the light intensity at the left side is

$$
I_L = \sqrt{\frac{\Gamma\mu^2}{\pi}} \int dt \left(e^{-2\Gamma(t-t_0)^2} + e^{-2\Gamma(t-\tau_0)^2} - 2\sin\theta_{AB} e^{-2\Gamma\left(t - \frac{t_0+\tau_0}{2}\right)^2 - \frac{\Gamma(t_0-\tau_0)^2}{2}} \right) = \frac{\sqrt{2}\mu}{2}\left(1 - e^{-\frac{\Gamma(t_0-\tau_0)^2}{2}} \sin\theta_{AB}\right). \tag{B2}
$$

where $\theta_{AB} = \theta_A - \theta_B$. Similarly, we can also obtain

$$
I_R = \frac{\sqrt{2}\mu}{2}\left(1 + e^{-\frac{\Gamma(t_0-\tau_0)^2}{2}} \sin\theta_{AB}\right). \tag{B3}
$$

Then the correlation of these two arms is

$$
\langle I_L I_R \rangle = \frac{\mu^2}{2} \int d\theta_{AB} \left(1 - e^{-\frac{\Gamma(t_0-\tau_0)^2}{2}} \sin\theta_{AB}\right)\left(1 + e^{-\frac{\Gamma(t_0-\tau_0)^2}{2}} \sin\theta_{AB}\right) = \frac{\mu^2}{2}\left(1 - \frac{1}{2} e^{-\Gamma(t_0-\tau_0)^2}\right). \tag{B4}
$$

The coincidence count rate of PR-WCPs is proportional to Eq. (B3).

APPENDIX C: BSM OF PR-WCPs

Assume that the PR-WCPs are prepared in Z basis, such as $|\sqrt{\mu}e^{i\alpha}\rangle_{A,H}\otimes|\sqrt{\mu}e^{i\beta}\rangle_{B,V}$, the joint state after passing through the BSM setup is

$$|\Upsilon_{AB}\rangle^{Z}_{H,V} = \left|\sqrt{\frac{\mu}{2}}ie^{i\alpha}\right\rangle_{1,H}\left|\sqrt{\frac{\mu}{2}}ie^{i\beta}\right\rangle_{1,V}\left|\sqrt{\frac{\mu}{2}}ie^{i\alpha}\right\rangle_{2,H}\left|\sqrt{\frac{\mu}{2}}ie^{i\beta}\right\rangle_{2,V}, \tag{C1}$$

from which we can see that the light at each output of the BSM is equal to a constant $\frac{\mu}{2}$, and the joint detection probability is proportional to the product of them

$$\langle I_{j,P}I_{j',P'}\rangle \propto \frac{\mu^2}{4}, \tag{C2}$$

where the subscripts $j, j' \in \{1,2\}$ and $P, P' \in \{H, V\}$.

If the PR-WCPs are prepared in X basis and have the same polarization, for example $|\sqrt{\mu}e^{i\alpha}\rangle_{A,+}\otimes|\sqrt{\mu}e^{i\beta}\rangle_{B,+}$, then the joint state after passing through the BSM is

$$|\Upsilon_{AB}\rangle^{X}_{+,+} = \left|\sqrt{\frac{\mu}{4}}\left(ie^{i\alpha}+e^{i\beta}\right)\right\rangle_{1,H}\otimes\left|\sqrt{\frac{\mu}{4}}i\left(ie^{i\alpha}+e^{i\beta}\right)\right\rangle_{1,V} \otimes\left|\sqrt{\frac{\mu}{4}}\left(e^{i\alpha}+ie^{i\beta}\right)\right\rangle_{2,H}\otimes\left|\sqrt{\frac{\mu}{4}}i\left(ie^{\alpha}+ie^{i\beta}\right)\right\rangle_{2,V}. \tag{C3}$$

The light intensity at each output is a function of $\alpha-\beta$,

$$I_{1,H} = I_{1,V} = \frac{\mu}{2}[1-\sin(\alpha-\beta)],$$
$$I_{2,H} = I_{2,V} = \frac{\mu}{2}[1+\sin(\alpha-\beta)], \tag{C4}$$

The joint detection probabilities are proportional to the second correlation of the light intensity at each output

$$\langle I_{1,H}I_{1,V}\rangle = \langle I_{2,H}I_{2,V}\rangle \propto \tfrac{3}{8}\mu^2,$$
$$\langle I_{1,H}I_{2,V}\rangle = \langle I_{2,H}I_{1,V}\rangle = \langle I_{1,H}I_{2,H}\rangle = \langle I_{1,V}I_{2,V}\rangle \propto \tfrac{1}{8}\mu^2, \tag{C5}$$

where $\langle\rangle$ is a double integral of α and β over 0 to 2π. The same joint detection events can be obtained if both Alice and Bob prepare their PR-WCPs in -45° polarization. If the PR-WCPs are prepared in different polarizations, such as $|\sqrt{\mu}e^{i\alpha}\rangle_{A,+}\otimes|\sqrt{\mu}e^{i\beta}\rangle_{B,-}$, then the joint state after passing through the BSM is

$$|\Upsilon_{AB}\rangle^{X}_{+,-} = \left|\sqrt{\frac{\mu}{4}}\left(ie^{i\alpha}+e^{i\beta}\right)\right\rangle_{1,H}\otimes\left|\sqrt{\frac{\mu}{4}}i\left(ie^{i\alpha}-e^{i\beta}\right)\right\rangle_{1,V} \otimes\left|\sqrt{\frac{\mu}{4}}\left(e^{i\alpha}+ie^{i\beta}\right)\right\rangle_{2,H}\otimes\left|\sqrt{\frac{\mu}{4}}i\left(ie^{\alpha}-ie^{i\beta}\right)\right\rangle_{2,V}. \tag{C6}$$

In this case, we can obtain the joint detection probabilities

$$\langle I_{1,H}I_{2,V}\rangle = \langle I_{2,H}I_{1,V}\rangle \propto \tfrac{3}{8}\mu^2,$$
$$\langle I_{1,H}I_{1,V}\rangle = \langle I_{2,H}I_{2,V}\rangle = \langle I_{1,H}I_{2,H}\rangle = \langle I_{1,V}I_{2,V}\rangle \propto \tfrac{1}{8}\mu^2. \tag{C7}$$

The same results can be obtained if Alice and Bob exchange their polarizations.

APPENDIX D: DECOY STATE

In this Appendix, we show how to calculate the parameters used for key estimation in Eq. (22) with standard decoy-state method. As we have demonstrated in this paper that PR-WCPs is equivalent to Poisson distributed PNs in BSM, so the photon number model is suitable for describing the quantum channel. In the decoy-state technique, in addition to signal states, Alice and Bob also send decoy states, which are also PR-WCPs but with different average photon number. From Eq. (4) we can see that in Fock state representation, the PR-WCP with intensity μ at the center of the pulse can be expressed as

$$\rho(\mu) = \sum_{k=0}^{\infty} e^{-\mu}\frac{\mu^k}{k!}\rho_k. \tag{D1}$$

Suppose at some moment, Alice and Bob prepare the PR-WCPs with intensities μ and υ, then the collision probability for the photon number state $\rho_i\otimes\rho_j$ is

$$P_{ij}^{\mu\upsilon} = e^{-\mu-\upsilon}\frac{\mu^i\upsilon^j}{i!j!}. \tag{D2}$$

Once all the quantum channels and measuring devices have been characterized before QKD, the yield Y_{ij}^{w} and the error probability e_{ij}^{w} of a successful BSM measurement for $\rho_i\otimes\rho_j$ can be determined [40], where $w = X, Y$ is the corresponding basis. In decoy-state technique, the gain $Q_{\mu\upsilon}^{w}$, and BER $E_{\mu\upsilon}^{w}$ satisfy the following equations [16]:

$$Q_{\mu\upsilon}^{w} = \sum_{i,j}P_{ij}^{\mu\upsilon}Y_{ij}^{w}, \quad E_{\mu\upsilon}^{w}Q_{\mu\upsilon}^{w} = \sum_{i,j}P_{ij}^{\mu\upsilon}Y_{ij}^{w}e_{ij}^{w}. \tag{D3}$$

From Eve's point of view, she can not distinguish the signal state from the decoy state, thus any of her PNS attacks will modify $P_{ij}^{\mu\upsilon}$, Y_{ij}^{w} or e_{ij}^{w}, which can be reflected from the values of $Q_{\mu\upsilon}^{w}$ and $E_{\mu\upsilon}^{w}$. In Eq. (D3), one always assumes that $P_{ij}^{\mu\upsilon}$ is known, which is determined by the nature of the light source, $Q_{\mu\upsilon}^{w}$ and $E_{\mu\upsilon}^{w}$ are the results of experimental measurement, and Y_{ij}^{w} and e_{ij}^{w} are obtained by solving the equations. Theoretically, when there are infinitely many decoy states, all parameters for key rate estimation can be obtained from this set of equations. When the average photon number μ and υ are less than 1, it has been proved that the portion of multiphoton terms tends to 0, so in fact, a finite decoy states are sufficient for parameter estimation [43].

In the following, we will derive $Q_{\mu\upsilon}^{w}$ and $E_{\mu\upsilon}^{w}$ for different combination of decoy-state and signal state. This derivation is inspired by the work of Ref. [17]. In Z basis, if Alice and Bob prepare their PR-WCPs in different polarizations, like $|\Upsilon_{\mu\upsilon}\rangle^{Z}_{H,V} = |\sqrt{\mu}e^{i\alpha}\rangle_H|\sqrt{\upsilon}e^{i\beta}\rangle_V$, then after passing through

the BSM, the joint state at the output is

$$|\Upsilon_{\mu\upsilon}\rangle_{H,V}^{Z}=\left|\sqrt{\frac{\eta_a\mu}{2}}ie^{i\alpha}\right\rangle_{1,H}\left|\sqrt{\frac{\eta_b\upsilon}{2}}e^{i\beta}\right\rangle_{1,V}\left|\sqrt{\frac{\eta_a\mu}{2}}e^{i\alpha}\right\rangle_{2,H}\left|\sqrt{\frac{\eta_b\upsilon}{2}}ie^{i\beta}\right\rangle_{2,V}, \tag{D4}$$

where η_a and η_b are the quantum state transmittance of Alice and Bob, which include both the channel transmittance and detection efficiency of the single-photon detectors. The detection probabilities of the four detectors in Fig. 1 are

$$D_{1H}=D_{2H}=1-(1-p_d)e^{-\frac{\eta_a\mu}{2}},\quad D_{1V}=D_{2V}=1-(1-p_d)e^{-\frac{\eta_b\upsilon}{2}}. \tag{D5}$$

The probability of successful detection events, as shown in Table I, contributed by this joint state is

$$\begin{aligned}Q_{H,V}^{Z}(\mu,\upsilon)&=\tfrac{1}{4}[D_{1H}(1-D_{2H})+D_{2H}(1-D_{1H})][D_{1V}(1-D_{2V})+D_{2V}(1-D_{1V})]\\&=(1-p_d)^2e^{-\frac{\eta_a\mu+\eta_b\upsilon}{2}}\left[1-(1-p_d)e^{-\frac{\eta_a\mu}{2}}\right]\left[1-(1-p_d)e^{-\frac{\eta_b\upsilon}{2}}\right].\end{aligned} \tag{D6}$$

The same result can also be obtained if Alice and Bob exchange their polarizations, that is $Q_{V,H}^{Z}(\mu,\upsilon)=Q_{H,V}^{Z}(\mu,\upsilon)$, and both of them are called correct successful detection events. If Alice and Bob prepare their states in the same polarization, for example both in horizontal polarization, then the joint state at the output is

$$|\Upsilon_{\mu\upsilon}\rangle_{H,H}^{Z}=\left|\sqrt{\frac{\eta_a\mu}{2}}ie^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{2}}e^{i\beta}\right\rangle_{1,H}\left|\sqrt{\frac{\eta_a\mu}{2}}e^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{2}}ie^{i\beta}\right\rangle_{2,H}, \tag{D7}$$

the corresponding detection probabilities are

$$\begin{aligned}D_{1H}&=1-(1-p_d)\exp\left(-\left|\sqrt{\frac{\eta_a\mu}{2}}ie^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{2}}e^{i\beta}\right|^2\right),\\D_{2H}&=1-(1-p_d)\exp\left(-\left|\sqrt{\frac{\eta_a\mu}{2}}e^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{2}}ie^{i\beta}\right|^2\right),\quad D_{1V}=D_{2V}=p_d.\end{aligned} \tag{D8}$$

Following the simplification process of Ref. [17], we set

$$x=\frac{\sqrt{\eta_a\mu\eta_b\upsilon}}{2},\quad y=(1-p_d)e^{-\frac{\eta_a\mu+\eta_b\upsilon}{4}},\quad \phi=\alpha-\beta. \tag{D9}$$

So, the probability of successful detection events provided by state $|\Upsilon_{\mu\upsilon}\rangle_{H,H}^{Z}$ is a function of ϕ, μ, and υ

$$Q_{H,H}^{Z}(\mu,\upsilon,\phi)=\frac{1}{2}p_d\left(y^2e^{-2x\sin\phi}+y^2e^{2x\sin\phi}-\frac{2y^4}{1-p_d}\right). \tag{D10}$$

By averaging $Q_{H,H}^{Z}(\mu,\upsilon,\phi)$ over ϕ, we can get

$$Q_{H,H}^{Z}(\mu,\upsilon)=p_dy^2\left(I_0(2x)-\frac{y^2}{1-p_d}\right), \tag{D11}$$

where $I_0(x)$ is the modified Bessel function of the first kind. Accordingly, we have $Q_{V,V}^{Z}(\mu,\upsilon)=Q_{H,H}^{Z}(\mu,\upsilon)$, and these are called incorrect successful detection events. The probabilities for correct, incorrect, and total successful detection events in Z basis are

$$Q_{\mu\upsilon}^{Z,C}=Q_{H,V}^{Z}(\mu,\upsilon)+Q_{V,H}^{Z}(\mu,\upsilon),\quad Q_{\mu\upsilon}^{Z,E}=Q_{H,H}^{Z}(\mu,\upsilon)+Q_{V,V}^{Z}(\mu,\upsilon),\quad Q_{\mu\upsilon}^{Z}=Q_{\mu\upsilon}^{Z,C}+Q_{\mu\upsilon}^{Z,E}. \tag{D12}$$

Considering the misalignment error e_d, the BER $E_{\mu\upsilon}^{Z}$ satisfies

$$E_{\mu\upsilon}^{Z}Q_{\mu\upsilon}^{Z}=\left(Q_{\mu\upsilon}^{Z,C}-Q_{\mu\upsilon}^{Z,E}\right)e_d+Q_{\mu\upsilon}^{Z,E}. \tag{D13}$$

In X basis, if Alice and Bob prepare their PR-WCPs in the same polarization, like $|\Upsilon_{\mu\upsilon}\rangle_{+,+}^{X}=|\sqrt{\mu}e^{i\alpha}\rangle_{+}|\sqrt{\upsilon}e^{i\beta}\rangle_{+}$, then after passing through the BSM, the joint state at the output is

$$\begin{aligned}|\Upsilon_{\mu\upsilon}\rangle_{+,+}^{X}=&\left|\sqrt{\frac{\eta_a\mu}{4}}ie^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{4}}e^{i\beta}\right\rangle_{1,H}\left|-\sqrt{\frac{\eta_a\mu}{4}}e^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{4}}ie^{i\beta}\right\rangle_{1,V}\\&\otimes\left|\sqrt{\frac{\eta_a\mu}{4}}e^{i\alpha}+\sqrt{\frac{\eta_b\upsilon}{4}}ie^{i\beta}\right\rangle_{2,H}\left|\sqrt{\frac{\eta_a\mu}{4}}ie^{i\alpha}-\sqrt{\frac{\eta_b\upsilon}{4}}e^{i\beta}\right\rangle_{2,V}.\end{aligned} \tag{D14}$$

The detection probabilities of the four detectors are

$$D_{1H} = D_{1V} = 1 - (1 - p_d)\exp\left(-\left|\sqrt{\frac{\eta_a\mu}{4}}ie^{i\alpha} + \sqrt{\frac{\eta_b\upsilon}{4}}e^{i\beta}\right|^2\right),$$
$$D_{2H} = D_{2V} = 1 - (1 - p_d)\exp\left(-\left|\sqrt{\frac{\eta_a\mu}{4}}e^{i\alpha} + \sqrt{\frac{\eta_b\upsilon}{4}}ie^{i\beta}\right|^2\right). \tag{D15}$$

From Table I, we can see that the correct and incorrect successful detection probabilities from this state are

$$Q^{X,C}_{+,+} = \tfrac{1}{4}[D_{1H}D_{1V}(1 - D_{2H})(1 - D_{2V}) + D_{2H}D_{2V}(1 - D_{1H})(1 - D_{1V})],$$
$$Q^{X,E}_{+,+} = \tfrac{1}{4}[D_{1H}D_{2V}(1 - D_{2H})(1 - D_{1V}) + D_{2H}D_{1V}(1 - D_{1H})(1 - D_{2V})]. \tag{D16}$$

A same result can be obtained if both of the PR-WCPs are prepared in "$-$" polarization. If Alice and Bob prepare their PR-WCPs in different polarizations, like $|\Upsilon_{\mu\upsilon}\rangle^X_{+,-} = |\sqrt{\mu}e^{i\alpha}\rangle_+|\sqrt{\upsilon}e^{i\beta}\rangle_-$, the correct and incorrect successful detection probabilities have the following forms:

$$Q^{X,C}_{+,-} = \tfrac{1}{4}[D_{1H}D_{2V}(1 - D_{2H})(1 - D_{1V}) + D_{2H}D_{1V}(1 - D_{1H})(1 - D_{2V})],$$
$$Q^{X,E}_{+,-} = \tfrac{1}{4}[D_{1H}D_{1V}(1 - D_{2H})(1 - D_{2V}) + D_{2H}D_{2V}(1 - D_{1H})(1 - D_{1V})]. \tag{D17}$$

The correct, incorrect, and total successful detection probabilities in X basis are

$$Q^{X,C}_{\mu\upsilon} = Q^{X,C}_{+,+} + Q^{X,C}_{-,-} + Q^{X,C}_{+,-} + Q^{X,C}_{-,+}, \quad Q^{X,E}_{\mu\upsilon} = Q^{X,E}_{+,+} + Q^{X,E}_{-,-} + Q^{X,E}_{+,-} + Q^{X,E}_{-,+}, \quad Q^{X}_{\mu\upsilon} = Q^{X,C}_{\mu\upsilon} + Q^{X,E}_{\mu\upsilon}. \tag{D18}$$

By averaging the detection probabilities over ϕ, the above three terms can be expressed as

$$Q^{X,C}_{\mu\upsilon} = 2y^2(I_0(2x) - 2yI_0(x) + y^2), \quad Q^{X,E}_{\mu\upsilon} = 2y^2[1 - 2yI_0(x) + y^2], \quad Q^{X}_{\mu\upsilon} = 2y^2[1 + 2y^2 + I_0(2x) - 4yI_0(x)]. \tag{D19}$$

Similarly, the BER in X basis satisfies

$$E^X_{\mu\upsilon}Q^Z_{\mu\upsilon} = \left(Q^{X,C}_{\mu\upsilon} - Q^{X,E}_{\mu\upsilon}\right)e_d + Q^{X,E}_{\mu\upsilon}. \tag{D20}$$

With finite decoy states, enough $Q^w_{\mu\upsilon}$ and $E^w_{\mu\upsilon}$, $w = Z, X$ can be predicted. By inserting these quantities into Eq. (D3), one can estimate parameters Y^w_{ij} and e^w_{ij}, which can inversely provide the information of $P^{\mu\upsilon}_{ij}$.

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

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

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).

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

[5] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[6] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[7] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[8] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[9] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).

[10] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[11] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[12] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

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

[14] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).

[15] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).

[16] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[17] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[18] 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.*, Phys. Rev. Lett. **111**, 130502 (2013).

[19] 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 *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).

[20] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature Commun. **5**, 3732 (2014).

[21] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).

[22] 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.*, Phys. Rev. Lett. **117**, 190501 (2016).

[23] 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.*, Phys. Rev. X **6**, 011024 (2016).

[24] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).
[25] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Phys. Rev. A **98**, 062323 (2018).
[26] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Appl. **11**, 034053 (2019).
[27] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018).
[28] J. Lin and N. Lütkenhaus, Phys. Rev. A **98**, 042332 (2018).
[29] W. Li, L. Wang, and S. Zhao, Sci. Rep. **9**, 15466 (2019).
[30] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sci. Rep. **9**, 3080 (2019).
[31] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **123**, 100506 (2019).
[32] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Phys. Rev. A **101**, 042330 (2020).
[33] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, Phys. Rev. Lett. **124**, 070501 (2020).
[34] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[35] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[36] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[37] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[38] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Nature (London) **526**, 682 (2015).
[39] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. von der Weid, Phys. Rev. A **88**, 052303 (2013).
[40] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[41] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[42] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[43] X. Ma, C. H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).