

Mode-pairing quantum key distribution based on heralded pair-coherent source with passive decoy-states

Zhigang Shen(沈志冈), Yuting Lu(鲁雨婷), Yang Yu(余杨), and Shengmei Zhao(赵生妹)
Citation: Chin. Phys. B, 2025, 34 (**9**): 090304. DOI: 10.1088/1674-1056/adcf89
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Asymmetric mode-pairing quantum key distribution with advantage distillation

Hai-Tao Wang(汪海涛), Chun Zhou(周淳), Yi-Fei Lu(陆宜飞), Chen-Peng Hao(郝辰鹏), Yan-Mei Zhao(赵燕美), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2025, 34 (**4**): 040305. DOI: 10.1088/1674-1056/adbb5c

Improved model on asynchronous measurement-device-independent quantum key distribution with realistic devices

Mingshuo Sun(孙铭烁), Chun-Hui Zhang(张春辉), Rui Zhang(章睿), Xing-Yu Zhou(周星宇), Jian Li(李剑), and Qin Wang(王琴)
Chin. Phys. B, 2024, 33 (**11**): 110302. DOI: 10.1088/1674-1056/ad757a

A new quantum key distribution resource allocation and routing optimization scheme

Lin Bi(毕琳), Xiaotong Yuan(袁晓同), Weijie Wu(吴炜杰), and Shengxi Lin(林升熙)
Chin. Phys. B, 2024, 33 (**3**): 030309. DOI: 10.1088/1674-1056/ad2503

Passive decoy-state quantum key distribution for the weak coherent photon source with finite-length key

Yuan Li(李源), Wansu Bao(鲍皖苏), Hongwei Li(李宏伟), Chun Zhou(周淳), Yang Wang(汪洋)
Chin. Phys. B, 2016, 25 (**1**): 010305. DOI: 10.1088/1674-1056/25/1/010305

Passive decoy-state quantum key distribution using weak coherent pulses with modulator attenuation

Li Yuan (李源), Bao Wan-Su (鲍皖苏), Li Hong-Wei (李宏伟), Zhou Chun (周淳), Wang Yang (汪洋)
Chin. Phys. B, 2015, 24 (**11**): 110307. DOI: 10.1088/1674-1056/24/11/110307

Mode-pairing quantum key distribution based on heralded pair-coherent source with passive decoy-states

Zhigang Shen(沈志冈)[1,†], Yuting Lu(鲁雨婷)[1,†], Yang Yu(余杨)[1], and Shengmei Zhao(赵生妹)[1,2,3,‡]

[1] *Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing* 210003, *China*
[3] *National Laboratory of Solid State Microstructures, Nanjing University, Nanjing* 210093, *China*

(Received 12 March 2025; revised manuscript received 19 April 2025; accepted manuscript online 23 April 2025)

A mode-pairing quantum key distribution based on heralded pair-coherent source with passive decoy-states is proposed, named HPCS-PDS-MP-QKD protocol, where the light sources at Alice and Bob sides are changed to heralded pair-coherent sources, and devices designed to implement passive decoy states are included at the transmitter sides to generate the decoy state pulses in the decoy-state window passively. With the defined efficient events and the designed pairing strategy, the key bits and bases can be obtained by data post-processing. Numerical simulation results verify the feasibility of the proposed protocol. The results show that the proposed protocol can exceed PLOB when the pairing interval setting is greater than 10^3, and the transmission distance exceeds 200 km. When the key transmission distance reaches 300 km and the maximum pairing interval is equivalent to 1, its performance is improved by nearly 1.8 times compared to the original MP-QKD protocol with a weak coherent source (WCS-MP-QKD), and by 6.8 times higher than that of WCS-MP-QKD with passive decoy states (WCS-PDS-MP-QKD). Meanwhile, the key transmission distance can reach 480 km, and surpasses the WCS-PDS-MP-QKD protocol by nearly 40 km. When the total pulse length is greater than 10^{11}, the key generation rate is almost equal to that of infinite pulses. It is a promising QKD protocol that breaks the PLOB bound without requiring phase tracking and locking, has a longer transmission distance and a higher key generation rate, and eliminates the potential of side channel attack.

Keywords: mode-pairing quantum key distribution, heralded pair-coherent source, passive decoy-state, key generation rate

PACS: 03.67.Hk, 03.67.Dd

DOI: 10.1088/1674-1056/adcf89 **CSTR:** 32038.14.CPB.adcf89

1. Introduction

Based on the fundamental principles of quantum mechanics such as the quantum no-cloning theorem and the uncertainty principle, quantum key distribution (QKD) protocol has established a secure key between the legitimate users, Alice and Bob. Since the advent of the first QKD protocol-the BB84 protocol,[1] many new types of QKD protocols have been proposed, such as the decoy-state QKD protocol[2,3] which is resistant to photon-number-splitting attacks, the measurement-device-independent QKD (MDI-QKD) protocol[4] who avoids the measurement-device-side attacks, and the twin-field QKD (TF-QKD) protocol[5] who can surpass the PLOB bound.[6]

Recently, many TF-QKD variants have been proposed and numerous experimental demonstrations have been performed[7–10] to show the feasibility of TF-QKD, including phase-matching QKD (PM-QKD),[11–13] send-or-not-send QKD (SNS-QKD),[14,15] and other variants.[16–19] However, the phase tracking and locking techniques are required during their experiments, so that the complexity and difficulty of the corresponding experiments are increased. Fortunately, mode-pairing quantum key distribution protocol (MP-QKD),[20] also known as asynchronous MDI-QKD,[21] was currently proposed to overcome the problem, that broke the PLOB bound without requiring phase tracking and locking. Instead of pairing only adjacent time slots, MP-QKD recycles the unpaired events in MDI-QKD by actively post-selecting coincidence events within a suitable pairing interval (l). And many experimental demonstrations are performed.[22–24] For example, Zhu *et al.* employed two independent off-the-shelf lasers to demonstrate a quadratic key-rate improvement over the traditional measurement-device-independent schemes in the regime of metropolitan and intercity distances without global phase locking.[22] Zhou *et al.* achieved secret key rates higher than TF-QKD by implementing an innovative but simpler measurement-device-independent QKD that realized repeater-like communication through asynchronous coincidence pairing.[23] Li *et al*. introduced a statistical analysis method based on the T-distribution to calculate confidence intervals of intensity fluctuations, and studied the decoy-state MP-QKD protocol with light source intensity fluctuations.[24]

Typically, the active modulation through acousto-optic/electro-optic modulators on light sources is used in QKD

[†]These authors contributed equally to this work.
[‡]Corresponding author. E-mail: zhaosm@njupt.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

protocol implementation. However, passive modulation of pulses is still necessary in certain cases even though the active modulation is sufficient to implement decoy-state MP-QKD. For instance, when the intensity modulator is imperfectly designed, leading to certain physical parameters of emitted pulses depending on specific circumstances, then the active modulation of pulse intensity in such cases can result in a serious security issue,[25–27] because the eavesdropper (Eve) can exploit these vulnerabilities to steal partial or complete key bits. Luckily, the passive decoy-state methods have already been proposed[28–32] and have been demonstrated to reduce information leakage.[33]

Moreover, weak coherent sources are often adopted in MP-QKD. The photon number distribution of WCS follows a Poisson distribution, and the probability of sending a single photon is very low, which affects the performance of MP-QKD. On the other hand, heralded pair-coherent source (HPCS)[34] has a higher single-photon probability, which is closer to the ideal single-photon source than WCS. HPCS utilizes spontaneous parametric down-conversion to generate photon pairs and predicts the arrival of one photon by using the detection result of another photon, so HPCS has significantly reduced the proportion of empty pulses in the QKD procedure.[35,36] Therefore, it is interesting to discuss the performance of MP-QKD by replacing WCS with HPCS and employing the passive decoy-state method.

In this paper, we propose a mode-pairing quantum key distribution based on heralded pair-coherent source with a passive decoy-state method, named HPCS-PDS-MP-QKD protocol. In the protocol, Alice (Bob) prepares her (his) single photon pulses with a heralded pair-coherent source, then inputs the pulses to a passive decoy state module to passively select the decoy state mode according to the response of its local detector. Then, she (he) transmits the pulses to Charlie, who may be an eavesdropper. With the measurement results declared by Charlie and the defined efficient events, the key bits and the bases are determined during the data post-processing for mode pairing and key mapping. The key rate of HPCS-PDS-MP-QKD is derived in detail and is analyzed by numerical simulations. The relationship between the key generation rate of HPCS-PDS-MP-QKD against the transmission distance, as well as the maximum pairing interval, is discussed.

2. The HPCS-PDS-MP-QKD

2.1. The protocol

The schematic diagram of HPCS-PDS-MP-QKD is illustrated in Fig. 1. At Alice's (Bob's) side, a time-correlated pulse is sent from a laser and is split by a parametric down conversion process of the nonlinear crystal (PDC) to two modes, the idler mode and the signal mode, where the idler mode photon is detected by a local single-photon detector D_1, while the signal mode photon is prepared to send to the third party Charlie (Eve) through a passive decoy state module. In the passive decoy-state module, the input pulse is firstly split into two paths (path S and path V) by a beam-splitter (BS_1), where path S is prepared for the signal state, while both path S and path V are prepared for the decoy state. Here, the signal state and the decoy state are randomly selected. When a signal-state pulse is selected, path V is blocked by using a variable optical attenuator (VOA_2), and the intensity and phase are modulated by phase modulator (PM_1) and VOA_1 on path S, respectively. When a decoy-state pulse is chosen, the pulses at these two paths are interfered at BS_2 (path S and path V are assumed in the same length), and the outcome mode r passively selects the decoy-state based on the response results of local detectors D_2. After the interference occurs at Charlie's side, Charlie announces the outcome of successful events. Alice and Bob then can achieve the key according to the pairing strategy and key mapping based on the announced measurement results. Finally, Alice and Bob obtain the secure key after error correction and privacy amplification.

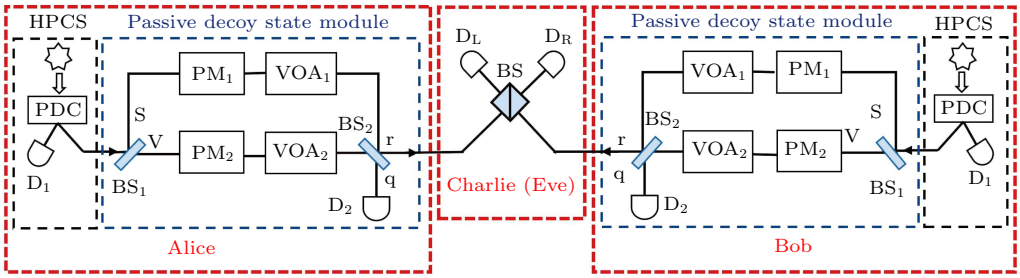


Fig. 1. The schematic diagram of the proposed HPCS-PDS-MP-QKD protocol. PDC represents the parametric down conversion process of the nonlinear crystal. BS: beam splitter, its parameters is 50:50. VOA: variable optical attenuator. PM: phase modulator, D: single-photon detector.

The details of the pairing strategy are listed as follows.

(i) Identifying the first successfully clicked round as the leading pulse.

(ii) Searching for the next successfully clicked round. If the interval between the new successfully clicked round and the existing leading pulse is within the maximum pairing interval, then these two rounds are paired, and the pairing is successful; If the pairing fails, the existing leading pulse is dis-

carded, and this round is set as a new leading pulse. Here, the maximum pairing interval refers to the pre-agreed maximum allowable pulse interval between two consecutive valid pairing measurement events, which is setup by Alice and Bob before communications.

(iii) Continually searching and repeating steps (i)–(ii) until all clicked rounds are paired.

The details of the proposed protocol are the following:

(I) State preparation: Alice (Bob) prepares entangled photon pairs. Assume there are N rounds in the protocol. In each round, Alice (Bob) randomly selects a signal state and a decoy state. In the i-th round ($i = 1,2,\ldots,N$), Alice prepares the photon state $\left|\sqrt{\mu_i^{\mathrm{a}}}\mathrm{e}^{\mathrm{i}\phi_i^{\mathrm{a}}}\right\rangle$ in the following way:

I-1 When a signal state is chosen, path V is blocked, Alice randomly selects the intensity μ_i^{a} from (0, μ), the phase ϕ_i^{a}, uniformly over [0,2π), modulated by PM_1.

I-2 When a decoy state is chosen, Alice selects the intensity μ_i^{a} from (0, μ) by the response events of the local detectors in the passive decoy-state module, where the pulse phase on both paths (path S, path V) are uniformly distribution over [0,2π), which are modulated by PM_1 and PM_2, separately.

Bob does the same operations as Alice for the state preparation.

(II) Measurement: Charlie performs single-photon interference on the pulses sent by Alice and Bob, and announces the measurement results, where only one of the two detectors click is defined as a successful event. Alice and Bob repeat the above two steps for N rounds.

(III) Mode pairing: Alice and Bob apply the above listed strategy to pair those rounds with two clicks as one pair for all the successful detection rounds when both Alice and Bob send the signal states. The phases and intensities from these two rounds form a data pair. The pairing strategy is the same as that of the MP-QKD protocol.

(IV) Basis sifting: Based on the intensity of the two paired rounds indexed i and j, if the intensity is (0, μ) or (μ, 0), Alice marks the 'basis' of the data pair as basis Z. If the intensity is (μ, μ), Alice marks the 'basis' of the data pair as basis X. If the intensity is (0, 0), it is marked as basis '0'. Bob sets the bases using the same strategy. Alice and Bob announce the basis for each data pair. If both of their basis is $X(Z)$, they keep the data pairs, otherwise, they discard the data pairs.

(V) Key mapping: For each Z basis pair at index i and j, if $(\mu_i^{\mathrm{a}},\ \mu_j^{\mathrm{a}}) = (0,\mu)$, Alice sets her key bit κ^{a} to 0; if $(\mu_i^{\mathrm{a}},\ \mu_j^{\mathrm{a}}) = (\mu,0)$, she set her key bit κ^{a} to 1. For X basis pairs (Alice and Bob being the same), there exists $(\phi_j^{\mathrm{a}} - \phi_i^{\mathrm{a}}) = \theta^{\mathrm{a}} + \pi\kappa^{\mathrm{a}}$, therefore, κ^{a} is set by $[(\phi_j^{\mathrm{a}} - \phi_i^{\mathrm{a}})/\pi \bmod 2]$ and θ^{a} is $[(\phi_j^{\mathrm{a}} - \phi_i^{\mathrm{a}}) \bmod \pi]$. Bob has the same steps except for an additional one, that is, for rounds i and j, if the detectors' clicks announced by Charlie occurs on the same side, *i.e.*, the responses of the detectors are (L, L) or (R, R), then Bob keeps his bit. If the detectors' clicks occur on different sides, *i.e.*, the detectors responses are (L, R) or (R, L), then Bob flips his bit. Only when the alignment angles of Alice and Bob are equal, that is, $\theta^{\mathrm{a}} = \theta^{\mathrm{b}}$, the data pair is kept; otherwise, the data pair is discarded.

(VI) Parameter estimation: Alice and Bob estimate the quantum bit error rate $E_{\mu\mu}^{Z}$ in Z pairs under the condition of sending signal states, with an overall intensity of $(\mu_{i,j}^{\mathrm{a}}, \mu_{i,j}^{\mathrm{b}}) = (\mu,\mu)$. They use different decoy-state modes of Z basis pairs under the condition of sending decoy states to estimate the single-photon pair ratio $q_{(1,1)}$, and use X basis pairs to estimate the single-photon phase error rate $e_{(1,1)}$.

(VII) Key distillation: Alice and Bob use the Z pairs under the condition of sending signal states to generate the key. They perform error correction and privacy amplification based on $E_{\mu\mu}^{Z}$, $q_{(1,1)}$, and $e_{(1,1)}$ to generate the secure key.

2.2. Decoy-state estimation

In HPCS-PDS-MP-QKD protocol, Alice and Bob use Z basis pairs to generate key. Compared with original MP-QKD protocol, the proposed protocol does not change any others except state preparation. Hence, HPCS-PDS-MP-QKD is a variant of the original MP-QKD. Similarly, the HPCS-PDS-MP-QKD protocol can also be considered as a dual-mode MDI-QKD scheme. It is shown that the dual-mode schemes have security,[37] so the security of our scheme is guaranteed.

The heralded pair-coherent source is a type of dual-mode light source, which operates on the principle of utilizing non-degenerate parametric down-conversion to generate entangled photon pairs (*i.e.*, signal photons and idler photons). The probability of generating n-photon state pulses in these two modes follows a thermal distribution[34] as

$$P_{\mu}(n) = \frac{1}{P_{\mathrm{Post}}(\mu)}\left[1-(1-d_1)(1-\eta_1)^n\right]\frac{\mu^{2n}}{(n!)^2}, \tag{1}$$

where μ is the average intensity of the signal photon pulse, d_1 represents the dark count of detector D_1 , η_1 represents the detection efficiency of detector D_1, and $P_{\mathrm{Post}}(\mu) = \mathrm{I}_0(2\mu) - (1-d_1)\mathrm{I}_0\left(2\mu\sqrt{1-\eta_1}\right)$ denotes the post-selection probability, $\mathrm{I}_0(x)$ is the modified Bessel function of the first kind.

Here, we only consider the phase number distribution after the passive decoy-state module. Assume that the laser emits photons in a coherent state with intensity μ, after passing through the beam splitter BS_1 and the phase modulators PM_1 and PM_2, the coherent states on path S and path V are $\left|\sqrt{\mu/2}\mathrm{e}^{\mathrm{i}\phi_1}\right\rangle$ and $\left|\sqrt{\mu/2}\mathrm{e}^{\mathrm{i}\phi_2}\right\rangle$, respectively. After their interference at BS_2, the joint probability $p_{n,m}$ of having n photons in mode r and m photons in mode q is the product of the two HPCS distributions with half average intensity. By measuring the outcome signal at the q side, say by D_2, the conditional photon number statistics of the remaining signal varies

depending on the result obtained. When the single-photon detector D_2 does not click, the probability of finding n photons in mode r (one decoy state) can be calculated as

$$q^0_{\mu'}(n) = \frac{1}{P_{\text{Post}}(\mu'/2)}\left[1-(1-d_1)(1-\eta_1)^n\right] \times \int_0^{2\pi}\frac{1}{2\pi}\frac{(\mu\alpha)^{2n}}{(n!)^2}\frac{d_1(1-d_2)}{P_{\text{Post}}((1-\alpha)\mu'\eta_2)}\,\mathrm{d}\theta, \quad (2)$$

where $\mu' = \mu^{\mathrm{S}} + \mu^{\mathrm{V}}$, $\alpha = \frac{1}{\mu'}\left(\frac{\mu'}{2} - \sqrt{\mu^{\mathrm{S}}\mu^{\mathrm{D}}}\sin\theta\right)$, $\theta = \phi_2 - \phi_1$, ϕ_1 and ϕ_2 are the phases modulated by PM_1 and PM_2, respectively. μ^{S} and μ^{V} are the intensities of the pulse on path S and path V, respectively. d_2 is the dark count of the detector D_2, and η_2 is its detection efficiency.

Correspondingly, when the single-photon detector D_2 clicks, the probability distribution of finding n photons in mode r (another decoy state) is

$$q^1_{\mu'}(n) = \frac{1}{P^2_{\text{Post}}(\mu'/2)}\left[1-(1-d_1)(1-\eta_1)^n\right]\frac{(\mu\alpha)^{2n}}{(n!)^2} \times \int_0^{2\pi}\frac{1}{2\pi}P_{\text{Post}}\left(\mu'(1-\alpha)\right)d\theta - q^0_{\mu'}(n). \quad (3)$$

For normalization, the probabilities of the two decoy states are normalized as

$$\begin{cases} P^0_{\mu'}(n) = q^0_{\mu'}(n)/N_{\mu'}, \\ P^1_{\mu'}(n) = q^1_{\mu'}(n)/\left(1-N_{\mu'}\right). \end{cases} \quad (4)$$

Here, $N_{\mu'}$ is a normalization constant, which equals

$$\frac{1}{P_{\text{Post}}(\mu'/2)}\int_0^{2\pi}\frac{1}{2\pi}\frac{P_{\text{Post}}(\mu'\alpha)\,d_1(1-d_2)}{P_{\text{Post}}((1-\alpha)\mu'\eta_2)}\,\mathrm{d}\theta.$$

For simplicity, we only consider the cases when both the detector D_2 click or no click for the decoy states.

Like the analysis discussed in Ref. [38], we employ three intensities decoy-state analysis[39] on the proposed scheme, and the round N is assumed large enough. For each round i, three intensities $0, \nu^{\mathrm{a}}, \mu^{\mathrm{a}}(0, \nu^{\mathrm{b}}, \mu^{\mathrm{b}})$ can be selected by Alice (Bob) with probabilities s_0, $s_{\nu^{\mathrm{a}}}(s_{\nu^{\mathrm{b}}})$, and $s_{\mu^{\mathrm{a}}}(s_{\mu^{\mathrm{b}}})$. Note that the sum of these probabilities should be equal to 1. To simplify the discussion, the probabilities of the two parties choosing an intensity are set to $s_{\nu^{\mathrm{a}}} = s_{\nu^{\mathrm{b}}}$ and $s_{\mu^{\mathrm{a}}} = s_{\mu^{\mathrm{b}}}$. Based on these pulses, Alice and Bob pair two locations indexed i and j, including those without successful clicks. The intensity vector of the $(i,\ j)$ pair can be denoted as $\boldsymbol{\mu} = \left(\mu^{\mathrm{a}}_i + \mu^{\mathrm{a}}_j, \mu^{\mathrm{b}}_i + \mu^{\mathrm{b}}_j\right)$, where, $\mu^{\mathrm{a(b)}}_i, \mu^{\mathrm{a(b)}}_j \in \left\{0, \nu^{\mathrm{a(b)}}, \mu^{\mathrm{a(b)}}\right\}$, and the probability of sending $\boldsymbol{\mu}$ can be expressed as $q^{\boldsymbol{\mu}} = \sum_{\left(\mu^{\mathrm{a}}_i+\mu^{\mathrm{a}}_j, \mu^{\mathrm{b}}_i+\mu^{\mathrm{b}}_j\right)=\boldsymbol{\mu}} s_{\mu^{\mathrm{a}}_i} s_{\mu^{\mathrm{a}}_j} s_{\mu^{\mathrm{b}}_i} s_{\mu^{\mathrm{b}}_j}$. Note that the probability is independent of the measurement results announced by Charlie.

Alice (Bob) performs the photon number detection by an auxiliary system. For each pair of locations $(i,\ j)$, the photon number measurement results obtained by Alice and Bob are denoted as k^{a} and k^{b}, respectively, which comprise the photon number measurement vector $\boldsymbol{k} = \left(k^{\mathrm{a}}, k^{\mathrm{b}}\right)$. Since the intensities sent by Alice and Bob for the pair $(i,\ j)$ are independent, the probability for given $\boldsymbol{\mu}$, the measurement $\boldsymbol{k}$ can be described as

$$Pr(\boldsymbol{k}|\boldsymbol{\mu}) = P_{\mu^{\mathrm{a}}_i+\mu^{\mathrm{a}}_j}(k^{\mathrm{a}})\,P_{\mu^{\mathrm{b}}_i+\mu^{\mathrm{b}}_j}\left(k^{\mathrm{b}}\right), \quad (5)$$

$$Pr(\boldsymbol{k}|\boldsymbol{\mu}) = P^{\mathrm{x}}_{\mu^{\mathrm{a}}_i+\mu^{\mathrm{a}}_j}(k^{\mathrm{a}})\,P^{y}_{\mu^{\mathrm{b}}_i+\mu^{\mathrm{b}}_j}\left(k^{\mathrm{b}}\right), \quad (6)$$

where $P_{\mu}(n)$ is determined by Eq. (1) and $P^{x(y)}_{\mu}(n)$ is determined in Eq. (4), $x, y \in \{0,\ 1\}$.

For simplicity, the symmetric case is considered, and $d_1 = d_2 = d$, $\eta_1 = \eta_2 = \eta$. Denote the probability for Alice and Bob's measurement $\boldsymbol{k}$ on the pair $(i,\ j)$ as $q_{\boldsymbol{k}}$, therefore, the probability for given $\boldsymbol{k}$, the intensity $\boldsymbol{\mu}$ can be expressed as

$$Pr(\boldsymbol{\mu}|\boldsymbol{k}) = \frac{q^{\boldsymbol{\mu}}Pr(\boldsymbol{k}|\boldsymbol{\mu})}{q_{\boldsymbol{k}}} = \frac{q^{\boldsymbol{\mu}}Pr(\boldsymbol{k}|\boldsymbol{\mu})}{\sum_{\boldsymbol{\mu}'}q^{\boldsymbol{\mu}'}Pr(\boldsymbol{k}|\boldsymbol{\mu}')}. \quad (7)$$

The values of $\boldsymbol{\mu}'$ are taken to be the same as those of $\boldsymbol{\mu}$, with different symbols used to avoid ambiguity in the summation. After Charlie completes the measurements and announces the outcomes from detectors L and R, Alice and Bob perform mode pairing and basis sifting according to the pairing strategy. If the intensity vector $\boldsymbol{\mu}$ on the pair $(i,\ j)$ satisfies $\mu^{\mathrm{a}}_i\mu^{\mathrm{a}}_j = \mu^{\mathrm{b}}_i\mu^{\mathrm{b}}_j = 0$, $\mu^{\mathrm{a}}_i + \mu^{\mathrm{a}}_j + \mu^{\mathrm{b}}_i + \mu^{\mathrm{b}}_j \neq 0$. Then it is a Z-basis pair. Here, we focus on the decoy-state estimation for Z-basis pairs, the estimation for X-basis pairs can be discussed by a similar way.

Suppose Alice and Bob successfully detect M^Z rounds for Z-basis pairs, in which there are E^Z error rounds. The total number of pairs with intensity $\boldsymbol{\mu}$ is denoted as $M^{Z,\boldsymbol{\mu}}$, and the erroneous pairs is denoted as $E^{Z,\boldsymbol{\mu}}$. Similarly, the total number of pairs, erroneous pairs with photon number $\boldsymbol{k}$ are denoted as $M^Z_{\boldsymbol{k}}$ and $E^Z_{\boldsymbol{k}}$, respectively, where $M^{Z,\boldsymbol{\mu}}_{\boldsymbol{k}}$ and $E^{Z,\boldsymbol{\mu}}_{\boldsymbol{k}}$ are for those with intensity $\boldsymbol{\mu}$. All they satisfy

$$\begin{cases} M^Z = \sum_{\boldsymbol{\mu}} M^{Z,\boldsymbol{\mu}} = \sum_{\boldsymbol{k}} M^Z_{\boldsymbol{k}} = \sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{k}} M^{Z,\boldsymbol{\mu}}_{\boldsymbol{k}}, \\ E^Z = \sum_{\boldsymbol{\mu}} E^{Z,\boldsymbol{\mu}} = \sum_{\boldsymbol{k}} E^Z_{\boldsymbol{k}} = \sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{k}} E^{Z,\boldsymbol{\mu}}_{\boldsymbol{k}}. \end{cases} \quad (8)$$

Through the protocol, the values of $M^{Z,\boldsymbol{\mu}}$ and $E^{Z,\boldsymbol{\mu}}$ are known, while the values of $M^Z_{\boldsymbol{k}}$ and $E^Z_{\boldsymbol{k}}$ are unknown, but they will be fixed after Charlie's announcement.

In practice, Alice and Bob first perform photon number measurements and obtain the result $\boldsymbol{k}$. Subsequently, both parties randomly select intensity setting $\boldsymbol{\mu}$ based on $\boldsymbol{k}$. Therefore, the intensity $\boldsymbol{\mu}$ depends solely on $\boldsymbol{k}$ and is independent of the results announced by Charlie. When all generated Z-basis pairs with photon number measurement outcomes in $\boldsymbol{k}$ are considered, the expected ratios of different intensities should be the same as the ratios of the emitted states, that is

$$\frac{M^{Z,\boldsymbol{\mu}}_{\boldsymbol{k}}}{M^{Z,\boldsymbol{\mu}'}_{\boldsymbol{k}}} = \frac{Pr(\boldsymbol{\mu},\boldsymbol{k})}{Pr(\boldsymbol{\mu}',\boldsymbol{k})} = \frac{q^{\boldsymbol{\mu}}Pr(\boldsymbol{k}|\boldsymbol{\mu})}{q^{\boldsymbol{\mu}'}Pr(\boldsymbol{k}|\boldsymbol{\mu}')}. \quad (9)$$

In the set of $M_{\boldsymbol{k}}^{Z}$, the number of pairs with intensity $\boldsymbol{\mu}$ is represented by $\mathcal{M}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}$, which is determined by the auxiliary systems, and is used to characterize the intensity chosen by Alice and Bob. According to the previous analysis, the expected ratio of the intensity $\boldsymbol{\mu}$ is expressed as

$$\mathbb{E}\left(\frac{\mathcal{M}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}}{M_{\boldsymbol{k}}^{Z}}\right)=Pr(\boldsymbol{\mu}|\boldsymbol{k})=\frac{q^{\boldsymbol{\mu}}Pr(\boldsymbol{k}|\boldsymbol{\mu})}{\sum_{\boldsymbol{\mu}'}q^{\boldsymbol{\mu}'}Pr(\boldsymbol{k}|\boldsymbol{\mu}')}, \tag{10}$$

where $\mathbb{E}(\cdot)$ represents the expected value. Correspondingly, within $E_{\boldsymbol{k}}^{Z}$ pairs, $\mathcal{E}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}$ represents the erroneous number of pairs with intensity $\boldsymbol{\mu}$, the corresponding ratio is

$$\mathbb{E}\left(\frac{\mathcal{E}_{\boldsymbol{k}}^{\boldsymbol{\mu},Z}}{E_{\boldsymbol{k}}^{Z}}\right)=Pr(\boldsymbol{\mu}|\boldsymbol{k})=\frac{q^{\boldsymbol{\mu}}Pr(\boldsymbol{k}|\boldsymbol{\mu})}{\sum_{\boldsymbol{\mu}'}q^{\boldsymbol{\mu}'}Pr(\boldsymbol{k}|\boldsymbol{\mu}')}. \tag{11}$$

Based on Eqs. (10) and (11), we obtain the following result:

$$\begin{cases}\mathbb{E}\left[\mathcal{M}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}\right]=Pr(\boldsymbol{\mu}|\boldsymbol{k})M_{\boldsymbol{k}}^{Z},\\ \mathbb{E}\left[\mathcal{E}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}\right]=Pr(\boldsymbol{\mu}|\boldsymbol{k})E_{\boldsymbol{k}}^{Z}.\end{cases} \tag{12}$$

The total number of pairs and the erroneous pairs with intensity $\boldsymbol{\mu}$ are denoted as $\mathcal{M}^{Z,\boldsymbol{\mu}}$ and $\mathcal{E}^{Z,\boldsymbol{\mu}}$, respectively, where

$$\begin{cases}\mathcal{M}^{Z,\boldsymbol{\mu}}=\sum_{\boldsymbol{k}}\mathcal{M}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}},\\ \mathcal{E}^{Z,\boldsymbol{\mu}}=\sum_{\boldsymbol{k}}\mathcal{E}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}.\end{cases} \tag{13}$$

Based on Eqs. (12) and (13), we obtain the following result:

$$\begin{cases}\mathbb{E}\left[\mathcal{M}^{Z,\boldsymbol{\mu}}\right]=\sum_{\boldsymbol{k}}Pr(\boldsymbol{\mu}|\boldsymbol{k})M_{\boldsymbol{k}}^{Z},\\ \mathbb{E}\left[\mathcal{E}^{Z,\boldsymbol{\mu}}\right]=\sum_{\boldsymbol{k}}Pr(\boldsymbol{\mu}|\boldsymbol{k})E_{\boldsymbol{k}}^{Z}.\end{cases} \tag{14}$$

For Z-pairs, the total ratio and the error ratio of pairs with intensity $\boldsymbol{\mu}$ and photon number $\boldsymbol{k}$ are defined as

$$\begin{aligned}&(m')^{Z,\boldsymbol{\mu}}=\frac{\mathcal{M}^{Z,\boldsymbol{\mu}}}{N^{\boldsymbol{\mu}}},\quad (e')^{Z,\boldsymbol{\mu}}=\frac{\mathcal{E}^{Z,\boldsymbol{\mu}}}{N^{\boldsymbol{\mu}}},\quad m_{\boldsymbol{k}}^{Z}=\frac{M_{\boldsymbol{k}}^{Z}}{N_{\boldsymbol{k}}},\\ &e_{\boldsymbol{k}}^{Z}=\frac{E_{\boldsymbol{k}}^{Z}}{N_{\boldsymbol{k}}},\quad (m')_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}=\frac{\mathcal{M}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}}{N^{\boldsymbol{\mu}}},\quad (e')_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}=\frac{\mathcal{E}_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}}{N^{\boldsymbol{\mu}}},\end{aligned} \tag{15}$$

where m (e) and m' (e') are used to distinguish between different variables, $N^{\boldsymbol{\mu}}:=q^{\boldsymbol{\mu}}N$ is the number of rounds with intensity $\boldsymbol{\mu}$, and $N_{\boldsymbol{k}}:=\sum_{\boldsymbol{\mu}}Pr(\boldsymbol{k}|\boldsymbol{\mu})N^{\boldsymbol{\mu}}$ is the number of rounds with photon number $\boldsymbol{k}$.

Based on the above analyses, it can be concluded that

$$\begin{aligned}\mathbb{E}\left[m^{Z,\boldsymbol{\mu}}\right]&=\mathbb{E}\left[\frac{\mathcal{M}^{Z,\boldsymbol{\mu}}}{N^{\boldsymbol{\mu}}}\right]=\frac{\mathbb{E}\left[\mathcal{M}^{Z,\boldsymbol{\mu}}\right]}{N^{\boldsymbol{\mu}}}=\frac{\sum_{\boldsymbol{k}}Pr(\boldsymbol{\mu}|\boldsymbol{k})M_{\boldsymbol{k}}^{Z}}{q^{\boldsymbol{\mu}}N}\\ &=\sum_{\boldsymbol{k}}Pr(\boldsymbol{k}|\boldsymbol{\mu})m_{\boldsymbol{k}}^{Z},\\ \mathbb{E}\left[e^{Z,\boldsymbol{\mu}}\right]&=\sum_{\boldsymbol{k}}Pr(\boldsymbol{k}|\boldsymbol{\mu})e_{\boldsymbol{k}}^{Z}.\end{aligned} \tag{16}$$

Similarly, we can obtain

$$\begin{cases}\mathbb{E}\left[m_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}\right]=Pr(\boldsymbol{k}|\boldsymbol{\mu})m_{\boldsymbol{k}}^{Z},\\ \mathbb{E}\left[e_{\boldsymbol{k}}^{Z,\boldsymbol{\mu}}\right]=Pr(\boldsymbol{k}|\boldsymbol{\mu})e_{\boldsymbol{k}}^{Z},\end{cases} \tag{17}$$

where $Pr(\boldsymbol{k}|\boldsymbol{\mu})$ is given by Eqs. (5) and (6). $\mathbb{E}\left[m^{Z,\boldsymbol{\mu}}\right]$ and $\mathbb{E}\left[e^{Z,\boldsymbol{\mu}}\right]$ are obtained experimentally. Subsequently, one can derive the lower bound $m_{(1,1)}^{Z,\boldsymbol{\mu},\mathrm{L}}$ of $m_{(1,1)}^{Z,\boldsymbol{\mu}}$ and the upper bound $e_{(1,1)}^{Z,\boldsymbol{\mu},\mathrm{U}}$ of $e_{(1,1)}^{Z,\boldsymbol{\mu}}$ according to Eq. (17).

The above is the analysis for the decoy-state in Z-basis. Similar steps can be applied to the X-basis to obtain the upper bound of the total ratio $m_{(1,1)}^{X,\mathrm{L}}$ and the lower bound of the error ratio $e_{(1,1)}^{X,\mathrm{U}}$ for single-photon pairs. In the decoy-state estimation, the asymptotic key rate formula under the mode-pairing scheme is expressed as

$$\begin{aligned}R&=m_{(1,1)}^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z,\mathrm{L}}\left[1-H\left(\frac{e_{(1,1)}^{X,\mathrm{U}}}{m_{(1,1)}^{X,\mathrm{L}}}\right)\right]\\ &\quad-fm^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}H\left(e^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}\right)\\ &=m^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}\left\{q_{(1,1)}\left[1-H\left(e_{(1,1)}\right)\right]\right.\\ &\quad\left.-fH\left(e^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}\right)\right\},\end{aligned} \tag{18}$$

where $q_{(1,1)}=m_{(1,1)}^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z,\mathrm{L}}/m^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}$, $m_{(1,1)}^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z,\mathrm{L}}$ is the lower bound on the ratio of single-photon pairs with intensity of $\boldsymbol{\mu}=(\mu^{\mathrm{a}},\mu^{\mathrm{b}})$, $m^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}$ is the ratio of pairs with intensity $\boldsymbol{\mu}=(\mu^{\mathrm{a}},\mu^{\mathrm{b}})$ in the Z basis, $e_{(1,1)}=e_{(1,1)}^{X,\mathrm{U}}/m_{(1,1)}^{X,\mathrm{L}}$ is the upper bound on the phase error rate of single-photon pairs with intensity $\boldsymbol{\mu}=(\mu^{\mathrm{a}},\mu^{\mathrm{b}})$, f is the error correction efficiency, and $H(\cdot)$ is the binary entropy function.

Furthermore, the key generation rate of the simulation formula is expressed as

$$R=r_p(p,l)\,r_{\mathrm{s}}\left\{q_{(1,1)}\left[1-H\left(e_{(1,1)}\right)\right]-fH\left(E_{\mu\mu}^{Z}\right)\right\}, \tag{19}$$

where

$$r_p(p,l)=\left[\frac{1}{p\left[1-(1-p)^{l}\right]}+\frac{1}{p}\right]^{-1}$$

is the pairing rate generated during each round, l is the maximum pairing interval, p is the probability of successful detection in each round, r_{s} is the probability that two paired round are Z pairs, $q_{(1,1)}$ denotes the single-photon pair ratio in all Z pairs, $e_{(1,1)}$ denotes the phase error rate of the single-photon pairs, $E_{\mu\mu}^{Z}=e^{(\mu^{\mathrm{a}},\mu^{\mathrm{b}}),Z}$ is the quantum bit error rate, f is the error correction efficiency. Detailed expressions for these parameters are shown in Appendix A.

3. Numerical simulation and discussion

Based on the key generation rate analysis in Section 2, we present the numerical simulation results of the key generation rate of the proposed HPCS-PDS-MP-QKD protocol. The basic parameters setting of the numerical simulation are shown in Table 1. Here, the detectors' detection efficiencies are assumed to be the same for the local and Charlie's side detectors.

Table 1. The basic parameters of numerical simulation. $P_d = d$ denotes the dark count rate of the single photon detector, e_d denotes the misalignment error, e_0 is the error rate caused by background light, $\eta_d = \eta$ denotes the detection efficiency of the single photon detector, α represents the attenuation coefficient of the fiber.

$d = P_d$	e_d	e_0	$\eta_d = \eta$	f	α
1.2×10^{-8}	4%	0.5	20%	1.15	0.2

Figure 2 shows the key generation rate of the proposed HPCS-PDS-MP-QKD protocol against the transmission distance under different maximum pairing intervals, together with the PLOB curve. The results show that, with the increase of the maximum matching interval l, the key generation rate increases. For the same transmission distance, say 300 km, the key generation rate for $l = 1$ is 9.2×10^{-10}, while it is 8.9×10^{-8} for $l = 10^2$, it is 2.3×10^{-6} for $l = 10^6$. Importantly, the key generation rate can exceed the PLOB bound, when l is greater than 10^3 and the transmission distance is greater than 200 km.

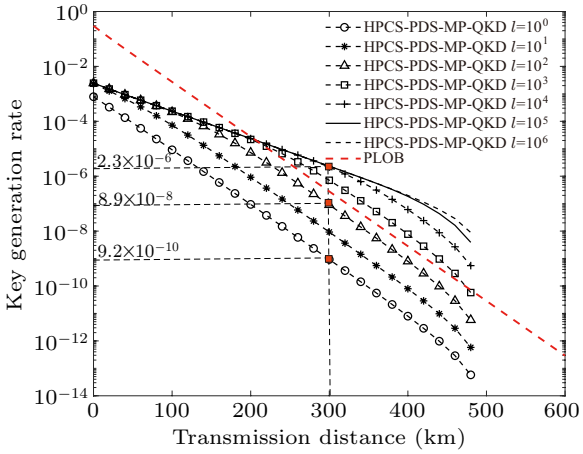


Fig. 2. The key generation rate of HPCS-PDS-MP-QKD protocol against the transmission distance under different maximum pairing intervals, l from 1 to 10^6.

Furthermore, we discuss the performance comparison of the proposed protocol with the original MP-QKD protocol. Figure 3 compares the key generation rates versus the transmission distance for three protocols: the proposed HPCS-PDS-MP-QKD, the original MP-QKD protocol (WCS-MP-QKD), and WCS-PDS-MP-QKD (WCS-MP-QKD with passive decoy state). These comparisons are shown under different maximum matching intervals. As can be seen from the figure, the proposed HPCS-PDS-MP-QKD protocol always exhibits improvement over the other two protocols for different maximum matching intervals. For the same maximum matching interval, the HPCS-PDS-MP-QKD protocol has a higher key generation rate. In addition, the HPCS-QKD protocol not only achieves a higher key rate compared to the the WCS-MP-QKD and WCS-PDS-MP-QKD protocols, but also maintains a key transmission distance of up to 480 km, approaching to that of the original MP-QKD protocol. It surpasses the WCS-MP-QKD protocol by nearly 40 km in terms of key transmission distance.

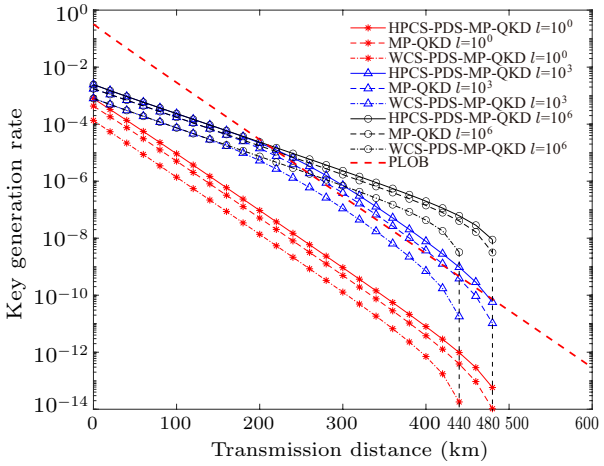


Fig. 3. The key generation rates of the HPCS-PDS-MP-QKD protocol, MP-QKD with WCS source (WCS-MP-QKD) and WCS-MP-QKD with passive decoy state (WCS-PDS-MP-QKD) against the transmission distance under different maximum matching intervals.

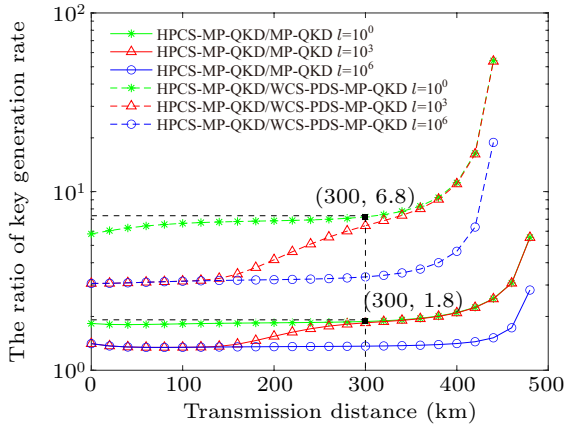


Fig. 4. The ratio of key generation rate of HPCS-MP-QKD over WCS-MP-QKD and WCS-PDS-MP-QKD against the transmission distance.

Figure 4 further shows the ratio of the key generation rate of HPCS-PDS-MP-QKD over WCS-MP-QKD, WCS-PDS-MP-QKD, against the transmission distance. The results demonstrate HPCS-PDS-MP-QKD has a performance superiority over both WCS-MP-QKD and WCS-PDS-MP-QKD protocols. Specifically, at 300-km transmission distance with $l = 1$, HPCS-PDS-MP-QKD achieves a 1.8-fold increase in key generation rate compared to WCS-MP-QKD, and a 6.8 times increase compared with WCS-PDS-MP-QKD. Under the same key transmission distance, as the maximum pairing interval increases, the ratio of the key transmission rates between the protocols decreases.

Finally, we discuss the finite size effects on the proposed protocol. Based on Eq. (19), we adopt the finite-size effects described in Ref. [41], rewrite key rate formula as

$$\begin{aligned} R_{\text{finite}} &= R - R_{\text{error}} \\ &= R - \frac{1}{N_t}\left(\log_2 \frac{8}{\varepsilon_{\text{cor}}} + 2\log_2 \frac{2}{\varepsilon' \hat{\varepsilon}} + 2\log_2 \frac{1}{\varepsilon_{\text{PA}}}\right), \end{aligned} \tag{20}$$

where ε' and $\hat{\varepsilon}$ are the failure probabilities introduced when the final key rate with single-photon pulse pairs is evaluated.

$\varepsilon_{\mathrm{PA}}$ is the probability that the privacy amplification based on two-universal hashing fails. $\varepsilon_{\mathrm{cor}}$ is the error probability when the strings of Alice and Bob are different, but the hash of them is identical. N_{t} is the total number of pulses.

Figure 5 shows the key generation rate of HPCS-PDS-MP-QKD protocol against the transmission distance under different N_t when the maximum matching intervals is $l = 10^6$. The results show that the key generation rate is increased as the total pulse length increases. When the total pulse length is 10^{11}, the key generation rate is almost equal to the infinite number of pulses.

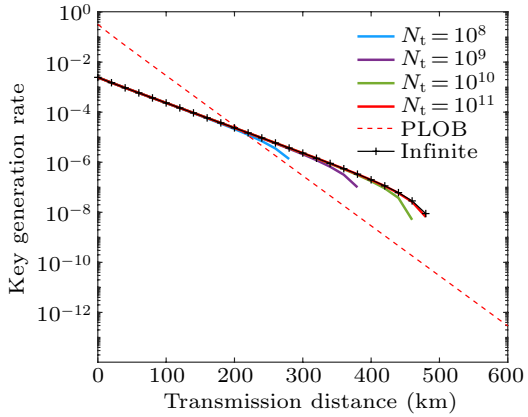


Fig. 5. The key generation rate of HPCS-PDS-MP-QKD protocol against the transmission distance under different N_{t}, the maximum matching intervals is $l = 10^6$ here.

4. Conclusion

To enhance the key generation rate, secure transmission distance and security against side channel attack, a mode-pairing quantum key distribution protocol based on heralded pair-coherent source with a passive decoy-state method is proposed, named HPCS-PDS-MP-QKD protocol. Numerical simulations demonstrate that when the maximum pairing interval is greater than 10^3, and the transmission distance exceeds 200 km, the proposed protocol can surpass the PLOB bound in key generation rate. Compared to WCS-MP-QKD and WCS-PDS-MP-QKD protocols, the proposed protocol exhibits significant advantages in both key rate and secure transmission distance. Notably, when the total pulse length is greater than 10^{11}, the finite-key effects can be negligible. The structure of passive decoy state devices can be extended to multiple passive decoy-states to further improve key generation performance. It indicates that the proposed protocol can keep the longer transmission distances, higher generation key rate of MP-QKD protocol, while avoid the side channel attack.

Appendix A: Simulation details

For simplicity, we denote the coherent pulse emitted by Alice in the i-th round as $\left|\sqrt{Z_i^{\mathrm{a}}\mu}\,\mathrm{e}^{\mathrm{i}\phi_i^{\mathrm{a}}}\right\rangle$, where $Z_i^{\mathrm{a}} \in \{0,1\}$, $\phi_i^{\mathrm{a}} \in [0,2\pi)$ is a random phase. Similarly, Bob's coherent state is $\left|\sqrt{Z_i^{\mathrm{b}}\mu}\,\mathrm{e}^{\mathrm{i}\phi_i^{\mathrm{a}}}\right\rangle$. Arrays $Z_i := \left[Z_i^{\mathrm{a}}, Z_i^{\mathrm{b}}\right] \in \{00,01,10,11\}$ represent the intensity vector of Alice and Bob in the i-th round. For the (i,j)-th paired pulses,

$$\tau_{i,j} = \left[\tau_{i,j}^{\mathrm{a}}, \tau_{i,j}^{\mathrm{b}}\right] := \left[Z_i^{\mathrm{a}} \oplus Z_j^{\mathrm{a}}, Z_i^{\mathrm{b}} \oplus Z_j^{\mathrm{b}}\right], \tag{A1}$$

where $\oplus$ represents modulo 2 addition. Then, when $\tau_{i,j} = [1,1]$, the (i,j) pair is an effective Z-basis pair. In the i-th round, two variables L_i and R_i are used to denote the click events of the L and R detectors in the i-th round. The variable for successful clicks is described by $Ck_i = L_i \oplus R_i$. It signifies the occurrence of a successful click only when $Ck_i = 1$.

The phase random coherent states emitted at round i can also be regarded as a mixture photon number states. The detection probability $P(Ck_i = 1|Z_i)$ under n photons can be expressed as

$$\begin{aligned} &P(Ck_i = 1|Z_i) \\ &\approx 1 - (1-2Pd)\left(\sum_{n=0}^{\infty} P_{\mu^{\mathrm{a}}}(n)(1-\eta_{\mathrm{s}})^n\right)^{Z_i^{\mathrm{a}}} \\ &\quad \left(\sum_{n=0}^{\infty} P_{\mu^{\mathrm{b}}}(n)(1-\eta_{\mathrm{s}})^n\right)^{Z_i^{\mathrm{b}}}, \end{aligned} \tag{A2}$$

where $\eta_{\mathrm{s}} = \eta_{\mathrm{d}} 10^{-\alpha s/10}$ is the channel transmittance from Alice (Bob) to Charlie, η_{d} is the detection efficiency of the detector at Charlie side, α is the channel transmission attenuation coefficient, s is the channel transmission length, and P_{d} is the dark count of the detectors at Charlie end. We denote the photon number distribution under the Z-basis pairs with intensity μ and photon number n in the signal state or decoy-state mode as $P_\mu(n)$, which is derived from Eqs. (1) and (4). The successful click probability of each round is

$$\begin{aligned} p := P(Ck_i = 1) &= \sum_{Z_i} P(Ck_i = 1|Z_i) P(Z_i) \\ &= \frac{1}{4}\sum_{Z_i} P(Ck_i = 1|Z_i). \end{aligned} \tag{A3}$$

The signal pairs are independent of each other, and the click probability caused by the intensity set Z after the pairing of round i and round j is

$$P(Z|Ck = 1) = \frac{P(Z, Ck = 1)}{P(Ck = 1)} = \frac{P(Ck = 1|Z)}{\sum_Z P(Ck = 1|Z)}. \tag{A4}$$

Suppose the photon number states emitted by Alice and Bob are $|n_i^{\mathrm{a}}\rangle$ and $|n_i^{\mathrm{b}}\rangle$, respectively, the detection probability $P(Ck_i = 1|n_i)$ is

$$P(Ck_i = 1|n_i) \approx 1 - (1-2P_{\mathrm{d}})(1-\eta_{\mathrm{s}})^{\left(n_i^{\mathrm{a}} + n_i^{\mathrm{b}}\right)}. \tag{A5}$$

In HPCS-PDS-MP-QKD, a successful click occurs when $\tau_{i,j} = [1,1]$. Thus, there are four possible cases, that is, $[Z_i, Z_j] \in \{[01,10],[10,01],[00,11],[11,00]\}$. The situation of

error cases are Err : $= \{[00,11],[11,00]\}$. For simplicity, several concise representations are adopted, that is,

$$\begin{aligned}
&P(Ck) = P(\text{Pair Clicked}) := P(Ck_i = Ck_j = 1) = p^2,\\
&P(E) = P(\text{Pair Effective}) := P(Z_i \oplus Z_j = 11),\\
&P(\text{Err}) = P(\text{Pair Erroneous}) := P([Z_i, Z_j] \in \text{Err}),\\
&P(S) = P(\text{Single-photon Pair}) := P(n_i \oplus n_j = 11). \qquad \text{(A6)}
\end{aligned}$$

Thus, the Z-pair ratio r_{s} can be calculated by

$$\begin{aligned}
r_{\text{s}} &= P(E|Ck) = P(Z_i \oplus Z_j = 11|Ck_i = 1, Ck_j = 1)\\
&= \frac{1}{16}\frac{1}{p^2}\sum_{Z_i \oplus Z_j = 11} P(Ck_i = 1|Z_i)\, P(Ck_j = 1|Z_j). \qquad \text{(A7)}
\end{aligned}$$

Alice and Bob estimate the qubit error rate of the key data in the Z-basis pairs, the overall strength is $(\mu^{\text{a}}_{i,j}, \mu^{\text{b}}_{i,j}) = (\mu, \mu)$, then the bit error rate is affected by the probability of different events occurring in the local detector (under the decoy state window), and the bit error rate $E^Z_{\mu\mu}$ is

$$\begin{aligned}
E^Z_{\mu\mu} &= P(\text{Err}|E, Ck) = \frac{P(\text{Err}, E|Ck)}{P(E|Ck)}\\
&= \frac{P(\text{Err}|Ck)}{P(E|Ck)} = r_{\text{s}}^{-1} P(\text{Err}|Ck)\\
&= \frac{1}{16}\frac{1}{r_{\text{s}}p^2}\sum_{[Z_i, Z_j] \in \text{Err}} P(Ck_i = 1|Z_i)\, P(Ck_j = 1|Z_j). \qquad \text{(A8)}
\end{aligned}$$

According to Eq. (4), it is estimated that the single photon pair rate q_{11} in the effective signal pair is

$$\begin{aligned}
q_{(1,1)} &= P(S|E, Ck) = \frac{P(S, E, Ck)}{P(E, Ck)} = \frac{1}{r_{\text{s}}p^2} P(S, E, Ck)\\
&= \frac{1}{r_{\text{s}}p^2}\sum_{Z_i, Z_j} P(S, E, Ck|Z_i, Z_j)\, P(Z_i, Z_j)\\
&= \frac{1}{16}\frac{1}{r_{\text{s}}p^2}\sum_{Z_i \oplus Z_j = 11} P(Ck|S, Z_i, Z_j)\, P(S|Z_i, Z_j)\\
&= \frac{1}{16}\frac{P^x_{\mu^{\text{a}}}(1) P^y_{\mu^{\text{b}}}(1)}{r_{\text{s}}p^2}\sum_{Z_i \oplus Z_j = 11} P(Ck_i = 1|n_i = Z_i)\\
&\quad \times P(Ck_j = 1|n_j = Z_j), \qquad \text{(A9)}
\end{aligned}$$

When the decoy-state estimation achieves the desired result, one can directly estimate the gain and error rate of the X basis using the following equation:[41]

$$\begin{aligned}
Y_{(1,1)} &= (1 - P_{\text{d}})^2 \left[\frac{\eta_{\text{L}}\eta_{\text{R}}}{2} + (2\eta_{\text{L}} + 2\eta_{\text{R}} - 3\eta_{\text{L}}\eta_{\text{R}}) P_{\text{d}}\right.\\
&\quad \left. + 4(1 - \eta_{\text{L}})\left(1 - \eta_{\text{R}} P^2_{\text{d}}\right)\right], \qquad \text{(A10)}\\
e_{(1,1)} &= \frac{\left[e_0 Y_{(1,1)} - (e_0 - e_{\text{d}})\left(1 - P^2_{\text{d}}\right)\frac{\eta_{\text{L}}\eta_{\text{R}}}{2}\right]}{Y_{(1,1)}}, \qquad \text{(A11)}
\end{aligned}$$

where $\eta_{\text{L}} = \eta_{\text{R}} = \eta_{\text{s}}$, e_0 is the error rate caused by background light, and e_{d} is the optical error rate caused by imperfect optical calibration of the system.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 62375140), the Postgraduate Research & Practice Innovation Program of Jiangsu Province, China (Grant No. KYCX24_1191 and SJCX25_0315), and the Open Research Fund of the National Laboratory of Solid State Microstructures (Grant No. M36055).

References

[1] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[3] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[4] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307
[5] Lucamarini M, Yuan Z L, Qi P, Dynes J F and Shields A J 2018 *Nature* **557** 400-403
[6] Pirandola S, Laurenza R, Ottaviani R and Banchi L 2017 *Nat. Commun.* **8** 15043
[7] Liu H, Jiang C, Zhu H T, Zou M, Yu Z W, Hu X L, Xu H, Ma S Z and Han Z Y 2018 *Phys. Rev. Lett.* **26** 5501
[8] Zhong X,Wang W, Qian L and Lo H K 2021 *npj Quantum Information* **7** 8
[9] Clivati C, Meda A, Donadello S and Virzi S 2022 *Nat. Commun.* **13** 157
[10] Wang S,Yin Z Q,He D Y and Chen W 2022 *Nat. Photon.* **16** 154
[11] Ma X F, Zeng L and Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[12] Zeng P, Wu W J and Ma X F 2020 *Phys. Rev. Appl.* **13** 064013
[13] Yu Y, Wang L, Zhao S M and Mao Q P 2021 *Opt. Express* **29** 2227
[14] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[15] Xue K, Zhao S M and Mao Q P 2021 *Quantum Information Processing* **20** 1-16
[16] Lin J and Lutkenhaus N 2018 *Phys. Rev. A* **980** 042332
[17] Wang R, Yin Z Q and Lu F Y 2020 *Commun. Phys.* **3** 149
[18] Li B H, Xie Y M, Li Z and Weng C X 2021 *Opt. Lett.* **46** 5529
[19] Yu Y, Li W, Wang L and Zhao S M 2024 *Phys. Rev. A* **109** 052609
[20] Zeng P, ZHou H Y, Wu W J and Ma X F 2022 *Nat. Commun.* **13** 3903
[21] Xie M Y, Lu Y S, Weng X C and Cao X Y 2022 *PRX Quantum* **3** 020315
[22] Zhu H T, Huang Y Z, Liu H, Zeng P, Zou M and Dai Y Q 2023 *Phys. Rev. Lett.* **130** 030801
[23] Zhou L, Jin J P, Xie Y M and Lu Y S 2023 *Phys. Rev. Lett.* **130** 250801
[24] Li Z H, Dou T Q, Cheng M, Liu Y and Tang J J 2024 *Opt. Lett.* **49** 6609-6612
[25] Jiang M S, Sun S H, Li C Y and Liang L M 2012 *Phys. Rev. A* **86** 032310
[26] Yang X L, Li Y Q and Li H W 2025 *Chin. Phys. B* **34** 020301
[27] Li J J, Wang Y, Li H W and Bao W S 2020 *Chin. Phys. B* **29** 030303
[28] Zhou J P, Zhou Y Y, Gu R W and Zhou X J 2022 *Int. J. Quantum Inform.* **20** 2250005
[29] Wang X, Lu F Y, Wang Z H, YIn Z Q and Wang S 2024 *Phys. Rev. A* **21** 6
[30] Xue K, Shen Z G and Zhao S M 2022 *Entropy* **24** 662
[31] Teng J, Lu F Y and Yin Z Q 2020 *New J. Phys.* **22** 103017
[32] Li Y, Bao W S, Li H W, Zhou C and Wang Y 2025 *Chin. Phys. B* **24** 110307
[33] Wang X B 2013 *Phys. Rev. A* **87** 012320
[34] Schiavon M, Vallone G and Ticozzi F 2016 *Phys. Rev. A* **93** 012331
[35] Han L, Yu Y, Lu W, Xue K, Li W and Zhao S M 2022 *Quantum Inf. Process.* **22** 37
[36] Wang L and Zhao S M 2017 *Quantum Inf. Process.* **16** 1
[37] Lo H K, Curty M and Qi B 2012 *Phys. Rev. A* **108** 130503
[38] Lu Z Y, Wang G, Li C and Cao Z 2024 *Phys. Rev. A* **109** 012401
[39] Zhang Z, Zhao Q, Razavi M and Ma X F 2017 *Phys. Rev. A* **95** 012333
[40] Hu X L, Yu Z W and Wang X B 2018 *Phys. Rev. A* **98** 032303
[41] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319