Advantages of Asynchronous Measurement-Device-Independent Quantum Key Distribution in Intercity Networks

Yuan-Mei Xie, Jun-Lin Bai, Yu-Shuo Lu, Chen-Xun Weng, Hua-Lei Yin,* and Zeng-Bing Chen†
National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China

(Received 21 February 2023; accepted 1 May 2023; published 22 May 2023)

The alternative variant of measurement-device-independent quantum key distribution (MDI QKD), called asynchronous MDI QKD or mode-pairing MDI QKD, offers similar repeaterlike rate-loss scaling but has the advantage of simple technology implementation by exploiting an innovative postmeasurement pairing technique. We herein present an evaluation of the practical aspects of decoy-state asynchronous MDI QKD. To determine its effectiveness, we analyze the optimal method of decoy-state calculation and examine the impact of asymmetrical channels and multiuser networks. Our simulations show that, under realistic conditions, aynchronous MDI QKD can furnish the highest key rate with MDI security as compared to other QKD protocols over distances ranging from 50 to 480 km. At fiber distances of 50 and 100 km, the key rates attain 6.02 and 2.29 Mbps, respectively, which are sufficient to facilitate real-time one-time-pad video encryption. Our findings indicate that experimental implementation of asynchronous MDI QKD in intercity networks can be both practical and efficient.

DOI: 10.1103/PhysRevApplied.19.054070

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] enables two remote parties to share secret keys protected from eavesdropping by the laws of physics. In the last 40 years, QKD has achieved rapid development in terms of secret-key rates [3–6], transmission distance [7–9], and network deployment [10–13]. Although the security of QKD has been proven in theory, the imperfections of realistic devices lead to various security loopholes [14–16], especially in detection [15].

Fortunately, measurement-device-independent (MDI) QKD is proposed [17], which assumes an untrusted intermediate node to perform two-photon Bell-state measurements, thus solving all security issues at the detection side [18]. Extensive work demonstrates the potential of MDI QKD, including experimental breakthroughs [19–25], on-chip implementations [26–28], and continuous theoretical developments [29–34]. Moreover, users in a MDI QKD network can share expensive detectors, and the topology of MDI QKD is naturally suitable for deployment in star-type networks. Additionally, side-channel-secure QKD has recently been experimentally realized, which is not only MDI but also immune to potential source imperfections [35,36]. However, the key rates of most forms of QKD are fundamentally bounded by the secret-key capacity of repeaterless QKD [37–40] due to photon loss in the channel. A rigorous theorem, the absolute repeaterless secret-key capacity (SKC_0), expresses this limit as $R = -\log_2(1-\eta)$ [39], i.e., the key rate R scales linearly with the channel transmittance η. Despite some progress in overcoming this bound [41–44], such devices remain elusive.

Twin-field (TF) QKD [45] and its variants [46–51] are proposed to break this bound. The protocols make the untrusted intermediate node use Bell-state measurements based on single-photon interference, rather than two-photon interference. Numerous works have advanced theory with finite-key analysis [52–55]. Reference [56] applies entangled coherent-state sources as untrusted relays to further increase the transmission distance of TF QKD by reducing the signal-to-noise ratio at the measurement nodes. Several experimental achievements have shown the performance of twin-field QKD over large loss [57–70], and the maximum distance of TF QKD has been experimentally increased to 830 km [68]. The idea of single-photon interference has also been implemented in device-independent QKD [71]. Nonetheless, as TF QKD requires stable long-distance single-photon interference, phase-tracking and phase-locking techniques are indispensable [45]. These techniques are complicated and expensive, and usually impose a negative impact on the system performance. For example, phase-tracking technology requires sending strong reference light, which reduces

*hlyin@nju.edu.cn
†zbchen@nju.edu.cn

the effective clock frequency of the quantum signal and increases background noise [61,62,67,68].

Recently, the alternative variant [72,73] of MDI QKD, called asynchronous MDI QKD [72] (also called mode-pairing MDI QKD [73]), is proposed. It asynchronously pairs two successful clicks within a long pairing time to establish a two-photon Bell state, thereby breaking SKC_0. Asynchronous MDI QKD is highly practical and has a noteworthy advantage over TF QKD in intercity-distance quantum communications, owing to its implementation simplicity and performance. Several exciting experiments have successfully verified the superior performance of asynchronous MDI QKD with accessible technology. Reference [74] realizes the experiment with a maximal distance of 407 km without global phase locking. Reference [75] demonstrates the first asynchronous MDI QKD that overcomes SKC_0 without global phase tracking and extends the maximal distance to 508 km. However, before asynchronous MDI QKD can be applied in real life, many issues of practicality necessitate resolution, such as identifying the optimal number of decoy states, determining the optimal calculation method of decoy states, and assessing the performance in asymmetric channels and networks.

In this work, we address these issues by introducing the joint-constraints technique [76] and alternative methods for phase-error-rate estimation to enable higher-rate asynchronous MDI QKD. By employing the three-intensity protocol alongside an additional *click filtering* operation—which is the known best choice for performance—we simulate the key rate of asynchronous MDI QKD in multiuser networks. For a network of five users, asynchronous MDI QKD result in the key rates of all links surpassing the secret-key capacity. Furthermore, using a 4-GHz repetition-rate system [68], secret-key rates of 6.02, 2.29, and 0.31 Mbps can be achieved at fiber distances of 50, 100, and 200 km, respectively. Asynchronous MDI QKD can achieve the highest key rate in the range of 170 to 480 km, compared with decoy-state QKD [77–79] and TF QKD [45]. What is more, our work provides conceptual differences between asynchronous MDI QKD and its synchronous version (original time-bin MDI QKD) [80] in Sec. V. Asynchronous MDI QKD holds the most promising potential as a solution for intercity-distance quantum communication in the future, owing to its minimal detector requirements and absence of strong light feedback.

II. PROTOCOL DESCRIPTION

Here, we consider an asymmetric asynchronous MDI QKD protocol using the three-intensity setting, which is similar to the protocol described in Ref. [75], but offers the option to use *click filtering* or not. The intensity of each laser pulse is randomly set to one of the three intensities $\mu_{a(b)}$ (signal), $\nu_{a(b)}$ (decoy), and $o_{a(b)}$ (vacuum), and the intensities satisfy $\mu_{a(b)} > \nu_{a(b)} > o_{a(b)} = 0$. A successful click is obtained when one and only one detector clicks in a time bin, and we refer to $(k_a|k_b)$ as a successful click when Alice sends intensity k_a and Bob sends k_b. The notation $[k_a^{\rm tot}, k_b^{\rm tot}]$ indicates an asynchronous coincidence where the combined intensity in the two time bins Alice (Bob) sent is $k_a^{\rm tot}$ ($k_b^{\rm tot}$). The details of the protocol are presented as follows.

1. Preparation. For each time bin, Alice chooses a phase value $\theta_a = 2\pi M_a/M$ with $M_a \in \{0, 1, \ldots, M-1\}$ at random. Then, she selects an intensity choice $k_a \in \{\mu_a, \nu_a, o_a\}$ with probabilities p_{μ_a}, p_{ν_a}, and $p_{o_a} = 1 - p_{\mu_a} - p_{\nu_a}$, respectively. Alice prepares a weak laser pulse $|e^{{\rm i}\theta_a}\sqrt{k_a}\rangle$ based on the chosen values. Similarly, Bob prepares a weak coherent pulse $|e^{{\rm i}\theta_b}\sqrt{k_b}\rangle$ ($k_b \in \{\mu_b, \nu_b, o_b\}$). Finally, Alice and Bob send their optical pulses to Charlie via the quantum channel.

2. Measurement. For each time bin, Charlie performs a first-order interference measurement on the two received pulses, and he publicly announces whether a successful click is obtained and which detector (D_L or D_R) clicked. The first two steps is repeated N times.

3. Coincidence pairing. The clicks that Alice and Bob retained for further processing depend on whether *click filtering* is applied. If they perform *click filtering*, Alice (Bob) announces whether she (he) applied the decoy intensity ν_a (ν_b) to the pulse sent for each event. Then they discard clicks $(\mu_a|\nu_b)$ and $(\nu_a|\mu_b)$, and keep all other clicks. Otherwise, they keep all clicks.

For all kept clicks, Alice and Bob always pair a click with the nearest one within a time interval T_c to form a successful coincidence. They discard the lone click that failed to find a partner within T_c. For each coincidence, Alice (Bob) computes the total intensity used between the two time bins $k_a^{\rm tot}$ ($k_b^{\rm tot}$) and the phase differences between the early (e) and late (l) time bins, $\varphi_{a(b)} = \theta_{a(b)}^l - \theta_{a(b)}^e$.

4. Sifting. Alice and Bob announce their computational results and then discard the data if $k_a^{\rm tot} = \mu_a + \nu_a$ or $k_b^{\rm tot} = \mu_b + \nu_b$. When there is a *click-filtering* operation, we define $\tilde{k}_{a(b)} = \mu_{a(b)}$; otherwise, we define $\tilde{k}_{a(b)} \in \{\mu_{a(b)}, \nu_{a(b)}\}$. For $[\tilde{k}_a, \tilde{k}_b]$ coincidence, Alice (Bob) extracts a **Z**-basis bit 0 (1) if she (he) sends $\tilde{k}_{a(b)}$ in the early time bin and $o_{a(b)}$ in the late time bin. Otherwise, Alice (Bob) extracts an opposite bit. Note that we use four intensity groups ($[\mu_a, \mu_b], [\mu_a, \nu_b], [\nu_a, \nu_b], [\nu_a, \mu_b]$) for the key generation when *click filtering* is not applied, while existing MDI QKD protocols typically use only one intensity group. For $[2\nu_a, 2\nu_b]$ and $[2\mu_a, 2\mu_b]$ coincidences, Alice and Bob calculate the relative phase difference $\varphi_{ab} = (\varphi_a - \varphi_b) \mod 2\pi$. They extract an **X**-basis bit 0 if $\varphi_{ab} = 0$ or π. Afterwards, Bob flips his bit value, if $\varphi_{ab} = 0$ and both detectors clicked, or $\varphi_{ab} = \pi$ and the same detector clicked twice. The coincidence with other phase differences is discarded.

5. Parameter estimation. Alice and Bob group their data into different sets $\mathcal{S}_{[k_a^{\rm tot},k_b^{\rm tot}]}$ and count the corresponding number $n_{[k_a^{\rm tot},k_b^{\rm tot}]}$. By using all the raw data they have obtained, Alice and Bob estimate the necessary parameters to calculate the key rate. They estimate the number of vacuum events, s_0^z, the number of single-photon pair events in the **Z** basis, s_{11}^z, the bit-error rate of the single-photon pairs in the **X** basis, e_{11}^x, and the phase-error rate associated with the single-photon pair events in the **Z** basis, ϕ_{11}^z.

6. Key distillation. Alice and Bob perform an error-correction step that reveals at most $\lambda_{\rm EC}$ bits of information. Under the condition of passing the checks in the error correction and privacy amplification steps, a $\varepsilon_{\rm tot}$-secure key of length [75,81]

$$\ell = \underline{s}_0^z + \underline{s}_{11}^z\left[1 - H_2\left(\overline{\phi}_{11}^z\right)\right] - \lambda_{\rm EC}\log_2\frac{2}{\varepsilon_{\rm cor}} - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} - 2\log_2\frac{1}{2\varepsilon_{\rm PA}}, \tag{1}$$

can be extracted, where $\underline{x}$ and $\overline{x}$ are the lower and upper bounds of the observed value x, respectively; $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Using the entropic uncertainty relation [75], the total secure coefficient $\varepsilon_{\rm tot} = 2(\varepsilon' + 2\varepsilon_e + \hat{\varepsilon}) + \varepsilon_0 + \varepsilon_1 + \varepsilon_\beta + \varepsilon_{\rm PA} + \varepsilon_{\rm cor}$, where $\varepsilon_{\rm cor}$ is the failure probability of error correction; $\varepsilon_{\rm PA}$ is the failure probability of privacy amplification; $\hat{\varepsilon}$ and ε' are the coefficients while using a chain rule for smooth entropies; ε_0, ε_1, and ε_e are the failure probabilities for estimating the terms of s_0^z, s_{11}^z, and ϕ_{11}^z, respectively.

III. THE KEY-RATE FORMULA

In the following description, let x^* be the expected value of x. In the asynchronous MDI QKD protocol, $[\tilde{k}_a, \tilde{k}_b]$ coincidence can be used to generate keys. Since the binary Shannon entropy function is concave, we can correct errors for each group $[\tilde{k}_a, \tilde{k}_b]$ separately to reduce the consumption of information, which does not affect the security of the protocol. Hence the amount of information consumed in error correction can be written as

$$\lambda_{\rm EC} = \sum_{\tilde{k}_a,\tilde{k}_b}\left[n_{[\tilde{k}_a,\tilde{k}_b]} f H_2\left(E_{[\tilde{k}_a,\tilde{k}_b]}\right)\right], \tag{2}$$

where f is the error-correction efficiency and $E_{[\tilde{k}_a,\tilde{k}_b]}$ is the bit-error rate of $[\tilde{k}_a, \tilde{k}_b]$ coincidence. Because vacuum states contain no information about their bit values, in the asymmetric case we can separately extract higher-valued vacuum components in each group $[\tilde{k}_a, \tilde{k}_b]$ to obtain higher key rates. The total number of vacuum components in the

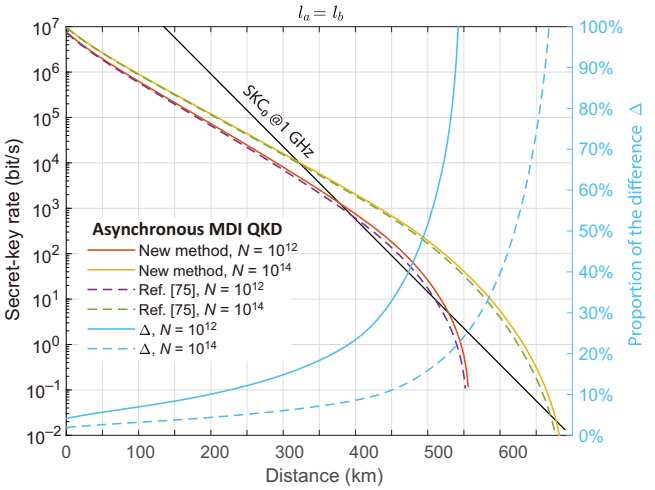

FIG. 1. Secret-key rates of the three-intensity asynchronous MDI QKD protocol with *click filtering* using different phase-error-rate estimation methods. Here $l_a(l_b)$ is the distance between Alice (Bob) and Charlie. The horizontal axis represents the total transmission distance $l = l_a + l_b$. The relative difference between the secret-key rates of the alternative method $R_{\rm new}$ and that of the original method $R_{\rm ori}$ is shown with the y axis on the right. $\Delta = (R_{\rm new} - R_{\rm ori})/R_{\rm ori}$. The numerical results here show that the alternative phase-error-rate estimation method has a notable advantage.

Z basis can be given by

$$\underline{s}_0^{z*} = \sum_{\tilde{k}_a,\tilde{k}_b}\max\left\{\frac{e^{-\tilde{k}_a}p_{[\tilde{k}_a,\tilde{k}_b]}}{p_{[o_a,\tilde{k}_b]}}\underline{n}^*_{[o_a,\tilde{k}_b]}, \frac{e^{-\tilde{k}_b}p_{[\tilde{k}_a,\tilde{k}_b]}}{p_{[\tilde{k}_a,o_b]}}\underline{n}^*_{[\tilde{k}_a,o_b]}\right\}. \tag{3}$$

Here $p_{[k_a^{\rm tot},k_b^{\rm tot}]}$ is the probability that $[k_a^{\rm tot}, k_b^{\rm tot}]$ coincidence occurs given the coincidence event, which is

$$p_{[k_a^{\rm tot},k_b^{\rm tot}]} = \sum_{k_a^e+k_a^l=k_a^{\rm tot}}\sum_{k_b^e+k_b^l=k_b^{\rm tot}}\frac{p_{k_a^e}p_{k_b^e}}{p_s}\frac{p_{k_a^l}p_{k_b^l}}{p_s}. \tag{4}$$

When *click filtering* is not applied, $p_s = 1$, otherwise $p_s = 1 - p_{\mu_a}p_{\nu_b} - p_{\nu_a}p_{\mu_b}$.

Next, we need to estimate the number and phase-error rate of the single-photon pairs in the **Z** basis, s_{11}^z and ϕ_{11}^z. Because the density matrices of single-photon pairs are identical in the **Z** and **X** bases, the expected ratio of different intensity settings is the same for all single-photon pairs [17,31]; namely,

$$\frac{\underline{s}_{11}^{z*}}{\underline{s}_{11}^{x*}} = \frac{t_{11}^{z*}}{t_{11}^{x*}} = \frac{\sum_{\tilde{k}_a,\tilde{k}_b}\left(\tilde{k}_a\tilde{k}_b e^{-\tilde{k}_a-\tilde{k}_b}p_{[\tilde{k}_a,\tilde{k}_b]}\right)}{4\nu_a\nu_b e^{-2\nu_a-2\nu_b}p_{[2\nu_a,2\nu_b]}}, \tag{5}$$

where t_{11}^z represents the number of errors of the single-photon pairs in the **Z**, while s_{11}^x and t_{11}^x denote the number

of single-photon pairs and their corresponding error count in $[2\nu_a, 2\nu_b]$ coincidence, respectively.

$$\underline{s}_{11}^{z*} = \frac{\sum_{\tilde{k}_a,\tilde{k}_b}\left(\tilde{k}_a\tilde{k}_b e^{-\tilde{k}_a-\tilde{k}_b}p_{[\tilde{k}_a,\tilde{k}_b]}\right)}{\nu_a\nu_b\mu_a\mu_b(\mu'-\nu')}\left[\mu_a\mu_b\mu'\left(e^{\nu_a+\nu_b}\frac{\underline{n}^*_{[\nu_a,\nu_b]}}{p_{[\nu_a,\nu_b]}} - e^{\nu_b}\frac{\overline{n}^*_{[o_a,\nu_b]}}{p_{[o_a,\nu_b]}}\right.\right.$$
$$\left.\left. - e^{\nu_a}\frac{\overline{n}^*_{[\nu_a,o_b]}}{p_{[\nu_a,o_b]}} + \frac{\underline{n}^*_{[o_a,o_b]}}{p_{[o_a,o_b]}}\right) - \nu_a\nu_b\nu'\left(e^{\mu_a+\mu_b}\frac{\overline{n}^*_{[\mu_a,\mu_b]}}{p_{[\mu_a,\mu_b]}} - e^{\mu_b}\frac{\underline{n}^*_{[o_a,\mu_b]}}{p_{[o_a,\mu_b]}} - e^{\mu_a}\frac{\underline{n}^*_{[\mu_a,o_b]}}{p_{[\mu_a,o_b]}} + \frac{\underline{n}^*_{[o_a,o_b]}}{p_{[o_a,o_b]}}\right)\right], \tag{6}$$

where

$$\begin{cases}\mu' = \mu_a, & \nu' = \nu_a, \quad \text{if} \quad \frac{\mu_a}{\mu_b} \le \frac{\nu_a}{\nu_b},\\ \mu' = \mu_b, & \nu' = \nu_b, \quad \text{if} \quad \frac{\mu_a}{\mu_b} > \frac{\nu_a}{\nu_b}.\end{cases} \tag{7}$$

We can use the technique of joint constraints [76] to obtain the tighter estimated value of s_{11}^{z*}. The details of the analytic results of joint constraints are shown in Appendix A. Then we can obtain the lower bound of s_{11}^{x*} with Eq. (5).

The upper bound of the single-photon pair errors in the **X** basis is

$$\overline{t}_{11}^{x} = m_{[2\nu_a,2\nu_b]} - \underline{m}^0_{[2\nu_a,2\nu_b]}, \tag{8}$$

where $m_{[2\nu_a,2\nu_b]}$ is the observed error bit number in the **X** basis, and $m^0_{[2\nu_a,2\nu_b]}$ is the error bit number in the **X** basis given that at least one of Alice and Bob sends vacuum component. The lower bound of the expected value $\underline{m}^{0*}_{[2\nu_a,2\nu_b]}$ can be given by

$$\underline{m}^{0*}_{[2\nu_a,2\nu_b]} = \frac{e^{-2\nu_a}p_{[2\nu_a,2\nu_b]}}{2p_{[o_a,2\nu_b]}}\underline{n}^*_{[o_a,2\nu_b]} + \frac{e^{-2\nu_b}p_{[2\nu_a,2\nu_b]}}{2p_{[2\nu_a,o_b]}}\underline{n}^*_{[2\nu_a,o_b]} - \frac{e^{-2\nu_a-2\nu_b}p_{[2\nu_a,2\nu_b]}}{2p_{[o_a,o_b]}}\overline{n}^*_{[o_a,o_b]}. \tag{9}$$

Using similar arguments, we obtain the tighter value of $\underline{m}^{0*}_{[2\nu_a,2\nu_b]}$ under the joint constraints [76].

For single-photon pairs, the expected value of the phase-error rate in the **Z** basis equals the expected value of the bit-error rate in the **X** basis, and the error rate $\overline{e}^x_{11} = \overline{t}^x_{11}/\underline{s}^x_{11}$. There are two methods for estimating $\overline{\phi}^z_{11}$. The first method involves using the random sampling method to estimate $\overline{\phi}^z_{11}$ from $\overline{e}^x_{11}$ [75]. Explicitly [82],

$$\overline{\phi}^z_{11} = \overline{e}^x_{11} + \gamma\left(\underline{s}^z_{11}, \underline{s}^x_{11}, \overline{e}^x_{11}, \varepsilon_e\right), \tag{10}$$

where

$$\gamma^U(n,k,\lambda,\epsilon) = \frac{[(1-2\lambda)AG/(n+k)] + \sqrt{[A^2G^2/(n+k)^2] + 4\lambda(1-\lambda)G}}{2 + 2[A^2G/(n+k)^2]}, \tag{11}$$

with $A = \max\{n,k\}$ and $G = (n+k)/nk\ln(n+k)/2\pi nk\lambda(1-\lambda)\epsilon^2$.

On the other hand, following Ref. [31], an alternative approach involves using the observed values of t^z_{11} to estimate the upper bound for ϕ^z_{11}. Specifically,

$$\overline{\phi}^z_{11} = \frac{\overline{t}^z_{11}}{\underline{s}^z_{11}}, \tag{12}$$

where the upper bound of t^z_{11} and the lower bound of s^z_{11} can be estimated by $\overline{t}^{z*}_{11}$ and $\underline{s}^{z*}_{11}$ with the Chernoff bound [see Eqs. (E1) and (E2) in Appendix E]. We can calculate $\overline{t}^{z*}_{11}$ with Eq. (5) and

$$\overline{t}^{x*}_{11} = m^*_{[2\nu_a,2\nu_b]} - \underline{m}^{0*}_{[2\nu_a,2\nu_b]}. \tag{13}$$

Then we estimate the lower bound of s_{11}^{z*} using the decoy-state method [77–79], which can be given by

TABLE I. Simulation parameters. Here $\eta_d = \eta_d^L = \eta_d^R$, $p_d = p_d^L = p_d^R$, and $\eta_d^L(\eta_d^R)$ and $p_d^L(p_d^R)$ are the detection efficiency and the dark count rate of the detector $D_L(D_R)$, respectively; α denotes the attenuation coefficient of the fiber; ω_{fib} is the fiber phase drift rate; E_{HOM} is the interference misalignment error rate; f is the error-correction efficiency; $\Delta\nu$ is the laser frequency difference; and ϵ is the failure probability considered in the error verification and finite data analysis.

η_d	p_d	α	ω_{fib}	E_{HOM}	f	$\Delta\nu$	ϵ
80%	0.1 Hz	0.16 dB/km	5900 rad/s	0.04	1.1	10 Hz	10^{-10}

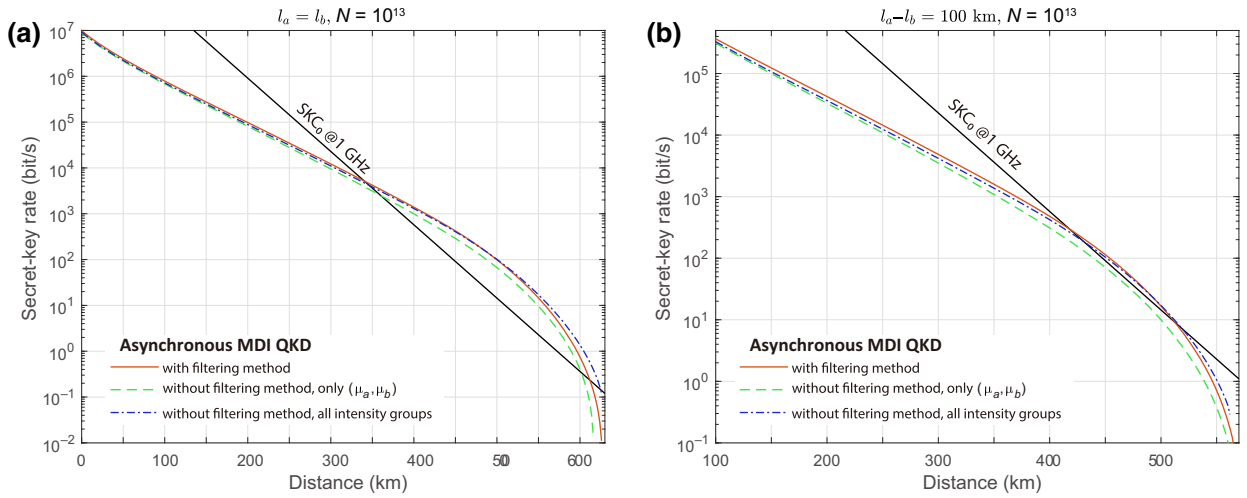

FIG. 2. Comparison of the secret-key rates of asynchronous MDI QKD with and without *click filtering* under two types of channels: (a) symmetric channel $l_a = l_b$ and (b) asymmetric channels $l_a - l_b = 100$ km. The horizontal axis represents the total transmission distance $l = l_a + l_b$.

IV. PERFORMANCE

A. Optimal decoy-state method

For the evaluation, we numerically optimize the secret-key rate $R := \ell F/N$ of asynchronous MDI QKD with Eq. (10) (original method Ref. [75]) and Eq. (12) (alternative method), which is shown in Fig. 1. Here F is the system clock frequency. In this work, we set failure parameters ε_{cor}, ε', ε_e, $\hat{\varepsilon}$, ε_β, and ε_{PA} to be the same value: ϵ. The experimental parameters are set to the values used in the state-of-the-art system, as shown in Table I. We denote the distance between Alice (Bob) and Charlie by $l_a(l_b)$. In Fig. 1, we set $F = 1$ GHz and $l_a = l_b$, and the source parameters of Alice and Bob are all the same. The genetic algorithm is exploited to globally search for the optimal value of light intensities and their corresponding probabilities. The black line is the results of SKC$_0$. We denote the relative difference between the key rate of the alternative method R_{alt} and that of the original method R_{ori} as $\Delta = (R_{\text{alt}} - R_{\text{ori}})/R_{\text{ori}}$. The results show that as the distance increases, the influence of statistical fluctuations becomes increasingly significant, and the key-rate advantage of the new phase-error-rate estimation method is also increasing. For example, at a fiber length of 600 km with $N = 10^{14}$, the secret-key rate obtained by the new phase-error-rate estimation method is approximately 1.49 times that of the original method. In the following key-rate calculations, we use the alternative phase-error-rate estimation method by default.

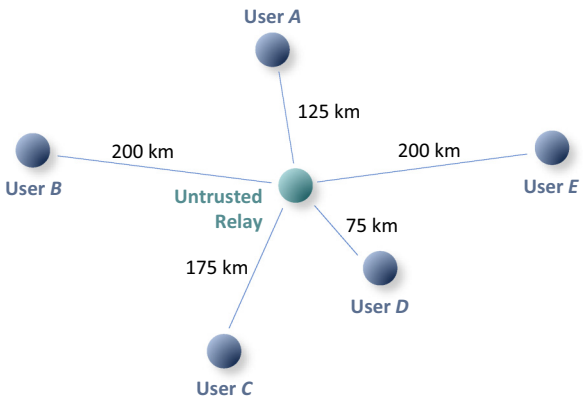

FIG. 3. Example of a scalable QKD network setup consisting of numerous users who may freely join or leave the network. Each user node has an asymmetric channel connected to an untrusted relay, through which it can establish a QKD link to others.

B. Optimal protocol

Figure 2 shows a comparison of the secret-key rates of asynchronous MDI QKD with and without *click filtering* under symmetrical $l_a = l_b$ and asymmetrical channels $l_a - l_b = 100$ km. The parameters are listed in Table I. $F = 1$ GHz and $N = 10^{13}$ are used. The green dotted line is a result of using only $[\mu_a, \mu_b]$ coincidence to form the secret key without *click filtering*. In the symmetric channel, Fig. 2(a), we can see that the key rate of asynchronous MDI QKD with *click filtering* is always higher than that of asynchronous MDI QKD without *click filtering* based on the $[\mu_a, \mu_b]$ group. This is expected since the filtering operation corresponds to a higher number of valid pairs and smaller statistical fluctuations in the estimation process. And the key rate of asynchronous MDI QKD with *click filtering* is higher than that of asynchronous MDI QKD without *click filtering* based on four intensity groups at short and medium distances. At a fiber length of 300 km, the secret-key rate obtained with *click filtering* is

TABLE II. Simulated secret-key rates per second for asynchronous MDI QKD, SNS QKD with the AOPP method, and PM QKD in the QKD network shown in Fig. 3 using the parameters in Table IV. The system clock frequency is 4 GHz and the transmission time is 22 h. Here, link *A*-*B* represents that user *A* communicates with user *B*. The sending intensities and corresponding probabilities are selected by the users to obtain the optimal key rate for each link. Note that here we consider a 50% duty cycle for the TF-type protocols [57,67,70].

Link	*A*-*B* (*A*-*E*)	*B*-*C* (*C*-*E*)	*B*-*D* (*D*-*E*)	*B*-*E*	*A*-*C*	*A*-*D*	*C*-*D*
SKC_0	5.77×10^3	4.80×10^3	1.45×10^4	2.30×10^3	1.21×10^4	3.64×10^4	3.03×10^4
Asynchronous MDI QKD	1.47×10^4	1.36×10^4	2.05×10^4	9.46×10^3	2.36×10^4	4.04×10^4	3.56×10^4
SNS QKD (AOPP)	1.18×10^4	1.09×10^4	1.64×10^4	7.53×10^3	1.78×10^4	3.05×10^4	2.72×10^4
PM QKD	2.56×10^3	2.40×10^3	3.22×10^3	1.71×10^3	4.19×10^3	6.91×10^3	6.01×10^3

approximately 1.11 times the one without *click filtering* based on four intensity groups, and 1.29 times the one based on $[\mu_a, \mu_b]$ group. At longer distances, the effectiveness of click filtering is diminished by a decrease in coincidence pairing efficiency due to less frequent photon clicks. Therefore, in scenarios where click filtering is not utilized, incorporating additional intensity groups ($[\mu_a, \nu_b], [\nu_a, \mu_b], [\nu_a, \nu_b]$) for key generation can lead to higher key rates at longer distances than using click filtering alone. The same trend is observed for the asymmetric channel [Fig. 2(b)].

C. Asynchronous MDI QKD networks

We provide a figure about a scalable QKD network setup consisting of numerous users who may freely join or leave the network in Fig. 3. Each user node has an asymmetric channel connected to an untrusted relay, through which it can establish a QKD link to others. The users will adjust the sending intensities and corresponding probability values so that each link can obtain the optimal key rate. The experimental parameters used here are listed in Table IV.

Table II shows simulated secret-key rates per second for asynchronous MDI QKD, sending-or-not-sending QKD (SNS QKD) with actively odd-parity pairing (AOPP) [83], and phase-matching QKD (PM QKD) [84] in the QKD intercity network. Assuming a clock rate of 4 GHz [68] and a transmission time of 22 h, which corresponds to approximately 3.2×10^{14} quantum pulses for asynchronous MDI QKD. We further assume that the quantum transmission duty ratio for the SNS QKD and PM QKD systems is 50% [57,67,70]. Note that duty cycle ratios are lower in many important TF QKD experiments, for example, the duty ratio at 402 km is 22.4% in Ref. [61], 45% in Ref. [62], and 40% in Ref. [68]. The duty cycle has two effects on the key rate. Firstly, the total number of quantum pulses transmitted per second depends on the system clock frequency and the duty cycle. Secondly, the key rate per second is obtained by multiplying the key rate per pulse with the total number of quantum pulses transmitted per second. We can see that asynchronous MDI QKD enables the key rates of all links to exceed SKC_0. Additionally, asynchronous MDI QKD always enjoys higher secret-key rates per clock than SNS QKD (AOPP) and PM QKD.

D. Practical advantages of asynchronous MDI QKD

We simulate the performance of our protocol assuming a 4-GHz clock rate and 22-h transmission time. Figure 4 presents the key rate per second versus fiber distance for asynchronous MDI QKD, together with four-intensity time-bin MDI QKD [76], SNS QKD (AOPP) [83], PM QKD [84], four-phase TF QKD [68], and four-intensity decoy-state QKD. For SNS QKD (AOPP), PM QKD, and four-phase TF QKD, we set the duty cycle to 50%, Charlie's transmission loss at Alice's (Bob's) side to 2 dB, the angles of misalignment to 20°, which contributes to an interference error rate of approximately 3%. We assume an insert loss on Bob's side of 2 dB and a misalignment error rate of $e_m = 0.02$ for decoy-state QKD. The interference misalignment error rate of decoy-state MDI QKD is set to 0.04, which corresponds to 27% error rate in the **X** basis. Device parameters are shown in Table IV. The simulation formulas of MDI QKD and decoy-state QKD are detailed in Appendix D 2 and D 3, respectively. We also include SKC_0 to prove the repeaterlike behavior for asynchronous MDI QKD. Simulation shows that the key rate of our protocol surpasses that of the decoy-state QKD protocol when $l > 170$ km, and it exceeds SKC_0 when $l > 330$ km. In the 170–483 km range, the performance

TABLE III. Secret-key rates of the three-intensity asynchronous MDI QKD protocol with *click filtering*. Here the fiber loss is 0.16 dB/km; the clock rate is 4 GHz; the dark count rates is 0.1 Hz; and the detection efficiency is $\eta_d = 80\%$.

Data size	10^{12}	5×10^{12}	10^{13}	10^{13}	5×10^{13}	5×10^{13}
Distance (km)	50	100	150	200	250	300
Secret-key rate	6.02 Mbps	2.29 Mbps	855.40 kbps	305.05 kbps	129.60 kbps	46.671 kbps

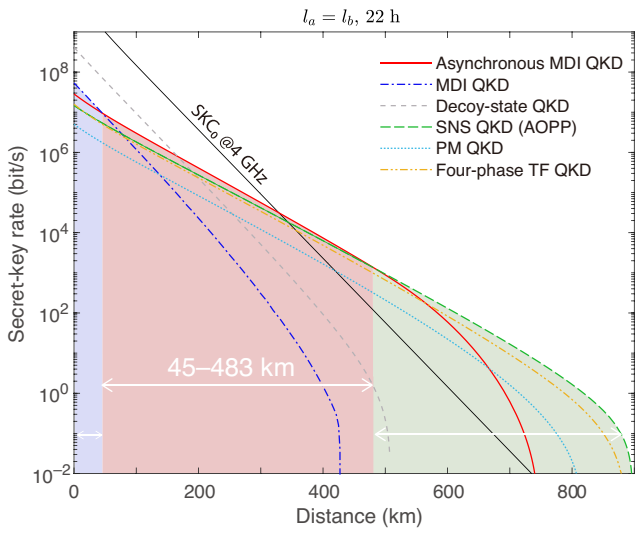

FIG. 4. Simulated secret-key rates for asynchronous MDI QKD, original time-bin MDI QKD, decoy-state QKD, SNS QKD with the AOPP method, PM QKD, and four-phase TF QKD under the state-of-the-art system. The horizontal axis represents the total transmission distance $l = l_a + l_b$.

of our protocol is better than that of the other five protocols, especially in the range of 200–300 km. We observe that, in the simulations, the key rates of decoy-state QKD surpass those of original time-bin MDI QKD due to the influence of the dark rate and finite key analysis. At short distances (less than 45 km), asynchronous MDI QKD has a slightly lower key rate compared to the original time-bin MDI QKD. This is attributed to the stronger light intensity of the signal state in the original MDI QKD, approaching 1, which results in a higher number of single-photon pairs in the **Z** basis. In Table III, we present the bits-per-second (bps) values of asynchronous MDI QKD at various typical distances, employing device parameters identical to those employed in Fig. 4. Our protocol can generate secret-keys rate of 0.31 Mbps at a fiber length of 200 km, thereby rendering it adequate for secure key-demanding applications such as real-time one-time-pad secure audio encryption in intra- and interurban areas.

V. DISCUSSION AND CONCLUSION

Here, we point out two conceptual differences between asynchronous MDI QKD and original MDI QKD.

i. In original MDI QKD, the total number of sent pluses allows for a direct measurement of the "gain", while the "yield" of single-photon pairs in the **Z** and **X** bases can be estimated using decoy-state methods [29]. However, in asynchronous MDI QKD, where postmeasurement coincidence pairing is utilized, there is no concept of the total sent pair number. Therefore, the terms "gain" and "yield" are not applicable.

ii. In asynchronous MDI QKD, the terms "three-intensity" and "four-intensity" refer to the number of light intensities used, and the intensities at different bases after pairing are associated. Specifically, in three-intensity asynchronous MDI QKD, there are two intensities in each of the **Z** and **X** bases after coincidence pairing. These intensities are associated as follows: in the **Z** basis, the intensities are μ and ν, while in the **X** basis, the intensities are 2μ and 2ν, and the nonbasis intensity is 0. In contrast, in the original three-intensity MDI QKD, there is only one intensity in the **Z** basis.

In the original MDI QKD protocol, a useful idea is to consider the double-scanning method [76]. We apply the double-scanning method to asynchronous MDI QKD. The derivation details of double scanning are shown in Appendix B. However, numerical results show that the method does not work for the three-intensity asynchronous MDI QKD protocol [85]. We remark that this phenomenon may be caused by the above two characteristics. In asynchronous MDI QKD, the number of single-photon pairs in the **Z** basis can be accurately estimated using **Z**-basis data, without the need for inefficient **X**-basis data. Additionally, there is a correlation between the intensities used to estimate the number of the **Z**-basis single-photon pairs and the intensities used to estimate the **X**-basis phase-error rate in asynchronous MDI QKD. In contrast, the intensity and decoy-state estimation in the **Z** and **X** bases are independent in original MDI QKD, which makes double scanning an effective strategy.

Furthermore, in the original MDI QKD protocol, we can improve the performance of the protocol by increasing the number of decoy states, such as four-intensity MDI QKD [31]. We also calculate the key rate of the four-intensity asynchronous MDI QKD protocol, in which the intensity of each laser pulse is randomly set to one of the four intensities $\mu_{a(b)}$ (signal), $\omega_{a(b)}$ (decoy 1), $\nu_{a(b)}$ (decoy 2) and $o_{a(b)}$ (vacuum), and the intensities satisfy $\mu_{a(b)} > \omega_{a(b)} > \nu_{a(b)} > o_{a(b)} = 0$. The detailed calculation of the protocol is presented in Appendix C. Comparing secret-key rates of the three-intensity and four-intensity asynchronous MDI QKD protocol with *click filtering*, we find that the optimal key rates for the four-intensity decoy-state method are nearly equal to the results for the three-intensity decoy-state method [85]. We remark that this situation is also due to the correlation between intensities at different bases. Therefore, the three-intensity asynchronous MDI QKD protocol is a good trade-off between the performance of key rates and the ease of implementation.

In this work, we present an analysis of the practical aspects of asynchronous MDI QKD. We provide refined decoy-state methods that enable higher-rate asynchronous MDI QKD. The numerical results of different asynchronous MDI QKD protocols demonstrate that the three-intensity protocol, with a *click-filtering* operation, can

provide a favorable balance between performance and ease of implementation. We introduce the decoy-state method for the asymmetric situation, which permits the direct application of our protocol to asynchronous MDI QKD experiments with asymmetric channels. Our work also provides useful insights into asynchronous MDI QKD: the decoy-state analysis for the **Z** and **X** bases of asynchronous MDI QKD are correlated, rendering the introduction of double scanning and additional decoy states ineffective for key-rate improvement. With its superior performance and straightforward design, asynchronous MDI QKD holds strong potential in future quantum networks spanning 200 to 400 km. We anticipate the application of the asynchronous concept to MDI multiparty quantum communication tasks, such as quantum conference key agreement [86], quantum secret sharing [86], and quantum digital signatures [87].

ACKNOWLEDGMENTS

The authors acknowledge Z. Yuan and L. Zhou for the insightful discussions. This work is supported by the National Natural Science Foundation of China (No. 12274223), the Natural Science Foundation of Jiangsu Province (No. BK20211145), the Fundamental Research Funds for the Central Universities (No. 020414380182), the Key Research and Development Program of Nanjing Jiangbei New Area (No. ZDYD20210101), the Program for Innovative Talents and Entrepreneurs in Jiangsu (No. JSSCRC2021484), and the Program of Song Shan Laboratory (Included in the management of Major Science and Technology Program of Henan Province) (No. 221100210800-02).

APPENDIX A: ANALYTIC RESULTS OF JOINT CONSTRAINTS

Here, we introduce the joint-constraints method to bound tighter values. Without loss of generality, we take Eq. (6) as an example. Similar operations can be applied to other parameters. We can rewrite Eq. (6) as

$$\underline{s}_{11}^{z*} \geq \frac{\sum_{\tilde{k}_a,\tilde{k}_b}\left(\tilde{k}_a\tilde{k}_b e^{-\tilde{k}_a-\tilde{k}_b}p_{[\tilde{k}_a,\tilde{k}_b]}\right)}{\nu_a\nu_b\mu_a\mu_b(\mu'-\nu')}\left(\underline{S}_1^*-\overline{S}_2^*\right), \tag{A1}$$

where

$$S_1 = \mu_a\mu_b\mu' e^{\nu_a+\nu_b}\frac{n_{[\nu_a,\nu_b]}}{p_{[\nu_a,\nu_b]}} + \nu_a\nu_b\nu' e^{\mu_b}\frac{n_{[o_a,\mu_b]}}{p_{[o_a,\mu_b]}} + \nu_a\nu_b\nu' e^{\mu_a}\frac{n_{[\mu_a,o_b]}}{p_{[\mu_a,o_b]}} + (\mu_a\mu_b\mu' - \nu_a\nu_b\nu')\frac{n_{[o_a,o_b]}}{p_{[o_a,o_b]}}, \tag{A2}$$

and

$$S_2 = \nu_a\nu_b\nu' e^{\mu_a+\mu_b}\frac{n_{[\mu_a,\mu_b]}}{p_{[\mu_a,\mu_b]}} + \mu_a\mu_b\mu' e^{\nu_b}\frac{n^*_{[o_a,\nu_b]}}{p_{[o_a,\nu_b]}} + \mu_a\mu_b\mu' e^{\nu_a}\frac{n_{[\nu_a,o_b]}}{p_{[\nu_a,o_b]}}. \tag{A3}$$

For $\underline{S}_1^*$, we define

$$S_1 := a_1\gamma_1 + a_2\gamma_2 + a_3\gamma_3 + a_4\gamma_4, \tag{A4}$$

where $a_1 = \mu_a\mu_b\mu' e^{\nu_a+\nu_b}/p_{[\nu_a,\nu_b]}$, $\gamma_1 = n_{[\nu_a,\nu_b]}$, $a_2 = \nu_a\nu_b\nu' e^{\mu_b}/p_{[o_a,\mu_b]}$, $\gamma_2 = n_{[o_a,\mu_b]}$, $a_3 = \nu_a\nu_b\nu' e^{\mu_a}/p_{[\mu_a,o_b]}$, $\gamma_3 = n_{[\mu_a,o_b]}$, $a_4 = \mu_a\mu_b\mu' - \nu_a\nu_b\nu'/p_{[o_a,o_b]}$, $\gamma_4 = n_{[o_a,o_b]}$. Denoting $\{b_1,b_2,b_3,b_4\}$ as the ascending order of $\{a_1,a_2,a_3,a_4\}$, and ξ_1, ξ_2, ξ_3, ξ_4 as the corresponding rearrange of $\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$ according to the ascending order of $\{a_1,a_2,a_3,a_4\}$, then we have the lower bound of S_1^* [76]:

$$\underline{S}_1^* := b_1\underline{(\xi_1+\xi_2+\xi_3+\xi_4)}^* + (b_2-b_1)\underline{(\xi_2+\xi_3+\xi_4)}^* + (b_3-b_2)\underline{(\xi_3+\xi_4)}^* + (b_4-b_3)\underline{\xi}_4^*. \tag{A5}$$

For $\overline{S}_2^*$, we define

$$S_2 := c_1\kappa_1 + c_2\kappa_2 + c_3\kappa_3 + c_4\kappa_4, \tag{A6}$$

where $a_1 = \mu_a\mu_b\mu' e^{\nu_a+\nu_b}/p_{[\nu_a,\nu_b]}$, $\gamma_1 = n_{[\nu_a,\nu_b]}$, $a_2 = \nu_a\nu_b\nu' e^{\mu_b}/p_{[o_a,\mu_b]}$, $\gamma_2 = n_{[o_a,\mu_b]}$, $a_3 = \nu_a\nu_b\nu' e^{\mu_a}/p_{[\mu_a,o_b]}$, $\gamma_3 = n_{[\mu_a,o_b]}$, $a_4 = (\mu_a\mu_b\mu' - \nu_a\nu_b\nu')/p_{[o_a,o_b]}$, $\gamma_4 = n_{[o_a,o_b]}$. Denoting $\{d_1,d_2,d_3\}$ as the ascending order of $\{c_1,c_2,c_3\}$, and χ_2, χ_3, as the corresponding rearrange of $\{\kappa_1,\kappa_2,\kappa_3\}$ according to the ascending order of $\{c_1,c_2,c_3\}$, then we have the upper bound of S_2^* [76]:

$$\overline{S}_2^* := d_1\times\overline{(\chi_1+\chi_2+\chi_3)}^* + (d_2-d_1)\times\overline{(\chi_2+\chi_3)}^* + (d_3-d_2)\times\overline{\chi}_3^*. \tag{A7}$$

APPENDIX B: DECOY-STATE ESTIMATION WITH THE DOUBLE-SCANNING METHOD

Here we apply the double-scanning method to asynchronous MDI QKD. Using the decoy-state method, we can estimate the lower bound of the number of single-photon pairs in the **X** basis

$$\underline{s}_{11}^{x*} = \frac{e^{-2\nu_a-2\nu_b}p_{[2\nu_a,2\nu_b]}}{\mu_a\mu_b(\tilde{\mu}'-\tilde{\nu}')}(\underline{S}^{+*} - \overline{S}^{-*} - \overline{H}^*), \tag{B1}$$

where

$$\begin{cases}\tilde{\mu}' = 2\mu_a,\ \tilde{\nu}' = 2\nu_a, & \text{if } \frac{\mu_a}{\mu_b} \leq \frac{\nu_a}{\nu_b},\\ \tilde{\mu}' = 2\mu_b,\ \tilde{\nu}' = 2\nu_b, & \text{if } \frac{\mu_a}{\mu_b} > \frac{\nu_a}{\nu_b},\end{cases} \tag{B2}$$

and

$$S^{+*} = \mu_a\mu_b\tilde{\mu}' e^{2\nu_a+2\nu_b}\frac{n^*_{[2\nu_a,2\nu_b]}}{p_{[2\nu_a,2\nu_b]}} + \nu_a\nu_b\tilde{\nu}' e^{2\mu_b}\frac{n^*_{[o_a,2\mu_b]}}{p_{[o_a,2\mu_b]}} + \nu_a\nu_b\tilde{\nu}' e^{2\mu_a}\frac{n^*_{[2\mu_a,o_b]}}{p_{[2\mu_a,o_b]}},$$
$$S^{-*} = \nu_a\nu_b\tilde{\nu}' e^{2\mu_a+2\mu_b}\frac{\overline{n}^*_{[2\mu_a,2\mu_b]}}{p_{[2\mu_a,2\mu_b]}} + \nu_a\nu_b\tilde{\nu}'\frac{n^*_{[o_a,o_b]}}{p_{[o_a,o_b]}},$$
$$H^* = \mu_a\mu_b\tilde{\mu}'\left(e^{2\nu_b}\frac{n^*_{[o_a,2\nu_b]}}{p_{[o_a,2\nu_b]}} + e^{2\nu_a}\frac{n^*_{[2\nu_a,o_b]}}{p_{[2\nu_a,o_b]}} - \frac{\overline{n}^*_{[o_a,o_b]}}{p_{[o_a,o_b]}}\right). \tag{B3}$$

The upper bound of the bit-error rate of single-photon pairs in the **X** basis e^{x*}_{11} satisfies

$$\overline{e}^{x*}_{11} = \frac{1}{\mu_a\mu_b\tilde{\mu}' e^{2\nu_a+2\nu_b}\underline{s}^{x*}_{11}}\left(\mu_a\mu_b\tilde{\mu}' e^{2\nu_a+2\nu_b}\frac{m^*_{[2\nu_a,2\nu_b]}}{p_{[2\nu_a,2\nu_b]}} - \frac{H}{2}\right). \tag{B4}$$

Denote $\tilde{n}_{[2\nu_a,2\nu_b]} = n_{[2\nu_a,2\nu_b]} - m_{[2\nu_a,2\nu_b]}$. We can divide the effective $[2\nu_a, 2\nu_b]$ coincidence into two kinds of events, the right effective events whose total number is $\tilde{n}_{[2\nu_a,2\nu_b]}$, and the wrong effective events whose total number is $m_{[2\nu_a,2\nu_b]}$. Denote $M = \mu_a\mu_b\tilde{\mu}' e^{2\nu_a+2\nu_b}\underline{m}^*_{[2\nu_a,2\nu_b]}/p_{[2\nu_a,2\nu_b]}$. We can rewrite Eq. (B1) as

$$\underline{s}^{x*}_{11} = \frac{e^{-2\nu_a-2\nu_b}p_{[2\nu_a,2\nu_b]}}{\mu_a\mu_b(\tilde{\mu}'-\tilde{\nu}')}(\underline{\tilde{S}}^{+*} - \overline{S}^{-*} + \underline{M}^* - \overline{H}^*), \tag{B5}$$

where

$$\tilde{S}^{+*} = \mu_a\mu_b\tilde{\mu}' e^{2\nu_a+2\nu_b}\frac{\tilde{n}^*_{[2\nu_a,2\nu_b]}}{p_{[2\nu_a,2\nu_b]}} + \nu_a\nu_b\tilde{\nu}' e^{2\mu_b}\frac{n^*_{[o_a,2\mu_b]}}{p_{[o_a,2\mu_b]}} + \nu_a\nu_b\tilde{\nu}' e^{2\mu_a}\frac{n^*_{[2\mu_a,o_b]}}{p_{[2\mu_a,o_b]}},$$
$$S^{-*} = \nu_a\nu_b\tilde{\nu}' e^{2\mu_a+2\mu_b}\frac{n^*_{[2\mu_a,2\mu_b]}}{p_{[2\mu_a,2\mu_b]}} + \nu_a\nu_b\tilde{\nu}'\frac{n^*_{[o_a,o_b]}}{p_{[o_a,o_b]}},$$
$$H^* = \mu_a\mu_b\tilde{\mu}'\left(e^{2\nu_b}\frac{n^*_{[o_a,2\nu_b]}}{p_{[o_a,2\nu_b]}} + e^{2\nu_a}\frac{n^*_{[2\nu_a,o_b]}}{p_{[2\nu_a,o_b]}} - \frac{n^*_{[o_a,o_b]}}{p_{[o_a,o_b]}}\right). \tag{B6}$$

For each group (H, M), we can calculate e^{x*}_{11} with Eqs. (B4) and (B5)

$$\overline{e}^{x*}_{11} = \frac{(\tilde{\mu}'-\tilde{\nu}')(M-H/2)}{\tilde{\mu}'(S^+ - S^- + M - H)}. \tag{B7}$$

By scanning (H, M) [76], we can get the worst case for e^{x*}_{11}, i.e.,

$$\max \quad e^{x*}_{11} \tag{B8}$$

$$\text{such that} \quad \underline{H} \le H \le \overline{H}, \quad \underline{M} \le M \le \overline{M}. \tag{B9}$$

With the formulas in Eqs. (2), (3), (5), (6), and (12), we can get the final key rate.

APPENDIX C: FOUR-INTENSITY ASYNCHRONOUS MDI QKD PROTOCOL

Here, we provide the decoy-state method for four-intensity asynchronous MDI QKD with *click filtering*. The core difference in the parameter estimation steps between the four-intensity protocol and the three-intensity protocol is to estimate the lower bound of the number of single-photon pairs in the **Z** basis. In the four-intensity protocol with *click filtering*, s^{z*}_{11} is bounded by

$$\underline{s}^{z*}_{11} = \frac{\sum_{\tilde{k}_a,\tilde{k}_b}\left(\tilde{k}_a\tilde{k}_b e^{-\tilde{k}_a-\tilde{k}_b}p_{[\tilde{k}_a,\tilde{k}_b]}\right)}{\nu_a\nu_b\omega_a\omega_b(\omega'-\nu')}\left[\omega_a\omega_b\omega'\left(e^{\nu_a+\nu_b}\frac{n^*_{[\nu_a,\nu_b]}}{p_{[\nu_a,\nu_b]}} - e^{\nu_b}\frac{\overline{n}^*_{[o_a,\nu_b]}}{p_{[o_a,\nu_b]}} - e^{\nu_a}\frac{\overline{n}^*_{[\nu_a,o_b]}}{p_{[\nu_a,o_b]}} + \frac{n^*_{[o_a,o_b]}}{p_{[o_a,o_b]}}\right) - \nu_a\nu_b\nu'\left(e^{\omega_a+\omega_b}\frac{\overline{n}^*_{[\omega_a,\omega_b]}}{p_{[\omega_a,\omega_b]}} - e^{\omega_b}\frac{n^*_{[o_a,\omega_b]}}{p_{[o_a,\omega_b]}} - e^{\omega_a}\frac{n^*_{[\omega_a,o_b]}}{p_{[\omega_a,o_b]}} + \frac{n^*_{[o_a,o_b]}}{p_{[o_a,o_b]}}\right)\right], \tag{C1}$$

where

$$\begin{cases}\omega' = \omega_a,\ \nu' = \nu_a & \text{if } \frac{\omega_a}{\omega_b} \le \frac{\nu_a}{\nu_b},\\ \omega' = \omega_b,\ \nu' = \nu_b & \text{if } \frac{\omega_a}{\omega_b} > \frac{\nu_a}{\nu_b},\end{cases} \tag{C2}$$

and $p_{[k^{\text{tot}}_a,k^{\text{tot}}_b]}$ is defined in Eq. (4). When *click filtering* is not applied, $p_s = 1$, otherwise $p_s = 1 - p_{\mu_a}p_{\omega_b} - p_{\mu_a}p_{\nu_b} - p_{\omega_a}p_{\mu_b} - p_{\omega_a}p_{\nu_b} - p_{\nu_a}p_{\mu_b} - p_{\nu_a}p_{\omega_b}$. Similarly, we use the technique of joint constraints to get the tight estimated value of s^{z*}_{11}. The calculation of the remaining parameter values can directly utilize Eqs. (2), (3), and (8)–(12).

TABLE IV. List of experimental parameters used in numerical simulations. The spectral filtering loss results from the use of dense-wavelength-division-multiplexing in dual-band TF-type QKD implementations [67,70], whereas asynchronous MDI QKD does not require the dual-band method. Additionally, the asynchronous MDI QKD system and the decoy-state QKD system do not require a reference pulse, allowing their duty cycle for quantum transmission to be 100%.

Fiber loss	Asynchronous MDI QKD 0.16 dB/km	Decoy-state QKD 0.16 dB/km	SNS QKD & PM QKD 0.16 dB/km	Four-phase TF QKD 0.16 dB/km
Charlie loss	...	2 dB	...	...
Detector efficiency	80%	80%	80%	80%
Dark count rate	0.1 Hz	0.1 Hz	0.1 Hz	0.1 Hz
Spectral filtering loss	0 dB	0 dB	2 dB at Alice-Charlie 2 dB at Bob-Charlie	2 dB at Alice-Charlie 2 dB at Bob-Charlie
Duty cycle	100	100	50	50
Laser frequency difference	10 Hz	...	...	...
Drift rates	5.9×10^3 rad/s	...	...	...
Number of phase slices	16	...	16	4

APPENDIX D: SIMULATION FORMULAS

The experimental parameters used for performance comparison of these protocols, asynchronous MDI QKD, decoy-state QKD, SNS QKD (AOPP), PM QKD, and four-phase TF QKD, are listed in Table IV.

1. Simulation formulas for asynchronous MDI QKD

In asynchronous MDI QKD, suppose Alice and Bob send intensities k_a and k_b with phase difference θ, the overall gain is given by [Eq. (C22) in Ref. [75]]

$$q_{(k_a|k_b)} = y^L_{(k_a|k_b)} I_0\left(\eta^L_d\sqrt{\eta_a k_a \eta_b k_b}\right) + y^R_{(k_a|k_b)} I_0\left(\eta^R_d\sqrt{\eta_a k_a \eta_b k_b}\right) - 2y^L_{(k_a|k_b)} y^R_{(k_a|k_b)} I_0\left[(\eta^L_d - \eta^R_d)\sqrt{\eta_a k_a \eta_b k_b}\right], \tag{D1}$$

where $y^{L(R)}_{(k_a|k_b)} = \left(1 - p^{L(R)}_d\right) e^{-[\eta^{L(R)}_d(\eta_a k_a + \eta_b k_b)/2]}$; η^L_d (η^R_d) and p^L_d (p^R_d) are the detection efficiency and the dark-count rate of the detector D_L (D_R), respectively; $\eta_a = 10^{-(\alpha l_a/10)}$ and $\eta_b = 10^{-(\alpha l_b/10)}$; $I_0(x)$ refers to the zero-order modified Bessel function of the first kind.

We define $N_{T_c} = FT_c$ as the number of time bins within time interval T_c. The total number of valid successful pairing results is [Eq. (C24) in Ref. [75]]

$$n_{\text{tot}} = \frac{Nq_{\text{tot}}}{1 + 1/q_{T_c}}, \tag{D2}$$

where q_{tot} is the probability of having a click event, and $q_{T_c} = 1 - (1 - q_{\text{tot}})^{N_{T_c}}$ is the probability that at least one click event occurs within the time interval T_c after a click time bin. When using the matching method without click filtering, $q_{\text{tot}} = \sum_{k_a,k_b} p_{k_a} p_{k_b} q_{(k_a|k_b)}$; when using the matching method with click filtering, $q_{\text{tot}} = \sum_{k_a,k_b} p_{k_a} p_{k_b} q_{(k_a|k_b)} - p_{\mu_a} p_{\nu_b} q_{(\mu_a|\nu_b)} - p_{\nu_a} p_{\mu_b} q_{(\nu_a|\mu_b)}$. The average of the pairing interval can be given by [Eq. (C25) in Ref. [75]]

$$T_{\text{mean}} = \frac{1 - N_{T_c} q_{\text{tot}}(1/q_{T_c} - 1)}{F q_{\text{tot}}}. \tag{D3}$$

The total number of set $\mathcal{S}_{[k^{\text{tot}}_a, k^{\text{tot}}_b]}$ (except set $\mathcal{S}_{[2\nu_a, 2\nu_b]}$) is [Eq. (C26) in Ref. [75]]

$$n_{[k^{\text{tot}}_a, k^{\text{tot}}_b]} = n_{\text{tot}} \sum_{k^e_a + k^l_a = k^{\text{tot}}_a} \sum_{k^e_b + k^l_b = k^{\text{tot}}_b} \times \left(\frac{p_{k^e_a} p_{k^e_b} q_{(k^e_a|k^e_b)}}{q_{\text{tot}}} \frac{p_{k^l_a} p_{k^l_b} q_{(k^l_a|k^l_b)}}{q_{\text{tot}}}\right). \tag{D4}$$

The total number of set $\mathcal{S}_{[2\nu_a, 2\nu_b]}$ is [Eq. (C27) in Ref. [75]]

$$n_{[2\nu_a, 2\nu_b]} = \frac{n_{\text{tot}}}{M\pi} \int_0^{2\pi} \left(\frac{p_{\nu_a} p_{\nu_b} q^{\theta}_{(\nu_a|\nu_b)}}{q_{\text{tot}}} \frac{p_{\nu_a} p_{\nu_b} q^{\theta}_{(\nu_a|\nu_b)}}{q_{\text{tot}}}\right) d\theta. \tag{D5}$$

The total number of errors in the **X** basis can be written as [Eq. (C28) in Ref. [75]]

$$m_{[2\nu_a,2\nu_b]}=\frac{n_{\mathrm{tot}}}{M\pi}p_{\nu_a}^2p_{\nu_b}^2\int_0^{2\pi}\left\{(1-E_{\mathrm{HOM}})\frac{\left[q^{\theta,L}_{(\nu_a|\nu_b)}q^{\theta+\delta,R}_{(\nu_a|\nu_b)}+q^{\theta,R}_{(\nu_a|\nu_b)}q^{\theta+\delta,L}_{(\nu_a|\nu_b)}\right]}{q_{\mathrm{tot}}^2}+E_{\mathrm{HOM}}\frac{\left[q^{\theta,L}_{(\nu_a|\nu_b)}q^{\theta+\delta,L}_{(\nu_a|\nu_b)}+q^{\theta,R}_{(\nu_a|\nu_b)}q^{\theta+\delta,R}_{(\nu_a|\nu_b)}\right]}{q_{\mathrm{tot}}^2}\right\}d\theta, \tag{D6}$$

where E_{HOM} is the interference misalignment error rate, and $\delta=T_{\mathrm{mean}}(2\pi\Delta\nu+\omega_{\mathrm{fib}})$ is the phase misalignment resulting from the fiber phase drift rate ω_{fib} and laser frequency difference $\Delta\nu$.

2. Simulation formulas for four-intensity MDI QKD

We denote the number and error number of detection event when Alice sends intensity k_a ($k_a\in\{\mu_a,\nu_a,\omega_a,o_a\}$), and Bob sends k_b ($k_b\in\{\mu_b,\nu_b,\omega_b,o_b\}$) in the $\mathbf{Z}(\mathbf{X})$ basis as $n^{z(x)}_{k_ak_b}$ and $m^{z(x)}_{k_ak_b}$, respectively. The key rate of time-bin MDI QKD is [29,76]

$$R=\frac{1}{N'}\left\{\underline{n}^z_0+\underline{n}^z_{11}\left[1-H_2\left(\overline{\phi}^z_{11}\right)\right]-\lambda_{\mathrm{EC}}-\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}-2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}}-2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\right\}, \tag{D7}$$

where $\lambda_{\mathrm{EC}}=n^z_{\mu_a\mu_b}fH_2\left(m^z_{\mu_a\mu_b}/n^z_{\mu_a\mu_b}\right)$.

Here we use the decoy-state analysis to consider the complete finite-key effects and apply the double-scanning method to MDI QKD [76]. The corresponding parameters in Eq. (D7) can be given by

$$\begin{aligned}
\underline{n}^{z*}_0&=\max\left\{\frac{e^{-\mu_a}p_{\mu_a}}{p_{o_a}}\underline{n}^{z*}_{o_a\mu_b},\frac{e^{-\mu_b}p_{\mu_b}}{p_{o_b}}\underline{n}^{z*}_{\mu_ao_b}\right\},\\
\underline{n}^{z*}_{11}&=\frac{\mu_a\mu_be^{-\mu_a-\mu_b}p_{\mu_a}p_{\mu_a}}{\nu_a\nu_b\omega_a\omega_b(\omega'-\nu')}\left(\underline{P}^{+*}-\overline{P}^{-*}+\underline{\hat{M}}^*-\overline{\hat{H}}^*\right),\\
\overline{t}^{x*}_{11}&=\frac{1}{\omega_a\omega_b\omega'e^{\nu_a+\nu_b}}\left(\hat{M}-\frac{\hat{H}}{2}\right),\\
\overline{t}^{z*}_{11}&=\frac{\mu_a\mu_be^{-\mu_a-\mu_b}p_{\mu_a}p_{\mu_a}}{\nu_a\nu_be^{-\nu_a-\nu_b}p_{\nu_a}p_{\nu_a}}\overline{t}^{x*}_{11},\\
\overline{\phi}^z_{11}&=\frac{\overline{t}^z_{11}}{\underline{n}^z_{11}},
\end{aligned} \tag{D8}$$

where

$$\begin{aligned}
\omega'=\omega_a,\ \nu'=\nu_a\quad&\text{if}\ \frac{\omega_a}{\omega_b}\le\frac{\nu_a}{\nu_b},\\
\omega'=\omega_b,\ \nu'=\nu_b\quad&\text{if}\ \frac{\omega_a}{\omega_b}>\frac{\nu_a}{\nu_b}
\end{aligned} \tag{D9}$$

and

$$\begin{aligned}
P^{+*}&=\omega_a\omega_b\omega'e^{\nu_a+\nu_b}\frac{(n^x_{\nu_a\nu_b}-m^x_{\nu_a\nu_b})^*}{p_{\nu_a}p_{\nu_b}}\\
&\quad+\nu_a\nu_b\nu'e^{\omega_a}\frac{n^{x*}_{\omega_ao_b}}{p_{\omega_a}p_{o_b}}+\nu_a\nu_b\nu'e^{\omega_b}\frac{n^{x*}_{o_a\omega_b}}{p_{o_a}p_{\omega_b}},\\
P^{-*}&=\nu_a\nu_b\nu'e^{\omega_a+\omega_b}\frac{n^{x*}_{\omega_a\omega_b}}{p_{\omega_a}p_{\omega_b}}+\nu_a\nu_b\nu'\frac{n^{x*}_{o_ao_b}}{p_{o_a}p_{o_b}},\\
\hat{M}^*&=\omega_a\omega_b\omega'e^{\nu_a+\nu_b}\frac{m^{x*}_{\nu_a\nu_b}}{p_{\nu_a}p_{\nu_b}},\\
\hat{H}^*&=\omega_a\omega_b\omega'\left(e^{\nu_b}\frac{n^{x*}_{o_a\nu_b}}{p_{o_a}p_{\nu_b}}+e^{\nu_a}\frac{n^{x*}_{\nu_ao_b}}{p_{\nu_a}p_{o_b}}-\frac{n^{x*}_{o_ao_b}}{p_{o_a}p_{o_b}}\right).
\end{aligned} \tag{D10}$$

By scanning $(\hat{H},\hat{M})$, we can obtain the secret-key rate

$$\min\quad R \tag{D11}$$

$$\text{such that}\quad \underline{\hat{H}}\le\hat{H}\le\overline{\hat{H}},\quad \underline{\hat{M}}\le\hat{M}\le\overline{\hat{M}}. \tag{D12}$$

Because of the dead time of the detector, only one of the four Bell states can be identified. In the simulation, we set

$$\begin{aligned}
n^z_{k_ak_b}&=N'p_{k_a}p_{k_b}p_d(1-p_d)^2e^{-[k_a\eta_a+k_b\eta_b)/2]}\left\{I_0(\sqrt{k_a\eta_ak_b\eta_b})-(1-p_d)e^{-[(k_a\eta_a+k_b\eta_b)/2]}\right.\\
&\quad\left.+\left[1-(1-p_d)e^{-(k_a\eta_a/2)}\right]\left[1-(1-p_d)e^{-(k_b\eta_b/2)}\right]\right\},\\
m^z_{k_ak_b}&=N'p_{k_a}p_{k_b}p_d(1-p_d)^2e^{-[(k_a\eta_a+k_b\eta_b)/2]}\left\{\left[I_0(\sqrt{k_a\eta_ak_b\eta_b})-(1-p_d)e^{-[(k_a\eta_a+k_b\eta_b)/2]}\right]\right\},
\end{aligned} \tag{D13}$$

and

$$n^x_{k_ak_b} = N' p_{k_a} p_{k_b} y^2_{k_ak_b} \left[1 + 2y^2_{k_ak_b} - 4y_{k_ak_b} I_0\left(\frac{\sqrt{k_a\eta_a k_b\eta_b}}{2}\right) + I_0(\sqrt{k_a\eta_a k_b\eta_b})\right],$$
$$m^x_{k_ak_b} = N' p_{k_a} p_{k_b} y^2_{k_ak_b} \left\{1 + y^2_{k_ak_b} - 2y_{k_ak_b} I_0\left(\frac{\sqrt{k_a\eta_a k_b\eta_b}}{2}\right) + E_{\mathrm{HOM}}\left[I_0(\sqrt{k_a\eta_a k_b\eta_b}) - 1\right]\right\}, \tag{D14}$$

where we have $y_{k_ak_b} = (1-p_d)e^{-[(k_a\eta_a + k_b\eta_b)/4]}$ and $E_{\mathrm{HOM}} = 0.04$. Note that in time-bin MDI QKD, two pulses form one bit, i.e., $N' = N/2$.

3. Simulation formulas for four-intensity decoy-state QKD

The key rate of decoy-state QKD is [82,88]

$$R = \frac{1}{N}\left\{\underline{n}^z_0 + \underline{n}^z_1\left[1 - H_2\left(\overline{\phi}^z_1\right)\right] - \lambda_{\mathrm{EC}} - 6\log_2\frac{23}{\varepsilon_{\mathrm{sec}}} - 2\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}\right\}, \tag{D15}$$

where $\lambda_{\mathrm{EC}} = (n^z_\mu + n^z_\nu) f H_2\left[(m^z_\mu + m^z_\nu)/(n^z_\mu + n^z_\nu)\right]$, and $n^{z(x)}_k$ and $m^{z(x)}_k$ are the number and error number of intensity pulse k ($k \in \{\mu, \nu, \omega, o\}$) measured in the $\mathbf{Z}(\mathbf{X})$ basis, respectively.

First, we extend the decoy-state analysis to finite-size cases. The number of vacuum events in the **Z** and **X** bases satisfy

$$\underline{n}^{z*}_0 = \frac{p_\mu e^{-\mu} + p_\nu e^{-\nu}}{p_o}\underline{n}^{z*}_o, \tag{D16}$$

and

$$\underline{n}^{x*}_0 = \frac{p_\omega e^{-\omega}}{p_o}\underline{n}^{x*}_o, \tag{D17}$$

respectively.

The number of single-photon events in the **Z** and **X** bases are

$$\underline{n}^{z*}_1 = \frac{(p_\mu\mu e^{-\mu} + p_\nu\nu e^{-\nu})\mu}{\mu\nu - \nu^2} \times\left(\frac{e^\nu \underline{n}^{z*}_\nu}{p_\nu} - \frac{\nu^2}{\mu^2}\frac{e^\mu \overline{n}^{z*}_\mu}{p_\mu} - \frac{\mu^2 - \nu^2}{\mu^2}\frac{\overline{n}^{z*}_o}{p_o}\right), \tag{D18}$$

and

$$\underline{n}^{x*}_1 = \frac{p_\omega\omega e^{-\omega}\mu}{\mu\nu - \nu^2}\left(\frac{e^\nu \underline{n}^{x*}_\nu}{p_\nu} - \frac{\nu^2}{\mu^2}\frac{e^\mu \overline{n}^{x*}_\mu}{p_\mu} - \frac{\mu^2 - \nu^2}{\mu^2}\frac{\overline{n}^{x*}_o}{p_o}\right), \tag{D19}$$

respectively. In addition, the number of bit errors $\overline{t}^x_1$ associated with the single-photon events in the **X** basis is also required. It is given by

$$\overline{t}^x_1 = m^x_\omega - \underline{m}^x_0, \tag{D20}$$

where $\underline{m}^{x*}_0 = (p_\omega e^{-\omega}/p_o)\underline{m}^{x*}_o$. Second, the formula for the phase-error rate of the single-photon events in the **Z** basis can be written as

$$\overline{\phi}^z_1 = \frac{\overline{m}^x_1}{\underline{n}^x_1} + \gamma\left(\underline{n}^z_1, \underline{n}^x_1, \frac{\overline{t}^x_1}{\underline{n}^x_1}, \varepsilon_e\right). \tag{D21}$$

In the simulation, we set

$$n^z_k = \frac{Np_k}{2}\left[1 - (1-p^z_d)^2 e^{-kq_z\eta^z}\right]\left[1 + (1-p^x_d)^2 e^{-kq_x\eta^x}\right],$$
$$m^z_k = \frac{Np_k}{2}\left[1 + (1-p^x_d)^2 e^{-kq_x\eta^x}\right] \times\left\{(e_0 - e^z_m)\left[1 - (1-p^z_d)^2\right]e^{-kq_z\eta^z} + e^z_m\left[1 - (1-p^z_d)^2 e^{-kq_z\eta^z}\right]\right\}, \tag{D22}$$

and

$$n^x_k = \frac{Np_k}{2}\left[1 - (1-p^x_d)^2 e^{-kq_x\eta^x}\right]\left[1 + (1-p^z_d)^2 e^{-kq_z\eta^z}\right],$$
$$m^x_k = \frac{Np_k}{2}\left[1 + (1-p^z_d)^2 e^{-kq_z\eta^z}\right] \times\left\{(e_0 - e^x_m)\left[1 - (1-p^x_d)^2\right]e^{-kq_x\eta^x} + e^x_m\left[1 - (1-p^x_d)^2 e^{-kq_x\eta^x}\right]\right\}, \tag{D23}$$

where $e_0 = 1/2$ is the error rate of the background noise, $e^z_m = e^x_m = e_m$, $p^z_d = p^x_d = p_d$, and $\eta^z = \eta^x = \eta_d 10^{-[(\alpha l + \eta_{\mathrm{int}})/10]}$. The code of decoy-state QKD and decoy-state MDI QKD has been uploaded to the open-source code website [85].

APPENDIX E: STATISTICAL FLUCTUATION ANALYSIS

In this Appendix, we introduce the statistical fluctuation analysis method [82] used in the simulation.

1. Chernoff bound

For a given expected value x^* and failure probability ε, we can use the Chernoff bound to estimate the upper and lower bounds of the observed value

$$\overline{x} = \varphi^U(x^*) = x^* + \frac{\beta}{2} + \sqrt{2\beta x^* + \frac{\beta^2}{4}}, \tag{E1}$$

and

$$\underline{x} = \varphi^L(x^*) = x^* - \sqrt{2\beta x^*}, \tag{E2}$$

where $\beta = \ln \epsilon^{-1}$.

2. Variant of Chernoff bound

The variant of the Chernoff bound can help us estimate the expected value from their observed values. One can apply the following equations to obtain the upper and lower bounds of x^*

$$\overline{x}^* = x + \beta + \sqrt{2\beta x + \beta^2} \tag{E3}$$

and

$$\underline{x}^* = \max\left\{x - \frac{\beta}{2} - \sqrt{2\beta x + \frac{\beta^2}{4}}, 0\right\}. \tag{E4}$$

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

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, and C. Ottaviani, *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[6] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, and S. El-Khoury, *et al.*, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, Nat. Photonics **17**, 422 (2023).

[7] C. Gobby, A. Yuan, and A. Shields, Quantum key distribution over 122 km of standard telecom fiber, Appl. Phys. Lett. **84**, 3762 (2004).

[8] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).

[9] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure Quantum Key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[10] M. Peev, *et al.*, The SECOQC quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[11] M. Sasaki, *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[12] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, and J. Cho, *et al.*, Cambridge quantum network, npj Quantum Inf. **5**, 101 (2019).

[13] Y.-A. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4600 kilometres, Nature **589**, 214 (2021).

[14] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[15] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[16] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Source attack of decoy-state quantum key distribution using phase information, Phys. Rev. A **88**, 022308 (2013).

[17] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[18] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[19] 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, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[20] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).

[21] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **112**, 190503 (2014).

[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, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[23] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).

[24] H.-L. Yin, W.-L. Wang, Y.-L. Tang, Q. Zhao, H. Liu, X.-X. Sun, W.-J. Zhang, H. Li, I. V. Puthoor, and L.-X. You, *et*

al., Experimental measurement-device-independent quantum digital signatures over a metropolitan network, Phys. Rev. A **95**, 042338 (2017).

[25] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. Paraïso, M. Lucamarini, Z. Yuan, and A. Shields, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Inf. **7**, 58 (2021).

[26] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Chip-based measurement-device-independent quantum key distribution, Optica **7**, 238 (2020).

[27] X. Zheng, P. Zhang, R. Ge, L. Lu, G. He, Q. Chen, F. Qu, L. Zhang, X. Cai, Y. Lu, S. Zhu, P. Wu, and X.-S. Ma, Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution, Adv. Photonics **3**, 055002 (2021).

[28] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics, Phys. Rev. X **10**, 031030 (2020).

[29] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[30] H.-L. Yin, W.-F. Cao, Y. Fu, Y.-L. Tang, Y. Liu, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent quantum key distribution with coherent-state superpositions, Opt. Lett. **39**, 5451 (2014).

[31] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A **93**, 042324 (2016).

[32] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, Optica **4**, 1016 (2017).

[33] W. Wang, F. Xu, and H.-K. Lo, Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks, Phys. Rev. X **9**, 041012 (2019).

[34] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, Quantum repeaters: From quantum networks to the quantum internet, Preprint ArXiv:2212.10820 (2022).

[35] C. Zhang, X.-L. Hu, C. Jiang, J.-P. Chen, Y. Liu, W. Zhang, Z.-W. Yu, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Side-Channel-Secure Quantum Key Distribution, Phys. Rev. Lett. **128**, 190503 (2022).

[36] J. Gu, X.-Y. Cao, Y. Fu, Z.-W. He, Z.-J. Yin, H.-L. Yin, and Z.-B. Chen, Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources, Sci. Bull. **67**, 2167 (2022).

[37] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and Reverse Secret-Key Capacities of a Quantum Channel, Phys. Rev. Lett. **102**, 050503 (2009).

[38] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[39] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[40] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal Limitations on Quantum Key Distribution Over a Network, Phys. Rev. X **11**, 041016 (2021).

[41] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Quantum repeater with encoding, Phys. Rev. A **79**, 032325 (2009).

[42] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Quantum communication without the necessity of quantum memories, Nat. Photonics **6**, 777 (2012).

[43] K. Azuma, K. Tamaki, and H.-K. Lo, All-photonic quantum repeaters, Nat. Commun. **6**, 6787 (2015).

[44] K. Azuma, K. Tamaki, and W. J. Munro, All-photonic intercity quantum key distribution, Nat. Commun. **6**, 10171 (2015).

[45] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[46] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[47] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[48] H.-L. Yin and Y. Fu, Measurement-device-independent twin-field quantum key distribution, Sci. Rep. **9**, 3045 (2019).

[49] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).

[50] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-Field Quantum Key Distribution Without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[51] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[52] K. Maeda, T. Sasaki, and M. Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, Nat. Commun. **10**, 3140 (2019).

[53] H.-L. Yin and Z.-B. Chen, Finite-key analysis for twin-field quantum key distribution with composable security, Sci. Rep. **9**, 17113 (2019).

[54] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses, Phys. Rev. Appl. **12**, 024061 (2019).

[55] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Inf. **7**, 22 (2021).

[56] B.-H. Li, Y.-M. Xie, Z. Li, C.-X. Weng, C.-L. Li, H.-L. Yin, and Z.-B. Chen, Long-distance twin-field quantum key distribution with entangled sources, Opt. Lett. **46**, 5529 (2021).

[57] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Experimental quantum

key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

[58] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution, Phys. Rev. Lett. **123**, 100506 (2019).

[59] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System, Phys. Rev. X **9**, 021046 (2019).

[60] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution Through Sending or Not Sending, Phys. Rev. Lett. **123**, 100505 (2019).

[61] X.-T. Fang, *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[62] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).

[63] H. Liu, *et al.*, Field Test of Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending Over 428 km, Phys. Rev. Lett. **126**, 250502 (2021).

[64] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses, npj Quantum Inf. **7**, 8 (2021).

[65] J.-P. Chen, C. Zhang, C. Liu, Yang Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, F. Liu, Hui Zhou, H.-F. Jiang, H. Chen, Teng-Yun Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photonics **15**, 570 (2021).

[66] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni, and D. Calonico, Coherent phase transfer for real-world twin-field quantum key distribution, Nat. Commun. **13**, 157 (2022).

[67] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photonics **15**, 530 (2021).

[68] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[69] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, and X.-B. Wang, *et al.*, Twin-field quantum key distribution without phase locking, Preprint ArXiv:2212.04311 (2022).

[70] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).

[71] Y.-M. Xie, B.-H. Li, Y.-S. Lu, X.-Y. Cao, W.-B. Liu, H.-L. Yin, and Z.-B. Chen, Overcoming the rate–distance limit of device-independent quantum key distribution, Opt. Lett. **46**, 1632 (2021).

[72] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference, PRX Quantum **3**, 020315 (2022).

[73] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).

[74] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, and Z. Wang, *et al.*, Experimental Mode-Pairing Measurement-Device-Independent Quantum Key Distribution Without Global Phase Locking, Phys. Rev. Lett. **130**, 030801 (2023).

[75] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, and Z. Yuan, Experimental quantum communication overcomes the rate-loss limit without global phase tracking, Preprint ArXiv:2212.14190 (2022).

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

[77] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[78] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[79] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[80] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[81] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[82] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Tight security bounds for decoy-state quantum key distribution, Sci. Rep. **10**, 14312 (2020).

[83] C. Jiang, X.-L. Hu, H. Xu, Z.-W. Yu, and X.-B. Wang, Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects, New J. Phys. **22**, 053048 (2020).

[84] P. Zeng, W. Wu, and X. Ma, Symmetry-Protected Privacy: Beating the Rate-Distance Linear Bound over a Noisy Channel, Phys. Rev. Appl. **13**, 064013 (2020).

[85] Y.-M. Xie, Comparison of secret key rates, https://github.com/yuan-meixie/key˙rate˙comparison.

[86] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-Distance Measurement-Device-Independent Multiparty Quantum Communication, Phys. Rev. Lett. **114**, 090501 (2015).

[87] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, Experimental quantum secure network with digital signatures and encryption, Natl. Sci. Rev. **10**, nwac228 (2023).

[88] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).