PHOTONICS Research

Measurement-device-independent quantum key distribution protocol with phase post-selection

Cong Jiang,[1,2] Xiao-Long Hu,[3] Zong-Wen Yu,[4] and Xiang-Bin Wang[1,2,5,6,7,*]

[1]Jinan Institute of Quantum Technology, Jinan 250101, China
[2]State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China
[3]School of Physics, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, China
[4]Data Communication Science and Technology Research Institute, Beijing 100191, China
[5]Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China
[6]Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China
[7]Frontier Science Center for Quantum Information, Beijing, China
*Corresponding author: xbwang@mail.tsinghua.edu.cn

Received 11 October 2021; revised 6 February 2022; accepted 19 February 2022; posted 22 February 2022 (Doc. ID 445617); published 30 June 2022

Measurement-device-independent quantum key distribution (MDI-QKD) protocol can remove all the loopholes of the detection devices and, thus, has attracted much attention. Based on the technique of single-photon interference, we propose a modified MDI-QKD protocol with phase post-selection. We prove the security of the announcement of the private phases in the X basis and show how to apply the phase post-selection method to the double-scanning four-intensity MDI-QKD protocol. The numerical results show that the phase post-selection method can significantly improve the key rates at all distances. In the double-scanning method, two parameters need to be scanned in the calculation of the final key rate, and the global parameter optimization is pretty time-consuming. We propose an accelerated method that can greatly reduce the running time of the global parameter optimization program. This makes the method practically useful in an unstable channel.

https://doi.org/10.1364/PRJ.445617

1. INTRODUCTION

Since the BB84 protocol was proposed in 1984 [1], quantum key distribution (QKD) has been studied for so many years in both theories and experiments [2–6]. The decoy-state BB84 protocol [7–9] was widely used in the experiments [10–14] and QKD networks [15–17] in which the decoy-state method can ensure the security of QKD with imperfect single-photon sources. Recently, an integrated space-to-ground quantum communication network over 4600 km was demonstrated by applying the decoy-state BB84 protocol [18]. But, in principle, the detectors in the BB84 protocol could be hacked by an eavesdropper due to the imperfections of the detectors [19,20]. Although there are some defense strategies against known attacks, we need a more robust method to protect the security with imperfect detectors.

Based on the virtual entanglement swapping, measurement-device-independent (MDI)-QKD protocol [21,22] can repair all the detection side vulnerabilities. The three-intensity MDI-QKD protocol [23–25] can ensure the security with both imperfect single-photon sources and detectors, but the key rate is pretty low. Many improved schemes were proposed to increase the key rate [26–29]. Among all those, the four-intensity MDI-QKD protocol [29] can improve the key rate by several orders of magnitude and becomes the mainstream of MDI-QKD protocol. The four-intensity MDI-QKD protocol has been applied to the experiments of long-distance MDI-QKD [30], free-space MDI-QKD [31], chip-based MDI-QKD [32–34], high-speed MDI-QKD [35], and so on [36,37]. Based on the four-intensity MDI-QKD protocol [29], we proposed a double-scanning method [38], which can further improve the key rate by up to 280% in typical experiment conditions. The double-scanning method [38] with four-intensity MDI-QKD protocol has been applied in a recent experiment [39].

Recently, based on single-photon interference, twin-field (TF)-QKD [40] was proposed. The TF-QKD can raise the key rate from the linear scale to square root scale of channel transmittance and break the PLOB bound [41], the key rate limit of repeaterless QKD. TF-QKD protocol and its variants [42–45] have been widely studied in theories [46–51] and experiments [52–57]. Specially, sending-or-not-sending (SNS) TF-QKD [42] has been realized in the 428 km field experiment

[58], the 511 km field experiment [59], and the 605 km laboratory experiment [60], which are the farthest field experiments and laboratory experiment to date.

One significant technique in TF QKD protocols is phase post-selection, which can reduce the phase-error or bit-error in the interference. In this paper, we propose a modified MDI-QKD protocol with phase post-selection to improve the key rate by reducing the estimated phase-error rate. The paper is arranged as follows. We first introduce the main idea of our modified protocol and prove its security. Then we show some numerical results to compare the modified protocol with other protocols. The paper is ended with concluding remarks.

2. PROTOCOL

Based on the decoy-state MDI-QKD protocol, we propose a modified protocol with phase post-selection. We assume Alice and Bob take the weak coherent state (WCS) sources to encode the quantum signals. The state of a WCS pulse with intensity μ and phase θ is denoted by

$$|e^{i\theta}\sqrt{\mu}\rangle = \sum_{m=0}^{\infty} \frac{e^{-\mu/2} e^{im\theta} \sqrt{\mu}^m}{\sqrt{m!}} |m\rangle, \tag{1}$$

where $|m\rangle$ is the m-photon state.

A. Main Idea

In the jth time window, Alice (Bob) sends out a strong reference pulse followed by a signal pulse in state $|e^{i(\theta_{aj}+\gamma_{aj})}\sqrt{\mu_a}\rangle(|e^{i(\theta_{bj}+\gamma_{bj})}\sqrt{\mu_b}\rangle)$ to the untrusted third-party Charlie, where γ_{aj} and γ_{bj} represent the public phase related to the strong reference pulse, and θ_{aj} and θ_{bj} represent the private phase. The public phases are known to everyone, and the private phases are randomly selected from $[0,2\pi)$. Some of the private phases are announced in the data post-processing, and the other private phases are never announced in the whole protocol.

For the received signal pulse pairs, Charlie is assumed to first compensate for the difference in public phases $\gamma_{aj} - \gamma_{bj}$ and then perform the Bell measurement. In this protocol, we will make post-selection for a set Q of signal pulse pairs in X basis. We make the post-selection according to the difference between the private phases of the pulse pair. The goal of this post-selection is to make the observed error rate in subset Q be small enough so as to make a better estimation for the phase-flip error rate of single-photon pairs in Z basis. For this goal, we need a small positive value λ in the following formula:

$$1 - |\cos(\theta_{aj} - \theta_{bj})| \le \lambda. \tag{2}$$

As we shall show later, such a post-selection can produce a smaller observed phase-flip error rate for the single-photon pairs if λ is small. Before going further, we first show the idea in more details by the example of the four-intensity protocol [29,38].

We shall post-select a subset of pulse pairs Q. By using results of all pulse pairs in X basis, we can evaluate the yield of the single-photon pairs, which can be used to obtain the yield of all single-photon pairs and also the yield of the single-photon pairs in set Q only. Then, to calculate the final key rate, we have two options. One is to ignore the subset Q and just calculate the key rate using the standard method of the four-intensity protocol. The other is to use the observed error rate in subset Q, then estimate the phase-flip error rate for single-photon pairs in Z basis, and finally calculate the final key rate by this. We will always choose the one that produces the higher key rate. A small λ results in a small observed error rate in subset Q, but the number of observed error events will also be small, which would cause large statistical fluctuations. Thus, there is a trade-off between the observed error rate and the number of observed error events, and we need to optimize λ to achieve the best estimation of the phase-flip error rate.

B. Implementation Process of the Protocol

We take the four-intensity MDI-QKD protocol with phase post-selection to show the whole implementation process.

There are four WCS sources o, x, y, z with different intensities at Alice's and Bob's sides, respectively. In X basis, Alice (Bob) uses WCS sources o_A, x_A, and y_A (o_B, x_B, and y_B) with intensities $\mu_{o_A} = 0$, μ_{x_A}, and μ_{y_A} ($\mu_{o_B} = 0$, μ_{x_B}, and μ_{y_B}), respectively. In Z basis, Alice (Bob) uses WCS source z_A (z_B) with intensity μ_{z_A} (μ_{z_B}). In the jth time window, Alice (Bob) randomly prepares a signal pulse in state $|e^{i(\theta_{aj}+\gamma_{aj})}\sqrt{\mu_{\alpha_A}}\rangle$ ($|e^{i(\theta_{bj}+\gamma_{bj})}\sqrt{\mu_{\beta_B}}\rangle$) with probability p_{α_A} (p_{β_B}) for $\alpha, \beta = o, x, y, z$, where θ_{aj} and θ_{bj} are randomly selected from $[0,2\pi)$. The signal pulse is encoded in X basis if $\alpha, \beta = o, x, y$ and in Z basis if $\alpha, \beta = z$. Then Alice (Bob) sends out the prepared signal pulse to Charlie. Charlie is assumed to first compensate for the difference in public phases, and then perform the Bell measurement to the received pulse pairs. Charlie announces the outcome to Alice and Bob. If two specific detectors click (for example, two and only two detectors corresponding to different polarizations click in the polarization coding scheme), Alice and Bob take it as an effective event, and Alice and Bob only keep the data of effective events.

To efficiently estimate the difference in public phases of the pulse pairs received in Charlie's detectors, the method performed in the TF-QKD experiments can be applied here [52–57]. Alice (Bob) encodes the strong reference pulses multiplexed with the signal pulses by modulating a continuous light into pulsed light. The signal pulses are quantum signals with random phases and single photon level intensities, while the strong reference pulses are classical signals with fixed phases and usually more than dozens to hundreds of times stronger than intensity of the signal pulses. Based on the recorded interference results of the strong reference pulses, Charlie can accurately estimate the relative difference in public phases of the received signal pulse pairs.

After Alice and Bob repeat the above process for N times and Charlie announces all the outcomes, they (Alice and Bob) acquire a series of data. Then, Alice and Bob first announce the intensity of the pulse corresponding to each effective event. For the effective events that both Alice and Bob take the x sources, they then announce the private phases θ_{aj} and θ_{bj}. The private phases of other effective events are never announced. We denote $\alpha\beta$ as the pulse pair source if Alice takes the α source and Bob takes the β source for $\alpha, \beta = o, x, y, z$. We use the following criteria for the effective events of the xx source to make post-selection for the subset Q:

$$1 - |\cos(\theta_{aj} - \theta_{bj})| \le \lambda. \tag{3}$$

With all those data, we can calculate the final key rate R. The calculation method is shown in Section 4.

3. SECURITY PROOF

Since only the private phases of the effective events of the xx source are revealed in this protocol, we only need to consider the security of those parts. For simplicity, we first consider the following virtual protocol.

For virtual protocol, to each pulse pair of the xx source, only Alice and Bob know the value $\delta_j = \theta_{aj} - \theta_{bj}$, but they do not know the phase values $\theta_{aj}, \theta_{bj}, \gamma_{aj}, \gamma_{bj}$. Here we choose the region $-\pi < \delta_j \leq \pi$ in our discussion. Therefore, the density operator of a signal pulse pair from any subset from whatever post-selection strategies that satisfy Eq. (3) can be written as

$$\rho = \frac{1}{4\pi}\int_0^{2\pi} \mathrm{d}\theta_{aj}[\Omega(\delta_i) + \Omega(\delta_i + \pi)], \tag{4}$$

where we have used the notation

$$\Omega(\delta_i) = \left|e^{i(\theta_{aj}+\gamma_{aj})}\sqrt{\mu_{x_A}}\right\rangle\left\langle e^{i(\theta_{aj}+\gamma_{aj})}\sqrt{\mu_{x_A}}\right| \otimes \left|e^{i(\theta_{aj}+\gamma_{bj}-\delta_i)}\sqrt{\mu_{x_B}}\right\rangle\left\langle e^{i(\theta_{aj}+\gamma_{bj}-\delta_i)}\sqrt{\mu_{x_B}}\right|. \tag{5}$$

Doing the integration in Eq. (4), we find that the density operator can be decomposed in the following convex form:

$$\rho = c_{11}|11\rangle\langle 11| + (1 - c_{11})\rho', \tag{6}$$

where $c_{11} = \mu_{ax}\mu_{bx}e^{-\mu_{ax}-\mu_{bx}}$ and $1 - c_{11}$ are positive values and ρ' is a density operator, which is $(\rho - c_{11}|11\rangle\langle 11|)/(-c_{11})$.

Hence, we have Lemma 1. For a pulse pair from any post-selected subset Q, it can be regarded as the classical mixture of a single-photon pair with probability c_{11} and another density operator with probability $1 - c_{11}$.

Obviously, even Alice and Bob know the values of θ_{aj} and θ_{bj}, but they never use the information of values of θ_{aj} and θ_{bj}; a pulse pair from subset Q can still be regarded as the classical mixture of a single-photon pair with probability c_{11} and another density operator with probability $1 - c_{11}$. We define Q_{11} as the set of single-photon pulse pairs from Q. Since in the distribution process no one can tell the difference between the pulse pairs from Q_{11} and the ideal single-photon pulse pairs in X basis, we have the following. (1) The yield of single-photon pulse pairs calculated from all effective events caused by pulse pairs in X basis is asymptotically equal to the yield of single-photon pulse pairs from set Q. (2) The bit-flip error rate of the effective events of single-photon pulse pairs from Q is asymptotically equal to the phase-flip error rate of all those effective events caused by single-photon pairs prepared in Z basis.

In the real protocol, Alice and Bob cannot know the values of each δ_j of the pulse pair from xx source before the private phases are announced. But if they announce the private phases through a secret channel that cannot be eavesdropped by anyone else, the above discussion still holds. In the following, we shall prove that the security of Alice and Bob's announcing the private phases through a private channel is equivalent to that of announcing the private phases through a public channel.

The private phases of the pulse pairs from Z basis are never announced; thus, those pulse pairs are the classical mixture of Fock states. To calculate the final key rate, we need to know the lower bound of the number of the effective events caused by single-photon pairs from Z basis $\underline{n_{11}}$ and the upper bound of its corresponding phase-flip error rate e^{ph}. Note the values of $\underline{n_{11}}$ and e^{ph} are objective facts, which do not change by any outside information when the quantum distribution process of the protocol is done and Charlie has announced all detection outcomes. This is to say, after Alice and Bob know this fact, they can announce the private phases of all pulse pairs from xx source, and this does not affect the security of the protocol. We suppose Alice and Bob get the values of $\underline{n_{11}}$ and e^{ph} through a secret channel, and get the lower bound of the number of the effective events caused by single photon pairs from Z basis $\underline{n_{11}}'$ and the upper bound of its corresponding phase-flip error rate $e^{\mathrm{ph}}{}'$ through a public channel. Since all observed values are the same in the case of secret channel and public channel, we have $\underline{n_{11}} = \underline{n_{11}}'$ and $e^{\mathrm{ph}} = e^{\mathrm{ph}}{}'$. This ends the proof.

4. KEY RATE FORMULA

The phase post-selection method can be combined with both the single-scanning method [29] and the double-scanning method [38] of the four-intensity MDI-QKD protocol. Here we take the phase post-selection method combined with the double-scanning method as an example to show the calculation method of the final key rate. The method can be easily generalized to the case of combining with the single-scanning method.

As discussed in Section 3, the phase post-selection does not affect the security; thus, the density matrix of the pulse pairs from source xx can still be regarded as the classical mixture of Fock states. We denote the density matrix of source $\alpha\beta = oo, ox, xo, oy, yo, xy, yx, xx, yy, zz$ by

$$\rho_{\alpha\beta} = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a_m^{\alpha} b_n^{\beta} |mn\rangle\langle mn|, \tag{7}$$

where

$$a_m^{\alpha} = \frac{\mu_{\alpha_A}^m e^{-\mu_{\alpha_A}}}{m!}, \quad b_n^{\beta} = \frac{\mu_{\beta_B}^n e^{-\mu_{\beta_B}}}{n!}, \tag{8}$$

and we denote the total number of instances of source $\alpha\beta = oo, ox, xo, oy, yo, xy, yx, xx, yy, zz$ by $N_{\alpha\beta}$ with

$$N_{\alpha\beta} = p_{\alpha_A} p_{\beta_B} N. \tag{9}$$

According to the data in X basis, Alice and Bob get the observed value of the number of effective events of source $\alpha\beta$, $n_{\alpha\beta}$. We denote the expected value of $n_{\alpha\beta}$ by $\langle n_{\alpha\beta}\rangle$. With Chernoff bound [61], we can estimate the expected value according to the observed value. We denote the estimated lower and upper bounds of the expected value by the superscripts L and U, respectively. Besides, we denote the number of wrong effective events of source xx as m_{xx} whose corresponding expected value is $\langle m_{xx}\rangle$.

With Eqs. (4)–(6), we can get the density matrix of the pulse pairs from set Q,

$$\rho_Q = c_{11}|11\rangle\langle 11| + (1 - c_{11})\rho', \tag{10}$$

where $c_{11} = \mu_{ax}\mu_{bx}e^{-\mu_{ax}-\mu_{bx}} = a_1^x b_1^x$ and $1 - c_{11}$ are positive values and ρ' is a density operator, which is $(\rho - c_{11}|11\rangle\langle 11|)/(1-c_{11})$. The criteria of the correct effective event and the

wrong effective event of the pulse pair in the set Q are the same as those of the source xx. We denote the observed number of wrong effective events in set Q by m_Q and its corresponding expected value by $\langle m_Q\rangle$.

As shown in Ref. [38], if $\frac{\mu_{y_B}}{\mu_{x_B}} \le \frac{\mu_{y_A}}{\mu_{x_A}}$, the lower bound of the expected value of the yield of the single-photon pulse pairs is

$$\langle s_{11}\rangle^L = \frac{\langle S_+\rangle^L + \frac{a_1^y b_2^y}{N_{xx}}\mathcal{M} - \langle S_-\rangle^U - a_1^y b_2^y \mathcal{H}}{a_1^x a_1^y (b_1^x b_2^y - b_2^x b_1^y)}, \tag{11}$$

where

$$\langle S_+\rangle = \frac{a_1^y b_2^y}{N_{xx}}\langle \tilde{m}_{xx}\rangle + \frac{a_1^x b_2^x a_0^y}{N_{oy}}\langle n_{oy}\rangle + \frac{a_1^x b_2^x b_0^y}{N_{yo}}\langle n_{yo}\rangle, \tag{12}$$

$$\langle S_-\rangle = \frac{a_1^x b_2^x}{N_{yy}}\langle n_{yy}\rangle + \frac{a_1^x b_2^x a_0^y b_0^y}{N_{oo}}\langle n_{oo}\rangle, \tag{13}$$

$$\mathcal{H} = \frac{a_0^x}{N_{ox}}\langle n_{ox}\rangle + \frac{b_0^x}{N_{xo}}\langle n_{xo}\rangle - \frac{a_0^x b_0^x}{N_{oo}}\langle n_{oo}\rangle, \tag{14}$$

$\langle \tilde{m}_{xx}\rangle = \langle n_{xx}\rangle - \langle m_{xx}\rangle$, and $\mathcal{M} = \langle m_{xx}\rangle$. Applying the joint constraint method [28,38], we can get the lower bound of $\langle S_+\rangle$, $\langle S_+\rangle^L$, the upper bound of $\langle S_-\rangle$, $\langle S_-\rangle^U$, and the lower and upper bounds of $\mathcal{H}$, $\mathcal{H}^L$, and $\mathcal{H}^U$. Applying the Chernoff bound, we can get the lower and upper bounds of $\mathcal{M}$, $\mathcal{M}^L$, and $\mathcal{M}^U$. For the case $\frac{\mu_{y_B}}{\mu_{x_B}} > \frac{\mu_{y_A}}{\mu_{x_A}}$, we can get similar formulas.

The upper bound of the expected value of the phase-flip error rate of the single-photon pairs from Z basis is

$$\langle e_{11}\rangle^U = \frac{\mathcal{M}/N_{xx} - \mathcal{H}/2}{a_1^x b_1^x \langle s_{11}\rangle^L}. \tag{15}$$

As discussed in Section 3, we can use the observed value in set Q to get $\langle e_{11}\rangle^U$. Let $\Delta \in [0,\pi]$ satisfy

$$\cos\frac{\Delta}{2} = 1 - \lambda, \tag{16}$$

where λ is defined in Eq. (2). With Eq. (10), it is easy to check that

$$\langle e_{11}\rangle'^U = \frac{\frac{\langle m_Q\rangle}{\Delta/\pi N_{xx}}}{a_1^x b_1^x \langle s_{11}\rangle^L}. \tag{17}$$

Since both Eqs. (15) and (17) are the upper bounds of the expected value of the phase-flip error rate, we can always use the smaller one to be the estimated upper bound. This is to say, for each group $(\mathcal{H},\mathcal{M})$, we apply Eq. (11) to calculate $\langle s_{11}\rangle^L$, and we have

$$\langle e_{11}^{\mathrm{ph}}\rangle^U = \min\left(\frac{\mathcal{M}/N_{xx} - \mathcal{H}/2}{a_1^x b_1^x \langle s_{11}\rangle^L}, \frac{\frac{\langle m_Q\rangle}{\Delta/\pi N_{xx}}}{a_1^x b_1^x \langle s_{11}\rangle^L}\right). \tag{18}$$

With the Chernoff bound, we can get the real value of the lower bound of the yield of the single-photon pulse pairs from source zz, $s_{11,Z}^L$, and its corresponding upper bound of the phase-flip error rate, $e_{11}^{\mathrm{ph},U}$,

$$s_{11,Z}^L = \frac{O^L(N_{zz}a_1^z b_1^z \langle s_{11}\rangle^L)}{N_{zz}a_1^z b_1^z}, \tag{19}$$

$$e_{11}^{\mathrm{ph},U} = \frac{O^U(N_{zz}a_1^z b_1^z s_{11,Z}^L \langle e_{11}^{\mathrm{ph}}\rangle^U)}{N_{zz}a_1^z b_1^z s_{11,Z}^L}, \tag{20}$$

where $O^U(Y)$ and $O^L(Y)$ are defined in Eqs. (A5) and (A6).

Then we have

$$R(\mathcal{H},\mathcal{M}) = p_{z_A}p_{z_B}\{a_1^z b_1^z s_{11,Z}^L[1 - h(e_{11}^{\mathrm{ph},U})] - f S_{zz} h(E_{zz})\} - \frac{1}{N}\left(\log_2\frac{8}{\varepsilon_{\mathrm{cor}}} + 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} + 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\right), \tag{21}$$

where $S_{zz} = n_{zz}/N_{zz}$ is the yield of the pulse pairs from source zz; E_{zz} is the bit-flip error rate of the effective event in source zz; $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon entropy; $\varepsilon_{\mathrm{cor}}$ is the failure probability of error correction; $\varepsilon_{\mathrm{PA}}$ is the failure probability of privacy amplification; and ε' and $\hat{\varepsilon}$ are the coefficients while using the chain rules of smooth min- and max-entropy. Finally, by scanning $(\mathcal{H},\mathcal{M})$, we can get the final key rate,

$$R = \min_{\substack{\mathcal{H}\in[\mathcal{H}^L,\mathcal{H}^U],\\ \mathcal{M}\in[\mathcal{M}^L,\mathcal{M}^U]}} R(\mathcal{H},\mathcal{M}). \tag{22}$$

5. NUMERICAL SIMULATION

We shall show the advantage of phase post-selection through the numerical simulation results. Similar to prior art works, we take linear model for channel transmittance [21,62] for the provably observed values of $n_{\alpha\beta}$ and $m_{\alpha\beta}$ in our simulation. The simulation method of m_Q is shown in Appendix B. The experiment parameters are listed in Table 1. In the optimization of the phase post-selection combined with the double-scanning method, except for the source parameters, λ is also a parameter to be optimized.

In the global parameter optimization process, if we directly scan $(\mathcal{H},\mathcal{M})$ in their range to calculate the key rate, it would be pretty time-consuming. We propose an accelerated method that can reduce the running time of the optimized program from several days to less than half an hour.

The accelerated method can reduce the scanning parameters from two to one. To clearly show this, we denote $T_Q = \frac{\langle m_Q\rangle}{\Delta/\pi N_{xx}}$, $T^L = \mathcal{M}^L/N_{xx} - \mathcal{H}^U/2$, $T^U = \mathcal{M}^U/N_{xx} - \mathcal{H}^L/2$, and $t_{11} = \mathcal{M}/N_{xx} - \mathcal{H}/2$.

If $T_Q \le T^L$, then no matter what values $(\mathcal{H},\mathcal{M})$ take, the worst case of the key rate must be achieved when $\mathcal{H} = \mathcal{H}^U$, $\mathcal{M} = \mathcal{M}^L$.

If $T_Q > T^L$, then for each certain $t_{11} \in [T^L, T^{U\prime}]$, where $T^{U\prime} = \min(T_Q, T^U)$, the worst case of the key rate is achieved when $\langle s_{11}\rangle^L$ is the smallest. With the simplest linear programming method, we can easily know that when $\mathcal{H} = H(t_{11})$, $\langle s_{11}\rangle^L$ is the smallest, and

Table 1. List of Experimental Parameters Used in Numerical Simulations[a]

p_d	e_d	η_d	f	α_f	ξ	N
1.0×10^{-7}	1.5%	40.0%	1.1	0.2	1.0×10^{-10}	1.0×10^{10}

[a]Here p_d is the dark counting rate per pulse of Charlie's detectors; e_d is the misalignment-error probability; η_d is the detection efficiency of Charlie's detectors; f is the error correction inefficiency; α_f is the fiber loss coefficient (dB/km); ξ is the failure probability while using Chernoff bound; N is the number of total pulse pairs sent out in the protocol.

$$H(t_{11}) = \begin{cases} \mathcal{H}^U, & t_{11} + \mathcal{H}^U/2 \le \mathcal{M}^U/N_{xx}, \\ 2(\mathcal{M}^U/N_{xx} - t_{11}), & t_{11} + \mathcal{H}^U/2 > \mathcal{M}^U/N_{xx}. \end{cases} \tag{23}$$

Then for each certain $t_{11} \in [T^L, T^{U\prime}]$, we have

$$\langle s_{11}\rangle^L = \frac{\langle S_+\rangle^L + a_1^y b_2^y [t_{11} - H(t_{11})/2] - \langle S_-\rangle^U}{a_1^x a_1^y (b_1^x b_2^y - b_2^x b_1^y)}, \tag{24}$$

$$\langle e_{11}^{\mathrm{ph}}\rangle^U = \frac{t_{11}}{a_1^x b_1^x \langle s_{11}\rangle^L}. \tag{25}$$

When we substitute $\langle s_{11}\rangle^L$ and $\langle e_{11}^{\mathrm{ph}}\rangle^U$ into Eqs. (19)–(21), we can get $R(t_{11})$. Finally, by scanning t_{11} in $[T^L, T^{U\prime}]$, we can get the final key rate, which is

$$R = \min_{t_{11}\in[T^L, T^{U\prime}]} R(t_{11}). \tag{26}$$

If $T_Q \ge T^U$, the above method is obviously correct. But for the case $T^L < T_Q < T^U$, we need to prove that the worst case of the key rate cannot be achieved in the range $(T^Q, T^U]$.

We denote $T^Q \le t_{11}^w < t_{11}^v \le T^U$. It is easy to check $H(t_{11}^w) \ge H(t_{11}^v)$; thus, we have $\langle s_{11}\rangle^L(t_{11}^w) < \langle s_{11}\rangle^L(t_{11}^v)$. With Eq. (18), we have

$$\begin{aligned} \langle e_{11}^{\mathrm{ph}}\rangle^U(t_{11}^w) &= \frac{T^Q}{a_1^x b_1^x \langle s_{11}\rangle^L(t_{11}^w)} > \langle e_{11}^{\mathrm{ph}}\rangle^U(t_{11}^v) \\ &= \frac{T^Q}{a_1^x b_1^x \langle s_{11}\rangle^L(t_{11}^v)}. \end{aligned} \tag{27}$$

Thus, we have $R(t_{11}^w) < R(t_{11}^v)$, which means the worst case of the key rate cannot be achieved in the range $(T^Q, T^U]$. This ends the proof.

Figures 1 and 2 are the comparison of the key rates with this work and the former methods [29,38] under the symmetric channel. The symmetric channel means the distance between Alice and Charlie L_{AC} is the same as that distance between Bob and Charlie L_{BC}. We also assume the source parameters of Alice and Bob are the same, which means $p_{\alpha_A} = p_{\alpha_B}$ and $\mu_{\alpha_A} = \mu_{\alpha_B}$.

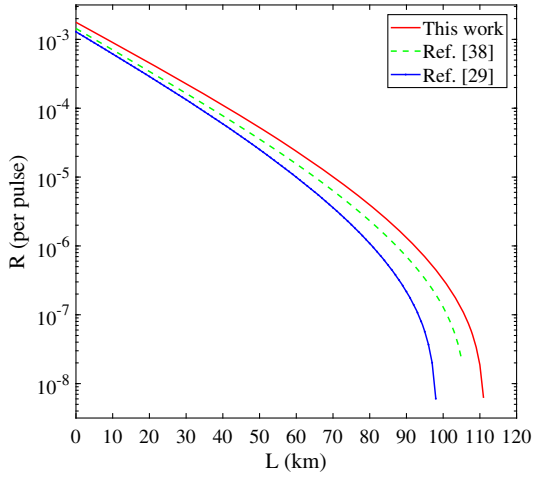

Fig. 1. Comparison of the key rates with this work and the former methods under the symmetric channel. The line of Ref. [38] is the key rates of the double-scanning four-intensity MDI-QKD protocol, and the line of Ref. [29] is the key rates of the original four-intensity MDI-QKD protocol. The experiment parameters are listed in Table 1.

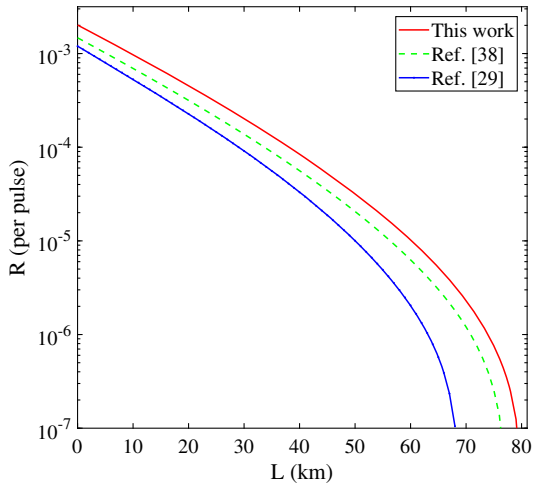

Fig. 2. Comparison of the key rates with this work and the former methods under the symmetric channels. The experiment parameters here are similar to those in Fig. 1 except that we set $N = 10^9$ and the misalignment-error probability $e_d = 0.005$.

The line of Ref. [38] is the key rates of the double-scanning four-intensity MDI-QKD protocol, and the line of Ref. [29] is the key rates of the original four-intensity MDI-QKD protocol. In Fig. 1, the experiment parameters are listed in Table 1. The numerical results show that the method of this work can significantly improve the key rate at all distances. Key rates in Table 2 show that the method of this work can improve the key rate by 35%–140% comparing with the results of the double-scanning four-intensity MDI-QKD protocol, which is the MDI-QKD protocol with the highest key rate so far. Considering a more practical case where a GHz system works only a second and then performs the data post-processing to extract fresh final keys, there are 10^9 total pulses sent out. Thus, in Fig. 2, we set $N = 10^9$ and the misalignment-error probability $e_d = 0.005$, and the other experiment parameters are listed in Table 1. Figure 2 shows that, with a smaller block size and misalignment-error probability, the key rates can be obviously improved even in the short distance. At the short distance such as 5 km, there are about 1.2×10^7 raw keys to perform error correction process. At a long distance such as 60 km, there are about 2×10^5 raw keys to perform error correction process. Considering that the bit-error rate of these raw keys is about 1%, the low density parity check code (LDPC) error correction algorithm can achieve good error correction inefficiency. While the high-speed field-programmable gate array (FPGA) is adopted to perform the LDPC error correction algorithm, the error correction speed can reach 55 Mb/s

Table 2. Key Rates of Some Points in Fig. 1

Methods	30 km	60 km	90 km	100 km
This work	2.24×10^{-4}	2.33×10^{-5}	1.28×10^{-6}	3.13×10^{-7}
Ref. [38]	1.64×10^{-4}	1.55×10^{-5}	7.01×10^{-7}	1.29×10^{-7}
Ref. [29]	1.33×10^{-4}	9.99×10^{-6}	2.17×10^{-7}	0

[63]. In such cases, the error correction can be completed in less than 1 s.

Except for the symmetric model, the method introduced in this work can be directly applied to the asymmetric channels by simply removing the constraints $p_{\alpha_A} = p_{\alpha_B}$ and $\mu_{\alpha_A} = \mu_{\alpha_B}$. Figures 3 and 4 are the comparison of the key rates with this work and the former methods [29,38] under the asymmetric channels. In the metro QKD network, the distance of QKD is usually less than 50 km, and the maximum possible asymmetry is about 20 km. Thus, we set $L_{AC} - L_{BC} = 20$ km. The other experiment parameters of Fig. 3 are the same as those of Fig. 1, and the other experiment parameters of Fig. 4 are the same as those of Fig. 2. The results show that the method of this work can obviously improve the key rates under the asymmetric channels.

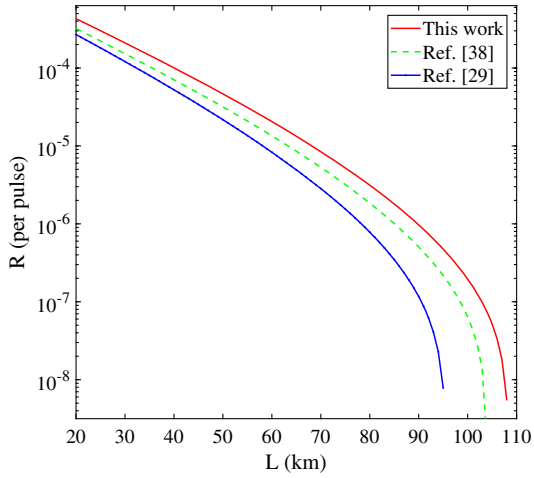

Fig. 3. Comparison of the key rates with this work and the former methods under the asymmetric channels. The experiment parameters are listed in Table 1, and we set $L_{AC} - L_{BC} = 20$ km.

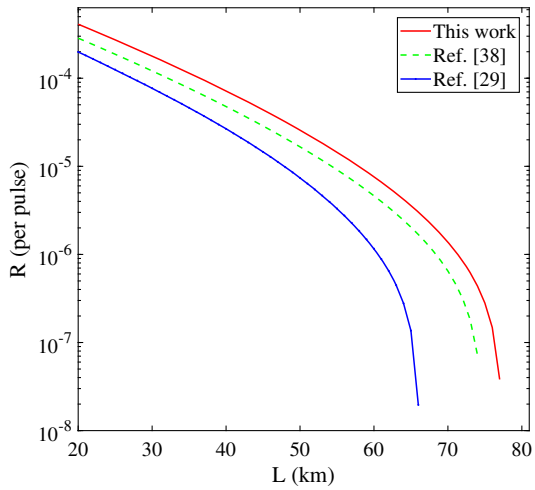

Fig. 4. Comparison of the key rates with this work and the former methods under the asymmetric channels. The experiment parameters here are similar to those in Fig. 3 except that we set $N = 10^9$ and the misalignment-error probability $e_d = 0.005$.

Compared with the former works of MDI-QKD, the method of this work can obviously improve the key rates. But if the infinite decoy-states and infinite-key are considered, both this work and former works can accurately estimate the phase-flip error rate and the counting rate of single-photons, and thus they have similar performances in cases that are limited by the PLOB bound [5,41].

6. CONCLUSION

Based on the technique of the single-photon interference, we propose a modified MDI-QKD protocol with phase post-selection. We prove the security of the announcement of the private phases of the pulse pairs from *xx* source. We also show how to apply the phase post-selection method to the double-scanning four-intensity MDI-QKD protocol. The numerical results show that the phase post-selection method can significantly improve the key rate at all distances. In principle, our method can be directly applied to free-space MDI-QKD. But due to the atmospheric turbulence or moving sites (such as the satellite), the channel is always unstable and changes rapidly, and how to efficiently apply our method to free space will be further studied in future works.

APPENDIX A: CHERNOFF BOUND

The Chernoff bound can help us estimate the expected value from their observed values [61]. Let $X_1, X_2, \ldots, X_n$ be n random samples, detected with the value 1 or 0, and let X denote their sum satisfying $X = \sum_{i=1}^{n} X_i$. E is the expected value of X. We have

$$E^L(X) = \frac{X}{1 + \delta_1(X)}, \tag{A1}$$

$$E^U(X) = \frac{X}{1 - \delta_2(X)}, \tag{A2}$$

where we can obtain the values of $\delta_1(X)$ and $\delta_2(X)$ by solving the following equations:

$$\left[\frac{e^{\delta_1}}{(1+\delta_1)^{1+\delta_1}}\right]^{\frac{X}{1+\delta_1}} = \xi, \tag{A3}$$

$$\left[\frac{e^{-\delta_2}}{(1-\delta_2)^{1-\delta_2}}\right]^{\frac{X}{1-\delta_2}} = \xi, \tag{A4}$$

where ξ is the failure probability.

Besides, we can use the Chernoff bound to help us estimate their real values from their expected values. Similar to Eqs. (A1)–(A4), the observed value, O, and its expected value, Y, satisfy

$$O^U(Y) = [1 + \delta_1'(Y)]Y, \tag{A5}$$

$$O^L(Y) = [1 - \delta_2'(Y)]Y, \tag{A6}$$

where we can obtain the values of $\delta_1'(Y, \xi)$ and $\delta_2'(Y, \xi)$ by solving the following equations:

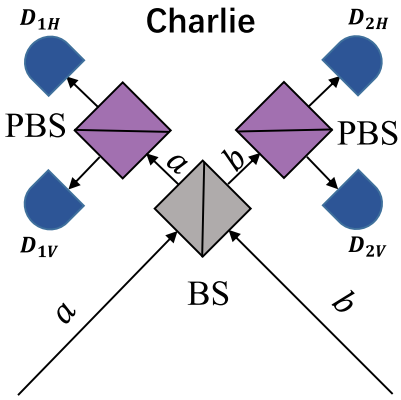

Fig. 5. Bell measurement setup of Charlie [21]. Here we take the polarization-encoding as an example to show the simulation method and the results of the phase-encoding are the same. BS, 50:50 beam splitter; PBS, polarization beam splitter; $D_{1H}, D_{1V}, D_{2H}, D_{2V}$, single-photon detectors.

$$\left[\frac{e^{\delta_1'}}{(1+\delta_1')^{1+\delta_1'}}\right]^Y = \xi, \tag{A7}$$

$$\left[\frac{e^{-\delta_2'}}{(1-\delta_2')^{1-\delta_2'}}\right]^Y = \xi. \tag{A8}$$

APPENDIX B: THE SIMULATION METHOD OF OBSERVED VALUES IN SET Q

A typical detection set-up of Charlie is shown in Fig. 5. In our numerical simulation, the channel is assumed to be a linear channel and the efficiency of detectors is regarded to be part of the channel; thus, we can take the real detector as a 100% detection efficiency detector with dark counting rate p_d. For the time window that Alice and Bob use the source xx, they shall send out a pulse pair in state $|e^{i(\theta_{aj}+\gamma_{aj})}\sqrt{\mu_{x_A}}\rangle \otimes |e^{i(\theta_{bj}+\gamma_{bj})}\sqrt{\mu_{x_B}}\rangle$. Since Charlie is assumed to compensate for the difference in public phases, γ_{aj} and γ_{bj} do not affect the measurement results. To simplify the symbols, we omit the subscript j of private phases and keep in mind that θ_a and θ_b are different in different time windows. Before entering the beam splitter (BS) of the Bell measurement setup of Charlie, the pulse pair is in state

$$|\psi_1\rangle = |e^{i\theta_a}\sqrt{\mu_a}\rangle \otimes |e^{i\theta_b}\sqrt{\mu_b}\rangle, \tag{B1}$$

where $\mu_a = \mu_{x_A}\eta_d\eta_a$, $\mu_b = \mu_{x_B}\eta_d\eta_b$, and η_a and η_b are the transmittance of the channel from Alice to Charlie and from Bob to Charlie, respectively.

We first consider the case that the polarization of the pulse pair is in $++$, where $+$ represents the 45° polarization, and we have

$$|\psi_1\rangle = e^{-\mu_a/2-\mu_b/2}e^{\sqrt{\mu_a}e^{i\theta_a}a_+^\dagger + \sqrt{\mu_b}e^{i\theta_b}b_+^\dagger}|00\rangle. \tag{B2}$$

After the BS and polarization beam splitter (PBS), the state becomes

$$|\psi_2\rangle = e^{-\mu_a/2-\mu_b/2}e^{\left(\frac{\sqrt{\mu_a}}{2}e^{i\theta_a}+\frac{\sqrt{\mu_b}}{2}e^{i\theta_b}\right)(a_H^\dagger+a_V^\dagger)} \times e^{\left(\frac{\sqrt{\mu_a}}{2}e^{i\theta_a}-\frac{\sqrt{\mu_b}}{2}e^{i\theta_b}\right)(b_H^\dagger+b_V^\dagger)}|00\rangle, \tag{B3}$$

where H and V are the horizontal and vertical polarization, respectively.

The measurement operator that D_{1H} and D_{1V} click is

$$\hat{M} = [I_{a_H} - (1-p_d)|0_{a_H}\rangle\langle 0_{a_H}|] \otimes [I_{a_V} - (1-p_d)|0_{a_V}\rangle\langle 0_{a_V}|] \otimes (1-p_d)|0_{b_H}\rangle\langle 0_{b_H}| \otimes (1-p_d)|0_{b_V}\rangle\langle 0_{b_V}|. \tag{B4}$$

Thus, the probability that D_{1H} and D_{1V} click is

$$p_{1H,1V} = \mathrm{tr}(\hat{M}|\psi_2\rangle\langle\psi_2|) = e^{-\mu_a-\mu_b}\left[e^{\frac{\mu_a}{4}+\frac{\mu_b}{4}+\frac{\sqrt{\mu_a\mu_b}}{2}\cos\delta} - (1-p_d)\right]^2(1-p_d)^2, \tag{B5}$$

where $\delta = \theta_a - \theta_b$.

With a similar method, we can conclude that the probabilities that D_{1H}, D_{2V} click, D_{2H}, D_{1V} click, and D_{2H}, D_{2V} click:

$$\begin{aligned} p_{1H,2V} &= p_{2H,1V} \\ &= e^{-\mu_a-\mu_b}\left[e^{\frac{\mu_a}{4}+\frac{\mu_b}{4}+\frac{\sqrt{\mu_a\mu_b}}{2}\cos\delta} - (1-p_d)\right] \\ &\quad\times\left[e^{\frac{\mu_a}{4}+\frac{\mu_b}{4}-\frac{\sqrt{\mu_a\mu_b}}{2}\cos\delta} - (1-p_d)\right](1-p_d)^2, \end{aligned} \tag{B6}$$

$$p_{2H,2V} = e^{-\mu_a-\mu_b}\left[e^{\frac{\mu_a}{4}+\frac{\mu_b}{4}-\frac{\sqrt{\mu_a\mu_b}}{2}\cos\delta} - (1-p_d)\right]^2(1-p_d)^2. \tag{B7}$$

According to the criteria for correct and wrong effective events in X basis, the probabilities that the input state $|\psi_1\rangle$ causes a wrong effective event and a correct effective event, P_W and P_R, are

$$P_W = p_{1H,2V} + p_{2H,1V}, P_R = p_{1H,1V} + p_{2H,2V}. \tag{B8}$$

With a similar method, we can get the probabilities that the other polarization input states cause a wrong effective event and a correct effective event are also P_W and P_R. Finally we have

$$m_Q = \frac{1}{2\pi}Np_{x_A}p_{x_B}\left(\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}}P_W\mathrm{d}\delta + \int_{\pi-\frac{\Delta}{2}}^{\pi+\frac{\Delta}{2}}P_W\mathrm{d}\delta\right), \tag{B9}$$

$$n_Q = \frac{1}{2\pi}Np_{x_A}p_{x_B}\left(\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}}P_R\mathrm{d}\delta + \int_{\pi-\frac{\Delta}{2}}^{\pi+\frac{\Delta}{2}}P_R\mathrm{d}\delta\right) + m_Q, \tag{B10}$$

where n_Q is the total number of the effective events in set Q.

Funding. Ministry of Science and Technology of China through the National Key Research and Development Program of China (2020YFA0309701); National Natural Science Foundation of China (12104184, 12174215, 11974204, 12147107); Shandong Provincial Natural Science Foundation (ZR2021LLZ007); Key R&D Plan of Shandong Province (2021ZDPT01); Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics (KF202110); Leading Talents of Quancheng Industry.

Disclosures. The authors declare no conflicts of interest.

Data Availability. All data that support the findings of this study are included within the paper.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (1984), pp. 175–179.
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
3. N. Gisin and R. Thew, "Quantum communication," Nat. Photonics **1**, 165–171 (2007).
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, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
6. 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**, 1301–1350 (2009).
7. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
8. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
9. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
10. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," Phys. Rev. Lett. **98**, 010503 (2007).
11. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
12. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. **98**, 010505 (2007).
13. 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).
14. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
15. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**, 075001 (2009).
16. T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," Opt. Express **18**, 27217–27225 (2010).
17. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express **19**, 10387–10409 (2011).
18. Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature **589**, 214–219 (2021).
19. 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**, 686–689 (2010).
20. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nat. Commun. **2**, 349 (2011).
21. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
22. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
23. K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," Phys. Rev. A **85**, 042307 (2012).
24. X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," Phys. Rev. A **87**, 012320 (2013).
25. 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).
26. F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Practical aspects of measurement-device-independent quantum key distribution," New J. Phys. **15**, 113007 (2013).
27. F. Xu, H. Xu, and H.-K. Lo, "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution," Phys. Rev. A **89**, 052333 (2014).
28. Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method," Phys. Rev. A **91**, 032318 (2015).
29. 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).
30. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, 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).
31. Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, W.-Y. Liu, X. Jiang, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, C.-Y. Lu, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space measurement-device-independent quantum key distribution," Phys. Rev. Lett. **125**, 260503 (2020).
32. 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).
33. 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**, 238–242 (2020).
34. L. Cao, W. Luo, Y. Wang, J. Zou, R. D. Yan, H. Cai, Y. Zhang, X. L. Hu, C. Jiang, W. J. Fan, X. Q. Zhou, B. Dong, X. S. Luo, G. Q. Lo, Y. X. Wang, Z. W. Xu, S. H. Sun, X. B. Wang, Y. L. Hao, Y. F. Jin, D. L. Kwong, L. C. Kwek, and A. Q. Liu, "Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems," Phys. Rev. Appl. **14**, 011001 (2020).

35. 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**, 312–315 (2016).
36. 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**, 1016–1023 (2017).
37. G. Roberts, M. Lucamarini, Z. Yuan, J. Dynes, L. Comandar, A. Sharpe, A. Shields, M. Curty, I. Puthoor, and E. Andersson, "Experimental measurement-device-independent quantum digital signatures," Nat. Commun. **8**, 1098 (2017).
38. 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).
39. Y.-P. Chen, J.-Y. Liu, M.-S. Sun, X.-X. Zhou, C.-H. Zhang, J. Li, and Q. Wang, "Experimental measurement-device-independent quantum key distribution with the double-scanning method," Opt. Lett. **46**, 3729–3732 (2021).
40. 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**, 400–403 (2018).
41. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nat. Commun. **8**, 15043 (2017).
42. 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).
43. K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound," arXiv:1805.05511 (2018).
44. 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).
45. 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).
46. Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, "Sending-or-not-sending twin-field quantum key distribution in practice," Sci. Rep. **9**, 3080 (2019).
47. 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).
48. 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).
49. H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, "Sending-or-not-sending twin-field quantum key distribution: breaking the direct transmission key rate," Phys. Rev. A **101**, 042330 (2020).
50. 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).
51. C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, "Composable security for practical quantum key distribution with two way classical communication," New J. Phys. **23**, 063038 (2021).
52. 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**, 334–338 (2019).
53. 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).
54. 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).
55. 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).
56. 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).
57. X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," Nat. Photonics **14**, 422–425 (2020).
58. H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, Y. Dai, S.-B. Tang, W. Zhang, H. Li, L. You, Z. Wang, Y. Hua, H. Hu, H. Zhang, F. Zhou, Q. Zhang, X.-B. Wang, T.-Y. Chen, and J.-W. Pan, "Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km," Phys. Rev. Lett. **126**, 250502 (2021).
59. J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, J.-W. Zhang, and Q. Pan, "Twin-field quantum key distribution over 511 km optical fiber linking two distant metropolitans," Nat. Photonics **15**, 570–575 (2021).
60. 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**, 530–535 (2021).
61. H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," Ann. Math. Stat. **23**, 493–507 (1952).
62. X.-L. Hu, Z.-W. Yu, and X.-B. Wang, "Efficient measurement-device-independent quantum key distribution without vacuum sources," Phys. Rev. A **98**, 032303 (2018).
63. Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s quantum key distribution," J. Lightwave Technol. **36**, 3427–3433 (2018).