Lu et al. *EPJ Quantum Technology* (2025) 12:103
https://doi.org/10.1140/epjqt/s40507-025-00408-4

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Experimental measurement-device-independent quantum key distribution with flawed state-preparation over 300 km

Yi-Fei Lu[1], Yan-Yang Zhou[1], Yang Wang[1], Yu Zhou[1], Xiao-Lei Jiang[1], Xin-Hang Li[2], Hai-Tao Wang[1], Yan-Mei Zhao[1], Jia-Ji Li[1], Chun Zhou[1], Hong-Wei Li[1], Lin-Jie Zhou[2*] and Wan-Su Bao[1*]

*Correspondence:
ljzhou@sjtu.edu.cn; bws@qiclab.cn
[1]Henan Key Laboratory of Quantum Information and Cryptography, IEU, Zhengzhou, 450001, China
[2]State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Lab of Navigation and Location Services, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China

Abstract

Quantum key distribution (QKD) promises theoretically secure communication. However, it encounters challenges in implementation security and performance due to inevitable device imperfections. Since the proposal of measurement-device-independent (MDI) QKD, the critical step toward practical security is to secure QKD with imperfect sources. The source imperfections manifest as state-preparation uncertainty (SPU) in various aspects, e.g., encoding uncertainty, intensity fluctuation, and imperfect vacuum states. Here, we perform an MDI-QKD experiment and achieve both high practical security and superior performance. We address the general form of SPU and guarantee a tight estimation of the secret key rate based on the operator dominance method. We achieve secure key distribution over 303.37 km, which not only represents the farthest distance in experiments involving SPU but also considers the most SPU scenarios. Our experimental results represent a significant step toward promoting practical and secure quantum communication.

Keywords: Quantum key distribution; State-preparation uncertainty; Measurement-device-independent

1 Introduction

Quantum key distribution (QKD) [1–4] enables two remote parties, Alice and Bob, to achieve information-theoretically secure communication. Despite its promise, the practical application of QKD faces various theoretical and experimental challenges. The disparity between idealized theoretical models and real-world QKD systems may compromise practical security and limit performance metrics such as the secret key rate (SKR) and transmission distance. While measurement-device-independent (MDI) QKD [5, 6] has significantly mitigated quantum attacks on the receiver, addressing imperfections at the source remains an urgent task to ensure robust security and optimal performance.

Many breakthrough experiments in MDI-QKD have been demonstrated, significantly improving key aspects such as SKR, transmission distance, repetition frequency, and integration [7–15]. These advancements highlight the potential for efficient long-distance quantum communication networks. However, strict assumptions are required on the source side that the quantum states are prepared without flaws. Hence, a crucial step to enhance practical security is securing MDI-QKD with imperfect sources. The role of the source is to prepare pure states according to predefined settings. In the widely employed decoy-state QKD [16–18], this involves preparing weak coherent states with precise intensity and encoding parameters, e.g., polarization [19–21], phase [22–24], or time-bin encoding [25–28]. However, the practical prepared states may be uncertain due to limitations in modulation precision and environmental disturbances. The experimental results indicate that the state-preparation uncertainties (SPUs) of both encoding and intensity follow the Gaussian distribution [29]. Addressing this discrepancy is crucial for enhancing both the practical security and performance of MDI-QKD systems.

Several security proofs have been developed to address SPU in QKD systems. The Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security analysis [30] could accommodate these issues through fidelity analysis, but the provable SKR decreases rapidly as channel loss increases. Some proofs provide conservative analysis based on simple characterizations of SPU intervals [29, 31, 32]. On the one hand, certain security proofs offer security analysis of QKD with only encoding SPU. For instance, the loss-tolerant (LT) method can achieve a high SKR by characterizing the encoding SPU [31, 33–37]. Alternatively, the virtual mutually unbiased bases method [38] can be employed to address the characterized encoding imperfections. It also could address the encoding SPU by regarding the encoding SPU as uncharacterized qubit sources [39–42]. Besides, the issue of unbalanced basis misalignment, a specific case of encoding SPU, has been analyzed with tolerant analysis in MDI-QKD [43]. On the other hand, current methods to address intensity SPU (i.e., intensity fluctuations) involve estimating the counting rates of single-photon states by considering the worst-case scenario using analytical formulas or linear programming [44–47]. Additionally, the issue of imperfect vacuum states is particularly critical due to the finite extinction ratio. However, the vacuum state is essential and serves as the signal state in the time-bin encoding scheme. The issues of the imperfect vacuum states have been analyzed in twin-field QKD [48] and side-channel-free QKD [49].

At present, some MDI-QKD experiments have been performed to address only the encoding SPU [36, 43, 50, 51]. In this work, to obtain both high performance and enhanced practical security, we perform an MDI-QKD experiment by considering the general form of SPU, including encoding uncertainty, intensity fluctuation, and the imperfect vacuum state. The core idea of our method is to construct operator inequalities, known as operator dominance method [52], to provide a tight estimation of the amount of secure keys. The operator dominance method was proposed in Ref. [52] to simplify the security proof of twin-field QKD in the finite-size regime. It could estimate the counting rate of one state by simply constructing the operator inequality with test states. Here, we employ this method to address the SPUs, leveraging its simplicity to accommodate various types of SPUs within a unified theoretical framework. To validate the proposed framework, we have successfully achieved a 303.37 km MDI-QKD over standard single-mode optical fiber in our experiment. Compared with previous MDI-QKD experiments which only consider the encoding SPU with a maximum distance of 170 km [51], our results not only address

more imperfect issues but also greatly extend the distance by 83.56 km in the finite case. Furthermore, compared to long-distance experiments that do not consider SPUs [8], our system maintains a similar secret key rate even at approximately 250 km. This shows that our approach performs robustly over long distances, paving the way for future advancements in secure quantum communication.

2 Results

2.1 Protocol

Step 1 (State preparation and characterization). In every round, Alice first selects a random bit 0 or 1, and determines the Z or X basis with probabilities p_z or p_x, respectively. In Z basis, Alice selects a intensity pair (τ_{a_1}, τ_{a_2}) which will be (μ, o), (ν, o), (o, o), (μ, ω), (ν, ω), (ω, ω), (μ, μ) or (ν, ν) with intensity $\mu > \nu > \omega > o \gtrsim 0$ and the random phases $\theta, \theta' \in [0, 2\pi)$. Here the state o is supposed to be 0 under the ideal condition. Then she prepares the coherent states $|e^{i\theta}\sqrt{\tau_{a_1}}\rangle|e^{i\theta'}\sqrt{\tau_{a_2}}\rangle$ or $|e^{i\theta'}\sqrt{\tau_{a_2}}\rangle|e^{i\theta}\sqrt{\tau_{a_1}}\rangle$ when the random bit is 0 or 1. In X basis, Alice selects a intensity $\tau_a \in \{\nu, \omega, o\}$ and the random phase $\theta \in [0, 2\pi)$, then prepare the coherent states $|e^{i\theta}\sqrt{\tau_a}\rangle|e^{i\theta}\sqrt{\tau_a}\rangle$ or $|e^{i\theta}\sqrt{\tau_a}\rangle|e^{i(\theta+\pi)}\sqrt{\tau_a}\rangle$ when the random bit is 0 or 1. In practical systems, the intensity and phase may be mixed. Alice could characterize the actual prepared states. In Z basis, as the phases are both random in two bins, the state when the random bit is 0 can be expressed as

$$\rho^z_{\tau_{a_1}\tau_{a_2}} = \sum_{i,j=0}^{\infty} q_{i,\tau_{a_1}} q_{j,\tau_{a_2}} |ij\rangle\langle ij|. \tag{1}$$

The state $\rho^z_{\tau_{a_2}\tau_{a_1}}$ when the random bit is 1 can be defined similarly. Here, we have defined that $q_{i,\tau} = \int_{x\in\Pi_\tau} f_x p_{i,x} dx$, where Π_τ represents the set of intensity distribution corresponding to the setting τ, f_x denotes the probability density function, and $p_{i,x} = e^{-x}x^i/i!$ is the Poisson distribution probability. In X basis, the relative phase between two bins is fixed as 0 or π in the ideal case, but the actual states with encoding SPU can be defined as $\rho^{x_0}_{\tau_a}$ and $\rho^{x_1}_{\tau_a}$ when the random bit is 0 and 1 with

$$\rho^{x_{0(1)}}_{\tau_a} = \sum_{k=0}^{\infty} q_{k,\tau_a} \int_{y\in\Lambda_{0(1)}} g_y |\chi_{k,y}\rangle\langle\chi_{k,y}| dy \triangleq \sum_{k=0}^{\infty} q_{k,\tau_a} \rho_k^{x_{0(1)}}, \tag{2}$$

where $\Lambda_{0(1)}$ represents the set of phase distribution and g_y denotes the probability density function, and the two-mode k-photon state is defined as

$$|\chi_{k,y}\rangle = \frac{1}{\sqrt{2^k}} \sum_{r=0}^{k} \sqrt{C_k^r} e^{iry} |r, k-r\rangle. \tag{3}$$

Bob independently selects the parameters and prepares the states in the same way. The prepared states are sent to Charlie through the quantum channel. Here, we note that the prepared states in Eqs. (1) and (2) implicitly imply that the states are independent and identically distributed (i.i.d.) and do not include the potential side-channels. These are summarized as the i.i.d. assumption and the qubit assumption, enabling us to confine our analysis to the modulation spaces.

Step 2 (Measurement). Charlie is supposed to perform the interference measurement and announce the measurement results $\{0, 1, \perp\}$. Here, 0 and 1 corresponds to a measurement of the Bell state $|\psi_0\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ and $(|01\rangle - |10\rangle)/\sqrt{2}$, and $\perp$ corresponds to other failed measurements. The honesty of Charlie is not necessary and the deception will affect the SKR but will not cause security issues.

Step 3 (Sifting). Alice and Bob sift the effective rounds when the measurement results are 0 or 1, and announce the selected intensity and basis for those rounds. They generate the bits for those effective rounds when both are Z basis and the intensity pairs are (μ, o) or (o, μ). They keep these bits as raw bits while Bob flips all of his bits. Other effective rounds are used to estimate the parameters.

Step 4 (Parameter estimation and postprocessing). They estimate the counting rate s_{11} and phase error rate e_x when both sides sent the single-photon states. The detailed estimation methods can be found in Sect. 3. By applying the error correction and privacy amplification methods, they distill the secret key bits from the raw bits, and the SKR is shown as [5, 53]

$$R_{\mathrm{MDI}} \geq p_z^2 p_\mu^2 \{q_{(1,1)} s_{11}[1 - h(e_x)] - f Q_{[\mu,\mu]} h(E_z)\}, \tag{4}$$

where p_z is the probability of selecting the Z basis and p_μ is the probability of choosing the intensity pairs (μ, o) or (o, μ), $q_{(1,1)} = q_{1,\mu}^2 q_{0,o}^2$, and $Q_{[\mu,\mu]}$ and E_z are the counting rate and error rate when both sides choosing the intensity pairs (μ, o) or (o, μ).

2.2 Experimental setup

As illustrated in Fig. 1(a), the MDI-QKD experimental setup consists of two senders, Alice and Bob, and a measurement node, Charlie. Each sender employs a free-running continuous-wave (CW) laser with a central wavelength of 1550.12 nm. The two lasers are independent without frequency locking. For this setup, we choose time-bin encoding as the Z basis and phase encoding as the X basis. A pulse train is modulated by two cascaded intensity modulators (IMs) with a temporal width of 400 ps and a repetition rate of 500 MHz. The first IM chops the CW light into fixed-intensity or vacuum pulses. Then the second IM modulates the fixed-intensity pulses into the signal or decoy states and enhances the extinction ratio of the vacuum pulses. In this way, we could generate four different intensity levels of optical pulses, and the intensity pairs fulfill the requirements of step 1 in Sect. 2.1. Note that the intensity pairs in Z and X bases are different. Two phase modulators (PMs) then randomize the phase of the pulses and modulate the phase difference between the two time bins. When the Z basis is selected, the two pulses in a pair are independently modulated with random phases. When the X basis is chosen, the first pulse in a pair is modulated with a random phase θ, while the second pulse is modulated with either θ or $\theta + \pi$, depending on the random bit. The modulators are driven by an arbitrary waveform generator and the IMs are biased with bias controllers. Two electrically polarization controllers (EPCs) compensate for polarization drift based on feedback from Charlie. Finally, the light pulses are attenuated to the single-photon level using electrically variable optical attenuators (EVOAs).

The quantum channel is the standard single-mode fiber with a typical loss coefficient of 0.2 dB/km. At the receiver, the light pulses first pass through polarization beam splitters (PBSs) to ensure identical polarization. Then the pulses interfere at the 50:50 beam

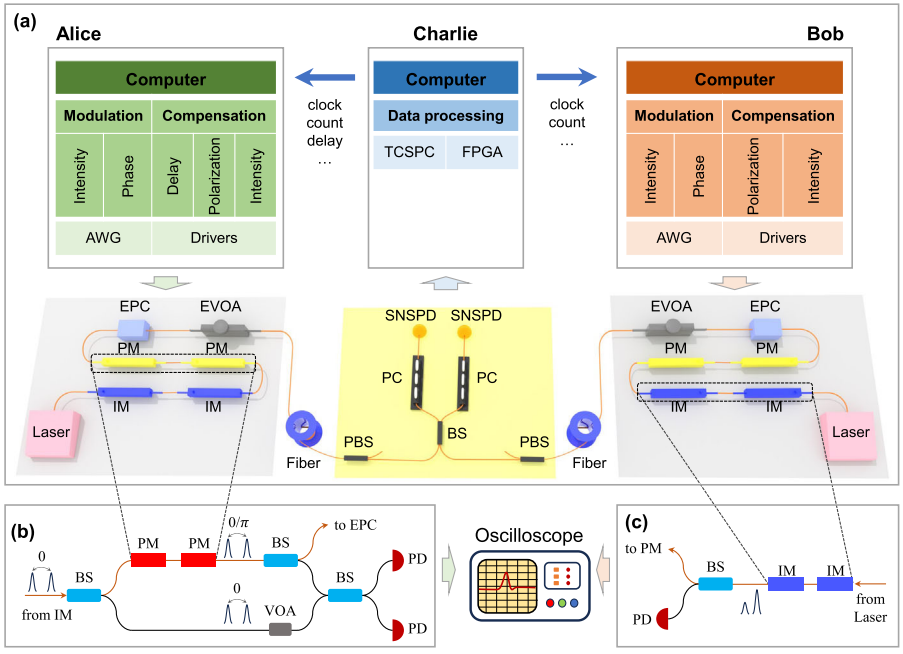

Figure 1 Experimental set-up. (a) MDI-QKD experimental system. The MDI-QKD system is controlled by three computers located at Alice, Bob, and Charlie. At the senders (Alice and Bob), the AWG and hardware drivers are employed to provide modulation signals while enabling system tracking, compensation, and precise calibration. At the receiver (Charlie), it performs interference measurement, samples the detection results, and provides feedback control information. The entire system is capable of continuous and stable operation. Within the system's optical path, the continuous-wave light is chopped into a train of pulses with four intensities by two IMs. Then the phases are modulated by two PMs for phase encoding and phase randomization. These four modulators are driven by an AWG, and the biases of the IMs are controlled by a bias controller. The polarization and time delay are compensated according to the feedback from Charlie. The encoded pulses are attenuated to the single-photon level by an EVOA and transmitted to Charlie. Bob's setup is the same as Alice's, but their modulations are independent. Alice, Bob, and Charlie are connected with the standard single-mode fiber. Charlie aligns the pulses from Alice and Bob with two PBSs and performs interference with a 50:50 BS. The interference pulses are detected with two SNSPDs. The electrical output signals of SNSPDs are processed with TCSPC and FPGA. The counting rate within 300 milliseconds of a SNSPD is sent to Alice and Bob for polarization compensation. The delay between Alice and Bob is sent to Alice for delay compensation. (b) Phase characterization scheme. The pulse is first split into two pulses, then one arm is modulated by PMs and the other arm serves as the reference pulses without phase modulation. After phase modulation, the signal pulse is then split with one for QKD and the other for characterization. The delay and attenuation of the two arms are balanced with fiber and VOA. The phase difference between two arms can be calculated according to the intensity ratio of two PDs. Then the modulated phase difference between the two bins is obtained. (c) Intensity characterization scheme. The signal pulses without attenuation are directly split with one detected with a PD and the other for QKD. AWG, arbitrary waveform generator; IM, intensity modulator; PM, phase modulator; EPC, electrically polarization controller; EVOA, electrically variable optical attenuator; PBS, polarization beam splitter; BS, beam splitter; PC, polarization controller; SNSPD, superconducting nanowire single-photon detector; TCSPC, time-correlated single-photon counting system; FPGA, field programmable gate array; PD, photodetector

splitter (BS). After adjusting the polarization with polarization controllers (PCs), the interference pulses are detected using superconducting nanowire single-photon detectors (SNSPDs). Considering that the period of the light pulses is 2 ns while the dead time of the SNSPDs is around 50 ns, Charlie will only announce the detection results of the Bell state $|\psi_1\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ or the failed detection $\perp$. The detection efficiency and dark count rate of the SNSPDs are calibrated to approximately 55% and 3E−8 in the sample interval.

The detection signals are sampled and processed with a time-correlated single-photon counting system (TCSPC) and a field programmable gate array (FPGA).

Charlie provides feedback to Alice and Bob on the counting rate of the one SNSPD every 300 milliseconds. Alice and Bob alternately adjust the EPCs to maximize the detector counting rate for polarization compensation, thereby achieving polarization tracking and compensation. Besides, Charlie provides feedback on the delay of Alice and Bob's pulses, and Alice adjusts the delay to achieve alignment. Alice and Bob both synchronize their operations with Charlie.

Alice and Bob characterize the SPUs with setups in Figs. 1(b) and (c). The phase characterization setup is shown in 1(b). In MDI-QKD, the two PMs will modulate the phase of two time bins, with the encoding based on the phase difference between them. To characterize the SPU, we split the pulses into two arms: one for phase modulation and the other serving as a reference. Then the split pulses are interfered with at a 50:50 beam splitter (BS). The pulses after interference are detected with classical photodetectors (PDs). We could calculate the phase difference of the interfered pulses. The difference in the phase differences calculated from the two bins represents the modulated phase. The intensity characterization setup is shown in 1(c), where a PD is directly used to measure pulses of varying intensities.

In the above steps, it can be seen that the entire QKD process can be divided into two phases: the key distribution mode and the SPU characterization mode. The switching between the two modes can be efficiently implemented using the optical switch or BS. As shown in the Figs. 1(b) and (c), we present a BS-based implementation for the two operational modes, enabling simultaneous source characterization and key generation. The brown lines represent the link for key generation, which incorporates additional BSs. The only cost of this configuration is the introduction of additional attenuation at the source side, which will not affect the key generation and can be compensated by adjusting the EVOA at the output. The characterization of SPUs can be flexibly conducted at any point during the key distribution process, allowing for precise and thorough assessment without compromising efficiency.

2.3 Experimental results

We implement the experiment with the standard single-mode fiber at the transmission distances of 101.15, 152.40, 202.31, 253.56, and 303.57 km. The frequency difference between Alice and Bob's lasers is kept within 4 MHz without frequency locking, which is shown in Fig. 5. We note that the frequency drift is caused only by the internal operation of the lasers. This means that the frequency drift is independent from the QKD setting choices and hence the impact of frequency drift is uniform across different encoded states. Besides, as the phase randomization is additionally performed in the state preparation step, there are no phase correlations between different pulses. Therefore, the i.i.d. assumption can be guaranteed in the presence of frequency drift.

Before the experiments at every distance, we characterize the modulated phase and intensity. The results show that the phase and intensity of the light pulses obey the Gaussian distribution. The characterized intensity SPU in the 303.57 km experiment and the characterized phase SPU are shown in Fig. 2. The detailed results are listed in Tables 2 and 3.

The simulated and experimental SKR results are shown in Fig. 3. The SKR is simulated based on the characterized results at 253.56 km in both the asymptotic and finite cases.

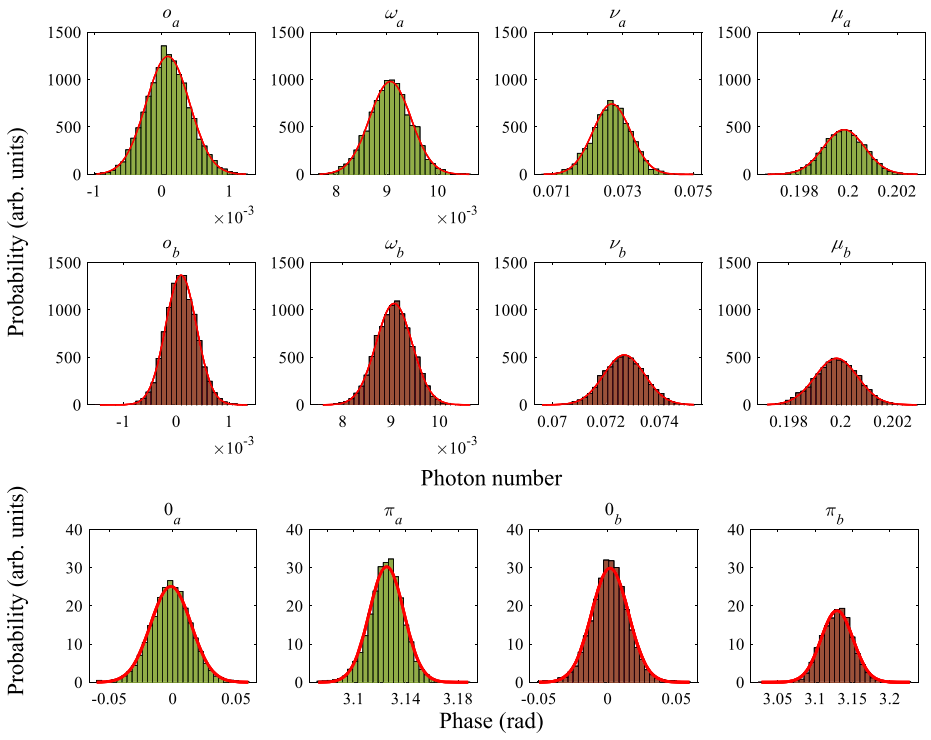

Figure 2 Results of intensity and phase characterization. The first two rows illustrate the intensity distribution, where intensity μ represents the signal state, while the others denote the decoy states. The last row shows the phase distribution. The subscripts *a* and *b* indicate Alice and Bob, respectively

And the simulation method is given in App. C. The experimental SKR results are represented by red dots and green triangles for the asymptotic and finite cases, respectively. The results show that a secure key distribution distance of 303.57 km can still be achieved even when simultaneously accounting for the encoding SPU, intensity modulation SPU, and the effects of non-ideal vacuum states. More experimental details are shown in App. A. In addition, we consider the finite effects [54] with security coefficient ε = 1E−10, and perform experiments with the total number N = 7.68E12, 7.50E13, 9.67E13, 5.08E14, and 5.34E14 at 101.15, 152.40, 202.31, 253.56 km, respectively. In the finite case, the achievable distance remains at 253.56 km. This distance is a significant improvement over previous experiments, demonstrating the robustness and reliability of our system under realistic conditions.

We compare our results with recent MDI-QKD experiments that consider SPUs in Table 1. Current experiments primarily focus on encoding SPU while neglecting the issues related to intensity modulation and non-ideal vacuum states. Our work accounts for the largest variety of SPUs while achieving the longest secure key distribution distance. At present, the farthest distance achieved in MDI-QKD experiments considering only encoding SPU is 170 km. We have significantly extended this distance to 303.37 km, demonstrating a substantial improvement in transmission capability. Moreover, our system achieves higher secret key rates. For instance, at a distance of 152.40 km, the rate reaches 23.9 bps, which surpasses the rate previously reported for a 50 km distance. Furthermore, when compared to long-distance experiments that do not account for SPUs [8], our system achieves a rate that remains on the same order of magnitude even at ap-

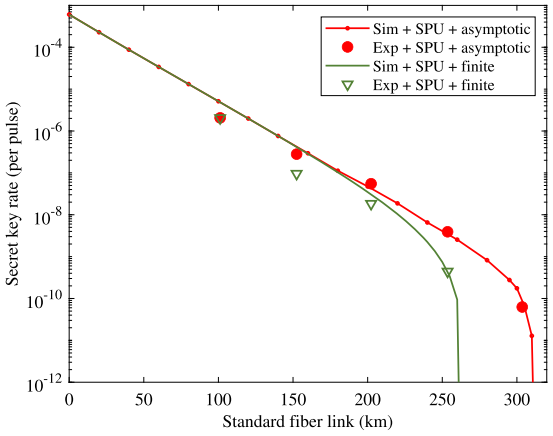

Figure 3 Secret key rate (SKR) in logarithmic scale versus transmission distance between Alice and Bob. The SKR is simulated according to the characterized results in our experiments in the asymptotic and finite cases. The experimental SKR results are shown with red dots and green triangles in the asymptotic and finite cases, respectively

Table 1 List of recent MDI-QKD experiments with SPUs. Three types of SPUs are considered: the encoding SPU, the intensity modulation SPU, and the effects of imperfect vacuum states

Reference	Encoding	Intensity	Vacuum	Distance (km)	Rate (bps)	Year	Notes
Yin [8]	×	×	×	259 404[a]	0.221 3.21E–04	2016	Without SPU
Tang [36]	✓	×	×	40[b]	10	2016	/
Wang [50]	✓	×	×	50	18.8	2019	/
Zhou [51]	✓	×	×	170	3.53	2020	/
Wei [12]	×	×	×	180	31	2020	Without SPU
Lu [43]	✓	×	×	50	21.4	2022	/
This work	✓	✓	✓	101.15 152.40 202.31 253.56 303.37[b]	510 23.9 4.58 0.11 0.0157	2025	/

[a] Ultra-low-loss fiber.
[b] Asymptotic.

proximately 250 km. This indicates that our approach maintains robust performance and efficiency over extended distances, highlighting its superiority in practical long-distance quantum communication scenarios.

3 Methods

Following the security analysis framework [33, 55, 56], a key step is to estimate the counting rate and error rate of the single-photon states. To facilitate this analysis, we consider the virtual entanglement version of the MDI-QKD protocol in the presence of SPU. In both the prepare-and-measure and entanglement versions, the classical and quantum information available to Eve, and the ultimate results for Alice and Bob are consistent. In the entanglement version, the phase error rate can be defined to quantify the information leakage to Eve. Therefore, the security is equivalent and the security of the QKD protocol can be guaranteed by proving the virtual entanglement version. When utilizing the weak coher-

ent source in MDI-QKD systems, it is crucial to estimate the single-photon counting rate under various conditions to obtain the counting rate and error rate of the single-photon states. In this scenario, the SPU occurs in both the encoding space and the intensity space. Especially, the vacuum states are essential for time-bin encoding but are impractical due to the limited extinction ratio. To tightly bound the observations of single-photon states in the presence of encoding and intensity SPUs, we construct operator dominance conditions, as summarized in Eqs. (9) and (12). This could relax the stringent requirements on state preparation while ensuring the robustness and performance of QKD systems.

3.1 Estimation of the phase error rate

To analyze the phase error rate, we consider the single-photon MDI-QKD where both Alice and Bob prepare the single-photon state and send them to Charlie. The single-photon states in Z basis are $\rho_1^{z_0} = |01\rangle$ or $\rho_1^{z_1} = |10\rangle$, a fraction in Eq. (1). The encoding states in these forms are guaranteed with the qubit assumptions, such that the states in high dimension is identical. We note that the qubit assumption can be removed by decomposing the non-qubit states into a direct sum of two states with one in a qubit space and the other one in the complementary space [57, 58], enabling a more general practical security analysis. In the entanglement protocol, Alice prepares the general state in Z basis as

$$|\phi\rangle_{ac_1} = \sum_{i\in\{0,1\}} \sqrt{p_i}|i\rangle_a|\bar{i},i\rangle_{c_1}, \tag{5}$$

where p_0 and p_1 are the probabilities of random bits 0 and 1, and are equal to 0.5 ideally. Here the ancillary system a is kept secretly and the actual system c_1 is sent to Charlie. Similarly, Bob prepares the states $|\phi\rangle_{bc_2}$ and sends system c_2 to Charlie.

Then the untrusted Charlie is supposed to perform the interference measurement and announce the results. The channel evolution and Charlie's operation on the composite systems c_1c_2 can be characterized by the POVM $\{\hat{C}_0, \hat{C}_1, \hat{C}_\perp\}$, corresponding to the announcement of the measurement results $\{0, 1, \perp\}$. Note that there is no assumption about POVM due to the feature of measurement device independent.

The phase error rate corresponding to the measurement results 0 and 1 can be shown as

$$\begin{aligned} e_{x_0} &= \frac{\mathrm{Tr}[(|+-\rangle\langle+-|+|-+\rangle\langle-+|)\otimes\hat{C}_0\hat{P}(|\phi\rangle_{ac_1}\otimes|\phi\rangle_{bc_2})]}{\mathrm{Tr}[\hat{C}_0\hat{P}(|\phi\rangle_{ac_1}\otimes|\phi\rangle_{bc_2})]}, \\ e_{x_1} &= \frac{\mathrm{Tr}[(|++\rangle\langle++|+|--\rangle\langle--|)\otimes\hat{C}_1\hat{P}(|\phi\rangle_{ac_1}\otimes|\phi\rangle_{bc_2})]}{\mathrm{Tr}[\hat{C}_1\hat{P}(|\phi\rangle_{ac_1}\otimes|\phi\rangle_{bc_2})]}, \end{aligned} \tag{6}$$

where $\hat{P}(|\cdot\rangle) = |\cdot\rangle\langle\cdot|$. The overall phase error rate can be defined based on the convexity of the binary entropy function as

$$e_x = \frac{\sum_i e_{x_i}\mathrm{Tr}[\hat{C}_i(\rho_{c_1}\otimes\rho_{c_2})]}{\mathrm{Tr}[(\mathbb{I}-\hat{C}_\perp)(\rho_{c_1}\otimes\rho_{c_2})]}. \tag{7}$$

Note that due to the dead-time of SPDs, the announcement of the Bell state $|\psi_0\rangle$ may be impossible and e_{x_1} is just the final phase error rate in most MDI-QKD systems. The denominators in Eq. (6) are just the counting rate of announcing 0 and 1 when Alice and

Bob prepare the composite states $|\phi\rangle_{ac_1} \otimes |\phi\rangle_{bc_2}$. The elements in the numerators in Eq. (6) are shown as

$$\mathrm{Tr}[|jk\rangle\langle jk| \otimes \hat{C}_i \hat{P}(|\phi\rangle_{ac_1} \otimes |\phi\rangle_{bc_2})] = \frac{1}{4}\mathrm{Tr}[\hat{C}_i(\varrho_j \otimes \varrho_k)], \tag{8}$$

where $i \in \{0,1\}$, $j,k \in \{+,-\}$, and $\varrho_\pm = \hat{P}[(|01\rangle \pm |10\rangle)/\sqrt{2}]$.

To estimate the phase error rate, we analyze the states in X basis. The single-photon states in X basis are $\rho_1^{x_0}$ and $\rho_1^{x_1}$, a fraction of the states in Eq. (2). To obtain the upper bound of the phase error rate, we give the operator dominance condition as

$$\varrho_\pm \le \sigma_\pm \triangleq \sum_{d\in\{z_0,z_1,x_0,x_1\}} \beta_d^\pm \rho_1^d, \tag{9}$$

with $\beta_d \in \mathbb{R}$. The details for the contribution of Eq. (9) are shown in App. B. Then we can obtain that

$$\varrho_j \otimes \varrho_k \le \varrho_j \otimes \sigma_k \le \sigma_j \otimes \sigma_k, j,k \in \{+,-\}. \tag{10}$$

This can be used to estimate the upper bound of Eq. (8) as

$$\mathrm{Tr}[\hat{C}_i(\varrho_j \otimes \varrho_k)] \le \mathrm{Tr}[\hat{C}_i(\sigma_j \otimes \sigma_k)] = \sum_{d,d'\in\{z_0,z_1,x_0,x_1\}} \beta_d^j \beta_{d'}^k \mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})], \tag{11}$$

where $\mathrm{Tr}[\hat{C}_i(\rho_1^{z_i} \otimes \rho_1^{z_{i'}})]$ is the probability of announcing measurement result i when Alice and Bob prepare the states ρ_1^d and $\rho_1^{d'}$, respectively. As these probabilities can be obtained directly in the single-photon MDI-QKD, the phase error rate can be estimated in the presence of encoding SPU. In the coherent source MDI-QKD, the phase error rate can be estimated in the same way on condition that the bounds of the probability $\mathrm{Tr}[\hat{C}_i(\rho_1^{z_i} \otimes \rho_1^{z_{i'}})]$ are estimated with the decoy-state method. We present the analysis in the next subsection.

3.2 Estimation of the single-photon counting rate

In the coherent source MDI-QKD, the actual prepared states are shown in Eqs. (1) and (2). The decoy-state method [16–18] can be applied to estimate different counting rates of the single-photon states. Below we show how to estimate the bounds of the single-photon counting rate to calculate the lower bound of s_{11} and the upper bound of the phase error rate e_x. As we consider the SPUs of the encoding, intensity modulation, and imperfect vacuum states, the decoy-state estimation should be modified.

To estimate these parameters, we give the operator dominance conditions as

$$\begin{aligned}
\rho_1^d &\ge \sum_{(\tau_1,\tau_2)} \beta_{\tau_1,\tau_2}^{d,0} \rho_{\tau_1,\tau_2}^z, d \in \{z_0,z_1\},\\
\rho_1^d &\le \sum_{(\tau_1,\tau_2)} \beta_{\tau_1,\tau_2}^{d,1} \rho_{\tau_1,\tau_2}^z, d \in \{z_0,z_1\},\\
\rho_1^d &\ge \sum_{\tau} \beta_{\tau}^{d,0} \rho_{\tau}^x, d \in \{x_0,x_1\},\\
\rho_1^d &\ge \sum_{\tau} \beta_{\tau}^{d,1} \rho_{\tau}^x, d \in \{x_0,x_1\},
\end{aligned} \tag{12}$$

with proper $\beta^{d,0}_{\tau_1,\tau_2}, \beta^{d,1}_{\tau_1,\tau_2}, \beta^{d,0}_{\tau}, \beta^{d,1}_{\tau} \in \mathbb{R}$. The details for the contribution of Eq. (12) are shown in App. B. The validity of Eq. (12) relies on the absence of correlations, such as those introduced by the pattern effect [59]. When considering the pattern effect, we could utilize the pattern sifting and alternate key distillation post-processing operations to remove the impact of correlations [59]. Besides, we also could utilize reference technique [60] to accommodate the correlations between setting choices, such as bit and basis choices. Here, we consider that the i.i.d. assumption is guaranteed.

With the operator dominance conditions in Eq. (12), we show how to estimate the parameters. The counting rate of the single-photon state s_{11} is defined as

$$s_{11} = \frac{1}{4} \sum_{d,d' \in \{z_0,z_1\}} \mathrm{Tr}[(\hat{C}_0 + \hat{C}_1)(\rho_1^d \otimes \rho_1^{d'})]. \tag{13}$$

According to the first operator dominance condition in Eq. (12), we can conclude the following formula with $d, d' \in \{z_0, z_1\}$

$$\rho_1^d \otimes \rho_1^{d'} \geq \sum_{(\tau_1,\tau_2)} \sum_{(\tau_3,\tau_4)} \beta^{d,0}_{\tau_1,\tau_2} \beta^{d',0}_{\tau_3,\tau_4} \rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4}. \tag{14}$$

Then the lower bound of the single-photon counting rate s_{11} is given by

$$s_{11} \geq \frac{1}{4} \sum_{d,d' \in \{z_0,z_1\}} \sum_{(\tau_1,\tau_2)} \sum_{(\tau_3,\tau_4)} \beta^{d,0}_{\tau_1,\tau_2} \beta^{d',0}_{\tau_3,\tau_4} \times \mathrm{Tr}[(\hat{C}_0 + \hat{C}_1)(\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4})], \tag{15}$$

where $\mathrm{Tr}[(\hat{C}_0 + \hat{C}_1)(\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4})]$ is the counting rate of announcing 0 and 1 when Alice and Bob prepare the states $\rho^z_{\tau_1,\tau_2}$ and $\rho^z_{\tau_3,\tau_4}$, respectively.

According to Eqs. (6)-(11), to obtain the upper bound of the phase error rate e_x, we only need to estimate the lower or upper bounds of $\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})]$ with $d, d' \in \{z_0, z_1, x_0, x_1\}$ according to the sign of the coefficient $\beta_d \beta_{d'}$ in Eq. (11). The bounds can be calculated the same as Eq. (14). We directly give the results in the following. For $d, d' \in \{z_0, z_1\}$, we have

$$\begin{aligned}
\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\geq \sum_{(\tau_1,\tau_2)} \sum_{(\tau_3,\tau_4)} \beta^{d,0}_{\tau_1,\tau_2} \beta^{d',0}_{\tau_3,\tau_4} \mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4})], \\
\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\leq \sum_{(\tau_1,\tau_2)} \sum_{(\tau_3,\tau_4)} \beta^{d,1}_{\tau_1,\tau_2} \beta^{d',1}_{\tau_3,\tau_4} \mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4})].
\end{aligned} \tag{16}$$

For $d \in \{z_0, z_1\}$ and $d' \in \{x_0, x_1\}$, we have

$$\begin{aligned}
\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\geq \sum_{(\tau_1,\tau_2)} \sum_{\tau} \beta^{d,0}_{\tau_1,\tau_2} \beta^{d',0}_{\tau} \mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^x_{\tau})], \\
\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\leq \sum_{(\tau_1,\tau_2)} \sum_{\tau} \beta^{d,1}_{\tau_1,\tau_2} \beta^{d',1}_{\tau} \mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^x_{\tau})].
\end{aligned} \tag{17}$$

For $d \in \{x_0, x_1\}$ and $d' \in \{z_0, z_1\}$, we have

$$\begin{aligned}
\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\geq \sum_{\tau} \sum_{(\tau_3,\tau_4)} \beta^{d,0}_{\tau} \beta^{d',0}_{\tau_3,\tau_4} \mathrm{Tr}[\hat{C}_i(\rho^x_{\tau} \otimes \rho^z_{\tau_3,\tau_4})], \\
\mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\leq \sum_{\tau} \sum_{(\tau_3,\tau_4)} \beta^{d,1}_{\tau} \beta^{d',1}_{\tau_3,\tau_4} \mathrm{Tr}[\hat{C}_i(\rho^x_{\tau} \otimes \rho^z_{\tau_3,\tau_4})].
\end{aligned} \tag{18}$$

And for $d, d' \in \{x_0, x_1\}$, we have

$$\begin{aligned} \mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\geq \sum_{\tau}\sum_{\tau'} \beta_{\tau}^{d,0}\beta_{\tau'}^{d',0}\mathrm{Tr}[\hat{C}_i(\rho_{\tau}^{x} \otimes \rho_{\tau'}^{x})], \\ \mathrm{Tr}[\hat{C}_i(\rho_1^d \otimes \rho_1^{d'})] &\leq \sum_{\tau}\sum_{\tau'} \beta_{\tau}^{d,1}\beta_{\tau'}^{d',1}\mathrm{Tr}[\hat{C}_i(\rho_{\tau}^{x} \otimes \rho_{\tau'}^{x})]. \end{aligned} \tag{19}$$

These parameters $\mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4})]$, $\mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^x_{\tau})]$, $\mathrm{Tr}[\hat{C}_i(\rho^x_{\tau} \otimes \rho^z_{\tau_3,\tau_4})]$ and $\mathrm{Tr}[\hat{C}_i(\rho^x_{\tau} \otimes \rho^x_{\tau'})]$ can be obtained directly in MDI-QKD systems, which are the probabilities of announcing result i when Alice and Bob prepare the states $\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4}$, $\rho^z_{\tau_1,\tau_2} \otimes \rho^x_{\tau}$, $\rho^x_{\tau} \otimes \rho^z_{\tau_3,\tau_4}$ and $\rho^x_{\tau} \otimes \rho^x_{\tau'}$, respectively.

4 Discussion

In this work, we have significantly advanced the MDI-QKD experiment by addressing the SPUs in various aspects and extending the maximum transmission distance to 303.37 km. To address these practical issues, we construct the operator dominance method and give a tight estimation of the amount of secure keys. While considering more kinds of SPUs, an improvement of 83.56 km has been achieved over previous MDI-QKD experiments that only considered encoding SPU. Additionally, even at the extended distance, our system maintains a rate comparable to long-distance MDI-QKD experiments that do not account for SPUs. These results highlight the practicality and robustness of our approach in practical MDI-QKD systems. Our work improves the practicality of current MDI-QKD systems and provides a foundation for future development and deployment in secure quantum communication.

As we aim to provide a comprehensive solution to the specific class of practical source imperfection only in the modulation spaces, there remain several crucial research directions in other aspects for future work. First, the encoding may be correlated with other degrees of freedom and hence introduces side channels, which might violate the qubit assumption [57, 58, 61–63]. Second, the correlations may also occur between nearby pulses, e.g., the pattern effect [59, 64], the setting choice correlations [60, 65], and the phase correlations [66]. This will undermine the condition that the quantum states are i.i.d. At present, a number of approaches can be employed to remove these assumptions [57–60, 63, 65]. Therefore, extending our framework to incorporate these methods and account for such imperfections will be an essential direction for achieving higher practical security in QKD for future research.

Appendix A: Detailed experimental results

In this section, we present the detailed experimental results. The Tables 2 and 3 give the parameters of Gaussian approximation of the phase and intensity distributions, respectively. The Table 4 lists the probabilities and the Table 5 shows the detailed experimental results.

Besides, as shown in Fig. 4, we measure the frequency difference of two independent lasers through beat frequency without feedback every 0.1 seconds in 30 minutes. The two lasers beat at a 50:50 BS and the results are detected with the classical PDs. The frequency difference then is analyzed with the detected time domain signals. Figure 5 shows the frequency difference between two free-running lasers.

Table 2 Parameters of Gaussian approximation of phase distributions. $\bar{x}$: mean, σ: standard deviation

	0_a	π_a	0_b	π_b
$\bar{x}$	–0.0017	3.1253	0.0015	3.1293
σ	0.0172	0.0143	0.018	0.0245

Table 3 Parameters of Gaussian approximation of intensity distributions. $\bar{x}$: mean, σ: standard deviation

Distance		μ_a	ν_a	ω_a	o_a	μ_b	ν_b	ω_b	o_b
101.15	$\bar{x}$	0.204089	0.060832	0.005893	9.15E–5	0.206184	0.060095	0.005776	9.93E–5
	σ	0.001058	0.000417	0.000307	0.000375	0.001186	0.000737	0.000453	0.000461
152.40	$\bar{x}$	0.200601	0.062914	0.006276	6.29E–5	0.204206	0.062903	0.006111	0.000137
	σ	0.001027	0.000603	0.000427	0.000439	0.001096	0.000607	0.000449	0.000511
202.31	$\bar{x}$	0.205472	0.061212	0.006039	7.98E–5	0.206309	0.061031	0.006095	7.33E–5
	σ	0.00097	0.000585	0.000409	0.00037	0.001148	0.0006	0.000457	0.000453
253.56	$\bar{x}$	0.198356	0.063045	0.008034	5.90E–5	0.200584	0.064894	0.007884	7.82E–5
	σ	0.000843	0.000899	0.000203	0.000132	0.000698	0.000611	0.000214	0.000226
303.57	$\bar{x}$	0.199829	0.072682	0.009065	9.20E–5	0.186857	0.072263	0.009337	0.000118
	σ	0.000847	0.000537	0.000407	0.000320	0.000763	0.000712	0.000348	0.000272

Table 4 Experimental parameters of the probability. $p_{(\tau_1,\tau_2)}$ denotes the probability of preparing the states with intensities τ_1 and τ_2, where the order of τ_1 and τ_2 is random

	$p_{(\mu,o)}$	$p_{(\nu,o)}$	$p_{(o,o)}$	$p_{(\nu,\nu)}$	$p_{(\mu,\mu)}$	$p_{(\mu,\omega)}$	$p_{(\nu,\omega)}$	$p_{(\omega,\omega)}$
Alice	0.7574	0.0382	0.0360	0.033	0.0284	0.0278	0.0408	0.0384
Bob	0.7460	0.0394	0.0378	0.035	0.0306	0.0326	0.0384	0.0402

Table 5 Experimental results of MDI-QKD at various quantum link fiber lengths

Distance (km)	$Q_{[\mu,\mu]}$	E_z	s_{11}	e_x	R_{MDI}
101.15	1.44E–5	0.0047	2.83E–4	0.0939	2.06E–6
152.40	1.78E–6	0.0036	3.55E–5	0.0845	2.80E–7
202.31	1.82E–7	0.0025	1.21E–5	0.1880	5.51E–8
253.56	1.89E–8	0.0027	1.30E–6	0.2331	3.92E–9
303.37	1.83E–9	0.0043	4.80E–8	0.2703	6.26E–11

Appendix B: Construction of operator dominance conditions

In this section, we analyze how to construct the operator dominance conditions in Eqs. (9) and (12).

For Eq. (9), we could restrict it as equality, i.e., $\varrho_{\pm} = \sum_{d\in\{z_0,z_1,x_0,x_1\}} \beta_d \rho_1^d$. Then it is equivalent to the following linear equations

$$\frac{1}{2}\begin{bmatrix} 2 & 0 & 1 & 1 \\ 0 & 0 & \int_{y\in\Gamma_0} g_y e^{iy} dy & \int_{y\in\Gamma_1} g_y e^{iy} dy \\ 0 & 0 & \int_{y\in\Gamma_0} g_y e^{-iy} dy & \int_{y\in\Gamma_1} g_y e^{-iy} dy \\ 0 & 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} \beta_{z_0}^{\pm} \\ \beta_{z_1}^{\pm} \\ \beta_{x_0}^{\pm} \\ \beta_{x_1}^{\pm} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ \pm 1 \\ \pm 1 \\ 1 \end{bmatrix}, \tag{B.1}$$

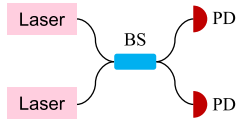

Figure 4 Schematic diagram of the frequency difference characterization scheme. BS, beam splitter; PD, photodetector

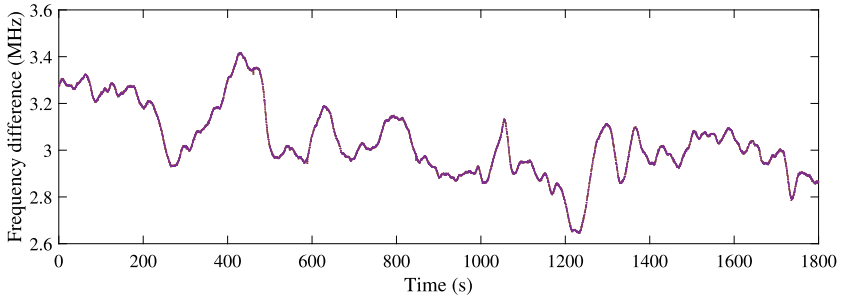

Figure 5 The frequency difference of two free-running lasers

which is also equivalent to the following real version as

$$\begin{bmatrix} 2 & 0 & 1 & 1 \\ 0 & 0 & \int_{y\in\Gamma_0} g_y \cos y dy & \int_{y\in\Gamma_1} g_y \cos y dy \\ 0 & 0 & \int_{y\in\Gamma_0} g_y \sin y dy & \int_{y\in\Gamma_1} g_y \sin y dy \\ 0 & 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} \beta_{z_0}^{\pm} \\ \beta_{z_1}^{\pm} \\ \beta_{x_0}^{\pm} \\ \beta_{x_1}^{\pm} \end{bmatrix} = \begin{bmatrix} 1 \\ \pm 1 \\ 0 \\ 1 \end{bmatrix}. \tag{B.2}$$

We could sovle this linear equations to obtain the coefficients $\beta_d^{\pm}$ with $d \in \{z_0, z_1, x_0, x_1\}$ for Eq. (9).

The contributions for Eq. (12) are a little complex due to the imperfect vacuum states. We first define the following two operators

$$\begin{aligned} \rho^{\mu} &\triangleq \frac{\rho_{\mu o}^{z}}{q_{0,\mu}} - \frac{\rho_{oo}^{z}}{q_{0,o}} = \sum_{j=1}^{\infty} \alpha_{j,\mu} |j\rangle\langle j| \otimes \rho_o, \\ \rho^{\nu} &\triangleq \frac{\rho_{\nu o}^{z}}{q_{0,\nu}} - \frac{\rho_{oo}^{z}}{q_{0,o}} = \sum_{j=1}^{\infty} \alpha_{j,\nu} |j\rangle\langle j| \otimes \rho_o \end{aligned} \tag{B.3}$$

where the coefficients $\alpha_{j,\tau} = q_{j,\tau}/q_{0,\tau} - q_{j,o}/q_{0,o}$ and the operator $\rho_o = \sum_{i=0}^{\infty} q_{i,o}|i\rangle\langle i|$. Then the linear combination of these two operators is given as

$$\alpha_{2,\nu}\rho^{\mu} - \alpha_{2,\mu}\rho^{\nu} = \sum_{j=1}^{\infty} \beta_j |j\rangle\langle j| \otimes \rho_o, \tag{B.4}$$

where the coefficient is defined as

$$\beta_j = \alpha_{2,\nu}\alpha_{j,\mu} - \alpha_{2,\mu}\alpha_{j,\nu} = \frac{1}{q_{0,\mu}q_{0,\nu}q_{0,o}q_{0,o}2!j!} \int_{\mu,\nu,o,o'} f_{\mu}f_{\nu}f_{o}f_{o'} \frac{G(\mu,\nu,o,o',j)}{e^{\mu+\nu+o+o'}} d\mu d\nu do do'. \tag{B.5}$$

The polarity of β_j is determined by the numerators $G(\mu,\nu,o,o',j) \triangleq (\nu^2 - o'^2)(\mu^j - o^j) - (\mu^2 - o^2)(\nu^j - o'^j)$. It is easy to verify that $G(\mu,\nu,o,o',1) < 0$ and $G(\mu,\nu,o,o',2) = 0$ with the conditions in Eq. (B.15). This means that $\beta_1 < 0$ and $\beta_2 = 0$. The numerators of $g(\mu,\nu,o,o',j)$ can be re-expressed by changing the order of summation as $G(\mu,\nu,o,o',j) = (\nu^2 - o'^2)(\mu^j - o^j) - (\mu^2 - o'^2)(\nu^j - o^j)$. Note that

$$\frac{\mu^{j+1} - o^{j+1}}{\nu^{j+1} - o^{j+1}} - \frac{\mu^j - o^j}{\nu^j - o^j} = \frac{(\mu + o)(\nu + o)}{(\nu^{j+1} - o^{j+1})(\nu^j - o^j)} \times \sum_{k=0}^{j-1} o^{j-k-1}(\mu^j \nu^k - \nu^j \mu^k) \geq 0. \tag{B.6}$$

Hence we can prove that

$$\beta_{j+1} \geq \beta_j \times \min_{\nu,o} \left\{ \frac{\nu^j - o^j}{\nu^{j-1} - o^{j-1}} \right\}. \tag{B.7}$$

Based on the mathematical induction method, we can conclude that $\beta_j \geq 0$ when $j \geq 2$. Therefore, based on Eq. (B.4), the following operator dominance conditions is valid

$$|1\rangle\langle 1| \otimes \rho_o \geq \frac{\alpha_{2,\nu}\rho^\mu - \alpha_{2,\mu}\rho^\nu}{\beta_1} = \frac{\alpha_{2,\nu}\rho^\mu - \alpha_{2,\mu}\rho^\nu}{\alpha_{2,\nu}\alpha_{1,\mu} - \alpha_{2,\mu}\alpha_{1,\nu}}. \tag{B.8}$$

At the same time, it is easy to verify that $\alpha_{j,\nu} > 0$, hence the following operator dominance condition is valid

$$|1\rangle\langle 1| \otimes \rho_o \leq \frac{\rho^\nu}{\alpha_{1,\nu}}. \tag{B.9}$$

If the vacuum state is perfect, hence Eqs. (B.8) and (B.9) give the first two operator dominance conditions in Eq. (12). Actually, Eq. (B.9) is irrelevant of the form of the state ρ_o, we could obtain the following condition as

$$\rho_1^{z_0} \leq \frac{1}{q_{0,o}} \sum_{j=1}^{\infty} \alpha_{j,\nu} |j\rangle\langle j| \otimes q_{0,o}|0\rangle\langle 0| \leq \frac{\rho^\nu}{q_{0,o}\alpha_{1,\nu}}, \tag{B.10}$$

which gives the second condition in Eq. (12).

To prove the first condition in Eq. (12), we first give the operator inequalities for the (unnormalized) state $q_{0,o}|10\rangle\langle 10| + q_{1,o}|11\rangle\langle 11|$ according to Eqs. (B.8) and (B.9), which are shown as

$$\begin{aligned} \Upsilon_{o,0} &\triangleq (q_{0,o} + q_{1,o} - 1)\mathbb{I} + \frac{\alpha_{2,\nu}\rho^\mu - \alpha_{2,\mu}\rho^\nu}{\alpha_{2,\nu}\alpha_{1,\mu} - \alpha_{2,\mu}\alpha_{1,\nu}} \leq q_{0,o}|10\rangle\langle 10| + q_{1,o}|11\rangle\langle 11| \\ \Upsilon_{o,1} &\triangleq \sum_{(\tau_0,o)\in\Pi'} \beta'_{\tau_0 o,1}\kappa_{\tau_0} \otimes \kappa_o \geq q_{0,o}|10\rangle\langle 10| + q_{1,o}|11\rangle\langle 11|. \end{aligned} \tag{B.11}$$

If we prepare another decoy states with preset intensity ω to replace the vacuum states, we also could obtain the operator inequalities for the (unnormalized) state $q_{0,o}|10\rangle\langle 10| + q_{1,o}|11\rangle\langle 11|$ similar to Eq. (B.11) as $q_{0,\omega}|10\rangle\langle 10| + q_{1,\omega}|11\rangle\langle 11| \geq \Upsilon_{\omega,0}$ and $\leq \Upsilon_{\omega,1}$. Therefore, the following operator dominance condition holds

$$\rho_1^{z_0} \geq \frac{q_{1,\omega}\Upsilon_{o,0} - q_{1,o}\Upsilon_{\omega,1}}{q_{1,\omega}q_{0,o} - q_{1,o}q_{0,\omega}}, \tag{B.12}$$

which gives the first condition in Eq. (12). The reason that the estimation is tight is that $q_{0,o} + q_{1,o} - 1$ is close enough to 0.

As the vacuum state is nonessential for X basis, the last two operator dominance conditions in Eq. (12) can be directly obtained according to Eqs. (B.8) and (B.9) as

$$\begin{aligned} \rho_1^d &\geq \frac{\alpha_{2,\nu}\sigma^{\mu,d} - \alpha_{2,\mu}\sigma^{\nu,d}}{\alpha_{2,\nu}\alpha_{1,\mu} - \alpha_{2,\mu}\alpha_{1,\nu}}, \\ \rho_1^d &\leq \frac{\sigma^{\nu,d}}{\alpha_{1,\nu}}, \end{aligned} \tag{B.13}$$

where the operators are defined similarly to Eq. (B.3) as

$$\begin{aligned} \sigma^{\mu,d} &\triangleq \frac{\rho_\mu^d}{q_{0,\mu}} - \frac{\rho_o^d}{q_{0,o}}, \\ \sigma^{\nu,d} &\triangleq \frac{\rho_\nu^d}{q_{0,\nu}} - \frac{\rho_o^d}{q_{0,o}}. \end{aligned} \tag{B.14}$$

The simple and sufficient but not necessary conditions for the above analysis are that for any $\mu \in \Pi_\mu$, $\nu \in \Pi_\nu$, $o, o' \in \Pi_o$, and $\omega, \omega' \in \Pi_\omega$ the following formulas hold

$$\begin{aligned} \mu &> o, \\ \nu &> o, \\ \mu + o &> \nu + o', \\ \mu &> \omega, \\ \nu &> \omega, \\ \mu + \omega &> \nu + \omega'. \end{aligned} \tag{B.15}$$

In perfect QKD systems, the intensities are fixed satisfying $\mu > \nu > \omega > o$, and the conditions in Eq. (B.15) are trusted. However, the set $\Pi_\tau(\tau \in \{\mu, \nu, \omega, o\})$ becomes complex due to the intensity fluctuation. At this time, the conditions in Eq. (B.15) are still reasonable. Even in the case that Eq. (B.15) can not be satisfied, the invalidity is only due to a small portion of states. That is, considering the Gaussian distribution, the probability of preparing those states is small as the actual intensity deviates from the nominal intensity. And the contribution of those partial states is negligible. It is easy to verify the polarity of β_j and $\alpha_{j,\nu}$ based on the mathematical induction method. Considering the worst case that the polarity of β_j and $\alpha_{j,\nu}$ do not satisfy the above analysis, we could optimize the intensities in advance.

Appendix C: Simulation method

We give the simulation method for $\mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^z_{\tau_3,\tau_4})]$, $\mathrm{Tr}[\hat{C}_i(\rho^z_{\tau_1,\tau_2} \otimes \rho^x_{\tau})]$, $\mathrm{Tr}[\hat{C}_i(\rho^x_{\tau} \otimes \rho^z_{\tau_3,\tau_4})]$, and $\mathrm{Tr}[\hat{C}_i(\rho^x_{\tau} \otimes \rho^x_{\tau'})]$ in Eqs. (16), (17), (18), and (19). As their are two bins, we define a unified definition as $Q^{zz(zx,xz,xx)}_{\tau_{a_1}\tau_{a_2},\tau_{b_1}\tau_{b_2}}$, where (τ_{a_1}, τ_{a_2}) and (τ_{b_1}, τ_{b_2}) are Alice and Bob's intensity choices in two bins, and the superscript denotes the bases. The counting rate can

be simulated as

$$\begin{aligned} Q^{zz(zx,xz,xx)}_{\tau_{a_1}\tau_{a_2},\tau_{b_1}\tau_{b_2}} &= \mathrm{Int}_{\tau_{a_1},\tau_{a_2},\tau_{b_1},\tau_{b_2},\theta,\vartheta}\left\{e^{-L(\tau_{a_1},\tau_{b_1},\theta)}(1-p_d)\right. \\ &\times [1-e^{-R(\tau_{a_1},\tau_{b_1},\theta)}(1-p_d)] \times [1-e^{-L(\tau_{a_2},\tau_{b_2},\vartheta)}(1-p_d)] \\ &+ [1-e^{-L(\tau_{a_1},\tau_{b_1},\theta)}(1-p_d)] \times e^{-R(\tau_{a_1},\tau_{b_1},\theta)}(1-p_d) \\ &\times \left.[1-e^{-R(\tau_{a_2},\tau_{b_2},\vartheta)}(1-p_d)]\right\}, \end{aligned} \tag{C.1}$$

where Int denotes the integral and the probability density functions are omitted, and we have defined that

$$\begin{aligned} L(\tau_a,\tau_b,\theta) &= \frac{\eta}{2}(\tau_a+\tau_b)+\eta\sqrt{\tau_a\tau_b}\cos\theta, \\ R(\tau_a,\tau_b,\theta) &= \frac{\eta}{2}(\tau_a+\tau_b)-\eta\sqrt{\tau_a\tau_b}\cos\theta. \end{aligned} \tag{C.2}$$

Here, $\theta,\vartheta\in[0,2\pi)$ for zz,zx,xz. But for xx, $\vartheta=\theta+\vartheta_a+\vartheta_b$, where ϑ_a,ϑ_b denotes the phase-encoding uncertainty. The counting rate $Q_{[\mu,\mu]}$ and the bit error rate E_z can be simulated as

$$\begin{aligned} Q_{[\mu,\mu]} &= p_0p_1Q^{zz}_{\mu_a o_a,\mu_b o_b}+p_0p_0Q^{zz}_{\mu_a o_a,o_b\mu_b}+p_1p_1Q^{zz}_{o_a\mu_a,\mu_b o_b}+p_1p_0Q^{zz}_{o_a\mu_a,o_b\mu_b}, \\ E_z &= \frac{1}{Q_z}(p_0p_1Q^{zz}_{\mu_a o_a,\mu_b o_b}+p_1p_0Q^{zz}_{o_a\mu_a,o_b\mu_b}). \end{aligned} \tag{C.3}$$

Author contributions

Y.L., Y.Z., Y.Z., X.J. and X. L. wrote the main manuscript text, and Y.L. and Y.Z.prepared Figs. 1-3. All authors reviewed the manuscript.

Funding information

This work was supported by National Key Research and Development Program of China (Grant No. 2020YFA0309702), Henan Science and Technology Major Project of the Department of Science & Technology of Henan Province (No. 241100210400), National Natural Science Foundation of China (Nos. U2130205, 62101597), and Natural Science Foundation of Henan (No. 242300421219).

Data availability

No datasets were generated or analysed during the current study.

Declarations

Competing interests

The authors declare no competing interests.

Received: 27 April 2025 Accepted: 12 August 2025 Published online: 25 August 2025

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
2. Xu F, Ma X, Zhang Q, Lo H-K, Pan J-W. Secure quantum key distribution with realistic devices. Rev Mod Phys. 2020;92(2):025002.
3. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira JL, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko VC, Vallone G, Villoresi P, Wallden P. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012–236.
4. Portmann C, Renner R. Security in quantum cryptography. Rev Mod Phys. 2022;94(2):025008.
5. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett. 2012;108(13):130503.
6. Braunstein SL, Pirandola S. Side-channel-free quantum key distribution. Phys Rev Lett. 2012;108(13):130502.
7. Tang YL, Yin HL, Chen SJ, Liu Y, Zhang WJ, Jiang X, Zhang L, Wang J, You LX, Guan JY, Yang DX, Wang Z, Liang H, Zhang Z, Zhou N, Ma X, Chen TY, Zhang Q, Pan JW. Field test of measurement-device-independent quantum key distribution. IEEE J Sel Top Quantum Electron. 2015;21(3):116–22.

8. Yin H-L, Chen T-Y, Yu Z-W, Liu H, You L-X, Zhou Y-H, Chen S-J, Mao Y, Huang M-Q, Zhang W-J, Chen H, Li MJ, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X-B, Pan J-W. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett. 2016;117(19):190501.
9. Comandar LC, Lucamarini M, Fröhlich B, Dynes JF, Sharpe AW, Tam SWB, Yuan ZL, Penty RV, Shields AJ. Quantum key distribution without detector vulnerabilities using optically seeded lasers. Nat Photonics. 2016;10(5):312–5.
10. Liu H, Wang W, Wei K, Fang X-T, Li L, Liu N-L, Liang H, Zhang S-J, Zhang W, Li H, You L, Wang Z, Lo H-K, Chen T-Y, Xu F, Pan J-W. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. Phys Rev Lett. 2019;122(16):160501.
11. Bacco D, Vagniluca I, Da Lio B, Biagi N, Della Frera A, Calonico D, Toninelli C, Cataliotti FS, Bellini M, Oxenløwe LK, Zavatta A. Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area. EPJ Quantum Technol. 2019;6(1):5.
12. Wei K, Li W, Tan H, Li Y, Min H, Zhang W-J, Li H, You L, Wang Z, Jiang X, Chen T-Y, Liao S-K, Peng C-Z, Xu F, Pan J-W. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys Rev X. 2020;10(3):031030.
13. Semenenko H, Sibson P, Hart A, Thompson MG, Rarity JG, Erven C. Chip-based measurement-device-independent quantum key distribution. Optica. 2020;7(3):238–42.
14. Cao L, Luo W, Wang YX, Zou J, Yan RD, Cai H, Zhang Y, Hu XL, Jiang C, Fan WJ, Zhou XQ, Dong B, Luo XS, Lo GQ, Wang YX, Xu ZW, Sun SH, Wang XB, Hao YL, Jin YF, Kwong DL, Kwek LC, Liu AQ. Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems. Phys Rev Appl. 2020;14(1):011001.
15. Lowndes D, Frick S, Hart A, Rarity J. A low cost, short range quantum key distribution system. EPJ Quantum Technol. 2021;8(1):15.
16. Hwang WY. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91(5):057901.
17. Lo HK, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94(23):230504.
18. Wang X-B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett. 2005;94(23):230503.
19. Liao S-K, Cai W-Q, Liu W-Y, Zhang L, Li Y, Ren J-G, Yin J, Shen Q, Cao Y, Li Z-P, Li F-Z, Chen X-W, Sun L-H, Jia J-J, Wu J-C, Jiang X-J, Wang J-F, Huang Y-M, Wang Q, Zhou Y-L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y-A, Liu N-L, Wang X-B, Zhu Z-C, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43–7.
20. Wei K, Li W, Tan H, Li Y, Min H, Zhang W-J, Li H, You L, Wang Z, Jiang X, Chen T-Y, Liao S-K, Peng C-Z, Xu F, Pan J-W. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys Rev X. 2020;10(3):031030.
21. Li W, Zhang L, Tan H, Lu Y, Liao S-K, Huang J, Li H, Wang Z, Mao H-K, Yan B, Li Q, Liu Y, Zhang Q, Peng C-Z, You L, Xu F, Pan J-W. High-rate quantum key distribution exceeding 110 mb s-1. Nat Photonics. 2023;17(5):416–21.
22. Lucamarini M, Patel KA, Dynes JF, Fröhlich B, Sharpe AW, Dixon AR, Yuan ZL, Penty RV, Shields AJ. Efficient decoy-state quantum key distribution with quantified security. Opt Express. 2013;21(21):24550–65.
23. Fröhlich B, Lucamarini M, Dynes JF, Comandar LC, Tam WWS, Plews A, Sharpe AW, Yuan Z, Shields AJ. Long-distance quantum key distribution secure against coherent attacks. Optica. 2017;4(1):163–7.
24. Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe AW, Dixon AR, Lavelle E, Dynes JF, Murakami A, Kujiraoka M, Lucamarini M, Tanizawa Y, Sato H, Shields AJ. 10-mb/s quantum key distribution. J Lightwave Technol. 2018;36(16):3427–33.
25. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussières F, Li M-J, Nolan D, Martin A, Zbinden H. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121(19):190502.
26. Semenenko H, Sibson P, Hart A, Thompson MG, Rarity JG, Erven C. Chip-based measurement-device-independent quantum key distribution. Optica. 2020;7(3):238–42.
27. Fan-Yuan G-J, Lu F-Y, Wang S, Yin Z-Q, He D-Y, Chen W, Zhou Z, Wang Z-H, Teng J, Guo G-C, Han Z-F. Robust and adaptable quantum key distribution network without trusted nodes. Optica. 2022;9(7):812–23.
28. Grünenfelder F, Boaron A, Resta GV, Perrenoud M, Rusca D, Barreiro C, Houlmann R, Sax R, Stasi L, El-Khoury S, Hänggi E, Bosshard N, Bussières F, Zbinden H. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. Nat Photonics. 2023;17(5):422–6.
29. Huang A, Mizutani A, Lo H-K, Makarov V, Tamaki K. Characterization of state-preparation uncertainty in quantum key distribution. Phys Rev Appl. 2023;19(1):014048.
30. Gottesman D, Lo H-K, Lütkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. Quantum Inf Comput. 2004;4(5):325–60.
31. Nagamatsu Y, Mizutani A, Ikuta R, Yamamoto T, Imoto N, Tamaki K. Security of quantum key distribution with light sources that are not independently and identically distributed. Phys Rev A. 2016;93(4):042325.
32. Mizutani A, Kato G, Azuma K, Curty M, Ikuta R, Yamamoto T, Imoto N, Lo H-K, Tamaki K. Quantum key distribution with setting-choice-independently correlated light sources. npj Quantum Inf. 2019;5(1):8.
33. Tamaki K, Curty M, Kato G, Lo H-K, Azuma K. Loss-tolerant quantum cryptography with imperfect sources. Phys Rev A. 2014;90(5):052314.
34. Xu F, Wei K, Sajeed S, Kaiser S, Sun S, Tang Z, Qian L, Makarov V, Lo H-K. Experimental quantum key distribution with source flaws. Phys Rev A. 2015;92(3):032305.
35. Mizutani A, Curty M, Lim CCW, Imoto N, Tamaki K. Finite-key security analysis of quantum key distribution with imperfect light sources. New J Phys. 2015;17(9):093011.
36. Tang Z, Wei K, Bedroya O, Qian L, Lo H-K. Experimental measurement-device-independent quantum key distribution with imperfect sources. Phys Rev A. 2016;93(4):042308.
37. Bourassa JE, Primaatmaja IW, Lim CCW, Lo H-K. Loss-tolerant quantum key distribution with mixed signal states. Phys Rev A. 2020;102(6):062607.
38. Li H-W, Hao C-P, Chen Z-J, Gong L, Lu Y-F, Wang Y, Li J-J, Zhang C-M, Wang R, Yin Z-Q, Cai Q-Y. Security of quantum key distribution with virtual mutually unbiased bases. Sci China, Phys Mech Astron. 2024;67(7):270313.

39. Yin Z-Q, Fung C-HF, Ma X, Zhang C-M, Li H-W, Chen W, Wang S, Guo G-C, Han Z-F. Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources. Phys Rev A. 2014;90(5):052319.
40. Wang C, Wang S, Yin Z-Q, Chen W, Li H-W, Zhang C-M, Ding Y-Y, Guo G-C, Han Z-F. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding. Opt Lett. 2016;41(23):5596–9.
41. Hwang W-Y, Su H-Y, Bae J. Improved measurement-device-independent quantum key distribution with uncharacterized qubits. Phys Rev A. 2017;95(6):062313.
42. Zhu J-R, Wu W-Z, Ji L, Zhang C-M, Wang Q. Experimental quantum key distribution with uncharacterized sources and projective measurements. Opt Lett. 2019;44(23):5703–6.
43. Lu F-Y, Wang Z-H, Yin Z-Q, Wang S, Wang R, Fan-Yuan G-J, Huang X-J, He D-Y, Chen W, Zhou Z, Guo G-C, Han Z-F. Unbalanced-basis-misalignment-tolerant measurement-device-independent quantum key distribution. Optica. 2022;9(8):886–93.
44. Wang X-B. Decoy-state quantum key distribution with large random errors of light intensity. Phys Rev A. 2007;75(5):052301.
45. Wang X-B, Yang L, Peng C-Z, Pan J-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. New J Phys. 2009;11(7):075006.
46. Li Y, Bao W-s, Li H-w, Zhou C, Wang Y. Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations. Phys Rev A. 2014;89(3):032329.
47. Jiang C, Yu Z-W, Hu X-L, Wang X-B. Robust twin-field quantum key distribution through sending or not sending. Natl. Sci. Rev. 2022;10(4).
48. Hu X-L, Jiang C, Yu Z-W, Wang X-B. Sending-or-not-sending twin field quantum key distribution with imperfect vacuum sources. New J Phys. 2022;24(6):063014.
49. Jiang C, Yu Z-W, Hu X-L, Wang X-B. Side-channel-free quantum key distribution with practical devices. arXiv:2205.08421v3 (2022).
50. Wang J, Liu H, Ma H, Sun S. Experimental study of four-state reference-frame-independent quantum key distribution with source flaws. Phys Rev A. 2019;99(3):032309.
51. Zhou X-Y, Ding H-J, Zhang C-H, Li J, Zhang C-M, Wang Q. Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources. Opt Lett. 2020;45(15):4176–9.
52. Maeda K, Sasaki T, Koashi M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. Nat Commun. 2019;10(1):3140.
53. Ma X, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution. Phys Rev A. 2012;86(6):062319.
54. Curty M, Xu F, Cui W, Lim CCW, Tamaki K, Lo H-K. Finite-key analysis for measurement-device-independent quantum key distribution. Nat Commun. 2014;5(1):3732.
55. Koashi M. Complementarity, distillable secret key, and distillable entanglement. arXiv: Quantum Phys. 2007.
56. Koashi M. Simple security proof of quantum key distribution based on complementarity. New J Phys. 2009;11(4):045018.
57. Pereira M, Curty M, Tamaki K. Quantum key distribution with flawed and leaky sources. npj Quantum Inf. 2019;5(1):62.
58. Gnanapandithan A, Qian L, Lo H-K. Hidden multidimensional modulation side channels in quantum protocols. Phys Rev Lett. 2025;134(13):130802.
59. Yoshino K-i, Fujiwara M, Nakata K, Sumiya T, Sasaki T, Takeoka M, Sasaki M, Tajima A, Koashi M, Tomita A. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. npj Quantum Inf. 2018;4(1):8.
60. Pereira M, Kato G, Mizutani A, Curty M, Tamaki K. Quantum key distribution with correlated sources. Sci Adv. 2020;6(37):4487.
61. Jiang M-S, Sun S-H, Li C-Y, Liang L-M. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. Phys Rev A. 2012;86(3):032310.
62. Huang A, Sun S-H, Liu Z, Makarov V. Quantum key distribution with distinguishable decoy states. Phys Rev A. 2018;98(1):012330.
63. Pereira M, Currás-Lorenzo G, Navarrete A, Mizutani A, Kato G, Curty M, Tamaki K. Modified bb84 quantum key distribution protocol robust to source imperfections. Phys Rev Res. 2023;5(2):023065.
64. Trefilov D, Sixto X, Zapatero V, Huang A, Curty M, Makarov V. Intensity correlations in decoy-state bb84 quantum key distribution systems. arXiv:2411.00709v1 (2024).
65. Pereira M, Currás-Lorenzo G, Mizutani A, Rusca D, Curty M, Tamaki K. Quantum key distribution with unbounded pulse correlations. Quantum Sci Technol. 2025;10(1):015001.
66. Marcomini A, Currás-Lorenzo G, Rusca D, Valle A, Tamaki K, Curty M. Characterising higher-order phase correlations in gain-switched laser sources with application to quantum key distribution. EPJ Quantum Technol. 2025;12(1):38.

Publisher's note