OPTICA

Unbalanced-basis-misalignment-tolerant measurement-device-independent quantum key distribution

Feng-Yu Lu,[1,2,3,5,†] Ze-Hao Wang,[1,2,3,†] Zhen-Qiang Yin,[1,2,3,6] Shuang Wang,[1,2,3,7] Rong Wang,[1,2,4] Guan-Jie Fan-Yuan,[1,2,3] Xiao-Juan Huang,[1,2,3] De-Yong He,[1,2,3] Wei Chen,[1,2,3] Zheng Zhou,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China
[2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
[3]State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China
[4]Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong SAR, China
[5]e-mail: luffy196@mail.ustc.edu.cn
[6]e-mail: yinzq@ustc.edu.cn
[7]e-mail: wshuang@ustc.edu.cn

Received 20 January 2022; revised 9 July 2022; accepted 12 July 2022; published 3 August 2022

Measurement-device-independent quantum key distribution (MDIQKD) is a revolutionary protocol since it is physically immune to all attacks on the detection side. However, the protocol still keeps the strict assumptions on the source side that specify that the four BB84 states must be perfectly prepared to ensure security. Some protocols release part of the assumptions in the encoding system to keep the practical security, but the performance would be dramatically reduced. In this work, we present a MDIQKD protocol that requires less knowledge of the encoding system to combat the troublesome modulation errors and fluctuations. We have also experimentally demonstrated the protocol. The result indicates a high performance and good security for practical applications. Its robustness and flexibility also exhibit a good value for complex scenarios such as the QKD networks.

https://doi.org/10.1364/OPTICA.454228

1. INTRODUCTION

Quantum key distribution (QKD) [1] allows two remote users, named Alice and Bob, to share secret random keys because of the information-theoretical security guaranteed by principles of quantum physics [2–6], even if there is an eavesdropper, who is named Eve. Unfortunately, practical QKD systems still suffer from troublesome attacks [7–11] rooted in the gaps between theoretical models and practical setups. The device-independent quantum key distribution (DIQKD) [12] is intrinsically immune to all side-channel attacks, but not practically usable due to its exorbitant demand for the detection efficiency and channel loss. As an alternative, some protocols [13,14] are proposed to remove all side channels on the vulnerable detection side. The measurement-device-independent quantum key distribution (MDIQKD) [14] is naturally immunes to all detection-side-channel attacks [7–9] while maintaining a comparable performance [15,16] compared to the regular prepare-and-measure QKD systems. The MDIQKD has received extensive attention since it offers a perfect balance between security and practicality.

The good properties of the MDIQKD have aroused widespread interest in recent years [15–26]. However, a fly in the ointment is that the security of the MDIQKD relies on the assumption that Alice and Bob can fully control their source side and perfectly prepare the four ideal BB84 states [1,27], which still impedes the unconditional security and hinders practical application. In practical systems, the preparation of the four states usually relies on the accurate modulation [15,16,28–31], which is still a great challenge due to the unbalanced path loss of interferometers [27], the limited precision of modulation signals, insufficient system bandwidth, errors in calibration, and the effects of various environments [32–35]. When the prepared states in MDIQKD are nonideal BB84 states, users can not accurately estimate the information leakage anymore since the important security assumption that "the density matrices of Z and X base should be indistinguishable" is broken. Indeed, the encoders can be calibrated in advance, but the cumbersome calibrations would unavoidably increase the experimental difficulty. Besides, it may introduce additional loopholes [36].

Some security proofs [27,37–49] successfully remove part of the demands in the coding system and greatly improve the practical security of the MDIQKD. However, some of them are overly pessimistic in their estimates of the information-leakage bound, assuming that the protocol performance would dramatically decrease with the misalignment [27,38–41]. Some other proofs

require additional information about the maximum misalignment [42,43,49] or previous characterization of the states [46–48], which may increase the experimental complexity. To promote practical applications, in this work we propose a MDIQKD whose source-side restrictions are greatly reduced. In this protocol, the users prepare a general Z basis and a simplified X basis that could be unbalanced, which are common scenarios in practical time-bin phase-coding systems. The protocol has an invariable high performance against the X-basis imbalances, and maintains its security even if the phase reference frame between the two users is misaligned [50,51]. The prepared states of the X basis are mixed states, and the prepared states of the Z basis are also misaligned.

In this work, we first introduce our protocol with the ideal single-photon sources. After that, an improved analysis is proposed for the scenarios where the states in the Z basis are not pure. To make our protocol practically useful with the existing weak coherent sources, the decoy state method [52–54] also is designed and a joint study method [55–57] against the statistical fluctuation [58–62] is proposed. Finally, we built a time-bin phase-coding MDIQKD system to experimentally demonstrate this protocol in nonasymptotic cases. The 25 MHz system ran continuously to accumulate sufficient data in several scenarios with different imbalances. The results indicate that the protocol can tolerate large imbalances and confirm its security and feasibility to simplify the experimental system, which would be promising for practical application and network scenarios. The details of security proofs against the collective attack and the parameter estimations can be found in Supplement 1.

2. SINGLE-PHOTON PROTOCOL

In the original MDIQKD, the four BB84 states (in other words, $|0\rangle$ and $|1\rangle$ as the Z basis, and $|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$ as the X basis), are required [14]. Our protocol reduces the demands so that Alice and Bob can prepare an unbalanced X basis that satisfies

$$|\varphi_2\rangle = c_0|0\rangle + c_1|1\rangle,\ |\varphi_3\rangle = c_0|0\rangle - c_1|1\rangle,$$
$$|\varphi_2'\rangle = c_0'|0\rangle + c_1' e^{i\theta}|1\rangle,\ |\varphi_3'\rangle = c_0'|0\rangle - c_1' e^{i\theta}|1\rangle, \quad (1)$$

where $|\varphi_2\rangle$ and $|\varphi_3\rangle$ ($|\varphi_2'\rangle$ and $|\varphi_3'\rangle$) correspond to Alice's (Bob's) original $|+\rangle$ and $|-\rangle$, respectively, and θ denotes the phase-reference frame misalignment [50,51] between two users. We use β (β') to describe the imbalance misalignment of Alice (Bob), and the positive real number coefficients $c_0 = \cos(45° + \beta)$ and $c_1 = \sin(45° + \beta)$ ($c_0' = \cos(45° + \beta')$ and $c_1' = \sin(45° + \beta')$), respectively, where $\beta \in (-45°, 45°)$. The protocol has an invariant high performance with different β, and maintains its security when the reference-frame misalignment $\theta \neq 0$ and the states in the X basis are not pure due to modulation fluctuations. As a matter of fact, the prepared mixed states in X basis can be regarded as uncharacterized $|\varphi_2\rangle$ and $|\varphi_3\rangle$ in Eq. (1). The detail of proof can be found in Supplement 1.

In each turn, Alice (Bob) randomly selects one of the four states and sends it to untrusted Charlie to perform a measurement. Charlie publicly announces if he has measured a successful event. If Charlie is honest, he should do the Bell state measurement (BSM) and announce $|\psi^-\rangle = \frac{\sqrt{2}}{2}(|01\rangle - e^{i\theta}|10\rangle)$. Charlie may not perform the required measurement because he is unreliable and θ is an unknown value, but the property of the MDIQKD guarantees the protocol security and an appropriate θ can maximize the secret key rate.

Protocol Procedure

The following outline describes the protocol procedure:

1. Preparation. In each turn, Alice (Bob) randomly prepares quantum state $|0\rangle$, $|1\rangle$, $|\varphi_2\rangle$ and $|\varphi_3\rangle$ ($|0\rangle$, $|1\rangle$, $|\varphi_2'\rangle$ and $|\varphi_3'\rangle$) and sends it to the untrusted measurement unit Charlie. We define that the code basis (the Z basis) is selected when the user prepares $|0\rangle$ or $|1\rangle$ and the test basis (the unbalanced X basis) is selected if Alice (Bob) prepares $|\varphi_2\rangle$ or $|\varphi_3\rangle$ ($|\varphi_2'\rangle$ or $|\varphi_3'\rangle$).

2. Measurement. Charlie projects his received pulse-pair to the Bell-state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + e^{-i\theta}|1\rangle|0\rangle)$ and publicly announces success or failure in each turn. Alice and Bob generate their raw key bits according to Charlie's announcement

3. Sifting. After the above trial has been repeated enough times, Alice and Bob publicly announce their basis for each turn. If both of them select the code basis, they maintain the raw key bit. Otherwise the raw key bit is discarded. The remained raw key bits are named sifted key bits.

4. Parameter estimation. By sacrificing some of the data for public discussion, users estimate the single-photon yield q_{nm}. According to the q_{nm}, the users estimate the bit and phase error rate.

5. Error correction and security amplification. According to the estimated parameters above, Alice and Bob perform the error correction and security amplification to generate the secret key bits.

According to the announcement of success or failure, Alice and Bob record or discard the data. When the users have accumulated sufficient data, they sacrifice some of the data for public discussion to estimate the q_{nm}, which is defined as the yield when Alice codes $|\varphi_n\rangle$ and Bob codes $|\varphi_m'\rangle$. This is especially true when both Alice and Bob select the Z basis: The raw key bits are generated according to the data. Other data are used in parameter estimations. The positive real coefficients c_0, c_1, c_0', c_1' can be accurately calculated by

$$c_0 = \sqrt{\frac{q_{10}q_{T1} - q_{11}q_{T0}}{q_{01}q_{10} - q_{00}q_{11}}},\ c_1 = \sqrt{\frac{q_{01}q_{T0} - q_{00}q_{T1}}{q_{01}q_{10} - q_{11}q_{00}}},$$
$$c_0' = \sqrt{\frac{q_{01}q_{1T} - q_{11}q_{0T}}{q_{01}q_{10} - q_{00}q_{11}}},\ c_1' = \sqrt{\frac{q_{10}q_{0T} - q_{00}q_{1T}}{q_{01}q_{10} - q_{11}q_{00}}}, \quad (2)$$

where $q_{Tm} = \frac{q_{2m}+q_{3m}}{2}$, $q_{nT} = \frac{q_{n2}+q_{n3}}{2}$ ($n, m \in \{0, 1\}$).

The information leakage is bounded by $H(e_p)$, where the $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denotes the binary Shannon entropy function and e_p is the phase error rate of the Z basis, which is described as

$$e_p = \frac{1}{2} - \frac{(q_{23} + q_{32}) - (q_{22} + q_{33})}{8(q_{00} + q_{01} + q_{10} + q_{11})\, c_0 c'_0 c_1 c'_1}, \quad (3)$$

which is invariant as if the relation in Eq. (1) is met. In other words, Eve's information can be precisely bounded even if the X basis is unbalanced. We note that the e_p would jump to 0.5 in several extreme cases where the four quantum states are not different from each other. More details can be found in Supplement 1. The secret key rate (SKR) is described by the Shor–Preskill formula [3]

$$R = q_C(1 - H(e_p) - H(e_b)), \quad (4)$$

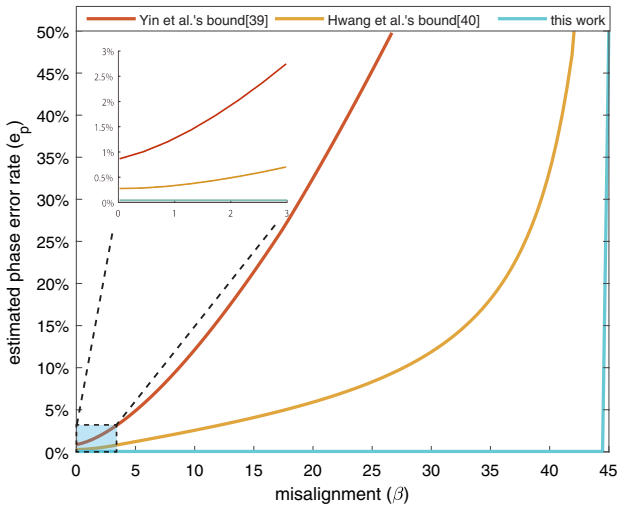

Fig. 1. Estimated phase error for several single-photon MDIQKDs versus the imbalance misalignment β. The performance of the uncharacterized qubits MDIQKDs reduced with the increasing β. In contrast, the performance of our protocol is nearly a constant value before approaching the extreme point that $\beta = 45°$. The simulation parameters are $P_d = 3 \times 10^{-6}$ (dark count rate), $P_\eta = 20\%$ (detection efficiency), and the transmission loss is 20 dB.

where $q_C = (q_{00} + q_{01} + q_{10} + q_{11})/4$ denotes the yield when Alice and Bob both select the Z basis, and the $e_b = (q_{00} + q_{11})/(q_{00} + q_{01} + q_{10} + q_{11})$ denotes the bit error rate when both of the users select the Z basis.

To demonstrate the property against the imbalance misalignment, we simulated our single-photon protocol and several ideal single-photon uncharacterized qubits MDIQKDs [39,40]. As illustrated in Fig. 1, the performance of the uncharacterized-qubit MDIQKDs decay with the increasing β (β'); in contrast, the performance of our protocol is invariant.

3. PROTOCOL WITH MIXED STATES

In practical systems, the prepared states could be mixed states due to modulation fluctuations. Our protocol can maintain its security in these mixed-state cases and we prove this property in two steps:

Test Basis. We first consider the scenario that the test basis is not pure. Here, we only introduce our key idea and the details of proof are in Supplement 1. Our key idea is proving that the mixed states in our test basis are equal to the uncharacterized states $|\varphi_2\rangle$ and $|\varphi_3\rangle$ with Eve's operation in the quantum channel.

We take Alice as an example, due to modulation fluctuations, the misalignment β is not a fixed value, but satisify the random distribution with the probability density function $P(\beta)$. The test basis can be described as mixed states

$$\rho_2 = \frac{1}{2}\left(\mathbb{I} + \hat{S}_X \sigma_X^\theta + \hat{S}_Z \sigma_Z\right),$$

$$\rho_3 = \frac{1}{2}\left(\mathbb{I} - \hat{S}_X \sigma_X^\theta + \hat{S}_Z \sigma_Z\right), \tag{5}$$

where σ_Z and σ_X^θ are Pauli matrices, $\mathbb{I}$ is the identity matrix, and $\hat{S}_Z$ ($\hat{S}_X$) denotes the Z (X) component of the prepared state in the Bloch sphere. The prepared state is a pure state if $\hat{S}_Z^2 + \hat{S}_X^2 = 1$ and a mixed state if $\hat{S}_Z^2 + \hat{S}_X^2 < 1$.

Defining Eve's operation

$$\varepsilon(\rho) = \lambda_0 \mathbb{I}\rho\mathbb{I} + \lambda_1 \sigma_Z \rho \sigma_Z, \tag{6}$$

which satisfies

$$\begin{cases} \lambda_0 + \lambda_1 = 1, \\ (\lambda_0 - \lambda_1)\sqrt{1 - \hat{S}_Z^2} = \hat{S}_X. \end{cases} \tag{7}$$

The ε can be intuitively regarded as Eve doing nothing with the probability λ_0 and performing the σ_Z operation with the probability λ_1. We then find that the ε satisfies

$$|0\rangle\langle 0| = \varepsilon(|0\rangle\langle 0|), \quad |1\rangle\langle 1| = \varepsilon(|1\rangle\langle 1|),$$

$$\rho_2 = \varepsilon(|\varphi_2\rangle\langle\varphi_2|), \quad \rho_3 = \varepsilon(|\varphi_3\rangle\langle\varphi_3|). \tag{8}$$

Therefore, the protocol security in the case where the test basis has modulation fluctuation equals to the security in the case where users prepare pure states $|0\rangle$, $|1\rangle$ and uncharacterized $|\varphi_2\rangle$, $|\varphi_3\rangle$ while Eve performs ε in the quantum channel. Noting that the operations in the quantum channel have nothing to do with security, we can claim that our protocol is secure in this scenario.

Code Basis. The code basis is usually well-aligned in practical time-bin phase coding systems so that the pure-state protocol is enough for most cases. However, if the Z basis is out of control due to the modulation error and fluctuation, we should consider an improved analysis. Here, we only introduce our key idea and offer more details in Supplement 1.

In this scenario, when Alice wants to prepare $|0\rangle$ ($|1\rangle$), she actually randomly prepares $\cos(\beta_0)|0\rangle + e^{i\theta}\sin(\beta_0)|1\rangle$ or $\cos(\beta_0)|0\rangle - e^{i\theta}\sin(\beta_0)|1\rangle$ ($\sin(\beta_1)|0\rangle + e^{i\theta}\cos(\beta_1)|1\rangle$ or $\sin(\beta_1)|0\rangle - e^{i\theta}\cos(\beta_1)|1\rangle$), where the randomness of "+" and "−" derive from Alice's random modulation of 0 or the π relative phase between the two time bins when selecting the code basis. In addition, because of the modulation fluctuations, the misalignment β_0 and β_1 are not fixed values, but are a random distribution with probability density functions $P_0(\beta_0)$ and $P_1(\beta_1)$. In other words, Alice actually prepares mixed states

$$\rho_0 = (1 - \xi)|0\rangle\langle 0| + \xi|1\rangle\langle 1|,$$

$$\rho_1 = \zeta|0\rangle\langle 0| + (1 - \zeta)|1\rangle\langle 1|. \tag{9}$$

The ξ and ζ are defined as the misalignment errors of Alice's $|0\rangle$ and $|1\rangle$.

Similarly, Bob's $|0\rangle$ and $|1\rangle$ are changed to

$$\rho_0' = (1 - \xi')|0\rangle\langle 0| + \xi'|1\rangle\langle 1|,$$

$$\rho_1' = \zeta'|0\rangle\langle 0| + (1 - \zeta')|1\rangle\langle 1|, \tag{10}$$

and the ξ' and ζ' are the misalignment errors of Bob's $|0\rangle$ and $|1\rangle$.

In the mixed-state scenario, the observable values are the mixed-state yields y_{nm} rather than q_{nm}. Our key idea is bounding the pure-state yields q_{nm} by the observed y_{nm} and the lower and upper bounds of the Z basis misalignments, namely; the υ^L and υ^U where $\upsilon \in \{\xi, \zeta, \xi', \zeta'\}$. Indeed, the misalignment errors are unknown values, but their lower and upper bounds can be estimated by previously calibration or be monitored by inserting a local single-photon detector (similar to the monitor SPD-Moni in Fig. 4). As far as the q_{nm} is bounded, the phase error e_p can be estimated similarly to the pure-state case.

We have also analyzed the decoy state method and the statistical fluctuation for the mixed-state scenarios. The details are provided in Supplement 1.

4. PROTOCOL WITH DECOY STATE METHOD

The above protocol is based on the ideal single-photon sources, which are still not practically available. Therefore, we propose a four-intensity, decoy state method to connect the theory with practice. In this section, we only analyze the asymptotic case where the data size is infinite; the nonasymptotic case that considers the statistical fluctuation [58] is introduced in Supplement 1.

In our method, Alice (Bob) prepares a phase randomized weak coherent pulse and randomly selects an intensity l (r) from a pre-decided set $\{\mu, \nu, \omega, o\}$ ($\{\mu', \nu', \omega', o\}$), where the μ (μ') is defined as the signal state and the others are defined as decoy states; the $o = 0$ is also named a vacuum state. If the signal state is selected, Alice (Bob) only selects the code basis. However, if other intensities are selected, they prepare the four quantum states just like the single-photon protocol. Alice and Bob record their data according to Charlie's announcement and sacrifice some of them to estimate the gains. They should publicly announce which intensity is selected. If both of them select the signal state, the recorded data would become the raw key bit. In other cases, they would announce which state is selected. According to their announcement, they can calculate the gains Q_{nm}^{lr}, where subscript nm denotes that Alice and Bob prepare $|\varphi_n\rangle$ and $|\varphi'_m\rangle$ ($|\varphi_0\rangle = |\varphi'_0\rangle = |0\rangle, |\varphi_1\rangle = |\varphi'_1\rangle = |1\rangle$), respectively, and the superscript lr denotes that Alice and Bob select, respectively, intensities l and r. With these Q_{nm}^{lr}, Alice and Bob can bound the single-photon yields tightly [37,52–56,63] so that the SKR can be described as

$$R = p_\mu p_{\mu'} \left[a_1^\mu b_1^\mu \underline{q}_C \left(1 - H(\bar{e}_p)\right) - Q_C^{\mu\mu} f H(E_C^{\mu\mu}) \right], \quad (11)$$

where the p_μ and p'_μ denote the probability of selecting the signal state, the $a_1^\mu = \mu e^{-\mu}$ ($b_1^\mu = \mu' e^{-\mu'}$) is the Poisson distribution probability for sending a single-photon state, the $Q_C^{\mu\mu}$ and $E_C^{\mu\mu}$ are, respectively, the observed gain and the observed error rate of the signal state pulse-pairs, $f = 1.16$ is the error correction efficiency, and the underline and overline are, respectively, the lower and upper bound.

Figure 2 shows the asymptotic SKR of the four-intensity, decoy state method. When the X basis is unbalanced, our protocol maintains an invariant result while other protocols may not work. The plots of our protocol with different imbalances are nearly overlapping with the original MDIQKD with perfect coding, which indicates higher robustness and better practicality of our protocol. Figure 3 shows the simulation of the unbalanced basis-misalignment tolerance. We can find that the asymptotic secret key rate is nearly invariant and the nonasymptotic secret key rate decreases slowly, which indicates that the asymptotic e_p is near invariant before closing to the extreme point and the nonasymptotic e_p is slightly affected by the unbalanced basis-misalignment β. The details of the nonasymptotic cases are introduced in Supplement 1.

It is worth noting that the analysis above is suitable for the pure-state scenario. The analysis for the mixed-state scenario is a little different, and the details can be found in Supplement 1.

5. EXPERIMENTAL DEMONSTRATION

We experimentally demonstrated our protocol in the nonasymptotic cases. The parameter estimation for the nonasymptotic cases is in Supplement 1. As illustrated in Fig. 4, our experimental setup consists of two identical legitimate users and an untrusted relay.

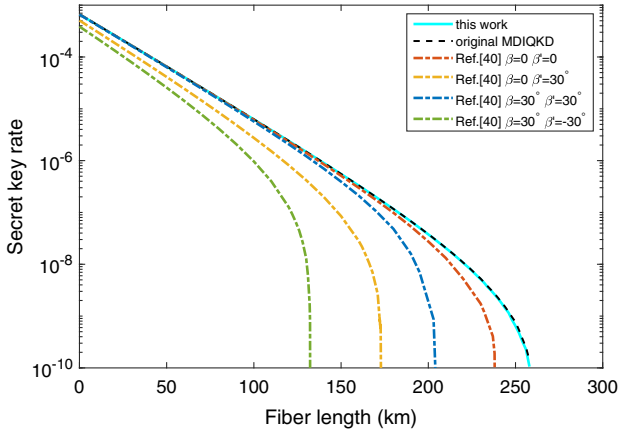

Fig. 2. SKR as a function of fiber length of different decoy state MDIQKDs in asymptotic cases. We simulated our protocol in many different combinations of β and β' and find that their asymptotic SKR are nearly indistinguishable in this figure so we only use a cyan solid line to represent our protocol with different β and β'. As a contrast, we simulate the asymptotic SKR of the original MDIQKD (black dashed line) without any misalignment ($\beta = \beta' = 0$). We can find that in an asymptotic case, our protocol with the imbalance misalignment has the same performance compared to the ideal original MDIQKD. We also simulated state-of-the-art uncharacterized qubits MDIQKD [40,41] (dot–dash line) with different β and β' and used lines in different colors to denote different imbalances. Red: $\beta = \beta' = 0$; Yellow: $\beta = 0$, $\beta' = 30°$; Blue: $\beta = 30°$, $\beta' = 30°$; and Green: $\beta = 30°$, $\beta' = -30°$. The simulation parameters are $P_d = 3 \times 10^{-6}$, $P_\eta = 20\%$, and the fiber loss is 0.2 dB/km.

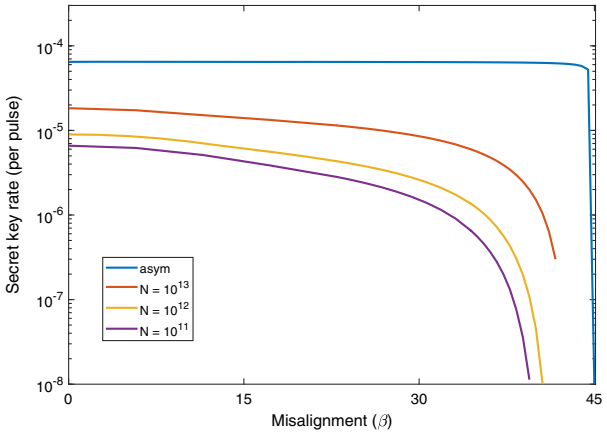

Fig. 3. Secret key rate as a function of the misalignment β in the decoy state cases. The blue line denotes the asymptotic case that the data size is infinite. The red, yellow, and purple lines denote the SKR with the data sizes, respectively, of 10^{13}, 10^{12}, and 10^{11}. The simulation parameters are $P_d = 3 \times 10^{-6}$, $P_\eta = 20\%$; the fiber length is 50 km; and the fiber loss is 0.2 dB/km. The failure probability ε using the Chernoff bound [64] is 5.73×10^{-7}.

Each of the legitimate users employs a CW laser (Wavelength References Clarity-NLL-1542-HP) that is frequency locked to a molecular absorption line of 1542.38 nm center wavelength. Then the CW lasers are chopped [28,29,41,65] into a 500 ps temporal width pulse sequence with a 25 MHz repetition by the intensity modulator IM-1, which is driven by a homemade narrow pulse generator. The phase modulator PM-1 next to the IM-1 actively

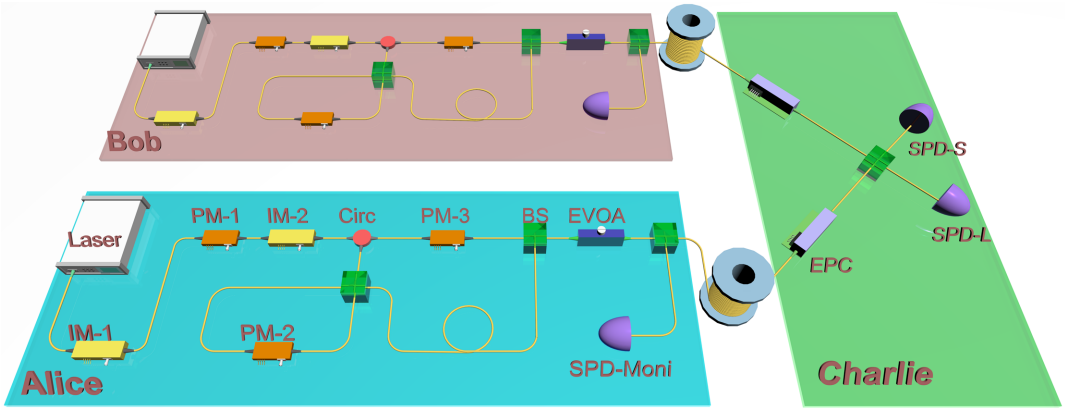

Fig. 4. Diagram of our experimental system. Laser, CW laser; IM, intensity modulator; PM, phase modulator; Circ, circulator; BS, beam splitter; EVOA, electric variable optical attenuator; EPC, electric polarization controller; and SPD, single-photon detector.

randomizes the phase of the pulses to avoid imperfect source attacks [66,67].

After that, the phase randomized coherent pulses are fed into the intensity modulator IM-2 to randomly modulate the four different intensities for our decoy state method. The IM-2 is driven by a homemade two-bit digital-to-analog converter (DAC) with a 25 Mb/s bitrate, and the digital pseudorandom numbers come from a driver board based on a field programmable gate array (FPGA) (PXIe-6547, National Instruments). In addition, when the vacuum state is selected, the IM-1 and IM-2 eliminate the pulse jointly to achieve a more than 50 dB extinction ratio.

Following the IM-2, a Sagnac interferometer connected to an asymmetric Mach–Zehnder structure (AMZS) that consists of a long and short path is employed to modulate the four quantum states. The PM-2 in the Sagnac interferometer allows users to modulate the interference of the Sagnac interferometer to switch the path. The constructive and destructive interference pipe the pulse into long and short paths, respectively, where the long path case denotes the late bin occupation $|0\rangle$ and the short path case denotes the early bin occupation $|1\rangle$. A medium interference would split the pulse into both of the paths to prepare a superposition of $|0\rangle$ and $|1\rangle$ so that the test basis is selected in this case. In the AMZS, a phase modulator PM-3 is inserted into the short path to modulate the relative phase of the two paths. The code of the test basis is defined as the relative phase of the two paths where 0 and π denote the $|\varphi_2\rangle$ and $|\varphi_3\rangle$, respectively. The PM-2 and the PM-3 are also driven by the homemade 2-bit DAC to randomly modulate the four quantum states where the digital random numbers also come from the FPGA-based driver board.

Finally, the pulses are attenuated to a single-photon level by an electric variable optical attenuator (EVOA) and split to two parts, one of which is measured by a local single-photon detector (SPD), and the results are recorded by the FPGA-based driver board to monitor the intensity of the four decoy states. According to the statistical result of the local SPD, users can adjust the EVOA and compensate for the DC drift of the IM-2 to keep the stability of the decoy states. The other part is sent to Charlie through a 25 km standard fiber for the BSM.

For the measurement unit Charlie, the two pulses interfere in the beam splitter (BS) and are detected by SPD-L and SPD-S (WT-SPD300, Anhui Qasky Quantum Technology) that work in the gated mode [68]. The BS and the two SPDs constitute a BSM device to project quantum states to the bell state $|\psi^-\rangle$ [14]. The two SPDs whose gate width, average efficiency, and dark count rate are 1 ns, 20.9%, and 3×10^{-6}, respectively, are triggered by 25 MHz gate signals, and the gate signals for SPD-L and SPD-S are aligned, respectively, with late bin occupation $|0\rangle$ and early bin occupation $|1\rangle$. The two electronic polarization controllers (EPCs) are employed to compensate for the polarization drift [28,69].

Table 1. Three Different Imbalances in Our Experiment

Imbalances	Alice's Imbalance β	Bob's Imbalance β'
case 1	0	0
case 2	0	10°
case 3	10°	10°

To demonstrate the imbalance tolerance, we experimentally demonstrate our protocol in three different imbalances, as listed in Table 1, and calculate the secret key rate by the analysis methods, respectively, for the pure-state case and mixed-state case. The system is continuously run to collect 5×10^{11} pulse pairs for the case of each imbalance. The improved four-intensity decoy state method against the effect of statistical fluctuation is proposed and employed for data processing, and the details are provded in Supplement 1). With the improved decoy state method, we successfully generate secret keys with SKRs of 1.10×10^{-6}, 7.37×10^{-7}, and 5.87×10^{-7} by the pure-state analysis method and SKRs of 8.56×10^{-7}, 6.39×10^{-7}, and 3.87×10^{-7} by the mixed-state analysis method. The maximum Z basis misalignment υ^U for the mixed-state analysis is set to 1%. We note that we process the data by two different analysis methods to generate the SKRs for the pure-state cases and the mixed-state cases.

Figure 5 illustrates the simulation of the nonasymptotic SKRs (only including the statistical fluctuation) and shows our experiment results in the enlarged subfigure. The experiment results indicate that the protocol maintains a good performance against the unbalanced basis in the nonasymptotic cases. In nonasymptotic cases, we can find that our protocol performance is worse than the original MDIQKD and the SKR decrease with the imbalance β and β'. The main reason is that our protocol estimates more quantities so that the impacts of the statistical fluctuations are more serious. A feasible solution for this problem is to improve the decoy state method [55–57,70]. Considering that our decoy state is primitive, the protocol performance could be further improved in following works.

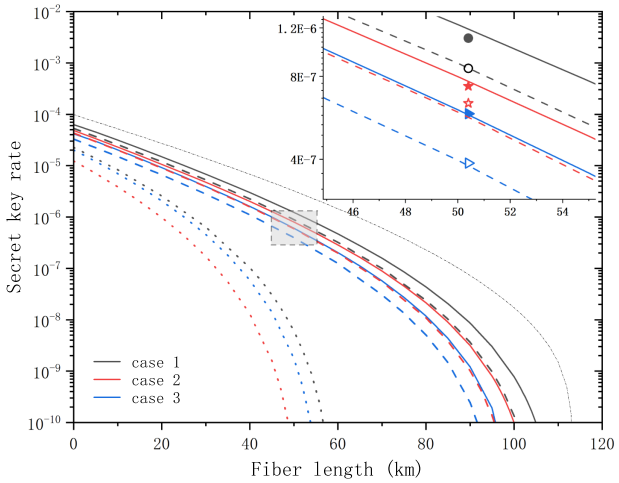

Fig. 5. Main figure illustrates nonasymptotic SKRs as the function of fiber length. The black, red, and blue denote the three different imbalances, as listed in Table 1. The solid lines and dash lines denote our protocol with the pure-state scenario and the mixed-state scenario. The dotted lines denote the state-of-the-art uncharacterized qubits MDIQKD [40] and the thin dash–dot line denotes the original MDIQKD without any imbalances. The simulation parameters are $P_d = 3 \times 10^{-6}$, $P_\eta = 20\%$; the data size $N = 5 \times 10^{11}$; the background error rate is 0.9%; the failure probability ε in using Chernoff bound [64] is fixed to 5.73×10^{-7}; the fiber loss is 0.2 dB/km; and the υ^L and υ^U for the mixed-state analysis are, respectively, 0 and 1%. The enlarged subfigure shows our experimental results. The solid geometries and hollow geometries denote the results, respectively, for the pure-state scenario and the mixed-state scenario.

6. DISCUSSION

In summary, we have proposed a MDIQKD that has the same performance compared to the original MDIQKD, but fewer assumptions in encoding systems are required. The new protocol has higher security since it is not only measurement device independent, but also is immune to some side-channel attacks that stem from the imperfect coding. In addition, it is more experimentally convenient since it simplifies the encoding system. We have successfully validated the protocol with a practical MDIQKD system, which is automatically calibrated and works continuously to collect sufficient data. We have collected 5×10^{11} pulse pairs in each of the three different imbalances and successfully generate a positive key rate. The performance would be further improved by employing a higher clockwork frequency, superconducting nanowire single-photon detectors, and improved decoy state methods. Due to the higher security, simpler coding method, and comparable key rate, this protocol would be beneficial for practical applications, especially in the scenarios where the precision of the control systems is limited or the calibration is difficult, such as the network scenarios. The performance in nonasymmetric scenarios could be further improved by designing more efficient decoy state methods or introducing better analysis for the finite-key size effect. This work would also provide inspiration to design protocols with fewer assumptions by combination with other protocols.

Funding. National Key Research and Development Program of China (2018YFA0306400); National Natural Science Foundation of China (61961136004, 62171424, 621714418); China Postdoctoral Science Foundation (2021M693098); Anhui Initiative in Quantum Information Technologies.

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

Supplemental document. See Supplement 1 for supporting content.

†These authors contributed equally to this paper.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, 1984), pp. 175–179.
2. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).
3. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
4. 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).
5. R. Renner, "Security of quantum key distribution," Int. J. Quantum Inf. **6**, 1–127 (2008).
6. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
7. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A **74**, 022313 (2006).
8. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).
9. 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).
10. X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, "Hacking quantum key distribution via injection locking," Phys. Rev. Appl. **13**, 034008 (2020).
11. A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, "Laser-damage attack against optical attenuators in quantum key distribution," Phys. Rev. Appl. **13**, 034017 (2020).
12. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).
13. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
14. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
15. Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over 200 km," Phys. Rev. Lett. **113**, 190501 (2014).
16. 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).
17. Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, and Q. Wang, "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett. **111**, 130502 (2013).
18. T. F. Da Silva, D. Vitoreti, G. B. Xavier, G. C. Do Amaral, G. P. Temporão, and J. P. Von Der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," Phys. Rev. A **88**, 052303 (2013).
19. S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," Nat. Photonics **9**, 397–402 (2015).
20. Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X.

Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Phys. Rev. X **6**, 011024 (2016).
21. L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nat. Photonics **10**, 312–315 (2016).
22. G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, "Experimental measurement-device-independent quantum digital signatures," Nat. Commun. **8**, 1098 (2017).
23. H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," Phys. Rev. Lett. **122**, 160501 (2019).
24. 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).
25. 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).
26. R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. L. Yuan, and A. J. Shields, "Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers," npj Quantum Inf. **7**, 58 (2021).
27. A. Ferenczi, V. Narasimhachar, and N. Lüitkenhaus, "Security proof of the unbalanced phase-encoded Bennett-Brassard 1984 protocol," Phys. Rev. A **86**, 042327 (2012).
28. C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, "Phase-reference-free experiment of measurement-device-independent quantum key distribution," Phys. Rev. Lett. **115**, 160502 (2015).
29. H. Liu, J. Wang, H. Ma, and S. Sun, "Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration," Optica **5**, 902–909 (2018).
30. 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).
31. X.-Y. Zhou, H.-J. Ding, M.-S. Sun, S.-H. Zhang, J.-Y. Liu, C.-H. Zhang, J. Li, and Q. Wang, "Reference-frame-independent measurement-device-independent quantum key distribution over 200 km of optical fiber," Phys. Rev. Appl. **15**, 064016 (2021).
32. K.-I. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses," npj Quantum Inf. **4**, 8 (2018).
33. G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution," Opt. Lett. **43**, 5110–5113 (2018).
34. F.-Y. Lu, X. Lin, S. Wang, G.-J. Fan-Yuan, P. Ye, R. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, G.-C. Guo, and Z.-F. Han, "Intensity modulator for secure, stable, and high-performance decoy-state quantum key distribution," npj Quantum Inf. **7**, 75 (2021).
35. W. Zhang, Y. Kadosawa, A. Tomita, K. Ogawa, and A. Okamoto, "State preparation robust to modulation signal degradation by use of a dual parallel modulator for high-speed BB84 quantum key distribution systems," Opt. Express **28**, 13965–13977 (2020).
36. N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, "Device calibration impacts security of quantum key distribution," Phys. Rev. Lett. **107**, 110501 (2011).
37. X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," Phys. Rev. A **87**, 012320 (2013).
38. Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution with uncharacterized qubit sources," Phys. Rev. A **88**, 062322 (2013).
39. Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources," Phys. Rev. A **90**, 052319 (2014).
40. W.-Y. Hwang, H.-Y. Su, and J. Bae, "Improved measurement-device-independent quantum key distribution with uncharacterized qubits," Phys. Rev. A **95**, 062313 (2017).
41. X.-Y. Zhou, H.-J. Ding, C.-H. Zhang, J. Li, C.-M. Zhang, and Q. Wang, "Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources," Opt. Lett. **45**, 4176–4179 (2020).
42. K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," Phys. Rev. A **90**, 052314 (2014).
43. Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, "Experimental measurement-device-independent quantum key distribution with imperfect sources," Phys. Rev. A **93**, 042308 (2016).
44. P. Zeng, W. Wu, and X. Ma, "Symmetry-protected privacy: beating the rate-distance linear bound over a noisy channel," Phys. Rev. Appl. **13**, 064013 (2020).
45. A. Jin, P. Zeng, R. V. Penty, and X. Ma, "Reference-frame-independent design of phase-matching quantum key distribution," Phys. Rev. Appl. **16**, 034017 (2021).
46. P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," Nat. Commun. **7**, 11712 (2016).
47. A. Winick, N. Lütkenhaus, and P. J. Coles, "Reliable numerical key rates for quantum key distribution," Quantum **2**, 77 (2018).
48. I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, "Versatile security analysis of measurement-device-independent quantum key distribution," Phys. Rev. A **99**, 062332 (2019).
49. J. E. Bourassa, I. W. Primaatmaja, C. C. W. Lim, and H.-K. Lo, "Loss-tolerant quantum key distribution with mixed signal states," Phys. Rev. A **102**, 062607 (2020).
50. A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," Phys. Rev. A **82**, 012304 (2010).
51. Z.-Q. Yin, S. Wang, W. Chen, H.-W. Li, G.-C. Guo, and Z.-F. Han, "Reference-free-independent quantum key distribution immune to detector side channel attacks," Quantum Inf. Process. **13**, 1237–1244 (2014).
52. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
53. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
54. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
55. 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).
56. 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).
57. F.-Y. Lu, Z.-Q. Yin, G.-J. Fan-Yuan, R. Wang, H. Liu, S. Wang, W. Chen, D.-Y. He, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, "Efficient decoy states for the reference-frame-independent measurement-device-independent quantum key distribution," Phys. Rev. A **101**, 052318 (2020).
58. X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," Phys. Rev. A **86**, 052305 (2012).
59. M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. Commun. **3**, 634 (2012).
60. 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).
61. C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," Phys. Rev. A **89**, 022307 (2014).
62. C. C. W. Lim, F. Xu, J.-W. Pan, and A. Ekert, "Security analysis of quantum key distribution with small block length and its application to quantum space communications," Phys. Rev. Lett. **126**, 100501 (2021).
63. Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, "Three-intensity decoy-state method for measurement-device-independent quantum key distribution," Phys. Rev. A **88**, 062339 (2013).

64. Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," Phys. Rev. A **95**, 012333 (2017).
65. 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).
66. S.-H. Sun, M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, "Partially random phase attack to the practical two-way quantum-key-distribution system," Phys. Rev. A **85**, 032304 (2012).
67. 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).
68. Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Robust countermeasure against detector control attack in a practical quantum key distribution system," Optica **6**, 1178–1184 (2019).
69. Y.-Y. Ding, W. Chen, H. Chen, C. Wang, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," Opt. Lett. **42**, 1023–1026 (2017).
70. 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).