CHINESE OPTICS LETTERS

Vol. 20, No. 9 | September 2022

Loss-tolerant measurement device independent quantum key distribution with reference frame misalignment

Jipeng Wang (王吉鹏), Zhenhua Li (李振华), Zhongqi Sun (孙仲齐), Tianqi Dou (窦天琦), Wenxiu Qu (屈文秀), Fen Zhou (周 芬), Yanxin Han (韩艳鑫), Yuqing Huang (黄雨晴), and Haiqiang Ma (马海强)*

School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

*Corresponding author: hqma@bupt.edu.cn

Received December 30, 2021 | Accepted May 10, 2022 | Posted Online June 21, 2022

Reference frame independent and measurement device independent quantum key distribution (RFI-MDI-QKD) has the advantages of being immune to detector side loopholes and misalignment of the reference frame. However, several former related research works are based on the unrealistic assumption of perfect source preparation. In this paper, we merge a loss-tolerant method into RFI-MDI-QKD to consider source flaws into key rate estimation and compare it with quantum coin method. Based on a reliable experimental scheme, the joint influence of both source flaws and reference frame misalignment is discussed with consideration of the finite-key effect. The results show that the loss-tolerant RFI-MDI-QKD protocol can reach longer key rate performance while considering the existence of source flaws in a real-world implementation.

Keywords: quantum key distribution; source flaw; measurement device independence.
DOI: 10.3788/COL202220.092701

1. Introduction

The first quantum key distribution (QKD) protocol, BB84 protocol[1], is proven secure in defending the formidable decryption ability in the approaching era of quantum computing[2–4]. In this decade, it is significant to narrow down the gap between ideal unconditional security and imperfect realistic devices. From the viewpoint of Eve, there are two main types of vulnerabilities to security, which are the light source at the transmitter and the detector at receiver[5–7]. As a countermeasure, the decoy state protocol can circumvent the photon number splitting attack, and a weak coherent source can be applied in QKD applications[8–10]. In addition, measurement device independent (MDI) protocol[11] can remove all the side channels' loopholes aiming at the measurement devices. Besides, MDI-QKD realizes a star-type quantum network and improves the ability of long distance transmission[12–14]. With the important practical prospect, it has been experimentally demonstrated to break through the 400 km fiber transmission[15] and applied in the chip-based platform as well as the free-space channel[16–19].

Reference frame misalignment is regarded as another inevitable problem of the QKD system, such as phase drift in the phase encoding scheme, which plays a severe negative role in disturbing the stable operation of QKD systems. By preparing and measuring the states by one more basis, the reference frame independent (RFI) protocol[20] is an effective solution to reduce the influence of reference frame misalignment on final key rates without extra requirements for a reference frame calibration device. Merging the advantages of the above two protocols, RFI-MDI-QKD is proposed[21] and experimentally demonstrated from the system clock 1 MHz to 50 MHz[22,23]. Recently, Zhou *et al.*[24] achieved the longest transmission distance of 200 km in a fiber system by combining the collective constraint and joint study strategy.

One of the assumptions in guaranteeing the security of MDI-QKD is the perfect preparation of quantum signals, which is not rigorous since perfect preparation devices in realistic scenarios do not exist. In Ref. [25], the impact of imperfect states is investigated in two types of phase encoding MDI-QKD schemes, and the rigorous estimation of secure key rates is given by the quantum coin (QC) method. Additionally, Ref. [26] proposed an improved and rigorous method to consider the basis dependent coding errors in MDI-QKD, where precise source coding can be loosened. Subsequently, the loss-tolerant (LT) protocol[27] proposed a more effective method to consider, but cut down the pessimistic impact source on secure key rate estimation. Reference [28] demonstrates the LT MDI-QKD experimentally as a compromised solution to balance the QKD's performance with the existence of source flaws. In this paper, we use the method of LT protocol to remove the perfect state assumption and investigate RFI-MDI-QKD with consideration of source flaw. Compared with the QC method, the comprehensive impact of both source flaw and reference frame misalignment

is analyzed numerically. Besides, we consider the finite-key analysis[26,29] in final key estimation and elaborate the protocol based on the feasible MDI-QKD application scheme to keep close combination of protocol theory and real-world practice.

2. Protocol

We introduce the RFI-MDI-QKD protocol based on the polarization multiplexing phase encoding scheme[23] illustrated in Fig. 1. The lasers of Alice and Bob sites emit the phase-randomized pulses with synchronized time and overlapped wavelength. Besides, the intensity of each laser pulse is modulated by the first intensity modulator (IM1), equiprobably and randomly, with three different intensities that are signal μ, decoy ν, and vacuum state 0, respectively. Then, a polarization multiplexing Mach–Zehnder interferometer (PMZI) is designed to split a single input pulse into two adjacent output pulses H and V with orthogonal polarization. Subsequently, phase modulators (PMs) and IMs are utilized for encoding. Particularly, bit 0 or 1 of the Z basis denoted by $|0_Z\rangle$ or $|1\rangle$ is prepared by suppressing pulse H or V via IM2. As for the X and Y basis, neither of the pulses H and V are suppressed. Meanwhile, the optical pulse V is modulated with the phase 0 or $\frac{\pi}{2}$ to prepare the bit 0 in the X or Y basis. Then, the encoded pulses are sent to the detector site (Charlie). A polarization controller (PC) is necessary to compensate for polarization drift due to the long transmission channel.

The role of Charlie is to detect a successful coincidence of quantum states, which are projected into the Bell state $|\Phi^{\pm}\rangle = \frac{|0_Z\rangle\otimes|0_Z\rangle\pm|1_Z\rangle\otimes|1_Z\rangle}{\sqrt{2}}$, $|\Psi^{\pm}\rangle = \frac{|0_Z\rangle\otimes|1_Z\rangle\pm|1_Z\rangle\otimes|0_Z\rangle}{\sqrt{2}}$, which corresponds to the case where they send the same or converse bit of the Z basis. $|\Phi^{\pm}\rangle$ cannot be distinguished and used for the key generation because two indistinguishable photons will meet at the beam splitter (BS) simultaneously, and Hong–Ou–Mandel (HOM) interference occurs[30]. However, for $|\Psi^{\pm}\rangle$, two photons arrive at the BS in different temporal windows, which leads to successful detection results, which are two different detectors triggered at that time. In the X or Y basis, $|\Psi^{+}\rangle$ can be detected when Alice and Bob share the same bit, while the detection result of $|\Psi^{-}\rangle$ corresponds to the preparation of the opposite bit. At the detection sites, Charlie announces which is the successful detection event of $|\Psi^{+}\rangle$ or $|\Psi^{-}\rangle$ via the classical channel, so Alice and Bob will know whether they have prepared the same bit ($i=j$) or should perform a bit flip to keep the bit in accordance with each other ($i\neq j$). After Alice and Bob announce to each other their basis α,β as well as their intensity choices $M_a, M_b \in \{\mu,\nu,0\}$, the detector result can be classified into correct gains and error gains, which is shown in Fig. 2. The estimation of gains $Q_{i\alpha,j\beta}^{M_aM_b}$, which denotes the gain when Alice and Bob send their states $|\phi_{i\alpha}\rangle$ and $|\phi_{j\beta}\rangle$, has been introduced explicitly now. In this paper, we apply the Chernoff bound method and consider statistical fluctuations into numerical simulation based on Refs. [22,23,26,29], The fluctuation range (upper and lower bounds) of the gain $Q_{i\alpha,j\beta}^{M_aM_b}$ with error probability $1-2\epsilon$ is given by

$$
\begin{aligned}
Q_{i\alpha,j\beta}^{M_aM_b,U} &= Q_{i\alpha,j\beta}^{M_aM_b}(1+\xi^{lr}),\\
Q_{i\alpha,j\beta}^{M_aM_b,L} &= Q_{i\alpha,j\beta}^{M_aM_b}(1-\xi^{lr}),\\
-\frac{f(\epsilon^{1.5})}{\sqrt{N^{M_aM_b}Q_{i\alpha,j\beta}^{M_aM_b}}} &\le \xi^{M_aM_b} \le \frac{f(\epsilon^4/16)}{\sqrt{N^{M_aM_b}Q_{i\alpha,j\beta}^{M_aM_b}}}.
\end{aligned}
\tag{1}
$$

Here, $f(x)=\sqrt{2\ln(x^{-1})}$ and $N^{M_aM_b}$ represents the total number of pulses that are sent from Alice and Bob with the

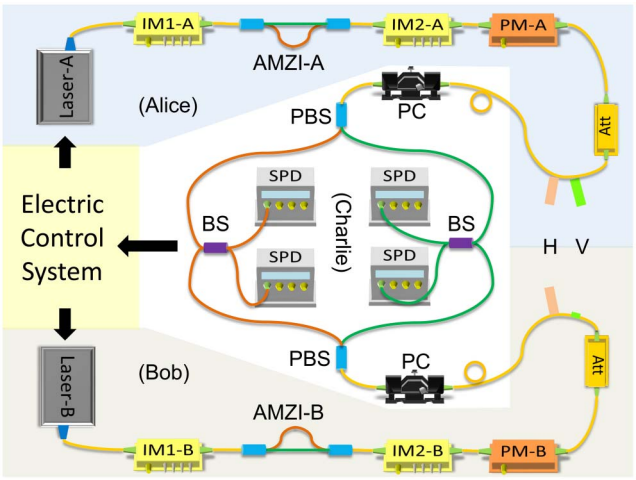

Fig. 1. Schematic diagram of phase encoding polarization multiplexing MDI-QKD protocol. BS, beam splitter; PBS, polarization beam splitter; PMZI, polarization-multiplexing Mach–Zehnder interferometer; PC, polarization controller and compensation. The polarization maintaining fibers separated by PBS are colored red and green to represent the orthogonal polarization H and V, respectively. The case is depicted by pulse H (red) and pulse V (green) when $|\phi_{0X}\rangle_A$ and $|\phi_{0Z}\rangle_B$ are prepared.

Case	DH0	DH1	DV0	DV1	Result
$\alpha=\beta=Z$ $i=j$		Click	Click		Error gain
	Click			Click	
	Click		Click		
		Click		Click	
$\alpha=\beta=Z$ $i\neq j$		Click	Click		Gain
	Click			Click	
	Click		Click		
		Click		Click	
$\alpha\neq\beta$ $i=j$		Click	Click		Error gain
	Click			Click	
	Click		Click		Gain
		Click		Click	
$\alpha\neq\beta$ $i\neq j$		Click	Click		
	Click			Click	
	Click		Click		Error gain
		Click		Click	

Fig. 2. Detector result. The figure illustrates how the double click of Charlie's site detector (DH0, DH1, DV0, DV1 shown in Fig. 1) corresponds to the gains or error rate, when Alice and Bob prepare their states $|\phi_{i\alpha}\rangle_A$ and $|\phi_{j\beta}\rangle_B$. The case is classified by their basis choices α,β and whether their bits are equal or not.

intensity choices M_a, M_b. Superscripts U and L indicate the upper and lower bounds of the corresponding quantity. Further, the corresponding single-photon yield $Y^{L(U)}_{i\alpha,j\beta}$ can be ranged by

$$
\begin{aligned}
Y^{L}_{i\alpha,j\beta} &= \frac{\mu_a^2\mu_b S_1 - \nu_a^2\nu_b S_2}{\mu_a\mu_b\nu_a\nu_b(\mu_a-\nu_a)},\\
S_1 &= Q^{\nu_a\nu_b,L}_{i\alpha,j\beta} e^{(\nu_a+\nu_b)} + Q^{0_a0_b,L}_{i\alpha,j\beta} - Q^{\nu_a0_b,U}_{i\alpha,j\beta} e^{\nu_a} - Q^{0_a\nu_b,U}_{i\alpha,j\beta} e^{\nu_b},\\
S_2 &= Q^{\mu_a\mu_b,U}_{i\alpha,j\beta} e^{(\mu_a+\mu_b)} + Q^{0_a0_b,U}_{i\alpha,j\beta} - Q^{\mu_a0_b,L}_{i\alpha,j\beta} e^{\mu_a} - Q^{0_a\mu_b,L}_{i\alpha,j\beta} e^{\mu_b},\\
Y^{U}_{i\alpha,j\beta} &= \frac{e^{(\nu_a+\nu_b)}Q^{0_a0_b,U}_{i\alpha,j\beta} + Q^{\nu_a\nu_b,U}_{i\alpha,j\beta} - e^{\nu_a}Q^{\nu_a0_b,L}_{i\alpha,j\beta} - e^{\nu_b}Q^{0_ab_b,L}_{i\alpha,j\beta}}{\nu_a\nu_b}.
\end{aligned}
\tag{2}
$$

Meanwhile, parts of gains are classified into error gains $EQ^{M_aM_b}_{\alpha\beta}$. As for the Z basis, $EQ^{\mu\mu}_{ZZ} = Q^{\mu\mu}_{0Z,0Z} + Q^{\mu\mu}_{1Z,1Z}$, and single-photon error rate $E^{11,U}_{\alpha\beta}$, we can see $E^{11,U(L)}_{ZZ} = \frac{Y^{U(L)}_{0Z,0Z}+Y^{U(L)}_{1Z,1Z}}{Y^{L(U)}_{0Z,0Z}+Y^{L(U)}_{1Z,1Z}+Y^{L(U)}_{1Z,0Z}+Y^{L(U)}_{0Z,1Z}}$. Similarly, the error rate of the other basis choice can find its lower or upper bound.

Above all, after $\lambda_{EC} = f_{EC}Q^{\mu\mu}_{ZZ}EQ^{\mu\mu}_{ZZ}$ is sacrificed for error correction, the final key of RFI-MDI-QKD can be bounded by[21,31]

$$
\begin{aligned}
R_L &= \mu_a\mu_b e^{-(\mu_a+\mu_b)}(1-I_E)\sum_{\alpha=\beta=Z} Y^{L}_{i\alpha,j\beta} - \lambda_{EC},\\
I_E &= (1-E^{11,U}_{ZZ})h\left(\frac{1+\nu_{\max}}{2}\right) + E^{11,U}_{ZZ}h\left[\frac{1+f(\nu_{\max})}{2}\right],\\
f(\nu_{\max}) &= \frac{\sqrt{\frac{C^L}{2} - (1-E^{11,U}_{ZZ})^2\nu^2_{\max}}}{E^{11,U}_{ZZ}},\\
\nu_{\max} &= \min\left(\frac{1}{1-E^{11,U}_{ZZ}}\sqrt{\frac{C^L}{2}}, 1\right).
\end{aligned}
\tag{3}
$$

Notice that $C^L = \sum_{\alpha,\beta\in\{X,Y\}}(1-2E^{11,L}_{\alpha\beta})^2$ is crucial, in which the RFI protocol takes effect and keeps the key rate vulnerable to the reference frame drift. When considering finite-key effect, the minimum of C is reckoned by choosing the corresponding $E^{11}_{\alpha\beta}$ value between its upper and lower bounds:

$$
C^L = \sum_{\alpha,\beta\in\{X,Y\}} \min:(1-2E^{11}_{\alpha\beta})^2, \text{ s.t. } \quad E^{11,L}_{\alpha\beta} \le E^{11}_{\alpha\beta} \le E^{11,U}_{\alpha\beta}.
\tag{4}
$$

When source flaws are considered, the phase error rate above $E^{11}_{\alpha\beta}$ is not simply the error rate derived from $Y_{i\alpha,j\beta}$ ($\alpha,\beta\in\{X,Y\}$) but given by the yield of fictitious or virtual states $Y^{\text{vir}}_{i\alpha,j\beta}$. Based on the LT protocol, the sending of Alice's states to Eve (Charlie) prepared in the Z basis can be equivalently written into the entanglement state, which is

$$
|\Psi_A\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle_{A1}\otimes|\phi_{0Z}\rangle_{A2E} + |1_Z\rangle_{A1}\otimes|\phi_{1Z}\rangle_{A2E}),
\tag{5}
$$

where $A1$, $A2$, and E are Alice's system to generate bit value, the extended system possessed by Alice, and the system sent to Eve, respectively. To be more understandable, the projective measurement is done on system $A1$ by the Z basis with a perfect outcome of bit 0 or 1. At the same time, the imperfect real state $|\phi_{1Z}\rangle$ or $|\phi_{0Z}\rangle$ is sent to Eve (Charlie). Now, consider a virtual protocol where system $A1$ is measured by the X or Y basis. In this case, a fictitious state $|\phi^{\text{vir}}_{j\alpha}\rangle$ ($\alpha,\beta\in\{X,Y\}$) sent to Eve is deduced, while $|\Psi_A\rangle$ can be rewritten by

$$
\begin{aligned}
|\Psi_A\rangle &= \frac{1}{\sqrt{2}}(|0_X\rangle_{A1}\otimes|\phi^{\text{vir}}_{0X}\rangle_{A2E} + |1_X\rangle_{A1}\otimes|\phi^{\text{vir}}_{1X}\rangle_{A2E}),\\
|\Psi_A\rangle &= \frac{1}{\sqrt{2}}(|0_Y\rangle_{A1}\otimes|\phi^{\text{vir}}_{0Y}\rangle_{A2E} + |1_Y\rangle_{A1}\otimes|\phi^{\text{vir}}_{1Y}\rangle_{A2E}).
\end{aligned}
\tag{6}
$$

Similarly, the fictitious state of Bob $|\phi^{\text{vir}}_{j\beta}\rangle$ can be also deduced as Alice's. Subsequently, the yields when Alice and Bob send their fictitious states can be expressed as

$$
Y^{\text{vir}}_{i\alpha,j\beta} = P^{\text{vir}}_{i\alpha}P^{\text{vir}}_{j\beta}[S^{i\alpha,\text{vir}}_{\sigma^A_t}(S^{j\beta,\text{vir}}_{\sigma^B_t})^T]\cdot q_{\sigma^A_t\otimes\sigma^B_t},
\tag{7}
$$

$$
\begin{aligned}
S^{i\alpha,\text{vir}}_{\sigma^A_t} &= [S^{i\alpha,\text{vir}}_{I^A}, S^{i\alpha,\text{vir}}_{X^A}, S^{i\alpha,\text{vir}}_{Y^A}, S^{i\alpha,\text{vir}}_{Z^A}],\\
S^{j\beta,\text{vir}}_{\sigma^B_t} &= [S^{j\beta,\text{vir}}_{I^B}, S^{j\beta,\text{vir}}_{X^B}, S^{j\beta,\text{vir}}_{Y^B}, S^{j\beta,\text{vir}}_{Z^B}],\\
q_{\sigma^A_t\otimes\sigma^B_t} &= [q_{I^A\otimes I^B}, q_{I^A\otimes X^B}, q_{I^A\otimes Y^B}, q_{I^A\otimes Z^B},\\
&\quad q_{X^A\otimes I^B}, q_{X^A\otimes X^B}, q_{X^A\otimes Y^B}, q_{X^A\otimes Z^B},\\
&\quad q_{Y^A\otimes I^B}, q_{Y^A\otimes X^B}, q_{Y^A\otimes Y^B}, q_{Y^A\otimes Z^B},\\
&\quad q_{Z^A\otimes I^B}, q_{Z^A\otimes X^B}, q_{Z^A\otimes Y^B}, q_{Z^A\otimes Z^B}].
\end{aligned}
\tag{8}
$$

Here, focusing on Alice, $P^{\text{vir}}_{i\alpha}$ denotes the probability of emitting Alice's fictitious state $|\phi^{\text{vir}}_{i\alpha}\rangle$ calculated by $\langle\Psi_A|(|\phi_{i\alpha}\rangle_A\langle\phi_{i\alpha}|_A\otimes Id)|\Psi_A\rangle$ that includes four elements, which is the Bloch vector of virtual states $|\phi^{\text{vir}}_{i\alpha}\rangle_A$ calculated by $\text{tr}(\sigma_t\rho^{\text{vir}}_{i\alpha})$, where $\rho^{\text{vir}}_{i\alpha}$ means the corresponding density matrix of state, and σ_t ($t\in\{I,X,Y,Z\}$) is Pauli matrices. For Bob, $S^{j\beta,\text{vir}}_{\sigma^B_t}$ and $P^{\text{vir}}_{j\beta}$ are deduced the same way. In the end, $q_{\sigma^A_t\otimes\sigma^B_t}$ indicates the transmission rate of $\sigma^A_t\otimes\sigma^B_t$ representing the composite system of transmission channels in the MDI-QKD protocol, which is Alice to Eve and Bob to Eve. Shown as Eq. (11) and elaborated in Section 3, the real state $|\phi_{1Z}\rangle$ or $|\phi_{0Z}\rangle$ can be quantified, which further implies $P^{\text{vir}}_{j\alpha}$, $P^{\text{vir}}_{j\beta}$, $S^{j\alpha,\text{vir}}_{\sigma^A_t}$, and $S^{j\beta,\text{vir}}_{\sigma^B_t}$ can also be quantified. However, $q_{\sigma^A_t\otimes\sigma^B_t}$ still remains unknown. The solution is to calculate them from the yield of actual states $Y_{i\alpha,j\beta}$ in a form similar to Eq. (9), which is

$$
q_{\sigma^A_t\otimes\sigma^B_t} = \frac{Y_{i\alpha,j\beta}}{P_{i\alpha}P_{j\beta}[S^{i\alpha}_{\sigma^A_t}(S^{j\beta}_{\sigma^B_t})^T]}.
\tag{9}
$$

The corresponding value for real states $P_{j\alpha}$, $P_{j\beta}$, $S^{j\alpha}_{\sigma^A_t}$, and $S^{j\beta}_{\sigma^B_t}$ can be quantified as well. Here, $q_{\sigma^A_t\otimes\sigma^B_t}$ can be regarded as an unknown 16-element aggregation. Therefore, only four states for the preparation of Alice and Bob, which are $i\alpha, j\beta\in(0Z, 1Z, 0X, 0Y)$, are sufficient to form a system of

linear equations to solve $q_{\sigma_t^A \otimes \sigma_t^B}$. As the mathematics relationship between the yield of actual and fictitious states implies, the yield of fictitious states can also find their bounds $Y_{i\alpha,j\beta}^{\mathrm{vir},L(U)}$ by substituting the upper and lower bounds $Y_{i\alpha,j\beta}^{L(U)}$ into Eq. (9). By this method, we could deduce fictitious phase error $E_{\alpha\beta}^{11,U(L)}(\alpha, \beta \in \{X,Y\})$ as well as corresponding C^L with the influence of source flaw and finite-key effect in the final key rate simulation.

3. Source Flaw

As the protocol requires, it is necessary to quantify $Q_{\alpha\beta}^{M_aM_b}$ while considering the source flaws and phase drift. In the following, the phase drift is denoted by ω characterizing the relationship between reference frames of the X and Y basis, which is $X_B = \cos\omega X_A + \sin\omega Y_A$ and $Y_B = \cos\omega Y_A - \sin\omega X_A$. Next, for the source flaw, $\delta_{1(2)}$ defines the deficiency in preparation of $|0(1)_Z\rangle$ and is mainly derived from the finite extinction ratio of IM2. In addition, δ_3 represents the imperfection due to asymmetrical attenuation between two arms of the PMZI. Also, $\theta_{1(2)}$ characterizes the imperfection of phase modulation on $|0_{X(Y)}\rangle$. The method to quantify the source flaws is to calibrate the derivation between a perfect preparation structure and an imperfect one. However, perfect modulation does not exist. Therefore, in the MDI-QKD protocol, a more rigorous approach is to quantify the source flaw of derivation between Alice and Bob rather than that of each site. It is equal to a situation where the Alice site is perfect, and all imperfections are attributed to the Bob site, which is actually the derivation of source flaw as well as the phase drift between Alice and Bob. In this way, the single-photon states of Alice are represented by

$$\begin{aligned}
&|\phi_{0Z}\rangle_A = |0_Z\rangle,\ |\phi_{1Z}\rangle_A = |1_Z\rangle,\\
&|\phi_{0X}\rangle_A = \frac{|0_Z\rangle + |1_Z\rangle}{\sqrt{2}} = |0_X\rangle,\\
&|\phi_{0Y}\rangle_A = \frac{|0_Z\rangle + i|1_Z\rangle}{\sqrt{2}} = |0_Y\rangle,
\end{aligned} \tag{10}$$

while Bob's are

$$\begin{aligned}
&|\phi_{0Z}\rangle_B = \cos(\delta_1)|0_Z\rangle + \sin(\delta_1)|1_Z\rangle,\\
&|\phi_{1Z}\rangle_B = \sin(\delta_2)|0_Z\rangle + \cos(\delta_2)|1_Z\rangle,\\
&|\phi_{0X}\rangle_B = \sin\left(\frac{\pi}{4}+\delta_3\right)|0_Z\rangle + \cos\left(\frac{\pi}{4}+\delta_3\right)e^{i(\theta_1+\omega)}|1_Z\rangle,\\
&|\phi_{0Y}\rangle_B = \sin\left(\frac{\pi}{4}+\delta_3\right)|0_Z\rangle + \cos\left(\frac{\pi}{4}+\delta_3\right)e^{i\left(\frac{\pi}{2}+\theta_2+\omega\right)}|1_Z\rangle.
\end{aligned} \tag{11}$$

Subsequently, the gains of detectors $Q_{H0(H1)}$ or $Q_{V0(V1)}$ are determined by the interference of coherent states arriving at BS1(2). Considering the case where both Alice and Bob prepare 0(1) bit in the Z basis, Alice's state with intensity μ_a arriving at BS1 and BS2 can be represented by $|e^{i\phi_a}\sqrt{\eta_a\mu_a}\rangle$ and zero. The total loss after the fiber channel distance L is estimated by $\eta_a = 10^{-\frac{\alpha L}{10}}\eta_{\mathrm{detector}}$, where α and η_{detector} denote the fiber channel attenuation coefficient and detector efficiency, respectively. For Bob, it corresponds to $|e^{i\phi_b}\sqrt{\eta_b\mu_b\sin^2(\delta_{1(2)})}\rangle$ and $|e^{i\phi_b}\sqrt{\eta_b\mu_b\cos^2(\delta_{1(2)})}\rangle$. As for the case when $|0_{X(Y)}\rangle$ is prepared by both sites, $|e^{i\phi_a}\sqrt{\eta_a\mu_a\cos^2\left(\frac{\pi}{4}\right)}\rangle$ and $|e^{i\phi_b}\sqrt{\eta_b\mu_b\cos^2(\frac{\pi}{4}+\delta_3)}\rangle$ represent the states at BS1. Meanwhile, $|e^{i(\phi_b+\theta_{1(2)}+\omega)}\sqrt{\eta_b\mu_b\sin^2(\frac{\pi}{4}+\delta_3)}\rangle$ and $|e^{i\phi_a}\sqrt{\eta_a\mu_a\sin^2\left(\frac{\pi}{4}\right)}\rangle$ arrive at BS2. According to Ref. [32], we define A ($\Delta\phi B$) as the coherent states of Alice (Bob) arriving at BS1(2), and, thus, the gains of corresponding detectors can be estimated by

$$\begin{aligned}
Q_0 &= \frac{1}{2\pi}\int_0^{2\pi} 1-(1-e_{\mathrm{dark}})\exp(-|A+e^{i\Delta\phi}B|^2)\mathrm{d}\Delta\phi,\\
Q_1 &= \frac{1}{2\pi}\int_0^{2\pi} 1-(1-e_{\mathrm{dark}})\exp(-|A+e^{i\pi}e^{i\Delta\phi}B|^2)\mathrm{d}\Delta\phi,
\end{aligned} \tag{12}$$

where e_{dark} characterizes the dark count rates of single-photon detectors. Additionally, the difference of randomized phase between Alice and Bob $\Delta\phi = \phi_a - \phi_b$ should be integrated over $[0, 2\pi)$. In the end, according to the meaning of each detector result shown in Fig. 2, $Q_{\alpha\beta}^{M_aM_b}$ could be estimated numerically in our simulation.

4. Analysis

In the beginning, the transmission performance of the RFI-MDI-QKD protocol by the LT and QC methods is illustrated in Fig. 3. For simplicity, δ_1,δ_2,δ_3 are assumed to be the same value δ, instead of being considered individually. It can be seen that, the key rate given by QC method[25] plunges more sharply with the distance, while the LT protocol achieves a much longer transmission distance, especially in the case of $\delta = 0.075$. When considering finite-key effect, LT can still keep its superiority, although the key rate and largest transmission distance shrink at smaller data size.

Then, the key rates at the fixed distance and $N^{M_aM_b}=10^{13}$ are studied in Fig. 4, where the X axis is source flaw δ and phase drift ω. To indicate the influence of δ and ω explicitly, there is only one variable for each key rate curve, in other words, phase drift is set to zero when the change of source flaw δ is investigated and vice versa. The discussion can be summarized into the following three points. (1) The decrease of key rates due to ω in the RFI-MDI-QKD protocol is very slight, which demonstrates its strong robustness against reference frame misalignment. Notice that source flaw θ is the imperfection of phase encoding and has the same effect of ω as Eq. (11) implies. Therefore, imperfect phase modulation θ can be tolerated as well. (2) The enlarging gap of key rates under the same source flaw and phase drift reveals that the LT protocol can provide better immunity at a longer transmission distance. (3) The tolerating limitations of source flaw δ are not finite. This is because the key rate is

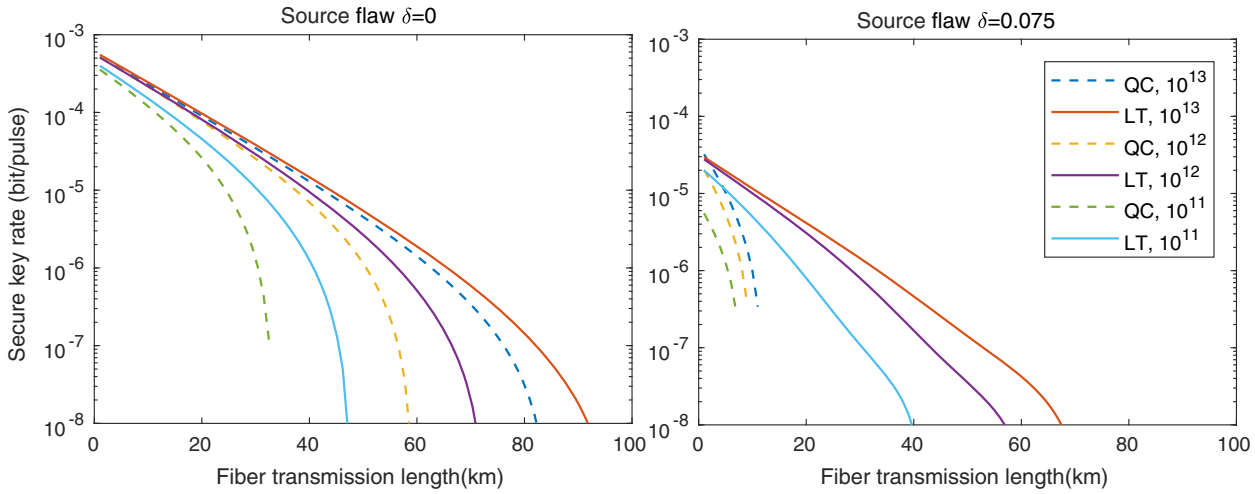

Fig. 3. Comparison of RFI-MDI-QKD with loss-tolerant (LT, solid line) and quantum coin (QC, dashed line) methods with different data sizes ($N^{M_aM_b} = 10^{11}, 10^{12}, 10^{13}$) and the source flaw ($\delta$ = 0 or 0.075). The intensities of signal and decoy states are optimized. Other simulation parameters are provided in Table 1.

Table 1. Simulation Parameter.

e_{dark}	f_{EC}	$N^{M_aM_b}$	ϵ	α	η_{detector}
1×10^{-7}	1.2	10^{13}	10^{-10}	0.2 dB/km	15%

restricted by growing λ_{EC} with the growth of δ. The upper bound $\delta = 0.09$ in our simulation has already covered the value of former experimental research[28].

The joint impact of both source flaws δ and phase drift ω on the LT RFI-MDI-QKD is presented by Fig. 5(a). It is noted that the key rate is symmetric about the phase drift of $\frac{\pi}{4}$. Concretely, the phase drift of $\frac{\pi}{4}$ leads to the severest error. However, the key rate cannot remain stable at δ near the tolerating limitation when the phase drift goes around $\frac{\pi}{4}$. In the end, to demonstrate the benefit of the RFI-QKD protocol more clearly, we also compare RFI-MDI-QKD with the original LT MDI-QKD protocol[28], where I_E is estimated directly by $h(E^{11}_{XX})$[28] in Fig. 5(b). Shown by their key rate ratio, the robustness superiority of RFI-MDI-QKD is obvious when phase drift happens to QKD systems.

5. Conclusion

In summary, we demonstrate the advantages of RFI-MDI-QKD and provide rigorous key rate estimation with source flaws under finite-key analysis. The protocol inherits the merits of four states preparation of the initial LT MDI-QKD protocol[27] compared to the previously reported six states RFI-MDI-QKD, which can evidently reduce the cost and complexity of the experimental system. Compared to Ref. [33] discussing

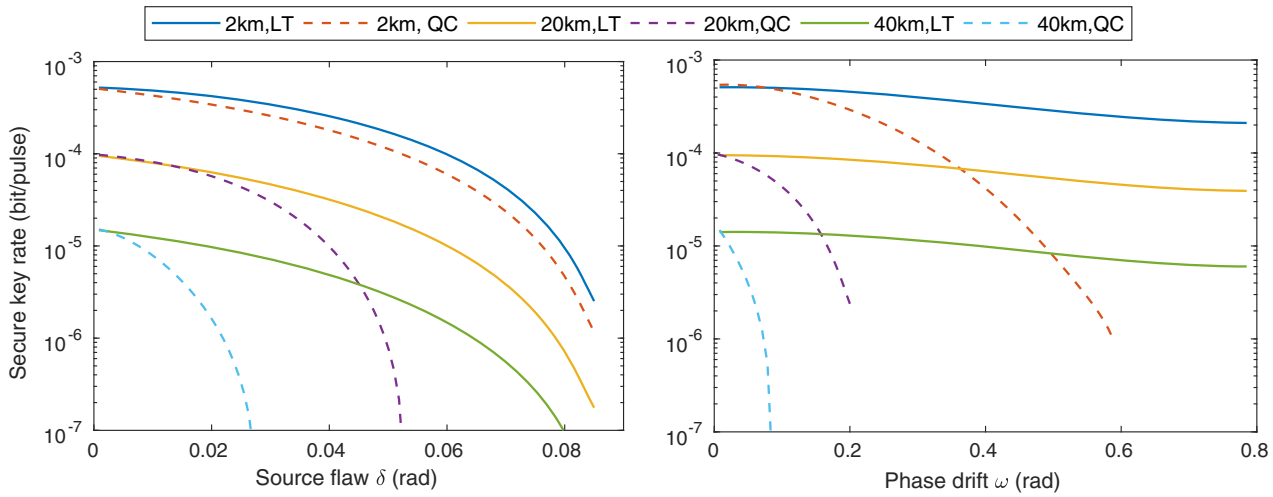

Fig. 4. Key rate versus source flaw δ and phase drift ω in the RFI-MDI-QKD protocol with LT (solid line) and QC (dashed line) methods at the fixed distance of 2 km (red), 20 km (purple), and 40 km (blue).

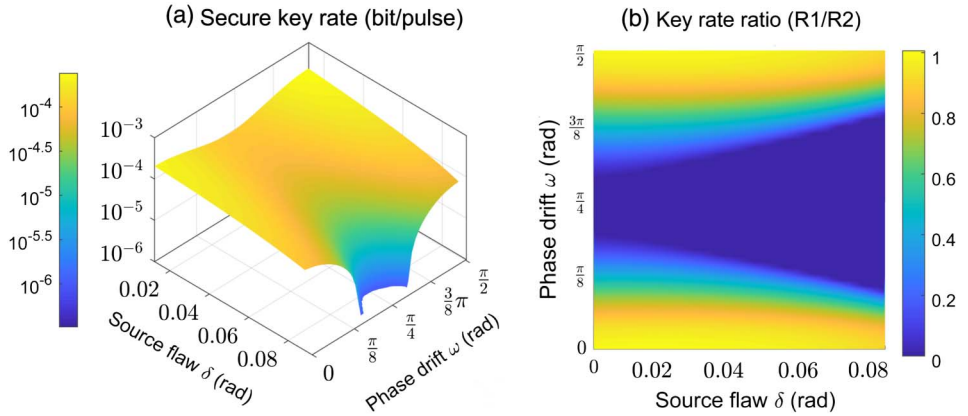

Fig. 5. (a) Key rate of loss-tolerant RFI-MDI-QKD under the joint impact of source flaw δ and phase drift $\omega \in [0, \pi/2]$ at 2 km. (b) Key rate ratio (R_1/R_2) of MDI-QKD to RFI-MDI-QKD protocol with the LT method, which is denoted by R_1 and R_2, respectively.

RFI-MDI-QKD with source flaw, apart from utilizing the finite-key analysis in the final key estimation, we step further to illustrate how much LT effects can be influenced by different phase drift and compare the protocol with the QC method. Conclusively, the LT RFI-MDI-QKD can alleviate the security vulnerability due to detector side-channel attacks, reference frame misalignment, and imperfect source preparation. The protocol can be regarded as a promising scheme for a wider real-world environment application, especially satellite-based and airborne-based applications, where a flexible relay links structure is needed[34,35]. In the end, this protocol can be further improved based on some new researches that make a contribution to RFI-MDI-QKD that boosts the key rate performance by optimized decoy-state[36] or using fewer states[37].

Acknowledgement

This work was supported by the State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) (No. IPOC2021ZT10), the National Natural Science Foundation of China (No. 11904333), and the Fundamental Research Funds for the Central Universities (No. 2019XD-A02).

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *International Conference on Computer System and Signal Processing* (IEEE, 1984), p. 175.
2. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
3. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301 (2009).
4. Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: challenges and solutions," Opt. Express **26**, 24260 (2018).
5. N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," New J. Phys. **4**, 44 (2002).
6. Y. Zhao, C.-H. Fred 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).
7. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686 (2010).
8. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
9. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
10. 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).
11. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
12. W. Wang, F. Xu, and H.-K. Lo, "Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks," Phys. Rev. X **9**, 041012 (2019).
13. 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).
14. G.-Z. Tang, S.-H. Sun, and C.-Y. Li, "Experimental point-to-multipoint plug-and-play measurement-device-independent quantum key distribution network," Chin. Phys. Lett. **36**, 070301 (2019).
15. 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).
16. 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).
17. L. Cao, W. Luo, Y. X. Wang, J. Zou, R. D. Yan, H. Cai, Y. Zhang, X. L. Hu, C. Jiang, W. J. Fan, X. Q. Zhou, B. Dong, X. S. Luo, G. Q. Lo, Y. X. Wang, Z. W. Xu, S. H. Sun, X. B. Wang, Y. L. Hao, Y. F. Jin, D. L. Kwong, L. C. Kwek, and A. Q. Liu, "Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems," Phys. Rev. Appl. **14**, 011001 (2020).
18. H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," Optica **7**, 238 (2020).
19. Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, W.-Y. Liu, X. Jiang, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, C.-Y. Lu, X.-B. Wang, Q. Zhang,

C.-Z. Peng, and J.-W. Pan, " Long-distance free-space measurement-device-independent quantum key distribution," arXiv:2006.05088 (2020).
20. A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," Phys. Rev. A **82**, 012304 (2010).
21. C.-M. Zhang, J.-R. Zhu, and Q. Wang, "Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution," Phys. Rev. A **95**, 032309 (2017).
22. C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution robust against environmental disturbances," Optica **4**, 1016 (2017).
23. 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 (2018).
24. 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).
25. K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," Phys. Rev. A **85**, 042307 (2012).
26. X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," Phys. Rev. A **87**, 012320 (2013).
27. 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).
28. 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).
29. M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," Nat. Commun. **5**, 3732 (2014).
30. H. Chen, X.-B. An, J. Wu, Z.-Q. Yin, S. Wang, W. Chen, and Z.-F. Han, "Hong–Ou–Mandel interference with two independent weak coherent states," Chin. Phys. B **25**, 020305 (2016).
31. 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).
32. X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," Phys. Rev. A **86**, 062319 (2012).
33. J.-Y. Liu, X.-Y. Zhou, and Q. Wang, "Reference-frame-independent measurement-device-independent quantum key distribution using fewer states," Phys. Rev. A **103**, 022602 (2021).
34. Y. Xue, W. Chen, S. Wang, Z. Yin, L. Shi, and Z. Han, "Airborne quantum key distribution: a review," Chin. Opt. Lett. **19**, 122702 (2021).
35. X. Wang, C. Dong, S. Zhao, Y. Liu, X. Liu, and H. Zhu, "Feasibility of space-based measurement-device-independent quantum key distribution," New J. Phys. **23**, 045001 (2021).
36. J.-Y. Liu, X.-Y. Zhou, C.-H. Zhang, H.-J. Ding, Y.-P. Chen, J. Li, and Q. Wang, "Boosting the performance of reference-frame-independent measurement-device-independent quantum key distribution," J. Light. Technol. **39**, 5486 (2021).
37. J.-Y. Liu, X.-Y. Zhou, and Q. Wang, "Reference-frame-independent measurement-device-independent quantum key distribution using fewer states," Phys. Rev. A **103**, 022602 (2021).