Finite-key security analysis against the Trojan-horse attack on practical reference-frame-independent measurement-device-independent quantum key distribution

Yang Zhou,[1,2,3,†] Hua-Jian Ding,[1,2,3,†] Jing-Yang Liu,[1,2,3] Chun-Hui Zhang,[1,2,3] Xing-Yu Zhou,[1,2,3] and Qin Wang[1,2,3,*]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[2] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[3] *Telecommunication and Networks, National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

(Received 8 June 2024; revised 18 December 2024; accepted 8 January 2025; published 4 February 2025)

Reference-frame-independent measurement-device-independent quantum key distribution (RFI MDI QKD) can resist side-channel attacks against detectors and slow variations of reference frames, thus presenting an advantageous approach for long-distance secure quantum communication. Nevertheless, if an eavesdropper implements a Trojan-horse attack (THA) by injecting bright light into sources, the back-reflected light may carry encoding information into the channel, thereby causing serious information leakage. In this paper, we theoretically evaluate the finite-key security of decoy-state RFI MDI QKD against a THA by employing the reference-state technique and a particular concentration inequality. Additionally, dual-parameter optimization and multibasis-estimation strategies are introduced to reduce statistical fluctuations effectively. Our work demonstrates that RFI MDI QKD can maintain a better performance even in the presence of large reference-frame drifts and a THA, representing a key advancement in strengthening the security of quantum communication in real-world implementations.

DOI: 10.1103/PhysRevApplied.23.024007

I. INTRODUCTION

Quantum key distribution (QKD) enables two remote parties, Alice and Bob, to securely establish cryptographic keys over an untrusted quantum channel [1]. Because of its theoretical unconditional security, it has been widely addressed and developed rapidly [2–5]. However, despite its rigorous mathematical security proof, due to imperfect devices, there are still some security vulnerabilities in practical systems. The existence of these vulnerabilities allows Eve to implement a number of attacks [6–14].

In actual QKD systems, security vulnerabilities at the sources often originate from information leakage due to side channels arising from mode dependencies or due to light-injection attacks, such as the Trojan-horse attack (THA) [15], which is one of the critical sources' attacks that can seriously threaten the security of realistic QKD systems. In a quantum version of a THA, a malicious eavesdropper Eve can inject bright light into the transmitter and then analyze the back-reflected light to gain some information about the signal state [16]. While the information may be partial—say, only the basis used—the security is still compromised, because Eve can now always choose the same basis to measure as Alice, for an intercept-and-resend attack. Lucamarini *et al.* [17] have initially presented quantitative security bounds against a THA by relating it to the specification of the optical elements. They have then proposed an architecture for a QKD transmitter to passively mitigate the potential information leakage from the Trojan-horse light. Subsequently, Tamaki *et al.* [18] and Navarrete *et al.* [19] have developed security frameworks of QKD systems using phase and intensity modulators in their transmitters, which may leak the setting information in an arbitrary way, by using the trace distance [20] and the Cauchy-Schwarz (CS) constraint [21], respectively. These pioneering efforts have received widespread attention and have been extended to the finite-key scenario [22], measurement-device-independent (MDI) QKD protocols [23,24], and even small-scale chip-based devices [25] and more [26,27].

In most QKD protocols, a shared reference frame is indispensable to reduce the quantum bit error rate (QBER) and enhance the key rate. The calibration of the reference

*Contact author: qinw@njupt.edu.cn

†These authors contributed equally to this work.

frame can be achieved by the alignment of polarization states for the polarization-encoding system or the compensation of the phase shift for the phase-encoding system, both of which have been widely studied [28–31]. However, these active calibration or compensation methods always require additional hardware and/or software, which increases the complexity of the system and reduces the real-time key rate. Alternatively, to address this issue, reference-frame-independent (RFI) QKD has been proposed to bypass the requirement of reference-frame alignment [32]. Subsequently, Yin *et al.* [33] have proposed the RFI-MDI-QKD protocol, which is immune to all detection attacks and is robust against slow reference-frame drifts, thereby providing the advantages of both security and practicality. Subsequently, several studies [34–37] have enhanced the practicality of the protocol and several experimental demonstrations [38–40] have been conducted to validate it.

A natural question arises: how secure are the RFI MDI QKD protocols against a THA? This is a critical issue that deserves attention. On the one hand, every quantum state could potentially be affected in QKD. Compared to the BB84 and MDI protocols, the RFI MDI protocol prepares an additional set of quantum states in a different basis, increasing the probability of a successful THA. On the other hand, in the RFI configuration, the only requirement imposed by this strategy is to have a stable and well-aligned key-generation basis. If the aligned basis is subjected to a THA without the knowledge of the communicating parties, the generated key becomes unreliable due to the instability and drift of the reference frame. In this situation, the information estimated by the bases used to calibrate the reference frame becomes inaccurate, as reference-frame drift caused by environmental factors differs fundamentally from that caused by a THA.

In this paper, we evaluate the finite-key security of practical RFI MDI QKD and we take the THA as an example to conduct a specific analysis. First and foremost, we employ the reference-state technique as the CS constraint [19,21] to incorporate potential information leakage caused by the THA from Alice's and Bob's devices into the security analysis. This only requires quantifying the isolation level of the QKD devices but it provides an efficient way to bound Eve's information. Second, for dependent random variables in the scenario considered, we use the recently proposed concentration inequality, called Kato's inequality [41], to bound the finite-key deviations. Additionally, we employ dual-parameter optimization [42] and multibasis-estimation methods [35,43] to reduce the effect on the statistical fluctuations. By doing so, we demonstrate that our RFI-MDI-QKD protocol is capable of generating secure keys even in the presence of large reference-frame drifts and a THA, representing a significant advancement toward practical implementation. This analysis can be extended to address other security vulnerabilities, including laser-damage attacks [44,45] and laser-seeding attacks [46,47]. Appendix A illustrates how laser-seeding attacks, which may partially modify the photon-number statistics of Alice's and Bob's signals, can be seamlessly incorporated into the analysis.

II. ATTACK ON THE SOURCES FOR RFI MDI QKD

We first introduce the protocol without any attacks and then provide a detailed introduction to the reference-state technique, and finally, we conduct a theoretical analysis of the security vulnerabilities caused by a THA as an example.

A. Decoy-state RFI MDI QKD

In RFI MDI QKD [33], Alice and Bob independently prepare their quantum states on three sets of orthogonal bases—the X, Y, and Z bases—which can be characterized using Pauli operators as σ_X, σ_Y, and σ_Z, respectively. Usually, it is assumed that one set of bases (the Z basis) is aligned, while the others (the X and Y bases) may exhibit deviation angles $\beta_{A(B)}$ due to drifts in the reference frame. Consequently, the encoding bases for Alice and Bob can be described as follows:

$$\begin{aligned} Z_{A(B)} &= Z, \\ X_{A(B)} &= X\cos\beta_{A(B)} + Y\sin\beta_{A(B)}, \\ Y_{A(B)} &= Y\cos\beta_{A(B)} - Y\sin\beta_{A(B)}. \end{aligned} \tag{1}$$

The subscripts A and B represent variables or probabilities associated with Alice and Bob, respectively. To simplify, we define $\Delta\beta = |\beta_A - \beta_B|$ and omit the subscripts without causing any confusion.

The steps of the RFI-MDI-QKD protocol can be summarized as follows:

(i) Alice (Bob) randomly encodes a quantum state the bit and basis of which is selected from $p(q) \in \{0_Z, 1_Z, 0_X, 1_X, 0_Y, 1_Y\}$ with probability p_p (p_q) and the intensity is set from $l(r) \in \{i, j, k, \ldots\}$ with probability p_l (p_r), where $|0\rangle_X = 1/\sqrt{2}(|0\rangle_Z + e^{i\beta_{A(B)}}|1\rangle_Z)$, $|1\rangle_X = 1/\sqrt{2}(|0\rangle_Z - e^{i\beta_{A(B)}}|1\rangle_Z)$, $|0\rangle_Y = 1/\sqrt{2}(|0\rangle_Z + ie^{i\beta_{A(B)}}|1\rangle_Z)$, and $|1\rangle_Y = 1/\sqrt{2}(|0\rangle_Z - ie^{i\beta_{A(B)}}|1\rangle_Z)$.

(ii) The photon pulses prepared by Alice and Bob pass through the channel and arrive at a third untrusted party, Charlie, who performs a Bell-state measurement (BSM) and announces all the corresponding measurement results.

(iii) After N rounds, Alice and Bob can determine gains $Q_{s,lr}$ and QBERs $T_{s,lr}$ in which Alice and Bob select intensity lr in the s basis, $s \in \{ZZ, XX, XY, YX, YY\}$.

(iv) Finally, they will perform parameter estimation and postprocessing to ensure that they share perfectly secret key pairs.

According to the security analysis presented in Refs. [37,40], decoy-state techniques [48,49] can be used to directly evaluate the single-photon-pair yield $Y_{s,11}$ and the single-photon-pair error rate $e_{s,11}$ in the s basis. However, the sources of Alice and Bob need to satisfy an important *assumption*: the basis-selection information and intensity-selection information of photon pulses in the channel cannot be accessible to Eve.

In practical QKD systems, Eve can exploit the security loopholes to carry out attacks. This can cause imperfections in the encoding of the sources, leading to information leakage. In Sec. III, we will focus on this issue and give a more comprehensive assessment of its impact.

B. Reference-state technique

In general, since all attacks at the detection end have been immunized in RFI MDI QKD, we focus on the security loopholes in the source, which may arise from information leakage due to side channels arising from mode dependencies or due to light-injection attacks, such as a THA or a laser-seeding attack. We also focus on the reference-state technique, which can provide high performance in the presence of source imperfections. The key idea is to consider some reference states, which are close to the actual states prepared by the protocol of interest, and use them to simplify the estimation of the parameters needed to guarantee the security of the protocol.

Specifically, when Alice selects a state encoded with information p and l, while Bob selects a state encoded with information q and r, the quantum state sent to Charlie can be expressed as

$$\left|\varphi_{p,q}^{l,r}\right\rangle_{CSE}=\sum_{n,m=0}^{\infty}\sqrt{\hat{p}_l^n\hat{p}_r^m}|nm\rangle_S\left|\hat{n}_p\hat{m}_q\right\rangle_{CE}, \tag{2}$$

where $\hat{p}_l^n(\hat{p}_r^m)$ represents the photon-number statistics after being attacked; $n_p(m_q)$ denote an $p(q)$-encoded $n(m)$-photon state by Alice (Bob), which contains the bit- or basis-encoding information, but after the sources are attacked, it will change into a unknown quantum state $\hat{n}_p(\hat{m}_q)$ and it will contain information about the injected light, while the specific form is related to different types of light-injection attacks; the subscript C denotes the qubit system sent by Alice and Bob to Charlie; the subscript $S=S_AS_B$ indicates the purification system; and system E includes the systems sent by Alice and Bob over the quantum channel, such as the back-reflected light from a possible THA. We can find that due to the presence of information leakage to Eve, $\left|\varphi_{p,q}^{l,r}\right\rangle_{CSE}$ corresponds to unwanted and possibly unknown modes caused by the attacks of the sources.

We introduce a virtual reference state

$$\left|\phi_{p,q}^{l,r}\right\rangle_{CSE}=\sum_{n,m=0}^{\infty}\sqrt{p_l^np_r^m}|nm\rangle_S\left|n_pm_q\right\rangle_{CE}, \tag{3}$$

where the state $\left|n_pm_q\right\rangle_{CE}$ can be decomposed into two parts to be characterized: one part is the ideal photon state $\left|n_pm_q\right\rangle_C$ under no attack and without any equipment defects; the other part is $|\sigma\rangle_E$, a state that does not depend on Alice's and Bob's settings. Therefore, when tracing out systems S and E, the reference state in the formula represents a perfect phase-randomized weak coherent pulse with no information leakage. By bounding the maximum deviation between the probabilities associated with the reference states and those associated with the actual states, we can obtain a relationship for the probabilities involving the actual states based on those of the reference states.

We define the gain $Q_{s,lr}^i$ in the RFI-MDI-QKD protocol as the conditional probability that Alice and Bob send pulses with intensity information l and r, respectively, in the s basis and Charlie announces a successful BSM in the ith round ($i=1,\ldots,N$). Due to the attacks of the sources, information of the quantum state is leaked, rendering the $Q_{s,lr}^i$ unable to be directly associated with $Y_{s,11}$ by decoy-state techniques. Since the reference state is never sent by the communicating parties in the actual protocol, the CS constraint [19,21] is needed to establish the relationship between the reference-state gain $Q_{s,lr}^{i,\mathrm{ref}}$ and the actual state gain $Q_{s,lr}^i$ (for more details, see Appendix B):

$$\delta_i\le\sqrt{Q_{s,lr}^{i,\mathrm{ref}}Q_{s,lr}^i}+\sqrt{(1-Q_{s,lr}^{i,\mathrm{ref}})(1-Q_{s,lr}^i)}, \tag{4}$$

where

$$\delta_i=\left|\sum_{p,q,l,r}p_pp_qp_lp_r\sum_{n,m}\sqrt{\hat{p}_l^n\hat{p}_r^mp_l^np_r^m}\langle\hat{n}_p\hat{m}_q|n_pm_q\rangle_{CE}\right| \tag{5}$$

explains the similarity between the actual state and the reference state. For different types of attack, the further-expression forms will also differ correspondingly.

Utilizing Eq. (4), the relationship between the reference-state gain and the actual state gain can be derived:

$$G_\delta^L\left(Q_{s,lr}^i\right)\le Q_{s,lr}^{i,\mathrm{ref}}\le G_\delta^U\left(Q_{s,lr}^i\right). \tag{6}$$

More detail on the CS constraint is set forth in Appendix B. Likewise, the single-photon-pair yield $Y_{s,11}^i$ can be estimated as

$$G_\delta^L\left(Y_{s,11}^{i,\mathrm{ref}}\right)\le Y_{s,11}^i\le G_\delta^U\left(Y_{s,11}^{i,\mathrm{ref}}\right). \tag{7}$$

Based on the fact of a reference state with no information leakage, we can estimate the parameters needed to guarantee the security of the actual protocol from the estimation that uses the reference states.

Utilizing the reference-state technique, our security analysis can enable RFI MDI QKD to resist attacks from the sources. Since the THA is a typical quantum hacking strategy at sources, and since analyzing specific attacks is more practical and valuable, in this paper, we mainly focus on the THA as a specific example to elaborate on the actual security analysis of the RFI MDI QKD under a THA, as shown in what follows. To ensure that our security analysis has general significance, we also conduct a simple analysis of other light-injection attacks, such as laser-damage attacks [44,45], laser-seeding attacks [46,47], etc. In Appendix A, we show how the case in which the photon-number statistics of Alice's and Bob's signals might be partially modified by laser-seeding attacks can also be straightforwardly included in the analysis.

C. Security vulnerabilities under a THA

When Eve has the ability to perform a THA, some of Eve's Trojan-horse light will reach the phase- and intensity-modulation modules of both Alice and Bob, carrying bit, basis, and intensity information into the channel, as illustrated in Fig. 1. At this point, Eve's probing system will interact with the modulation systems, allowing Eve to extract both the intensity and bit and basis information from the back-reflected light. Eve acquires the encoding information by analyzing the back-reflected Trojan-horse light because the reflected light has been modulated by the encoders. Furthermore, this attack is not aimed at intercepting the quantum states sent by Alice and Bob, so it would not draw the attention of the senders and receiver. Since Eve is not constrained by single-photon-level measurements, she can obtain the full knowledge of the key. By using a THA, she could potentially completely compromise the security of the QKD system.

Specifically, we first consider a virtual protocol with no attack. The quantum state sent to Charlie can be expressed as

$$\left|\varphi_{p,q}^{l,r}\right\rangle_{CS}=\sum_{n,m=0}^{\infty}\sqrt{p_l^n p_r^m}|nm\rangle_S|n_p m_q\rangle_C, \tag{8}$$

where $p_l^n(p_r^m)$ represents the determined photon-number statistics, e.g., in a weak coherent source as $p_l^n=e^{-l}l^n/n!$; the purification system S satisfies $\mathrm{Tr}_S\left\{\left|\varphi_{p,q}^{l,r}\right\rangle_{CS}\left\langle\varphi_{p,q}^{l,r}\right|\right\}=\sum_{n,m}p_l^n p_r^m|n_p m_q\rangle_C\langle n_p m_q|$.

However, when Eve sends Trojan-horse photons to Alice and Bob through the channel, she has the potential to alter the operational state of the laser and influence the information within the quantum state. Here, we assume that Eve sends coherent states $|\sqrt{t_{\mathrm{in}}}e^{i\theta}\rangle$ with average photon number t_{in}. When it passes through the encoding module and then reflects back to Eve's end, its state changes to $|\sqrt{t_{\mathrm{out},p}}e^{i\theta_{p,l}}\rangle$ ($|\sqrt{t_{\mathrm{out},q}}e^{i\theta_{q,r}}\rangle$), which may carry the internal bit and basis and intensity-encoding information of Alice (Bob). This indicates that the quantum states transmitted to the channel by Alice and Bob at this time contain not only their own coded photons but also Trojan-horse photons. Consequently, $|n_p m_q\rangle_C$, containing bit and basis information, largely becomes unknown photon-number states $|\hat{n}_p\hat{m}_q\rangle_{CE}=|n_p m_q\rangle_C\otimes|\sqrt{t_{\mathrm{out},p}}e^{i\theta_{p,l}}\sqrt{t_{\mathrm{out},q}}e^{i\theta_{q,r}}\rangle_E$. It is worth noting that when a coherent state passes through the transmitter of a QKD system, its photon-number statistics remain unchanged, yet it might alter the photon-number statistics of the pulses $p_l^n(p_r^m)$ originally emitted by the lasers of Alice and Bob to nondeterministic photon-number statistics $\hat{p}_l^n(\hat{p}_r^m)$. Therefore, the state given by Eq. (8) will transform into the form of Eq. (2) and this quantum state can be viewed as a high-dimensional composite system consisting of encoded photons and back-reflected Trojan-horse photons.

By analyzing the back-reflected Trojan-horse light, Eve could potentially intercept the quantum state information prepared by Alice and Bob. Specifically, for the intensity information, Eve can use the trace distance to quantitatively characterize the distinguishability of two quantum states reflected back to her [20,25]. Since the Trojan-horse light passes through the intensity-encoding modulator, the light that is reflected back will exhibit varying intensities, thereby carrying the intensity information. For bit and basis information, the Bloch-sphere bound [50] can quantitatively evaluate the basis dependence, directly reflecting the distinguishability of the quantum states.

In conclusion, Eve can intercept the sensitive encoding information in the RFI-MDI-QKD system via the THA, thereby undermining the security assumption that enables the utilization of standard decoy-state techniques for parameter estimation. Hence, evaluating the security of decoy-state RFI MDI QKD against the THA stands as the primary objective to be addressed in the subsequent sections of this paper.

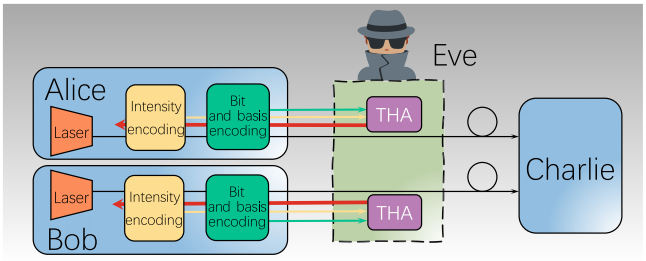

FIG. 1. A schematic representation of a THA in RFI MDI QKD. Eve injects Trojan-horse light (represented by red arrows) into Alice's and Bob's transmitters and analyzes the back-reflected light (represented by yellow and green arrows), which might carry the internal intensity and Alice's and Bob's bit and basis encoding information.

III. SECURITY PROOF

A. Practical finite-key security analysis

To enhance the practicality of security analysis in RFI MDI QKD, we constrain finite-key deviations by employing Kato's inequality. Additionally, multibasis-estimation and dual-parameter optimization methods are applied to reduce the impact of statistical fluctuations.

Here, we introduce the four-intensity decoy-state method to obtain an improved performance. The signal state u is prepared solely on the Z basis, while the decoy states v and w are prepared on either the X or Y bases. The vacuum state o can be prepared on any set of bases. It is important to note that the preparation process ensures independence between intensity information and bit and basis information. Based on the above analysis, $Y_{s,11}^{i,\mathrm{ref}}$ can be considered to be uniformly indistinguishable. In order to achieve tighter constraints, the basis pairs used to prepare the decoy-state pulses can be expanded for multibasis estimation:

$$\begin{aligned} d \in \{&XX, XY, YX, YY, XX+YY, \\ &XY+YX, XX+XY+YX+YY\}, \end{aligned} \tag{9}$$

in which the elements of the set can be written as d_i ($i = 1, 2, \ldots, 7$).

The decoy-state techniques can be employed to linearly combine the gains of reference state $Q_{d_i,lr}^{\mathrm{ref}}$ and thus we can derive the reference-state single-photon-pair yield $Y_{d_i,11}^{\mathrm{ref}}$ and the single-photon-pair bit error rate $T_{d_i,11}^{\mathrm{ref}}$. For convenience, we express $Y_{d_i,11}^{\mathrm{ref}}(T_{d_i,11}^{\mathrm{ref}})$ as $Y_{d_i,11}^{\mathrm{ref}}(T_{d_i,11}^{\mathrm{ref}}) = p_{11}\tilde{Y}_{d_i,11}^{\mathrm{ref}}(\tilde{T}_{d_i,11}^{\mathrm{ref}})$, where $p_{11} = p_l p_r p_l^1 p_r^1$ represents the joint probability of Alice and Bob sending l-intensity and r-intensity single-photon pulses. They can be estimated as [35,42,43]

$$\begin{aligned} \tilde{Y}_{d_i,11}^{\mathrm{ref}} &\geq \frac{Q_1 - Q_2 + Q_3}{p_v^1 p_w^1 \left(p_w^1 p_v^2 - p_v^1 p_w^2\right)}, \\ \tilde{T}_{d_i,11}^{\mathrm{ref}} &\leq \frac{P_{d_i} - H_{d_i}/2}{p_v^1 p_w^1}, \end{aligned} \tag{10}$$

where

$$\begin{aligned} Q_1 &= p_v^1 p_v^2 (\tilde{Q}_{d_i,ww}^{\mathrm{ref}} - \tilde{T}_{d_i,ww}^{\mathrm{ref}}) + p_w^1 p_w^2 p_v^0 \tilde{Q}_{d_i,ov}^{\mathrm{ref},L} \\ &\quad + p_w^1 p_w^2 p_v^0 \tilde{Q}_{d_i,vo}^{\mathrm{ref},L}, \\ Q_2 &= p_w^1 p_w^2 \tilde{Q}_{d_i,vv}^{\mathrm{ref},U} + p_w^1 p_w^2 p_v^0 \tilde{Q}_{d_i,oo}^{\mathrm{ref},U}, \\ Q_3 &= p_v^1 p_v^2 (P_{d_i} - H_{d_i}). \end{aligned} \tag{11}$$

Here, $P_{d_i} = \tilde{T}_{d_i,ww}^{\mathrm{ref}}$ and $H_{d_i} = p_w^0 \tilde{Q}_{d_i,wo}^{\mathrm{ref}} + p_w^0 \tilde{Q}_{d_i,ow}^{\mathrm{ref}} - p_w^0 p_w^0 \tilde{Q}_{d_i,oo}^{\mathrm{ref}}$ are the parameters that should be optimized in the next steps. $\tilde{Q}_{d_i,lr}^{\mathrm{ref}}$ ($\tilde{T}_{d_i,lr}^{\mathrm{ref}}$) represents the average gain (the average QBER) when Alice and Bob, respectively, send pulses of sources lr under the d_i basis. Similar to $\tilde{Y}_{d_i,11}^{\mathrm{ref}}$, we have $\tilde{Q}_{d_i,lr}^{\mathrm{ref}}(\tilde{T}_{d_i,lr}^{\mathrm{ref}}) = Q_{d_i,lr}^{\mathrm{ref}}(T_{d_i,lr}^{\mathrm{ref}})/(p_l p_r p_{d_i})$.

After calculating all elements under the d basis, the optimal reference-state single-photon-pair yield and bit error rate contributed in the ZZ basis are derived:

$$\begin{aligned} \tilde{Y}_{ZZ,11}^{\mathrm{ref}} &= \max\left\{\tilde{Y}_{d_1,11}^{\mathrm{ref}}, \tilde{Y}_{d_2,11}^{\mathrm{ref}}, \ldots, \tilde{Y}_{d_7,11}^{\mathrm{ref}}\right\}, \\ \tilde{T}_{ZZ,11}^{\mathrm{ref}} &\leq \frac{T_{ZZ,uu}^{\mathrm{ref},U} + p_u^0 p_u^0 T_{ZZ,oo}^{\mathrm{ref},U} - p_u^0 T_{ZZ,ou}^{\mathrm{ref},L} - p_u^0 T_{ZZ,uo}^{\mathrm{ref},L}}{p_u^1 p_u^1}. \end{aligned} \tag{12}$$

Subsequently, Kato's inequality is used to bound the actual gains (the function is defined in Appendix B):

$$K_{N,\varepsilon}^L\left(N_{lr}^{d_i}\right) \leq \sum_{i=1}^{N} Q_{d_i,lr}^i \leq K_{N,\varepsilon}^U\left(N_{lr}^{d_i}\right), \tag{13}$$

where $N_{lr}^{d_i}$ is the number of successful d_i-basis rounds of sources lr, an observable quantity in an actual experiment. The failure probability of this inequality is ε. Combining with Eq. (6), we obtain

$$G_\delta^L\left[\frac{1}{N}K_{N,\varepsilon}^L\left(N_{lr}^{d_i}\right)\right] \leq Q_{d_i,lr}^{\mathrm{ref}} \leq G_\delta^U\left[\frac{1}{N}K_{N,\varepsilon}^U\left(N_{lr}^{d_i}\right)\right]. \tag{14}$$

Similarly, $T_{d_i,11}^{\mathrm{ref}}$ can be estimated through the number of bit errors $M_{lr}^{d_i}$ in d_i-basis rounds of sources lr observed in the actual protocol, with the specific expression being as follows:

$$G_\delta^L\left[\frac{1}{N}K_{N,\varepsilon}^L\left(M_{lr}^{d_i}\right)\right] \leq T_{d_i,lr}^{\mathrm{ref}} \leq G_\delta^U\left[\frac{1}{N}K_{N,\varepsilon}^U\left(M_{lr}^{d_i}\right)\right]. \tag{15}$$

B. Eve's information

In the RFI-MDI-QKD protocol, the amount of information leaked to Eve I_E is related to the single-photon-pair error rate under the ZZ basis e_{11}^{ZZ}. It can be expressed as [33]

$$\begin{aligned} I_E &= \left(1 - e_{11}^{ZZ}\right) H_2\left(\frac{1+W}{2}\right) + e_{11}^{ZZ} H_2\left(\frac{1+V}{2}\right), \\ W &= \min\left\{\sqrt{C/2}/\left(1 - e_{11}^{ZZ}\right), 1\right\}, \\ V &= \sqrt{\frac{C}{2} - \left(1 - e_{11}^{ZZ}\right)^2 W^2}/e_{11}^{ZZ}, \end{aligned} \tag{16}$$

where $H_2(x)$ is the binary Shannon entropy function $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ and the intermediate variable C can be obtained as

$$C = \left(1 - 2e_{11}^{XX}\right)^2 + \left(1 - 2e_{11}^{XY}\right)^2 + \left(1 - 2e_{11}^{YX}\right)^2 + \left(1 - 2e_{11}^{YY}\right)^2. \tag{17}$$

Next, we calculate the single-photon-pair error rate under different bases, which include the d basis and the ZZ basis. We take e_{11}^{XX} as the representative, which can be expressed as

$$e_{11}^{XX} = \frac{M_{11}^{XX}}{N_{11}^{XX}}, \tag{18}$$

where N_{11}^{XX} is the number of successful rounds when Alice and Bob send single-photon pulses in the XX basis and M_{11}^{XX} is the corresponding number of bit errors.

By using Kato's inequality, the lower bound of N_{11}^{XX} is estimated based on the single-photon-pair yield as

$$N_{11}^{XX} \geq \bar{K}_{N,\varepsilon}^{L}\left(\sum_{i=1}^{N} Y_{XX,11}^{i}\right), \tag{19}$$

which can be further expressed with the CS constraint as

$$N_{11}^{XX} \geq \bar{K}_{N,\varepsilon}^{L}\left[NG_{\delta}^{L}\left(Y_{XX,11}^{\mathrm{ref}}\right)\right]. \tag{20}$$

Similarly, M_{11}^{XX} can be derived from the reference-state single-photon-pair bit error rate $T_{XX,11}^{\mathrm{ref}}$ as

$$M_{11}^{XX} \leq \bar{K}_{N,\varepsilon}^{U}\left[NG_{\delta}^{U}\left(T_{XX,11}^{\mathrm{ref}}\right)\right]. \tag{21}$$

C. Secure key rate

Upon obtaining the estimated parameters as discussed above, Alice and Bob proceed with error correction and privacy amplification. Additionally, by scanning and optimizing the dual-parameter P_{d_i} and H_{d_i} values under different basis combinations, they can ultimately determine the optimal secure key rate shared as

$$\begin{aligned} R &= \min : R\left(H_{d_i}, P_{d_i}\right) \\ &= \frac{N_{11}^{ZZ,L}(1-I_E) - \lambda_{EC} - 2\log\frac{1}{\varepsilon_{PA}} - 7\sqrt{\frac{\log(2/\hat{\varepsilon})}{N_{11}^{ZZ,L}}}}{N}, \\ &\text{subject to} \quad \left[H_{d_i}\right]^L \leq \left[H_{d_i}\right] \leq \left[H_{d_i}\right]^U, \\ &\left[P_{d_i}\right]^L \leq \left[P_{d_i}\right] \leq \left[P_{d_i}\right]^U, \end{aligned} \tag{22}$$

where λ_{EC} denotes the number of bits consumed in the error correction and we set it as $\lambda_{EC} = N_{uu}^{ZZ} f_{\mathrm{ec}} H_2(M_{uu}^{ZZ}/N_{uu}^{ZZ})$, which means that it depends on the total number of pulses detected in the ZZ basis N_{uu}^{ZZ}, the total number of bit errors M_{uu}^{ZZ}, and the error-correction efficiency f_{ec}. Following the security analysis in Refs. [19,24,51], the secure key rate can be against the collective attacks with ε_{PA} and $\hat{\varepsilon}$, which are the failure probability of privacy amplification and the error-probability that measures the accuracy of estimating the smooth min-entropy, respectively.

IV. SIMULATIONS

In this section, we present a numerical-simulation result of the decoy-state RFI-MDI-QKD protocol under the THA, which is grounded in a typical linear-channel model [52]. In this model, the optical pulses emitted by Alice (Bob), upon propagation through the channel, reach Charlie and can be characterized as $\sum_{k=0}^{n} C_n^k \eta^k (1-\eta)^{n-k} |k\rangle\langle k|$, where η denotes the channel transmittance. To streamline the analysis, we focus on symmetric channel conditions, implying equal Alice-Charlie and Bob-Charlie communication distances. Furthermore, we fix Charlie's detector efficiencies at $\eta_d = 65\%$ and their dark-count rates at $P_d = 7.2 \times 10^{-8}$. Regarding the security parameters of the protocol, we set $f_{\mathrm{ec}} = 1.2$ and $\varepsilon_{PA} = \hat{\varepsilon} = 10^{-5}$. Here, we implement the global-optimization algorithm to optimize the parameters u, v, w, P_u, P_v, and P_w, ensuring a comprehensive and robust evaluation of the performance of the protocol under these simulated conditions.

It is noted that under the THA attack, the form of δ_i in Eq. (5) can be further expressed as

$$\delta_i = \left| \sum_{p,q,l,r} p_p p_q p_l p_r \langle\sigma| \sqrt{t_{\mathrm{out},p}}\, e^{i\theta_{p,l}} \sqrt{t_{\mathrm{out},q}}\, e^{i\theta_{q,r}} \rangle_E \right|, \tag{23}$$

which is directly related to the isolation of sources and also characterizes to some extent the impact of the THA on RFI MDI QKD. It can also be derived as a function of the isolation of the transmitter in the experiment. When the reference-state $|\sigma\rangle_E$ is chosen as $|\mathbf{vac}\rangle_E$ and we assume that Eve's side-channel information is highly attenuated by the isolator, with total isolation of system I_{tot} at Alice's and Bob's end, we can obtain

$$\delta_i = \left| \sum_{p,q,l,r} p_p p_q p_l p_r e^{-[(t_{\mathrm{out},p} + t_{\mathrm{out},q})/2]} \right| \geq e^{-I_{tot}}. \tag{24}$$

Here, both I_{tot} and t_{out} can be characterized and calibrated in the experiment [17,19].

The simulation results, as shown in Fig. 2, assess the performance of the RFI-MDI-QKD protocol under varying values of δ, particularly at the rotation angle of the reference frame $\Delta\beta = \pi/4$, with the number of transmitted

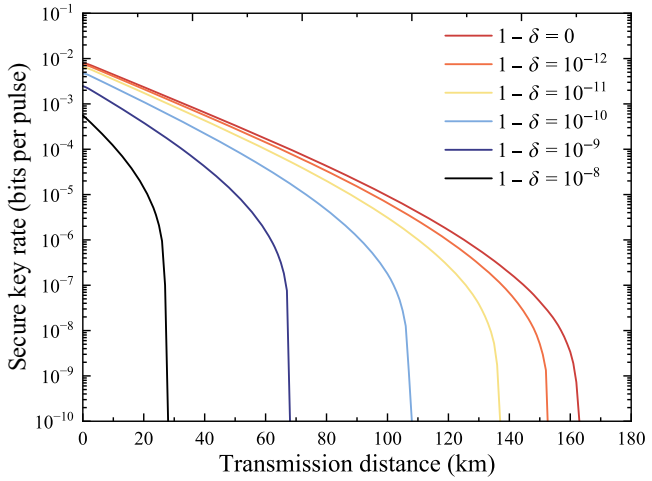

FIG. 2. The secure key rate for $N = 10^{12}$ and different values of the quantity δ with the rotation angle of the reference frame $\Delta\beta = \pi/4$. The dark-count rate is set to $P_d = 7.2 \times 10^{-8}$, Charlie's detection efficiency being $\eta_d = 65\%$. Also, we fix the loss coefficient of the channel to $\alpha = 0.2$ dB/km. The method of this work presents advantageous results in the long-distance regime. In the presence of a large reference frame, when $\delta > 1 - 10^{-12}$, our scheme can still maintain the secure key rate within an acceptable range.

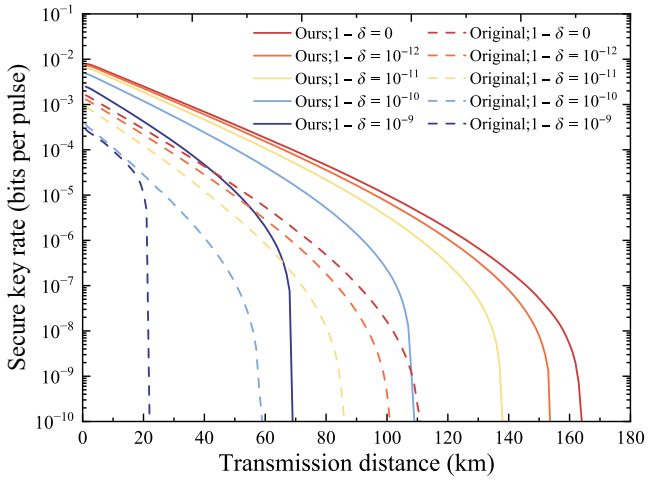

FIG. 3. Comparisons of our protocol (solid lines) with the original three-intensity decoy-state RFI MDI QKD (dash lines) for different values of the quantity δ, given the data size $N = 10^{12}$ and the rotation angle of the reference frames $\Delta\beta$ fixed to $\pi/4$. We use the same experimental parameters as considered in Fig. 2. The method of our work presents advantageous results compared with the original.

optical pulses fixed at $N = 10^{12}$ for all curves. We mainly select these values of δ based on the actual I_{tot} and t_{out} values from the experiment in Refs. [19,22]. We observe that as the value of δ decreases, symbolizing a reduced capability of the system to isolate Trojan-horse light, there is a marked decline in the achievable key rate. In scenarios in which there is a significant drift in the reference frames of both parties, even a minimal THA by Eve can severely impact the performance of the protocol. If we can control $\delta = 1$, it can be assumed that the system is completely impervious to the THA. In practical experimental setups, this can be approached by enhancing the isolation at the transmitter, which can be achieved by incorporating specific devices such as power limiters based on the thermo-optical defocusing effect [53]. These devices can limit the incoming or outgoing optical energy injected by Eve but they have a minimal impact on encoding. From our simulation results, it is evident that when $\delta > 1 - 10^{-12}$, our protocol can mitigate these effects of the THA to a certain extent, maintaining the secure key rate within an acceptable range. This indicates that with appropriate system design and parameter optimization, the adverse effects of the THA can be significantly reduced, enhancing the overall security and reliability of the RFI-MDI-QKD protocol.

To illustrate the advantages of dual-parameter optimization and multibasis-estimation strategies, we compare our protocol with the original three-intensity decoy-state RFI-MDI-QKD protocol as shown in Fig. 3. The dashed lines in the figure depict the results of the original three-intensity scheme, while the solid lines represent our work. It is clear that our method achieves noticeably improved performance. This enhancement is mainly attributed to a more refined and accurate estimation of $Y^{\text{ref}}_{ZZ,11}$, which is particularly beneficial in scenarios with finite-key lengths, effectively countering the impacts of statistical fluctuations. It is key to acknowledge, however, that despite the marked performance elevation of our protocol over the three-intensity scheme, it brings with it a corresponding increase in computational and implementation complexity. This complexity arises from the addition of more stringent constraint mechanisms.

Moreover, Fig. 4 offers a comparison of our RFI-MDI-QKD protocol with the MDI-QKD protocol [24]. In the scenarios in which there is no rotation angle of the reference frame, the performances of these two protocols under identical attack are remarkably similar, except that there is a degradation at long distances, which is due to a severe finite-size effect, as depicted by the orange dashed and solid lines, respectively. In contrast, when significant reference-frame drifts are present alongside similar attack conditions, the strengths of RFI MDI QKD become prominently visible. Besides, the key-rate deterioration in RFI MDI QKD is considerably milder compared to that in MDI QKD, as illustrated by the comparisons between the yellowish and azure lines. Thus, in scenarios characterized by the combined challenges of the THA and reference-frame drifts, our RFI-MDI-QKD protocol demonstrates superior robustness. This indicates that the reference-frame stability and the THA resistance are both important in practical

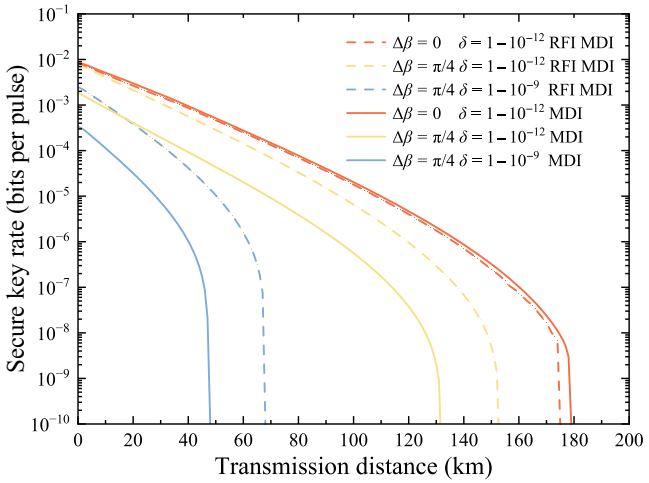

FIG. 4. Comparisons of the RFI-MDI-QKD protocol (dashed lines) with MDI QKD (solid lines) for different values of the quantities δ and $\Delta\beta$. Our results show that, in scenarios in which both a THA and reference-frame drift are present, our RFI-MDI-QKD protocol exhibits greater robustness.

settings and that our approach offers significant advantages over MDI QKD, showcasing its enhanced viability and applicability in practical environments.

Meanwhile, not only can Kato's inequality be used to bound $N_{lr}^{d_i}$ and $M_{lr}^{d_i}$ but the same function can be achieved using other concentration inequalities, such as Azuma's inequality [54], the expression for which can be found in Appendix C. As depicted in Fig. 5, the implementation of Azuma's inequality yields less favorable results compared to Kato's inequality. This outcome can be attributed to the inherent characteristics of these inequalities. Intuitively, Azuma's inequality is simpler in terms of mathematical

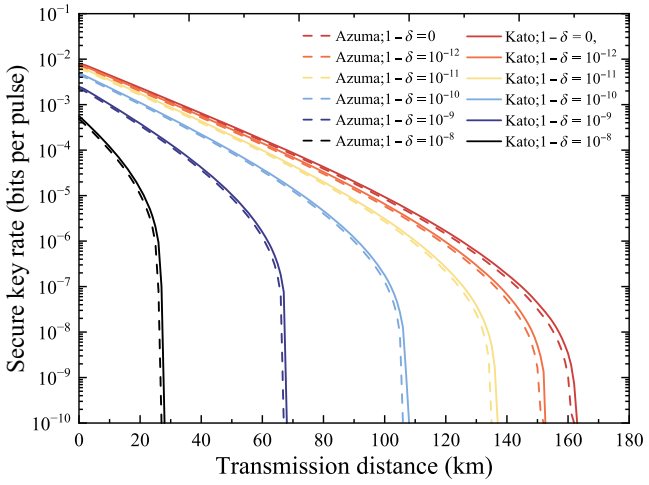

FIG. 5. The finite secure key rate simulation of our protocol using Azuma's or Kato's inequalities with $N = 10^{12}$ and $\Delta\beta = \pi/4$. In comparison, the bound on the estimation quantities of Azuma's inequality is not as tight as that of Kato's inequality.

computational complexity. Kato's inequality allows users to predict the results that they expect to obtain before actually performing the experiment, which establishes more stringent and compact constraints [55]. While Azuma's inequality may provide a more straightforward approach, Kato's inequality ensures a more robust and tightly bound estimation. This superiority in constraint efficacy directly translates into the enhanced performance and reliability of our protocol, as evidenced by the results and comparisons presented in our work.

V. CONCLUSIONS

In summary, we theoretically evaluate the security of the decoy-state RFI MDI QKD in practice. By utilizing the reference-state technique to characterize the impact of attacks, we take the THA as a specific example for analysis and this analysis can be extended to other security vulnerabilities, such as laser-seeding attacks. The reference-state technique is applied to characterize the information leakage in the phase- and intensity-modulation modules, which makes the defects related to the isolation of QKD to a security parameter and thus the information obtained by Eve can be more tightly estimated. The concentration inequality constraints yield tighter results for the finite-key effect and the utilization of dual-parameter optimization and multibasis-estimation methods significantly improves the performance of the secure key rate between the communicating parties, especially in terms of the maximum achievable distance. Overall, our RFI-MDI-QKD protocol exhibits enhanced robustness against both security loopholes and reference-frame drifts.

Our work aims to address the security of sources in the RFI-MDI-QKD protocol and we analyze it specifically in the case of a THA, representing a step toward its practical application. This analysis can be extended to other security vulnerabilities, such as laser-damage attacks [44,45], laser-seeding attacks [46,47], etc. If we consider laser-damage attacks, the security analysis needs to select the reference state as the worst possible quantum state of light intensity that could be obtained after an attack. Thus, through our security analysis, Alice and Bob can use reference-state techniques to bound a single experimental parameter δ_i that encapsulates the effects of laser-injection attacks. It is worth noting that this work can be extended to the novel measurement-device-independent protocols such as twin-field QKD [56], which can be further investigated in future work.

ACKNOWLEDGMENTS

This work is supported by the Industrial Prospect and Key Core Technology Projects of Jiangsu provincial key R & D Program (Grant No. BE2022071), the National Natural Science Foundation of China (Grants No. 12074194,

No. 62401287, and No. 62471248), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX23_1039).

APPENDIX A: SECURITY ANALYSIS AGAINST LASER-SEEDING ATTACK

Here, we consider the security analysis under the case in which Eve may carry out a laser-seeding attack, which can increase and control the intensity of the light emitted by the laser diode in the transmitter of a QKD system [46,47]. By injecting intense external light into the laser diode, the intensity of the output light may be changed and some side-channel information can then be extracted by Eve. Unlike the THA, which analyzes back-reflected light that is originally from an external independent source, a laser-seeding attack manipulates the functioning of the laser diode of the transmitter directly. The goal of this attack is to directly change the intensity of such quantum states and cause intensity fluctuations in the transmitted pulses passively.

In particular, we assume that Eve uses Trojan-horse light as the injection light; we shall then consider that Eve's attack changes all the intensities l (r) by the same factor λ. That is, we assume that $l' = \lambda l$ ($r' = \lambda r$) for all l (r) and that the photon-number statistics of Alice's (Bob's) signal satisfy $p^n_l = p^n_{l'} = e^{-l'} l'^n/n!$ ($p^n_r = p^n_{r'} = e^{-r'} r'^n/n!$), with $l' \in [l, \lambda l]$ ($r' \in [r, \lambda r]$), being λ a multiplicative factor that depends on Eve's attack.

We also consider, as in the main text, that δ_i is upper bounded by I_{tot} and that Eve may use this light of intensity t_{tot} to learn information about the settings p (q) and r (l). This means, according to Eq. (5), that

$$\delta_i = \left| \sum_{p,q,l,r} p_p p_q p_l p_r e^{-[(t_{\text{out},p} + t_{\text{out},q})/2]} \right| \geq e^{-\frac{I_{\text{tot}} + (1+\lambda-2\sqrt{\lambda})(l+r)}{2}}. \tag{A1}$$

In Fig. 6, we show the effect that the multiplicative factor λ has on the bounds on the secret key rate. We consider that the transmitted-signal number is $N = 10^{12}$ and that $I_{\text{tot}} = 10^{-4}$. The different values of the multiplicative factor λ are given in Ref. [19]. As we can see in Fig. 6, the key rate decreases significantly as λ increases. Compared to the situation without an attack, the secure key shared between Alice and Bob in the RFI-MDI-QKD protocol is affected in terms of both the distance and the key rate. This also demonstrates that our security analysis of the RFI-MDI-QKD sources can be extended to laser-seeding attacks. However, it is worth noting that λ is expected to be small if the isolation of Alice's and Bob's transmission is sufficiently high, which is also necessary to reduce the information leakage to a minimum.

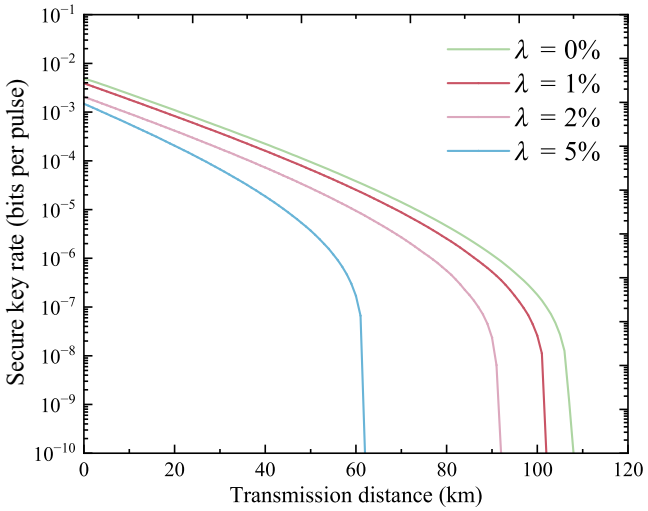

FIG. 6. The secure key rate for $N = 10^{12}$ and different values of the quantity λ with the rotation angle of the reference frame $\Delta\beta = \pi/4$. The experimental parameters used for the simulation are the same as those used in Fig. 2.

APPENDIX B: CAUCHY-SCHWARZ CONSTRAINT

According to Ref. [57], if we define the pure states of a quantum system as $|X_1\rangle$ and $|X_2\rangle$, then for any positive operator $\hat{O} \leq I$, by applying the Cauchy-Schwarz constraint to these two vectors we have that

$$|\langle X_1|\hat{O}|X_2\rangle| \leq \sqrt{\langle X_1|\hat{O}|X_1\rangle \langle X_2|\hat{O}|X_2\rangle}. \tag{B1}$$

Since the real part of a complex number is equal to or smaller than its absolute value, one can rewrite Eq. (A1) as

$$\frac{1}{2}(\langle X_1|\hat{O}|X_2\rangle) + \langle X_2|\hat{O}|X_1\rangle) \leq \sqrt{\langle X_1|\hat{O}|X_1\rangle \langle X_2|\hat{O}|X_2\rangle}. \tag{B2}$$

Next, consider two inequalities in the form of Eq. (B2), such that in one inequality we set $\hat{O} = \hat{M}$ and in the other $\hat{O} = \hat{I} - \hat{M}$. By adding these inequalities, we obtain

$$\begin{aligned} &\frac{1}{2}(\langle X_1|X_2\rangle) + \langle X_2|X_1\rangle) \\ &\quad \leq \sqrt{\langle X_1|\hat{M}|X_1\rangle \langle X_2|\hat{M}|X_2\rangle} \\ &\qquad + \sqrt{\langle X_1|(\hat{I} - \hat{M})|X_1\rangle \langle X_2|(\hat{I} - \hat{M})|X_2\rangle}. \end{aligned} \tag{B3}$$

Note that one has the freedom to choose the global phase of the quantum state $|X_2\rangle$ such that the inner product $\langle X_1|X_2\rangle$ becomes real and positive. By exploiting this freedom, we

have that

$$\langle X_1|X_2\rangle \le \sqrt{\langle X_1|\hat{M}|X_1\rangle\langle X_2|\hat{M}|X_2\rangle} + \sqrt{\langle X_1|(\hat{I}-\hat{M})|X_1\rangle\langle X_2|(\hat{I}-\hat{M})|X_2\rangle} \quad \text{(B4)}$$

and

$$\langle X_1|X_2\rangle \le \sqrt{\langle X_1|\hat{M}|X_1\rangle\langle X_2|\hat{M}|X_2\rangle} + \sqrt{(1-\langle X_1|\hat{M}|X_1\rangle)(1-\langle X_2|\hat{M}|X_2\rangle)}. \quad \text{(B5)}$$

By solving Eq. (B5), we obtain

$$G_\delta^L(\langle X_1|\,\hat{M}\,|X_1\rangle) \le \langle X_2|\,\hat{M}\,|X_2\rangle \le G_\delta^U(\langle X_1|\,\hat{M}\,|X_1\rangle), \quad \text{(B6)}$$

where

$$G_\delta^L(x) = \begin{cases} llg_\delta^-(x), & x > 1-\delta^2, \\ 0, & \text{else}, \end{cases}$$
$$G_\delta^U(x) = \begin{cases} g_\delta^+(x), & x < \delta^2, \\ 1, & \text{else}, \end{cases} \quad \text{(B7)}$$

with $\delta = \langle X_1|X_2\rangle$ and $g_\delta^\pm(x) = x + (1-\delta^2)(1-2x) \pm 2\delta\sqrt{(1-\delta^2)x(1-x)}$. Note that $G_\delta^L(x)$ and $G_\delta^U(x)$ are concave with respect to $0 \le x \le 1$ for any fixed $0 \le \delta \le 1$.

In this paper, let $|X_1\rangle$ be the actual state $\left|\varphi_{p,q}^{l,r}\right\rangle_{CSE}$, let $|X_2\rangle$ be the reference state $\left|\phi_{p,q}^{l,r}\right\rangle_{CSE}$, and let $\hat{M}$ be $\hat{\mathcal{M}}_{\text{Bell}}^i$, corresponding to Eve's measurement operator associated with a specific Bell state in the i round, which acts on the systems C and E. Then, Eq. (4) can be obtained. Here, $Q_{s,lr}^i = \langle\varphi_{p,q}^{l,r}|\hat{\mathcal{M}}_{\text{Bell}}^i|\varphi_{p,q}^{l,r}\rangle$ and $Q_{s,lr}^{i,\text{ref}} = \langle\phi_{p,q}^{l,r}|\hat{\mathcal{M}}_{\text{Bell}}^i|\phi_{p,q}^{l,r}\rangle$.

APPENDIX C: KATO'S INEQUALITY AND AZUMA'S INEQUALITY

In this appendix, we will simply introduce two kinds of concentration bounds for dependent random variables used in our analysis.

1. Kato's inequality

Let $\{X_m\}$ be a list of random variables and let $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_m$ be an increasing chain of σ algebras verifying $E(X_v|F_u) = X_v$ for $v \le u$. Suppose that $0 \le X_m \le 1$ for all m. In this case, for any $n \in \mathbb{N}$, $a \in \mathbb{R}$, and $b \in \mathbb{R}_{\ge 0}$,

$$P\left\{\sum_{m=1}^n E(X_m|F_{m-1}) - X_m \ge \left[b + a\left(\frac{2\sum_{m=1}^n X_m}{n} - 1\right)\right]\sqrt{n}\right\} \le \exp\left[\frac{-2\left(b^2-a^2\right)}{\left(1+\frac{4a}{3\sqrt{n}}\right)^2}\right] \quad \text{(C1)}$$

holds. Moreover, we denote that $\Lambda = \sum_m^n X_m$ and replacing $X_m \to 1 - X_m$ and $a \to 1 - a$ in Eq. (C1), it trivially follows that

$$P\left\{\sum_{m=1}^n E(X_m|F_{m-1}) - \Lambda \ge \left[b + a\left(\frac{2\Lambda}{n} - 1\right)\right]\sqrt{n}\right\} \le \exp\left[\frac{-2(b^2-a^2)}{\left(1+\frac{4a}{3\sqrt{n}}\right)^2}\right] \quad \text{(C2)}$$

and

$$P\left\{\Lambda - \sum_{m=1}^n E(X_m|F_{m-1}) \ge \left[b + a\left(\frac{2\Lambda}{n} - 1\right)\right]\sqrt{n}\right\} \le \exp\left[\frac{-2(b^2-a^2)}{\left(1-\frac{4a}{3\sqrt{n}}\right)^2}\right]. \quad \text{(C3)}$$

In order to obtain a tight bound for Eq. (C2), we should address $\min\{b + a[(2\Lambda/n) - 1]\}\sqrt{n}$ by $\exp\left[-2(b^2-a^2)/\left(1+\frac{4a}{3\sqrt{n}}\right)^2\right] = \varepsilon$. Its solution is

$$a_1 = \frac{3\left\{72\sqrt{n}\Lambda(n-\Lambda)\ln\varepsilon - 16n^{3/2}\ln^2\varepsilon + 9\sqrt{2}(n-2\Lambda)\sqrt{-n^2\ln\varepsilon\,[9\Lambda(n-\Lambda) - 2n\ln\varepsilon]}\right\}}{4(9n - 8\ln\varepsilon)\,[9\Lambda(n-\Lambda) - 2n\ln\varepsilon]},$$
$$b_1 = \frac{\sqrt{18na^2 - (16a^2 + 24a\sqrt{n} + 9n)\ln\varepsilon}}{3\sqrt{2n}}. \quad \text{(C4)}$$

Then, for any known measurement result of random variables Λ, the upper bound of the mathematical expectations can be obtained via

$$\sum_{m=1}^{n} E(X_m|F_{m-1}) \leq \Lambda + \left[b_1 + a_1\left(\frac{2\Lambda}{n} - 1\right)\right]\sqrt{n} \equiv K_{n,\varepsilon}^{U}(\Lambda), \quad \text{(C5)}$$

and with known expectations, the lower bound of Λ is

$$\Lambda \geq \frac{\sum_{m=1}^{n} E(X_m|F_{m-1}) - (b_1 - a_1)\sqrt{n}}{1 + \frac{2a_1}{\sqrt{n}}} \equiv \bar{K}_{n,\varepsilon}^{L}\left[\sum_{m=1}^{n} E(X_m|F_{m-1})\right]. \quad \text{(C6)}$$

With a similar process for Eq. (C3), we can also obtain

$$\sum_{m=1}^{n} E(X_m|F_{m-1}) \geq \Lambda - \left[b_2 + a_2\left(\frac{2\Lambda}{n} - 1\right)\right]\sqrt{n} \equiv K_{n,\varepsilon}^{L}(\Lambda) \quad \text{(C7)}$$

and

$$\Lambda \leq \frac{\sum_{m=1}^{n} E(X_m|F_{m-1}) + (b_2 - a_2)\sqrt{n}}{1 - \frac{2a_2}{\sqrt{n}}} \equiv \bar{K}_{n,\varepsilon}^{U}\left[\sum_{m=1}^{n} E(X_m|F_{m-1})\right], \quad \text{(C8)}$$

given by

$$a_2 = \frac{-3\left\{72\sqrt{n}\Lambda(n-\Lambda)\ln\varepsilon - 16n^{3/2}\ln^2\varepsilon - 9\sqrt{2}(n-2\Lambda)\sqrt{-n^2\ln\varepsilon\,[9\Lambda(n-\Lambda) - 2n\ln\varepsilon]}\right\}}{4(9n - 8\ln\varepsilon)\,[9\Lambda(n-\Lambda) - 2n\ln\varepsilon]},$$
$$b_2 = \frac{\sqrt{18na^2 - (16a^2 + 24a\sqrt{n} + 9n)\ln\varepsilon}}{3\sqrt{2n}}. \quad \text{(C9)}$$

2. Azuma's inequality

According to Azuma's inequality,

$$P\left[\sum_{m=1}^{n} E(X_m|F_{m-1}) - \Lambda \geq b\sqrt{n}\right] \leq \exp\left(\frac{-b^2}{2}\right),$$
$$P\left[\Lambda - \sum_{m=1}^{n} E(X_m|F_{m-1}) \geq b\sqrt{n}\right] \leq \exp\left(\frac{-b^2}{2}\right). \quad \text{(C10)}$$

Equating the right-hand sides to ε and solving for b, we have that

$$\Lambda \leq \sum_{m=1}^{n} E(X_m|X_1, \ldots, X_{m-1}) + \Delta, \quad \text{(C11)}$$

except with probability at most ε for each of the bounds, where $\Delta = \sqrt{2n\ln\varepsilon^{-1}}$.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.

[2] H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

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

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

[5] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

[6] V. Makarov, Controlling passively quenched single photon detectors by bright light, New J. Phys. **11**, 065003 (2009).

[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] 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).

[9] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phase remapping attack in practical quantum-key-distribution systems, Phys. Rev. A **75**, 032314 (2007).

[10] B. Qi, C. H. F. Fung, H. K. Lo, and X. F. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).
[11] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, Insecurity of detector-device-independent quantum key distribution, Phys. Rev. Lett. **117**, 250505 (2016).
[12] H. Tan, W. Y. Zhang, L. Zhang, W. Li, S. K. Liao, and F. Xu, External magnetic effect for the security of practical quantum key distribution, Quantum Sci. Technol. **7**, 045008 (2022).
[13] 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).
[14] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, Protecting fiber-optic quantum key distribution sources against light-injection attacks, PRX Quantum **3**, 040307 (2022).
[15] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).
[16] A. Vakhitov, V. Makarov, and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. **52**, 691 (2001).
[17] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, Phys. Rev. X **5**, 031030 (2015).
[18] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).
[19] Á. Navarrete and M. Curty, Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks, Quantum Sci. Technol. **7**, 035021 (2022).
[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, United Kingdom, 2000).
[21] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, 4487 (2020).
[22] W. Wang, K. Tamaki, and M. Curty, Finite-key security analysis for quantum key distribution with leaky sources, New J. Phys. **20**, 083027 (2018).
[23] W. Wang, K. Tamaki, and M. Curty, Measurement-device independent quantum key distribution with leaky sources, Sci. Rep. **11**, 1678 (2021).
[24] H. J. Ding, J. Y. Liu, X. Y. Zhou, C. H. Zhang, J. Li, and Q. Wang, Improved finite-key security analysis of measurement-device-independent quantum key distribution against a Trojan-horse attack, Phys. Rev. Appl. **19**, 044022 (2023).
[25] H. Tan, W. Li, L. K. Zhang, K. J. Wei, and F. H. Xu, Chip-based quantum key distribution against Trojan-horse attack, Phys. Rev. Appl. **15**, 064038 (2021).
[26] T. T. Luo, X. R. Sun, C. F. Huang, Y. Chen, Z. R. Zhang, and K. J. Wei, Security analysis against the Trojan horse attack on practical polarization-encoding quantum key distribution systems, Phys. Rev. A **109**, 042608 (2024).
[27] J. Gu, X. Y. Cao, Y. Fu, Z. W. He, Z. J. Yin, H. L. Yin, and Z. B. Chen, Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources, Sci. Bull **67**, 2167 (2022).
[28] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, Nat. Photonics **9**, 832 (2015).
[29] 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).
[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] 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 (2016).
[32] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Reference-frame-independent quantum key distribution, Phys. Rev. A **82**, 012304 (2010).
[33] 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 (2014).
[34] Q. Li, C. Zhu, S. Ma, K. Wei, and C. Pei, Reference-frame-independent and measurement-device-independent quantum key distribution using one single source, Int. J. Theory Phys. **57**, 2192 (2018).
[35] 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).
[36] D. Lee, S. Hong, Y. W. Cho, H. T. Lim, S. W. Han, H. Jung, S. Moon, K. J. Lee, and Y. S. Kim, Reference-frame-independent measurement-device-independent quantum key distribution using fewer quantum states, Opt. Lett. **45**, 2624 (2020).
[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).
[38] 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).
[39] 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).
[40] 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).

[41] G. Kato, Concentration inequality using unconfirmed knowledge, ArXiv:2002.04357.

[42] 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).

[43] 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. Lightwave Technol. **39**, 5486 (2021).

[44] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser damage helps the eavesdropper in quantum cryptography, Phys. Rev. Lett. **112**, 070503 (2014).

[45] V. Makarov, J. P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Creation of backdoors in quantum communications via laser damage, Phys. Rev. A **94**, 030302 (2016).

[46] A. Huang, Á Navarrete, S. H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, Phys. Rev. Appl. **12**, 064043 (2019).

[47] F. Y. Lu, P. Ye, Z. H. Wang, S. Wang, Z. Q. Yin, R. Wang, X. J. Huang, W. Chen, D. Y. He, G. J. Fan-Yuan, G. C. Guo, and Z. F. Han, Hacking measurement-device-independent quantum key distribution, Optica **10**, 520 (2023).

[48] X. B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[49] H. K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[50] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).

[51] L. Sheridan, T. P. Le, and V. Scarani, Finite-key security against coherent attacks in quantum key distribution, New J. Phys. **12**, 123019 (2010).

[52] Q. Wang and X. B. Wang, Simulating of the measurement-device independent quantum key distribution with phase randomized general sources, Sci. Rep. **4**, 4612 (2014).

[53] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim, Securing practical quantum communication systems with optical power limiters, PRX Quantum **2**, 030304 (2021).

[54] K. Azuma, Weighted sums of certain dependent random variables, Tohoku Math. J. Second Ser. **19**, 357 (1967).

[55] G. Currás-Lorenzo, A. Navarrete, M. Pereira, and K. Tamaki, Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory, Phys. Rev. A **104**, 012406 (2021).

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

[57] H. K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Inf. Comput. **7**, 431 (2007).