frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 07 February 2023
DOI 10.3389/fphy.2023.1101631

Security analysis of measurement-device-independent quantum conference key agreement with weak randomness

Xiao-Lei Jiang[1,2], Yang Wang[1,2,3]*, Yi-Fei Lu[1,2], Jia-Ji Li[1,2], Hai-Long Zhang[1,2], Mu-Sheng Jiang[1,2], Chun Zhou[1,2] and Wan-Su Bao[1,2]*

[1]Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou, China, [2]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, China, [3]National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing, China

Check for updates

OPEN ACCESS

EDITED BY
Goutam K. Samanta,
Physical Research Laboratory, India

REVIEWED BY
Hongyi Zhou,
Institute of Computing Technology (CAS), China
Pei Zeng,
The University of Chicago, United States

*CORRESPONDENCE
Yang Wang,
✉ wy@qiclab.cn
Wan-Su Bao,
✉ bws@qiclab.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 18 November 2022
ACCEPTED 19 January 2023
PUBLISHED 07 February 2023

CITATION
Jiang X-L, Wang Y, Lu Y-F, Li J-J, Zhang H-L, Jiang M-S, Zhou C and Bao W-S (2023), Security analysis of measurement-device-independent quantum conference key agreement with weak randomness.
Front. Phys. 11:1101631.
doi: 10.3389/fphy.2023.1101631

Quantum conference key agreement (QCKA) allows multiple users to distribute secret conference keys over long distances. Measurement-device-independent QCKA (MDI-QCKA) is an effective QCKA scheme, which closes all detection loopholes and greatly enhances QCKA's security in practical application. However, an eavesdropper (Eve) may compromise the security of practical systems and acquire conference key information by taking advantage of the weak randomness from the imperfect quantum devices. In this article, we analyze the performance of the MDI-QCKA scheme based on the weak randomness model. Our simulation results show that even a small proportion of weak randomness may lead to a noticeable fluctuation in the conference key rate. For the case with finite-key size, we find that the weak randomness damages the performance of MDI-QCKA to different degrees according to the data size of total pulses transmitted. Furthermore, we infer that QCKA based on single-photon interference technology may perform better in resisting weak randomness vulnerabilities. Our work contributes to the practical security analysis of multiparty quantum communication and takes a further step in the development of quantum networks.

KEYWORDS

measurement-device-independent, conference key agreement, weak randomness, finite-key, security analysis

1 Introduction

Quantum key distribution (QKD) has become the art of two legitimate parties (Alice and Bob) distributing secret information by virtue of the laws of physics [1]. It has information-theoretical security regardless of the unlimited computational power of an eavesdropper (Eve) [2, 3]. Over the past decades, QKD has developed rapidly and made remarkable progress in terms of theory and practice.

At present, the two-party scheme is the main direction of most theoretical and experimental works. In fact, multi-party quantum communication protocols have also been proposed and studied. The quantum conference key agreement (QCKA) [4–7] is one of the most promising applications that distributes the conference key among multiple parties over a long distance. Particularly, combing the MDI [8] technology *via* post-selected Greenberger–Horne–Zeilinger (GHZ) entangled states [9, 10], allows measurement-device-independent QCKA (MDI-QCKA) [11] to eliminate all side-channel attacks in detectors and plays a vital role in the construction and development of quantum networks. Furthermore, MDI-QCKA has been studied under different conditions consisting of finite-key size [12], continuous variables [13, 14], four users with the W state [15], and device independence [16, 17]. Recently, based on single-photon interference technology, some new QCKA protocols have also been proposed in which the conference key rate and transmission distance are improved greatly [18–23].

In terms of the practical quantum communication system, Eve may choose quantum devices of state preparation or measurement as the target of her (his) attack, which may result in bit encoding and basis selection being modulated not at random [24–27]. Li et al. proposed a weak randomness model [28–30] to analyze the quantum state preparation vulnerability in the BB84 protocol. Recently, this security analysis technology has been applied in the reference-frame-independent QKD (RFI-QKD) [31], MDI-QKD [32], and sending-or-not-sending twin-field QKD (SNS TF-QKD) [33]. Under the condition of weak randomness, the states prepared consisted of random and non-random parts [28]. States prepared from the non-random part may lead to the leakage of secret key information to Eve. In fact, the weak randomness model is also appropriate for the QCKA for two reasons. First, three communicators (Alice, Bob, and Charlie) are required in the QCKA to perform quantum state preparation operation, which has to be affected by imperfections of quantum devices. Eve may exploit the weak randomness of imperfect devices to intervene in bit encoding and the basis selection process. Second, based on the decoy-state method, signal states or decoy states emitted by Alice, Bob, and Charlie are transmitted in the optical channel. In this case, Eve may perform attenuation operation to maximize the leaked information. Consequently, it is necessary to consider QCKA protocols' and the practical security of weak randomness.

In this article, we analyze the performance of the decoy-state MDI-QCKA [11] based on the weak randomness model. First, we analyze the potential influence of weak randomness on the conference key rate in the asymptotic case. Second, we analytically derive the formula of the length of the conference key with finite-key size by exploiting the Chernoff bound [34–36]. Utilizing the experimental parameters from Ref. [11], we numerically simulate the secret conference key rate under the condition of weak randomness. The results demonstrate that the performance of MDI-QCKA deteriorates rapidly, even with the fraction of weak randomness. For the case with finite-key size, we notice that weak randomness damages the performance of MDI-QCKA differently for different data sizes of total transmitted pulses, and the impact of weak randomness on the conference key rate may be greater than the data size of the total transmitted pulses. Moreover, we compare the results with our previous work and notice that utilizing single-photon interference technology in the QCKA may enhance resistance to vulnerabilities of weak randomness.

The remainder of the article is organized as follows: in Section 2, we describe a decoy-state MDI-QCKA protocol. In Section 3, we analyze the security of the decoy-state MDI-QCKA protocol based on the weak randomness model in both asymptotic and non-asymptotic cases. In Section 4, we present the numerical simulation results and a discussion. Finally, the conclusion is drawn in Section 5.

2 Protocol description

Here, let us review the three-intensity decoy-state MDI-QCKA protocol; the description of the protocol is as follows:

(1) State preparation. Alice, Bob, and Charlie randomly modulate the intensities $\alpha_a \in A = \{\mu_a, \nu_a, w_a\}$, $\beta_b \in B = \{\mu_b, \nu_b, w_b\}$, and $\gamma_c \in C = \{\mu_c, \nu_c, w_c\}$ with the probability of $p_{\mu_a}, p_{\nu_a}, p_{w_a} = 1 - p_{\mu_a} - p_{\nu_a}$, $p_{\mu_b}, p_{\nu_b}, p_{w_b} = 1 - p_{\mu_b} - p_{\nu_b}$, and $p_{\mu_c}, p_{\nu_c}, p_{w_c} = 1 - p_{\mu_c} - p_{\nu_c}$, respectively. Here, $\mu_{a(b,c)}$ denotes the signal state, $\nu_{a(b,c)}$ denotes the decoy state, 0 denotes the vacuum state, and $\mu_{a(b,c)} > \nu_{a(b,c)} > w_{a(b,c)} > 0$. For bit encoding and basis selection, Alice, Bob, and Charlie randomly choose a bit value from $\mathrm{K} \in \{0, 1\}$ and select a basis from $W \in \{Z, X\}$ with the probability of P_Z and P_X, respectively. Then, they send phase-randomized coherent states to an untrusted fourth party David *via* the quantum channel.

(2) Measurement. David performs a GHZ-state measurement of pulses sent by Alice, Bob, and Charlie and projects the received pulses into a GHZ state. Here, David only identifies two of the eight GHZ states: $|\Phi_0^+\rangle = 1/\sqrt{2}(|HHH\rangle + |VVV\rangle)$ and $|\Phi_0^-\rangle = 1/\sqrt{2}(|HHH\rangle - |VVV\rangle)$. Meanwhile, David announces the measurement results to Alice, Bob, and Charlie *via* an authenticated channel. Three legitimate members only retain the raw data of the correct GHZ-state measurement results and discard the mismatched measurement results. Here, three legitimate members employ information on the Z basis to generate the secret conference key and the X basis to estimate parameters.

(3) Sifting. Three legitimate members publish their basis and intensity choices *via* an authenticated channel. Once they choose the same basis with Alice's intensity α_a, Bob's intensity β_b, and Charlie's intensity $\gamma_{c,}$ David announces a successful measurement event, and three legitimate members record the number of detected pulses.

(4) Parameter estimation. First, Alice, Bob, and Charlie calculate the single-photon counting rate of successful measurement events on the Z or X basis. Second, they calculate the bit error rate on the X basis for the intensity combination $\alpha_a\beta_b\gamma_c$ $(\alpha_a \in A, \beta_b \in B, \gamma_c \in C)$. Finally, they verify the bit error rate of the X basis.

(5) Error correction. Here, we assume that the raw conference key of Alice refers to the reference raw key. Bob and Charlie perform an error correction step so that their raw keys match the raw key of Alice. This error correction operation consumes information at most $Leak_{EC}$ bits. In order to ensure that three legitimate members possess the same conference keys, they conduct an error verification operation.

(6) Private amplification. In order to decrease Eve's information on three legitimate members' conference keys, three legitimate members also use a random two-universal hash function to obtain the final conference key pairs (S_A, S_B, S_C).

3 Security analysis with weak randomness

For the security analysis of decoy-state MDI-QCKA under the condition of weak randomness, hidden variables ξ, ζ, and ς from Eve are assumed to determine the states which are prepared by three legitimate members, and Eve should take responsibility for all abovementioned weak randomness imperfections. The probabilities of non-random part states prepared by three legitimate members are p_1, p_2, and p_3. If $p_{1(2,3)} = 1$, all conference key information may be leaked to Eve, that is, $R = 0$. If $p_1 = p_2 = p_3 = 0$, Eve cannot obtain information theoretically. If $0 < p_{1(2,3)} < 1$, we can apply the weak randomness model to estimate the maximum quantity of information stolen by Eve.

Here, we suppose that the binary set of bits S, T, and G prepared by Alice, Bob, and Charlie, respectively, decide bit encoding and basis selection. $|S|$, $|T|$, and $|G|$ represent the order of sets S, T, and G, respectively. Because of the weak randomness imperfection in the practical system, the random number cannot be perfectly prepared, which shows that partial bits belonging to sets S, T, and G are mastered by Eve. S is made up of a non-random part S_1 and a random part S_2. T is made up of a non-random part T_1 and a random part T_2. G is made up of a non-random part G_1 and a random part G_2. This is rational to assume by considering two scenarios. First, Eve may attack the random number generator and obtain partial random number information. Second, the state may be modulated by different laser diodes from three legitimate members, and Eve may distinguish them by observing characteristics such as the spectrum and timing sequence. Here, we define the weak randomness parameter $p_1 = \frac{|S_1|}{|S|}$ at Alice, $p_2 = \frac{|T_1|}{|T|}$ at Bob, and $p_3 = \frac{|G_1|}{|G|}$ at Charlie. However, we cannot ensure that the capability of Eve attacking Alice is identical to her (him) attacking Bob or Charlie. That is, $p_1 = p_2 = p_3$ is not necessarily satisfied.

Under the condition of weak randomness, Eve attenuates the quantum states from random parts S_2, T_2, and G_2 with a certain probability in the channel. For this case, the non-random part quantum states reach David without attenuation. Here, we assume that bit errors only come from random parts, and that the states of non-random part do not generate bit errors. If Eve performs attenuation and keeps the error rate within a rational range, her (his) presence cannot be detected by three legitimate members. Considering signal loss, the non-random probability in David's side may be amplified. Consequently, the maximum transmission distance may compromise, the gain of single-photon on the Z basis may decrease, and the bit error rate may increase.

3.1 Decoy-state MDI-QCKA with weak randomness

Based on the weak randomness model, Alice, Bob, and Charlie prepare quantum states as follows:

$$\rho'_{Alice} = \frac{p_1}{2}\sum_{k_a=0,1}|k_a\rangle\langle k_a|_{Alice}\otimes|k_a\rangle\langle k_a|_{Eve} + (1-p_1)\rho_{Alice}\otimes|2\rangle\langle 2|_{Eve}, \tag{1}$$

$$\rho'_{Bob} = \frac{p_2}{2}\sum_{k_b=0,1}|k_b\rangle\langle k_b|_{Bob}\otimes|k_b\rangle\langle k_b|_{Eve} + (1-p_2)\rho_{Bob}\otimes|2\rangle\langle 2|_{Eve}, \tag{2}$$

$$\rho'_{Charlie} = \frac{p_3}{2}\sum_{k_c=0,1}|k_c\rangle\langle k_c|_{Charlie}\otimes|k_c\rangle\langle k_c|_{Eve} + (1-p_3)\rho_{Charlie}\otimes|2\rangle\langle 2|_{Eve}, \tag{3}$$

where Eve can obtain information about Alice's (Bob's and Charlie's) system according to the auxiliary quantum state. For Alice's (Bob's and Charlie's) system, if Eve's auxiliary quantum state is $|k_a\rangle\langle k_a|_{Eve}(|k_b\rangle\langle k_b|_{Eve}, |k_c\rangle\langle k_c|_{Eve})$, Eve may acquire the conference key information k_a (k_b, k_c). If Eve's auxiliary quantum state is $|2\rangle\langle 2|_{Eve}$, three legitimate members prepare perfect GHZ states ρ_{Alice}, ρ_{Bob}, and $\rho_{Charlie}$, and Eve cannot distinguish between different quantum states in this case. Compared with MDI-BB84 QKD, the quantum state prepared and transmitted in the MDI-QCKA is a GHZ state. The raw key of Alice needs to be determined as the reference raw key, and the other two parties need to compare and sift their keys. In addition, the definition of successful gain in the MDI-QCKA is similar to that of the MDI-BB84 QKD, and the final bit error rate of the MDI-QCKA is one of the bit error rates calculated by Bob or Charlie.

In the decoy-state MDI-QCKA protocol, three legitimate members may prepare signal and decoy states using the same laser diodes with the same random probabilities p_1, p_2, p_3. Furthermore, signal and decoy states can also be prepared using different laser diodes. For this case, signal and decoy states prepared by three legitimate members can be distinguished with the probabilities p_1, p_2, p_3. If signal states are distinguished, Eve can perform PNS attack [37] without being detected, and Eve performs an attenuate operation in the quantum channel when signal states are not distinguished.

Then, we may estimate the parameters under the condition of weak randomness. The final conference key rate of the decoy-state MDI-QCKA can be given by [11]:

$$R = Q_0^Z + Q_{111}^Z\left[1 - H\left(e_{111}^{PZ}\right)\right] - H\left(\max\left\{E_{\alpha_a\beta_b\gamma_c}^{ZAB}, E_{\alpha_a\beta_b\gamma_c}^{ZAC}\right\}\right) f Q_{\mu_a\mu_b\mu_c}^Z, \tag{4}$$

where Q_0^Z denotes the gain when Alice sends vacuum states while David gets a successful GHZ state measurement event on the Z basis. Q_{111}^Z is the gain of single-photon states on the Z basis. $H(x) = -\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. Here, the raw conference key of Alice is assumed as the reference raw key. For the case of asymptotic data, we can consider that the phase error rate of the Z basis e_{111}^{PZ} is equal to the bit error rate of the X basis e_{111}^{BX}. $E_{\alpha_a\beta_b\gamma_c}^{ZAB}$ ($E_{\alpha_a\beta_b\gamma_c}^{ZAC}$) is the overall bit errors between Alice and Bob (Charlie). f is the error correction efficiency and $Q_{\mu_a\mu_b\mu_c}^Z$ is the overall gain on the Z basis.

The overall gain and bit error rate can be expressed as

$$Q_{\mu_a\mu_b\mu_c}^W = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\sum_{k=0}^{\infty}\frac{\mu_a^n\mu_b^m\mu_c^k}{n!m!k!}e^{-\mu_a-\mu_b-\mu_c}Y_{nmk}^W, \tag{5}$$

$$E_{\mu_a\mu_b\mu_c}^W Q_{\mu_a\mu_b\mu_c}^W = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\sum_{k=0}^{\infty}\frac{\mu_a^n\mu_b^m\mu_c^k}{n!m!k!}e^{-\mu_a-\mu_b-\mu_c}e_{nmk}^{BW}Y_{nmk}^W, \tag{6}$$

where $W = X, Z$. Y_{nmk}^W is the yield on the X or Z basis when Alice, Bob, and Charlie prepare n-photon states, m-photon states, and k-photon states, respectively, and e_{nmk}^W is the bit error rate corresponding to this case.

The gain of single-photon states on the Z basis can be given by

$$Q_{111}^Z = \mu_a\mu_b\mu_c e^{-\mu_a-\mu_b-\mu_c}Y_{111}^Z, \tag{7}$$

the gain when Alice sends the vacuum state while David gets a successful GHZ-state measurement event on the Z basis is given by

$$Q_0^Z = e^{-\mu_a}Q_{0\mu_b\mu_c}^Z. \tag{8}$$

Considering the condition of weak randomness, the probability of Alice, Bob, and Charlie preparing non-random part quantum states are p_1, p_2, and p_3, respectively. Eve not only attenuates the states in random parts to amplify the non-random proportion at David's side but also controls the probability of attenuation to ensure that she (he) will not be detected by three members. We assume that Eve only attenuates the random portion of the single photon, and that multiphotons are not actually used to generate secret keys. The probability of signal loss from the random part is given by

$$p_{loss1}^{W} = \mu_a\mu_b\mu_c e^{-\mu_a-\mu_b-\mu_c}\frac{Y_{111}^{W} - \left(p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3\right)}{1 - \left(p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3\right)}. \tag{9}$$

The non-random proportion of quantum states reaching David's side can be expressed as

$$p_{non-rand1}^{W} = \frac{p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3}{Y_{111}^{W}}. \tag{10}$$

The gain of the random part single-photon states which can generate conference keys on the Z basis can be expressed as

$$Q_{111}' \geq Q_{111}^{Z} - \tilde{Q}_{111}^{Z} = Q_{111}^{Z}\left(1 - p_{non-rand1}^{Z}\right), \tag{11}$$

where $\tilde{Q}_{111}^{Z}$ is the gain of the non-random part single-photon states which cannot generate conference keys. The gain of the random part single-photon states when Alice sends the vacuum state while David gets a successful GHZ state measurement event which can generate conference keys on the Z basis can be expressed as

$$Q_0' \geq Q_0^{Z} - \tilde{Q}_0^{Z} = Q_0^{Z}\left(1 - p_{non-rand1}^{Z}\right), \tag{12}$$

where $\tilde{Q}_0^{Z}$ is the gain of the non-random part single-photon states when Alice sends the vacuum state while David obtains a successful GHZ state measurement result which cannot generate conference keys.

Considering the attenuation operation from Eve, the value of the bit error rate e_{111}^{BX} under the condition of weak randomness can be given by

$$\begin{aligned} e_{111}' &= \frac{e_{111}^{BX}}{1 - p_{non-rand1}^{X}} \\ &= \frac{e_{111}^{BX}Y_{111}^{X}}{Y_{111}^{X} - \left(p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3\right)}. \end{aligned} \tag{13}$$

With the method mentioned in [38, 39], we can calculate the value of Y_{111}^{X} and the value of e_{111}^{BX}. Then, combining Eqs. 11–13, we can obtain the final conference key rate of the decoy-state MDI-QCKA under the condition of weak randomness.

3.2 Finite-key analysis with weak randomness

Here, we employ the weak randomness model to analyze the security of the decoy-state MDI-QCKA and derive formulas for the lower bound of the successful single-photon gain and the upper bound of the bit error rate. The final length of the conference keys on the Z basis can be given by [11, 12]:

$$l \geq s_0^{Z} + s_{111}^{Z,L}\left[1 - H\left(e_{111}^{BX,U}\right)\right] - Leak_{EC}, \tag{14}$$

where s_0^{Z} denotes the number of measurement results when Alice sends the vacuum state while David gets a successful GHZ state measurement event on the Z basis. $s_{111}^{Z,L}$ is the lower bound of the successful single-photon counting rate s_{111}^{Z}, and $e_{111}^{BX,U}$ is the upper bound of the bit error rate e_{111}^{BX} on the X basis. $Leak_{EC} = H\left(\max\left\{E_{\alpha_a\beta_b\gamma_c}^{ZAB}, E_{\alpha_a\beta_b\gamma_c}^{ZAC}\right\}\right) f n^{Z}$ is the amount of the consumed information in the error correction operation. n^{Z} is the total number of detection events when Alice, Bob, and Charlie prepare states on the Z basis.

Let s_{nmk}^{Z} be the total number of successful detection events obtained by David when Alice, Bob, and Charlie prepare n-photon states, m-photon states, and k-photon states on the Z basis, respectively. For the intensity combination $\alpha_a\beta_b\gamma_c$ ($\alpha_a \in A$, $\beta_b \in B$, $\gamma_c \in C$), the expected value of n_{abc}^{Z} can be expressed as

$$\bar{n}_{abc}^{Z} = \sum_{n,m,k=0}^{\infty} p_{abc|nmk}^{Z} s_{nmk}^{Z}, \tag{15}$$

where $p_{abc|nmk}^{Z}$ denotes the conditional probability when Alice, Bob, and Charlie prepare n-photon states, m-photon states, and k-photon states on the Z basis, respectively, with the intensity combination $\alpha_a\beta_b\gamma_c$ ($\alpha_a \in A$, $\beta_b \in B$, $\gamma_c \in C$). It can be given by

$$p_{abc|nmk}^{Z} = \frac{p_{abc}^{Z}}{\tau_{nmk}^{Z}} p_{a|n} p_{b|m} p_{c|k}, \tag{16}$$

where $\tau_{nmk}^{Z} = \sum p_{abc}^{Z} \frac{e^{-a-b-c} a^n b^m c^k}{n!m!k!}$ denotes the probability when Alice, Bob, and Charlie prepared n-photon states, m-photon states, and k-photon states on the Z basis, respectively, and p_{abc}^{Z} is the probability when Alice, Bob, and Charlie modulate the intensity α_a, β_b, and γ_c on the Z basis. $p_{a|n}$, $p_{b|m}$, and $p_{c|k}$ are the photon number distribution probabilities of Alice, Bob, and Charlie, respectively.

On the basis of Eq. 9, we can also derive the probability of random part signal loss in the case of finite-key size:

$$p_{loss2}^{W} = \frac{s_{111}^{W} - \tau_{111}^{W}\left(p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3\right)N}{N - \left(p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3\right)N}. \tag{17}$$

The non-random proportion of quantum states reaching David's side can be expressed as

$$p_{non-rand2}^{W} = \frac{\tau_{111}^{W}\left(p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3\right)N}{s_{111}^{W}}, \tag{18}$$

where N denotes the total data size of transmitted pulses, $W = X, Z$.

Taking independent events into account, we exploit the Chernoff bound [34–36] to calculate the number of practical measurement events, which can be expressed as

$$\left|\bar{n}_{abc}^{Z} - n_{abc}^{Z}\right| \leq \delta\left(n_{abc}^{Z}, \varepsilon_1\right) \tag{19}$$

with the probability at least 1 − $2\varepsilon_1$, where $\delta(x, y) \in [-\Delta, \hat{\Delta}]$, with$\Delta = \sqrt{2x\ln\left(16y^{-4}\right)}$ and $\hat{\Delta} = \sqrt{2x\ln\left(y^{-3/2}\right)}$.

Furthermore, s_{nmk}^{X} denotes the total number of the correct measurement events observed by David when Alice, Bob, and Charlie prepared n-photon states, m-photon states, and k-photon states on the X basis, respectively, and v_{nmk}^{X} denotes the corresponding number of bit errors. m_{abc}^{X} denotes the total number of bit errors when Alice, Bob, and Charlie prepared states on the X basis and $m_{abc}^{X} = \sum_{n,m,k=0} v_{nmk}^{X}$. For the intensity combination $\alpha^a\beta^b\gamma^c$ ($\alpha^a \in A$, $\beta^b \in B$, $\gamma^c \in C$), the expected value of m_{abc}^{X} can be given by

$$\bar{m}_{abc}^{X} = \sum_{n,m,k=0}^{\infty} p_{abc|nmk}^{X} v_{nmk}^{X}, \tag{20}$$

where $p_{abc|nmk}^{X}$ denotes the conditional probability when Alice, Bob, and Charlie prepare n-photon states, m-photon states, and k-photon states on the X basis, respectively, with the intensity combination $\alpha_a\beta_b\gamma_c$ ($\alpha_a \in A$, $\beta_b \in B$, $\gamma_c \in C$). It can be given by

$$p^X_{abc|nmk} = \frac{p^X_{abc}}{\tau^X_{nmk}} p_{a|n} p_{b|m} p_{c|k}, \tag{21}$$

where $\tau^X_{nmk} = \sum p^X_{abc} \frac{e^{-a-b-c} a^n b^m c^k}{n!m!k!}$ denotes the probability when Alice, Bob, and Charlie prepared n-photon states, m-photon states, and k-photon states on the X basis, respectively, and p^X_{abc} is the probability when Alice, Bob, and Charlie modulate the intensity α_a, β_b, and γ_c on the X basis, respectively.

For the case of finite sample sizes, the relation between the expected value and observed value of m^X_{ab} under the Chernoff bound [34–36] can be established as

$$\left|\bar{m}^X_{abc} - m^X_{abc}\right| \le \delta\left(m^X_{abc}, \varepsilon_2\right), \tag{22}$$

with the probability at least $1 - 2\varepsilon_2$, where $\delta(x, y) \in [-\Delta, \hat{\Delta}]$, with$\Delta = \sqrt{2x \ln(16y^{-4})}$ and $\hat{\Delta} = \sqrt{2x \ln(y^{-3/2})}$.

The number of single-photon detections from a non-random set which cannot generate conference keys on the Z basis can be expressed as

$$\tilde{s}^Z_{111} = \tau^Z_{111}(1 - p_1)(1 - p_2)(1 - p_3)N. \tag{23}$$

The number of single-photon detections from a random set is supposed to satisfy

$$s'_{111} \ge s^{Z,L}_{111} - \tilde{s}^Z_{111} = s^{Z,L}_{111}\left(1 - p^Z_{non-rand2}\right). \tag{24}$$

The number of detections from the non-random part when Alice sends a vacuum state while David gets a successful GHZ state measurement event on the Z basis can be expressed as

$$\tilde{s}^Z_0 = \tau^Z_{011}(1 - p_1)(1 - p_2)(1 - p_3)N. \tag{25}$$

The secure single-photon detection from the random part when Alice sends a vacuum state while David gets a successful GHZ state measurement event on the Z basis is supposed to satisfy

$$s'_0 \ge s^{Z,L}_0 - \tilde{s}^Z_0 = s^{Z,L}_0\left(1 - p^Z_{non-rand2}\right). \tag{26}$$

The lower bound of the single-photon detection on the Z basis can be given by

$$s^Z_{111} \ge s^{Z,L}_{111} = \tau^Z_{111} \frac{p_{1|\mu_a} p_{2|\mu_b} p_{1|\mu_c} N^Z_{\mu_a \nu_b \nu_c} - p_{1|\mu_a} p_{2|\nu_b} p_{1|\nu_c} N^Z_{\mu_a \mu_b \mu_c}}{p^2_{1|\mu_a} p_{1|\nu_c} p_{1|\mu_c}\left(p_{1|\nu_b} p_{2|\mu_b} - p_{1|\mu_b} p_{2|\nu_b}\right)}, \tag{27}$$

where

$$\begin{aligned} N^Z_{\mu_a \nu_b \nu_c} = {} & \frac{n^{Z,L}_{\mu_a \nu_b \nu_c}}{p_{\nu_a} p_{\nu_b} p_{\nu_c} p_Z} - \frac{p_{0|\nu_a} n^{Z,U}_{w_a \nu_b \nu_c}}{p_{w_a} p_{\nu_b} p_{\nu_c} p_Z} - \frac{p_{0|\nu_b} n^{Z,U}_{\mu_a w_b \nu_c}}{p_{\mu_a} p_{w_b} p_{\nu_c} p_Z} - \frac{p_{0|\nu_c} n^{Z,U}_{\mu_a \nu_b w_c}}{p_{\mu_a} p_{\nu_b} p_{w_c} p_Z} \\ & + \frac{p_{0|\mu_a} p_{0|\nu_b} n^{Z,L}_{w_a w_b \nu_c}}{p_{w_a} p_{w_b} p_{\nu_c} p_Z} + \frac{p_{0|\mu_a} p_{0|\nu_c} n^{Z,L}_{w_a \nu_b w_c}}{p_{w_a} p_{\nu_b} p_{w_c} p_Z} + \frac{p_{0|\nu_b} p_{0|\nu_c} n^{Z,L}_{\mu_a w_b w_c}}{p_{\mu_a} p_{w_b} p_{w_c} p_Z} \\ & + \frac{2 p_{0|\mu_a} p_{0|\nu_b} p_{0|\nu_c} n^{Z,L}_{w_a w_b w_c}}{p_{w_a} p_{w_b} p_{w_c}}, \end{aligned} \tag{28}$$

$$\begin{aligned} N^Z_{\mu_a \mu_b \mu_c} = {} & \frac{n^{Z,U}_{\mu_a \mu_b \mu_c}}{p_{\mu_a} p_{\mu_b} p_{\mu_c} p_Z} - \frac{p_{0|\mu_a} n^{Z,L}_{w_a \mu_b \mu_c}}{p_{w_a} p_{\mu_b} p_{\mu_c} p_Z} - \frac{p_{0|\mu_b} n^{Z,L}_{\mu_a w_b \mu_c}}{p_{\mu_a} p_{w_b} p_{\mu_c} p_Z} - \frac{p_{0|\mu_c} n^{Z,L}_{\mu_a \mu_b w_c}}{p_{\mu_a} p_{\mu_b} p_{w_c} p_Z} \\ & + \frac{p_{0|\mu_a} p_{0|\mu_b} n^{Z,U}_{w_a w_b \mu_c}}{p_{w_a} p_{w_b} p_{\mu_c} p_Z} + \frac{p_{0|\mu_a} p_{0|\mu_c} n^{Z,U}_{w_a \mu_b w_c}}{p_{w_a} p_{\mu_b} p_{w_c} p_Z} + \frac{p_{0|\mu_b} p_{0|\mu_c} n^{Z,U}_{\mu_a w_b w_c}}{p_{\mu_a} p_{w_b} p_{w_c} p_Z} \\ & + \frac{2 p_{0|\mu_a} p_{0|\mu_b} p_{0|\mu_c} n^{Z,U}_{w_a w_b w_c}}{p_{w_a} p_{w_b} p_{w_c}}. \end{aligned} \tag{29}$$

The number of successful single-photon detection when Alice sends a vacuum state while David gets a successful GHZ state measurement event on the Z basis can be given by

$$s^Z_0 = \frac{n^Z_{w_a \mu_b \mu_c} + n^Z_{w_a \mu_b \nu_c} + n^Z_{w_a \nu_b \mu_c} + n^Z_{w_a \nu_b \nu_c}}{p_{0|\mu_a} + p_{0|\nu_a}}, \tag{30}$$

where $n^{Z,U}_{abc}$ is the upper bound and $n^{Z,L}_{abc}$ is the lower bound of n^Z_{abc}, which can be deduced from Eq. 19 by using the Chernoff bound.

Considering the attenuation operation from Eve, the value of the bit error rate e^{BX}_{111} under the condition of weak randomness can be given by

$$\begin{aligned} e'_{111} &= \frac{e^{BX}_{111}}{1 - p^X_{non-rand2}} \\ &= \frac{e^{BX}_{111} Y^X_{111}}{Y^X_{111} - \left(p_1 + p_2 + p_3 + p_1 p_2 p_3 - p_1 p_2 - p_1 p_3 - p_2 p_3\right)}, \end{aligned} \tag{31}$$

where Y^X_{111} denotes the successful single-photon counting rate on the X basis, and it can be given by

$$Y^X_{111} \ge Y^{X,L}_{111} = \frac{p_{1|\mu_a} p_{2|\mu_b} p_{1|\mu_c} N^X_{\mu_a \nu_b \nu_c} - p_{1|\mu_a} p_{2|\nu_b} p_{1|\nu_c} N^X_{\mu_a \mu_b \mu_c}}{p^2_{1|\mu_a} p_{1|\nu_c} p_{1|\mu_c}\left(p_{1|\nu_b} p_{2|\mu_b} - p_{1|\mu_b} p_{2|\nu_b}\right)}, \tag{32}$$

where

$$\begin{aligned} N^X_{\mu_a \nu_b \nu_c} = {} & \frac{n^{X,L}_{\mu_a \nu_b \nu_c}}{p_{\nu_a} p_{\nu_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_a} n^{X,U}_{w_a \nu_b \nu_c}}{p_{w_a} p_{\nu_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_b} n^{X,U}_{\mu_a w_b \nu_c}}{p_{\mu_a} p_{w_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_c} n^{X,U}_{\mu_a \nu_b w_c}}{p_{\mu_a} p_{\nu_b} p_{w_c} p_X} \\ & + \frac{p_{0|\mu_a} p_{0|\nu_b} n^{X,L}_{w_a w_b \nu_c}}{p_{w_a} p_{w_b} p_{\nu_c} p_X} + \frac{p_{0|\mu_a} p_{0|\nu_c} n^{X,L}_{w_a \nu_b w_c}}{p_{w_a} p_{\nu_b} p_{w_c} p_X} + \frac{p_{0|\nu_b} p_{0|\nu_c} n^{X,L}_{\mu_a w_b w_c}}{p_{\mu_a} p_{w_b} p_{w_c} p_X} \\ & + \frac{2 p_{0|\mu_a} p_{0|\nu_b} p_{0|\nu_c} n^{X,L}_{w_a w_b w_c}}{p_{w_a} p_{w_b} p_{w_c}}, \end{aligned} \tag{33}$$

$$\begin{aligned} N^X_{\mu_a \mu_b \mu_c} = {} & \frac{n^{X,U}_{\mu_a \mu_b \mu_c}}{p_{\mu_a} p_{\mu_b} p_{\mu_c} p_X} - \frac{p_{0|\mu_a} n^{X,L}_{w_a \mu_b \mu_c}}{p_{w_a} p_{\mu_b} p_{\mu_c} p_X} - \frac{p_{0|\mu_b} n^{X,L}_{\mu_a w_b \mu_c}}{p_{\mu_a} p_{w_b} p_{\mu_c} p_X} - \frac{p_{0|\mu_c} n^{X,L}_{\mu_a \mu_b w_c}}{p_{\mu_a} p_{\mu_b} p_{w_c} p_X} \\ & + \frac{p_{0|\mu_a} p_{0|\mu_b} n^{X,U}_{w_a w_b \mu_c}}{p_{w_a} p_{w_b} p_{\mu_c} p_X} + \frac{p_{0|\mu_a} p_{0|\mu_c} n^{X,U}_{w_a \mu_b w_c}}{p_{w_a} p_{\mu_b} p_{w_c} p_X} + \frac{p_{0|\mu_b} p_{0|\mu_c} n^{X,U}_{\mu_a w_b w_c}}{p_{\mu_a} p_{w_b} p_{w_c} p_X} \\ & + \frac{2 p_{0|\mu_a} p_{0|\mu_b} p_{0|\mu_c} n^{X,U}_{w_a w_b w_c}}{p_{w_a} p_{w_b} p_{w_c}}. \end{aligned} \tag{34}$$

Furthermore, the number of bit errors on the X basis is related to the single-photon detection s^X_{111}, and it can be expressed as

$$v^X_{111} \le v^{X,U}_{111} = \frac{\tau^X_{111} M^X_{\nu_a \nu_b \nu_c}}{p_{1|\nu_a} p_{1|\nu_b} p_{1|\nu_c}}, \tag{35}$$

where

$$\begin{aligned} M^X_{\nu_a \nu_b \nu_c} = {} & \frac{m^{X,U}_{\nu_a \nu_b \nu_c}}{p_{\nu_a} p_{\nu_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_a} m^{X,L}_{w_a \nu_b \nu_c}}{p_{w_a} p_{\nu_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_b} m^{X,L}_{\nu_a w_b \nu_c}}{p_{\nu_a} p_{w_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_c} m^{X,L}_{\nu_a \nu_b w_c}}{p_{\nu_a} p_{\nu_b} p_{w_c} p_X} \\ & - \frac{p_{0|\nu_a} p_{0|\nu_b} m^{X,L}_{w_a w_b \nu_c}}{p_{w_a} p_{w_b} p_{\nu_c} p_X} - \frac{p_{0|\nu_a} p_{0|\nu_c} m^{X,L}_{w_a \nu_b w_c}}{p_{w_a} p_{\nu_b} p_{w_c} p_X} - \frac{p_{0|\nu_b} p_{0|\nu_c} m^{X,L}_{\nu_a w_b w_c}}{p_{\nu_a} p_{w_b} p_{w_c} p_X} \\ & + \frac{2 p_{0|\nu_a} p_{0|\nu_b} p_{0|\nu_c} n^{x,U}_{w_a w_b w_c}}{p_{w_a} p_{w_b} p_{w_c}}, \end{aligned} \tag{36}$$

where $m^{X,U}_{abc}$ is the upper bound and $m^{X,L}_{abc}$ is the lower bound of m^X_{abc}, which can be deduced from Eq. 22 by using the Chernoff bound.

Adopting the same calculation method of s^Z_{111} from Eq. 27, we can calculate the number of single-photon detection on the X basis s^X_{111}. Next, we calculate the theoretical value of the bit error rate on the X basis

$$e^{BX}_{111} \le e^{BX,U}_{111} = \frac{v^{X,U}_{111}}{s^{X,L}_{111}}. \tag{37}$$

Finally, combining Eqs. 24, 26, 31, we can derive the secret conference key length of the decoy-state MDI-QCKA under the condition of weak randomness.

TABLE 1 List of experimental parameters applied in the numerical simulation. Here, α denotes the fiber loss coefficient (dB/km), p_d is the dark count rate of David's detectors, η_d is the detection efficiency of the David's detectors, e_d is the optical misalignment-error probability, f is the error correction inefficiency, and ε is the security bound when considering statistical fluctuation analysis.

α	p_d	η_d (%)	e_d	f	ε
0.2	10^{-7}	90	0.015	1.16	10^{-10}

4 Numerical simulations

In this section, based on the fiber-based channel model and the experimental parameters in Ref. [11], we simulate the performance of the decoy-state MDI-QCKA with the effect of weak randomness in both asymptotic and finite-key size cases.

Here, we define the fiber transmittance of Alice, Bob, and Charlie as $\eta_a = 10^{-\alpha L_a/10}$, $\eta_b = 10^{-\alpha L_b/10}$, and η_c =, respectively, with $10^{-\alpha L_c/10}$. $\alpha = 0.2(dB/km)$ is the loss coefficient of the standard fiber link, $L_{a,b,c}$ is the fiber length, and $p_d = 10^{-7}$ is the dark count rate of David's detectors. $\eta_d = 90\%$ is the detection efficiency of David. e_d is the optical misalignment-error probability, and the efficiency of error correction is $f = 1.16$. $R = \ell/N$ denotes the conference key rate, and N is the total data size of transmitted pulses. Here, we fix the security bound when considering statistical fluctuations analysis $\varepsilon = \varepsilon_1 = \varepsilon_2 = 10^{-10}$. The list of numerical experimental parameters is given in Table 1.

In Figure 1, we simulate the performance of the decoy-state MDI-QCKA in the asymptotic case. Here, we assume that three legitimate members are symmetrical in the system. p_1, p_2, $p_3 = 0$ means that randomness in the quantum-prepared operation is perfect, and p_1, p_2, $p_3 = 10^{-x}(x = 10, 8, 6)$ means that Eve can master different randomness information. As shown in the results, we can deduce that the lack of randomness on either side will cause information leakage and affect the generation of the conference key. Although Eve only masters one party randomness information for $p_1 = 10^{-10}$ and p_2, $p_3 = 0$, the maximum transmission distance dropped evidently from 207 km to 149 km. Particularly, when the parameters of weak randomness p_1, p_2, $p_3 = 10^{-6}$, the achievable transmission distance decreases to 132 km.

For the case with finite-key size, we simulate the conference key rate with the effects of weak randomness as shown in Figure 2. Here, we fixed the data size of the total transmitted signals $N = 10^{14}$. The results show that weak randomness evidently limits the conference key rate and achievable transmission distance. Although Eve only masters one party randomness information for $p_1 = 10^{-6}$, 10^{-5}, 10^{-4}, and p_2, $p_3 = 0$, the achievable transmission distance decreases to 26, 42, and 49 km, respectively. When the weak randomness parameters p_1, p_2, $p_3 = 10^{-6}$, 10^{-5}, 10^{-4}, the achievable transmission distance decreases to 34, 50, and 66 km, respectively.

As shown in Figure 3, the curves from right to left are acquired by the data size of transmitted pulses $N = 10^x(x = 15, 14, 13, 12)$. We can see that the greater the data size of the total transmitted pulses, the more obvious the effect of weak randomness. In detail, the achievable transmission distance decreases to 51.63%, 44.25%, 35.05%, and 23.75% when $N = 10^{15}$, 10^{14}, 10^{13}, 10^{12}, respectively. When the data size of the total transmitted signals increases, the number of quantum states attenuated increases. In the practical system, the leaked information may also increase because Eve can take advantage of the relationship between the expected values and observed values of different modulated states.

In order to further analyze the impact of weak randomness in the case of finite-key size, we consider the conference key rate for $N = 10^{14}$, 10^{13} with different weak randomness parameters $p_1, p_2, p_3 = 0, 10^{-x}(x = 6, 5, 4)$. As shown in Figure 4, we can notice that the conference key

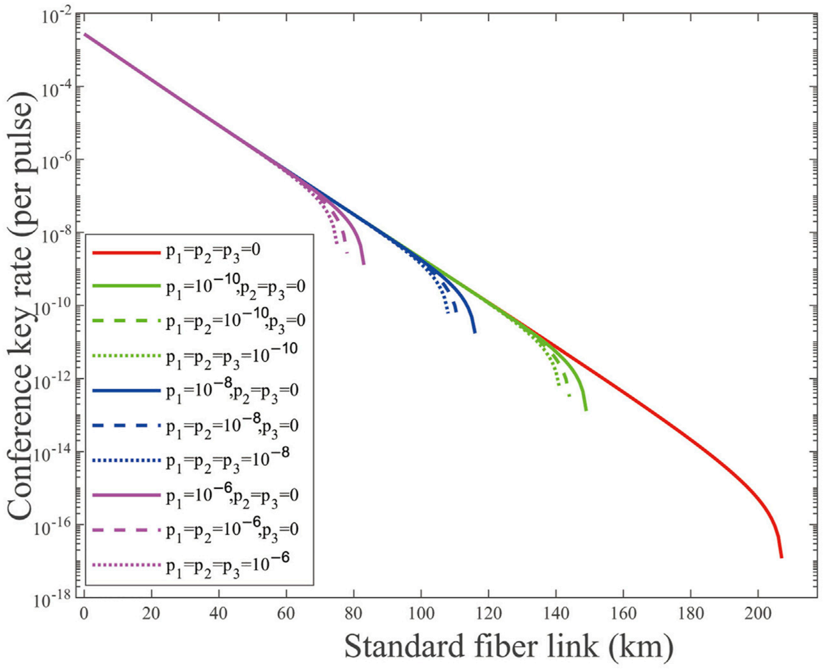

FIGURE 1
(Color online) Conference key rate (per pulse) on a logarithmic scale *vs.* transmission distance in the asymptotic case for $p_{1,2,3} = 0, 10^{-x}(x = 10, 8, 6)$. The solid lines are the results of weak randomness existing in one party, the dashed lines are the results of weak randomness existing in two parties, and the dotted lines are the results of weak randomness existing in three parties.

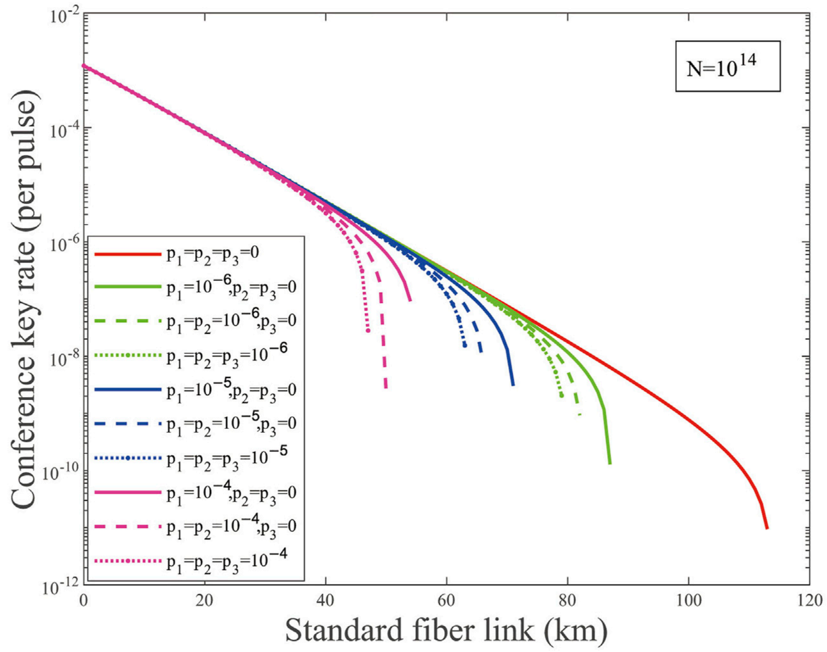

FIGURE 2
(Color online) Conference key rate (per pulse) on a logarithmic scale *vs.* transmission distance for $p_{1,2,3}$ = 0, 10^{-x}(x = 6, 5, 4) and the total number of transmitted signals N = 10^{14}. The solid lines are the results of weak randomness existing in one party, the dashed lines are the results of weak randomness existing in two parties, and the dotted lines are the results of weak randomness existing in three parties.

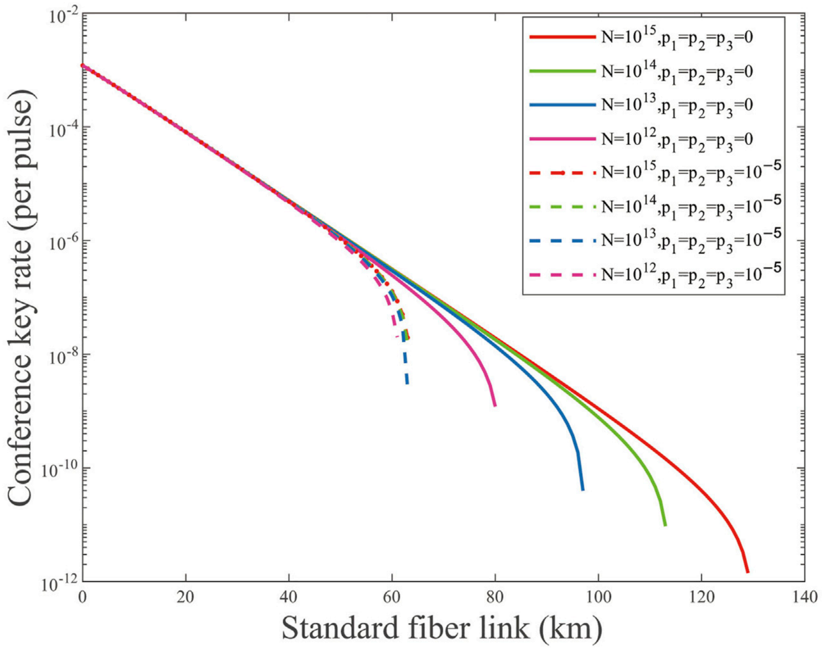

FIGURE 3
(Color online) Conference key rate (per pulse) on a logarithmic scale *vs.* transmission distance for $p_{1,2,3}$ = 0, 10^{-5} and different total numbers of transmitted signals N = 10^x(x = 15, 14, 13, 12). The solid lines are the results of $p_{1,2,3}$ = 0, and the dashed lines are the results of $p_{1,2,3}$ = 10^{-5}.

rate lines for $N = 10^{13}$ and $N = 10^{14}$ overlap approximately when the weak randomness parameters are $p_1, p_2, p_3 \geq 10^{-5}$. We also deduce that the impact of weak randomness on the conference key rate is stronger than the total data size of transmitted pulses when p_1, p_2, $p_3 \geq 10^{-5}$.

Finally, let $R(p)$ be the conference key rate with weak randomness and $R(0)$ be the conference key rate without weak randomness. The relationship between $R(p)/R(0)$ and transmission distance for p_1, p_2, p_3 = 0, 10^{-6} and $N = 10^{14}$ is shown in Figure 5. Compared with our

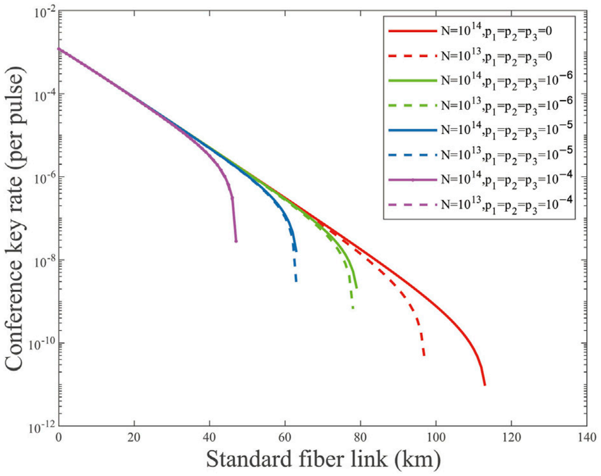

FIGURE 4
(Color online) Conference key rate (per pulse) on a logarithmic scale *vs.* transmission distance for $p_{1,2,3} = 0, 10^{-x} (x = 6, 5, 4)$ and different values of $N = 10^{14}, 10^{13}$. The solid lines are the results of $N = 10^{14}$, and the dashed lines are the results of $N = 10^{13}$.

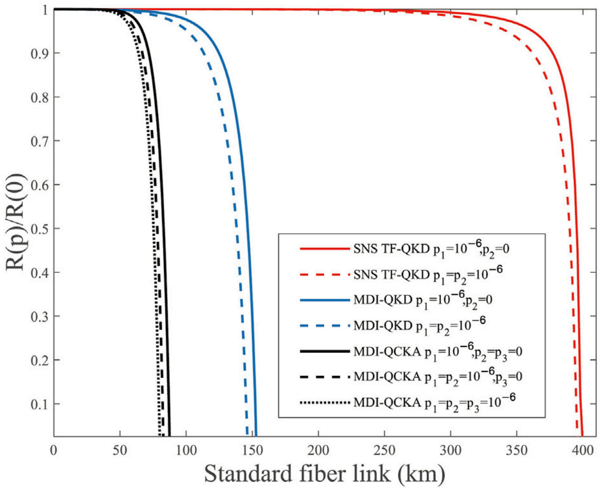

FIGURE 5
(Color online) $R(p)/R(0)$ *vs.* transmission distance with $p_1, p_2, p_3 = 0, 10^{-6}$ and $N = 10^{14}$. The red lines are the results of SNS TF-QKD, the blue lines are the results of MDI-QKD, and the black lines are the results of MDI-QCKA.

previous studies on MDI-QKD [32] and SNS TF-QKD [33], we can find that MDI-QCKA is more susceptible to weak randomness. In fact, all three legitimate members need to prepare quantum states in the practical MDI-QCKA system, and it is more difficult to protect random information than the other two. In addition, we notice that SNS TF-QKD can better resist weak random imperfection and realize longer transmission distance; therefore, we suspect that QCKA based on single-photon interference technology may perform better in resisting weak randomness, which deserves further study.

From the simulation results presented previously, we can find that the security of MDI-QCKA is sensitive to weak randomness in both asymptotic and finite-key size cases. Furthermore, we find that weak randomness damages the performance of MDI-QCKA to different degrees for different data sizes of the total transmitted signals. Finally, we conclude that QCKA based on the single-photon technology may be better resistant to weak random vulnerabilities.

5 Conclusion

In conclusion, we employ the weak randomness model to analyze the security of the decoy-state MDI-QCKA and study the performance of the decoy-state MDI-QCKA in both the asymptotic case and non-asymptotic case. The simulation results demonstrate that the weak randomness of the practical QCKA system is non-negligible. The conference key rate and achievable transmission distance will be significantly compromised due to the attenuation operation of Eve. Moreover, we find that weak randomness impacts the conference key rate differently for different data sizes of transmitted pulses and the impact may be greater than that of the data size of transmitted pulses in some cases. To avoid such a vulnerability risk in a QCKA system, two approaches can be considered. First, protecting randomness information from leakage. Second, the risk of the side channels at the source should be reduced and distinguishability of the quantum states in all degrees of freedom should be avoided. Compared with our previous work, we infer that QCKA based on single-photon interference technology may have more development prospects in resisting weak randomness, which is also our future research direction.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

Methodology: X-LJ; software: X-LJ and YW; writing—original draft preparation: X-LJ; writing—review and editing: Y-FL, CZ, J-JL, H-LZ, and M-SJ; supervision: W-SB; funding acquisition: W-SB and YW.

Funding

This research was funded by the National Natural Science Foundation of China (Grant No. 62101597), the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan (Grant No. 202300410534), and the Anhui Initiative in Quantum Information Technologies.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Bennett C, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing; 10-12 December 1984; Bangalore (1984). p. 175–9.

2. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. *Rev Mod Phys* (2020) 92:025002. doi:10.1103/revmodphys.92.025002

3. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, et al. Advances in quantum cryptography. *Adv Opt Photon* (2020) 12:1012–236. doi:10.1364/aop.361502

4. Cabello A. *Multiparty key distribution and secret sharing based on entanglement swapping* (2000). *arXiv preprint quant-ph/0009025*.

5. Chen K, Lo HK. Multi-partite quantum cryptographic protocols with noisy ghz states. *Qic* (2007) 7:689–715. doi:10.26421/qic7.8-1

6. Matsumoto R. Multiparty quantum-key-distribution protocol without use of entanglement. *Phys Rev A* (2007) 76:062316. doi:10.1103/physreva.76.062316

7. Murta G, Grasselli F, Kampermann H, Bruß D. Quantum conference key agreement: A review. *Adv Quan Tech* (2020) 3:2000025. doi:10.1002/qute.202000025

8. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Phys Rev Lett* (2012) 108:130503. doi:10.1103/physrevlett.108.130503

9. Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* (1999) 283:2050–6. doi:10.1126/science.283.5410.2050

10. Shor PW, Preskill J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys Rev Lett* (2000) 85:441–4. doi:10.1103/physrevlett.85.441

11. Fu Y, Yin HL, Chen TY, Chen ZB. Long-distance measurement-device-independent multiparty quantum communication. *Phys Rev Lett* (2015) 114:090501. doi:10.1103/PhysRevLett.114.090501

12. Chen R, Bao W, Zhou C, Li H, Wang Y, Bao H. Biased decoy-state measurement-device-independent quantum cryptographic conferencing with finite resources. *Opt Express* (2016) 24:6594–605. doi:10.1364/oe.24.006594

13. Wu Y, Zhou J, Gong X, Guo Y, Zhang ZM, He G. Continuous-variable measurement-device-independent multipartite quantum communication. *Phys Rev A* (2016) 93:022325. doi:10.1103/physreva.93.022325

14. Ottaviani C, Lupo C, Laurenza R, Pirandola S. Modular network for high-rate quantum conferencing. *Commun Phys* (2019) 2:1–6. doi:10.1038/s42005-019-0209-6

15. Zhu C, Xu F, Pei C. W-state analyzer and multi-party measurement-device-independent quantum key distribution. *Sci Rep* (2015) 5:17449–10. doi:10.1038/srep17449

16. Ribeiro J, Murta G, Wehner S. Fully device-independent conference key agreement. *Phys Rev A* (2018) 97:022307. doi:10.1103/physreva.97.022307

17. Holz T, Kampermann H, Bruß D. Genuine multipartite bell inequality for device-independent conference key agreement. *Phys Rev Res* (2020) 2:023251. doi:10.1103/physrevresearch.2.023251

18. Grasselli F, Kampermann H, Bruß D. Conference key agreement with single-photon interference. *New J Phys* (2019) 21:123002. doi:10.1088/1367-2630/ab573e

19. Zhao S, Zeng P, Cao WF, Xu XY, Zhen YZ, Ma X, et al. Phase-matching quantum cryptographic conferencing. *Phys Rev Appl* (2020) 14:024010. doi:10.1103/physrevapplied.14.024010

20. Cao XY, Gu J, Lu YS, Yin HL, Chen ZB. Coherent one-way quantum conference key agreement based on twin field. *New J Phys* (2021) 23:043002. doi:10.1088/1367-2630/abef98

21. Cao XY, Lu YS, Li Z, Gu J, Yin HL, Chen ZB. High key rate quantum conference key agreement with unconditional security. *IEEE Access* (2021) 9:128870–6. doi:10.1109/access.2021.3113939

22. Li Z, Cao XY, Li CL, Weng CX, Gu J, Yin HL, et al. Finite-key analysis for quantum conference key agreement with asymmetric channels. *Quan Sci. Technol.* (2021) 6:045019. doi:10.1088/2058-9565/ac1e00

23. Bai JL, Xie YM, Li Z, Yin HL, Chen ZB. Post-matching quantum conference key agreement. *Opt Express* (2022) 30:28865–81. doi:10.1364/oe.460725

24. Yin ZQ, Fung CHF, Ma X, Zhang CM, Li HW, Chen W, et al. Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Phys Rev A* (2013) 88:062322. doi:10.1103/physreva.88.062322

25. Tamaki K, Curty M, Kato G, Lo HK, Azuma K. Loss-tolerant quantum cryptography with imperfect sources. *Phys Rev A* (2014) 90:052314. doi:10.1103/physreva.90.052314

26. Pereira M, Curty M, Tamaki K. Quantum key distribution with flawed and leaky sources. *npj Quan Inf* (2019) 5:1–12. doi:10.1038/s41534-019-0180-9

27. Pereira M, Kato G, Mizutani A, Curty M, Tamaki K. Quantum key distribution with correlated sources. *Sci Adv* (2020) 6:eaaz4487. doi:10.1126/sciadv.aaz4487

28. Li HW, Yin ZQ, Wang S, Qian YJ, Chen W, Guo GC, et al. Randomness determines practical security of bb84 quantum key distribution. *Sci Rep* (2015) 5:16200–8. doi:10.1038/srep16200

29. Li HW, Xu ZM, Cai QY. Small imperfect randomness restricts security of quantum key distribution. *Phys Rev A* (2018) 98:062325. doi:10.1103/physreva.98.062325

30. Sun SH, Tian ZY, Zhao MS, Ma Y. Security evaluation of quantum key distribution with weak basis-choice flaws. *Sci Rep* (2020) 10:18145–8. doi:10.1038/s41598-020-75159-6

31. Zhang CM, Wang WB, Li HW, Wang Q. Weak randomness impacts the security of reference-frame-independent quantum key distribution. *Opt Lett* (2019) 44:1226–9. doi:10.1364/ol.44.001226

32. Jiang XL, Deng XQ, Wang Y, Lu YF, Li JJ, Zhou C, et al. Weak randomness analysis of measurement-device-independent quantum key distribution with finite resources. *Photonics* (2022) 9:356. doi:10.3390/photonics9050356

33. Jiang XL, Wang Y, Lu YF, Li JJ, Zhou C, Bao WS. Security analysis of sending or not-sending twin-field quantum key distribution with weak randomness. *Entropy* (2022) 24:1339. doi:10.3390/e24101339

34. Chernoff H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann Math Statist* (1952) 23:493–507. doi:10.1214/aoms/1177729330

35. Curty M, Xu F, Cui W, Lim CCW, Tamaki K, Lo HK. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat Commun* (2014) 5:3732–7. doi:10.1038/ncomms4732

36. Wang Y, Bao WS, Zhou C, Jiang MS, Li HW. Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources. *Phys Rev A* (2016) 94:032335. doi:10.1103/physreva.94.032335

37. Lütkenhaus N, Jahma M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J Phys* (2002) 4:44. doi:10.1088/1367-2630/4/1/344

38. Xu F, Curty M, Qi B, Lo HK. Practical aspects of measurement-device-independent quantum key distribution. *New J Phys* (2013) 15:113007. doi:10.1088/1367-2630/15/11/113007

39. Wang Y, Bao WS, Zhou C, Jiang MS, Li HW. Finite-key analysis of practical decoy-state measurement-device-independent quantum key distribution with unstable sources. *J Opt Soc Am B* (2019) 36:B83–B91. doi:10.1364/josab.36.000b83