photonics

MDPI

Article

Weak Randomness Analysis of Measurement-Device-Independent Quantum Key Distribution with Finite Resources

Xiao-Lei Jiang [1,2], Xiao-Qin Deng [1,2], Yang Wang [1,2,3,*], Yi-Fei Lu [1,2], Jia-Ji Li [1,2] and Chun Zhou [1,2] and Wan-Su Bao [1,2,*]

[1] Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, China; jxl@qiclab.cn (X.-L.J.); dxq@qiclab.cn (X.-Q.D.); lyf@qiclab.cn (Y.-F.L.); ljj@qiclab.cn (J.-J.L.); zc@qiclab.cn (C.Z.)

[2] Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China

[3] National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China

* Correspondence: wy@qiclab.cn (Y.W.); bws@qiclab.cn (W.-S.B.)

Abstract: The ideal quantum key distribution (QKD) protocol requires perfect random numbers for bit encoding and basis selecting. Perfect randomness is of great significance to the practical QKD system. However, due to the imperfection of practical quantum devices, an eavesdropper (Eve) may acquire some random numbers, thus affecting the security of practical systems. In this paper, we analyze the effects of the weak randomness in the measurement-device-independent QKD (MDI-QKD) with finite resources. We analytically derive concise formulas for estimating the lower bound of the single-photon yield and the upper bound of the phase error rate in the case of the weak randomness. The simulation demonstrates that the final secret key rate of MDI-QKD with finite resources is sensitive to state preparation, even with a small proportion of weak randomness, the secure key rate has a noticeable fluctuation. Therefore, the weak randomness of the state preparation may bring additional security risks. In order to ensure the practical security of the QKD system, we are supposed to strengthen the protection of state preparation devices.

Keywords: quantum key distribution; weak randomness; security analysis; finite resources

check for updates

Citation: Jiang, X.-L.; Deng, X.-Q.; Wang, Y.; Lu, Y.-F.; Li, J.-J.; Zhou, C.; Bao, W.-S. Weak Randomness Analysis of Measurement-Device-Independent Quantum Key Distribution with Finite Resources. *Photonics* **2022**, *9*, 356. https://doi.org/10.3390/photonics9050356

Received: 27 April 2022
Accepted: 16 May 2022
Published: 18 May 2022

1. Introduction

Theoretically, the quantum key distribution (QKD) can provide unconditional security for confidential communications of two legitimate parties, Alice and Bob [1]. Unfortunately, because of the imperfection of the practical system, many quantum attacks may take advantage of the loopholes introduced by imperfect devices [2–4], such as the wavelength attack [5], the detector control attack [6,7], the Trojan horse attack [8,9]. Actually, such kinds of attack methods have been experimentally demonstrated on QKD systems and cannot be ignored in terms of practical security.

In order to overcome the practical QKD system security threat, proposing new protocols and security patching have been two main solutions. Lo et al. proposed [10] the measurement-device-independent QKD (MDI-QKD) protocol, which is immune to all detector channel attacks without making any security assumptions about the quantum devices. Recently, twin-field QKD (TF-QKD) [11] and the asynchronous MDI-QKD [12] have been proposed, respectively. Their key rate can exceed the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [13]. Both MDI-QKD and TF-QKD have made significant progress in term of theory and experiment [14–32]. Although MDI-QKD and TF-QKD can resist all attacks on quantum state measurement devices, Eve may shift their target to quantum state preparation devices [33–38].

It has been hypothesized that Eve may control imperfect quantum state preparation devices so that bit encoding and measurement basis selection may be nonrandomly modulated in a practical QKD system [39]. Because of the quantum state preparation vulnerability of the weak randomness, a security evaluation of the weak randomness is of great significance in the practical QKD system. Based on this practical security threat, Li et al. proposed [40] a weak randomness model of the BB84 protocol. Under the model, the quantum states which Alice prepared are divided into two parts: the random part and the non-random part where the non-random part may be controlled by Eve to acquire more information. Zhang et al. [41] also analyzed reference-frame-independent QKD (RFI-QKD) security under the impact of the weak randomness, and briefly discussed the RFI-MDI-QKD under weak randomness.

In this paper, we will analyze the effects of weak randomness in vacuum + weak decoy-state MDI-QKD with finite resources [42–46] based on the universally composable framework. Here, we will present a tight security analysis in MDI-QKD with finite resources. In analyzing the weak randomness in MDI-QKD, we assume that the quantum states prepared by both Alice and Bob could be controlled by Eve with a certain probability [47], but Eve does not necessarily have the same abilities to control Alice or Bob. We also suppose that the quantum states prepared by both Alice and Bob are controlled by hidden variables λ and δ from Eve, where λ determines the quantum states prepared by Alice, δ determines the quantum states prepared by Bob. The non-random probability of quantum states prepared by Alice is p_1, and the random probability is $1 - p_1$. The non-random probability of quantum states prepared by Bob is p_2, and the random probability is $1 - p_2$. When $p_1 = 1$ or $p_2 = 1$, it shows that Eve can obtain all the information, that is, $R = 0$. When $p_1 = p_2 = 0$, it indicates that Eve cannot directly acquire information, so the security can be assured. When $0 < p_1 < 1, 0 < p_2 < 1$, the weak randomness model could be applied to estimate the amount of the leaked information obtained by Eve. From the experimental parameters, we deduce that the weak randomness of the state preparation has threatened the security of MDI-QKD, and MDI-QKD with finite resources has extremely strict requirements of state preparation. We should put forward higher requirements of state preparation randomness to ensure the practical security of the QKD system.

The rest of paper is organized as follows: we describe a practical vacuum + weak decoy-state MDI-QKD protocol with biased basis choice in Section 2. In Section 3, we present the weak randomness analysis for the protocol with finite resources and deduce concise formulas of bounding the yield and the bit error rate for the single-photon events. The numerical simulations are shown in Section 4 and the conclusion is summarized in Section 5.

2. Protocol Description

In a practical QKD system, we usually choose the weak coherent state source, which contains the vacuum state, the single photon state and the multiphoton state, instead of the single photon source. We focus on the vacuum + weak decoy-state MDI-QKD, and the description of the protocol is presented as follows [48]:

1. Preparation: Alice and Bob randomly modulate the intensities $\alpha_a \in \mathrm{A} = \{\mu_a, v_a, 0\}$ and $\beta_b \in \mathrm{B} = \{\mu_b, v_b, 0\}$ with probability of $p_{\mu_a}, p_{v_a}, p_{0_a} = 1 - p_{\mu_a} - p_{v_a}$ and $p_{\mu_b}, p_{v_b}, p_{0_b} = 1 - p_{\mu_b} - p_{v_b}$, respectively. Where $\mu_{a(b)}$ is the signal state intensity, $v_{a(b)}$ is the decoy state intensity, 0 is the vacuum state. For signal states, Alice and Bob only choose the Z basis. For decoy states, Alice and Bob randomly choose a bit value from $\{0, 1\}$, and select Z basis and X basis in probability of p_z and $1 - p_z$, respectively. Finally, they prepared a phase randomized, weak coherent pulse based on the selected value and send it to Charlie via a quantum channel.
2. Measurement and alignment: Charlie performs Bell state measurements (BSM) of pulses from Alice and Bob, and then publishes the measurements to Alcie and Bob. Both parties conduct basis alignment in open channel and compare their intensity: $\mu_a(v_a), \mu_b(v_b)$. They retain correct measurement results and discard mismatched measurement results. At this time, the number of pulses successfully detected in

the Z basis and X basis are n_{ab}^{Z} and n_{ab}^{X}, and the subscript indicates the intensity combinations chosen by Alice and Bob: $\{\mu_a\mu_b, \mu_a v_b, v_a\mu_b, v_a v_b, \mu_a 0, v_a 0, 0\mu_b, 0v_b\}$.

3. Parameter estimation: Firstly, Alice and Bob calculate the number of bit error in X basis m_{ab}^{X}. Second, they calculate the number of successful measurement results corresponding to the single photon pulse in Z basis s_{11}^{Z} and the number of phase error c_{11}^{Z}. Finally, they calculate the phase error rate in Z basis $e_{ph} = c_{11}^{Z}/s_{11}^{Z} \le \tilde{e}_{ph}$, where $\tilde{e}_{ph}$ refers to the phase bit error rate which needs to be met. Execution continues if complied, otherwise the agreement will be terminated.
4. Post-processing: Alice and Bob perform error correction, and the process consumes information at most as $leak_{EC}$ bits. They also use hash functions to perform error verification to ensure that both parties get the same key, and it requires consumption information of $\log_2 \frac{2}{\varepsilon_{cor}}$ bits, where ε_{cor} is the probability of passing the error verification process for the key pairs (X_A, X_B). In the end, after the two parties perform the secret amplification operation, the key pairs are obtained by Alice is S_A, and the key pairs obtained by Bob is S_B.

3. Security Analysis

3.1. Security Bound

We first introduce the universally composable framework:

Definition 1 ([42]). *If the key pairs (S_A, S_B) generated by Alice and Bob satisfy the following conditions, the protocol is said to be ε-secure:*

- *Correctness. If the probability of keys S_A, S_B being not identical is maximal ε_{cor}, the keys are said to be ε_{cor}-correct :*
$$Pr(S_A \neq S_B) \le \varepsilon_{cor},$$
- *Screcy. The keys S_A, S_B are said to be ε_{sec}-secure with respect to the Eve holding a quantum system E if:*
$$\frac{1}{2} p_{abort} \|\rho_{AE} - \rho_U \otimes \rho_E\| \le \varepsilon_{\text{sec}},$$
$$\frac{1}{2} p_{abort} \|\rho_{BE} - \rho_U \otimes \rho_E\| \le \varepsilon_{\text{sec}}.$$

where p_{abort} denotes the probability of protocol failure aborted, $\rho_{AE}(\rho_{BE})$ denotes the classical-quantum states of the system for Alice (Bob) and system E, and ρ_U denotes the fully mixed state on S_A or S_B.

The entropic uncertainty relation to establish a bound on the smooth min-entropy of the raw key conditioned on Eve's information based on the composable security definition has been extended to the case with finite resources [43]. Here, we do the finite-key analysis based on the composable framework. The length of ε-secure keys in the Z basis is presented as follows [45]:

$$\ell \ge s_0^{Z} + s_{11}^{Z,L}\left[1 - H\left(e_{ph}^{U}\right)\right] - leak_{EC} - 6\log_2 \frac{21}{\varepsilon_{\text{sec}}} - \log_2 \frac{2}{\varepsilon_{cor}}. \tag{1}$$

with ε_{cor}-correct and ε_{sec}-secure, where s_0^{Z} refers to the number of measurement events when one party sends a vacuum state and Charlie obtains a successful BSM. s_{11}^{Z} and e_{ph}^{U} are the lower bound of the single photon count rate and the upper bound of the phase error rate in Z basis, respectively. $H(x) = -\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, and $leak_{EC}$ is the number of bits consumed in the post-processing step.

3.2. Parameter Estimation

First of all, we consider the state preparation stage with weak randomness, supposing that Alice and Bob prepare binary set of bits S and T, respectively, to randomly encode the bit and select the basis. We apply $|S|, |T|$ representing the number of elements of the set S and T, respectively. Due to the imperfection of the quantum devices, a part of the set S and T can be mastered by Eve. For the set of quantum states prepared by Alice, which is consisted of random part S_1 and non-random part S_2. For the set of quantum states prepared by Bob, which is consisted of random part T_1 and non-random part T_2. This assumption is reasonable by considering two cases: the first one is that the random number generator devices may be imperfect so that part of the random numbers may be leaked to Eve. The second one is that the imperfect state modulation may be prepared by different laser diodes from Alice and Bob, which can be partly distinguished by observing the properties of the spectrum, timing sequence. We define the probability of non-random parameter at Alice as $p_1 = \frac{|S_2|}{|S|}$, the probability of non-random parameter at Bob as $p_2 = \frac{|T_2|}{|T|}$. In a practical QKD system, we cannot guarantee the attack capabilities of Eve against Alice is the same as Bob, so we cannot ensure $p_1 = p_2$. For the weak randomness condition, quantum states prepared by Alice and Bob in the practical system could be expressed as follows:

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

$$\rho'_{\text{Bob}} = \frac{p_2}{2} \sum_{\beta=0,1} |\beta\rangle\langle\beta|_{Bob} \otimes |\beta\rangle\langle\beta|_{Eve} + (1-p_2)\rho_{Bob} \otimes |2\rangle\langle 2|_{Eve}. \tag{3}$$

where the quantum states prepared by Alice and Bob can be divided into two parts: the first term on the right-hand side of Equations (2) and (3) denote that the quantum states are prepared from a non-random set, the second term denote that the quantum states are prepared from a random set. The auxiliary quantum state of Eve is related to the system of Alice (Bob). For the system of Alice, if the auxiliary quantum state of Eve is $|\alpha\rangle\langle\alpha|_{Eve}$, it indicates that Eve can obtain the key of Alice α. For the system of Bob, if the auxiliary quantum state of Eve is $|\beta\rangle\langle\beta|_{Eve}$, it indicates that Eve can obtain the key of Bob β. For the system of Alice and Bob, if the auxiliary quantum state of Eve is $|2\rangle\langle 2|_{Eve}$, it indicates that Alice and Bob prepared the perfect BB84 quantum states ρ_{Alice} and ρ_{Bob}, and Eve cannot distinguish different encoding states at this point. Eve can distinguish random part S_1 and non-random part S_2 of Alice by observing auxiliary quantum states (and the random part T_1 and non-random part T_2 of Bob). The practical QKD system requires completely true random numbers for preparing quantum states. However, the weak randomness of practical QKD systems is universal because of the imperfection of quantum devices.

Note that the weak coherent state source encoding can be supposed to be a special non-random encoding case in the practical MDI-QKD system, where the quantum states from non-random part can be detected by exploiting the photon number splitting(PNS) attack. If the mean photon number of the weak coherent source is μ, the probability of non-random is the probability of multiphoton $p_{1(2)}$. Actually, the PNS attack can be detected by applying the decoy-state method. However, because of the device variances, the weak randomness attack cannot be detected by utilizing the decoy-state method.

Under the weak randomness model, Eve wants to acquire more information so we can assume that Eve only performs a certain probability attenuation operation on the quantum states of the random part, and does not perform on the quantum states of the non-random part. Then we can suppose that the final bit error only come from the random part, and the non-random part does not produce the bit error. Based on the attenuation operation, the nonrandom probability in Charlie's side can be amplified by considering the signal loss so that the maximal transmission distance may be decreased seriously. Moreover, because of the attenuation operation of the attacker, the single photon successful gain under Z basis is reduced, and the bit error rate under X basis is doubled, so the length of the final security key may be significantly reduced. The specific parameters are estimated as follows:

Firstly, let s^Z_{nm} be the total numbers of successful detection events Charlie obtains when Alice and Bob prepare n-photon states and m-photon states in Z basis, and n^Z be the total numbers of events when quantum states are prepared by Alice and Bob in Z basis and are successfully detected by Charlie. For $\{\mu_a\mu_b, \mu_a v_b, v_a\mu_b, v_a v_b, \mu_a 0, v_a 0, 0\mu_b, 0v_b\}$, the expected value of n^Z_{ab} can be expressed as:

$$\bar{n}^Z_{ab} = \sum_{n,m=0}^{\infty} p^Z_{ab|nm} s^Z_{nm}, \tag{4}$$

where $p^Z_{ab|nm}$ is the conditional probabilities that Alice and Bob prepared n-photon states and m-photon states in Z basis with intensity $\{\mu_a\mu_b, \mu_a v_b, v_a\mu_b, v_a v_b, \mu_a 0, v_a 0, 0\mu_b, 0v_b\}$. Based on Bayes' rule, it can be expressed as:

$$p^Z_{ab|nm} = \frac{p^Z_{ab}}{\tau^Z_{ab}} p_{a|n} p_{b|m}. \tag{5}$$

where $\tau^Z_{ab} = \sum p^Z_{ab} \frac{e^{-a-b} a^n b^m}{n!m!}$ is the probability of Alice and Bob prepared n-photon states and m-photon states in Z basis, and p^Z_{ab} is the probability of Alice and Bob modulate the intensity α_a and β_b in Z basis. $p_{a|n}$ and $p_{b|m}$ is the photon number distributions of Alice and Bob, respectively.

Subsequently, for the case of weak randomness model, the probability of quantum states prepared by Alice with non-randomness is p_1, and the probability of quantum states prepared by Bob with non-randomness is p_2. The probability of single-photon states prepared by both parties with randomness state is $\tau_{11}(1-p_1)(1-p_2)$, and the probability with non-randomness is $\tau_{11}(1-(1-p_1)(1-p_2)) = \tau_{11}(p_1+p_2-p_1p_2)$. The probability with randomness when only one party prepares a single photon state is $\tau_{01}(1-p_1)(1-p_2)$, the probability with non-randomness is $\tau_{01}(1-(1-p_1)(1-p_2)) = \tau_{01}(p_1+p_2-p_1p_2)$. In a practical quantum system, Eve may attenuate the quantum states prepared by Alice and Bob. Considering the weak randomness attenuation, signal loss may happen in random set $S_1(T_1)$, but all quantum states prepared in non-random set $S_2(T_2)$ arrive to Charlie without signal loss. The probability of signal loss both two parties prepare and send single photon state in random set under Z basis is:

$$p^Z_{loss} = \frac{s^Z_{11} - \tau^Z_{11}(p_1+p_2-p_1p_2)N}{N-(p_1+p_2-p_1p_2)N}, \tag{6}$$

the proportion of quantum states arriving at Charlie with non-randomness is:

$$p^Z_{non-rand} = \frac{\tau^Z_{11}(p_1+p_2-p_1p_2)N}{s^Z_{11}}, \tag{7}$$

the proportion of quantum states arriving at Charlie with randomness is:

$$p^Z_{rand} = \frac{s^Z_{11} - \tau^Z_{11}(p_1+p_2-p_1p_2)N}{s^Z_{11}}, \tag{8}$$

where N is the total number of transmitting signals.

Considering independent event conditions, we exploit $Chernoff$ bound [49] to perform finite-size key analysis on MDI-QKD. For the finite sample sizes, the number of practical measurement events can be satisfied [48]:

$$\left|\bar{n}^Z_{ab} - n^Z_{ab}\right| \le \delta\left(n^Z_{ab}, \varepsilon_1\right), \tag{9}$$

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

Additionally, let s_{nm}^{X} be the total numbers of Charlie acquiring the successful detection events when Alice and Bob prepare n-photon states and m-photon states in X basis, and v_{nm}^{X} be the corresponding number of bit error. m_{ab}^{X} is the total amounts of bit error when Alice sends states in X basis and $m_{ab}^{X} = \sum\limits_{n,m=0} v_{nm}^{X}$. For $\{\mu_a\mu_b, \mu_a v_b, v_a\mu_b, v_a v_b, \mu_a 0, v_a 0, 0\mu_b, 0v_b\}$, the expected numbers of bit error m_{ab}^{X} can be expressed as:

$$\bar{m}_{ab}^{X} = \sum_{n,m=0}^{\infty} p_{ab|nm}^{X} v_{nm}^{X}, \tag{10}$$

where $p_{ab|nm}^{X}$ is the conditional probabilities that Alice and Bob prepare n-photon states and m-photon states in X basis with $\{\mu_a\mu_b, \mu_a v_b, v_a\mu_b, v_a v_b, \mu_a 0, v_a 0, 0\mu_b, 0v_b\}$. Based on Bayes' rule, it can be expressed as:

$$p_{ab|nm}^{X} = \frac{p_{ab}^{X}}{\tau_{ab}^{X}} p_{a|n} p_{b|m}. \tag{11}$$

where $\tau_{ab}^{X} = \sum p_{ab}^{X} \frac{e^{-a-b} a^n b^m}{n!m!}$ the probability of Alice prepare n-photon states and Bob and m-photon states in X basis. p_{ab}^{X} is the probability that Alice and Bob modulate the intensity μ_a and β_b in X basis, and $p_{a|n}$ and $p_{b|m}$ is the photon number distributions of Alice and Bob, respectively.

Similarly, within the independent event conditions, for the finite sample sizes, the $\bar{m}_{ab}^{X}$ under the $chernoff$ bound can be satisfied [48]:

$$\left|\bar{m}_{ab}^{X} - m_{ab}^{X}\right| \leq \delta\left(m_{ab}^{X}, \varepsilon_2\right), \tag{12}$$

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

Actually, the probability of signal loss both two parties prepare and send single photon state in random set under X basis is:

$$p_{loss}^{X} = \frac{s_{11}^{X} - \tau_{11}^{X}(p_1 + p_2 - p_1 p_2)N}{N - (p_1 + p_2 - p_1 p_2)N}, \tag{13}$$

the proportion of quantum states arriving at Charlie with non-randomness is:

$$p_{non-rand}^{X} = \frac{\tau_{11}^{X}(p_1 + p_2 - p_1 p_2)N}{s_{11}^{X}}, \tag{14}$$

the proportion of quantum states arriving at Charlie with randomness is:

$$p_{rand}^{X} = \frac{s_{11}^{X} - \tau_{11}^{X}(p_1 + p_2 - p_1 p_2)N}{s_{11}^{X}}. \tag{15}$$

Note that, only the single-photon pulses from the random set can be used to generate secret keys. In analyzing the impacts of weak randomness, the number of single photon sent by both parties in Z basis which cannot generate secret keys is as follows:

$$\tilde{s}_{11}^{Z} = \tau_{11}^{Z}(1 - p_1)(1 - p_2)N, \tag{16}$$

the number of single photon sent by both parties which can generate secret keys satisfies:

$$s_{11}' \geq s_{11}^{Z,L} - \tilde{s}_{11'}^{Z}, \tag{17}$$

the lower bound of the number of single photons sent by one party in Z basis which cannot generate secret keys is as follows:

$$\tilde{s}_0^Z = \tau_{01}^Z(1-p_1)(1-p_2)N, \tag{18}$$

the number of single photon sent by one party which can generate secret keys satisfies:

$$s_0' \geq s_0^Z - \tilde{s}_0^Z ., \tag{19}$$

where the lower bound of the successful counts of the single photon sent by two parties in Z basis $s_{11}^{Z,L}$ satisfies [50]:

$$\begin{aligned} s_{11}^{Z,L} \geq & \Big[\Big(p_{1|v_a} p_{2|\mu_a} p_{1|v_b} p_{2|\mu_b} - p_{2|v_a} p_{1|\mu_a} p_{2|v_b} p_{1|\mu_b} \Big) N_{v_a v_b}^Z - p_{1|v_b} p_{2|v_b} (p_{1|v_a} p_{2|\mu_a} - p_{2|v_a} p_{1|\mu_a}) N_{v_a \mu_b}^Z \\ & - p_{1|v_a} p_{2|v_a} (p_{1|v_b} p_{2|\mu_b} - p_{2|v_b} p_{1|\mu_b}) N_{\mu_a v_b}^Z \Big] \times \frac{\tau_{11}^Z}{p_{1|v_a} p_{1|v_b} (p_{1|v_a} p_{2|\mu_a} - p_{2|v_a} p_{1|\mu_a})(p_{1|v_b} p_{2|\mu_b} - p_{2|v_b} p_{1|\mu_b})}, \end{aligned} \tag{20}$$

the number of successful counts of the single photon sent by one party in Z basis satisfies:

$$s_0^Z = e^{-\mu_a} n_{0\mu_b}^Z + e^{-v_a} n_{0\mu_b}^Z + e^{-\mu_a} n_{0v_b}^Z + e^{-v_a} n_{0v_b}^Z, \tag{21}$$

where

$$N_{v_a v_b}^Z = \frac{n_{v_a v_b}^{Z,L}}{p_{v_a} p_{v_b} p_Z} - \frac{p_{0|v_a} n_{0v_b}^{Z,U}}{p_{0_a} p_{v_b} p_Z} - \frac{p_{0|v_b} n_{v_a 0}^{Z,U}}{p_{v_a} p_{0_b} p_Z} + \frac{p_{0|v_a} p_{0|v_b} n_{00}^{Z,L}}{p_{0_a} p_{0_b}}, \tag{22}$$

$$N_{v_a \mu_b}^Z = \frac{n_{v_a \mu_b}^{Z,U}}{p_{v_a} p_{v_b} p_Z} - \frac{p_{0|v_a} n_{0\mu_b}^{Z,L}}{p_{0_a} p_{\mu_b} p_Z} - \frac{p_{0|\mu_b} n_{v_a 0}^{Z,L}}{p_{v_a} p_{0_b} p_Z} + \frac{p_{0|v_a} p_{0|\mu_b} n_{00}^{Z,U}}{p_{0_a} p_{0b}}, \tag{23}$$

$$N_{\mu_a v_b}^Z = \frac{n_{\mu_a v_b}^{Z,U}}{p_{\mu_a} p_{v_b} p_Z} - \frac{p_{0|\mu_a} n_{0v_b}^{Z,L}}{p_{0_a} p_{v_b} p_Z} - \frac{p_{0|v_b} n_{\mu_a 0}^{Z,L}}{p_{\mu_a} p_{0_b} p_Z} + \frac{p_{0|\mu_a} p_{0|\mu_b} n_{00}^{Z,U}}{p_{0_a} p_{0b}}. \tag{24}$$

in the same way, we deduce the lower bound $n_{ab}^{Z,L}$ and upper bound $n_{ab}^{Z,U}$ of n_{ab}^Z by applying the $Chernoff$ bound.

Under the weak randomness condition, due to the attenuation operation of the attacker on the quantum channel, the probability of non-randomness in Charlie increases, so the bit error rate in X basis satisfies:

$$e_b' = e_b^X \frac{Y_{11}^X}{Y_{11}^X - (p_1 + p_2 - p_1 p_2)}, \tag{25}$$

where Y_{11}^X is the number of single photons yield in the X basis, it satisfies [50]:

$$\begin{aligned} Y_{11}^X = & \Big[\Big(p_{1|v_a} p_{2|\mu_a} p_{1|v_b} p_{2|\mu_b} - p_{2|v_a} p_{1|\mu_a} p_{2|v_b} p_{1|\mu_b} \Big) N_{v_a v_b}^X - p_{1|v_b} p_{2|v_b} (p_{1|v_a} p_{2|\mu_a} - p_{2|v_a} p_{1|\mu_a}) N_{v_a \mu_b}^X \\ & - p_{1|v_a} p_{2|v_a} (p_{1|v_b} p_{2|\mu_b} - p_{2|v_b} p_{1|\mu_b}) N_{\mu_a v_b}^X \Big] \times \frac{1}{p_{1|v_a} p_{1|v_b} (p_{1|v_a} p_{2|\mu_a} - p_{2|v_a} p_{1|\mu_a})(p_{1|v_b} p_{2|\mu_b} - p_{2|v_b} p_{1|\mu_b})}, \end{aligned} \tag{26}$$

in fact, the bit error rate in X basis without weak randomness is:

$$e_b^X = \frac{v_{11}^{X,U}}{s_{11}^{X,L}}, \tag{27}$$

the upper bound of the number of single photon bit error in X basis satisfies:

$$v_{11}^{X,U} \leq \frac{\tau_{11}^X M_{v_a v_b}^X}{p_{1|v_a} p_{1|v_b}}, \tag{28}$$

where

$$M^{X}_{v_a v_b}=\frac{m^{X,U}_{v_a v_b}}{p_{v_a}p_{v_b}p_X}-\frac{p_{0|v_a}m^{X,L}_{0v_b}}{p_{0_a}p_{v_b}p_X}-\frac{p_{0|v_b}m^{X,L}_{v_a 0}}{p_{v_a}p_{0_b}p_X}+\frac{p_{0|v_a}p_{0|v_b}n^{x,U}_{00}}{p_{0_a}p_{0_b}}. \tag{29}$$

here, $m^{X,L}_{ab}$ and $m^{X,U}_{ab}$ is the lower and upper bound of m^{X}_{ab}, respectively, and they can be obtained by the $Chernoff$ bound.

When Alice and Bob prepare single photon states in X basis, exploiting the same calculation methods we can acquire the total numbers of successful detection events Charlie obtains in X basis s^{X}_{11} comparable to the total number of successful detection events Charlie obtains in the Z basis s^{Z}_{11}.

In asymptotic conditions, we can assume that the phase bit error rate in Z basis is equal to the bit error rate in X basis, that is, $e_{ph}=e^{X}_{b}$. However, under the condition of the finite length of the key, there is a deviation between e_{ph} and e'_b. We suppose the deviation between the two is θ. Exploiting the random sampling method of Fung et al. [51], we can estimate the phase error rate of the single photon events:

$$\Pr(e_{ph}\geq e'_b+\theta)\leq\frac{\sqrt{s^{X,L}_{11}+s^{Z,L}_{11}}}{\sqrt{e'_b(1-e'_b)s^{X,L}_{11}s^{Z,L}_{11}}}2^{-(s^{X,L}_{11}+s^{Z,L}_{11})\sigma(\theta)}, \tag{30}$$

where

$$\sigma(\theta){=}H(e'_b+\theta-\frac{s^{X,L}_{11}}{s^{X,L}_{11}+s^{Z,L}_{11}}\theta)-(1-\frac{s^{X,L}_{11}}{s^{X,L}_{11}+s^{Z,L}_{11}})H(e'_b+\theta)-\frac{s^{X,L}_{11}}{s^{X,L}_{11}+s^{Z,L}_{11}}H(e'_b), \tag{31}$$

for a given probability of failure ε_{sec}:

$$\varepsilon_{\text{sec}}=\frac{\sqrt{s^{X,L}_{11}+s^{Z,L}_{11}}}{\sqrt{e'_b(1-e'_b)s^{X,L}_{11}s^{Z,L}_{11}}}2^{-(s^{X,L}_{11}+s^{Z,L}_{11})\sigma(\theta)}, \tag{32}$$

it can be calculated from $\theta=g(\varepsilon_{\text{sec}},e'_b,s^{X,L}_{11},s^{Z,L}_{11})$,where

$$g(a,b,c,d)=\sqrt{\frac{(c+d)(1-b)b}{cd\ln 2}\log_2(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2})}, \tag{33}$$

the upper bound of the phase error rate of the single-photon events in Z basis e_{ph} can be expressed as :

$$e^{U}_{ph}\leq e'_b+g(\varepsilon_{\text{sec}},e'_b,s^{X,L}_{11},s^{Z,L}_{11}), \tag{34}$$

According to Equations (17), (19) and (34), we can calculate the length of final security key of the decoy-state MDI-QKD protocol with the weak randomness:

$$\ell'\geq s'_0+s'_{11}\left[1-H\left(e^{U}_{ph}\right)\right]-leak_{EC}-6\log_2\frac{21}{\varepsilon_{\text{sec}}}-\log_2\frac{2}{\varepsilon_{cor}}. \tag{35}$$

4. Numerical Simulations and Discussions

In this section, we numerically simulate the performance of effects of weak randomness on MDI-QKD with finite resources. We consider a fiber-based channel model and experimental parameters from [44], and define α = 0.2 (dm/km) as the fiber loss coefficient, $\eta_d=0.145$ as the detection efficiency of the relay Charlie, and $p_d=6\times10^{-7}$ as the dark count for detectors. L is the length of fiber between Charlie and Alice (Bob). The security bound is fixed to $\varepsilon=10^{-10}$, and $f=1.16$ is the efficiency of error correction. $R=\ell/N$ is the secret key rate, where N is the total number of transmitting signals sent by Alice. The numerical parameters are listed in Table 1.

Table 1. List of experimental parameters applied in the numerical simulation in the following table: α (dm/km) is the loss coefficient of the fiber, f is the efficiency of error correction, η_d is the efficiency for the Charlie-side detector, e_d is the optical misalignment error rate, p_d is the dark count for detectors, and ε is the predetermined security bound.

α	f	η_d	e_d	p_d	ε
0.2	1.16	0.145	0.015	6×10^{-7}	10^{-10}

Firstly, we analyze the effects of weak randomness existing only one party (Alice or Bob) in Figure 1, where we suppose Alice and Bob are symmetrical in the practical QKD system. Here, we assume $p_2 = 0$ which means that Eve just masters the randomness information of Alice. $p_1 = 0, 10^{-x}(x = 6, 5, 4, 3)$ means that Eve has different abilities of mastering the randomness information of Alice. As shown in Figure 1, the dashed lines from right to left are obtained for different weak randomness parameters $p_1 = 0, 10^{-x}(x = 6, 5, 4, 3)$ with the fixed finite number of total pulses $N = 10^{15}$. We can deduce that although Eve just masters the randomness information of one party when $N = 10^{15}$, the generation of the security key rate will be seriously affected, and the security key is no longer being generated when $p_1 \geq 10^{-3}$. Particularly, when the parameter of weak randomness p_1 rises from 0 to 10^{-3}, the achievable transmission distance declines from 182 km to 36 km.

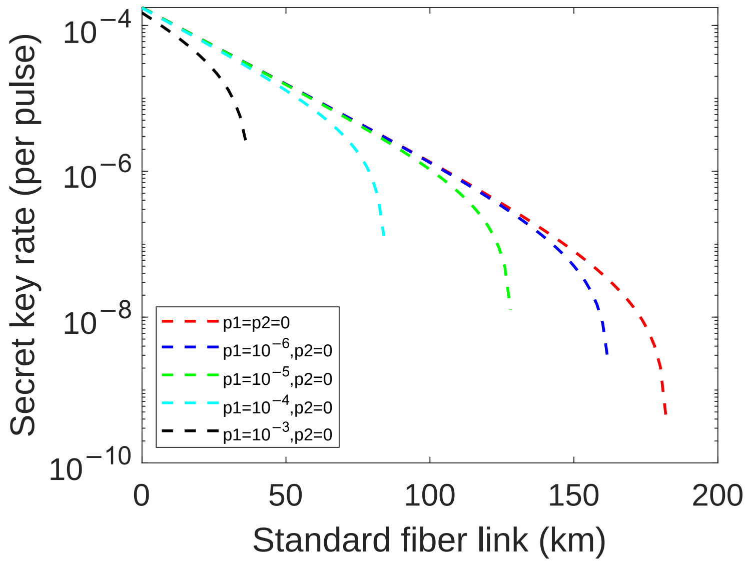

Figure 1. (Color online) The secret key rates (per pulse) in logarithmic scale versus transmission distance between Alice and Bob when just one party exists the weak randomness parameters and $p_1 = 0, 10^{-x}(x = 6, 5, 4, 3)$ (curves from right to left) and another one do not exist weak randomness $p_2 = 0$ for fixed $N = 10^{15}$.

Actually, compared with the general BB84 protocol, the MDI-QKD protocol is more vulnerable to the weak randomness of state preparation. The reason is that both of Alice and Bob perform the state preparation operation, which is different from BB84 protocol where just Alice performs the state preparation operation. In the practical MDI-QKD system, the possibility of the random number for bit encoding and basis selecting leaked to Eve may be greater because of the imperfection of the quantum devices.

Moreover, considering the practical MDI-QKD system with finite resources, we divide the weak randomness model into two cases. The first one is that the signal states and the decoy states may be modulated with the same laser diode by Alice and Bob so that both of the signal states and decoy states in Alice and Bob will be modulated with the same non-random probability p_1 and p_2. The second one is that the signal states and the decoy states may be modulated with the different laser diode by Alice and Bob. The signal states and the decoy states which are prepared by Alice and Bob are supposed to be distinguished with the nonrandom probability p_1 and p_2 and the different signal states cannot be distinguished. If the signal states can be distinguished from the decoy states, Eve can exploit the PNS attack without detection. If the signal states cannot be distinguished from the decoy states, Eve can attenuate the states in the quantum channel.

In order to perform a better simulation, we then study the effects of weak randomness for different finite number of total pulses N. We define $p_1 = p_2 = 10^{-6}$ as the secret key rate with weak randomness influence and $p_1 = p_2 = 0$ as the secure key rate without weak randomness influence. The effects of weak randomness for the secure key rate with different $N = 10^x(x = 13, 14, 15, 16)$ are shown in Figure 2. Corresponding simulation results are shown in Figure 2, the solid lines from left to right are obtained for different total numbers of transmitting signals $N = 10^x(x = 13, 14, 15, 16)$ with the fixed weak randomness parameters $p_1 = p_2 = 0$ and the dashed lines from left to right are obtained for different finite number of total pulses $N = 10^x(x = 13, 14, 15, 16)$ with the fixed weak randomness parameters $p_1 = p_2 = 10^{-6}$. We can find that even though the weak randomness parameter is obtained as small as 10^{-6} , it will significantly affect the generation of the security key rate, which means that even small proportions of weak randomness can bring Eve a lot of information. As illustrated in Figure 2, because of Eve's attenuation operation, the greater the total numbers of transmitting signals, the greater the reduction of the secure transmission distance. The achievable transmission distance declines 17.89%, 15.38%, 10.97%, 5.88% when $N = 10^{16}, 10^{15}, 10^{14}, 10^{13}$, respectively.

Apparently, with the number of total pulse increases, so does the number of quantum states which may be attenuated. Eve may obtain more information due to the relation between the expected values and the observed values for the case with different modulated states in the practical QKD system. In this case, the number of modulated states distinguished by Eve may increase which leads to more leakage of the security key information so we are supposed to control the number of total pulses within a rational range rather than arbitrarily choosing.

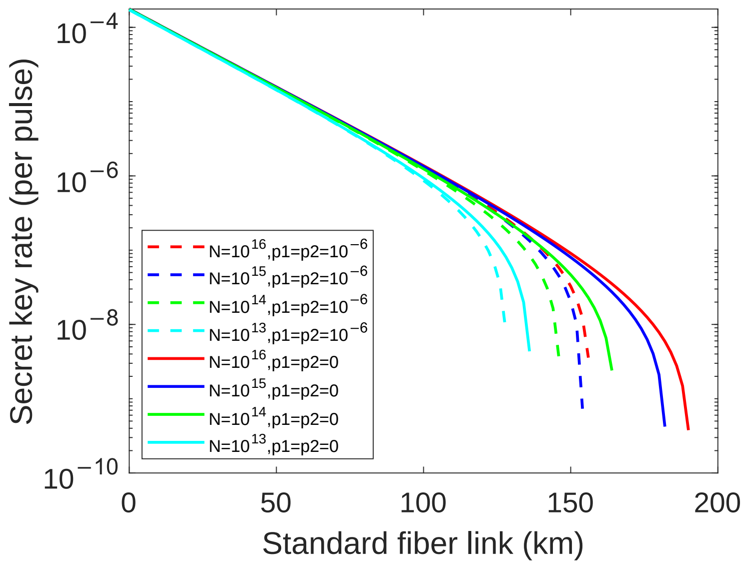

Figure 2. (Color online) The secret key rates (per pulse) in logarithmic scale versus transmission distance between Alice and Bob with weak randomness parameters $p_1 = p_2 = 0, 10^{-6}$ for different $N = 10^x(x = 13, 14, 15, 16)$ (curves from left to right). The dashed lines are results of $p_1 = p_2 = 10^{-6}$ for different N, and the solid lines are the results of $p_1 = p_2 = 0$ for different N.

To further research the effects of the weak randomness for different N, we consider the secure key rate for $N = 10^{15}, 10^{16}$ with different weak randomness parameters $p_1 = p_2 = 0, 10^{-x}(x = 6, 5, 4, 3)$ in Figure 3. As illustrated in Figure 3, the solid lines from right to left are obtained for different weak randomness parameters $p_1 = p_2 = 0, 10^{-x}(x = 6, 5, 4, 3)$ with the fixed finite number of total pulses $N = 10^{16}$ and the dashed lines from right to left are obtained for different weak randomness parameters $p_1 = p_2 = 0, 10^{-x}(x = 6, 5, 4, 3)$ with the fixed finite number of total pulses $N = 10^{15}$. We can discover that the security key rate of two different N lines are approximately asymptotic when the weak randomness parameters $p_1 = p_2 \geq 10^{-5}$, which means that the influence of the weak randomness on final security key rate is stronger than the finite number of total pulses. The security key rate of two different N lines are not asymptotic when the weak randomness parameters $p_1 = p_2 \leq 10^{-6}$, which means that the influence of the weak randomness on the final security key rate is weaker than the finite number of total pulses.

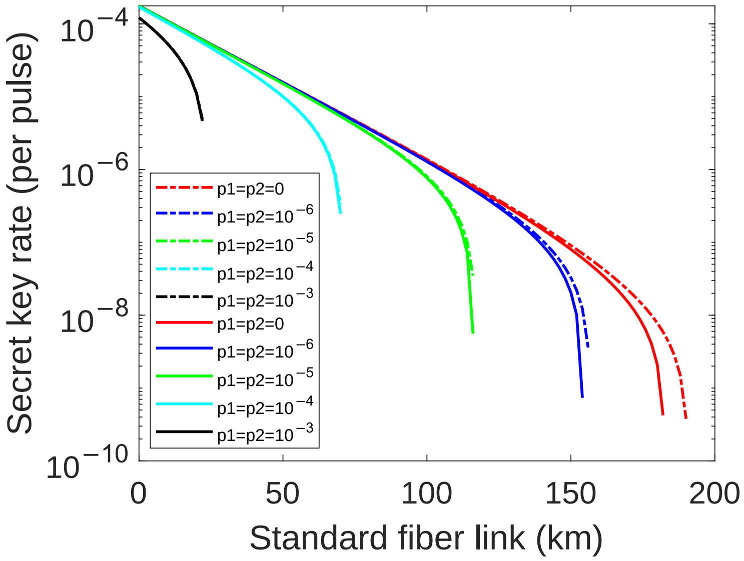

Figure 3. (Color online) The secret key rates (per pulse) in logarithmic scale versus transmission distance between Alice and Bob with $p_1 = p_2 = 0, 10^{-x}(x = 6, 5, 4, 3)$ (curves from right to left) for different $N = 10^{15}, 10^{16}$. The dashed lines are results of $N = 10^{16}$ with different weak randomness parameters, and the solid lines are the results of $N = 10^{15}$ with different weak randomness parameters.

From the above simulation results, we can deduce that the weak randomness has a non-negligible effect on the secret key rate of the MDI-QKD with finite resources, even though the weak randomness parameter is small. Moreover, the effects of the weak randomness on final security key rate may perform differently for the different finite number of total pulses.

5. Conclusions

In conclusion, we analyze the effects of weak randomness on the security key rate of MDI-QKD with finite resources, and demonstrate that MDI-QKD has high security demand of quantum state preparation. The MDI-QKD system generates fewer security keys and the achievable transmission distance declines from 182 km to 36 km when just one party exists the weak randomness p_1 which rises from 0 to 10^{-3}. The system can no longer generate a security key when $p_1(p_2) \geq 10^{-3}$. Considering the condition of finite resources, even though the weak randomness parameter is obtained as small as 10^{-6} or 10^{-5}, it will significantly affect the generation of the security key rate, which means that even small proportions of weak randomness can bring Eve a lot of information. Additionally, because of Eve's attenuation operation, the greater the total numbers of transmitting signals, the greater the reduction of the secure transmission distance where the achievable transmission distance declines 17.89%, 15.38%, 10.97%, 5.88% for $N = 10^{16}, 10^{15}, 10^{14}, 10^{13}$. Moreover, the influence of the weak randomness on the final security key rate is stronger than the total numbers of transmitting signals when $p_1, p_2 \geq 10^{-5}$, and the influence of the weak randomness on the final security key rate is weaker than total numbers of transmitting signals when $p_1, p_2 \leq 10^{-6}$.

Finally, we conclude that the practical decoy-state MDI-QKD system requires strict randomness in the state preparation. In order to avoid the weak randomness loopholes, two aspects can be seriously considered in the practical MDI-QKD system: the first one is to protect the true random numbers from information leakage to Eve, and the another one is that the state modulation apparatus are supposed to be carefully designed so that different modulated quantum states in the side of both Alice and Bob cannot be distinguished in all degrees of freedom. For example, the narrow spectral filter and the time filter can be applied in the practical experiment to reduce the distinguishability.

Author Contributions: Conceptualization, X.-L.J.; methodology, X.-L.J. and Y.W.; software, X.-L.J. and Y.W.; validation, X.-L.J. and X.-Q.D.; formal analysis, X.-L.J., Y.W. and Y.-F.L.; investigation, X.-L.J. and X.-Q.D.; writing—original draft preparation, X.-L.J., X.-Q.D. and Y.W.; writing—review and editing, C.Z., J.-J.L. and W.-S.B.; supervision, W.-S.B.; project administration, W.-S.B.; funding acquisition, W.-S.B. and Y.W. All authors have read and agreed to the published version of the manuscript.

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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

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, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
3. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
4. Sun, S.; Huang, A. A Review of Security Evaluation of Practical Quantum Key Distribution System. *Entropy* **2022**, *24*, 260. [CrossRef] [PubMed]
5. Li, H.W.; Wang, S.; Huang, J.Z.; Chen, W.; Yin, Z.Q.; Li, F.Y.; Zhou, Z.; Liu, D.; Zhang, Y.; Guo, G.C.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **2011**, *84*, 062308. [CrossRef]
6. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
7. Qian, Y.J.; He, D.Y.; Wang, S.; Chen, W.; Yin, Z.Q.; Guo, G.C.; Han, Z.F. Robust countermeasure against detector control attack in a practical quantum key distribution system. *Optica* **2019**, *6*, 1178–1184. [CrossRef]
8. Jain, N.; Anisimova, E.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **2014**, *16*, 123030. [CrossRef]
9. Lucamarini, M.; Choi, I.; Ward, M.B.; Dynes, J.F.; Yuan, Z.; Shields, A.J. Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X* **2015**, *5*, 031030. [CrossRef]
10. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
11. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
12. Xie, Y.M.; Lu, Y.S.; Weng, C.X.; Cao, X.Y.; Jia, Z.Y.; Bao, Y.; Wang, Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference. *PRX Quantum* **2022**, *3*, 020315. [CrossRef]
13. Pirandola, S.; Laurenza, R.; Ottaviani, C. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef] [PubMed]

14. Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, Y.H.; Chen, S.J.; Mao, Y.; Huang, M.Q.; Zhang, W.J.; et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef] [PubMed]
15. Wang, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optica* **2017**, *4*, 1016–1023. [CrossRef]
16. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
17. Liu, H.; Wang, J.; Ma, H.; Sun, S. Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration. *Optica* **2018**, *5*, 902–909. [CrossRef]
18. Liu, H.; Wang, W.; Wei, K.; Fang, X.T.; Li, L.; Liu, N.L.; Liang, H.; Zhang, S.J.; Zhang, W.; Li, H.; et al. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. *Phys. Rev. Lett.* **2019**, *122*, 160501. [CrossRef]
19. Wei, K.; Li, W.; Tan, H.; Li, Y.; Min, H.; Zhang, W.J.; Li, H.; You, L.; Wang, Z.; Jiang, X.; et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **2020**, *10*, 031030. [CrossRef]
20. Woodward, R.I.; Lo, Y.; Pittaluga, M.; Minder, M.; Paraïso, T.; Lucamarini, M.; Yuan, Z.; Shields, A. Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers. *Npj Quantum Inf.* **2021**, *7*, 58. [CrossRef]
21. Zhang, X.; Wang, Y.; Jiang, M.; Lu, Y.; Li, H.; Zhou, C.; Bao, W. Phase-Matching Quantum Key Distribution with Discrete Phase Randomization. *Entropy* **2021**, *23*, 508. [CrossRef]
22. Hu, X.L.; Jiang, C.; Yu, Z.W.; Wang, X.B. Practical Long-Distance Measurement-Device-Independent Quantum Key Distribution By Four-Intensity Protocol. *Adv. Quantum Technol.* **2021**, *4*, 2100069. [CrossRef]
23. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
24. Cui, C.; Yin, Z.Q.; Wang, R.; Chen, W.; Wang, S.; Guo, G.C.; Han, Z.F. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **2019**, *11*, 034053. [CrossRef]
25. Zhong, X.; Wang, W.; Qian, L.; Lo, H.K. Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses. *Npj Quantum Inf.* **2021**, *7*, 8. [CrossRef]
26. Fang, X.T.; Zeng, P.; Liu, H. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **2020**, *14*, 422–425. [CrossRef]
27. Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *Npj Quantum Inf.* **2019**, *5*, 64. [CrossRef]
28. Lu, Y.F.; Wang, Y.; Jiang, M.S.; Zhang, X.X.; Liu, F.; Li, H.W.; Zhou, C.; Tang, S.B.; Wang, J.Y.; Bao, W.S. Sending or Not-Sending Twin-Field Quantum Key Distribution with Flawed and Leaky Sources. *Entropy* **2021**, *23*, 1103. [CrossRef]
29. Pittaluga, M.; Minder, M.; Lucamarini, M.; Sanzaro, M.; Woodward, R.I.; Li, M.J.; Yuan, Z.; Shields, A.J. 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photonics* **2021**, *15*, 530–535. [CrossRef]
30. Liu, H.; Jiang, C.; Zhu, H.T.; Zou, M.; Yu, Z.W.; Hu, X.L.; Xu, H.; Ma, S.; Han, Z.; Chen, J.P.; et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Phys. Rev. Lett.* **2021**, *126*, 250502. [CrossRef]
31. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.J.; Han, Z.Y.; Ma, S.Z.; Hu, X.L.; Li, Y.H.; Liu, H.; et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photonics* **2021**, *15*, 570–575. [CrossRef]
32. Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Wang, R.Q.; Ye, P.; Zhou, Y.; Fan-Yuan, G.J.; Wang, F.X.; Zhu, Y.G.; et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **2022**, *16*, 154–161. [CrossRef]
33. Lu, F.Y.; Yin, Z.Q.; Wang, R.; Fan-Yuan, G.J.; Wang, S.; He, D.Y.; Chen, W.; Huang, W.; Xu, B.J.; Guo, G.C.; et al. Practical issues of twin-field quantum key distribution. *New J. Phys.* **2019**, *21*, 123030. [CrossRef]
34. Yin, Z.Q.; Fung, C.H.F.; Ma, X.; Zhang, C.M.; Li, H.W.; Chen, W.; Wang, S.; Guo, G.C.; Han, Z.F. Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **2013**, *88*, 062322. [CrossRef]
35. Pereira, M.; Kato, G.; Mizutani, A.; Curty, M.; Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **2020**, *6*, eaaz4487. [CrossRef]
36. Lu, Y.F.; Wang, Y.; Jiang, M.S.; Liu, F.; Zhang, X.X.; Bao, W.S. Finite-key analysis of sending-or-not-sending twin-field quantum key distribution with intensity fluctuations. *Quantum Inf. Process.* **2021**, *20*, 135. [CrossRef]
37. Mizutani, A.; Kato, G.; Azuma, K.; Curty, M.; Ikuta, R.; Yamamoto, T.; Imoto, N.; Lo, H.K.; Tamaki, K. Quantum key distribution with setting-choice-independently correlated light sources. *Npj Quantum Inf.* **2019**, *5*, 8. [CrossRef]
38. Zhang, X.X.; Wang, Y.; Jiang, M.S.; Zhou, C.; Lu, Y.F.; Bao, W.S. Finite-key analysis of asymmetric phase-matching quantum key distribution with unstable sources. *J. Opt. Soc. Am. B* **2021**, *38*, 724–731. [CrossRef]
39. Li, H.W.; Yin, Z.Q.; Wang, S.; Qian, Y.J.; Chen, W.; Guo, G.C.; Han, Z.F. Randomness determines practical security of BB84 quantum key distribution. *Sci. Rep.* **2015**, *5*, 16200. [CrossRef]
40. Li, H.W.; Xu, Z.M.; Cai, Q.Y. Small imperfect randomness restricts security of quantum key distribution. *Phys. Rev. A* **2018**, *98*, 062325. [CrossRef]
41. Zhang, C.M.; Wang, W.B.; Li, H.W.; Wang, Q. Weak randomness impacts the security of reference-frame-independent quantum key distribution. *Opt. Lett.* **2019**, *44*, 1226–1229. [CrossRef]
42. Müller-Quade, J.; Renner, R. Composability in quantum cryptography. *New J. Phys.* **2009**, *11*, 085006. [CrossRef]

43. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef] [PubMed]
44. Curty, M.; Xu, F.; Cui, W.; Lim, C.C.W.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 3732. [CrossRef] [PubMed]
45. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307. [CrossRef]
46. Wang, Y.; Bao, W.S.; Zhou, C.; Jiang, M.S.; Li, H.W. Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources. *Phys. Rev. A* **2016**, *94*, 032335. [CrossRef]
47. Li, H.W.; Xu, Z.M.; Yin, Z.Q.; Cai, Q.Y. Security of practical quantum key distribution with weak-randomness basis selection. *Phys. Rev. A* **2020**, *102*, 022605. [CrossRef]
48. Zhou, C.; Bao, W.S.; Zhang, H.L.; Li, H.W.; Wang, Y.; Li, Y.; Wang, X. Biased decoy-state measurement-device-independent quantum key distribution with finite resources. *Phys. Rev. A* **2015**, *91*, 022313. [CrossRef]
49. Tang, Y.L.; Yin, H.L.; Chen, S.J.; Liu, Y.; Zhang, W.J.; Jiang, X.; Zhang, L.; Wang, J.; You, L.X.; Guan, J.Y.; et al. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **2014**, *113*, 190501. [CrossRef]
50. Wang, Y.; Bao, W.S.; Zhou, C.; Jiang, M.S.; Li, H.W. 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. [CrossRef]
51. Fung, C.H.F.; Ma, X.; Chau, H. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **2010**, *81*, 012318. [CrossRef]